Pellsche Gleichung

Satz Pellsche Gleichung

Alle Lösungen $(p,q) \in \mathbb{N}^2$ der Pellschen Gleichung treten als Näherungsbruch $\frac{p}{q}$ in der Kettenbruchentwicklung von $\sqrt{d}$ auf.

Beweis:

- Sei (p,q) eine Lösung, d.h. $1 = p^2 - dq^2 = (p + \sqrt{d}q)(p - \sqrt{d}q)$.
- Es folgt $p - \sqrt{d}q = \frac{1}{p+\sqrt{d}q}$. Teilen durch q liefert

$$\frac{p}{q} - \sqrt{d} = \frac{1}{pq+\sqrt{d}q^2} = \frac{1}{(\frac{p}{q}+\sqrt{d})q^2} < \frac{1}{2q^2}.$$

- Damit taucht $\frac{p}{q}$ in der Kettenbruchentwicklung von $\sqrt{d}$ auf.

Primzahltest für Mersenne-Primzahlen

Satz Lucas-Lehmer Test

Sei $n = 2^p - 1 \in \mathbb{N}$ für $p \in \mathbb{P} \setminus \{2\}$. Wir definieren die Folge S_k durch $S_1 = 4$ und $S_k = S_{k-1}^2 - 2$. Falls $n | S_{p-1}$, dann ist n prim.

Beweis:

$\Rightarrow$ Seien $\omega = 2 + \sqrt{3}, \bar{\omega} = 2 - \sqrt{3}$ im Ring $\mathbb{Z}[\sqrt{3}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{3}$.

- Wir zeigen zunächst $S_k = \omega^{2^{k-1}} + \bar{\omega}^{2^{k-1}}$ per Induktion über k.
- **IA** für $k = 1$: $\omega + \bar{\omega} = 4 = S_1$.
- **IS** $k - 1 \to k$: Wegen $\omega\bar{\omega} = 1$ gilt

$$S_k = S_{k-1}^2 - 2 \overset{IV}{=} (\omega^{2^{k-2}} + \bar{\omega}^{2^{k-2}})^2 - 2 = \omega^{2^{k-1}} + 2 + \omega^{2^{k-1}} - 2.$$

Primzahltest für Mersenne-Primzahlen

Beweis: (Fortsetzung)

- Nach Voraussetzung gilt $n|S_{p-1}$, d.h. $cn = S_{p-1} = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}}$.
- Multiplikation mit $\omega^{2^{p-2}}$ liefert $\omega^{2^{p-1}} = -1 + cn\omega^{2^{p-2}}$.
- Annahme: n ist zusammengesetzt.
- D.h. es existiert ein primes $q|n$ mit $2 < q \leq \sqrt{n}$. Es folgt
$$\omega^{2^{p-1}} \equiv -1 \bmod q \text{ und } \omega^{2^p} \equiv 1 \bmod q.$$
- Damit ist $\mathrm{ord}(\omega) = 2^p$ in $R := \mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}] = \mathbb{Z}/q\mathbb{Z} \oplus (\mathbb{Z}/q\mathbb{Z})\sqrt{3}$.
- Es gilt $R^* \subseteq R \setminus \{0\}$ und damit $|R^*| \leq q^2 - 1$. Es folgt
$$2^p = \mathrm{ord}(\omega) \leq |R^*| \leq q^2 - 1 < n. \text{ (Widerspruch: } n = 2^p - 1)$$

Anmerkung: Man kann auch die Umkehrung n prim $\Rightarrow n|S_{p-1}$ zeigen.

Lucas-Lehmer Primzahltest

Algorithmus Lucas-Lehmer Primzahltest

EINGABE: $n = 2^p - 1 \in \mathbb{N}$ für $p \in \mathbb{P} \setminus \{2\}$.

