Disclaimer

Dies sind Notizen zu den Übungen der Zahlentheorie. Sie sind *ohne Gewähr* und *ohne Anspruch auf Vollständigkeit.* Der Author Christoph-Simon Senjak veröffentlicht diese Notitzen als zusätzliche Verständnis-Hilfe. Sie sind kurz gehalten und weder didaktisch noch typographisch aufbereitet. Ihre Lektüre ersetzt nicht das eigenständige Bearbeiten der Übungsblätter, die Anwesenheit in der Zentralübung und die Anfertigung eigener Notitzen!

Aufgabe 5

Sei $\alpha(p,n) = \max\{k \mid p^k \leq n\}$, und weiterhin $V(n) := \operatorname{lcm}\{1,\dots,n\}$, und außerdem $M = \frac{1}{2}V(n)$. Offenbar $\forall_p . p^{\alpha(p,n)} \mid V(n)$, und somit $V(n) = \prod_p p^{\alpha(p,n)}$. Also $M = 2^{\alpha(2,n)-1}\prod_{p>2} p^{\alpha(p,n)}$.

Behauptung: $M \cdot H_n \notin \mathbb{Z}$, woraus direkt folgt $H_n \notin \mathbb{Z}$:

Offenbar ist für jedes $k \neq 2^{\alpha(2,n)}$, $M \cdot \frac{1}{k} \in \mathbb{Z}$. Entsprechend ist $M(H_n - 2^{-\alpha(2,n)}) \in \mathbb{Z}$. Andererseits ist $M \cdot 2^{-\alpha(2,n)}$ sicher keine ganze zahl, weil $M = 2^{\alpha(2,n)-1}\prod_{p>2} p^{\alpha(p,n)}$. Dann kann MH_n ebenfalls keine ganze zahl sein, also sicher auch nicht H_n. □

Aufgabe 6

Teilaufgabe a

Sei

$$\lambda a + \mu b = ab - a - b$$

Dann also

$$(\lambda + 1)a + (\mu + 1)b = ab$$

Also $b \mid \lambda + 1$ und $a \mid \mu + 1$. Aber $\lambda + 1 = 0$ ist nicht möglich, da $\lambda \geq 0$. Dann muss aber $(\lambda + 1) \geq b$ sein. Analog muss $(\mu + 1) \geq a$ sein. Damit ist die Gleichung nicht mehr zu erfüllen. □

Teilaufgabe b

Es fällt auf dass $ab - a - b + 1 = (a-1)(b-1)$, also $m \geq (a-1)(b-1)$. Da a, b teilerfremd gibt es ganze zahlen λ_0, μ_0 mit $\lambda_0 a + \mu_0 b = m$, und da m positiv ist, muss mindestens eine der beiden Variablen positiv sein. Sei o.B.d.A. $\lambda_0 \leq 0$. Offenbar ist für alle ganzzahligen c auch $(\lambda_0 + cb)a + (\mu_0 - ca)b = m$. Wir können c so wählen, dass $0 \leq \lambda_0 + cb < b$. Dann gilt

$$\begin{aligned}(\lambda_0 + cb)a + (\mu_0 - ca)b &= m \\ (\mu_0 - ca)b &= m - \underbrace{(\lambda_0 + cb)a}_{\leq a(b-1)}\end{aligned}$$

aber $m - (\lambda_0 + cb)a \geq (a-1)(b-1) - a(b-1) = -(b-1)$. Wäre nun $(\mu_0 - ca)b \leq -(b-1)$, dann wäre aus Teilbarkeitsgründen $(\mu_0 - ca)b < -(b-1)$, also wäre insbesondere $\mu_0 - ca < 0$. Dann aber $(\mu_0 - ca)b \leq -b$. Aber $(\mu_0 - ca)b = m - (\lambda_0 + cb)a \geq -(b-1)$. Also ist $(\mu_0 - ca)b > -(b-1)$, also $\geq b - (b-1) = 1$. □

Teilaufgabe c

Offenbar sind nur die Zahlen $0 \leq n \leq 4 \cdot 6 = 24$ interessant, da der Rest nach Teilaufgabe b sowieso in $M_{5,7}$ ist. Diese sind:

$$\begin{aligned}
0 &= 0 \cdot 7 + 0 \cdot 5 \\
5 &= 0 \cdot 7 + 1 \cdot 5 \\
7 &= 1 \cdot 7 + 0 \cdot 5 \\
10 &= 0 \cdot 7 + 2 \cdot 5 \\
12 &= 1 \cdot 7 + 1 \cdot 5 \\
14 &= 2 \cdot 7 + 0 \cdot 5 \\
15 &= 0 \cdot 7 + 3 \cdot 5 \\
17 &= 1 \cdot 7 + 2 \cdot 5 \\
19 &= 2 \cdot 7 + 1 \cdot 5 \\
20 &= 0 \cdot 7 + 4 \cdot 5 \\
21 &= 3 \cdot 7 + 0 \cdot 5 \\
22 &= 1 \cdot 7 + 3 \cdot 5 \\
24 &= 2 \cdot 7 + 2 \cdot 5
\end{aligned}$$

Aufgabe 7

Teilaufgabe a

Seien zwei Zahlen $\xi, \eta \in \mathbb{Z}[\sqrt{d}]$ gegeben, und setze $\zeta := \frac{\xi}{\eta}$. Offenbar ist $\zeta \in \mathbb{Q}[\sqrt{d}]$, also $\zeta = z_1 + z_2\sqrt{d}$, mit $z_1, z_2 \in \mathbb{Q}$ und $N(\zeta) = z_1^2 - dz_2^2$. Nun gibt es zwei ganze Zahlen q_1, q_2 die jeweils minimalen Abstand zu z_1, z_2 haben, und es gibt rationale δ_1, δ_2, sodass $z_1 = q_1 + \delta_1, z_2 = q_2 + \delta_2$. Also

$$\frac{\xi}{\eta} = (q_1 + \delta_1) + (q_2 + \delta_2)\sqrt{d}$$

Also

$$\frac{\xi}{\eta} = \underbrace{(q_1 + q_2\sqrt{d})}_{\in \mathbb{Z}[\sqrt{d}]} + (\delta_1 + \delta_2\sqrt{d})$$

Wir wissen, dass $\delta_1, \delta_2 \leq \frac{1}{2}$. Damit ist $|N(\delta_1 + \delta_2\sqrt{d})| = |\underbrace{\delta_1^2}_{\leq \frac{1}{4}} - d\underbrace{\delta_2^2}_{\leq \frac{1}{4}}| < 1$ für $d \in \{2, 3\}$, also $|N(\eta(\delta_1 + \delta_2\sqrt{d}))| < |N(\eta)|$.

Teilaufgabe b

Es gilt $N(2) = 4$, $N(11) = 121$, $N(7 \pm 3\sqrt{3}) = 49 - 27 = 22$, zwei Elemente sind aber genau dann assoziiert, wenn sie die gleiche Norm haben. Dies ist kein Widerspruch, weil die Faktoren nicht prim in $\mathbb{Z}[\sqrt{3}]$ sind: $2 = -(1+\sqrt{3})(1-\sqrt{3})$, $11 = -(1 + 2\sqrt{3})(1 - 2\sqrt{3})$, $7 \pm 3\sqrt{3} = (1 \pm \sqrt{3})(1 \pm 2\sqrt{3})$.

Teilaufgabe c

$$22 = (1+\sqrt{3})^2(1+2\sqrt{3})(1-2\sqrt{3})$$

Aufgabe 9

$N(\sqrt{-5}) = 5$, somit ist $\sqrt{-5}$ irreduzibel. Außerdem ist $\sqrt{-5}(a+b\sqrt{-5}) = -5b+\sqrt{-5}a$, also ist der Realteil jeder durch $\sqrt{-5}$ teilbaren Zahl durch 5 teilbar. Ist umgekehrt der Realteil einer Zahl durch 5 teilbar, so gilt $5a+b\sqrt{-5} = \sqrt{-5}(b-a\sqrt{-5})$. Wegen $(a+b\sqrt{-5})(c+d\sqrt{-5}) = ac-5bd+(ad+bc)\sqrt{-5}$ folgt direkt dir Primalität von $\sqrt{-5}$.

$N(7) = 49$, und da $a^2+5b^2 = 7$ keine Lösungen hat, ist 7 damit irreduzibel. Andererseits ist $7^2 = 2^2+3^2\cdot 5 = (2+3\sqrt{-5})(2-3\sqrt{-5})$, aber $7 \nmid 2\pm 3\sqrt{-5}$.

$(2+5\sqrt{-5})(2-5\sqrt{-5}) = 29$, also ist 29 reduzibel, und kann damit auch nicht prim sein.

Aufgabe 10

Es gilt $m \mid x-a$ und $n \mid x-b$, also auch $d \mid x-a$ und $d \mid x-b$. Existiert ein solches x, ist damit insbesondere $d \mid (a-x)-(b-x) = a-b$, also $a \equiv b \mod d$. Sei umgekehrt $d \mid a-b$.

Man betrachte das Gleichungssystem

$$\begin{aligned} x &= a+\mu m \\ x &= b+\nu n \end{aligned}$$

Es gilt also $a+\mu m = b+\nu n$, somit $dt = a-b = \nu n-\mu m$. Also sind μ und ν durch d teilbar, also $t = \frac{\nu}{d}n-\frac{\nu}{d}m = \nu\frac{n}{d}-\mu\frac{m}{d}$. Da nun $\gcd(\frac{n}{d},\frac{m}{d}) = 1$, existiert eine Linearkombination, sodass $1 = \nu'\frac{n}{d}-\mu'\frac{m}{d}$. Damit $t = t\nu'\frac{n}{d}-t\mu'\frac{m}{d}$, also $a-b = t\nu' n-t\mu' m$, also $a+t\mu' m = b+t\mu' n = x$.

Seien nun $x_1 = a+\mu_1 m = b+\nu_1 n$ und $x_2 = a+\mu_2 m = b+\nu_2 n$. Nun ist $x_1-x_2 = (\mu_1-\mu_2)m = (\nu_1-\nu_2)n$. Also $n \mid x_1-x_2$ und $m \mid x_1-x_2$, also $\operatorname{lcm}(n,m) \mid x_1-x_2$.

Aufgabe 11

Teilaufgabe a

Modulo 2 sind die Fibonacci-Zahlen periodisch $0,1,1$, modulo 3 sind sie periodisch $0,1,1,2,0,2,2,1$, modulo 5 sind sie periodisch $0,1,1,2,3,0,3,3,1,4,0,4,4,3,2,0,2,2,4,1,0$, und Modulo 7 $0,1,1,2,3,5,1,6,0,6,6,5,4,2,6,1,0$.

