Solovay-Strassen Primzahltest

Satz Solovay-Strassen Primzahltest

Ein ungerades $n \geq 3$ ist prim gdw für alle $a \bmod n$ mit $\mathrm{ggT}(a, n) = 1$ gilt

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n.$$

Falls $a \notin \mathbb{P}$, so gilt die Kongruenz für höchstens die Hälfte aller a.

Beweis:

- $\Rightarrow$ Falls n prim ist, so ist die Kongruenz die Euler-Identität.
- $\Leftarrow$ Für alle zu n teilerfremden $a \bmod n$ gelte $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$.
  - Annahme: n ist zusammengesetzt.
  - Quadrieren liefert $a^{n-1} \equiv 1 \bmod n$. D.h. n ist eine Carmichael-Zahl.
  - Damit gilt $n = \prod_{i=1}^{s} p_i$ mit $s, p_i \geq 3$.
  - CRT liefert einen Isomorphismus $\Phi : U_n \to \prod_{i=1}^{s} U_{p_i}$.
  - Sei g ein Generator modulo p_1. Damit gilt $\left(\frac{g}{p_1}\right) = -1$.
  - Sei $a \in \mathbb{Z}$ mit $\Phi(a) = (g, 1, \ldots, 1)$. Für das Jacobi Symbol gilt
    $$\left(\frac{a}{n}\right) = \prod_{i=1}^{s}\left(\frac{a}{p_i}\right) = \prod_{i=1}^{s}\left(\frac{a \bmod p_i}{p_i}\right) = \left(\frac{g}{p_1}\right)\prod_{i=1}^{s}\left(\frac{1}{p_i}\right) = (-1).$$

Solovay-Strassen Primzahltest

Beweis: (Fortsetzung)

- Wir zeigen nun, dass der linke Term $a^{\frac{n-1}{2}} \not\equiv (-1) \bmod n$.
- Es gilt $\Phi(-1) = (-1, \ldots, -1)$, aber $\Phi(a^{\frac{n-1}{2}}) = (g^{\frac{n-1}{2}}, 1, \ldots, 1)$.
- Da $p_i \geq 3$ für alle i, folgt $(-1, \ldots, -1) \not\equiv (g^{\frac{n-1}{2}}, 1, \ldots, 1)$.
- Für dieses a gilt also die Kongruenz nicht. (Widerspruch)

- Sei $A := \{a \in U_n \mid a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\}$. Wir zeigen, dass $|A| \leq \frac{1}{2}|U_n|$.
- Wir wissen bereits, dass $A \subsetneq U_n$.
- Ferner ist A eine Untergruppe von U_n. (Übung)
- Damit teilt $|A|$ die Ordnung $|U_n|$, und es folgt $|A| \leq \frac{1}{2}|U_n|$.

Definition Euler-Zeugen

$A := \{a \in U_n \mid a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\}$ heißt Menge der *Euler-Zeugen*.

Solovay-Strassen Primzahltest

Algorithmus Solovay-Strassen Primzahltest

EINGABE: $n \in \mathbb{N}$ ungerade, $\ell \in \mathbb{N}$

1. FOR $i = 1$ to ℓ
   1. Wähle $a_i \in \{1, \ldots, n-1\}$ zufällig.
   2. Falls $\mathrm{ggT}(a_i, n) > 1$, Ausgabe “zusammengesetzt” und Abbruch.
   3. Falls $a_i^{\frac{n-1}{2}} \not\equiv (\frac{a_i}{n}) \bmod n$, Ausgabe “zusammengesetzt” und Abbruch.
2. Ausgabe “prim”.

Laufzeit: $\mathcal{O}(k \log^3 n) = \mathcal{O}(\log^3 n)$ für konstantes k.

Fehlerws Solovay-Strassen Primzahltest

Korrektheit:

- Falls n prim ist, so ist die Ausgabe korrekt.
- Falls n zusammengesetzt ist, erhalten wir Ausgabe “prim” mit

$$\begin{aligned}\mathrm{Ws}[\text{Ausgabe “prim”} \mid n \notin \mathbb{P}] &= \mathrm{Ws}[a_1, \ldots, a_\ell \in A] \\ &= \prod_{i=1}^{\ell} \mathrm{Ws}[a_i \in A] \leq (\tfrac{1}{2})^\ell.\end{aligned}$$

