Primzahltests für Mersenne-Primzahlen

Ausarbeitung zum Vortrag im Seminar zur
Computeralgebra im WS 2010/2011
bei Frau Prof. Dr. G. Nebe, RWTH Aachen

Michael H. Mertens
Matrikelnummer: 289246

Inhaltsverzeichnis

1 Verwendete Resultate aus der Zahlentheorie **3**
1.1 Elementare Zahlentheorie 3
1.2 Quadratische Reste 4
1.3 Quadratische Zahlkörper 6

2 Elliptische Kurven **9**
2.1 Geometrie elliptischer Kurven 9
2.2 Elliptische Kurven als ABELsche Gruppen 11
2.3 Supersingularität und Kombinatorik 13
2.4 Isogenien und komplexe Multiplikation 14

3 Lucas-Lehmer Test für Mersenne-Zahlen **20**

4 Mersenne-Zahlen und Elliptische Kurven **24**

5 Algorithmen und Effizienz **28**

Einleitung

Die vorliegende Ausarbeitung behandelt hauptsächlich auf der Grundlage des Artikels "An elliptic curve test for Mersenne primes" von Benedict H. Gross (geb. 1950) eine Möglichkeiten, mit Hilfe elliptischer Kurven Mersenne-Zahlen auf Primeigenschaft zu testen. Gottfried Wilhelm Leibniz (1646-1716) vermutete, dass für jede Primzahl p die Zahl $M_p = 2^p - 1$ ebenfalls eine Primzahl ist. Das Beispiel $M_{11} = 2^{11} - 1 = 23 \cdot 89$ zeigt aber, dass dies offenbar nicht der Fall ist. Genauer ist bis heute noch nicht einmal bekannt, ob es unendlich viele Primzahlen p gibt, so dass M_p prim ist. Man kennt bis jetzt (Stand 08.09.2010) genau 47 Mersennesche Primzahlen (Quelle: http://www.mersenne.org), also scheint es sehr sinnvoll zu sein, neue Testverfahren hierfür zu entwickeln.

In dieser Ausarbeitung wird wie folgt vorgegangen:
Zunächst werden in den Abschnitten 1 und 2 verwendete Resultate aus der elementaren und algebraischen Zahlentheorie (Quadratische Reste, Quadratische Zahlkörper) und über elliptische Kurven bereitgestellt (nur zum Teil bewiesen, da dies den Rahmen sprengen würde).
Im 3. Abschnitt wird der bekannte Test von Édouard Lucas neu mit Begriffen der algebraischen Geometrie interpretiert, nämlich als Quadrieren eines Punktes auf dem eindimensionalen algebraischen Torus über $\mathbb{Q}$ zum quadratischen Zahlkörper $\mathbb{Q}(\sqrt{3})$, und bewiesen.
Ziel des 4. Abschnittes ist es, einen neuen Primzahltest für Mersenne-Zahlen vorzustellen, der auf dem Quadrieren eines Punktes auf der elliptischen Kurve zu

$$y^2 = x^3 - 12x$$

über dem Körper $\mathbb{Q}$ basiert. Dies ist der von Gross vorgeschlagene Test.
Zum Schluss werden im 5. Abschnitt die beide Tests hinsichtlich ihrer Effizienz verglichen und eine Implementierung in dem Software-Paket `Sage` vorgestellt.

Es wird weitestgehend die übliche Notation für Zahlbereiche ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$,...) verwendet, außerdem bezeichne $\mathbb{P}$ die Menge aller positiven Primzahlen in $\mathbb{Z}$.

1 Verwendete Resultate aus der Zahlentheorie

1.1 Elementare Zahlentheorie

Definition 1.1.
Zu $p \in \mathbb{P}$ heißt $M_p := 2^p - 1$ die p-te Mersenne-***Zahl***.

Wir werden uns in der ganzen Ausarbeitung mit der Frage beschäftigen, wann M_p eine Primzahl ist. Dazu zunächst ein paar kleine Beobachtungen:

Lemma 1.2.

1. *Ist $M_p \in \mathbb{P}$, so ist notwendigerweise $p \in \mathbb{P}$.*
2. *Es gilt für alle $p \in \mathbb{P} \setminus \{2\}$:*

$$M_p \equiv 7 \pmod{24}.$$

Beweis. zu 1.: Nehmen wir an, p wäre nicht prim, z.B. $p = k \cdot \ell$, wobei k, $\ell > 1$. Dann gilt

$$\begin{aligned} M_p = 2^p - 1 &= 2^{k\cdot\ell} - 1 \\ &= (2^k)^\ell - 1 \\ &= \underbrace{(2^k - 1)}_{>1} \cdot \sum_{i=0}^{\ell-1} 2^i \cdot (-1)^{\ell-i} \end{aligned}$$

Damit ist aber offensichtlich eine nicht-triviale Faktorisierung von M_p gefunden, das aber als prim vorausgesetzt war. Das ist ein Widerspruch und die Behauptung ist gezeigt.
zu 2.: Nach dem Chinesischen Restsatz ist die Behauptung äquivalent dazu, dass

$$M_p \equiv 1 \pmod{3} \text{ und } M_p \equiv 7 \pmod{8}.$$

Da für ungerades $p \in \mathbb{P}$ gilt, dass $2^p \equiv 2 \pmod{3}$, ist in der Tat

$$M_p = 2^p - 1 \equiv 1 \pmod{3}.$$

Desweiteren ist p als ungerade Primzahl insbesondere größer oder gleich 3, also ist $2^p \equiv 0 \pmod{8}$ und damit ist

$$M_p \equiv -1 \equiv 7 \pmod{8}.$$

Daraus folgt die Behauptung.

□

1.2 Quadratische Reste

Neben diesen elementaren Beobachtungen brauchen wir auch einige Resultate über quadratische Reste, die hier nur zitiert sein sollen. Für Beweise und umfassendere Informationen sei z.B. auf [ReUl], S.237ff verwiesen.

Definition 1.3.

1. *Seien $a \in \mathbb{Z}$, $p \in \mathbb{P}$ und $\mathrm{ggT}(a,p) = 1$. Dann heißt a ein **quadratischer Rest** modulo p, wenn es ein $x \in \mathbb{Z}$ gibt mit*

$$a \equiv x^2 \pmod{p}.$$

*Anderenfalls heißt a ein **quadratischer Nichtrest** modulo p.*

2. *Für a, p wie in 1. heißt der Ausdruck*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{, falls } a \text{ quadratischer Rest modulo } p \\ -1 & \text{, falls } a \text{ quadratischer Nichtrest modulo } p \end{cases}$$

das Legendre-***Symbol***.

Bemerkung 1.4.

1. *Es gilt für ungerades $p \in \mathbb{P}$:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Diese Identität nennt man auch das Euler-***Kriterium***.

2. *Das* Legendre-*Symbol ist multiplikativ, das bedeutet,*

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Beweis. zu 1. Diese Identität folgt sofort aus dem kleinen Satz von Fermat, laut dem

$$a^{p-1} \equiv 1 \pmod{p}$$

gilt, falls $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Ist a ein quadratischer Rest modulo p, dann gibt es ein $x \in \mathbb{Z}$ mit

$$x^2 \equiv a \pmod{p}.$$

Dann ist aber auch

$$x^{p-1} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

wobei nach Voraussetzung $\left(\frac{a}{p}\right) = 1$.

Ist a kein Quadrat modulo p, dann hat offenbar $a^{\frac{p-1}{2}}$ Ordnung 2 in $(\mathbb{Z}/p\mathbb{Z})^*$, also ist $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
zu 2. Folgt sofort aus 1.

□

Aufgrund dieser Bemerkung reicht es offenbar, die LEGENDRE-Symbole von Primzahlen und -1 beschreiben zu können. Eine Möglichkeit dazu liefern die folgenden Sätze:

Satz 1.5.
Sei p eine ungerade Primzahl.

1. -1 *ist genau dann ein quadratischer Rest modulo p, wenn* $p \not\equiv 3 \pmod 4$,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{, falls } p \equiv 1 \pmod 4 \text{ oder } p = 2 \\ -1 & \text{, falls } p \equiv 3 \pmod 4 \end{cases}.$$

2. 2 *ist genau dann quadratischer Rest modulo p, wenn* $p \equiv \pm 1 \pmod 8$, *mit anderen Worten*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{, falls } p \equiv \pm 1 \pmod 8 \\ -1 & \text{, falls } p \equiv \pm 3 \pmod 8 \end{cases}$$

Der folgende Satz ist das Quadratische Reziprozitätsgesetz, das CARL FRIEDRICH GAUSS (1777-1855) zuerst im Jahre 1801 bewies.

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

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

1.3 Quadratische Zahlkörper

Wie in der Einleitung bereits angedeutet, werden einige Betrachtungen in $\mathbb{Q}(\sqrt{3})$ ablaufen und einige Resultate über quadratische Zahlköper benutzt.

Definition 1.7.