Aufgabe 12

Teilaufgabe a

Es gilt $f_{n+1} = f_{n+1}f_1+f_nf_0 = f_{n+1}+0$. Per Induktion $f_{n+m+2} = f_{n+m}+f_{n+m+1} = f_{n+1}f_m+f_nf_{m-1}+f_{n+1}f_{m+1}+f_nf_m = f_{n+1}(f_m+f_{m+1})+f_n(f_{m-1}+$

$f_m) = f_{n+1}f_{m+2} + f_n f_{m+1}$.

Teilaufgabe b

Teil i ist klar, weil f_{n+m} eine Linearkombination ist aus f_n und f_m. Für Teil ii gilt zunächst für $k = 1$ trivialerweise $\gcd(f_n, f_n) = f_n$. Sei nun, als Induktionsschritt, bekannt, dass $f_n \mid f_{kn}$, also insbesondere $f_n \mid \gcd(f_n, f_{kn})$. Dann ist, mit Teil i, $f_n \mid \gcd(f_n, f_{kn}) \mid f_{(k+1)n} = f_{n+kn}$. Es ist $f_{19} = 113 \cdot 37$.

Aufgabe 13

Teilaufgabe a

Wir stellen fest, dass $x^2 = x \Leftrightarrow x(x-1) = 0$. Wir betrachten zunächst Primzahlpotenzen p^k. Wenn $x(x-1) \equiv 0 \mod p^k$, dann muss x oder $x-1$ teilbar sein durch p. Aber x und $x-1$ sind teilerfremd. Entsprechend kann nur eine der beiden Zahlen durch p teilbar sein. Dann muss sie auch durch p^k teilbar sein, denn das Produkt muss ein Vielfaches von p^k sein. Dann ist aber $x \equiv p^k$ oder $x - 1 \equiv p^k \mod p^k$. Also sind die einzigen idempotenten Elemente in $\mathbb{Z}/p^k\mathbb{Z}$ gleich 0 und 1.

Sei nun $m = \prod_i p_i^{k_i}$. Dann ist nach dem chinesischen Restsatz $\mathbb{Z}/m\mathbb{Z}$ isomorph zu $\prod_i \mathbb{Z}/p_i^{k_i}\mathbb{Z}$, und darin sind genau die Elemente idempotent, deren komponenten alle selbst idempotent, also 0 oder 1 sind. Damit gibt es so für jede Teilmenge an Primteilern ein idempotentes Element, also 2^r.

Teilaufgabe b

Es ist $60 = 3 \cdot 4 \cdot 5$. Die idempotenten Elemente sind:

$$\begin{aligned}
1 &= 0 \cdot 3 \cdot 4 \cdot 5 + 1 \\
16 &= 3 \cdot 5 + 1 = 4 \cdot 4 \\
21 &= 4 \cdot 5 + 1 = 3 \cdot 7 \\
25 &= 3 \cdot 4 \cdot 2 + 1 = 5 \cdot 5 \\
36 &= 7 \cdot 5 + 1 = 3 \cdot 3 \cdot 4 \\
40 &= 13 \cdot 3 + 1 = 2 \cdot 4 \cdot 5 \\
45 &= 4 \cdot 11 + 1 = 3 \cdot 3 \cdot 5 \\
60 &= 3 \cdot 4 \cdot 5
\end{aligned}$$

Aufgabe 14

Wir wissen, $(p-1)! \equiv -1 \mod p$ genau dann, wenn p prim. Es gilt

$$
\begin{aligned}
(p-1)! &= \\
&= \prod_{k=1}^{p-1} k \\
&= \prod_{k=1}^{\frac{p-1}{2}} k \cdot \prod_{k=\frac{p+1}{2}}^{p-1} k \\
&= \prod_{k=1}^{\frac{p-1}{2}} k \cdot \prod_{k=1}^{\frac{p-1}{2}} (p-k) \\
&\equiv \prod_{k=1}^{\frac{p-1}{2}} k \cdot \prod_{k=1}^{\frac{p-1}{2}} (-k) \\
&\equiv \prod_{k=1}^{\frac{p-1}{2}} k \cdot (-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k \\
&\equiv (-1)^{\frac{p-1}{2}} (\prod_{k=1}^{\frac{p-1}{2}} k)^2 \\
&\equiv (-1)^{\frac{p-1}{2}} (\frac{p-1}{2})!^2
\end{aligned}
$$

Aufgabe 15

Es gilt

$$
\begin{aligned}
\sum_{k\geq 1} \mu(k) F(x^{\frac{1}{k}}) &= \\
&= \sum_{k\geq 1} \mu(k) \sum_{l\geq 1} f(x^{\frac{1}{kl}}) \\
&= \sum_{n\geq 1} \sum_{k|n} \mu(k) f(x^{\frac{1}{n}}) \\
&= \sum_{n\geq 1} f(x^{\frac{1}{n}}) \sum_{k|n} \mu(k) \\
&= \sum_{n\geq 1} f(x^{\frac{1}{n}}) \delta_1(n) \\
&= f(x^{\frac{1}{1}}) = f(x)
\end{aligned}
$$

Aufgabe 16

Definiere

$$
g(n) := \sum_{1\leq k\leq n \, \gcd(k,n)=1} e^{2i\pi \frac{k}{n}}
$$

Es gilt $\sum_{\gcd(k,n)=d} e^{2i\pi\frac{k}{n}} = \sum_{gcd(k,\frac{n}{d})=1} e^{2i\pi\frac{kd}{n}} = g(\frac{n}{d})$. Weiterhin ilt $\sum_{d|n} g(\frac{n}{d}) = \sum_{d|n} g(d) = \sum_{k=1}^{n} e^{2i\pi\frac{k}{n}} = \delta_1(n)$, also nach dem möbius'schen Umkehrsatz $g(n) = \sum_{d|n} \mu(\frac{n}{d})\delta_1(d) = \mu(n)$.

Aufgabe 17

Teilaufgabe a

Lösung 1

Es ist $\tau(\prod_i p_i^{k_i}) = \prod_i (k_i + 1)$. Das Produkt ist ungerade genau dann, wenn all seine Faktoren ungerade sind. Das ist genau dann der fall, wenn alle k_i gerade sind.

Lösung 2

Zu jedem Teiler $d < \sqrt{n}$ existiert genau ein Teiler $\frac{n}{d} > \sqrt{n}$. Lediglich wenn $\sqrt{n} \in \mathbb{Z}$, existiert $\sqrt{n}$ als ungepaarter Teiler.

Teilaufgabe b

$n^{\tau(n)} = \prod_{d|n} n = \prod_{d|n} d\frac{n}{d} = (\prod_{d|n} d)(\prod_{d|n} \frac{n}{d}) = (\prod_{d|n} d)^2$.

Teilaufgabe c

Es ist $(\sum_{k=1}^{n+1} k)^2 = (\sum_{k=1}^{n} k + n + 1)^2 = (\sum_{k=1}^{n} k)^2 + 2(\sum_{k=1}^{n} k)(n+1) + (n+1)^2 = (\sum_{k=1}^{n} k)^2 + \frac{2n(n+1)(n+1)}{2} + (n+1)^2 = (\sum_{k=1}^{n} k)^2 + (n+1)^3$. Damit gilt nach Induktion $(\sum_{k=1}^{n} k)^2 = \sum_{k=1}^{n} k^3$. Für $n = p^k$ gilt damit bereits die zu beweisende Gleichung. Da die summatorische Funktion einer multiplikativen Funktion wieder Multiplikativ ist, gilt also für $n = \prod_i p_i^{k_i}$ dass $\sum_{d|n} \tau(d)^3 = \prod_i (\sum_h d \mid p_i^{k_i} \tau(d)^3) = \prod_i (\sum_{k=1}^{k_i} k^3) = \prod_i (\sum_{k=1}^{k_i} k)^2 = (\prod_i (\sum_{k=1}^{k_i} k))^2 = (\sum_{d|n} \tau(n))^2$.

Aufgabe 18

Wir nutzen die Darstellung $\phi(\prod_i p_i^{k_i}) = \prod_i p_i^{k_i-1}(p_i - 1)$

Teilaufgabe a

- i. $\prod_i p_i^{k_i-1}(p_i - 1) = 2$. Ist n durch irgendeine Primzahl $p \geq 5$ teilbar, wäre $\phi(n) \geq 4$. Ist $3 \mid n$, so ist $3^{k_2-1} \cdot 2 \mid 2$, was nur für $k_2 = 1$ möglich ist. Für

$2 \nmid n$, also $n = 3$, gilt nun $\phi(3) = 2$. Ist $2 \mid n$, dann muss $k_1 = 1$ gelten, denn sonst wäre $2^{k_1-1} \cdot 1 \neq 1$. Es bleibt also $n = 6$, und es gilt tatsächlich $\phi(6) = 2$. Ist nun $3 \nmid n$, bleibt $2^{2-1}(2-1)$, also $n = 4$, mit $\phi(4) = 2$.

- ii. $\prod_i p_i^{k_i-1}(p_i - 1)$ ist gerade, sobald ein $p_i \neq 2$ Teiler von n ist. Also kann nur $n = 2^k$ gelten, aber $\phi(2^k) = 2^{k-1} \neq 3$.
- iii. $10 = 2 \cdot 5 = \prod_i p_i^{k_i-1}(p_i - 1)$. Es ist also sicher $p_k \leq 10+1$, es bleiben also die Primfaktoren $2, 3, 5, 7, 11$. $7 \nmid 10$, und $7 - 1 \nmid 10$. $3 \nmid 10$. Andererseits ist $3 - 1 \mid 10$, aber $5 - 1 \nmid 10$. Somit bleiben nur noch die Faktoren 2 und 11, und diese sind Lösungen, $n = 11$ und $n = 22$.
- iv. Es bleiben die Primzahlen $2, 3, 5, 7, 11, 13$. Es ist $13, 13 - 1, 11, 11 - 1, 5, 5 - 1, 7 - 1, 3 \nmid 14$. Zwar sind $2, 3 - 1 \mid 14$, aber $7 - 1 \nmid 14$.

