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-Symbol definiert einen Gruppenhomomorphismus

$$\left(\frac{\cdot}{p}\right) : \begin{cases} \mathbb{F}_p^\times \to \{+1, -1\} \\ a \mapsto \left(\frac{a}{p}\right) \end{cases} .$$

Für $p = 2$ ist dies der triviale Homomorphismus, für ungerade p ist er surjektiv. Insbesondere gibt es dann jeweils $\frac{p-1}{2}$ quadratische Reste und Nichtreste.

Beweis: Für $p = 2$ ist $\mathbb{F}_2^\times = \{1\}$, und $1 = 1^2$ ist ein quadratischer Rest.

Sei nun p ungerade. Der Homomorphismus

$$\begin{cases} \mathbb{F}_p^\times \to \mathbb{F}_p^\times \\ x \mapsto x^2 \end{cases}$$

hat den Kern $\{+1, -1\}$, also besteht das Bild aus $\frac{p-1}{2}$ Elementen, den quadratischen Resten.

Trivialerweise ist das Produkt zweier quadratischer Reste wieder ein quadratischer Rest. Ist $a = x^2$ ein quadratischer Rest und b ein Nichtrest, so ist auch ab ein quadratischer Nichtrest, denn wäre $ab = y^2$, wäre $b = (yx^{-1})^2$ ein quadratischer Rest. Da Multiplikation mit b injektiv ist, folgt, daß sich jeder quadratische Nichtrest in der Form bc darstellen läßt, wobei c ein quadratischer Rest ist. Damit folgt, daß das Produkt zweier quadratischer Nichtreste ein quadratischer Rest ist, denn $bc \cdot bd = b^2cd$, wobei c und d Quadrate in $\mathbb{F}_p^\times$ sind.

∎

Lemma (EULER): Für ungerades p ist und $a \in \mathbb{F}_p^\times$ ist $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Beweis: g sei ein erzeugendes Element von $\mathbb{F}_p^\times$. Dann ist offensichtlich jede Potenz g^r mit geradem r ein quadratischer Rest, und da es genau $\frac{p-1}{2}$ verschiedene solcher Potenzen gibt, sind das auch *alle* quadratischen Reste. Somit ist g^r genau dann ein quadratischer Rest, wenn r 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 $i \neq j$ zwei verschiedene Zahlen, genauso auch b_i und b_j. Außerdem kann auch nie $|a_i| = |b_j|$ sein, denn sonst wäre einerseits $a_i + b_j = 0$, andererseits gäbe es aber Zahlen $1 \leq k, \ell \leq h$, so daß $a_i \equiv kq$ und $b_j \equiv \ell q \bmod p$. Also wäre $(k + \ell)q$ durch p teilbar, was nicht möglich ist, denn $k + \ell \leq 2h = p - 1$. Damit sind die Beträge der a_i und der b_j genau die Zahlen von 1 bis h, d.h.

$$a_1 \cdots a_m b_1 \cdots b_n = (-1)^m h!.$$

Vergleich mit der obigen Kongruenz zeigt, daß dann $q^h \equiv (-1)^m \bmod p$ ist, also nach dem vorigen Lemma $\left(\frac{q}{p}\right) = (-1)^m$. ∎

2. Schritt (GAUSS): Für zwei ungerade Primzahlen $p \neq q$ ist

$$\left(\frac{q}{p}\right) = (-1)^M \quad \text{mit} \quad M = \sum_{i=1}^{h} \left[\frac{iq}{p}\right] \quad \text{und} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Im *Beweis* sei zunächst auch noch der Fall $q = 2$ zugelassen. Für $i \leq h$ sei $r_i = iq - p \cdot \left[\frac{iq}{p}\right]$; dann ist $0 \leq r_i < p$ und $iq = p \cdot \left[\frac{iq}{p}\right] + r_i$. Falls iq modulo p kongruent ist zu einem negativen Element $a_j \in R$, ist also $r_i = p + a_j$; falls $r_i \equiv b_j > 0$ ist dagegen $r_i = b_j$. Somit ist

$$\sum_{i=1}^{h} iq = p \sum_{i=1}^{h} \left[\frac{iq}{p}\right] + \sum_{i=1}^{m} (a_i + p) + \sum_{i=1}^{n} b_i = pM + mp + \sum_{i=1}^{m} a_i + \sum_{i=1}^{n} b_i.$$