1. *Sei $m \in \mathbb{Z}$ quadratfrei, d.h. jeder Primfaktor von m kommt nur in der ersten Potenz vor. Dann verstehen wir unter $\mathbb{Q}(\sqrt{m}) \subset \mathbb{C}$ den bezüglich Inklusion kleinsten Zerfällungskörper des Polynoms $f(x) = x^2 - m$ in $\mathbb{Q}[x]$.*

2. *Ist $m \geq 0$ heißt $\mathbb{Q}(\sqrt{m})$ ein **reell-quadratischer Zahlkörper**. Anderenfalls heißt $\mathbb{Q}(\sqrt{m})$ **imaginär-quadratischer Zahlkörper**, wobei in diesem Fall der Ausdruck $\sqrt{m}$ als $i\sqrt{-m}$ zu verstehen ist.*

3. *Unter dem **Ganzheitsring** $\mathcal{O}_K$ des Körpers $K := \mathbb{Q}(\sqrt{m})$ verstehen wir alle Elemente von K mit einem Minimalpoynom aus $\mathbb{Z}[X]$,*

$$\mathcal{O}_K := \{\alpha \in K \mid \mu_\alpha(X) \in \mathbb{Z}[X]\},$$

wobei μ_α das Minimalpolynom von α bezeichnet.

4. *Die Abbildung*

$$^{-}\colon \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}(\sqrt{m}),\ \alpha = a + \sqrt{m}b \mapsto \overline{\alpha} := a - \sqrt{m}b$$

*ist der einzige nicht-triviale Körperautomorphismus von $\mathbb{Q}(\sqrt{m})$. $\overline{\alpha}$ heißt das zu α **konjugierte** Element.*

5. *Für $\alpha \in \mathbb{Q}(\sqrt{m})$ heißt*

$$\mathrm{Spur}(\alpha) = \alpha + \overline{\alpha} \in \mathbb{Q}$$

*die **Spur** von α,*

$$\nu(\alpha) = \alpha \cdot \overline{\alpha} \in \mathbb{Q}$$

*die **Norm** von α.*

6. *Unter $\mathbb{Z}[\sqrt{m}]$ verstehen wir den Teilring von $\mathbb{Q}(\sqrt{m})$, mit*

$$\mathbb{Z}[\sqrt{m}] := \{\alpha = a + \sqrt{m}b \in \mathbb{Q}(\sqrt{m}) \mid a, b \in \mathbb{Z}\}.$$

Bemerkung 1.8.

1. *ν ist multiplikativ, also $\nu(\alpha \cdot \beta) = \nu(\alpha) \cdot \nu(\beta)$, denn $^{-}$ ist ein Körperautomorphismus.*

2. *Man beachte, dass $\mathbb{Z}[\sqrt{m}]$ im allgemeinen KEIN faktorieller Ring ist, insbesondere kann es irreduzible Elemente in $\mathbb{Z}[\sqrt{m}]$ geben, die nicht prim sind. Ein Beispiel dafür ist $\mathbb{Z}[\sqrt{-5}]$, wo sich $6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$ auf zwei verschiedene Weisen in irreduzible Faktoren zerlegen lässt, die aber nicht assoziiert sind. Damit sind diese Faktoren nicht prim.*

Es soll hier nicht das Ziel sein, die Theorie quadratischer Zahlkörper vollständig zu behandeln, daher begnügen wir uns mit einem Lemma, das später noch benötigt wird, und dem DIRICHLETschen Einheitensatz.

Lemma 1.9.
Sei $p \in \mathbb{P}$ und $m \in \mathbb{Z}$ quadratfrei mit $\left(\frac{m}{p}\right) = -1$. Dann ist p auch prim in $\mathbb{Z}[\sqrt{m}]$.

Beweis. p ist genau dann prim in $\mathbb{Z}[\sqrt{m}]$, wenn $p\mathbb{Z}[\sqrt{m}] \subseteq \mathbb{Z}[\sqrt{m}]$ ein Primideal ist, also wenn $\mathbb{Z}[\sqrt{m}]/p\mathbb{Z}[\sqrt{m}]$ ein Integritätsbereich ist. Zunächst ist klar, dass $\mathbb{Z}[\sqrt{m}] \cong \mathbb{Z}[x]/\langle x^2 - m\rangle$ und damit gilt

$$\mathbb{Z}[\sqrt{m}]/p\mathbb{Z}[\sqrt{m}] \cong \mathbb{Z}[x]/\langle p, x^2 - m\rangle \cong \mathbb{F}_p[x]/\langle x^2 - m\rangle \cong \mathbb{F}_{p^2}.$$

Zur letzten Isomorphie ist zu sagen, dass m nach Voraussetzung ein quadratischer Nichtrest modulo p ist und $x^2 - m$ daher irreduzibel in $\mathbb{F}_p[x]$ ist. Damit ist $p\mathbb{Z}[\sqrt{m}]$ ein maximales Ideal in $\mathbb{Z}[\sqrt{m}]$, also insbesondere ein Primideal.

□

Bemerkung 1.10.
Allgemein gibt es 3 Möglichkeiten, wie sich eine Primzahl p aus $\mathbb{Z}$ in $\mathcal{O}_{Q(\sqrt{m})}$ verhalten kann. Dazu betrachtet man das Verhalten des von p erzeugten Ideals in $\mathcal{O}_{Q(\sqrt{m})}$ in Bezug auf Zerlegbarkeit,

$$\langle p\rangle_{\mathcal{O}_{Q(\sqrt{m})}} = \begin{cases} \langle p\rangle_{\mathcal{O}_{Q(\sqrt{m})}} \\ \mathfrak{p}\mathfrak{p}' \\ \mathfrak{p}^2 \end{cases},$$

*wobei $\mathfrak{p}, \mathfrak{p}' \trianglelefteq \mathcal{O}_{Q(\sqrt{m})}$, $\mathfrak{p} \neq \mathfrak{p}'$ Primideale sind. Im ersten Fall heißt $\langle p\rangle_{\mathcal{O}_{Q(\sqrt{m})}}$ **träge**, im zweiten Fall **zerlegt** und im dritten Fall heißt $\langle p\rangle_{\mathcal{O}_{Q(\sqrt{m})}}$ **verzweigt**.*

Der folgende Satz stammt von PETER GUSTAV LEJEUNE DIRICHLET (1805-1859).

Satz 1.11. DIRICHLET***scher Einheitensatz***
Sei K ein algebraischer Zahlkörper, also eine endliche Körpererweiterung von $\mathbb{Q}$. Dann gilt für die Einheitengruppe des Ganzheitsrings von K

$$\mathcal{O}_K^* \cong \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{r+s-1} \times (\mathbb{Z}/e\mathbb{Z}),$$

wobei r die Anzahl der Einbettungen von K in $\mathbb{R}$ und s die Anzahl der Paare von Einbettungen von K in $\mathbb{C}$, deren Bild nicht in $\mathbb{R}$ liegt, ist. Man zählt deswegen

hier Paare, weil man durch Komposition mit dem Konjugationsautomorphismus sofort eine weitere Einbettung findet. e bezeichnet die Anzahl der Einheitswurzeln in K, also komplexe Nullstellen von Polynomen der Form $c(X) = X^n - 1$.

Lemma 1.12. *Für einen quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{m})$ gilt die Beziehung*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{, falls } m \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{m}] & \text{sonst} \end{cases}$$

Beweis. vgl. [Kr], Satz (2.7).

□

Bemerkung 1.13. *Ist K ein reell-quadratischer Zahlkörper, so ist der freie Anteil von $\mathcal{O}_K^* \cong \mathbb{Z}$, also insbesondere zyklisch. Ein Erzeuger dieses freien Anteils heißt* ***Fundamentaleinheit****.*

2 Elliptische Kurven

2.1 Geometrie elliptischer Kurven

Ein Ziel dieses Vortrags wird es sein, die gegebenen Beweise für den Lucas-Lehmer-Test und das von Gross vorgeschlagenen Test auch im Lichte der algebraischen Geometrie zu betrachten. Dazu seien hier die nötigen Resultate vorgestellt, wobei ich aufgrund zu großen Umfanges zum größten Teil auf die Herleitungen und Beweise verzichte. Diese sind u.a. in [Wer] oder in [Si] angegeben.

Definition 2.1.
Es sei K ein Körper, $\overline{K}$ der algebraische Abschluss von K und $\mathcal{P}_2(K)$ den 2-dimensionalen projektiven Raum über K.

1. *Es sei $f \in K[X,Y,Z]_{hom}$ ein homogenes Polynom. Dann definiert f eine **projektive ebene Kurve**, die mit C_f bezeichnet wird.*
   Zu einem Erweiterungskörper L von K bezeichnet

$$C_f(L) = \{[a:b:c] \in \mathcal{P}_2(L) \mid f(a,b,c) = 0\}$$

   *die Menge der L-**rationalen Punkte** von C_f.*

2. *Eine projektive ebene Kurve C_f heißt **singulär** im Punkt $P = [a:b:c] \in C_f(L)$, falls alle partiellen Ableitungen von f in P verschwinden, also*

$$\frac{\partial f}{\partial X}(a,b,c) = \frac{\partial f}{\partial Y}(a,b,c) = \frac{\partial f}{\partial Z}(a,b,c) = 0.$$

3. *C_f heißt **nicht-singulär**, wenn C_f in keinem Punkt von $\overline{K}$ singulär ist.*

Definition 2.2.

