Wolfgang K. Seiler

Zahlentheorie

Vorlesung an der Universität Mannheim
im Frühjahrssemester 2014

Dieses Skriptum entstel
geringer Verzögerung e
nen Fall mit einem Leh
bei dieser Entstehensw
handelt es sich wohl le
sondern auch um Fehler
Teile aus anderen Skript
übernommen sind, ist
mogen.

Das Skriptum sollte d
trauen gegen seinen In
teilen Sie mir dies bitte
mannheim.de) mit. Auc
finden, bin ich für entsp

Falls genügend viele H
Listen mit Berichtigun
der online Version werd

Biographische Angaben
den entsprechenden A
ics archive (www-histo
auch die meisten abge
Mathematikern bezog i
ternetauftritt.

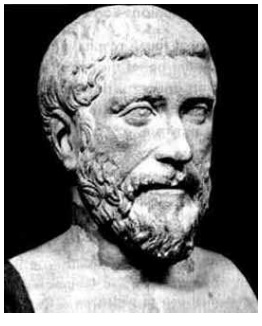
Kapitel 1
Ganze Zahlen und ihre Primzerlegung

§1: Rationale und irrationale Zahlen

Die Zahlentheorie beschäftigt sich, wie schon ihr Name sagt, mit Zahlen. Nun würde allerdings eine Umfrage wohl ergeben, daß sich nach Ansicht eines Großteils der Bevölkerung die gesamte Mathematik mit Zahlen beschäftigt – auch wenn beispielsweise im neunbändigen Analysislehrbuch von JEAN DIEUDONNÉ abgesehen von den dreiteiligen Abschnittsnummern praktisch keine Zahlen außer 0, 1 und 2 vorkommen.

Die Zahlentheorie unterscheidet sich dadurch von anderen Teilen der Mathematik, daß es dort vor allem um *ganze* Zahlen geht, oft sogar einfach um die natürlichen Zahlen $1, 2, 3, \ldots$. Die frühe griechische Philosophie der Pythagoräer beispielsweise stand unter dem Motto *Alles ist Zahl.* Sie konnten die musikalischen Harmonien auf einfache Verhältnisse natürlicher Zahlen zurückführen und waren überzeugt, daß dies auch für alle anderen Proportionen galt.

Umso größer war der Schock, als um 450 v.Chr. einer von ihnen, wahrscheinlich HIPPASSOS VON METAPONT, herausfand, daß es in der Geometrie Längenverhältnisse gibt, die sich *nicht* so beschreiben lassen. Schlimmer noch: Ein Beispiel dafür bietet ausgerechnet das Wahrzeichen der Pythagoräer, das Pentagramm. HIPPASSOS VON METAPONT nahm deshalb auch ein schlimmes Ende: Nach einigen Überlieferungen wurde er von den erzürnten Pythagoräern ertränkt, nach anderen ließen ihn die Götter als Strafe für seine Schandtat bei einem Schiffsuntergang ertrinken.



PYTHAG
Als ung
und gin
über Ma
von Dic
bildung
persisch
schaft u
er, um d
frei und
weiter r
und phi

Wir wollen uns hier mit einem ein
beschäftigen, dem Verhältnis zwi
nes Quadrats. In einem Quadrat
aufgefaßt werden als Hypotenuse
gen Dreiecks mit Katheten der L
des PYTHAGORAS (der tatsächlic
PYTHAGORAS sein dürfte) die Lä
ist $\sqrt{2}$.

Wäre $\sqrt{2}$ als Verhältnis a/b zwe
könnten wir ohne Beschränkung d
destens eine der beiden Zahlen a u
wir einfach so lange durch zwei k

Quadrieren wir beide Seiten der
die neue Gleichung $a^2/b^2 = 2$; d
Zahl sein. Damit müßte aber auch
ungerade, so auch $a^2 = 2 \cdot (2c^2 +$
ist, ist $a^2 = 2b^2$ durch vier teilba
gerade, ein Widerspruch. Somit is

Auch das Verhältnis zwischen U
ses, für das wir heute die Bezeich
allerdings erfordert der Beweis
ihn trotzdem hier vorstellen, denn
retische Aussagen teilweise nur a
Mathematik bewiesen werden k

dieser Umweg über die reelle Analysis:

Wir gehen zunächst aus von einem beliebigen Polynom $P(x)$ mit reellen Koeffizienten von einem geraden Grad $2n$. Dazu definieren wir das Polynom

$$Q(x) \underset{\text{def}}{=} P(x) - P''(x) + P^{(4)}(x) - \cdots + (-1)^n P^{(2n)}(x)$$

als die alternierende Summe der Ableitungen gerader Ordnung von P. Weiter betrachten wir die Funktion $S(x) = Q'(x)\sin x - Q(x)\cos x$; ihre Ableitung ist

$$\begin{aligned} S'(x) &= Q''(x)\sin x + Q'(x)\cos x - Q'(x)\cos x + Q(x)\sin x \\ &= \big(Q''(x) + Q(x)\big)\sin x\,. \end{aligned}$$

In $Q''(x) = P''(x) - P^{(4)}(x) + \cdots + (-1)^{n-1}P^{(2n)}(x)$ kommen bis auf $P(x)$ genau dieselben Terme vor wie in $Q(x)$, allerdings mit dem jeweils anderen Vorzeichen. Daher ist $Q''(x) + Q(x) = P(x)$ und $S(x) = Q'(x)\sin x - Q(x)\cos x$ ist eine Stammfunktion von $P(x)\sin x$. Damit folgt die

Formel von Hermite:

$$\int_0^\pi P(x)\sin x\,dx = S(\pi) - S(0) = Q(\pi) + Q(0)\,,$$

denn $\sin 0 = \sin\pi = 0$, $\cos 0 = 1$ und $\cos\pi = -1$.

Wir nehmen nun an, $\pi = a/b$ sei eine rationale Zahl, und wenden die gerade bewiesene Formel an auf das spezielle Polynom

$$P_n(x) \underset{\text{def}}{=} \frac{x^n(a-bx)^n}{n!}\,;$$

wir erhalten

$$I_n \underset{\text{def}}{=} \int_0^\pi P_n(x)\sin x\,dx = Q_n(\pi) + Q_n(0)$$

mit $Q_n(x) \underset{\text{def}}{=} P_n(x) - P_n''(x) + P_n^{(4)}(x) - \cdots + (-1)^n P_n^{(2n)}(x)$.

$P_n(x)$ ist im Intervall $(0,\,\pi)$ genau
daher ist auch $I_n > 0$. Außerdem

$P_n(\pi - x) = (\pi - x)^n\big(a - b(\pi -$

Das Maximum von P_n in $(0,\,\pi)$
wie das der Funktion $f(x) = x(a$
es sich dabei um die Intervallmit
dort ist

$$P_n\Big(\frac{a}{2b}\Big) = \frac{1}{n!}\Big($$

Schätzen wir das Integral ab du
Integranden, erhalten wir daher d

$$I_n \le$$

und sehen, daß I_n für $n \to \infty$ ge
als jede Potenz einer reellen Zahl

$$\lim_{n\to}$$

Andererseits ist aber $I_n = Q_n(0$
der Symmetrie von P_n einfach 2
daß alle $Q_n(0)$ ganze Zahlen sin
Ableitungen von $P_n(x)$ an der Ste
Nach der binomischen Formel ist

$$P_n(x) = \frac{x^n(a-bx)^n}{n!} =$$

die k-te Ableitung verschwindet
$k = n + i \ge n$ ist

$$P_n^{(k)}(0) = \frac{1}{n!}\Big($$

ebenfalls eine ganze Zahl, da der
ansonsten nur ganze Zahlen daste

Somit ist also I_n für jedes $n \in \mathbb{N}$
einer Folge positiver ganzer Zah

also führt die Annahme, $\pi = a/b$ sei eine rationale Zahl, zu einem Widerspruch, der die Irrationalität von π zeigt.

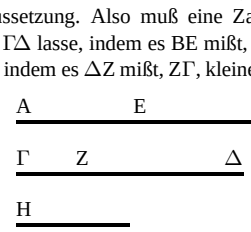
Wenn man schon dabei ist, kann man leicht auch noch viele andere wichtige Zahlen als irrational erkennen; auf dem ersten Übungsblatt ist ein Beweis für die Irrationalität der EULERschen Zahl e skizziert, und mit nur wenig mehr Aufwand als im Fall der Quadratwurzel aus zwei läßt sich auch leicht zeigen, daß *jede* Quadratwurzel einer natürlichen Zahl entweder ganzzahlig oder irrational ist. Dasselbe gibt für höhere Wurzeln und sogar für Nullstellen aller Polynome mit ganzzahligen Koeffizienten und höchstem Koeffizient eins, allerdings brauchen wir zum Beweis einen Satz, den zwar fast jeder kennt, dessen Beweis man aber nur selten sieht: Die eindeutige Primzerlegung der natürlichen Zahlen. Der Beweis dieses Satzes wiederum verwendet eine Konstruktion, die wahrscheinlich bereits den Pythagoräern bekannt war und die wir heute als EUKLIDischen Algorithmus bezeichnen. Wie sich zeigen wird, ist er zusammen mit einer ganzen Reihe von Varianten ein nicht nur in der Zahlentheorie allgegenwärtiges Werkzeug; es lohnt sich also, ihn gleich jetzt zum Beginn der Vorlesung etwas ausführlicher zu betrachten.

§2: Der Euklidische Algorithmus

Bei EUKLID, in Proposition 2 des siebten Buchs seiner *Elemente,* wird er (in der Übersetzung von CLEMENS THAER in Oswalds Klassikern der exakten Wissenschaft) so beschrieben:

> *Zu zwei gegebenen Zahlen, die nicht prim gegeneinander sind, ihr größtes gemeinsames Maß zu finden.*
>
> Die zwei gegebenen Zahlen, die nicht prim, gegeneinander sind, seien AB, ΓΔ. Man soll das größte gemeinsame Maß von AB, ΓΔ finden.
>
>
>
>
> Wenn ΓΔ hier AB mißt – sich selbst mißt es auch – dann ist ΓΔ gemeinsames Maß von ΓΔ, AB. Und es ist klar, daß es auch das größte ist, denn keine Zahl größer ΓΔ kann ΓΔ messen.
>
> Wenn ΓΔ aber AB nicht mißt, und man nimmt bei AB, ΓΔ abwechselnd immer das kleinere vom größeren weg, dann muß (schließlich) eine Zahl

übrig bleiben, die die vorangehend
übrig bleiben; sonst müßten AB,
Voraussetzung. Also muß eine Za
mißt. ΓΔ lasse, indem es BE mißt,
lasse, indem es ΔZ mißt, ZΓ, kleine



Da ΓZ AE mißt und AE ΔZ, muß
sich selbst, muß also auch das Ganz
ΓZ auch BE; es mißt aber auch EA
Und es mißt auch ΓΔ; ΓZ mißt als
Maß von AB, ΓΔ. Ich behaupte, d
ΓZ nicht das größte gemeinsame
Zahl größer ΓZ die Zahlen AB u
sei H. Da H dann ΓΔ mäße und ΓΔ
auch das Ganze BA messen, müßte
aber ΔZ; also müßte H auch ΔZ
messen, müßte also auch den Rest
dies ist unmöglich. Also kann kein
messen; ΓZ ist also das größte gem
beweisen sollen.

Aus heutiger Sicht erscheint hier d
Größen nicht teilerfremd sein dü
daß in der griechischen Philosop
Sonderrolle einnahm und nicht a
begannen erst mit der Zwei. Dem
sition 1 des siebten Buchs fast wö
den Fall von teilerfremden Größe
auch in Griechenland als Zahl an
terscheidung ohnehin bedeutung
der ggT ungleich eins sein soll, a

Das dem EUKLIDischen Algorit
Wechselwegnahme oder wechsel
chischen Mathematik spätestens
chen Jahrhunderts bereits wohlb

sis (ἀνταναιρεσις) oder auch Anthyphairesis (ἀνθυφαιρεσις), und auch der Algorithmus selbst geht mit ziemlicher Sicherheit, wie so vieles in den Elementen, *nicht* erst auf EUKLID zurück: Seine *Elemente* waren das wohl mindestens vierte Buchprojekt dieses Namens, und alles spricht dafür, daß er vieles von seinen Vorgängern übernommen hat. Seine Elemente waren dann aber mit Abstand die erfolgreichsten, so daß die anderen in Vergessenheit gerieten und verloren gingen; EUKLID wurde schließlich als *der* Stoichist bekannt nach dem griechischen Titel στοιχεῖα der Elemente.

Es ist nicht ganz sicher, ob EUKLID (Εὐκλειδης) wirklich gelebt hat; es ist möglich, wenn auch sehr unwahrscheinlich, daß EUKLID nur ein Pseudonym für eine Autorengruppe ist. (Das nebenstehende Bild aus dem 18. Jahrhundert ist reine Phantasie.) EUKLID ist vor allem bekannt als Autor der *Elemente*, in denen er die Geometrie seiner Zeit systematisch darstellte und (in gewisser Weise) auf wenige Definitionen sowie die berühmten fünf Postulate zurückführte; sie entstanden um 300 v. Chr. EUKLID arbeitete wohl am Museion in Alexandrien; außer den Elementen schrieb er ein Buch über Optik und weitere, teilweise verschollene Bücher.

Wenn wir nicht mit Zirkel und Lineal arbeiten, sondern rechnen, können wir die mehrfache „Wegnahme“ einer Strecke von einer anderen einfacher beschreiben durch eine Division mit Rest: Sind a und b die (als natürliche Zahlen vorausgesetzten) Längen der beiden Strecken und ist $a : b = q$ Rest r, so kann man q mal die Strecke b von a wegnehmen; was übrig bleibt ist eine Strecke der Länge $r < b$.

EUKLIDs Konstruktion wird dann zu folgendem Algorithmus für zwei natürliche Zahlen a, b:

Schritt 0: Setze $r_0 = a$ und $r_1 = b$.

Schritt i, $i \geq 1$**:** Falls r_i verschwindet, endet der Algorithmus mit $\mathrm{ggT}(a, b) = r_{i-1}$; andernfalls sei r_{i+1} der Rest bei der Division von r_{i-1} durch r_i.

EUKLID behauptet, daß dieser Algorithmus stets endet und daß das Ergebnis der größte gemeinsame Teiler der Ausgangszahlen a, b ist, d.h. die größte natürliche Zahl, die sowohl a als auch b teilt.

Da der Divisionsrest r_{i+1} stets e
und eine Folge immer kleiner we
notwendigerweise nach endlich v
der Algorithmus in der Tat stets en
endet, ist ebenfalls leicht zu sehe

$$r_{i-1} = q_i r_i + r_{i+1}$$

so daß jeder gemeinsame Teiler v
ist und umgekehrt jeder gemeins
teilt. Somit haben r_i und r_{i-1}
und r_{i+1}, insbesondere haben sie d
Durch Induktion folgt, daß in je
ist. Im letzten Schritt ist $r_i = 0$; d
ist, ist dann $r_{i-1} = \mathrm{ggT}(r_i, r_{i-1})$

§3: Der erweiterte Euklid

Mehr als zwei Tausend Jahre na
sis und EUKLIDischem Algorithm
BACHET DE MÉZIRIAC in der zwe
plaisants et délectables qui se fo
folgende:

Il y a 41 personnes en un banqu
qui en tout dépensent 40 sous, ma
femme 3 sous, chaque enfant 4
d'hommes, combien de femmes, c

(Bei einem Bankett sind 41 Pers
zusammen vierzig Sous ausgeben
Frau drei Sous und jedes Kind 4
wie viele Frauen und wie viele K

Sobald man weiß, daß zwölf De
ein Pfund), kann man dies in ein l
Ist x die Zahl der Männer, y die
muß gelten $x + y + z = 41$ und $4x$

Im Gegensatz zum Fall der in Schule und Linearer Algebra betrachteten Gleichungssystemen kommen hier natürlich nur natürliche Zahlen als Lösungen in Frage.

CLAUDE GASPAR BACHET SIEUR DE MÉZIRIAC (1581-1638) verbrachte den größten Teil seines Lebens in seinem Geburtsort Bourg-en-Bresse. Er studierte bei den Jesuiten in Lyon und Milano und trat 1601 in den Orden ein, trat aber bereits 1602 wegen Krankheit wieder aus und kehrte nach Bourg zurück. Sein Buch erschien 1612; 1959 brachte der Verlag Blanchard eine vereinfachte Ausgabe heraus. Am bekanntesten ist BACHET für seine lateinische Übersetzung der *Arithmetika* von DIOPHANTOS. In einem Exemplar davon schrieb FERMAT seine Vermutung an den Rand. Auch Gedichte von BACHET sind erhalten. 1635 wurde er Mitglied der französischen Akademie der Wissenschaften.

Zur Lösung kann man zunächst die erste Gleichung nach z auflösen und in die zweite Gleichung einsetzen; dies führt auf die Gleichung

$$\frac{11}{3}x + \frac{8}{3}y = \frac{79}{3} \quad \text{oder} \quad 11x + 8y = 79\,.$$

Bei einer solchen Gleichung ist *a priori* nicht klar, ob es überhaupt Lösungen gibt: Die Gleichung $10x + 8y = 79$ beispielsweise kann keine haben, denn für ganze Zahlen x, y ist $10x + 8y$ stets gerade. Allgemein kann $ax + by = c$ höchstens dann ganzzahlige Lösungen haben, wenn der ggT von a und b Teiler von c ist.

BACHET DE MÉZIRIAC hat bewiesen, daß sie in diesem Fall auch stets Lösungen hat; das Kernstück dazu ist seine Proposition XVIII, wo er zu zwei teilerfremden Zahlen a, b ganze Zahlen x, y konstruiert, für die $ax - by = 1$ ist: *Deux nombres premiers entre eux estant donnéz, treuuer le moindre multiple de chascun d'iceux, surpassant de l'unité un multiple de l'autre.* Die Methode ist eine einfache Erweiterung des EUKLIDischen Algorithmus, und genau wie letzterer nach EUKLID benannt ist, da ihn dieser rund 150 Jahre nach seiner Entdeckung in seinem Lehrbuch darstellte, heißt auch BACHETs Satz heute *Identität von* BÉZOUT, weil dieser ihn 142 Jahre später, im Jahre 1766, in seinem Lehrbuch beschrieb (und auf Polynome verallgemeinerte).

ETIENN
Ile-de-F
waren.
senscha
menstel
Im 176
Cours d
lon et d
stellt. S
ins Eng
vard ber
durch s
n und r

Zur Lösung von Problemen wie d
gemein den größten gemeinsame
bination dieser Zahlen darstellen
des EUKLIDischen Algorithmus n
vom erweiterten EUKLIDischen A

Die Gleichung

$$r_{i-1} =$$

läßt sich umschreiben als

$$r_{i+1} =$$

so daß r_{i+1} eine ganzzahlige Line
entsprechend auch r_i Linearkom
induktiv, daß der ggT von a und
von a und b dargestellt werden ka

Algorithmisch sieht dies folgende

Schritt 0: Setze $r_0 = a$, $r_1 = b$, c
ist dann

$$r_{i-1} = \alpha_{i-1}a + \beta_{i-}$$

Im i-ten Schritt werden neue Zal
chungen auch für $i + 1$ gelten:

Schritt i, $i \geq 1$**:** Falls r_i verschw

$$\text{ggT}(a, b) = r_{i-}$$

Andernfalls dividiere man r_{i-1} durch r_i; der Divisionsrest sei r_{i+1}. Dann ist

$$\begin{aligned} r_{i+1} = r_{i-1} - q_i r_i &= (\alpha_{i-1}a + \beta_{i-1}b) - q_i(\alpha_i a + \beta_i b) \\ &= (\alpha_{i-1} - q_i\alpha_i)a + (\beta_{i-1} - q_i\beta_i)b\,; \end{aligned}$$

die gewünschten Gleichungen gelten also für

$$\alpha_{i+1} = \alpha_{i-1} - q_i\alpha_i \quad \text{und} \quad \beta_{i+1} = \beta_{i-1} - q_i\beta_i\,.$$

Genau wie oben folgt, daß der Algorithmus für alle natürlichen Zahlen a und b endet und daß am Ende der richtige ggT berechnet wird; außerdem sind die α_i und β_i so definiert, daß in jedem Schritt $r_i = \alpha_i a + \beta_i b$ ist, insbesondere wird also im letzten Schritt der ggT als Linearkombination der Ausgangszahlen dargestellt.

Als Beispiel wollen wir den ggT von 200 und 148 als Linearkombination darstellen. Im nullten Schritt haben wir 200 und 148 als die trivialen Linearkombinationen

$$200 = 1 \cdot 200 + 0 \cdot 148 \quad \text{und} \quad 148 = 0 \cdot 200 + 1 \cdot 148\,.$$

Im ersten Schritt dividieren wir, da 148 nicht verschwindet, 200 mit Rest durch 148:

$$200 = 1 \cdot 148 + 52 \quad \text{und} \quad 52 = 1 \cdot 200 - 1 \cdot 148\,.$$

Da auch $52 \neq 0$, dividieren wir im zweiten Schritt 148 durch 52:

$148 = 2 \cdot 52 + 44$ und $44 = 148 - 2 \cdot (1 \cdot 200 - 1 \cdot 148) = 3 \cdot 148 - 2 \cdot 200$.

Auch $44 \neq 0$; wir machen also weiter: $52 = 1 \cdot 44 + 8$ und

$8 = 52 - 44 = (1 \cdot 200 - 1 \cdot 148) - (3 \cdot 148 - 2 \cdot 200) = 3 \cdot 200 - 4 \cdot 148$.

Im nächsten Schritt erhalten wir $44 = 5 \cdot 8 + 4$ und

$4 = 44 - 5 \cdot 8 = (3 \cdot 148 - 2 \cdot 200) - 5 \cdot (3 \cdot 200 - 4 \cdot 148) = 23 \cdot 148 - 17 \cdot 200$.

Bei der Division von acht durch vier schließlich ist der Divisionsrest null; damit ist $4 = 23 \cdot 148 - 17 \cdot 200$ der ggT von 148 und 200.

Zur Lösung des Problems von BACHET müssen wir die Gleichung $11x + 8y = 79$ betrachten. Dazu stellen wir zunächst den ggT von 11 und 8 als Linearkombination dieser Zahlen dar.

Elf durch acht ist eins Rest drei, a

Im nächsten Schritt dividieren wir
Rest zwei, also ist $2 = 1 \cdot 8 - 2 \cdot 3$ =

Im letzten Schritt wird daher dre
erstens, daß der ggT gleich eins ist
zweitens, daß gilt $1 = 3 - 2 = (1 \cdot 1$

Damit haben wir auch eine Dars
von elf und acht:

$$79 = 79 \cdot (3 \cdot 11 - 4$$

Dies ist allerdings nicht die gesuc
nicht an 237 Männer, -316 Frau

Nun ist aber die obige Gleichun
Möglichkeit zur Darstellung der
und elf: Da $8 \cdot 11 - 11 \cdot 8$ verschw
faches dieser Gleichung dazuadd
Lösung

$$(3 + 8k) \cdot 11 -$$

Entsprechend können wir auch e
chung zur Darstellung von 79 add

$$79 = (237 + 8k)$$

Wir müssen k so wählen, daß sow
als auch die Anzahl $-(316 + 11$
nicht negativ wird, d.h. $-\frac{237}{8} \leq$
kommt nur $k = -29$ in Frage; es
und dazu noch $41 - 5 - 3 = 33$ K
sich in der Tat auf $5 \cdot 4 + 3 \cdot 3 + 3$

Entsprechend kann der erweiterte
anderer diophantischer Gleichung
gen also, bei denen nur ganzzah
trachten hier nur die lineare Glei
zwei Unbekannte $x, y \in \mathbb{Z}$.

Der größte gemeinsame Teiler $d = \text{ggT}(a, b)$ von a und b teilt offensichtlich jeden Ausdruck der Form $ax + by$ mit $x, y \in \mathbb{Z}$; falls d kein Teiler von c ist, kann es also keine ganzzahlige Lösung geben.

Ist aber $c = rd$ ein Vielfaches von d und ist $d = \alpha a + \beta b$ die lineare Darstellung des ggT nach dem erweiterten EUKLIDischen Algorithmus, so haben wir mit $x = r\alpha$ und $y = r\beta$ offensichtlich eine Lösung gefunden.

Ist (x', y') eine weitere Lösung, so ist

$$a(x - x') + b(y - y') = c - c = 0 \quad \text{oder} \quad a(x - x') = b(y' - y)\,.$$

$v = a(x-x') = b(y'-y)$ ist also ein gemeinsames Vielfaches von a und b und damit auch ein Vielfaches des kleinsten gemeinsamen Vielfachen von a und b. Dieses kleinste gemeinsame Vielfache ist ab/d, es muß also eine ganze Zahl m geben mit

$$x - x' = m \cdot \frac{b}{d} \quad \text{und} \quad y' - y = m \cdot \frac{a}{d}\,.$$

Die allgemeine Lösung der obigen Gleichung ist somit

$$x = r\alpha - m \cdot \frac{b}{d} \ \text{ und } \ y = r\beta + m \cdot \frac{a}{d} \quad \text{mit} \quad m \in \mathbb{Z}\,.$$

§4: Der Aufwand des Euklidischen Algorithmus

Im Beweis, daß der EUKLIDische Algorithmus stets nach endlich vielen Schritten abbricht, hatten wir argumentiert, daß der Divisionsrest stets kleiner ist als der Divisor, so daß er irgendwann einmal null werden muß; dann endet der Algorithmus.

Damit haben wir auch eine obere Schranke für den Rechenaufwand zur Berechnung von $\text{ggT}(a, b)$: Wir müssen höchstens b Divisionen durchführen.

Das erscheint zwar auf den ersten Blick als ein recht gutes Ergebnis; wenn man aber bedenkt, daß der EUKLIDische Algorithmus heute in der Kryptographie auf über 600-stellige Zahlen angewendet wird, verliert diese Schranke schnell ihre Nützlichkeit: Da unser Universum ein geschätztes Alter von zehn Milliarden Jahren, also ungefähr $3 \cdot 10^{18}$ Sekunden hat, ist klar, d
puter, der zu Beginn des Univers
einen verschwindend kleinen Bru
hätte. Wäre 10^{600} eine realistisch
an eine Anwendung des EUKLI
Zahlen nicht einmal denken.

Tatsächlich ist 10^{600} aber natürlic
bislang noch nicht wissen, wie re
den, suchen wir die kleinsten nati
nen notwendig sind; dies wird un
13. Jahrhundert führen.

Im Falle $n = 1$ sind offensichtl
Zahlen; wenn $a = b$ ist, kommt
aus.

Dies ist allerdings ein eher untypi
rekursiv verallgemeinern läßt, d
KLIDischen Algorithmus ist der I
Ersterer ist schließlich der Rest b
letzterer der Divisor. Die kleinste
mit nur einer Division auskommt

Als nächstes suchen wir die kleins
notwendig sind. Ist r der Rest b
zweite Division. Für diese muß r
wobei q der Quotient bei der erst
eins, die kleinstmöglichen Werte

$$r = 1, \quad b = 2$$

Allgemeiner seien a_n und b_n die
notwendig sind, und r sei der Rest
Division $b : r$ ist dann $b_n \geq a_{n-}$
Werte sind damit

$r = b_{n-1}, \quad b_n = a_{n-1}$ und a_n

Da wir $a_1 = 2$ und $b_1 = 1$ kenn
berechnen; was wir erhalten, sind

Sie sind durch folgende Rekursionsformel definiert:

$$F_0 = 0, \qquad F_1 = 1 \qquad \text{und} \qquad F_n = F_{n-1} + F_{n-2} \quad \text{für } n \geq 2\,.$$

FIBONACCI führte sie ein, um die Vermehrung einer Karnickelpopulation durch ein einfaches Modell zu berechnen. In seinem 1202 erschienenen Buch *Liber abaci* schreibt er:

Ein Mann bringt ein Paar Karnickel auf einen Platz, der von allen Seiten durch eine Mauer umgeben ist. Wie viele Paare können von diesem Paar innerhalb eines Jahres produziert werden, wenn man annimmt, daß jedes Paar jeden Monat ein neues Paar liefert, das vom zweiten Monat nach seiner Geburt an produktiv ist?

LEONARDO PISANO (1170–1250) ist heute vor allem unter seinem Spitznamen FIBONACCI bekannt; gelegentlich nannte er sich auch BIGOLLO, auf Deutsch *Tunichtgut* oder *Reisender.* Er ging in Nordafrika zur Schule, kam aber 1202 zurück nach Pisa. Seine Bücher waren mit die ersten, die die indisch-arabischen Ziffern in Europa einführten. Er behandelt darin nicht nur Rechenaufgaben für Kaufleute, sondern auch zahlentheoretische Fragen, beispielsweise daß man die Quadratzahlen durch Aufaddieren der ungeraden Zahlen erhält. Auch betrachtet er nichtlineare Gleichungen, die er approximativ löst, und erinnert an viele in Vergessenheit geratene Ergebnisse der antiken Mathematik.

Wie wir gerade gesehen haben, kann man mit den FIBONACCI-Zahlen nicht nur Karnickelpopulationen beschreiben, sondern – wie GABRIEL LAMÉ 1844 entdeckte – auch eine Obergrenze für den Aufwand beim EUKLIDischen Algorithmus angeben:

Satz von Lamé (1844)**:** Die kleinsten natürlichen Zahlen a, b, für die beim EUKLIDischen Algorithmus $n \geq 2$ Divisionen benötigt werden, sind $a = F_{n+2}$ und $b = F_{n+1}$. ∎

(Für $n = 1$ gilt der Satz nur, wenn wir zusätzlich voraussetzen, daß $a \neq b$ ist; für $n \geq 2$ ist dies automatisch erfüllt.)

GABRIE
1817 M
bis 182
Mines.
Rußlan
nieur u
sik, Ch
erhielt e
techniq
sik und
1836/37
Paris-V

Um die Zahlen F_n durch eine gese
wir (genau wie man es auch für di
tun würde) die Definitionsgleichu

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = A \begin{pmatrix} F_n \\ F_{n-} \end{pmatrix}$$

schreiben; dann ist

$$\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = A^{n-1}$$

Das charakteristische Polynom v

$$\det(A - \lambda E) = (1 -$$

die Eigenwerte von A sind dahe
Matrix, deren Spalten aus den zug
also $A = B^{-1} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} B$ und

$$\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = A^{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} =$$

Auch ohne die Matrix B zu bere
in der Form $F_n = a\lambda_1^{n-1} + b\lambda_2^{n-1}$
und b durch λ_2 dividieren, erhalte
$F_a = a\lambda_1^n + b\lambda_2^n$, deren Koeffizi
und $n = 1$ bestimmen können:

$$F_0 = 1 = a\lambda_1^0 + b\lambda_2^0 = a +$$

Damit ist $b = 1 - a$, und die zweite Gleichung wird zu

$$a(\lambda_1 - \lambda_2) + \lambda_2 = a\sqrt{5} + \lambda_2 = 1 \Longrightarrow a = \frac{1-\lambda_2}{\sqrt{5}} = \frac{\lambda_1}{\sqrt{5}}\,.$$

Also ist $b = 1 - a = -\dfrac{\lambda_2}{\sqrt{5}}$ und $F_n = \dfrac{\lambda_1^n - \lambda_2^n}{\sqrt{5}}$.

Numerisch ist

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \approx 1{,}618034, \quad \lambda_2 = 1 - \lambda_1 = \frac{1-\sqrt{5}}{2} \approx -0{,}618034$$

und $\sqrt{5} \approx 2{,}236068$; der Quotient $\lambda_2^n/\sqrt{5}$ ist also für jedes n kleiner als $1/2$. Daher können wir F_n auch einfacher berechnen als nächste ganze Zahl zu $\lambda_1^n/\sqrt{5}$. Insbesondere folgt, daß F_n exponentiell mit n wächst.

Die Gleichung $\lambda^2 - \lambda - 1 = 0$ läßt sich umschreiben als $\lambda(\lambda - 1) = 1$ oder $\lambda : 1 = 1 : (\lambda - 1)$. Diese Gleichung charakterisiert den *goldenen Schnitt:* Stehen zwei Strecken a und b in diesem Verhältnis, so auch die beiden Strecken b und $a - b$. Die positive Lösung λ_1 wird traditionell mit dem Buchstaben ϕ bezeichnet; F_n ist also der zur nächsten ganzen Zahl gerundete Wert von $\phi^n/\sqrt{5}$.

Die beiden kleinsten Zahlen, für die wir n Divisionen brauchen, sind nach LAMÉ $a = F_{n+2}$ und $b = F_{n+1}$. Aus der geschlossenen Formel für die FIBONACCI-Zahlen folgt

$$\begin{aligned} n &\approx \log_\phi \sqrt{5}\, b - 1 = \log_\phi b + \log_\phi \sqrt{5} - 1 = \frac{\ln b}{\ln \phi} + \frac{\ln \sqrt{5}}{\ln \phi} - 1 \\ &\approx 2{,}078 \ln b + 0{,}672\,. \end{aligned}$$

Für beliebige Zahlen $a > b$ können nicht mehr Divisionen notwendig sein als für die auf b folgenden nächstgrößeren FIBONACCI-Zahlen, also gibt obige Formel für jedes b eine obere Grenze. Die Anzahl der Divisionen wächst daher nicht (wie oben bei der naiven Abschätzung) wie b, sondern höchstens wie $\log b$. Für sechshundertstellige Zahlen a, b müssen wir daher nicht mit 10^{600} Divisionen rechnen, sondern mit weniger als drei Tausend, was auch mit weniger leistungsfähigen Computern problemlos und schnell möglich ist.

Tatsächlich gibt natürlich auch di
den tatsächlichen Aufwand wiede
weniger auskommen. Im übrigen
den ggT auf andere Weise nicht
können. Da wir aber für Zahlen
Anwendungen interessieren, selb
sten Fall ganz gut leben können,
eingegangen. Interessenten finde
4.5.2+3 des Buchs
DONALD E. KNUTH: The Art of Co
merical Algorithms, *Addison-Wes*

§5: Die multiplikative Stru

Eine Primzahl ist bekanntlich ei
Teiler hat, nämlich die Eins und s
Algorithmus liefert eine wichtige

Lemma: Wenn eine Primzahl da
teilt, teilt sie mindestens einen de

Beweis: Angenommen, die Primz
Da der ggT von a und p Teiler vo
drungen gleich eins sein; es gibt

$$1 = \alpha a + \beta p$$

Dann ist $b = \alpha ab + \beta pb$ durch p
sind Vielfache von p.

Daraus folgt induktiv

Satz: Jede natürliche Zahl läßt s
ein Produkt von Primzahlpotenze

Beweis: Wir zeigen zunächst, da
als Produkt von Primzahlpotenz
Fall wäre, gäbe es ein minimale

die Eins sein, denn die ist ja das leere Produkt, und es kann auch keine Primzahl sein, denn die ist ja das Produkt mit sich selbst als einzigem Faktor. Somit hat M einen echten Teiler N, d.h. $1 < N < M$. Da M das minimale Gegenbeispiel war, lassen sich N und $\frac{M}{N}$ als Produkte von Primzahlpotenzen schreiben, also auch $M = N \cdot \frac{M}{N}$.

Bleibt noch zu zeigen, daß die Produktdarstellung bis auf die Reihenfolge der Faktoren eindeutig ist. Auch hier gäbe es andernfalls wieder ein minimales Gegenbeispiel M, das somit mindestens zwei verschiedene Darstellungen

$$M = \prod_{i=1}^{r} p_i^{e_i} = \prod_{j=1}^{s} q_j^{f_j}$$

hätte. Da die Eins durch kein Produkt dargestellt werden kann, in dem wirklich eine Primzahl vorkommt, ist $M > 1$, und somit steht in jedem der beiden Produkte mindestens eine Primzahl.

Da p_1 Teiler von M ist, teilt es auch das rechtsstehende Produkt, also nach dem gerade bewiesenen Lemma mindestens einen der Faktoren, d.h. mindestens ein q_j. Da q_j eine Primzahl ist, muß dann $p_1 = q_j$ sein. Da M als minimales Gegenbeispiel vorausgesetzt war, unterscheiden sich die beiden Produkte, aus denen dieser gemeinsame Faktor gestrichen wurde, höchstens durch die Reihenfolge der Faktoren, und damit gilt dasselbe für die beiden Darstellungen von M. ∎

Als erste Anwendung dieses Satzes können wir zeigen

Satz: Die reelle Zahl x erfülle die Gleichung

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \quad \text{mit} \quad a_i \in \mathbb{Z}\,.$$

Dann ist x entweder ganzzahlig oder irrational.

Beweis: Jede rationale Zahl x kann als Quotient $x = p/q$ zweier zueinander teilerfremder ganzer Zahlen p und q geschrieben werden. Multiplizieren wir die Gleichung

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0$$

mit q^n, erhalten wir die nennerlo

$$p^n + a_{n-1}p^{n-1}q + \cdot$$

Auflösen nach p^n führt auf

$$p^n = -a_{n-1}p^{n-1}q -$$
$$= q(-a_{n-1}p^{n-1} -$$

d.h. q muß ein Teiler von p^n se Primfaktorzerlegung von p^n sowi von p und q nur für $q = \pm 1$ der Zahl, wie behauptet.

§6: Kongruenzenrechnun

Zwei ganze Zahlen lassen sich dividieren. Trotzdem – oder gerad in der Zahlentheorie eine große R Behandlung ist die Kongruenzen

Definition: Wir sagen, zwei ga modulo m für eine natürliche Za

$$x \equiv$$

wenn $x - y$ durch m teilbar ist.

Die Kongruenz modulo m defini tion auf $\mathbb{Z}$: Jede ganze Zahl ist ko ist durch jede natürliche Zahl tei so auch $y - x = -(x - y)$, un $y \equiv z \bmod m$, so sind $x - y$ und Summe $x - z$, und damit ist auch

Zwei Zahlen $x, y \in \mathbb{Z}$ liegen gena wenn sie bei der Division durch gibt somit m Äquivalenzklassen, $0, 1, \ldots, m-1$ entsprechen.

Lemma: Ist $x \equiv x'$ mod m und $y \equiv y'$ mod m, so ist auch

$$x \pm y \equiv x' \pm y' \bmod m \quad \text{und} \quad x'y' \equiv xy \bmod m\,.$$

Beweis: Sind $x - x'$ und $y - y'$ durch m teilbar, so auch

$$(x \pm y) - (x' \pm y') = (x - x') \pm (y - y') \qquad \text{und}$$
$$xy - x'y' = x(y - y') + y'(x - x') \qquad \blacksquare$$

Im folgenden wollen wir das Symbol „mod“ nicht nur in Kongruenzen wie $x \equiv y$ mod m benutzen, sondern auch – wie in vielen Programmiersprachen üblich – als Rechenoperation:

Definition: Für eine ganze Zahl x und eine natürliche Zahl m bezeichnet x mod m jene ganze Zahl $0 \le r < m$ mit $x \equiv r$ mod m.

x mod m ist also einfach der Divisionsrest bei der Division von x durch m.

Da nach dem gerade bewiesenen Lemma die Addition, Subtraktion und Multiplikation mit Kongruenzen vertauschbar sind, können wir auf der Menge aller Äquivalenzklassen Rechenoperationen einführen. Übersichtlicher wird das, wenn wir statt dessen die Menge

$$\mathbb{Z}/m \underset{\text{def}}{=} \{0, 1, \ldots, m-1\}$$

betrachten. Wir definieren eine Addition durch

$$x \oplus y = (x + y) \bmod m = \begin{cases} x + y & \text{falls } x + y < m \\ x + y - m & \text{sonst} \end{cases}$$

und entsprechend eine Multiplikation gemäß

$$x \odot y = (xy) \bmod m\,.$$

Für $m = 4$ haben wir also folgende Operationen:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

und

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Um diese Tabellen zu interpretier
griffe aus der Algebra erinnern:

Definition: *a)* Eine *Gruppe* ist
Verknüpfung $\times: G \times G \to G$, fü
1.) $(x \times y) \times z = x \times (y \times z)$ fü
2.) Es gibt ein Element $e \in G$, so
3.) Zu jedem $x \in G$ gibt es ein x

Die Gruppe heißt *kommutativ* od

4.) $x \times y = y \times x$ für alle $x, y \in$

b) Eine Abbildung $\varphi: G \to H$ z
Verknüpfungen $\times$ und $\otimes$ heißt (
alle $x, y \in G$ gilt: $\varphi(x \times y) = \varphi(x)$
wir von einem *Isomorphismus.* Di
in Zeichen $G \cong H$, wenn es eine

c) Ein *Ring* ist eine Menge R
$+, \cdot: R \times R \to R$, so daß gilt
1.) Bezüglich + ist R eine abelsc
2.) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ für alle
3.) Es gibt ein Element $1 \in R$, so
4.) $x \cdot (y + z) = x \cdot y + x \cdot z$ und $(x +$
Der Ring heißt *kommutativ,* wenn
5.) $x \cdot y = y \cdot x$ für alle $x, y \in R$

d) Eine Abbildung $\varphi: R \to S$
Homomorphismus, wenn für alle

$$\varphi(r + s) = \varphi(r) + \varphi(s)$$

wobei + und $\cdot$ auf der linken Sei
zeichnen und rechts die von S.
morphismus, wenn φ bijektiv ist,
wenn es einen Isomorphismus φ:

Lemma: Für jedes $m \in \mathbb{N}$ ist $\mathbb{Z}/m$ mit den Operationen $\oplus$ und $\odot$ ein Ring.

Beweis: Wir betrachten die Abbildung

$$\varphi\colon \begin{cases} \mathbb{Z} \to \mathbb{Z}/m \\ x \mapsto x \bmod m \end{cases}.$$

Nach dem obigen Lemma ist

$$\varphi(x + y) = \varphi(x) \oplus \varphi(y) \quad \text{und} \quad \varphi(xy) = \varphi(x) \odot \varphi(y)\,.$$

Da $\mathbb{Z}$ bezüglich + eine abelsche Gruppe ist, gilt somit dasselbe für $\mathbb{Z}/m$ bezüglich $\oplus$: Wenn zwei ganze Zahlen gleich sind, sind schließlich auch ihre Divisionsreste modulo m gleich. Das Neutralelement ist $\varphi(0) = 0$, und das additive Inverse ist $\varphi(-x) = m - \varphi(x)$. Auch die Eigenschaften von $\odot$ folgen sofort aus den entsprechenden Eigenschaften der Multiplikation ganzer Zahlen; das Neutralelement ist $\varphi(1) = 1$. ∎

Man beachte, daß $\mathbb{Z}/m$ im allgemeinen kein Körper ist: In $\mathbb{Z}/4$ beispielsweise ist $2 \odot 2 = 0$, und in einem Körper kann ein Produkt nur verschwinden, wenn mindestens einer der beiden Faktoren verschwindet.

Im folgenden werden wir die Rechenoperationen in $\mathbb{Z}/m$ einfach mit + und · bezeichnen, wobei jedesmal aus dem Zusammenhang klar sein sollte, ob wir von der Addition und Multiplikation in $\mathbb{Z}/m$ oder der in $\mathbb{Z}$ reden. Der Malpunkt wird dabei, wie üblich, oft weggelassen.

§7: Der chinesische Restesatz

Der Legende nach zählten chinesische Generäle ihre Truppen, indem sie diese mehrfach antreten ließen in Reihen verschiedener Breiten $m_1, \ldots, m_r$ und jedesmal nur die Anzahl a_r der Soldaten in der letzten Reihe zählten. Aus den r Relationen

$$x \equiv a_1 \bmod m_1, \quad \ldots, \quad x \equiv a_r \bmod m_r$$

bestimmten sie dann die Gesamtzahl x der Soldaten.

Ob es im alten China wirklich
konnten, sei dahingestellt; Beispi
falls bereits 1247 in den chinesis
in neun Bänden von CH'IN CHIU-
dort nicht um Soldaten, sondern u

CH'IN CHIU-SHAO oder QIN JIUSHAO wu
eine wilde Jugend mit vielen Affairen fol
Berufsleben in Armee, öffentlicher Verw
cher studierte er an der Akademie von H
unbekannter Lehrer Mathematik bei. Insb
entstandenen *Neun Bücher der Rechenku*
anspruchsvolleren *Mathematischen Abhan*
einen der bedeutendsten Mathematiker r
Restesatz schreibt er, daß er ihn von den I
nur rein mechanisch anwendeten ohne il
in Meixian, wohin er nach einer seiner v
schaften geschickt worden war.

Wir wollen uns zunächst überle
solches Verfahren überhaupt funk
die obigen r Relationen eine nat
denn ist x eine Lösung und M i
sämtlichen m_i, so ist $x + M$ au
aller m_i kongruent zur Null.

Außerdem gibt es Relationen obi
weise das System

$$x \equiv 2 \bmod 4$$

dessen erste Gleichung nur gerade
ungerade hat. Das Problem hier be
Teiler von vier und sechs ist, so d
etwas über x mod 2 aussagt: Na
zweiten aber ungerade.

Dieses Problem können wir dadu
zulassen, die paarweise teilerfrem
jedes gemeinsame Vielfache der
sein muß, so daß wir x modulo e
nen.

Chinesischer Restesatz: Das System von Kongruenzen

$$x \equiv a_1 \bmod m_1, \quad \ldots, \quad x \equiv a_r \bmod m_r$$

hat für paarweise teilerfremde Moduln m_i genau eine Lösung x mit $0 \le x < m_1 \cdots m_r$. Jede andere Lösung $y \in \mathbb{Z}$ läßt sich in der Form $x + km_1 \cdots m_r$ schreiben mit $k \in \mathbb{Z}$.

Mit den Begriffen aus dem vorigen Paragraphen läßt sich dies auch anders formulieren: Die Zahl x mod m_i können wir auffassen als Element von $\mathbb{Z}/m_i$, das r-Tupel aus allen diesen Zahlen also als Element von $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$. Man überlegt sich leicht, daß das kartesische Produkt von zwei oder mehr Gruppen wieder eine Gruppe ist: Die Verknüpfung wird einfach komponentenweise definiert, und das Neutralelement ist dasjenige Tupel, dessen sämtliche Komponenten Neutralelemente der jeweiligen Faktoren sind. Genauso folgt, daß das kartesische Produkt von zwei oder mehr Ringen wieder ein Ring ist.

In algebraischer Formulierung haben wir dann die folgende Verschärfung des obigen Satzes:

Chinesischer Restesatz *(Algebraische Form)***:** Die Abbildung

$$\varphi\colon \begin{cases} \mathbb{Z}/m_1 \cdots m_r \to \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r \\ \qquad\qquad x \mapsto (x \bmod m_1, \ldots, x \bmod m_r) \end{cases}$$

ist ein Isomorphismus von Ringen.

Wir *beweisen* den Satz in dieser algebraischen Form:

Zunächst ist

$$\psi\colon \begin{cases} \mathbb{Z} \to \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r \\ x \mapsto (x \bmod m_1, \ldots, x \bmod m_r) \end{cases}$$

ein Ringhomomorphismus, denn nach dem Lemma aus dem vorigen Paragraphen ist der Übergang zu den Restklassen modulo jeder der Zahlen m_i mit Addition und Multiplikation vertauschbar. Da $\psi(x)$ nur von x mod $m_1 \cdots m_r$ abhängt, folgt daraus, daß auch φ ein Ringhomomorphismus ist.

φ ist injektiv, denn ist $\varphi(x) = \varphi$
alle i; da die m_i paarweise teiler
Produkt der m_i teilbar, was für x
möglich ist.

Nun ist φ aber eine Abbildung z
aus je $m_1 \cdots m_r$ Elementen bes
schen zwei gleichmächtigen end
surjektiv, also bijektiv, und somit

Aus Sicht der chinesischen Gen
Angenommen, ein General weiß,
ihm stehen. Er läßt sie in Zehne
stehen fünf Soldaten. Bei Elferre
hen sechs. Da $10 \cdot 11 \cdot 13 = 143$
dies die Anzahl eindeutig festleg
daten nun tatsächlich vor ihm ste
Möglichkeit, einige Soldaten abz
Tausend die Divisionsreste modu
sie auf das Tripel $(5, 9, 6)$ stoßen
eine effizientere Methode finden.

Dazu verhilft uns der erweiterte E

Wir beginnen mit dem Fall zweie

$$x \equiv a \bmod m$$

mit zueinander teilerfremden Za
nach dem erweiterten EUKLIDis
schreiben. Somit ist

$$1 - \alpha m = \beta n \equiv \begin{cases} 1 & \bmod m \\ 0 & \bmod n \end{cases}$$

also löst

$$x = \beta n a + \alpha m$$

das Problem.

x ist natürlich nicht die einzige Lösung; wenn wir ein gemeinsames Vielfaches von m und n addieren, ändert sich nichts an den Kongruenzen. Da wir von teilerfremden Zahlen ausgegangen sind, ist das Produkt das kleinste gemeinsame Vielfache; die allgemeine Lösung ist daher

$$x + (\beta n + \lambda b)a + (\alpha m - \lambda a)b\,.$$

Insbesondere ist die Lösung eindeutig modulo nm.

Als Beispiel betrachten wir die beiden Kongruenzen

$$x \equiv 1 \bmod 17 \quad \text{und} \quad x \equiv 5 \bmod 19\,.$$

Wir müssen als erstes den erweiterten EUKLIDischen Algorithmus auf die beiden Moduln 17 und 19 anwenden:

$$19 : 17 = 1 \text{ Rest } 2 \Longrightarrow 2 = 19 - 17$$

$$17 : 2 = 8 \text{ Rest } 1 \Longrightarrow 1 = 17 - 8 \cdot 2 = 9 \cdot 17 - 8 \cdot 19$$

Also ist $9 \cdot 17 = 153 \equiv 0 \bmod 17$ und $\equiv 1 \bmod 19$; außerdem ist $-8 \cdot 19 = -152$ durch 19 teilbar und $\equiv 1 \bmod 17$. Die Zahl

$$x = -152 \cdot 1 + 153 \cdot 5 = 613$$

löst somit das Problem. Da 613 größer ist als $17 \cdot 19 = 323$, ist allerdings nicht 613 die kleinste positive Lösung, sondern $613 - 323 = 290$.

Bei mehr als zwei Kongruenzen gehen wir rekursiv vor: Wir lösen die ersten beiden Kongruenzen $x \equiv a_1 \bmod m_1$ und $x \equiv a_2 \bmod m_2$ wie gerade besprochen; das Ergebnis ist eindeutig modulo $m_1 m_2$. Ist c_2 eine feste Lösung, so läßt sich die Lösung schreiben als Kongruenz

$$x \equiv c_2 \bmod m_1 m_2\,,$$

und da die m_i paarweise teilerfremd sind, ist auch $m_1 m_2$ teilerfremd zu m_3. Mit EUKLID können wir daher das System

$$x \equiv c_2 \bmod m_1 m_2 \quad \text{und} \quad x \equiv a_3 \bmod m_3$$

lösen und die Lösung schreiben als

$$x \equiv c_3 \bmod m_1 m_2 m_3$$

und so weiter, bis wir schließlich x modulo dem Produkt aller m_i kennen und somit das Problem gelöst haben.

Im Beispiel des oben angesproch

$$x \equiv 5 \bmod 10, \quad x \equiv$$

lösen wir also zunächst nur das S

$$x \equiv 5 \bmod 10$$

Da $1 = 11 - 10$, ist $11 \equiv 0 \bmod$
ist $-10 \equiv 0 \bmod 10$ und $-10 \equiv$

$$x = 5 \cdot 11$$

eine Lösung; die allgemeine Lös
kleinste positive Lösung ist -35

Unser Ausgangssystem ist somit

$$x \equiv 75 \bmod 110$$

Um es zu lösen, müssen wir zun
von 110 und 13 darstellen. Hier b
an, also verwenden wir den erwe

$$110 : 13 = 8 \text{ Rest}$$

$$13 : 6 = 2 \text{ Rest } 1 \Longrightarrow 1 =$$

Also ist $17 \cdot 13 = 221 \equiv 1$ mo
$-2 \cdot 110 = 220 \equiv 1 \bmod 13$ und $\equiv$
unseres Problems ist somit

$$75 \cdot 221 -$$

Die allgemeine Lösung ist

$$15\,255 + k \cdot 110 \cdot 13 = 1$$

Da $15\,255 : 1\,430 = 10$ Rest 955 i
vor sich stehen.

Alternativ läßt sich die Lösung e
in einer geschlossenen Form da
n-maligen statt $(n-1)$-maligen
rithmus und größeren Zahlen sch

$$x \equiv a_i \bmod m$$

zu lösen, berechnen wir zunächst für jedes i das Produkt

$$\widehat{m}_i = \prod_{j \neq i} m_j$$

der sämtlichen übrigen m_j und bestimmen dazu ganze Zahlen α_i, β_i, für die gilt $\alpha_i m_i + \beta_i \widehat{m}_i = 1$. Dann ist

$$x = \sum_{j=1}^{n} \beta_j \widehat{m}_j a_j \equiv \beta_i \widehat{m}_i a_i = (1 - \alpha_i m_i) a_i \equiv a_i \bmod m_i \,.$$

Natürlich wird x hier – wie auch bei der obigen Formel – oft größer sein als das Produkt der m_i; um die kleinste Lösung zu finden, müssen wir also noch modulo diesem Produkt reduzieren.

Im obigen Beispiel wäre

$$\begin{array}{llll} m_1 = 10 & \widehat{m}_1 = 11 \cdot 13 = 143 & 1 = 43 \cdot 10 - 3 \cdot 143 \\ m_2 = 11 & \widehat{m}_2 = 10 \cdot 13 = 130 & 1 = -59 \cdot 11 + 5 \cdot 130 \\ m_3 = 13 & \widehat{m}_3 = 10 \cdot 11 = 110 & 1 = 17 \cdot 13 - 2 \cdot 110 \,, \end{array}$$

also

$$x = -3 \cdot 143 \cdot 5 + 5 \cdot 130 \cdot 9 - 2 \cdot 110 \cdot 6 = -2145 + 5850 - 1320 = 2385 \,.$$

Modulo $10 \cdot 11 \cdot 13$ erhalten wir natürlich auch hier wieder 955.

Damit kennen wir nun auch zwei konstruktive Beweise des chinesischen Restesatzes und wissen, wie man Systeme von Kongruenzen mit Hilfe des erweiterten EUKLIDischen Algorithmus lösen kann.

§8: Prime Restklassen

Wie wir gesehen haben, können wir auch in $\mathbb{Z}/m$ im allgemeinen nicht dividieren. Allerdings ist Division doch sehr viel häufiger möglich als in den ganzen Zahlen. Dies wollen wir als nächstes genauer untersuchen:

Lemma: Zu zwei gegebenen natürlichen Zahlen a, m gibt es genau dann ein $x \in \mathbb{N}$ mit $ax \equiv 1 \bmod m$, wenn ggT$(a, m) = 1$ ist.

Beweis: Wenn es ein solches x
$ax = 1 + my$, d.h. $1 = ax - my$
von a und m Teiler der Eins sein,

Sind umgekehrt a und m teilerf
ten EUKLIDischen Algorithmus
(gegebenenfalls mehrfache) Addi
sich nötigenfalls erreichen, daß
$ax \equiv 1 \bmod m$.

Definition: Ein Element $a \in$
ggT$(a, m) = 1$ ist.

Nach dem gerade bewiesenen L
Restklasse a ein $x \in \mathbb{Z}/m$, so
folgende Lemma nicht verwunde

Lemma: Die primen Restklasse
tiplikation eine Gruppe.

Beweis: Wir müssen uns zunäch
primer Restklassen wieder eine p
beide teilerfremd zu m, so auc
Primteiler von ab und m, so wä
oder b, also gemeinsamer Teiler
Eins ist natürlich eine prime Re
Inversen ist kein Problem: Nach d
so daß $ax \equiv 1 \bmod m$ ist, und die
daß auch $x \bmod m$ eine prime Re
Multiplikation gilt für alle Elem
primen Restklassen.

Definition: Die Gruppe $(\mathbb{Z}/m)^\times$
Restklassengruppe, ihre Ordnung
heißt EULERsche φ-Funktion.

LEONHARD EULER (1707–1783) wurde in Basel geboren und ging auch dort zur Schule und, im Alter von 14 Jahren, zur Universität. Dort legte er zwei Jahre später die Magisterprüfung in Philosophie ab und begann mit dem Studium der Theologie; daneben hatte er sich seit Beginn seines Studium unter Anleitung von JOHANN BERNOULLI mit Mathematik beschäftigt. 1726 beendete er sein Studium in Basel und bekam eine Stelle an der Petersburger Akademie der Wissenschaften, die er 1727 antrat. Auf Einladung FRIEDRICHS DES GROSSEN wechselte er 1741 an die preußische Akademie der Wissenschaften; nachdem sich das Verhältnis zwischen den beiden dramatisch verschlechtert hatte, kehrte er 1766 nach St. Petersburg zurück. Im gleichen Jahr erblindete er vollständig; trotzdem schrieb er rund die Hälfte seiner zahlreichen Arbeiten (Seine gesammelten Abhandlungen umfassen 73 Bände) danach. Sie enthalten bedeutende Beiträge zu zahlreichen Teilgebieten der Mathematik, Physik, Astronomie und Kartographie.

Lemma: *a)* Für zwei zueinander teilerfremde Zahlen $n, m \in \mathbb{N}$ ist $\varphi(nm) = \varphi(n)\varphi(m)$.
b) Für $m = \prod_{i=1}^{r} p_i^{e_i}$ ist $\varphi(m) = \prod_{i=1}^{r} \left(p_i^{e_i-1}(p_i - 1)\right)$.

Beweis: a) Eine Zahl a ist genau dann teilerfremd zum Produkt nm, wenn a mod n teilerfremd zu n und a mod m teilerfremd zu m ist. Da nach dem chinesischen Restesatz $\mathbb{Z}/nm \cong \mathbb{Z}/n \times \mathbb{Z}/m$ ist, ist daher auch $(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$.

b) Wegen *a)* genügt es, dies für Primzahlpotenzen p^e zu beweisen. Eine Zahl a ist genau dann teilerfremd zu p^e, wenn sie kein Vielfaches von p ist. Unter den Zahlen von 1 bis p^e gibt es genau p^{e-1} Vielfache von p, also ist $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$. ∎

Korollar: $\mathbb{Z}/m$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Beweis: Das einzige, was $\mathbb{Z}/m$ zu einem Körper eventuell fehlt, ist die Existenz von multiplikativen Inversen für alle von null verschiedenen Elemente. Dies ist offenbar äquivalent zur Formel $\varphi(m) = m - 1$, und die gilt nach dem Lemma genau dann, wenn m prim ist. ∎

Der Körper $\mathbb{Z}/p$ mit p Elementen
die zugehörige prime Restklasse
chend als $\mathbb{F}_p^\times$. Dabei steht das
endliche Körper gelegentlich auc
man hier auch die Abkürzung GF
für Körper; das gelegentlich in In
loisfeld ist also ein Übersetzungs

Wir wollen uns als nächstes übe
dieses Körpers aus den Potenzen
brauchen wir zunächst noch ein L

Definition: Die Ordnung eines
schriebenen) Gruppe G ist die k
gleich dem Einselement ist. Falls
a habe unendliche Ordnung.

Lemma (LAGRANGE): In einer e
nes jeden Elements die Gruppenc

Beweis: Die Potenzen des Eleme
eine Untergruppe H von G, deren
von H ist. Wir führen auf G e
Vorschrift $g \sim h$, falls gh^{-1} in
Äquivalenzklasse eines jeden El
ten, nämlich $g, ga, \ldots, ga^{r-1}$. Da
klassen ist, muß die Gruppenordn

JOSEPH-
SEPPE L
studierte
von HA
tik wec
ein aus
In einer
diesem
nung v
EULERS
zehn Ja
EULERS

Akademie. 1787 wechselte er an die Pariser Académie des Sciences, wo er bis zu seinem Tod blieb und unter anderem an der Einführung des metrischen Systems beteiligt war. Seine Arbeiten umspannen weite Teile der Analysis, Algebra und Geometrie.

Korollar: Für zwei zueinander teilerfremde Zahlen a, m ist

$$a^{\varphi(m)} \equiv 1 \bmod m\,.$$

Beweis: Klar, denn $\varphi(m)$ ist die Ordnung der primen Restklassengruppe modulo m. ∎

Für eine Primzahl $N = p$ bezeichnet man diese Aussage auch als den *kleinen Satz von* FERMAT:

Satz (FERMAT): Für jede nicht durch die Primzahl p teilbare ganze Zahl a ist $a^{p-1} \equiv 1 \bmod p$. Für alle $a \in \mathbb{Z}$ ist $a^p \equiv a \bmod p$.

Beweis: Die erste Aussage ist klar, da $\varphi(p) = p - 1$ ist. Für die zweite müssen wir nur noch beachten, daß für durch p teilbare Zahlen a sowohl a^p als auch a kongruent null modulo p sind. ∎

Der französische Mathematiker PIERRE DE FERMAT (1601–1665) wurde in Beaumont-de-Lomagne im Departement Tarn et Garonne geboren. Bekannt ist er heutzutage vor allem für seine 1994 von ANDREW WILES bewiesene Vermutung, wonach die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ keine ganzzahlige Lösung mit $xyz \neq 0$ hat. Dieser „große“ Satzes von FERMAT, von dem FERMAT lediglich in einer Randnotiz behauptete, daß er ihn beweisen könne, erklärt den Namen der obigen Aussage. Obwohl FERMAT sich sein Leben lang sehr mit Mathematik beschäftigte und wesentliche Beiträge zur Zahlentheorie, Wahrscheinlichkeitstheorie und Analysis lieferte, war er hauptberuflich Jurist.

Satz: Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.

Beweis: Da die multiplikative Gruppe eines Körpers mit q Elementen aus allen Körperelementen außer der Null besteht, hat sie die Ordnung $q-1$, d.h. nach LAGRANGE ist die Ordnung eines jeden Elements ein Teiler

von $q - 1$. Wir müssen zeigen,
dessen Ordnung *genau* $q - 1$ ist.

Für jeden Primteiler p_i von $q - 1$

$$x^{(q-}$$

höchstens $(q-1)/p_i$ Lösungen i
Körperelement a_i mit $a_i^{(q-1)/p_i} \neq$

q_i sei die größte Potenz von p_i,
$(q-1)/q_i$-te Potenz von a_i. Dan

$$g_i^{q_i} = a_i^{q-1} = 1$$

g_i hat also die Ordnung q_i. Da di
dener Primzahlen p_i sind, hat da
aller q_i als Ordnung, also $q - 1$. D
Körpers zyklisch.

