Primzahltests mit Elliptischen Kurven

vorgelegt als Bachelorarbeit
der Fakultät für Mathematik, Informatik und Naturwissenschaften
der Rheinisch-Westfälischen Technischen Hochschule Aachen

Gutachterin: Prof. Dr. G. Nebe, Lehrstuhl D für Mathematik

Michael H. Mertens
Matrikelnummer: 289246

März 2011

Inhaltsverzeichnis

Einleitung

Die vorliegende Arbeit basiert im Wesentlichen auf der Idee des Artikels "An elliptic curve test for Mersenne primes" von Gross[1] (vgl. [Gro05]), der dort einerseits den klassischen Test für Mersenne[2]-Primzahlen von Lucas[3] und Lehmer[4] mittels algebraischer Geometrie neu interpretiert, nämlich als Quadrieren eines Punktes auf dem algebraischen Torus über dem Körper $\mathbb{Q}$ zum Erweiterungskörper $\mathbb{Q}(\sqrt{3})$, und andererseits einen neuen Test vorstellt, der auf dem Quadrieren eines Punktes auf der elliptischen Kurve zur Gleichung

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

basiert.
Die grundlegende Idee des Artikels ist es, eine Gruppe zu finden, deren Ordnung und nach Möglichkeit einfache Struktur (z.B. zyklische Gruppen, deren Ordnung eine Primzahlpotenz ist) man für bestimmte Sorten von Primzahlen in gewisser Weise leicht bestimmen kann, und dann in dieser Gruppe zu rechnen. Da die Struktur elliptischer Kurven als Abelsche Gruppen weitgehend verstanden ist, eignen sie sich gut für dieses Vorgehen. Gross wandte diese Idee, wie gesagt, auf Mersenne-Zahlen, also Zahlen der Form

$$M_p = 2^p - 1, \quad p \in \mathbb{P}$$

an. Robert Denomme[5] und Gordan Savin[6] fanden später geeignete Kurven um Fermat[7]-Primzahlen

$$F_n = 2^{2^n} + 1, \quad n \in \mathbb{N}_0$$

bzw. Primzahlen der Form

$$3^{2^\ell} - 3^{2^{\ell-1}} + 1 \text{ bzw. } 2^{2^\ell} - 2^{2^{\ell-1}} + 1$$

zu testen (vgl. [DS08]).
Ziel dieser Arbeit wird es sein, die erwähnten Testverfahren für Mersenne- und Fermat-Zahlen vorzustellen und einen entsprechenden Test für Thabit[8]-Zahlen, also Zahlen der Form

$$K_n = 3 \cdot 2^n - 1, \quad n \in \mathbb{N}_0$$

bzw. allgemeiner Zahlen der Form

$$K(h, n) = h \cdot 2^n - 1, \quad h \geq 3 \text{ ungerade}, n \in \mathbb{N}_0$$

[1] Benedict Hyman Gross, geboren 1950, amer. Mathematiker, Zahlentheorie, algebraische Geometrie
[2] Marin Mersenne, 1588-1648, frz. Mathematiker und Theologe, Zahlentheorie
[3] Édouard Lucas, 1842-1891, frz. Mathematiker, Zahlentheorie und Unterhaltungsmathematik
[4] Derrick Henry Lehmer, 1905-1991, amer. Mathematiker, Zahlentheorie
[5] Robert Denomme, amer. Mathematiker, Zahlentheorie
[6] Gordan Savin, amer. Mathematiker, Zahlentheorie
[7] Pierre de Fermat, 1607-1665, frz. Mathematiker und Jurist, Zahlentheorie, Wahrscheinlichkeitsrechnung, Differentialrechnung
[8] Thabit ibn Qurra, 826-901, syr. Mathematiker, Astronom, Philosoph, Zahlentheorie und Geometrie

zu entwickeln.
Dazu werden im ersten Kapitel die benötigten Resultate aus der Zahlentheorie, u.a. über das quadratische Reziprozitätsgesetz und quadratische Zahlkörper, bereitgestellt. Im zweiten Kapitel wird ein Überblick über die benötigte Theorie elliptischer Kurven gegeben. Der Inhalt des dritten Kapitels werden dann die Tests für Mersenne- und Fermat-Primzahlen sein, während das vierte Kapitel von mir gefundene Alternativen zu Gross' Test für Mersenne-Zahlen und den von mir gefundenen Test für verallgemeinerte Thabit-Zahlen beschreibt.

Kapitel 1

Grundlagen aus der Zahlentheorie

1.1 Elementare Zahlentheorie

Definition 1.1.

1. *Zu $p \in \mathbb{P}$ heißt $M_p := 2^p - 1$ die p-te* Mersenne-***Zahl***.
2. *Für jedes $n \in \mathbb{N}_0$ heißt $F_n := 2^{2^n} + 1$ die n-te* Fermat-***Zahl***.
3. *Für $n \in \mathbb{N}_0$ heißt $K_n := 3 \cdot 2^n - 1$ die n-te* Thabit-***Zahl***.
   Unter einer ***verallgemeinerten*** Thabit-***Zahl*** *verstehen wir eine Zahl der Form $K(h,n) = h \cdot 2^n - 1$ für ungerades $h \in \mathbb{N}$, $h \geq 3$ und $n \in \mathbb{N}_0$.*

Es wird in der gesamten Arbeit um die Frage gehen, wann diese Zahlen Primzahlen sind. Dazu zunächst ein paar kleine Beobachtungen:

Lemma 1.2.

1. *Ist $2^p - 1$ eine Primzahl, so ist notwendigerweise $p \in \mathbb{P}$ und für jedes $p \in \mathbb{P} \setminus \{2\}$ ist*
$$M_p \equiv 7 \pmod{24}.$$
2. *Ist $2^k + 1$ eine ungerade Primzahl, so ist notwendigerweise k eine Potenz von 2, also gibt es ein $n \in \mathbb{N}_0$ mit $k = 2^n$.*
3. *Für $n > 2$ ist $K_n \equiv -1 \pmod{24}$ und falls $n \equiv 1 \pmod 4$, so ist K_n keine Primzahl.*

Beweis. ad 1.: Nehmen wir an, p wäre nicht prim, d.h. es gibt $k, \ell > 1$ mit $p = k \cdot \ell$. Dann gilt

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

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.
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

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

Des Weiteren 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.
ad 2.: Sei $k = 2^n \cdot \ell$ für $n, \ell \in \mathbb{Z}$ geeignet und $\ell > 1$ ungerade. Dann gilt:

$$\begin{aligned} 2^k + 1 &= 1 - (-2^{2^n})^\ell \\ &= (1 + 2^{2^n}) \underbrace{\sum_{i=0}^{\ell-1} (-2^{2^n})^i}_{>1}, \end{aligned}$$

also ist eine nichttriviale Faktorisierung von $2^k + 1$ gefunden. Damit $2^{2^n \ell} + 1$ prim sein kann, muss also $\ell = 1$ gelten.
ad 3.: Es sei $n \geq 3$. Dann ist $3 \cdot 2^n = (3 \cdot 2^3) \cdot 2^{n-3}$ durch 24 teilbar, also ist $K_n \equiv -1 \pmod{24}$. Ist $n \equiv 1 \pmod 4$, so ist $K_n = 3 \cdot 2^n - 1 \equiv 3 \cdot 2 - 1 \equiv 0 \pmod 5$ und damit kann K_n nicht prim sein, da nach Voraussetzung $n \geq 3$, also $K_n \geq 23$ gilt. □

Über jede dieser Zahlenarten gibt es zahlreiche unbeantwortete Fragen, z.B. ob es unendlich viele Primzahlen der jeweiligen Form gibt. Neben den Zahlen an sich gibt es auch weitere Phänomene in der Zahlentheorie, bei denen diese Zahlen eine Rolle spielen. Eine Auswahl dieser Phänomene wird im folgenden Satz vorgestellt, doch zuvor ist noch eine Definition erforderlich. Die Bezeichnungen wurden aus [Bor72] übernommen.

Definition 1.3.

1. *Zu einer natürlichen Zahl $n \in \mathbb{N}$ bezeichnet*

$$\sigma(n) := \sum_{d|n} d$$

*die **Teilersumme** von n und*

$$\tau(n) := \sum_{d|n, d \neq n} d = \sigma(n) - n$$

*die Summe der **echten Teiler** von n.*

2. *Eine natürliche Zahl $n \in \mathbb{N}$ heißt **vollkommen**, falls*

$$\sigma(n) = 2 \cdot n \text{ bzw. } \tau(n) = n$$

gilt.

3. *Zwei natürliche Zahlen $n, m \in \mathbb{N}$ heißen **befreundet**, falls*

$$\tau(n) = m \qquad \text{und} \qquad \tau(m) = n$$

gilt.

4. *Es sei $M \subset \mathbb{C}$ mit $\{0,1\} \subseteq M$. Dann bildet die Menge*

$$Kon(M) := \{z \in \mathbb{C} \mid z \text{ aus } M \text{ konstruierbar}\}$$

*einen Teilkörper von $\mathbb{C}$. Hierbei heißt z aus M **konstruierbar**, falls z in endlich vielen Schritten durch Schneiden von Geraden und Kreisen durch Punkte aus M erhalten werden kann.*

Bemerkung 1.4.
*Man nennt σ und τ **zahlentheoretische Funktionen**. Eine wichtige Eigenschaft von σ ist die Multiplikativität, d.h. für $a, b \in \mathbb{N}$ teilerfremd ist*

$$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b).$$

Allerdings ist τ nicht multiplikativ.

Satz 1.5.

1. *Es sei $N \in \mathbb{N}$ eine gerade Zahl. Dann ist N genau dann vollkommen, wenn gilt*

$$N = 2^{p-1} \cdot M_p$$

für $M_p \in \mathbb{P}$.

2. *Sei $n \geq 3$. Dann ist das regelmäßige n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^k \cdot p_1 \cdot \cdots \cdot p_r$ für ein $k \in \mathbb{N}$ und paarweise verschiedene* Fermat-*Primzahlen p_j.*

3. *Für $n \in \mathbb{N}$, $n \geq 2$ seien die* Thabit-*Zahlen K_{n-1} und K_n sowie $r := 9 \cdot 2^{2n-1} - 1$ Primzahlen, wobei K_ℓ im Sinne von Definition 1.1 zu verstehen ist. Dann sind die Zahlen $a := 2^n \cdot K_{n-1} \cdot K_n$ und $b := 2^n \cdot r$ befreundet.*

Beweis. ad 1.: Sei zunächst $N = 2^{p-1} \cdot M_p$ mit $M_p \in \mathbb{P}$. Dann ist

$$\sigma(N) = \sigma(2^{p-1}) \cdot \sigma(M_p) = \left(\sum_{j=0}^{p-1} 2^j\right) \cdot (M_p + 1) = (2^p - 1) \cdot 2^p = 2 \cdot N,$$

also ist N vollkommen.
Ist umgekehrt N vollkommen, dann ist $N = 2^k \cdot \ell$ mit $\ell \in \mathbb{N}$ ungerade und es gilt einerseits $\sigma(N) = 2N = 2^{k+1} \cdot \ell$ und andererseits, da ℓ ungerade und damit teilerfremd zu 2^k ist

$$\sigma(N) = \sigma(2^k) \cdot \sigma(\ell) = (2^{k+1} - 1) \cdot \sigma(\ell).$$

Es folgt also

$$\sigma(\ell) = \frac{2^{k+1}}{2^{k+1} - 1}\ell = \ell + \frac{\ell}{2^{k+1} - 1}.$$