1. *Eine **elliptische Kurve** über einem Körper K ist eine nicht-singuläre projektive Kurve C_f mit*

$$f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3, \quad a_i \in K.$$

   Die Gleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4xZ^2 + a_6Z^3$$

   *nennt man auch die Weierstrass-**Gleichung** der elliptischen Kurve, f nennt man auch das Weierstrass-**Polynom** der elliptischen Kurve.*

2. *Unter der **Diskriminante** einer elliptischen Kurve versteht man den Ausdruck*

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

wobei die Koeffizienten b_j gegeben sind durch

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6 \text{ und} \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Die a_i sind hierbei die Koeffizienten von f wie in 1.

3. *Sei K ein Zahlkörper und $\mathfrak{P}$ ein Primideal von K. Dann bezeichnet $\hat{E}_f$ die* ***Reduktion*** *der elliptischen Kurve E_f modulo $\mathfrak{P}$, indem man f die Koeffizienten von f modulo $\mathfrak{P}$ auffasst. Man sagt, E_f habe* ***gute Reduktion*** *modulo $\mathfrak{P}$, falls $\hat{E}_f$ wieder eine elliptische Kurve ist, also nicht-singulär ist.*

Bemerkung 2.3.

1. *Die eigentümliche Nummerierung der a_i hat historische Gründe und ist in dieser Form allgemein üblich.*
2. *Ab sofort bezeichne E_f die elliptische Kurve zum* Weierstrass*-Polynom f über dem Körper K.*

Nun definiert nicht jedes f wie in 1.10 1) eine elliptische Kurve. Einen einfachen Test auf Singularität von C_f liefert das folgende

Lemma 2.4.
Es sei $f \in K[X, Y, Z]$ ein Weierstrass*-Polynom. Dann ist C_f genau dann nicht-singulär, wenn die Diskriminante Δ von C_f nicht verschwindet.*

Beweis. Siehe [Wer], S.28, Proposition 2.3.3.

□

Bemerkung 2.5.
Fasst man den affinen Raum $\mathcal{A}_2(K)$ eingebettet in den projektiven Raum auf vermöge

$$\iota : \mathcal{A}_2(K) \to \mathcal{P}_2(K), P = (x, y) \mapsto [x : y : 1],$$

so lässt sich leicht nachrechnen, dass der einzige Punkt einer jeder elliptischen Kurve, der nicht in $\iota(\mathcal{A}_2(K))$ liegt, der unendlich ferne Punkt $\mathcal{O} = [0 : 1 : 0]$ ist. Daher kann man statt der angegebenen Weierstrass*-Gleichung auch die* ***affine*** Weierstrass***-Gleichung***

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

betrachten und $E_f(K)$ als affine Nullstellenmenge des Weierstrass*-Polynoms vereinigt mit $\mathcal{O}$ auffassen:*

$$E_f(K) = Null_a(f) \cup \{\mathcal{O}\} = \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

2.2 Elliptische Kurven als abelsche Gruppen

Bis hierher haben wir elliptische Kurven nur als rein geometrische Objekte betrachtet. Man kann nun, und das ist für die kommenden Betrachtungen essentiell, auf $E_f(K)$ die Struktur einer ABELschen Gruppe erklären:

Satz 2.6.
Es sei K ein Körper $E_f(K)$ eine elliptische Kurve mit WEIERSTRASS*-Polynom $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \in K[x,y]$. Es seien $P_1, P_2 \in E_f(K) \setminus \{\mathcal{O}\}$, mit $P_i = (x_i, y_i)$. $E_f(K)$ wird zu einer* ABEL*schen Gruppe mit Verknüpfung + und neutralem Element $\mathcal{O}$ durch*

$$\begin{aligned} -P &= (x, -y - a_1x - a_3) \\ x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3 \end{aligned}$$

mit $P_1 + P_2 := (x_3, y_3)$ *und*

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{falls } x_1 \neq x_2 \\ \frac{3x_1^2 + 2a_2x_+ a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{falls } x_1 = x_2 \end{cases}$$

$$\nu = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{falls } x_1 \neq x_2 \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{falls } x_1 = x_2 \end{cases}$$

Bemerkung 2.7.
Oft wird die WEIERSTRASS*Gleichung in reduzierter Form angegeben, nämlich*

$$f(x,y) = y^2 - x^3 - ax - b.$$

Dann gilt für die Gruppenstruktur auf $E_f(K)$

1. *Für $P = (x,y) \in E_f(K)$ ist*

$$-P := (x, -y)$$

2. *Es ist $P_1 + P_2 = P_3 = (x_3, y_3)$ mit*

$$x_3 = \begin{cases} \lambda^2 - x_1 - x_2 & \text{, falls } P_2 \neq \pm P_1 \\ \lambda^2 - 2x_1 & \text{, falls } P_2 = P_1 \text{ und } y_1 \neq 0 \end{cases}, \quad y_3 = \lambda(x_1 - x_3) - y_1,$$

wobei

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & \text{, falls } P_2 \neq \pm P_1 \\ \frac{3x_1^3 + a}{2y_1} & \text{, falls } P_2 = P_1 \text{ und } y_1 \neq 0 \end{cases}.$$

Für $P = (x,0)$ ist $P + P = \mathcal{O}$.

Bemerkung 2.8.
Es sei $K = \mathbb{R}$. Dann kann man sich die Addition auf $E(\mathbb{R})$ geometrisch wie folgt verstehen:
Seien P und Q Punkte von $E(\mathbb{R})$. Ist $Q \neq \pm P$ so erhält man $P+Q$, indem man den Schnittpunkt der Gerade durch P und Q mit $E(\mathbb{R})$ bestimmt und diesen an der x-Achse spiegelt (vgl. Abbildung 1). Für $P = Q$ tut man dasselbe mit der Tangente an $E(\mathbb{R})$ in P. Dies bezeichnet man auch als Quadrieren von P (vgl. Abbildung 2). Ist $P = -Q$, so erhält man als Gerade eine Parallele zur y-Achse, deren Schnittpunkt mit $E(\mathbb{R})$ man dann als den unendlich fernen Punkt $\mathcal{O}$ interpretiert.

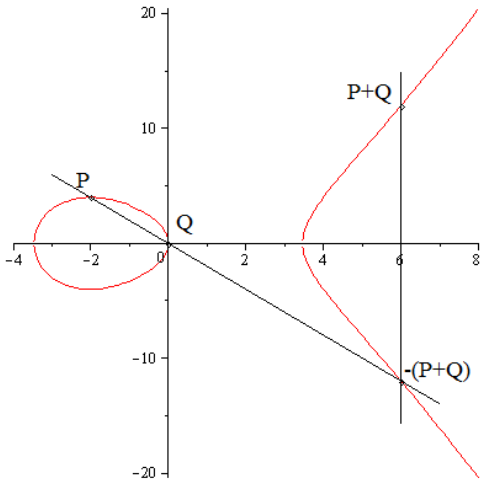

Abbildung 1: Addition zweier verschiedener Punkte auf einer elliptischen Kurve

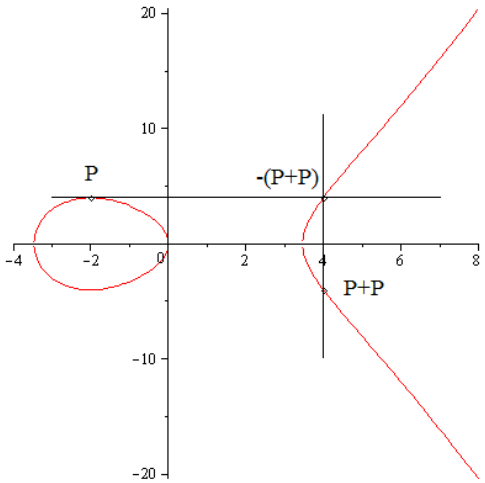

Abbildung 2: Quadrieren eines Punktes auf einer elliptischen Kurve

2.3 Supersingularität und Kombinatorik

Lemma 2.9.
Sei K ein Körper der Charakteristik $p \in \mathbb{P}$ und E_f eine elliptische Kurve über K. Dann gilt: Die Abbildung

$$\Phi : \mathcal{P}_2(\overline{K}) \to \mathcal{P}_2(\overline{K}),\ [x : y : z] \mapsto [x^p : y^p : z^p]$$

definiert einen Gruppenhomomorphismus

$$\Phi : E_f(\overline{K}) \to E_f(\overline{K}).$$

Φ *heißt der* FROBENIUS-***Endomorphismus*** *(nach* FERDINAND GEORG FROBENIUS*, 1849-1917).*

Beweis. Das Φ eine Abbildung von $\mathcal{P}_2(\overline{K})$ in sich selbst ist, ist offensichtlich. Wir zeigen die Wohldefiniertheit der Einschränkung auf $E(\overline{K})$:
Sei $P = [x : y : z] \in E_f(\overline{K})$ und das WEIERSTRASS-Polynom f von $E_f(\overline{K})$ sei

$$f(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4xZ^2 - a_6Z^3, quada_i \in K.$$

In $\overline{K}$ ist nun bekanntermaßen $(\alpha + c\beta)^p = \alpha^p + c\beta^p$ für $\alpha, \beta \in \overline{K}$, $c \in K$. Dann folgt aber, da $f(P) = f(x, y, z) = 0$ gilt:

$$\begin{aligned} 0 = f(P)^p &= f(x, y, z)^p = (y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3)^p \\ &= (y^p)^2z^p + a_1x^py^pz^p + a_3y^p(z^p)^2 - (x^p)^3 - a_2(x^p)^2z^p - a_4x^p(z^p)^2 - a_6(z^p)^3 \\ &= f(x^p, y^p, z^p) = f(\Phi(P)) \end{aligned}$$

