Der nächste Satz gibt einen Primzahltest, wenn die Primfaktorzerlegung von $n-1$ bekannt ist. Also nützlich (insbesondere aber nicht nur) für die Fermatschen Zahlen $2^{2^m}+1$.

Satz 4.19 (Primzahltest von Brillhart und Selfridge)

Sei $n-1 = \prod_{i=1}^{k} q_i^{e_i}$ mit $q_i \in \mathbb{P}$ paarweise verschieden.

$n \in \mathbb{P} \iff \forall\, 1 \le i \le k \;\; \exists\, a_i \in \mathbb{N}$ sodass

(i) $(a_i, n) = 1$

(ii) $a_i^{n-1} \equiv 1 \mod n$

(iii) $a_i^{(n-1)/q_i} \not\equiv 1 \mod n$

Beweis $\Rightarrow$: Sei a eine beliebige primitive Wurzel mod n und $a_i := a \quad \forall\, 1 \le i \le k$

Dann erfüllt a_i die drei Bedingungen.

$\Leftarrow$: Es gilt $\left.\begin{array}{l} \operatorname{ord}_n(a_i) \mid n-1 \\ \text{und } \operatorname{ord}_n(a_i) \nmid \frac{n-1}{q_i} \end{array}\right\} \forall\, 1 \le i \le k$ (L. 4.7)

also $q_i^{e_i} \mid \operatorname{ord}_n(a_i)$

Ausserdem gilt $a_i^{\phi(n)} \equiv 1 \mod n$ (Satz von Euler-Fermat)

$\Rightarrow \operatorname{ord}_n(a_i) \mid \phi(n)$ (L. 4.7)

$\Rightarrow q_i^{e_i} \mid \phi(n) \quad \forall\, 1 \le i \le k$

$\Rightarrow \prod_{i=1}^{k} q_i^{e_i} \mid \phi(n)$

d.h. $n-1 \mid \phi(n)$

$\Rightarrow n-1 \leq \phi(n)$

$\Rightarrow n \in \mathbb{P}$ $\square$

Korollar 4.20: Sei $N \in \mathbb{N}^+$

$2^N+1 \in \mathbb{P}$ wenn (i) $N = 2^n$ für ein $n \in \mathbb{N}$

(ii) $3^{2^{2^n}} \equiv 1 \mod 2^{2^n}+1$

(iii) $3^{2^{(2^n-1)}} \not\equiv 1 \mod 2^{2^n}+1$

} d.h. 3 ist eine Primitive Wurzel mod $2^{2^n}+1$

Es gilt sogar „genau dann wenn" - später:
Wir brauchen Ergebnisse aus dem Kapitel über quadratische Reste.

Dieser Test für Fermatsche Zahlen ist zwar schnell
(für $F_n := 2^{2^n}+1$ muss man $\sim \log_2(F_n)$ mal ein Quadrat mod F_n ausrechnen),
allerdings wachsen die Fermatschen Zahlen so schnell, dass die
Rechnung immerhin viel Zeit und viel Speicherplatz brauchen würde.
Man beachte: die kleinste Fermatsche Zahl, von der nicht bekannt
ist, ob sie eine Primzahl ist, ist F_{33}, die 2 585 827 973 Ziffern hat.

Ein Primzahltest für Mersennesche Zahlen

(hier ist die Zerlegung von $n+1$ anstatt $n-1$ bekannt).

Satz 4.21 (Lucas-Lehmer Test)

Sei $p \in \mathbb{P}$ und die Folge $(S_n)_{n \in \mathbb{N}^+}$ rekursiv definiert durch:

$$S_1 := 4$$
$$S_n := S_{n-1}^2 - 2$$

Dann ist $2^p - 1 \in \mathbb{P} \Leftrightarrow 2^p - 1 \mid S_{p-1}$

Beweis: Ausgelassen (siehe Wolfart)

Der Lucas-Lehmer Test wird in der online-Suche nach Mersenneschen Primzahlen verwendet

(GIMPS: Great Internet Mersenne Prime Search, www.mersenne.org)

Beispiel: $M_5 = 2^5 - 1 = 31$

$$S_1 \equiv 4 \mod 31$$
$$S_2 \equiv 4^2 - 2 \equiv 14 \mod 31$$
$$S_3 \equiv 14^2 - 2 \equiv 194 \equiv 8 \mod 31$$
$$S_4 \equiv 8^2 - 2 \equiv 62 \equiv 0 \mod 31$$

$$\Rightarrow 31 \in \mathbb{P}$$

Der schnellste bisher bekannte universelle Primzahltest ist der AKS-Primzahltest (Agarwal, Kayal, Saxena), der Laufzeit $O((\log n)^6) \log(\log n)$ braucht.

Es gibt weitere, schnellere Primzahltests die zwar keine definitive Antwort geben können, aber die bestimmen können, dass eine vorgegebene Zahl mit sehr hoher Wahrscheinlichkeit prim bzw. zusammengesetzt ist.