Teilaufgabe b

- i. Offenbar muss $2 \mid n$ gelten. Dann ist $\phi(n) = \prod_i p_i^{k_i-1}(p_i - 1) = 2^{k_1-1} \underbrace{\prod_{i>1} p_i^{k_i-1}(p_i - 1)}_{\text{gerade wenn } \neq 1}$. Also ist n eine Zweierpotenz, und weil $\phi(2^k) = 2^{k-1}$, sind die Lösungen genau die Zweierpotenzen ungleich 1.
- ii. Offenbar $3 \mid n$. Es ist $\phi(2^{k_1} 3^{k_2} \prod_{i>2} p_i^{k_i}) = 2^{k_1} 3^{k_2-1} \prod_{i>2} p_i^{k_i-1}(p_i - 1)$, und das Produkt der anderen Primzahlen ist wieder ungerade oder gleich 1, muss also 1 sein, denn sonst wäre der Exponent von 2 zu groß. Also gilt genau für die Zahlen $n \in \{2^n 3^m \mid m, n \in \mathbb{N}_1\}$ dass $\phi(n) = \frac{n}{3}$.

Aufgabe 19

Teilaufgabe a

Wir spalten n auf in $n = \underbrace{p_1 \cdot \ldots \cdot p_n}_{n_1} \cdot \underbrace{q_1^{k_1} \cdot \ldots \cdot q_k^{l_k}}_{n_2}$, wobei $\gcd(n_1, n_2) = 1$ und $l_i \geq 2$, und n_1 quadratfrei. Ist $d^2 \mid n$ und $d \neq 1$, so ist $d^2 | n_2$. Also haben wir

$$\sum_{d^2|n} \mu(d) = \sum_{d^2|n_2} \mu(d)$$

Wir müssen nur quadratfreie d betrachten, da sonst $\mu(d) = 0$. Ist $d^2 \mid n_2$, so ist auch $d \mid n_2$. Ist umgekehrt d quadratfrei und $d \mid n_2$, so auch $d^2 \mid n_2$. Für quadratfreies d ist $d \mid n_2$ aber äquivalent zu $d \mid q_1 \cdot \ldots \cdot q_l =: m$. Das heißt, wir haben

$$\sum_{d^2|n_2} \mu(d) = \sum_{d|m} \mu(d) = \delta_1(m) = \delta_1(n_2)$$

Aber $n_2 = 1$ gilt genau dann, wenn $n = n_1$ quadratfrei ist. Also

$$\sum_{d^2|n} \mu(d) = |\mu(n)| = \begin{cases} 1 & \text{für quadratfreies } n \\ 0 & \text{sonst} \end{cases}$$

Teilaufgabe b

Es ist bekanntlich $\frac{1}{\zeta(s)} = \sum_{n\geq 1} \frac{\mu(n)}{n^s}$. Also ist $\frac{1}{\zeta(2s)} = \sum_{n\geq 1} \frac{\mu(k)}{k^{2s}}$. Nun ist $\frac{1}{\zeta(2s)} \cdot \zeta(s) = (\sum_{n\geq 1} \frac{\mu(n)}{n^{2s}})(\sum_{n\geq 1} \frac{1}{n^s}) = \sum_{k,l\geq 1} \frac{\mu(k)}{(k^2 l)^s} = \sum_{n\geq 1} \frac{a(n)}{n^s}$ mit $a(n) = \sum_{k^2 l = n} \mu(k) = |\mu(n)|$ nach Teilaufgabe a.

Aufgabe 20

Sei $M(x) = \{n \in \mathbb{N}_1 : n \leq x\}$ und $A_k(x) = \{n \leq x : n = k^2 m, m \text{ quadratfrei}\}$. Dann ist insbesondere $A_1(x) = \operatorname{sqfr}(x)$. Außerdem sind alle A_k paarweise disjunkt, und somit $\dot{\bigcup}_{k\leq\sqrt{x}} A_k(x) = M(x)$, also $\sum_{k\leq\sqrt{x}} \#A_k(x) = \lfloor x \rfloor$. Offenbar ist $\#A_k(x) = \#A_1(\frac{x}{k^2}) = \#\operatorname{sqfr}(\frac{x}{k^2})$. Also $\sum_{k\leq\sqrt{x}} \#\operatorname{sqfr}(\frac{x}{k^2}) = \lfloor x \rfloor$, also $\sum_{k\leq x} \#\operatorname{sqfr}(\frac{x^2}{k^2}) = \lfloor x^2 \rfloor$. Sei nun $f(x) = \#\operatorname{sqfr} x^2$, dann ist $\sum_{k\leq x} \#\operatorname{sqfr}(\frac{x^2}{k^2}) = \sum_{k\leq x} f(x) = \lfloor x^2 \rfloor$. Nach dem Möbius'schen Umkehrsatz gilt nun $f(x) = \sum_{k\leq x} \mu(k) \lfloor (\frac{x}{k})^2 \rfloor$. Bekanntlich gilt $0 \leq \xi^2 - \lfloor \xi^2 \rfloor < 1$. Also $f(x) = \sum_{k\leq x} \mu(k)(\frac{x}{k})^2 + r_k(x)$, wobei $0 < |r_k(x)| \leq 1$. Also $f(x) = \sum_{k\leq x} r_k(x) + \sum_{k\leq x} \mu(k)(\frac{x}{k})^2$. Nun $\frac{f(x)}{x^2} = \sum_{k\leq x} \frac{r_k(x)}{x^2} + \sum_{k\leq x} \frac{\mu(k)}{k^2}$, und $0 \leq |\sum_{k\leq x} \frac{r_k(x)}{x^2}| \leq \sum_{k\leq x} \frac{|r_k(x)|}{x^2} \leq \sum_{k\leq x} \frac{1}{x^2} = \frac{\lfloor x \rfloor}{x^2} \to 0$ für $x \to \infty$. Also $\lim_{x\to\infty} \frac{f(x)}{x^2} = \lim_{x\to\infty} \frac{\#\operatorname{sqfr}(x^2)}{x^2} = \lim_{x\to\infty} \frac{\#\operatorname{sqfr} x}{x} = \lim_{x\to\infty} \sum_{k\leq x} \frac{\mu(k)}{k^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$.

Aufgabe 21

Teilaufgabe a

Seien $n, m > 1$. Dann ist $10^{nm} - 1 = (10^n - 1)(10^m + 10^{2m} + \ldots + 10^{(n-1)m})$.

Teilaufgabe b

Für den Fall $q = 3$ gilt $10^p \equiv 1 \mod 27$. Da $10 \not\equiv 1 \mod 27$, folgt, dass $\operatorname{ord}_{(\mathbb{Z}/27)^*}(10) = p$. Andererseits ist $\varphi(27) = 18$, also nach dem Satz von Euler $10^{18} \equiv 1 \mod 27$. Also $p \mid 18$. Aber $p > 3$, dies ist also nicht möglich. $q = 3$ kann also nicht auftreten.

Sei jetzt $q \neq 3$. Dann $10^p \equiv 1 \mod q$. Wäre $10 \equiv 1 \mod q$, wäre auch $q \mid 10 - 1 = 9$, was wegen $q \neq 3$ unmöglich ist. Somit $10 \not\equiv 1 \mod q$. Es folgt $\operatorname{ord}_{(\mathbb{Z}/q)*}(10) = p$. Aus dem kleinen Satz von Fermat $10^{q-1} \equiv 1 \mod q$ folgt nun $p \mid q - 1$, also $q = 1 + kp$. Da q und p ungerade sind, muss k gerade sein, also $q \equiv 1 \mod 2p$.

Beispiele

- Sei $p = 5$. Es ist $E(5) = 11111 = 41 \cdot 271$. Es sind $41 \equiv 271 \equiv 1 \mod 10$.

- Sei $p = 7$. Es ist $E(7) = 1111111 = 239 \cdot 4649$. Es sind $239 = 34 \cdot 7 + 1$, und $4649 = 664 \cdot 7 + 1$

Aufgabe 22

Lösung

Es ist bekanntlich $\zeta'(s) = -\sum_{n\geq 1} \frac{\log n}{n^s}$, und $\frac{1}{\zeta(s)} = \sum_{n\geq 1} \frac{\mu(n)}{n^s}$. Bekanntlich ist $\sum_{d|n} \Lambda(d) = \log n$. Also ist nach dem Möbius'schen Umkehrsatz $\Lambda = \mu * \log$. Andererseits ist $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n\geq 1} \frac{(\mu * \log)(n)}{n^s} = \sum_{n\geq 1} \frac{\Lambda(n)}{n^s}$.

Alternative Lösung

Mit der Produktdarstellung der Zetafunktion:

Es ist $-\frac{\zeta'(s)}{\zeta(s)} = -\frac{d}{ds}\log(\zeta(s)) = -\frac{d}{ds}\log\prod_p \frac{1}{1-p^{-s}} = -\frac{d}{ds}\sum_p -\log(1-p^{-s}) = \frac{d}{ds}\sum_p \log(1-p^{-s})$. Nun ist $-\log(1-p^{-s}) = \sum_{n=1}^{\infty} \frac{1}{np^{-sn}} \leq \sum_{n=1}^{\infty} \frac{1}{p^{-sn}} = p^{-s}\sum_{n=1}^{\infty} \frac{1}{p^n} = p^{-s}\frac{1}{1-p^{-1}} \leq 2p^{-s} \leq 2$. Also ist $|\sum_{p\geq\omega} \log(1-p^{-s})| \leq \sum_{p\geq\omega} |\log(1-p^{-s})| \leq \sum_{p\geq\omega} 2p^{-s} = 2\sum_{p\geq\omega} p^{-s}$. Sei nun ein beliebiges aber festes ε gegeben mit $s > 1+\varepsilon$. Dann ist $2\sum_{p\geq\omega} p^{-s} \leq 2\sum_{p\geq\omega} p^{-1-\epsilon}$, und dies konvergiert gegen 0 für $\omega \to \infty$, da es kleiner als die entsprechenden Teilsummen von $2\zeta(1+\varepsilon)$ ist, und ist unabhängig von s. Somit Konvergieren die Partialsummen von $\frac{d}{ds}\sum_p \log(1-p^{-s})$ uniform. Es ist nun $\sum_p \frac{d}{ds}\log(1-p^{-s}) = \sum_p \frac{\log p}{p^s-1} = \sum_p \frac{p^{-s}\log p}{1-p^{-s}} = \sum_p \frac{\log p}{p^s}\sum_{n=0}^{\infty} p^{-ns} \leq -\sum_p \frac{\log p}{p^s}\zeta(1+\varepsilon) = \zeta(1+\varepsilon)\sum_p \frac{\log p}{p^s} \leq \zeta(1+\varepsilon)\sum_p \frac{\log p}{p^{1+\epsilon}}$ und somit konvergiert die Reihe uniform, weshalb $\sum$ und $\frac{d}{dt}$ kommutieren. Es ist nun also $-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p}{p^s}\sum_{n=0}^{\infty} p^{-ns} = \sum_p (\log p)\sum_{n=0}^{\infty} p^{-n} = \sum_{n=0}^{\infty} \Lambda(n)n^{-s}$.