Definition: Ein Element g eines
Wurzel, wenn es die zyklische Gr

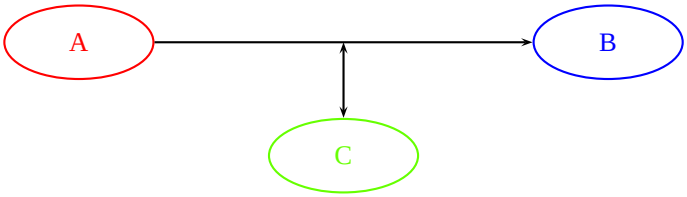
Selbst im Fall der Körper $\mathbb{F}_p$ gi
solche primitive Wurzel explizit
Üblicherweise wählt man zufäll
die Ordnung $p - 1$ hat. Die W
$\varphi(p-1) : (p-1)$, was für di
Der Test, ob die Ordnung gleich
effizient durchführen, wenn die
denn dann kann man einfach teste
ten $(p-1)/p_i$ von eins verschie
sie in der Kryptographie benötig
so daß man hier im allgemeinen v
dann testet, ob $r + 1$ prim ist. Im
geeignete Tests kennenlernen.

Kapitel 2
Anwendungen in der Kryptologie

§1: New directions in cryptography

Kryptologie ist zusammengesetzt aus den beiden griechischen Wörtern κρυπτός = verborgen, versteckt und λόγος = Rede, Darlegung, Vernunft; sie ist also die Wissenschaft vom Geheimen. Sie besteht aus der Kryptographie (von γράφή = Das Schreiben), die Geheimschriften entwickelt, und der Kryptanalyse (von ἀναλύειν = auflösen, zerlegen), die versucht, letztere zu analysieren mit dem Ziel, sie zu knacken.

Die Grundsituation ist also die folgende:



A möchte eine Nachricht x an B übermitteln, jedoch besteht die Gefahr, daß alles, was er an B schickt, auf dem Weg dorthin von C gelesen und vielleicht auch verändert wird; außerdem könnte C eventuell versuchen, sich gegenüber B als A ausgeben oder umgekehrt.

Die Kryptographie versucht, dies zu verhindern, indem A anstelle von x einen Chiffretext c schickt, aus der zwar B, nicht aber C die Nachricht x und gegebenenfalls weitere Informationen rekonstruieren kann. Natürlich bietet diese Verschlüsselung für sich allein

noch keinen Schutz, denn C kö
ter von A oder B angreifen, um
oder nach der Entschlüsselung a
schlüsselungsprogramm so mani
ihn keine Hürde mehr ist, er kön
Computer und/oder Monitor au
ter. Die Enthüllungen über NSA
nichts gibt, was ein hinreichend e
Trotzdem macht es gute Kryptog
schwierig oder sogar unmöglich,

In der klassischen Kryptographie
genauso oder zumindest sehr ähnl
dere kann jeder, der eine Nachric
sprechend verschlüsselte Nachric
diese Verfahren daher als *symmet*

Der Nachteil eines solchen Verfah
werk jeder Teilnehmer mit jedem
muß. In militärischen Netzen wa
das gesamte Netz denselben Schl
für jeden Tag im voraus festgele
beispielsweise einem Mobilfunkn

1976 publizierten MARTIN HEL
Stanford, und sein Forschungsa
beit mit dem Titel *New directio*
form. Theory **22**, 644–654), in d
*Ver*schlüsselung und den der *En*
trennen: Es sei schließlich nicht
schlüsselten Nachricht auch in de

Der Vorteil eines solchen *asymm*
potentielle Empfänger nur einen
noch sicher sein könnte, daß nur e
Der Schlüssel müßte nicht einm
(meistens) nichts schadet, wenn
kann. In einem Netzwerk mit n

n Schlüssel, um es jedem Teilnehmer zu ermöglichen, mit jedem anderen sicher zu kommunizieren. Die Schlüssel könnten sogar in einem öffentlichen Verzeichnis stehen. Bei einem symmetrischen Kryptosystem wäre der gleiche Zweck nur erreichbar mit $\frac{1}{2}n(n-1)$ Schlüsseln, die auf einem sicheren Weg wie etwa bei einem persönliches Treffen oder durch vertrauenswürdige Boten ausgetauscht werden müßten.

BAILEY WHITFIELD DIFFIE wurde 1944 geboren. Erst im Alter von zehn Jahren lernte er lesen; im gleichen Jahr hielt eine Lehrerin an seiner New Yorker Grundschule einen Vortrag über Chiffren. Er ließ sich von seinem Vater alle verfügbare Literatur darüber besorgen, entschied sich dann 1961 aber doch für ein Mathematikstudium am MIT. Um einer Einberufung zu entgehen, arbeitete er nach seinem Bachelor bei Mitre; später, nachdem sein Interesse an der Kryptographie wieder erwacht war, kam er zu Martin Hellman nach Stanford, der ihn als Forschungsassistent einstellte. Ab 1991 arbeitete er als *chief security officer* bei Sun Microsystems, von 2010 bis 2012 war er bei ICANN für Sicherheit zuständig.

MARTIN HELLMAN wurde 1945 in New York geboren. Er studierte Elektrotechnik zunächst bis zum Bachelor an der dortigen Universität; für Master und Promotion studierte er in Stanford. Nach kurzen Zwischenaufenthalten am Watson Research Center der IBM und am MIT wurde er 1971 Professor an der Stanford University. Seit 1996 ist er emeritiert, gibt aber immer noch Kurse, mit denen er Schüler für mathematische Probleme interessieren will. Seine home page findet man unter `http://www-ee.stanford.edu/~hellman/` .

DIFFIE und HELLMAN machten nur sehr vage Andeutungen, wie so ein System mit öffentlichen Schlüsseln aussehen könnte. Es ist zunächst einmal klar, daß ein solches System keinerlei Sicherheit gegen einen Gegner mit unbeschränkter Rechenkraft (In der Kryptographie spricht man von einem BAYESschen Gegner) bieten kann, denn die Verschlüsselungsfunktion ist eine bijektive Abbildung zwischen endlichen Mengen, und jeder, der die Funktion kennt, kann zumindest im Prinzip auch ihre Umkehrfunktion berechnen.

Wer im Gegensatz zum BAYESsch
cen verfügt, kann diese Berechnu
realistischem Aufwand durchfüh
heit eines Kryptosystems mit ö
immer leistungsfähiger werden u
rithmen gefunden werden, sind s
die Ewigkeit gedacht, sondern nu
Zukunft. Derzeit geht man in der
ner 2^{128} oder gar mehr Entschl
und bezeichnet ein System dah
Untersuchung kein Angriff beka
und einer nicht vernachlässigbar
liefert. Man spricht dann von 128-
natürlich nicht bewiesen ist.

Einige Stellen, darunter auch das
formationstechnik, halten derzeit
reichend. Dieser Auffassung schl
derzeit in Deutschland üblichen
Geheimzahl mit dem sogenannten
heit bei knapp 112 Bit liegt.

DIFFIE und HELLMAN bezeichnen
nicht mit vertretbarem Aufwand
kann, als *Einwegfunktion* und wo
selung verwenden. Das allein füh
tikablen Kryptosystem, denn be
auch für den legitimen Empfänge
entschlüsseln. DIFFIE und HELLM
tion mit *Falltür* vor, wobei der leg
öffentlichen Schlüssel noch über
dem er (und nur er) diese Falltür

Natürlich hängt alles davon ab,
Falltür wirklich gibt. DIFFIE und
unter den Experten einige Skeps
Funktionen zu finden.

Tatsächlich gab es wohl bereits damals Systeme, die auf solchen Funktionen beruhten, auch wenn sie nicht in der offenen Literatur dokumentiert waren: Die britische *Communications-Electronics Security Group* (CESG) hatte bereits Ende der sechziger Jahre damit begonnen, nach entsprechenden Verfahren zu suchen, um die Probleme des Militärs mit dem Schlüsselmanagement zu lösen, aufbauend auf (impraktikablen) Ansätzen von AT&T zur Sprachverschlüsselung während des zweiten Weltkriegs. Die CESG sprach nicht von Kryptographie mit öffentlichen Schlüsseln, sondern von *nichtgeheimer Verschlüsselung*, aber das Prinzip war das gleiche.

Erste Ideen dazu sind in einer auf Januar 1970 datierten Arbeit von JAMES H. ELLIS zu finden, ein praktikables System in einer auf den 20. November 1973 datierten Arbeit von CLIFF C. COCKS. Wie im Milieu üblich, gelangte nichts über diese Arbeiten an die Öffentlichkeit; erst 1997 veröffentlichten die *Government Communications Headquarters* (GCHQ), zu denen CESG gehört, einige Arbeiten aus der damaligen Zeit; eine Zeitlang waren sie auch auf dem Server `http://www.cesg.gov.uk/` zu finden, wo sie allerdings inzwischen anscheinend wieder verschwunden sind.

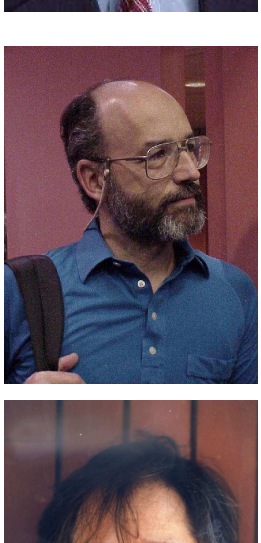
Im akademischen Bereich gab es ein Jahr nach Erscheinen der Arbeit von DIFFIE und HELLMAN das erste Kryptosystem mit öffentlichen Schlüsseln: Drei Wissenschaftler am Massachusetts Institute of Technology fanden nach rund vierzig erfolglosen Ansätzen 1977 schließlich jenes System, das heute nach ihren Anfangsbuchstaben mit RSA bezeichnet wird: RON RIVEST, ADI SHAMIR und LEN ADLEMAN.

RIVEST, SHAMIR und ADLEMAN gründeten eine Firma namens RSA Computer Security Inc., die 1983 das RSA-Verfahren patentieren ließ und auch nach Auslaufen dieses Patents im September 2000 weiterhin erfolgreich im Kryptobereich tätig ist. 2002 erhielten RIVEST, SHAMIR und ADLEMAN für die Entdeckung des RSA-Systems den TURING-Preis der *Association for Computing Machinery* ACM, ein jährlich vergebener Preis, der als eine der höchsten Auszeichnungen der Informatik gilt.

RSA ist übrigens identisch mit dem von COCKS vorgeschlagenen System, so daß einige Historiker auch Zweifel an den Behauptungen der

RONALD
im US-
zunächs
seinen
Informa
sistenzp
ogy, wo
noch au
te eine
sche Ve
Er ist K
home p

ADI SH
dierte z
nach sei
tut, wo
in Infor
der Uni
er ans
fessor i
Entwick
folgreic
auch ei
großer
http://
profile/

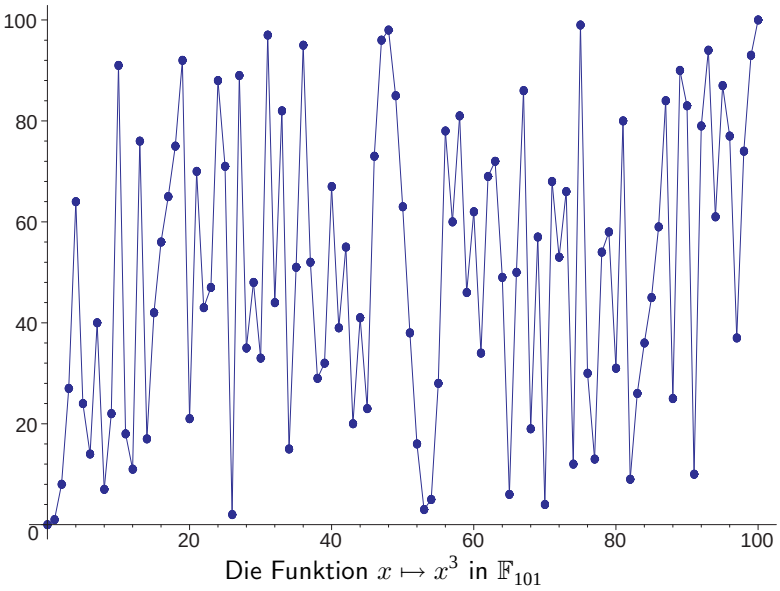


LEONAR
boren.
in Math
hielt. Th
che Alg
1980 w
seit 198
ifornia
sich mi
biologie
nung m
beitete
hat er
larbiolo
science

GCHQ haben. Die Beschreibung durch RIVEST, SHAMIR und ADLEMAN erschien 1978 unter dem Titel *A method for obtaining digital signatures and public-key cryptosystems* in Comm. ACM **21**, 120–126.

§2: Das RSA-Verfahren

Für eine natürliche Zahl e ist die reelle Funktion $x \mapsto x^e$ für positive x monoton ansteigend und bijektiv; ihre Umkehrfunktion $x \mapsto \sqrt[e]{x}$ läßt sich mit etwa demselben Aufwand berechnen wie die Funktion selbst. Betrachten wir $x \mapsto x^e$ allerdings als Funktion von $\mathbb{Z}/N \to \mathbb{Z}/N$, so erhalten wir einen sehr chaotisch aussehenden Graphen und können uns daher Hoffnungen machen, daß diese Funktion vielleicht als Grundlage einer kryptographischen Verschlüsselung brauchbar sein könnte.



Die Funktion $x \mapsto x^3$ in $\mathbb{F}_{101}$

Dazu muß sie natürlich zunächst einmal injektiv sein. Da die Ordnung eines Elements von $(\mathbb{Z}/N\mathbb{Z})^\times$ Teiler von $\varphi(N)$ ist, muß insbesondere e teilerfremd zu $\varphi(N)$ sein. Dann lassen sich mit dem erweiterten EUKLIDischen Algorithmus Zahlen $d, k \in \mathbb{N}$ finden, so daß $de - k\varphi(N) = 1$

ist, d.h. für jedes zu N teilerfrem

$$(x^e)^d = x^{ed} = x$$

Somit sind die Funktionen

$$\begin{cases} (\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times \\ x \mapsto x^e \end{cases}$$

zueinander invers.

Die Beschränkung auf prime Res
wendungen ungünstig: Am einfac
deren Länge kleiner ist als die der
schen 0 und $N-1$ auffassen, vers
Empfänger könnte dann die Zahl e
und daraus die Nachricht rekonst
für *quadratfreie* Zahlen N, d.h. Z
teilbar sind, auch möglich:

Satz: Für eine quadratfreie natür
nen

$$\begin{cases} \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \\ x \mapsto x^e \end{cases}$$

bijektiv und invers zueinander.

Beweis: Als quadratfreie Zahl is
zahlen p_i, und $\varphi(N)$ ist das Prod
Somit ist auch $ed \equiv 1 \bmod \varphi(p_i)$
Restesatz genügt es, wenn wir de
Ist $N = p$ prim, so ist die Null da
in $(\mathbb{Z}/p)^*$ liegt, und sie wird vo
abgebildet.

Jeder, der e und N kennt, kann
dazu als erstes $\varphi(N)$ bestimmen
ist das möglich, wenn er die Pri
fachere alternative Verfahren sind
tel über Faktorisierungsalgorithm

mit heutigen Mitteln für ein Produkt zweier gut gewählter Primzahlen nicht mehr mit realistischem Aufwand möglich, wenn dieses Produkt mehr als etwa 250 Dezimalstellen hat. Natürlich wird diese Schranke im Laufe der Jahrzehnte ansteigen, und wahrscheinlich können einzelne Geheimdienste schon heute etwas mehr als der Rest der Welt. Es ist aber unwahrscheinlich, daß bei einem schon seit Jahrhunderten untersuchten Problem wie der Faktorisierung ganzer Zahlen ausgerechnet einem Geheimdienst ein Durchbruch gelingen sollte, von dem der Rest der Welt nichts bemerkt. Die Effekte einer leistungsfähigeren Hardware lassen sich durch großzügige Sicherheitszuschläge kompensieren.

Für eine Primzahl $N = p$ kann natürlich jeder ganz einfach $\varphi(p) = p - 1$ berechnen; ist $N = pq$ dagegen das Produkt zweier Primzahlen, so ist die Bestimmung von

$$\varphi(N) = (p-1)(q-1) = N - (p+q) + 1$$

äquivalent zur Kenntnis der Faktorisierung: Kennt man nämlich das Produkt $N = pq$ sowie die Summe $N + 1 - \varphi(N) = p + q$ der beiden Primzahlen, so kann man sie einfach berechnen als Lösungen der quadratischen Gleichung

$$(x-p)(x-q) = x^2 - \big(N + 1 - \varphi(N)\big)x + N = 0\,.$$

Auch bei Produkten von mehr als drei Primzahlen ist keine Methode zur Berechnung der EULERschen φ-Funktion bekannt, die effizienter wäre als der Umweg über die Faktorisierung, allerdings wird die Faktorisierung bei konstanter Größenordnung von N tendenziell einfacher, wenn die Anzahl der Faktoren steigt, da wir es dann zumindest teilweise mit kleineren Faktoren zu tun haben.

Zur praktischen Durchführung des RSA-Verfahrens wählt sich daher jeder Teilnehmer zwei verschiedene Primzahlen p, q, die unbedingt geheim gehalten werden müssen, und eine natürliche Zahl e, die keinen gemeinsamen Teiler mit $(p-1)(q-1)$ hat. Die Zahlen $N = pq$ und e sind sein öffentlicher Schlüssel, der beispielsweise in einem Verzeichnis publiziert werden kann.

Des weiteren berechnet er ein gemeinsames Vielfaches λ von $p-1$ und $q-1$, zum Beispiel das kleinste gemeinsame Vielfache oder aber einfach

$\lambda = \varphi(N) = (p-1)(q-1)$, und da
Algorithmus natürliche Zahlen d
kann erreicht werden, daß $d <$
führt also im Allgemeinen auch z
Zahl d ist sein geheimer Schlüss

$$\big(a^e\big)^d = a \cdot$$

ist für alle a, läßt sich die Entsc
Potenzieren mit d.

Jeder, der den öffentlichen Schli
richten verschlüsseln: Er bricht d
ganze Zahlen zwischen 0 und N -
net für jeden so dargestellten Bloc
schickt diesen an den Inhaber des
$b^d \bmod N = a^{ed} \bmod N = a$, und
braucht, kann dies niemand auße

§3: Weitere Anwendunge

Im Gegensatz zu symmetrische
Verfahrens nicht nur die Möglic
erlaubt noch eine ganze Reihe we

a) Identitätsnachweis

Hier geht es darum, in Zugangs
oder bei einer Bestellung im Inte
weisen: Mit RSA ist das beispiel
Inhaber des geheimen Schlüssels
berechnen kann, für die $b^e \equiv a$
jeder überprüfen, der den öffentli

Falls also der jeweilige Gegenüb
Antwort das zugehörige b verlan
Schlüsselverzeichnisses die Richt
der Identität seines Partners überz
information oder Paßwörtern ist

Abhören: Falls jedesmal ein neues zufälliges a erzeugt wird, nützt ein einmal abgehörtes b nichts.

Grundsätzlich bräuchte man hier kein Kryptosystem mit öffentlichen Schlüsseln; in der Tat funktionierten die ersten Freund-/Feinderkennungssysteme für Flugzeuge zur Zeit des zweiten Weltkriegs nach diesem Prinzip, aber damals natürlich mit einem klassischen symmetrischen Kryptosystem, wobei alle Teilnehmer mit demselben Schlüssel arbeiteten. Der Vorteil eines asymmetrischen Systems besteht darin, daß sich keiner der Teilnehmer für einen anderen ausgeben kann, was beispielsweise wichtig ist, wenn man sich gegenüber weniger vertrauenswürdigen Personen identifizieren muß.

Trotzdem ist das Verfahren in dieser Form nicht als Ersatz zur Übertragung von rechtlich bindender Information geeignet, da der Gegenüber anhand des öffentlichen Schlüssels jederzeit zu einer willkürlich gewählten Zahl b die Zahl $a = b^e \bmod N$ erzeugen kann um dann zu behaupten, er habe b als Antwort darauf empfangen. Daher kann der Inhaber des geheimen Schlüssels zwar seine Identität beweisen, aber sein Gegenüber kann später nicht beispielsweise vor Gericht beweisen, daß er dies (zum Beispiel bei einer Geldabhebung oder Bestellung) getan hat. Falls dies eventuell nötig werden könnte, ist das hier vorgestellte Verfahren also ungeeignet; es funktioniert nur zwischen Personen, die einander vertrauen können.

Eine mögliche Modifikation bestünde darin, daß man beispielsweise noch zusätzlich verlangt, daß die Zahl a eine spezielle Form hat, etwa daß die vordere Hälfte der Ziffernfolge identisch mit der hinteren Hälfte ist. Ohne Kenntnis von d hat man praktisch keine Chancen eine Zahl b zu finden, für die $b^e \bmod N$ eine solche Gestalt hat: Bei Zahlen mit $2r$ Ziffern liegt die Wahrscheinlichkeit dafür bei 10^{-r}.

b) Elektronische Unterschriften

Praktische Bedeutung hat vor allem eine andere Variante: die elektronische Unterschrift. Hier geht es darum, daß der Empfänger erstens davon überzeugt wird, daß eine Nachricht tatsächlich vom behaupteten Absender stammt, und daß er dies zweitens auch einem Dritten gegenüber beweisen kann. (In D
Unterschriften, sofern gewisse f
rechtsverbindlich.)

Um einen Nachrichtenblock a r
berechnet der Inhaber des öffen
geheimen Schlüssel d die Zahl

$$b = a$$

und sendet das Paar (a, b) an den

$$b^e \equiv$$

falls ja, akzeptiert er dies als unt
Kenntnis des geheimen Schlüsse
(a, b) zu erzeugen, kann er auch g
der Absender selbst die Nachrich

Für kurze Nachrichten ist dieses
praktikabel; in vielen Fällen kann
verzichten, da $b^e \bmod N$ für ein
grenzender Wahrscheinlichkeit k

Falls die übermittelte Nachricht g
und b natürlich noch vor der Übert
des Empfängers oder nach irgen
schlüsselt werden.

Bei langen Nachrichten ist die Ver
mehr akzeptabel, und selbst, we
verzichten kann, ist das Unterso
aufwendig. Deshalb unterschreib
sondern einen daraus extrahierten
erstens von der gesamten Nachric
den Empfänger (praktisch) unmö
gen, die zum gleichen Hashwert
sogenannten *Geburtstagsparadox*
te der Länge $2n$ erforderlich sin
Hashalgorithmen, die 160 Bit lie

von etwa 80 Bit, was heute nicht mehr als wirklich sicher gelten kann. Die heute gebräuchlichen Hashalgorithmen liefern Werte mit 224 oder 256 Bit, was einer 112- oder 128-Bit Sicherheit entspricht. Die Algorithmen funktionieren ähnlich wie symmetrische Kryptoverfahren; sie versuchen durch Konfusion und Diffusion ein Ergebnis zu berechnen, dessen sämtliche Bits in einer nicht offensichtlichen Weise von jedem einzelnen Nachrichtenbit abhängen.

c) SSL und TLS

Eine wichtige Anwendung elektronischer Unterschriften ist die Veröffentlichung von RSA-Schlüsseln: Falls es einem Angreifer gelingt, einem Teilnehmer A einen falschen öffentlichen Schlüssel von Teilnehmer B unterzuschieben, kann (nur) der Angreifer die Nachrichten von A an B lesen, und er kann sich gegenüber A mittels elektronischer Unterschrift als B ausgeben. Daher sind öffentliche Schlüssel meist unterschrieben von einer Zertifizierungsstelle. Auch deren Unterschrift muß natürlich gegen Manipulationen gesichert sein, beispielsweise indem sie von der nächsthöheren Zertifizierungsstelle unterschrieben ist. An der Spitze der Zertifizierungshierarchie stehen Stellen, deren elektronische Unterschrift jeder Teilnehmer kennen sollte, weil es sich entweder um staatliche Stellen handelt, deren elektronische Unterschriften auf leicht zugänglichen Webseiten verifiziert werden können, oder aber – in der Praxis häufiger – weil die Unterschriften dieser Stellen in Mail- und Browserprogramme eingebaut sind. Letzteres bietet selbstverständlich keine Sicherheit gegen manipulierte Browserprogramme aus dubiosen Quellen, die möglicherweise auch die Mafia als Zertifizierungsstelle anerkennen.

Zertifizierte Unterschriften werden insbesondere angewandt bei den Standards SSL und TLS für sichere Internetverbindungen.

SSL steht für *secure socket layer,* TLS für *transport layer security;* Zweck ist jeweils der Aufbau einer sicheren Internetverbindung. Wie im Internet üblich, können dazu die verschiedensten Verfahren benutzt werden; die auf Grundlage von RSA zählen derzeit zu den populärsten.

Natürlich ist RSA zu aufwendig, um damit eine längere Kommunikation wie beispielsweise eine *secure shell* Sitzung zu verschlüsseln; tatsächlich dient RSA daher nur
ein konventionelles Kryptoverfah
auf das sich die Beteiligten unter

Am einfachsten wäre es, wenn d
ches Verfahren wählt und dann
Servers verschlüsselt an diesen s
RSA-Schlüssel. Letzteres ist im a
zunächst der Server dem Client s

Da der Client nicht sicher sein kan
zu sein, schickt der Server diesen
Zertifikat, das sowohl seine Ide
enthält und von einer Zertifizieru

Die öffentlichen Schlüssel der gä
bereits erwähnt, in die Browserp
kannten Zertifizierungsstellen wie
sität Mannheim fragt der Browse
erkennen will oder nicht. Bei *secu*
typischerweise keinerlei Zertifika
beim ersten Verbindungsaufbau
anerkannt werden soll und speich
davon; dieser wird bei späteren V
benutzt.

d) Blinde Unterschriften und

Einer der erfolgversprechendsten
tosystems besteht darin, sich auf
verlassen.

So sollte es durch gutes Zureden
monstrationszwecken zum Unters
bewegen: Eine Folge von Nullen
tion hat schließlich keine rechtlic

Nun muß eine sinnlose Nachricht
sein: Sie kann sorgfältig präparier

die ein Zahlungsversprechen enthält, (N, e) der öffentliche Schlüssel des Opfers und r eine Zufallszahl zwischen 2 und $N - 2$. Dann wird

$$x = m \cdot r^e \bmod N$$

wie eine Zufallsfolge aussehen, für die man eine Unterschrift

$$u = x^d \bmod N = (mr^e)^d \bmod N = m^d r \bmod N$$

bekommt. Multiplikation mit r^{-1} macht daraus eine Unterschrift unter die Zahlungsverpflichtung m.

Das angegebene Verfahren kann nicht nur von Trickbetrügern benutzt werden; blinde Unterschriften sind auch die Grundlage von *digitalem Bargeld*.

Zahlungen im Internet erfolgen meist über Kreditkarten; die Kreditkartengesellschaften haben also einen recht guten Überblick über die Ausgaben ihrer Kunden und machen teilweise auch recht gute Geschäfte mit Kundenprofilen.

Digitales Bargeld will die Anonymität von Geldscheinen mit elektronischer Übertragbarkeit kombinieren und so ein anonymes Zahlungssystem z.B. für das Internet bieten.

Es wir ausgegeben von einer Bank, die für jede angebotene Stückelung einen öffentlichen Schlüssel (N, e) bekanntgibt. Eine Banknote ist eine mit dem zugehörigen geheimen Schlüssel unterschriebene Seriennummer.

Die Seriennummer kann natürlich nicht einfach *jede* Zahl sein; sonst wäre jede Zahl kleiner N eine Banknote. Andererseits dürfen die Seriennummern aber auch nicht von der Bank vergeben werden, denn sonst wüßte diese, welcher Kunde Scheine mit welchen Seriennummern hat. Als Ausweg wählt man Seriennummern einer sehr speziellen Form: Ist $N > 10^{150}$, kann man etwa als Seriennummer eine 150-stellige Zahl wählen, deren Ziffern spiegelsymmetrisch zur Mitte sind, d.h. ab der 76. Ziffer werden die vorherigen Ziffern rückwärts wiederholt. Die Wahrscheinlichkeit, daß eine zufällige Zahl x nach Anwendung des öffentlichen Exponenten auf so eine Zahl führt, ist 10^{-75} und damit vernachlässigbar.

Seriennummern werden von den
che Seriennummer m erzeugt d
$mr^e \bmod N$ an die Bank und e
eine Unterschrift u für diese Nac
daraus durch Multiplikation mit
für die Seriennummer N, und mi

Der Zahlungsempfänger berechn
gültigen Seriennummer hat, kan
unterschriebenen Geldschein vor
nicht sicher sein, daß dieser Geld
wurde.

Deshalb muß er die Seriennumm
Datenbank bereits ausbezahlter
darin noch nicht vorkommt, wi
bekommt sein Geld; andernfalls

Bei 10^{75} möglichen Nummern li
zwei Kunden, die eine (wirklich)
mer erzeugen, bei etwa $10^{-37,5}$
einem Spielschein fünf Wochen

Lotto zu haben, liegt dagegen bei
Faktor sechzig höher. Zwei gleic
auszuschließen, wenn auch theor

Falls wirklich einmal zufälliger
erzeugt worden sein sollten, kann
der zweite Geldschein mit ders
wird, so daß der zweite Kunde
zusätzliche Gebühr gesehen wer
Wahrscheinlichkeit nie fällig wir
werden kann.

Da digitales Bargeld nur in klei
scheine im Millionenwert wären
lich anonym und würden wegen
zur Geldwäsche auch in keinem s
wäre der theoretisch mögliche Ve

Digitales Bargeld der gerade beschriebenen Form wurde 1982 von DAVID CHAUM vorgestellt; 1990 gründete er eine Firma namens DigiCash, die es kommerziell vermarkten sollte. Zu deren Kunden gehörte beispielsweise auch die Deutsche Bank, die allerdings nur 27 Kunden fand, die Zahlungen damit akzeptierten. DigiCash wurde 1998 zahlungsunfähig; derzeit gibt es meines Wissens keine ähnlichen Zahlungssysteme.

e) Bankkarten mit Chip

Bankkarten speichern ihre Information sowohl in einem Chip, als auch, unabhängig davon, auf einem einen Magnetstreifen. Dort stehen Informationen wie Kontenname und -nummer, Bankleitzahl, Gültigkeitsdauer *usw.;* dazu kommt verschlüsselte Information, die unter anderem die Geheimzahl enthält, die aber auch von den obengenannten Daten abhängt. Zur Verschlüsselung verwendet man hier ein konventionelles, d.h. symmetrisches Kryptoverfahren; derzeit noch meist Triple-DES.

Der Schlüssel, mit dem dieses arbeitet, muß natürlich streng geheimgehalten werden: Wer ihn kennt, kann problemlos die Geheimzahlen fremder Karten ermitteln und eigene Karten zu beliebigen Konten erzeugen.

Um eine Karte nur anhand der Magnetstreifeninformation zu überprüfen, muß daher eine Verbindung zu einem Zentralrechner aufgebaut werden, an den sowohl der Inhalt des Magnetstreifens als auch die vom Kunden eingetippte Zahl übertragen werden; dieser wendet Triple-DES mit dem Systemschlüssel an und meldet dann, wie die Prüfung ausgefallen ist.

Der Chip enthält ebenfalls die Kontendaten; zusätzlich ist dort auch noch in einem auslesesicheren Register Information über die Geheimzahl gespeichert. Daher muß die eingegebene PIN nicht an einen Zentralrechner übertragen werden, sondern wird vom Lesegerät an den Chip weitergegeben, der dann entscheidet, ob die Eingabe akzeptiert wird oder nicht.

Da frei programmierbare Chipkarten relativ billig sind, muß dafür Sorge getragen werden, daß ein solches System nicht durch einen *Yes-Chip* unterlaufen werden kann, der ebenfalls die Konteninformationen enthält,

ansonsten aber ein Programm, das
Das Terminal muß also, bevor es
zunächst einmal den Chip auther
daß es sich um einen vom Banke
delt.

Aus diesem Grund sind die Kor
vaten RSA-Schlüssel des Konso
kennen den öffentlichen Schlüsse
überprüfen.

Solche Chipkarten wurden hier in
ausgegeben; Einzelheiten über die
technische Implementierung wu
geheimgehalten. Trotzdem macht
namens SERGE HUMPICH daran,
verschaffte sich dazu ein (im frei
untersuchte sowohl die Kommun
als auch die Vorgänge innerhalb
analysators. Damit gelang es ihr
des Terminals zu entschlüsseln un
übersetzen. Durch dessen Analyse
dur und die Prüflogik entschlüsse
daß hier mit RSA gearbeitet wurd

Blieb noch das Problem, den Mo
sich ein japanisches Programm a
für kleinere Zahlen gedacht war, a
natürlich auch für jemanden, der d
nicht versteht, kein Problem. Nac
damit den Modul faktorisiert:

$$2135987035920910082395$$
$$6417406442524165008583$$
$$= 1113954325148827987925$$
$$\times 191748170252450443937$$

Als er seine Ergebnisse über einen
teilte, zeigte sich, was dieses sic

Es erreichte, daß HUMPICH wegen des Eindringens in ein DV-System zu zehn Monaten Haft auf Bewährung sowie einem Franc Schadenersatz plus Zinsen verurteilt wurde; dazu kamen 12 000 F Geldstrafe. Einzelheiten findet man in seinem Buch

SERGE HUMPICH: Le cerveau bleu, Xo, 2001

Ab November 1999 hatten neu ausgegebene Bankkarten noch ein zusätzliches Feld mit einer Unterschrift, die im Gegensatz zum obigen 320-Bit-Modul einen 768-Bit-Modul verwendet. Natürlich können damit erzeugte Unterschriften nur von neueren Terminals überprüft werden, so daß viele Transaktionen weiterhin nur über den 320-Bit-Modul mit inzwischen wohlbekannter Faktorisierung „geschützt“ waren. Die heutigen Standards behandelt der nächste Paragraph.

§4: Wie groß sollten die Primzahlen sein?

Das Beispiel der ersten französischen Bankkarten zeigt, daß RSA höchstens dann sicher ist, wenn die Primzahlen p und q deutlich größer sind als man im ersten Augenblick denkt. Wir müssen uns daher die Frage stellen, wie groß die Primzahlen nach heutigen Standards sein müssen, um einen Angriff mit hinreichender Sicherheit auszuschließen.

Ein treu sorgender Staat läßt seine Bürgern bei einer derart wichtigen Frage natürlich nicht allein: Zwar gibt es noch keine oberste Bundesbehörde für Primzahlen, aber das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen publizieren jedes Jahr ein Dokument mit dem Titel *Geeignete Kryptoalgorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001.*

SigV steht für die aufgrund des Signaturgesetzes SigG erlassene Signaturverordnung; beide gemeinsam legen fest, daß elektronische Unterschriften in Deutschland grundsätzlich zulässig und rechtsgültig sind, sofern sie gewisse Bedingungen erfüllen. Zu diesen Bedingungen gehört unter anderem, daß das Verfahren und die Schlüssellänge gemeinsam

einen „geeigneten Kryptoalgorit
Veröffentlichung der Bundesnetz

Da Rechner immer schneller ur
auf der mathematisch-algorithm
oder größere Fortschritte zu ver
Empfehlungen nur für etwa sech
relativ stabil; daher sind die Emp
ausnahmsweise sieben Jahre gült
sein sollen, sind elektronische Ur

Die neuesten Richtlinien stamme
am 20. Februar 2014 im Bundesa
2048 Bit, aber wirklich verbind
Unterschied hängt mit Implemen
Betriebssystem SECCOS zusamr

Die beiden Primfaktoren p, q soll
der erzeugt werden und aus einer

$$\varepsilon_1 < |\log_2$$

gilt. Als *Anhaltspunkte* werden d
vorgeschlagen; ist p die kleine
$2^{-10}p < q < 2^{30}p \approx 10^9 p$ g
somit zwar ungefähr dieselbe Grö
beieinander liegen. Der Grund da
torisierungsverfahren auf Grundl
Falls für eine Zahl N und eine n
Quadratzahl x^2 ist, ist $N = x^2$
Faktoren gefunden sind. Probiert
systematisch durch, führt dieses V
zum Erfolg, je näher die beiden Fa
werden uns in Kapitel über Faktor

Nachdem die Primzahlen gefunde
Exponent e gewählt werden, wob
tatsächlich dürfte noch oft $e = 3$
private Exponent d so gewählt, d

Auch wenn das Verfahren primär für Unterschriften verwendet werden soll, darf man also nicht vom privaten Exponenten ausgehen, denn wie wir im Kapitel über Kettenbrüche sehen werden, läßt sich ein kleiner privater Exponent aus e und $N = pq$ mit recht geringem Aufwand bestimmen.

§5: Praktische Gesichtspunkte

Wenn $N = pq$ um die zwei Tausend Bit hat, wird im allgemeinen auch das kgV von $p-1$ und $q-1$ nicht viel kleiner sein, und bei der obigen Vorgehensweise können wir erwarten, daß dann auch zumindest der private Exponent d ebenfalls in dieser Größenordnung ist. Damit ist klar, daß zumindest x^d mod N nicht einfach durch sukzessive Multiplikation mit x berechnet werden kann: Unser Sicherheitsstandard beruht schließlich auf der Annahme, daß niemand 2^{128} oder gar noch mehr Rechenoperationen ausführen kann. Hinzu kommt, daß x^d so groß ist, daß kein heutiger Computer diese Zahl speichern könnte. Um die Länge der Zwischenergebnisse in Grenzen zu halten, muß nach jeder Multiplikation sofort modulo N reduziert werden.

Auch das Problem der vielen Multiplikationen läßt sich in den Griff bekommen: Um beispielsweise x^{32} zu berechnen brauchen wir keine 31 Multiplikationen, sondern erhalten das Ergebnis über die Formel

$$x^{32} = \left(\left(\left(\left(x^2\right)^2\right)^2\right)^2\right)^2$$

mit nur fünf Multiplikationen (genauer: Quadrierungen).

Entsprechend können wir für jede gerade Zahl $n = 2m$ die Potenz x^n als Quadrat von x^m berechnen. Für einen ungeraden Exponenten e ist $e-1$ gerade, wenn wir also x^e als Produkt von x und x^{e-1} berechnen, können wir zumindest im nächsten Schritt wieder die Formel für gerade Exponenten verwenden. Somit reichen pro Binärziffer des Exponenten ein bis zwei Multiplikationen; der Aufwand wächst also nur proportional zur Stellenzahl von e. Für den ebenfalls recht populären Verschlüsselungsexponenten $e = 2^{16}+1 = 65537$ beispielsweise braucht man nur 17 Multiplikationen, nicht 65536.

Hinreichend große Primzahlen s
die Sicherheit des RSA-Verfahre
ner, vor dem eine Nachricht gesc
in der Wahl seiner Mittel und k
torisierungsversuch angreifen. So
sind, muß man sich daher auch da

In der bislang dargestellten sogen
eine ganze Reihe alternativer Ang
kleinen öffentlichen oder privaten

Da der Aufwand einer Exponenti
Exponenten wächst, bevorzugen
insbesondere wird in der Praxis s
Exponent $e = 3$ verwendet (was
deten Primzahlen kongruent zwe
die Verschlüsselung recht schnell
vate Exponent d sehr einfach bes
es Zahlen $d < \lambda = \text{kgV}(p-1, q-$
Im Falle $e = 3$ kommen nur $k =$
nur testen, welche der beiden Zah
ganzzahlig ist.

Bei so vielen Vorteilen muß es
ganz offensichtlichen: Ist nämlic
te Wurzel aus N, so ist $x^3 < N$
Die Kubikwurzel aus dieser ganz
werden.

Kurze Nachrichten sind allerding
blematisch. Ein Grund liegt darin
der Multiplikation verträglich ist:

Nehmen wir an, unsere Nachric
kleiner als $2^{2\ell}$. Dann gibt es eine
sich $x = yz$ als Produkt zweier Z
als 2^ℓ (oder als eine etwas grö
für alle Zahlen y von null bis
berechnen und die Ergebnisse in

Chiffretext $c = x^e \bmod N$ auf x zurückzuschließen, berechnen wir für jedes dieser Ergebnisse in $\mathbb{Z}/N$ den Quotienten c/y^e. (Falls sich dieser Quotient nicht bilden läßt, ist y^e nicht teilerfremd zu $N = pq$, und wir erhalten sogar eine Faktorisierung von N; das ist aber für gut gewählte, große N extrem unwahrscheinlich.) Falls einer dieser Quotienten als Eintrag $z^e \bmod N$ in unserer Tabelle auftaucht, haben wir eine Relation der Form $c \equiv y^e \cdot z^e = (yz)^e \bmod N$ gefunden, und damit kennen wir $x = yz$.

Um diese Attacke zu verhindern, muß bei 128-Bit-Sicherheit $\ell \geq 128$ sein, die übermittelten Nachrichten müssen also mindestens 256 Bit lang sein. Auch dann sind wir allerdings noch nicht unbedingt auf der sicheren Seite, denn wenn nur wenige Nachrichten in Frage kommen, kann ein Gegner die einfach alle mit dem öffentlichen Schlüssel chiffrieren und schauen, wann das Ergebnis mit dem Chiffretext übereinstimmt. Beim praktischen Einsatz von RSA werden daher nie einfach die zu übermittelnden Nachrichten übertragen, sondern Blöcke eines vorher festgelegten Formats. Diese Formate sehen vor, daß alle unbenutzten Positionen mit Zufallsbits gefüllt werden und daß jeder Block mindestens 128 Zufallsbits enthält. Auf dem Niveau der 128-Bit-Sicherheit ist dann jede Entschlüsselung durch systematisches Probieren ausgeschlossen, denn Nachrichtenlängen größer 256 Bit sind bei den heute üblichen Parameterwerten ohnehin selbstverständlich.

Falls eine Nachricht an mehrere Empfänger geschickt wird, müssen – vor allem bei kleinen Verschlüsselungsexponenten wie $e = 3$ – die Zufallsbits für jeden Empfänger neu erzeugt werden, denn wenn jedes Mal derselbe Block x verschlüsselt wird und dabei – wie dies häufig in der Praxis der Fall ist – stets mit drei potenziert wird, kennt ein Gegner anschließend $x^3 \bmod N_i$ für die Moduln N_i der sämtlichen Empfänger, kann also nach dem chinesischen Restesatz x^3 modulo dem Produkt der N_i berechnen, und da dieses Produkt bei mindestens drei Empfängern größer ist als x^3, kennt er x^3 und damit auch x.

Bei der Wahl der Schlüsseldaten geht man stets aus vom öffentlichen Exponenten e und berechnet dann dazu nach dem EUKLIDischen Algorithmus den privaten Exponenten d. Dadurch ist praktisch sichergestellt, daß dieser in der Größenordnung von N liegen wird, und das muß auch

so sein: Im Kapitel über Kettenb
faktorisiert werden kann, wenn d

§6: Verfahren mit diskret

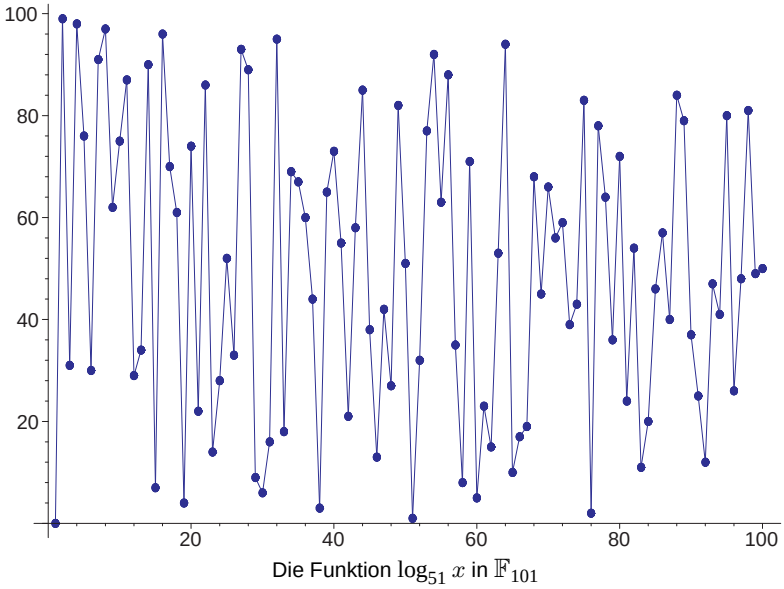
Kurz nach der Veröffentlichung
DIFFIE und HELLMAN ein Verfah
ganz ohne vorvereinbarte Schlüs
baren über eine unsichere Leitu
nur sie kennen.

Ausgangspunkt ist wieder das Pot
wir aber die Exponentialfunktion
Ihre Umkehrfunktion bezeichnet
mus zur Basis a:

$$y = a^x =$$

Trotz dieser formalen Übereinstim
terschiede zwischen reellen Log
lichen Körpern: Während reelle
Funktionen sind, die man leicht m
kann, sieht der diskrete Logarith
der Abbildung zu sehen ist. Auc
Basis $a > 1$ für jede positive Zah
viel schwerer zu entscheiden, ob
Modulo sieben etwa sind $2, 4$ und
$3, 5$ und 6 keine Zweierlogarithm
tel I gesehen haben, ist aber die
zyklisch, so daß es stets Elemente
Null annimmt, die sogenannten
etwa drei und fünf.

Die Berechnung der Potenzfunkt
Multiplizieren ist auch in endlich
funktion, den diskreten Logarith
schlechtere Verfahren. Die derz
von diskreten Logarithmen in Kö
wa denselben Aufwand wie die



Die Funktion $\log_{51} x$ in $\mathbb{F}_{101}$

Größenordnung N. Diese Diskrepanz zwischen Potenzfunktion und Logarithmen kann kryptologisch ausgenutzt werden.

Als Körper verwendet man entweder Körper von Zweipotenzordnung, die wir in dieser Vorlesung nicht betrachten werden, oder Körper von Primzahlordnung. Da es für viele interessante Körper von Zweipotenzordnung bereits Chips gibt, die dort diskrete Logarithmen berechnen, dürften Körper von Primzahlordnung bei ungefähr gleicher Elementanzahl wohl etwas sicherer sein: Es gibt einfach viel mehr Primzahlen als Zweierpotenzen, und jeder Fall erfordert einen neuen Hardwareentwurf. Falls man die Primzahlen hinreichend häufig wechselt, dürfte sich dieser Aufwand für kaum einen Gegner lohnen. Außerdem ist das Rechnen modulo einer Primzahl einfacher als das Rechnen in einem Körper von Zweipotenzordnung.

Beim DIFFIE-HELLMAN-Verfahren, dem ältesten auf der Grundlage diskreter Logarithmen, geht es wie gesagt darum, daß zwei Teilnehmer, die weder über gemeinsame Schlüsselinformation noch über eine sichere

Leitung verfügen, einen Schlüsse

Dazu einigen sie sich zunächst
Primzahl p und eine natürliche
$x \mapsto a^x$ möglichst viele Werte an

Als nächstes wählt Teilnehmer
sprechend $y < p$; A schickt u
$v = a^y \bmod p$.

Sodann berechnet A die Zahl v^x
und B entsprechend $u^y \bmod p$
haben also auf verschiedene Weis
als Schlüssel in einem klassisch
wobei sie sich wohl meist auf ein
da solche Schlüssel typischerwe
haben, während die Primzahl p e

Ein Gegner, der den Datenausta
p, a, u und v; um $a^{xy} \bmod p$ zu f
mus von u oder v berechnen.

Mit den besten heute bekannten
p eine Primzahl von bis zu etwa
etwa 665 Bit. Auch in diesem
selbst bei massiver Parallelisierun

Natürlich gibt es keine Garantie,
als den bislang bekannten Verfah
risierungen auch in weitaus grö
bräuchte er allerdings einen Du
tischen oder auf der technischen
Grundlage zu sehen ist.

Trotzdem gibt es einen verhält
Schlüsselaustausch nach DIFFIE
in the middle attack. Dabei unte
zwischen A und B und gibt sich
So kann er mit beiden Teilnehme
die damit verschlüsselte Kommu

und gegebenenfalls manipuliert werden. In der vorgestellten Form funktioniert das Verfahren also nur, wenn man sicher sein weiß, mit wem man kommuniziert.

§6: DSA

DSA steht für *Digital Signature Algorithm*, ein Algorithmus der im *Digital Signature Standard* DSS der USA festgelegt ist und neben RSA auch zu den von der Bundesnetzagentur empfohlenen „Geeigneten Algorithmen“ zählt. Seine Sicherheit beruht auf diskreten Logarithmen, allerdings wird das klassische Verfahren dadurch modifiziert, daß die Sicherheit zwar auf dem diskreten Logarithmenproblem in einem großen Körper beruht, die Rechenoperationen bei der Anwendung des Algorithmus aber nur eine deutlich kleinere Untergruppe verwenden.

Für diese kleine Untergruppe wählt man eine Primzahl q mit einer Länge von mindestens 224 Bit. (Das entspricht der Länge der Hashwerte, die in der Praxis anstelle des Texts unterzeichnet werden.) Zu dieser Primzahl q sucht man eine Primzahl $p \equiv 1 \bmod q$, für deren Länge die Bundesnetzagentur mindestens 2048 Bit vorschreibt.

Daß die mit der empfohlenen RSA-Modullänge übereinstimmt, ist kein Zufall: Auch wenn kein direkter Zusammenhang zwischen Faktorisierung und der Berechnung diskreter Logarithmen bekannt ist, hat bislang doch jede neue Idee für einen Faktorisierungsalgorithmus auch zu einem Algorithmus zur Berechnung diskreter Logarithmen geführt, und auch die Laufzeiten dieser Algorithmen sind bei gleicher Zahlenlänge ungefähr gleich.

Als nächstes muß ein Element g gefunden werden, dessen Potenzen im Körper $\mathbb{F}_p$ eine Gruppe der Ordnung q bilden. Das ist einfach: Man starte mit irgendeinem Element $g_0 \in \mathbb{F}_p \setminus \{0\}$ und berechne seine $(p-1)/q$-te Potenz. Falls diese ungleich eins ist, muß sie wegen $g_0^{p-1} = 1$ die Ordnung q haben; andernfalls muß ein neues g_0 betrachtet werden.

Die so bestimmten Zahlen q, p und g werden veröffentlicht und können auch in einem ganzen Netzwerk global eingesetzt werden. Geheimer Schlüssel jedes Teilnehmers ist e
der zugehörige öffentliche Schlüs

Unterschreiben lassen sich mit di
mit $0 \leq m < q$, insbesondere also
man für jede Nachricht eine Zufa

$$r = (g^k$$

Da q eine Primzahl ist, hat k ein n
kann also durch k dividieren und

$$sk \equiv m$$

ist; die Unterschrift unter die Nac
Zahlen r und s modulo q. Sie kann
der den geheimen Schlüssel x ke

Überprüfen kann die Unterschrift
Inverse zu s modulo q, so ist $k \equiv$
Ordnung q hat,

$$r \equiv g^k \equiv g^{tm} g$$

In dieser Gleichung sind die link
öffentlich bekannt, die Gleichung
Die Unterschrift wird anerkannt
sind. Ein Angreifer müßte sich
diskretes Logarithmenproblem m

§7: Ausblick

Dieses kurze Kapitel konnte selbs
sicht über die Kryptographie od
tographie geben: Auch das RSA-
angegriffen werden als der direk
dieser Methoden werden wir im
nen, und auch sonst werden im w
gelegentlich Themen aus der Kry

Mit Ausnahme von Verfahren wie dem sogenannten *one time pad* gibt es für keines der heute benutzten Kryptoverfahren einen Sicherheitsbeweis, nicht einmal in dem Sinn, daß man den Aufwand eines Gegners zum Knacken des Verfahrens in irgendeiner realistischen Weise nach unten abschätzen könnte. Seriöse Kryptographie außerhalb des Höchstsicherheitsbereichs muß sich daher damit begnügen, daß die Verantwortlichen für den Einsatz eines Verfahrens und der Wahl seiner Parameter (wie den Primzahlen bei RSA) darauf achten, auf dem neuesten Stand der Forschung zu bleiben und ihre Wahl so treffen, daß nicht nur die bekannten Angriffsmethoden versagen, sondern daß auch noch ein recht beträchtlicher Sicherheitszuschlag für künftige Entwicklungen und für nicht publizierte Entwicklungen bleibt.

Auf ewige Sicherheit kann man mit Verfahren wie RSA ohnehin nicht hoffen: Als RSA 1977 von MARTIN GARDNER im *Scientific American* vorgestellt wurde, bekam er von RIVEST, SHAMIR und ADLEMAN die 129-stellige Zahl

$$114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541$$

(seither bekannt als RSA-129) und eine damit verschlüsselte Nachricht, für deren Entschlüsselung die drei einen Preis von hundert Dollar ausgesetzt hatten. Sie schätzten, daß eine solche Entschlüsselung etwa vierzig Quadrillionen ($4 \cdot 10^{25}$) Jahre dauern würde. (Heute sagt RIVEST, daß dies auf einem Rechenfehler beruhte.) Tatsächlich wurde der Modul 1994 faktorisiert in einer gemeinsamen Anstrengung von 600 Freiwilligen, deren Computer immer dann, wenn sie nichts besseres zu tun hatten, daran arbeiteten. Nach acht Monaten war die Faktorisierung gefunden: Die obige Zahl ist gleich

$$\begin{aligned}&4905295108476509491478496199038981334177646384933878439908205773276913299326670954996198819083446141317764296799294253979828853 3\,.\end{aligned}$$

Mit dem Schema $A = 01$ bis $Z = 26$ und Zwischenraum gleich 00 ergab sich die Nachricht *The Magic Words are Squeamish Ossifrage.*

Auch bei den heute als sicher geltenden symmetrischen Kryptoverfahren rechnet niemand ernsthaft damit, daß sie noch in hundert Jahren sicher sind: Diese Verfahren werden üblicherweise so gewählt, daß man auf

eine Sicherheit für etwa dreißig J
aber auch das niemand.

Falls sich sogenannte *Quanten*
alle heute bekannten Verfahren
Schlüsseln, egal ob mit diskreten
Kurven, unsicher sein. Bislang kö
Bit rechnen, und nicht alle Expert
che geben wird, die mit mehreren

Wer mehr über Kryptographie wis
beispielsweise bei

BUCHMANN: Einführung in die K

oder natürlich auch im Skriptum
Kryptologie-Vorlesung.

Mehr über die Geschichte der Kry
ist (mathematikfrei) zu finden in

STEVEN LEVY: **crypto:** how the
privacy in the digital age, *Penguii*

Kapitel 3
Primzahlen

Wie wir aus dem ersten Kapitel wissen, sind Primzahlen die Grundbausteine für die multiplikative Struktur der ganzen Zahlen, und aus Kapitel zwei wissen wir, daß sie auch wichtige Anwendungen außerhalb der Zahlentheorie haben. Es lohnt sich also auf jeden Fall, sie etwas genauer zu untersuchen.

§ 1: Die Verteilung der Primzahlen

Als erstes stellt sich die Frage, wie viele Primzahlen es gibt. Die Antwort finden wir schon in EUKLIDs Elementen; der dort gegebene Beweis dürfte immer noch der einfachste sein: Es gibt unendlich viele Primzahlen, denn gäbe es nur endlich viele Primzahlen $p_1, \ldots, p_n$, so könnten wir deren Produkt P bilden und die Primzerlegung von $P+1$ betrachten. Da P durch alle p_i teilbar ist, ist $P+1$ durch kein p_i teilbar, im Widerspruch zur Existenz der Primfaktorzerlegung. Somit muß es noch weitere, also unendlich viele Primzahlen geben.

Um nicht ganz auf dem Stand von vor rund zweieinhalb Jahrtausenden stehen zu bleiben, wollen wir uns noch einen zweiten, auf EULER zurückgehenden Beweis ansehen.

Dazu betrachten wir für eine reelle Zahl $s > 1$ die unendliche Reihe

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} .$$

Als erstes müssen wir uns überlegen, daß diese Reihe konvergiert. Da alle Summanden positiv sind, müssen wir dafür nur zeigen, daß es eine

gemeinsame obere Schranke für a
$x \mapsto 1/x^s$ für $x > 0$ monoton fal
die Abschätzung $1/n^s \leq 1/x^s$, d

$$\sum_{n=1}^{N} \frac{1}{n^s} = 1 + \sum$$

$$< 1 + \int_1^{\infty} \frac{dx}{x^s} =$$

Somit ist $\zeta(s)$ für alle $s > 1$ wohl

Einen Zusammenhang mit Primz

Satz: *a)* Für $s > 1$ ist $\zeta(s) = \prod_{p \text{ pri}}$

b) Für alle $N \in \mathbb{N}$ und alle reelle

Beweis: Wir beginnen mit *b)*. Fü
$1 \leq 1$; sei also $N \geq 2$, und seien
kleiner oder gleich N. Nach der
Reihe ist

$$\frac{1}{1 - \frac{1}{p_k^s}}$$

und das Produkt der rechtsstehen
der Eindeutigkeit der Primzerlegu
die n keinen Primteiler größer N
$n \leq N$, womit *b)* bewiesen wäre.

Die Differenz zwischen $\zeta(s)$ un
von *b)* ist gleich der Summe über
Primteiler größer N haben. Diese
der Summe aller $1/n^s$ mit $n > N$
von $\zeta(s)$ gegen null für $N \to \infty$.

Auch daraus folgt, daß es unendlich viele Primzahlen gibt: Gäbe es nämlich nur endlich viele, so stünde auf der rechten Seite von *b)* für jedes hinreichend große N das Produkt über die *sämtlichen* Primzahlen. Da es nur endlich viele Faktoren hat, wäre es auch für $s = 1$ endlich, und damit müßte

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

kleiner oder gleich dieser Zahl sein, im Widerspruch zur Divergenz der harmonischen Reihe.

Verglichen mit dem Beweis aus EUKLIDs Elementen ist EULERs Methode erheblich komplizierter. Um trotzdem ihre Existenzberechtigung zu haben, sollte sie uns daher auch mehr Informationen liefern. In welchem Maße sie dies tatsächlich leistet, geht wahrscheinlich sogar noch deutlich über alles hinaus, was EULER seinerzeit träumen konnte.

Zunächst einmal können wir Teil *b)* für $s = 1$ zu einer quantitativen Abschätzung bezüglich der Anzahl $\pi(N)$ der Primzahlen kleiner oder gleich N umformulieren: Wie oben im Konvergenzbeweis für $\zeta(s)$ können wir aus der Monotonie der Funktion $x \mapsto 1/x$ folgern, daß für alle $N \in \mathbb{N}$ gilt

$$\log(N+1) = \int_1^{N+1} \frac{dx}{x} < \sum_{n=1}^{N} \frac{1}{n} < 1 + \int_1^{N} \frac{dx}{x} = 1 + \log N\,.$$

Zur Abschätzung der linken Seite beachten wir einfach, daß der Faktoren $1/(1-1/p)$ für $p = 2$ gleich zwei ist, ansonsten aber kleiner. Somit ist

$$\log(N+1) < \sum_{n=1}^{N} \frac{1}{n} \le \prod_{\substack{p \le N \\ p \text{ prim}}} \frac{1}{1-\frac{1}{p}} \le 2^{\pi(N)}$$

und damit

$$\pi(N) \ge \frac{\log\log(N+1)}{\log 2}\,.$$

Wie wir bald sehen werden, ist das allerdings eine sehr schwache Abschätzung.

EULERs Methode erlaubt uns auc
gleichen mit der Dichte beispielsw
gesehen haben, konvergiert $\zeta(s)$
vergiert die Summe $\zeta(2)$ der in
mit seiner Methode zeigen, daß
divergiert, so daß die Primzahle
liegen als die Quadratzahlen und
Exponenten $x > 1$.

Zum Beweis fehlt uns nur noch
wollen uns überlegen, daß für all
den Intervallenden stimmen beid
eine lineare Funktion. Es reicht
konvexe Funktion ist, daß also ihr
positiv ist. Das ist aber klar, denn
Primzahl p ist daher

$$1 - \frac{1}{p} \ge 4^{-1/p}$$

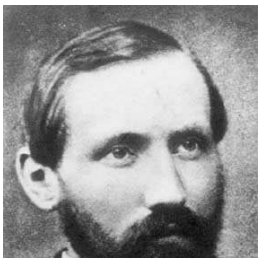
Zusammen mit der vorigen Absch

$$\log(N+1) < \prod_{\substack{p \le N \\ p \text{ prim}}} \frac{1}{1}$$

wobei die Summe im Exponente
Da $\log(N+1)$ für $N \to \infty$ gege
Summe der inversen Primzahlen

Mit diesen Bemerkungen fängt al
$\zeta(s)$ für das Verständnis der Funk
dert nach EULER erkannte RIEMA
Nützlichkeit für das Studium von
komplexe Argumente s betrachte
tionen einer komplexer Veränderl
$\zeta(s)$ auch für komplexe Zahlen m
Imaginärteil des Exponenten führ
Betrag eins.

RIEMANNs wesentliche Erkenntnis war, daß sich $\zeta(s)$ fortsetzen läßt zu einer analytischen Funktion auf der gesamten Menge der komplexen Zahlen mit Ausnahme der Eins (wo die ζ-Funktion wegen der Divergenz der harmonischen Reihe keinen endlichen Wert haben kann).



GEORG FRIEDRICH BERNHARD RIEMANN (1826-1866) war Sohn eines lutherischen Pastors und schrieb sich 1946 auf Anraten seines Vaters an der Universität Göttingen für das Studium der Theologie ein. Schon bald wechselte an die Philosophische Fakultät, um dort unter anderem bei GAUSS Mathematikvorlesungen zu hören. Nach Promotion 1851 und Habilitation 1854 erhielt er dort 1857 einen Lehrstuhl. Trotz seines frühen Todes initiierte er grundlegende auch noch heute fundamentale Entwicklungen in der Geometrie, der Zahlentheorie und über abelsche Funktionen. Wie sein Nachlaß zeigte, stützte er seine 1859 aufgestellte Vermutung über die Nullstellen der ζ-Funktion auf umfangreiche Rechnungen.

