

Primzahltest für Fermat-Zahlen

Wir betrachten Zahlen $G_n = 2^{2^n} + 1$ und möchten sie auf Primalität testen.

Zunächst zeige der Leser leicht selbst, daß G_n höchstens dann prim sein kann, wenn n selbst eine Zweierpotenz ist¹.

Ist $N = G_n$ prim, so besitzt die multiplikative Gruppe des Körpers \mathbb{Z}_N 2^n Elemente.

Ein Erzeuger ζ dieser multiplikativen Gruppe ist offenbar dadurch charakterisiert, daß $\zeta^{2^n} = 1$ und $\zeta^{2^{n-1}} = -1$. Man überlegt leicht, daß alle Nicht-Quadrate Erzeuger von \mathbb{Z}_N^* sind. Mittels des quadratischen Reziprozitätsgesetzes rechnet man dann leicht nach, daß 3 ein Nicht-Quadrat und daher ein Erzeuger ist. Setzt man also $\zeta = \zeta_0 = 3$ und $\zeta_{k+1} = \zeta_k^2$, so ist $\zeta_k = \zeta^{2^k}$ und somit $\zeta_{n-1} = -1$.

Ist dagegen $N = G_n$ nicht prim, so ist die Ordnung der multiplikativen Gruppe \mathbb{Z}_N^* sicher kleiner als 2^n ; daher kann in der Folge (ζ_n) , die durch wiederholtes Quadrieren aus 3 entsteht, nicht $\zeta_{n-1} = -1$ zustande kommen. Sonst wäre ja die Ordnung von 3 in \mathbb{Z}_N^* ein Teiler von 2^n , also selbst eine Zweierpotenz $2^k < 2^n$. Damit wären ζ_k und auch die weiteren Folgenglieder 1.

Also ist $\zeta_{n-1} = -1$ eine notwendige und hinreichende Bedingung dafür, daß G_n prim ist.

Das folgende einfache Pari-Programm realisiert den Test:

```
gausstest(n) =
{
    local (p=2^n+1, t=Mod(3,p)); print(p);
    for(i=1, n-1, t=t^2);

    if(t== -1, return(1), return(0));
}
```

Damit läßt sich in einigen Stunden zeigen, daß z.B. die Fermatzahl $F_{20} = G_{2^0}$ nicht prim ist.

Bis F_{32} läßt sich – im Prinzip mit obigem Test – bisher zeigen, daß die Fermatzahlen ab F_4 nicht prim sind. Speziell von der Fermatzahl $F_{382447} = 2^{382447} + 1$ ist aber sogar ein Faktor bekannt. (Siehe auch http://en.wikipedia.org/wiki/Fermat_number).

(p-1) - Test . Der obige Test für Fermat-Zahlen ist ein Spezialfall des sog. (p-1)-Tests:

Eine Zahl N ist genau dann prim, wenn es in \mathbb{Z}_N ein Element der Ordnung $N-1$ gibt!

Dies ist offenbar gleichbedeutend mit:

Eine Zahl N ist genau dann prim, wenn es ein Element $a \in \mathbb{Z}_N$ gibt mit

$$a^{N-1} = 1$$
$$a^q \neq 1 \quad \text{für alle Primteiler } q \text{ von } N-1.$$

Will man dies ausnutzen, muß man natürlich die Primfaktorzerlegung von $N-1$ kennen.

Bei der obigen Anwendung des (p-1)-Tests auf Fermat-Zahlen ist die Faktorisierung von $N-1$ ja gerade durch eine Zweierpotenz gegeben und daher besonders einfach.

1 Man nennt $F_n := G_{2^n}$ eine Fermat-Zahl

2 Als ersten Primzahltest hatten wir seinerzeit den Fermat-Test kennengelernt. Dabei wird nachgeprüft, ob $a^{N-1} = 1$ gilt für ein zufällig gewähltes Element $a \in \mathbb{Z}_N^*$. In diesem Fall gilt dann nur $\text{ord } a \mid N-1$, während beim p-1 Test $\text{ord } a = N-1$ gezeigt werden soll.