Andererseits ist

$$\sum_{i=1}^{h} iq = \frac{h(h+1)}{2} \cdot q = \frac{1}{2} \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot q = \frac{p^2-1}{8} \cdot q.$$

Außerdem wissen wir aus dem ersten Schritt, daß

$$\{-a_1, \ldots, -a_m, b_1, \ldots, b_n\} = \{1, \ldots, h\}$$

ist, d.h.

$$-\sum_{i=1}^{m} a_i + \sum_{i=1}^{n} b_i = \sum_{i=1}^{h} i = \frac{h(h+1)}{2} = \frac{p^2-1}{8}$$

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 Reziprozitätsgesetzes müssen wir nun nur noch alles kombinieren: Nach dem zweiten und dem dritten Schritt ist

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^M \cdot (-1)^N = (-1)^{M+N} = (-1)^{hk} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \,.$$

∎

CARL FRIEDRICH GAUSS (1777–1855) leistete wesentliche Beiträge zur Zahlentheorie, zur nichteuklidischen Geometrie, zur Funktionentheorie, zur Differentialgeometrie und Kartographie, zur Fehlerrechnung und Statistik, zur Astronomie und Geophysik *usw.* Als Direktor der Göttinger Sternwarte baute er zusammen mit dem Physiker Weber den ersten Telegraphen. Er leitete die erste Vermessung und Kartierung des Königreichs Hannover und zeitweise auch den Witwenfond der Universität Göttingen; seine hierbei gewonnene Erfahrung benutzte er für erfolgreiche Spekulationen mit Aktien. Seine 1801 veröffentlichten *Disquisitiones arithmeticae* sind auch noch heute fundamental für die Zahlentheorie.

FERDINAND GOTTHOLD MAX EISENSTEIN (1823–1852), genannt Gotthold, wurde in Berlin geboren. Als einziges seiner sechs Geschwister starb er nicht bereits während der Kindheit an Meningitis. Im Alter von 17 Jahren, noch als Schüler, besuchte er Mathematikvorlesungen der Universität, unter anderem bei DIRICHLET. Ab 1842 las er die *Disquisitiones arithmeticae* von GAUSS, den er 1844 in Göttingen besuchte. Trotz zahlreicher wichtiger Arbeiten erhielt er nie eine gut bezahlte Position und überlebte vor allem dank der Unterstützung durch ALEXANDER VON HUMBOLDT. 1847 habilitierte er sich in Berlin und hatte dort unter anderem RIEMANN als Studenten. Er starb 29-jährig an Tuberkulose.

Bemerkung: Die rechten Seiten der Gleichungen im quadratischen Reziprozitätsgesetz lassen sich auch durch Kongruenzbedingungen ausdrücken: $(p-1)/2$ ist genau dann gerade, wenn $p \equiv 1 \bmod 4$, entsprechend für q. Somit ist

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} +1 & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv q \equiv 3 \bmod 4 \end{cases} .$$

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.

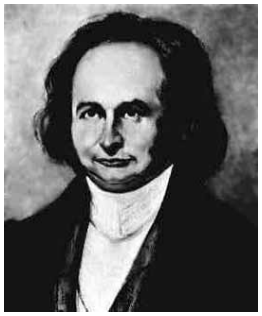
§3: Das Jacobi-Symbol

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-Symbol definiert als

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)^{e_i}.$$

Falls m und n nicht teilerfremd sind, setzen wir $\left(\frac{m}{n}\right) = 0$.



CARL GUSTAV JACOB JACOBI (1804–1851) wurde in Potsdam als Sohn eines jüdischen Bankiers geboren und erhielt den Vornamen Jacques Simon. Im Alter von zwölf Jahren bestand er sein Abitur, mußte aber noch vier Jahre in der Abschlußklasse des Gymnasiums bleiben, da die Berliner Universität nur Studenten mit mindestens 16 Jahren aufnahm. 1824 beendete er seine Studien mit dem Staatsexamen für Mathematik, Griechisch und Latein und wurde Lehrer. Außerdem promovierte er 1825 und begann mit seiner Habilitation. Etwa gleichzeitig konvertierte er zum Christentum, so daß er ab 1825 an der Universität Berlin und ab 1826 in Königsberg lehren konnte. 1832 wurde er dort Professor. Zehn Jahre später mußte er aus gesundheitlichen Gründen das rauhe Klima Königsbergs verlassen und lebte zunächst in Italien, danach für den Rest seines Lebens in Berlin. Er ist vor allem berühmt durch seine Arbeiten zur Zahlentheorie und über elliptische Integrale.

