

Seminar: Primzahltests
Referenten: Jens Bernheiden
Matthias Döppe

Datum: 09.06.1998



Benötigte Sätze für die Primzahltests (Ohne Beweis):

Satz 1:

N ungerade, $\text{ggT}(N,D)=1 \Rightarrow \Psi_D(N) = N - \left(\frac{D}{N}\right) \Leftrightarrow N$ Primzahl.

Satz 2:

N ungerade, $\text{ggT}(N,QD)=1$, $N - \left(\frac{D}{N}\right)$ teilt $\Psi_D(N) \Leftrightarrow N$ Primzahl.

Satz 3:

N ungerade, es existiert eine Lucas-Folge $U=U(P,Q)$ mit Diskriminante $D=P^2-4Q$ und $\text{ggT}(N,QD)=1$
 $\Leftrightarrow N|U_{\Psi_D(N)}$

Satz 4:

N ungerade, es existiert eine Lucas-Folge $U=U(P,Q)$ mit Diskriminante $D=P^2-4Q$
und $\left(\frac{D}{N}\right) = -1$, $N|U_{N+1}$
 $\Rightarrow \text{ggT}(N,QD)=1$.

Satz 5:

N ungerade, q ein Primfaktor der Primfaktorzerlegung von $N+1$,
Angenommen: es existiert die Lucas-Folgen $U=U(P,Q)$ und $V=V(P,Q)$ mit der Diskriminante $D \neq 0$, $\text{ggT}(P,Q)=1$ oder das $\text{ggT}(N,Q)=1$.
 $N|U_{(N+1)/q}$ und $N|V_{(N+1)/2} \Rightarrow N|V_{(N+1)/2q}$.

Satz 6:

p teilt nicht $2QD \Rightarrow V_{p-(D/p)} \equiv 2Q^{(1-(D/p))/2} \pmod{p}$

Satz 7:

Angenommen: es existiert ein $\rho(n) \Rightarrow n|U_k \Leftrightarrow \rho(n)|k$

Satz 8:

$U_{2n} = U_n V_n$

Definitionen:

$$\Psi_D(N) = \frac{1}{2^{s-1}} \prod_{i=1}^s \left(p_i^{e_i-1} \left(p_i - \left(\frac{D}{p_i} \right) \right) \right) = \frac{1}{2^{s-1}} \prod_{i=1}^s (p_i^{e_i} \pm p_i^{e_i-1}), \text{ wobei } N = \prod_{i=1}^s p_i^{e_i}$$

$\rho(n)$ ist die kleinste Zahl r , so daß N/U_r

Legendre-Symbol:

c^2 ein quadratischer Rest und p Primzahl

$$\left(\frac{a}{p} \right) = \begin{cases} 0 & \rightarrow a \equiv 0 \pmod{p} \\ 1 & \rightarrow a \equiv c^2 \pmod{p} \\ -1 & \rightarrow a \equiv b \pmod{p} \end{cases}$$

Gaussches Reziprozitätsgesetz:

q und p sind ungerade Primzahlen und $p \neq q$, dann: $\left(\frac{q}{p} \right) = \left(\frac{p}{q} \right) (-1)^{\frac{q-1}{2} \frac{p-1}{2}}$

Jacobi-Symbol:

Def.: $\left(\frac{a}{b} \right) = \prod_{p|b} \left(\frac{a}{p} \right)^{e_p}$, wobei: $|b| = \prod_{p|b} p^{e_p}$, $e_p \geq 1$

Es gelten folgende Regeln:

1. $\left(\frac{aa'}{b} \right) = \left(\frac{a}{b} \right) \left(\frac{a'}{b} \right)$

2. $\left(\frac{a}{bb'} \right) = \left(\frac{a}{b} \right) \left(\frac{a}{b'} \right)$

3. $\left(\frac{2}{b} \right) = (-1)^{\frac{b^2-1}{8}} = \begin{cases} +1 & \rightarrow b \equiv \pm 1 \pmod{8} \\ -1 & \rightarrow b \equiv \pm 3 \pmod{8} \end{cases}$

4. $\left(\frac{-1}{b} \right) = (-1)^{\frac{b-1}{2}} = \begin{cases} +1 & \rightarrow b \equiv +1 \pmod{4} \\ -1 & \rightarrow b \equiv -1 \pmod{4} \end{cases}$

5. a und b sind relativ prim ($\text{ggT}(a,b)=1$), ungerade und $b \geq 3$:

$$\left(\frac{a}{b} \right) = \left(\frac{b}{a} \right) (-1)^{\frac{a-1}{2} \frac{b-1}{2}}$$

Das Jacobi-Symbol ist dann Legendre-Symbol, wenn b eine Primzahl ist.

Primzahltests:

1. Test (Beweis mit den Sätzen 2,3,4,6 und 7)

- $N > 1$ und ungerade und $N + 1 = \prod_{i=1}^s q_i^{f_i}$
- Angenommen es existiert ein D mit $\left(\frac{D}{N}\right) = -1$ und für jedes q_i von $N+1$ existiert eine Lucas-Folge $\left(U_n^{(i)}\right)_{n \geq 0}$ mit $D = P^2 - 4Q_i$, wobei gilt: $\text{ggT}(P_i, Q_i) = 1$ oder $\text{ggT}(N, Q_i) = 1$ und außerdem gilt: N teilt $U_{N+1}^{(i)}$ und N teilt nicht $U_{(N+1)/q_i}^{(i)}$, dann ist N eine Primzahl

Nachteile des Tests: Kenntnis über Primzahlzerlegung von $N+1$, Berechnung von U_{N+1}

2. Test (Beweis mit dem Sätzen 5 und 8)

- $N > 1$ und ungerade und $N + 1 = \prod_{i=1}^s q_i^{f_i}$
- Angenommen es existiert ein D mit $\left(\frac{D}{N}\right) = -1$ und für jedes q_i von $N+1$ existiert eine Lucas-Folge $\left(V_n^{(i)}\right)_{n \geq 0}$ mit $D = P^2 - 4Q_i$, wobei gilt: $\text{ggT}(P_i, Q_i) = 1$ oder $\text{ggT}(N, Q_i) = 1$ und außerdem gilt: N teilt $V_{(N+1)/2}^{(i)}$ und N teilt nicht $V_{(N+1)/2q_i}^{(i)}$, dann ist N eine Primzahl

Nachteile des Tests: Siehe Test 1, ein q_i der Primzahlzerlegung von $N+1$ muß mindestens 2^2 sein

3. Test (Beweis mit den Sätzen 3,4,5,6 und 7)

- $N > 1$ und ungerade und q ein Primfaktor von $N+1$, wobei gilt: $2q > \sqrt{N} + 1$
- Angenommen es existiert eine Lucas-Folge $\left(V_n\right)_{n \geq 0}$ Diskriminante $D = P^2 - 4Q$, wobei gilt: $\text{ggT}(P, Q) = 1$ oder $\text{ggT}(N, Q) = 1$, $\left(\frac{D}{N}\right) = -1$ und außerdem gilt: N teilt $V_{(N+1)/2}$ und N teilt nicht $V_{(N+1)/2q}$, dann ist N eine Primzahl

Nachteile des Tests: Wissen über Primzahlzerlegung, mindestens ein q , so daß gilt:

$$2q > \sqrt{N} + 1$$

Anwendung der Tests besonders für Zahlen der Form: $N = A \cdot 2^B - 1$, weil die Primzahlzerlegung von $N + 1 = \text{Zerlegung}(A) \cdot 2^B$ relativ einfach zu bewältigen ist (über 2^B lassen sich sehr große Zahlen konstruieren).