Kapitel 5: Quadratische Reste

In diesem Kapitel bezeichnet p eine ungerade Primzahl.

Motivation: Wir wollen $aX^2+bX+c \equiv 0 \mod p$ lösen

Angenommen $a \not\equiv 0$, können wir annehmen, wegen der Existenz von a^{-1}, dass $a \equiv 1$

Also $X^2+bX+c \equiv 0$, und $2^{-1} = \frac{1}{2} = \frac{p+1}{2}$ existiert $\mod p$.

$(X+\frac{b}{2})^2 + c - (\frac{b}{2})^2 \equiv 0$ d.h. $(X+\frac{b}{2})^2 \equiv (\frac{b}{2})^2 - c \mod p$.

Wir wollen eine Kongruenz der Gestalt $x^2 \equiv m \mod p$ lösen

Def: Eine Zahl $a \in \mathbb{Z}$ mit $p \nmid a$ heisst ein
quadratischer Rest modulo p wenn $\exists\, b \in \mathbb{Z}$ sodass

$$b^2 \equiv a \mod p.$$

Wenn kein solches b existiert, heisst a ein
quadratischer Nichtrest modulo p

Man beachte: Die Begriffe sind nur für $p \nmid a$ definiert.

Lemma 5.1: Seien $a, b, c \in (\mathbb{Z}/p\mathbb{Z})^\times$,

a, b quadratische Reste
c ein quadratischer Nichtrest

Dann ist ab ein quadratischer Rest
und ac, bc quadratische Nichtreste

Beweis: Sei $a \equiv x^2 \mod p$

$b \equiv y^2 \mod p$ für $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$

Dann ist $ab \equiv (xy)^2 \mod p$.

Wäre $ac \equiv z^2 \mod p$ für ein $z \in (\mathbb{Z}/p\mathbb{Z})^\times$

so wäre $x^2 c \equiv z^2 \mod p$

$\Rightarrow (x^{-1})^2 x^2 c \equiv (x^{-1})^2 z^2 \mod p$ (x^{-1} existiert da $x \in (\mathbb{Z}/p\mathbb{Z})^\times$)

$\Rightarrow \quad c \equiv (x^{-1}z)^2 \mod p$ ↯

also ist ac ein quadratischer Nichtrest

ähnlich ist bc ein quadratischer Nichtrest □

Wir definieren eine Notation als Abkürzung für

„a ist ein quadratischer Rest $\mod p$"

bzw. Nichtrest

Def: Für $a \in \mathbb{Z}$ ist das <u>Legendre-Symbol</u> $\left(\frac{a}{p}\right)$ definiert durch

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{wenn } a \text{ ein quadratischer Rest } \mod p \text{ ist} \\ -1 & \text{wenn } a \text{ ein quadratischer Nichtrest } \mod p \text{ ist} \\ 0 & \text{wenn } p \mid a \end{cases}$$

Bemerkung: Wenn $a \equiv b \mod p$, ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

also ist das Legendre-Symbol auf Restklassen wohldefiniert.

Lemma 5.2: Sei g eine primitive Wurzel mod p und $n \in \mathbb{N}$.

Dann gilt $\left(\frac{g^n}{p}\right) = (-1)^n$

Beweis: Es ist klar, dass $\left(\frac{g^n}{p}\right) \neq 0$.

Sei $n = 2m$ gerade, dann ist $g^n \equiv (g^m)^2 \mod p$

also $\left(\frac{g^n}{p}\right) = 1 = (-1)^n$

Sei n ungerade und wäre $g^n \equiv h^2$ für $h \in \mathbb{Z}$

Es ist $h \equiv g^m$ für ein $m \in \mathbb{N}$ (da $\{g, g^2, \dots, g^{p-1}\} = \{1, \dots, p-1\}$)

$\Rightarrow g^n \equiv (g^m)^2 \equiv g^{2m}$

$\Rightarrow g^{n-2m} \equiv 1$

$\Rightarrow p-1 = \operatorname{ord}_p(g) \mid n-2m$

$\Rightarrow n$ gerade ↯ □

Korollar 5.3: In $(\mathbb{Z}/p\mathbb{Z})^\times$ existieren genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste mod p.

Beweis: Es gibt eine primitive Wurzel g und $g, g^2, \dots, g^{p-1}$ sind die primen Restklassen

die Restklassen $g^2, g^4, \dots, g^{p-1}$ sind quadratische Reste

$g, g^3, \dots, g^{p-2}$ sind quadratische Nichtreste □

Lemma 5.4: Seien $a, b \in \mathbb{Z}$

(i) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Bemerkung: (i) heisst das Eulersche Kriterium

Mit (ii) können wir das Ausrechnen von $\left(\frac{n}{p}\right)$ auf das entsprechende Problem für Primzahlen $\left(\frac{q}{p}\right)$ reduzieren.

Beweis: Nächstes Mal.