Für Leser, die nicht mit dem Konzept der analytischen Fortsetzung vertraut sind, möchte ich ausdrücklich darauf hinweisen, daß dies selbstverständlich nicht bedeutet, daß die definierende Summe der ζ-Funktion für reelle Zahlen kleiner eins oder komplexe Zahlen mit Realteil kleiner oder gleich eins konvergiert: Analytische Fortsetzung besteht darin, daß eine differenzierbare Funktion (die im Komplexen automatisch beliebig oft differenzierbar ist und um jeden Punkt in eine TAYLOR-Reihe entwickelt werden kann) via TAYLOR-Reihen über ihren eigentlichen Definitionsbereich hinweg ausgedehnt wird. Man kann beispielsweise zeigen, das $\zeta(-1) = -\frac{1}{12}$ ist. Setzt man $s = -1$ in die für $s > 1$ gültige Reihe ein, erhält man die Summe aller natürlicher Zahlen, die selbstverständlich nicht gleich $-\frac{1}{12}$ ist, sondern divergiert. Entsprechend hat $\zeta(s)$ Nullstellen bei allen geraden negativen Zahlen, obwohl auch hier die entsprechenden Reihen divergieren. Diese Nullstellen bezeichnet man als die sogenannten *trivialen* Nullstellen der ζ-Funktion, da sie sich sofort aus einer bei der Konstruktion der analytischen Fortsetzung zu beweisenden Funktionalgleichung ablesen lassen. Für die Primzahlverteilung spielen vor allem die übrigen, die sogenannten nichttrivialen Nullstellen, eine große Rolle.

Wie wir gerade gesehen haben, einem gewissen Sinne dichter als auf das Problem der Primzahlve (deutlich einfacheren) Verteilung

Die Folge der Abstände zwischen zahlen ist einfach die Folge der u

$$(n+1)^2 -$$

Zwei aufeinanderfolgende Quadr ferenz $Q' - Q = 2\sqrt{Q} + 1$.

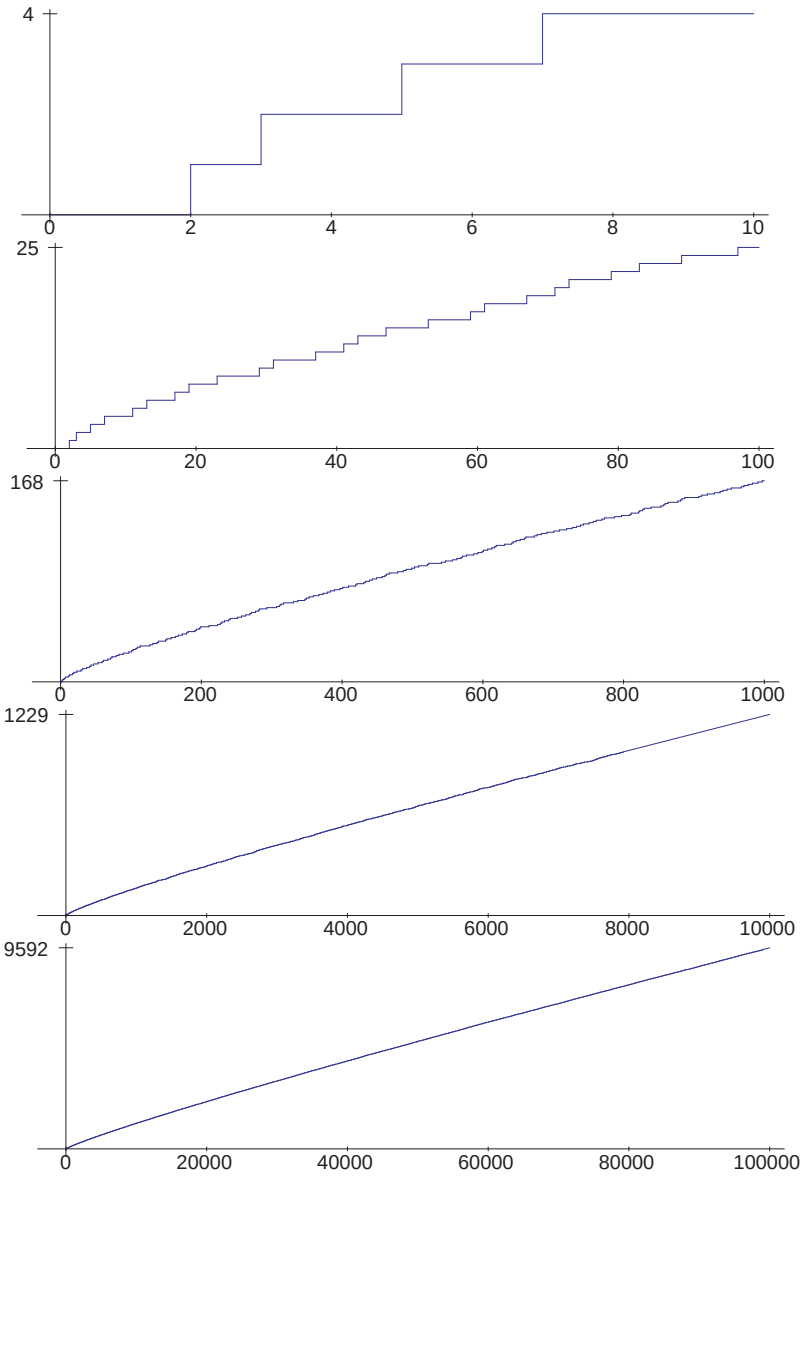
Bei den Primzahlen ist die Situat EULER meinte sogar, die Verteilu das der menschliche Verstand nie Abstand zwischen zwei verschi eins, der Abstand zwischen zwe einen Stelle vor, denn außer der ungerade.

Der Abstand zwei ist schon deut der Abstand zwischen drei und fü zahlen $10^{100} + 35737$ und $10^{100} +$ daß es unendlich viele solcher P Untersuchungen deuten sogar dar Größenordnung n bei ungefähr konnte noch niemand auch nur be

Eine obere Grenze für den Abstan Primzahlen gibt es genauso wenig und $2 \leq i \leq n$, so ist die Zahl Primzahl. Der Abstand zwische gleich $n! + 1$ und ihrem Nachfolg

Um einen ersten Eindruck von der men, betrachten wir den Graphen

$$\pi: \begin{cases} \mathbb{R}_{>0} \to \mathbb{N}_0 \\ x \mapsto \text{Anza} \end{cases}$$



Die Abbildungen auf der vorigen
null bis 10^i für $i = 1, \ldots, 5$. Wie
glatter, und bei den beiden letzten
sich um den Graphen einer diffe
Schreibweise $\pi(x)$ statt – wie bis

Auf den ersten Blick sieht diese
sich allerdings die Zahlenwerte
$\pi(x)$ etwas langsamer wächst al
$x/\log x$ ist eine deutlich bessere
auch mit unseren sehr elementare
beweisen:

Satz: Es gibt Konstanten $c_1, c_2 >$

$$c_1 \frac{x}{\log x} <$$

Beweis: Wir betrachten die neue

$$\vartheta(x) =$$

wobei ein Summationsindex p hie
soll, daß wir über alle *Primzahle*
schaft summieren.

Dann ist einerseits

$$\pi(x) = \sum_{p \le x} \frac{\log p}{\log p}$$

andererseits ist

$$\vartheta(x) = \sum_{p \le x} \log p \ge \sum_{\sqrt{x} < p \le x} \log$$

$$= \frac{1}{2} \log(x) \Big(\pi(x) - \pi\big(\sqrt$$

und damit auch $\pi(x) < \dfrac{2\vartheta(x)}{\log x} +$
zeigen können

1. Es gibt Konstanten $c_1, c_3 > 0$, so daß $c_1 x < \vartheta(x) < c_3 x$
2. $\displaystyle\sum_{p\le x} \frac{\log p}{p} = \log x + O(1)$,

dann folgt die Behauptung des Satzes.

Zum Beweis der ersten Aussage betrachten wir die Primzerlegung

$$n! = \prod_{p\le n} p^{e_p}$$

von $n!$. Unter den natürlichen Zahlen bis n sind $\left[\frac{n}{p}\right]$ durch p teilbar, $\left[\frac{n}{p^2}\right]$ durch p^2, *usw.;* daher ist

$$e_p = \sum_{k\ge 1} \left[\frac{n}{p^k}\right] \quad \text{und} \quad \log n! = \sum_{p\le n} e_p \log p = \sum_{p\le n}\sum_{k\ge 1} \left[\frac{n}{p^k}\right] \log p\,.$$

Die Summanden mit $k > 1$ liefern dabei nur einen kleinen Beitrag:

$$\sum_{p\le n}\sum_{k\ge 2} \left[\frac{n}{p^k}\right] \log p \le \sum_{p\le n} \left(\log p \cdot \sum_{k\ge 2} \frac{n}{p^k} \right) = n \sum_{p\le n} \frac{\log p}{p(p-1)}$$

nach der Summenformel für die geometrische Reihe:

$$\sum_{k\ge 2} \frac{1}{p^k} = \frac{1}{p^2} \cdot \frac{1}{1-\frac{1}{p}} = \frac{1}{p^2-p} = \frac{1}{p(p-1)}\,.$$

Zur weiteren Abschätzung ersetzen wir die Summe über alle Primzahlen kleiner oder gleich n durch die Summe über alle Zahlen bis n und beachten, daß für reellen $x \ge 2$ gilt $\log x < \sqrt{x}$, also

$$\frac{\log x}{x(x-1)} < \frac{\sqrt{x}}{x^2} = \frac{1}{x^{3/2}}:$$

$$\sum_{p\le n} \frac{\log p}{p(p-1)} \le \sum_{i=2}^{n} \frac{\log i}{i(i-1)} \le \sum_{i=2}^{n} \frac{1}{i^{3/2}}\,.$$

Da $\sum_{i=1}^{\infty} \frac{1}{i^s}$ für alle $s > 1$ konvergiert, konvergiert die rechts stehende Summe für $n \to \infty$ gegen einen endlichen Wert (ungefähr 1,612375), ist also $O(1)$, und damit ist $\sum_{k\ge 2} \frac{1}{p^k} = O(n)$. Setzen wir dies in die Formel für $\log n!$ ein, erhalten w
schätzungen, daß

$$\log n! = \sum_{p\le n}$$

Dies können wir vergleichen mit

$$\log n! = n \log$$

deren Beweis für Leser, die ihn no
Paragraphen skizziert ist. Kombin
nen Formel, ist also

$$\sum_{p\le n} \left[\frac{n}{p}\right] \log$$

Damit ist

$$\sum_{p\le 2n} \left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] \right) \log$$

Hier ist $\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]$ stets entw
Primzahlen p mit $n < p < 2n$ ist

$$\vartheta(2n) - \vartheta(n) = \sum_{n<p<2n} \log p \le$$

Die Formel $\vartheta(2n) - \vartheta(n) = O(n$
reelle Zahl x ersetzen; somit ist

$$\vartheta(x) = \sum_{i=0}^{\infty} \left(\vartheta\left(\frac{x}{2^i}\right) - \vartheta\left($$

womit die obere Schranke für $\vartheta($

Bevor wir uns der unteren Schra
die zweite Aussage. Natürlich ist

$$\sum_{p\le n} \frac{n}{p} \log p = \sum_{p\le n} \left[\frac{n}{p}\right] \log$$

$$= n \log n + O($$

denn wie wir gerade gesehen haben ist $\vartheta(n) = O(n)$. Kürzen wir die obige Formel durch n, erhalten wir die gewünschte Aussage

$$\sum_{p\le n} \frac{\log p}{p} = \log n + O(1)\,,$$

die natürlich auch dann gilt, wenn wir n durch eine reelle Zahl x ersetzen: Der Term $O(1)$ schluckt alle dabei auftretenden zusätzlichen Fehler.

Für $0 < \alpha < 1$ ist daher

$$\sum_{\alpha x<p\le x} \frac{\log p}{p} = \log x - \log \alpha x + O(1) = \log \frac{1}{\alpha} + O(1)\,,$$

wobei der Fehlerterm $O(1)$ nicht von α abhängt.

Da $\log \frac{1}{\alpha}$ für $\alpha \to 0$ gegen ∞ geht, ist für hinreichend kleine Werte von α und $x > c/\alpha$ für irgendein $c > 2$ beispielsweise

$$\sum_{\alpha x<p\le x} \frac{\log p}{p} > 10\,,$$

und für solche Werte von α und c ist dann

$$10 < \sum_{\alpha x<p\le x} \frac{\log p}{p} < \frac{1}{\alpha x} \sum_{\alpha x<p\le x} \log p \le \frac{\vartheta(x)}{\alpha x}\,.$$

Somit ist $10\alpha x < \vartheta(x)$, womit auch die untere Schranke aus der ersten Behauptung bewiesen wäre und damit der gesamte Satz. ∎

Der bewiesene Satz ist nur ein schwacher Abglanz dessen, was über die Funktion $\pi(x)$ bekannt ist. Zum Abschluß des Kapitels seien kurz einige der wichtigsten bekannten und vermuteten Eigenschaften von $\pi(x)$ zusammengestellt. Diese knappe Übersicht folgt im wesentlichen dem Artikel *Primzahlsatz* aus

> DAVID WELLS: Prime Numbers – The Most Mysterious Figures in Math, *Wiley*, 2005,

einer Zusammenstellung im Lexikonformat von interessanten Tatsachen und auch bloßen Kuriosa aus dem Umkreis der Primzahlen.

GAUSS kam 1792, im Alter von 15
zur Vermutung, daß $\pi(x)$ ungefäh
garithmus von x sein sollte:

$$\pi(x) \approx \mathrm{Li}$$

Auch LEGENDRE versuchte, $\pi(x)$
hern. Er stellte dazu eine Liste all
das sind immerhin 33 860 Stück,
Graphen von π möglichst gut an
Buch *Essai sur la théorie des nor*

$$\pi(x) \approx \frac{}{\log}$$

Über ein halbes Jahrhundert späte
sage: PAFNUTIJ L'VOVIČ ČEBYŠE
bekannt in der Schreibweise Tsch

$$\lim_{x\to\infty}$$

existiert, dann muß er den Wert e

1852 bewies er dann ein deutlich
große Werte von x ist

$$c_1 \cdot \frac{x}{\log x} < \pi(x) < c_2 \cdot \frac{x}{\log x}$$

1896 schließlich zeigten der fran
LOMON HADAMARD (1865–1963)
JEAN GUSTAVE NICOLAS BARON
unabhängig voneinander die Aus
kannt ist:

$$\pi(x)$$

Dies bedeutet nun freilich nicht, d
von LEGENDRE überflüssig wären

Funktionen asymptotisch gleich eins ist, erlaubt schließlich immer noch beträchtliche Unterschiede zwischen den beiden Funktionen: Nur der *relative* Fehler muß gegen null gehen.

Offensichtlich ist für jedes $a \in \mathbb{R}$

$$\lim_{x\to\infty} \frac{x/\log x}{x/(\log x - a)} = \lim_{x\to\infty} \frac{\log x - a}{\log x} = 1 - \lim_{x\to\infty} \frac{a}{\log x} = 1\,,$$

und es ist auch nicht schwer zu zeigen, daß

$$\lim_{x\to\infty} \frac{x/\log x}{\mathrm{Li}(x)} = 1$$

ist. Nach dem Primzahlsatz ist daher auch für jedes $a \in \mathbb{R}$

$$\pi(x) \sim \frac{x}{\log x - a} \quad \text{und} \quad \pi(x) \sim \mathrm{Li}(x)\,.$$

Wie DE LA VALLÉE POUSSIN zeigte, liefert der Wert $a = 1$ unter allen reellen Zahlen a die beste Approximation an $\pi(x)$, aber $\mathrm{Li}(x)$ liefert eine noch bessere Approximation. Für kleine Werte von x sieht man das auch in der folgenden Tabelle, in der alle reellen Zahlen zur nächsten ganzen Zahl gerundet sind. Wie kaum anders zu erwarten, liefert LEGENDREs Formel für 10^4 und 10^5 die besten Werte:

n	$\pi(n)$	$\frac{n}{\log n}$	$\frac{n}{\log n-1}$	$\frac{n}{\log n-1{,}08366}$	$\mathrm{Li}(n)$
10^3	168	145	169	172	178
10^4	1 229	1 086	1 218	1 231	1 246
10^5	9 592	8 686	9 512	9 588	9 630
10^6	78 489	72 382	78 030	78 534	78 628
10^7	664 579	620 420	661 459	665 138	664 918
10^8	5 761 455	5 428 681	5 740 304	5 769 341	5 762 209
10^9	50 847 478	48 254 942	50 701 542	50 917 519	50 849 235

Wenn wir genaue Aussagen über $\pi(x)$ machen wollen, sollten wir also etwas über die Differenz $\mathrm{Li}(x) - \pi(x)$ wissen. Hier kommen wir in das Reich der offenen Fragen, und nach derzeitigem Verständnis hängt alles ab von der oben erwähnten RIEMANNschen Zetafunktion. Nach einer berühmten Vermutung von RIEMANN haben alle nichttrivialen Nullstellen von $\zeta(s)$ den Realteil ein halb. Falls dies stimmt, ist

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x)\,.$$

Die RIEMANNsche Vermutung ist
bleme der heutigen Mathematik;
Probleme und ist auch eines der s
Lösung das CLAY Mathematics In
Preis von jeweils einer Million D
siehe http://www.claymath.o

Anhang: Die Eulersche Summe

Die EULERsche Summenformel e
Integral zurückzuführen und dad
handhabbar zu machen. Wir betr
bare Funktion f, deren Definition

Für eine reelle Zahl x bezeichnen
Zahl kleiner oder gleich x; außer
$\{x\} \underset{\text{def}}{=} x - [x]$ ein für den gebr
Zahl k ist somit $\{x\} = x - k$ für

Partielle Integration führt auf die

$$\int_k^{k+1} \big(\{x\} - \tfrac{1}{2}\big) f'(x)\,dx = \big(x$$

$$= \frac{f($$

Addition aller solcher Gleichung

$$\int_1^n \big(\{x\} - \tfrac{1}{2}\big) f'(x)\,dx = \frac{f(1)}{2}$$

womit man die Summe der $f(k)$

Satz (EULERsche Summenform
tion $f\colon D \to \mathbb{R}$, deren Definitio

ist

$$\sum_{k=1}^{n} f(k) = \int_1^n f(x)\,dx + \frac{f(1)+f(n)}{2} + \int_1^n \left(\{x\} - \tfrac{1}{2}\right) f'(x)\,dx\,.$$

■

Für die Abschätzung von $n!$ interessiert uns speziell der Fall, daß $f(x) = \log x$ der natürliche Logarithmus ist; hier wird die EULERsche Summenformel zu

$$\begin{aligned}\log n! &= \int_1^n \log x\,dx + \frac{\log n}{2} + \int_1^n \frac{\{x\} - \frac{1}{2}}{x}\,dx \\ &= x(\log x - 1)\Big|_1^n + \frac{\log n}{2} + \int_1^n \frac{\{x\} - \frac{1}{2}}{x}\,dx \\ &= n(\log n - 1) + 1 + \frac{\log n}{2} + \int_1^n \frac{\{x\} - \frac{1}{2}}{x}\,dx\,.\end{aligned}$$

In dieser Formel stört noch das rechte Integral; dieses können wir wie folgt abschätzen: Für eine natürliche Zahl k ist

$$\begin{aligned}\int_k^{k+1} \frac{\{x\} - \frac{1}{2}}{x}\,dx &= \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{x}{k + \frac{1}{2} + x}\,dx \\ = \int_0^{\frac{1}{2}} \left(\frac{x}{k + \frac{1}{2} + x} - \frac{x}{k + \frac{1}{2} - x}\right) dx &= \int_0^{\frac{1}{2}} \frac{-2x^2}{\left(k + \frac{1}{2}\right)^2 - x^2}\,dx\,.\end{aligned}$$

Im Intervall von 0 bis $\frac{1}{2}$ ist der Integrand monoton fallend, d.h.

$$0 \geq \frac{-2x^2}{\left(k + \frac{1}{2}\right)^2 - x^2} \geq \frac{-\frac{1}{2}}{\left(k + \frac{1}{2}\right)^2 - \frac{1}{4}} = \frac{-2}{(2k+1)^2 - 1} \geq -\frac{1}{2k^2}\,,$$

und damit ist

$$0 \geq \int_k^{k+1} \frac{\{x\} - \frac{1}{2}}{x}\,dx = \int_0^{\quad}$$

denn wir können das Integral ab
Länge des Integrationsintervalls
Summation von $k = 1$ bis $n - 1$ s

$$0 \geq \int_1^n \frac{\{x\} - \frac{1}{2}}{x}\,dx \geq$$

für das störende Integral aus der
konvergiert, konvergiert auch da
Grenzwert I. Somit ist

$$\log n! = n(\log n -$$

also folgt insbesondere die Absch

$$\log n! =$$

die wir im Beweis des Satzes übe

§2: Das Sieb des Eratosth

Das klassische Verfahren zur Be
einer bestimmten Schranke geht
vorchristlichen Jahrhundert. Es fu

Um alle Primzahlen kleiner oder g
man zunächst die Zahlen von eins

Eins ist nach Definition keine Pri
wie EUKLID war die Eins nicht ei
Eins durch. Die Zwei ist prim, abe
keine Primzahlen, werden also du
von jeder Zahl nachprüfen, ob s
streichen einfach nach der Zwei j

Die erste nichtdurchgestrichene Zahl der Liste ist dann die Drei. Sie muß eine Primzahl sein, denn hätte sie einen von eins verschiedenen kleineren Teiler, könnte das nur die Zwei sein, und alle Vielfachen von zwei (außer der Zwei selbst) sind bereits durchgestrichen.

Auch die echten Vielfachen der Drei sind keine Primzahlen, werden also durchgestrichen. Auch dazu streichen wir wieder einfach jede dritte Zahl aus der Liste durch, unabhängig davon, ob sie bereits durchgestrichen ist oder nicht. (Alle durch sechs teilbaren Zahlen sind offensichtlich schon durchgestrichen.)

Genauso geht es weiter mit der Fünf *usw.;* nach jedem Durchgang durch die Liste muß offenbar die erste noch nicht durchgestrichene Zahl eine Primzahl sein, denn alle Vielfache von kleineren Primzahlen sind bereits durchgestrichen, und wenn eine Zahl überhaupt einen echten Teiler hat, dann ist sie natürlich auch durch eine echt kleinere Primzahl teilbar.

Wie lange müssen wir dieses Verfahren durchführen? Wenn eine Zahl x Produkt zweier echt kleinerer Faktoren u, v ist, können u und v nicht beide größer sein als $\sqrt{x}$: Sonst wäre schließlich $x = uv$ größer als x. Also ist einer der beiden Teiler u, v kleiner oder gleich $\sqrt{x}$, so daß x mindestens einen Teiler hat, dessen Quadrat kleiner oder gleich x ist. Damit ist eine zusammengesetzte Zahl x durch mindestens eine Primzahl p teilbar mit $p^2 \leq x$.

ERATOSTHENES (Ερατοσθένες) wurde 276 v.Chr. in Cyrene im heutigen Libyen geboren, wo er zunächst von Schülern des Stoikers ZENO ausgebildet wurde. Danach studierte er noch einige Jahre in Athen, bis ihn 245 der Pharao PTOLEMAIOS III als Tutor seines Sohns nach Alexandrien holte. 240 wurde er dort Bibliothekar der berühmten Bibliothek im Museion.
Heute ist er außer durch sein Sieb vor allem durch seine Bestimmung des Erdumfangs bekannt. Er berechnete aber auch die Abstände der Erde von Sonne und Mond und entwickelte einen Kalender, der Schaltjahre enthielt. 194 starb er in Alexandrien, nach einigen Überlieferungen, indem er sich, nachdem er blind geworden war, zu Tode hungerte.

Für das Sieb des ERATOSTHENES, angewandt auf die Zahlen von eins

bis N heißt das, daß wir aufhö
durchgestrichene Zahl p ein Qu
sicher sein, daß jede zusammen
kleineren Primteiler als p hat und
noch nicht durchgestrichenen Zah

Damit lassen sich leicht von Hand
etwas Fleiß auch die bis Tausend,

Trotzdem kann uns ERATOSTHENE
wissen Zahlen nicht prim sind: W
$[a, b]$ suchen, d.h. also Primzahle

$$a \leq$$

so können wir ERATOSTHENES au
den wie gerade eben auf das Inter

Wir gehen aus von einer Liste p_1
wählen wir r so, daß die Chancen
Intervall $[a, b]$ noch einigermaße
einer Primzahl p_r, die ungefähr in
$b - a$ liegt.

Nun können wir mit jeder der Pri
Fall; wir müssen nur wissen, wo

Dazu berechnen wir für jedes p_i d
ist $a - r_i$ durch p_i teilbar, liegt a
erste Zahl, die wir streichen müs
an streichen wir einfach, ohne no
gehabt jede p_i-te Zahl durch.

Was nach r Durchgängen noch
aus $[a, b]$, die durch keine der P
zwar noch größere Primteiler hab
malem Aufwand für den Großteil
daß sie keine Primzahlen sind. F
fahren, aber die sind allesamt erhe
so daß sich diese erste Reduktion

§3: Fermat-Test und Fermat-Zahlen

Nach dem kleinen Satz von FERMAT gilt für jede Primzahl p und jede nicht durch p teilbare Zahl a die Formel $a^{p-1} \equiv 1 \bmod p$. Im Umkehrschluß folgt sofort:

Falls für eine natürliche Zahl $1 \le a \le p-1$ *gilt* $a^{p-1} \not\equiv 1 \bmod p$*, kann* p *keine Primzahl sein.*

Beispiel: Ist $p = 129$ eine Primzahl? Falls ja, ist nach dem kleinen Satz von FERMAT $2^{128} \equiv 1 \bmod 129$. Tatsächlich ist aber

$$2^7 = 128 \equiv -1 \bmod 129\,,$$

also hat die Zwei in $(\mathbb{Z}/129)^\times$ die Ordnung 14. Da 14 kein Teiler von 128 ist, kann $2^{128} \bmod 129$ nicht eins sein. (Wegen $128 \equiv 2 \bmod 14$ ist $2^{128} \equiv 2^2 = 4 \bmod 129$.) Somit ist 129 keine Primzahl.

Dieses Ergebnis hätten wir natürlich auch durch Probedivisionen leicht gefunden: Da 129 die Quersumme 12 hat, ist die Zahl durch drei teilbar; ihre Primzerlegung ist $129 = 3 \cdot 43$.

Keine Kopfrechenaufgabe ist die Frage, ob $F_{20} = 2^{2^{20}} + 1$ eine Primzahl ist. Falls ja, wäre nach dem kleinen Satz von FERMAT insbesondere

$$3^{F_{20}-1} = 1 \bmod F_{20}, \quad \text{also} \quad 3^{(F_{20}-1)/2} \equiv \pm 1 \bmod F_{20}\,.$$

Nachrechnen zeigt, daß dies nicht der Fall ist, allerdings ist das „Nachrechnen“ bei dieser 315 653-stelligen Zahl natürlich keine Übungsaufgabe für Taschenrechner: 1988 brauchte eine Cray X-MP dazu 82 Stunden, der damals schnellste Supercomputer Cray-2 immerhin noch zehn; siehe

JEFF YOUNG, DUNCAN A. BUELL: The Twentieth Fermat Number is Composite, *Math. Comp.* **50** (1988), 261–263.

Damit war gezeigt, daß F_{20} keine Primzahl ist. (Die anscheinend etwas weltabgewandt lebenden Autoren meinten, dies sei die aufwendigste bis dahin produzierte 1-Bit-Information.)

Umgekehrt können wir leider nicht folgern, daß p eine Primzahl ist, wenn für ein $a \in \mathbb{N}$ mit $1 < a < p-1$ gilt $a^{p-1} \equiv 1 \bmod p$. So ist beispielsweise $18^{322} \equiv 1 \bmod 32$
setzt. Immerhin gibt es nicht viel
einzigen Möglichkeiten sind $a =$

Es kann nicht vorkommen, daß f
alle $1 \le a \le n$ gilt $a^{n-1} \equiv 1$ m
so ist für jedes Vielfache a von
kann also nicht kongruent eins
Zumindest für die a mit ggT$(a,$
erfüllt sein.

Bei großen Zahlen n mit nur wen
solches a zu erwischen, recht k
beispiele sind, wird uns der FER
führen.

Definition: Eine natürliche Zah
sie keine Primzahl ist, aber trot
ggT$(a, n) = 1$ gilt: $a^{n-1} \equiv 1$ mo

ROBERT DANIEL CARMICHAEL (1879–19
unter anderem Bücher über die Relativität
über Gruppentheorie veröffentlichte. Ab
zeigte 1910, daß 561 die gerade definier
noch eine Reihe von Arbeiten über solche

Satz: Eine natürliche Zahl n ist
wenn sie das Produkt von minc
ungeraden Primzahlen ist, wobe
Teiler von $n-1$ ist.

Beweis: Sei zunächst $n = \prod p_i$
Primzahlen, für die $p_i - 1$ Teiler
Restesatz ist dann $(\mathbb{Z}/N)^\times \cong \prod$
die Ordnung eines jeden Element
$n-1$; also ist auch in $(\mathbb{Z}/n)^\times$ die
von $n-1$. Damit gilt für jedes z
$a^{n-1} \equiv 1 \bmod n$, d.h. n ist eine

Umgekehrt sei n eine CARMICHAEL-Zahl. Dann ist n ungerade, denn für gerade Zahlen n ist $(n-1)^{n-1} \equiv (-1)^{n-1} = -1 \bmod n$.

Als nächstes wollen wir uns überlegen, daß n Produkt verschiedener Primzahlen sein muß: Angenommen, in der Primzerlegung von n tritt eine Primzahl p mehrfach auf, d.h. $n = p^e q$ mit einer zu p teilerfremden Zahl q. Nach dem binomischen Lehrsatz gilt

$$(p+1)^{p^{e-1}} = \sum_{k=0}^{p^{e-1}} \binom{p^{e-1}}{k} p^k ,$$

und für alle $k \neq 0$ ist

$$\begin{aligned}\binom{p^{e-1}}{k} p^k &= \frac{p^{e-1}(p^{e-1}-1)\cdots(p^{e-1}-k+1)}{k!} p^k \\ &= p^{e-1} \cdot \frac{p^{e-1}}{1} \cdot \frac{p^{e-1}-2}{2} \cdots \frac{p^{e-1}-(k-1)}{k-1} \cdot \frac{p^k}{k} .\end{aligned}$$

In jedem der Brüche $(p^{e-1}-\ell)/\ell$ kommt p in Zähler und Nenner mit der gleichen Potenz vor, denn $\ell < p^{e-1}$ und $p^{e-1} - \ell \equiv -\ell \bmod p^{e-1}$. Im letzten Bruch p^k/k steht p im Zähler offensichtlich mit einer höheren Potenz als im Nenner; insgesamt ist der Ausdruck also mindestens durch p^e teilbar. Somit ist $(1+p)^{p^{e-1}} \equiv 1 \bmod p^e$; in $(\mathbb{Z}/p^e)^\times$ gibt es daher Elemente, deren Ordnung ein Vielfaches von p ist. Da nach dem chinesischen Restesatz $(\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p^e)^\times \times (\mathbb{Z}/q)^\times$ ist, gibt es dann auch in $(\mathbb{Z}/n)^\times$ ein solches Element a. Da $n-1$ nicht durch p teilbar ist, ist n kein Vielfaches dieser Ordnung, so daß a^{n-1} modulo n nicht eins sein kann. Damit ist n keine CARMICHAEL-Zahl; eine CARMICHAEL-Zahl muß also Produkt verschiedener Primzahlen sein.

Für jeden Primteiler p von n muß $p-1$ ein Teiler von $n-1$ sein, denn nach dem chinesischen Restesatz ist $(\mathbb{Z}/n)^\times$ das Produkt der Gruppen $(\mathbb{Z}/p)^\times$, es gibt also in $(\mathbb{Z}/n)^\times$ eine primitive Wurzel a modulo p. Da $a^{n-1} \equiv 1 \bmod n$ und damit insbesondere modulo p ist, muß $n-1$ ein Vielfaches der Ordnung $p-1$ von a modulo p sein.

Schließlich müssen wir uns noch überlegen, daß n ein Produkt von mindestens drei Primzahlen ist: Da n nach Definition keine Primzahl

ist, wäre $n = pq$ sonst das Produ
gesehen haben, müßte

$$n - 1 = pq - 1 = (p-1)q$$

sowohl durch $p-1$ als auch d
$p-1$ und $q-1$ durcheinander t
ausgeschlossen haben.

Als Beispiel können wir ein Prod
drei primen Faktoren betrachten,

$$1729 = 7 \times 13 \times 19 \quad \text{für } t =$$

für $t = 6$. Hier ist $n - 1 = 1296t^3$
offensichtlich durch $6t$, $12t$ und 1
Zahl.

Natürlich muß nicht jede CARMI
kleinste CARMICHAEL-Zahl beisp
keinen einzigen Primfaktor kongr

Eine größte CARMICHAEL-Zahl g

W.R. ALFORD, ANDREW GRANV
infinitely many Carmichael numb

gibt es unendlich viele. Konkr
CARMICHAEL-Zahlen kleiner od
destens gleich $x^{2/7}$ ist. Die tatsä
größer sein, ist aber immer noch s

Für große Zahlen p wird es zuneh
nur für ein a den FERMAT-Test be
nungen von

SU HEE KIM, CARL POMERAN
Probable Prime is Composite,

geben folgende obere Schranke f
zufällig gewählte Zahl p der angeg
Test mit einem vorgegebenen a
ist:

$p \approx 10^{60}$	10^{70}	10^{80}	10^{90}	10^{100}
$\varepsilon \leq 7{,}16 \cdot 10^{-2}$	$2{,}87 \cdot 10^{-3}$	$8{,}46 \cdot 10^{-5}$	$1{,}70 \cdot 10^{-6}$	$2{,}77 \cdot 10^{-8}$
$p \approx 10^{120}$	10^{140}	10^{160}	10^{180}	10^{200}
$\varepsilon \leq 5{,}28 \cdot 10^{-12}$	$1{,}08 \cdot 10^{-15}$	$1{,}81 \cdot 10^{-19}$	$2{,}76 \cdot 10^{-23}$	$3{,}85 \cdot 10^{-27}$
$p \approx 10^{300}$	10^{400}	10^{500}	10^{600}	10^{700}
$\varepsilon \leq 5{,}8 \cdot 10^{-29}$	$5{,}7 \cdot 10^{-42}$	$2{,}3 \cdot 10^{-55}$	$1{,}7 \cdot 10^{-68}$	$1{,}8 \cdot 10^{-82}$
$p \approx 10^{800}$	10^{900}	10^{1000}	10^{2000}	10^{3000}
$\varepsilon \leq 5{,}4 \cdot 10^{-96}$	$1{,}0 \cdot 10^{-109}$	$1{,}2 \cdot 10^{-123}$	$8{,}6 \cdot 10^{-262}$	$3{,}8 \cdot 10^{-397}$

(Sie geben natürlich auch eine allgemeine Formel an, jedoch ist diese zu grausam zum Abtippen.)

Wenn wir RSA-Moduln von 2048 Bit konstruieren wollen, brauchen wir etwa dreihundertstellige Primzahlen; hier liegt die Irrtumswahrscheinlichkeit bei einem einzigen FERMAT-Test also bei höchstens $5{,}8 \cdot 10^{-29}$. Wenn das zu hoch ist, kann man mit mehreren zufällig gewählten Basen testen und dadurch dir Fehlerwahrscheinlichkeit deutlich verringern – auch wenn es wohl gewagt wäre, zwei solche Tests als unabhängig anzunehmen.

Die Bundesnetzagentur empfiehlt, bei probabilistischen Primzahltests für die Erzeugung von RSA-Moduln eine Irrtumswahrscheinlichkeit von höchsten $2^{-100} \approx 7{,}89 \cdot 10^{-31}$ zuzulassen. Da die Wahrscheinlichkeiten in obiger Tabelle obere Schranken sind, könnte das vielleicht schon mit einem Test erreicht sein; besser sind auf jeden Fall mehrere oder, noch besser, ein Test, der wirklich *beweisen* kann, daß eine Zahl prim ist.

Einige Leute reden bei Zahlen, die einen FERMAT-Test bestanden haben, von „wahrscheinlichen Primzahlen“. Das ist natürlich Unsinn: Eine Zahl ist entweder *sicher* prim oder *sicher* zusammengesetzt; für Wahrscheinlichkeiten gibt es hier keinen Spielraum. Besser ist der ebenfalls gelegentlich zu hörende Ausdruck „industrial grade primes“, also „Industrieprimzahlen“, der ausdrücken soll, daß wir zwar nicht *bewiesen* haben, daß die Zahl wirklich prim ist, daß sie aber für (manche) „industrielle Anwendungen“ gut genug ist.

Zumindest grundsätzlich läßt sich der FERMAT-Test auch ausbauen zu einem echten Primzahltest; die
schwache Version eines Satzes vo

Satz: Ist für zwei natürliche Za
für jeden Primteiler q von $p-1$
Primzahl.

Beweis: Offensichtlich muß dann
$p-1$ sein. Wie wir aus Kapitel
nung $\varphi(p)$, und für jede zusam
angegebenen Formel leicht, daß
sein.

HENRY CABOURN POCKLINGTON (1870–
studierte an dem College, aus 1904 die U
denten dort auf Examen in London vorber
sowohl in Experimentalphysik als auch in
dene Stipendien des St. John's College i
fellow. 1896 erhielt er den Doktorgrad der
ausliefen, wurde er Physiklehrer an einer S
Pensionierung 1926, obwohl er mehrfach
sogar *fellow* der *Royal Society* wurde. Zwi
Arbeiten, zunächst hauptsächlich aus der
aber vor allem aus der Mathematik,

Der Nachteil des gerade bewiese
von $p-1$ kennen müssen; wenn
Dezimalstellen suchen, ist das m
Für Zahlen spezieller Bauart kann
Wenn wir von einer Zahl n mit
ausgehen, läßt sich so testen, ob

Die einfachsten Kandidaten für
eine ungerade Primzahl p ist alle
Primzahl. Auf den Fall $p = 2$ wer

Bei kleinen geraden Zahlen b m
gentlich Chancen, daß $b^r + 1$ ein
das nur selten vor. Ein Beispiel w

$p = 24^4 +$

Hier hat $p-1 = 24^4$ nur 2 und 3 als Primteiler, wir müssen also eine Zahl a finden, so daß

$$a^{p-1} \equiv 1 \bmod p, \quad a^{(p-1)/2} \not\equiv 1 \bmod p \quad \text{und} \quad a^{(p-1)/3} \not\equiv 1 \bmod p$$

ist. Dazu berechnen wir am besten zunächst $x = a^{(p-1)/6} \bmod p$, sodann $y = a^{(p-1)/3} \bmod p = x^2 \bmod p$ und $z = a^{(p-1)/2} \bmod p = x^3 \bmod p$. Wenn p eine Primzahl ist, muß offensichtlich $z \equiv -1 \bmod p$ sein, und wenn dies gilt, ist auch $a^{(p-1)} \equiv 1 \bmod p$.

Für $a = 2$ erhalten wir $x = 92553, y = 239223$ und $z = 1$; das beweist nichts. Für $a = 3$ ist sogar bereits $x = 1$, aber für $a = 5$ wird $x = 92554$, $y = 92553$ und $z = 331776 \equiv -1 \bmod p$. Dies *beweist*, daß p eine Primzahl ist.

Als nächstes wollen wir uns überlegen, wann $n = 2^r + 1$ prim sein kann. Für ungerade r ist n durch drei teilbar, denn $2^r \equiv (-1)^r \equiv -1 \bmod 3$; für $r > 1$ kann n dann also nicht prim sein. Auch wenn r nur durch eine ungerade Zahl $u > 1$ teilbar ist, kann $2^r + 1$ nicht prim sein, denn ist $r = uv$, so ist $2^r = (2^v)^u \equiv (-1)^u \equiv -1 \bmod 2^v + 1$, so daß $2^v + 1$ ein nichttrivialer Teiler ist. Die einzigen Kandidaten für Primzahlen sind daher die Zahlen

$$F_n = 2^{2^n} + 1\,,$$

bei denen der Exponent r eine Zweierpotenz ist. Sie heißen FERMAT-Zahlen, weil FERMAT zwischen 1630 und 1640 in mehreren Briefen, unter anderem an PASCAL und an MERSENNE, die Vermutung äußerte, diese Zahlen seien allesamt prim.

Für $F_0 = 3, F_1 = 5, F_2 = 17$ sieht man das mit bloßem Auge und mit auch $F_3 = 257$ gibt es keine nennenswerten Schwierigkeiten. Für größere Werte von n können wir den obigen Test anwenden; da 2 der einzige Primteiler von $F_n - 1$ ist, wird er hier einfach einfach zur folgenden Aussage:

Lemma: F_n ist genau dann eine Primzahl, wenn es ein a gibt mit

$$a^{(F_n-1)/2} \equiv -1 \bmod F_n\,.$$

■

Für $F_4 = 2^{16} + 1 = 65\,537$ ist
ein a finden, so daß $a^{2^{15}} \equiv -1$ n
nach 15 Quadrierungen das nutz
gewünschte -1. Damit ist F_4 als
wußte.

Für $F_5 = 2^{32} + 1 = 429\,4967\,29$
brauchen also schon 31 Quadrieru
nutzlose Eins, für $a = 3$ aber das
auch modulo F_5 deutlich von
Primzahl und FERMATs obige Ver
die einzige seiner vielen Vermutu

Der erste, der erkannte, daß F_5
GOLDBACH in Sankt Petersburg
gemacht hatte. Nachdem EULER
fand er 1732 schließlich die Fakto
EULER viel rechnete, fand er dies
systematisches Ausprobieren all
von F_5: dafür hätte er im schlimm
zahlen dividieren müssen!

Stattdessen benutzte EULER den k
Aussagen über mögliche Teiler v
fand

Lemma: Jeder Primteiler p von

Beweis: Ist $2^{2^n} \equiv -1 \bmod F_n$, s
$2^{2^{n+1}} \equiv 1 \bmod p$. Die Ordnung
von 2^{n+1}, also eine Zweierpotenz
ein Teiler von 2^n, so daß $2^{2^n} \equiv$
die genaue Ordnung. Diese muß a
Teiler der Gruppenordnung sein,
beweist.

Somit wußte EULER, daß jeder Pr
haben muß; Primzahlen dieser Fo

was das Problem schon viel handhabbarer erscheinen läßt. Dazu kam, daß er Glück hatte: Schon für $k = 10$ bekam er einen Teiler. Nach 193, 257, 449 und 577 ist 641 bereits die fünfte Primzahl dieser Form!

Tatsächlich aber machte er sich trotzdem zuviel Arbeit, denn wie der französische Mathematiker EDOUARD LUCAS (1842–1891) fand, gilt sogar

Lemma: Für $n \geq 3$ ist jeder Primteiler p von F_n kongruent eins modulo 2^{n+2}.

Beweis: Wir gehen genauso vor wie EULER, suchen aber ein Element von $\mathbb{F}_p^\times$, dessen Ordnung 2^{n+2} ist. Ein solches Element haben wir gefunden, wenn wir in $\mathbb{F}_p^\times$ ein x finden mit $x^2 = 2$. Wegen der Beziehung

$$\left(2^{2^{n-1}} + 1\right)^2 = 2^{2^n} + 1 + 2^{2^{n-1}+1} \equiv 2^{2^{n-1}+1} \bmod F_n$$

haben wir zunächst eine Zahl y gefunden mit $y^2 \equiv 2^u \bmod F_n$, wobei $u = 2^{n-1} + 1$ eine ungerade Zahl ist. Mit dem erweiterten EUKLIDischen Algorithmus können wir daher ganze Zahlen v, w finden mit $uv+2w = 1$. Damit ist auch

$$2 = 2^{uv+2w} = (2^u)^v \cdot (2^w)^2 = y^{2v} \cdot 2^{2w} = (y^v \cdot 2^w)^2$$

ein Quadrat in $\mathbb{F}_p^\times$. ∎

Mit dieser Verschärfung seines Lemmas hätte sich EULER auf Primzahlen der Form $128k + 1$ beschränken können und hätte bereits im zweiten Anlauf (nach einem vergeblichen Versuch mit 257) seinen Faktor gefunden.

Auch wenn er nie etwas darüber publiziert hat, hätte er auch beweisen können und bewies vielleicht auch, daß sein Kofaktor $q = 6\,700\,417$ ebenfalls eine Primzahl ist: Da jeder Primteiler p von q insbesondere auch F_5 teilt, muß $p \equiv 1 \bmod 128$ sein, und wenn es einen echten Teiler gibt, gibt es auch einen der kleiner ist als $\sqrt{q} \approx 2588{,}5$. Es gibt nur zwanzig Zahlen der Form $128k + 1$ unterhalb von $\sqrt{q}$, und nur fünf davon sind prim: Neben den bereits bekannten Kandidaten 257 und 641 sind das noch 769, 1153 und 1409. Fünf einfache Divisionen mit Rest

zeigen, daß q durch keine diese
bewiesen, daß auch q prim sein m

Die Suche nach FERMAT-Primzah
Zahlen beschäftigt auch heute no
kern; die jeweils neuesten Ergebn
ten von www.fermatsearch.org
daß F_n für $5 \leq n \leq 32$ sowie vi
setzt ist; oft sind auch zumindest
Primzahlen mit $n > 4$ wurden
auch noch nicht bewiesen, daß es
die *keine* Primzahlen sind.

Der oben angegebene Beweis vo
wir beim Primzahltest für F_4 m
ten: Da 2 modulo F_4 ein Quadr
$(F_4 - 1)/2$ gleich eins sein, de
Potenz der Wurzel aus 2. Aus dies
von F_{20} nicht mit $a = 2$ gearbei
effizienter gewesen wäre. Wie w
sehen werden, konnten sich die
leicht davon überzeugen, daß dr
der Aufwand für die Entscheidun
ist, erfordert einen Aufwand, der
EUKLIDischen Algerithmus auf a
nicht viel mehr als die Berechnu
als $(-1)^{2^{20}} + 1 = 2$ berechnen kan

Kehren wir zurück zu Primzahlte
$n - 1$ zumindest teilweise fakto
folgende Satz:

Satz: Angenommen $n = uv$ i
Zahlens $u < v$, und wir kennen
Falls es ein $a \in \mathbb{N}$ gibt, so daß a^n

$$\text{ggT}\left(a^{(n-1)/q_i} -\right.$$

ist n eine Primzahl.

Beweis: Angenommen, p sei ein echter Primteiler von n, und a erfülle die angegebenen Bedingungen. Die Ordnung der Restklasse von a in $(\mathbb{Z}/p)^\times$ sei r; sie ist natürlich ein Teiler von $p-1$.

Da $a^{n-1} \equiv 1 \bmod n$ und damit erst recht modulo des Teilers p, ist r auch Teiler von $n-1$; da $a^{(n-1)/q_i} - 1$ aber teilerfremd zu n ist, ist $a^{(n-1)/q_i}$ nicht kongruent eins modulo p; die Ordnung r teilt also keine der Zahlen $(n-1)/q_i$. Somit teilt r zwar das volle Produkt $u\prod q_i^{e_i}$, nicht aber das Produkt, in dem auch nur ein Exponent e_i erniedrigt wurde. Somit ist r für jedes i ein Vielfaches von $q_i^{e_i}$ und damit auch ein Vielfaches von v. Da r ein Teiler von $p-1$ ist, folgt insbesondere daß $v < p$ sein muß. Nun ist aber $n = uv$ und $u < v$, d.h. $v > \sqrt{n}$. Damit haben wir gezeugt, daß jeder echte Primteiler von n größer als $\sqrt{n}$ sein muß. Da dies unmöglich ist, gibt es keine echten Primteiler, d.h. n ist eine Primzahl. ∎

§4: Der Test von Miller und Rabin

Der Test von MILLER und RABIN ist eine etwas strengere Version des Tests von FERMAT: Um zu testen, ob p eine Primzahl sein kann, schreiben wir $p-1$ zunächst als Produkt $2^n u$ einer Zweierpotenz und einer ungeraden Zahl; sodann berechnen wir $a^u \bmod p$. Falls wir das Ergebnis eins erhalten, ist erst recht $a^{p-1} \equiv 1 \bmod p$, und wir können nicht folgern, daß p zusammengesetzt ist.

Andernfalls quadrieren wir das Ergebnis bis zu n-mal modulo p. Falls dabei nie eine Eins erscheint, folgt nach FERMAT, daß p zusammengesetzt ist. Falls vor der ersten Eins eine von -1 (*bzw.* $p-1$) verschiedene Zahl erscheint, folgt das auch, denn im Körper $\mathbb{F}_p$ hat die Eins nur die beiden Quadratwurzeln ± 1. In allen anderen Fällen erfahren wir nicht mehr als bei FERMAT.

Algorithmisch funktioniert der Test also folgendermaßen:

Schritt 0: Wähle ein zufälliges a, schreibe $p - 1 = 2^n u$ mit einer ungeraden Zahl u und berechne $b = a^u \bmod p$. Falls dies gleich Eins ist, endet der Algorithmus und wir konnten nicht zeigen, daß p eine zusammengesetzte Zahl ist; sie kann prim sein.

Schritt $i, 1 \le i \le n$**:** Falls b
und wir können nicht ausschließe
frühestens im zweiten Schritt der
und der Algorithmus endet. And
und es geht weiter mit Schritt $i +$

Schritt $n + 1$**:** Der Algorithmus
mengesetzt ist.

Beispiel: Ist 247 eine Primzahl?
247 = 1 ist, können wir mit FERMA
Da aber $77^{123} \bmod 247 = 77$ ist,
und RABIN im zweiten Schritt, w
daß die Zahl zusammengesetzt se

Hätten wir allerdings mit $a = 87$ g
$87^{123} \equiv 1 \bmod 247$ berechnet un
mengesetzt erkannt.

GARY L
men sei
sität vo
probabi
mer die
dies hie
Basen
noch of
richtig.
Univers
Mellon
hauptsä
metrie.

MICHAE
Familie
chen U
Nach se
er 1957
chen U
mathem
ist er
Lehrstu
Seine F

Preis erhielt, beschäftigen sich mit der Komplexität mathematischer Operationen und der Sicherheit von Informationssystemen. Seine home page in Harvard ist zu finden unter www.seas.harvard.edu/directory/Rabin .

Anscheinend wurde der Test von MILLER und RABIN bereits 1974, also vor MILLERs Veröffentlichung, von SELFRIDGE verwendet; daher sieht man gelegentlich auch die korrektere Bezeichnung *Test von* MILLER, RABIN *und* SELFRIDGE.

Der amerikanische Mathematiker JOHN L. SELFRIDGE promovierte 1958 an der University of California in Los Angelos. Bis zu seiner Emeritierung lehrte er an der Northern Illinois University. Seine Arbeiten befassen sich vor allem mit der analytischen sowie der konstruktiven Zahlentheorie. Vierzehn davon schrieb er mit PAUL ERDŐS. math.niu.edu/faculty/index.php?cmd=detail&id=91

§5: Der Test von Agrawal, Kayal und Saxena

Im August 2002 stellten MANINDRA AGRAWAL, NEERAJ KAYAL und NITIN SAXENA, zwei Bachelor-Studenten am Indian Institute of Technology in Kanpur und ihr Professor, einen Primzahltest vor, der ebenfalls auf dem kleinen Satz von FERMAT beruht, aber (natürlich auf Kosten eines erheblich größeren Aufwands) immer die richtige Antwort liefert; er ist inzwischen erschienen in

> MANINDRA AGRAWAL, NEERAJ KAYAL, NITIN SAXENA: PRIMES is in P, *Annals of Mathematics* **160** (2004), 781-793.

Selbstverständlich war dies nicht der erste Primzahltest, der deutlich schneller als Probedivisionen zeigt, ob eine gegebene Zahl prim ist oder nicht; es ist auch bei weitem nicht der schnellste solche Test. Er hat aber gegenüber anderen solchen Tests zwei Besonderheiten:

1. Zu seinem Verständnis ist – nach einigen in der letzten Zeit gefundenen Vereinfachungen – nur elementare Zahlentheorie notwendig.
2. Es ist der bislang einzige Test, von dem man beweisen kann, daß seine Laufzeit für n-stellige Zahlen durch ein Polynom in n begrenzt werden kann.

MANINI
1991 se
Technol
fenthalt
seither
hauptsä
von Alg
ENA erl
den Gö
veröffen
formati

http:/

NEERAJ
seinen
AGRAW
pur. Ne
mit der
chen Ri
nomgle
kurzen
inzwisc

http:/
people

NITIN S
nen Bac
MANINI
ogy in
tation ü
auf Frag
ein Jahr
danach
tum Co
Centrun
2006–2
CENTER
fessur a
Sein Int
bra und
theorie.

http:/

Für uns ist vor allem der erste Punkt wichtig; der zweite ist zwar ein für Komplexitätstheoretiker sehr interessantes Ergebnis, hat aber keinerlei praktische Bedeutung: Im Buch

> VICTOR SHOUP: A computational Introduction to Number Theory and Algebra, *Cambridge University Press*, ^{2}2008 (*Volltext* unter `http://shoup.net/ntb/`),

dem dieser Paragraph im wesentlichen folgt, argumentiert SHOUP, daß alternative Algorithmen, so man sich auf Zahlen von weniger als 2^{256} Bit beschränkt, durch eine vergleichbare Schranke abgeschätzt werden können, und natürlich sind die Zahlen, mit denen wir es üblicherweise zu tun haben, deutlich kleiner. In der Praxis sind die alternativen Algorithmen deutlich schneller.

(2^{256} liegt knapp über 10^{77}; derzeitige Schätzungen für die Anzahl der Nukleonen im Universum liegen bei etwa 10^{80}. Damit ist klar, daß kein Computer, der mit irgendeiner Art von heute bekannter Technologie arbeitet, je eine solche Zahl speichern kann, geschweige denn damit rechnen.)

Im folgenden wird es daher nur um eine mathematische Betrachtung des Algorithmus von AGRAWAL, KAYAL und SAXENA gehen; für einen (kurzen und elementaren) Beweis der Komplexitätsaussage sei beispielsweise auf das zitierte Buch von SHOUP verwiesen.

Die Grundidee des Algorithmus steckt im folgenden

Satz: $n > 1$ sei eine natürliche Zahl und $a \in \mathbb{N}$ sei dazu teilerfremd. n ist genau dann prim, wenn im Polynomring über $\mathbb{Z}/N$ gilt:

$$(X + a)^n = X^n + a\,.$$

Beweis: Nach dem binomischen Lehrsatz ist

$$(X + a)^n = X^n + a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i X^{n-i}\,.$$

Für eine Primzahl n gilt nach den
Gleichung $a^n = a$. Außerdem ist
fizient

$$\binom{n}{i} = \frac{n(n-$$

durch n teilbar, da n Faktor des
Somit verschwinden in $\mathbb{Z}/n$ alle
Gleichung aus dem Satz ist bewie

Umgekehrt sei n eine zusamme
von n. Genauer sei $n = p^e m$ m
Dann ist der Zähler von $\binom{n}{p}$ gena
$(n-1), \ldots, (n-p+1)$ sind alle
ist genau durch p teilbar. Somit
aber durch p^e und damit erst rec
über $\mathbb{Z}/n$ ausmultiplizieren, kann
verschwinden, und damit kann di

In dieser Form führt der Satz alle
len Primzahltest: Das Ausmultipl
auf $n+1$ Summanden, der Auf
damit vergleichbar damit, daß wi
nachprüfen, ob n ohne Rest durc
Idee von AGRAWAL, KAYAL und
es bereits reicht, Gleichungen d
nem geeigneten Polynom $X^r -$
nachzuprüfen.

Konkret geht ihr Algorithmus fol

n sei die zu testende natürliche Z
ihrer Binärziffern.

1. Schritt: Stelle sicher, daß n k
Zahl ist.

Das läßt sich beispielsweise da
Quadratwurzel, Kubikwurzel *us*

erkennt, daß es sich um keine natürliche Zahl handelt. Der ungünstigste Fall ist offenbar der, daß n eine Zweierpotenz sein könnte; man muß also bis zur $[\log_2 n]$-ten Wurzel gehen.

2. Schritt: Finde die kleinste natürliche Zahl $r > 1$ mit der Eigenschaft, daß entweder $\mathrm{ggT}(n, r) > 1$ ist oder aber $\mathrm{ggT}(n, r) = 1$ ist und n mod r in $(\mathbb{Z}/r)^\times$ eine größere Ordnung als $4\ell(n)^2$ hat.

Dies geschieht einfach dadurch, daß man die Zahlen $r = 2, 3, \ldots$ allesamt durchprobiert, bis zum ersten mal eine der beiden Bedingungen erfüllt ist. Die Bedingung über die Ordnung der Restklasse von n in $(\mathbb{Z}/r)^\times$ prüft man nach, indem man nacheinander ihre Potenzen ausrechnet, bis man entweder eine Eins gefunden hat oder aber der Exponent größer als $4\ell(n)^2$ ist.

3. Schritt: Falls $r = n$, ist n prim und der Algorithmus endet.

In der Tat: Dann haben wir für alle $r < n$ überprüft, daß $\mathrm{ggT}(n, r) = 1$ ist. Wenn der Algorithmus etwas taugt, darf er natürlich höchstens für sehr kleine Werte von n mit diesem Schritt enden.

4. Schritt: Falls im zweiten Schritt ein r gefunden wurde, für das der ggT von n und r größer als eins ist, muß n zusammengesetzt sein und der Algorithmus endet.

Denn dann haben wir einen Teiler von n gefunden.

Andernfalls kennen wir nun eine zu n teilerfremde Zahl r, für die n mod r in $(\mathbb{Z}/r)^\times$ eine größere Ordnung als $4\ell(n)^2$ hat.

5. Schritt: Teste für $j = 1, \ldots, \ell \underset{\text{def}}{=} 2\ell(n)[\sqrt{r}] + 1$, ob über $\mathbb{Z}/n$

$$(X + j)^n \equiv X^n + j \bmod (X^r - 1)\,.$$

Sobald ein j gefunden wird, für das dies nicht erfüllt ist, endet der Algorithmus mit dem Ergebnis n *ist zusammengesetzt.*

Falls nämlich n eine Primzahl ist, stimmen $(X + j)^n$ und $X^n + j$ als Polynome mit Koeffizienten aus $\mathbb{Z}/n$ nach obigem Satz überein, sind also erst recht auch gleich modulo $(X^r - 1)$.

6. Schritt: Wenn alle Tests im fünften Schritt bestanden sind, ist n eine Primzahl.

Dies zu beweisen ist die Hauptarb

Nach den Kommentaren zu den
Algorithmus für eine Primzahl n
müssen zeigen, daß er auch zusar

Sei also n eine zusammengesetz
natürlichen Zahl ist, wird dies im
werden im folgenden daher annel

Das r aus dem zweiten Schritt
denn als zusammengesetzte Zahl
Der Algorithmus kann daher nic
„n ist prim“ enden. Falls er im vi
Schritt einen Teiler von n, und w
zusammengesetzt“.

Für den Rest des Paragraphen k
zweite Schritt auf ein r führte, f
zeigen, daß einer der Tests im für
natürliche Zahl j gibt mit

$$1 \le j \le \ell \quad \text{und} \quad (X + j)^n \not\equiv$$

Wir nehmen an, das sei nicht der
von n. Dieser muß größer als r s
bereits mit dem vierten Schritt sp

Jede Kongruenz modulo n ist ers
können daher davon ausgehen, da

$$(X + j)^n \equiv X^n + j$$

Wenn wir zum Faktorring $R = \mathbb{F}_p$

$$(X + j)^n = X^n +$$

Um diese seltsame Relation gena
jede zu r teilerfremde natürliche

$$\widehat{\sigma}_k\colon \begin{cases} \mathbb{F}_p[X] \to \\ g \mapsto g \end{cases}$$

die in jedem Polynom g die Varia

Lemma: $\widehat{\sigma}_k$ ist surjektiv und sein Kern besteht genau aus den Vielfachen des Polynoms $X^r - 1$.

Beweis: Wir betrachten $\widehat{\sigma}_k$ nur für Indizes k, die zu r teilerfremd sind. Zu jedem solchen Index gibt es daher ein k', so daß $kk' \equiv 1 \bmod r$ ist, und modulo $X^r - 1$ ist damit $X^{kk'} \equiv X$. Für ein beliebiges Polynom $g \in \mathbb{F}_p[X]$ und $h(X) = g(X^{k'})$ ist daher in R

$$\widehat{\sigma}_k(h) = h(X^k) = g(X^{kk'}) = g(X) = g\,,$$

die Abbildung ist also surjektiv.

Was ihren Kern betrifft, so enthält er auf jeden Fall $X^r - 1$ und alle seine Vielfachen, denn

$$\widehat{\sigma}_k(X^r - 1) = (X^{kr} - 1) \bmod (X^r - 1) = 1^k - 1 = 0\,,$$

da $X^r \equiv 1 \bmod (X^r - 1)$.

Umgekehrt sei g irgendein Polynom aus dem Kern von $\widehat{\sigma}_k$. Dann ist das Polynom $h(X) = g(X^k)$ modulo $X^r - 1$ gleich dem Nullpolynom, ist also ein Vielfaches von $X^r - 1$. Konkret sei $h = (X^r - 1)f$. Im Faktorring R ist dann

$$g(X) = g(X^{kk'}) = h(X^{k'}) = (X^{k'r} - 1)f(X^{k'}) = 0\,,$$

denn wegen $X^r = 1$ in R ist dort $X^{k'r} - 1 = 0$.

In $\mathbb{F}_p[X]$ muß $g(X)$ daher ein Vielfaches von $X^r - 1$ sein, und genau das war die Behauptung über den Kern von $\widehat{\sigma}_k$. ∎

Da alle Vielfachen von $X^r - 1$ im Kern von $\widehat{\sigma}_k$ liegen, definiert $\widehat{\sigma}_k$ eine Abbildung σ_k von R nach R, die jedem Polynom g mod $(X^r - 1)$ aus R das Element $\widehat{\sigma}_k(g)$ zuordnet; nach dem gerade bewiesenen Lemma hängt dieses wirklich nur von der Restklasse g mod $(X^r - 1)$ ab. Außerdem zeigt das Lemma, daß σ_k sowohl surjektiv als auch injektiv ist, denn der Kern von $\widehat{\sigma}_k$ ist gleich dem Kern der Restklassenabbildung von $\mathbb{F}_p[X]$ nach R. Damit ist σ_k ein bijektiver Homomorphismus von R nach R, ein sogenannter *Automorphismus* von R. Wir haben damit für jede zu r teilerfremde natürliche Zahl k einen Automorphismus $\sigma_k\colon R \to R$, der jedem Polynom in X das entsprechende Polynom in X^k zuordnet. Da wir in R rechnen, werden natür
betrachtet.