Damit ist also $\Phi(P) \in E_f(\overline{K})$, demnach ist die Einschränkung wohldefiniert. Es bleibt noch zu zeigen, dass Φ die Gruppenstruktur respektiert: Seien $P_1, P_2 \in E_f(\overline{K})$ mit $P_i = [x_i, y_i, z_i]$, bzw. in affinen Koordinaten $P_i = (x_i, y_i)$. Es reicht, diese Punkte zu betrachten, denn der einzige Punkt ohne eine affine Koordinatendarstellung in $E_f(\overline{K})$ ist $\mathcal{O}$ und offenbar ist $\Phi(\mathcal{O}) = \mathcal{O}$ und damit $\Phi(P_1 + \mathcal{O}) = \Phi(P_1) = \Phi(P_1) + \mathcal{O} = \Phi(P_1) + \Phi(\mathcal{O})$.
Sei also $P_1 + P_2 \neq \mathcal{O}$. Dann gilt $P_1 + P_2 = (x_3, y_3)$ mit

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3 \end{aligned}$$

für gewisse $\lambda, \nu \in \overline{K}$. Dann ist aber mit den gleichen Überlegungen wie oben

$$\Phi(P_1 + P_2) = ((\lambda^p)^2 + a_1\lambda^p - a_2 - x_1^p - x_2^p, -(\lambda^p + a_1)x_3^p - \nu^p - a_3).$$

Ebenso rechnet man nach, dass λ^p und ν^p genau die Konstanten aus Bemerkung (1.15) für die Summe der Punkte $\Phi(P_i) = (x_i^p, y_i^p)$ sind. Damit gilt also

$$\Phi(P_1 + P_2) = \Phi(P_1) + \Phi(P_2).$$

Den Fall $P_1 + P_2 = \mathcal{O}$ behandelt man vollkommen analog. Damit ist also Φ tatsächlich ein Gruppenhomomorphismus.

□

Definition 2.10.
Es sei $K = \mathbb{F}_q$ ein endlicher Körper der Charakteristik p und E_f eine elliptische Kurve über K.

1. *Der Ausdruck*
$$\mathrm{Spur}(\Phi) = q + 1 - |E_f(K)|$$
*heißt die **Spur** des* Frobenius*-Endomorphismus.*

2. *E_f heißt **supersingulär** genau dann, wenn p die Spur des* Frobenius*-Endomorphismus teilt,*
$$p \,|\, \mathrm{Spur}(\Phi).$$
Anderenfalls heißt E_f gewöhnlich.

Bemerkung 2.11. *Der Begriff „supersingulär“ hat nichts mit „singulär“ zu tun. Eine elliptische Kurve ist per Definition nicht singulär, kann aber sehr wohl supersingulär sein.*

Der folgende wichtige Satz wurde von Helmut Hasse (1898-1979) im Jahre 1931 bewiesen.

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

Beweis. Der Beweis erfordert einiges mehr an Theorie über elliptische Kurven als hier bereitgestellt werden kann, daher sei hier der Beweis aus [Si], Theorem V.1.1 und Lemma V.1.2 zitiert.

□

2.4 Isogenien und komplexe Multiplikation

Da elliptische Kurven als abelsche Gruppen einen ausgezeichneten Punkt $\mathcal{O}$ besitzen, scheint es sinnvoll, Abbildungen zwischen elliptischen Kurven zu studieren, die diesen Punkt fest lassen:

Definition 2.13.
Es seien $E_1 = E_f$ und $E_2 = E_g$ elliptische Kurven über einem Körper K.

1. *Eine Abbildung*
$$\phi : E_1 \to E_2$$
heißt ***rational****, falls ϕ eine Äquivalenzklasse $R = (R_1, R_2, R_3) \in \overline{K}[X, Y, Z]^3$ von homogenen Polynomen gleichen Grades ist, die nicht alle durch f teilbar sind, und $g((R_1, R_2, R_3))$ durch f teilbar ist. R und S heißen hierbei äquivalent, falls stets*
$$f \mid (R_i S_j - R_j S_i) \quad \forall\, i, j$$
gilt.

2. *Eine rationale Abbildung*
$$\phi : E_1 \to E_2$$
heißt ***definiert*** *im Punkt $P \in E_1(\overline{K})$, falls es einen Vertreter (R_1, R_2, R_3) und ein $i \in \{1, 2, 3\}$ gibt mit $R_i(P) \neq 0$. Ist dies für jeden Punkt von $E_1(\overline{K})$ der Fall, so ist ϕ ein* ***Morphismus****.*

3. *Ein Morphismus*
$$\phi : E_1 \to E_2$$
mit $\phi(\mathcal{O}) = \mathcal{O}$ heißt ***Isogenie****. Die Kurven E_1 und E_2 heißen* ***isogen****, falls es eine nicht-triviale Isogenie $\phi : E_1 \to E_2$ gibt, d.h. $\phi(E_1) \neq \{\mathcal{O}\}$.*

4. *Unter* $\mathrm{Hom}(E_1, E_2)$ *verstehen wir die Menge aller Isogenien $\phi : E_1 \to E_2$,*
$$\mathrm{Hom}(E_1, E_2) = \{\phi : E_1 \to E_2 \mid \phi(\mathcal{O}) = \mathcal{O}\}.$$
Ist $E_1 = E_2$, so ist
$$\mathrm{End}(E_1) = \mathrm{Hom}(E_1, E_1)$$
der ***Endomorphismenring*** *von E_1.*

Bemerkung 2.14.

1. $\mathrm{Hom}(E_1, E_2)$ *ist eine Gruppe mit der Addition als Verknüpfung. Für $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ gilt*
$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

2. $\mathrm{End}(E_1)$ *ist bildet einen Ring mit der Addition und der Komposition von Abbildungen als Multiplikation,*
$$(\phi \cdot \psi)(P) = \phi(\psi(P)).$$

Beispiel 2.15.

1. *Für $m \in \mathbb{Z}$ definiert die Multiplikation mit m auf kanonische Weise eine Isogenie auf einer elliptischen Kurve E:*
$$[m] : E \to E, P \mapsto mP := \begin{cases} \underbrace{P + \ldots + P}_{m \text{ Stück}} & \text{, falls } m > 0 \\ -m(-P) & \text{, falls } m < 0 \end{cases}.$$
Diese Abbildung ist offenbar für jeden Punkt $P \in E$ wohldefiniert , da E als ABEL*sche 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. Umgekehrt ist auch jede Isogenie ein Gruppenhomomorphismus (vgl. [Si], Theorem V.4.8).*

Bemerkung 2.16.

1. $\mathrm{End}(E)$ *ein Integritätsbereich der Charakteristik 0. Genauer gilt stets*

$$\mathrm{End}(E) \text{ ist } \begin{cases} \text{isomorph zu } \mathbb{Z} \\ \text{eine Ordnung in } \mathbb{Q}(\sqrt{d}) \text{ mit } d < 0 \\ \text{eine Ordnung in Quaternionenalgebra } \left(\frac{a,b}{\mathbb{Q}}\right), \text{ wo } a, b < 0 \end{cases}.$$

Unter der Quaternionenalgebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ *versteht man den 4-dimensionalen* $\mathbb{Q}$*-Vektorraum mit Basis* $\{1, i, j, k\}$ *mit den Multiplikationsregeln*

$$i^2 = a, \quad j^2 = b, \quad k = i \cdot j \text{ und } j \cdot i = -k.$$

Eine ***Ordnung*** *in* $\mathbb{Q}(\sqrt{d})$ *bzw.* $\left(\frac{a,b}{\mathbb{Q}}\right)$ *ist dabei ein endlich erzeugter freier* $\mathbb{Z}$*-Modul vom Rang* 2 *respektive* 4*, der zugleich eine Ringstruktur trägt.*

2. *Meistens sind für einen Körper der Charakteristik 0 alle Isogenien einer elliptischen Kurve* E *auf eine Multiplikation mit* $m \in \mathbb{Z}$ *zurückzuführen, das heißt*

$$\mathrm{End}(E) \cong \mathbb{Z}.$$

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.*

Satz 2.17.
Es sei E *eine elliptische Kurve über einem Körper* K *der Charakteristik* q*. Dann ist* E *genau dann supersingulär, wenn* $\mathrm{End}(E)$ *isomorph zu einer Ordnung in* $\left(\frac{a,b}{\mathbb{Q}}\right)$ *ist.*

Beweis*.* siehe [Si], Theorem V.3.1

□

Der folgende Satz (vgl. [Si2], S.184) gibt eine weitere Methode an, in einer bestimmten Situation eine elliptische Kurve auf Supersingularität zu testen. Der Beweis erfordert allerdings ebenfalls deutlich mehr Theorie als hier zur Verfügung steht.

