Primzahltest

- Wir wollen testen, ob eine gegebene Zahl n eine Primzahl ist.
- Effizienter Algorithmus zum Faktorisieren ist unbekannt.
- Kontraposition des Kleinen Satzes von Fermat liefert:
  Falls $a^{n-1} \neq 1 \bmod n$ für ein $a \in \mathbb{Z}_n^*$, dann ist n nicht prim.
- Leider muss ein solcher Zeuge $a \in \mathbb{Z}_n^*$ nicht immer existieren.

Definition Carmichael-Zahl

Sei $n \in \mathbb{N}$ zusammengesetzt. Wir bezeichnen n als *Carmichael-Zahl* falls $a^{n-1} = a \bmod n$ für alle $a \in \mathbb{Z}_n^*$.

Bsp:

- Die kleinsten Carmichael-Zahlen sind 561, 1105, 1729, 2465.
- Es gibt unendlich viele Carmichael-Zahlen (Beweis 1994).

Definition Fermatsche Pseudoprimzahl-Basis

Sei $n \in \mathbb{N}$ zusammengesetzt. Wir bezeichnen $a \in \mathbb{Z}_N^*$ als *Pseudoprimzahl-Basis* für n, falls $a^{n-1} = 1 \bmod n$.

Dichte der Pseudoprimzahl-Basen

Satz Pseudoprimzahlen-Basen bilden Untergruppe

Sei $n \in \mathbb{N}$ zusammengesetzt und keine Carmichael-Zahl. Dann ist höchstens die Hälfte aller $a \in \mathbb{Z}_N^*$ eine Pseudoprimzahl-Basis für n.

Beweis:

- Pseudoprimzahl-Basen $P = \{a \in \mathbb{Z}_n^* \mid a^{n-1} = 1 \bmod n\}$.
- Wir zeigen nun, dass P eine echte Untergruppe von $\mathbb{Z}_n^*$ ist.
- *Abgeschlossenheit:* Seien $a, b \in P$. Dann ist $(ab)^{n-1} = a^{n-1}b^{n-1} = 1 \bmod n$, d.h. $ab \in P$.
- *Neutrales Element:* $1 \in P$, denn $1^{n-1} = 1 \bmod n$.
- *Inverses Element* zu $a \in P$ ist $a^{n-2} \bmod n$, denn
  - $a \cdot a^{n-2} = a^{n-1} = 1 \bmod n$.
  - $a^{n-2} \in P$, da $(a^{n-2})^{n-1} = (a^{n-1})^{n-2} = 1 \bmod n$.
- Da n keine Carmichael-Zahl ist, gilt $P \neq \mathbb{Z}_n^*$.
- Nach Satz von Lagrange gilt $|\mathbb{Z}_n^*| = |P| \cdot \mathrm{ind}_{\mathbb{Z}_n^*}(P)$.
- D.h. $\mathrm{ind}_{\mathbb{Z}_n^*}(P) \geq 2$ und damit $|P| \leq \frac{1}{2}|\mathbb{Z}_n^*|$.

Primzahltest für Nicht-Carmichael-Zahlen

Satz Fermattest

Sei $n \in \mathbb{N}$ keine Carmichael-Zahl und $k \in \mathbb{N}$. Dann kann in Zeit $\mathcal{O}(k \log^3 n)$ mit Fehlerwahrscheinlichkeit $\approx 2^{-k}$ entschieden werden, ob n prim ist.

Beweis:

Algorithmus FERMATTEST

EINGABE: $n, k \in \mathbb{N}$

1. For $i \leftarrow 1$ to k
   1. Wähle $a \in_R \mathbb{Z}_n \setminus \{0\}$.
   2. Falls $\mathrm{ggT}(a, n) > 1$, Ausgabe "n zusammengesetzt".
   3. Falls $a^{n-1} \neq 1 \mod n$, Ausgabe "n zusammengesetzt".
2. Ausgabe "n prim".

