Wolfgang K. Seiler
Tel. 2515

A5, C201

8. Mai 2014

Probeklausur zur Zahlentheorie

• • • **Schreiben Sie bitte auf jedes Blatt Ihren Namen!** • • •

Aufgabe 1: (*4 Punkte*)

a) Heute vor 65 Jahren, am 8. Mai 1949, verabschiedete der Parlamentarische Rat das Grundgesetz für die Bundesrepublik Deutschland. An welchem Wochentag geschah dies?

Lösung: Von einem Jahr zum nächsten verschieben sich die Wochentage im Falle eines Jahrs mit 365 Tagen um einen, bei Schaltjahren um zwei Tage. In den letzten 65 Jahren gab es 16 Schaltjahre (1952 – 2012 alle vier Jahre, denn 2000 ist zwar durch 100, aber auch durch 400 teilbar), also verschoben sich die Wochentage zwischen 1949 und 2014 um $65+16 = 81 \equiv 4 \bmod 7$. Da heute Donnerstag ist, war der 8. Mai 1949 somit ein Sonntag.

b) Heute in 65 Jahren ist der 8. Mai 2079. Auf welchen Wochentag fällt dieser?

Lösung: Wieder gibt es innerhalb der 65 Jahre 16 Schaltjahre (2016 – 2076), also werden die Wochentage wieder um vier verschoben, und der 8. Mai 2079 ist ein Montag.

Aufgabe 2: (*12 Punkte*)

a) Bestimmen Sie den größten gemeinsamen Teiler von 1111 und 2552, und stellen Sie diesen als ganzzahlige Linearkombination dieser beiden Zahlen dar!

Lösung: Anwendung des Euklidischen Algorithmus führt auf

$$\begin{aligned}
2552 : 1111 = 2 \text{ Rest } 330 &\Longrightarrow 330 = 2552 - 2\cdot 1111 \\
1111 : 330 = 3 \text{ Rest } 121 &\Longrightarrow 121 = 1111 - 3\cdot(2552 - 2\cdot 1111) = 7\cdot 1111 - 3\cdot 2552 \\
330 : 121 = 2 \text{ Rest } 88 &\Longrightarrow 88 = 2552 - 2\cdot 1111 - 2\cdot(7\cdot 1111 - 3\cdot 2552) = 7\cdot 2552 - 16\cdot 1111 \\
121 : 88 = 1 \text{ Rest } 33 &\Longrightarrow 33 = 7\cdot 1111 - 3\cdot 2552 - (7\cdot 2552 - 16\cdot 1111) = 23\cdot 1111 - 10\cdot 2552 \\
88 : 33 = 2 \text{ Rest } 22 &\Longrightarrow 22 = 7\cdot 2552 - 16\cdot 1111 - 2\cdot(23\cdot 1111 - 10\cdot 2552) = 27\cdot 2552 - 62\cdot 1111 \\
33 : 22 = 1 \text{ Rest } 11 &\Longrightarrow 11 = 23\cdot 1111 - 10\cdot 2552 - (27\cdot 2552 - 62\cdot 1111) = 85\cdot 1111 - 37\cdot 2552
\end{aligned}$$

Da 22 durch elf teilbar ist, folgt: $\operatorname{ggT}(1111, 2552) = 11 = 85\cdot 2552 - 37\cdot 1111$.

b) Zeigen Sei: Eine zweistellige Zahl ist genau dann prim, wenn sie nicht durch zwei, drei, fünf oder sieben teilbar ist.

Lösung: Wenn eine zweistellige Zahl durch zwei, drei, fünf oder sieben teilbar ist, kann sie offensichtlich nicht prim sein. Ist sie umgekehrt durch keine dieser vier Zahlen teilbar, so muß jeder Primteiler größer oder gleich der nächsten Primzahl elf sein. Da $11^2 = 121 > 99$ ist, kann es nur einen solchen Primteiler geben, die Zahl ist also prim.

c) Geben Sie die Primfaktorzerlegung von 1111 und 2552 an! Dabei muß nur für Faktoren größer fünfzig bewiesen werden, daß es sich tatsächlich um Primzahlen handelt.