- D.h. wir erhalten $\mathrm{Ws}[\text{Ausgabe “zusammenges.”} \mid n \notin \mathbb{P}] \geq 1 - 2^{-\ell}$.
- Für Kryptographie-Anwendungen wählt man gewöhnlich $\ell \geq 80$.
- *Vorsicht:* Die Fehlerwahrscheinlichkeit ist nicht höchstens 2^{-80}.
- Ein Fehler entsteht, falls die Ausgabe “prim” ist, obwohl $n \notin \mathbb{P}$.
- D.h. die Fehlerwahrscheinlichkeit des Algorithmus ist

$$\begin{aligned}\mathrm{Ws}[n \notin \mathbb{P} \mid \text{Ausgabe “prim”}] &= \frac{\mathrm{Ws}[\text{Ausgabe “prim”} \mid n \notin \mathbb{P}] \cdot \mathrm{Ws}[n \notin \mathbb{P}]}{\mathrm{Ws}[\text{Ausgabe “prim”}]} \\ \leq \frac{\mathrm{Ws}[\text{Ausgabe “prim”} \mid n \notin \mathbb{P}] \cdot \mathrm{Ws}[n \notin \mathbb{P}]}{\mathrm{Ws}[n \in \mathbb{P}]} &\approx 2^{-\ell} \log n. \quad \text{(ohne Beweis)}\end{aligned}$$

Miller-Rabin Primzahltest

Idee: Für primes n gilt $a^{n-1} \equiv 1 \bmod n$.
Sukzessives Wurzelziehen auf beiden Seiten liefert ± 1.

Satz Miller-Rabin Primzahltest

Ein ungerades $n \geq 3$, n keine Primpotenz mit $n - 1 = 2^r d$, d ungerade, ist prim gdw für alle zu n teilerfremden $a \in \mathbb{Z}$ gilt

$$a^d \equiv 1 \bmod n \text{ oder } a^{2^k d} \equiv (-1) \bmod n \text{ für ein } 0 \leq k < r.$$

Falls $a \notin \mathbb{P}$, erfüllt höchstens ein Viertel aller a die Bedingung.

Beweis:

$\Rightarrow$ Sei n prim und $a \in U_n$ beliebig. Es gilt $a^{n-1} = 1$.

- Falls $a^d \neq 1$, existiert ein minimales $0 \leq k < r$ mit $a^{2^{k+1} d} = 1$.
- Da $a^{2^k d} \neq 1$, gilt $a^{2^k d} = (-1)$, weil 1 die Wurzeln ± 1 besitzt.

$\Leftarrow$ Sei $n = \prod_{i=1}^{s} p_i^{e_i}$ mit $s \geq 2$. Wir definieren die Primzeugen $S := \{a \in U_n | a^d \equiv 1 \bmod n \text{ oder } a^{2^k d} \equiv (-1) \bmod n \text{ für ein } k\}$.

- Wir müssen zeigen, dass $|S| \leq \frac{1}{4}\varphi(n)$.

Miller-Rabin Primzahltest

Beweis: (Fortsetzung)

- Sei $k := \max_{j \in \mathbb{N}_0}\{\exists b \in U_n \text{ mit } b^{2^j d} = (-1)\}$ und $m = 2^k d$.
- Wir definieren die folgenden vier Mengen $J \supseteq K \supseteq L \supseteq M$ mit

$$\begin{aligned} J &:= \{a \in U_n \mid a^{n-1} \equiv 1 \bmod n\} \\ K &:= \{a \in U_n \mid a^m \equiv \pm 1 \bmod p_i^{e_i} \text{ für alle } i\} \\ L &:= \{a \in U_n \mid a^m \equiv \pm 1 \bmod n\} \\ M &:= \{a \in U_n \mid a^m \equiv 1 \bmod n\}. \end{aligned}$$

- Alle Mengen sind Untergruppen von U_n. Es gilt $S \subseteq L$.
- Wir zeigen $|L| = 2|M|$ und $|K| \geq 2^s|M|$. Damit gilt

$$\varphi(n) \geq |K| \geq 2^s|M| = 2^{s-1}|L| \geq 2^{s-1}|S|.$$

- Es gilt $s \geq 2$. Für $s \geq 3$ ist die Behauptung bewiesen.
- Für $s = 2$ ist n keine Carmichael-Zahl. D.h. J ist eine echte Untergruppe von U_n und damit $|K| \leq |J| \leq \frac{1}{2}\varphi(n)$.

Miller-Rabin Primzahltest

Beweis: (Fortsetzung)

- z.z.: $|L| = 2|M|$. Sei $b \in U_n$ mit $b^m = (-1)$.
- Für jedes $a \in M$ liegt $ba \in L$, aber nicht in M. D.h. $|L| = 2|M|$.
- z.z.: $|K| = 2^s|M|$.
- Wir konstruieren zu jedem $\epsilon \in \{\pm 1\}^s$ ein $b_\epsilon \in U_n$ mit
$$b_\epsilon^m \equiv \epsilon_i \bmod p_i^{e_i} \text{ für alle } i = 1, \ldots, s.$$
- Dazu betrachten wir wieder $b \in U_n$ mit $b^m \equiv (-1) \bmod n$. Es folgt
$$b^m \equiv (-1) \bmod p_i^{e_i} \text{ und } b^{2m} \equiv 1 \bmod p_i^{e_i} \text{ für alle } i.$$
- Wir konstruieren b_ϵ mittels CRT als Lösung der Kongruenzen
$$x \equiv \begin{cases} b \bmod p_i^{e_i} & \text{falls } \epsilon_i = (-1) \\ b^2 \bmod p_i^{e_i} & \text{falls } \epsilon_i = 1 \end{cases}.$$
- Für die Lösung b_ϵ gilt $b_\epsilon^m \equiv \epsilon_i \bmod p_i^{e_i}$ für alle i.