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:

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

Im Beweis zu Satz 4.4 wird die Weil-Paarung verwendet. Zur Erläuterung dessen dient der folgende

Satz 2.19.
Es sei K ein Körper der Charakteristik p und $m \in \mathbb{N}$ mit $\mathrm{ggT}(m,p) = 1$. Dann existiert eine Abbildung

$$e_m : \mathrm{Kern}([m]) \times \mathrm{Kern}([m]) \to \mu_m,$$

wobei μ_m die Gruppe der m-ten Einheitswurzeln in $\overline{K}$ bezeichnet, mit den Eigenschaften

1. *e_m ist bilinear,*

   $$e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T) \text{ und } e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2).$$

2. *e_m ist alternierend: $e_m(T,T) = 1$*

3. *e_m ist nicht ausgeartet, das heißt, falls $e_m(S,T) = 1$ für alle $T \in \mathrm{Kern}([m])$, so ist $S = \mathcal{O}$. Damit ist e_m surjektiv.*

4. *e_m ist mit der Operation der Galois-Gruppe*

   $$\mathrm{Gal}_{\overline{K}/K} := \{\varphi \in \mathrm{Aut}(\overline{K} \mid \varphi(k) = k \quad \forall k \in K\} \leq \mathrm{Aut}(\overline{K}) :$$

   Für $\sigma \in \mathrm{Gal}_{\overline{K}/K}$ ist

   $$e_m(\sigma(S),\sigma(T)) = \sigma(e_m(S,T)).$$

e_m nennt man die Weil-***Paarung***.

Beweis. siehe [Si], Theorem III.8.1.

□

Bemerkung 2.20. *e_m wird normalerweise mit noch 2 weiteren Eigenschaften erklärt, für die die nötigen Begriffe hier nicht erklärt wurden.*

Eine für den späteren Beweis wichtige Isogenie ist die Multiplikation mit 2, die man auch als Quadrieren eines Punktes bezeichnet. Der folgende Satz beschreibt das Bild dieser Isogenie (vgl. [Hus], Theorem (4.1)).

Satz 2.21. *Es sei $E_f(K)$ 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.

Beweis. Die Gleichung $2 \cdot (x, y) = (x', y')$ ist genau dann lösbar in $E_f(K)$, wenn $2 \cdot (x, y) = (0, y')$ in $E_g(K)$ lösbar ist, mit

$$g(x,y) = y^2 - (x + x' - \alpha)(x + x' - \beta)(x + x' - \gamma).$$

Es reicht daher zu zeigen, dass die Existenz von $Q = (x, y)$ mit $2 \cdot Q = (0, y')$ zu der Tatsache äquivalent ist, dass $-\alpha$, $-\beta$ und $-\gamma$ Quadrate in K sind.
Es gilt nun für die Tangente $y = \lambda x + \delta$ an $E_f(K)$ in Q eingesetzt in f

$$\begin{aligned}
&(\lambda x + \delta)^2 = x^3 + ax^2 + bx + c \\
\Leftrightarrow &0 = x^3 + (a - \lambda)x^2 + (b - 2\lambda\delta) + c - \underbrace{\delta^2}_{=y'^2=c} \\
\Leftrightarrow &0 = x(x^2 + (a - \lambda^2)x + (b - 2\lambda\delta)) \qquad (+)
\end{aligned}$$

Da wir die Tangente an f betrachten, muss der quadratische Faktor $x^2 + (a - \lambda^2)x + (b - 2\lambda\delta)$ Diskriminante 0 haben, da Q eine doppelte Nullstelle liefern muss. Daher gilt

$$\begin{aligned}
&(\lambda^2 - a)^2 = 4(b - 2\lambda y') \\
\Leftrightarrow\ &(\lambda^2 - a + u)^2 = 2u\lambda^2 - 2au + u^2 + 4(b - 2\lambda y') \\
&\qquad\qquad = 2u\lambda^2 - 8\lambda y' + (u^2 + 4b - 2ua) \quad (*)
\end{aligned}$$

Die rechte Seite muss nun ebenfalls die Diskriminante 0 haben, da auf der linken Seite ein vollständiges Quadrat steht, also

$$\begin{aligned}
&0 = 8^2 y'^2 - 4 \cdot 2u(u^2 + 4b - 2ua) \\
\Leftrightarrow &0 = u^3 - 2au^2 + 4bu - 8c \qquad \text{Substituiere } u = -2v \\
\Leftrightarrow &0 = -8(v^3 + av^2 + bv + c) \\
\Leftrightarrow &v \in \{\alpha, \beta, \gamma\} \\
\Leftrightarrow &u \in \{-2\alpha, -2\beta, -2\gamma\}
\end{aligned}$$

Ersetzt man nun in $(*)$ $u = 2\alpha$ und verwendet die Beziehungen

$$-a = \alpha + \beta + \gamma, \qquad b = \alpha\beta + \alpha\gamma + \beta\gamma, \qquad c = -\alpha\beta\gamma$$

so erhält man für λ folgendes:

$$\begin{aligned}&(\lambda^2+\alpha+\beta+\gamma-2\alpha)^2=\\&-4\alpha\lambda^2-8\lambda y'+(4\alpha^2+4[\alpha\beta+\alpha\gamma+\beta\gamma]-4\alpha[\alpha+\beta+\gamma])\\\Leftrightarrow&(\lambda^2-\alpha+\beta+\gamma)^2=4(\alpha'\lambda-\beta'\gamma')^2,\end{aligned}$$

wobei $\alpha'^2=-\alpha$, $\beta'^2=-\beta$ und $\gamma'^2=-\gamma$, die es zunächst in einem geeigneten Erweiterungskörper von K gibt.
Zieht man nun die Quadratwurzel aus der letzten Gleichung, so erhält man schließlich

$$\begin{aligned}&\lambda^2-\alpha+\beta+\gamma)=\pm2(\alpha'\lambda-\beta'\gamma')\\\Leftrightarrow&\lambda^2\mp2\alpha'\lambda-\alpha=-\beta\mp2\beta'\gamma'-\gamma\\\Leftrightarrow&(\lambda\mp\alpha')^2=(\beta'\mp\gamma')^2\end{aligned}$$

Da auf beiden Seiten der Gleichung Quadrate stehen, ist damit die Existenz von λ in K äquivalent ist zu der Existenz von α', β' und γ' in K. Durch Einsetzen in die Gleichung $(+)$ verifiziert man, dass der Punkt Q für

$$x=\frac{1}{2}(\lambda^2+\alpha+\beta+\gamma),\qquad y=\lambda x+y'$$

die Bedingungen erfüllt.
Damit ist der Beweis vollständig.

□

3 Lucas-Lehmer Test für Mersenne-Zahlen

Wir kommen nun zum eigentlichen Thema des Vortrages, nämlich Primzahltests für MERSENNE-Zahlen. Dazu wird zunächst der Test, den ÉDOUARD LUCAS (1842-1891) 1876 erfunden hat und der von DERRICK HENRY LEHMER (1905-1991) 1935 verbessert wurde, noch einmal neu interpretiert und bewiesen, nämlich als sukzessives Quadrieren eines Punktes des eindimensionalen algebraischen Torus über $\mathbb{Q}$ zu $\mathbb{Q}(\sqrt{3})$. Dazu betrachten wir den reell-quadratischen Zahlkörper $K := \mathbb{Q}(\sqrt{3})$ bzw. den Teilring $R := \mathbb{Z}[\sqrt{3}]$. Für $q \in \mathbb{P}$ betrachten wir

$$T(q) := \{\alpha \in R \mid \nu(\alpha) \equiv 1 \pmod{q}\}$$

als Untergruppe von $(R/qR)^*$. Nach dem Einheitensatz von DIRICHLET (Satz 1.11) und Bemerkung 1.12 ist R der Ganzheitsring von K und daher isomorph zu $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle\varepsilon\rangle \times \langle -1\rangle$. Die Fundamentaleinheit

$$\varepsilon = 2 + \sqrt{3}$$

hat hier Norm 1. Wir werden später sehen, dass ε unter gewissen Voraussetzungen auch ein Erzeuger von $T(q)$ ist.

Proposition 3.1.
Sei $q \in \mathbb{P}$ 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 $T(q)$.

Beweis. Da $q \equiv 7 \pmod{24}$, gilt insbesondere auch $q \equiv 3 \pmod{4}$ und $q \equiv 1 \pmod{3}$, also gilt mit dem quadratischen Reziprozitätsgesetz

$$\left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right) \overset{vgl.(1.2)}{=} -\left(\frac{1}{3}\right) = -1,$$

so dass 3 ein quadratischer Nichtrest modulo q ist. Damit ist aber nach Lemma(1.8) q auch ein Primelement in $R = \mathbb{Z}[\sqrt{3}]$. Das macht nun R/qR zu einem Körper mit q^2 Elementen, also ist $(R/qR)^* \cong C_{q^2-1}$.
Sei nun

$$\nu_q : G := (R/qR)^* \to H := (\mathbb{Z}/q\mathbb{Z})^*,\ \alpha + qR \mapsto \nu(\alpha) \pmod{q}.$$