Lösung: Nach *a)* sind beide Zahlen durch elf teilbar; $1111 : 11 = 101$ ist eine Primzahl, da es durch keine der Primzahlen $2, 3, 5$ und 7 teilbar und das Argument aus *b)* offensichtlich nicht nur für zweistellige Zahlen, sondern auch für dreistellige bis 120 gilt.

$2552 : 11 = 232$ ist durch vier teilbar, da 32 durch 4 teilbar ist; $232 : 4 = 58 = 2 \cdot 29$. Somit ist $1111 = 11 \cdot 101$ und $2552 = 2^3 \cdot 11 \cdot 29$.

d) Bestimmen Sie alle $(x, y) \in \mathbb{Z}^2$ mit $1111x + 2552y = 111$!

Lösung: Da 111 nicht durch $\mathrm{ggT}(1111, 2552) = 11$ teilbar ist, gibt es keine Lösungen, denn für alle $(x, y) \in \mathbb{Z}^2$ ist $1111x + 2552y$ durch diesen ggT teilbar.

e) Bestimmen Sie alle $(x, y) \in \mathbb{Z}^2$ mit $1111x + 2552y = 121$!

Lösung: Da $121 = 11^2$ durch elf teilbar ist, gibt es nun Lösungen. Nach *a)* ist

$$85 \cdot 2552 - 37 \cdot 1111 = 11\,;$$

Multiplikation dieser Gleichung mit elf führt zur ersten Lösung $x = -37 \cdot 11 = -407$ und $y = 11 \cdot 85 = 935$. Die weiteren Lösungen erhalten wir durch Addition einer Lösung der homogenen Gleichung $1111u + 2552v = 0$. Division durch den ggT elf vereinfacht diese zur Gleichung $101u + 232v = 0$ mit teilerfremden Koeffizienten; die Lösungen sind also von der Form $u = 232k$ und $v = -101k$ mit $k \in \mathbb{Z}$. Die Lösungen der Ausgangsgleichung sind daher die Elemente der Menge

$$\left\{(232k - 407, 935 - 101k) \;\middle|\; k \in \mathbb{Z}\right\}.$$

Aufgabe 3: *(7 Punkte)*

a) Finden Sie in $\left(\mathbb{Z}/1009\mathbb{Z}\right)^\times$ ein Element x, für das $15x = 22$ ist!

Lösung: Dazu muß zunächst das multiplikative Inverse von 15 bestimmt werden, d.h. wir müssen den ggT 1 von 15 und 1009 als Linearkombination dieser beiden Zahlen darstellen.

$$\begin{aligned} 1009 : 15 = 67 \quad \text{Rest } 4 &\Longrightarrow 4 = 1009 - 67 \cdot 15 \\ 15 : 4 = 3 \quad \text{Rest } 3 &\Longrightarrow 3 = 15 - 3 \cdot (1009 - 67 \cdot 15) = 202 \cdot 15 - 3 \cdot 1009 \\ 4 : 3 = 1 \quad \text{Rest } 1 &\Longrightarrow 1 = 1009 - 67 \cdot 15 - (202 \cdot 15 - 3 \cdot 1009) = 4 \cdot 2009 - 269 \cdot 15 \end{aligned}$$

Somit ist $-269 \cdot 15 \equiv 1 \bmod 1009$, also $-22 \cdot 269 \cdot 15 \equiv 22 \bmod 1009$.

$$-269 \cdot 22 = -5918 \equiv -5918 + 6 \cdot 1009 = 136 \bmod 1009\,,$$

also ist $x = 136$. Probe: $15 \cdot 136 = 2040 = 2 \cdot 1009 + 22$

b) Was ist $2^{20} \bmod 1009$?

Lösung: $2^{10} = 1024 \equiv 15 \bmod 1009$, also ist $2^{20} \equiv 15^2 = 225 \bmod 1009$.

c) Zeigen Sie, daß die Zwei eine primitive Wurzel modulo 29 ist!