Miller-Rabin Primzahltest

Beweis: (Fortsetzung)

- Wir definieren $M_a := \{ab_\epsilon | \epsilon \in \{-1,1\}^s\}$ für $a \in M$.
- Es gilt $M_a \subseteq K$. Falls $M_a \cap M_{a'} = \emptyset$ für $a \neq a'$, folgt $|K| \geq 2^s|M|$.
- Annahme: $M_a \cap M_{a'} \neq \emptyset$ für $a \neq a'$ mit $a, a' \in M$.
- Dann existieren ϵ, ϵ' mit $ab_\epsilon \equiv a'b_{\epsilon'} \bmod n$. Es folgt
$$(\frac{b_\epsilon}{b_{\epsilon'}})^m \equiv (\frac{a}{a'})^m \equiv 1 \bmod n, \text{ da } a, a' \in M.$$
- Es folgt $(\frac{b_\epsilon}{b_{\epsilon'}})^m \equiv 1 \bmod p_i^{e_i}$ für alle i.
- b_ϵ, $b_{\epsilon'}$ nehmen mod $p_i^{e_i}$ entweder die Werte b oder b^2 an.
- Falls $b_\epsilon \not\equiv b_{\epsilon'} \bmod p_i^{e_i}$ folgt $(\frac{b_\epsilon}{b_{\epsilon'}})^m \equiv (-1) \bmod p_i^{e_i}$.
- D.h. $b_\epsilon \equiv b_{\epsilon'} \bmod p_i^{e_i}$ für alle i und damit $b_\epsilon \equiv b_{\epsilon'} \bmod n$.
- Aus $ab_\epsilon \equiv a'b_{\epsilon'} \bmod n$ folgt $a \equiv a' \bmod n$. (Widerspruch)

Algorithmus Miller-Rabin Primzahltest

Algorithmus Miller-Rabin Primzahltest

EINGABE: $n \geq 3$ ungerade, $\ell \in \mathbb{N}$

1. Falls n eine Primpotenz ist, Ausgabe “zusammengesetzt”.
2. Berechne $n - 1 = 2^r d$ mit d ungerade.
3. Für $i = 1, \ldots, \ell$
   1. Wähle $a_i \in \{1, \ldots, n-1\}$ zufällig.
   2. Falls $\mathrm{ggT}(a_i, n) > 1$, Ausgabe “zusammengesetzt”.
   3. Setze $k = 0$. Berechne $a_k := a_i^d \bmod n$
   4. While $a_k \not\equiv 1 \bmod n$ und $k < r$
      1. Setze $k := k + 1$. Berechne $a_k := a_{k-1}^2 \bmod n$.
   5. Falls $k = r$ und $a_k \not\equiv 1 \bmod n$, Ausgabe “zusammengesetzt”.
   6. Falls $k > 0$ und $a_{k-1} \not\equiv (-1) \bmod n$, Ausgabe “zusammengesetzt”.
4. Ausgabe “prim”.

Algorithmus Miller-Rabin Primzahltest

- **Laufzeit:** $\mathcal{O}(\ell \log^3 n) = \mathcal{O}(\log^3 n)$ für konstantes ℓ.
  Übung: Schritt 1 kann in Laufzeit $\mathcal{O}(\log^3 n)$ realisiert werden.
- **Korrektheit:** Für primes n ist die Ausgabe stets korrekt.
- Für $n \notin \mathbb{P}$ gilt analog zur Analyse des Solovay-Strassen Tests

$$\begin{aligned} \text{Ws}[\text{Ausgabe “prim”} \mid n \notin \mathbb{P}] &= \text{Ws}[a_1, \ldots, a_\ell \in S] \\ &= \prod_{i=1}^{\ell} \text{Ws}[a_i \in S] \leq (\tfrac{1}{4})^\ell. \end{aligned}$$

- D.h. wir benötigen für die gleiche Schranke wie im Solovay-Strassen Test nur die Hälfte der Iterationen ℓ.
- Man kann sogar zeigen, dass $S \subseteq A$.
- D.h. die Primzeugen sind in den Euler-Zeugen enthalten.
- Seien also $a_1, \ldots, a_\ell$ eine Wahl der Zahlen in Schritt 3.1, so dass der Miller-Rabin Test n irrtümlich als prim ausweist.
- Dann irrt auch der Solovay-Strassen Test für $a_1, \ldots, a_\ell$.
- D.h. der Miller-Rabin Test beinhaltet den Solovay-Strassen Test.