Aufgabe 23

Teilaufgabe a

Es ist $P(s)\zeta(s) = \sum_{n=1}^{\infty} \frac{(1_{\mathbb{P}} * 1)(n)}{n^s}$, und $(1_{\mathbb{P}} * 1)(n) = \sum_{d|n} 1_{\mathbb{P}}(d) = \omega(n)$.

Teilaufgabe b

Es ist $\sum_{n\geq 1} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$. Somit $\sum_{n\geq 1} \frac{(\mu*\omega)(n)}{n^s} = \frac{1}{\zeta(s)}P(s)\zeta(s) = P(s)$. Also $\mu * \omega = 1_{\mathbb{P}}$.

Aufgabe 24

Wir beweisen, dass sowohl (a) als auch (b) äquivalent sind zu

c) $Q(x) \sim \frac{x}{\log Q(x)}$

- (a) $\Rightarrow$ (c): Sei x beliebig aber fest, und n so gewählt dass $q_n \leq x < q_{n+1}$, also $n = Q(x)$. Dann auch $\frac{q_n}{n \log n} \leq \frac{x}{n \log n} < \frac{q_{n+1}}{n \log n} = \frac{q_{n+1} \cdot (n+1) \log(n+1)}{(n+1) \log(n+1) \cdot n \log n}$. Wir wissen nun, dass die rechte und die linke Seite gegen 1 gehen für $x \to \infty$. Also $\frac{x}{n \log n} = \frac{x}{Q(x) \log Q(x)} \to 1$.

- (c) $\Rightarrow$ (a): Seien eine Indexfolge (w_k) so gewählt, dass $q_1 = q_2 = \ldots = q_{w_1} < q_{w_1+1} = \ldots = q_{w_2} < \ldots$, also $q_i = q_j$ für $w_k < i, j \leq w_{k+1}$ und $w_k < w_{k+1}$. Also ist (q_{w_k}) eine strikt monotone Teilfolge von (q_n), und es gilt $Q(q_{w_k}) = w_k$.

  Sei nun $\alpha \in [0; 1)$ und $x_{\alpha,k} = (1-\alpha) q_{w_k} + \alpha q_{w_{k+1}}$. Wegen (c) gilt

  $$1 = \lim_{k \to \infty} \frac{x_{0,k}}{Q(x_{0,k}) \log Q(x_{0,k})} = \lim_{k \to \infty} \frac{q_{w_k}}{w_k \log w_k}$$

  Damit aber auch

  $$1 = \lim_{\alpha \to 1} \lim_{k \to \infty} \frac{x_{\alpha,k}}{Q(x_{\alpha,k}) \log Q(x_{\alpha,k})} = \lim_{k \to \infty} \frac{q_{w_{k+1}}}{w_k \log w_k}$$

  und somit

  $$1 = \lim_{k \to \infty} \frac{q_{w_{k+1}}}{w_k \log w_k} \cdot \frac{w_k \log w_k}{q_{w_k}} = \lim_{k \to \infty} \frac{q_{w_{k+1}}}{q_{w_k}}$$

  Sei nun n gegeben, und k so gewählt, dass $q_{w_k} < q_n = q_{w_{k+1}}$, also $w_k < n \leq w_{k+1}$.

  Somit $\frac{q_{w_k}}{n \log n} < \frac{q_n}{n \log n} = \frac{q_{w_{k+1}}}{n \log n}$. Also $\frac{q_{w_k}}{w_{k+1} \log w_{k+1}} < \frac{q_n}{n \log n} \leq \frac{q_{w_{k+1}}}{w_k \log w_k}$. Nun ist aber $q_{w_k} \sim q_{w_{k+1}} \sim w_{k+1} \log w_{k+1}$ und $q_{w_{k+1}} \sim w_k \log w_k$. Also $q_n \sim n \log n$.

- (b) $\Rightarrow$ (c): Ist $\lim_{x \to \infty} \frac{Q(x) \log x}{x} = 1$, so ist auch $\lim_{x \to \infty} (\log Q(x) + \log \log(x) - \log(x)) = 0$, also $\lim_{x \to \infty} (\log x)(\frac{\log Q(x)}{\log x} + \frac{\log \log(x)}{\log x} - 1) = 0$, also $\lim_{x \to \infty} \frac{\log Q(x)}{\log x} = 1$. Nun ist, mit (b), $(\lim_{n \to \infty} \frac{\log Q(x)}{\log x})(\lim_{n \to \infty} \frac{Q(x) \log x}{x}) = \lim_{n \to \infty} \frac{Q(x) \cancel{(\log x)} (\log Q(x))}{x \cancel{\log x}} = \lim_{n \to \infty} \frac{Q(x)(\log Q(x))}{x} = 1$.

- (c) $\Rightarrow$ (b): Es ist $\lim_{n \to \infty} \frac{Q(x) \log Q(x)}{x} = 1$, also $\lim_{n \to \infty} (\log Q(x) + \log \log Q(x) - \log x) = 0$, also $\lim_{n \to \infty} \log Q(x)(1 + \frac{\log \log Q(x)}{\log Q(x)} - \frac{\log x}{\log Q(x)}) = 0$. Da Q unbeschränkt ist, folgt $\lim_{x \to \infty} \frac{\log x}{\log Q(x)} = 1$. Nun ist $1 = (\lim_{x \to \infty} \frac{\log x}{\log Q(x)})(\lim_{x \to \infty} \frac{Q(x) \log Q(x)}{x}) = \lim_{x \to \infty} \frac{\log x \cdot \cancel{\log Q(x)} \cdot Q(x)}{\cancel{\log Q(x)} \cdot x} = \lim_{x \to \infty} \frac{Q(x) \log x}{x}$

Aufgabe 25

Teilaufgabe a

Bekanntlich ist $\sum_{0 < n \leq y} \frac{1}{n} = \log y + \gamma + o(1)$. Also $\sum_{x < n \leq 2x} \frac{1}{n} = \sum_{0 < n \leq 2x} \frac{1}{n} - \sum_{0 < n \leq x} \frac{1}{n} = (\log 2x + \gamma + o(1)) - (\log x + \gamma + o(1)) = \log 2 + o(1)$, wobei die $o(1)$-terme jeweils gegen 0 gehen.

Teilaufgabe b

Bekanntlich ist $\sum_{0<p\leq y} \frac{1}{p} = \log\log y + \beta + o(1)$. Somit $\sum_{x<p\leq x^2} \frac{1}{p} = \sum_{0<p\leq x^2} \frac{1}{p} - \sum_{0<p\leq x} \frac{1}{p} = \log\log x^2 + \beta + o(1) - \log\log x - \beta - o(1) = \log(2\log x) - \log\log x + o(1) = \log 2 + \log\log x - \log\log x + o(1) = \log 2 + o(1)$, wobei die $o(1)$-terme jeweils gegen 0 gehen.

Aufgabe 26

Es gilt

$$\int_n^{n+1} f(\lfloor x \rfloor)dx = \int_n^{n+1} f(n)dx = f(n)$$

und

$$\int_n^{n+1} f(\lceil x \rceil)dx = \int_n^{n+1} f(n+1)dx = f(n+1)$$

Andererseits ist wegen der Monotonie

$$\int_n^{n+1} f(\lfloor x \rfloor)dx \geq \int_n^{n+1} f(x)dx \geq \int_n^{n+1} f(\lceil x \rceil)dx$$

also

$$f(n) \geq \int_n^{n+1} f(x)dx \geq f(n+1)$$

Damit weicht $\int_n^{n+1} f(x)dx$ um höchstens $f(n)-f(n+1)$ von $f(n)$ bzw. $f(n+1)$ ab. Also weicht $\int_1^n f(x)dx = \sum_{k=1}^{n-1} \int_k^{k+1} f(x)dx$ um höchstens $\sum_{k=1}^{n} (f(k) - f(k+1))$ ab von $\sum_{k=1}^{n} f(k)$ und $\sum_{k=1}^{n} f(k+1)$. Aber

$$\sum_{1\leq k\leq n} (f(k) - f(k+1)) = f(1) - \underbrace{f(n+1)}_{o(1)}$$

Insbesondere ist damit $(f(n) - f(n+1))_n$ eine Nullfolge. Wir haben also gezeigt, dass

$$\lim_{n\to\infty} |\sum_{k=1}^{n} f(k) - \int_1^n f(k)dk| < \infty$$

Für $x \in \mathbb{N}$ ist die Aussage damit gezeigt. Sei nun $x \notin \mathbb{N}$. Dann ist

$$\sum_{1\leq n\leq x} f(n) - \int_1^x f(t)dt = \underbrace{\sum_{1\leq n\leq \lfloor x\rfloor} f(n) - \int_1^{\lfloor x\rfloor} f(t)dt}_{\text{konvergiert}} - \int_{\lfloor x\rfloor}^x f(t)dt$$

und

$$\int_{\lfloor x\rfloor}^x f(t)dt \leq \int_{\lfloor x\rfloor}^x f(\lfloor t\rfloor)dt \leq \int_{\lfloor x\rfloor}^{\lfloor x\rfloor+1} f(\lfloor t\rfloor)dt = f(\lfloor x\rfloor) = o(1)$$

Aufgabe 28

Teilaufgabe a

Es ist $a^2 \equiv 1 \mod p^k \Leftrightarrow p^k \mid a^2 - 1 \Leftrightarrow p^k \mid (a+1)(a-1)$. Da p ungerade ist, kann nicht gleichzeitig $p \mid a+1$ und $p \mid a-1$, also insbesondere entweder $p^k \mid a+1$ oder $p^k \mid a-1$. Damit bleiben die Lösungen $\pm 1 \mod p^k$.

Teilaufgabe b

Ist $2^k \mid (a+1)(a-1)$, so sind sicher sowohl $a+1$, als auch $a-1$, gerade, weil das Produkt gerade ist, und sich die Faktoren um 2 unterscheiden. Andererseits können nicht beide gleichzeitig durch 4 teilbar sein, da sie sich um 2 unterscheiden. Für $k \geq 2$ bedeutet $4 \nmid a \pm 1$ insbesondere, dass auch $2^k \nmid a \pm 1$.