Unmittelbar aus der Definition fo
phismen σ_k miteinander kommut

$$\sigma_k \circ \sigma_{k'} =$$

denn in allen drei Fällen wird im

Speziell für das Element $X + j$ au
und $j = 1, \ldots, \ell$ ist andererseits a

$$\sigma_n(X +$$

denn für diese j wurde ja nach u
Schritt bestanden.

Wir wollen genauer untersuchen,
ist. Dazu definieren zwei Arten v

$$C(f) = \left\{k \in (\mathbb{Z}/r)^\times \;\middle|\; \sigma_k(f\right.$$
$$D(k) = \left\{f \in R \;\middle|\; \sigma_k(f) = f\right.$$

Beide Mengen enthalten mit zwe
für zwei Elemente $k, k' \in C(f)$ i

$$\sigma_{kk'}(f) = \sigma_k(f)\sigma_{k'}(f) = \sigma_k\big(\sigma$$

und für $f, g \in D(k)$ ist

$$\sigma_k(fg) = \sigma_k(f)\sigma$$

Der Rest des Beweises besteht
ge $D(n)$ auf zwei verschiedene
Widerspruch herleiten zur Annah
trotzdem vom Algorithmus als Pr
ren zunächst zwei neue Zahlen:

- s sei die Ordnung der Restkl
  Teiler von $p^s - 1$, denn $p^s \equiv$

- t sei die Ordnung der von den Restklassen von p und n erzeugten Untergruppe von $(\mathbb{Z}/r)^\times$, d.h also die Ordnung der kleinsten Untergruppe, die beide Restklassen enthält. Da diese Untergruppe insbesondere die Restklasse von p und deren Potenzen enthält, ist t ein Vielfaches von s.

Als nächstes betrachten wir einen Körper K mit p^s Elementen. Einen solchen Körper kann man konstruieren, indem man den Vektorraum $\mathbb{F}_p^s$ identifiziert mit dem Vektorraum aller Polynome vom Grad kleiner s mit Koeffizienten aus $\mathbb{F}_p$ und dort eine Multiplikation einführt, die zwei Polynomen deren Produkt modulo einem festen irreduziblen Polynom vom Grad s über $\mathbb{F}_p$ zuordnet. Man kann zeigen (siehe Algebra-Vorlesung oder entsprechendes Lehrbuch), daß es für jedes s ein solches Polynom gibt, und daß zwei verschiedene irreduzible Polynome vom Grad s zu isomorphen Körpern führen.

Aus Kapitel 1 wissen wir, daß die multiplikative Gruppe jedes endlichen Körpers zyklisch ist; $K^\times$ ist also eine zyklische Gruppe der Ordnung $p^s - 1$. Diese Zahl ist, wie wir gerade gesehen haben, ein Vielfaches von r; somit gibt es in $K^\times$ (mindestens) ein Element ζ der Ordnung r. Für irgendein solches Element definieren wir einen Homomorphismus

$$\widehat{\tau}\colon \begin{cases} \mathbb{F}_p[X] \to K \\ \qquad g \mapsto g(\zeta) \end{cases} .$$

Da $\widehat{\tau}(X^r - 1) = \zeta^r - 1$ verschwindet, induziert $\widehat{\tau}$ einen Ringhomomorphismus $\tau\colon R \to K$. Die angekündigten Abschätzungen der „Größe“ von $D(n)$ beziehen sich auf die Mächtigkeit der Menge $S = \tau\big(D(n)\big)$:

Lemma: $S = \tau\big(D(n)\big)$ hat höchstens $n^{2[\sqrt{t}]}$ Elemente.

Beweis: Wir gehen davon aus, daß n weder eine Primzahl noch eine Primzahlpotenz ist; daher gibt es außer dem Primteiler p noch mindestens einen weiteren Primteiler q. Wenn wir (in $\mathbb{N}$) Potenzen der Form $n^u p^v$ und $n^{u'} p^{v'}$ mit $u, u', v, v' \in \mathbb{N}_0$ betrachten, sind diese daher genau dann gleich, wenn $(u, v) = (u', v')$ ist: Ist nämlich $u \neq u'$, so tritt g in der Primzerlegung der beiden Elemente mit verschiedenen Exponenten

auf, und ist $u = u'$, aber $v \neq v'$, s
die Menge

$$I = \{n^u p^v \mid$$

mindestens $\big([\sqrt{t}]+1\big)^2$ Elemente,
als t.

Nun war aber t definiert als die O
die von den Restklassen von n u
mindestens zwei Elemente

$$k = n^u p^v \quad u$$

aus I geben, die dieselbe Restkla
gilt: $k \equiv k' \bmod r$. Da die Expon
sind und p ein Teiler von n ist, kö
Schranke für k und k' nehmen.

Nun sei $f \in R$ ein Element vor
$C(f)$ und $D(n)$ ist dann auch n ei
$C(f)$ stets die Eins und nach de
Primzahl p, denn Potenzieren mit
mit zwei Elementen stets auch de
die Restklassen modulo r aller E
sind daher k und k' Elemente vor

$$\sigma_k(f) = f^k \quad$$

Wegen $k \equiv k' \bmod r$ ist aber σ_k
$f^k = f^{k'}$ für jedes $f \in D(n)$. So
Nullstellen des Polynoms $X^k -$
von k und k', und da $\tau(f)$ im Kör
Nullstellen, wie der Grad angibt.
k und k' hat das Polynom daher h
kann auch S nicht mehr Element

Als untere Grenze für die Elemen

Lemma: S enthält mindestens $2^{\min(t,\ell)} - 1$ Elemente.

Beweis: Wegen der bestandenen Tests in Schritt 5 liegt $\tau(X+j)$ in $D(n)$ für $j = 1, \ldots, \ell$. Da $p > r > t \geq m$ ist, sind die Zahlen von 1 bis m auch modulo p paarweise verschieden. Die Teilmenge

$$P = \Big\{ \prod_{j=1}^{m} (X+j)^{e_j} \;\Big|\; e_j \in \{0,1\} \text{ und } \sum_{j=1}^{m} e_j < m \Big\}$$

von $\mathbb{F}_p[X]$ enthält daher $2^m - 1$ Polynome.

Aus diesen Polynomen können wir Elemente von R *bzw.* K machen, indem wir für die Variable X die Restklasse $\eta = X \bmod (X^r - 1)$ *bzw.* das oben gewählte Element ζ der Ordnung r einsetzen; wir erhalten Teilmengen

$$P(\eta) = \big\{ f(\eta) \;\big|\; f \in P \big\} \subseteq R \quad \text{und} \quad P(\zeta) = \big\{ f(\zeta) \;\big|\; f \in P \big\} \subseteq K\,.$$

Da sowohl n als auch p in $D(n)$ liegen und mit zwei Elementen auch deren Produkt, liegt $P(\eta)$ in $D(n)$ und damit $\tau\big(P(\eta)\big) = P(\zeta)$ in S. Das Lemma ist daher bewiesen, sobald wir gezeigt haben, daß $P(\zeta)$ mindestens $2^m - 1$ Elemente enthält.

Falls dies nicht der Fall wäre, müßte es in P zwei verschiedene Polynome g und h geben, für die $g(\zeta) = h(\zeta)$ wäre. Wir müssen also zeigen, daß $g(\zeta) = h(\zeta)$ nur dann gelten kann, wenn $g = h$ ist.

Wie im vorigen Lemma folgt, da $1, p$ und n alle drei sowohl in $C\big(g(\eta)\big)$ als auch in $C\big(h(\eta)\big)$ liegen, daß alle natürlichen Zahlen k der Form $k = n^u p^v$ in diesen beiden Mengen liegen.

Da $g(\zeta) = h(\zeta)$, gilt für jedes solche k

$$\begin{aligned} 0 &= g(\zeta)^k - h(\zeta)^k = \tau\big(g(\eta)\big)^k - \tau\big(h(\eta)\big)^k = \tau\big(g(\eta)^k\big) - \tau\big(h(\eta)^k\big) \\ &= \tau\big(g(\eta^k)\big) - \tau\big(h(\eta^k)\big) = g(\zeta^k) - h(\zeta^k)\,. \end{aligned}$$

Da ζ in K die Ordnung r hat, hängt ζ^k nur von k mod r ab; die Anzahl verschiedener Restklassen der Form $n^u p^v$ modulo r hatten wir oben mit t bezeichnet. Somit hat die Differenz $g - h$ mindestens t Nullstellen. Andererseits sind aber g und h und damit auch ihre Differenz Polynome

vom Grad höchstens $t - 1$, also
$g = h$. Somit enthält S mindesten

Zum Abschluß des Beweises, da
SAXENA stets die richtige Antw
zeigen, daß die Schranken aus de
der Voraussetzung bewiesen wurd
prim erkannt wird, einander wide
größer ist als die obere:

Lemma: $2^{\min(t,\ell)} - 1 > n^{2[\sqrt{t}]}$.

Beweis: Da $\ell(n) > \log_2 n$, genüg

$$2^{\min(t,\ell)} -$$

Da beide Exponenten natürliche
daß $\min(t,\ell) > 2\ell(n)[\sqrt{t}]$ ist,
mindestens eins unterscheiden, is
mindestens zwei. Wir müssen d
größer sind als $2\ell(n)[\sqrt{t}]$.

Für $\ell = 2\ell(n)[\sqrt{r}] + 1$ ist das kla
von $(\mathbb{Z}/r)^\times$ bezeichnet und dami

Die Ungleichung $t > 2\ell(n)[\sqrt{t}]$
$t > 2\ell(n)\sqrt{t}$ ist, und dies wied
$t > 4\ell(n)^2$. Nun ist aber t die Or
die von den Restklassen von n u
Schritt des Algorithmus sicherges
der Restklasse von n schon größer
für t trivial.

Damit ist die Korrektheit des Alg

Kapitel 4
Faktorisierungsverfahren

Die MERSENNE-Zahl $M_{67} = 2^{67} - 1$ ist keine Primzahl, denn

$$13^{M_{67}-1} \equiv 81\,868\,480\,399\,682\,966\,751 \not\equiv 1 \bmod M_{67}\,.$$

Somit ist M_{67} ein Produkt von mindestens zwei nichttrivialen Faktoren. Welche sind das?

FRANK NELSON COLE gab das Ergebnis am 31. Oktober 1903 auf einer Sitzung der American Mathematical Society bekannt: Er schrieb die Zahl

$$2^{67} - 1 = 147\,573\,952\,589\,676\,412\,927$$

auf eine der beiden Tafeln und

$$193\,707\,721 \times 761\,838\,257\,287$$

auf die andere. Dieses Produkt rechnete er wortlos aus nach der üblichen Schulmethode zur schriftlichen Multiplikation, und als er dieselbe Zahl erhielt, die auf der anderen Tafel stand, schrieb er ein Gleichheitszeichen zwischen die beiden Zahlen und setzte sich wieder. Das Ergebnis, d.h. die Faktorisierung von M_{67}, findet ein Computeralgebrasystem heute in weniger als einer Sekunde; für die damalige Zeit war sie eine Sensation! COLE gab später zu, daß er drei Jahre lang jeden Sonntag nachmittag daran gearbeitet hatte. Er versuchte M_{67} in der Form $x^2 - y^2$ darzustellen, wobei er mit Hilfe quadratischer Reste Kongruenzbedingungen für x modulo verschiedener relativ kleiner Primzahlen aufstellte und auch verwendete, daß jeder Teiler von M_{67} kongruent eins modulo 67 und kongruent ± 1 modulo acht sein muß. Dies führte zu einer ganzen Reihe von Kongruenzen für x, die er in

$$x \equiv 1\,160\,932\,384 \bmod 1\,323\,536\,760$$

zusammenfassen konnte. Untersu

$$x_k = 1\,323\,536\,7$$

frühestens für $k = 287$ in Frage k

$$M_{67} = 381\,015\,982$$
$$= 193\,707\,721$$

Für Einzelheiten siehe

F. N. COLE: On the factoring
Soc. **10** (1903), 134–137 o
bull/1903-10-03/S0002-990

FRANK
sachuse
Mathem
te er da
KLEIN i
treuten
er 1886
sitionen
Professu
er bis z
sich ha
pentheo

Der Auftritt von COLE schlug se
he Wellen, daß seine Faktorisier
vorkommt in einer New Yorker (o
mit dem Titel *The five hysterica*
junger Mathematiker um, weil e
$2^{67} - 1$ ausgeht und die Tochter d
an die Tafel schreibt. Einzelheiten
unter http://www.playscripts
lesen. (Die Show verschwand nac
Versenkung; sie wurde seither nu
aufgeführt.)

COLE konnte für seine Faktorisie
über die Struktur von Faktoren

und auch bei den von ihm selbst gefundenen Eigenschaften potentieller Faktoren konnte er die spezielle Struktur von M_{67} ausnutzen. Ähnlich arbeiten auch heutige Mathematiker an der Faktorisierung spezieller Zahlen, beispielsweise im Rahmen des Cunningham-Projekts zur Faktorisierung von Zahlen der Form $b^n \pm 1$ für kleine Basen b. Für die Faktorisierung von RSA-Moduln kann man natürlich nicht mit solchen Techniken arbeiten. In diesem Kapitel soll es um Verfahren gehen, mit denen man eine zufällig gegebene Zahl ohne spezielle Struktur faktorisieren kann.

Es gibt kein „bestes“ Faktorisierungsverfahren; für Zahlen verschiedener Größenordnungen haben jeweils andere Verfahren ihre Stärken. Auch Vorwissen über die zu faktorisierende Zahl kann bei der Wahl eines geeigneten Verfahrens helfen: Bei einem RSA-Modul, der das Produkt zweier Primzahlen ähnlicher Größenordnung ist, wird man anders vorgehen als bei einer Zahl der Form $b^n \pm 1$. Mehr noch als bei Primzahltests gilt, daß asymptotische Komplexitätsaussagen als Auswahlkriterium nutzlos sind: Das für die Faktorisierung 150-stelliger RSA-Moduln heute optimale Verfahren, das Zahlkörpersieb, wird beim Versuch eine sechsstellige Zahl zu faktorisieren, oft nicht in der Lage sein die Faktoren zu trennen, und selbst in den Fällen, in denen es erfolgreich ist, braucht es erheblich länger als einfache Probedivisionen. Auch liefern die meisten Faktorisierungsverfahren nur *irgendeinen* Faktor; der muß nicht prim sein, und sein Kofaktor schon gar nicht. Falls also ein Faktor m einer Zahl N gefunden ist, müssen anschließend m und N/m weiter untersucht werden, und da diese Zahlen kleiner sind als N, sind dazu möglicherweise andere Verfahren besser als das zuerst angewandte.

Im folgenden sollen einige der einfachsten gebräuchlichen Verfahren vorgestellt werden.

§1: Die ersten Schritte

a) Test auf Primzahl

Der schlimmste Fall für praktisch jedes Faktorisierungsverfahren tritt dann ein, wenn die zu faktorisierende Zahl eine Primzahl ist: Gerade

bei den fortgeschrittenen Verfahre
terium als das Auffinden eines F
bei ganz kleinen Zahlen) zu Be
Primzahltest stehen. Da auch das
läßt sich eventuell auch das noch
Situation her (beispielsweise bei
zu rechnen ist.

b) Abdividieren kleiner Prim

Bei kleinen zusammengesetzten
Art der Faktorisierung im allgem
nacheinander durchzuprobieren, i
abdividiert, wie es geht. Sobald d
der gerade betrachteten Primzahl,
Primzahl ist und hat n vollständig

Die genaue Vorgehensweise ist
Liste der Primzahlen bis zu einer
gegebenenfalls muß diese zunäch
den.

1. Schritt: Setze M gleich der zu

2. Schritt: Solange M durch p t
notiere p als Faktor.

3. Schritt: Falls $M = 1$, sind alle
mus endet. Falls $M < p^2$, ist M
Faktoren hinzugefügt; danach en
mus. In allen anderen Fällen wir
und es geht zurück zum zweiten S

Als Beispiel wollen wir die Zahl

Im ersten Schritt werden $M = 1\,2$

Im zweiten Schritt ist nun $p = 2$. I
durch p dividieren; wir notieren al
durch $M/2 = 617\,283\,945$. Diese

zum dritten Schritt, wo offensichtlich keines der Abbruchkriterien erfüllt ist. Somit wird $p = 3$ und es geht zurück zum zweiten Schritt.

Das neue M ist durch drei teilbar, genauso auch $M/3 = 205\,761\,315$. Also wird nochmals durch drei dividiert, und wir erhalten den nicht mehr durch drei teilbaren Quotienten 68 587 105. Somit werden zwei Faktoren drei notiert und es geht weiter zum dritten Schritt. Dort wird $p = 5$ gesetzt, und es geht wieder zurück zu Schritt 2.

Das aktuelle $M = 68\,587\,105$ ist durch fünf teilbar; $M/5 = 13\,717\,421$. Dies wird das neue M; und da es nicht durch fünf teilbar ist, notieren wir nur einen Faktor fünf.

Im dritten Schritt wird wieder p erhöht und es geht zurück zum zweiten Schritt. Dort passiert nun allerdings lange Zeit nichts, denn keine der Primzahlen zwischen sieben und 3 593 teilt das aktuelle M. Erst wenn p im dritten Schritt auf 3 607 gesetzt wird, finden wir wieder einen Faktor. Wir notieren ihn, ersetzen M durch $M/3\,607 = 3803$, was offensichtlich nicht durch 3 607 teilbar ist, und gehen weiter zum dritten Schritt.

Dort ist nun offensichtlich $M < p^2$, also ist M eine Primzahl, und

$$1\,234\,567\,890 = 2 \cdot 3^2 \cdot 5 \cdot 3\,607 \cdot 3\,803$$

ist vollständig faktorisiert.

Es ist klar, daß wir schon eine zwanzigstellige Zahl nur mit viel Glück auf diese Weise mit vertretbarem Aufwand vollständig faktorisieren können. Trotzdem ist Abdividieren selbst für noch viel größere Zahlen ein sinnvoller erster Schritt, denn die auf größere Faktoren spezialisierten Verfahren schaffen es im allgemeinen nicht, auch kleine Primfaktoren voneinander zu trennen.

Um Abdividieren statt zur vollständigen Faktorisierung nur zur Identifikation „kleiner“ Primfaktoren zu verwenden, ist lediglich eine kleine Modifikation des dritten Schritts notwendig: Wir legen eine Suchgrenze S fest und brechen im dritten Schritt auch dann ab, wenn $p > S$ ist. Im letzteren Fall können wir selbstverständlich nicht behaupten, daß das verbleibende M eine Primzahl ist; M muß dann mit anderen Verfahren weiter bearbeitet werden. Bei der Wahl einer geeigneten Schranke S

sollte man die Kapazität des Ar
keit des verwendeten Computers
für den der Algorithmus auf alle
bruchteilen ausgeführt werden ka
besseren Computern läßt sich au
lion und bei derzeit aktuellen schn
oder etwa 2^{30} in weniger als einer

§ 2: Die Verfahren von Pol

In den Jahren um 1975 entwickel
M. POLLARD mehrere recht einf
ganzer Zahlen sowie zur Berechn
heute noch (teils in verbesserter F
algorithmischen Zahlentheorie ge
die beiden bekanntesten vorgeste
mindest kurz auf mathematisch a
eingehen. Die hier behandelten V
nen des nächsten Paragraphen di
zum Erfolg führen, je kleiner die
allerdings sehr kleine Primfaktor
Verfahren der Wahl für die Weiter
erhaltenen „Rests“, von dem man
faktoren mehr hat.

JOHN M. POLLARD ist ein britischer Ma
com arbeitete. Er veröffentlichte zwische
Arbeiten, größtenteils auf dem Gebiet de
auch für seine Beiträge zur Kryptographie
den hier vorgestellten Faktorisierungsalgo
Zahlkörpersieb, eine Variante des weiter
sen Weiterentwicklungen derzeit die sch
Zahlen sind. Seine home page, um die er
sites.google.com/site/jmptidcott2/.

Bei den in diesem und dem näc
fahren besteht das Ziel immer dari
dies erreicht ist, bricht das Verfah

sein Kofaktor werden für sich weiter untersucht – wobei natürlich immer an erster Stelle ein Primzahltest stehen sollte.

a) Die Monte-Carlo-Methode

Monte Carlo ist ein Stadtteil von Monaco, der vor allem für seine Spielbank bekannt ist. An deren Spieltischen sollen Roulette-Schüsseln idealerweise rein zufällig für jedes Spiel von neuem eine Zahl zwischen 0 und 36 bestimmen.

Eine ähnliche Idee läßt sich auch für die Faktorisierung einer ganzen Zahl N verwenden: Ausgehend von einer Folge $(x_i)_{i\in\mathbb{N}}$ zufällig gewählter Zahlen zwischen 1 und N (oder 0 und $N-1$) bildet man jeweils den ggT von x_i mit N in der Hoffnung, einen nichttrivialen Teiler zu finden.

Für einen Primteiler p von N können wir erwarten, daß im Mittel eine von p Zahlen x_i durch p teilbar ist. Dann ist auch ggT(x_i, N) durch p teilbar, kann aber möglicherweise größer als p sein.

Beim einfachen Abdividieren finden wir p, nachdem wir alle Primzahlen bis einschließlich p durchprobiert haben; wie wir im letzten Kapitel gesehen haben, sind dies etwa $p/\log p$ Stück. Für jede davon brauchen wir eine Division, verglichen mit durchschnittlich $p/2$ EUKLIDischen Algorithmen bei der obigen Methode, die nicht einmal eine Garantie dafür bietet, den Faktor zu finden. Von daher hat die neue Methode zumindest in der bislang betrachteten Form ausschließlich Nachteile und ist keine sinnvolle Alternative zum Abdividieren.

POLLARDs Idee zur Beschleunigung beruht auf dem im Anhang genauer erklärten Geburtstagsparadoxon: Die Wahrscheinlichkeit dafür, daß eine gegebene Zufallszahl durch p teilbar ist, liegt zwar nur bei $1:p$, aber die Wahrscheinlichkeit, daß zwei der x_i modulo p gleich sind, steigt in der Nähe von etwa $\sqrt{p}$ Folgengliedern ziemlich steil von nahe null zu nahe eins. Wenn wir also anstelle der größten gemeinsamen Teiler von N mit den x_i die mit den Differenzen $x_i - x_j$ berechnen, haben wir bereits bei einer Folge der Länge um $\sqrt{p}$ gute Chancen, einen nichttrivialen ggT zu finden.

Auch in dieser Form ist das Verfa
ein neues x_i mit $i \approx \sqrt{p}$ erzeugt
ggT von $x_i - x_j$ berechnen, was
daß der Gesamtaufwand nicht pro

$$\int_0^{\sqrt{p}}$$

was keine Ersparnis ist. Dazu kor
genglieder gespeichert werden m
einen Platzbedarf in der Größeno

Dieses Problem können wir umg
zahlen verwenden, sondern algori
dozufallszahlen erzeugen. Typis
Rekursionsvorschrift der Form x
ratischen Polynom Q. (Die bei
zufallsgeneratoren nach der line
Monte-Carlo-Methode zur Faktor
man einfach Polynome der Form
und $c \neq -2$ sein sollte, denn ei
diese Wahlen keine guten Pseudo
Wahlen von c stets gute Generat
aber die praktischen Erfahrungen

Wegen der speziellen Form der R
modulo p nur ab von x_i mod p; ins
falls $x_i \equiv x_j \bmod p$, und entspre
die Zahlen x_{i+r} und x_{j+r} modulo
periodisch mit einer Periode π, d

Das Problem, Periodizität in ein
in der Zahlentheorie auf, sonder
henanalyse und anderen Anwend
seiner Lösung, auch als Hase u
stammt von FLOYD (1967) und be

Wird eine Folge (y_i) *irgendwann*
daß $y_k = y_{2k}$ *ist.*

In der Tat, ist $y_{i+\pi} = y_i$ für alle $i \geq r$, so können wir für k jedes Vielfache $\ell\pi$ der Periode nehmen, das mindestens gleich r ist.

ROBERT W. FLOYD (1936–2001) beendete seine Schulausbildung bereits im Alter von 14 Jahren, um dann mit einem Stipendium an der Universität von Chicago zu studieren, wo er mit 17 einen Bachelor in *liberal arts* bekam. Danach finanzierte er sich durch Arbeit ein zweites Bachelorstudium in Physik, das er 1958 abschloß. Damit war seine akademische Ausbildung beendet; er arbeitete als Operator in einem Rechenzentrum, brachte sich selbst Programmieren bei und begann einige Jahre später mit der Publikation wissenschaftlicher Arbeiten auf dem Gebiet der Informatik. Mit 27 wurde er Assistenzprofessor in Carnegie Mellon, fünf Jahre später erhielt er einen Lehrstuhl in Stanford. Zu den vielen Entwicklungen, die er initiierte, gehört die semantische Verifikation von Programmen, Design und Analyse von Algorithmen, Refactoring, dazu kommen Arbeiten über Graphentheorie und das FLOYD-STEINBERG dithering in der Computergraphik. 1978 erhielt er den TURING-Preis, die höchste Auszeichnung der Informatik. Stanfords Nachruf auf FLOYD ist zu finden unter news-service.stanford.edu/news/2001/november7/floydobit-117.html .

Damit sieht der Grobablauf der Monte-Carlo-Faktorisierung einer natürlichen Zahl N folgendermaßen aus:

Schritt 0: Man wähle ein quadratisches Polynom Q und einen Startwert x_0. Setze $x = y = x_0$.
Schritt $i, i > 0$**:** Ersetze x durch $Q(x)$ mod N und ersetze y durch $Q\big(Q(y)\big)$ mod N; berechne dann ggT$(x - y, N)$. Falls dieser weder eins noch N ist, wurde ein Faktor gefunden.

Man beachte, daß hier im i-ten Schritt $x = x_i$ und $y = x_{2i}$ ist; wir erzeugen also die Folge der x_i (Schildkröte) und die der x_{2i} (Hase) simultan, ohne Zwischenergebnisse zu speichern.

Das Teuerste an diesem Algorithmus sind die EUKLIDischen Algorithmen zur ggT-Berechnung; da wir (sofern wir kleine Primfaktoren zuvor ausgeschlossen haben) nicht wirklich erwarten, daß hier häufig ein nichttriviales Ergebnis herauskommt, liegt es nahe, deren Anzahl möglichst zu reduzieren.

Eine Strategie dazu besteht darin,
modulo N aufzumultiplizieren u
mit N zu berechnen. Die „gewisse
sonst besteht die Gefahr, daß das
gleich durch mehrere Primteiler
Effizienzgründen auch nicht zu k
bereits ausgeschlossen sind, zeig
fassung von etwa hundert Differe
bereits bei den „kleinen“ Faktoren
tet wurde, bieten sich auch höher

Praktisch bedeutet das, daß wir
Anfangswert eins und dann im i-t
ersetzen. Nur falls i durch die
anschließend der ggT von N und
weiter mit dem $(i + 1)$-ten Schritt

Die Monte-Carlo-Methode wird a
Folge der x_i mod p nicht von An
aber, da es nur p Restklassen m
werden, d.h. sie beginnt auf dem
wann in den Kreis. Erfahrungsge
im Auffinden sechs- bis achtstel
langsam, und kleine Faktoren kan

Als Beispiel wollen wir die sechs

$$F_6 = 2^{64} + 1 = 18\,4$$

betrachten. Mit dem quadratisc
Startwert $x_0 = 2$ und einem EU
hundert Folgegliedern findet ein
onen in Sekundenbruchteilen de
wie sein Kofaktor 67 280 421 310
faktorisiert.

Anhang: Das Geburtstagspa

Angenommen, in einem Raum be

Wahrscheinlichkeit dafür, daß zwei davon am gleichen Tag Geburtstag haben?

Um diese Frage wirklich beantworten zu können, müßte man die (recht inhomogene) Verteilung der Geburtstage über das Jahr kennen; wir beschränken uns stattdessen auf ein grob vereinfachtes Modell ohne Schaltjahre mit 365 gleich wahrscheinlichen Geburtstagen. Dann ist die Wahrscheinlichkeit dafür, daß von n Personen keine zwei am gleichen Tag Geburtstage haben,

$$\prod_{k=0}^{n-1}\left(1-\frac{k}{365}\right),$$

denn für eine Person ist das überhaupt keine Bedingung, und jede weitere Person muß die Geburtstage der schon betrachteten Personen vermeiden. (Da der Faktor mit $k = 365$ verschwindet, wird die Wahrscheinlichkeit für $n > 365$ zu null, wie es nach dem DIRICHLETschen Schubfachprinzip auch sein muß.)

Nachrechnen ergibt für $n = 23$ ungefähr den Wert 0,4927; bei 23 Personen liegt also die Wahrscheinlichkeit für zwei gleiche Geburtstage bei 50,7%. Tatsächlich dürfte sie noch deutlich höher liegen, denn bei Geburtstagen ist die Annahme einer Gleichverteilung sicherlich falsch.

Bei einer guten Folge von Zufallszahlen sollten die Restklassen modulo p in sehr guter Näherung gleichverteilt sein; die Wahrscheinlichkeit dafür, daß unter n Zufallszahlen keine zwei in der gleichen Restklasse liegen, ist somit

$$P_n = \prod_{k=0}^{n-1}\left(1-\frac{k}{p}\right).$$

Da wir uns für einigermaßen große Werte von p interessieren (die kleinen haben wir schon abdividiert), können wir davon ausgehen, daß

$$\left(1-\frac{1}{p}\right)^p \approx e \quad \text{und} \quad \left(1-\frac{1}{p}\right) \approx e^{-1/p}$$

ist; für nicht zu große Werte von k ist dann auch

$$\left(1-\frac{k}{p}\right) \approx e^{-k/p},$$

und für nicht zu große Werte von

$$P_n = \prod_{k=0}^{n-1}\left(1-\frac{k}{p}\right) \approx \prod_{k=0}^{n-1} e$$

Für $p = 365$ etwa ergibt dies den korrekten Wert 0,4927.

Wenn wir im Exponenten noch de ren, können wir abschätzen, für einen vorgegebenen Wert erreich

$$e^{-\frac{n^2}{2p}} = P \Longleftrightarrow \frac{n^2}{2p} =$$

Damit liegt P_n bei etwa 50%, fa $p = 365$ ergibt dies die immer no

Für $P = 1/1000$ ergibt sich n sprechend $n \approx 0{,}0447\sqrt{p}$. Die W n Zufallszahlen zwei mit derselb also bei der Größenordnung $n \approx$ wahrscheinlich.

b) Die ($p-1$)-Methode

POLLARDs zweite Methode beru Für einen Primteiler p von N, zu p teilerfremde natürliche Za $(a^r - 1) \bmod N$ und N ist also d

Natürlich ist $p - 1$ nicht bekann nur durch vergleichsweise kleine Schranke mit der Eigenschaft, d größer B teilbar ist. Dann ist d q^e, die höchstens gleich B sind, wenn auch ein extrem großes, das berechnen läßt. Für jedes konkr nismäßig einfach berechnet werd der für jede Primzahl $q \le B$ mo

immer noch kleiner oder gleich B ist; mit dem Algorithmus zur modularen Exponentiation aus §5 des zweiten Kapitels geht das auch für sechs- bis siebenstellige Werte von B noch recht flott.

Insgesamt funktioniert POLLARDs $(p-1)$-Methode zur Faktorisierung einer natürlichen Zahl N also folgendermaßen:

Schritt 0: Wähle eine Schranke B und eine Basis a zwischen 1 und N.

Schritt 1: Erstelle (z.B. nach ERATOSTHENES) eine Liste aller Primzahlen $q \le B$.

Schritt 2: Berechne für jede dieser Primzahlen q den größten Exponenten e derart, daß auch noch $q^e \le B$ ist, d.h. $e = [\log B / \log q]$. Ersetze dann den aktuellen Wert von a durch $a^{q^e} \bmod N$.

Schritt 3: Berechne ggT$(a-1, N)$. Falls ein Wert ungleich eins oder N gefunden wird, war das Verfahren erfolgreich, ansonsten nicht.

Es ist klar, daß der Erfolg dieses Verfahrens wesentlich davon abhängt, daß N einen Primteiler p hat mit der Eigenschaft, daß alle Primfaktoren von $p-1$ relativ klein sind. Ob dies der Fall ist, läßt sich im Voraus nicht sagen; die $(p-1)$-Methode liefert daher gelegentlich ziemlich schnell sogar 20- oder 30-stellige Faktoren, während sie andererseits deutlich kleinere Faktoren oft nicht findet.

Als Beispiel betrachten wir noch einmal $M_{67} = 2^{67}-1$. Wenn wir mit der Basis $a = 17$ und der Schranke $B = 3\,000$ arbeiten, wird a modulo M_{67} potenziert zum neuen

$a = 111\,153\,665\,932\,902\,146\,348$ mit ggT$(a-1, M_{67}) = 193\,707\,721$.

Damit ist (in Sekundenbruchteilen auf einem Standard-PC) eine nichttriviale Faktorisierung gefunden, und ein Primzahltest zeigt, daß sowohl der gefundene Faktor als auch sein Komplement prim sind.

Warum die Methode Erfolg hatte, sehen wir an der Faktorisierung der um eins verminderten Faktoren:

$$193\,707\,720 = 2^3 \cdot 3^3 \cdot 5 \cdot 67 \cdot 2\,677 \quad \text{und}$$

$$761\,838\,257\,286 = 2 \cdot 3^2 \cdot 29 \cdot 67 \cdot 2\,551 \cdot 8\,539\,.$$

Für jede Schranke $B \ge 2\,677$ ist also der erste Faktor ein Teiler des endgültigen $a-1$, aber für $B < 8\,539$ ist der zweite Faktor keiner.

c) Varianten

Falls $p-1$ nicht nur relativ klein
Methode nicht zum Erfolg. In sol
vielleicht $p+1$ oder irgendeine an
Primfaktoren hat. Wir brauchen
bei denen es nicht auf die Primf
auf die anderer Zahlen in der Näh

Um solche Varianten zu finden, e
Methode etwas abstrakter unter g
zu betrachten.

Dort rechnen wir in der primen F
implizit auch in $(\mathbb{Z}/p)^\times$ für jede
ihn kennen, oder nicht. In $(\mathbb{Z}/p)^\times$
Potenz gleich dem Einselement; g
für die der Exponent r ein Vielfa
Methode wird ein r berechnet, da
einer gewissen Schranke teilbar is
keine Primzahlpotenz oberhalb d
von $p-1$.

Allgemeiner können wir statt in
anderen Paar von Gruppen rech
chen Gruppe G_N, deren Element
über $(\mathbb{Z}/N)$ auffassen lassen; au
Gruppenmultiplikation für zwei
rechenarten über $\mathbb{Z}/N$ zurückfü
mente von G_N zu Tupeln über
so erhaltenen Tupel bildet eine G
in G_N implizit auch eine Rechnu

Die Elementanzahl von G_p sei N

Wir wählen irgendein Element v
selben Exponenten r, mit dem w
modulo N potenziert haben. Falls
wir ein Element $b \in G_N$, dessen

von G_p ist. Ist daher b_i die i-te Koordinate von b und e_i die von e, so muß die Differenz $b_i - e_i$ durch p teilbar sein, und mit etwas Glück können wir p als ggT von n und $b_i - e_i$ bestimmen.

Bleibt nur noch das Problem, geeignete Gruppen zu finden. Bei der $(p-1)$-Methode ist $G_N = (\mathbb{Z}/N)^\times$ und $N(p) = p-1$.

Für die $(p+1)$-Methode benutzt POLLARD die Tatsache, daß es nicht nur zu jeder Primzahl p, sondern auch zu jeder Primzahlpotenz p^r einen Körper mit entsprechender Elementanzahl. Dieser Körper $\mathbb{F}_{p^r}$ ist natürlich verschieden vom Ring $\mathbb{Z}/p^r$; er ist ein r-dimensionaler Vektorraum über $\mathbb{F}_p$ mit geeignet definierter Multiplikation.

Speziell für $r = 2$ hat der Körper $\mathbb{F}_{p^2}$ eine multiplikative Gruppe $\mathbb{F}_{p^2}^\times$ der Ordnung $p^2 - 1 = (p+1)(p-1)$. Sie hat $\mathbb{F}_p^\times$ als Untergruppe und die Faktorgruppe $G_p = \mathbb{F}_{p^2}^\times / \mathbb{F}_p^\times$ hat die Ordnung $N(p) = p+1$. Das Rechnen in dieser Gruppe mit Repräsentanten modulo N ist etwas trickreich und benutzt die hier nicht behandelten LUCAS-Sequenzen.

Derzeit am populärsten ist eine andere Wahl von G_N und G_p: Wir nehmen für G_N eine elliptische Kurve über $\mathbb{Z}/N$. Dabei handelt es sich um die Menge aller Punkte $(x, y) \in (\mathbb{Z}/N)^2$, die einer vorgegebenen Gleichung $y^2 = x^3 - ax - b$ genügen, wobei a, b Elemente von $\mathbb{Z}/N$ sind, für die $\Delta = 4a^3 - 27b^2$ teilerfremd zu N ist; dazu kommt ein weiterer Punkt O, den wir formal als $(0, \infty)$ schreiben. G_p ist dann die entsprechende Punktmenge in $\mathbb{F}_p^2$ zusammen mit O. Nach einem Satz von HELMUT HASSE (1898–1979) ist

$$p + 1 - 2\sqrt{p} < N(p) < p + 1 + 2\sqrt{p}\,,$$

und wie man inzwischen weiß, kann man auch für fast jeden Wert, der diese Ungleichung erfüllt, Parameterwerte a und b finden, so daß $N(p)$ gleich diesem Wert ist. Wenn man mit hinreichend vielen verschiedenen Kurven arbeitet, ist daher die Chance recht groß, daß der Exponent r wenigstens für eine davon ein Vielfaches von $N(p)$ ist.

Die Multiplikation ist folgendermaßen definiert: Durch zwei Punkte (x_1, y_1) und (x_2, y_2) auf der Kurve geht genau eine Gerade; setzt man deren Gleichung $y = mx + c$ in die Kurvengleichung ein, erhält man

ein Polynom dritten Grades in x.
stellen x_1, x_2, und daneben noch
Schnittpunkt der Geraden mit d
Summe der beiden Punkte definie

$$(x_1, y_1) \oplus (x_2, y_2$$

Man kann zeigen, daß dies die Me
mit Neutralelement O macht, in
bei der klassischen $(p-1)$-Meth

Unter den Faktorisierungsmetho
des zu findenden Faktors abhängt
Kurven die für große Zahlen der
schon Faktoren mit bis zu 67 Ste
großer Primzahlen wie beispielsw
thoden allerdings der schlechtest
deren Aufwand nur von der Größe
meist besser geeignet.

§3: Das Verfahren von Fe

Die bisher betrachteten Verfahre
wenn die zu faktorisierende Zahl
teiler hat. Das hier beschriebene V
schnell ans Ziel, wenn sie sich als
toren schreiben läßt. In seiner ein
binomischen Formel $x^2 - y^2 = (x$
ungerader Primzahlen, so ist

$$N = (x+y)(x-y) \quad \text{mit}$$

Ausmultiplizieren führt auf die B

FERMAT berechnet für $y = 0, 1, 2,$
Quadrat x^2 stößt, hat er zwei Fak
halben Differenz der beiden Fakt
Ziel, je näher die beiden Faktore

Vorschrift der Bundesnetzagentur, daß die beiden Faktoren eines RSA-Moduls zwar ungefähr gleich groß sein sollten, daß sie aber doch einen gewissen Mindestabstand einhalten müssen.

Anstelle der Zahlen $N + y^2$ kann man auch für ein festes k die Zahlen $kN + y^2$ betrachten. Falls dies eine Quadratzahl x^2 ist, gilt entsprechend

$$kN = x^2 - y^2 = (x + y)(x - y)\,,$$

und wenn man Glück hat, sind ggT$(x \pm y, N)$ echte Faktoren von N. Wenn man Pech hat, sind es freilich einfach die beiden Zahlen eins und N. Trotzdem lassen sich darauf sehr effiziente Faktorisierungsverfahren aufbauen, denn die obige Gleichung besagt ja auch, daß wir nur *irgendwie* zwei Zahlen x, y finden müssen mit $x^2 \equiv y^2 \bmod N$ und dann eine Chance haben, daß ggT$(x \pm y, N)$ uns zwei Faktoren von N liefert. Je mehr solche Paare (x, y) wir finden, desto größer sind die Erfolgschancen.

Der Grundalgorithmus zum Finden solcher Paare ist das sogenannte quadratische Sieb, mit dem wir uns als nächstes beschäftigen wollen.

In seiner einfachsten Variante wählen wir uns ein quadratisches Polynom, z.B. das Polynom

$$f(x) = \left(x + \left\lfloor\sqrt{N}\right\rfloor\right)^2 - N\,.$$

Für jedes x ist dann $f(x) \equiv \left(x + \left\lfloor\sqrt{N}\right\rfloor\right)^2 \bmod N$, wobei links und rechts verschiedene Zahlen stehen. Insbesondere steht links im allgemeinen keine Quadratzahl.

Falls wir allerdings Werte $x_1, x_2, \ldots, x_r$ finden können, für die das Produkt der $f(x_i)$ eine Quadratzahl ist, dann ist

$$\prod_{i=1}^{r} f(x_i) \equiv \prod_{i=1}^{r} \left(x + \left\lfloor\sqrt{N}\right\rfloor\right)^2 \bmod N$$

eine Relation der gesuchten Art.

Diese Strategie erklärt die Wahl d
die Zahlen $x + \left\lfloor\sqrt{N}\right\rfloor$ als auch

$$f(x) = \left(x + \left\lfloor\sqrt{N}\right\rfloor\right)^2 - N$$

Für x-Werte, die deutlich kleine
werden wir es im folgenden zu
der Größenordnung $\sqrt{N}$; bei der
Quadrat minus N produzieren, w
oder deren Funktionswert deutlic
$\left\lfloor\sqrt{N}\right\rfloor$ genauso gut eine andere Z
det werden; es kommt nur darauf
liegt.

Um geeignete x_i zu finden, betr
zahlen, die sogenannte Faktorba
Faktorisierung einer etwa hunder
Tausend Primzahlen, deren größte
im einstelligen Millionenbereich

n	n-te Primzahl
100 000	1 299 709
200 000	2 750 159
300 000	4 256 233
400 000	5 800 079
500 000	7 368 787

Beim quadratischen Sieb interes
Produkt von Primzahlen aus $\mathcal{B}$
darstellbar ist. Ist $f(x_i) = \prod_{p\in\mathcal{B}}$

$$\prod_{i=1}^{r} f(x_i)^{\varepsilon_i}$$

genau dann ein Quadrat, wenn
Dies hängt natürlich nur ab von
können ε_i und e_{ip} daher als Elem

auffassen und bekommen dann über $\mathbb{F}_2$ die Bedingungen

$$\sum_{i=1}^{r} e_{ip}\varepsilon_i = 0 \quad \text{für alle } p \in \mathcal{B}\,.$$

Betrachten wir die ε_i als Variablen, ist dies ein homogenes lineares Gleichungssystem in r Variablen mit soviel Gleichungen, wie es Primzahlen in der Faktorbasis gibt. Dieses Gleichungssystem hat nichttriviale Lösungen, falls die Anzahl der Variablen die der Gleichungen übersteigt, falls es also mehr Zahlen x_i gibt, für die $f(x_i)$ über der Faktorbasis faktorisiert werden kann, als Primzahlen in der Faktorbasis.

Für jede nichttriviale Lösung ist

$$\prod_{i=1}^{r} f(x_i)^{\varepsilon_i} = \prod_{i=1}^{r} \left(x + \left\lceil\sqrt{N}\right\rceil\right)^{2\varepsilon_i} \bmod N$$

eine Relation der Form $x^2 \equiv y^2 \bmod N$, die mit einer Wahrscheinlichkeit von etwa ein halb zu einer Faktorisierung von N führt. Falls wir zehn linear unabhängige Lösungen des Gleichungssystems betrachten, führt also mit einer Wahrscheinlichkeit von etwa 99,9% mindestens eine davon zu einer Faktorisierung.

Da ε_i nur die Werte 0 und 1 annimmt, stehen in obigem Produkt natürlich keine echten Potenzen: Man multipliziert einfach nur die Faktoren miteinander, für die $\varepsilon_i = 1$ ist. Außerdem interessieren nicht die links- und rechtsstehenden Quadrate, sondern deren Quadratwurzeln; tatsächlich also berechnet man (hier natürlich in $\mathbb{N}_0$)

$$x = \prod_{p\in\mathcal{B}} p^{\frac{1}{2}\sum_{i=1}^{r}\varepsilon_i e_{ip}} \bmod N \quad \text{und} \quad y = \prod_{i=1}^{r}\left(x + \left\lceil\sqrt{N}\right\rceil\right)^{\varepsilon_i} \bmod N\,.$$

Zum besseren Verständnis des Grundprinzips wollen wir versuchen, damit die Zahl 15 zu faktorisieren. Dies ist zwar eine sehr untypische Anwendung, da das quadratische Sieb üblicherweise erst für mindestens etwa vierzigstellige Zahlen angewandt wird, aber zumindest das Prinzip sollte auch damit klarwerden.

Als Faktorbasis verwenden wir die Menge

$$\mathcal{B} = \{2, 3, 7, 11\}\,;$$

die Primzahl fünf fehlt, da $3 \cdot 5 =$
die sowohl drei als auch fünf en
linke wie auch die rechte Seite d
ist. Bei realistischen Anwendung
keine Rücksicht nehmen, denn da
höchstens siebenstellig und som
Faktoren.

Wir berechnen $f(x)$ für $x = 1,$
haben, die über der Faktorbasis
torisierbaren Werte sind in folgen

x	$x + \left\lceil\sqrt{N}\right\rceil$	$f(x)$	*Fa*
1	4	1	
3	6	21	
5	8	49	
6	9	66	
10	13	154	
54	57	3234	2

Die erste und die dritte Zeile sind
Art, nämlich

$$4^2 \equiv 1 \bmod 15$$

Die zweite Relation ist nutzlos, d
dagegen führt zur Faktorisierung,

$$\text{ggT}(4 + 1, 15) = 5$$

Da dies aber ein Zufall ist, der
nie vorkommt, wollen wir das i
$x = 3, 6, 10$ und 51 arbeiten:

$$\begin{aligned} 6^2 &\equiv 3 \cdot 7 && \text{mod} \\ 9^2 &\equiv 2 \cdot 3 \cdot 11 && \text{mod} \\ 13^2 &\equiv 2 \cdot 7 \cdot 11 && \text{mod} \\ 57^2 &\equiv 2 \cdot 3 \cdot 7^2 \cdot 11 && \text{mod} \end{aligned}$$

Multipliziert man die ersten drei

$$(6 \cdot 9 \cdot 13)^2 \equiv (2$$

oder $702^2 \equiv 462^2 \bmod 15$. Da

$$\text{ggT}(702 - 462, 15) = \text{ggT}(240, 15) = 15$$

ist, bringt das leider nichts.

Wir erhalten auch dann rechts ein Quadrat, wenn wir das Produkt der ersten, dritten und vierten Relation bilden; dies führt auf

$$(6 \cdot 13 \cdot 57)^2 \equiv (2 \cdot 3 \cdot 7^2 \cdot 11)^2 \bmod 15$$

oder $4446^2 \equiv 3234^2 \bmod 15$. Hier ist

$$\text{ggT}(4446 - 3234, 15) = \text{ggT}(1212, 15) = 3\,,$$

womit wir die Zahl 15 faktorisiert haben – wenn auch nicht unbedingt auf die einfachstmögliche Weise.

Bei realistischen Beispielen sind die Funktionswerte $f(x)$ deutlich größer als die Primzahlen aus der Faktorbasis; außerdem liegen die vollständig faktorisierbaren Zahlen viel dünner als hier: Bei der Faktorisierung einer hundertstelligen Zahl etwa muß man davon ausgehen, daß nur etwa jeder 10^9-te Funktionswert über der Faktorbasis zerfällt.

Daher ist es wichtig, ein Verfahren zu finden, mit dem diese wenigen Funktionswerte schnell und einfach bestimmt werden können. Das ist zum Glück möglich:

Der Funktionswert $f(x)$ ist genau dann durch p teilbar, wenn

$$f(x) \equiv 0 \bmod p$$

ist. Für ein Polynom f mit ganzzahligen Koeffizienten ist offensichtlich $f(x) \equiv f(y) \bmod p$, falls $x \equiv y \bmod p$ ist. Daher ist für ein x mit $f(x) \equiv 0 \bmod p$ auch

$$f(x + kp) \equiv 0 \bmod p \quad \text{für alle } k \in \mathbb{Z}\,.$$

Es genügt daher, im Bereich $0 \le x < p - 1$ nach Werten zu suchen, für die $f(x)$ durch p teilbar ist.

Dazu kann man f auch als Polynom über dem Körper mit p Elementen betrachten und nach Nullstellen in diesem Körper suchen. Für Polynome

großen Grades und große Werte
hier, bei einem quadratischen Po
eine quadratische Gleichung löse
auch gilt

$$f(x) = \left(x + \left[\sqrt{N}\right]\right)^2 - N$$

und diese Gleichung ist genau dan
gibt mit Quadrat N, wenn also in

$$w^2 \equiv$$

ist. Für $p > 2$ hat $f(x) = 0$ in $\mathbb{F}_p$

$$x = -$$

andernfalls gibt es keine Lösung.

Insbesondere kann also $f(x)$ nu
modulo p ein Quadrat ist; dies is
der Fall. Offensichtlich sind alle a
daher gar nicht erst in die Faktorb

Im Kapitel über quadratische Res
große N und p leicht und schnell
Quadrat ist; der Aufwand entspri
angewandten EUKLIDischen Algo
daß sich für solche Quadrate rela
modulo p berechnen lassen.

Das eigentliche Sieben zum Auffi
zerlegbaren Funktionswerte $f(x)$
Man legt ein Siebintervall $x = 0$,
Feld der Länge $M + 1$ für jedes x

Für jede Primzahl p aus der Fakto
Nullstellen $x_{1/2}$ von f modulo
subtrahiert von jedem Feldeleme
$x_2 + kp$ eine Approximation von

Falls $f(x)$ über der Faktorbasis k
am Ende der entsprechende Feld

null sein; um keine Fehler zu machen, untersucht man daher für alle Feldelemente, die betragsmäßig unterhalb einer gewissen Grenze liegen, durch Abdividieren, ob sie wirklich komplett faktorisieren, und man bestimmt auf diese Weise auch *wie* sie faktorisieren. Damit läßt sich dann das oben erwähnte Gleichungssystem über $\mathbb{F}_2$ aufstellen und, falls genügend viele Relationen gefunden sind, nichttrivial so lösen, daß eine der daraus resultierenden Gleichungen $x^2 \equiv y^2 \bmod p$ zu einer nichttrivialen Faktorisierung von N führt.

Als zwar immer noch untypisch kleines Beispiel, das besser und schneller durch Abdividieren faktorisiert werden könnte, betrachten wir die Zahl $N = 5\,352\,499$. Wir nehmen als Faktorbasis alle Primzahlen kleiner hundert modulo derer N ein Quadrat ist; Nachrechnen zeigt, daß

$$\mathcal{B} = \{3, 5, 11, 13, 17, 19, 23, 31, 41, 43, 53, 59, 83, 89\}$$

dann 14 Elemente enthält. Für jedes davon müssen wir die quadratische Gleichung $f(x) \equiv 0 \bmod p$ lösen, was hier natürlich selbst durch Ausprobieren recht schnell möglich wäre. Die Lösungsmengen sind

$p =$	3	5	11	13	17	19	23
Lösungen	$\{1,2\}$	$\{0,4\}$	$\{0,5\}$	$\{4,11\}$	$\{6,9\}$	$\{2,8\}$	$\{0,20\}$
$p =$	31	41	43	53	59	83	89
Lösungen	$\{27,28\}$	$\{3,4\}$	$\{26,35\}$	$\{39,52\}$	$\{2,33\}$	$\{35,70\}$	$\{23,68\}$

Wenn wir damit das Intervall der natürlichen Zahlen von 1 bis 20 000 sieben, erhalten wir 18 Zahlen, die über der Faktorbasis komplett zerfallen:

i	x_i	$f(x_i)$	*Faktorisierung*
1	23	104397	$3 \cdot 17 \cdot 23 \cdot 89$
2	121	571857	$3 \cdot 11 \cdot 13 \cdot 31 \cdot 43$
3	533	2747217	$3 \cdot 11 \cdot 17 \cdot 59 \cdot 83$
4	635	3338205	$3 \cdot 5 \cdot 13 \cdot 17 \cdot 19 \cdot 53$
5	741	3974417	$31 \cdot 41 \cdot 53 \cdot 59$
6	895	4938765	$3 \cdot 5 \cdot 13 \cdot 19 \cdot 31 \cdot 43$
7	2013	13361777	$11 \cdot 13 \cdot 41 \cdot 43 \cdot 53$
8	2185	14879505	$3 \cdot 5 \cdot 17 \cdot 23 \cdot 43 \cdot 59$
9	2477	17591601	$3 \cdot 31 \cdot 43 \cdot 53 \cdot 83$
10	2649	19268945	
11	4163	36586077	
12	4801	45256497	
13	5497	55643601	
14	6253	68023857	
15	10991	171643917	
16	11275	179281245	
17	14575	279852045	
18	18535	429286605	

Ein Vektor $\vec{\varepsilon} \in \mathbb{F}_2^{18}$, für den $\prod f$
das lineare Gleichungssystem m

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Der GAUSS-Algorithmus führt a

$$(\sigma, \mu + \rho, \mu + \rho, \mu + \rho, \sigma$$
$$\nu + \mu + \lambda, \nu + \sigma + \mu + \tau$$

mit sechs freien Parametern λ,
$\lambda = \mu = \sigma = 1$, $\nu = \rho = \tau = 0$, s

$$\vec{\varepsilon} = (1, 1, 1, 1, 1, 1,$$

Sie führt auf die beiden Zahlen

$$x = \prod_{p\in\mathcal{B}} p^{\frac{1}{2}\sum_{i=1}^{r}\varepsilon_i e_{ip}} \bmod N = 854\,237 \quad \text{und}$$

$$y = \prod_{i=1}^{r}\left(x + \left\lfloor\sqrt{N}\right\rfloor\right)^{\varepsilon_i} \bmod N = 3\,827\,016\,.$$

Leider ist die Differenz dieser beiden Zahlen teilerfremd zu N.

Setzen wir in einem zweiten Versuch $\nu = 1$ statt $\nu = 0$, so erhalten wir die weitere Lösung

$$\vec{\varepsilon} = (1,1,1,1,1,0,1,1,1,1,0,1,0,1,1,0,1,0),$$

die uns die Zahlen

$$x = \prod_{p\in\mathcal{B}} p^{\frac{1}{2}\sum_{i=1}^{r}\varepsilon_i e_{ip}} \bmod N = 1\,020\,903 \quad \text{und}$$

$$y = \prod_{i=1}^{r}\left(x + \left\lfloor\sqrt{N}\right\rfloor\right)^{\varepsilon_i} \bmod N = 4\,093\,611$$

liefert. Nun ist der ggT der Differenz mit N gleich 1 237, womit wir die Faktorisierung

$$5\,352\,499 = 1237 \times 4327$$

gefunden haben. In diesem Fall sind die beiden Faktoren sogar bereits Primzahlen; das wird natürlich im allgemeinen nicht der Fall sein – es sei denn, man startet wie hier mit dem Produkt zweier Primzahlen.

Natürlich hätte uns jede der bisher behandelten Methoden dieses Ergebnis mit erheblich geringerem Aufwand und auch erheblich schneller geliefert; das quadratische Sieb entwickelt seine Stärken erst bei erheblich größeren Zahlen, für die es dann oft tagelang rechnet.

Dabei verwendet man das quadratische Sieb meist nicht in der hier vorgestellten Einfachstsversion, sondern mit verschiedenen Optimierungen.

Bei realistischen Anwendungen wird der überwiegende Teil der Rechenzeit für das Sieben gebraucht. Dies läßt sich relativ einfach parallelisieren, indem man das Sieben für verschiedene Teilintervalle auf verschiedene Computer verteilt. Auf diese Weise können mehrere Tausend

Computer jeweils ein Teilinterva
denen Faktorisierungen an eine Z
eingegangen sind, kann diese ein
und dieses lösen.

Eine weitere Verbesserung, die z
auch kleineren Zahlen führt, be
noms f mehrere Polynome zu v
auf verschiedene Computer verte
auch negative Werte annehmen
werden, indem man bei der Fakt
gebliebenen Zahlen auch noch di
Faktorbasis aufnimmt.

Ab etwa 120 bis 130 Stellen w
auch mit komplizierteren als nu
tet wird, das sogenannte Zahlkö
daß die dahinterstehende Theorie
tet; konkret gerechnet wird alle
Dieses Zahlkörpersieb ist die
Faktorisierung von Zahlen, die
Größenordnung sind; von diesem
für RSA aus. Der derzeitige Re
Dezember 2009 gefundene Fakt
dreißigstelligen *challenge numb*
tionales Team; dazu wurde von
schiedenen Clustern von Compu
`http://eprint.iacr.org/2010/0`

Kapitel 5
Kettenbrüche

§1: Der Kettenbruchalgorithmus

Der EUKLIDische Algorithmus läßt sich auch verwenden, um eine reelle Zahl durch Brüche zu approximieren. Beginnen wir der Einfachheit halber mit einer rationalen Zahl $\alpha = \frac{n}{m}$ mit $n, m \in \mathbb{N}$. Der erste Schritt des EUKLIDischen Algorithmus dividiert n durch m:

$$n : m = q_0 \text{ Rest } r_1 \Longrightarrow \alpha = \frac{n}{m} = q_0 + \frac{r_1}{m} .$$

Falls $r_1 \neq 0$ ist, wird im zweiten Schritt m durch r_1 dividiert:

$$m : r_1 = q_1 \text{ Rest } r_2 \Longrightarrow \frac{m}{r_1} = q_1 + \frac{r_2}{r_1} \Longrightarrow \alpha = q_0 + \frac{1}{q_1 + \dfrac{r_2}{r_1}} .$$

Ist auch noch r_2 von Null verschieden, wird sodann r_1 durch r_2 dividiert:

$$r_1 : r_2 = q_2 \text{ Rest } r_3 \Longrightarrow \frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2} \Longrightarrow \alpha = q_0 + \frac{1}{q_1 + \dfrac{1}{q_2 + \dfrac{r_3}{r_2}}} ,$$

und so weiter. Die Konstruktion muß nach endlich vielen Schritten abbrechen, denn die Folge der Reste r_i beim EUKLIDischen Algorithmus ist monoton fallend und muß daher schließlich Null erreichen. Damit ist α dargestellt als ein sogenannter **Kettenbruch**.

Wir können die Konstruktion auch so formulieren, daß sie nur von der Zahl $\alpha = \frac{n}{m}$ abhängt: Der Quotient bei der Division mit Rest von n

durch m ist $q_0 = [\alpha]$, und der du
führt zu folgender Formulierung

Setze zur Initialisierung $c_0 = [\alpha]$

$$\alpha = c_0 + \alpha_1$$

Im i-ten Schritt, $i \geq 1$, bricht der
andernfalls wird c_i definiert als
$1/\alpha_i$ und α_{i+1} so, daß gilt

$$\frac{1}{\alpha_i} =$$

Offensichtlich ist dann

$$\alpha = c_0 + \alpha_0 = c_0 + \frac{}{c_1}$$

$$= \cdots = c_0 + \frac{}{c_1 +}$$

Da diese Darstellung sehr viel P
oft auch die kompaktere Schreibw

$$\alpha = [c_0, c$$

Falls der Algorithmus mit $\alpha_r =$
natürlich nur c_r im Nenner, und v
$[c_0, c_1, \ldots, c_r]$.

So, wie der Algorithmus jetzt fo
irrationale Zahlen α anwenden. D
sonst hätten wir ja eine Darstellun
aber nach dem r-ten Schritt abbr
entsteht, wenn wir $\alpha_r = 0$ setzen
r-te **Konvergente** der Kettenbruc

Als Beispiel betrachten wir $\alpha = \sqrt{2}$. Hier ist $c_0 = \lfloor\sqrt{2}\rfloor = 1$ und $\alpha_1 = \sqrt{2} - 1$. Also ist

$$\frac{1}{\alpha_1} = \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)} = \sqrt{2}+1\,,$$

d.h. $c_1 = \lfloor 1+\sqrt{2}\rfloor = 2$ und $\alpha_2 = 1+\sqrt{2}-2 = \sqrt{2}-1 = \alpha_1$. Damit wiederholt sich ab jetzt alles, d.h.

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2+\cdots}}}}}\,.$$

In Analogie zu periodischen Dezimalbrüchen schreibt man dies auch kurz in der Form

$$\sqrt{2} = [1,2,2,2,\ldots] = [1,\overline{2}]\,.$$

Die ersten Partialbrüche sind

$$P_0 = 1, \quad P_1 = 1+\frac{1}{2} = 1{,}5, \quad P_2 = 1 + \cfrac{1}{2+\frac{1}{2}} = \frac{7}{5} = 1{,}4\,,$$

$$P_3 = 1 + \cfrac{1}{2+\cfrac{1}{2+\frac{1}{2}}} = \frac{17}{12} = 1{,}41\overline{6} \quad \text{und} \quad P_4 = 1 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\frac{1}{2}}}} = \frac{41}{29}\,,$$

was ungefähr gleich 1,4137931 ist. Die Fehler $\sqrt{2} - P_n$ sind, gerundet auf sechs Nachkommastellen, die Zahlen

$$0{,}414214,\ -0{,}085786,\ 0{,}014214,\ -0{,}002453 \quad \text{und} \quad 0{,}000420\,;$$

verglichen mit den kleinen Nennern $1, 2, 5, 12$ und 29 haben wir also erstaunlich gute Übereinstimmungen, und im übrigen ist auch die Kettenbruchentwicklung erheblich regelmäßiger als die Dezimalbruchdarstellung von $\sqrt{2}$.

Als zweites Beispiel betrachten
$c_0 = 3$ und $\alpha_1 = \pi - 3 \approx 0{,}1415$

$$c_1 = \left\lfloor \frac{1}{\pi - 3} \right\rfloor = 7$$

Im nächsten Schritt ist $c_2 = \left\lfloor \frac{1}{\alpha_2} \right.$
geht es mit $c_3 = 1$, $c_4 = 292$, c_5
Muster ist weder erkennbar, noch

Die Kettenbruchentwicklung von

$$\pi = [3, 7, 15, 1,$$

Die ersten Partialbrüche und ihre

$$3 \qquad 3\frac{1}{7} \qquad 3\frac{15}{106}$$

$$0{,}14 \qquad -0{,}0013 \qquad 8{,}3 \cdot 10^{-}$$

Auch hier haben wir wieder, ve
exzellente Approximationseigens

§2: Geometrische Formul

Wir wollen uns zunächst überle
tenbruchentwicklung einer irrati
ner Größenordnung des Nenners
dieser Zahl liefern.

