Zusammenfassung Modulo-Arithmetik

1. Seien $a, b \in \mathbb{Z}$. Dann gibt es $\alpha, \beta \in \mathbb{Z}$ sodass $\alpha a + \beta b = \mathrm{ggT}(a, b)$.

2. Seien $m \in \mathbb{N}_{>0}$ und $a \in \mathbb{Z}$. Es gibt dann und nur dann ein $b \in \mathbb{Z}$ mit $ab \equiv 1 \bmod m$, wenn $\mathrm{ggT}(a, m) = 1$. In dem Fall heißt a invertierbar modulo m und es gibt genau ein solches b mod m, das manchmal auch als a^{-1} mod m geschrieben wird.

3. **Chinesischer Restsatz:** Seien $m, n \in \mathbb{N}_{>0}$ teilerfremd und $a \in \mathbb{Z}$. Dann ist a mod mn eindeutig bestimmt durch a mod m und a mod n. Umgekehrt gibt es für jede Restklasse b_1 mod m und b_2 mod n eine eindeutig bestimmte Restklasse a mod mn sodass $a \equiv b_1$ mod m und $a \equiv b_2$ mod n.

   Diese Bijektion zwischen $\{0, 1, \ldots, mn-1\}$ und $\{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\}$ gegeben durch $a \leftrightarrow (b_1, b_2)$ ist kompatibel mit Addition und Multiplikation mod mn bzw. mod m und mod n:

$$\begin{aligned} a + a' \bmod mn \quad &\longleftrightarrow \quad (b_1 + b_1' \bmod m,\ \ b_2 + b_2' \bmod n) \\ a \cdot a' \bmod mn \quad &\longleftrightarrow \quad (b_1 \cdot b_1' \bmod m,\ \ b_2 \cdot b_2' \bmod n) \end{aligned}$$

4. **Satz von Euler-Fermat:** Sei $m \in \mathbb{N}_{>0}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann gilt $a^{\varphi(m)} \equiv 1 \bmod m$. Dabei ist φ die *Euler'sche Phi-Funktion*, die die Anzahl der zu m teilerfremden Elemente von $\{1, 2, \ldots, m\}$ bezeichnet.

   - Spezialfall: **Kleiner Satz von Fermat:** Wenn $m = p$ prim ist und $p \nmid a$, dann gilt $a^{p-1} \equiv 1 \bmod p$. Äquivalent dazu: $a^p \equiv a \bmod p$ für alle $a \in \mathbb{Z}$.

5. **Ordnung eines Elementes:** Sei $m \in \mathbb{N}_{>0}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann gibt es eine kleinste ganze Zahl $r \geq 1$ sodass $a^r \equiv 1 \bmod m$. Diese Zahl heißt *Ordnung von a modulo m* und wird $r =: \mathrm{ord}_m(a)$ geschrieben. Die Ordnung hat folgende Eigenschaften:

   (a) $\mathrm{ord}_m(a) \mid \varphi(m)$
   (b) $\mathrm{ord}_m(a) = 1$ ist äquivalent zu $a \equiv 1 \bmod m$.
   (c) $\mathrm{ord}_m(a) = 2$ ist äquivalent zu $a^2 \equiv 1 \bmod m$ und $a \not\equiv 1 \bmod m$, etc.
   (d) $a^k \equiv 1 \bmod m \iff \mathrm{ord}_m(a) \mid k$.
   (e) $a^k \equiv a^l \bmod m \iff k \equiv l \bmod \mathrm{ord}_m(a)$.

6. **Primitivwurzeln:** Sei $m \in \mathbb{N}_{>0}$ und $a \in \mathbb{Z}$. Die Restklasse von a modulo m heißt *Primitivwurzel modulo m*, wenn $\mathrm{ggT}(a, m) = 1$ und $\mathrm{ord}_m(a) = \varphi(m)$. Äquivalent dazu: Für jedes $c \in \mathbb{Z}$ mit $\mathrm{ggT}(c, m) = 1$ gibt es ein $r \in \mathbb{N}_{>0}$ sodass $c \equiv a^r \bmod m$. Äquivalent dazu: Die Menge $\{a, a^2, a^3, \ldots\}$ enthält Repräsentanten jeder zu m teilerfremden Restklasse modulo m. Die Primitivwurzeln haben folgende Eigenschaften:

   (a) Eine Primitivwurzel modulo m existiert dann und nur dann, wenn $m \in \{1, 2, 4, p^k, 2p^k : p > 2 \text{ prim}, k \in \mathbb{N}_{\geq 1}\}$.
   (b) Wenn es mindestens eine Primitivwurzel modulo m gibt, dann gibt es insgesamt genau $\varphi(\varphi(m))$ Primitivwurzeln modulo m.

7. **Quadratische Reste:** Sei $m \in \mathbb{N}_{>0}$ und $a \in \mathbb{Z}$. Die Restklasse von a modulo m heißt *quadratischer Rest modulo m*, wenn es ein $b \in \mathbb{Z}$ gibt sodass $a \equiv b^2 \bmod m$. Anderenfalls heißt sie *quadratischer Nichtrest modulo m*. Aus dem chinesischen Restsatz folgt: Wenn $m = p_1^{e_1} \cdots p_r^{e_r}$ die kanonische Primfaktorzerlegung von m ist, dann ist a dann und nur dann ein quadratischer Rest modulo m, wenn a ein quadratischer Rest modulo $p_i^{e_i}$ ist für alle i.

8. **Quadratische Reste modulo einer Primpotenz:** Sei $a \in \mathbb{Z}, k \in \mathbb{N}_{\geq 1}$.