Damit muss, da $\sigma(\ell) \in \mathbb{N}$ ist, $2^{k+1} - 1$ ein Teiler von ℓ sein, also in $\sigma(\ell)$ als Summand auftauchen, was nur für $\ell = 2^{k+1} - 1$ sein kann. Dann ist aber $\sigma(\ell) = \ell + 1$, also ist ℓ prim und die Behauptung folgt.
ad 2.: Der formale Beweis hierfür wäre zu umfangreich, daher sei er hier nur skizziert. Ein vollständiger Beweis ist z.B. in [Str98, §10] gegeben.
Der Schnitt von einer Gerade und einem Kreis beziehungsweise zwei Kreisen läuft auf das Lösen einer quadratischen Gleichung hinaus, sodass $Kon(M)$ abgeschlossen ist unter

Wurzelziehen und komplexer Konjugation ist. Jeder solche Konstruktionsschritt liefert eine Körpererweiterung vom Grad höchstens 2. Damit folgt also, dass das regelmäßige n-Eck genau dann konstruierbar ist, wenn $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ eine 2-Potenz ist, was genau dann der Fall ist, wenn n die oben gegebene Form hat, wobei $\varphi(n)$ die EULERsche φ-Funktion bezeichne.
ad 3.: Die Behauptung ist äquivalent zu der Aussage, dass $\sigma(a) = \sigma(b) = a + b$ gilt. Es ist

$$\begin{aligned}\sigma(a) &= \sigma(2^n) \cdot \sigma(K_{n-1}) \cdot \sigma(K_n) = (2^{n+1} - 1) \cdot (K_{n-1} + 1) \cdot (K_n + 1)\\ &= (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1}\\ \sigma(b) &= \sigma(2^n) \cdot \sigma(r) = (2^{n+1} - 1) \cdot (r + 1) = (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1}\\ a + b &= 2^n \cdot (K_{n-1}K_n - 1 + 9 \cdot 2^{2n-1} - 1) = (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1}\end{aligned}$$

□

Bereits EUKLID[1] konnte zeigen, dass der Ausdruck $2^{p-1} \cdot (2^p - 1)$ stets eine gerade vollkommene Zahl liefert, wenn $2^p - 1$ eine Primzahl ist. Etwa 2000 Jahre später bewies EULER[2], dass umgekehrt auch jede gerade vollkommene Zahl von dieser Form ist. Es ist bis heute nicht bekannt, ob ungerade vollkommene Zahlen existieren, man vermutet allerdings, dass dem nicht so ist. Im Jahr 1991 konnten BRENT[3], COHEN[4] und TE RIELE[5] allerdings eine untere Schranke von 10^{300} für ungerade vollkommene Zahlen angeben (vgl. [RPB91]).
Den in Satz 1.5.2 angegebenen Zusammenhang zwischen FERMAT-Primzahlen und Konstruierbarkeit regelmäßiger Polygone bewies GAUSS[6] im Jahre 1801 in den *Disquisitiones Arithmeticae*, wobei er bereits 1796 als Spezialfall eine Konstruktionsmethode für das regelmäßige 17-Eck angab (vgl. [Str98, S. 151 ff]).
Die Formel für befreundete Zahlen wurde von THABIT im 9. Jahrhundert nach Christus entdeckt und im westlichen Europa 1636 von FERMAT bzw. 1638 von DESCARTES[7] wiederentdeckt. Aus dem Werk *De numeris amicabilibus* aus dem Jahr 1747 von EULER stammt ein Beweis von Satz 1.5.3 für verallgemeinerte THABIT-Zahlen. Demnach gilt:

Sind $K(h, n) := h \cdot 2^n - 1$, $K(h, n - k) = h \cdot 2^{n-k} - 1$ *und* $r := h^2 \cdot 2^{2n-k} - 1$ *Primzahlen mit* $h = 2^{k+1} - 1$ *und* $k, n \in \mathbb{N}$, *dann sind die Zahlen* $a := 2^n \cdot K(h, n) \cdot K(h, n - k)$ *und* $b := 2^n \cdot r$ *befreundet.*

[1] EUKLID, ca. 360-280 v.Chr., gr. Mathematiker, Geometrie und Arithmetik
[2] LEONHARD EULER, 1707-1783, schweiz. Mathematiker, Analysis, Variationsrechnung, Zahlentheorie, Algebra
[3] RICHARD P. BRENT, geboren 1946, austr. Mathematiker und Informatiker, algorithmische Zahlentheorie
[4] GRAEME LAWRENCE COHEN, austr. Mathematiker, Zahlentheorie
[5] HERMANUS JOHANNES JOSEPH TE RIELE, geboren 1947, niederl. Mathematiker, algorithmische Zahlentheorie
[6] CARL FRIEDRICH GAUSS, 1777-1855, dt. Mathematiker und Astronom, Zahlentheorie, Statistik, Analysis, elliptische Funktionen
[7] RENÉ DESCARTES, 1598-1650, frz. Mathematiker und Philosoph, analytische Geometrie, Differentialrechnung, Zahlentheorie

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 [RU07, S.237 ff] verwiesen.

Definition 1.6.

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. Man beachte, dass $a \in p\mathbb{Z}$ weder ein quadratischer Rest, noch ein quadratischer Nichtrest modulo p ist.*

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[8]-***Symbol***.

Bemerkung 1.7.

1. *Es gilt für ungerades $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = 1$:*
$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$
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. ad 1.: Diese Identität folgt sofort aus dem kleinen Satz von Fermat, laut dem
$$a^{p-1} \equiv 1 \pmod{p}$$
für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = 1$ gilt. 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
$$x^{p-1} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$
und 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 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
ad 2.: Folgt sofort aus 1. □

[8] Adrien-Marie Legendre, 1752-1833, frz. Mathematiker, Zahlentheorie und Analysis

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

Satz 1.8.
Sei p eine ungerade Primzahl.

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

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

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

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

BEWEIS. ad 1.: Siehe [RU07, 7.1.4 Korollar, S. 243].
ad 2.: Siehe [RU07, 7.1.5 Satz, S. 246]. □

Der folgende Satz ist das Quadratische Reziprozitätsgesetz, das GAUSS zuerst im Jahre 1801 bewies.

Satz 1.9. ***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

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

BEWEIS. Siehe [RU07, 7.2.2, S. 254 ff]. □

1.3 Quadratische Zahlkörper

In diesem Abschnitt sei stets $m \in \mathbb{Z}$ quadratfrei, d.h. $m = p_1 \cdot ... \cdot p_\ell$ für paarweise verschiedene Primzahlen $p_j \in \mathbb{P}$.

Definition 1.10.

1. *Wir verstehen 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 $m > 0$, so 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 $\mathbb{Z}[X]$, also*

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

wobei μ_α das Minimalpolynom von α über $\mathbb{Q}$ bezeichnet.

4. *Die Abbildung*

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

*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*

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

Bemerkung 1.11.

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

2. *Man beachte, dass $\mathcal{O}_K$ für einen quadratischen Zahlkörper K im Allgemeinen* kein *faktorieller Ring ist, insbesondere kann es irreduzible Elemente in $\mathcal{O}_K$ geben, die nicht prim sind. Ein Beispiel dafür ist $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} \overset{1.14}{=} \mathbb{Z}[\sqrt{-5}]$, 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.*
   Allerdings gilt, dass $\mathcal{O}_K$ stets ein DEDEKIND[9]*-Ring ist, d.h. dass jedes Ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ mit $\mathfrak{a} \neq \{0\}, \mathcal{O}_K$ eine bis auf Reihenfolge eindeutige Zerlegung in Primideale $\mathfrak{p}_1, ..., \mathfrak{p}_r$ besitzt (vgl. [Neu07, (3.3) Theorem],*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r.$$

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 1.12.
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 $p\mathbb{Z}[\sqrt{m}] \trianglelefteq \mathbb{Z}[\sqrt{m}]$ 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 1.13.
Allgemein gibt es 3 Möglichkeiten, wie sich eine Primzahl p aus $\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ verhalten kann. Dazu betrachtet man das Verhalten des von p erzeugten Ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ in Bezug auf Zerlegbarkeit:

1. *$\langle p\rangle_{\mathcal{O}_{\mathbb{Q}(\sqrt{m})}} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ ist selbst ein Primideal.*

2. *Es ist $\langle p\rangle_{\mathcal{O}_{\mathbb{Q}(\sqrt{m})}} = \mathfrak{p}\overline{\mathfrak{p}}$, wobei $\mathfrak{p} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ ein Primideal ist und $\overline{\mathfrak{p}} := \{\overline{\alpha} \mid \alpha \in \mathfrak{p}\} \neq \mathfrak{p}$.*

3. *Es ist $\langle p\rangle_{\mathcal{O}_{\mathbb{Q}(\sqrt{m})}} = \mathfrak{p}^2$ für ein Primideal $\mathfrak{p} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$.*

*Im ersten Fall heißt $\langle p\rangle_{\mathcal{O}_{\mathbb{Q}(\sqrt{m})}}$ **träge**, im zweiten Fall **zerlegt** und im dritten Fall heißt $\langle p\rangle_{\mathcal{O}_{\mathbb{Q}(\sqrt{m})}}$ **verzweigt**. Es gilt, dass $\langle p\rangle_{\mathcal{O}_{\mathbb{Q}(\sqrt{m})}}$ höchstens dann verzweigt sein kann, wenn $p \mid 2m$.*

[9] JULIUS WILHELM RICHARD DEDEKIND, 1831-1916, dt. Mathematiker, algebraische Zahlentheorie, Gruppentheorie

Lemma 1.14.
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. Sei $\alpha = a + b\sqrt{m} \in \mathcal{O}_K$. Dann ist das Minimalpolynom von α über $\mathbb{Q}$ gerade

$$\mu_{\alpha,\mathbb{Q}}(x) = x^2 + 2ax + (a^2 - b^2 m) \in \mathbb{Z}[x].$$

Damit ist also $2a \in \mathbb{Z}$.
Ist $a \in \mathbb{Z}$, so folgt wegen $a^2 - b^2 m \in \mathbb{Z}$ auch $b^2 m \in \mathbb{Z}$. Da m quadratfrei ist, muss daher $b \in \mathbb{Z}$ gelten.
Ist $a = \frac{u}{2}$ mit $u \in \mathbb{Z}$ ungerade und $b = \frac{x}{2}$. Dann ist auch $\frac{1}{4}(u^2 - dx^2) \in \mathbb{Z}$, was aber erzwingt, dass auch x^2 und damit x ungerade ist. Also haben wir

$$x^2 \equiv u^2 \equiv 1 \pmod 4.$$

In diesem Fall folgt unmittelbar $m \equiv 1 \pmod 4$ und damit die Behauptung. □

Der folgende Satz stammt von Dirichlet[10].

Satz 1.15. Dirichlet***scher Einheitensatz***
Sei K ein algebraischer Zahlkörper, also eine endliche Körpererweiterung von $\mathbb{Q}$. Dann gilt für die Einheitengruppe des Ganzheitsrings von K

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

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 $c(X) = X^n - 1$.

Beweis. Siehe [Neu07, (7.4) Theorem] □

Korollar 1.16.
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****.*

[10] Peter Gustav Lejeune Dirichlet, 1805-1859, dt. Mathematiker, Analysis und Zahlentheorie

Kapitel 2

Elliptische Kurven

2.1 Geometrie elliptischer Kurven

Ein Ziel dieser Arbeit wird es sein, elliptische Kurven für Primzahl-Tests zu verwenden. 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 [Sil86], [ST92], [Hus87] oder [Wer01] angegeben.

