Wiederholung

Def: <u>Carmichaelzahl</u> $n > 1$

(i) $n \notin \mathbb{P}$

(ii) $a^{n-1} \equiv 1 \mod n \quad \forall a \in \mathbb{Z}$ mit $(a,n)=1$.

Satz 4.12: $n = q_1 \cdots q_k$ $(q_i \in \mathbb{P})$ ist eine Carmichaelzahl genau dann wenn

(i) $k \geq 2$

(ii) n ist quadratfrei $(q_i \neq q_j$ für $i \neq j)$

(iii) $q_i - 1 \mid n-1 \quad \forall 1 \leq i \leq k$

Beweis: $\Rightarrow$ (i): klar

(ii): Angenommen $n = p^a b$ mit $p \in \mathbb{P}$, $a \geq 2$ und $(p,b)=1$ (eventuell $b=1$)

Dann ist $(p^{a-1}b+1, n) = 1$

und $(p^{a-1}b+1)^{n-1} = (p^{a-1}b)^{n-1} + \binom{n-1}{1}(p^{a-1}b)^{n-2} + \cdots$

$$\cdots + \binom{n-1}{n-3}(p^{a-1}b)^2 + \binom{n-1}{n-2}p^{a-1}b + 1$$

$$\equiv 0 + 0 + \cdots + 0 + (n-1)p^{a-1}b + 1 \mod n$$

$$\equiv 1 - p^{a-1}b \mod n$$

$$\not\equiv 1 \mod n \quad \lightning$$

(iii): Sei a_i eine primitive Wurzel mod q_i (existiert nach Satz 4.10)

Nach dem Chinesischen Restsatz gibt es eine Zahl x sodass

$$x \equiv a_1 \mod q_1$$
$$x \equiv 1 \mod q_2$$
$$x \equiv 1 \mod q_3$$
$$\vdots$$
$$x \equiv 1 \mod q_k$$

insbesondere ist $(x, q_i) = 1 \quad \forall i$

also $(x, n) = 1$

$\operatorname{ord}_{q_i}(x) = q_i - 1$ (da x eine primitive Wurzel mod q_i ist)

und $x^{n-1} \equiv 1 \mod n = q_1 \cdots q_k$

also $x^{n-1} \equiv 1 \mod q_i$

$\Rightarrow q_i - 1 = \operatorname{ord}_{q_i}(x) \mid n-1$ (L. 4.7)

ähnlich gilt $q_i - 1 \mid n-1 \quad \forall 1 \le i \le k$

$\Leftarrow$: Sei $(a, n) = 1$

$\Rightarrow (a, q_i) = 1 \quad \forall 1 \le i \le k$

$\Rightarrow a^{q_i - 1} \equiv 1 \mod q_i$ (kleiner Fermatscher Satz)

$\Rightarrow a^{n-1} \equiv 1 \mod q_i$ $(q_i - 1 \mid n-1)$

1 ist eine Lösung zu $z \equiv 1 \mod q_i \quad \forall 1 \le i \le k$

Nach dem Chinesischen Restsatz ist die Lösung eindeutig mod $q_1 \cdots q_k = n$

$\Rightarrow a^{n-1} \equiv 1 \mod n$ □

Korollar 4.14: Eine Carmichaelzahl ist stets ungerade und hat mindestens drei Primfaktoren

Beweis: Wäre 2 ein Primfaktor einer Carmichaelzahl n, p ein weiterer Primfaktor ($p \neq 2$ wegen (ii))

dann ist $n-1$ ungerade und $p-1$ gerade,

also $p - 1 \nmid n - 1$ ↯

Hätte n nur zwei Primfaktoren $q < p$

dann gilt $p-1 \mid n-1 = pq - 1$

$= (p-1)q + q - 1$

$\Rightarrow p-1 \mid q-1$

aber $q < p$ ↯ □

Wegen der Existenz von Carmichaelzahlen, kann der kleine Fermatsche Satz nicht als unfehlbarer Primzahltest verwendet werden.

Gibt es andere Möglichkeiten?

Proposition 4.15: Sei $n \in \mathbb{N}$, $n \geq 2$

Es gibt eine Zahl $a \in \mathbb{Z}$ mit $\operatorname{ord}_n(a) = n-1$

$\Leftrightarrow n \in \mathbb{P}$

Beweis: $\Leftarrow$: Satz 4.10

$\Rightarrow$: Angenommen es gibt ein solches a.

Es ist $a^{\phi(n)} \equiv 1 \mod n$

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

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

$\Rightarrow$ Es gibt mindestens $n-1$ Zahlen in $1, \ldots, n-1$ die zu n teilerfremd sind

$\Rightarrow$ Es gibt keinen Teiler $\neq 1$ von n in $2, \ldots, n-1$

$\Rightarrow n \in \mathbb{P}$. □

Satz 4.16 (Wilson): Sei $2 \leq n \in \mathbb{N}$

Dann ist $n \in \mathbb{P} \Leftrightarrow (n-1)! \equiv -1 \mod n$.