1. Setze $S_1 = 4$
2. For $i = 2$ to $p - 1$
   1. Berechne $S_i := S_{i-1}^2 - 2 \bmod n$.

AUSGABE: $\begin{cases} \text{prim} & \text{falls } S_{p-1} \equiv 0 \bmod n. \\ \text{zusammengesetzt} & \text{sonst.} \end{cases}$

- **Korrektheit:** Folgt aus vorigem Satz, inklusive Anmerkung.
- **Laufzeit:** $\mathcal{O}(p \log^2 n) = \mathcal{O}(\log^3 n)$.
- Bsp: $n = 2^3 - 1 = 7$ ist prim, denn $S_2 = S_1^2 - 2 = 14 \equiv 0 \bmod 7$.

Lucas-Test

Satz Lucas-Test

Ein $n \in \mathbb{N}$ ist prim gdw ein $a \bmod n$ existiert mit

$$a^{n-1} \equiv 1 \bmod n, \text{ aber } a^{\frac{n-1}{q}} \not\equiv 1 \bmod n \text{ für alle Primteiler } q \text{ von } n-1.$$

Beweis:

- $\Rightarrow$ Sei n prim. Dann ist U_n zyklisch und die obigen Identitäten gelten falls a eine Primitivwurzel modulo n ist.
- $\Leftarrow$ Aus den Identitäten folgt $\mathrm{ord}(a) = n-1$ in U_n. D.h. $n-1 | \varphi(n)$.
  - Damit gilt $n-1 \leq \varphi(n) < n$, woraus $\varphi(n) = n-1$ folgt.
  - Annahme: $n = ab$ mit $1 < a, b < n$.
  - Da $0|n$ und $a|n$, gilt $\varphi(n) \leq n-2$. (Widerspruch)

Bsp: 11 ist prim, denn

$$2^{10} \equiv 1 \bmod 11,\ 2^5 \equiv (-1) \bmod 11 \text{ und } 2^2 = 4 \bmod 11.$$

Nachteil: Lucas-Test benötigt vollständige Faktorisierung von $n-1$.

Pocklington-Test

Satz Pocklington-Test

Ein $n \in \mathbb{N}$, $n-1 = RF$, $F \geq \sqrt{n}$, ist prim gdw ein $a \bmod n$ existiert mit

$$a^{n-1} \equiv 1 \bmod n \text{ und } \mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) = 1 \text{ für alle Primteiler } q \text{ von } F.$$

Beweis:

- $\Rightarrow$ Sei n prim und a Generator von U_n. Dann gilt $a^{n-1} \equiv 1 \bmod n$ und $a^{\frac{n-1}{q}} \not\equiv 1 \bmod n$, d.h. $\mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) = 1$.
- $\Leftarrow$ Annahme: n ist zusammengesetzt.
  - Sei p Primteiler von n mit $p \leq \sqrt{n}$. Sei $d = \mathrm{ord}(a^R)$ in U_p.
  - Es gilt $(a^R)^F = a^{n-1} \equiv 1 \bmod n$ und damit $(a^R)^F \equiv 1 \bmod p$.
  - D.h. $d | F$. Wir zeigen $d = F$. Sei q ein Primteiler von $\frac{F}{d}$. Dann gilt
    $$1 \equiv (a^R)^d \equiv (a^R)^{\frac{F}{q}} = a^{\frac{n-1}{q}} \bmod p \text{ bzw. } \mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) \geq p.$$
  - Sei also $d = F$. Wegen $d = \mathrm{ord}(a^R)$ in U_p folgt $d | p-1$ und damit
    $$F = d \leq p - 1 < \sqrt{n}. \quad \text{(Widerspruch: } F \geq \sqrt{n})$$

Bsp: : 11 ist prim, da $2^{10} \equiv 1 \bmod 10$ und $\mathrm{ggT}(2^5 - 1, 11) = 1$.

Pocklington Primzahltest

Algorithmus Pocklington

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

1. Faktorisiere $n-1$ partiell in RF mit $F > \sqrt{n}$.
2. For $a = 1, \ldots, n-1$
   1. Falls $a^{n-1} \equiv 1 \bmod n$ und $\mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) = 1$ für alle Primteiler q von F, Ausgabe “prim” und Abbruch.
3. Ausgabe “zusammengesetzt”.