Sei der Fall betrachtet, dass $4 \nmid a-1$. Dann muss jedenfalls $2^{k-1} \mid a+1$, da sonst das Produkt $(a+1)(a-1)$ nicht durch 2^k teilbar sein könnte. Das bedeutet, $a+1 = 2^{k-1}l$, also $a = 2^{k-1}l - 1$. Ist l gerade, also $l = 2l'$, so ist $a = 2^k l' - 1$, also $a \equiv -1 \mod 2^k$. Ist andererseits l ungerade, also $l = 2l'+1$, so ist $a = 2^k l' + 2^{k-1} - 1$, also $a \equiv 2^{k-1} - 1 \mod 2^k$.

Analog der Fall dass $4 \nmid a+1$.

Aufgabe 29

Teilaufgabe a

Seien $k, l \mid m$. Dann ist $(xy)^m = x^m y^m = 1$.

Sei umgekehrt $(xy)^m = x^m y^m = 1$. Wir können nun i, j als die k- bzw. l-reste wählen, sodass $m = km_k + i$ und $m = lm_l + j$, und damit $x^i y^j = 1$. Dann ist auch $x^{ik} y^{jk} = y^{jk} = 1$ und analog $x^{il} = 1$. Somit $l \mid jk$ und $k \mid il$. Sei nun $1 = \gcd(l,k)$. Dann gilt $l \mid j$ und $k \mid i$. Das ist aber nur möglich für $i = j = 0$.

Teilaufgabe b

Es ist $\operatorname{ord} y^d = l/d$, also wieder $\gcd(\operatorname{ord} x, \operatorname{ord} y^d) = 1$, und wir können Teilaufgabe a anwenden.

Aufgabe 30

Nach dem Lemma aus der Vorlesung wissen wir $p_i^{k_i} \mid \operatorname{ord}(x_i)$. Sei also $r_i := \operatorname{ord}(x_i)/p_i^{k_i}$ und $y_i = x_i^{r_i}$. Dann ist $\gcd(\operatorname{ord} y_i, \operatorname{ord} y_j) = \gcd(p_i^{k_i}, p_j^{k_j}) = 1$, also nach Aufgabe 29 auch $\operatorname{ord}(y_i y_j) = p_i^{k_i} p_j^{k_j}$, und analog $\operatorname{ord}(\prod_i y_i) = \prod_i p_i^{k_i} = n$.

Aufgabe 31

Durch Brute Force

Wir benutzen das folgende Haskell-Programm:

```
m_8_mod_p_x p x m = (m ^ 8) `mod` p == x
all_mod_p_x p x = filter (m_8_mod_p_x p x) [0..p]
```

und erhalten:

- `all_mod_p_x 29 1` → `[1,12,17,28]`
- `all_mod_p_x 29 7` → `[3,7,22,26]`
- `all_mod_p_x 29 14` → `[]`
- `all_mod_p_x 31 1` → `[1,30]`
- `all_mod_p_x 31 7` → `[13,18]`
- `all_mod_p_x 31 14` → `[10,21]`

Durch Überlegen

Zunächst machen wir uns eine Tabelle mit den Quadraten des Halbsystems.

```
        0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
mod 29  0  1  4  9 16 25  7 20  6 23 13  5 28 24 22 22
mod 31  0  1  4  9 16 25  5 18  2 19  7 28 20 14 10  8
```

Wir wissen: Sind $x_1, \ldots, x_n$ die Lösungen der Gleichung $x^n = 1$, und ist y eine Lösung der Gleichung $y^n = k$, so lassen sich die anderen Lösungen berechnen durch $x_1 y, \ldots, x_n y$. Es reicht also, die Gleichung $x^8 = 1$ vollständig zu lösen, und für die anderen Gleichungen nur eine Lösung zu finden.

Die Gleichung $x^8 \equiv 1 \mod 29$ ist gleichbedeutend mit $(x^4)^2 \equiv 1 \mod 29$. Das bedeutet, einer von zwei Fällen tritt ein.

- $x^4 \equiv 1 \mod 29$, also $(x^2)^2 \equiv 1 \mod 29$
  - $x^2 \equiv 1 \mod 29$
    - $x \equiv 1 \mod 29$
    - $x \equiv -1 \equiv 28 \mod 29$
  - $x^2 \equiv -1 \equiv 28 \mod 29$
    - $x \equiv 12 \mod 29$
    - $x \equiv -12 \equiv 17 \mod 29$
- $x^4 \equiv -1 \equiv 28 \mod 29$

- $x^2 \equiv 12 \mod 29$ nicht lösbar
- $x^2 \equiv 17 \mod 29$ nicht lösbar

Also $x \in \{1, 12, 17, 28\}$.

Wir suchen nun eine Lösung für $x^8 \equiv 7 \mod 29$. Also $x^4 \equiv -6$, also $x^2 \equiv 9$, also $x \equiv 3$. Wir erhalten als Lösungen also $3 \cdot 1 \equiv 3$, $3 \cdot 12 \equiv 7$, $3 \cdot 17 \equiv 22$, $3 \cdot 28 \equiv 26$. Da kein Quadrat in der Tabelle 14 ist, ist $x^8 \equiv 14 \mod 29$ nicht lösbar.

Bei 31 fällt auf, dass -1 keine Wurzel ist. Also können nur die Lösungen -1 und 1 existieren.

Für $x^8 \equiv 7$ folgt $x^4 \equiv 10$ oder $x^4 \equiv -10 \equiv 21$, letzteres ist nicht lösbar. Aus $x^4 \equiv 10$ folgt $x^2 \equiv 14$ oder $x^2 \equiv -14 \equiv 17$. weieder ist letzteres nicht möglich, und aus Ersterem folgt $x \equiv 13$ und $x \equiv -13 \equiv 18$.

Für $x^8 \equiv 14$ folgt $x^4 \equiv 18$, also $x^2 \equiv 7$, also $x \equiv 10$, und wir erhalten die Lösungen wieder durch Multiplikation, also 10 und $-10 \equiv 21$.

Aufgabe 32

Teilaufgabe a

Es ist $g^{p-1} = 1$. Also ist $g^{\frac{p-1}{2}}$ Lösung der quadratischen Gleichung $x^2 = 1$. Diese hat aber höchstens zwei Lösungen, nämlich 1 und -1, und 1 fällt weg weil $\operatorname{ord} g > \frac{p-1}{2}$. Somit $g^{\frac{p-1}{2}} = -1$, also $\log_g(-1) = \frac{p-1}{2}$.

Teilaufgabe b

Es ist $(g^{\log_g g'})^{\log_{g'} g} = g^{\log_g g' \log_{g'} g} = g$, was nur für Exponenten $\equiv 1 \mod p-1$ geht.

Aufgabe 33

Es ist

$$2^n \equiv \begin{cases} 1 \mod 5 & \text{für } n \equiv 0 \mod 4 \\ 2 \mod 5 & \text{für } n \equiv 1 \mod 4 \\ 4 \mod 5 & \text{für } n \equiv 2 \mod 4 \\ 3 \mod 5 & \text{für } n \equiv 3 \mod 4 \end{cases}$$

Damit ist

$$\left(\frac{2^n - 1}{5}\right) = \begin{cases} \left(\frac{0}{5}\right) = 0 & \text{für } n \equiv 0 \mod 4 \\ \left(\frac{1}{5}\right) = 1 & \text{für } n \equiv 1 \mod 4 \\ \left(\frac{3}{5}\right) = -1 & \text{für } n \equiv 2 \mod 4 \\ \left(\frac{2}{5}\right) = -1 & \text{für } n \equiv 3 \mod 4 \end{cases}$$

Es ist insbesondere $\gcd(5, 2^n - 1) \neq 1$ genau dann, wenn $n \equiv 0 \mod 4$, was ausgeschlossen ist für ungerade n. Es ist außerdem $2^n - 1 \equiv 3 \mod 4$ für ungerade $n \geq 3$

Also folgt mit dem QRG, dass $\left(\frac{5}{2^n-1}\right) = \left(\frac{2^n-1}{5}\right)$, also 1 für $n \equiv 1 \mod 4$ und -1 für $n \equiv 3 \mod 4$. Nach dem 1. Ergänzungssatz gilt dasselbe für $\left(\frac{-1}{n}\right)$.

Aufgabe 34

Teilaufgabe a

Nach dem Euler-Kriterium ist $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$. Aber a ist quadratischer Rest. Also $1 \equiv a^{\frac{p-1}{2}} \mod p$. Also $a \equiv a^{\frac{p-1}{2}+1} = a^{\frac{p+1}{2}} = (a^{\frac{p+1}{4}})^2 \mod p$.

Teilaufgabe b

Es ist $x = a^{\frac{p+1}{4}} = (x^2)^{\frac{p+1}{4}} = (x^{\frac{p+1}{4}})^2$.

Aufgabe 35

Wir beweisen dies durch Induktion nach m. Sei zunächst $m = 3$. Es gilt $\left(\frac{2}{3}\right) = -1 = (-1)^{\frac{8}{8}}$, da 2 kein Quadrat ist. Betrachte nun $\left(\frac{2}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{m-2}{m}\right)$. Es ist sicher $\gcd(m-2, m) = 1$, da m ungerade. Also ist $\left(\frac{m-2}{m}\right) = \left(\frac{m}{m-2}\right) = \left(\frac{2}{m-2}\right)$. Nach Induktionsannahme ist $\left(\frac{2}{m-2}\right) = (-1)^{\frac{(m-2)^2-1}{8}}$, und damit $\left(\frac{2}{m}\right) = (-1)^{\frac{m-1}{2}}(-1)^{\frac{(m-2)^2-1}{8}} = (-1)^{\frac{m-1}{2}+\frac{m^2-4m+3}{8}} = (-1)^{\frac{4m-4}{8}+\frac{m^2-4m+3}{8}} = (-1)^{\frac{m^2-1}{8}}$.

Aufgabe 36

Teilaufgabe a

Sei $\varphi = \frac{1+\sqrt{5}}{2}$. Es ist $\varphi^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{3+\sqrt{5}}{2} = 1+\varphi$. Weiterhin ist $\frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = \frac{1-5}{4} = -1$, also $\varphi^{-1} = -\frac{1-\sqrt{5}}{2}$.