Für eine Primzahl n und ein nicht dadurch teilbares m stimmt das JACOBI-Symbol natürlich mit dem LEGENDRE-Symbol überein, und man kann sich fragen, ob man hier wirklich einen neuen Namen braucht. Dieser ist gerechtfertigt, weil es einen ganz wesentlichen Unterschied zwischen den beiden Symbolen gibt: Beispielsweise ist

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)^{\frac{3^2-1}{8}} \cdot (-1)^{\frac{5^2-1}{8}} = (-1) \cdot (-1) = 1,$$

aber zwei ist offensichtlich kein quadratischer Rest modulo 15: Sonst müßte es schließlich erst recht quadratischer Rest modulo drei und modulo fünf sein, aber die entsprechenden LEGENDRE-Symbole sind -1. In der Tat gibt es modulo 15 nur vier quadratische Reste: 1, 4, 6 und 10.

Das JACOBI-Symbol gibt daher keine Auskunft darüber, ob eine Zahl quadratischer Rest ist oder nicht; lediglich wenn es gleich -1 ist, können wir sicher sein, daß wir es mit einem quadratischen Nichtrest zu tun haben, denn dann muß ja auch schon für mindestens einen Primteiler

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 Reziptozitätsgesetz 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

$$N = \text{Anzahl der Indizes } i \text{ mit } p_i \equiv 3 \bmod 4 \text{ und } e_i \text{ ungerade} .$$

Die Faktoren $p_i^{e_i}$ sind genau dann kongruent eins modulo vier, wenn $p_i \equiv 1 \bmod 4$ oder e_i gerade ist, denn $3^2 \equiv 1 \bmod 4$. Andernfalls ist $p_i^{e_i} \equiv 3 \equiv -1 \bmod 4$. Somit ist auch $n \equiv (-1)^N \bmod 4$, also

$$(-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}e_i} = (-1)^N = (-1)^{\frac{n-1}{2}} .$$

Ist dies gleich +1, so ist die rechte Seite der Gleichung für $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)$ ebenfalls +1, andernfalls zeigt das gleiche Argument für m, daß sie gleich $(-1)^{(m-1)/2}$ ist. In jedem Fall erhalten wir daher die gewünschte Formel

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} .$$

Genauso folgt auch, daß $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$ ist, denn dies ist +1 für $m \equiv \pm 1 \bmod 8$ und -1 für $m \equiv \pm 3 \bmod 8$. Das Produkt zweier Primzahlen kongruent ± 1 modulo acht ist wieder kongruent ± 1, genauso das zweier Primzahlen kongruent ± 3 modulo acht. Damit führt dieselbe Argumentation wie oben zum Ziel. ∎

Als Anwendung können wir uns überlegen, modulo welcher Primzahlen eine vorgegebene Zahl a quadratischer Rest ist. Modulo seiner Primteiler verschwindet a und ist somit ein Quadrat. Sei also p kein Teiler von a.

Für $a = 2$ haben wir gesehen, daß $\left(\frac{2}{p}\right)$ nur von der Kongruenzklasse p mod 8 abhängt; wegen der Multiplikativität des JACOBI-Symbols reicht es also, wenn wir ungerade a betrachten. Nach dem gerade bewiesenen Gesetz ist dann

$$\left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}}\left(\frac{p}{a}\right) .$$

Für festes a ist $(a-1)/2$ ein konstanter Wert, $(p-1)/2$ hängt nur ab von p mod 4, und $\left(\frac{p}{a}\right)$ hängt ab von p mod a. Insgesamt hängt es also nur ab von p mod $4a$, ob a ein quadratischer Rest oder Nichtrest modulo p ist.