- **Laufzeit:** $\mathcal{O}(k \log^3 n) = \mathcal{O}(\log^3 n)$ für konstantes k.
- In der Praxis genügt die Wahl $k = 80$.

Korrektheit von FERMATTEST

Beweis: Fehlerwahrscheinlichkeit

- Falls n prim ist, dann ist die Ausgabe stets korrekt.
- Schritt 2.2: Falls $a \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$, dann ist Teiler von n gefunden.
- Schritt 2.3: Falls $a^{n-1} \neq 1 \bmod n$, dann ist a ein Zeuge für die Zusammengesetztheit von n.
- Für zusammengesetzte n ist fehlerhafte Ausgabe "prim" möglich.
- Pro Iteration:

$$\text{Ws}(\text{Ausgabe "n zusammengesetzt"} \mid \text{n zusammengesetzt}) \geq \tfrac{1}{2}.$$

- Nach k Iterationen:

$$\begin{aligned} \epsilon &:= \text{Ws}(\text{Ausgabe "n prim"} \mid \text{n zusammengesetzt}) \\ &= (1 - \text{Ws}(\text{Ausgabe "n zusammengesetzt"} \mid \text{n zusammengesetzt}))^k \\ &\leq 2^{-k} \end{aligned}$$

- Fehlerwahrscheinlichkeit

$$\text{Ws}(\text{n zusammengesetzt} \mid \text{Ausgabe "n prim"}) \approx \epsilon.$$

Spezieller Chinesischer Restsatz

Satz Spezieller Chinesischer Restsatz

Seien $m, n \in \mathbb{N}$ teilerfremd und $a, b \in \mathbb{Z}$. Dann existiert genau eine Lösung $x \in \mathbb{Z}_{mn}$ des Gleichungssystems

$$\left| \begin{array}{rcl} x & = & a \bmod m \\ x & = & b \bmod n \end{array} \right| .$$

Beweis:

- **Existenz:** EEA liefert $r, s \in \mathbb{Z}$ mir $mr + ns = \mathrm{ggT}(m, n) = 1$.
- D.h. $mr = 1 \bmod n$ und $ns = 1 \bmod m$.
- Wir definieren $x = ans + bmr \bmod mn$.
- Damit gilt $x = a \bmod m$ und $x = b \bmod n$.

- **Eindeutigkeit:** Seien x, x' Lösungen des Gleichungssystems.
- Dann gilt $x = a = x' \bmod m$ und $x = b = x' \bmod n$.
- Damit wird die Differenz $x - x'$ sowohl von m als auch n geteilt.
- Da $\mathrm{ggT}(m, n) = 1$, folgt $mn \mid x - x'$ und damit $x = x' \bmod mn$.

Chinesischer Restsatz

Satz Chinese Remainder Theorem (CRT)

Seien $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd und $a_1, \ldots, a_n \in \mathbb{Z}$. Dann existiert genau eine Lösung $x \in \mathbb{Z}_{m_1 \cdot \ldots \cdot m_n}$ des Gleichungssystems

$$\left| \begin{array}{rcl} x & = & a_1 \bmod m_1 \\ x & = & a_2 \bmod m_2 \\ & \vdots & \\ x & = & a_n \bmod m_n \end{array} \right| .$$

Beweis: Induktion über n

- **IV** für $n = 2$ liefert der Spezielle Chinesische Restsatz.
- **IS** für $n - 1 \to n$. Nach IA existiert für die ersten $n - 1$ Gleichungen eine eindeutige Lösung $y \in \mathbb{Z}_{m_1 \cdot \ldots \cdot m_n}$.
- Spezieller CRT-Satz liefert eindeutiges $x \in \mathbb{Z}_{m_1 \cdot \ldots \cdot m_n}$ mit

$$\left| \begin{array}{rcl} x & = & y \bmod m_1 \cdot \ldots \cdot m_{n-1} \\ x & = & a_n \bmod m_n \end{array} \right| .$$