Definition 2.1.
Es sei K ein Körper, $\overline{K}$ der algebraische Abschluss von K und

$$\mathcal{P}_2(K) := \left\{ \langle \begin{pmatrix} a \\ b \\ c \end{pmatrix} \langle = [a:b:c] \mid \begin{pmatrix} a \\ b \\ c \end{pmatrix} \in K^3 \setminus \{0\} \right\}$$

der 2-dimensionale projektive 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 $\mathcal{C}_f$ bezeichnet wird.*
   Zu einem Erweiterungskörper L von K bezeichnet

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

   *die Menge der L-**rationalen Punkte** von $\mathcal{C}_f$.*

2. *Eine projektive ebene Kurve $\mathcal{C}_f$ heißt **singulär** im Punkt*

   $$P = [a:b:c] \in \mathcal{C}_f(L),$$

   falls alle formalen 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. *Die Kurve $\mathcal{C}_f$ heißt **nicht-singulär**, wenn $\mathcal{C}_f$ 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 E_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 die Weierstrass[1]-***Gleichung*** *der elliptischen Kurve, f nennt man das* Weierstrass-***Polynom*** *der elliptischen Kurve.*

2. *Unter der **Diskriminante** beziehungsweise der j**-Invariante** einer elliptischen Kurve E_f versteht man den Ausdruck*

$$\begin{aligned}\Delta(E_f) &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\ j(E_f) &:= \frac{c_4^3}{\Delta(E_f)},\end{aligned}$$

wobei die Koeffizienten b_j und c_4 gegeben sind durch

$$\begin{aligned}b_2 &= a_1^2 + 4a_2,\\ b_4 &= 2a_4 + a_1a_3,\\ b_6 &= a_3^2 + 4a_6\\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2\\ c_4 &= b_2^2 - 24b_4.\end{aligned}$$

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

3. *Sei K ein algebraischer Zahlkörper und $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ ein Primideal. Dann bezeichnet $\widehat{E}_f$ 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 $\widehat{E}_f$ 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 Definition 2.2 1. eine elliptische Kurve. Einen einfachen Test auf Singularität von E_f liefert das folgende

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

[1] Karl Theodor Wilhelm Weierstrass, 1815-1897, dt. Mathematiker, Analysis, Funktionentheorie, Variationsrechnung

BEWEIS. Siehe [Wer01, 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:*

$$\begin{aligned} E_f(K) &= Null_a(f) \cup \{\mathcal{O}\} \\ &= \{(x, y) \in K \times K \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}. \end{aligned}$$

In diesem Sinne lassen sich elliptische Kurven als affine Varietäten betrachten:

Bemerkung 2.6.
Sei E_f eine elliptische Kurve über einem Körper K mit WEIERSTRASS*-Polynom f. Dann ist*

$$I(E_f) := \{g \in \overline{K}[x, y] \mid g(P) = 0 \quad \forall P \in E_f\}$$

ein Primideal in $\overline{K}[x, y]$. Damit ist E_f eine affine Varietät.

Dies gibt Anlass zu folgender

Definition 2.7.
Sei E_f eine elliptische Kurve über einem Körper K mit WEIERSTRASS*-Polynom f. Dann heißt*

$$K[E_f] := K[x, y]/I(E_f)$$

der ***Koordinatenring*** *von E_f. Dieser ist ein Integritätsbereich (denn $I(E_f) \trianglelefteq K[x, y]$ ist ein Primideal) und sein Quotientenkörper $K(E_f)$ heißt der* ***Funktionenkörper*** *von E_f über K.*

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 $E_f(L)$ die Struktur einer ABELschen[2] Gruppe erklären:

Satz 2.8.
Es sei K ein Körper $E_f(L)$ 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 $P_1, P_2 \in E_f(L) \setminus \{\mathcal{O}\}$, mit $P_i = (x_i, y_i)$. $E_f(L)$ wird zu einer* ABEL*schen Gruppe mit Verknüpfung + und neutralem Element $\mathcal{O}$ durch*

$$\begin{aligned}
-P_1 &= (x_1, -y_1 - a_1x_1 - a_3),\\
P_1 + P_2 &:= (x_3, y_3) \text{ wobei}\\
x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2\\
y_3 &= -(\lambda + a_1)x_3 - \nu - a_3\\
\lambda &= \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{falls } x_1 \neq x_2 \\ \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3} & \text{falls } x_1 = x_2 \end{cases}\\
\nu &= \begin{cases} \frac{y_1x_2-y_2x_1}{x_2-x_1} & \text{falls } x_1 \neq x_2 \\ \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3} & \text{falls } x_1 = x_2 \end{cases}.
\end{aligned}$$

Korollar 2.9.

1. *In der Situation von Satz 2.8 gilt, falls $a_1 = a_2 = a_3 = 0$ und $\mathrm{char}(K) \neq 2, 3$ gilt, für die x-Koordinate $x(2P)$ eines Punktes $2P := P + P \neq \mathcal{O}$ mit $P = (x, y)$ auf E_f die Beziehung*
$$x(2P) = \frac{x^4 - 2a_4x^2 - 8a_6x + a_4^2 - 4a_2a_6}{4x^3 + 4a_4x + 4a_6}$$

2. *Ist in 1. zusätzlich $3P := P + P + P \neq \mathcal{O}$, so ist*
$$x(3P) = x - \frac{8(x^3 + a_4x + a_6)(x^6 + 5a_4x^4 + 20a_6x^3 - 5a_4^2x^2 - 4a_4a_6x - 8a_6^2 - a_4^3)}{(3x^4 + 6a_4x^2 + 12a_6x - a_4^2)^2}$$

BEWEIS. ad 1.: Einsetzen von $P_1 = P_2 = P$ in Satz 2.8 liefert unter ausnutzen der Beziehung $y^2 = x^3 + a_4x + a_6$ die Behauptung:

$$\begin{aligned}
x(2P) =& \frac{(3x^2 + a_4)^2 - 4(2x)y^2}{4y^2}\\
=& \frac{9x^4 + 6a_4x^2 + a_4^2 - (8x^4 - 8a_4x^2 - 8a_6x)}{4x^3 + 4a_4x + 4a_6}\\
=& \frac{x^4 - 2a_4x^2 - 8a_6x + a_4^2}{4x^3 + 4a_4x + 4a_6}.
\end{aligned}$$

[2] NIELS HENRIK ABEL, 1802-1831, norweg. Mathematiker, elliptische Integrale und Funktionen, Begründung der Gruppentheorie

ad 2.: Es ist $3P = 2P + P$, also folgt mit Satz 2.8

$$\begin{aligned} x(3P) = x(2P+P) &= \frac{y(2P)^2 + y^2 - 2\cdot y(2P)\cdot y}{x(2P)^2 + x^2 - 2\cdot x(2P)\cdot x} - x(2P) - x \\ &= \frac{[x(2P)^3 + a_4\cdot x(2P) + a_6] + [x^3 + a_4x + a_6]}{x(2P)^2 + x^2 - 2\cdot x(2P)\cdot x} \\ &+ \frac{2\cdot\frac{1}{2}([3x^2 + a_4]\cdot x(2P) - x^3 + a_4x + 2a_6)}{x(2P)^2 + x^2 - 2\cdot x(2P)\cdot x} \\ &- x(2P) - x. \end{aligned}$$

Benutzt man nun Punkt 1 liefert eine leichte, aber lange Rechnung die Behauptung. □

Allgemeiner gilt der

Satz 2.10.

1. *Sei E_f eine elliptische Kurve über einem Körper K mit $char(K) \neq 2, 3$ mit $f(x,y) = y^2 - x^3 - a_4x - a_6 \in K[x,y]$. Wir definieren die **Divisionspolynome** rekursiv vermöge*

$$\begin{aligned} \psi_0 &= 0, \qquad \psi_1 = 1, \qquad \psi_2 = 2y, \\ \psi_3 &= 3x^4 + 6a_4x^2 + 12a_6x - a_4^2, \\ \psi_4 &= 4y(x^6 + 5a_4x^4 + 20a_6x^3 - 5a_4^2x^2 - 4a_4a_6x - 8a_6^2 - a_4^3), \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad (m \geq 2), \\ 2y\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad (m \geq 3). \end{aligned}$$

   Dann ist ψ_n für ungerades n bzw. ψ_n/y für gerades n Polynome in x.

2. *Fasst man nun E_f als $\mathbb{Z}$-Modul auf (vgl. Beispiel 2.16) und ist $P = (x,y)$ ein Punkt von E_f mit $mP \neq \mathcal{O}$, $m \in \mathbb{N}$, so gilt:*

$$mP = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{2m}}{2\psi_m^4}\right).$$

Beweis. ad 1.: Die Behauptung ist offensichtlich für $n \leq 4$.
Sei nun die Behauptung für alle $k < n$ für ein n gezeigt.
Ist $n = 2m + 1$, so ist

$$\psi_n = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3.$$

Dann ist o.B.d.A. m ungerade (ansonsten argumentiere man genauso), also ist nach Induktionsvoraussetzung $\psi_{m+2}\psi_m^3$ ein Polynom in x und es ist ψ_{m-1}, $\psi_{m+1} \in yK[x]$, demnach ist $\psi_{m-1}\psi_{m+1}^3 \in y^4K[x]$. Fasst man die Polynome nun in Koordinatenring von E_f auf, so kann y^2 durch $x^3 + a_4x + a_6$ ersetzt werden und die Behauptung folgt.
Ist nun $n = 2m$, so ist

$$2y\psi_n = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).$$

Für gerades m folgt dann nach Induktionsvoraussetzung, dass $\psi_m, \psi_{m\pm2} \in yK[x]$ und $\psi m \pm 1 \in K[x]$, also ist $\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \in y^2K[x]$, also gilt $\psi_n \in yK[x]$. Für ungerades m argumentiere man analog.
ad 2.: Für $m = 1$ ist die Behauptung klar.
Sei die Behauptung für ein $m \in \mathbb{N}$ wahr, dann folgt für $(m+1)P \neq \mathcal{O}$ die Behauptung durch elementares Nachrechnen unter Verwendung von $(m+1)P = mP + P$ und Satz 2.8. □

Ein analytischer Beweis von Satz 2.10 nebst einer Herleitung der Definition der Divisionspolynome findet sich z.B. in [Lan78, Chapter 2, §§1-2]. Dort wird allerdings einige hier nicht eingeführte Theorie, wie analytische Eigenschaften der WEIERSTRASSschen $\wp$-Funktion, verwendet.

Bemerkung 2.11.
Oft wird, sofern $\mathrm{char}(K) \neq 2, 3$ *gilt, 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* $P_1 + P_2 = (x_3, y_3)$ *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* $P + P = \mathcal{O}$ *(vgl. Lemma 2.13).*

Bemerkung 2.12.
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 2.1). Im Fall* $P = Q$ *tut man dasselbe mit der Tangente an* $E(\mathbb{R})$ *in* P*. Dies bezeichnet man auch als Quadrieren von* P *(vgl. Abbildung 2.2). 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.*

Diese Werkzeuge reichen aus, um die Punkte von Ordnung 2 einer elliptischen Kurve zu charakterisieren, also Punkte P mit $2P := P + P = \mathcal{O}$ (vgl. [ST92]).