Wir zeigen zunächst:

$$\varphi^n = F_n\varphi + F_{n-1}$$

Für $n = 1$ ist dies offensichtlich. Für $n > 1$ durch Induktion:

$$\begin{aligned}
\varphi^{n+1} &= \varphi \cdot \varphi^n = \\
&= \varphi \cdot (F_n\varphi + F_{n-1}) \\
&= F_n\varphi^2 + F_{n-1}\varphi = \\
&= F_n(\varphi + 1) + F_{n-1}\varphi = \\
&= (F_n + F_{n-1})\varphi + F_n = \\
&= F_{n+1}\varphi + F_n
\end{aligned}$$

Analog ist $(-\varphi^{-1})^2 = \frac{1-\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = \frac{3-\sqrt{5}}{2} = 1 + (-\varphi^{-1})$. Also können wir mit dem selben Argument zeigen, dass $(-\varphi^{-1})^n = F_n(-\varphi^{-1}) + F_{n-1}$.

Also

$$\varphi^n - (-\varphi^{-1})^n = F_n(\varphi - (-\varphi^{-1})) = F_n\sqrt{5}$$

also

$$F_n = \frac{\varphi^n - (-\varphi^{-1})^n}{\sqrt{5}}$$

Teilaufgabe b

$q \mid f_m \Leftrightarrow f_m \equiv 0 \mod q$, also $f_m = 0$ in $\mathbb{Z}/q$. Das gilt offenbar, wenn

$$(1+\sqrt{5})^m = (1-\sqrt{5})^m$$

Ist $\left(\frac{5}{q}\right) = 1$, so sind $1 \pm \sqrt{5} \in \mathbb{Z}/q$, und es muss gelten

$$(1+\sqrt{5})^{q-1} = (1-\sqrt{5})^{q-1}$$

Es ist $-1 \not\equiv 5$ und $1 \not\equiv 5$, also können wir den kleinen Satz von Fermat anwenden, und erhalten

$$(1+\sqrt{5})^{q-1} = (1-\sqrt{5})^{q-1} = 1$$

Ist $\left(\frac{5}{q}\right) = -1$, muss gelten

$$(1+\sqrt{5})^{q+1} = (1-\sqrt{5})^{q+1}$$

also

$$\left(\frac{1+\sqrt{5}}{1-\sqrt{5}}\right)^{q+1} = 1$$

Es ist

$$\begin{aligned}
\frac{1+\sqrt{5}}{1-\sqrt{5}} &= \frac{(1+\sqrt{5})^2}{(1-\sqrt{5})(1+\sqrt{5})} \\
&= \frac{1+2\sqrt{5}+5}{1-5} \\
&= -\frac{1}{4}(6+2\sqrt{5}) \\
&= -\frac{1}{2}(3+\sqrt{5})
\end{aligned}$$

Nun ist $(-\frac{3}{2})^2 - (-\frac{1}{2}\sqrt{5})^2 = \frac{9}{4} - \frac{5}{4} = 1$. Also ist $\frac{1+\sqrt{5}}{1-\sqrt{5}}$ Lösung der Pell'schen Gleichung mit $D = 5$. Bekanntlich hat diese die Ordnung $p+1$ wenn D kein quadratischer Rest ist. Also ist $(\frac{1+\sqrt{5}}{1-\sqrt{5}})^{p+1} = 1$.

Teilaufgabe c

Sei zunächst $\left(\frac{5}{q}\right) = 1$. Dann ist wieder

$$(1+\sqrt{5})^p \equiv (1-\sqrt{5})^p \mod q$$

also

$$(\frac{1+\sqrt{5}}{1-\sqrt{5}})^p \equiv 1 \mod q$$

Es ist aber sicher

$$(\frac{1+\sqrt{5}}{1-\sqrt{5}})^{q-1} \equiv 1 \mod q$$

da die einzelnen Potenzen 1 sind. Also $p \mid q-1$.

Sei nun $\left(\frac{5}{q}\right) = -1$. Dann ist wieder $\frac{1+\sqrt{5}}{1-\sqrt{5}}$ Lösung der Pell'schen Ungleichung (siehe oben). Also

$$(\frac{1+\sqrt{5}}{1-\sqrt{5}})^{q+1} \equiv 1 \mod q$$

und da wie vorher

$$(\frac{1+\sqrt{5}}{1-\sqrt{5}})^p \equiv 1 \mod q$$

wieder $p \mid q+1$.

Aufgabe 37

Modulare Betrachtungen sind jeweils Komponentenweise. Es sei $\omega = \begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix}$, und wir schreiben Skalare multipliziert mit der Einheitsmatrix als Skalare.

Als Induktionsanfang betrachten wir Pell$(\mathbb{Z}/p^2, D)$. Wir wissen, dass die Ordnung $p(p+1)$ ist, und dass Pell$(\mathbb{Z}/p, D)$ Zyklisch von Ordnung $p+1$ ist. Sei g Generator von Pell$(\mathbb{Z}/p, D)$. Ist $g^{p+1} \equiv 1 \mod p^2$, so ist $(g+p\omega)^{p+1} = g^{p+1} + (p+1)pg^p\omega = 1 + pg^{-1}\omega \neq 1 \mod p^2$, aber $(g+p\omega)^p \equiv g^p \equiv 1 \mod p$, also Erzeuger von Pell$(\mathbb{Z}/p, D)$.

Wir zeigen, dass g dann auch Generator ist von Pell$(\mathbb{Z}/p^2, D)$. Es reicht dafür zu zeigen, dass $g^{\frac{p(p+1)}{q}} \not\equiv 1 \mod p^2$ für alle Primteiler $q \mid p(p+1)$, denn jedenfalls ist $g^{p(p+1)} \equiv 1 \mod p^2$. Ist $q \mid p(p+1)$, so gibt es zwei Fälle:

Im 1. Fall ist $q = p$. Dann ist $g^{\frac{p(p+1)}{q}} = g^{p+1}$. Aber wir wählten g so, dass $g^{p+1} \not\equiv 1 \mod p^2$.

Im 2. Fall ist $q \mid p+1$ Primteiler von $p+1$. Angenommen $g^{\frac{p(p+1)}{q}} \equiv 1 \mod p^2$. Dann ist auch $g^{\frac{p(p+1)}{q}} \equiv 1 \mod p$. Nun ist $g = g_1 + g_2\omega$. Die Matritzen 1 und ω kommutieren, deshalb ist

$$(g_1+g_2\omega)^p = \sum_{\nu=0}^{p} \binom{p}{\nu} g_1^\nu (g_2\omega)^{p-\nu} \equiv g_1^p + (g_2\omega)^p = g_1^p + g_2^p D^{(p-1)/2}\omega =$$

$$g_1^p + g_2^p(\frac{D}{p})\omega = g_1^p - g_2^p\omega = g_1 - g_2\omega = \overline{g} \mod p$$

Ist nun aber $g^{\frac{p(p+1)}{q}} \equiv 1 \mod p$, so ist $\overline{g}^{\frac{p+1}{q}} \equiv 1 \mod p$. Aber da g ein Generator war, ist auch $\overline{g}$ ein Generator. Dies ist ein Widerspruch.

Im Induktionsschluss betrachten wir Pell$(\mathbb{Z}/p^{k+1}, D)$, und einen Generator g von Pell$(\mathbb{Z}/p^k, D)$. Die Gruppe hat die Ordnung $p^k(p+1)$. Wieder ist zu zeigen, dass $g^{\frac{p^k(p+1)}{q}} \not\equiv 1 \mod p^{k+1}$ für $q \mid p^k(p+1)$ Primteiler.

Für $q = p$ müssen wir zeigen $g^{p^{k-1}(p+1)} \not\equiv 1 \mod p^{k+1}$. Angenommen es wäre $g^{p^{k-1}(p+1)} \equiv 1 \mod p^{k+1}$. Dann wäre auch $g^{p^{k-1}(p+1)} \equiv 1 \mod p^k$. Andererseits ist g Generator von Pell$(\mathbb{Z}/p^k, D)$, also ist $g^{p^{k-2}(p+1)} \not\equiv 1 \mod p^k$, also $g^{p^{k-1}(p+1)} \equiv 1 + ap^{k-1} \mod p^{k+1}$ mit $p \nmid a$. Also $g^{p^k(p+1)} \equiv (1+ap^k)^p \equiv 1 + ap^{k+1} \not\equiv 1 \mod p^{k+1}$.

Für $q \mid p+1$ haben wir wieder: Angenommen $g^{\frac{p^k(p+1)}{q}} \equiv 1 \mod p^{k+1}$, dann ist $g^{\frac{p^k(p+1)}{q}} \equiv 1 \mod p$, und analog zu vorher $g^{p^k} \equiv \overline{g} \mod p$ oder $g^{p^k} \equiv g \mod p$, was jedenfalls wie vorher der Generatoreigenschaft von g widerspricht.

Aufgabe 38

Nach den Voraussetzungen ist $a^{N-1} \equiv 1 \mod N$ für $\gcd(a, N) = 1$, also ist N zumindest Carmichael-Zahl.

Seien $p, q \mid N$ zwei verschiedene Primteiler. Sei a quadratischer Rest modulo p und b nichtquadratischer Rest modulo q. Nach dem chinesischen Restsatz existiert nun ein c sodass $c \equiv a \mod p$ und $c \equiv b \mod q$.

Da N Carmichael, ist $p - 1 \mid N - 1$, also $\frac{p-1}{2} \mid \frac{N-1}{2}$, also $\frac{N-1}{2} = k\frac{p-1}{2}$ für ein $k \in \mathbb{Z}$. Also $c^{\frac{N-1}{2}} = (c^{\frac{p-1}{2}})^k \equiv (\frac{c}{p})^k = 1^k = 1 \mod p$.

Es ist $q-1 \mid N-1$. Wir zeigen nun, dass $r := \frac{N-1}{q-1}$ ungerade ist: Angenommen, $\frac{N-1}{q-1}$ wäre gerade. Dann würde für $q \nmid a$ gelten $a^{\frac{N-1}{2}} = (a^{\frac{q-1}{2}})^{2k} \equiv 1 \mod q$. Andererseits existiert wegen ii. ein a mit $a^{\frac{N-1}{2}} \equiv -1 \mod N$, also auch $a^{\frac{N-1}{2}} \equiv -1 \mod q$, was ein Widerspruch wäre.

Nun ist also r ungerade, also $c^{\frac{N-1}{2}} = (c^{\frac{q-1}{2}})^r \equiv (\frac{c}{q})^r = (-1)^r = -1 \mod q$.

Insgesamt ist damit $c \not\equiv 1 \mod q$ und $c \not\equiv -1 \mod p$, also $c \nmid \pm 1 \mod N$. Widerspruch.