Betrachten wir als Beispiel den Fall $a = 3$. Hier ist $(a-1)/2 = 1$, also

$$(-1)^{\frac{(a-1)}{2}\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases},$$

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

$$y = g^{2^e} \quad \text{und} \quad z = g^q$$

folgt, daß y die Ordnung q hat und z die Ordnung 2^e.

Da q und 2^e teilerfremd sind, gibt es nach dem erweiterten EUKLIDischen Algorithmus ganze Zahlen u, v, so daß

$$2^e u + qv = 1$$

ist. Hierbei muß v offensichtlich eine ungerade Zahl sein, denn sonst wäre die Summe auf der linken Seite eine gerade Zahl.

Damit ist

$$g = g^{2^e u + qv} = g^{2^e u} g^{qv} = y^u z^v$$

und entsprechend für jedes r

$$g^r = y^{ur} z^{vr}.$$

Da es bei Potenzen von y nur auf den Exponenten modulo q ankommt und bei solchen von z nur auf den Exponenten modulo 2^e, heißt dies, daß sich jedes Element von $\mathbb{F}_p^\times$ in der Form

$$a = y^\alpha z^\beta \quad \text{mit} \quad 0 \le \alpha < q \quad \text{und} \quad 0 \le \beta < 2^e$$

schreiben läßt.

$a = g^r$ ist genau dann ein quadratischer Rest, wenn r eine gerade Zahl ist; die beiden Quadratwurzeln sind dann $\pm g^{r/2}$. Falls wir nur a kennen, ist dies allerdings nicht sonderlich nützlich zur Berechnung dieser Wurzeln, denn erstens kennen wir im allgemeinen das Element g nicht explizit, und zweitens kennen wir auch den Exponenten r nicht. Ersteres wäre kein großes Problem, denn es gibt effiziente probabilistische Algorithmen, um sich mögliche Werte für g zu verschaffen, letzteres aber ist ein diskretes Logarithmenproblem modulo p, also nur dann effizient lösbar, wenn die Primzahl p ziemlich klein ist.

Auch der etwas komplizierteren (und bislang ebenfalls nicht explizit bekannten) Form $a = y^\alpha z^\beta$ können wir ansehen, wann a quadratischer Rest ist: Da v eine ungerade Zahl ist, ist r genau dann gerade, wenn auch

vr gerade ist, und das wiederum ist äquivalent dazu, daß $\beta = vr \bmod 2^e$ 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 $p \equiv 1 \bmod 8$ oder $p \equiv 5 \bmod 8$. Zumindest im letzteren Fall können wir wieder eine explizite Formel für die Quadratwurzeln aufstellen: In diesem Fall ist $p - 1 \equiv 4 \bmod 8$, d.h. $p - 1$ ist zwar durch vier, nicht aber durch acht teilbar. Somit ist

$$p - 1 = 4q = 2^2 q \quad \text{mit einer ungeraden Zahl } q ,$$

d.h. $e = 2$. Daher kann k nun die vier Werte $0, 1, 2, 3$ annehmen; für quadratische Reste gibt es die beiden Möglichkeiten $k = 0$ und $k = 2$.

Im Fall $k = 0$ können wir wie oben argumentieren: Dann ist

$$x_{1/2} = \pm a^{(q+1)/2} = \pm a^{(\frac{p-1}{4}+1)/2} = \pm a^{(p+3)/8} .$$

Für $k = 2$ sind die Wurzeln $\pm a^{(q+1)/2} z$, wobei z wie oben definiert und nicht explizit bekannt ist. z ist nach Definition q-te Potenz eines primitiven Elements, und das gilt offenbar für jedes Element, dessen Ordnung gleich 2^e ist. (Hier ist natürlich $e = 2$, aber das folgende Argument gilt für jedes e.)

Wenn wir die q-te Potenz *irgendeines* Elements aus $\mathbb{F}_p^\times$ berechnen, erhalten wir ein Element, dessen Ordnung eine Zweierpotenz ist, die 2^e teilt. Falls sie nicht gleich 2^e ist, muß das Element Quadrat eines anderen sein; die Elemente von Zweipotenzordnung, die genaue Ordnung 2^e haben, sind daher genau die quadratischen Nichtreste. Einen solchen können wir uns verschaffen, wenn wir irgendeinen quadratischen Nichtrest modulo p kennen: Da q ungerade ist, ist dann auch dessen q-te Potenz quadratischer Nichtrest, und wegen $p - 1 = 2^e q$ muß diese Potenz Zweipotenzordnung haben. Um z zu finden, reicht es also, *irgendeinen* quadratischen Nichtrest modulo p zu finden.