Dazu betrachten wir (im wesentl
STARK in seinem Buch *An Introd*
1978) das Problem der rationalen
Seite: Zur reellen Zahl $\alpha > 0$
den Nullpunkt, und offensichtlic
dieser Geraden außer dem Nullpu
ganzzahligen Koordinaten liegt.
wir durch Punkte $(q, p) \in \mathbb{Z} \times \mathbb{Z}$,

(Die Reihenfolge der Koordinaten mag auf den ersten Blick verwundern; sie kommt daher, daß wir die Steigung α der Geraden durch die Steigung des Ortsvektors zum Punkt (q, p) annähern wollen, und die ist p/q.)

Die folgende Konstruktion liefert Punkte P_n nahe der Geraden, die für gerade n stets unterhalb $y = \alpha x$ liegen und für ungerade n darüber:

Wir starten mit $P_{-2} = (1, 0)$ und $P_{-1} = (0, 1)$.

Zu zwei Punkten $P = (q, p)$ und $P' = (q', p')$, die auf verschiedenen Seiten der Geraden liegen, gibt es stets eine nichtnegative ganze Zahl $c \in \mathbb{N}_0$, so daß $P + cP'$ entweder auf der Geraden liegt oder aber auf derselben Seite wie P, während $P + (c+1)P'$ auf der anderen Seite liegt.

Liegt nämlich beispielsweise P unterhalb der Geraden, so ist $p/q < \alpha$, also $p - \alpha q < 0$. Für den oberhalb der Geraden liegenden Punkt P' ist entsprechend $p' - \alpha q' > 0$. Damit ist klar, daß

$$c = \left[\left| \frac{p - \alpha q}{p' - \alpha q'} \right|\right]$$

das Verlangte leistet. Man überlegt sich leicht, daß diese Formel auch gilt, wenn P oberhalb und P' unterhalb der Geraden liegt.

Zähler und Nenner des obigen Bruchs lassen sich einfach geometrisch interpretieren: $(q, \alpha q)$ hat dieselbe x-Koordinate wie $P = (q, p)$ und liegt auf der Geraden $y = \alpha x$; daher ist $p - \alpha q$ der (gerichtete) vertikale Abstand von P zur Geraden und $p' - \alpha q'$ entsprechend der von P'.

Ausgehend von $P = P_{-2} = (1, 0)$ und $P' = P_{-1} = (0, 1)$ definieren wir nun die Punkte P_n für $n \geq 0$ mit dem wie oben definierten $c = c_n$ aus ihren beiden Vorgängern rekursiv als

$$P_n = P_{n-2} + c_n P_{n-1} .$$

Dann liegt P_n auf derselben Seite der Geraden wie P_{n-2}, für gerades n also unterhalb und für ungerades oberhalb – es sei denn, irgendwann einmal liegt ein P_n *auf* der Geraden. In diesem Fall ist α rational und wir brechen die Konstruktion ab. Für irrationales α erhalten wir eine unendliche Folge von Punkten P_n.

Bezeichnen wir mit $d_n = p_n - \alpha$
des Punktes $P_n = (q_n, p_n)$ von d
Formel

$$c_n =$$

Daher verschwindet c_n genau dan

Ist dagegen $|d_{n-1}| < |d_{n-2}|$, so i
auf derselben Seite der Geraden l

$$d_n = d_{n-2} + c_n d_{n-1}$$

$$= d_{n-1} \left(\left[\left| \frac{d_{n-2}}{d_{n-1}} \right| \right] \right.$$

betragsmäßig kleiner als d_{n-1}. (
schiedene Vorzeichen haben!) Fal
von P_{n-1} zur Geraden $y = \alpha x$ kle
auch für alle folgenden Indizes, u

Die ersten beiden Abstände sind
ab, welche der beiden Zahlen der

Der nächste Punkt ist $P_0 = (1, c_0$
und der Betrag davon ist kleiner
der Koeffizient c_n von Null versc

Aus den Beziehungen $p_n = p_{n-}$
sehen wir daher, daß die Folge d
monoton ansteigt, während die Fo

$$\left| \alpha - \frac{}{} \right.$$

strikt monoton fällt. Die Brüch
Annäherungen an α.

Wir können die obigen Rekursion
gleichung

$$\begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} = \left($$

wenden wir darauf den Multiplikationssatz für Determinanten an, erhalten wir die Formel

$$p_n q_{n-1} - q_n p_{n-1} = -(p_{n-1}q_{n-2} - q_{n-1}p_{n-2})\,.$$

Für $n = 0$ ist $p_{-1}q_{-2} - q_{-1}p_{-2} = 0 \cdot 0 - 1 \cdot 1 = -1$; daraus folgt induktiv die Formel $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$. Insbesondere sind die Zahlen p_n und q_n stets teilerfremd, p_n/q_n ist also ein gekürzter Bruch.

Als nächstes wollen wir uns überlegen, daß die Folge dieser Brüche gegen α konvergiert. Da P_n und P_{n+1} auf verschiedenen Seiten der Geraden $y = \alpha x$ liegen, ist für $n \geq 0$

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\frac{p_{n+1}q_n - q_{n+1}p_n}{q_n q_{n+1}}\right|$$
$$= \frac{1}{q_n q_{n+1}} = \frac{1}{q_n(q_{n-1} + c_{n+1}q_n)} \leq \frac{1}{q_n^2}\,.$$

Da die Folge der q_n strikt monoton ansteigt, konvergiert die Folge der p_n/q_n somit gegen α, und dies sogar extrem gut: Ist p/q eine rationale Approximation einer irrationalen Zahl α, so kann der Fehler im allgemeinen bis zu $1/2q$ betragen; hier ist er höchstens $1/q^2$ und tatsächlich wohl, da wir recht grob abgeschätzt haben, meist noch kleiner. Wie wir gleich sehen werden, muß umgekehrt p/q eine Konvergente der Kettenbruchentwicklung von α sein, wenn $|\alpha - p/q| < 1/2q^2$ ist.

Zuvor müssen wir uns aber noch überlegen, daß die hier betrachteten Brüche p_n/q_n tatsächlich die Konvergenten der in §1 definierten Kettenbruchentwicklung sind und daß die hier betrachteten Zahlen c_i mit denen übereinstimmen, die der Kettenbruchalgorithmus liefert.

Dazu setzen wir

$$\alpha_n = \left|\frac{d_{n-1}}{d_{n-2}}\right| = -\frac{d_{n-1}}{d_{n-2}}\,;$$

zumindest für $n \geq 1$ ist dann $\alpha_n < 1$. Wegen $c_n = \left[\left|d_{n-2}/d_{n-1}\right|\right]$ ist dann $c_n = [1/\alpha_n]$. Division der Beziehung $d_n = d_{n-2} + c_n d_{d-1}$ durch d_{n-1} führt auf

$$\frac{d_n}{d_{n-1}} = \frac{d_{n-2}}{d_{n-1}} + c_n \quad \text{oder} \quad -\alpha_{n+1} = -\frac{1}{\alpha_n} + c_n\,,$$

was wir wiederum umformen kön

$$\frac{1}{\alpha_n} =$$

Da $c_n = [1/\alpha_n]$ ist $\alpha = c_0 + \alpha_1$, ierten Folgen der c_n und α_n.

Insbesondere liefern unsere Reku und q_n Zähler und Nenner der K lung von α, was wir als Satz festh

Satz: Ist $\alpha = [c_0, c_1, c_2, \dots]$ die Zahl, so lassen sich die Konverg berechnen:

$$p_0 = c_0, q_0 = 1, p$$
$$p_n = p_{n-2} + c_n p_{n-1} \quad \text{und}$$

Die so berechneten Zahlen p_n un $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$ für

Zu *beweisen* gibt es hier nichts bereits bewiesen für die Koordin gerade gesehen haben, sind das Konvergenten.

Für spätere Anwendungen wolle sich α aus α_n sowie den Konv berechnet läßt: Nach Definition is

$$\alpha_n = -\frac{d_{n-1}}{d_{n-2}}$$

Damit ist $\alpha_n(\alpha q_{n-2} - p_{n-2}) = p$ der Terme auf $\alpha(\alpha_n q_{n-2} + \alpha q_{n-}$

$$\alpha = \frac{\alpha_n}{\alpha_n}$$

§3: Optimale Approximation

Nach den Vorbereitungen im letzten Paragraphen können wir nun beweisen, daß Kettenbrüche in der Tat bestmögliche Approximationen sind im folgenden Sinne: Ist r/s irgendein Bruch, dessen Nenner s zwischen den Nennern q_{n-1} und q_n zweier Konvergenten der Kettenbruchentwicklung liegt, so ist p_{n-1}/q_{n-1} eine bessere Approximation als r/s:

Lemma: p_n/q_n seien die Konvergenten der Kettenbruchentwicklung einer reellen Zahl α. Falls α irrational ist oder rational mit einem Nenner echt größer q_n, $n \geq 2$, so ist für jede rationale Zahl r/s mit $s \leq q_n$ und $r/s \notin \{p_{n-1}/q_{n-1}, p_n/q_n\}$

$$\left|\alpha - \frac{r}{s}\right| > \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| .$$

Beweis: Wir betrachten die Punkte $P_{n-1} = (q_{n-1}, p_{n-1})$, $P_n = (q_n, p_n)$ und $R = (s, r)$. Es genügt zu zeigen, daß der vertikale Abstand von P_{n-1} zur Geraden $y = \alpha x$ einen kleineren Betrag hat als der von R.

Wir schreiben R als ganzzahlige Linearkombination $R = kP_{n-1} + \ell P_n$ der Punkte P_{n-1} und P_n. Das ist möglich, denn die Determinante des linearen Gleichungssystems

$$\begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix} \begin{pmatrix} k \\ \ell \end{pmatrix} = \begin{pmatrix} r \\ s \end{pmatrix}$$

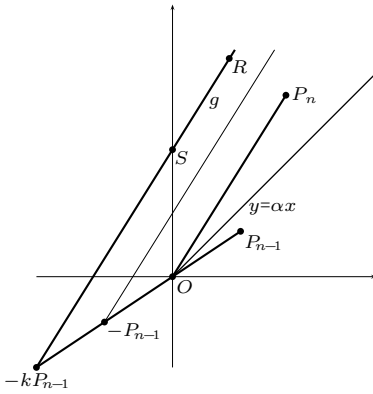
ist nach dem Satz am Ende des vorigen Paragraphen gleich

$$p_{n-1}q_n - p_n q_{n-1} = (-1)^{n-1} .$$

Die somit eindeutig bestimmte Lösung (k, ℓ) des Gleichungssystems ist ganzzahlig, denn wenn wir sie nach der CRAMERschen Regel ausdrücken, sind k und ℓ Brüche mit dieser Determinante im Nenner und einer ganzzahligen Determinante im Zähler.

Für das Folgende wollen wir uns auf den Fall $p_{n-1}/q_{n-1} < \alpha < p_n/q_n$ beschränken; der Fall $p_{n-1}/q_{n-1} > \alpha > p_n/q_n$ geht völlig analog.

Wir betrachten die Gerade g dur
nach unserer Annahme ist ihre St



indem wir $k = -1$ setzen, denn in
Geraden $y = \alpha x$ am kleinsten. I
denselben Abstand von $y = \alpha x$
von S größer ist als die von $-P_n$
von $y = \alpha x$ als P_{n-1}. Im Fall $k <$

Als nächstes betrachten wir den F
sonst wäre die x-Koordinate $s =$
Punkt kP_{n-1} liegt unterhalb der G
sich dieser mit steigender Abszi
entweder dieselbe Abszisse wie
Abstand somit höchstens gleich
fache des Abstands von P_{n-1} is
gewünschte strikte Ungleichung.
wegen der Voraussetzung $R \neq P_n$

Bleibt noch der Fall $k = 0$. Dann
Anderseits kann ℓ auch nicht grö
kommt dieser Fall gar nicht vor.

Als nächstes wollen wir uns üb
Konvergenten der Kettenbruche

bereits, daß für die Konvergenten gilt

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}\,.$$

Dies charakterisiert die Konvergenten allerdings noch nicht: Betrachten wir etwa die Kettenbruchentwicklung von $\alpha = \sqrt{3}$. Der Algorithmus liefert zunächst $c_0 = \lfloor\sqrt{3}\rfloor = 1$ und $\alpha_1 = \sqrt{3} - 1$. Der Kehrwert davon ist

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} \Longrightarrow c_1 = 1 \quad \text{und} \quad \alpha_2 = \frac{\sqrt{3}-1}{2}\,.$$

Der Kehrwert davon ist

$$\frac{2}{\sqrt{3}-1} = \sqrt{3}+1 \Longrightarrow c_2 = 2 \quad \text{und} \quad \alpha_3 = \sqrt{3}-1 = \alpha_1\,.$$

Ab hier wiederholt sich also alles periodisch, d.h.

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cdots}}}} = [1, \overline{1,2}]\,.$$

Die ersten Konvergenten der Kettenbruchentwicklung sind

$$1, \quad 2, \quad 1\frac{2}{3}, \quad 1\frac{3}{4}, \quad 1\frac{8}{11} \quad \text{und} \quad 1\frac{11}{15}\,;$$

da die Folge der Nenner monoton steigt, gibt es also keine Konvergente mit Nenner sieben. Trotzdem ist

$$\left|\sqrt{3} - 1\frac{5}{7}\right| \approx 0{,}017765 < 0{,}2 = \frac{1}{50} < \frac{1}{49} = \frac{1}{7^2}\,.$$

Dafür gilt aber der folgende Satz, dessen zweite Hälfte bereits 1808 von ADRIEN-MARIE LEGENDRE (1752–1833) bewiesen wurde:

Satz: *a)* Eine irrationale Zahl α erfüllt für jedes $n \geq 2$ mindestens eine der beiden Ungleichungen

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2} \quad \text{oder} \quad \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2}\,.$$

b) Erfüllen zwei ganze Zahlen p,

ist $\frac{p}{q}$ eine Konvergente der Kette

Beweis: a) Angenommen, beide U
tiplikation mit q_{n-1} *bzw.* q_n habe

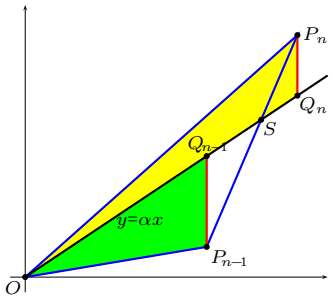
$$\left|q_{n-1}\alpha - p_{n-1}\right| \geq \frac{1}{2q_{n-}$$

Wir nehmen für den Beweis wie
ist; der umgekehrte Fall geht völl

Nach unserer Annahme liegt der
der Geraden $y = \alpha x$, und $P_n = (q$

Das Kreuzprodukt (siehe Anha
hat als Betrag die Fläche des da
das Dreieck mit Ecken O, P_{n-1}
Beziehung $p_n q_{n-1} - q_n p_{n-1} =$ (
daher gleich $1/2$.

Als nächstes betrachten wir zu d
tionen $Q_i = (q_i, \alpha q_i)$ in y-Richt
Dreiecke $\triangle OP_iQ_i$. Nach Voraus
für $i = n-1$ und $i = n$ mindesten
Höhe ist q_i, also ist die Fläche jede



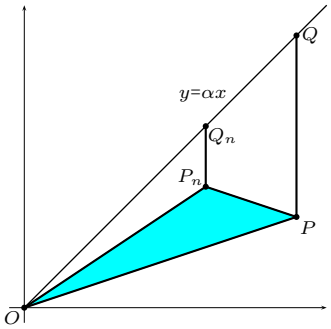
ist das zweite dieser Dreiecke das kleinere. Daher ist die Fläche des Dreiecks $\triangle OP_{n-1}P_n$ größer als die Summe der Flächen der Dreiecke $\triangle OP_{n-1}Q_{n-1}$ und $\triangle OP_nQ_n$, also größer als $1/4 + 1/4 = 1/2$. Dies ist ein Widerspruch zur obigen direkten Berechnung dieser Fläche.

b) Wir können natürlich voraussetzen, daß der Bruch p/q gekürzt ist, denn für jede nichtgekürzte Darstellung ist die Bedingung echt schärfer.

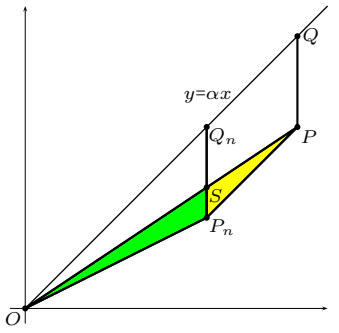
Da die Folge der Nenner q_n strikt monoton ansteigt, gibt es genau ein n, so daß $q_n \le q < q_{n+1}$ ist; wir müssen zeigen, daß $p/q = p_n/q_n$ ist. Andernfalls ist $pq_n - qp_n \neq 0$, also – da dies eine ganze Zahl ist – $|pq_n - qp_n| \ge 1$. Setzen wir $P = (q, p)$, so ist also die Fläche des Dreiecks $\triangle OPP_n$ mindestens gleich $1/2$.

Seien wieder $Q = (q, \alpha q)$ und $Q_n = (q_n, \alpha q_n)$ die Projektionen der betrachteten Punkte auf die Gerade $y = \alpha x$. Die Länge der Strecke $\overline{PQ}$ ist $|\alpha q - p|$, was nach Voraussetzung kleiner als $1/2q$ ist. Nach dem Lemma zu Beginn dieses Paragraphen ist die Strecke $\overline{P_nQ_n}$ kürzer als $\overline{PQ}$, also ebenfalls kleiner als $1/2q$ und damit erst recht kleiner als $1/2q_n$. Somit haben beide Dreiecke $\triangle OPQ$ und $\triangle OP_nQ_n$ Flächen, die kleiner sind als $1/4$.

Wir wollen uns überlegen, daß dann auch die Fläche des Dreiecks $\triangle OPP_n$ kleiner als $1/2$ sein muß, im Widerspruch zur obigen Rechnung. Die Geometrie hängt dabei stark davon ab, wie die Punkte P und P_n sowohl zueinander wie auch in Bezug auf die Gerade $y = \alpha x$ liegen.



Betrachten wir als erstes den Fall, daß p_n/q_n zwischen α und p/q liegt. Dann liegt der Punkt P_n im Innern des Dreiecks $\triangle OPQ$, also ist das gesamte Dreieck $\triangle OPP_n$ im Dreieck $\triangle OPQ$ enthalten. Da ersteres mindestens die Fläche $1/2$ hat, letzteres aber weniger als $1/4$, kann dieser Fall offensichtlich nicht vorkommen.

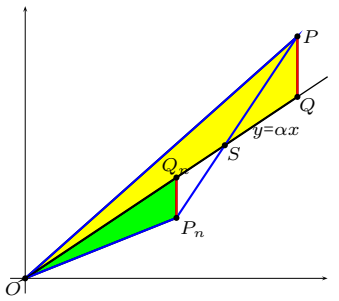


die verdoppelte Fläche des gesam

$$\left|\overline{SP_n}\right| \cdot q_n + \left|\overline{SP_n}\right| \cdot (q - q_n) =$$

denn da q zwischen q_n und q_{n+1} keinen größeren Abstand von der steht aber die verdoppelte Fläch wissen, daß sie höchstens gleich auftreten kann.

Bleibt noch der Fall, daß α zwis also auf verschiedenen Seiten schneidet ihre Verbinungsstrecke Damit sind wir in einer ähnliche Das Dreieck $\triangle OPP_n$ ist gleich Dreieck $\triangle OPQ$ plus $\triangle SP_nQ_n$



Anhang: Das Kreuzprodukt zweier Vektoren

Im $\mathbb{R}^3$ (und nur dort) gibt es eine bilineare Verknüpfung, die zwei Vektoren einen dritten zuordnet, das (vielleicht aus der Schule bekannte) Vektorprodukt oder Kreuzprodukt. Wie schon der Name sagt, ordnet es je zwei Vektoren v und w aus $\mathbb{R}^3$ einen *Vektor* zu, und dieser wird mit $v \times w \in \mathbb{R}^3$ bezeichnet. Er ist festgelegt durch folgende Eigenschaften:

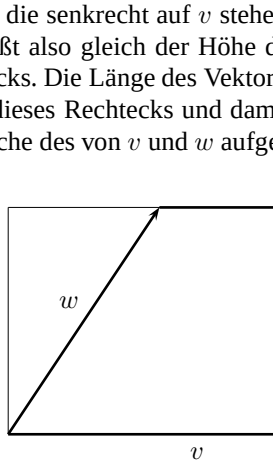
- $v \times w$ hat die Länge $|v \times w| = |v|\,|w|\,|\sin \measuredangle(v,w)|$.
  Insbesondere ist also $v \times w = \vec{0}$, wenn v und w auf einer Geraden liegen, denn dann bilden sie einen Winkel von null oder 180 Grad, so daß der Sinus verschwindet.
- $v \times w$ steht senkrecht sowohl auf v als auch auf w.
  Falls $v \times w \neq \vec{0}$ ist, spannen v und w eine Ebene auf, auf der (da wir im $\mathbb{R}^3$ sind) genau ein eindimensionaler Unterraum senkrecht steht. Darin gibt es allerdings für jede vorgegebene positive Länge zwei Vektoren, die sich durch ihr Vorzeichen unterscheiden. Um $v \times w$ eindeutig festzulegen, brauchen wir daher noch eine weitere Bedingung:
- Die drei Vektoren v, w und $v \times w$ bilden ein Rechtssystem, d.h. wenn sich die Finger der *rechten* Hand so ausrichten lassen, daß der Daumen in Richtung von v zeigt, der Zeigefinger in Richtung von w und der Mittelfinger in Richtung von $v \times w$.

Alternativ kann man ein Rechtssystem auch so definieren, daß sich, ein von v nach w gedrehter Korkenzieher in Richtung $v \times w$ in den Kork bohrt. Ähnlich geht es auch mit Schrauben; da es allerdings neben den (üblichen) Rechtsschrauben auch die (seltenen) Linksschrauben gibt, ist diese Definition eventuell zirkulär: Alles hängt davon ab, wie man Rechtsschrauben definiert.

Aus jeder dieser Regeln folgt sofort die *Antikommutativität* des Vektorprodukts:

$$v \times w = -w \times v\,.$$

Weitere Rechenregeln lassen sich leicht geometrisch ableiten: Da der Sinus eines Winkels gleich Gegenkathete durch Hypothenuse ist, ist in der von v und w aufgespannten Ebenen $|w|\,|\sin \measuredangle(v,w)|$ gleich der Länge des auf die senkrecht auf v stehe
das heißt also gleich der Höhe d
Rechtecks. Die Länge des Vektor
inhalt dieses Rechtecks und dam
der Fläche des von v und w aufge



Daraus folgt nun sofort das Distri

$$v \times (w + u)$$

für den zweiten Faktor, und wege
wiederum das für den ersten:

$$(u + v) \times w$$

Um das Vektorprodukt in Koord
wir zunächst die Produkte der K
Da sie allesamt die Länge eins ha
recht stehen, ist klar, daß das Pro
toren bis aufs Vorzeichen gleich
ab von der Orientierung des Ko
Vektors e_i mit sich selbst ist natü
mit sich selbst, gleich dem Nullve
ist null Grad.

Für die folgende Rechnung wolle
dieser Reihenfolge ein Rechtssyst
der Fall, wenn e_1 nach rechts, e_2

Dann folgt sofort, daß

$$e_1 \times e_2 = e_3$$

ist, und nach einigen Fingerübungen auch findet man auch die Formeln

$$e_2 \times e_3 = e_1 \quad \text{und} \quad e_1 \times e_3 = -e_2\,.$$

Die Produkte mit vertauschten Faktoren sind natürlich gerade das negative davon, und $e_i \times e_i = 0$. Für

$$v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \quad \text{und} \quad w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}$$

ist also

$$v \times w = (v_1e_1 + v_2e_2 + v_3e_3) \times (w_1e_1 + w_2e_2 + w_3e_3)\,,$$

nach den obigen Rechenregeln gleich

$$\sum_{i=1}^{3}\sum_{j=1}^{3} v_iw_j\, e_i \times e_j$$

$$= (v_2w_3 - v_3w_2)e_1 + (v_3w_1 - v_1w_3)e_2 + (v_1w_2 - v_2w_1)e_3\,,$$

d.h.

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \times \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \begin{pmatrix} v_2w_3 - v_3w_2 \\ v_3w_1 - v_1w_3 \\ v_1w_2 - v_2w_1 \end{pmatrix}\,.$$

Dies läßt sich dadurch merken, daß man im Schema

$$\begin{array}{ccccccccc} e_1 & & e_2 & & e_3 & & e_1 & & e_2 \\ & \searrow & & \times & & \times & & \swarrow & \\ v_1 & & v_2 & & v_3 & & v_1 & & v_2 \\ & \swarrow & & \times & & \times & & \searrow & \\ w_1 & & w_2 & & w_3 & & w_1 & & w_2 \end{array}$$

von e_i ausgeht und als dessen Koeffizient das Zweierprodukt entlang der schrägen Linie nach rechts unten *positiv* und das entlang der schrägen Linie nach links unten *negativ* nimmt; man wendet also die SARRUSsche Regel an auf die „Determinante“

$$\begin{vmatrix} e_1 & e_2 & e_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{vmatrix}\,.$$

§4: Kettenbrüche und Ka

Schon in den ältesten bekannten K
nach astronomischen Gesetzmäßi
Sonne, dem Umlauf des Mondes
Erde um sich selbst.

Der Tag als Zeiteinheit ist ein so
bensrhythmus, daß er als Zeitei
selbstverständlich war, daß als Ta
der Erde um ihre Achse genon
Minuten längere Zeitraum, bis s
zuwendet.

Als nächstgrößere Einheit führte
Woche ein; ob sie sich dabei vor
Mondphasen leiten ließen, ist unb
sieben Tagen auch einfach desha
Zahl galt.

Definitiv vom Mond abgeleitet
bekanntlich um die Erde; die Ze
trägt ungefähr 27,3 Tage. Diese
allerdings für die Kalenderrechn
mung wurden seit Alters her di
Mondphasen verwendet. Da der M
Sonnenlicht reflektiert, hängen d
Sonne und Mond; für den Kalen
synodische Monat von 29,53 Ta
stand wiederholt. (Der tatsächlich
ist wegen der komplizierten Mon
Mittel kommt man auf den synod

Da 29,53 keine ganze Zahl ist, las
feste Anzahl von Tagen definier
Kalender mal 29, mal 30 Tage ha

Einer der einfachsten und zugleich
der islamische: Sobald mindesten

neuen Mond gesehen haben, beginnt ein neuer Monat, bei bewölktem Himmel unabhängig davon dreißig Tage nach dem letzten Monatsanfang. Alle zwölf Monate beginnt ein neues Jahr.

Es ist klar, daß bei einer solchen Festlegung die Länge der Monate sowohl innerhalb eines Jahres als auch von Jahr zu Jahr schwankt, außerdem sind die Jahre nicht synchron zum Umlauf der Erde um die Sonne. Da der Kalender auf der arabischen Halbinsel entstand, wo Jahreszeiten keine Rolle spielen und auch die Landwirtschaft das ganze Jahr über konstante Bedingungen vorfindet, ist letzteres dort kein Nachteil.

Für Regionen mit ausgeprägten Jahreszeiten oder jährlich wiederkehrenden Ereignissen ist die Synchronisation des Kalenders mit der Sonne wichtiger als die mit dem Mond. Das wohl älteste Beispiel eines reinen Sonnenjahrs bietet der ägyptische Kalender. Da die für die Landwirtschaft fundamentalen jährlichen Nilüberschwemmungen ungefähr mit der ersten Sichtung des Sterns Sirius übereinstimmten, wurde dieses Ereignis als Beginn des neuen Jahrs genommen. Dies ist das sogenannte *siderische* Jahr mit einer Länge von 365,256 Tagen. Obwohl die Ägypter wußten, daß diese Länge ungefähr $365\frac{1}{4}$ Tage beträgt, legten Sie doch fest, daß jedes Jahr genau 365 Tage haben sollte, verteilt auf zwölf Monate zu jeweils dreißig Tagen sowie fünf Zusatztage.

Ein Jahr, das wirklich synchron zu den Jahreszeiten ist, sollte allerdings nicht anhand des Fixsternhimmels definiert werden, sondern anhand jahreszeitlicher Phänomene wie beispielsweise der Tag- und Nachtgleiche oder dem Durchgang der Sonne durch den Frühlingspunkt. Das ist (im Mittel) das sogenannte *tropische* Jahr mit einer Länge von 356,2422 Tagen. Der Unterschied zum siderischen Jahr ist zwar gering, aber – wie wir gleich sehen werden – trotzdem relevant.

Viel bedeutender als dieser Unterschied war aber zunächst einmal die Tatsache, daß ein Jahr mit exakt 365 Tagen natürlich im Laufe der Jahrhunderte zu einem Verlust der Synchronisation des Kalenders mit den Jahreszeiten führt. Aus diesem Grund beauftragte GAIUS JULIUS CAESAR (100–44) den alexandrinischen Astronomen SOSIGENES mit einer Kalenderreform, die die damit verbundene Verschiebung des Jahresanfang (die sich in nur 120 Jahren auf einen Monat summiert) kompensieren sollte.

Das Ergebnis, der *Julianischer Ka*
1. Januar des Jahres 709 *ab urbe*
Rom. In unserer heutigen Zeitre
Jahr 45 v.Chr. Die Monatsnamen
ders sind die heute noch gebräu
klassischen ägyptischen Kalende
jedem vierten Jahr ein Schalttag e

Dabei blieb es bis ins sechzehn
astronomisch etwas zu lange Ju
beispielsweise der Frühjahrsson
Um dies zu korrigieren, setzte
PAGNI, 1502–1585, Papst ab 157
von deren Empfehlungen in den
durch vierhundert teilbar sind, au
Gregorianische Kalender trat in
dem 15. Oktober 1582 in Kraft; u
des Julianischen Kalenders zu ko
noch Julianischen Donnerstag, d
schen Ländern galt der Julianisc
schließlich (mit den verschieden
den Gregorianischen ersetzt – zul

Um die Neuerung des Gregorianis
ten wir die Kettenbruchentwicklu

$$[365, 4, 7, $$

und hat die Konvergenten

$$365, \quad 365\frac{1}{4}, \quad 365\frac{7}{29}, \quad 36$$

Der Julianische Kalender verwen
vergente $365\frac{1}{4}$. Unter den folge
mit einem Nenner, der sich gut fü
würde. Am ehesten kommt vielle
er ungefähr ein Drittel von hund
ximation $365\frac{8}{33}$, so sollten unter

24 pro 99 Jahre. Nimmt man stattdessen 24 Schaltjahre pro Jahrhundert, was der Regel entspricht, daß durch hundert teilbaren Jahre *keine* Schaltjahre sind, so sorgt der Unterschied zwischen 99 und 100 dafür, daß nach jeweils 400 Jahren eine Vierjahresperiode fehlt. Auch diese hat Anspruch auf ein Schaltjahr, daher die Gregorianische Regel, daß durch hundert teilbare Jahre *keine* Schaltjahre sind, es sei denn, die Jahreszahl sei sogar durch vierhundert teilbar. Innerhalb einer jeden Periode von 400 Jahren gibt es also $100 - 3 = 97$ Schaltjahre; das Gregorianische Jahr hat somit eine Länge von $365\frac{97}{400}$ Tagen, eine praktikable Zahl in der Nähe der Konvergente $365\frac{8}{33}$.

Zum Einstieg in die Kalenderrechnung beginnen wir mit dem einfachsten Problem, den Wochentagen, und überlegen wir uns, auf welchen Wochentag der T-te Tag des M-ten Monats im Jahr J fällt.

Alle Wochen haben exakt sieben Tage und die Jahre haben nach einer recht klaren Regel 365 oder 366 Tage; es ist daher relativ einfach, den Wochentag für den i-ten Tag des Jahres zu berechnen, sofern man ihn für irgendeinen anderen Tag dieses Jahres kennt: Er hängt innerhalb eines Jahres schließlich nur ab von $i \bmod 7$.

Um auch die Abhängigkeit vom Jahr noch zu berücksichtigen, ist es am einfachsten, die Tage nicht vom 1. Januar des jeweils betrachteten Jahres aus zu zählen, sondern ab irgendeinem festen Datum. Historisch sinnvoll wäre hier beispielsweise das Datum der Einführung des Gregorianischen Kalenders; da hier aber Jahr, Monat und Tag „krumme“ Zahlen sind, würde dies zu unnötig komplizierten mathematischen Formeln mit zu vielen willkürlich erscheinenden Konstanten führen.

Für die Mathematik ist es unerheblich, ob zum fiktiven Anfangspunkt bereits der Gregorianische Kalender in Gebrauch war oder nicht; wir können daher beispielsweise ausgehen von einem 1. Januar eines fiktiven Jahres Null. (Die Zählung der Jahre ab Christi Geburt wurde im sechsten Jahrhundert initiiert von DIONYSIUS EXIGUUS, der allerdings ein falsches Geburtsjahr 1 berechnete, auf das wir uns heute noch beziehen. Jahre davor interessierten ihn nicht; der erste der auch Jahre zuvor in Bezug auf Christi Geburt datierte, war wohl der angelsächsische Theologe und Historiker BEDA VENERABILIS (673–735), der – da er keine Null kannte – das Jahr vor dem Jahr ei
bezeichnete.)

Wenn wir dem fiktiven 1. Janua
Einfachheit halber davon ausgeh
war, können wir die Nummer des
gendermaßen berechnen: Bis da
denen jedes mindestens 365 Tag
$365(J-1)$ Tage zusammen. Wa
Julianischen Kalender hätte es
gorianischen sind aber die durch
Jahre keine Schaltjahre, also müs
subtrahieren. Der i-te Tag des Jah

$$365(J-1) + [(J-1)/4] -$$

Um den zugehörigen Wochentag
den Wochentag des Tags Numm
von irgendeinem bekannten Datu
2014 ist der $(31 + 28 + 31 + 10)$
die Nummer

$$365 \cdot 2013 + 503 -$$

Diese Zahl ist kongruent vier m
Montag. Geben wir den Wochenta
vorsehen, von Montag ausgehend
der Tag mit Nummer i also auf
wobei die Null dem normgemäß

Tatsächlich hätten wir die obige
Da $365 \equiv 1 \bmod 7$ ist, reicht es,

$$(J-1) + [(J-1)/4] - [(J -$$

berechnen, im Beispiel also

$$2013 + 503 - 20 + 5$$

Um den Wochentag zu einem
können, müssen wir immer noch

der T-te Tag des M-ten Monats ist. Eine sehr einfache Methode besteht darin, daß wir zählen, wie viele Tage vor dem Ersten des jeweiligen Monats bereits vergangen sind. Dabei müssen wir natürlich zwischen Schaltjahren und gewöhnlichen Jahren unterscheiden: Für letztere seien dies t_M Tage, für erste s_M. Dann haben wir folgende Tabelle:

M =	1	2	3	4	5	6	7	8	9	10	11	12
t_M =	0	31	59	90	120	151	181	212	243	273	304	334
s_M =	0	31	60	91	121	152	182	213	244	274	305	335

Dann fällt der T-te Tag des M-ten Monats des Jahrs J auf den Wochentag mit der Nummer

$$(J-1) + [(J-1)/4] - [(J-1)/100] + [(J-1)/400] + t_M + T$$

modulo sieben, falls J kein Schaltjahr ist; andernfalls muß t_M durch s_M ersetzt werden. Es genügt natürlich, die Zahlen t_M oder s_M modulo 7 einzusetzen, also

M =	1	2	3	4	5	6	7	8	9	10	11	12
t_M mod 7 =	0	3	3	6	1	4	6	2	5	0	3	5
s_M mod 7 =	1	4	4	0	2	5	0	3	6	1	4	6

Da wohl niemand eine dieser beiden Tabellen auswendig lernen möchte, stellt sich die Frage, ob es vielleicht auch eine geschlossene Formel gibt. Dazu ignorieren wir zunächst einmal die historisch überkommenen Monatslängen und tun so, als könnte ein Mathematiker am grünen Tisch festlegen, wie er 365 Tage auf zwölf Monate verteilt.

Für ihn wäre die am wenigsten irreguläre Verteilung der Monatslängen wohl die, bei der Tag i eines Jahres mit N Tagen genau dann im k-ten Monat liegt, wenn gilt

$$\frac{(k-1)N}{12} < i \le \frac{kN}{12} \quad \text{oder} \quad k - 1 < \frac{12i}{N} \le k\,,$$

d.h. k ist die kleinste ganze Zahl größer oder gleich $12i/N$. Für ein Jahr mit $N = 365$ Tagen würde dies auf die Monatslängen

$$30, 30, 31, 30, 31, 30, 30, 31, 30, 31, 30, 31$$

führen, in einem Schaltjahr mit N
dreißig und alle geraden Monat
29 Tagen kann bei einer derartige

Trotzdem läßt sich auch unser ch
solche Formel bringen: Nehmen
Tagen und zwölf Monaten. Dann
Monate der Längen

$$30, 31, 30, 31, 30, 3$$

wir haben also wie im wirkliche
derfolgende Monate mit 31 Tage
und Dezember/Januar, hier sind e
Wenn wir zyklisch um eine Posit
an der ersten Stelle steht, stimme
abgesehen vom Februar, der hier
Folge der Monatslängen.

(Kurioserweise gab es 1712 in Sc
und einem 30. Februar: 1699 w
gorianischen Kalender überzugel
1700 zu streichen. Danach wurd
wieder synchron zum Julianisch
einen 30. Februar als zweiten Sch
Kalender dann endgültig und abr

Die Anzahl der Tage vor dem Erst
hypothetischen Kalender einfach
Verschiebung wird diese Formel
werden durch eine Verschiebung i
zeigt, sind in einem Jahr mit 367
hat, vor dem Ersten des M-ten M
vergangen. Somit ist für unseren

$$t_M = \begin{cases} \left[\frac{367M-362}{12}\right] \\ \left[\frac{367M-362}{12}\right] \end{cases}$$

$$s_M = \begin{cases} \left[\frac{367M-362}{12}\right] \\ \left[\frac{367M-362}{12}\right] \end{cases}$$

Der Wochentag des T-ten Tags im M-ten Monat des Jahrs J ist somit

$$(J-1)+\left[\frac{J-1}{4}\right]-\left[\frac{J-1}{100}\right]+\left[\frac{J-1}{400}\right]+\left[\frac{367M-362}{12}\right]+\delta_M+T$$

modulo sieben mit

$$\delta_M=\begin{cases}0 & \text{falls } M\le 2\\ -1 & \text{falls } M\ge 3 \text{ und } J \text{ Schaltjahr}\\ -2 & \text{falls } M\ge 3 \text{ und } J \text{ kein Schaltjahr}\end{cases}.$$

Diese Formel gilt selbstverständlich nur für Daten nach dem Gregorianischen Kalender; bei älteren Daten muß man zunächst wissen, auf welchem Kalender und welchem Jahresanfang sie beruhen.

Als beispielsweise der amerikanische Naturwissenschaftler, Philosoph und Politiker BENJAMIN FRANKLIN geboren wurde, zeigten die Kalender in seiner Heimatstadt Boston den 6. Januar 1705. Massachusetts war zu der Zeit noch britische Kolonie, und da Großbritannien den Gregorianischen Kalender erst 1752 einführte, ist das ein Julianisches Datum. Gregorianisch ist sein Geburtstag elf Tage später, d.h. am 17. Januar. Allerdings handelt es sich dabei nicht um den 17. Januar 1705, sondern um den des Jahres 1706: In Großbritannien begann das neue Jahr damals nämlich nicht am ersten Januar, sondern am 25. März. Auf den 31. Dezember 1705 folgte also der 1. Januar 1705 und auf den 24. März 1705 der 25. März 1706. Solche Besonderheiten bei der Interpretation alter Datumsangaben gibt es viele; hier ist also Vorsicht geboten.

Mindestens genauso wichtig wie eine verbesserte Schaltjahrregel war für Papst Gregor das Datum des Osterfests; auch darum sollte sich seine Kommission kümmern. Damit kam nun plötzlich auch der Mond in den Kalender, denn 325 beschloß das Konzil von Nicäa (bei Konstantinopel), daß Ostern stets am ersten Sonntag nach dem ersten Vollmond am oder nach der Frühlings-Tag-und-Nacht-Gleiche zu feiern sei. (Man beachte, daß das erste *nach* im Sinne eines $>$, das zweite im Sinne eines $\ge$ definiert ist. Der Grund für das $>$ lag darin, daß so Ostern nur sehr selten gleichzeitig mit dem jüdischen Pascha-Fest begangen wird.)

Der erste Vollmond am oder nach der Frühlings-Tag-und-Nacht-Gleiche kann nicht einfach nach einer ähnlichen Regel wie der Monatsanfang im islamischen Kalender bestimmt werden, also etwa dann, wenn ihn

mindestens zwei vertrauenswürdi
österliche Festkreis beginnt berei
mußte daher im Voraus berechnet
matiker DONALD E. KNUTH sagt
Art of Computer Programming: T
important application of arithme
was the calculation of the Easter
torically significant. So ordnete
bei seiner Neuordnung des Bildu
Diözese mindestens ein Geistlich
datum zuverlässig zu berechnen
Gregor das Osterdatum berechne

Wir brauchen Informationen über
und über die Tag-Nacht-Gleiche
gorianische Kalender das tropisch
recht lange konstant am 21. März
nung des Osterdatums geht man
man Wochentage bestimmt, habe
noch das Problem mit den Mondp

Die mittlere Zeitspanne zwische
Umlaufzeit des Mondes, beträgt e
mit seinen 365,2422 Tagen bestel

365,2422 : 29

solchen Zykeln. Die Kettenbruch

[12, 2, 1, 2

mit Konvergenten

$$12,\quad 12\frac{1}{3},\quad 12\frac{3}{8},\quad 12\frac{4}{11},$$

Für einen Kalender, der sowohl m
synchronisiert ist, könnte man als
binieren, wobei in erster Näheru
Tatsächlich war man im fünften
heblich weiter: Der um 440 v.Ch

Astronomen METON verwendete die Konvergente mit Nenner 19. Ein Metonischer Zyklus besteht besteht demnach aus 19 Jahren, darunter zwölf *Gemeinjahren* aus zwölf Monaten und sieben *Schaltjahren* aus 13 Monaten. Die Monate hatten teils 29, teils 30 Tage. Der darauf basierende Kalender wurde in Griechenland bis 46 v.Chr. verwendet. Die Synchronisation zwischen Sonnen- und Mondzykeln ist fast perfekt:

$$19 \cdot 365{,}2422 = 6939{,}6018 \quad \text{und} \quad 235 \cdot 29{,}5306 = 6939{,}691\,,$$

der Fehler pro Zyklus liegt also bei nur etwa zwei Stunden. Seit Einführung des Gregorianischen Kalenders sind etwas über 22 Metonische Zykeln vergangen; der akkumulierte Fehler liegt also noch unter zwei Tagen.

Der Gregorianische Kalender geht deshalb bei der Bestimmung des Osterdatums nicht von astronomischen Beobachtungen aus, sondern von Metonischen Zykeln, allerdings mit einer Korrektur für den akkumulierten Fehler. Ebenfalls unberücksichtigt bleiben die Irregularitäten der realen Mondbewegung; gerechnet wird mit einer Approximation der *mittleren* Mondbewegung. Auf den ersten Blick seltsam erscheinen mag auch die Tatsache, daß bei der Fehlerkorrektur mit der *Julianischen* Jahreslänge von $365\frac{1}{4}$ Tagen gerechnet wird; der Grund lag wohl vor allem darin, daß Papst Gregor bisherige Praktiken nicht mehr als unbedingt notwendig ändern wollte.

Die wesentliche Größe, mit der die Mondphasen in unseren an der Sonne orientierten Kalender gebracht werden, ist der sogenannte *Epakt*. Mit diesem Wort bezeichneten die Griechen die Anzahl der Tage, die an Neujahr seit dem letzten Neumond des alten Jahres vergangen waren. Gemäß dem Metonischen Zyklus sollte diese Zahl sich alle 19 Jahre wiederholen; in der Kalenderrechnung wird daher die um eins vermehrte Restklasse modulo 19 der Jahreszahl als die „Goldene Zahl" bezeichnet. (Die Addition der Eins kommt natürlich daher, daß zur Zeit ihrer Einführung die Null in der europäischen Mathematik noch nicht vorkam.)

Wenn jedes Jahr genau 365 Tage hätte, könnten wir einfach mit den $12 \times 29{,}5 = 354$ Tagen eines Mondjahrs vergleichen und wüßten dann,

daß sich die Mondphase an einen
verschiebt. Als *Mondphase* bezeic
die seit dem letzten Neumond ver

Eine der vielen Vereinfachunger
liegt darin, daß man innerhalb d
wesentlichen von dieser Formel a

Da die Schalttage Ende Februar e
Vollmond am oder nach dem 21
mit dem klassischen Epakt, der M
gäbe es schließlich algorithmisch
für die Schaltjahre. Aus Effizienz
einem *verschobenen* Epakt zu re
geeigneten Datums, das näher be

Die Länge eines lunaren Zyklus
einfacheren Rechnen sollten wir
in den Ostern fällt, auf den gan
Vollmond nach dem 21. März is
19. April, und sein Abstand zum
als Tag mit Mondphase 14 betrac
Neumonds vor dem 5. April zu
5. Aprils. Somit bietet sich an, al
des 5. Aprils zu nehmen. Gemäß
sollte auch sie sich alle 19 Jahre
innerhalb eines Metonischen Zyk
verschieben.

Damit brauchen wir nur noch f
den tatsächlichen Wert der Mond
den verschobenen Epakt allgeme
Gregorianischen Reform gebräu
Jahr J als

$$E = \big(14 + 11 \cdot ($$

Der erste Vollmond am oder nach
dem 19. April, und Ostern war d

wird Ostern noch heute in fast allen orthodoxen Kirchen berechnet; die einzige Ausnahme ist die finnische.

Der Gregorianische Kalender modifiziert diese Formel durch drei zusätzliche Terme: Zunächst berücksichtigt er, daß der Metonische Zyklus nicht wirklich exakt ist, insbesondere dann nicht, wenn man mit dem Julianischen Jahr arbeitet:

$$19 \cdot 365{,}25 = 6939{,}750 \quad \text{und} \quad 235 \cdot 29{,}5306 = 6939{,}691\,;$$

hier beträgt die Differenz also 0,059 Tage pro Zyklus und

$$0{,}059 \times \frac{100}{19} \approx 0{,}31$$

Tage pro Jahrhundert. Die Gregorianische Osterformel approximiert dies durch $8/25 = 0{,}32$, addiert allerdings im h-ten Jahrhundert nicht $[8h/25]$, sondern $\big[(5+8h)/25\big]$. Diese Modifikation soll in erster Linie dafür sorgen, daß Ostern möglichst selten mit dem jüdischen Paschafest zusammenfällt. Für das Jahrhundert wird dabei die gleiche Konvention benutzt wie für die Feier des Jahrtausendanfangs am 1. Januar 2000: Das h-te Jahrhundert beginnt mit dem Jahr $100(h-1)$, d.h. $h = [J/100]+1$.

Da der Gregorianische Kalender bei der Korrektur der Metonischen Zyklen mit Julianischen Jahren arbeitet, am Ende aber ein Gregorianisches Datum braucht, müssen als nächstes die unterschiedlichen Anzahlen von Schalttagen berücksichtigt werden, d.h. die „ausfallenden“ Schalttage des Gregorianischen Kalenders müssen subtrahiert werden. Das sind drei Stück pro 400 Jahre, also wird $[3h/4]$ subtrahiert. Dies ergäbe die neue Formel

$$E = \left(14 + 11 \cdot (J \bmod 19) + \left[\frac{5+8h}{25}\right] - \left[\frac{3h}{4}\right]\right) \bmod 30\,.$$

Tatsächlich gibt es noch eine weitere Modifikation, die dafür sorgen soll, daß die 19 Epakte eines Metonischen Zyklus alle verschieden sind und $E = 0$ nicht auftritt: Falls $E = 0$ ist oder falls $E = 1$ ist und $J \bmod 19 > 10$, wird E um eins erhöht. Der (berechnete) Vollmond ist dann E Tage vor dem 19. April, und Ostern wird weiterhin am darauf folgenden Sonntag gefeiert.

Das Jahr $J = 2014$ liegt im $h = 2$
Somit ist

$$E = \left(14 + 11 \cdot 0 + \left[\frac{1}{}\right.\right.$$

Der rechnerische Vollmond ist da
erst am 15. April um 9 Uhr 42.)
20. April 2014, also wird dann O

§5: Eine kryptographische

Beim RSA-Verfahren wählt ma
ziemlich klein, z.B. $e = 3$ oder
daß zumindest die Verschlüsselu
zur Entschlüsselung mit einem E
Moduls arbeiten muß.

Für jemanden, der RSA hauptsäc
verwendet, würde sich anbieten,
relativ klein zu wählen. Dann kö
terschreiben, und falls jeder Emp
dessen höherer Aufwand bei der Ü

Natürlich kann man nicht $d = 3$
Exponent muß schließlich gehein
ihn durch Probieren zu erraten.

Andererseits geht man heute bei s
aus, daß ein Verfahren sicher ist,
lichkeiten durchprobieren muß, s
einer Schlüssellänge von 128 B
scheinen 2048 Bit für einen priva
hoch.

Trotzdem läßt sich hier nicht wes
kurze private Exponenten nicht
sondern auch wesentlich schnelle

Wir gehen aus von einem öffentlichen RSA-Schlüssel (N, e) sowie dem zugehörigen privaten Exponenten d. Dann gibt es bekanntlich eine natürliche Zahl k, so daß $ed - k\varphi(N) = 1$ ist. Dies können wir umschreiben als

$$\frac{e}{\varphi(N)} - \frac{k}{d} = \frac{1}{d\varphi(N)} .$$

Falls d sehr viel kleiner ist als $\varphi(N)$ haben wir hier einen Bruch mit dem großen Nenner $\varphi(N)$ sehr gut angenähert durch einen Bruch mit dem sehr viel kleineren Nenner d. Für hinreichend kleines d ist das nur möglich, wenn k/d eine Konvergente der Kettenbruchentwicklung von $e/\varphi(N)$ ist.

Das mag zunächst harmlos erscheinen, denn die Sicherheit von RSA beruht ja gerade darauf, daß niemand außer dem Inhaber des privaten Schlüssels d die Faktorisierung $N = pq$ und damit den Wert von

$$\varphi(N) = (p-1)(q-1) = N - (p+q) + 1$$

kennt. Dafür kennt aber jeder den Wert von N, und wie die obige Gleichung zeigt, liegt der recht nahe bei $\varphi(N)$: Die Primzahlen p und q sind schließlich nur von der Größenordnung $\sqrt{N}$. Damit sollte k/d auch eine gute Approximation für e/N liefern.

In der Tat zeigte Kryptologe MICHAEL JAMES WIENER 1990 ein Resultat, wonach insbesondere der folgende Satz gilt:

Satz: Ist $N = pq$ Produkt zweier Primzahlen p und q mit $p < q < 2q$, und ist $d < \frac{1}{3}\sqrt[4]{N}$ der private Exponent zum öffentlichen Exponenten $e < \varphi(N)$, so ist d Nenner einer Konvergenten der Kettenbruchentwicklung von e/N.

Beweis: Wegen $ed \equiv 1 \bmod \varphi(N)$ gibt es ein $k \in \mathbb{N}$; so daß $ed - k\varphi(N) = 1$ ist; wegen $e < \varphi(N)$ ist dabei $k < d$. Nach dem Satz von LEGENDRE aus §3 reicht es, wenn wir zeigen können, daß

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

ist, denn dann ist k/d eine Kon
von e/N.

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed - kN}{dN}\right|$$
$$= \left|\frac{(ed - k\varphi($$
$$= \left|\frac{1 + k(\varphi(N$$
$$= \left|\frac{1 + k(1 -$$
$$< \frac{k(p+q)}{dN} .$$

Natürlich ist $p < \sqrt{N}$, und we
$p + q < 3\sqrt{N}$. Außerdem ist $k <$

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{3k\sqrt{N}}{dN} =$$

Dies ist genau dann kleiner als 1
raussetzung ist aber d sogar klein
wäre.

Um d zu berechnen, müssen wir d
bestimmen, bis für einen der N
modulo N invers ist zu der mit
praktisch immer bereits beim erst

Tatsächlich gibt es Algorithmen
nenten $d < N^{0,289}$ rekonstruieren
daß man vielleicht sogar in viele
Algorithmen eine realistische Er
Attacken arbeitet man allerdings
anderen Verfahren zur diophantis

Private Exponenten müssen somit immer groß sein. Falls man von einem vorgegebenen öffentlichen Exponenten ausgeht, ist das für realistische N mit an Sicherheit grenzender Wahrscheinlichkeit erfüllt; Vorsicht ist nur geboten, wenn man mit dem privaten Exponenten startet. Daher verlangen auch die Vorschriften der Bundesnetzagentur, daß man immer vom öffentlichen Exponenten e ausgehen muß, und erst daraus einen privaten Exponenten berechnet.

§6: Die Kettenbruchentwicklung der Eulerschen Zahl

Aufgabe 1*b)* des neunten Übungsblatts läßt eine erstaunliche Regelmäßigkeit in der Kettenbruchentwicklung von e vermuten:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1 \cdots] .$$

Diese Entwicklung ist bereits im 18. Kapitel der 1748 erschienenen *Introductio in analysin infinitorium* von EULER enthalten; HERMITE bewies sie 1873 im Rahmen seiner Arbeit über die Transzendenz von e mit anderen Methoden die zusammenhängen mit der Approximation der Exponentialfunktion durch rationale Funktionen. Sein Schüler PADÉ entwickelte später eine systematische Theorie solcher Approximationen, die PADÉ-Approximanten, die in der Numerik eine große Rolle spielen für die näherungsweise Berechnung von Standardfunktionen. Durch Kombination solcher Ideen kamen verschiedene Mathematiker zu immer einfacheren Beweisen; der hier wiedergegebene Beweis von HENRY COHN erschien 2006 im *American Mathematical Monthly;* direkt dahinter folgt eine Arbeit von THOMAS J. OSLER, der den Beweis so verallgemeinert, daß er auch die Kettenbruchentwicklungen der Wurzeln aus e liefert.

Wir können die obige Kettenbruchentwicklung noch etwas regelmäßiger schreiben, indem wir beachten, daß für alle $x \in \mathbb{R}$ gilt

$$1 + \frac{1}{0 + \dfrac{1}{1 + x}} = 1 + (1 + x) = 2 + x \, ;$$

der obige Kettenbruch kann also auch geschrieben werden als

$$[1, 0, 1, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \ldots] .$$

Hier läßt sich der n-te Koeffizie
drücken: Für $n = 3k + 1$ mit $k \in$

Für die Kettenbruchentwicklung
daran nur wenig ändern: Hier wo

$$c_{3k} = c_{3k+2} = 1 \quad \text{und}$$

ist für alle $k \in \mathbb{N}_0$, d.h.

$$\sqrt[M]{e} = [1, M - 1, 1, 1, 3M - 1$$

Wir gehen aus von diesem Ket
gegen $\sqrt[M]{e}$ konvergiert. Nach d
der Zähler p_n und der Nenner q_n
bruchs $[c_0, c_1, c_2, \ldots]$ rekursiv be

$$p_0 = c_0, q_0 = 1, p$$

$$p_n = p_{n-2} + c_n p_{n-1} \quad \text{und}$$

Speziell für die hier betrachtete K
die Anfangsterme $p_0 = q_0 = p_1 =$
bedeutet, daß die erste Konverge
bruchentwicklung von e also, ni
obiger Rekursionsformel; da die
wir je nach Restklasse von n drei

$$\begin{aligned} p_{3k} &= p_{3k-2} + p_{3k-1} \\ p_{3k+1} &= p_{3k-1} + \big((2k+1) - 1\big) M p \\ p_{3k+2} &= p_{3k} + p_{3k+1} \end{aligned}$$

Wir müssen zeigen, daß die Fol
konvergiert.

Der Trick dazu hängt mit PADÉ-A
darauf nicht eingehen, sondern o
grale

$$A_k = \int_0^1 \frac{x^k (x-1)^k}{k! M^{k+1}} e^{x/M} \, dx$$

$$\text{und} \qquad C_k = \int_0^1 \frac{x^k(x-1)^{k+1}}{k!M^{k+1}} e^{x/M}\,dx$$

betrachten.

Satz: Für alle $k \in \mathbb{N}_0$ gilt:

$$p_{3k} - q_{3k}\sqrt[M]{e} = -A_k$$
$$p_{3k+1} - q_{3k+1}\sqrt[M]{e} = B_k$$
$$p_{3k+2} - q_{3k+2}\sqrt[M]{e} = C_k$$

Da in allen drei Integranden der Zähler kleiner als eins und die Exponentialfunktion höchstens $\sqrt[M]{e}$ ist, während der Nenner für $k \to \infty$ gegen ∞ geht, ist

$$\lim_{k\to\infty} A_k = \lim_{k\to\infty} B_k = \lim_{k\to\infty} C_k = 0\,;$$

daher folgt aus diesem Satz sofort

Korollar: $\lim\limits_{n\to\infty} \dfrac{p_n}{q_n} = \sqrt[M]{e}$, d.h.

$$\sqrt[M]{e} = [1, M-1, 1, 1, 3M-1, 1, 1, 5M-1, 1, 1, 7M-1, 1, \dots].$$

Insbesondere ist $e = [1, 0, 1, 1, 2, 1, 1, 4, 1, \dots] = [2, 1, 2, 1, 1, 4, 1, \dots]$.

■

Der obige Satz wird durch Induktion bewiesen. Für $k = 0$ ist

$$A_0 = \int_0^1 \frac{1}{M} e^{x/M}\,dx = e^{x/M}\Big|_0^1 = \sqrt[M]{e} - 1$$

$$B_0 = \int_0^1 \frac{x}{M} e^{x/M}\,dx = (x-M)e^{x/M}\Big|_0^1 = (1-M)\sqrt[M]{e} + M$$

$$C_0 = \int_0^1 \frac{x-1}{M} e^{x/M}\,dx = (x-1-M)e^{x/M}\Big|_0^1 = -M\sqrt[M]{e} + M + 1$$

Nach den eingangs angegebenen
ist

$$p_0 = q_0 = 1, \quad p_1 = M, \quad q_1 = M$$

Die drei Formeln aus dem Satz we

$$1 - \sqrt[M]{}$$
$$M - (M-1)\sqrt[M]{}$$
$$1 + M - M\sqrt[M]{}$$

die offensichtlich alle drei richtig

Für den Induktionsschritt brauch
tegralen A_k, B_k und C_k. Hier gil

a) $A_k = -B_{k-1} - C_{k-1}$
b) $B_k = -\big((2k+1)M - 1\big)A_k$
c) $C_k = B_k - A_k$

Zum *Beweis* von *a)* wenden wir
Produkts an auf das Produkt der
Für ein solches Dreierprodukt ist

$$\frac{d}{dx}x^k(x$$

$$= kx^{k-1}(x-1)^k e^{x/M} + kx^k($$

Division durch $k!M^k$ macht dara

$$\frac{d}{dx}\frac{x^k(x}{k}$$

$$= \frac{x^{k-1}(x-1)^k e^{x/M}}{(k-1)!M^k} + \frac{x^k(x}{(k-}$$

Integrieren wir beide Seiten von
Seite den Wert null, da die Stam
Intervallenden verschwindet. Re
grale C_{k-1}, B_{k-1} und A_k; somi
beweist.

Der Beweis von *b)* geht ähnlich: Wir berechnen zunächst die Ableitung von $x^k(x-1)^{k+1}e^{x/M}$ und dividieren wieder durch $k!M^k$; wir erhalten

$$\begin{aligned}
&\frac{d}{dx}\frac{x^k(x-1)^{k+1}}{k!M^k}e^{x/M}\\
&= \frac{x^{k-1}(x-1)^{k+1}}{(k-1)!M^k}e^{x/M} + \frac{(k+1)x^k(x-1)^k}{k!M^k}e^{x/M} + \frac{x^k(x-1)^{k+1}}{k!M^{k+1}}e^{x/M}\\
&= \frac{kMx^{k-1}(x-1)^{k+1} + M(k+1)x^k(x-1)^k + x^k(x-1)^{k+1}}{k!M^{k+1}}e^{x/M}\\
&= \frac{x^{k-1}(x-1)^k\big(kM(x-1) + (k+1)Mx + x(x-1)\big)}{k!M^{k+1}}e^{x/M}\\
&= \frac{x^{k-1}(x-1)^k\Big(\big((2k+1)M-1\big)x - kM + x^2\Big)}{k!M^{k+1}}e^{x/M}\\
&= \big((2k+1)M-1\big)\frac{x^k(x-1)^k}{k!M^{k+1}}e^{x/M} - \frac{x^{k-1}(x-1)^k}{(k-1)!M^k}e^{x/M}\\
&\qquad + \frac{x^{k+1}(x-1)^k}{k!M^{k+1}}e^{x/M}\,.
\end{aligned}$$

Wenn wir die linke Seite dieser Gleichung von 0 bis 1 integrieren, erhalten wir wieder den Wert null, bei der rechten erhalten wir

$$\big((2k+1)M-1\big)A_{k-1} - B_k + C_{k-1}\,.$$

Auflösen nach B_k zeigt die Behauptung *b)*

Zum Beweis von *c)* schließlich gehen wir aus von der Gleichung $(x-1)^2 = x(x-1) - (x-1)$ und multiplizieren diese mit

$$\frac{x^k(x-1)^{k-1}}{k!M^{k+1}}e^{x/M}\,.$$

Integration von 0 bis 1 führt auf die Gleichung $C_k = B_k - A_k$.

Damit sind alle drei Relationen bewiesen, und wir können mit dem Induktionsschritt zum Beweis unseres zentralen Satzes beginnen. Sei also $k \geq 1$; wir nehmen an, daß die drei Gleichungen für $k-1$ gelten.

