Primzahltests

Julia Bicker

28.Mai.2019

Lucas-Lehmer Test
Sei $n = 2^p - 1$ für ungerade Primzahl p $\in \mathbb{P}$.
Sei weiterhin die Folge S_k definiert durch:

$$S_1 = 4$$
$$S_k = S_{k-1}^2 - 2$$

n ist genau dann prim, falls n die Zahl S_{p-1} teilt.

Lucas Test
Eine natürliche Zahl n ist genau dann eine Primzahl, wenn es eine natürliche Zahl $0 < a < n$ gibt mit

$$a^{n-1} \equiv 1 \mod n, \text{ aber } a^{\frac{n-1}{q}} \not\equiv 1 \mod n$$

für alle Primteiler q von $n - 1$.

Pocklington Test
Sei $n \in \mathbb{N}$, sodass $n - 1$ eine Faktorisierung der Form $n - 1 = R * F$ besitzt, wobei alle Primteiler von F bekannt sind. Weiterhin gebe es eine natürliche Zahl $0 < a < n$ mit

$$a^{n-1} \equiv 1 \mod n \text{ und } ggT(a^{\frac{n-1}{q}} - 1, n) = 1$$

für alle Primteiler q von F. Ist dann $F \geq \sqrt{n}$, dann ist n eine Primzahl.

Pepin Test
Die Zahl $F_k = 2^{2^k} + 1$, $k \geq 1$ ist genau dann eine Primzahl wenn gilt

$$3^{\frac{F_k - 1}{2}} \equiv -1 \mod F_k$$

Solovay-Strassen Test
Sei $n \geq 3$ ungerade. Dann ist n genau dann eine Primzahl, wenn für jede natürliche Zahl a mit $0 < a < n$ und $ggT(a, n) = 1$ gilt

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

Falls n nicht prim ist, ist die Kongruenz für mindestens die Hälfte aller a nicht erfüllt.

Miller-Rabin Test
Sei $n \geq 3$ und $n - 1 = 2^t m$ für m ungerade. n ist genau dann eine Primzahl, wenn für jede zu n teilerfremnde natürliche Zahl a mit $0 < a < n$ gilt

$$a^m \equiv 1 \mod n \text{ oder } a^{2^s m} \equiv -1 \mod n \text{ für ein } s \in \{0, 1, ..., t - 1\}$$

Ist n keine Primzahl, so erfüllt höchstens $\frac{1}{4}$ aller a eine der Bedingungen.