Letzteres ist im Fall $p \equiv 5 \bmod 8$ einfach: Hier ist zwei nach dem quadratischen Reziprozitätsgesetz quadratischer Nichtrest; daher können wir

$$z = 2^q = 2^{(p-1)/4}$$

setzen. Für $k = 2$ ist somit

$$x_{1/2} = \pm a^{(p+3)/8} \cdot 2^{(p-1)/4} .$$

Um das Ganze wirklich explizit zu machen, müssen wir nun nur noch die beiden Fälle $k = 0$ und $k = 2$ algorithmisch voneinander unterscheiden, 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 wieder direkt nachrechnen:

$$w^4 = a^{(p+3)/4} = a^2 \cdot a^{(p-1)/2} = a^2 \left(\frac{a}{p}\right) = a^2$$

nach EULER, falls a 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. Die Wahrscheinlichkeit, mehr als zehn Versuche zu brauchen, liegt dann bei $1 : 1024$, die für mehr als zwanzig Versuche ist kleiner als eins zu einer Million, *usw.*

Der folgende Algorithmus von SHANKS funktioniert für beliebige ungerade Primzahlen p; für $p \equiv 3 \bmod 4$ und $p \equiv 5 \bmod 8$ ist es aber natürlich effizienter, die obigen Verfahren zu benutzen.

p sei eine beliebige ungerade Primzahl, und $a \in \mathbb{F}_p^\times$ sei ein quadratischer Rest; der Algorithmus bestimmt unter dieser Voraussetzung ein Element $x \in \mathbb{F}_p^\times$ mit der Eigenschaft, daß x und $-x$ Quadrat a haben.

Indem wir $p - 1$ so lange wie möglich durch zwei dividieren (oder die hinteren Bits betrachten) bestimmen wir zunächst die Zerlegung $p - 1 = 2^e q$ mit einer ungeraden Zahl q.

Im *ersten Schritt* wird dann ein quadratischer Nichtrest modulo p bestimmt, indem wir so lange Zufallszahlen $n \bmod p$ erzeugen, bis $\left(\frac{n}{p}\right) = -1$ ist. Dann berechnen wir $z = n^q \bmod p$ und wissen, daß diese Restklasse genau die Ordnung 2^e hat.

Im *zweiten Schritt* werden einige Variablen initialisiert; wir setzen

$$y \leftarrow z, \quad r \leftarrow e, \quad u \leftarrow a^{(q-1)/2}, \quad b \leftarrow au^2, \quad x \leftarrow au\,,$$

wobei alle Berechnungen modulo p durchgeführt werden. Danach ist

$$ab = x^2, \quad y^{2^{r-1}} = -1 \quad \text{und} \quad b^{2^{r-1}} = 1\,,$$

denn $ab = a^2u^2 = x^2$, und die beiden hinteren Gleichungen bedeuten nach EULER einfach, daß $y = z$ quadratischer Nichtrest ist, a und damit auch $b = au^2$ aber (nach Voraussetzung) quadratischer Rest.

Diese drei Gleichungen werden als Schleifeninvarianten durch den gesamten Algorithmus beibehalten; für $b = 1$ besagen sie, daß x eine Quadratwurzel aus a ist.

Im *dritten Schritt* testen wir daher, ob $b = 1$ ist; falls ja, endet der Algorithmus mit den Lösungen $\pm x$. Andernfalls suchen wir die kleinste

natürliche Zahl m, für die $b^{2^m} = 1$ ist; die dritte Schleifeninvariante zeigt, daß es ein solches m gibt und $m \le r-1$ ist.

