Euklidische Division

1. Euklidische Division:

- Landau Notation: $f(n) = \mathcal{O}(g(n))$.
- Definitionen: Gruppe, Ring, Ideal
- Teilbarkeit und Teilbarkeit mit Rest (euklidisch)
- Beispiel für euklidische Ringe
  - $\mathbb{Z}$ euklidisch mit $N(x) = |x|$
  - $\mathbb{Z}[i]$ mit $N(z) = z\bar{z}$
  - $\mathbb{Z}[X]$ mit $N(p) = \mathrm{grad}(p)$
- Prim $\Rightarrow$ irreduzibel, aber irreduzibel $\not\Rightarrow$ prim.
- Faktoriell: In Primelemente zerlegbar.
- Euklidisch $\Rightarrow$ Hauptidealring $\Rightarrow$ faktoriell
- ggT, Lemma von Bézout: $\exists x, y$ mit $\mathrm{ggT}(a, b) = xa + yb$.
- Euklidischer Algorithmus, Erweiterter Euklidischer Algorithmus

Kongruenzrechnung

2. Kongruenzrechnung:

- $a \equiv b \bmod n \Leftrightarrow n | (a - b)$
- Binomische Formel mod p: $(a+b)^p \equiv a^p + b^p \bmod p$.
- Kleiner Fermat: $a^p \equiv a \bmod p$.
- Lemma über Teiler und Vielfache:

$$a \equiv b \bmod n \text{ gilt modulo aller Teiler von } n \text{ und}$$
$$a \equiv b \bmod n \Leftrightarrow ma \equiv mb \bmod mn.$$

- Lineare Gleichungen $ax \equiv b \bmod n$. Sei $d = \mathrm{ggT}(a, n) = ya + zn$. Löse als $x \equiv y\frac{b}{d} \bmod \frac{n}{d}$.
- Wichtiger Spezialfall $d = 1$: Multipliziere mit $y = a^{-1} \bmod n$.
- Chinesischer Restsatz: Lösung für $a_i x \equiv b \bmod n_i$, $i = 1, \ldots, n$. Sei $n = \prod_{i=1}^{s} p_i^{r_i}$. Dann gilt $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}$.

3. Restklassen:

- Additive Gruppe: $\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} | a \in \mathbb{Z}\}$.
- Multiplikative Gruppe: $U_n = (\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \mid \mathrm{ggT}(a, n) = 1\}$.
- Eulersche φ-Funktion: $\varphi(n) := |U_n|$.
- Für $n = \prod_{i=1}^{s} p_i^{r_i}$ gilt $\varphi(n) = \prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1)$. Mittels CRT gilt
$$U_n \cong U_{p_1^{r_1}} \times \ldots \times U_{p_s^{r_s}}.$$
- Satz von Euler: $a^{|G|} = 1$.
- Satz von Lagrangre: $\mathrm{ord}(a) || G|$.
- Endliche Körper $\mathbb{F}_p$: $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper gdw p prim.
- Konstruktion von $\mathbb{F}_{p^r}$ mittels irreduziblem $q(X)$, $\mathrm{grad}(q(X)) = r$.

Struktur abelscher Gruppen

4. Struktur abelscher Gruppen

- Jede zyklische Gruppe ist abelsch.
- Isomorphiesatz:

  Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$.
- Darstellung von Gruppen
- Klassifikationssatz: $G \cong \mathbb{Z}^r \times \prod_{i=1}^{\ell} \mathbb{Z}/n_i\mathbb{Z}$.
- Normalformen: Primteiler und Elementarteiler.
- U_n ist zyklisch gdw $n = 2, 4$, $n = p^r$ oder $n = 2p^r$.

Quadratische Gleichungen

5. Quadratische Gleichungen:

- Allgemeine Wurzelberechnung mit Hilfe des diskreten Logarithmus, Baby-Step Giant-Step Algorithmus
- Quadratische Reste und das Legendre-Symbol
- Euler-Identität: $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$.
- $(\frac{-1}{p}) = (-1) \Leftrightarrow p \equiv 3 \bmod 4$, $(\frac{2}{p}) = (-1) \Leftrightarrow p \equiv \pm 3 \bmod 8$.
- Reziprozität: $(\frac{q}{p}) = -(\frac{p}{q}) \Leftrightarrow p \equiv q \equiv 3 \bmod 4$, sonst $(\frac{q}{p}) = (\frac{p}{q})$.
- Berechnung des Jacobi-Symbols (analog Euklidischer Alg.).
- Quadratwurzel-Berechnung: Algorithmus von Tonelli und Shanks.

Kettenbrüche und Primzahltests

6. Kettenbrüche:

- Kettenbruchalgorithmus (analog zum Euklidischen Algorithmus)
- Terminierung des Algorithmus gdw Eingabe rational.
- Konvergenz der Näherungsbrüche und Best-Approximation.
- Jede sehr gute rationale Approximation ist ein Näherungsbruch.

7. Primzahltests:

- Lucas-Test: $a^{n-1} \equiv 1 \bmod n$, $a^{\frac{n-1}{q}} \not\equiv 1 \bmod n$.
- Pocklington-Test: $a^{n-1} \equiv 1 \bmod n$ und $\mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) = 1$.
- Carmichael-Zahlen: $a^{n-1} \equiv 1 \bmod n$ für alle $a \in U_n$.
- Solovay-Strassen Test: $a^{\frac{n-1}{2}} \overset{?}{\equiv} (\frac{a}{n}) \bmod n$.
- Miller-Rabin Test: $a^d \equiv 1$ oder $a^{2^k d} \equiv (-1)$ für $n - 1 = 2^r d$.

Faktorisierung und Lösen polynomieller Gleichungen

8. Faktorisierung:

- Fermat Faktorisierung: Konstruiere Quadrat $y^2 = x^2 - n$.
- Faktorisierung mit Faktorbasen
  - Morrison-Brillhart mittels Kettenbrüchen
  - Quadratisches Sieb
- Pollards $(p-1)$-Methode: Berechne Vielfaches k von $p-1$.
- Quadratische Erweiterung $\mathbb{F}_p^2 = \mathbb{F}_p[\sqrt{D}] \cong \mathbb{F}_p[X]/(X^2 - D)$.
- Froebenius-Automorphismus $f_p : x \mapsto x^p \bmod p$
- Cippolas Algorithmus
- Williams $(p+1)$-Methode

9. Lösen polynomieller Gleichungen:

- Liften quadratischer Gleichungen, p-adische Zahlen
- Hensel-Lemma: $f(\tilde{x} + ap^k) \equiv 0 \bmod p^{k+1} \Leftrightarrow f'(\tilde{x})a \equiv -\frac{f(\tilde{x})}{p^k} \bmod p$.
- Lösen von Gleichungen modulo n mittels Liften und CRT.