Lösung: $\left(\mathbb{Z}/29\mathbb{Z}\right)^\times$ hat 28 Elemente; die Ordnung eines Elements ist nach LAGRANGE ein Teiler davon. Wäre die Zwei keine primitive Wurzel, wäre ihre Ordnung ein echter Teiler von 28; unter den beiden maximalen echten Teilern von 28, der Vier und der 14, gäbe es also mindestens einen, der ein Vielfaches der Ordnung wäre. $2^4 = 16$ ist auch modulo 29 von eins verschieden. $2^{10} = 1024 = 35 \cdot 29 + 9$, also ist

$$2^{14} \equiv 16 \cdot 9 = 144 \equiv 28 \equiv -1 \bmod 29\,.$$

Somit ist die Ordnung der Zwei kein echter Teiler von 28, also gleich 28. Die Zwei ist daher eine primitive Wurzel modulo 29.

Aufgabe 4: (*6 Punkte*)

a) $N = pqr$ sei ein Produkt dreier paarweise verschiedener Primzahlen. Zeigen Sie, daß für *jede* natürliche Zahl a gilt: $a^{(p-1)(q-1)(r-1)+1} \equiv a \bmod N$!

Lösung: Nach dem kleinen Satz von FERMAT ist $a^{p-1} \equiv 1 \bmod p$ für alle zu p teilerfremden Zahlen a. Damit ist für diese Zahlen auch $a^{(p-1)m} \equiv 1 \bmod p$ für jedes $m \in \mathbb{N}$ und $a^{(p-1)m+1} \equiv a \bmod p$. Insbesondere ist $a^{(p-1)(q-1)(r-1)+1} \equiv a \bmod p$. Eine nicht zu p teilerfremde natürliche Zahl a ist ein Vielfaches von p; solche a sind, wie auch alle ihre Potenzen, modulo p gleich null. Daher ist

$$a^{(p-1)(q-1)(r-1)+1} \equiv a \bmod p \qquad \text{für alle } a \in \mathbb{N}\,.$$

Genauso folgt, daß auch

$$a^{(p-1)(q-1)(r-1)+1} \equiv a \bmod q \quad \text{und} \quad a^{(p-1)(q-1)(r-1)+1} \equiv a \bmod r \qquad \text{für alle } a \in \mathbb{N}\,;$$

nach dem chinesischen Restesatz ist also $a^{(p-1)(q-1)(r-1)+1} \equiv a \bmod N$ für *alle* $n \in \mathbb{N}$.

b) Gilt dies auch, wenn man $(p-1)(q-1)(r-1)$ durch irgendein gemeinsames Vielfaches von $p-1$, $q-1$ und $r-1$ ersetzt?

Lösung: Natürlich; in diesem Fall arbeitet man im obigen Argument einfach mit anderen Faktoren m.

Aufgabe 5: (*7 Punkte*)

a) Die Zahl $N = 25\,591$ ist Produkt zweier ungefähr gleich großer Primzahlen. Finden Sie diese!

Lösung: Dazu ist das Verfahren von FERMAT am besten geeignet: $N+1$ und $N+4$ haben keine ganzzahlige Quadratwurzel, aber $N + 9 = 25\,600 = 160^2$. Daher ist

$$N = 160^2 - 3^2 = (160-3)(160+3) = 157 \cdot 163\,.$$

b) Finden Sie den kleinstmöglichen RSA-Exponenten e zum RSA-Modul N!

Lösung: e muß teilerfremd sein zu $p-1 = 156$ und $q-1 = 162$. Gerade e kommen somit nicht in Frage, und auch $e = 3$ ist Teiler sogar von beiden Zahlen. Keine der beiden ist aber durch fünf teilbar; daher ist $e = 5$ der kleinstmögliche Exponent.

c) Finden Sie zu diesem Exponenten e einen privaten Exponenten d!