Lemma 2.13.
Sei E_f *eine elliptische Kurve mit* WEIERSTRASS*-Polynom* $f(x, y) = y^2 - x^3 - a_2x^2 - a_4x - a_6$*. Beachte, dass die Koeffizienten* a_1 *und* a_3 *hier nicht auftrteten. Sei weiterhin* $P = (x, y)$ *ein Punkt auf* $E_f \setminus \{\mathcal{O}\}$*. Dann gilt:*

Der Punkt P *hat genau dann Ordnung 2 in* E_f*, wenn* $y = 0$ *gilt.*

BEWEIS. Der Punkt P hat genau dann Ordnung 2 in E_f, wenn er die Gleichung $P = -P$ erfüllt. Laut Satz 2.8 ist für $P = (x, y)$ das Inverse $-P = (x, -y)$, also ist

$$P = -P \quad \Leftrightarrow \quad y = 0.$$

□

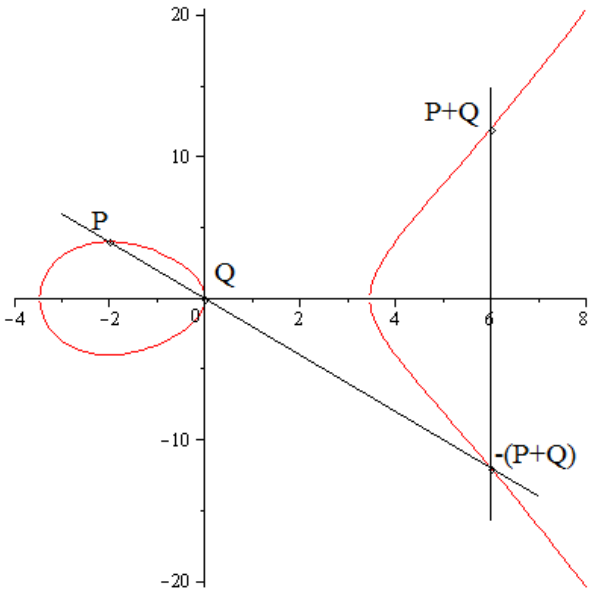

Abbildung 2.1: Addition zweier verschiedener Punkte auf einer elliptischen Kurve

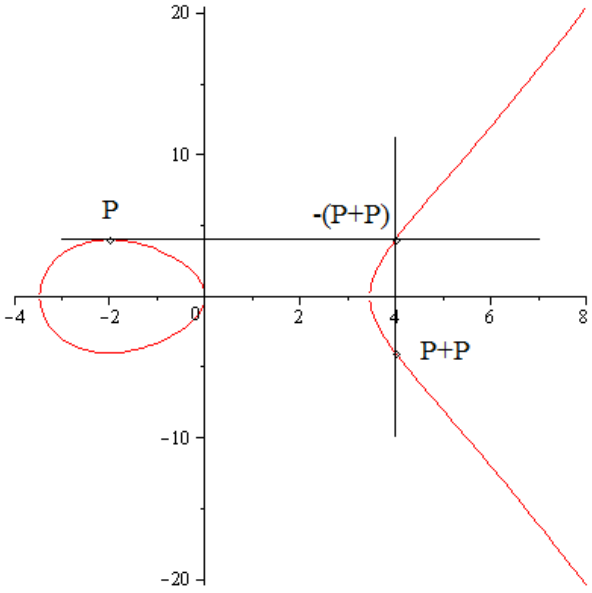

Abbildung 2.2: Quadrieren eines Punktes auf einer elliptischen Kurve

2.3 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 2.14.
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 2.15.

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 2.16.

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

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

   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[3]-Endomorphismus (s.u.) im Falle eines endlichen Grundkörpers ist eine Isogenie. Umgekehrt ist auch jede Isogenie ein Gruppenhomomorphismus (vgl. [Sil86, Theorem V.4.8]).

Lemma 2.17.
Sei $K = \mathbb{F}_q$ ein Körper der Charakteristik $p \in \mathbb{P}$, $q = p^r$ und E_f eine elliptische Kurve über K. Dann gilt: Die Abbildung

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

definiert einen Gruppenhomomorphismus

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

Φ_r heißt der FROBENIUS-***Endomorphismus*** *.*

BEWEIS. Dass Φ_r 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

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

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

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

Damit ist also $\Phi_r(P) \in E_f(\overline{K})$, demnach ist die Einschränkung wohldefiniert. Damit ist Φ_r eine Isogenie, also nach Beispiel 2.15.2 ein Gruppenhomomorphismus. □

Definition 2.18.
Seien E_1 und E_2 elliptische Kurven über einem Körper K und $\phi : E_1 \to E_2$ eine nichtkonstante rationale Abbildung über K. Dann haben wir eine Injektion der Funktionenkörper

$$\phi^* : K(E_1) \to K(E_2),\ f \mapsto f \circ \phi.$$

[3]FERDINAND GEORG FROBENIUS, 1849-1917, dt. Mathematiker, Gruppen- und Darstellungstheorie

1. *Der* ***Grad*** *von ϕ ist* 0*, falls ϕ konstant ist. Anderenfalls ist*

$$\mathrm{Grad}(\phi) := [K(E_1) : \phi^* K(E_2)]$$

der Grad der (endlichen) Körpererweiterung $K(E_1)/\phi^* K(E_2)$ (für den Beweis der Endlichkeit von $[K(E_1) : \phi^* K(E_2)]$ vgl. [Har77, II.6.8]).

2. *Die Abbildung ϕ heißt* ***separabel*** *(****inseparabel****, **rein inseparabel**), falls dies entsprechend für die Körpererweiterung $K(E_1)/\phi^*(K(E_2))$ gilt.*

Lemma 2.19.
Sei $K = \mathbb{F}_q$ ein Körper der Charakteristik $p > 0$ mit $q = p^r$ und E_f eine elliptische Kurve über K. Dann gilt für den Frobenius*-Endomorphismus $\Phi_r : E_f \to E_f$ von E und $m, n \in \mathbb{Z}$. Dann ist die Isogenie*

$$m + n\Phi_r : E_f \to E_f$$

genau dann separabel, wenn $p \nmid m$.

Beweis. Siehe [Sil86, Corollary III.5.5]. □

Lemma 2.20.
Seien E_f, E_g elliptische Kurven über einem Körper K und $\phi : E_f \to E_g$ eine nichtkonstante, separable Isogenie. Dann ist

$$|\mathrm{Kern}(\phi)| = \mathrm{Grad}(\phi)$$

Beweis. Siehe [Sil86, Theorem III.4.10 (c)]. □

Satz 2.21.
Sei $\phi : E_1 \to E_2$ eine nicht-konstante Isogenie zwischen zwei elliptischen Kurven E_1 und E_2 über einem Körper K. Sei weiterhin $\mathrm{Grad}(\phi) = m$. Dann gibt es eine eindeutig bestimmte Isogenie

$$\widehat{\phi} : E_2 \to E_1$$

mit

$$\widehat{\phi} \circ \phi = [m].$$

Beweis. Siehe [Sil86, III.6.1]. □

Definition 2.22.
Die Abbildung $\widehat{\phi} : E_2 \to E_1$ aus Satz 2.21 heißt die zu ϕ ***duale Isogenie****.*

Wir brauchen später ein paar elementare Eigenschaften der Grad-Funktion, die wir in folgendem Lemma festhalten:

Lemma 2.23.
Sei E_f eine elliptische Kurve über einem Körper K und $\phi, \psi \in \mathrm{End}(E_f)$ seien Isogenien von E_f. Dann gilt

1. *Die Abbildung*

$$\mathrm{Grad} : \mathrm{End}(E_f) \to \mathbb{Z}$$

ist eine positiv definite quadratische Form auf dem $\mathbb{Z}$-Modul $\mathrm{End}(E_f)$.

2. *Für $m \in \mathbb{Z}$ ist $\mathrm{Grad}([m]) = m^2$.*

3. *Ist $K = \mathbb{F}_q$ mit $q = p^r$, so ist $\mathrm{Grad}(\Phi_r) = q$.*

BEWEIS. ad 1.: Siehe [Sil86, Corollary III.6.3].
ad 2.: Siehe [Sil86, Theorem III.6.2(d)].
ad 3.: Siehe [Sil86, Proposition II2.11(c)]. □

Korollar 2.24. *Sei $m \in \mathbb{Z} \setminus \{0\}$ und E_f eine elliptische Kurve über einem Körper K.*

1. *Ist* $\mathrm{char}(K) = 0$ *oder* $\mathrm{ggT}(m, \mathrm{char}(K)) = 1$, *so ist*

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

2. *Ist* $\mathrm{char}(K) = p > 0$, *dann ist entweder*

$$\mathrm{Kern}([p^r]) = \{\mathcal{O}\} \qquad \textit{für alle } r \geq 1$$

oder

$$\mathrm{Kern}([p^r]) \cong \mathbb{Z}/p^r\mathbb{Z} \qquad \textit{für alle } r \geq 1.$$

BEWEIS. ad 1.: Nach Voraussetzung ist gemäß Lemma 2.19 die Abbildung $[m]$ separabel und es ist $\mathrm{Grad}([m]) = m^2$. Mit Lemma 2.20 folgt daher

$$|\mathrm{Kern}([m])| = m^2.$$

Entsprechendes gilt auch für jedes d mit $d \mid m$. Schreibt man nun $\mathrm{Kern}([m])$ als Produkt von zyklischen Gruppen, so folgt aus Ordnungsgründen, dass

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

ad 2.: Siehe [Sil86, Corollary III.6.4 (c)]. □

Definition 2.25. *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 ein endlich erzeugter freier $\mathbb{Z}$-Modul vom Rang 2 respektive 4, der zugleich eine ein Teilring von $\mathbb{Q}(\sqrt{d})$ bzw. $\left(\frac{a,b}{\mathbb{Q}}\right)$ ist.*

Bemerkung 2.26.

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

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

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.*

Im Beweis zu Proposition 3.7 wird die Weil[4]-Paarung verwendet. Zur Erläuterung dessen dient der folgende

Satz 2.27.
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, also*

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

2. *e_m ist alternierend, also $e_m(S,T) = e_m(T,S)^{-1}$*

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 verträglich mit der Operation der* Galois[5]*-Gruppe*

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

   das bedeutet für $\sigma \in \mathrm{Gal}_{\overline{K}/K}$ ist

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

5. *Es gilt für $S \in \mathrm{Kern}([mm'])$ und $T \in \mathrm{Kern}([m])$*

$$e_{mm'}(S,T) = e_m([m']S, T).$$

   Man sagt, e_m und $e_{mm'}$ sind kompatibel.

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

Beweis. Siehe [Sil86, Theorem III.8.1]. □

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. [Hus87, Chapter 1, Theorem (4.1)]).

Satz 2.28.
Es sei $E_f(K)$ eine elliptische Kurve über einem Körper K ($\mathrm{char}(K) \neq 2$) mit Weierstrass*-Polynom*

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

wobei $\alpha, \beta, \gamma \in K$ seien.
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.

[4] André Weil, 1906-1998, frz. Mathematiker, algebraische Geometrie, Zahlentheorie
[5] Évariste Galois, 1811-1832, frz. Mathematiker, Begründung der Galois- und Gruppentheorie

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

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

wobei hier u als zusätzliche Unbekannte eingefügt wurde. 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 $L := K(\alpha', \beta', \gamma')$ von K gibt.
Zieht man nun die Quadratwurzel aus der letzten Gleichung, so erhält man schließlich

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

Zieht man nun auf beiden Seiten die Quadratwurzel, so erhält man für λ vier Lösungen

$$\begin{aligned} \lambda_1 &= \alpha' + \beta' - \gamma', & \lambda_2 &= \alpha' - \beta' + \gamma', \\ \lambda_3 &= -\alpha' + \beta' + \gamma', & \lambda_4 &= -\alpha' - \beta' - \gamma' \end{aligned}$$

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 Bedingung $2Q = (0, y')$ erfüllt.
Sind also $\alpha', \beta', \gamma' \in K$, so auch jede mögliche Lösung für λ, also auch x und y.
Ist umgekehrt ohne Beschränkung der Allgemeinheit $\lambda_1 \in K$, dann teilt $(X - \lambda_1)$ das Polynom $p(X) = (X^2 - a)^2 - 4(b - 2y'X)$ in $K[X]$ (vgl. $(*)$) und offenbar zerfällt $p(X)$ in $L[X]$ in Linearfaktoren. Weiterhin gilt $[L : K] \mid 8$. Nun zerfällt auch $q(X) := \frac{p(X)}{X - \lambda_1}$ in $L[X]$ in Linearfaktoren und hat Grad 3, sodass aus wenigstens eine weitere Wurzel von $p(X)$ in K liegen muss, ansonsten müsste es einen Körper E mit $K \leq E \leq L$ mit $[E : K] = 3$ und das kann nicht sein. Sei o.B.d.A. $\lambda_2 \in K$. Dann ist auch

$$\lambda_1 + \lambda_2 = 2\alpha' \in K$$

und damit auch α', denn $char(K) \neq 2$. Weiterhin gilt

$$\frac{\lambda_1 - \lambda_2}{2} = \beta' - \gamma' \in K,$$

sagen wir $\gamma' = c + \beta'$ mit $c \in K$. Nach Voraussetzung ist

$$-\gamma = \gamma'^2 = c^2 - \beta + 2c\beta' \in K,$$

also auch $\beta' \in K$ und damit ist $\gamma' \in K$. Damit ist gezeigt, dass $-\alpha, -\beta, -\gamma$ Quadrate in K sind und so auch die Behauptung. $\square$

2.4 Supersingularität und Kombinatorik

Eine wichtige Eigenschaft mancher elliptischer Kurven über endlichen Körpern ist die Supersingularität. So werden wir diese Eigenschaft einer bestimmten Kurve kombiniert mit der HASSE-Ungleichung ausnutzen, um die $\mathbb{F}_p$-rationalen Punkte dieser Kurve zu zählen.
Zur Definition der Supersingularität benötigen wir zunächst noch ein wenig Vorarbeit.