   - Sei $p > 2$ eine ungerade Primzahl und $p \nmid a$. Dann ist a genau dann ein quadratischer Rest modulo p^k, wenn a ein quadratischer Rest modulo p ist.
   - Sei $k \geq 3$ und $2 \nmid a$. Dann ist a genau dann ein quadratischer Rest modulo 2^k, wenn a ein quadratischer Rest modulo $2^3 = 8$ ist.

   Mit 7. und 8. ist die Frage der quadratischen Reste also reduziert auf: *"Was sind die quadratischen Reste modulo ungerader Primzahlen?"*. Diese Frage kann mit dem Legendre- und Jacobi-Symbol beantwortet werden.

9. **Legendre-Symbol:** Wenn p eine ungerade Primzahl ist und $a \in \mathbb{Z}$, dann ist das Legendre-Symbol $\left(\frac{a}{p}\right)$ definiert als

$$\left(\frac{a}{p}\right) := \begin{cases} +1 & a \text{ ist quadratischer Rest modulo } p \text{ und } p \nmid a \\ -1 & a \text{ ist quadratischer Nichtrest modulo } p \\ 0 & p \mid a. \end{cases}$$

   Das Legendre-Symbol hat folgende Eigenschaften:

   (a) Wenn p eine ungerade Primzahl ist, gilt $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$.

   (b) Daraus folgt einerseits Multiplikativität: $\left(\frac{a_1}{p}\right) \cdot \left(\frac{a_1}{p}\right) = \left(\frac{a_1 \cdot a_2}{p}\right)$, und andererseits: -1 ist genau dann ein quadratischer Rest modulo einer ungeraden Primzahl p, wenn $p \equiv 1 \bmod 4$.

10. **Jacobi-Symbol:** Wenn n eine ungerade natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{e_1} \cdots p_r^{e_r}$ ist, so ist das *Jacobi-Symbol* $\left(\frac{a}{n}\right)$ für $a \in \mathbb{Z}$ definiert als $\left(\frac{a}{n}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i}$, wobei die Symbole auf der rechten Seite Legendre-Symbole sind. Eigenschaften:

    (a) Wenn n eine ungerade Primzahl ist, sind Legendre- und Jacobi-Symbol per Definition ident.

    (b) Das Jacobi-Symbol hängt nur von a modulo n und n ab.

    (c) Das Jacobi Symbol ist oben und unten multiplikativ: $\left(\frac{a_1}{n}\right) \cdot \left(\frac{a_1}{n}\right) = \left(\frac{a_1 \cdot a_2}{n}\right)$ und $\left(\frac{a}{n_1}\right) \cdot \left(\frac{a}{n_2}\right) = \left(\frac{a}{n_1 \cdot n_2}\right)$ für $a, a_1, a_2 \in \mathbb{Z}$ und ungerade $n, n_1, n_2 \in \mathbb{N}$.

    (d) Reziprozitätsgesetz: $\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}} \left(\frac{n}{m}\right)$ für alle teilerfremden ungeraden natürlichen Zahlen $m, n > 1$.

    (e) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} +1 & n \equiv 1 \bmod 4 \\ -1 & n \equiv 3 \bmod 4 \end{cases}$

    (f) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} +1 & n \equiv \pm 1 \bmod 8 \\ -1 & n \equiv \pm 3 \bmod 8 \end{cases}$

    Achtung! Das Jacobi-Symbol $\left(\frac{a}{n}\right) \in \{-1, 0, 1\}$ trifft nur dann eine Aussage darüber, ob a ein quadratischer Rest modulo n ist, wenn n eine (ungerade) Primzahl ist. Es ist dennoch praktisch, um die Werte des Legendre-Symbols effizient auszurechnen. Der Algorithmus dazu ähnelt dem euklidischen Algorithmus zur Berechnung des ggT (siehe Wikipedia oder Raach-Skripten).

Anmerkung. Die Punkte 7.-10. besprechen, welche Restklassen modulo n quadratische Reste sind. Eine naheliegende nächste Frage ist, welche Restklassen sich als dritte, vierte oder höhere Potenzen darstellen lassen: *"Sei $d \in \mathbb{N}$. Welche Restklassen modulo n sind Kongruent zu x^d für irgendein $x \in \mathbb{Z}$?"* Die Antwort für $d > 2$ ist selbst für Primzahlen $n = p$ etwas komplizierter und hängt von $p - 1 \bmod d$ ab. Zum Beispiel kann es passieren, dass jede Restklasse modulo p eine d-te Potenz ist. Das passiert genau dann, wenn $\mathrm{ggT}(p-1, d) = 1$. Die Situation für $d = 2$ ist deshalb einfacher, weil für ungerade Primzahlen $\mathrm{ggT}(p-1, 2)$ immer $2 \neq 1$ ist.

Anmerkung. Natürlich gibt es viele andere interessante Themen, die dem zahlentheoretischen Allgemeinwissen zugeordnet werden können, wie z.B. das LTE-Lemma, pythagoräische Tripel (die durch die *indischen Formeln* gegeben sind), zahlentheoretische Funktionen, Carmichael-Zahlen, Kreisteilungspolynome, die pellsche Gleichung und viele mehr. Der Fokus dieses Blattes liegt aber bewusst auf den grundlegenden Strukturen der Modulo-Arithmetik (sprich: Die Struktur des Ringes $\mathbb{Z}/m\mathbb{Z}$ für fixes $m \in \mathbb{N}_{>0}$).