Zahlentheorie Klausurzettel

coole tricks

- $(p-1)! \equiv -1 \bmod p$
- Falls $d := \gcd(a, M) \mid b$, hat $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{M}{d}$ eine Lösung
- $\sum_{i=0}^{k} b^i = \frac{b^{k+1}-1}{b-1}$
- $\varphi(n) = \prod_i \left(p_i^{k_i} - p_i^{k_i-1}\right)$
- $a^k \equiv 1 \bmod M \implies \mathrm{ord}_M(a) \mid k$
- $\mathrm{ord}_M(ab) = \mathrm{ord}_M(a)\mathrm{ord}_M(b)$ falls $\gcd(\mathrm{ord}_M(a), \mathrm{ord}_M(b)) = 1$

sätze

- chinesischer Restsatz: Sei $x \equiv c_k \bmod m_k$ gelöst mit Lösung $C \bmod M := \prod_i c_i$. Sei $x = My + C$, dann ist für $x \equiv c_{k+1} \bmod m_{k+1}$ die Lösung $y \equiv M^{-1}(c_{k+1} - C) \bmod m_{k+1}$.
- $\sum_{d|n} \varphi(d) = n$
- Euler: $a^{\varphi(M)} \equiv 1 \bmod M$
- Carmichael-Funktion: $\lambda(M) = \mathrm{lcm}_i\left(p_i^{k_i} - p_i^{k_i-1}\right)$
- verschärfter Euler: $a^{\lambda(M)} \equiv 1 \bmod M$
- Rabin: Sei $N - 1 = 2^k m$. Falls $a^m \not\equiv 1 \bmod N$ und $a^{2^j m} \not\equiv -1 \bmod N$, ist N zusammengesetzt. $P \geq 1 - \left(\frac{1}{4}\right)^n$
- Euler: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$
- quadratische Reziprozität: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
- Pépin: $F_n + 1$ prim $\implies 3^{\frac{1}{2}(F_n-1)} \equiv -1 \bmod F_n$ mit $F_n = 2^{2^n} + 1$
- Gauß'sches Lemma: $\left(\frac{a}{p}\right) = (-1)^{\mu}$ mit μ die Zahl der negativen Restklassen in $a, 2a, ..., \frac{p-1}{2}a \bmod p$
- Fermat: $p = a^2 + b^2 \implies p \equiv 1 \bmod 4$
- $n = a^2 + b^2 \implies n = 2^k m^2 \prod_i p_i$ mit $p \equiv 1 \bmod 4$
- Lagrange: $n = a^2 + b^2 + c^2 + d^2$
- Gauß: $n \neq 4^l(8k+7) \implies n = a^2 + b^2 + c^2$
- $n = a + b + c$ mit a, b, c Dreieckszahlen
- Hilbert: $g(k) = \min\left\{m \in \mathbb{N} \mid \forall n \in \mathbb{N} : n = \sum_{i=1}^{m} x_i^k, x_i \in \mathbb{N}\right\}$
- $n = \sum_{i=1}^{G(k)} x_i^k$ mit $n > C$. $G(k)$ sei der kleinstmögliche Wert
- Kettenbruch: $\langle b_0, b_1, ..., b_n \rangle = b_0 + \frac{1}{b_1 + \frac{1}{...+\frac{1}{b_n}}} = \frac{p_n}{q_n}$
  - Kettenbrüche bilden: $\alpha_0 = \alpha, a_i = \lfloor \alpha_i \rfloor, \alpha_{i+1} = \frac{1}{\{\alpha_0\}}$
- $\langle a_0, a_1, ..., a_n, x \rangle = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}$ mit $p_n = a_n p_{n-1} + p_{n-2}$ und $q_n = a_n q_{n-1} + q_{n-2}$
- $\mid \alpha - \frac{p_n}{q_n} \mid < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$
- Legendre: $\mid \alpha - \frac{p}{q} \mid < \frac{1}{2q^2} \implies \frac{p}{q}$ Teilbruch von α
- Standardform: Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ Lösung von $Ax^2 + Bx + C = 0$ mit $A > 0$ und $\gcd(A, B, C) = 1$. Dann ist $\alpha = \frac{P + \sqrt{D}}{Q}$ mit $D = \begin{cases} \frac{B^2 - 4AC}{4} & 2 \mid B \\ B^2 - 4AC & \text{else} \end{cases}$ und $(P, Q) = \begin{cases} (\mp\frac{B}{2}, \pm A) & 2 \mid B \\ (\mp B, \pm 2A) & \text{else} \end{cases}$
- $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ heißt reduziert, falls $\alpha > 1$ und $-1 < \mid \alpha < 0$ mit $\mid \alpha = \frac{P - \sqrt{D}}{Q}$
  - Falls $Q \mid (D - P^2)$, dann gilt: α ist reduziert $\implies 0 < P < \sqrt{D}$ und $\sqrt{D} - P < Q < \sqrt{D} + P$
  - es gibt nur endlich viele reduzierte α mit Diskriminante D.
- Lagrange: $\alpha = \langle \overline{a_0, a_1, ..., a_n} \rangle \implies \alpha$ ist reduziert
- $\sqrt{N} = \langle a_0, \overline{a_1, ..., a_n, 2a_0} \rangle$ mit $a_0 = \lfloor \sqrt{N} \rfloor$
- Pell'sche Gleichung: $x^2 - Ny^2 = 1$