Definition 2.29.
Es sei $K = \mathbb{F}_q$ ein endlicher Körper der Charakteristik p mit $q = p^r$ und E_f eine elliptische Kurve über K. Der Ausdruck

$$\mathrm{Spur}(\Phi_r) = q + 1 - |E_f(K)|$$

*heißt die **Spur** des* FROBENIUS*-Endomorphismus.*

Satz 2.30.
Sei K ein Körper der Charakteristik $p > 0$, $f \in K[x]$ das WEIERSTRASS*-Polynom der elliptischen Kurve E_f über K und für $r \in \mathbb{N}$ sei*

$$\Phi_r : E_f \to (E_f)^{p^r}$$

*die p^r-*FROBENIUS*-Abbildung. Dann sind folgende Aussagen äquivalent*

1. $\mathrm{Kern}(\Phi_r) = \{0\}$ *für ein $r \in \mathbb{N}$.*
2. $\widehat{\Phi}_r$ *ist inseparabel für ein $r \in \mathbb{N}$.*
3. *Die Abbildung $[p] : E_f \to E_f$ ist rein inseparabel und es gilt $j(E_f) \in \mathbb{F}_{p^2}$.*
4. $\mathrm{End}(E_f)$ *ist eine Ordnung in einer Quaternionenalgebra.*

Ist K zusätzlich perfekt, so lassen sich Aussagen 1. und 2. ersetzen durch

1' $\mathrm{Kern}(\Phi_r) = \{0\}$ *für alle $r \in \mathbb{N}$.*

2' $\widehat{\Phi}_r$ *ist rein inseparabel für alle $r \in \mathbb{N}$.*

BEWEIS. Siehe [Sil86, Theorem V.3.1] und [Deu41]. □

Definition 2.31.
*Hat eine elliptische Kurve E_f eine der Eigenschaften aus Satz 2.30, so heißt E_f **supersingulär**. Anderenfalls heißt E_f **gewöhnlich**.*

Für eine alternative Einführung der Supersingularität und Herleitung der Behauptungen in Satz 2.30 sei auf [Hus87, Chapter 13, §§3, 5, 6], dort insbesondere Proposition 3.8, Proposition 5.6 , Proposition 6.2 und Theorem 6.3, verwiesen.

Bemerkung 2.32. *Der Begriff „supersingulär“ hat nichts mit „singulär“ zu tun. Eine elliptische Kurve über einem endlichen Körper ist per Definition nicht singulär, kann aber sehr wohl supersingulär sein.*

Der folgende Satz bietet eine Charakterisierung für Supersingularität, die sich im Folgenden als praktisch erweisen wird.

Satz 2.33.
Sei $K = \mathbb{F}_p$ für ein $p \in \mathbb{P}$ und E_f eine elliptische Kurve über K. Weiterhin sei Φ_r wie in Satz 2.30.

1. *Die Kurve E_f ist genau dann supersingulär, wenn*
$$\mathrm{Spur}(\Phi_r) \equiv 0 \pmod{p}.$$
2. *Ist $r = 1$, so ist E_f genau dann supersingulär, wenn*
$$|E_f(\mathbb{F}_p)| = p + 1.$$

Beweis. Über die Injektion
$$[\ \ ] : \mathbb{Z} \to \mathrm{End}(E_f)$$
lässt sich $\mathbb{Z}$ als Teilmenge von $\mathrm{End}(E_f)$ auffassen.

1. Sei nun $t := \Phi_r + \widehat{\Phi}_r \in \mathrm{End}(E_f)$. Dann gilt
$$[0] = (\Phi_r - \Phi_r) \circ (\Phi_r - \widehat{\Phi}_r) = \Phi_r^2 - t\Phi_r + [q],$$
denn $\mathrm{Grad}(\Phi_r) = q$ mit $q := p^r$. Es ist $\mathbb{F}_q$ der Fixkörper von Φ_r, also folgt unmittelbar, dass
$$E_f(\mathbb{F}_q) = \mathrm{Kern}(\Phi_r - 1).$$
Mit Lemma 2.19 folgt nun, dass $\Phi_r - 1$ separabel ist und mit Lemma 2.20, dass
$$|E_f(\mathbb{F}_q)| = |\mathrm{Kern}(\Phi_r - 1)| = \mathrm{Grad}(\Phi_r - 1) = (\Phi_r - 1) \circ (\widehat{\Phi}_r - 1) = q - t + 1.$$
Damit ist offenbar nach Definition 2.29 damit $t = \mathrm{Spur}(\Phi_r) \in \mathbb{Z}$ und $\widehat{\Phi}_r$ ist genau dann rein inseparabel, wenn $t \equiv 0 \pmod{p}$. Mit Satz 2.30 folgt dann die Behauptung.
2. folgt für $r = 1$ und $p = q$ aus 1.

□

Der folgende wichtige Satz wurde von Hasse[6] im Jahre 1931 bewiesen.

Satz 2.34. Hasse***sche Ungleichung***
Es sei $K = \mathbb{F}_q$ ein Körper der Charakteristik $p \in \mathbb{P} \setminus \{2\}$ 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. Nach dem Beweis von Satz 2.33 ist für $q = p^r$
$$[t] := [\mathrm{Spur}(\Phi_r)] = \Phi_r + \widehat{\Phi}_r.$$
Also sind auch die Grade dieser Isogenien gleich. Mit Lemma 2.23 ist dann also
$$\mathrm{Spur}(\Phi_r)^2 = \mathrm{Grad}(\Phi_r + \widehat{\Phi}_r) = \mathrm{Grad}(\Phi_r) + \mathrm{Grad}(\widehat{\Phi}_r) - \langle \Phi_r, \widehat{\Phi}_r \rangle,$$

[6] Helmut Hasse, 1898-1979, dt. Mathematiker, algebraische Zahlentheorie, Klassenkörpertheorie

wobei $\langle \cdot, \cdot \rangle$ die zu der positiv definiten quadratischen Form Grad gehörige Bilinearform bezeichne. Also ist für alle $m, n \in \mathbb{Z}$ und $\phi, \psi \in \mathrm{End}(E_f)$ folgendes richtig:

$$0 \leq \mathrm{Grad}(m\psi - n\phi) = m^2 \,\mathrm{Grad}(\psi) + mn\langle \psi, \phi \rangle + n^2 \,\mathrm{Grad}(\phi),$$

insbesondere gilt also für $m = -\langle \psi, \phi \rangle$ und $n = 2\,\mathrm{Grad}(\psi)$ also

$$0 \leq \mathrm{Grad}(\psi)[4\,\mathrm{Grad}(\psi)\,\mathrm{Grad}(\phi) - \langle \psi, \phi \rangle^2],$$

woraus für $\psi \neq 0$

$$|\langle \psi, \phi \rangle| \leq 2\sqrt{\mathrm{Grad}(\psi)\,\mathrm{Grad}(\phi)}$$

folgt. In unserem Fall gilt also (beachte $\mathrm{Grad}(\Phi_r) = q$):

$$\mathrm{Spur}(\Phi_r)^2 \leq 2q + 2\sqrt{q \cdot q} \Leftrightarrow |\mathrm{Spur}(\Phi_r)| \leq 2\sqrt{q}.$$

Nach der Definition von $\mathrm{Spur}(\Phi_r)$ folgt die Behauptung. □

Lemma 2.35.
Sei $q \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl und E_f eine supersinguläre elliptische Kurve über $\mathbb{F}_q$. Dann ist die Gruppe der $\mathbb{F}_q$-rationalen Punkte von E entweder zyklisch oder enthält eine Untergruppe, die isomorph ist zu $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Beweis. Nach Korollar 2.24 ist für jedes $m \in \mathbb{Z}$ mit $\mathrm{ggT}(m, q) = 1$

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

Da E_f nach Voraussetzung supersingulär ist, folgt mit Satz 2.33, dass $|E(q)| = q + 1$, wobei $E(q) := E_f(\mathbb{F}_q)$. Nach dem Strukturssatz über endlich erzeugte Abelsche Gruppen ist also

$$E(q) \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \text{ mit } d_1 \,|\, d_2 \text{ und } d_1 \cdot d_2 = |E(q)| = q + 1,$$

denn $E(q)$ ist eine Untergruppe von $\mathrm{Kern}([q+1]) \cong (\mathbb{Z}/(q+1)\mathbb{Z}) \times (\mathbb{Z}/(q+1)\mathbb{Z})$.
Des Weiteren ist d_1 ein Teiler von $|\mathbb{F}_q^*|$. Das folgt aus der Surjektivität und der Verträglichkeit mit der Operation der Galois-Gruppe $\mathrm{Gal}_{\overline{\mathbb{F}_q}/\mathbb{F}_q}$ der Weil-Paarung. Es gibt dann nämlich $S, T \in \mathrm{Kern}([d_1]) \cap E(q) = \mathrm{Kern}([d_1])$ mit $e_{d_1}(S, T) = \zeta$, wo $\zeta \in \overline{\mathbb{F}_q}$ eine primitive d_1-te Einheitswurzel ist. Lässt man nun $\sigma \in \mathrm{Gal}_{\overline{\mathbb{F}_q}/\mathbb{F}_q}$ auf beiden Seiten operieren, so folgt, da sich die linke Seite der Gleichung nicht ändert (denn S und T sind $\mathbb{F}_q$-rational), dass $\zeta \in \mathbb{F}_q$. Damit ist dann

$$d_1 = \mathrm{ord}(\zeta) \mid |\mathbb{F}_q^*| = q - 1.$$

Also gilt $d_1 \mid \mathrm{ggT}(q-1, q+1) = 2$. Also ist $E(q)$ entweder zyklisch (für $d_1 = 1$) oder enthält eine Untergruppe isomorph zu $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Das war die Behauptung. □

2.4.1 Beispiel: Elliptische Kurven mit Gleichung $y^2 = x^3 - ax$

Im Folgenden wird hauptsächlich mit Kurven der Form E_a mit Weierstrass-Gleichung $y^2 = x^3 - ax$, $a \in \mathbb{Z} \setminus \{0\}$ über $\mathbb{Q}$ und deren Reduktionen modulo gewisser Primzahlen $q \in \mathbb{P}$ gearbeitet werden. Daher halten wir hier einige Eigenschaften dieser Kurven fest. Man sieht z.B. unmittelbar, dass E_a aufgefasst über dem Körper $\mathbb{Q}(i)$ komplexe Multiplikation durch die ganzen Gausszschen Zahlen $\mathbb{Z}[i]$ hat vermöge

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

Weiterhin ist $\Delta(E_a) = 2^6 \cdot a^3$, so dass E_a gute Reduktion modulo $q \in \mathbb{P}$ besitzt, falls $q \nmid a$. Daraus resultiert das folgende