Als erstes wollen wir zeigen, daß

$$p_{3k} - q_{3k}\sqrt[M]{e} = -A_k$$

ist. Nach den Rekursionsformeln ten ist

$$p_{3k} = p_{3k-2} + p_{3k-1}$$

also ist

$$\begin{aligned}
p_{3k} - q_{3k}\sqrt[M]{e} &= \big(p_{3k-2} - q\\
&= B_{k-1} + C_k
\end{aligned}$$

nach Induktionsannahme und der

Genauso können wir auch bei de hen:

$$\begin{aligned}
p_{3k+1} - q_{3k+1}\sqrt[M]{e} &= \big(p_{3k-1}\\
&\quad + \big(\\
&= C_{k-1}
\end{aligned}$$

und

$$\begin{aligned}
p_{3k+2} - q_{3k+2}\sqrt[M]{e} &= \big(p_{3k}\\
&= -A_k
\end{aligned}$$

Somit gelten alle drei Beziehunge beweist den Satz sowie die Kette Wurzeln.

Wer sich genauer dafür interes hingeschriebenen Integrale A_k, B deten Originalarbeiten (und even konsultieren:

HENRY COHN: A Short Proof of t sion of e, *American Mathematica*

und

THOMAS J. OSLER: A Proof o of $e^{1/M}$, *American Mathematical*

Das *American Mathematical M Mathematical Association of Ame*

Kapitel 6
Quadratische Zahlkörper

Ein Zahlkörper ist ein Körper K, der den Körper $\mathbb{Q}$ der rationalen Zahlen enthält und als $\mathbb{Q}$-Vektorraum endlichdimensional ist. Im zweidimensionalen Fall reden wir von quadratischen Zahlkörpern. Die algebraische Zahlentheorie untersucht die (noch zu definierenden) ganzen Zahlen eines solchen Zahlkörpers. In dieser Vorlesung geht es zwar eher um elementare als um algebraische Zahlentheorie, jedoch werden wir im nächsten Kapitel sehen, daß ein Umweg über quadratische Zahlkörper auch bei rein ganzzahligen Problemen gelegentlich hilfreich sein kann.

§ 1: Grundbegriffe der Ringtheorie

Als erstes wollen wir uns überlegen, in welchen Zahlbereichen außer $\mathbb{Z}$ wir noch sinnvoll von Teilbarkeit und eventuell auch Division mit Rest reden können. Wir brauchen dazu selbstverständlich zumindest eine Addition und eine Multiplikation, d.h. einen der bereits in Kapitel 1, §6 definierten *Ringe.* Wenn wir eindeutige Quotienten wollen, müssen wir aber noch zusätzlich voraussetzen, daß es keine sogenannte *Nullteiler* gibt, d.h. von null verschiedene Elemente r, s, deren Produkt gleich null ist. Ist nämlich $y = qs$, so ist dann auch $y = (q + r)s$, was unserer Vorstellung von Teilbarkeit mit eindeutig bestimmtem Quotienten widerspricht.

Definition: *a)* Ein Ring heißt *nullteilerfrei* wenn gilt: Ist $x \cdot y = 0$, so muß mindestens einer der beiden Faktoren x, y verschwinden. Ein nullteilerfreier kommutativer Ring heißt *Integritätsbereich* (englisch *domain*).

b) Wir sagen, ein Element u eine
$x \in R$, in Zeichen $u|x$, wenn es e
c) $u \in R$ heißt *größter gemeinsa*
von x und von y ist und wenn fü
von x und y gilt: $v|u$.
d) Ein Element $e \in R$ heißt *Einhe*
Die Menge aller Einheiten von R
e) Zwei Elemente $x, y \in R$ hei
$e \in R$ gibt, so daß $y = e \cdot x$.

Der Prototyp eines kommutative
Zahlen; er ist ein Integritätsbereic
ganze Zahlen sind somit genau
Betrag haben. Man beachte, daß i
+2 als auch -2 ein größter gem
ggT ist also nicht eindeutig besti

Der Ring $\mathbb{Z}/m$ ist genau dann nul
Fall ist er sogar ein Körper. Ist abe
in ein Produkt mit $a, b > 1$, so ist

Die Menge aller $n \times n$-Matrizen
einen der hier ausgeschlossenen
nullteilerfrei, enthält aber viele E

Auch die Polynome über einem K
nomring $k[X]$. Auch er ist ein In

Lemma: Ist R ein Integritätsber

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X \right.$$

Seine Einheiten sind genau die E

Beweis: Wenn wir Addition un
Regeln definieren, ist klar, daß R

zeigen, daß $R[X]$ nullteilerfrei ist, betrachten wir zwei Polynome

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{und} \quad g = \sum_{j=0}^{m} b_j X^j ,$$

die beide von Null verschieden sind. Wir können etwa annehmen, daß n und m so gewählt sind, daß a_n und b_m beide nicht verschwinden. Da R Integritätsbereich ist, kann dann auch das Produkt $a_n b_m$ nicht verschwinden, also ist der führende Term $a_n b_m X^{n+m}$ von fg von Null verschieden und damit auch fg selbst. Tatsächlich beweist dies sogar etwas mehr als die Nullteilerfreiheit, denn wir wissen nun, daß sich bei der Multiplikation zweier Polynome die Grade addieren.

Ist $f \in R[X]$ eine Einheit, so gibt es ein $g \in R[X]$ mit $fg = 1$; da das konstante Polynom 1 den Grad null hat, muß dasselbe auch für f und g gelten, d.h. $f, g \in R$ und damit in $R^\times$. ∎

Für jeden Ring R gilt

Lemma: *a)* Die Menge $R^\times$ aller Einheiten von R ist eine abelsche Gruppe bezüglich der Multiplikation.
b) Ein kommutativer Ring R ist genau dann ein Integritätsbereich, wenn die folgende *Kürzungsregel* erfüllt ist: Gilt für $x, y, z \in R$ und $z \neq 0$ die Gleichung $xz = yz$, so ist $x = y$.
c) Zwei Elemente x, y eines Integritätsbereich R sind genau dann assoziiert, wenn $x|y$ und $y|x$.
d) Ein größter gemeinsamer Teiler, so er existiert, ist bis auf Assoziiertheit eindeutig bestimmt.

Beweis: a) Sind $e, f \in R$ Einheiten, so gibt es Elemente e', f' mit $ee' = ff' = 1$. Damit ist $(ef)(f'e') = e(ff')e' = ee' = 1$, d.h. auch ef ist eine Einheit. Außerdem ist jede Einheit invertierbar, denn offensichtlich ist e' ein multiplikatives Inverses zu e.
b) Ist R ein Integritätsbereich und $xz = yz$, so ist $(x - y)z = 0$; da $z \neq 0$ vorausgesetzt war, folgt $x - y = 0$, also $x = y$. Folgt umgekehrt aus $xz = yz$ und $z \neq 0$ stets $x = y$, so ist R nullteilerfrei, denn ist $xy = 0$ und $y \neq 0$, so ist $xy = 0y$, also $x = 0$.
c) Ist $y = ex$, so ist x ein Teiler von y. Da Einheiten invertierbar sind, ist auch $x = e^{-1}y$, d.h. $y|x$.

Gilt umgekehrt $x|y$ und $y|x$, so g
$y = q'x$. Damit ist $1x = x = ($
Einheit.
d) Sind u, v zwei größte gemeins
nition u Teiler von v und v Teiler

Manchmal haben wir sogar eine e
Sinn:

Definition: *a)* Ein Element x ei
zibel, falls gilt: x ist keine Einhe
Elemente aus R, so muß y oder z
b) Ein Integritätsbereich R heißt *fa*
des Element $x \in R$ läßt sich bis a
deutig schreiben als Produkt $x =$
irreduziblen Elementen $p_i \in R$ u
(*ZPE* steht für *Z*erlegung in *P*rim

Lemma: In einem faktoriellen F
einen größten gemeinsamen Teile

Beweis: Wir wählen zunächst au
ler Elemente einen Vertreter; für
Produkt irreduzibler Elemente re
Elemente betrachten, die Vertrete

Sind $x = u \prod_{i=1}^{r} p_i^{e_i}$ und $y = v$
irreduzibel die entsprechenden Z
toren, so können wir, indem wir n
o.B.d.A. annehmen, daß $r = s$ ist
$\prod_{i=1}^{r} p_i^{\min(e_i, f_i)}$ ein ggT von x un
Teiler von x, wenn $g_i \leq e_i$ für all

§2: Die Elemente quadrat

Ein quadratischer Zahlkörper ist
betrachtet die Dimension zwei ha

unabhängiges Element α. Die drei Elemente $1, \alpha, \alpha^2$ müssen aber linear abhängig sein; es gibt also rationale Zahlen p, q, r, so daß $p\alpha^2+q\alpha+r$ verschwindet. Indem wir mit dem Hauptnenner von p, q, r multiplizieren, erhalten wir eine entsprechende Gleichung mit ganzzahligen Koeffizienten, und wenn wir dann noch durch deren ggT dividieren, erhalten wir teilerfremde ganze Zahlen A, B, C, so daß $A\alpha^2 + B\alpha + C = 0$ ist.

Nach der Lösungsformel für quadratische Gleichungen folgt

$$\alpha = -\frac{B}{2A} \pm \frac{\sqrt{B^2 - 4AC}}{2A} .$$

Den Ausdruck $\Delta = B^2 - 4AC$ unter der Wurzel bezeichnen wir als die *Diskriminante* von α. Für $\alpha = \sqrt{W}$ mit $W \in \mathbb{Z}$ beispielsweise ist $A = 1, B = 0$ und $C = -W$, also $\Delta = 4W$. Für $\alpha = \frac{1}{3} + \frac{1}{5}\sqrt{2}$ haben wir die Gleichung

$$\alpha^2 - \frac{2}{3}\alpha + \frac{1}{9} - \frac{2}{25} = \alpha^2 - \frac{2}{3}\alpha + \frac{7}{225} = 0 \Longrightarrow 225\alpha^2 - 150\alpha + 7 = 0 ;$$

hier ist die Diskriminante somit $\Delta = 150^2 - 4 \cdot 225 \cdot 7 = 16200$.

Wegen der Irrationalität von α muß auch $\sqrt{\Delta}$ irrational sein, d.h. Δ ist kein Quadrat. Wegen der Eindeutigkeit der Primzerlegung in $\mathbb{Z}$ können wir ganze Zahlen $Q, D \in \mathbb{Z}$ finden, so daß $\Delta = Q^2 D$ und $\sqrt{\Delta} = Q\sqrt{D}$ ist mit einer quadratfreien Zahl D, d.h. einer Zahl D, die durch keine Quadratzahl ungleich eins teilbar ist. Somit läßt sich α in der Form $r + s\sqrt{D}$ schreiben mit $r, s \in \mathbb{Q}$. Da K als $\mathbb{Q}$-Vektorraum zweidimensional ist, läßt sich jedes Element von K so schreiben, als Vektorraum ist also $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$.

Umgekehrt ist $\mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$ für jedes Nichtquadrat D ein Körper, denn natürlich liegen Summe und Differenz zweier Elemente wieder in diesem Vektorraum und wegen

$$(r + s\sqrt{D})(u + v\sqrt{D}) = (ru + svD) + (rv + su)\sqrt{D}$$

auch das Produkt. Für den Quotienten können wir wie bei den komplexen Zahlen über die dritte binomische Formel argumentieren:

$$\frac{r + s\sqrt{D}}{u + v\sqrt{D}} = \frac{(r + s\sqrt{D})(u - v\sqrt{D})}{(u + v\sqrt{D})(u - v\sqrt{D})} = \frac{ru - svD}{u^2 - v^2 D} + \frac{su - rv}{u^2 - v^2 D} .$$

Wir bezeichnen diesen Körper ku

Für $D > 0$ ist $\mathbb{Q}[\sqrt{D}]$ ein Teilkör
einem *reellquadratischen* Zahlkö
auch imaginäre Elemente; hier re
schen Zahlkörper.

§3: Die Hauptordnung ein

Jede rationale Zahl ist Lösung ein
ganzzahligen Koeffizienten a, b, v
darf; sie ist genau dann eine ganz

Entsprechend ist jedes Element
Polynomgleichung

$$a_n X^n + a_{n-1} X^{n-1} + \dots$$

denn da K nach Definition ein en
können die Potenzen von x nich
gibt also für irgendein n eine line

$$\lambda_n x^n + \lambda_{n-1} x^{n-1} + \dots$$

Multiplikation mit dem Hauptner
eine Polynomgleichung mit ganz

Definition: Ein Element x eines
einer Polynomgleichung

$$x^n + a_{n-1} x^{n-1}$$

mit ganzzahligen Koeffizienten $a_$
genügt.

Man kann relativ einfach zeige
Zahlkörper K einen Ring bilde
sche Zahlkörper beschränken, be
können, sei hier auf einen solche

Wir betrachten also einen quadratischen Zahlkörper $K = \mathbb{Q}[\sqrt{D}]$. Ein Element $\alpha = r + s\sqrt{D}$ mit $r, s \in \mathbb{Q}$ ist genau dann ganz, wenn es einer Gleichung der Form $x^2 + ax + b = 0$ genügt mit $a, b \in \mathbb{Z}$. Da

$$x^2 = (r + s\sqrt{D})^2 = (r^2 + s^2 D) + 2rs\sqrt{D}$$

ist, genügt x der Gleichung

$$x^2 - 2rx + (r^2 - s^2 D) = 0\,.$$

Somit müssen $c = 2r$ und $d = r^2 - s^2 D$ ganze Zahlen sein.

Für $r \in \mathbb{Z}$ ist die erste Bedingung trivialerweise erfüllt und die zweite genau dann, wenn auch s eine ganze Zahl ist: Da D keinen Nenner hat, ist der Nenner von $r^2 - s^2 D$ in diesem Fall das Quadrat des Nenners von s.

Falls r keine ganze Zahl ist, muß es wegen der ersten Bedingung von der Form $r = c/2$ sein mit einer ungeraden Zahl c. Notwendige Bedingung für die Ganzheit von $r^2 - s^2 D$ ist dann, daß auch $s = e/2$ von dieser Form ist. Dann ist

$$r^2 - s^2 D = \frac{c^2 - e^2 D}{4} \in \mathbb{Z} \Longrightarrow c^2 - e^2 D \equiv 0 \bmod 4\,.$$

c und e sind ungerade Zahlen; ihre Quadrate sind also kongruent eins modulo vier. Somit ist $r^2 - s^2 D$ genau dann ganz, wenn $D \equiv 1 \bmod 4$ ist.

In $\mathbb{Q}[\sqrt{D}]$ ist ein Element $r + s\sqrt{D}$ daher für $D \not\equiv 1 \bmod 4$ genau dann ganz, wenn r und s beide ganz sind; die Menge der ganzen Zahlen ist also $\mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$. Diese Menge ist offensichtlich eine abelsche Gruppe bezüglich der Addition, und da das Quadrat von $\sqrt{D}$ die ganze Zahl D ist, ist sie auch abgeschlossen bezüglich der Multiplikation; die ganzen Zahlen bilden also einen Ring.

Im Fall $D \equiv 1 \bmod 4$ ist $r + s\sqrt{D}$ auch ganz, wenn r und s beide jeweils die Hälfte einer ungeraden Zahl sind. Insbesondere ist also auch

$$\beta_D = \frac{1 + \sqrt{D}}{2}$$

eine ganze Zahl, und offensichtl
Zahlen, die sich als $u + v\beta_D$ mit
der ganzen Zahlen ist also $\mathbb{Z} \oplus \mathbb{Z}$

$$\beta_D^2 = \frac{1 + 2\sqrt{D} + D}{4} = \frac{D}{}$$

liegt wieder in dieser Menge, da
ganze Zahl ist.

Die ganzen Zahlen in $\mathbb{Q}[\sqrt{D}]$ b
diesen Ring bezeichnen wir als di
Wie wir gerade gesehen haben, is

$$\mathcal{O}_D = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}\sqrt{D} \\ \mathbb{Z} \oplus \mathbb{Z}\beta_D \quad \text{mit} \quad \beta_D = \end{cases}$$

Beim Körper $K = \mathbb{Q}[i]$ der komp
Imaginärteil ist $D = -1 \equiv 3$ m
einfach $\mathcal{O}_{-1} = \mathbb{Z} \oplus \mathbb{Z}i$, die soge
Für $D = -3 \equiv 1 \bmod 4$ dagegen
Zahl und $\mathcal{O}_{-3} = \mathbb{Z} \oplus \mathbb{Z}\beta_{-3}$.

Dieses Beispiel wirft die Frage au
wirklich so geschickt war: Wir hät
können, daß $r + s\sqrt{D}$ genau dann
Zahlen sind.

Einer der Gründe ist sicherlich,
körpern keine ausgezeichneten
im quadratischen Fall ist $\sqrt{D}$ ni
Element. Im Falle $D = -3$ beisp
primitive sechste Einheitswurzel
„weniger ganz“ oder „weniger au

Viel wichtiger ist aber, daß wir
eine Chance auf eindeutige Primz

Definition: *a)* Sind $R \leq S$ Inte
$x \in S$ ganz über R, wenn es eine

$$x^n + r_{n-1}x^{n-1} + \cdots +$$

genügt.
b) R heißt ganzabgeschlossen oder normal, wenn jedes über R ganze Element des Quotientenkörpers K von R in R liegt.

Satz: Ein faktorieller Ring ist ganzabgeschlossen.

Beweis: Jedes Element x des Quotientenkörpers eines Rings R kann als Quotient $x = p/q$ mit $p, q \in R$ dargestellt werden. Falls R faktoriell ist, können wir dabei annehmen, daß p und q teilerfremd sind. x ist genau dann ganz über R, wenn es ein $n \in \mathbb{N}$ und Elemente $r_0, \ldots, r_{n-1} \in R$ gibt derart, daß

$$x^n = -r_{n-1}x^{n-1} - \cdots - r_1 x - r_0$$

ist. Multiplikation mit q^n macht daraus die Gleichung

$$p^n = -r_{n-1}p^{n-1}q - \cdots - r_1 pq^{n-1} - r_o q^n \,.$$

Hier ist die rechte Seite durch q teilbar, also auch die linke. Da p und q als teilerfremd vorausgesetzt war, ist das nur möglich, wenn q eine Einheit ist, d.h. $x = p/q$ liegt in R. ∎

§4: Normen und Spuren in quadratischen Zahlkörpern

Beginnen wir mit einem Beispiel: Die Hauptordnung von $K = \mathbb{Q}[\sqrt{-5}]$ ist $\mathcal{O}_{-5} = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{-5}]$, und dort haben wir die beiden Produktzerlegungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) \,.$$

Folgt daraus, daß $\mathcal{O}_{-5}$ nicht faktoriell ist?

Bevor wir diese Frage beantworten können, müssen wir zunächst wissen, ob möglicherweise die Faktoren auf der rechten Seite noch weiter zerlegt werden können. Solche Fragen lassen sich oft entscheiden, indem man die *Normen* der beteiligten Elemente betrachtet.

Definition: *a)* Für ein Elements $\alpha = r + s\sqrt{D}$ von $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$ heißt $\overline{\alpha} = r - s\sqrt{D}$ das zu α konjugierte Element.
b) Die Norm von α ist

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = (r + s\sqrt{D})(r - s\sqrt{D}) = r^2 - s^2 D \in \mathbb{Q} \,.$$

c) Die Spur von α ist $\mathrm{Sp}(\alpha) = \alpha + \overline{\alpha} = 2r \in \mathbb{Q}$.

Lemma: *a)* Für $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$
b) Für $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$ ist $\mathrm{N}(\alpha\beta)$
c) $\alpha \in \mathbb{Q}[\sqrt{D}]$ ist Wurzel der qu

$$X^2 - \mathrm{Sp}(\alpha$$

d) $\alpha \in \mathbb{Q}[\sqrt{D}]$ ist genau dann ga
e) $\alpha \in \mathcal{O}_D$ ist genau dann eine E

Beweis: a) Folgt sofort durch dir
und $\beta = u + v\sqrt{D}$ ist

$$\overline{\alpha\beta} = \overline{(ru + svD) + (rv + su)}$$
$$= (r - s\sqrt{D})(u - v\sqrt{D})$$

b) Nach Definition ist

$$\mathrm{N}(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta$$

c) Ist offensichtlich, denn α und

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - (\alpha +$$

d) folgt sofort aus *c)* und der Def

e) Ist $\alpha \in \mathcal{O}_D^\times$ eine Einheit, so
ment $\beta \in \mathcal{O}_D$, und wegen $\alpha\beta =$
Die Norm ist also eine Einheit vo

Ist umgekehrt $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = \pm 1$,
ganzes Inverses.

Das können wir beispielsweise an
Zerlegungen $6 = 2 \cdot 3 = (1 + \sqrt{-}$

$$\mathrm{N}(2) = 2 \cdot 2 = 4, \quad \mathrm{N}(3) = 3 \cdot$$

Echte Primteiler einer dieser Za
haben. Wegen

$$\mathrm{N}(a + b\sqrt{}$$

müßte für solche Elemente $b =$
$a \in \mathbb{Q}$ offensichtlich nicht mögl

und $1 \pm \sqrt{-5}$ allesamt irreduzibel, und die Zahl sechs läßt sich auf zwei verschiedene Weisen als Produkt irreduzibler Elemente schreiben. (Es ist klar, daß 2 und 3 nicht zu $1 \pm \sqrt{-5}$ assoziiert sein können, denn die Normen assoziierter Elemente unterscheiden sich höchstens im Vorzeichen.)

Damit haben wir gezeigt, daß die Hauptordnung von $\mathbb{Q}[\sqrt{-5}]$ nicht faktoriell ist.

§5: Euklidische Ringe

In Kapitel I bewiesen wir die eindeutige Primzerlegung in $\mathbb{Z}$ mit Hilfe des EUKLIDischen Algorithmus. Wenn wir Beispiele für faktorielle Ringe $\mathcal{O}_D$ suchen, liegt es daher nahe, nach Ringen zu suchen, in denen es einen EUKLIDischen Algorithmus gibt. Solche Ringe heißen EUKLIDische Ringe.

Wie wir gesehen haben, ist die Division mit Rest das wichtigste Werkzeug beim EUKLIDischen Algorithmus, und wie sich in diesem Abschnitt herausstellen wird, brauchen wir kein weiteres. Wir definieren daher

Definition: Ein EUKLIDischer Ring ist ein Integritätsbereich R zusammen mit einer Abbildung $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$, so daß gilt: Ist $x|y$, so ist $\nu(x) \leq \nu(y)$, und zu je zwei Elementen $x, y \in R$ gibt es Elemente $q, r \in R$ mit

$$x = qy + r \quad \text{und} \quad r = 0 \quad \text{oder} \quad \nu(r) < \nu(y)\,.$$

Wir schreiben auch $x : y = q$ Rest r und bezeichnen r als Divisionsrest bei der Division von x durch y.

Das Standardbeispiel ist natürlich der Ring $\mathbb{Z}$ der ganzen Zahlen mit $\nu(x) = |x|$. Ein anderes Beispiel ist der Polynomring $k[X]$ über einem Körper k: Hier können wir $\nu(f)$ für ein Polynom $f \neq 0$ als den Grad von f definieren; dann erfüllt auch die Polynomdivision mit Rest die Forderung an einen EUKLIDischen Ring.

Man beachte, daß weder der Quotient noch der Divisionsrest eindeutig bestimmt sein muß: Beispielsweise ist schon in $\mathbb{Z}$ einerseits

15 : 4 = 3 Rest 3, andererseits a
im EUKLIDischen Algorithmus m
führt.

Lemma: In einem EUKLIDischen
$x, y \in R$ einen ggT. Dieser kann
berechnet werden und läßt sich a
Koeffizienten aus R darstellen.

Beweis: In jedem Integritätsberei
mit $x, y, q, r \in R$, daß die gem
denen von y und r sind. Speziell
wir dabei r als Divisionsrest wä
KLIDischen Algorithmus, danach
eine Folge von Divisionsresten r
jedem Schritt die gemeinsamen Te
und r_i sind. Außerdem ist stets en
daß die Folge nach endlich vielen
muß. Auch hier sind die gemeinsa
die gemeinsamen Teiler von x u
sind die gemeinsamen Teiler von
von r_{n-1}, und unter diesen gibt es
selbst. Somit haben auch x und
nämlich den nach dem EUKLIDis
von Null verschiedenen Division

Auch die lineare Kombinierbark
jeder Division mit Rest ist der Di
Dividend und Divisor darstellbar
ginnen wir mit Dividend x und
earkombinationen von x und y da
auch alle folgenden Dividenden
rangegangenen Division Lineark
ist es auch ihr Divisionsrest. Ins
nichtverschwindender Divisionsr
und die Koeffizienten können wie
KLIDischen Algorithmus berechn

Lemma: *a)* In einem EUKLIDischen Ring R ist jedes Element $x \neq 0$ mit $\nu(x) = 0$ eine Einheit.
b) Ist $x = yz \neq 0$, wobei y, z keine Einheiten sind, so ist $\nu(y) < \nu(x)$ und $\nu(z) < \nu(x)$.

Beweis: a) Wir dividieren eins durch x mit Rest: $1 : x = q$ Rest r. Dann ist entweder $r = 0$ oder aber $\nu(r) < \nu(x) = 0$. Letzteres ist nicht möglich, also ist $qx = 1$ und x eine Einheit.

b) Da y und z Teiler von x sind, sind $\nu(y), \nu(z) \leq \nu(x)$. Um zu zeigen, daß $\nu(y)$ echt kleiner als $\nu(x)$ ist, dividieren wir y mit Rest durch x; das Ergebnis sei q Rest r, d.h. $y = qx + r$ mit $r = 0$ oder $\nu(r) < \nu(x)$. Wäre $r = 0$, wäre y ein Vielfaches von x, es gäbe also ein $u \in R$ mit $y = ux = u(yz) = (uz)y$. Damit wäre $uz = 1$, also z eine Einheit, im Widerspruch zur Annahme. Somit ist $\nu(r) < \nu(x)$.

Als Teiler von x ist y auch Teiler von $r = y - qx = y(1 - qz)$, also muß $\nu(y) \leq \nu(r) < \nu(x)$ sein. Genauso folgt, daß auch $\nu(z) < \nu(x)$ ist. ∎

Satz: Jeder EUKLIDische Ring ist faktoriell.

Beweis: Wir müssen zeigen, daß jedes Element $x \neq 0$ aus R bis auf Reihenfolge und Assoziiertheit eindeutig als Produkt aus einer Einheit und geeigneten Potenzen irreduzibler Elemente geschrieben werden kann. Wir beginnen damit, daß sich x überhaupt in dieser Weise darstellen läßt.

Dazu benutzen wir die Betragsfunktion $\nu: R \setminus \{0\} \to \mathbb{N}_0$ des EUKLIDischen Rings R und beweisen induktiv, daß für $n \in \mathbb{N}_0$ alle $x \neq 0$ mit $\nu(x) \leq n$ in der gewünschten Weise darstellbar sind.

Ist $\nu(x) = 0$, so ist x nach obigem Lemma eine Einheit. Diese kann als sich selbst mal dem leeren Produkt von Potenzen irreduzibler Elemente geschrieben werden.

Für $n > 1$ unterscheiden wir zwei Fälle: Ist x irreduzibel, so ist $x = x$ eine Darstellung der gewünschten Form, und wir sind fertig.

Andernfalls läßt sich $x = yz$ als Produkt zweier Elemente schreiben, die beide keine Einheiten sind. Somit sind nach obigem Lemma $\nu(y) < \nu(x)$ und $\nu(z) < \nu(x)$, beide lassen si
als Produkte von Einheiten und P
ben. Damit läßt sich auch $x = yz$

Als nächstes müssen wir uns übe
Reihenfolge und Einheiten eind
hierzu ist die folgende Zwischenl

*Falls ein irreduzibles Element p e
einen der beiden Faktoren.*

Zum *Beweis* betrachten wir den gg
ein Teiler von p, also bis auf Asso
Fall ist p Teiler von x und wir sin

$$1 =$$

als Linearkombination von p u
macht daraus $y = \alpha px + \beta xy$, un
rechten Seite durch p teilbar: Bei
daraus, daß nach Voraussetzung p
von y, und die Zwischenbehaupt

Induktiv folgt sofort:

*Falls ein irreduzibles Element p
destens einen der Faktoren x_i.*

Um den Beweis des Satzes zu b
jedes $n \in \mathbb{N}_0$ alle Elemente mit ν
Einheiten eindeutige Primfaktorz

Für $n = 0$ ist x eine Einheit; hier

Seien nun

$$x = u \prod_{i=1}^{r}$$

zwei Zerlegungen eines Elements
daß alle $e_i, f_j \geq 1$ sind. Dann
Produkts, also auch des zweiten. W
also mindestens eines der Eleme

Einheit w gleich q_j. Da p_1 keine Einheit ist, ist $\nu(x/p_1) < \nu(x)$; nach Induktionsannahme hat also $x/p_1 = x/(wq_j)$ eine bis auf Reihenfolge und Einheiten eindeutige Zerlegung in irreduzible Elemente. Damit hat auch x diese Eigenschaft. ∎

Bemerkung: Die Umkehrung dieses Satzes gilt nicht: Beispielsweise sind nach einem Satz von GAUSS auch $\mathbb{Z}[X]$ sowie Polynomringe in mehr als einer Veränderlichen über $\mathbb{Z}$ oder einem Körper faktoriell, aber keiner dieser Ringe ist EUKLIDisch, da sich weder der ggT eins von 2 und X in $\mathbb{Z}[X]$ noch der ggT eins von X und Y in $k[X,Y]$ als Linearkombination der Ausgangselemente schreiben läßt.

Wir interessieren uns in diesem Kapitel vor allem für quadratische Zahlkörper; daher wollen wir uns fragen, wann die Hauptordnung eines solchen Körpers EUKLIDisch ist.

Dazu brauchen wir zunächst eine Abbildung ν nach $\mathbb{N}_0$. Für $\mathbb{Z}$ konnten wir einfach den Betrag nehmen; für die Hauptordnung eines quadratischen Zahlkörpers können wir unser Glück versuchen mit dem Betrag der Norm.

Falls die Hauptordnung $\mathcal{O}_D$ von $\mathbb{Q}[\sqrt{D}]$ zusammen mit dieser Abbildung ein EUKLIDischer Ring ist, muß es zu je zwei Elementen $r, s \in \mathcal{O}_D$ mit $s \neq 0$ ein Element $q \in \mathcal{O}_D$ geben, so daß $|\mathrm{N}(r - sq)| < |\mathrm{N}(s)|$ ist. Division durch s macht daraus die Ungleichung

$$\left|\mathrm{N}\left(\frac{r}{s} - q\right)\right| < |\mathrm{N}(1)| = 1\,.$$

Da sich jedes Element von $\mathbb{Q}[\sqrt{D}]$ als so ein Quotient r/s darstellen läßt, muß es also zu jedem $x \in \mathbb{Q}[\sqrt{D}]$ ein $q \in \mathcal{O}_D$ geben, so daß $|\mathrm{N}(x - q)| < 1$ ist. Dies zeigt auch, wie man im EUKLIDischen Fall die Division mit Rest durchführt: Man berechnet den Quotienten x/y zunächst im Körper $\mathbb{Q}[\sqrt{D}]$ und nimmt dann das bezüglich der Norm nächstgelegene Element von $\mathcal{O}_D$.

Betrachten wir als Beispiel die Division von $23 + 9i$ durch $2 - 3i$ im Ring $\mathbb{Z}[i]$ der GAUSSschen Zahlen. In $\mathbb{Q}[i]$ ist

$$\frac{23 + 9i}{2 - 3i} = \frac{(23 + 9i)(2 + 3i)}{13} = \frac{19}{13} + \frac{87}{13}i\,.$$

Da $19 : 13 = 1$ Rest 6 und $87 : 13$
aus $\mathbb{Z}[i]$ am nächsten bei dieser Z

$$\frac{19}{13} + \frac{87}{13}i - (1$$

ist $(6^2 + 4^2)/13^2 = 52/169$ und da

$$(23 + 9i) : (2 - 3i$$

ein mögliches Ergebnis der Divis

$$(23 + 9i) : (2 -$$

denn auch die Norm von 3 ist klei
jeweils als Dividend minus Divis

Um zu sehen, in welchen der
Rest stets möglich ist, betrachte
beschränken uns dabei zunächst a

Um besser zu sehen, welche Term
und welche negativ sind, schreib
$D > 0$; seine Elemente lassen sich
wobei $i = \sqrt{-1}$ die imaginäre Ei

Wir betrachten $\mathbb{Q}[\sqrt{-D}]$ als Teilr
dann ist

$$\mathrm{N}(r + is\sqrt{D}) = (r + is\sqrt{D})(r -$$

einfach das Quadrat des übliche
genau dann ein EUKLIDischer Ri
wenn es zu jedem Element $x \in$
$|x - q| < 1$ ist. Da $\mathbb{Q}[\sqrt{-D}]$ dic
scheiben mit Radius eins um die
Zahlenebene überdecken. Bei de
cher Kreisscheiben liegen, muß z
in $\mathbb{Q}[\sqrt{-D}]$ liegen: Andernfalls s
Ungleichung nicht erfüllt ist.

Die Punkte aus $\mathcal{O}_D$ bilden ein G
$q \in \mathcal{O}_D$ definieren wir dessen *Wi*

als den Abschluß der Menge aller $z \in \mathbb{C}$, die näher bei q liegen als bei jedem der anderen Gitterpunkte:

$$W(q) = \left\{ z \in \mathbb{C} \;\middle|\; \forall q' \in \mathcal{O}_{-D} : |z-q| \le |z-q'| \right\}$$

Offensichtlich liegt jedes $z \in \mathbb{C}$ in mindestens einem dieser Wirkungsbereiche, und falls $W(q) \subseteq \left\{ z \in \mathbb{C} \;\middle|\; |z-q| < 1 \right\}$, folgt insbesondere, daß jedes Element von $\mathbb{Q}[\sqrt{-D}]$ im Innern einer Kreisscheibe mit Radius eins um einen Gitterpunkt liegt: Dann ist der Ring $\mathcal{O}_{-D}$ EUKLIDisch.

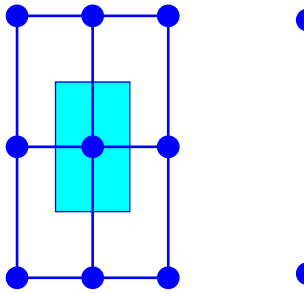
Der Wirkungsbereich eines Gitterpunkts z unterscheidet sich von dem des Nullpunkts nur durch eine Verschiebung um z; entsprechendes gilt auch für die Kreise mit Radius eins um die beiden Punkte. Daher reicht es, zu untersuchen, wann der Wirkungsbereich des Nullpunkts ganz im Innern des Einheitskreises liegt.

Die Struktur des Wirkungsbereichs hängt ab von $D \bmod 4$: Falls $D \not\equiv -1 \bmod 4$, d.h. $D \not\equiv 3 \bmod 4$, ist $\mathcal{O}_{-D} = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{-D}]$. In der komplexen Zahlenebene bilden diese Punkte ein Rechteckgitter mit den Gitterpunkten $q = r + is\sqrt{D}$ zu $r, s \in \mathbb{Z}$. Der Wirkungsbereich des Nullpunkts ist daher das Rechteck mit Ecken $\pm\frac{1}{2} \pm \frac{i}{2}\sqrt{D}$, und die am weitesten von der Null entfernte Punkte sind die Ecken mit Abstand

$$\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{D}}{2}\right)^2} = \frac{\sqrt{1+D}}{2}.$$

Dies ist genau dann echt kleiner als eins, wenn $D \le 2$ ist, d.h. $D = 1$ oder $D = 2$.

Für $D = 3$ überdecken zwar die abgeschlossenen Kreisscheiben mit Radius eins um die Gitterpunkte ganz $\mathbb{C}$, aber die gerade betrachteten Eckpunkte sind Elemente des Körpers $\mathbb{Q}[\sqrt{-3}]$, die in keiner offenen Kreisscheibe um einen Gitterpunkt liegen. Das ist allerdings hier kein Problem, denn in $\mathbb{Q}[\sqrt{-3}]$ sind diese Eckpunkte ja selbst Gitterpunkte: Für $D \equiv 3 \bmod 4$ gibt es schließlich mehr ganze Zahlen in $\mathbb{Q}[\sqrt{-D}]$.



Hier wird das Gitter $\mathcal{O}_{-D}$ erzeu
Der Nullpunkt hat somit sechs
$\pm\frac{1}{2}\pm\frac{i}{2}\sqrt{D}$. Die Wirkungsbereich
durch die Geraden $x = \pm\frac{1}{2}$, und au
wir die Mittelsenkrechte zur Verb
durch den Streckenmittelpunkt,
senkrecht auf dieser Strecke.

Eine Drehung um 90° kann in
werden durch Multiplikation mit

$$\left\{ \left(\pm\frac{1}{2} \pm \frac{i}{2}\sqrt{D} \right) +$$

Zwei der Ecken des Wirkungsbe
auf der imaginären Achse; Einset
daß deren Imaginärteile gleich ±
vier Ecken liegen auf den Gerade
führt die Rechnung auf die Imagi

Der Abstand dieser Punkte vom

$$\sqrt{\left(\frac{1}{2}\right)^2 + \frac{(\sqrt{D} - 1/\sqrt{D})^2}{16}} = \frac{1}{4}$$

dies ist genau dann kleiner als ei

$$2 + D + \frac{1}{D} < 4^2 =$$

Die einzigen $D \equiv 3 \bmod 4$, die dies erfüllen, sind $D = 3, D = 7$ und $D = 11$. Für diese ist auch $\frac{1}{4}(\sqrt{D} + 1/\sqrt{D}) < 1$, so daß dann und nur dann der gesamte Wirkungsbereich der Null im Einheitskreis liegt.

Die einzigen imaginärquadratischen Zahlkörper $\mathbb{Q}[\sqrt{D}]$, deren Hauptordnung bezüglich der Norm EUKLIDisch ist, sind somit die mit

$$D \in \{-1, -2, -3, -7, -11\};$$

von diesen wissen wir damit auch, daß ihre Hauptordnung faktoriell ist.

Es ist nicht bekannt, ob es andere $D < 0$ gibt, für die die Hauptordnung bezüglich einer anderen Funktion $\nu\colon \mathcal{O}_D \setminus \{0\} \to \mathbb{N}_0$ EUKLIDisch ist. Bekannt ist aber, daß die einzigen weiteren faktoriellen Hauptordnungen $\mathcal{O}_D$ die sind mit $D \in \{-19, -43, -67, -163\}$: *siehe* H. STARK: A complete determination of the complex fields of class-number one, *Michigan J. of Math.* **14** (1967), 1–27. Die Methoden seines Beweises liegen deutlich über dem Niveau dieser Vorlesung.

Im reellquadratischen Fall wird die Ungleichung $|\mathrm{N}(z-q)| - 1$ für $z = x + y\sqrt{D}$ und $q = r + s\sqrt{D}$ zu

$$\left|(x-r)^2 - (y-v)^2 D\right| < 1\,.$$

Betrachten wir für festes $q = r + s\sqrt{D} \in \mathcal{O}_D$ die Menge Z_q aller $(x, y) \in \mathbb{R}^2$, für die $z = x + y\sqrt{D}$ diese Ungleichung erfüllt, erhalten wir also einen Bereich, der durch Hyperbeln begrenzt wird, und wir müssen zeigen, daß die Vereinigung aller Z_q für $q \in \mathcal{O}_D$ ganz $\mathbb{R}^2$ ist. Durch mühsames Abhaken vieler Einzelfälle folgt aus einer ganzen Reihe von Arbeiten, daß dies genau dann der Fall ist, wenn

$$D \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}\,.$$

Die letzten offenen Fälle wurden 1950 untersucht in H. CHATLAND, H. DAVENPORT: Euclid's algorithm in real quadratic fields, *Canadian J. Math.* **2** (1950), 289–296; dort sind auch die weiteren Arbeiten zitiert, aus denen zusammen schließlich das obige Ergebnis folgt.

Genau für diese D ist also $\mathcal{O}_D$ EUKLIDisch bezüglich der Norm. Es gibt zahlreiche weitere positive D, für die $\mathcal{O}_D$ faktoriell ist; vermutungsweise sind es sogar unendlich viele. Ob einige dieser Ringe möglicherweise

bezüglich einer anderen Abbildu
ist nicht bekannt, und die Nicht
natürlich nur schwer zu beweisen

§6: Einheiten in quadratis

Ist $x + y\sqrt{D}$ eine Einheit in $\mathcal{O}_D$ (
von einer Einheit des Zahlkörpers
eine Einheit in $\mathbb{Z}$ sein, also gleich

Im imaginärquadratischen Fall ist
Terme; hier kommt also nur der
zahligen Lösungen sind offensic
$D = -1$ der GAUSSschen Zahler
sind auch echt halbzahlige Werte
dies führt offensichtlich nur für D
$x = \pm\frac{1}{2}$ und $y = \pm\frac{1}{2}$. Damit habe

Lemma: In einem imaginärquad
für $D \neq -1$ und $D \neq -3$ nur die E
noch die Einheiten $\pm i$, und in $\mathbb{Q}$
sechsten Einheitswurzeln ± 1 und

In reellquadratischen Körpern fü
Gleichung $x^2 - Dy^2 = \pm 1$ mit ein
ausschließen, daß es unendlich vi

Betrachten wir zunächst den Fall,
bezeichnet man als die PELLsche

JOHN PELL (1611–1685) wurde im engli
Schule. Bereits 1624 begann er sein Stud
er seinen Bachelor und 1630 seinen Mas
1654–1658 war er als Diplomat im Auft
JOHANN HEINRICH RAHN (1622–1676) ver
ist ein Beispiel der obigen Gleichung zu
PELL benannte. Tatsächlich wurde sie wo
und Astronom BRAHMAGUPTA (598–670)

zurück auf LAGRANGE (1736–1813), der die Gleichung als ein Problem bezeichnet, das FERMAT den englischen Mathematikern stellte. Nach seiner Rückkehr aus Zürich wurde PELL Priester. 1663 wählte ihn die Royal Society zum Mitglied, 1675 wurde er deren Vizepräsident.

Mit der PELLschen Gleichung werden wir uns im nächsten Kapitel genauer beschäftigen, und wir werden sehen, daß sie stets unendlich viele Lösungen hat. Als Vorbereitung dazu wollen wir uns hier etwas genauer mit der Struktur der Einheitengruppe beschäftigen. Dazu betrachten wir die Abbildung

$$\lambda\colon \begin{cases} \mathcal{O}_D^\times \to \mathbb{R}^2 \\ \quad \alpha \mapsto (\log|\alpha|, \log|\overline{\alpha}|) \end{cases}$$

Da eine Einheit Norm ± 1 hat, ist $|\alpha| \cdot |\overline{\alpha}| = 1$, das Bild von λ liegt also auf der zweiten Winkelhalbierenden $y = -x$ von $\mathbb{R}^2$. Außerdem sind α und $\overline{\alpha}$ reell, so daß α genau dann im Kern von λ liegt, wenn $\alpha = \pm 1$ ist.

Das Bild von λ ist diskret, denn hat $\lambda(\alpha)$ höchstens den Abstand M vom Nullpunkt, so ist $\log|\alpha| \le M$ und $\log|\overline{\alpha}| \le M$. Ist $\log R = M$, so ist also $|\alpha| \le R$ und $|\overline{\alpha}| \le R$. Damit ist $|\mathrm{Sp}(\alpha)| \le 2R$ und $|\mathrm{N}(\alpha)| \le R^2$. Da Norm und Spur ganzzahlig sind, gibt es also für beide nur endlich viele Möglichkeiten, und da für ein ganzes Element Norm und Spur zusammen mit dem führenden Koeffizienten eins die Koeffizienten der quadratischen Gleichung sind, gibt es auch nur endlich viele quadratische Gleichungen und damit nur endlich viele Möglichkeiten für α.

Somit gibt es im Bild von λ ein Element $\lambda(\alpha) = (r, -r)$ mit *minimalem* $r > 0$. Wir wollen uns überlegen, daß das jeder andere Punkt im Bild ein ganzzahliges Vielfaches davon ist. Da mit $(s, -s)$ auch $(-s, s)$ im Bild liegt, können wir uns dabei auf Punkte $(s, -s)$ mit $s \ge 0$ beschränken.

Für einen solchen Punkt $\lambda(\beta) = (s, -s)$ gibt es jedenfalls ein größtes $n \in \mathbb{N}_0$, so daß $nr \le s$ ist. Dann ist

$$\lambda(\beta\alpha^{-n}) = \lambda(\beta) - n\lambda(\alpha) = (s, -s) - n(r, -r) = (s - nr, nr - s),$$

so daß auch dieser Punkt im Bild liegt. Nach Wahl von n ist aber $0 \le s - nr < r$; wegen der Minimalität von r ist also $s - nr = 0$, d.h. $s = nr$ und $\beta = \alpha^n$.

Damit haben wir bewiesen

Satz: Falls es im reellquadratisc
ment aus $\mathcal{O}_D^\times$ gibt, dessen Norm
entsprechendes Element α mit k
$\mathcal{O}_D$ sind genau die Elemente $\pm\alpha^$
Einheitengruppe unendlich.

Im nächsten Kapitel werden wi
Zahlkörper eine solche „Grundein
reellquadratischen Zahlkörpers be
te der Form $\pm\alpha^n$ mit $n \in \mathbb{Z}$ und

Bevor wir das im einzelnen unt
dieses Kapitels und zur Vorbereit
einer nichtkommutativen Variant

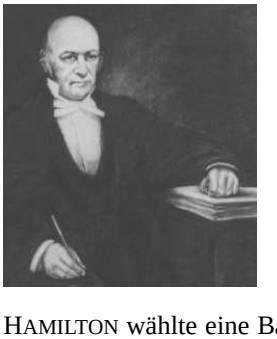
§ 7: Quaternionen

Nachdem durch die komplexen Za
versehen war, versuchten viele M
erreichen. Natürlich kann weder
zu einem Körper gemacht werde
algebraische Erweiterung von $\mathbb{R}$
von $\mathbb{R}$ gleich $\mathbb{C}$ ist, muß dann $n =$

Die damaligen Mathematiker war
es, einfach irgendeine Art von M
bedingt allen Körperaxiomen ge
ohnehin noch niemand.

Erst 1940 konnte HEINZ HOPF
Vektorfelder auf Sphären) zeigen
bilineare Abbildung $\mathbb{R}^n \times \mathbb{R}^n \to$
eine Zweierpotenz ist, und 1958
und mit verschiedenen Methoden
daß auch noch $n \le 8$ sein muß
$n = 1, 2, 4$ und 8 in Frage komme
bereits entsprechende Produkte

natürlich die reelle *bzw.* komplexe Multiplikation. Den Fall $n = 4$ löste HAMILTON 1843: Er fand eine Multiplikation auf $\mathbb{R}^4$, die zwar nicht kommutativ ist, ansonsten aber alle Körperaxiome erfüllt. Man spricht in so einem Fall von einem *Schiefkörper* oder, in der neueren Literatur, einer *Divisionsalgebra*. HAMILTON bezeichnete seine vierdimensionalen Zahlen als *Quaternionen.* Kurz danach konstruierte ARTHUR CAYLEY (1821–1895) ein nicht-assoziatives Produkt auf $\mathbb{R}^8$; die so erhaltenen „Zahlen“ nannte er *Oktaven.*



WILLIAM ROWEN HAMILTON (1805–1865) wurde in Dublin geboren; bereits mit fünf Jahren sprach er Latein, Griechisch und Hebräisch. Mit dreizehn begann er, mathematische Literatur zu lesen, mit 21 wurde er, noch als Student, Professor der Astronomie am Trinity College in Dublin. Er verlor allerdings schon bald sein Interesse an der Astronomie und beschäftigte sich stattdessen mit mathematischen und physikalischen Problemen. Am bekanntesten ist er für seine Entdeckung der Quaternionen, vorher publizierte er aber auch bedeutende Arbeiten über Optik, Dynamik und Algebra.

HAMILTON wählte eine Basis von $\mathbb{H} = \mathbb{R}^4$, die aus der Eins sowie drei „imaginären Einheiten“ $\mathbf{i}, \mathbf{j}, \mathbf{k}$ besteht, d.h. $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$. Außerdem postulierte er, daß $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$ sein sollte; daraus lassen sich dann über das Assoziativgesetz auch die anderen Produkte imaginärer Einheiten berechnen.

Damit ist, wenn man die Gültigkeit des Distributivgesetzes postuliert, eine Multiplikation auf $\mathbb{R}^4$ definiert; der Beweis, daß hierbei alle Körperaxiome außer der Kommutativität der Multiplikation erfüllt sind, enthält wie üblich nur einen etwas schwierigeren Punkt, die Existenz von Inversen; der Rest ist mühsame Abhakerei.

Zum Glück fand CAYLEY 1858 einen einfacheren Weg: Die vier komplexen 2×2-Matrizen

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ und } K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

erfüllen dieselben Relationen

$$I^2 = J^2 = K^2 = -E \quad \text{und} \quad IJ = -JI = K\,;$$

wir können also die Quaternion
Matrix

$$aE + bI + cJ + dK =$$

Da für Matrizen das Assoziativge
ten, ist klar, daß das Produkt zwei
ben Form ist und daß auch die Q
und Distributivgesetz erfüllt.

Die Quaternionen entsprechen
Matrizen der Form

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \quad \text{mit}$$

Die Determinante dieser Matrix i

Definieren wir in Analogie zum K
der das konjugierte Element zu γ
$\overline{\gamma} = a - bi - cj - dk$, so entspric

$$\begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$$

Damit folgt insbesondere, daß γ
verschwindet, wenn $\gamma = 0$ ist. Wi
Norm $\mathrm{N}(\gamma)$ der Quaternion γ, und
Inverse zu γ – sowohl für die Lin

$\mathrm{N}(\gamma)$ ist gleichzeitig die Determi
dem Multiplikationssatz für Deter

$$\mathrm{N}(\gamma\delta)$$

Kapitel 7
Quadratische Formen

Eine quadratische Form ist ein Ausdruck der Form

$$F(x,y) = Ax^2 + Bxy + Cy^2 \quad \text{mit} \quad A,B,C \in \mathbb{Z}\,;$$

die Zahlentheorie interessiert sich vor allem dafür, welche Werte $F(x,y)$ für $x,y \in \mathbb{Z}$ annehmen kann.

§ 1: Summen zweier Quadrate

Der einfachste Fall ist die Form $F(x,y) = x^2+y^2$. Sie hängt eng zusammen mit der Hauptordnung $\mathbb{Z}[i]$ von $\mathbb{Q}[i]$, denn

$$x^2 + y^2 = (x+iy)(x-iy)$$

ist die Norm von $x+iy$. Eine ganze Zahl n ist also genau dann als Summe zweier Quadrate darstellbar, wenn sie die Norm einer GAUSSschen ganzen Zahl ist.

Das Quadrat einer geraden Zahl ist durch vier teilbar, das einer ungeraden Zahl $2k+1$ ist $4k^2+4k+ \equiv 1 \bmod 4$; somit ist jede Summe zweier Quadrate kongruent null, eins oder zwei modulo vier. Eine Zahl kongruent drei modulo vier kann also nicht als Summe zweier Quadratzahlen auftreten.

Auf der Suche nach positiven Ergebnissen können wir uns auf Primzahlen beschränken, denn wie FIBONACCI bereits im dreizehnten Jahrhundert zeigte, gilt:

Lemma: Sind zwei Zahlen $n,m \in \mathbb{N}$ darstellbar als Summen zweier Quadrate, so gilt dasselbe für ihr Produkt nm.

Beweis: Wenn n und m als Sum
gibt es $\alpha,\beta \in \mathbb{Z}[i]$, so daß $n =$
Multiplikativität der Norm ist da
und damit als Summe zweier Qua

FIBONACCI bewies dieses Lemma
Normen GAUSSscher Zahlen; er
Darstellung des Produkts als Sum
dabei um dieselbe Formel, zu der
Gleichung $\mathrm{N}(\alpha)\cdot\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta)$

$$(a^2+b^2)(c^2+d^2) =$$

Da $2 = 1^2+1^2$ als Summe zw
wir daher nur die ungeraden Prim
bereits, daß Zahlen kongruent dr
Quadrate sein können.

Satz: Eine ungerade Primzahl p
zweier Quadrate, wenn $p \equiv 1$ m
bis auf die Reihenfolge der Summ

Beweis: Aus Kapitel I, §8 wissen
Körper $\mathbb{F}_p$ von einem einzigen E
ist dann $g^{4k} = 1$, also $g^{2k} = -1$. S

In $\mathbb{Z}$ gibt es daher Zahlen x, für
ausgedrückt, $x^2+1 = \ell p$ für ein $\ell \in$
Vertreter mit Betrag kleiner $p/2$
daß $|x| < p/2$ ist; dann ist mit ei

$$x^2 + 1 = \ell p < \frac{p^2}{4}$$

Es gibt also ein $\ell < p$, so daß
kleinste solche ℓ sei m; wir müss

Zunächst ist klar, daß m eine u
Formel $x^2+y^2 = mp$ mit gerade

gerade oder beide ungerade sind; $x \pm y$ sind also gerade und

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = \frac{x^2+y^2}{2} = \frac{m}{2}p\,,$$

im Widerspruch zur Minimalität von m.

Falls die Behauptung falsch wäre, müßte somit $m \geq 3$ sein. Wir definieren dann zwei neue Zahlen $u, v \in \mathbb{Z}$ durch die Bedingungen

$$|u| < \frac{m}{2}, \quad |v| < \frac{m}{2}, \quad u \equiv x \bmod m \quad \text{und} \quad v \equiv y \bmod m\,.$$

Offensichtlich können nicht beide dieser Zahlen verschwinden, denn sonst wären x und y beide durch m teilbar, also wäre $x^2 + y^2 = mp$ durch m^2 teilbar. Das kann aber nicht sein, denn p ist prim und $m < p$. Weiter ist

$$u^2 + v^2 \equiv x^2 + y^2 = mp \equiv 0 \bmod m\,,$$

also gibt es eine natürliche Zahl r, so daß $u^2 + v^2 = rm$ ist. Da $u^2 + v^2$ kleiner ist als $\frac{1}{2}m^2$, ist $r < \frac{m}{2}$.

Nach der zu Beginn des Paragraphen zitierten Formel von FIBONACCI, d.h. also durch explizite Berechnung von $(u+iv)(x+iy)$ und Berechnung der Norm davon, erhalten wir die Formel.

$$(rm)(mp) = (u^2+v^2)(x^2+y^2) = (xu+yv)^2 + (xv-yu)^2\,.$$

Dabei ist nach Definition von u und v

$$xu + yv \equiv x^2 + y^2 \equiv 0 \bmod m \text{ und } xv - yu \equiv xy - yx \equiv 0 \bmod m\,,$$

beide Zahlen sind also durch m teilbar. Somit gibt es natürliche Zahlen X, Y mit

$$(rm)(mp) = m^2rp = (mX)^2 + (mY)^2 \quad \text{oder} \quad rp = X^2 + Y^2\,.$$

Da $r < \frac{m}{2}$, widerspricht dies der Minimalität von m.

Damit haben wir gezeigt, daß $m = 1$ sein muß, d.h. p läßt sich als Summe zweier Quadrate darstellen. Wir müssen uns noch überlegen, daß diese Darstellung bis auf die Reihenfolge der Faktoren eindeutig ist.

Angenommen, es gibt zwei Darstellungen $p = x^2 + y^2 = u^2 + v^2$. In $\mathbb{Z}[i]$ ist dann

$$p = (x+iy)(x-iy) = (u+iv)(u-iv)\,.$$

Alle Faktoren haben Norm p und
vorigen Kapitels wissen wir, daß
also faktorieller Ring ist. Daher u
gen nur durch Einheiten von $\mathbb{Z}[i]$
Nach dem Lemma aus §6 sind es
ist entweder $x^2 = u^2$ und $y^2 = v^2$
keit bewiesen wäre.

Als erste Anwendung davon kön
der GAUSSschen Zahlen bestimm

Korollar: Eine Primzahl $p \in \mathbb{N}$ i
$p \equiv 3 \bmod 4$. Andernfalls zerfäll
komplexer irreduzibler Elemente

Beweis: $p = 2 = (1+i)(1-i)$ zer
die Primzerlegung, denn $N(1 \pm i$

Falls eine ungerade Primzahl p ei
durch $r - is$ teilbar. Da die Norm
Einheiten, muß $N(r \pm is) = p$ sein
sind, denn ein echter Teiler müßt
haben. Außerdem folgt, daß sich
durch eine Einheit von p untersch
muß diese gleich eins sein, d.h. d

$$p = (r+is)($$

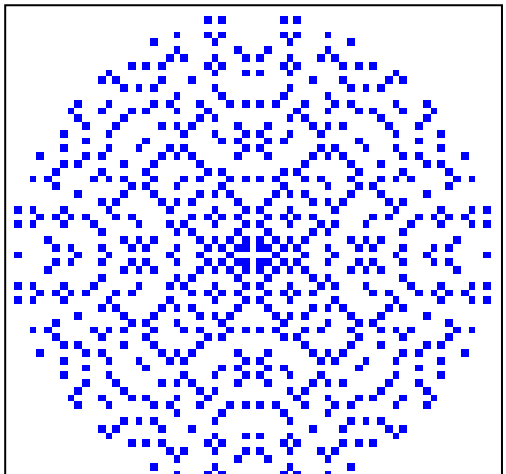
Nach dem Satz ist daher $p \equiv 1$ m

Ist umgekehrt $p \equiv 1 \bmod 4$, so gil
r, s, so daß $p = r^2 + s^2$ ist, d.h. $p =$
Argument aus dem vorigen Absch
ist.

Somit zerfallen genau die Primza
genau die $p \equiv 3 \bmod 4$ bleiben p

In der Abbildung sind die GAUS
höchstens 1000 durch Quadrate

Mancher Leser wird hier ein gelegentlich von Designern verwendetes Muster erkennen.



Kehren wir zurück zur Ausgangsfrage: Wann kann eine vorgegebene natürliche Zahl als Summe zweier Quadrate dargestellt werden?

Satz: Eine natürliche Zahl n läßt sich genau dann als Summe zweier Quadrate schreiben, wenn jeder Primteiler $p \equiv 3 \bmod 4$ in der Primzerlegung von n mit einer geraden Potenz auftritt.

Beweis: Zunächst ist die Bedingung hinreichend, denn da mit n auch jedes Produkt $c^2 n$ als Summe zweier Quadrate darstellbar ist, können wir die Primteiler $p \equiv 3 \bmod 4$ ignorieren. Nach dem gerade bewiesenen Satz wissen wir, daß jede Primzahl $p \equiv 1 \bmod 4$ Summe zweier Quadrate ist, und natürlich gilt dies auch für $2 = 1^2 + 1^2$. Damit ist nach dem obigen Lemma auch jedes Produkt solcher Primzahlen als Summe zweier Quadrate darstellbar.

Umgekehrt sei $n = x^2 + y^2$ und $d = \mathrm{ggT}(x, y)$. Mit $x = du$, $y = dv$ und $n = d^2 m$ ist dann $m = u^2 + v^2$, und m enthält genau dann einen Primteiler $p \equiv 3 \bmod 4$ in ungerader Potenz, wenn dies für n der Fall ist.

Ein solcher Primteiler p teilt auch
der GAUSSschen Zahlen. Falls p
mindestens einen der beiden Fa
zeigt, daß es dann auch den and
Summe $2u$ und Differenz $2iv$; da
p also die zueinander teilerfremd

Somit ist p in $\mathbb{Z}[i]$ keine Primza
$p = 2$ oder $p \equiv 1 \bmod 4$ sein. D
von n zugleich ein Teiler von d
Potenz auf.

Für zusammengesetzte Zahlen is
Quadrate im allgemeinen nicht m
in $\mathbb{Z}[i]$ läßt sich die Anzahl versch
Natürlich entsprechen auch für
Darstellungen als Summe zweie
als Norm eines Elements von $\mathbb{Z}[$
Reihenfolge auf dieselbe Zerlegu

Aus der Primzerlegung von n i
zerlegung in $\mathbb{Z}[i]$ schließen: Pri
bleiben nach obigem Korollar au
eins modulo vier sind Produkte
Die beiden Faktoren sind nicht as
$p = x^2 + y^2$ wäre gerade. Die Zw
irreduziblen Elemente $1 \pm i$, und
$(1 - i) \cdot i = 1 + i$.

Wir sortieren daher in der Primz
klassen modulo vier der Primfakt

$$n = 2^e \prod_{j=1}^{r} p_j^{f_j} \prod_{k=1}^{s} q_k^{2g_k} \quad \text{mit}$$

Für jedes p_j wählen wir ein $\pi_j \in$

ist n in $\mathbb{Z}[i]$ assoziiert zu

$$(1+i)^{2e}\prod_{j=1}^{r}\pi_j^{f_j}\prod_{j=1}^{r}\overline{\pi}_j^{f_j}\prod_{k=1}^{s}q_k^{2g_k}\ .$$

Ein Element $\alpha\in\mathbb{Z}[i]$, für das $\mathrm{N}(\alpha)=n$ sein soll, hat daher bis auf eine Einheit die Form

$$\alpha=(1+i)^{e}\prod_{j=1}^{r}\pi_j^{h_j}\prod_{j=1}^{r}\overline{\pi}_j^{f_j-h_j}\prod_{k=1}^{s}q_k^{g_k}\ ,$$

mit $0\le h_j\le f_j$. Die Anzahl verschiedener Möglichkeiten ist somit gleich dem Produkt der (f_j+1), wobei hier allerdings die Darstellungen $n=x^2+y^2$ und $n=y^2+x^2$ für $x\neq y$ als verschieden gezählt werden.

Die im Vergleich zur Größe von n meisten verschiedenen Darstellungen gibt es offenbar dann, wenn n ein Produkt verschiedener Primzahlen ist, die allesamt kongruent eins modulo vier sind. In diesem Fall ist die Anzahl der Darstellungen gleich zwei hoch Anzahl der Faktoren.

