

Agarwal-Kayal-Saxena Primzahltest (2002)

Satz AKS-Primzahltest

Ein $n \in \mathbb{N}$, n keine Primzahlpotenz, ist prim gdw für alle $a \in \mathbb{Z}$ gilt

$$(X + a)^n \equiv X^n + a \pmod{n} \text{ im Polynomring } \mathbb{Z}[X].$$

Beweis:

⇒ Sei n prim. Mit der Binomischen Formel mod n (Folie 48) gilt

$$(X + a)^n \equiv X^n + a^n \equiv X^n + a \pmod{n}.$$

⇐ Sei $n \notin \mathbb{P}$. Schreibe $n = p^\ell m$ für $p \in \mathbb{P}$, $\ell \geq 1$ und $\text{ggT}(p, m) = 1$.

● Wir zeigen $(X + 1)^n \not\equiv X^n + 1 \pmod{n}$. Der Koeffizient von X^p ist

$$\binom{n}{p} = \frac{n(n-1)\dots(n-p+1)}{p(p-1)\dots 1} \in \mathbb{N}.$$

● Im Zähler ist $n = p^\ell m$ durch p teilbar.

● Damit sind $n - 1, n - 2, \dots, n - (p - 1)$ nicht durch p teilbar.

● Im Nenner taucht ebenfalls ein p auf. Damit können wir schreiben

$$\binom{n}{p} = p^{\ell-1} m' \text{ mit } \text{ggT}(p, m') = 1.$$

● Es folgt $\binom{n}{p} \not\equiv 0 \pmod{p^\ell}$ und mittels CRT auch $\binom{n}{p} \not\equiv 0 \pmod{n}$.

● D.h. der Koeffizient von X^p verschwindet in $(X + 1)^n$ nicht.

Anmerkung:

- Im AKS-Algorithmus (2002) wird $(X + a)^n \equiv X^n + a \pmod{n}$ modulo Polynomen $X^r - 1$ kleinen Grades $r = \mathcal{O}(\log^{\frac{15}{2}} n)$ getestet.
- Dies führt zu einem deterministischen Primzahltest ohne Fehler.
- Allerdings ist der AKS-Test deutlich langsamer als Miller-Rabin.

Faktorisierungsalgorithmen

Idee: Konstruiere $x, y \in \mathbb{Z}$ mit $x^2 \equiv y^2 \pmod{n}$ und $x \not\equiv \pm y \pmod{n}$.

Ziel: Berechne nicht-triviale Teiler von n , faktorisieren rekursiv.

Lemma Differenz von Quadraten

- 1 Sei $n \notin \mathbb{P}$ ungerade. Dann gilt $n = x^2 - y^2$ mit $x, y \in \mathbb{N}_0$ und $x \not\equiv \pm y \pmod{n}$.
- 2 Sei $x^2 - y^2 = cn$ mit $x, y, c \in \mathbb{Z}$ und $x \not\equiv \pm y \pmod{n}$. Dann sind $a := \text{ggT}(x + y, n)$ und $b := \text{ggT}(x - y, n)$ nicht-triviale Teiler von n .

Beweis:

(1) Sei $n = ab$ mit $2 < b \leq a \leq n$. Setze $x = \frac{a+b}{2}, y = \frac{a-b}{2} \in \mathbb{N}_0$.

• Dann gilt $x^2 - y^2 = \frac{(a+b)^2 - (a-b)^2}{4} = \frac{4ab}{4} = n$.

• Wir zeigen $x \not\equiv y \pmod{n}$. Analog folgt $x \not\equiv -y \pmod{n}$.

• Aus der Annahme $x \equiv y \pmod{n}$ folgt

$$\frac{a+b}{2} \equiv \frac{a-b}{2} \pmod{n} \Leftrightarrow 2b \equiv 0 \pmod{2n} \Leftrightarrow b \equiv 0 \pmod{n}. \text{ (Widerspruch)}$$



Differenz von Quadraten

- (2) Aus $x^2 - y^2 = cn$ folgt $(x + y)(x - y) \equiv n$, d.h. $n \mid (x + y)(x - y)$.
- Wegen $x \pm y \not\equiv 0 \pmod n$ sind beide Faktoren kein Vielfaches von n .
 - D.h für $a = \text{ggT}(x + y, n)$ und $b = \text{ggT}(x - y, n)$ gilt $a, b < n$.
 - Annahme: $a = \text{ggT}(x + y, n) = 1$ (analog für b). Dann gilt
$$n = \text{ggT}((x + y)(x - y), n) = \text{ggT}(x - y, n) = b \text{ (Widerspruch).}$$
 - D.h. für beide Teiler a, b von n gilt $1 < a, b < n$.

Fermat Faktorisierung

Algorithmus Fermat Faktorisierung

EINGABE: $n \in \mathbb{N}$ zusammengesetzt

- 1 Setze $x := \lceil \sqrt{n} \rceil - 1$.
- 2 REPEAT
 - 1 Setze $x := x + 1$ und $z := x^2 - n$.
 - 2 Falls $z = y^2$ berechne y .
- 3 UNTIL $z = y^2$ für ein $y \in \mathbb{N}$ und $x \not\equiv \pm y \pmod{n}$.

AUSGABE: $\text{ggT}(x \pm y, n)$

Korrektheit: folgt aus vorigem Lemma.