Lösung: Dazu muß der ggT von e mit einem zu e teilerfremden gemeinsamen Vielfachen von $p-1$ und $q-1$ als Linearkombination dargestellt werden. 156 und 162 sind beide gerade und durch drei teilbar; also ist

$$\frac{156 \cdot 162}{6} = 4212$$

ein solches Vielfaches.

$$\begin{aligned} 4212 : 5 = 842 \quad \text{Rest } 2 &\Longrightarrow 2 = 4212 - 842 \cdot 5 \\ 5 : 2 = 2 \quad \text{Rest } 1 &\Longrightarrow 1 = 5 - 2 \cdot (4212 - 842 \cdot 5) = 1685 \cdot 5 - 2 \cdot 4212 \end{aligned}$$

Somit ist $1685 \cdot 5 \equiv 1 \bmod 4212$, und wir können $d = 1685$ setzen.

Aufgabe 6: *(4 Punkte)*

a) Zeigen Sie: Die Anzahl der Nullen, mit denen die Zahl $n!$ endet, ist $\sum_{i=1}^{\infty} \left[\frac{n}{5^i}\right]$!

Lösung: Für jede Primzahl p hat die maximale p-Potenz, die $n!$ teilt, den Exponenten $\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$. Die Anzahl der Nullen am Ende von $n!$ ist der Exponent der maximalen Zehnerpotenz, die $n!$ teilt, also das Minimum der obigen Ausdrücke für $p = 2$ und $p = 5$. Da jeder einzelne Summand monoton fallend mit p ist, gilt dasselbe für die Summe; das Minimum wird also für $p = 5$ angenommen, und das zeigt die Behauptung.

b) Wie viele Nullen stehen am Ende von $1000!$?

Lösung: $\sum_{i=1}^{\infty} \left[\frac{n}{5^i}\right] = \left[\frac{1000}{5}\right] + \left[\frac{1000}{25}\right] + \left[\frac{1000}{125}\right] + \left[\frac{1000}{725}\right] = 200 + 40 + 8 + 1 = 249\,.$

Aufgabe 7: *(4 Punkte)*

a) Was ist eine CARMICHAEL-Zahl?

Lösung: Eine CARMICHAEL-Zahl ist eine zusammengesetzte Zahl n mit der Eigenschaft, daß $a^{n-1} \equiv 1 \bmod n$ für alle zu n teilerfremden Zahlen $a \in \mathbb{Z}$.

b) Zeigen Sie, daß 1105 eine CARMICHAEL-Zahl ist! (*Hinweis:* $13 \cdot 17 = 221$)

Lösung: Wie aus der Vorlesung bekannt, ist n genau dann eine CARMICHAEL-Zahl, wenn für jeden Primteiler $p|n$ auch $p - 1$ Teiler von $n - 1$ ist. $1105 = 5 \cdot 221 = 5 \cdot 13 \cdot 17$. Da $1104 = 2^4 \cdot 3 \cdot 23$ durch vier, zwölf und sechzehn teilbar ist, folgt die Behauptung.

Aufgabe 8: *(8 Punkte)*

a) Faktorisieren Sie $N = 7991$ mit POLLARDs $(p-1)$-Methode mit Suchgrenze $B = 6$ und der Basis $a = 2$!

Lösung: Die Primzahlpotenzen kleiner oder gleich fünf sind $2^2 = 4, 3$ und 5. Wir ersetzen $a = 2$ nacheinander durch seine Potenzen modulo N mit diesen Exponenten. Zunächst wir $a = 2$ also ersetzt durch $a^4 = 16$, dann wird dies ersetzt durch $16^3 = 2^{12} = 4096$, und schließlich muß noch diese Zahl durch ihre fünfte Potenz modulo 7991 ersetzt werden:

$$4096 \cdot 4096 = 16\,777\,216 = 2099 \cdot 7991 + 4107\,;$$

also ist $4096^2 \equiv 4107 \bmod 7991$.

$$4107^2 = 16\,867\,449 = 2110 \cdot 7991 + 6439\,;$$

also ist $4096^4 \equiv 6439 \bmod 7991$.