Additiver CRT-Isomorphismus

Satz Additiver CRT-Isomorphismus

Sei $N = m_1 \cdot \ldots \cdot m_n$ für paarweise teilerfremde $m_1, \ldots, m_n$. Dann gilt

$$\mathbb{Z}_N \cong \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}.$$

Beweis:

- Wir definieren $f : \mathbb{Z}_N \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ vermöge
$$x \bmod N \mapsto (x \bmod m_1, \ldots, x \bmod m_n).$$
- CRT-Satz liefert zu jedem $f(x)$ das eindeutige x, d.h. f ist injektiv.
- Da $|\mathbb{Z}_N| = N = m_1 \cdot \ldots \cdot m_n = |\mathbb{Z}_{m_1}| \cdot \ldots \cdot |\mathbb{Z}_{m_n}|$, ist f bijektiv.
- Ferner ist f ein Homomorphismus, denn

$$\begin{aligned} f(x+y) &= ((x+y \bmod N) \bmod m_1, \ldots, (x+y \bmod N) \bmod m_n) \\ &= (x+y \bmod m_1, \ldots, x+y \bmod m_n) = f(x) + f(y). \end{aligned}$$

- Damit ist f ein Isomorphismus.
- Man beachte: Sowohl f als auch f^{-1} sind effizient berechenbar.

Anwendung des CRT-Isomorphismus

Korollar Anwendung des CRT-Isomorphismus

Sei $N = m_1 \cdot \ldots \cdot m_n$ für paarweise teilerfremde $m_1, \ldots, m_n$. Dann gilt für alle $x, a \in \mathbb{Z}$, dass $x = a \bmod N$ gdw

$$\left| \begin{array}{rcl} x & = & a \bmod m_1 \\ x & = & a \bmod m_2 \\ & \vdots & \\ x & = & a \bmod m_n \end{array} \right| .$$

Anwendung:

- Seien die m_i, $i \in [n]$ Primzahlen oder Primzahlpotenzen.
- Für viele Probleme sind effiziente Algorithmen in $\mathbb{Z}_N$ nicht bekannt, wohl aber in $\mathbb{Z}_{m_i}$. Vorgehensweise zum Lösen in $\mathbb{Z}_N$:
  - Berechne mittels Isomorphismus f Darstellung in $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$.
  - Löse die algorithmischen Probleme für alle $\mathbb{Z}_{m_i}$, $i \in [n]$ separat.
  - Berechne mittels Isomorphismus f^{-1} die Lösungen in $\mathbb{Z}_N$.

Multiplikativer CRT-Isomorphismus

Satz Multiplikativer CRT-Isomorphismus

Sei $N = m_1 \cdot \ldots \cdot m_n$ für paarweise teilerfremde $m_1, \ldots, m_n$. Dann gilt

$$\mathbb{Z}_N^* \cong \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^*.$$

Beweis:

- Definieren denselben Isomorphismus f wie zuvor.
- Zeigen zunächst, dass für $a \in \mathbb{Z}_N^*$ gilt $f(a) \in \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^*$.
- Es gilt $\mathrm{ggT}(a, N) = 1$, d.h. es gibt $x, y \in \mathbb{Z}$ mit $ax + Ny = 1$.
- Damit ist $ax + m_1 \cdot \ldots \cdot m_n y = 1$ bzw. $\mathrm{ggT}(a, m_i) = 1$ für $i \in [n]$.
- Sei umgekehrt $\mathrm{ggT}(a, m_i) = 1$ für alle $i \in [n]$.
- Aus dem Satz zur Teilerfremdheit folgt damit $\mathrm{ggT}(a, N) = 1$.
- f ist nach CRT-Satz injektiv und für teilerfremde m_i gilt
  $|\mathbb{Z}_N^*| = \phi(N) = \phi(m_1 \cdot \ldots \cdot m_n) = \phi(m_1) \cdot \ldots \phi(m_n) = |\mathbb{Z}_{m_1}^*| \cdot \ldots \cdot |\mathbb{Z}_{m_n}^*|$.
  (Übungsaufgabe)
- Dass f ein Homomorphismus ist, folgt analog zum vorigen Beweis.