Aufgabe 39

Angenommen N wäre nicht prim. Dann existiert ein primteiler $p \mid N$ mit $p \leq \sqrt{N}$. Ist $a^q \equiv 1 \mod N$, so ist auch $a^q \equiv 1 \mod p$. Andererseits ist nach Voraussetzung $a - 1$ und N und damit auch p Teilerfremd, und somit $a \not\equiv 1 \mod p$. Also $\mathrm{ord}_{(\mathbb{Z}/p)^*}(a) = q$. Aber $q > \sqrt{N} \geq p$. Widerspruch.

Aufgabe 40

Lösung 1

Es existiert ein Isomorphismus $\psi : (\mathbb{Z}/N)^* \xrightarrow{\sim} (\mathbb{Z}/p)^* \times (\mathbb{Z}/q)^*$, $\psi : a \mapsto (\alpha(a), \beta(a))$.

Es ist

$$N - 1 = pq - 1 = (p-1)(q-1) + (p-1) + (q-1)$$

Somit

$$a^{(N-1)/2} = a^{\frac{(p-1)(q-1)}{2}} a^{\frac{p-1}{2}} a^{\frac{q-1}{2}}$$

Modulo q erhalten wir:

$$\begin{aligned} a^{(N-1)/2} = \quad & (a^{\frac{q-1}{2}})^{p-1} a^{\frac{p-1}{2}} a^{\frac{q-1}{2}} \equiv & \mid \text{Euler} \\ & \underbrace{\left(\frac{a}{q}\right)^{p-1}}_{p \text{ ungerade}} \left(\frac{a}{q}\right) a^{\frac{p-1}{2}} \equiv \left(\frac{a}{q}\right) a^{\frac{p-1}{2}} = \\ & \left(\frac{a}{q}\right) a^{\frac{2q-2}{2}} = \left(\frac{a}{q}\right) a^{q-1} \equiv & \mid \text{Fermat} \\ & \left(\frac{a}{q}\right) \end{aligned}$$

Die zu erfüllende Gleichung modulo q reduziert also zu

$$\begin{aligned} \left(\frac{a}{N}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) &\equiv \left(\frac{a}{q}\right) \\ \left(\frac{a}{p}\right) &\equiv 1 \end{aligned}$$

Daraus folgt, da $q > 2$, $\left(\frac{a}{p}\right) = 1$ in ganz $\mathbb{Z}$, also muss a quadratischer Rest modulo p sein.

Modulo p gilt analog

$$\begin{aligned} a^{(N-1)/2} = (a^{\frac{p-1}{2}})^{q-1} a^{\frac{p-1}{2}} a^{\frac{q-1}{2}} &\equiv \\ \left(\frac{a}{p}\right)^q a^{\frac{q-1}{2}} = \left(\frac{a}{p}\right) a^{\frac{\frac{p+1}{2}+1}{2}} &= \\ a^{\frac{p-1}{4}} & \end{aligned}$$

und die Gleichung reduziert damit zu

$$\left(\frac{a}{q}\right) \equiv a^{\frac{p-1}{4}}$$

Nun hängt $\left(\frac{a}{q}\right)$ nur von $\beta(a)$ ab, während die Erfüllbarkeit der Gleichung nur von $\alpha(a)$ abhängt, weil wir modulo p arbeiten. Da ψ ein Isomorphismus ist, können wir a so wählen, dass $\alpha(a)$ und $\beta(a)$ beliebig sind, und nicht voneinander abhängen. Unabhängig von $\beta(a)$ hat die Gleichung $\left(\frac{a}{q}\right) \equiv a^{\frac{p-1}{4}}$ genau $\frac{p-1}{4}$ Lösungen. Andererseits kann man $\beta(a)$ frei wählen, also erhält man $\frac{(q-1)(p-1)}{4} = \frac{\varphi(N)}{4}$ Möglichkeiten.

Lösung 2

Da $q-1$ gerade und $p-1 = 2(q-1)$, folgt $4 \mid p-1$ und $8 \mid (q-1)(p-1) = \varphi(N) = \#(Z/N)^*$. Man berechnet $N-1 = (q-1)(2q+1) = \frac{p-1}{2}(2q+1)$. Sein nun g_1 eine Primitivwurzel modulo q. Damit gilt $g_1^{(q-1)/2} \equiv -1 \mod q \Rightarrow$

$g_1^{(N-1)/2} \equiv (-1)^{2p+1} \equiv -1 \mod q$. Sei g_2 eine Primitivwurzel modulo p und $\omega := g_2^{(p-1)/4}$. Da $\omega^2 \equiv -1 \mod p$, ist ω eine primitive 4-te Einheizwurzel modulo p. Es folgt $g_2^{(N-1)/2} \equiv g_2^{\frac{p-1}{4}(2q+1)} \equiv (-1)^q\omega \equiv -\omega \mod p$. Vermöge des Chinesischen Restsatzes $(\mathbb{Z}/N)^* \stackrel{\sim}{=} (\mathbb{Z}/q)^* \times (\mathbb{Z}/p)^*$ lässt sich jedes Element $x \in (\mathbb{Z}/N)^*$ repräsentieren als $x = x(k,l) \hat{=} (g_1^k, g_2^l) \in (\mathbb{Z}/q)^* \times (\mathbb{Z}/p)^*$ mit $k \in \mathbb{Z}/(q-1)$ und $l \in \mathbb{Z}/(p-1)$. Es ist dann $x^{(N-1)/2} = x(k,l)^{(N-1)/2} \hat{=} ((-1)^k, (-\omega)^l)$. Daraus folgt

$$\begin{aligned} x^{(N-1)/2} \equiv +1 &\quad\Leftrightarrow\quad k \text{ gerade und } 4 \mid l \\ x^{(N-1)/2} \equiv -1 &\quad\Leftrightarrow\quad k \text{ ungerade und } l \equiv 2 \mod 4 \end{aligned}$$

Die Anzahl der Elemente $x \in (\mathbb{Z}/N)*$ in beiden Fällen ist jewels $\varphi(N)/8$, so dass also für die Gruppe $G_\pm := \{x \in (\mathbb{Z}/N)^* : x^{(N-1)/2} = \pm 1\}$ gilt $\#G_\pm = \varphi(N)/4$.

Aufgabe 41

Bezeichne

$$\psi : \left| \begin{array}{c} \mathbb{Z}/N \stackrel{\sim}{\to} \mathbb{Z}/p \times \mathbb{Z}/q \\ x \mapsto (x \mod p, x \mod q) \end{array} \right.$$

den kanonischen Isomorphismus. Es ist $ed' = 1 + k\lambda(N)$. Sei zunächst $\gcd(x,N) = 1$. Es reicht zu zeigen, dass $x^{\lambda(N)} \equiv 1 \mod N$, denn daraus folgt dass $x^{ed'} \equiv x^{1+k\lambda(N)} \equiv x(1^k) \equiv x \mod N$. Es ist $\operatorname{ord}_p x \mid p-1$ und $\operatorname{ord}_q x \mid q-1$, also $\operatorname{lcm}(\operatorname{ord}_p x, \operatorname{ord}_q x) \mid \operatorname{lcm}(p-1, q-1)$. Es ist aber $\psi(x^{\operatorname{lcm}(\operatorname{ord}_p x, \operatorname{ord}_q x)}) = ((x \mod p)^{\operatorname{lcm}(\operatorname{ord}_p x, \operatorname{ord}_q x)}, (x \mod q)^{\operatorname{lcm}(\operatorname{ord}_p x, \operatorname{ord}_q x)}) = (1,1) = \psi(1)$, also $\operatorname{ord}_N x \mid \operatorname{lcm}(\operatorname{ord}_p x, \operatorname{ord}_q x) \mid \lambda(N)$.

Die Nullteiler sind genau die $\psi^{-1}(0,b)$ und $\psi^{-1}(a,0)$. Hier gilt $(\psi^{-1}(0,b))^{k \operatorname{lcm}(p-1,q-1)+1} = \psi^{-1}(0, b^{k \operatorname{lcm}(p-1,q-1)+1}) = \psi^{-1}(0, b(b^{k \operatorname{lcm}(p-1,q-1)})) = \psi^{-1}(0,b)$.

Nicht jedes d' erfüllt $ed' \equiv 1 \mod \varphi(n)$. Umgekehrt erfüllt aber jedes d dass $ed \equiv 1 \mod \lambda(N)$. Insbesondere ist $d' \equiv d \mod \lambda(n)$.

Aufgabe 42

Teilaufgabe a

Sei wieder der kanonische Isomorphismus ψ zwischen $\mathbb{Z}/N$ und $\mathbb{Z}/p \times \mathbb{Z}/q$ gegeben. Wir beweisen zunächst, dass es mindestens r Fixpunkte gibt. Sei $t = \gcd(e-1, p-1)$, also $t \mid e-1$ und $t \mid p-1$. Dann bildet $x \mapsto x^t$ immer jeweils t Elemente auf jedes Bildelement ab. Insbesondere haben wir Elemente $f_1, \ldots, f_t \in \mathbb{Z}/p^*$, sodass $f_i^t = 1$. Es ist nun aber $f_i^e = f_i^{\frac{e-1}{t}t+1} = (f_i^t)^{\frac{e-1}{t}} f_i = f_i$. Sei umgekehrt $f^e = f$ in $(\mathbb{Z}/p)^*$, und $f^e = f$. Dann insbesondere $f^{e-1} = 1$, also $f^{t\frac{e-1}{t}} = 1$. Aber $\gcd(\frac{e-1}{t}, p-1) = 1$, da $t = \gcd(e-1, p-1)$. Also existiert ein s, sodass $s\frac{e-1}{t} \equiv 1 \mod p-1$, und somit $1^s = ((f^t)^{\frac{e-1}{t}})^s = (f^t)^{k(p-1)+1} = 1^k f^t = f^t$. Es gibt also genau so viele Elemente $f^e = f$ wie Elemente $f^t = 1$. Außerdem ist $0^e = 0$. Somit haben wir mindestens $1+t$ Elemente. Analog für $\mathbb{Z}/q$ die Elemente $0, g_1, \ldots, g_u$. Nun ist $\psi(f_i, g_j)^e = \psi(f_i^e, g_j^e) = \psi(f,g)$. Also haben wir $(1+t)\cdot(1+u)$ Elemente.

Da sowohl in $\mathbb{Z}/p$ als auch in $\mathbb{Z}/q$ mindestens $0, 1, -1$ existieren, ist $r \geq 3 \cdot 3 = 9$.

Ein nichttrivialer Fixpunkt wäre ein Urbild von $(0, \pm 1)$, $(\pm 1, \pm 1)$ oder $(\pm 1, 0)$. Es ist $1 = \psi(1, 1)$. Haben wir ein Urbild $u = \psi(0, \pm 1)$, so ist $u \mp 1 = \psi((0, \pm 1) + (\pm 1, \mp 1)) = \psi(\pm 1, 0)$. Also $u \mp 1 \equiv \pm 1 \mod p$ und $q \mid u \mp 1$.