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 quadratische Reste

Im ersten Paragraphen des Kapitels über quadratische Formen haben wir uns überlegt, welche natürliche Zahlen sich als Summe zweier Quadrate darstellen lassen. Allgemeiner kann man sich fragen, welche ganzen Zahlen sich durch irgendeine vorgegebene Quadratische Form darstellen lassen. GAUSS untersucht diese Frage für die quadratische Formen

$$Q(x,y) = ax^2 + 2bxy + cy^2\,;$$

im Gegensatz zu unserer bisherigen (auf LAGRANGE zurückgehenden) Praxis beschränkt er sich also auf Formen, bei denen der Koeffizient des gemischten Terms gerade ist. Die Matrix $M = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ zu einer solchen Form hat nur ganzzahlige Einträge, und auf Grund früherer Resultate von LAGRANGE wußte er, daß er für solche Formen bessere Ergebnisse erwarten konnte. In Abschnitt 154 seines zahlentheoretischen Hauptwerks *Disquisitiones Arithmeticae* zeigt er den folgenden

Satz: Ist $n = ax^2 + 2bxy + cy^2$ für zwei zueinander teilerfremde ganze Zahlen x, y, so ist $b^2 - ac$ ein quadratischer Rest modulo n.

Sein *Beweis* startet mit der für beliebige Zahlen u, v gültigen Formel

$$\begin{aligned}&(ax^2 + 2bxy + cy^2)(av^2 - 2buv + cu^2)\\ &= \big((u(bx+cy) - v(ax+by)\big)^2 - (b^2-ac)(ux+vy)^2\,,\end{aligned}$$

die der Leser durch Ausmultiplizieren nachrechnen soll. Da es wohl kaum falsch sein kann, einem Ratschlag von GAUSS zu folgen, möchte ich diese Aufforderung auch an die Leser dieses Skriptums weitergeben.

Da x und y teilerfremd sind, lassen sich nach dem erweiterten EUKLIDischen Algorithmus ganze Zahlen u, v finden, für die $ux + vy = 1$ ist. Setzt man diese in obige Formel ein, vereinfacht sich diese zu

$$n \cdot (av^2 - 2buv + cu^2) = \big((u(bx+cy) - v(ax+by)\big)^2 - (b^2-ac)\,,$$

modulo n ist also $b^2 - ac$ ein Quadrat, wie behauptet. ∎

Als Beispiel können wir nochmals die quadratische Form $Q(x,y) = x^2 + y^2$ 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 rechnen muß, die monatelang rechnen.) Dieses N schickt er an B.

B wählt sich nun eine zufällige Zahl x zwischen eins und N und schickt deren Quadrat $y = x^2 \bmod N$ an A.

A kennt die Faktorisierung von N; nach dem Algorithmus aus dem vorigen Paragraphen kann er also die Gleichungen

$$z^2 \equiv y \bmod p \quad \text{und} \quad z^2 \equiv y \bmod q$$

lösen; die jeweiligen Lösungsmengen seien $\{a_1, a_2\}$ und $\{b_1, b_2\}$. Nach dem chinesischen Restesatz kann er sich vier Elemente

$$u_{ij} \equiv \begin{cases} a_i \bmod p \\ b_j \bmod q \end{cases} \quad \text{mit} \quad i,j \in \{1,2\}$$

zwischen null und $N-1$ konstruieren, die allesamt die Kongruenz $u_{ij}^2 \equiv y \bmod N$ erfüllen. Er entscheidet sich zufällig für eine dieser vier Möglichkeiten (dies entspricht dem Münzwurf) und schickt das entsprechende $u = u_{ij}$ an B.

B kennt nun zwei Zahlen x und u, die beide das Quadrat y haben. Möglicherweise ist $u = x$; in diesem Fall hat er keine neue Information bekommen, und er hat verloren. Das gleiche gilt im Fall $u \equiv -x \bmod N$, d.h. $u = N - x$.

Ist aber $u \not\equiv \pm x$, was mit 50%-iger Wahrscheinlichkeit eintritt, hat B gewonnen und muß das nun gegenüber A beweisen.