$$4096 \cdot 6439 = 26\,374\,144 = 3300 \cdot 7991 + 3844\,;$$

also ist $4096^5 \equiv 3844 \bmod 7991$. Von der um eins verminderten Zahl 3843 bilden wir den ggT mit 7991:

$$\begin{aligned} 7991 : 3843 &= 2 \quad \text{Rest } 305 \\ 3843 : 305 &= 12 \quad \text{Rest } 183 \\ 305 : 183 &= 1 \quad \text{Rest } 122 \\ 183 : 122 &= 1 \quad \text{Rest } 61 \\ 122 : 61 &= 2 \quad \text{Rest } 0 \end{aligned}$$

Damit haben wir mit 61 einen nichttrialen Faktor gefunden; da $7991 : 61 = 131$, ist $7991 = 61 \cdot 131$.

b) Welche Bedingung muß die Suchgrenze B erfüllen, damit POLLARDs Methode für 7991 zum Erfolg führt?

Lösung: $61 - 1 = 60 = 2^2 \cdot 3 \cdot 5$ und $131 - 1 = 130 = 2 \cdot 5 \cdot 13$. Damit der Faktor 61 gefunden wird, muß also $B \geq 5$ sein; damit nicht auch 131 mit im ggT steckt, muß $B < 13$ sein, d.h. $5 \leq B \leq 12$.

Aufgabe 9: *(8 Punkte)*

a) Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{12}$!

Lösung: Der erste Koeffizient ist $c_0 = \lfloor\sqrt{12}\rfloor = 3$; übrig bleibt $\alpha_0 = \sqrt{12} - 3$.

$$\frac{1}{\alpha_0} = \frac{1}{\sqrt{12}-3} = \frac{\sqrt{12}+3}{12-9} = 1 + \frac{1}{3}\sqrt{12}$$

hat, da $3 \leq \sqrt{12} < 4$, größtes Ganzes zwei, also ist $c_1 = 2$ und $\alpha_1 = \frac{1}{3}\sqrt{12} - 1$.

$$\frac{1}{\alpha_1} = \frac{3}{\sqrt{12}-3} = \frac{3\sqrt{12}+9}{12-3^2} = \sqrt{12}+3$$

hat größtes Ganzes $c_2 = 6$ und $\alpha_2 = \sqrt{12} + 3 - 6 = \sqrt{12} - 3 = \alpha_0$. Somit wiederholt sich ab hier alles; die weiteren Koeffizienten sind abwechselnd zwei und sechs, d.h.

$$\sqrt{12} = [3; 2, 6, 2, 6, \dots] = [3; \overline{2, 6}] = 3 + \cfrac{1}{2 + \cfrac{1}{6 + \cfrac{1}{2 + \cfrac{1}{6 + \cfrac{1}{2 + \ddots}}}}}.$$

b) Finden Sie eine ganzzahlige Lösung der Gleichung $x^2 - 12y^2 = 1$!

Lösung: Wir wissen vom zehnten Übungsblatt, das für jede solche Lösung x/y eine Konvergente der gerade berechneten Kettenbruchentwicklung von $\sqrt{12}$ sein muß. Die erste Konvergente $3 = \frac{3}{1}$ liefert offensichtlich keine Lösung; die nächste ist $3 + \frac{1}{2} = \frac{7}{2}$, und hier ist $7^2 - 12 \cdot 2^2 = 49 - 12 \cdot 4 = 1$. Also ist $(7, 3)$ eine Lösung.

c) Was ist $x = [2; \overline{2}] = [2; 2, 2, 2, \dots] = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}$?

Lösung: Offensichtlich ist $x = 2 + \frac{1}{x}$, also $x^2 = 2x + 1$ oder $x^2 - 2x - 1 = 0$. Somit ist $(x-1)^2 = 2$, also ist x eine der beiden Zahlen $1 \pm \sqrt{2}$. Da der Kettenbruch gegen eine positive Zahl konvergiert, kommt nur $x = 1 + \sqrt{2}$ in Frage.