Man muss also eine Primzahl finden, sodass $f \equiv \pm 1 \mod p$ und $p \mid N$.

Teilaufgabe c

```
fastexpm n k m = if k == 0 then 1 else let x = fastexpm n (div k 2) m in
  mod (x * x * (if 1 == mod k 2 then n else 1))
isFix e m l = fastexpm l e m == l
filter (isFix 65 47299541) [0..47299540]
--> [0,1,6536748,6536749,13073497,34226044,40762792,40762793,47299540]
```

Aufgabe 43

Da p, q teilerfremd, ist nach dem chinesischen Restsatz wieder $\psi : x \mapsto (x \mod p, x \mod q)$ ein kanonischer Ringhomomorphismus zwischen $\mathbb{Z}/pq$ und $\mathbb{Z}/p \times \mathbb{Z}/q$. Es gilt wegen $ed \equiv 1 \mod (p-1)(q-1)$ auch $ed \equiv 1 \mod p-1$, also $ed = (p-1)k + 1$. Nun ist

$$\begin{aligned} x^{(p-1)k+1} &= \\ x \cdot x^{p-1} \cdot x^{(p-1)(k-1)} &= \\ x^p \cdot x^{(p-1)(k-1)} &= \qquad \mid \text{Carmichael} \\ x \cdot x^{(p-1)(k-1)} &= \\ x^{(p-1)(k-1)+1} & \end{aligned}$$

Durch wiederholte Anwendung erhalten wir damit $x^{ed} = x^{p-1+1} = x^p$.

Das Problem bei Carmichael-Zahlen ist, dass sie kleinere Faktoren haben, weshalb sie sich leichter faktorisieren lassen.

Aufgabe 44

Teilaufgabe a

Für eine quadratzahl $N = \lceil \sqrt{N} \rceil^2$ terminiert der Algorithmus sofort. Ansonsten lässt sich N faktorisieren in faktoren a und b, sodass $a < \sqrt{N}$ und $b > \sqrt{N}$. Da N ungerade ist, müssen a und b ungerade sein, und somit ist $\frac{b+a}{2}, \frac{b-a}{2} \in \mathbb{N}_1$. Es ist wegen AM-GM $\sqrt{N} < \frac{b+a}{2}$, also insb. $\lceil \sqrt{N} \rceil \leq \frac{b+a}{2}$. Nun ist $(\frac{b+a}{2} - \frac{b-a}{2})(\frac{b+a}{2} + \frac{b-a}{2}) = N$, also $(\frac{b+a}{2})^2 - N = (\frac{b-a}{2})^2$, spätestens dann terminiert der Algorithmus also. Das folgende Java-Programm

```
public class Doer                                          {

    static boolean isSquare (int a)                        {
        double sq = Math.sqrt(a)                           ;
        return sq == Math.ceil(sq)                        ;}

    static int[] factorize (int N)                         {
```

```
        int x = (int) Math.ceil(Math.sqrt(N))             ;

        while (!isSquare(x*x - N))                        {
          x++                                            ;}

        int y = (int) Math.sqrt(x*x - N)                  ;
        int[] ret = new int[2]                            ;
        ret[0] = x + y                                    ;
        ret[1] = x - y                                    ;
        return ret                                       ;}

    public static void main (String[] args)               {
        int[] fs = new int[] { 3763, 23843, 39889 }       ;
        for (int i = 0; i < fs.length; ++i)               {
            int[] r = factorize(fs[i])                    ;
            assert (fs[i] == r[0] * r[1])                 ;
            System.out.println(fs[i] + " = "
              + r[0] + " * " + r[1])                   ;}}}
```

sagt:

```
3763 = 71 * 53
23843 = 211 * 113
39889 = 353 * 113
```

Man beachte, dass man für große Zahlen (`BigInteger`) für die Wurzel das Newton-Verfahren benutzen würde. Die Nutzung von Floating-Point-Variablen funktioniert nur für kleine Zahlen.

Teilaufgabe b

Es ist $(x_0 + k)^2 - N = y^2$, und $u = x + y$ und $v = x - y$, also $2y = u - v$. Nun wissen wir, dass

$$\begin{aligned} y = \\ \sqrt{(\lceil\sqrt{N}\rceil^2 + k)^2 - N} = \\ \sqrt{(\lceil\sqrt{N}\rceil + N)(\lceil\sqrt{N}\rceil - N) + 2k\lceil\sqrt{N}\rceil + k^2} \geq \\ \sqrt{\sqrt{N}(2k + \frac{k^2}{\sqrt{N}})} = \\ \sqrt[4]{N}\sqrt{2k + \frac{k^2}{\sqrt{N}}} \end{aligned}$$

und somit

$$\alpha\sqrt[4]{N} \geq \sqrt[4]{N}\sqrt{2k + \frac{k^2}{\sqrt{N}}}$$

also

$$\alpha \geq \sqrt{2k + \frac{k^2}{\sqrt{N}}}$$

Für sehr große N ist $\frac{k^2}{\sqrt{N}}$ verschwindend, also haben wir

$$k \approx \alpha^2/2$$

Teilaufgabe c

Es ist $2^{m-7} \leq |p-q| \leq \alpha\sqrt[4]{N}$. Also

$$\begin{aligned} 2^{m-7} &\leq \alpha\sqrt[4]{2^{2m}} \\ 2^{m-7} &\leq \alpha 2^{\frac{m}{2}} \\ 2^{\frac{m}{2}-7} &\leq \alpha \\ 2^{249} &\leq \alpha \\ k &\approx 2^{497} \end{aligned}$$

was eine viel zu große Anzahl an Schritten ist.

Aufgabe 45

Das folgende Programm nutzt sich schnelle Faktorisierung aus, und die Tatsache, dass $ed \equiv 1 \mod (p-1)(q-1) \Rightarrow ed \equiv 1 \mod (p-1)$:

```
public class MiniRsa                                    {
    static boolean isSquare (int a)                     {
        double sq = Math.sqrt(a)                        ;
        return sq == Math.ceil(sq)                     ;}

    static int[] factorize (int N)                      {
        int x = (int) Math.ceil(Math.sqrt(N)), xxN      ;
        while (!isSquare(xxN = x*x - N)) x++            ;
        int y = (int) Math.sqrt(x*x - N)                ;
        return new int[] { x + y, x - y }              ;}

    static int crackMiniRsa (int N, int e)              {
        int[] Nf = factorize(N)                         ;
        int p = Nf[0]-1, q = Nf[1]-1, pq = p * q, d = 0 ;
        while ( (e * d) % p != 1 ) d++                  ;
        while ( (e * d) % pq != 1) d+=p                 ;
        return d                                       ;}

    public static void main (String[] args)             {
        System.out.println(crackMiniRsa(8881, 17))    ;}}
```

Den letzten Schritt kann man auch unter Anwendung des chinesischen Restsatzes und des Euklidischen Algorithmus machen. Jedenfalls ergibt sich $d = 5113$.

Aufgabe 46

Teilaufgabe a

Es ist die Folge $(x^m)_m$ auf jeden Fall periodisch, und die Periodenlänge t teilt $\varphi(N) = (p-1)(q-1)$. Andererseits ist $e^r \nmid (p-1)(q-1)$, also e kein Nullteiler im Ring $\mathbb{Z}/(p-1)(q-1)$. Somit ist $e^{\operatorname{ord} e} = 1$, also $x^{e^{\varphi((p-1)(q-1))}} = x$.

Aufgabe 47

Wir lösen die Aufgabe, indem wir uns programmatisch eine Tabelle der Exponenten von 11 anlegen, um schnell logarithmieren zu können:

```
import java.util.*                                          ;
public class Aufg47                                         {
    static class LogTable                                   {
        int N, modulus                                      ;
        Hashtable<Integer, Integer> logTable =
            new Hashtable<Integer, Integer>()               ;
        public LogTable (int N, int modulus)                {
            this.N = N                                      ;
            this.modulus = modulus                          ;
            int k = N, exp = 1                              ;
            do                                              {
                logTable.put(exp, k)                        ;
                ++exp                                       ;
                k = k * N % modulus                        ;}
            while (k != N)                                 ;}
        public int log(int n)                               {
            if (n == 0) return 1                            ;
            return logTable.get(n)                         ;}}
    public static void main(String[] args)                  {
        LogTable lt = new LogTable(11, 8039)                ;
        int alpha = lt.log(5655)                            ;
        int beta = lt.log(5802)                             ;
        int K = ((int) Math.pow(11, alpha*beta)) % 8039     ;
        System.out.println("alpha=" + alpha +"; beta="
                           + beta + "; K=" + K)            ;}}

// Ausgabe: alpha=1604; beta=5035; K=1460
```

Aufgabe 48

Teilaufgabe a

Ist $p \equiv 1 \mod 8$, so auch $p \equiv 1 \mod 4$, also $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = 1$. Ist $p \equiv 3 \mod 8$, ist $p \equiv -1 \mod 4$, also $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$, also $\left(\frac{-2}{p}\right) = 1$. Jedenfalls ist -2 quadratischer Rest, also existiert ein m mit $p \mid m^2 + 2$, also $p = (m + \sqrt{-2})(m - \sqrt{-2})$. Andererseits ist $p \nmid m \pm \sqrt{-2}$, entsprechend kann p nicht prim sein in $\mathbb{Z}[\sqrt{-2}]$. Also muss es eine Faktorisierung geben. Andererseits ist $\mathrm{N}(p) = p^2$, p kann also höchstens Produkt von zwei Zahlen sein. Das kann aber nur sein, wenn $p = (x + \sqrt{-2}y)(x - \sqrt{-2}y) = x^2 + 2y^2$.

Die umgekehrte Richtung folgt, da $x^2 + 2y^2$ für ungerade Zahlen immer 1 oder 3 mod 8 ist.

Teilaufgabe b

Ist $p = x^2 + 2y^2 = (x + \sqrt{-2}y)(x - \sqrt{-2}y) = \xi\bar{\xi}$, bedeutet dies, dass alle Faktoren in konjugierten Paaren vorkommen müssen. Für Primteiler wie aus Teilaufgabe a die sich so zerlegen lassen ist dies erfüllt. Für Primteiler $p \equiv 5, 7 \mod 8$ muss gelten, dass sie in gerader Potenz auftreten. Dieser Schluss lässt sich trivial umkehren.