Lemma 2.36.
Es sei $q \in \mathbb{P}$ mit $q \equiv -1 \pmod 4$ und $q \nmid a$. Dann ist die Reduktion $\widehat{E}_a$ von E_a modulo q supersingulär und es gibt genau $q+1$ $\mathbb{F}_q$-rationale Punkte von $\widehat{E}_a$, also

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

Beweis. Nach Satz 2.33 reicht es zu zeigen, dass $\widehat{E}_a$ supersingulär ist.
Die Abbildung $[i]$ lässt sich ebenfalls reduzieren, indem man unter i eine primitive vierte Einheitswurzel in $\overline{\mathbb{F}_q}^*$ versteht.
Sei nun Φ der Frobenius-Endomorphismus von $\mathbb{F}_q$. Dann ist

$$(\Phi \circ [i])(P) = (-x^q, i^q y^q) \quad \text{und} \quad ([i] \circ \Phi)(P) = (-x^q, iy^q)$$

für jeden Punkt $P = (x, y)$ von $\widehat{E}_a$.
Es ist aber $q \equiv -1 \pmod 4$, also ist $i^q = -i \neq i$. Das heißt, dass $\mathrm{End}(\widehat{E}_a)$ nicht kommutativ ist. Das kann aber nach Bemerkung 2.26 nur dann sein, wenn $\mathrm{End}(\widehat{E}_a)$ isomorph zu einer Ordnung in einer Quaternionenalgebra über $\mathbb{Q}$ ist. Nach Satz 2.30 ist das aber genau dann der Fall, wenn $\widehat{E}_a$ supersingulär ist. □

Mit einer kleinen Einschränkung an den Parameter a erhält man sogar das

Lemma 2.37.
Ist $q \in \mathbb{P}$ eine Primzahl mit $q \equiv -1 \pmod q$ und $a \in \mathbb{Z}$ kein Quadrat modulo q. Dann ist die Punktgruppe der Reduktion elliptischen Kurve E_a modulo q zyklisch, also

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

Beweis. Gemäß Lemma 2.35 gilt, dass $E_a(q)$ entweder wie behauptet zyklisch ist oder eine Untergruppe isomorph zu $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ enthält. Der zweite Fall kann jedoch nicht eintreten, denn dann würde mit Korollar 2.24 und Satz 2.30 folgen, dass alle 2-Torsionspunkte von $E_a(q)$ bereits $\mathbb{F}_q$-rational sind, also alle Wurzeln von $x^3 - ax = x \cdot (x^2 - a)$ in $\mathbb{F}_q$ liegen. Nach Voraussetzung ist a aber kein Quadrat in $\mathbb{F}_q$, also haben wir einen Widerspruch und $E_a(q)$ ist zyklisch. □

Da die Weierstrass-Gleichung hier recht einfach ist, erhält man ganz elementar eine Alternative zu Satz 2.28:

Satz 2.38.
Es sei $\mathcal{O} \neq P = (x_0, y_0)$ ein $\mathbb{F}_q$-rationaler Punkt der Kurve $\widehat{E}_a$ mit $q \in \mathbb{P} \setminus \{2, 3\}$, $q \nmid a$. Falls x_0 kein Quadrat in $\mathbb{F}_q$ ist, so ist auch $(x_0^2 - a)$ kein Quadrat in $\mathbb{F}_q$ und es gibt keinen Punkt $Q \in \widehat{E}_a(\mathbb{F}_q) =: E_a(q)$ mit $2 \cdot Q = P$.

Beweis. Wegen $y_0^2 = x_0(x_0^2 - a)$ muss offenbar, da x_0 ein Nichtquadrat ist, auch $x_0^2 - a$ ein Nichtquadrat sein, ansonsten ist P nicht $\mathbb{F}_q$-rational. Sei nun $\mathbb{Q} = (x, y) \in E_a(q)$ mit $2 \cdot Q \neq \mathcal{O}$. Dann ist nach Korollar 2.9

$$x(2 \cdot Q) = \frac{(x^2 + a)^2}{4x(x^2 - a)},$$

also ein Quadrat in $\mathbb{F}_q$. Insbesondere kann dann der Punkt $P = (x_0, y_0)$ nicht durch 2 teilbar sein. □

Kapitel 3

Mersenne- und Fermat-Primzahlen

3.1 Mersenne-Zahlen

3.1.1 Der Lucas-Lehmer-Test

Wir werden zuächst nach der Methode von Gross den Lucas-Lehmer-Test, den Édouard Lucas 1876 erfunden hat und der von Derrick Henry Lehmer 1935 verbessert wurde, neu interpretieren, nämlich als sukzessives Quadrieren eines Punktes des eindimensionalen algebraischen Torus über $\mathbb{Q}$ zu $\mathbb{Q}(\sqrt{3})$, und beweisen. Dazu betrachten wir den reellquadratischen Zahlkörper $K := \mathbb{Q}(\sqrt{3})$ und seinen Ganzheitsring $R := \mathbb{Z}[\sqrt{3}]$ (vgl. Lemma 1.14). 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 (vgl. Satz 1.15) ist die Einheitengruppe R^* 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 $T(q) \cong C_{q+1}$ zyklisch von Ordnung $q+1$ und ε ist kein Quadrat in $T(q)$.

Beweis. Da $q \equiv 7 \pmod{24}$ ist auch $q \equiv 3 \pmod{4}$ und $q \equiv 1 \pmod{3}$, also gilt mit dem quadratischen Reziprozitätsgesetz (vgl. Satz 1.9)

$$\left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right) \overset{1.9}{=} -\left(\frac{1}{3}\right) = -1,$$

so dass 3 ein quadratischer Nichtrest modulo q ist. Damit ist aber nach Lemma 1.12 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 der nichttriviale Körperautomorphismus $^-$ auf $\mathbb{Q}(\sqrt{3})$ mit $\overline{\sqrt{3}} = -\sqrt{3}$ induziert einen nichttrivialen Körperautomorphismus auf $\mathbb{F}_{q^2} \cong R/qR \cong \mathbb{Z}[x]/(p, x^2 - 3)$. Der einzige nichttriviale Körperautomorphismus von $\mathbb{F}_{q^2}$ ist aber der FROBENIUS-Automorphismus, sodass ν_q die Norm der Körpererweiterung $R/qR \cong \mathbb{F}_{q^2}$ über $\mathbb{F}_q$ ist mit $\nu_q(\alpha) = \alpha^{q+1}$ für $\alpha \in R/qR$. Sei nun $\alpha \in (R/qR)^*$ ein Erzeuger der Gruppe $(R/qR)^*$. Dann hat $\nu_q(\alpha) = \alpha^{q+1} \in \mathbb{F}_q^*$ Ordnung $q - 1 = |\mathbb{F}_q^*|$, ist also ein Erzeuger von $\mathbb{F}_q^*$. Damit ist ν_q surjektiv.
Nun ist $\mathrm{Kern}(\nu_q) = T(q)$, 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[1] Satz 90 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 3.1 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 3.1, also hat $\varepsilon^{\frac{q+1}{2}}$ Ordnung 2.

Wir definieren nun die LUCAS-Folge ganzer Zahlen vermöge

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

Die ersten Werte der Folge sind

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

[1] DAVID HILBERT, 1862-1943, dt. Mathematiker, (algebraische) Geometrie, Zahlentheorie, Logik, math. Physik

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

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

Des Weiteren 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*

$$L_k \not\equiv 0 \pmod{M_p} \text{ für } k \in \{0, ..., p-3\} \text{ und } L_{p-2} \equiv 0 \pmod{M_p}.$$

Umgekehrt gilt, dass M_p prim ist, wenn

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

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 3.1 $T(M_p) = \langle\varepsilon\rangle$ 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 $L_{p-2} = \mathrm{Spur}(\varepsilon^{2^{p-2}}) \equiv 0 \pmod{M_p}$, da f offenbar das Minimalpolynom zu $\varepsilon^{2^{p-2}}$ ist. Damit hat aber keine kleinere Potenz von ε diese Eigenschaft und daher ist $L_k = \mathrm{Spur}(\varepsilon^{2^k}) \not\equiv 0 \pmod{M_p}$ für $0 \le k \le p-3$.
Sei nun $q \in \mathbb{P}$ ein Teiler von M_p, der auch L_{p-2} teilt. Damit gilt (alles modulo q)

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

Ist nun q prim in R, so ist $|T(q)| = q + 1$ nach dem Beweis zu Proposition 3.1 und ν_q ist ein Gruppenepimorphismus.

Ist q nicht prim, so kann das Ideal qR nur zerlegt sein, denn $q \nmid 2 \cdot 3$, also $qR = \mathfrak{q}\overline{\mathfrak{q}}$ mit $\mathfrak{q} \neq \overline{\mathfrak{q}}$ und $\mathfrak{q} \trianglelefteq R$ prim. Dann ist nach dem Chinesischen Restsatz

$$(R/qR)^* \cong (R/\mathfrak{q} \times R/\overline{\mathfrak{q}})^* \cong \mathbb{F}_q^* \times \mathbb{F}_q^*,$$

also ist $|(R/qR)^*| = (q-1)^2$. Auch in diesem Fall ist ν_q analog wie oben definiert surjektiv, was allerdings hier zu weit führen würde. Dies folgt nach der Klassifikation quadratischer Formen, vgl. [Kne02, Satz 12.2, S.51], so dass mit dem Homomorphiesatz folgt, dass $|T(q)| = q - 1$. Da aber nach dem Satz von LAGRANGE[2] 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 folgt die Behauptung genau wie im Beweis zu Satz 3.4. □

Algorithmus 3.6. (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.

[2] JOSEPH-LOUIS LAGRANGE, 1736-1813, ital. Mathematiker und Astronom, Variationsrechnung, Zahlentheorie, Gruppentheorie

3.1.2 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 (vgl. [Gro05]). E hat die Diskriminante

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

also besitzt E eine gute Reduktion zu allen Primzahlen $q > 3$. Die MORDELL[3]-WEIL-Gruppe von E ist isomorph zu $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ und wird erzeugt von $P = (-2, 4)$ mit unendlicher Ordnung und $Q = (0, 0)$ mit Ordnung 2.
Nach Lemma 2.36 wissen wir bereits, dass die Reduktion E modulo q für $q \equiv -1 \pmod 4, q > 3$ supersingulär ist.

Proposition 3.7.
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. Der erste Teil folgt unmittelbar mit Lemma 2.37, denn $\left(\frac{12}{q}\right) = -1$.
Gemäß Satz 2.38 ist $P = (-2, 4)$ höchstens dann in $2E(q)$, wenn -2 ein Quadrat modulo q ist, aber

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

□

Wir definieren nun eine Folge rationaler Zahlen über die x-Koordinaten der sukzessiven Quadrate des Punktes P aus Lemma 2.36 vermöge

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

$x(Q)$ entspricht hier der Projektion auf die erste Koordinate des Punktes Q. Durch Anwenden von Korollar 2.9 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 3.8.
Es sei $M_p = 2^p - 1$ eine Primzahl. Dann ist $G_k(G_k^2 - 12)$ eine Einheit in $\mathbb{Z}/M_p\mathbb{Z}$ 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. Hierbei ist stets G_k als ganze Zahl zu verstehen, indem man die G_k mit seinem Vertreter modulo M_p in $\{0, ..., M_p - 1\}$ identifizert.

[3]LOUIS JOEL MORDELL, 1888-1972, amer.-brit. Mathematiker, DIOPHANTische Gleichungen

BEWEIS. Sei zunächst M_p eine Primzahl. Dann folgt mit Proposition 3.7 , 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 $G_k(G_k^2 - 12)$ Einheiten modulo M_p, 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}, wobei man auch hier G_{p-1} mit seinem Restklassenvertreter modulo M_p identifiziert. 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. Also gilt:

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

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

Aus diesem Satz lässt sich ein Testverfahren sofort ableiten:

Algorithmus 3.9.