Wegen der Multiplikativität von ν ist ν_q offenbar ein wohldefinierter Gruppenhomomorphismus, denn ν_q ist offensichtlich verteterunabhängig.
Behauptung: ν_q ist sogar ein Epimorphismus.
Denn es gilt einerseits ganz allgemein, dass $\bar{}$ auf $\mathbb{Z}[\sqrt{m}]$ einen nicht-trivialen Ringautomorphismus induziert, das heißt, dass für $p \in \mathbb{P}$ mit $\left(\frac{m}{p}\right) = -1$ auch einen nicht-trivialen Ringautomorphismus auf $\mathbb{Z}[\sqrt{m}]/p\mathbb{Z}[\sqrt{m}]$ definiert, indem man einfach die Restklassen modulo p betrachtet. Hier ist $\bar{}$ sogar ein Körperautomorphismus von $\mathbb{F}_{p^2}$, denn $\mathbb{Z}[\sqrt{m}]/p\mathbb{Z}[\sqrt{m}] \cong \mathbb{F}_p[x]/(x^2 - m) \cong \mathbb{F}_{p^2}$. Der einzige nichttriviale Körperautomorphismus auf $\mathbb{F}_{p^2}$ ist aber der FROBENIUS-Automorphismus $x \mapsto x^p$. Damit muss also stets $\overline{\alpha} = \alpha^p$ für $\alpha \in \mathbb{Z}[\sqrt{m}]/p\mathbb{Z}[\sqrt{m}]$ gelten. Damit gilt dann

$$\nu_p(\alpha) = \alpha^{p+1}.$$

Sei nun α ein Erzeuger von $\mathbb{F}_{p^2}^*$. Dann sei

$$n := \nu_p(\alpha) = \alpha^{p+1} \in \mathbb{F}_p$$

und k die Ordnung von n in $\mathbb{F}_p^*$. Da die Ordnung von α nun $p^2 - 1$ ist und $n = \alpha^{p+1}$, ist also $k = p - 1$, was aber die Ordnung von $\mathbb{F}_p^*$ ist. Damit ist n ein Erzeuger von $\mathbb{F}_p^*$ und ν_p ist surjektiv.
Nun ist $\text{Kern}(\nu_q) = T(q)$, also ist nach dem Homomorphiesatz $G/T(q) \cong H$, also gilt insbesondere

$$|T(q)| = \frac{|G|}{|H|} = q + 1$$

und $T(q)$ ist als Untergruppe einer zyklischen Gruppe ebenfalls zyklisch.
Nun zu ε: Nach HILBERTs Satz 90 (benannt nach DAVID HILBERT (1862-1943)) kann ε als Element von K aufgefasst wie folgt als Quotient dargestellt werden,

$$\varepsilon = \beta/\overline{\beta} \qquad \text{mit } \beta := 3 + \sqrt{3},$$

und wegen $\beta\overline{\beta} = 6$ haben wir also

$$\varepsilon = \beta^2/6.$$

Damit gilt nun (alle Äquivalenzen verstehen sich modulo q).

$$\begin{aligned}
\varepsilon^{\frac{q+1}{2}} &= \frac{\beta^{q+1}}{6^{\frac{q+1}{2}}} \\
&\equiv \frac{6}{6^{\frac{q+1}{2}}} \\
&\equiv \left(6^{-1}\right)^{\frac{q-1}{2}} \\
&\equiv \left(\frac{6}{q}\right) \qquad \text{vgl. Bemerkung (1.4)} \\
&= -1
\end{aligned}$$

Damit ist also ε kein Quadrat in $T(q)$ und die Behauptung ist gezeigt.

□

Bemerkung 3.2.
Unter den Voraussetzungen von Proposition 2.1 gilt: ε ist ein Erzeuger von $T(q)$, denn offenbar ist $\varepsilon \in T(q)$ und die Ordnung von ε ist $q + 1$, da $\varepsilon^{\frac{q+1}{2}} \equiv -1 \pmod{q}$ nach dem Beweis zu Proposition 2.1, also hat $\varepsilon^{\frac{q+1}{2}}$ Ordnung 2.

Wir definieren nun die LUCAS-Folge ganzer Zahlen vermöge

$$L_k := \text{Spur}(\varepsilon^{2^k}).$$

Die ersten Werte der Folge sind

$$L_0 = 4, \quad L_1 = 14, \quad L_2 = 194, \quad L_3 = 37634.$$

Bemerkung 3.3.
Die Werte der LUCAS*-Folge können über die Rekursion*

$$L_0 = 4, \quad L_k = L_{k-1}^2 - 2$$

berechnet werden.

Beweis. Es ist

$$4 = L_0 = \mathrm{Spur}(\varepsilon^1).$$

Desweiteren gilt für jedes $k \in \mathbb{N}_0$:

$$\begin{aligned} L_{k+1} &= \mathrm{Spur}(\varepsilon^{2^{k+1}}) = \varepsilon^{2^{k+1}} + \overline{\varepsilon^{2^{k+1}}} \\ &= (\varepsilon^{2^k})^2 + (\overline{\varepsilon^{2^k}})^2 \\ &= (\varepsilon^{2^k} + \overline{\varepsilon^{2^k}})^2 - 2 \cdot \varepsilon^{2^k}\overline{\varepsilon^{2^k}} \\ &= \mathrm{Spur}(\varepsilon^{2^k})^2 - 2 \cdot \underbrace{\nu(\varepsilon)^{2^k}}_{=1} \\ &= L_k^2 - 2. \end{aligned}$$

Das war die Behauptung.

□

Damit haben wir alles Nötige für den Beweis des LUCAS-LEHMER-Tests:

Satz 3.4.
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* $\mathrm{ggT}(L_k, M_p) = 1$ *für* $k \in \{0, ..., p-3\}$ *und* $\mathrm{ggT}(L_{p-2}, M_p) > 1$ *gilt.*

Beweis. Sei zunächst $M_p \in \mathbb{P}$. Nach Lemma 1.2 ist dann $M_p \equiv 7 \pmod{24}$ und somit ist nach Proposition 2.1 $T(M_p) = \langle\varepsilon\rangle$ zyklisch und hat Ordnung $M_p+1 = 2^p$. Damit hat also $\varepsilon^{2^{p-2}}$ Ordnung 4 in $T(M_p)$ und somit gilt $f(\varepsilon^{2^{p-2}}) \equiv 0 \pmod{M_p}$ mit $f(x) = x^2+1$. Damit ist aber $x_{p-2} = \mathrm{Spur}(\varepsilon^{2^{p-2}}) \equiv 0 \pmod{M_p}$, da f offenbar das Minimalpolynom zu $\varepsilon^{2^{p-2}}$ ist. Damit hat aber keine kleinere Potenz von ε diese Eigenschaft und daher ist $x_k = \mathrm{Spur}(\varepsilon^{2^k}) \not\equiv 0 \pmod{M_p}$ für $0 \le k \le p-3$.
Sei nun $q \in \mathbb{P}$ ein Teiler von M_p, der auch x_{p-2} teilt. Damit gilt (alles modulo q)

$$\begin{aligned} & x_{p-2} \equiv 0 \\ \Leftrightarrow & \mathrm{Spur}(\varepsilon^{2^{p-2}}) \equiv 0 \\ \Leftrightarrow & \varepsilon^{2^{p-2}} \equiv -\overline{\varepsilon^{2^{p-2}}} \\ \Rightarrow & \varepsilon^{2^{p-2}} \text{ hat Ordnung 4 in } T(q) \\ \Rightarrow & \varepsilon \text{ hat Ordnung } 2^p = M_p + 1 \text{ in } T(q) \end{aligned}$$

Nun ist aber $|T(q)| = q \pm 1$, je nachdem, ob q in R prim bleibt oder zerfällt. Ist q prim in R, so ist $|T(q)| = q+1$ nach dem Beweis zu Proposition 2.1. Anderenfalls ist R/qR ein Ring mit $|(R/qR)^*| = (q-1)^2$. Dann ist $\nu_q : (R/qR)^* \to (\mathbb{Z}/q\mathbb{Z})^*$ (s.o.) ein Gruppenepimorphismus, so dass mit dem Homomorphiesatz folgt, dass $|T(q)| = q - 1$ gilt.
Da aber nach dem Satz von LAGRANGE die Ordnung von ε die Gruppenordnung $|T(q)|$ teilt, muss $M_p = q$ gelten, also ist $M_p \in \mathbb{P}$.
Damit ist die Behauptung bewiesen.

□

Meistens wird eine äquivalente Variante von Satz 3.4 verwendet, die sich auch besser als Grundlage für einen Algorithmus eignet:

Korollar 3.5.
Für $p \in \mathbb{P}$ ist die MERSENNE*-Zahl M_p genau dann eine Primzahl, wenn M_p den $p-2$-ten Wert der* LUCAS*-Folge L_{p-2} teilt:*

$$M_p \in \mathbb{P} \Leftrightarrow L_{p-2} \equiv 0 \pmod{M_p}.$$

Beweis. Ist $M_p \in \mathbb{P}$, so folgt sofort nach Satz 3.4, dass

$$L_{p-2} \equiv 0 \pmod{M_p}.$$

Ist umgekehrt M_p ein Teiler von L_{p-2}, dann ist insbesondere $\mathrm{ggT}(M_p, L_{p-2}) = M_p > 1$. Daraus folgt aber sofort, dass $\mathrm{ggT}(M_p, L_{p-3}) = 1$ gelten muss, denn angenommen, es wäre $\mathrm{ggT}(M_p, L_{p-3}) = d \neq 1$, dann gilt:

$$k \cdot M_p = L_{p-2} = L_{p-3}^3 - 2$$

für ein $k \in \mathbb{Z}$. Es ist aber auch $M_p = m \cdot d$ und $L_{p-3} = \ell \cdot d$, also folgt, dass $-2 \equiv 0 \pmod{d}$, also $d = 2$. Aber M_p ist ungerade, also haben wir einen Widerspruch.
Außerdem gilt für $k \in \{1, ..., p-3\}$

$$\mathrm{ggT}(M_p, L_k) = 1 \Rightarrow \mathrm{ggT}(M_p, L_{k-1}) = 1,$$

denn wäre wieder $\mathrm{ggT}(M_p, L_{k-1}) = d$, also $L_{k-1} = de$ und $M_p = df$, so folgt für geeignete $a, b \in \mathbb{Z}$

$$1 = aL_k + bM_p = aL_{k-1}^2 - 2a + bM_p \equiv -2a \pmod{d},$$

also, da d ungerade sein muss, $a \equiv (-2)^{-1} \pmod{d}$. Dann ist aber $L_k \equiv -2 \pmod{d}$, also muss insbesondere L_k ungerade sein, was aber offenbar ein Widerspruch ist, da L_k immer gerade ist.
Also gilt $\mathrm{ggT}(L_k, M_p) = 1$ für $k \in \{0, ...p-3\}$ und $\mathrm{ggT}(L_{p-2}, M_p) > 1$ und nach Satz 3.4 ist somit $M_p \in \mathbb{P}$. □