§2: Anwendung auf die Berechnung von π

Aus der Analysis I ist bekannt, daß gilt

$$\arctan x=x-\frac{x^3}{3}+\frac{x^5}{5}-\frac{x^7}{7}+\frac{x^9}{9}-\frac{x^{11}}{11}+\frac{x^{13}}{13}-\frac{x^{15}}{15}+\cdots\ ;$$

falls es jemand nicht mehr weiß: Die Ableitung des Arkustangens ist $1/(1+x^2)$, und nach der Summenformel für die geometrische Reihe ist

$$\frac{1}{1+x^2}=1-x^2+x^4-x^6+x^8-x^{10}+x^{12}-x^{14}+\cdots\ .$$

Durch gliedweise Integration folgt wegen $\arctan 0=0$ die obige Formel. Eine bekannte Anwendung davon ist der Spezialfall $x=1$:

$$\frac{\pi}{4}=\arctan 1=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\frac{1}{11}+\frac{1}{13}-\frac{1}{15}+\cdots\ .$$

Zur praktischen Berechnung von π ist diese Formel allerdings völlig unbrauchbar und der Alptraum eines jeden Numerikers: Zunächst einmal sind alternierende Summen grundsätzlich problematisch, allerdings ist

das hier vergleichsweise harmlos
den von seinem Vorgänger subtra

$$\frac{\pi}{4}=\frac{2}{1\cdot 3}+\frac{2}{5\cdot 7}+$$

mit lauter positiven Gliedern. Die
monoton fallend, so daß die Run
hinreichend langer Summation gr
Man muß also, wenn man eine en
hinten nach vorne summieren un
nung die Anzahl der Terme festl
der Summanden muß die gesamte

Dazu kommt, daß die Reihe extr
wir obige Gleichung durch zwei

$$\frac{\pi}{8}=\sum_{n=0}^{\infty}\frac{}{(4$$

die Teilsummen

$$S_N=\sum_{n=0}^{N}\frac{}{($$

so erhalten wir für die ersten Zeh

N	10	
$\pi-8S_N$	$4{,}5\cdot 10^{-2}$	5,0
N	100 000	1 00
$\pi-8S_N$	$5{,}0\cdot 10^{-6}$	5, 0

Für eine zusätzliche Dezimalstell
lich genau verzehnfacht werden
mehrere Billionen Ziffern von π
Wege zur Berechnung von π gebe

Einer davon benutzt Zahlen mit
Darstellungen als Summen zweie
tangens konvergiert sicherlich um
Wenn wir also den Winkel $\frac{\pi}{4}$ aufte

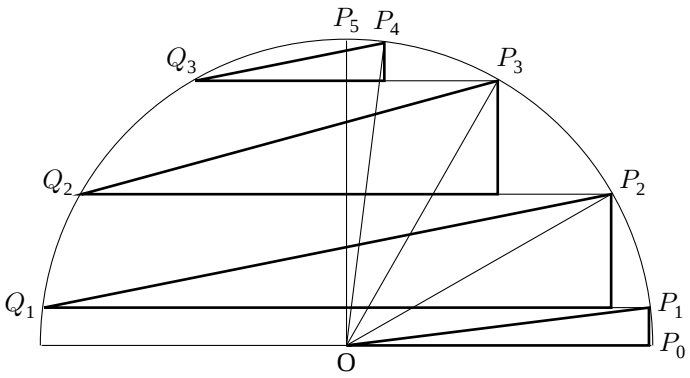
deren Tangens wir kennen, sollten bessere Ergebnisse zu erwarten sein. Genau das können wir mit solchen Zahlen erreichen.

Angenommen, wir haben für eine Zahl n die r verschiedenen Darstellungen

$$n = x_1^2 + y_1^2 = \cdots = x_r^2 + y_r^2$$

als Summen von Quadraten, wobei $y_1 < \cdots < y_r$ sei. Dann ist $x_i = y_{r-i}$, denn wir können ja in jeder Darstellung die Reihenfolge der Faktoren vertauschen. Wir wollen außerdem voraussetzen, daß n nicht das Doppelte eines Quadrats ist, so daß stets $x_i \neq y_i$ und somit r eine gerade Zahl ist.

Die Punkte $P_i = (x_i, y_i)$ und $Q_i = (-x_i, y_i)$ für $i = 1, \ldots, r$ liegen auf der Kreislinie $x^2 + y^2 = n$ um den Nullpunkt O, genauso die drei Punkte $P_0 = \left(\sqrt{n}, 0\right)$, $Q_0 = \left(-\sqrt{n}, 0\right)$ und $P_{r+1} = \left(0, \sqrt{n}\right)$.



Da die y-Koordinaten y_i der P_i der Größe nach geordnet sind, ist

$$\frac{\pi}{2} = \sum_{i=0}^{r} \measuredangle OP_iP_{i+1} = 2 \sum_{i=0}^{r/2-1} \measuredangle OP_iP_{i+1} + \measuredangle OP_{r/2}P_{r/2+1}\,.$$

Leider ist keines der Dreiecke $\triangle OP_iP_{i+1}$ rechtwinklig, so daß uns die ganzzahligen Koordinaten der (meisten) P_i bei der Berechnung der Winkel $\measuredangle OP_iP_{i+1}$ nichts nützen.

Nun lehrt uns aber ein Satz der El
diesem Paragraphen bewiesene) S
$\measuredangle OP_iP_{i+1}$ doppelt so groß ist w
gehört zu einem rechtwinkligen
nichts am Winkel, wenn wir den P
Projektion $P_i' = (x_{i+1}, y_i)$ von P_i

$$\frac{\pi}{2} = 2\measuredangle OP_0'P_1 + 4 \sum_{i=1}^{r/2-1} \measuredangle$$

Division durch zwei macht darau

$$\frac{\pi}{4} = \measuredangle OP_0'P_1 + 2 \sum_{i=1}^{r/2-1} \measuredangle$$

In dieser Darstellung sind die drei
allen Fällen die Eckpunkte eines r
samt ganzzahlige Koordinaten, un
haben ganzzahlige Längen. Somi
ausdrücken durch Arkustangensw

Als Beispiel betrachten wir das
Primzahlen kongruent eins modul
den Darstellungen

$$5 = 1^2 + 2^2, \quad 13 = 2^$$

verschafft man sich leicht die vie

$$1105 = 4^2 + 33^2 = 9^2 +$$

zu denen natürlich auch noch vie
Wir haben also

$$P_1 = (33, 4)\,, \quad P_2 = (32, 9$$
$$P_8 = (4, 33)\,, \quad P_7 = (9, 32$$

dazu kommen noch die beiden
$P_9 = (0, \sqrt{1105})$.

Die Q_i für $1 \le i \le 8$ unterscheiden sich von den P_i nur durch das Vorzeichen der Abszisse. Damit können wir die Tangenten aller Winkel bei O berechnen:

$$\tan \measuredangle OP_0P_1 = \tan \measuredangle OP_8P_9 = \frac{y_1}{x_1} = \frac{4}{33}$$

$$\tan \measuredangle OP_1P_2 = \tan \measuredangle OP_7P_8 = \tan 2\measuredangle Q_1P_1P_2 = \frac{y_2 - y_1}{x_1 + x_2} = \frac{5}{65} = \frac{1}{13}$$

$$\tan \measuredangle OP_2P_3 = \tan \measuredangle OP_6P_7 = \tan 2\measuredangle Q_2P_2P_3 = \frac{y_3 - y_2}{x_2 + x_3} = \frac{3}{63} = \frac{1}{21}$$

$$\tan \measuredangle OP_3P_4 = \tan \measuredangle OP_5P_6 = \tan 2\measuredangle Q_3P_3P_4 = \frac{y_4 - y_3}{x_3 + x_4} = \frac{11}{55} = \frac{1}{5}$$

$$\tan \measuredangle OP_4P_5 = \tan 2\measuredangle Q_4P_4P_5 = \frac{y_5 - y_4}{x_4 + x_5} = \frac{1}{47}$$

Die Summe aller dieser Winkel ist

$$\frac{\pi}{4} = \arctan\frac{4}{33} + 2\arctan\frac{1}{13} + 2\arctan\frac{1}{21} + 2\arctan\frac{1}{5} + \arctan\frac{1}{47}\,.$$

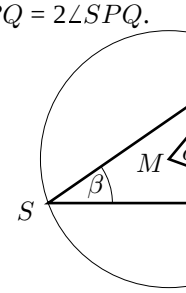
Approximieren wir dies, indem wir jede der TAYLOR-Reihen durch das TAYLOR-Polynom vom Grad n ersetzen, erhalten wir die folgenden betragsmäßigen Abweichungen Δ_n zwischen π und dem Vierfachen dieser Summe:

n	1	3	5	7	9
Δ_n	$2{,}5 \cdot 10^{-2}$	$5{,}2 \cdot 10^{-4}$	$1{,}4 \cdot 10^{-5}$	$4{,}4 \cdot 10^{-7}$	$1{,}4 \cdot 10^{-8}$
n	11	13	15	17	19
Δ_n	$5 \cdot 10^{-10}$	$4{,}9 \cdot 10^{-10}$	$6 \cdot 10^{-13}$	$2{,}1 \cdot 10^{-14}$	$7{,}7 \cdot 10^{-16}$

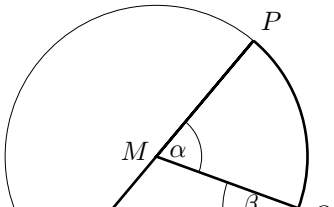
Die Verbesserung gegenüber der Berechnung via $\frac{\pi}{4} = \arctan 1$ ist dramatisch: Die dort betrachtete Teilsumme S_N entspricht der Auswertung des TAYLOR-Polynoms vom Grad $n = 4N + 3$, und selbst wenn wir N auf hundert Millionen setzen, haben wir noch einen Fehler von $5 \cdot 10^{-7}$. Mit dem neuen Ansatz kommen wir bereits mit TAYLOR-Polynomen vom Grad neun auf einen Fehler, der gerade mal ein Zehntel davon beträgt. An Stelle von hundert Millionen Summanden mußten wir dazu nur fünf TAYLOR-Polynome mit jeweils fünf Summanden auswerten.

Anhang: Der Satz vom In

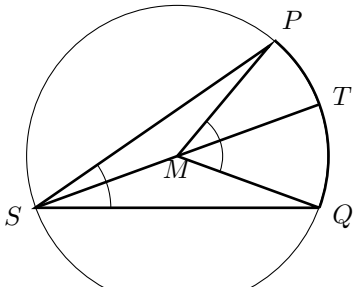
Satz: P, Q, S seien Punkte auf
Dann ist $\angle MPQ = 2\angle SPQ$.



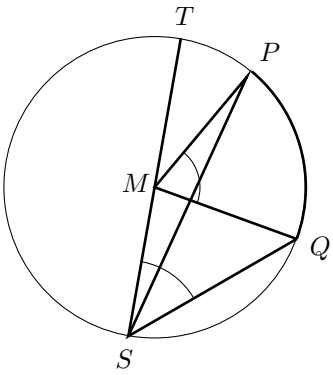
Beweis: Am einfachsten ist der F



Der allgemeine Fall kann auf



Bleibt noch der Fall, daß P und A auf derselben Seite des Durchmessers $\overline{ST}$ liegen. Auch in diesem Fall erfüllen wieder sowohl die Punkte S, P, T, M als auch die Punkte S, Q, T, M die Voraussetzungen des Satzes, und beides Mal sind wir in der Situation des eingangs bewiesenen Spezialfalls. Dieses Mal führt die Subtraktion dieser beiden Ergebnisse zum gewünschten Resultat für die Ausgangssituation mit den Punkten S, P, Q, M.



Damit ist der Satz vollständig bewiesen. ∎

§3: Der Satz von Lagrange

Es ist nicht möglich, eine beliebige natürliche Zahl als Summe von höchstens drei Quadratzahlen zu schreiben; das kleinste Gegenbeispiel ist die Sieben. Wie EULER vermutete und LAGRANGE bewies, kommt man aber immer mit höchstens vier Quadratzahlen aus.

Einer der vielen Beweise dieses Satzes ist recht ähnlich zu dem des Zweiquadratesatzes aus §1; statt mit dem Ring $\mathbb{Z}[i]$ der GAUSSschen Zahlen arbeiten wir aber mit dem Ring

$$\mathbb{Z} \oplus \mathbb{Z}\mathbf{i} \oplus \mathbb{Z}\mathbf{j} \oplus \mathbb{Z}\mathbf{k}$$

der ganzen Quaternionen. Auch hier haben wir eine Normabbildung, und eine ganze Zahl n ist offensichtlich genau dann als Summe von vier Quadraten darstellbar, wenn sie Norm einer ganzen Quaternion ist. Wegen der Multiplikativität der Norm reicht es also wieder, wenn wir Primzahlen p betrachten.

Zur Vorbereitung zeigen wir zunächst

Lemma: Zu jeder Primzahl p gibt es ganze Zahlen $x, y, z \in \mathbb{Z}$ und eine natürliche Zahl $m < p$, so daß gilt: $mp = x^2 + y^2 + z^2$

Beweis: Für $p = 2$ ist $2 = 1^2 + 1^2$

Von den Zahlen a^2 mit $0 \leq a \leq$ modulo p, denn $a^2 - b^2 = (a + b)$ sind beide Faktoren kleiner als p.

$$\mathcal{M}_1 = \{-a^2 \mid$$

und

$$\mathcal{M}_2 = \{1 + a^2 \mid$$

keine zwei Elemente, die modulo gen disjunkt sind und jede davo Vereinigung $p + 1$ Elemente; hier te geben, die modulo p kongruen mit $-x^2 \equiv 1 + y^2 \bmod p$, d.h. x^2 $x, y \leq \frac{1}{2}(p-1)$, ist dabei $m < p$

Lemma: Jede Primzahl p läßt Quadraten schreiben.

Beweis: Für $p = 2$ wissen wir d dem vorigen Lemma gibt es ein mp als Summe von sogar höchste die kleinste natürliche Zahl, für Quadraten darstellbar ist. Natürli

Wäre ℓ eine gerade Zahl, so wär gerade, und dazu gibt es drei Mög sind gerade, oder alle sind unger Rest ungerade. Im letzteren Fall v anordnen, daß w und x gerade si sind in allen drei Fällen $w \pm x$ u

$$\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)$$

im Widerspruch zur Minimalität das Lemma falsch wäre, müßte ℓ

Wir betrachten die modulo ℓ zu w, x, y, z kongruenten ganzen Zahlen W, X, Y, Z vom Betrag kleiner $\ell/2$. Wie schon beim Zwei-Quadrate-Satz können diese nicht allesamt verschwinden, denn sonst wären w, x, y, z durch ℓ teilbar, also ihre Quadratsumme ℓp durch ℓ^2, was wegen $\ell < p$ für eine Primzahl p nicht möglich ist.

Somit ist $0 < W^2 + X^2 + Y^2 + Z^2 < 4 \cdot \left(\frac{\ell}{2}\right)^2 = \ell^2$. Andererseits ist aber

$$W^2 + X^2 + Y^2 + Z^2 \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \bmod \ell\,;$$

also ist

$$W^2 + X^2 + Y^2 + Z^2 = \ell m \quad \text{mit} \quad 1 \le m < \ell\,.$$

Damit haben die Quaternionen

$$q = w + \mathbf{i}x + \mathbf{j}y + \mathbf{k}z \quad \text{und} \quad Q = W + \mathbf{i}X + \mathbf{j}Y + \mathbf{k}Z$$

die Normen $\mathrm{N}(q) = \ell p$ und $\mathrm{N}(Q) = \ell m$, ihr Produkt hat also die Norm $\ell^2 mp$. Zumindest von der Norm her spricht also nichts dagegen, daß dieses Produkt durch ℓ teilbar sein könnte.

Tatsächlich ist $q\overline{Q}$ durch ℓ teilbar, und das sieht man am schnellsten durch brutales Nachrechnen: In

$$\begin{aligned} q\overline{Q} = \quad & (wW + xX + yY + zZ) \; + (-wX + xW - yZ + zY)\mathbf{i} \\ & + (-wY + yW - zX + xZ)\mathbf{j} + (-wZ + zW - xY + yX)\mathbf{k} \end{aligned}$$

sind alle vier Klammern durch ℓ teilbar, denn modulo ℓ sind alle Großbuchstaben gleich den entsprechenden Kleinbuchstaben, so daß die Koeffizienten von $\mathbf{i}, \mathbf{j}, \mathbf{k}$ trivialerweise modulo ℓ verschwinden, und für den Realteil haben wir

$$wW + xX + yY + zZ \equiv w^2 + x^2 + y^2 + z^2 = \ell p \equiv 0 \bmod \ell\,.$$

Somit ist

$$\frac{q\overline{Q}}{\ell} = A + B\mathbf{i} + C\mathbf{j} + D\mathbf{k}$$

eine Quaternion mit ganzzahligen Koeffizienten, und

$$A^2 + B^2 + C^2 + D^2 = \mathrm{N}\left(\frac{q\overline{Q}}{\ell}\right) = \frac{\mathrm{N}(q\overline{Q})}{\ell^2} = \frac{\mathrm{N}(q)\mathrm{N}(Q)}{\ell^2} = mp\,.$$

Dies widerspricht aber der Minimalität von ℓ.

Somit muß $\ell = 1$ sein, und der Satz ist bewiesen. ∎

Satz (LAGRANGE)**:** Jede natürli
höchstens vier Quadraten schreib

Beweis: Wie wir in Kapitel 6, §7
genau dann als Summe von höch
sie Norm einer ganzen Quaterni
daß sich jede Primzahl als Summ
ben läßt (und die Eins natürlich
Multiplikativität der Norm.

§4: Quadratische Formen

Nachdem wir in den vorigen K
spezielle quadratische Form x^2+y
Zahlkörper $\mathbb{Q}[i]$ als auch zu Anwe
haben, wollen wir uns nun etwas
Formen beschäftigen. In den näch
auf quadratische Zahlkörper und

Viele abstrakte Aussagen über qu
wenn wir sie in lineare Algebra ü

$$Ax^2 + Bxy + Cy^2 = \begin{pmatrix} x & y \end{pmatrix}$$

die quadratische Form kann also a
beschrieben werden.

Die Determinante von Q ist AC -
die Zahl $B^2 - 4AC$, die wir in Ka
ments eines quadratisches Zahlkö
hoffen, daß uns die lineare Algeb
über die Werte einer quadratisch
zwischen den Diskriminanten ve
schen Zahlkörpers gibt.

Die reellen Werte, die eine quadr
nicht davon ab, in welcher Basis d
wir können die Basis daher bei B

Das ist zum Beispiel nützlich bei der Frage, wann eine quadratische Form nur positive oder nur negative Werte annimmt:

Definition: Eine symmetrische Matrix $Q \in \mathbb{R}^{2\times 2}$ und die dadurch definierte quadratische Form $f_Q(x,y) = (x\ y)Q\binom{x}{y}$ heißen $\left\{\begin{matrix}\text{positiv}\\\text{negativ}\end{matrix}\right\}$ semidefinit, wenn $f_Q(x,y)\ \left\{\begin{matrix}\geq\\\leq\end{matrix}\right\}\ 0$ für alle $x,y \in \mathbb{R}$. Sie heißen $\left\{\begin{matrix}\text{positiv}\\\text{negativ}\end{matrix}\right\}$ definit, wenn zusätzlich $f(x,y)$ nur für $x = y = 0$ verschwindet.

Ein typisches Beispiel einer positiv definiten quadratischen Form ist x^2+y^2; hier ist Q einfach die Einheitsmatrix. Die negative Einheitsmatrix führt auf die negativ definite Form $-x^2 - y^2$, die Diagonalmatrix mit Einträgen +1 und -1 auf $x^2 - y^2$, was sowohl positive als auch negative Werte annehmen kann.

Beispiele von positiv semidefiniten, aber nicht positiv definiten Formen sind etwa $x^2, (x+y)^2$ oder $(3x-4y)^2$ mit zugehörigen Matrizen

$$Q_1 = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, \quad Q_2 = \begin{pmatrix}1 & 1\\1 & 1\end{pmatrix} \quad \text{und} \quad Q_3 = \begin{pmatrix}3 & -6\\-6 & 4\end{pmatrix}.$$

Für ein allgemeines Kriterium, wann eine Matrix positiv oder negativ (semi-)definit ist, erinnern wir uns an einen Satz aus der linearen Algebra:

Satz: Alle Eigenwerte einer symmetrischen Matrix $Q \in \mathbb{R}^{n\times n}$ sind reell und ihre geometrische Vielfachheit stimmt mit der algebraischen überein. Eigenvektoren zu verschiedenen Eigenwerten stehen senkrecht aufeinander; insbesondere hat $\mathbb{R}^n$ eine Orthonormalbasis aus Eigenvektoren von Q.

Für Leser, die diesen sogenannten *Spektralsatz* nicht kennen, sei kurz ein Beweis für den Spezialfall $n = 2$ skizziert.

Die Matrix $Q = \begin{pmatrix}a & b\\b & c\end{pmatrix}$ hat das

$$\det(Q-\lambda E) = \begin{vmatrix}a-\lambda & \\ b & \end{vmatrix}$$

$$= \lambda^2 - (a+c)\lambda + ac - b^2 = \Big($$

$$= \left(\lambda - \frac{a+c}{2}\right.$$

die Eigenwerte sind also $\lambda_{1/2} =$

Da die Summe zweier Quadrate ist die Wurzel reell, und damit ha

Für $n = 2$ gibt es genau dann Vielfachheit ungleich eins, wen teristischen Polynoms gleich sin Wurzel verschwindet, d.h. $a = c$ eine Diagonalmatrix, der Eigenr auch die geometrische Vielfachhe

Ist $\lambda_1 \neq \lambda_2$ und sind $\vec{a}_1, \vec{a}_2$ Eigenv

$$(Q\vec{a}_1)\cdot\vec{a}_2 = (\lambda_1$$

Andererseits ist (wie man nötige Vektoren $\vec{v}, \vec{w}$ und eine Matrix dem Skalarprodukt $\vec{v}\cdot(Q^T\vec{w})$, wo bezeichnet. Für eine symmetrisch

$$(Q\vec{a}_1)\cdot\vec{a}_2 = \vec{a}_1\cdot(Q\vec{a}_2)$$

Da $\lambda_1 \neq \lambda_2$, können $\lambda_1(\vec{a}_1\cdot\vec{a}_2)$ wenn $\vec{a}_1\cdot\vec{a}_2$ verschwindet, d.h. $\vec{a}$

Auch ein weiteres allgemeines R sich hier einfach und direkt bew

einer $n \times n$-Matrix ist gleich der Determinante und die Summe gleich der Spur, der Summe der Diagonalelemente also.

Für symmetrische 2×2-Matrizen folgt dies sofort aus den obigen Formeln für die beiden Eigenwerte: Bei der Addition fällt die Wurzel weg, so daß wir Summe $a + c$ erhalten, und das Produkt ist nach der dritten binomischen Formel gleich

$$\left(\frac{a+c}{2}\right)^2 - \left[\left(\frac{a-c}{2}\right)^2 + b^2\right] = ac - b^2 = \det Q\,.$$

Ist $\vec{a}_1$ ein Eigenvektor zu λ_1 und $\vec{a}_2$ einer zu λ_2, so können wir jeden Vektor $\binom{x}{y}$ aus $\mathbb{R}^2$ als Linearkombination $\binom{x}{y} = u\vec{a}_1 + v\vec{a}_2$ schreiben. Der Zeilenvektor $(x\ y)$ ist dann die entsprechende Linearkombination $u\vec{a}_1^T + v\vec{a}_2^T$ der zu den $\vec{a}_i$ gehörigen Zeilenvektoren $\vec{a}_i^T$, und

$$(x\ y)Q\begin{pmatrix}x\\y\end{pmatrix} = (u\vec{a}_1^T + v\vec{a}_2^T)Q(u\vec{a}_1 + v\vec{a}_2)$$

$$= (u\vec{a}_1^T + v\vec{a}_2^T)\Big(uQ\vec{a}_1 + vQ\vec{a}_2\Big) = (u\vec{a}_1^T + v\vec{a}_2^T)\Big(u\lambda_1\vec{a}_1 + v\lambda_2\vec{a}_2\Big)$$

$$= \lambda_1 u^2\Big(\vec{a}_1^T\vec{a}_1\Big) + \lambda_2 uv\Big(\vec{a}_1^T\vec{a}_2\Big) + \lambda_1 uv\Big(\vec{a}_2^T\vec{a}_1\Big) + \lambda_2 v^2\Big(\vec{a}_2^T\vec{a}_2\Big)\,.$$

Das Matrixprodukt $\vec{a}_i^T\vec{a}_j$ ist gleich dem üblichen Skalarprodukt $\vec{a}_i \cdot \vec{a}_j$; da die a_i aufeinander senkrecht stehen, verschwindet es für $i \neq j$, d.h.

$$(x\ y)Q\begin{pmatrix}x\\y\end{pmatrix} = \lambda_1 u^2\vec{a}_1 \cdot \vec{a}_1 + \lambda_2 v^2\vec{a}_2 \cdot \vec{a}_2\,,$$

wobei die Skalarprodukte der $\vec{a}_i$ mit sich selbst natürlich positiv sind. Falls wir $\vec{a}_1$ und $\vec{a}_2$ als Einheitsvektoren wählen, sind sie eins und können ganz weggelassen werden.

Damit ist klar, daß die quadratische Form genau dann nur nichtnegative Werte annimmt, wenn λ_1 und λ_2 beide positiv sind; genau dann, wenn beide negativ sind, nimmt sie nur nichtpositive Werte an. Die Matrix Q und die zugehörige quadratische Form sind also genau dann positiv *bzw.* negativ semidefinit, wenn beide Eigenwerte ≥ 0 *bzw.* ≤ 0 sind. Sie sind positiv *bzw.* negativ definit, wenn beide echt positiv *bzw.* negativ sind.

Für eine positiv oder negativ sem
minante ≥ 0 sein; bei einer defi
sie positiv oder negativ definit ist
beiden Eigenwerte (falls $\neq 0$) dass
das Vorzeichen ihrer Summe, der
positiv ist, müssen a und c dasse
gleich der Spur der Matrix ist, fol

Lemma: *a)* Eine symmetrische
oder negativ definit, wenn ihre D
definit, wenn der Eintrag links obe
definit.
b) Die quadratische Form $Ax^2 + B$
ihre Diskriminante $B^2 - 4AC$ n
positiv, sonst negativ definit.

So nützlich der Wechsel zu eine
Fall auch war, für die meisten za
nur solche Basiswechsel helfen, d
zahlige Punkte überführen. Hier g

Lemma: Die lineare Abbildung

$$\varphi\colon \begin{cases} \mathbb{R} \\ \begin{pmatrix} x \\ y \end{pmatrix} \end{cases}$$

definiert genau dann eine Bijekti
Matrix A ganzzahlig sind und de

Beweis: Da die Spaltenvektoren
$\binom{1}{0}$ und $\binom{0}{1}$ sind, ist klar, daß $\varphi($
Einträge von M ganzzahlig sind.
$\varphi^{-1}(\mathbb{Z}^2) \subseteq \mathbb{Z}^2$ sein, d.h. auch M^{-}
In diesem Fall sind $\det M$ und d
eins, also ist $\det M = \pm 1$.

Hat umgekehrt eine Matrix M mit ganzzahligen Einträgen Determinante ± 1, so hat auch M^{-1} ganzzahlige Einträge, denn die Spaltenvektoren von M^{-1} sind die Lösungen der linearen Gleichungssysteme $M\binom{x}{y} = \binom{1}{0}$ und $M\binom{x}{y} = \binom{0}{1}$, die wir nach der CRAMERschen Regel ausdrücken können durch Brüche mit ganzzahligen Zählern und det M im Nenner. ∎

Setzen wir für so eine Matrix M das Bild $M\binom{x}{y}$ an Stelle von $\binom{x}{y}$ in die quadratische Form ein, erhalten wir das Ergebnis

$$\left(M\begin{pmatrix}x\\y\end{pmatrix}\right)^T \cdot Q \cdot M\begin{pmatrix}x\\y\end{pmatrix} = (x\ \ y)\left(M^TQM\right)\begin{pmatrix}x\\y\end{pmatrix},$$

das wir auch erhalten hätten, wenn wir $\binom{x}{y}$ in die quadratische Form zur Matrix M^TQM eingesetzt hätten. Da $\binom{x}{y} \mapsto M\binom{x}{y}$ eine Bijektion von $\mathbb{Z}^2$ nach $\mathbb{Z}^2$ definiert, nehmen die quadratischen Formen zu Q und zu M^TQM also dieselben Werte an. Deshalb definieren wir

Definition: Die quadratischen Formen mit Matrizen Q_1 und Q_2 heißen *äquivalent*, wenn es eine Matrix M mit ganzzahligen Einträgen und det $M = \pm 1$ gibt, so daß $Q_2 = M^TQ_1M$.

Lemma: Zwei äquivalente quadratische Formen haben dieselbe Diskriminante.

Beweis: Bis auf den Faktor -4 ist die Diskriminante gleich der Determinante der Matrix und $\det Q_2 = \det M^T \cdot \det Q_1 \cdot \det M = \det Q_1$, da $\det M = \det M^T = \pm 1$ ist. ∎

§5: Kettenbruchentwicklung quadratischer Irrationalitäten

Die rationalen Zahlen sind genau diejenigen reellen Zahlen, deren Kettenbruchentwicklung nach endlich vielen Schritten abbricht. Wir wollen sehen, daß wir auch quadratische Irrationalitäten, d.h. Elemente eines quadratischen Zahlkörpers, die nicht in $\mathbb{Q}$ liegen, durch ihre Kettenbruchentwicklung charakterisieren können.

In den Beispielen der Kettenbruch
wir in Kapitel 5 auf periodische
charakteristisch für quadratische

Nach der Formel am Ende von §
aus dem Algorithmus zur Kettenb

$$\alpha = \frac{\alpha_n}{\alpha_n}$$

wobei p_n und q_n Zähler und Nen

$$M = \begin{pmatrix} p_{n-2} & p_{n-1} \\ q_{n-2} & q_{n-1} \end{pmatrix} \quad \text{ist}$$

die Vektoren $\binom{\alpha}{1}$ und $M\binom{\alpha_n}{1}$ sin

Als quadratische Irrationalität ge
$A\alpha^2 + B\alpha + C = 0$; der Vektor $\binom{\alpha}{1}$
$Ax^2 + Bxy + Cy^2$ annulliert. Da
Vielfachen von dieser Form annu
$\binom{\alpha}{1}$ proportionalen Vektor $M\binom{\alpha_n}{1}$

Die Matrix zur quadratischen Fo
aus dem vorigen Paragraphen w
$M\binom{\alpha_n}{1}$ dann die quadratische Gle
Nach Kapitel 5, §2 ist $\det M = p$
neue quadratische Form ist also
besondere dieselbe Diskriminant
minante wie α, denn da die Multi
$\mathbb{Z}^2 \to \mathbb{Z}^2$ definiert, sind die Eintr
teilerfremd, wenn es die von M^T

Dies ist ein wesentlicher Schritt f

Satz (LAGRANGE $\sim$1766): Die
tionalen Zahl α wird genau dann
Irrationalzahl ist.

Beweis: Angenommen, α hat eine
Dann gibt es ein n und ein $k > 0$,

am Ende von §2 von Kapitel 5 ist daher

$$\alpha = \frac{\alpha_n p_{n-2} + p_{n-1}}{\alpha_n q_{n-2} + q_{n-1}} = \frac{\alpha_{n+k} p_{n+k-2} + p_{n+k-1}}{\alpha_{n+k} q_{n+k-2} + q_{n+k-1}} = \frac{\alpha_n p_{n+k-2} + p_{n+k-1}}{\alpha_n q_{n+k-2} + q_{n+k-1}}.$$

Daraus folgt die Gleichheit von $(\alpha_n p_{n-2} + p_{n-1})(\alpha_n q_{n+k-2} + q_{n+k-1})$ und $(\alpha_n q_{n-2} + q_{n-1})(\alpha_n p_{n+k-2} + p_{n+k-1})$, und ausmultipliziert wird dies zu einer quadratischen Gleichung für α_n. Der Koeffizient von α_n^2 ist $p_{n-2}q_{n+k-2} + q_{n-2}p_{n+k-2}$, was als Summe positiver Zahlen nicht null sein kann; wir haben also eine echte quadratische Gleichung. Somit läßt sich α_n in der Form $\alpha = r + s\sqrt{D}$ schreiben, und damit auch

$$\alpha = \frac{\alpha_n p_{n-2} + p_{n-1}}{\alpha_n q_{n-2} + q_{n-1}}.$$

Umgekehrt sei $\alpha = r + s\sqrt{D}$ mit quadratfreiem D eine quadratische Irrationalität, die der Gleichung $A_0\alpha^2 + B_0\alpha + C_0 = 0$ genüge. Dann zeigt die Konstruktionsvorschrift für die α_n, daß auch diese Zahlen sowie ihre Inversen in entsprechender Form geschrieben werden können und damit Gleichungen der Form

$$A_n\alpha_n^2 + B_n\alpha_n + C_n = 0$$

genügen. Um diese Gleichung zu bestimmen, betrachten wir die Funktion $f(x) = A_0x^2 + B_0x + C_0$, die für $x = \alpha$ verschwindet, setzen

$$\alpha = \frac{\alpha_n p_{n-2} + p_{n-1}}{\alpha_n q_{n-2} + q_{n-1}}$$

ein und multiplizieren mit dem Hauptnenner. Zumindest für die Koeffizienten A_n und C_n ergeben sich einigermaßen erträgliche Formeln:

$$A_n = A_0p_{n-1}^2 + B_0p_{n-1}q_{n-1} + C_0q_{n-1}^2 = q_{n-1}^2 f\left(\frac{p_{n-1}}{q_{n-1}}\right)$$

und

$$C_n = A_0p_{n-2}^2 + B_0p_{n-2}q_{n-2} + C_0q_{n-2}^2 = q_{n-2}^2 f\left(\frac{p_{n-2}}{q_{n-2}}\right).$$

Da f eine quadratische Funktion ist, führt die TAYLOR-Entwicklung um α auf die Formel

$$f\left(\frac{p_{n-1}}{q_{n-1}}\right) = f(\alpha) + f'(\alpha)\left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right) + \frac{f''(\alpha)}{2}\left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right)^2.$$

Hierbei ist $f(\alpha) = 0$, und $\left|\alpha - \frac{p_n}{q_n}\right.$

$$|A_n| \leq |f$$

Genauso zeigt man die Ungleich
sind die Beträge der Koeffiziente
von n unabhängige Konstante.

Wie wir oben gesehen haben, hat
Diskriminante $\Delta = B_n^2 - 4A_nC$
folgen aus der obigen Schranken
$B_n^2 = \Delta + 4A_nC_n$, so daß auch d

Somit gibt es nur endlich viele Tr
lich viele verschiedene Werte für
$k \geq 1$ geben derart, daß $\alpha_n = \alpha_{n+}$
wird spätestens ab der n-ten Stell

Der gerade bewiesene Satz chara
entwicklung periodisch *wird;* er
wicklung einer quadratischen Irra
und in der Tat kennen wir Beispie
bei denen das nicht der Fall ist. F
entwicklung brauchen wir also no

Satz: Die Kettenbruchentwicklu
ist genau dann rein periodisch,
Element $\overline{\alpha}$ zwischen -1 und 0 lie

Beweis: Sei zunächst $\alpha > 1$ und –
reinen Periodizität der Folge der
die konjugierten Elemente $\overline{\alpha}_{i+1}$ au
zweier Koeffizienten auch auf die

Die Gleichung $\alpha = c_0 + \alpha_1$ wird
Konjugation zu $\overline{\alpha} = c_0 + \overline{\alpha}_1$. Da
und 0 liegt, ist somit $0 < -\overline{\alpha}_1$

$c_0 = [\alpha] \geq 1$ folgt außerdem -1

Wir wollen induktiv zeigen, daß auch für alle $i > 0$ gilt

$$c_i = [-\overline{\alpha}_{i+1}] \quad \text{und} \quad -1 < \frac{1}{\overline{\alpha}_{i+1}} < 0\,.$$

Dazu nehmen wir an, dies gelte für $i-1$. Aus

$$\frac{1}{\alpha_i} = c_i + \alpha_{i+1} \quad \text{und} \quad -1 < \frac{1}{\overline{\alpha}_i} < 0$$

folgt wie im Fall $i = 0$, daß $c_i = [-\overline{\alpha}_{i+1}]$ ist, und da die Koeffizienten c_i für $i > 0$ bei jeder Kettenbruchentwicklung mindestens gleich eins sind, folgt auch die Ungleichung für $1/\overline{\alpha}_{i+1}$ genau wie dort.

Daraus folgt nun leicht die Periodizität der Kettenbruchentwicklung von α: Wir wissen bereits, daß sie periodisch *wird;* es gibt also irgendeinen Index $m \geq 0$ und eine Periode k, so daß $\alpha_{n+k} = \alpha_n$ für alle $n \geq m$. Wir betrachten das minimale m mit dieser Eigenschaft. Die Kettenbruchentwicklung von α ist genau dann rein periodisch, wenn $m = 0$ ist. Für $m \geq 1$ können wir aber aus $\alpha_{m+k} = \alpha_m$ und $c_{m+k} = c_m$ folgern, daß auch $c_{m+k-1} = [-\overline{\alpha}_{m+k}] = [-\overline{\alpha}_m] = c_{m-1}$ ist. Aus den Gleichungen

$$\frac{1}{\alpha_{m+k-1}} = c_{m+k-1} + \alpha_{m+k} \quad \text{und} \quad \frac{1}{\alpha_{m-1}} = c_{m-1} + \alpha_m$$

folgt dann aber, daß auch $\alpha_{m-1+k} = \alpha_{m-1}$ ist, im Widerspruch zur Minimalität von m. Somit ist $m = 0$, die Kettenbruchentwicklung von α also rein periodisch.

Umgekehrt habe α eine rein periodische Kettenbruchentwicklung der Periode k mit Koeffizienten $c_0, c_1, \ldots$. Wegen $c_k = c_0$ ist dabei auch c_0 positiv, denn alle c_n mit $n > 0$ müssen ja positiv sein. Somit ist insbesondere $\alpha > 1$.

Um zu sehen, daß $\overline{\alpha}$ zwischen -1 und 0 liegt, beachten wir, daß $\overline{\alpha}$ dieselbe quadratische Gleichung erfüllt wie α. Da diese Gleichung genau zwei Nullstellen hat und α größer als eins ist, genügt es, wenn wir zeigen, daß diese Gleichung im Intervall $(-1,\ 0)$ eine Nullstelle hat. Das wiederum folgt aus dem Zwischenwertsatz, wenn wir zeigen können, daß die quadratische Funktion auf der linken Seite an den Stellen 0 und -1 Werte mit entgegengesetzten Vorzeichen annimmt.

Für $k = 1$ ist $\alpha = c_0 + \alpha_1 = c_0 + \frac{1}{\alpha}$ Funktion $x^2 - c_0 x - 1$ nimmt an $x = 1$ den Wert $c_0 > 0$; somit g beiden Punkten.

Für $k \geq 2$ verwenden wir die be aus Kapitel 5, §2, und beachten, Gleichung

$$\alpha = \frac{\alpha_k p_{k-2} + p}{\alpha_k q_{k-2} + q}$$

Überkreuzmultiplikation macht d

$$q_{k-1}\alpha^2 + (q_{k-2}$$

Hier nimmt die quadratische Fun und an der Stelle -1 den Wert

$$q_{k-1} - (q_{k-2} - p_{k-2}) - p_{k-1}$$

Dieser ist positiv, da sowohl die Fo der Konvergenten von α monoton

§6: Die Pellsche Gleichung

Im letzten Kapitel hatten wir gese die Gleichung $x^2 - Dy^2 = \pm 1$ graphen ist die Lösung der PELL $(x, y) \in \mathbb{Z}^2$ oder – da es auf das Vo $(x, y) \in \mathbb{N}^2$.

Faktorisierung der linken Seite d

$$(x + y\sqrt{D})$$

und damit ist

$$x - y\sqrt{D} = \frac{1}{x + y\sqrt{D}} =$$

Wegen der Positivität der rechten Seite ist $\frac{x}{y} > \sqrt{D}$, also folgt

$$\left|x - y\sqrt{D}\right| = x - y\sqrt{D} = \frac{1}{y^2\left(\frac{x}{y} + \sqrt{D}\right)} < \frac{1}{2y^2\sqrt{D}} < \frac{1}{2y^2}\,.$$

Nach dem Satz aus Kapitel 5, §3 muß $\frac{x}{y}$ somit eine Konvergente der Kettenbruchentwicklung von $\sqrt{D}$ sein.

Umgekehrt liefert aber nicht jede Konvergente der Kettenbruchentwicklung von $\sqrt{D}$ eine Lösung der PELLschen Gleichung: Beispielsweise hat $\sqrt{13} = [3, 1, 1, 1, 1, 6, \dots]$ die Brüche

$$\frac{4}{1},\quad \frac{7}{2},\quad \frac{11}{3},\quad \frac{18}{5},\quad \frac{119}{33}$$

als seine ersten Konvergenten, aber

$$4^2 - 13 = 3,\quad 7^2 - 13\cdot 2^2 = -3,\quad 11^2 - 13\cdot 3^2 = 4$$
$$18^2 - 13\cdot 5^2 = -1 \quad\text{und}\quad 119^2 - 13\cdot 33^2 = 4\,.$$

Zumindest *a priori* ist nicht klar, ob es überhaupt eine Konvergente gibt, die auf eine Lösung der PELLschen Gleichung führt.

Um hier mehr zu erfahren, müssen wir uns die Kettenbruchentwicklung von $\sqrt{D}$ genauer ansehen. Dabei sei D im folgenden stets eine quadratfreie natürliche Zahl.

Das konjugierte Element zu $\sqrt{D}$ ist $-\sqrt{D}$ und somit kleiner als -1; die Kettenbruchentwicklung von $\sqrt{D}$ ist also nicht rein periodisch. Betrachten wir aber $\alpha = \lfloor\sqrt{D}\rfloor + \sqrt{D}$, so ist natürlich $\alpha > 1$. und $\overline{\alpha} = \lfloor\sqrt{D}\rfloor - \sqrt{D}$ liegt zwischen -1 und 0. Somit hat α eine rein periodische Kettenbruchentwicklung. Die Periode sei k und die Koeffizienten seien $c_0, c_1, \dots$.

Die Kettenbruchentwicklung von $\sqrt{D} = \alpha - \lfloor\sqrt{D}\rfloor$ unterscheidet sich von der von α nur im ganzzahligen Anteil. Dieser ist im Falle von α gleich $2\lfloor\sqrt{D}\rfloor$, im Falle von $\sqrt{D}$ nur $\lfloor\sqrt{D}\rfloor$. Danach folgen in beiden Fällen die c_i mit $i \geq 1$. Wegen $c_k = c_0 = 2\lfloor\sqrt{D}\rfloor$ gilt daher

Satz: Ist D eine quadratfreie nati
der Koeffizienten der Kettenbruch
Bezeichnet k die Periode, so ist c

Bezeichnet p_n/q_n wieder die n-t
wicklung, so ist nach der schon o

$$\sqrt{D} = \frac{\alpha}{\alpha}$$

Ist speziell $n = rk$ ein Vielfach
tenbruchentwicklung mit Koeffiz
gerade bewiesenen Satz stimmt da
d.h.

$$\frac{1}{\alpha_{rk}} = c_0 + \sqrt{}$$

Einsetzen in die obige Formel fü

$$\sqrt{D} = \frac{\alpha_{rk}p_{rk-2} + p_{rk-}}{\alpha_{rk}q_{rk-2} + q_{rk-}}$$

oder

$$(q_{rk-2} + q_{rk-1}c_0)\sqrt{D} + q_{rk-1}$$

Durch Koeffizientenvergleich fol

$$p_{rk-2} = q_{rk-1}D - p_{rk-1}c_0$$

Setzen wir dies ein in die aus Kap

$$p_m q_{m-1} - q_$$

mit $m = rk - 1$, erhalten wir die

$$p_{rk-1}^2 - p_{rk-1}q_{rk-1}c_0$$
$$= p_{rk-1}^2 - D$$

Im Falle einer geraden Periode
$r \in \mathbb{N}$ eine Lösung der PELLsch
liefern nur die geradzahligen Vie
ungeradzahligen zu Lösungen de

Im Eingangsbeispiel $D = 13$ zeigt eine genauere Rechnung, daß sich die Koeffizienten $1, 1, 1, 1, 6$ periodisch wiederholen, wir haben also die ungerade Periode fünf. Damit liefern die vierte, vierzehnte, vierundzwanzigste Konvergente der Kettenbruchentwicklung Lösungen der Gleichung $x^2 - Dy^2 = -1$, was wir für die vierte bereits nachgerechnet haben. Lösungen der PELLschen Gleichung liefern die neunte, neunzehnte *usw.* Konvergente. Die neunte Konvergente ist

$$[3, 1, 1, 1, 1, 6, 1, 1, 1] = \frac{649}{180},$$

und in der Tat ist

$$649^2 - 13 \cdot 180^2 = 421\,201 - 13 \cdot 32\,400 = 421\,201 - 421\,200 = 1\,.$$

Allgemein haben wir gezeigt, daß die PELLsche Gleichung für jedes quadratfreie D eine Lösung hat; zusammen mit dem Satz aus Kapitel 6, §6 folgt, daß die Einheitengruppe eines jeden reellquadratischen Zahlkörpers unendlich ist und daß es speziell für die Gruppe der Einheiten mit Norm eins (der sogenannten Einseinheiten) ein Element $\alpha \in \mathcal{O}_D$ gibt, so daß jede Einseinheit in der Form $\pm\alpha^r$ mit einem $r \in \mathbb{Z}$ geschrieben werden kann. α ist die kleinste Einseinheit größer eins.

Natürlich kann auch α in der Form $p_n + q_n\sqrt{D}$ geschrieben werden, wobei p_n/q_n eine Konvergente der Kettenbruchentwicklung von $\sqrt{D}$ ist. Da Zähler und Nenner der Konvergenten strikt monoton ansteigen mit n, handelt es sich hier um die *erste* Konvergente p_n/q_n, für die $p_n^2 - Dq_n^2 = 1$ ist.

Mit Rechnungen, die sehr ähnlich zu den obigen sind, kann man zeigen, daß die oben gefundenen Indizes m mit $p_m^2 - Dq_m^2 = \pm 1$ tatsächlich die einzigen sind mit dieser Eigenschaft. Da wir schon viel mit Kettenbrüchen gerechnet haben und es noch viele andere interessante Teilgebiete der Zahlentheorie zu entdecken gilt, möchte ich auf diese Rechnungen verzichten.

Wer sich für diese Rechnungen interessiert, findet sie zum Beispiel in

WINFRIED SCHARLAU, HANS OPOLKA: Von Fermat bis Minkowski – Eine Vorlesung über Zahlentheorie und ihre Entwicklung, *Springer,* 1980

im Kapitel über LAGRANGE im (nur im Inh
der Fermatschen (Pellschen) Gleichung al
den obigen Beweis verstanden hat, muß r
unterschiedlichen Bezeichnungen: Was h
hier $1/\alpha_n$. Die hiesigen c_n werden dort r

Wenn wir dieses Ergebnis akzept
eines jeden reellquadratischen Za
zumindest für $D \not\equiv 1 \bmod 4$: Da
Einheiten genau den ganzzahlige
$x^2 - Dy^2 = \pm 1$ entsprechen. Ist k
lung von $\sqrt{D}$ und p/q die $(k-1$
die Grundeinheit, und jede ander
$r \in \mathbb{Z}$ schreiben. Für gerades k s
rades k bekommen wir für gerad
der Norm -1.

Bleibt die Frage, für welche D d
Diese Frage muß nicht nur in die
Es handelt sich hier um eines der
die trotz jahrhundertelanger Bem

Die zweite Frage ist: Was passi
sen, sind dann auch die Zahlen $\frac{1}{2}($
x, y ganz, es kann also auch Ein
haben wir beim Eingangsbeispi
nengelernt: Für die dritte Konve
N $\left(\frac{1}{2}(11 + 3\sqrt{13}\right) = 1$. Wie eine
genau dann möglich, wenn $D \equiv$
che D. Wenn es eine Grundeinh
Potenz in $\mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$, der Kettenb
dritte Potenz der Grundeinheit. E
in §16, 5D des Buchs

HELMUT HASSE: Vorlesungen üb

Kapitel 8
Quadratische Reste

§1: Das Legendre-Symbol

Definition: Für eine Primzahl p und eine nicht durch p teilbare natürliche Zahl a ist das LEGENDRE-Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{falls es ein } x \in \mathbb{N} \text{ gibt mit } x^2 \equiv a \bmod p \\ -1 & \text{sonst} \end{cases}$$

Im ersten Fall bezeichnen wir a als *quadratischen Rest* modulo p, andernfalls als quadratischen Nichtrest. Für eine durch p teilbare Zahl a setzen wir $\left(\frac{a}{p}\right) = 0$.

Sind a, b zwei modulo p kongruente natürliche Zahlen, so ist offensichtlich $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Wir haben daher auch für $a \in \mathbb{F}_p^\times$ ein wohldefiniertes LEGENDRE-Symbol $\left(\frac{a}{p}\right)$, das durch die Vorschrift $\left(\frac{0}{p}\right) = 0$ auf ganz $\mathbb{F}_p$ fortgesetzt wird.

ADRIEN-MARIE LEGENDRE (1752–1833) wurde in Toulouse oder Paris geboren; jedenfalls ging er in Paris zur Schule und studierte Mathematik und Physik am dortigen Collège Mazarin. Ab 1775 lehrte er an der Ecole Militaire und gewann einen Preis der Berliner Akademie für eine Arbeit über die Bahn von Kanonenkugeln. Andere Arbeiten befaßten sich mit der Anziehung von Ellipsoiden und der Himmelsmechanik. Ab etwa 1785 publizierte er auch Arbeiten über Zahlentheorie, in denen er z.B. das quadratische Reziprozitätsgesetz bewies sowie die Irrationalität von π und π^2.

Lemma: Das LEGENDRE-Symb
phismus

$$\left(\frac{\cdot}{p}\right) : \begin{cases} \mathbb{F}^\times \\ \end{cases}$$

Für $p = 2$ ist dies der triviale Ho
surjektiv. Insbesondere gibt es da
Nichtreste.

Beweis: Für $p = 2$ ist $\mathbb{F}_2^\times = \{1\}$, u

Sei nun p ungerade. Der Homom

$$\begin{cases} \mathbb{F}_ \\ \end{cases}$$

hat den Kern $\{+1, -1\}$, also best
quadratischen Resten.

Trivialerweise ist das Produkt z
quadratischer Rest. Ist $a = x^2$ ein
so ist auch ab ein quadratischer
$b = (yx^{-1})^2$ ein quadratischer Re
folgt, daß sich jeder quadratische
wobei c ein quadratischer Rest is
quadratischer Nichtreste ein quad
wobei c und d Quadrate in $\mathbb{F}_p^\times$ si

Lemma (EULER): Ist p eine ung
so ist $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Beweis: g sei ein erzeugendes El
jede Potenz g^r mit geradem r ei
$\frac{p-1}{2}$ verschiedene solcher Potenz
schen Reste. Somit ist g^r genau
gerade ist.

Da g ein erzeugendes Element ist, kann $g^{(p-1)/2}$ nicht gleich eins sein; da nach dem kleinen Satz von FERMAT aber sein Quadrat $g^{p-1} = 1$ ist, folgt $g^{(p-1)/2} = -1$. Für $a = g^r$ ist somit

$$a^{\frac{p-1}{2}} = (g^r)^{\frac{p-1}{2}} = \left(g^{\frac{p-1}{2}}\right)^r = (-1)^r$$

genau dann gleich eins, wenn a ein quadratischer Rest ist, und -1 sonst. ∎

Korollar: Für ungerades p ist

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases}.$$

∎

§2: Das quadratische Reziprozitätsgesetz

Quadratisches Reziprozitätsgesetz: Für zwei verschiedene ungerade Primzahlen p, q ist

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \quad \text{und} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Zum *Beweis* betrachten wir ein zum Nullpunkt symmetrisches Vertretersystem von $\mathbb{F}_p^\times$ in $\mathbb{Z}$, nämlich

$$R = \{-h, \ldots, -1, 1, \ldots, h\} \quad \text{mit} \quad h = \frac{p-1}{2}.$$

Weiter sei $S = \{q, 2q, \ldots, hq\}$. Da p und q teilerfremd sind, haben zwei verschiedene Elemente von S verschiedene Restklassen modulo p.

1. Schritt (GAUSS): q sei eine beliebige Primzahl und $p \neq q$ eine ungerade Primzahl. Dann ist $\left(\frac{q}{p}\right) = (-1)^m$, wobei m die Anzahl jener Elemente von S bezeichnet, die modulo p kongruent sind zu einem negativen Element von R.

Beweis: $a_1, \ldots, a_m$ seien die negativen Elemente von R, die zu Elementen aus S kongruent sind, $b_1, \ldots, b_n$ die positiven. Dann ist

$$a_1 \cdots a_m b_1 \cdots b_n \equiv \prod_{i=1}^{h}(iq) = h!q^h \bmod p.$$

Natürlich sind a_i und a_j für $i \neq$ auch b_i und b_j. Außerdem kann au einerseits $a_i + b_j = 0$, andererse so daß $a_i \equiv kq$ und $b_j \equiv \ell q$ mod was nicht möglich ist, denn $k + \ell$ der a_i und der b_j genau die Zahle

$$a_1 \cdots a_m b_1 \cdot$$

Vergleich mit der obigen Kongrue ist, also nach dem vorigen Lemm

2. Schritt (GAUSS): Für zwei ung

$$\left(\frac{q}{p}\right) = (-1)^M \quad \text{mit} \quad M = \sum_i$$

Im *Beweis* sei zunächst auch noc sei $r_i = iq - p \cdot \left[\frac{iq}{p}\right]$; dann ist 0 iq modulo p kongruent ist zu eine $r_i = p + a_j$; falls $r_i \equiv b_j > 0$ ist

$$\sum_{i=1}^{h} iq = p\sum_{i=1}^{h}\left[\frac{iq}{p}\right] + \sum_{i=1}^{m}(a_i + p)$$

Andererseits ist

$$\sum_{i=1}^{h} iq = \frac{h(h+1)}{2} \cdot q = \frac{1}{2}$$

Außerdem wissen wir aus dem er

$$\{-a_1, \ldots, -a_m, b$$

ist, d.h.

$$-\sum_{i=1}^{m} a_i + \sum_{i=1}^{n} b_i = \sum_i$$

und damit ist $\sum_{i=1}^{n} b_i = \frac{p^2-1}{8} + \sum_{i=1}^{m} a_i$. Setzen wir das alles in die obige Formel ein, erhalten wir die Beziehung

$$\frac{p^2-1}{8} \cdot q = (M+m)p + \frac{p^2-1}{8} + 2\sum_{i=1}^{m} a_i$$

oder

$$\frac{p^2-1}{8} \cdot (q-1) = (M+m)p + 2\sum_{i=1}^{m} a_i \,.$$

Im Falle einer ungeraden Primzahl q steht rechts eine gerade Zahl; damit muß auch $M+m$ gerade sein, d.h. $(-1)^M = (-1)^m$, und die Behauptung folgt aus dem ersten Schritt.

Für $q = 2$ ist $M = 0$, da $\left[\frac{2i}{p}\right]$ für alle $i \le h$ verschwindet. Modulo zwei wird die obige Beziehung daher zu

$$\frac{p^2-1}{8} \equiv mp \equiv m \bmod 2\,,$$

so daß die Behauptung auch hier aus dem ersten Schritt folgt. ∎

3. Schritt (EISENSTEIN): p und q seien ungerade Primzahlen,

$$h = \frac{p-1}{2}, \quad k = \frac{q-1}{2}, \quad M = \sum_{i=1}^{h} \left[\frac{iq}{p}\right] \quad \text{und} \quad N = \sum_{i=1}^{k} \left[\frac{ip}{q}\right] .$$

Dann ist $M + N = hk$.

Beweis: Im Innern des Rechtecks mit Ecken $(0,0), (\frac{p}{2},0), (0,\frac{q}{2})$ und $(\frac{p}{2},\frac{q}{2})$ liegen hk Gitterpunkte, nämlich die Punkte (i,j) mit $1 \le i \le h$ und $1 \le j \le k$.

Die Diagonale des Rechtecks liegt auf der Geraden $y = \frac{q}{p}x$ und enthält keine Gitterpunkte. Unterhalb der Diagonalen liegen $\left[\frac{iq}{p}\right]$ Punkte mit Abszisse i, insgesamt also M Punkte. Darüber liegen $\left[\frac{ip}{q}\right]$ Punkte mit Ordinate i, insgesamt also N Punkte. Somit ist $hk = M + N$. ∎

Zum *Beweis* des quadratischen R
nur noch alles kombinieren: Nach
ist

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^M \cdot (-1)^N =$$

CARL F
liche Be
Geomet
ometrie
Statistik
rektor d
dem Ph
die erst
Hannov
versität
benutzte
Seine 18
sind auc

FERDIN
genannt
seiner s
der Kin
ren, noc
gen der
1842 las
den er
wichtig
sition u
durch A
er sich i
als Stud

Bemerkung: Die rechten Seiten
Reziprozitätsgesetz lassen sich au
drücken: $(p-1)/2$ ist genau dan
chend für q. Somit ist

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} +1 & \text{falls} \\ -1 & \text{falls} \end{cases}$$

Ist $p = 8r + k$, so ist $p^2 = 64r^2 + 16r + k^2 \equiv k^2 \bmod 16$, also ist $p^2 - 1 \equiv k^2 - 1 \bmod 16$. Für $k = \pm 1$ ist dies null, für $k = \pm 3$ acht. Somit ist

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{falls } p \equiv \pm 1 \bmod 8 \\ -1 & \text{falls } p \equiv \pm 3 \bmod 8 \end{cases}.$$

Das quadratische Reziprozitätsgesetz läßt sich gelegentlich dazu verwenden, um ein LEGENDRE-Symbol einfach zu berechnen. Wenn wir beispielsweise entscheiden wollen, ob sieben ein quadratischer Rest modulo 17 ist, sagt es uns (da $17 \equiv 1 \bmod 4$), daß $\left(\frac{7}{17}\right) = \left(\frac{17}{7}\right)$ ist. Letzteres ist gleich $\left(\frac{3}{7}\right)$, da $17 \equiv 3 \bmod 7$. Hier haben wir zwei Primzahlen, die beide kongruent drei modulo vier sind, also ist $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$, denn die Eins ist natürlich modulo jeder Primzahl ein quadratischer Rest. Also ist sieben modulo 17 ein quadratischer Nichtrest.

Genauso können wir auch leicht feststellen, ob 13 quadratischer Rest modulo 1 000 003 ist: Da $13 \equiv 1 \bmod 4$, ist $\left(\frac{13}{1\,000\,003}\right) = \left(\frac{1\,000\,003}{13}\right)$. Da $1\,000\,003 \equiv 4 \bmod 13$, ist dies gleich $\left(\frac{4}{13}\right)$, und das ist natürlich eins, da $4 = 2^2$ modulo jeder Primzahl ein Quadrat ist. Somit ist auch 13 ein Quadrat modulo 1 000 003.

Das Problem bei dieser Vorgehensweise besteht darin, daß wir normalerweise nicht soviel Glück haben wie hier und als Reduktionen stets Primzahlen erhalten. Wir sollten daher ein quadratisches Reziprozitätsgesetz haben, das auch funktioniert, wenn die beteiligten Zahlen nicht prim sind.

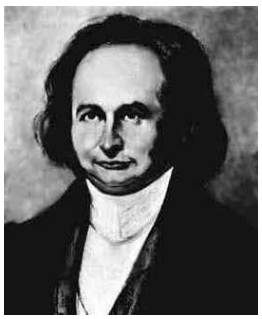
§3: Das Jacobi-Symbol

Wie wir in §1 gesehen haben, definiert das LEGENDRE-Symbol in Bezug auf seinen „Zähler“ einen Homomorphismus; wir können versuchen, es zu erweitern, indem wir dasselbe auch für den „Nenner“ postulieren:

Definition: Ist $n = \prod_{i=1}^{r} p_i^{e_i}$ eine ungerade Zahl und m eine zu n teilerfremde Zahl, so ist das JACOBI-Sy

$$\left(\frac{m}{n}\right) =$$

Falls m und n nicht teilerfremd s



CARL G
Potsdam
und erh
von zw
noch vi
bleiben,
mindest
Studien
chisch
moviert
Etwa gl
daß er a
Königsberg lehren konnte. 1832 wurde er
gesundheitlichen Gründen das rauhe Klim
Italien, danach für den Rest seines Lebens
Arbeiten zur Zahlentheorie und über ellip

Für eine Primzahl n und ein ni
JACOBI-Symbol natürlich mit dem
kann sich fragen, ob man hier v
Dieser ist gerechtfertigt, weil es
zwischen den beiden Symbolen g

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)$$

aber zwei ist offensichtlich kein
müßte es schließlich erst recht qu
dulo fünf sein, aber die entsprec
In der Tat gibt es modulo 15 nur v

Das JACOBI-Symbol gibt daher k
quadratischer Rest ist oder nicht; l
wir sicher sein, daß wir es mit e
haben, denn dann muß ja auch s

des „Nenners“ das LEGENDRE-Symbol gleich -1 sein, während ein quadratischer Rest modulo einer Zahl n erst recht quadratischer Rest modulo eines jeden Teilers von n sein muß.

Die Nützlichkeit des JACOBI-Symbols kommt in erster Linie daher, daß auch dafür das quadratische Reziprozitätsgesetz gilt und es somit zur Berechnung von LEGENDRE-Symbolen verwendet werden kann:

Satz: Für zwei ungerade Zahlen m, n mit ggT$(m, n) = 1$ ist

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \quad \text{und} \quad \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

Beweis: Sei $n = \prod_{i=1}^{r} p_i^{e_i}$ und $m = \prod_{j=1}^{s} q_j^{f_j}$. Nach Definition des JACOBI-Symbols und weil das LEGENDRE-Symbol bei festgehaltenem „Nenner“ einen Homomorphismus definiert, ist dann

$$\left(\frac{n}{m}\right) = \prod_{j=1}^{s}\left(\frac{n}{q_j}\right)^{f_j} = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right)^{e_i f_j} \text{ und } \left(\frac{m}{n}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right)^{e_i f_j}.$$

Nach dem quadratischen Reziprozitätsgesetz aus §2 ist daher

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left((-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}\right)^{e_i f_j} = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\frac{q_j-1}{2}e_i f_j}$$

$$= (-1)^{\left(\sum_{i=1}^{r}\frac{p_i-1}{2}e_i\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}f_j\right)} = \left((-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}e_i}\right)^{\sum_{j=1}^{s}\frac{q_j-1}{2}f_j}.$$

Dies ist genau dann gleich +1, wenn mindestens einer der beiden Exponenten gerade ist; andernfalls ist es gleich -1.

Im Produkt

$$(-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}e_i} = \prod_{i=1}^{r}(-1)^{\frac{p_i-1}{2}e_i}$$

können wir alle Faktoren weglassen, für die e_i gerade ist oder aber $p_i \equiv 1 \bmod 4$. Das Produkt ist also gleich $(-1)^N$ mit

N = Anzahl der Indizes i mit $p_i \equiv 3 \bmod 4$ und e_i ungerade.