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` $G = 0$.

3.2 Fermat-Zahlen

Die Untersuchungen in diesem Abschnitt basieren im Wesentlichen auf einem Artikel von Denomme und Savin (vgl. [DS08]).

3.2.1 Der Pépin-Test

Auch für Fermat-Primzahlen gibt es einen recht einfachen klassischen Test, der auf Pépin[4] zurückgeht. Im wesentlichen basiert er auf der Beobachtung, dass, falls F_n eine Primzahl ist, die Gruppe $(\mathbb{Z}/F_n\mathbb{Z})^*$ stets zyklisch von Ordnung 2^{2^n} ist und von 3 erzeugt wird. Es gibt auch andere ganze Zahlen, die diese Gruppe immer erzeugen, nämlich die, die modulo F_n keine Quadrate sind, dort ergeben sich entsprechende Test-Möglichkeiten:

Satz 3.10. *(*Pépin-***Test***)*
Die Fermat*-Zahl $F_n = 2^{2^n} + 1$ ist genau dann eine Primzahl, wenn*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Beweis. Angenommen, es gilt die Kongruenz gilt und es sei $q \in \mathbb{P}$ ein Primfaktor von F_n. Dann gilt

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{q},$$

bzw. durch quadrieren beider Seiten der Kongruenz

$$3^{F_n-1} \equiv 1 \pmod{q}.$$

Also muss die Ordnung von 3 in $\mathbb{F}_q^*$ ein Teiler von $F_n - 1 = 2^{2^n}$ sein. Da dies eine 2-Potenz ist und $3^{\frac{F_n-1}{2}} \not\equiv 1 \pmod{q}$, muss die Ordnung von 3 genau $F_n - 1$ sein. Andererseits ist diese höchstens $q - 1$, also folgt $F_n - 1 \leq q - 1$, also $F_n = q \in \mathbb{P}$.
Sei umgekehrt $F_n \in \mathbb{P}$. Dann ist nach dem Quadratischen Reziprozitätsgesetz 3 kein Quadrat modulo F_n (beachte $F_n \equiv 1 \pmod 4$ und $F_n \equiv 2 \pmod 3$):

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

also mit dem Euler-Kriterium

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

und damit die Behauptung. □

Der hieraus resultierende Test ist sehr leicht algorithmisch umzusetzen und zu implementieren (eine Möglichkeit hierzu findet sich in Anhang B.1.2).

Algorithmus 3.11.

EINGABE : $n \in \mathbb{N}$
ALGORITHMUS : `Berechne` P:=$3^{\frac{F_n-1}{2}} \pmod{F_n}$
AUSGABE : F_n `ist prim, falls` P$\equiv -1 \pmod{F_n}$
F_n `ist nicht prim, sonst.`

[4] Jean François Théophile Pépin, 1826-1904, frz. Mathematiker, Zahlentheorie

3.2.2 Fermat-Primzahlen und Elliptische Kurven

In diesem Abschnitt bezeichne E die elliptische Kurve mit WEIERSTRASS-Gleichung

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

über dem Körper der rationalen Zahlen und $E(p)$ die Gruppe der $\mathbb{F}_p$-rationalen Punkte der Reduktion $\widehat{E}$ von E modulo einer Primzahl $p \in \mathbb{P}$. Für E ist

$$\Delta(E) = 2^6,$$

also hat E gute Reduktion modulo jeder ungeraden Primzahl. Die Gruppe der $\mathbb{F}_p$-rationalen Punkte dieser Kurve ist zwar im Allgemeinen nicht zyklisch, aber hier gilt, wie unten gezeigt wird, dass $E(F_n)$ als $\mathbb{Z}[i]$-Modul isomorph ist zu $\mathbb{Z}[i]/(1+i)^{2^n}$ und dass diese Eigenschaft für den quadratischen Twist E_{30} von E erhalten bleibt. Dies wird die Möglichkeit geben, einen Primzahltest zu formulieren. Dazu werden zunächst wieder einige Eigenschaften der Kurve E gesammelt:

Proposition 3.12.
Sei $p \in \mathbb{P}$ mit $p \equiv 1 \pmod 4$ und $p = a^2 + b^2$ für $a, b \in \mathbb{Z}$ mit $a + bi \equiv 1 \pmod{2+2i}$. Dann gilt

$$|E(p)| = p + 1 - 2a.$$

BEWEIS. Siehe [IR82, Chapter 18, §5, Theorem 5] □

Korollar 3.13.
Ist $n > 1$ und $F_n = 2^{2^n} + 1 \in \mathbb{P}$, dann ist $|E(F_n)| = 2^{2^n}$.

BEWEIS. Es ist $F_n = 1^2 + (2^{2^{n-1}})^2$ und wegen $n > 1$ ist $(2^{2^{n-1}})$ durch $4 = (2+2i)(1-i)$ teilbar, also ist

$$1 + 2^{2^{n-1}} i \equiv 1 \pmod{2+2i}.$$

Damit folgt mit Proposition 3.12, dass $|E(F_n)| = F_n + 1 - 2 \cdot 1 = 2^{2^n}$ gilt. □

Bemerkung 3.14.

1. *E hat komplexe Multiplikation durch den Ring der ganzen* GAUSS*schen Zahlen $\mathbb{Z}[i]$. Die Abbildung*

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

   ist ein Endomorphismus von E, so dass E zu einem $\mathbb{Z}[i]$-Modul wird. Entsprechendes gilt für die Reduktionen $E(p)$ von E für $p \equiv 1 \pmod 4$, wobei hier i eine primitive vierte Einheitswurzel in $\mathbb{F}_p$ bezeichne.

2. *Die Abbildung $[1+i]$ ist eine Isogenie vom Grad 2 und annuliert außer $\mathcal{O}$ nur den Punkt $Q = (0, 0)$.*

Proposition 3.15.
Sei $n > 1$ und $F_n \in \mathbb{P}$. Dann gilt

$$E(F_n) \cong \mathbb{Z}[i]/(1+i)^{2^n}$$

als $\mathbb{Z}[i]$-Modul.

BEWEIS. Da $\mathbb{Z}[i]$ ein EUKLIDischer Ring ist, ist klar, dass $E(F_n)$ als endlich erzeugter $\mathbb{Z}[i]$-Modul isomorph zu der additiven Gruppe

$$\mathbb{Z}[i]/(a_1) \oplus \mathbb{Z}[i]/(a_2) \oplus ... \oplus \mathbb{Z}[i]/(a_k)$$

für ein $k \in \mathbb{N}$ und $a_j \in \mathbb{Z}[i]$ für alle j sein muss. Es bezeichne (a_j) das von a_j erzeugte Hauptideal in $\mathbb{Z}[i]$. Nun ist jedes $\mathbb{Z}[i]/(a_j)$ eine Untergruppe von $E(F_n)$, seine Ordnung muss also $|E(F_n)| \overset{3.13}{=} 2^{2^n}$ teilen. Damit ist aber $|\mathbb{Z}[i]/(a_j)| = \nu(a_j)$ eine Potenz von $2 = -i(1+i)^2$. Da $\mathbb{Z}[i]$ EUKLIDisch, also insbesondere faktoriell ist, muss es zu jedem $j \in \{1, ..., k\}$ ein eindeutig bestimmtes $m_j \in \mathbb{N}$ geben mit

$$(a_j) = ((1+i)^{m_j}).$$

Wegen Grad$([1+i]) = 2$ hat der Annihilator von $(1+i)$ genau 2 Elemente, also ist $k = 1$. Das war zu zeigen. □

Wir wissen nun, dass $E(F_n)$ ein zyklischer $\mathbb{Z}[i]$-Modul ist. Um einen Erzeuger P dieses Moduls zu finden, betrachten wir den quadratischen Twist E_t von E, wobei E_t der Gleichung

$$ty^2 = x^3 - x, \quad t \in \mathbb{Z}$$

genügt. Es gilt die

Bemerkung 3.16.
Sei $F_n \in \mathbb{P}$ und $t \neq 0$ ein quadratischer Rest modulo F_n. Dann definiert die Abbildung

$$\alpha : E(F_n) \to E_t(F_n),\ (x, y) \mapsto (x, t^{\frac{1}{2}} \cdot y)$$

einen Isomorphismus von $\mathbb{Z}[i]$-Moduln.

BEWEIS. Da $t \not\equiv 0 \pmod{F_n}$ nach Voraussetzung, ist φ offenbar bijektiv. Sei nun $(x, y) \in E(F_n)$. Da die Vertäglichkeit der skalaren Multiplikation mit ganzen Zahlen offensichtlich ist, reicht es nachzurechnen, dass $\alpha([i](x, y)) = [i](\alpha((x, y))$ gilt:

$$\alpha([i](x, y)) = \alpha(-x, iy) = (-x, it^{\frac{1}{2}}y) = [i](x, t^{\frac{1}{2}}y) = [i]\alpha((x, y)).$$

□

Bemerkung 3.17.
Sei $x \in \mathbb{Z}$ so, dass $x^3 - x$ nicht quadratfrei ist, also $x^3 - x = t \cdot y^2$. Dann ist der Punkt $P = (x, y)$ ein rationaler Punkt von E_t.

Beispiel 3.18.
Sei $x = 5$. Dann ist $x^3 - x = 30 \cdot 2^2$, also ist $P = (5, 2)$ ein rationaler Punkt von E_{30}. Des Weiteren gilt für $F_n \in \mathbb{P}$

$$\left(\frac{30}{F_n}\right) = \left(\frac{2}{F_n}\right)\left(\frac{3}{F_n}\right)\left(\frac{5}{F_n}\right) = 1 \cdot (-1) \cdot (-1) = 1,$$

also ist 30 ein Quadrat modulo F_n. Diese Eigenschaft wird später noch wichtig werden.

Wir benötigen eine konkrete Formel für die Multiplikation mit $1 + i$ auf E_t. das liefert die folgende

Bemerkung 3.19.
Die Steigung der Geraden durch (x, y) und $i(x, y) = (-x, iy)$ ist

$$A = \frac{(1-i)y}{2x}.$$

Dies eingesetzt in Satz 2.8 liefert dann $(1+i)(x, y) = (x', y')$ mit

$$x' = tA^2 = \frac{1}{2}\left(\frac{x}{i} + \frac{i}{x}\right) \tag{3.1}$$

$$y' = -y - A(x' - x) \tag{3.2}$$

Dies führt nun zu der

Proposition 3.20.
Sei $n > 1$ und $F_n \in \mathbb{P}$. Dann ist der Punkt $P = (5, 2)$ ein Erzeuger des $\mathbb{Z}[i]$-Moduls

$$E_{30}(F_n) \cong \mathbb{Z}[i]/(1+i)^{2^n}.$$

Beweis. Angenommen, es gibt einen Punkt $R \in E_{30}(F_n)$ mit

$$(5, 2) \equiv (1+i) \cdot R \pmod{F_n}.$$

Gleichung 3.1 in Bemerkung 3.19 liefert dann sofort

$$5 \equiv 30 \cdot A^2 \pmod{F_n}$$

und das ist ein Widerspruch, denn 5 ist kein Quadrat modulo F_n, 30 aber schon (vgl. Beispiel 3.18):

$$\left(\frac{5}{F_n}\right) \overset{1.9}{=} \left(\frac{F_n}{5}\right) = \left(\frac{2}{5}\right) \overset{1.8}{=} -1.$$

□

Bemerkung 3.21.
Im Beweis zur vorigen Proposition wurde im Wesentlichen nur benutzt, dass 30 modulo F_n ein Quadrat ist, falls $n > 1$. Das selbe Argument funktioniert natürlich auch für andere geeignete Werte von t. Wählt man beispielsweise $x = 7$ in Bemerkung 3.17, so erhält man $7^3 - 7 = 21 \cdot 4^2$, also $t = 21$ und $P = (7, 4)$. Mit dem Quadratischen Reziprozitätsgesetz erhält man hier wieder, dass 7 kein Quadrat modulo F_n ist, 21 aber schon. Das liefert die analoge Aussage zu Proposition 3.20 für E_{21} und $P = (7, 4)$.