Beweis: $\Leftarrow$: Sei $n \notin \mathbb{P}$ und k ein nicht-trivialer Teiler

Dann ist $k \in \{2, \dots, n-1\}$

also $(n-1)! \equiv 0 \mod k$

wenn $x \equiv -1 \mod n$

dann ist $x \equiv -1 \mod k$

also ist $(n-1)! \not\equiv -1 \mod n$.

$\Rightarrow$: Sei $n = p \in \mathbb{P}$

Angenommen $m \in \{1, 2, \dots, p-1\}$ mit $m^2 \equiv 1 \mod p$

Dann ist $m^2 - 1 = (m+1)(m-1) \equiv 0 \mod p$

$\Rightarrow m+1 \equiv 0$ oder $m-1 \equiv 0 \mod p$

$\Rightarrow m \equiv \pm 1 \mod p$

Also sind 1 und $p-1$ die einzigen Restklassen, die zu sich selbst invers sind.

$\Rightarrow$ alle Restklassen in $\{2, \dots, p-2\}$ können in Paare $\{a_i, b_i\}$ aufgeteilt werden, mit $a_i b_i \equiv 1 \mod p$.

$\Rightarrow (p-1)! \equiv 1 \cdot (p-1) \mod p$

$\equiv -1 \mod p$

□

Diese zwei Tests sind aber rechnerisch sehr aufwändig:

Für Prop. 4.15 muss man eventuell Potenzreihen von $\sim n$ verschiedenen Zahlen bis Exponent $\sim n$ ausrechnen - $\sim n^2$ Schritte.

für Satz 4.16 muss man $\sim n$ Zahlen multiplizieren, $\sim n$ Schritte.

Deswegen sind sie in der Praxis nicht nützlich.

Idee: Prop 4.15 könnte man eventuell verbessern, wenn man wüsste, wo man am besten nach primitiven Wurzeln suchen sollte.

Den folgenden Satz verwenden wir ohne Beweis

Satz 4.17 (Burgess): $\forall\, \delta > 0\ \exists\, C$ sodass folgendes gilt:

Sei $p \in \mathbb{P}$. Dann existiert eine primitive Wurzel $a \bmod p$ mit $a \leq C p^{(\frac{1}{4}+\delta)}$.

Das heisst, mindestens eine primitive Wurzel erscheint „früh".

Daraus folgt folgende Verbesserung von Prop. 4.15

Satz 4.18 (Primzahltest von Pollard)

Es gibt ein Zahl n_0 sodass $\forall\, n \in \mathbb{N},\ n > n_0$ gilt

$n \in \mathbb{P} \iff$ (i) n keine Quadratzahl ist

(ii) n keinen Primteiler $p \leq n^{1/3}$ besitzt

und (iii) $k^{n-1} \equiv 1 \bmod n \quad \forall\, k \leq n^{1/3}$.

Beweis: $\Rightarrow$: klar

$\Leftarrow$: Angenommen $n \notin \mathbb{P}$

Nach (ii) ist dann $n = pq$ mit $p, q \in \mathbb{P}$
und $n^{1/3} < q \leq p < n^{2/3}$.

Nach (i) ist $p \neq q$.

Sei $\delta = \frac{1}{40}$. Nach Satz 4.17 existiert C sodass eine primitive Wurzel a modulo p existiert mit

$$\begin{aligned} a &\leq C p^{\frac{1}{4}+\frac{1}{40}} \\ &< C n^{\frac{1}{6}+\frac{1}{60}} \\ &= C n^{11/60} \\ &< n^{1/5} \qquad \text{für } n > n_0 := C^{60} \end{aligned}$$

Also $\operatorname{ord}_p(a) = p-1$

und nach (iii) ist $a^{n-1} \equiv 1 \mod n$

$$\begin{aligned} &\Rightarrow a^{n-1} \equiv 1 \mod p \\ &\Rightarrow p-1 \mid n-1 \qquad (\text{L } 4.7) \\ &\qquad = pq-1 \\ &\qquad = (p-1)q + q - 1 \\ &\Rightarrow p-1 \mid q-1 \end{aligned}$$

aber $p > q$ ↯ □

Bemerkung: Satz 4.18 liefert einen Primzahltest, der $O(n^{1/3})$ Schritte braucht, mit Laufzeit $o(n^{\frac{1}{3}+\varepsilon})$ für jedes $\varepsilon > 0$.

Vermutung (Artin): Sei $a \in \mathbb{N}$ keine Quadratzahl.

Dann existiert $p \in \mathbb{P}$ sodass a eine primitive Wurzel mod p ist.

Bisher waren alle Primzahltests universell, d.h. sie funktionieren für beliebige Zahlen n.

Andere Tests nutzen zusätzliches Wissen über n, sind also für Zahlen einer bestimmten Form geeignet.