- Sei $\sqrt{N} = \langle a_0, \overline{a_1, ..., a_n, 2a_0} \rangle$ mit Teilbrüchen $\frac{p_n}{q_n}$. Dann: $a_{n+1} = 2\lfloor \sqrt{N} \rfloor \implies p_n^2 - Nq_n^2 = (-1)^{n+1}$
- Seien (x_1, y_1) und (x_2, y_2) Lösungen, dann ist $(x_1x_2 + Ny_1y_2, x_1y_2 + y_1x_2)$ auch Lösung.
- Sei (p, q) gegebene Lösung, dann lassen sich mit $x + y\sqrt{N} = \left(p + q\sqrt{N}\right)^n$ weitere Lösungen (x, y) finden.
- abc-Vermutung: Sei $a + b = c$ und $\gcd(a, b, c) = 1$. Dann $\forall \varepsilon > 0 \exists C_\varepsilon > 0 : \left(c > C_\varepsilon \implies c < \operatorname{rad}(abc)^{1+\varepsilon}\right)$
- Dirichlet-Charakter mod m:
  - $\chi(a) = 0 \implies \gcd(a, m) > 1$
  - $a \equiv b \bmod m \implies \chi(a) = \chi(b)$
  - $\chi(a)\chi(b) = \chi(ab)$
- Hauptcharakter: $\chi_0(a) = (\gcd(a, m) == 1)$
- Index: $\operatorname{ind}_g(a) = \min\{i \in \mathbb{N} : g^i \equiv a \bmod p^e\}$
  - $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g(a) + \operatorname{ind}_g(b) \bmod \varphi(p^e)$
- $\sum\limits_{\chi \in \mathcal{C}_m} \chi(a) = \begin{cases} \varphi(m) & a \equiv 1 \bmod m \\ 0 & \text{else} \end{cases}$
- $\sum\limits_{a \in (\mathbb{Z}/m\mathbb{Z})^*} \chi(a) = \begin{cases} \varphi(m) & \chi = \chi_0 \\ 0 & \text{else} \end{cases}$
- Gauß-Summen: $g_{a(\chi)} = \sum\limits_{t=0}^{p-1} \chi(t) e\left(\frac{at}{p}\right)$ und $g_{a(\chi_0)} = \sum_{t=0}^{p-1} e\left(\frac{at}{p}\right)$ mit $e(x) = e^{2\pi i x}$
  - $g_{a(\chi)} = \begin{cases} 0 & p \mid a \\ \chi(a^{-1}) g_1(\chi) & \text{else} \end{cases}$
- Jacobi-Summe: $J(\chi, \psi) = \sum\limits_{\substack{0 \le a, b \le p-1 \\ a+b \equiv 1 \bmod p}} \chi(a)\psi(b)$
  - $J(\chi_0, \chi) = 0$, $J(\chi_0, \chi_0) = p$
  - $J(\chi, \overline{\chi}) = -\chi(-1)$
  - $J(\chi, \psi) = \frac{g(\chi)g(\psi)}{g(\chi\psi)}$ mit $\chi\psi \neq \chi_0$
- Faltung: $f * g(n) = \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right)$
- Möbius-Funktion: $\mu\left(n := \prod_{i=1}^r p_i\right) = \begin{cases} 1 & n = 1 \\ 0 & \exists p : p^2 \mid n \\ (-1)^r & \text{else} \end{cases}$
- $f(n) = \sum_{d \mid n} F(d) \mu\left(\frac{n}{d}\right)$ mit $F = f * \mathbb{1}$
- Quadratische Form: $F(x_1, ..., x_n) = \sum\limits_{1 \le i, j \le n} a_{i,j} x_i x_j = xAx^T$
  - Diskriminante: $D(F) = \det(A)$
- $F \sim G$, falls $\exists T = \mathbb{Z}^{n \times n}$ mit $\det(T) = 1$ und $B = TAT^T$. Dafür muss $\det(T) = \pm 1$ gelten.
- binäre quadratische Form: $f(x, y) = ax^2 + bxy + cy^2$
  - Diskriminante: $d(f) = b^2 - 4ac$
- Falls $d < 0$: $h(d) = \#\{(a, b, c) \in \mathbb{Z}^3 : \gcd(a, b, c) = 1, b^2 - 4ac = d, 0 < a < \sqrt{\frac{|d|}{3}} - a < b \le a < c \vee 0 \le b \le a = c\}$