Laufzeit:

- Schritt 1: Es ist kein Algorithmus mit Laufzeit $\mathrm{poly}(\log n)$ bekannt.
- Schritt 2: Für zusammengesetzte Zahlen n Schleifendurchläufe.
- D.h. der Algorithmus ist schlechter als eine naive Probedivision.

Hoffnung: Schritt 1 ist unnötig. D.h. es genügt zu testen, ob

$$a^{n-1} \equiv 1 \bmod n \text{ für ein } a \bmod n.$$

Carmichael-Zahlen

Definition Carmichael-Zahl

Ein zusammengesetztes $n \in \mathbb{N}$ heißt *Carmichael-Zahl*, falls $a^{n-1} \equiv 1 \bmod n$ für alle $a \in U_n$.

Lemma Struktur der (n-1)-ten Einheitswurzeln

Sei $n = 2^r \prod_{i=1}^{s} p_i^{r_i} \in \mathbb{N}$ und $G = \{x \in U_n \mid x^{n-1} = 1\}$. Dann ist

$$U_n/G \cong U_{2^r} \times \prod_{i=1}^{s} \mathbb{Z}/m_i\mathbb{Z} \text{ mit } m_i = \frac{p_i^{r_i-1}(p_i-1)}{\mathrm{ggT}(p_i-1,n-1)}.$$

Beweis: (s. [M-S,P], S.92)

Struktur von Carmichael-Zahlen

Satz Struktur von Carmichael-Zahlen

Sei $n \in \mathbb{N}$ zusammengesetzt.

1. n ist Carmichael gdw n keine mehrfachen Primteiler besitzt und
$$p - 1 | n - 1 \text{ für jeden Primteiler } p \text{ von } n.$$
2. Jede Carmichael-Zahl ist ungerade und besitzt ≥ 3 Primteiler.

Beweis:

(1) n ist eine Carmichael-Zahl gdw $\{x \in U_n \mid x^{n-1} = 1\} = U_n$.

- Mit vorigem Lemma muss damit die folgende Gruppe trivial sein
$$U_n/G \cong U_{2^r} \times \prod_{i=1}^{s} \mathbb{Z}/m_i\mathbb{Z}.$$
- Insbesondere gilt damit $m_i = 1$ für alle i. D.h.
$$m_i = \frac{p_i^{r_i-1}(p_i-1)}{\mathrm{ggT}(p_i-1,n-1)} = 1 \text{ für alle } i.$$
- Dies ist äquivalent zu
$$r_i = 1 \text{ und } \mathrm{ggT}(p_i - 1, n - 1) = p_i - 1 \text{ bzw. } p_i - 1 | n - 1.$$
- Wegen $r_i = 1$ besitzt n keine mehrfachen Primteiler.

Struktur von Carmichael-Zahlen

Beweis: (Fortsetzung)

(2) Sei n Carmichael. Aus $U_n/G \cong U_{2^r} \times \prod_{i=1}^{s} \mathbb{Z}/m_i\mathbb{Z}$ folgt $r \leq 1$.

- Annahme: $r = 1$.
- Da $n \notin \mathbb{P}$ enthält n einen ungeraden Primteiler q.
- Mit (1): Das gerade $q-1$ teilt das ungerade $n-1$. (Widerspruch)
- Annahme: n besitzt nur zwei Primteiler, d.h. $n = pq$ mit $p < q$.
- Aus $q-1 | n-1$ folgt

$$0 \equiv n-1 = pq-1 = p(q-1)+p-1 \equiv p-1 \bmod q-1.$$

- Es folgt $p \equiv 1 \bmod q$. Wegen $p < q$ gilt $p = 1$. (Widerspruch)

Bsp: Die drei kleinsten Carmichael Zahlen sind

$$561 = 3 \cdot 11 \cdot 17,\ 1105 = 5 \cdot 13 \cdot 17 \text{ und } 1729 = 7 \cdot 13 \cdot 19.$$