Handout zum Vortrag „Primzahltests für MERSENNE-Primzahlen“

Michael H. Mertens

16. Oktober 2010

Die Nummerierung ist im Wesentlichen konsistent mit der Nummerierung der Ausarbeitung zum Vortrag. Für ausführliche Diskussionen der einzelnen Resultate siehe dort.

Definitionen

- p-te MERSENNE-Zahl: $M_p = 2^p - 1$
- LUCAS-Folge: $L_{k+1} = L_k^2 - 2$, $L_0 = 4$.
- $G_{k+1} = \frac{(G_k^2+12)^2}{4G_k(G_k^2-12)}$, $G_0 = -2$.
- $\varepsilon = 2 + \sqrt{3}$
- E bezeichnet in Abschnitt 4 stets die elliptische Kurve mit der WEIERSTRASS-Gleichung $y^2 = x(x^2-12)$ über $\mathbb{Q}$, $\hat{E}$ die Reduktion von E modulo einer Primzahl q.

Hauptresultate

Satz 3.4 (LUCAS-LEHMER)
Falls die MERSENNE-Zahl $M_p = 2^p - 1$, $p \in \mathbb{P}$ eine Primzahl ist, dann gilt $L_k \not\equiv 0 \pmod{M_p}$ für $k \in \{0, ..., p-3\}$ und $L_{p-2} \equiv 0 \pmod{M_p}$.
Umgekehrt gilt, dass M_p prim ist, wenn $\text{ggT}(L_k, M_p) = 1$ für $k \in \{0, ..., p-3\}$ und $\text{ggT}(L_{p-2}, M_p) > 1$ gilt.

Algorithmus 5.1 (LUCAS-LEHMER-**Test**)

EINGABE:	$p \in \mathbb{P}$
ALGORITHMUS:	$L \leftarrow 4$
	`Für` k `zwischen` 1 `und` $p-2$ `berechne`
	$L \leftarrow L^2 - 2 \pmod{M_p}$
AUSGABE:	M_p `ist prim, falls` $L = 0$
	M_p `ist zusammengesetzt, sonst.`

Satz 4.3
Es sei $M_p = 2^p - 1$ eine Primzahl. Dann ist $G_k(G_k^2 - 12)$ eine Einheit in $\mathbb{Z}_{M_p}$ für $k \in \{0, ..., p-2\}$ und $G_{p-1} \equiv 0 \pmod{M_p}$.
Gilt umgekehrt $\mathrm{ggT}(G_k(G_k^2-12), M_p) = 1$ für $k \in \{0, ...p-2\}$ und $\mathrm{ggT}(G_{p-1}, M_p) > 1$, so ist die MERSENNE-Zahl M_p prim.

Algorithmus 5.2 (**Elliptic-Test**)

EINGABE:	$p \in \mathbb{P}$
ALGORITHMUS:	$G \leftarrow -2$
	`Für` k `zwischen` 1 `und` $p-1$ `berechne`
	$G \leftarrow (G^2+12)^2/4G(G^2-12) \pmod{M_p}$
	`Falls` G `nicht existiert: Abbruch`
AUSGABE:	M_p `ist zusammengesetzt, falls Abbruch oder` $G \neq 0$
	M_p `ist prim, falls` $G = 0$.

Grundlegende Hilfsresultate

Satz 1.6 Quadratisches Reziprozitätsgesetz
Es seien p und q ungerade Primzahlen.
Dann gilt

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

oder äquivalent dazu

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{, falls } p \text{ und } q \equiv -1 \pmod 4 \\ \left(\frac{q}{p}\right) & \text{sonst} \end{cases}.$$

Satz 2.12 HASSE**sche Ungleichung**
Es sei $K = \mathbb{F}_q$ ein Körper der Charakteristik $p \in \mathbb{P}$ und E_f eine elliptische Kurve über K. Dann gilt für die Anzahl der K-rationalen Punkte von E_f

$$q + 1 - 2\sqrt{q} \leq |E_f(K)| \leq q + 1 + 2\sqrt{q}.$$

Beispiele für Isogenien

1. Für $m \in \mathbb{Z}$ definiert die Multiplikation mit m auf kanonische Weise eine Isogenie auf einer elliptischen Kurve E:

$$[m] : E \to E, P \mapsto mP := \begin{cases} \underbrace{P + ... + P}_{m \text{ Stück}} & \text{, falls } m > 0 \\ -m(-P) & \text{, falls } m < 0 \end{cases}.$$

   Diese Abbildung ist offenbar für jeden Punkt $P \in E$ wohldefiniert , da E als ABELsche Gruppe ein $\mathbb{Z}$-Modul ist und ist eine rationale Abbildung, da dies offenbar für die Addition zweier Punkte gilt.

2. Der FROBENIUS-Endomorphismus im Falle eines endlichen Grundkörpers ist eine Isogenie.

3. Wenn es Endomorphismen von E gibt, die sich nicht als Multiplikation mit einer ganzen Zahl ausdrücken lassen, so hat E **komplexe Multiplikation**. über endlichen Körpern ist das immer der Fall, denn dort gibt es stets den FROBENIUS-Endomorphismus, der sich nicht als Multiplikation darstellen lässt.

Spezielle Hilfsresultate

Satz 2.18
Es sei L ein algebraischer Zahlkörper und E_f eine elliptische Kurve über L mit komplexer Multiplikation in einem Teilkörper K von $\overline{L}$ und guter Reduktion bezüglich eines Primideals $\mathfrak{P}$ von K. Es bezeichne weiterhin L' das Kompositum von L und K, also den kleinsten Teilkörper von $\overline{K}$, der K und L enthält und $\hat{E_f}$ die Reduktion von E_f modulo $\mathfrak{P}$.
Dann gilt:

$$\hat{E} \text{ ist } \begin{cases} \text{gewöhnlich, falls } \mathfrak{P} \text{ in } L' \text{ zerlegt} \\ \text{supersingulär, falls } \mathfrak{P} \text{ in } L' \text{ träge ist oder verzweigt} \end{cases} .$$

Satz 2.21
Es sei E_f eine elliptische Kurve über einem Körper K ($\mathrm{char}(K) \neq 2$) mit WEIERSTRASS-Polynom

$$f(x,y) = y^2 - x^3 - ax^2 - bx - c = y^2 - (x-\alpha)(x-\beta)(x-\gamma).$$

Für den Punkt $P = (x', y') \in E_f(K)$ existiert genau dann ein Punkt $Q = (x, y)$ mit $2 \cdot Q = P$, wenn $(x' - \alpha)$, $(x' - \beta)$ und $(x' - \gamma)$ Quadrate in K sind.

Proposition 3.1
ei $q \in \mathbb{P}$ mit $q \equiv 7 \pmod{24}$. Dann ist $T(q) \cong C_{q+1}$, also $T(q)$ ist zyklisch und hat Ordnung $q+1$, und ε ist kein Quadrat in $T(q)$.

Proposition 4.2
Es sei $q \in \mathbb{P}$ mit $q \equiv 7 \pmod{24}$. Dann ist $E(q)$ zyklisch und hat Ordnung $q+1$,

$$E(q) \cong C_{q+1}.$$

Der Punkt $P = (-2, 4) \in E(q)$ ist nicht durch 2 teilbar.