Bsp. Fermat Faktorisierung

Bsp:

- Für $n = 187$ gilt $x = \lceil \sqrt{n} \rceil = 14$ und $x^2 - n = 196 - 187 = 3^2$.
- Es gilt $14 \not\equiv \pm 3 \pmod{187}$.
- Wir erhalten $\text{ggT}(14 \pm 3, 187) = \{11, 17\}$ mit $11 \cdot 17 = 187$.
- Für $n = 175$ ist $x = 14$. Die erste Quadratzahl ist
$$(x + 6)^2 - n = 20^2 - n = 400 - 175 = 225 = 15^2.$$
- Es gilt $20 \not\equiv \pm 15 \pmod{175}$.
- Wir erhalten $\text{ggT}(20 \pm 15, 175) = \{5, 35\}$ mit $5 \cdot 35 = 175$.

Laufzeit Fermat Faktorisierung

Laufzeit:

- Sei $n = ab$ ungerade mit $1 < b \leq \sqrt{n} \leq a < n$.
- Für $x = \frac{a+b}{2} \geq \sqrt{ab} = \sqrt{n}$ ist $x^2 - n = y^2$ mit $y = \frac{a-b}{2}$.
- Es folgt $(x + \sqrt{n})(x - \sqrt{n}) = y^2$.
- Die Iterationen in Schritt 2 sind damit beschränkt durch

$$x - \sqrt{n} = \frac{y^2}{x + \sqrt{n}} \leq \frac{\left(\frac{a-b}{2}\right)^2}{2\sqrt{n}} \leq \frac{(a-b)^2}{8\sqrt{n}}.$$

- D.h. für $n = ab$ mit Differenz $a - b = \mathcal{O}(n^{\frac{1}{4}})$ ist dies konstant.
- Für $n = ab$ mit a, b gleicher Bitgröße gilt $a - b = \mathcal{O}(\sqrt{n})$ und damit $x - \sqrt{n} = \mathcal{O}(\sqrt{n})$. Dies ist vergleichbar mit Probedivision.
- I. Allg. gilt $a - b = \mathcal{O}(n)$ und wir erhalten $\mathcal{O}(n^{\frac{3}{2}})$ Iterationen.

Motivation Faktorbasis

Bsp: : Wir betrachten die Fermat Faktorisierung von $93 = 3 \cdot 31$.

- Es gilt $\lceil \sqrt{93} \rceil = 10$. Wir erhalten folgende Liste

x	10	11	12	13	14	15	16	17
$x^2 - 93$	7	28	51	76	193	132	163	196

- D.h. das erste Quadrat taucht bei $17 = \frac{3+31}{2}$ auf.

- Aus den ersten beiden Einträgen folgt aber

$$10^2 \equiv 7 \pmod{93} \text{ und } 11^2 \equiv 28 = 2^2 \cdot 7 \pmod{93}.$$

- Multiplikation beider Gleichungen liefert

$$(10 \cdot 11)^2 \equiv (17)^2 \equiv 2^2 \cdot 7^2 = (14)^2 \pmod{93}.$$

- Es gilt $17 \not\equiv \pm 14 \pmod{93}$ und $\text{ggT}(17 \pm 14, 93) = \{3, 31\}$.

Ziel: Kombiniere die Gleichungen, so dass ein Quadrat entsteht.

Faktorbasis

Definition Faktorbasis

Für ein $b \in \mathbb{N}$ definieren wir die Faktorbasis

$$B = \{-1\} \cup \{p \in \mathbb{P} \mid p \leq b\}.$$

Ein $n \in \mathbb{Z}$ heißt *b-glatt*, falls $n = \prod_{p \in B} p^{e_p}$ mit $e_p \in \mathbb{N}_0$.

Bsp: -28 ist 7-glatt, aber nicht 5-glatt.

High-Level Faktorisierung mit Faktorbasen

Algorithmus FAKTORBASIS

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

- 1 Wähle $b \in \mathbb{N}$ geeignet. Sei $B = \{p_1, \dots, p_s\}$.
- 2 Definiere leere Matrix E .
- 3 For $i = 0 \dots s$
 - 1 Wähle x_i solange, bis $z_i \equiv x_i^2 \pmod{n}$ b -glatt. Schreibe $z_i = \prod_{j=1}^s p_j^{e_{i,j}}$.
 - 2 Nimm $(e_{i,1} \bmod 2, \dots, e_{i,s} \bmod 2)$ als Zeile in E auf.
- 4 Berechne $f \in \mathbb{F}_2^{s+1} \setminus \{0\}^{s+1}$ mit $fE = \{0\}^s$ über \mathbb{F}_2 , d.h.
$$\sum_{i=1}^{s+1} f_i e_{i,j} \equiv 0 \pmod{2} \text{ für alle } j = 1, \dots, s.$$
- 5 Setze $x \equiv \prod_{i=1}^{s+1} x_i^{f_i} \pmod{n}$ und $y \equiv \prod_{j=1}^s p_j^{\frac{\sum_{i=1}^{s+1} f_i e_{i,j}}{2}} \pmod{n}$.
- 6 Falls $x \equiv \pm y \pmod{n}$, zurück zu Schritt 4 (oder zu Schritt 3).

AUSGABE: $\text{ggT}(x \pm y, n)$