Anzahl Nullstellen modularer Gleichungen

Satz Nullstellen einer Quadratischen Gleichung

Sei $N \in \mathbb{N}$ ungerade mit Primfaktorzerlegung $N = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$. Dann existieren 2^k Lösungen der Gleichung $x^2 = 1 \bmod N$ in $\mathbb{Z}_N^*$.

Beweis:

- CRT-Isomorphismus: $x^2 = 1 \bmod N$ gdw $x^2 = 1 \bmod p_i^{e_i}$, $i \in [n]$.
- Für jede Gleichung $x^2 = 1 \bmod p_i^{e_i}$ sind $x = \pm 1$ Lösungen.
- $1 \neq (-1) \bmod p_i^{e_i}$, da $p_i^{e_i} > 2$. D.h. die Lösungen sind verschieden.
- Damit sind alle möglichen Vektoren $v \in \{-1, 1\}^k$ Lösungen in $\mathbb{Z}^*_{p_1^{e_1}} \times \ldots \times \mathbb{Z}^*_{p_k^{e_k}}$.
- CRT-Satz: Diese 2^k Lösungen führen zu 2^k Lösungen in $\mathbb{Z}_N$.

Spezialfall RSA-Modul $N = pq$

Korollar Anzahl Lösungen für RSA-Modul

Sei $N = pq$ mit p, q prim. Dann besitzt die Gleichung $x^2 = 1 \bmod N$ vier Lösungen in $\mathbb{Z}_N^*$.

Bsp:

- $x^2 = 1 \bmod 15$ besitzt die Lösungen

$$\left| \begin{array}{l} x_1 = 1 \bmod 3 \\ x_1 = 1 \bmod 5 \end{array} \right|, \left| \begin{array}{l} x_2 = 1 \bmod 3 \\ x_2 = 4 \bmod 5 \end{array} \right|, \left| \begin{array}{l} x_3 = 2 \bmod 3 \\ x_3 = 1 \bmod 5 \end{array} \right|, \left| \begin{array}{l} x_4 = 2 \bmod 3 \\ x_4 = 4 \bmod 5 \end{array} \right|.$$

- In $\mathbb{Z}_N^*$ entspricht dies $x_1 = 1, x_2 = 4, x_3 = 11, x_4 = 14$.

Faktorisieren mit nicht-trivialen Wurzeln

Satz Faktorisieren mit nicht-trivialen Wurzeln

Sei $N = pq$ ungerade mit p, q prim. Sei $x \in \mathbb{Z}_N^*$ eine Lösung von $x^2 = 1 \bmod N$ mit $x \neq \pm 1 \bmod N$. Dann kann die Faktorisierung von N in Zeit $\mathcal{O}(\log^2 N)$ berechnet werden.

Beweis:

- $x^2 = 1 \bmod N$ besitzt die vier Wurzel
$$1 = (1,1),\ -1 = (-1,-1),\ (1,-1) \text{ und } (-1,1).$$
- OBdA sei $x = (1,-1)$, d.h. $x = 1 \bmod p$ und $x = (-1) \bmod q$.
- D.h. $x - 1 = (0,-2)$ und $x - 1 = 0 \bmod p$, $x - 1 = (-2) \bmod q$.
- Damit gilt p teilt $x - 1$ und q teilt $x - 1$ nicht wegen $q > 2$.
- Daraus folgt $\mathrm{ggT}(N, x-1) = p$.
- p kann in Zeit $\mathcal{O}(\log^2 N)$ mittels EUKLID berechnet werden.
- Analog kann man $\mathrm{ggT}(N, x+1) = q$ zeigen.