4 Mersenne-Zahlen und Elliptische Kurven

In diesem Abschnitt werden einige Eigenschaften der elliptischen Kurve E über $\mathbb{Q}$ mit der affinen WEIERSTRASS-Gleichung

$$y^2 = x^3 - 12x = x(x^2 - 12)$$

betrachtet, die letzten Endes dann zum Beweis des Primzahltests von B.H. GROSS führen. E hat die Diskriminante

$$\Delta = -(8 \cdot (2 \cdot (-12))^3) = 2^{12} \cdot 3^3,$$

ist also in jedem Körper der Charakteristik $q > 3$ regulär, man sagt E besitzt eine gute Reduktion zu allen Primzahlen $q > 3$. Über dem Körper $\mathbb{Q}(i)$ hat E komplexe Multiplikation, z.B. durch den Endomorphismus $[i]$ ($\mathrm{End}(E) \cong \mathbb{Z}[i]$):

$$[i] : E(\mathbb{Q}(i)) \to E(\mathbb{Q}(i)), (x, y) \mapsto (-x, i \cdot y).$$

Dies führt gleich zum ersten

Lemma 4.1.
Es sei $q \in \mathbb{P} \setminus \{2, 3\}$ mit $q \equiv 3 \pmod 4$. Dann ist die Reduktion $\hat{E}$ von E modulo q supersingulär und es gibt genau $q+1$ $\mathbb{F}_q$-rationale Punkte von E, also

$$|\hat{E}(\mathbb{F}_q)| =: |E(q)| = q + 1.$$

Beweis. Es ist zunächst zu zeigen, dass $\hat{E}$ supersingulär ist. Laut Satz 2.18 gilt dazu, dass $\hat{E}$ supersingulär ist, falls $\langle q \rangle$, das von q erzeugte Ideal in $\mathbb{Q}$ in $\mathbb{Q}(i)$ träge ist, also auch in $\mathbb{Z}[i]$ ein Primideal bleibt. Da $q \equiv 3 \pmod 4$, ist das der Fall (vgl. Zwei-Quadrate-Satz von FERMAT), also ist $\hat{E}$ supersingulär. Damit teilt q insbesondere die Spur des FROBENIUS-Endomorphismus, wenn man $\hat{E} = E(q)$ betrachtet, also die $\mathbb{F}_q$-rationalen Punkte von E:

$$q \,|\, |E(q)| - q - 1 \Leftrightarrow |E(q)| = k \cdot q + 1 \text{ für ein } k \in \mathbb{Z}.$$

Nach der HASSE-Ungleichung ist aber

$$|q + 1 - |E(q)|| \leq 2\sqrt{q},$$

also folgt

$$|(k-1)q| \leq 2\sqrt{q} \lneqq q,$$

denn $q \geq 7$ nach Voraussetzung. Das erzwingt aber $k = 1$ und damit

$$|E(q)| = q + 1.$$

Das war zu zeigen.

□

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.

Beweis. Laut Lemma 4.1 ist die Reduktion $\hat{E}$ modulo q supersingulär und $E(q)$ hat Ordnung $q+1$, denn insbesondere ist $q \equiv 3 \pmod 4$. Nach [Si], Corollary III.6.4 und Theorem V.3.1 ist dann für jedes $m \in \mathbb{Z}$ mit $\mathrm{ggT}(m,q)=1$

$$\mathrm{Kern}([m]) \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$$

und

$$\mathrm{Kern}([q]) = \{\mathcal{O}\}.$$

Sei nun $K = \mathbb{F}_q$. Dann ist auch $\hat{E}(K)$ endlich, sagen wir, $|\hat{E}(K)| = n$. Dann ist $\hat{E}(K)$ eine endliche Untergruppe von $\mathrm{Kern}([n])$, also gilt nach dem Strukturssatz über endlich erzeugte ABELsche Gruppen

$$\hat{E}(K) \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \text{ mit } d_1 \mid d_2 \text{ und } d_1 \cdot d_2 = n.$$

Außerdem ist d_1 kein Vielfaches der Charakteristik q von K, denn dann hätte $\hat{E}(K)$ eine Untergruppe isomorph zu $(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}) \leq \mathrm{Kern}([q])$. $\mathrm{Kern}([q])$ ist aber trivial, da $\hat{E}$ supersingulär ist. Also ist dies nicht möglich. Desweiteren ist d_1 ein Teiler von $|\mu(K)|$, der Kardinalität der Untergruppe aller Einheitswurzeln in K von K^*. Das folgt aus der Surjektivität und der Verträglichkeit mit der Operation der GALOIS-Gruppe $\mathrm{Gal}_{\overline{K}/K}$ der WEIL-Paarung. Es gibt dann nämlich $S,T \in \mathrm{Kern}([d_1]) \cap \hat{E}(K) = \mathrm{Kern}([d_1])$ mit $e_{d_1}(S,T) = \zeta$, wo $\zeta \in \overline{K}$ eine primitive d_1-te Einheitswurzel ist. Lässt man nun $\sigma \in \mathrm{Gal}_{\overline{K}/K}$ auf beiden Seiten operieren, so folgt, da sich die linke Seite der Gleichung nicht ändert (denn S und T sind K-rational), dass $\zeta \in K$. Damit ist dann

$$d_1 = \mathrm{ord}(\zeta) \mid |\mu(K)|.$$

Da $\mu(K) \leq K^*$ teilt d_1 auch $|K^*|$.
Weiterhin folgt, dass $d_1 \mid \mathrm{ggT}(q-1, q+1) = 2$. Also ist $E(q)$ entweder zyklisch (für $d_1 = 1$) oder enthält eine Untergruppe isomorph zu $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
Letzteres kann aber nicht eintreten, denn das würde bedeuten, dass $\mathrm{Kern}([2]) \leq E(q)$, also dass alle Punkte von $\hat{E}(\overline{K})$, die mit 2 multipliziert $\mathcal{O}$ ergeben, $\mathbb{F}_q$-rational sind, also insbesondere alle Wurzeln von

$$\circledast \qquad x^3 - 12x = x(x^2 - 12)$$

in $\overline{\mathbb{F}_q}$. Aber $\left(\frac{12}{q}\right) = -1$, also hat $x^2 - 12$ keine Wurzeln in $\mathbb{F}_q$. Damit scheidet also $d_1 = 2$ aus und $E(q)$ ist zyklisch.
Wir betrachten E nun über einem Erweiterungskörper L von $\mathbb{F}_q$, so dass $\beta^2 = 12$ in L. Dann faktorisiert $\circledast$ vollständig zu

$$x(x-\beta)(x-\overline{\beta}).$$

Dann gilt mit Satz 2.19, dass $Q = (x,y)$ genau dann in $2\hat{E}(L)$ liegt, wenn x, $(x-\beta)$ und $(x-\overline{\beta})$ Quadrate in L sind. Ist nun Q ein $\mathbb{F}_q$-rationaler Punkt, dann gilt aber, dass $(x-\beta)$ und $(x-\overline{\beta})$ genau dann Quadrate in L sind, wenn (x^2-12) ein Quadrat in $\mathbb{F}_q$ ist. Es gilt nämlich, falls $(x-\beta) = \ell^2, \quad \ell \in L$, dann ist $(x-\overline{\beta}) = \overline{(x-\beta)} = \overline{\ell}^2$, denn $x \in \mathbb{F}_q$, also ist $\overline{x} = x$. Dann ist

$$(x^2-12) = \ell^2 \cdot \overline{\ell}^2 = \underbrace{\nu_q(\ell)}_{\in \mathbb{F}_q}^2,$$

also ist dann auch $(x^2 - 12)$ ein Quadrat in $\mathbb{F}_q$. Die Umkehrung ist banal.
Also ist $P = (-2, 4)$ höchstens dann in $2\hat{E}(L)$, wenn $((-2)^2 - 12) = -8$ ein Quadrat modulo q ist, aber

$$\left(\frac{-8}{q}\right) = \left(\frac{-2}{q}\right) = -1,$$

also ist P kein Quadrat in $\hat{E}(L)$, also erst recht nicht in $E(q)$, und das war die Behauptung.