Aus der Kongruenz $x^2 \equiv y \bmod N = pq$ folgen natürlich die entsprechenden Kongruenzen modulo p und modulo q; es gibt daher Indizes $\mu, \nu \in \{1,2\}$, so daß $x \equiv a_\mu \bmod p$ und $x \equiv b_\nu \bmod q$. Falls sich A genau für dieses Indexpaar entschieden hat, ist $x = u$; falls er sich für das Paar (i,j) mit $\mu \neq i$ und $\nu \neq j$ entschieden hat, ist $u \equiv -x \bmod N$, denn $a_1 \equiv -a_2 \bmod p$ und $b_1 \equiv -b_2 \bmod q$.

Falls sich A aber für ein Paar (i,j) entschieden hat, in dem genau einer der beiden Indizes gleich dem entsprechenden Index in (μ,ν) ist, sind x und u modulo einer der beiden Primzahlen p, q kongruent, modulo der anderen ist x kongruent zu $-u$. Um zu beweisen, daß dieser für ihn günstige Fall eingetreten ist, kann B daher ggT$(x-u, N)$ berechnen

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 wir uns auf eindimensionale Wellen beschränken und damit auch nur diffuse Reflektion in einer Richtung betrachten, der Querrichtung des Konzertsaals.

Eine Welle hat eine räumliche wie auch zeitliche Periodizität. Zeitlich periodische Funktionen sind beispielsweise Sinus und Kosinus; wie die FOURIER-Analysis lehrt, läßt sich jede stückweise stetige zeitlich periodische Funktion (bis auf sogenannte Nullfunktionen) aus Sinus- und Kosinusfunktionen zusammensetzen, so daß es reicht, solche Funktionen zu betrachten.

Da der Umgang mit den Additionstheoremen für trigonometrische Funktionen recht umständlich ist, schreibt man Wellen allerdings meist komplex in der Form $f(t) = Ae^{i\omega t}$ mit der Maßgabe, daß nur der Realteil dieser Funktion physikalische Realität beschreibt. Aufgrund der EULERschen Formel $e^{i\varphi} = \cos\varphi + i\sin\varphi$ lassen sich so, falls man für A beliebige komplexe Konstanten zuläßt, alle Funktionen der Art $a\cos\omega t + b\sin\omega t$ als Realteile erhalten, und da beispielsweise

$$\cos(\alpha+\beta) = \mathfrak{Re}\, e^{i(\alpha+\beta)} = \mathfrak{Re}(e^{i\alpha}e^{i\beta}) = \cos\alpha\,\cos\beta - \sin\alpha\,\sin\beta$$

ist, lassen sich auf diese Weise auch die Additionstheoreme auf einfache Multiplikationen von Exponentialfunktionen zurückführen.

Auch die räumliche Periodizität läßt sich mit trigonometrischen oder – besser – Exponentialfunktionen ausdrücken; hier schreiben wir entsprechend $g(x) = Be^{ikx}$.

Um einen räumlich und zeitlich periodischen Vorgang zu beschreiben, kombinieren wir die beiden Ansätze und betrachten beispielsweise die Funktion

$$\psi(x,t) = Ae^{i(\omega t - kx)} = Ae^{ik(\frac{\omega}{k}t - x)}\,.$$

Wie man der zweiten Form ansieht, hängt $\psi(x,t)$ nur ab von $x - \frac{\omega}{t}t$, was wir auch so interpretieren können, daß

$$v = \frac{\omega}{k} = \frac{\lambda}{T} = \frac{\lambda\omega}{2\pi}$$

die Ausbreitungsgeschwindigkeit der Welle ist; denn eine Änderung der Zeit um Δt hat denselben Effekt wie eine Änderung des Orts um $v\cdot\Delta t$.

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.

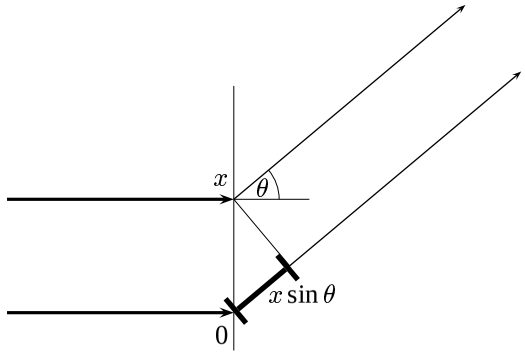
Schallwellen breiten sich bei 20° C in Luft mit einer Geschwindigkeit von etwa $v = 343\,\text{m/s}$ aus; der hörbare Frequenzbereich beginnt bei $\nu = 16\,\text{Hz}$ und kann bis zu etwa $\nu 20\,\text{kHz}$ gehen. Die Wellenlängen, mit denen wir es zu tun haben, variieren also zwischen etwa $\lambda = 21{,}5\,\text{m}$ 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 verschiedenen Punkten unter einem Winkel θ ausgehen haben, wie die Zeichnung zeigt, einen Laufwegunterschied von $x\sin\theta$, wobei x den Abstand der beiden Punkte bezeichnet.