Die Faktoren $p_i^{e_i}$ sind genau dan
$p_i \equiv 1 \bmod 4$ oder e_i gerade ist
$p_i^{e_i} \equiv 3 \equiv -1 \bmod 4$. Somit ist a

$$(-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}e_i}$$

Ist dies gleich +1, so ist die rech
ebenfalls +1, andernfalls zeigt d
gleich $(-1)^{(m-1)/2}$ ist. In jedem F
Formel

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)$$

Genauso folgt auch, daß $\left(\frac{2}{m}\right) =$
$m \equiv \pm 1 \bmod 8$ und -1 für $m \equiv$
zahlen kongruent ± 1 modulo ac
das zweier Primzahlen kongruent
Argumentation wie oben zum Zie

Als Anwendung können wir uns ü
eine vorgegebene Zahl a quadratis
verschwindet a und ist somit ein

Für $a = 2$ haben wir gesehen, d
se p mod 8 abhängt; wegen der
reicht es also, wenn wir ungerad
wiesenen Gesetz ist dann

$$\left(\frac{a}{p}\right) = (-$$

Für festes a ist $(a-1)/2$ ein konst
p mod 4, und $\left(\frac{p}{a}\right)$ hängt ab von p
von p mod $4a$, ob a ein quadratis

Betrachten wir als Beispiel den F

$$(-1)^{\frac{(a-1)}{2}\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$$

und

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & \text{falls } p \equiv 1 \bmod 3 \\ -1 & \text{falls } p \equiv 2 \bmod 3 \end{cases}.$$

Somit ist für eine Primzahl $p > 3$

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{falls } p \bmod 12 \in \{1, 11\} \\ -1 & \text{falls } p \bmod 12 \in \{5, 7\} \end{cases}.$$

Für $a = 5$ ist $(a-1)/2 = 2$ gerade, also

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{falls } p \bmod 5 \in \{1, 4\} \\ -1 & \text{falls } p \bmod 5 \in \{2, 3\} \end{cases},$$

§4: Berechnung der modularen Quadratwurzel

Das quadratische Reziprozitätsgesetz zeigt uns schnell, ob die Gleichung $x^2 \equiv a \bmod p$ für eine gegebene Primzahl p und eine ganze Zahl a lösbar ist; es gibt uns aber keinen Hinweis darauf, wie wir diese Lösung finden können. Darum soll es in diesem Paragraphen gehen.

Am einfachsten lassen sich Quadratwurzeln modulo zwei ziehen, denn modulo zwei ist jede Zahl ihre eigene Quadratwurzel. Im folgenden sei daher p eine ungerade Primzahl; wir zerlegen

$$p - 1 = 2^e \cdot q$$

in eine Zweierpotenz 2^e und eine ungerade Zahl q.

Da die multiplikative Gruppe $\mathbb{F}_p^\times$ modulo p zyklisch ist, gibt es ein Element $g \in \mathbb{F}_p^\times$, so daß

$$\mathbb{F}_p^\times = \{g, g^2, \ldots, g^{p-1} = 1\}$$

genau aus den Potenzen von g besteht.

Die Ordnung eines Elements g^r läßt sich leicht berechnen: Da g^{rn} genau dann zu eins wird, wenn $p-1$ den Exponenten rn teilt, ist rn für die Ordnung n das kleinste gemeinsame Vielfache von r und $p-1$. Das kleinste gemeinsame Vielfache ist bekanntlich gleich dem Produkt, dividiert durch den größten gemeinsamen Teiler. Damit ist die Ordnung

$$n = \frac{p-1}{\mathrm{ggT}(r, p-1)}.$$

Speziell für die beiden Elemente

$$y = g^{2^e}$$

folgt, daß y die Ordnung q hat un

Da q und 2^e teilerfremd sind, gibt
Algorithmus ganze Zahlen u, v, s

$$2^e u$$

ist. Hierbei muß v offensichtlich
wäre die Summe auf der linken S

Damit ist

$$g = g^{2^e u + qv}$$

und entsprechend für jedes r

$$g^r =$$

Da es bei Potenzen von y nur au
und bei solchen von z nur auf de
daß sich jedes Element von $\mathbb{F}_p^\times$ in

$$a = y^\alpha z^\beta \quad \text{mit} \quad 0 \leq$$

schreiben läßt.

$a = g^r$ ist genau dann ein quadrati
die beiden Quadratwurzeln sind d
dies allerdings nicht sonderlich nü
denn erstens kennen wir im allgem
zweitens kennen wir auch den E
großes Problem, denn es gibt ef
um sich mögliche Werte für g
diskretes Logarithmenproblem m
wenn die Primzahl p ziemlich kle

Auch der etwas komplizierteren
bekannten) Form $a = y^\alpha z^\beta$ könn
Rest ist: Da v eine ungerade Zahl

vr gerade ist, und das wiederum ist äquivalent dazu, daß $\beta \equiv vr \bmod 2^e$ eine gerade Zahl ist.

$a^q = y^{\alpha q} z^{\beta q} = z^{\beta q}$ ist eine Potenz von z; es gibt also eine ganze Zahl k zwischen null und $2^e - 1$, so daß $a^q z^k = 1$ ist, nämlich

$$k = -\beta q \bmod 2^e \in \{0, 1, 2, \ldots, 2^e - 1\} ,$$

und auch diese Zahl ist genau dann gerade, wenn a quadratischer Rest ist. Mit dieser Zahl k sind dann

$$x = \pm a^{(q+1)/2} z^{k/2}$$

die beiden Quadratwurzeln des quadratischen Rests a, denn

$$x^2 = a^{q+1} z^k = a(a^q z^k) = a .$$

Sobald wir den Wert $z^{k/2}$ kennen, können wir also die Quadratwurzeln von a bestimmen, und wir wir gleich sehen werden, läßt sich dieser Wert erheblich schneller berechnen als ein diskreter Logarithmus.

Zumindest für die „Hälfte“ aller Primzahlen haben wir damit überhaupt kein Problem: Eine ungerade Zahl hat bei Division durch vier offensichtlich entweder Rest eins oder Rest drei; wir betrachten zunächst den Fall, daß $p \equiv 3 \bmod 4$. (Solche Primzahlen werden in der Kryptologie gelegentlich als BLUMsche Primzahlen bezeichnet.)

Ist $p \equiv 3 \bmod 4$, so ist $p - 1 \equiv 2 \bmod 4$, d.h. $p - 1$ ist zwar durch zwei, nicht aber durch vier teilbar. Mithin ist $p - 1 = 2q$ mit einer ungeraden Zahl q, d.h. der oben definierte Exponent e ist eins. Damit kommen für k nur die Werte $k = 0$ und $k = 1$ in Frage, und für einen quadratischen Rest a muß $k = 0$ sein. Dann sind sowohl z^k als auch $z^{k/2}$ gleich eins, also sind die beiden Wurzeln aus a einfach

$$x_{1/2} = \pm a^{(q+1)/2} = \pm a^{(\frac{p-1}{2}+1)/2} = \pm a^{(p+1)/4} ,$$

was sich leicht berechnen läßt. Die Richtigkeit dieser Formel läßt sich auch direkt nachprüfen, denn nach dem Lemma von EULER ist

$$x_{1/2}^2 = a^{(p+1)/2} = a \cdot a^{(p-1)/2} = a \cdot \left(\frac{a}{p}\right) .$$

Ist also a ein quadratischer Rest, so ist $x_{1/2}^2 = a$; wendet man die Formel fälschlicherweise auf einen quadratischen Nichtrest an, ist $x_{1/2}^2 = -a$.

Für $p \equiv 1 \bmod 4$ ist entweder p
mindest im letzteren Fall können
die Quadratwurzeln aufstellen: In
$p - 1$ ist zwar durch vier, nicht al

$$p - 1 = 4q = 2^2 q \quad \text{m}$$

d.h. $e = 2$. Daher kann k nun d
quadratische Reste gibt es die bei

Im Fall $k = 0$ können wir wie obe

$$x_{1/2} = \pm a^{(q+1)/2} =$$

Für $k = 2$ sind die Wurzeln $\pm$
und nicht explizit bekannt ist. z
primitiven Elements, und das gi
Ordnung gleich 2^e ist. (Hier ist
Argument gilt für jedes e.)

Wenn wir die q-te Potenz *irgendei*
ten wir ein Element, dessen Ordn
Falls sie nicht gleich 2^e ist, muß da
die Elemente von Zweipotenzord
sind daher genau die quadratisch
wir uns verschaffen, wenn wir irg
dulo p kennen: Da q ungerade
quadratischer Nichtrest, und we
Zweipotenzordnung haben. Um
quadratischen Nichtrest modulo

Letzteres ist im Fall $p \equiv 5 \bmod 8$
ratischen Reziprozitätsgesetz qua

$$z = 2^q$$

setzen. Für $k = 2$ ist somit

$$x_{1/2} = \pm a^{\cdot}$$

Um das Ganze wirklich explizit zu
beiden Fälle $k = 0$ und $k = 2$ algo

aber das ist einfach: Wir berechnen zunächst

$$w = a^{(p+3)/8} ;$$

falls $u^2 = a$ ist, sind $x_{1/2} = \pm w$ die beiden Quadratwurzeln. Andernfalls multiplizieren wir w mit $2^{(p-1)/4}$; falls das Quadrat dieses Elements von $\mathbb{F}_p$ gleich a ist, sind die Quadratwurzeln $\pm 2^{(p-1)/4} w$; andernfalls ist a quadratischer Nichtrest.

Auch dies läßt sich mit dem Lemma von EULER aus §1 direkt nachrechnen:

$$w^4 = a^{(p+3)/4} = a^2 \cdot a^{(p-1)/2} = a^2 \left(\frac{a}{p}\right) = a^2 ,$$

falls a ein quadratischer Rest modulo p ist. Damit ist $w^2 = \pm a$.

Falls $w^2 = a$, sind die beiden Wurzeln $\pm w$; andernfalls ist $w^2 = -a$. Da zwei quadratischer Nichtrest ist, ist nach EULER $2^{(p-1)/2} = -1$, also hat $w \cdot 2^{(p-1)/4}$ das Quadrat a.

Bleibt noch der Fall, daß $p \equiv 1 \bmod 8$. Dies ist der schwerste und allgemeinste Fall, denn während $p \equiv 3 \bmod 4$ äquivalent ist zu $e = 1$ und $p \equiv 5 \bmod 8$ zu $e = 2$ kann e hier jeden Wert größer oder gleich drei annehmen. Damit wird auch die Anzahl 2^e der möglichen Werte von k deutlich größer; die Suche nach dem richtigen Exponenten k wird also aufwendiger.

Auch z selbst ist im allgemeinen Fall schwerer zu finden: Während wir für $p \equiv 5 \bmod 8$ wissen, daß zwei ein quadratischer Nichtrest ist, gibt es für $p \equiv 1 \bmod 8$ keine entsprechende Wahl; hier ist $\left(\frac{2}{p}\right) = 1$, und man weiß nur, daß der kleinste quadratische Nichtrest *irgendeine* Zahl zwischen eins und $1 + \sqrt{p}$ ist, was für große Werte von p viel zu viele Möglichkeiten offenläßt.

Leider gibt es keinen effizienten deterministischen Algorithmus zur Bestimmung eines quadratischen Nichtrests modulo einer beliebigen Primzahl; da wir aber wissen, daß die Hälfte aller Restklassen modulo p quadratische Nichtreste sind, kann man in der Praxis leicht welche finden, indem man einfach Zufallszahlen erzeugt und nach der EULERschen Formel oder dem quadratischen Reziprozitätsgesetz das

LEGENDRE-Symbol berechnet. D
Versuche zu brauchen, liegt dann
Versuche ist kleiner als eins zu ei

Der folgende Algorithmus von S
gerade Primzahlen p; für $p \equiv 3$
natürlich effizienter, die obigen V

p sei eine beliebige ungerade Prim
Rest; der Algorithmus bestimmt u
$x \in \mathbb{F}_p^\times$ mit der Eigenschaft, daß

Indem wir $p - 1$ so lange wie
die hinteren Bits betrachten) be
$p - 1 = 2^e q$ mit einer ungeraden

Im *ersten Schritt* wird dann ei
bestimmt, indem wir so lange
$\left(\frac{n}{p}\right) = -1$ ist. Dann berechnen
diese Restklasse genau die Ordnu

Im *zweiten Schritt* werden einige

$$y \leftarrow z, \quad r \leftarrow e, \quad u \leftarrow a$$

wobei alle Berechnungen modulo

$$ab = x^2, \quad y^{2^{r-1}} =$$

denn $ab = a^2 u^2 = x^2$, und die b
nach EULER einfach, daß $y = z$ q
auch $b = au^2$ aber (nach Vorausse

Diese drei Gleichungen werden
gesamten Algorithmus beibehalt
Quadratwurzel aus a ist.

Im *dritten Schritt* testen wir da
Algorithmus mit den Lösungen $\pm$
natürliche Zahl m, für die b^{2^m}
zeigt, daß es ein solches m gibt u

Im *vierten Schritt* setzen wir

$$t \leftarrow y^{2^{r-m-1}}, \quad y \leftarrow t^2, \quad r \leftarrow m, \quad x \leftarrow xt, \quad b \leftarrow by$$

und gehen zurück zum dritten Schritt.

Die obigen Schleifeninvarianten gelten auch wieder nach den Zuweisungen im vierten Schritt: Für $ab = x^2$ kommt das einfach daher, daß das neue x gleich dem alten mal t ist, wohingegen das neue b aus dem alten durch Multiplikation mit $y = t^2$ entsteht. Die Gleichung $y^{2^r} = -1$ gilt weiterhin, weil das neue y die 2^{r-m}-te Potenz des alten ist, so daß seine m-te Potenz gleich dem alten Wert von y^{2^r} ist; da das neue r gleich m ist, folgt die Behauptung. Daß auch die dritte Schleifeninvariante erhalten bleibt, folgt aus der Gültigkeit der zweiten, und der Algorithmus endet nach endlich vielen Iterationen, da r bei jeder Wiederholung des vierten Schritt um mindestens eins kleiner wird und $r = 1$ äquivalent ist zu $b = 1$.

DANIEL SHANKS (1917–1996) wurde in Chicago geboren, wo er zur Schule ging und 1937 einen Bachelorgrad in Physik der University of Chicago erwarb. Er arbeitete bis 1950 in verschiedenen Positionen als Physiker, danach als Mathematiker. 1949 begann er ein *graduate* Studium der Mathematik an der University of Maryland, zu dessen Beginn er der erstaunten Fakultät als erstes eine fertige Doktorarbeit vorlegte. Da zu einem *graduate* Studium auch Vorlesungen und Prüfungen gehören, wurde diese noch nicht angenommen; da er während seines Studiums Vollzeit arbeitete, dauerte es noch bis 1954, bevor er alle Voraussetzungen erfüllte; dann wurde die Arbeit in praktisch unveränderter Form akzeptiert. Erst 1977 entschloß er sich, eine Stelle an einer Universität anzunehmen; ab dann bis zu seinem Tod war er Professor an der University of Maryland.

SHANKS schrieb außer seinem Buch *Solved and unsolved problems in number theory* über achtzig Arbeiten, vor allem auf dem Gebiet der algorithmischen Zahlentheorie und der Primzahlverteilung, aber auch der Numerik. 1962 berechnete er π mit der für damals sensationellen Genauigkeit von 100 000 Dezimalstellen. Näheres findet man in seinem Nachruf in den *Notices of the AMS* vom August 1997, der unter www.ams.org/notices/199707/comm-shanks.pdf auch im Netz zu finden ist.

§5: Anwendungen quadratischer Reste

Zum Abschluß dieses Kapitels sollen kurz noch einige Anwendungen quadratischer Reste vorgestellt werden:

a) Quadratische Formen und

Im ersten Paragraphen des Kapite
uns überlegt, welche natürliche Z
darstellen lassen. Allgemeiner k
Zahlen sich durch irgendeine vorg
lassen. GAUSS untersucht diese F

$$Q(x, y) = a$$

im Gegensatz zu unserer bisherig
Praxis beschränkt er sich also auf
gemischten Terms gerade ist. Di
Form hat nur ganzzahlige Einträg
LAGRANGE wußte er, daß er für
warten konnte. In Abschnitt 154 s
Disquisitiones Arithmeticae zeigt

Satz: Ist $n = ax^2 + 2bxy + cy^2$ f
Zahlen x, y, so ist $b^2 - ac$ ein qu

Sein *Beweis* startet mit der für be

$$(ax^2 + 2bxy + cy$$

$$= \big((u(bx + cy) - v(ax +$$

die der Leser durch Ausmultipli
kaum falsch sein kann, einem Ra
ich diese Aufforderung auch an di

Da x und y teilerfremd sind, la
KLIDischen Algorithmus ganze Z
ist. Setzt man diese in obige Form

$$n \cdot (av^2 - 2buv + cu^2) = \big((u($$

modulo n ist also $b^2 - ac$ ein Qu

Als Beispiel können wir nochmal

$$Q(x, y$$

betrachten. Hier ist $b^2 - ac = -1$, falls sich eine natürliche Zahl n als Summe zweier teilerfremder Quadrate darstellen läßt, muß also -1 modulo n ein Quadrat sein.

Ist eine Primzahl $p = x^2 + y^2$ als Summe zweier Quadrate darstellbar, so sind x und y automatisch teilerfremd, also muß $\left(\frac{-1}{p}\right) = 1$ sein. Nach dem Korollar am Ende von §1 ist dies für ungerades p genau dann der Fall, wenn $p \equiv 1 \bmod 4$ ist; für $p = 2$ ist $\left(\frac{-1}{2}\right) = \left(\frac{1}{2}\right) = 1$. Somit kann eine Primzahl $p \equiv 3 \bmod p$ nicht als Summe zweier Quadrate geschrieben werden.

Das wissen natürlich bereits aus §1 des vorigen Paragraphen; für beliebige quadratische Formen aber ist obiger Satz von GAUSS der Ausgangspunkt für eine genauere Untersuchung. Details dazu führen sehr schnell weit in die algebraische Zahlentheorie und können daher im Rahmen dieser Vorlesung nicht behandelt werden.

b) Münzwurf per Telephon

A und B können sich nicht einigen, wer von ihnen eine dringend notwendige aber unangenehme Arbeit übernehmen soll. Also werfen sie eine Münze. Vorher entscheidet sich etwa A für „Wappen“, B für „Zahl“, dann wirft A die Münze in die Luft. Wenn sie mit Wappen nach oben auf den Boden fällt, hat er gewonnen, andernfalls B.

Stellen wir uns nun aber vor, A und B stehen nicht nebeneinander, sondern befinden sich an verschiedenen Orten und diskutieren per Telephon, wer was machen soll. Auch hier könnte A wieder eine Münze werfen, allerdings sieht jetzt nur A, wie sie zu Boden fällt; wenn er gewinnt, muß B sehr viel Vertrauen in ihn haben, um das zu glauben.

Mit Hilfe von quadratischen Resten läßt sich der Münzwurf so simulieren, daß *beide* den Ausgang überprüfen können und jeder mit der gleichen Wahrscheinlichkeit gewinnt.

Dazu wählt sich A zwei Primzahlen p und q die so groß sind, daß B das Produkt $N = pq$ nicht mit einem Aufwand von nur wenigen Minuten faktorisieren kann. (p und q können also deutlich kleiner sein als bei

RSA, wo man mit Gegnern rec
Dieses N schickt er an B.

B wählt sich nun eine zufällige Za
deren Quadrat $y = x^2 \bmod N$ an

A kennt die Faktorisierung von
vorigen Paragraphen kann er also

$$z^2 \equiv y \bmod p$$

lösen; die jeweiligen Lösungsmen
dem chinesischen Restesatz kann

$$u_{ij} \equiv \begin{cases} a_i \bmod p \\ b_j \bmod q \end{cases}$$

zwischen null und $N - 1$ kons
$u_{ij}^2 \equiv y \bmod N$ erfüllen. Er ent
vier Möglichkeiten (dies entspri
entsprechende $u = u_{ij}$ an B.

B kennt nun zwei Zahlen x un
Möglicherweise ist $u = x$; in dies
bekommen, und er hat verloren. D
d.h. $u = N - x$.

Ist aber $u \neq \pm x$, was mit 50%-i
gewonnen und muß das nun gege

Aus der Kongruenz $x^2 \equiv y \bmod$
chenden Kongruenzen modulo p
$\mu, \nu \in \{1, 2\}$, so daß $x \equiv a_\mu$ m
genau für dieses Indexpaar entsc
das Paar (i, j) mit $\mu \neq i$ und $\nu \neq$
denn $a_1 \equiv -a_2 \bmod p$ und $b_1 \equiv$

Falls sich A aber für ein Paar $(i,$
der beiden Indizes gleich dem er
x und u modulo einer der beide
der anderen ist x kongruent zu $-$
günstige Fall eingetreten ist, kan

und erhält einen der beiden Primfaktoren p oder q. (Der andere ist ggT($x + u, N$).) Damit hat er N faktorisiert und schickt das Ergebnis an A.

Wenn B sich nicht an die Regeln hält und ein y an A schickt, das kein Quadrat modulo N ist, merkt A dies bei der Berechnung der modularen Quadratwurzeln; falls A ein u schickt, dessen Quadrat von y verschieden ist, kann B dies leicht feststellen, denn wenn er verloren hat, muß $u = x$ oder $u = N - x$ sein. (Er kann natürlich auch u^2 mod N berechnen.)

c) Akustik von Konzerthallen

Alte Konzerthallen waren zwangsläufig sehr hoch: Andernfalls wäre die Luft während eines längeren Konzert bei voll besetztem Saal zu schnell verbraucht gewesen. Mit den Fortschritten der Lüftungstechnik verschwand diese Notwendigkeit; dafür sorgten steigende Bau- und Heizungskosten für immer niedrigere Säle. Auf die Luftqualität hatte das keinen nennenswerten Einfluß; die Akustik der Hallen allerdings wurde deutlich schlechter.

Der Grund dafür ist intuitiv recht klar und wurde auch durch Messungen und Hörerbefragungen in einer Reihe von Konzertsälen experimentell bestätigt: Die Hörer bevorzugen Schall, der von den Seitenwänden kommt und daher mit verschiedener Stärke bei den beiden Ohren eintrifft gegenüber Schall von oben, der beide Ohren mit gleicher Stärke erreicht und somit keinen räumlichen Eindruck hinterläßt.

Eine mögliche Abhilfe bestünde darin, die Decken aus absorbierendem Material zu bauen. Dem steht entgegen, daß in einem großen Konzertsaal aller Schall, der von der Bühne kommt, den Hörer auch wirklich erreichen sollte: Ansonsten müßte der Schall aus Lautsprechern kommen und man könnte sich das Konzert genauso gut daheim per Radio oder CD anhören.

Der Schall muß daher von der Decke reflektiert werden, darf die Ohren der Zuhörer aber nicht von oben erreichen. Er sollte daher beispielsweise möglichst diffus zu den Seitenwänden hin gestreut werden, so daß der größte Teil der Energie die Zuhörer über die Seitenwände erreicht.

Der Einfachheit halber wollen
beschränken und damit auch nur
betrachten, der Querrichtung des

Eine Welle hat eine räumliche w
periodische Funktionen sind beis
FOURIER-Analysis lehrt, läßt sich
odische Funktion (bis auf sogena
Kosinusfunktionen zusammenset
nen zu betrachten.

Da der Umgang mit den Additions
tionen recht umständlich ist, schr
plex in der Form $f(t) = Ae^{i\omega t}$
alteil dieser Funktion physikalisc
EULERschen Formel $e^{i\varphi} = \cos$
für A beliebige komplexe Konst
$a\cos\omega t + b\sin\omega t$ als Realteile er

$$\cos(\alpha + \beta) = \mathfrak{Re}\, e^{i(\alpha+\beta)} = \mathfrak{Re}($$

ist, lassen sich auf diese Weise au
Multiplikationen von Exponentia

Auch die räumliche Periodizität
– besser – Exponentialfunktione
sprechend $g(x) = Be^{ikx}$.

Um einen räumlich und zeitlich
kombinieren wir die beiden Ansä
Funktion

$$\psi(x,t) = Ae^{i(\omega$$

Wie man der zweiten Form ansi
was wir auch so interpretieren kö

$$v = \frac{\omega}{k}$$

die Ausbreitungsgeschwindigkeit
Zeit um Δt hat denselben Effekt

Da Sinus und Kosinus die Periode 2π haben, müssen wir für eine Schwingung der Frequenz ν den Parameter ω gleich $2\pi\nu$ wählen, denn dann fallen $1/\nu$ Perioden in das Intervall $0 \le t \le 1$. Aus diesem Grund wird $\omega = 2\pi\nu$ als die *Kreisfrequenz* der Schwingung bezeichnet. In der räumlichen Dimension nimmt die Wellenlänge λ die Rolle der zeitlichen Periode ein; dementsprechend muß hier $k = 2\pi/\lambda$ gesetzt werden. Diese Konstante wird als *Wellenzahl* bezeichnet.

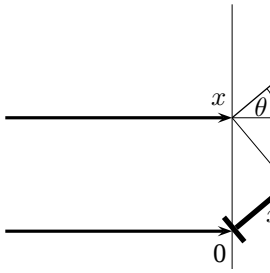
Schallwellen breiten sich bei 20° C in Luft mit einer Geschwindigkeit von etwa $v = 343\,\text{m/s}$ aus; der hörbare Frequenzbereich beginnt bei $\nu = 16\,\text{Hz}$ und kann bis zu etwa $\nu 20\,\text{kHz}$ gehen. Die Wellenlängen, mit denen wir es zu tun haben, variieren also zwischen etwa $\lambda = 21{,}5\,\text{m}$ und $\lambda = 1{,}75\,\text{cm}$. Der Kammerton a' mit 440 Hz hat eine Wellenlänge von knapp 78 cm.

Bei einer Reflektion können wir nach HUYGENS annehmen, daß von jedem Punkt der reflektierenden Fläche eine neue Welle ausgeht; ihre Amplitude ist gleich der Amplitude der dort eintreffenden Welle mal einem Reflektionsfaktor $\rho(x)$, der im Idealfall gleich eins ist.

CHRISTIAAN HUYGENS (1629–1695) kam aus einer niederländischen Diplomatenfamilie. Dadurch und später auch durch seine Arbeit hatte er Kontakte zu führenden europäischen Wissenschaftlern wie DESCARTES und PASCAL. Nach seinem Studium der Mathematik und Jura arbeitete er teilweise auch selbst als Diplomat, interessierte sich aber bald vor allem für Astronomie und den Bau der dazu notwendigen Instrumente. Er entwickelte eine neue Methode zum Schleifen von Linsen und erhielt ein Patent für die erste Pendeluhr. Trotz des französisch-niederländischen Kriegs arbeitete er einen großen Teil seines Lebens an der *Académie Royale des Sciences* in Paris, wo beispielsweise LEIBNIZ viel Mathematik bei ihm lernte. HUYGENS war ein scharfer Kritiker sowohl von NEWTONS Theorie des Lichts als auch seiner Gravitationstheorie, die er für absurd und nutzlos hielt. Gegen Ende seines Lebens beschäftigte er sich mit der Möglichkeit außerirdischen Lebens.

Da es uns nur um den mittleren Schalldruck, nicht aber um seine Variation geht, können wir den ωt-Term ignorieren und einfach mit der Funktion Ae^{-ikx} arbeiten. Wir interessieren uns, wieviel Schall unter welchem Winkel reflektiert wird.

Die Schallwellen die von zwei ver
kel θ ausgehen haben, wie die Z
schied von $x \sin\theta$, wobei x den A



Der Laufwegunterschied von x
$e^{-ikx\sin\theta}$. Wählen wir also die
(die wir in den zu ignorierenden
hineinziehen können), ist die Su
henden Strahlen gleich

$$\int_{-\infty}^{\infty} \rho(x)$$

das ist die sogenannte FOURIER-
im Punkt $u = k\sin\theta$. Wenn w
verteilen wollen, müssen wir die
FOURIER-Transformierte möglich

Eine Möglichkeit dazu sind das, w
ter bezeichnen: Die Decke besteh
möglichst großem Reflektionsgr
stufenförmig mit dem Querschn
Stelle um den Betrag h über der N
Schall gegenüber dem an der N
Weg $2h$ zurücklegen; dies kann n
der Reflektionsfunktion $r(x)$ den

Bei den sogenannten SCHROEDER-Reflektoren werden die Abstände zur Nullinie so gewählt, daß die Längen $2\omega h$ gleich den quadratischen Resten modulo einer ungeraden Primzahl sind, die Decke ist also treppenförmig aufgebaut, wobei die n-te Stufe eine Höhe proportional zu $n^2 \bmod p$ hat. Das obige FOURIER-Integral läßt sich dann approximieren durch die diskrete FOURIER-Transformierte

$$\widehat{r}(m) = \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} e^{2\pi i n^2/p} e^{-2\pi i n m t} = \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} e^{2\pi i n(n-m)/p} .$$

Ihr Betragsquadrat ist

$$\begin{aligned} |\widehat{r}(m)|^2 &= \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} e^{2\pi i n(n-m)/p} \cdot \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} e^{-2\pi i n(n-m)/p} \\ &= \frac{1}{p} \sum_{n=0}^{p-1} \sum_{k=0}^{p-1} e^{2\pi i n(n-m)/p} e^{-2\pi i k(k-m)/p} \\ &= \frac{1}{p} \sum_{n=0}^{p-1} \sum_{k=0}^{p-1} e^{2\pi i \left(n^2-k^2-(n-k)m\right)/p} \end{aligned}$$

Die Summanden hängen nur ab von den Restklassen modulo p der Indizes k und n, und für festes n durchläuft mit k auch $n-k$ alle diese Restklassen. Daher können wir dies weiter ausrechnen als

$$\begin{aligned} |\widehat{r}(m)|^2 &= \frac{1}{p} \sum_{n=0}^{p-1} \sum_{k=0}^{p-1} e^{2\pi i \left(n^2-(n-k)^2-km\right)/p} \\ &= \frac{1}{p} \sum_{k=0}^{p-1} e^{-2\pi i k m/p} \sum_{n=0}^{p-1} e^{2\pi i \left((n^2-(n-k)^2\right)/p} \\ &= \frac{1}{p} \sum_{k=0}^{p-1} e^{-2\pi i k m/p} \sum_{n=0}^{p-1} e^{2\pi i (2kn-k^2)/p} . \end{aligned}$$

Die zweite Summe können wir schreiben als

$$e^{-2\pi i k^2} \sum_{n=0}^{p-1} e^{4\pi i k n/p} .$$

Für $k = 0$ ist sowohl der Vorfaktor eins, wir erhalten also insgesamt aber gleich null, denn

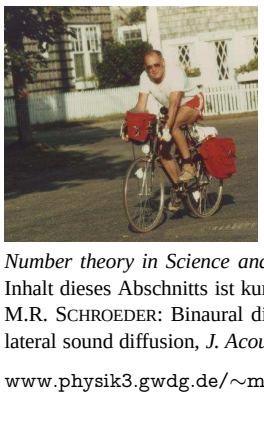
$$e^{4\pi i k/p} \sum_{n=0}^{p-1} e^{4\pi i k n/p} = \sum_{n=0}^{p-1} e^{4\pi i (k$$

die Summe ändert also ihren W eins verschiedenen Zahl $e^{4\pi i k/p}$ schwinden. Somit ist

$$|\widehat{r}(m)|^2$$

für alle m, wir haben also die gev

Die obige Abbildung zeigt den gitter, hier für $p = 23$. Entspr den verschiedensten Primzahlen Opernhäusern, oft allerdings verb terial.



MANFR Ahlen sität G beitete ray Hil diese A 1969 w Univers rung le

Number theory in Science and Commun

Inhalt dieses Abschnitts ist kurz im erste M.R. SCHROEDER: Binaural dissimilarity lateral sound diffusion, *J. Acoust. Soc. Am*

www.physik3.gwdg.de/~mrs

Kapitel 9
Die Fermat-Vermutung für Zahlen und für Polynome

§1: Zahlen und Funktionen

Zum Beweis der eindeutigen Primzerlegung in der Hauptordnung eines Zahlkörpers mußten wir nur nachweisen, daß diese ein EUKLIDischer Ring ist, denn wie wir aus Kapitel 6, §5 wissen, ist jeder EUKLIDische Ring faktoriell. Da der Polynomring in einer Veränderlichen über einem Körper EUKLIDisch ist, gilt also auch dort das Gesetz von der eindeutigen Primzerlegung, wobei die irreduziblen Polynome die Rolle der Primzahlen einnehmen.

Besonders einfach ist die Situation, wenn der Grundkörper k algebraisch abgeschlossen ist: Dann hat jedes nichtkonstante Polynom $f \in k[x]$ eine Nullstelle a und ist damit durch $x - a$ teilbar. In diesem Fall sind also alle irreduziblen Polynome linear.

Die Zerlegung in irreduzible Elemente ist bekanntlich nur eindeutig bis auf Einheiten, und die Einheiten eines Polynomrings sind nach §1 aus Kapitel 6 gerade die des Koeffizientenrings, hier also die von Null verschiedenen Elemente von k. Durch Multiplikation mit einem solchen Element kann man den höchsten Koeffizienten eines jeden Polynoms zu eins machen; die irreduziblen Polynome über einem algebraisch abgeschlossenen Körper sind also bis auf Assoziiertheit genau die Polynome der Form $x - a$ mit $a \in k$ und sie entsprechen eindeutig den Elementen von k.

Den Primzahlen von $\mathbb{Z}$ entsprech
algebraisch abgeschlossenen Kö
über k, wir können also geometri

Natürlich gibt es – zum Teil betr
und dem Polynomring über eine
Analogie so interessant: Da es fü
Instrumentarium gibt, kann man
sultate auf den jeweils anderen F
neuen Sätzen und sonst zumindes

Als Beispiel für Parallelen und U
ationen wollen wir die FERMAT-V
bekanntlich um 1637 an den Ran
von Alexandrien, daß die Gleichu

$$x^n +$$

für $n \geq 3$ keine Lösung in ganzen
vialen Lösungen, bei denen eine d
französische Übersetzung der Ari
übrigens von BACHET DE MÉZIRI
erweiterten EUKLIDischen Algor
MATs Randbemerkung erst, als de
MAT 1670 die Arithmetik mit der
zuvor gestorbenen Vaters veröffe

Die direkte Verallgemeinerung a
Die Gleichung $f^n + g^n = h^n$
nome über einem algebraisch ab
Für beliebig vorgegebene Kons
$h = \sqrt[n]{f^n + g^n}$ setzen. Das sin
für Polynome interessieren, unint
Lösungen $x^n + 0^n = x^n$ der klass

Auch wenn wir verlangen, daß
positiv sein sollen, gibt es triviale
Polynom und sind $a, b, c \in k$ so, d
$(af)^n + (bf)^n = (cf)^n$. Was wir h
folgende Analogon zur klassische

Für $n \geq 3$ gibt es keine paarweise teilerfremden Polynome f, g, h mit positivem Grad, so daß $f^n + g^n = h^n$ ist.

Für Körper positiver Charakteristik ist selbst das noch falsch: Über einen Körper der Charakteristik p ist schließlich $f^p + g^p = (f + g)^p$ für beliebige Polynome f und g, und dasselbe gilt auch wenn man den Exponenten p durch eine seiner Potenzen ersetzt. Wir können also höchstens für Körper der Charakteristik null erwarten, daß diese Vermutung für alle Exponenten $n \geq 3$ richtig ist, und genau das werden wir im übernächsten Paragraphen (zumindest für den Körper der komplexen Zahlen) auch beweisen. Zunächst aber wollen wir schauen, was im bei FERMAT ausgeschlossenen Fall des Exponenten zwei passiert.

§2: Pythagoräische Tripel

Betrachten wir zunächst den Fall der Polynome, wobei wir uns der Einfachheit halber gleich auf Polynome mit komplexen Koeffizienten beschränken wollen. Ist $f^2 + g^2 = h^2$, so ist

$$f^2 = h^2 - g^2 = (h + g)(h - g)\,.$$

Wenn wir f und g als teilerfremd voraussetzen, sind auch g und h teilerfremd und somit auch $h + g$ und $h - g$, denn jeder gemeinsame Teiler dieser beiden Polynome wäre auch ein Teiler ihrer Summe $2h$ sowie ihrer Differenz $2g$.

Wenn wir die Zerlegung von f^2 in irreduzible Faktoren vergleichen mit der von $h + g$ und $h - g$ folgt somit, daß jeder irreduzible Faktor von f entweder in $h + g$ oder in $h - g$ in gerader Potenz auftreten muß. Da jede komplexe Zahl ein Quadrat ist, können wir auch eine eventuell auftretende Einheit als Quadrat schreiben; somit gibt es zwei Polynome $u, v \in \mathbb{C}[x]$ derart, daß

$$u^2 = h + g, \quad v^2 = h - g \quad \text{und} \quad uv = f$$

ist, d.h.

$$f = uv, \quad g = \frac{u^2 - v^2}{2} \quad \text{und} \quad h = \frac{u^2 + v^2}{2}\,.$$

Starten wir umgekehrt mit zwei
$u, v \in \mathbb{C}[x]$, erhalten mit Hilfe
chung $f^2 + g^2 = h^2$. Damit ken
und die restlichen erhalten wir, in
gemeinsamen Faktor multiplizier

Nehmen wir als ein einfaches Be

$$f = 4x, \quad g = x^2$$

in der Tat ist

$$(2x)^2 + \left(x^2 -$$

Hier erhalten wir also mit geringe
über alle Lösungen.

Versuchen wir das gleiche auch
Satzes von PYTHAGORAS bezeic
Zahlen mit $x^2 + y^2 = z^2$ als p
che Tripel gibt es ein rechtwinkl
und $|z|$.

Wir bezeichnen das Tripel $(x, y,$
Vielfaches eines anderen schreib
keinen gemeinsamen Teiler habe
kennen, können wir daraus die
denn jede nichtprimitive Lösung

Wie im Fall der Polynome gehe
(x, y, z) und wenden die dritte bi

$$x^2 = z^2 - y^2$$

Hier können wir leider nicht meh
$z - y$ teilerfremd und damit Quad
so sind ihre Summe und ihre Di
teilbar. Wir müssen uns also zur
klarwerden.

Für eine primitive Lösung $(x, y,$
sein, denn ist d ein gemeinsamer

beide durch d^2 teilbar, also auch ihre Summe z^2. Wegen der eindeutigen Zerlegbarkeit einer natürlichen Zahl in Primfaktoren ist dann auch z durch d teilbar, d.h. d ist ein gemeinsamer Teiler von x, y und z.

Insbesondere können daher x und y nicht beide gerade sein; mindestens eine der beiden Zahlen muß ungerade sein. Andererseits können aber auch nicht beide Zahlen ungerade sein: Wäre nämlich $x = 2u + 1$ und $y = 2v + 1$, so wäre

$$z^2 = (2u + 1)^2 + (2v + 1)^2 = 4u^2 + 4u + 1 + 4v^2 + 4v + 1 \equiv 2 \bmod 4\,,$$

was unmöglich ist, da modulo vier nur null und eins Quadrate sind.

Somit muß in einem primitiven pythagoräischen Tripel (x, y, z) eine der beiden Zahlen x, y gerade sein und die andere ungerade. Da mit (x, y, z) auch (y, x, z) ein primitives pythagoräisches Tripel ist, genügt es, wenn wir diejenigen Tripel betrachten, in denen x gerade ist und y ungerade. Offensichtlich ist dann auch z ungerade.

Für so ein Tripel steht in der Gleichung

$$x^2 = z^2 - y^2 = (z + y)(z - y)$$

rechts das Produkt zweier gerader Zahlen. Im Gegensatz zur Situation bei den Polynomen haben wir hier also keine teilerfremden Faktoren.

Dividieren wir aber durch zwei, so können wir wie oben argumentieren, daß $\frac{1}{2}(z+y)$ und $\frac{1}{2}(z-y)$ teilerfremd sind, denn jeder gemeinsame Teiler wäre Teiler ihrer Summe z und ihrer Differenz y.

Jetzt können wir wieder die eindeutige Primzerlegung anwenden: Da

$$x^2 = 2^2 \cdot \left(\frac{z + y}{2}\right) \cdot \left(\frac{z - y}{2}\right)\,,$$

wobei die beiden Klammern teilerfremd sind, gibt es ganze Zahlen u, v, so daß

$$u^2 = \left(\frac{z + y}{2}\right)\,, \quad v^2 = \left(\frac{z + y}{2}\right) \quad \text{und} \quad 2uv = x$$

ist, also

$$x = 2uv, \quad y = u^2 - v^2 \quad \text{und} \quad z = u^2 - v^2\,.$$

Umgekehrt definieren diese Form
ein primitives pythagoräisches Tr
x und y erhalten wir so auch jed
etwa das seit Jahrtausenden beka
Sakralbauten und -anlagen auch d
Tripel nachweisen lassen, steht zu
möglicherweise bereits in einige
teilweise bekannt waren; entspre
bekannte algebraische Geometer
der nach seiner Emeritierung auc
der Mathematik veröffentlichte. M
er sich ausführlich in

B.L. VAN DER WAERDEN: Geomet
Springer, 1983

§3: Der Satz von Mason

In diesem Abschnitt wollen wir,
für $n \geq 3$ keine zueinander teile
$f, g, h \in \mathbb{C}[x]$ gibt mit $f^n + g^n =$

Der *Beweis* beruht darauf, daß
Nullstellen wie f und g haben
$f^n + g^n = h^n$, so hat auch die Su
gleich zum Grad relativ wenige
n-facher Vielfachheit. Nach eine
Satz können in einer solchen Si
wenige verschiedene Nullstellen

Satz: Bezeichnet $n_0(f)$ die Anz
stellen eines Polynoms f, so gil
Polynome f, g, h mit $f + g = h$

$$n_0(fgh) \geq \max(d$$

Bevor wir diesen Satz beweisen, w
daraus wirklich die FERMAT-Verm

Für drei nichtkonstante teilerfremde Polynome f, g, h mit $f^n + g^n = h^n$ ist nach dem Satz von MASON

$$\begin{aligned} n_0\big(f^n g^n h^n\big) &\geq \max\big(\deg f^n, \deg g^n, \deg h^n\big) + 1 \\ &= n \max\big(\deg f, \deg g, \deg h\big) + 1\,. \end{aligned}$$

Andererseits ist aber

$$\begin{aligned} n_0\big(f^n g^n h^n\big) &= n_0\big(fgh\big) \\ &\leq \deg f + \deg g + \deg h \\ &\leq 3 \max\big(\deg u(x), \deg v(x), \deg w(x)\big)\,, \end{aligned}$$

denn die Anzahl *verschiedener* Nullstellen einer Potenz eines Polynoms ist gleich der Anzahl verschiedener Nullstellen des Polynoms selbst, und die Nullstellenanzahl eines Polynom kann nicht größer sein als der Grad.

Damit haben wir insgesamt die Ungleichung

$$\begin{aligned} &3 \max\big(\deg f, \deg g, \deg h\big) \\ &\geq n_0\big(f^n g^n h^n\big) \\ &\geq n \max\big(\deg f, \deg g, \deg h\big) + 1\,, \end{aligned}$$

die bei nichtkonstanten Polynomen nur für $n \leq 2$ gelten kann. Somit gibt es für $n \geq 3$ keine nichtkonstanten teilerfremden Polynome, für die $f^n + g^n = h^n$ ist.

Zu einem vollständigen Beweis der FERMAT-Vermutung für Polynome fehlt nun nur noch der Beweis des Satzes von MASON. Die Idee dazu ist folgende: Ist $f + g = h$, so betrachten wir den Quotienten g/f im rationalen Funktionenkörper $\mathbb{C}(x)$. Da f und g teilerfremd sind, ist das ein gekürzter Bruch. Falls wir diesen auch in der Form $g/f = G/F$ schreiben können mit Polynomen F, G vom Grad höchstens $n_0(fgh) - 1$ schreiben können, so haben auch f und g höchstens den Grad $n_0(fgh) - 1$. Wegen $f + g = h$ gilt dasselbe auch für h, und damit wäre der Satz bewiesen.

Um g/f als Quotienten zweier neuer Polynome auszudrücken, schreiben wir zunächst

$$\frac{g}{f} = \frac{S}{R} \quad \text{mit} \quad R = \frac{f}{h} \;\text{ und }\; S = \frac{g}{h}\,.$$

Dabei ist $R + S = 1$, die Summe
also. Aus der Gleichung

$$R' + S' =$$

folgt die neue Darstellung

$$\frac{g}{f} = \frac{S}{R}$$

Rechts stehen die logarithmische
und Nenner, und damit lassen sich
Spiel bringen: Nach der LEIBNIZ-

$$(uv)' = u'v + uv',$$

die logarithmische Ableitung eine
der logarithmischen Ableitungen
die logarithmische Ableitung ein
logarithmischer Ableitung des Z
des Nenners ist. Schreiben wir

$$f = f_0 \prod_{i=1}^{r} (x - a_i)^{n_i}, \quad g = g_0 \prod_{j=1}^{s}$$

so ist also

$$\frac{R'}{R} = \frac{f'}{f} - \frac{h'}{h} = \sum_{i=}$$

$$\frac{S'}{S} = \frac{g'}{g} - \frac{h'}{h} = \sum_{j=}$$

$$\text{und} \quad \frac{g}{f} = \frac{R'/R}{S'/S} = -$$

Erweitern wir Zähler und Nenner mit dem Hauptnenner aller Summanden erweitern, d.h. mit dem Polynom vom Grad $r + s + t = n_0(fgh)$

$$H = \prod_{i=1}^{r}(x - a_i) \cdot \prod_{j=1}^{s}(x - b_j) \cdot \prod_{k=1}^{t}(x - c_k)\,,$$

so erhalten wir im Zähler wie auch im Nenner Summen von Polynomen vom Grad $n_0(fgh) - 1$, als Polynome vom Grad höchstens $n_0(fgh) - 1$, wie gewünscht. Damit ist der Satz von MASON bewiesen.

§4: Die abc-Vermutung

Der Erfolg des Satzes von MASON beim Beweis der FERMAT-Vermutung für Polynome legt es nahe, etwas ähnliches auch im klassischen Fall zu versuchen.

Da natürliche Zahlen weder Grade noch Nullstellen haben, müssen wir dazu den Satz von MASON zunächst einmal so umformulieren, daß wir eine Aussage bekommen, die ein sinnvolles Analogon für natürliche Zahlen hat.

Dazu ordnen wir einem Polynom f anstelle der Anzahl $n_0(f)$ seiner (verschiedenen) Nullstellen ein *Polynom* $N_0(f)$ dazu, das genau diese Nullstellen mit jeweils der Vielfachheit eins haben soll: Für

$$f = f_0 \prod_{i=1}^{r}(x - a_i)^{n_i} \quad \text{sei} \quad N_0(f) \underset{\text{def}}{=} \prod_{i=1}^{r}(x - a_i)\,,$$

so daß der Grad von $N_0(f)$ gerade die im vorigen Paragraphen definierte Zahl $n_0(f)$ ist.

Der Vorteil des Polynoms $N_0(f)$ besteht darin, daß wir eine analoge Definition leicht auch für natürliche Zahlen hinschreiben können: Für

$$n = \prod_{i=1}^{r} p_i^{e_i} \quad \text{setzen wir} \quad N_0(n) \underset{\text{def}}{=} \prod_{i=1}^{r} p_i\,.$$

Mit Hilfe der Polynome $N_0(f)$ läßt sich der Satz von MASON folgendermaßen umformulieren:

Gilt für drei teilerfremde Polynom
so hat jedes der drei Polynome
nom $N_0(fgh)$.

In dieser Formulierung kommt i
bei natürlichen Zahlen keine Ver
den Grad lediglich als eine Meth
zuzuordnen, so können wir, wenn
einfach ganz auf ihn verzichten; f
es nahe, ihn durch den Betrag zu

Gemäß dieser Philosophie könn
Aussage formulieren:

A1: *Ist* $c = a+b$ *für drei zueinande*
so ist jede der drei Zahlen kleiner

Damit haben wir eine sinnvolle A
den, die – falls sie korrekt ist – sof
Gibt es nämlich drei natürliche Z
$x^n + y^n = z^n$ für ein $n \geq 3$, so g
de Zahlen x, y, z mit dieser Eige
Zahlen durch ihren größten geme
falls obige Aussage richtig ist, jed
sein als $N_0(x^n y^n z^n)$. Nun ist abe

$$N_0(x^n y^n z^n)$$

d.h. jede der drei Zahlen $x^n, y^n,$

$$(xyz)^n = x$$

was für $n \geq 3$ offensichtlich nich

Angesichts der Komplexität des
an einen so einfachen Beweis zu
Aussage in dieser Form falsch:

Betrachten wir etwa die Gleichu
drei Summanden teilerfremd zue
größer als $N_0(8 \cdot 1 \cdot 9) = 2 \cdot 3 = 6$

Da der Grad eines Polynoms nicht durch konstante Faktoren beeinflußt wird, könnte man versuchen, als „richtiges“ Analogon zum Satz von MASON eine abgeschwächte Aussage zu nehmen, die nur eine Abschätzung bis auf einen konstanten Faktor enthält, etwa

A2: *Ist $c = a+b$ für drei zueinander teilerfremde natürliche Zahlen a, b, c, so gibt es eine Konstante K derart, daß jede der drei Zahlen kleiner ist als $K \cdot N_0(abc)$.*

Diese Aussage ist trivialerweise richtig: Wir müssen nur eine Konstante K wählen, die größer ist als das Maximum von a, b und c. Leider ist sie auch völlig nutzlos, denn solange die Konstante von a, b und c abhängen darf, haben wir keine Chance, damit die FERMAT-Vermutung zu beweisen.

Wir müssen die Aussage also noch einmal umformulieren:

A3: *Es gibt eine Konstante K, so daß gilt: Ist $c = a+b$ für drei zueinander teilerfremde natürliche Zahlen a, b, c, so ist jede der drei Zahlen kleiner als $K \cdot N_0(abc)$.*

Wie wir gleich sehen werden, würde hieraus die FERMAT-Vermutung zumindest für alle hinreichend großen Exponenten n folgen, allerdings ist die Aussage, so wie sie dasteht, leider immer noch falsch:

Betrachten wir die Gleichung

$$a_n + b_n = c_n \quad \text{mit} \quad a_n = 3^{2^n} - 1, \quad b_n = 1 \quad \text{und} \quad c_n = 3^{2^n}. \quad (*)$$

Wäre sie richtig, müßte für jedes n gelten:

$$3^{2^n} \le K N_0\big((3^{2^n} - 1)3^{2^n}\big) = K \cdot 3 \cdot N_0(3^{2^n} - 1)\,.$$

Um $N_0(3^{2^n} - 1)$ abzuschätzen, beachten wir, daß gilt

$$3^{2^n} = \big(3^{2^{n-1}}\big)^2 \quad \text{und} \quad 3^{2^n} - 1 = \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-1}} - 1\big)$$

nach der dritten binomischen Formel. Wenden wir dies mehrfach an, erhalten wir

$$\begin{aligned} 3^{2^n} - 1 &= \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-1}} \\ &= \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-2}} \\ &= \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-2}} \\ &= \cdots \\ &= \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-2}} \end{aligned}$$

In der letzten Zeile steht ein Prod
$3^{2^n} - 1$ durch 2^{n+1} teilbar. Das Pr
Primteiler von $3^{2^n} - 1$ erfüllt dah

$$N_0(3^{2^n} - 1) \le 2$$

denn das Produkt aller ungerad
$(3^{2^n} - 1)/2^n$ sein.

Falls **A3** korrekt wäre, müßte nac

$$3^{2^n} \le \frac{3K}{2^n}(3^2$$

Das kann aber unmöglich der Fa
ist der Faktor $\frac{3K}{2^n}$ kleiner als eins,
sein müßte.

Auf der Suche nach einem Analo
wir daher noch weiter abschwäch
aufgestellte

abc-Vermutung von MASSER un
eine Konstante $K(\varepsilon)$, so daß für
a, b, c mit $a+b = c$ gilt: Jede der d
$K(\varepsilon) \cdot N_0(abc)^{1+\varepsilon}$.

Diese Vermutung ist, im Gegens
offen.

Wir wollen uns überlegen, daß s
die FERMAT-Vermutung implizier

Dazu betrachten wir eine Lösung $x^n + y^n = z^n$ mit o.B.d.A. teilerfremden natürlichen Zahlen x, y, z und wählen uns irgendein $\varepsilon > 0$. Nach der abc-Vermutung gibt es dazu eine Konstante $K(\varepsilon)$, so daß x^n, y^n und z^n allesamt höchstens gleich

$$K(\varepsilon)N_0(x^n y^n z^n)^{1+\varepsilon} = K(\varepsilon)N_0(xyz)^{1+\varepsilon} \leq K(\varepsilon)(xyz)^{1+\varepsilon}$$

sind. Für ihr Produkt gilt daher

$$x^n y^n z^n \leq K(\varepsilon)^3 (xyz)^{3(1+\varepsilon)} \quad \text{oder} \quad (xyz)^{n-3-3\varepsilon} \leq K(\varepsilon)^3 .$$

$K(\varepsilon)^3$ ist eine feste Zahl; es gibt daher einen Exponenten m derart, daß $2^m > K(\varepsilon)^3$ ist. Da das Produkt xyz auf jeden Fall nicht kleiner als zwei sein kann, ist dann für $n - 3 - 3\varepsilon > m$ oder $n > m + 3 + 3\varepsilon$ insbesondere

$$(xyz)^{n-3-3\varepsilon} > K(\varepsilon)^3 .$$

Für Exponenten $n > m + 3 + 3\varepsilon$ kann daher die FERMAT-Gleichung keine Lösung in natürlichen Zahlen haben.

Ob und gegebenenfalls welche konkreten Schranken für n man damit erreichen kann, hängt natürlich davon ab, wie $K(\varepsilon)$ von ε abhängt. Dazu gibt es im Augenblick nicht einmal Vermutungen.

Für weitere Informationen zu §3 und §4 sei auf einen Vortrag verwiesen, den SERGE LANG in Zürich vor einem „allgemeinen“ Publikum hielt und dem ich hier im wesentlichen gefolgt bin:

SERGE LANG: Die abc-Vermutung, *Elemente der Mathematik* **48** (1993), 89-99

Der Artikel ist (wie die gesamte Zeitschrift *Elemente der Mathematik)* unter `http://www.bibliothek.uni-regensburg.de/ezeit/?2135837` frei zugänglich.

§5: Die Frey-Kurve

Da die FERMAT-Vermutung seit 1994 bewiesen ist, die abc-Vermutung aber immer noch offen, mußte der Beweis der FERMAT-Vermutung

natürlich andere Wege gehen. Di
biete, die weit jenseits dessen lie
theorie spezialisierter Diplom-Ma
lernen kann, aber zumindest die
man nämlich Summenbeziehunge
ein gewisses Minimum an verschi
spielt in modifizierter Weise in de

Der Anstoß kam 1984 von GERH
Universität Saarbrücken, wo er a
scher Kurven arbeitete. Heute lei
am Institut für experimentelle Ma
vereinigten) Universität Essen un
elliptischer (und anderer) Kurven

Elliptische Kurven sind ebene K
Form $y^2 = f_3(x)$ beschrieben w
Grad drei mit drei verschiedene
reellen Zahl nicht negativ sein k
mit x-Koordinaten, für die $f_3(x)$
mit y auch $-y$ die obige Gleichu
x-Achse.

Falls $f_3(x)$ nur zwei verschieden
stellen doppelt sein, und bei diese
wir reden dann von einer Knoten

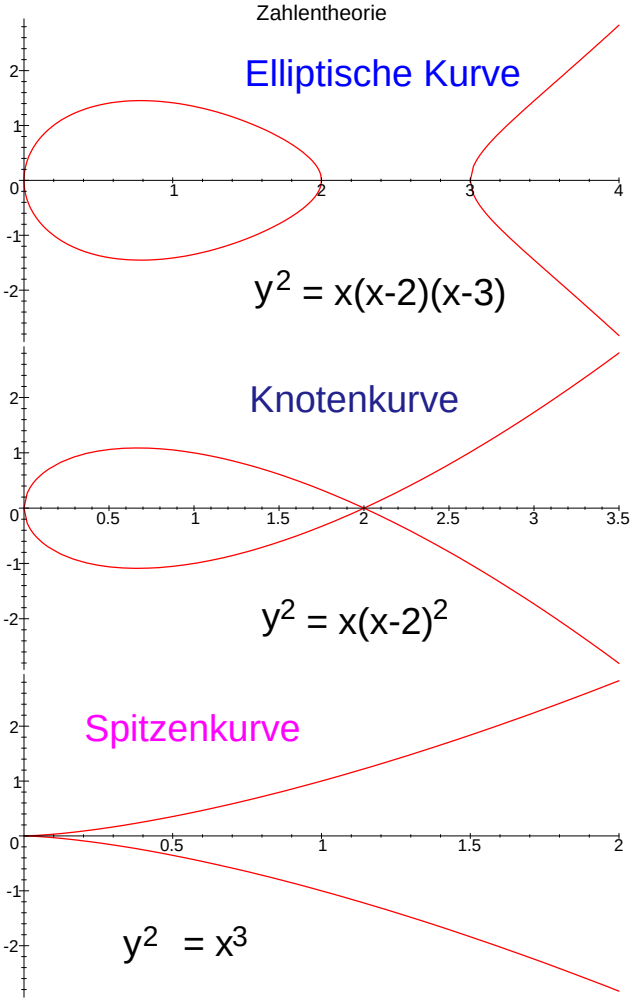
Hat schließlich $f_3(x)$ nur eine, da
eine Spitzenkurve.

FREY betrachtete eine (hypothetis

$$x^n +$$

der FERMAT-Gleichung mit teilerf
$n \geq 5$. (Den Fall $n = 4$ hat, wie wi
gelöst, den Fall $n = 3$ nicht viel
Lösung gibt, dann gibt es auch ein
ten ℓ, denn ist ℓ ein Primteiler vo

$$a^\ell + b^\ell = c^\ell \quad \text{mit} \quad a =$$



eine Lösung, und auch a, b, c sind Fall $\ell \geq 5$ zu betrachten, denn v von n nehmen, bedeutet $\ell = 2$, was für $n = 2$ kein Widerspruch $n = 4$ und damit auch jede höhere ausgeschlossen ist. Für den Fall ℓ werden.

Zur obigen Lösung definiert FREY

$$y^2 = x(x$$

zu, die er aber nicht nur über de trachtet, sondern auch über den ga

Ist allgemein

$$y^2 = (x - x_1$$

eine Kurvengleichung mit ganzen x und y auch ganze Zahlen eins betrachten. Wir sprechen wieder Knotenkurve oder einer Spitzenk stellen x_1, x_2 und x_3 modulo p no

Die obige Gleichung definiert ge alle drei Nullstellen verschieden s minante

$$\Delta = (x_1 - x_2)$$

von Null verschieden ist. Modulo wenn Δ auch modulo p noch von Teiler von Δ ist.

Speziell für die FREY-Kurve $y^2 =$

$$\Delta = (0 - a^\ell)(0 - b^\ell)\big(a^\ell - (-b$$

stets von Null verschieden; modul p ein Teiler von Δ ist, d.h., wenn

Da die Diskriminante als ℓ-te Pote lich groß ist, heißt das, daß es im V

erstaunlich wenige Primzahlen gibt, modulo derer wir *keine* elliptische Kurve erhalten; wir sind also wieder einer ähnlichen Situation wie bei der abc-Vermutung. Die FREYsche Kurve sieht damit so aus, als sei sie fast zu schön, um wirklich zu existieren.

Einen Anhaltspunkt zum Beweis dieser Nichtexistenz liefert eine Vermutung, die auf um 1955 durchgeführte Rechnungen und Spekulationen des japanischen Mathematikers TANIYAMA zurückgeht und heute je nach Autor mit irgendeiner Kombination der drei Namen TANIYAMA, SHIMURA und WEIL bezeichnet wird. Danach sollte es zu einer elliptischen Kurve E mit ganzzahligen Koeffizienten eine surjektive Abbildung $X_0(N) \to E$ von einer sogenannten Modulkurve $X_0(N)$ auf E geben, wobei N im wesentlichen das Produkt aller Primzahlen p ist, modulo derer E keine elliptische Kurve mehr ist. Wie FREYs Rechnungen zeigen, hat seine Kurve vor diesem Hintergrund sehr seltsame Eigenschaften.

Als er damals hier in Mannheim über seine Resultate vortrug, meinte er noch, er glaube nicht, daß die FERMAT-Vermutung so bewiesen werde; er veröffentlichte sein Ergebnis auch nicht in einer der großen internationalen Fachzeitschriften, sondern als Band 1, Heft 1 einer gerade neu gestarteten Schriftenreihe der Universität Saarbrücken, in einfachster Aufmachung xerographiert mit einem nur schwarz-weiß gestalteten Karton als Umschlag:

GERHARD FREY: Links between stable elliptic curves and certain diophantine equations, *Annales Universitatis Saraviensis, Series Mathematicae,* **1** *(1), 1986*

1987 verschärfte der französische Mathematiker JEAN-PIERRE SERRE die TANIYAMA-Vermutung, und aus dieser stärkeren Vermutung folgt in der Tat, daß die FREY-Kurve nicht existieren kann. Leider ist die SERREsche Vermutung bis heute noch nicht bewiesen.

SERRE erhielt übrigens 2002 den ersten der vom norwegischen Parlament gestifteten ABEL-Preise, die seither zur Erinnerung an den norwegischen Mathematiker NIELS HENRIK ABEL (1802–1829) jedes Jahr in gleicher Weise und gleicher Ausstattung wie die Nobel-Preise für hervorragende Leistungen auf dem Gebiet der Mathematik vergeben werden.

SERRE stellte jedoch noch zusätzlich seine sogenannte ε-Vermutung auf,

und auch aus der TANIYAMA-Verm
folgt die Nichtexistenz der FREY-
tung. Diese ε-Vermutung bewies
Berkeley 1990. Die Grundidee se
als eine Art zweidimensionale Ve
ARD KUMMER (1810–1893), der
genannte reguläre Primzahlen als
p heißt regulär, wenn die Haupt
Einheitswurzeln faktoriell ist.) D
heblich aufwendiger.

Damit war also die FERMAT-Ver
YAMA-Vermutung. Diese Vermu
re mathematische Forschung erh
Vermutung) bewies WILES 1994.