□

Wir definieren nun eine Folge rationaler Zahlen über die x-Koordinaten der sukzessiven Quadrate des Punktes P aus der Proposition vermöge

$$G_k = x(2^k \cdot P).$$

$x(Q)$ entspricht hier der Projektion auf die erste Koordinate des Punktes Q. Durch Anwenden von Satz 2.6 erhält man sofort die Rekursionsformel

$$G_0 = -2, \qquad G_k = \frac{(G_{k-1}^2 + 12)^2}{4G_{k-1}(G_{k-1}^2 - 12)}.$$

Diese Formel wird im folgenden Satz für den Primzahltest benötigt:

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.*

Beweis. Sei zunächst M_p eine Primzahl. Dann folgt mit Proposition 4.2, dass

$$E(M_p) \cong C_{M_p+1} = C_{2^p}.$$

Da $P = (-2, 4)$ außerdem nicht durch 2 teilbar ist, erzeugt P die Gruppe $E(M_p)$. Damit ist

$$2^{p-1} \cdot P = (0, 0),$$

denn $2^{p-1} \cdot P$ hat wie $(0, 0)$ Ordnung 2 in $E(M_p)$ und das $E(M_p)$ zyklisch ist, müssen die beiden Punkte gleich sein, demnach ist insbesondere

$$G_{p-1} = x(2^{p-1} \cdot P) \equiv 0 \pmod{M_p}.$$

Da P Ordnung 2^p hat, kann $2^k \cdot P$ für $k < p - 1$ nicht auch Ordnung 2 haben, also ist auch

$$G_k \not\equiv 0 \pmod{M_p}$$

und damit sind die G_k und offenbar auch die $G_k(G_k^2-12)$ M_p-adische Einheiten, da 12 kein Quadrat modulo M_p ist.

Sei umgekehrt $\mathrm{ggT}(G_k(G_k^2 - 12), M_p) = 1$ für $1 \leq k \leq p-2$ und q ein gemeinsamer Primteiler von $M_p = 2^p - 1$ und G_{p-1}. Dann ist $2^{p-1} \cdot P = (0,0) \in E(q)$, denn $x(2^{p-1} \cdot P) = 0$ in $E(q)$. Demnach hat also $2^{p-1} \cdot P$ Ordnung 2 in $E(q)$, also hat P Ordnung $2^p = M_p + 1$. Aber nach der HASSEschen Ungleichung ist die Ordnung von $E(q)$ durch $q + 1 - a_q$ mit $|a_q| \leq 2\sqrt{q}$ beschränkt und damit auch die Ordnung von P:

$$M_p + 1 \leq q + 1 + 2\sqrt{q},$$

aber damit ist zwangsläufig $M_p = q$ und damit ist $M_p \in \mathbb{P}$. Das war zu zeigen.

□

Zu diesem Satz gibt es eine äquivalente Formulierung, die sich besser für die Umsetzung in einen Algorithmus eignet (vgl. Abschnitt 5).

Korollar 4.4.
Sei M_p eine MERSENNE*-Zahl. M_p ist genau dann eine Primzahl, wenn $G_{p-1} \in \mathbb{Z}/M_p\mathbb{Z}$ existiert und*

$$G_{p-1} \equiv 0 \pmod{M_p}.$$

Beweis. Es sei zunächst $M_p \in \mathbb{P}$. Dann folgt nach Satz 4.3, dass $G_{p-1} \equiv 0 \pmod{M_p}$.
Falls $G_{p-1} \equiv 0 \pmod{M_p}$, so ist $\mathrm{ggT}(G_{p-1}, M_p) = M_p > 1$. Dann folgt auch

$$G_{p-1} = \frac{(G_{p-2}^2 + 12)^2}{4G_{p-2}(G_{p-2}^2 - 12)} \equiv 0 \pmod{M_p}.$$

Dieser Ausdruck ist genau dann wohldefiniert, wenn $G_{p-2}(G_{p-2}^2 - 12)$ eine Einheit modulo M_p ist. Aber aufgrund der rekursiven Definition impliziert aber die Existenz von G_k stets die Tatsache, dass $G_{k-1}(G_{k-1}^2 - 12)$ eine Einheit modulo M_p ist für $k \in \{2, ..., p-1\}$. Dann ist nach Satz 4.3 M_p eine Primzahl und die Behauptung gezeigt. □

5 Algorithmen und Effizienz

Ausgehend von den Korollaren 3.5 und 4.4 lassen sich nun leicht Algorithmen erstellen, die eine MERSENNE-Zahl M_p darauf testen, ob sie eine Primzahl ist. Der erste vorgestellte Algorithmus ist der klassische LUCAS-LEHMER-Test:

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.`

Der Algorithmus ist offenbar eine Umformulierung von Korollar 3.5, so dass über die Funktionalität nichts mehr zu zeigen ist. Er benötigt $\mathcal{O}(p)$ Multiplikationen von L modulo M_p. Ein möglicher Algorithmus für den Primzahltest von GROSS basierend auf Korollar 4.4 kann wie folgt formuliert werden:

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` $G = 0$.

Ein möglicher Vorteil des Elliptic-Tests ist nun, dass die Schleife gegebenenfalls vorzeitig abgebrochen wird, falls M_p keine Primzahl ist, während beim LUCAS-LEHMER-Test in jedem Fall alle $p-2$ Folgenglieder berechnet werden müssen. Wenn man bedenkt, dass es unter den 1 329 726 Primzahlen unterhalb von 20 996 012 nur 40 eine MERSENNEsche Primzahl liefern (Quelle: www.mersenne.org), scheint das deutlich für den Elliptic-Test zu sprechen, im Falle des Abbruchs kommt er mit $\mathcal{O}(\lambda)$ arithmetischen Operationen aus, wobei $\lambda \ll p$.
Beide Algorithmen wurden von mir in `Sage` implementiert.
`print_timing` ist eine Timer-Funktion, die ich von der Webseite

www.daniweb.com/code/snippet216610.html

übernommen habe, denn sie hat mit den Algorithmen an sich nichts zu tun. Der Zusatz `@print_timing` aktiviert den Timer, wenn die Ausgabe gewünscht ist. Alle übrigen Funktionen sind von mir selbst geschrieben.
Die Funktion `LucLeh(p)` testet für das eingegebene p die Zahl $M_p = 2^p - 1$ mittels des LUCAS-LEHMER-Tests darauf, ob sie eine Primzahl ist, die Funktion

`Elliptic(p)` verwendet dazu den Elliptic-Test die Funktionen `FLucLeh` bzw. `FElliptic` tun respektive das gleiche, sind aber für große p, bei denen bekannt ist, dass es sich um Primzahlen handelt, etwas schneller, da hier auf die Abfrage, ob $p \in \mathbb{P}$ verzichtet wurde. Die Funktion `MersenneExp(test,n)` schließlich berechnet mit dem Verfahren `test` alle Exponenten p unterhalp von `n`, für die M_p prim ist. Zusätzlich wird hier die benötigte Zeit gemessen.
Bei mehreren Experimenten mit den von mir geschriebenen Funktionen bot sich allerdings ein unerwartetes Bild, denn der Lucas-Lehmer-Test war durchschnittlich etwa 16-mal schneller als der Elliptic-Test (vgl. Tabelle). Grund hierfür ist wohl die Tatsache, dass der einzige Exponent unterhalb von 10 000, für die der Elliptic-Test vorzeitig die Schleife verlässt, 23 ist (mit `Sage` nachgerechnet) und sich sonst dieser Vorteil demnach nicht bemerkbar machen kann.

`n`	Zeit `MersenneExp(1,n)` in ms	Zeit `MersenneExp(2,n)` in ms
10	1.166	1.913
50	3.067	38.708
100	6.731	102.648
500	323.642	6005.995
1000	1729.314	45150.361
10000	2805339.922	76076245.263

Der Lucas-Lehmer-Test ist also zumindest für so kleine Primzahlen schneller als der Elliptic-Test. Um die theoretische Überlegung von oben für größere Primzahlen bestätigen oder widerlegen zu können stand mir leider die nötige Rechenleistung nicht zur Verfügung (allein für die Suche nach den Exponenten $\leq 10\,000$ war bei meiner Implementierung eine Rechenzeit von etwa 20 Stunden mit einem 1.66 GHz-Prozessor notwendig).

Literatur

[Gr] Benedict H. Gross, *"An elliptic curve test for Mersenne primes"*, J. Number Theory 110 (2005) 114-119

[Si] Joseph H. Silverman, *"The Arithmetic of Elliptic Curves"*, Springer, 1986

[Si2] Joseph H. Silverman, *"Advanced Topics in the Arithmetic of Elliptic Curves"*, Springer, 1995

[Wer] Annette Werner, *„Elliptische Kurven in der Kryptographie"*, Springer, 2001

[Wil] Wolfgang Willems, *„Codierungstheorie und Kryptographie"*, Birkhäuser, 2008

[Hus] Dale Husemöller, *"Elliptic Curves"*, Springer, 1987

[ReUl] Reinhold Remmert, Peter Ullrich, *„Elementare Zahlentheorie"*, Birkhäuser, 3. Auflage (2007)

[Kr] Aloys Krieg, *„Algebraische Zahlentheorie"*, Skript zur Vorlesung, Aachen 2004

[Sto] Michael Stoll *„Elliptische Kurven I"*, Skript zur Vorlesung, Bremen, 2000

[YJ] Song Y. Yang, Glyn James *"Testing Mersenne Primes with Elliptic Curves"*, Computer algebra in scientific computing, 303–312, Springer, Berlin 2006