Der Laufwegunterschied von $x\sin\theta$ entspricht einem Phasenfaktor $e^{-ikx\sin\theta}$. Wählen wir also die Phase im Nullpunkt als Referenz (die wir in den zu ignorierenden Phasenfaktor der einfallenden Welle hineinziehen können), ist die Summe aller unter dem Winkel θ abgehenden Strahlen gleich

$$\int_{-\infty}^{\infty} \rho(x) e^{-ikx\sin\theta}\,dx\,;$$

das ist die sogenannte FOURIER-Transformierte von $\rho(x)$, ausgewertet im Punkt $u = k\sin\theta$. Wenn wir den Schall möglichst gleichmäßig verteilen wollen, müssen wir die Funktion ρ daher so wählen, daß ihre FOURIER-Transformierte möglichst konstant ist.

Eine Möglichkeit dazu sind das, was Physiker als *Reflektions-Phasengitter* bezeichnen: Die Decke besteht aus einem Material mit konstantem, möglichst großem Reflektionsgrad, aber die Höhe der Decke variiert stufenförmig mit dem Querschnitt. Wenn die Höhe der einer festen Stelle um den Betrag h über der Nullinie liegt, muß der dort reflektierte Schall gegenüber dem an der Nullinie reflektierten den zusätzlichen Weg $2h$ zurücklegen; dies kann man formal so ausdrücken, daß man in der Reflektionsfunktion $r(x)$ den zusätzlichen Faktor $e^{2i\omega h}$ einfügt.

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 wie auch jeder der Summanden gleich eins, wir erhalten also ingesamt p. Für $k \neq 0$ und $k < p$ ist die Summe aber gleich null, denn

$$e^{4\pi i k/p} \sum_{n=0}^{p-1} e^{4\pi i k n/p} = \sum_{n=0}^{p-1} e^{4\pi i (k+1) n/p} = \sum_{n=1}^{p} e^{4\pi i k n/p} = \sum_{n=0}^{p-1} e^{4\pi i k n/p} \,,$$

die Summe ändert also ihren Wert nicht, wenn man sie mit der von eins verschiedenen Zahl $e^{4\pi i k/p}$ multipliziert, und damit muß sie verschwinden. Somit ist

$$|\widehat{r}(m)|^2 = \frac{1}{p} e^0 \cdot p = 1$$

für alle m, wir haben also die gewünschte Diffusionseigenschaft.

Die obige Abbildung zeigt den Querschnitt über ein solches Phasengitter, hier für $p = 23$. Entsprechende SCHROEDER-Reflektoren zu den verschiedensten Primzahlen gibt es in vielen Konzertsälen und Opernhäusern, oft allerdings verborgen hinter schalldurchlässigem Material.

MANFRED ROBERT SCHROEDER wurde 1926 in Deutschland geboren. Er studierte Physik an der Universität Göttingen, wo er 1952 promovierte. Danach arbeitete er bei den AT & T Bell Laboratories in Murray Hill, New Jersey auf dem Gebiet der Akustik; diese Arbeit führte unter anderem zu 45 Patenten. 1969 wechselte er als Professor für Akustik an die Universität Göttingen, wo er bis zu seiner Emeritierung lehrte. Er schrieb mehrere Bücher, unter anderem *Number theory in Science and Communication* und *Fractals, Chaos, Power Laws*. Der Inhalt dieses Abschnitts ist kurz im ersten dieser Bücher dargestellt sowie ausführlich in M.R. SCHROEDER: Binaural dissimilarity and optimum ceilings for concert halls: More lateral sound diffusion, *J. Acoust. Soc. Am.* **65** (4), 1979

www.physik3.gwdg.de/~mrs