Diese Beobachtungen werden nun helfen, einen Test für Fermat-Primzahlen mithilfe der Kurve E_{30} zu konstruieren. Er wird über die $\mathbb{Z}[i]$-Modulstruktur von E_{30} erklärt. Man beachte, dass man in $\mathbb{Z}[i]$ die Faktorisierung

$$F_n = f_n \cdot \overline{f_n} \text{ mit } f_n = 2^{2^{n-1}} + i \in \mathbb{Z}[i]$$

hat. Damit ist F_n dann und nur dann prim in $\mathbb{Z}$, wenn f_n prim in $\mathbb{Z}[i]$ ist. Es gilt folgender

Satz 3.22.
Sei $P = (5, 2)$ ein Punkt auf der getwisteten Kurve E_{30} mit der Gleichung $30y^2 = x^3 - x$ und $n > 1$. Dann ist die Fermat-Zahl $F_n = 2^{2^n} + 1$ genau dann prim, wenn

$$(1+i)^{2^n - 1} \cdot P \equiv Q \pmod{f_n}$$

gilt, wobei $Q = (0, 0)$ der einzige Punkt von Ordnung $(1+i)$ in E_{30} ist.

BEWEIS. Angenommen, die Kongruenz gilt. Dann sei $p \in \mathbb{P}$ ein Primfaktor von F_n mit $p < \sqrt{F_n}$. Da F_n nicht durch 3 oder 5 teilbar ist, ist insbesondere $p \geq 7$ und E_{30} hat damit gute Reduktion modulo p. Da p ein Teiler von F_n ist, gilt die Kongruenz

$$\left(2^{2^{n-1}}\right)^2 \equiv -1 \pmod{p},$$

so dass nach Satz 1.8 bzw. dem Zwei-Quadrate-Satz von FERMAT $p \equiv 1 \pmod 4$ gilt. Das bedeutet wiederum, dass es ein Primelement $\pi \in \mathbb{Z}[i]$ gibt mit $p = \pi\overline{\pi}$. Ohne Einschränkung kann man dann annehmen, dass $\pi \mid f_n$, da π prim ist. Damit gilt die Kongruenz

$$(1+i)^{2^n-1} \cdot P \equiv Q \pmod{\pi}.$$

Multipliziert man beide Seiten der Kongruenz mit $(1+i)$, so folgt

$$(1+i)^{2^n} \cdot P \equiv \mathcal{O} \pmod{\pi},$$

wobei $\mathcal{O}$ wieder den unendlich fernen Punkt bezeichne. Das bedeutet, dass P einen $\mathbb{Z}[i]$-Teilmodul von $E_{30}(\pi)$ erzeugt, der isomorph zu $\mathbb{Z}[i]/((1+i)^{2^n})$ ist. Dieser Modul hat Ordnung $\nu((1+i)^{2^n}) = 2^{2^n} = F_n - 1$. Damit folgt

$$F_n - 1 \leq |E_{30}|.$$

Mit der HASSEschen Ungleichung (vgl. Satz 2.34) folgt dann aber

$$|E_{30}(\pi)| \leq p + 1 + 2\sqrt{p} = (1+\sqrt{p})^2$$

(Man beachte hierbei, dass $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/(\pi)$).
Damit haben wir aber einen Widerspruch, denn nun haben wir wegen $p^2 < F_n$

$$p^2 - 1 < F_n - 1 \leq (1+\sqrt{p})^2$$

und das ist für keine Primzahl $p > 2$ möglich. Damit muss also F_n selbst schon prim sein.
Nehmen wir umgekehrt an, dass $F_n \in \mathbb{P}$. Dann ist, da die Körper $\mathbb{Z}/F_n\mathbb{Z}$ und $\mathbb{Z}[i]/(f_n)$ isomorph sind, auch die Kurven $E_{30}(F_n)$ und $E_{30}(f_n)$ isomorph. Mit Proposition 3.12 folgt dann, dass

$$E_{30} \cong \mathbb{Z}[i]/\left((1+i)^{2^n}\right)$$

als $\mathbb{Z}[i]$-Modul und nach Proposition 3.20 wird er von $P = (5, 2)$ erzeugt. Damit hat insbesondere $(1+i)^{2^n-1} \cdot P$ die Ordnung $(1+i)$. Der einzige Punkt mit dieser Ordnung ist aber Q und daraus folgt die Behauptung. □

Korollar 3.23. *Mit den Voraussetzungen von Satz 3.22 ist die* FERMAT*-Zahl F_n genau dann prim, wenn x_m und f_n für alle $m \in \{1, ..., 2^n - 1\}$ relativ prim sind und $x_{2^n} \equiv 0 \pmod{f_n}$ mit*

$$x_1 := 5, \qquad x_{m+1} = \frac{1}{2}\left(\frac{x_m}{i} + \frac{i}{x_m}\right).$$

BEWEIS. Nach Bemerkung 3.19 ist x_m genau die x-Koordinate des Punktes $(1+i)^{m-1} \cdot P$ und die Behauptung folgt sofort mit Satz 3.22. □

Auch für diesen Test geben wir hier einen Algorithmus und eine Implementierung in `Magma` in Anhang B.2.2 an:

Algorithmus 3.24.

EINGABE : $n \in \mathbb{N}$, $n \geq 4$
ALGORITHMUS : $f_n \leftarrow 2^{2^{n-1}} + i$
$D \leftarrow 5$
`Für` k `zwischen` 1 `und` $2^n - 1$ `berechne`
$D \leftarrow 1/2 * (D/i + i/D) \pmod{f_n}$
`Falls` D `nicht existiert: Abbruch`
AUSGABE : F_n `ist zusammengesetzt, falls Abbruch oder` $D \neq 0$
F_n `ist prim, falls` $D = 0$.

Kapitel 4

Neue Primzahltests

4.1 Alternative Tests für Mersenne-Zahlen

4.1.1 Herleitung

Die in Abschnitt 3.1.2 über den Primzahltest von Gross erläuterten Eigenschaften der gegebenen elliptischen Kurve sind nicht unbedingt einzigartig unter elliptischen Kurven. Dementsprechend kann man durch die Wahl einer anderen Kurve mit ähnlichen Eigenschaften auch einen anderen Primzahltest für Mersenne-Zahlen herleiten.
Wir beschränken uns hierbei auf Kurven der Form E_a mit Weierstrass-Gleichung

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

wie in Abschnitt 2.4.1. Der Grund dafür liegt darin, dass wenn man die im Softwarepaket Magma implemetierte Version der von John Cremona[1] über elliptische Kurven über $\mathbb{Q}$ nach geeigneten Kurven durchsucht, bleiben automatisch nur Kurven der Form E_a übrig. Im Anhang A findet sich ein möglicher Magma-Code dazu. Man sorgt nacheinander dafür, dass die vorhanden Kurven komplexe Multiplikation (Anhang A.1.1), gute Reduktion modulo allen Primzahlen $q \equiv 7 \pmod{24}$ (Anhang A.1.2), Supersingularität der Reduktion (Anhang A.1.3) und schließlich noch für eine zyklische Punktgruppe der Reduktion modulo der ersten Mersenne-Primzahlen. Von den

```
> DB:=CremonaDatabase();
> # DB;
847550
```

elliptische Kurven in der Datenbank bleiben so noch

```
> # L;
81
```

Kurven übrig. Mittels

```
> forall(t){E: E in L | aInvariants(E)[1] eq 0 and aInvariants(E)[2] eq 0 and}
aInvariants(E)[3] eq 0 and aInvariants(E)[5] eq 0};
true
```

[1] John Cremona, brit. Mathematiker, Zahlentheorie, elliptische Kurven, Modulformen, Computeralgebra

überzeugt man sich, dass alle diese 81 Kurven von der Form E_a sind. Unter Beachtung der Beweise in den Abschnitten 2.4.1 und 3.1.2 erhält man folgende Bedingungen für die gesuchte Kurve und einen geeigneten Punkt $\mathbb{F}_p$-rationalen Punkt $P = (x_0, y_0)$ für $p \equiv 7 \pmod{24}$:

1. a ist kein Quadrat modulo p, ansonsten ist $E_a(p)$ nicht zyklisch.
2. x_0 ist kein Quadrat modulo p, ansonsten ist P kein Erzeuger von $E_a(p)$.
3. $(x_0 - a)^2$ ist kein Quadrat modulo p, ansonsten ist P nicht $\mathbb{F}_p$-rational, denn $x_0(x_0 - a)^2$ muss ein Quadrat modulo p sein.

Da $p \equiv 7 \pmod{24}$, sind sicherlich alle Zahlen der Form

$$\circledast \quad (-1)^k \cdot 2^\ell \cdot 3^m \cdot n^2 \text{ für } \ell \in \mathbb{N}_0,\ n \in \mathbb{N} \text{ und } k, m \in \{0, 1\},\ k \neq m.$$

keine Quadrate modulo p. Durch Durchsehenen der Faktorisierungen der einzelnen Koeffizienten a verifiziert man unter Beachtung der Tatsache, dass -1 und 3 keine Quadrate modulo p mit $p \equiv 7 \pmod{24}$, 2 aber schon, dass jedes einzelne der 81 a ein Nichtquadrat modulo p ist.
In Anhang A.1.5 wird das betragsmäßig kleinste x_0 von der Form $\circledast$ bestimmt, allerdings nur für $\ell, n \leq 100$, da die Rechnungen ansonsten unnötig lange dauern. Falls sich so kein x_0 finden lässt, wird auf die entsprechende Kurve verzichtet.
Die folgende Tabelle stellt nun die gefunden Werte für a nebst den zugehörigen Werten für x_0 dar. Führt man den `Magma`-Code wie in Anhang A dargestellt aus, so benötigen die Rech-

a	-8	-2	12	108	3	27	54
x_0	-2	-1	-2	6	-1	3	-2
a	6	-72	24	216	-18	-200	-50
x_0	-2	6	-4	-4	3	-4	-2
a	-2700	300	75	675	-968	-242	-1352
x_0	-50	-18	-9	-25	-2	-1	-1250
a	-338	-1800	-450	3468	31212	-2888	-722
x_0	-625	12	6	-50	150	-4	-2

nungen auf einem Core i7, 940-Prozessor mit 2,93 GHz 118.790 s CPU-Zeit und 27.84 MB Speicherplatz.
Zusammenfassend können wir folgenden Satz formulieren:

Satz 4.1.
Es sei $p \in \mathbb{P} \setminus \{2\}$ und M_p die zugehörige Mersenne*-Zahl. Weiter seien $a, G_0^{(a)} \in \mathbb{Z}$ mit den Eigenschaften 1.-3. beliebig und E_a die elliptische Kurve mit* Weierstrass*-Gleichung $y^2 = x^3 - ax$. Definiere*

$$G_{k+1}^{(a)} := \frac{(G_k^{(a)^2} + a)^2}{4 \cdot G_k^{(a)} \cdot (G_k^{(a)^2} - a)}$$

Dann ist M_p genau dann eine Primzahl, wenn $G_{p-1}^{(a)}$ existiert und es gilt

$$G_{p-1}^{(a)} \equiv 0 \pmod{M_p}.$$

Wählt man speziell

$$a \in \{-8, -2, 12, 108, 3, 27, 54, 6, -72, 24, 216, -18, -200, -50, 2700, 300, 75, 675, -968, -242, -1352, -338, -1800, -450, 3468, 31212, -2888, -722\}$$

(das sind alle möglichen Werte in der CREMONA*-Datenbank nach Durchführen von Anhang A.1.1-5) ergeben sich als Startwerte*

$$G_0^{(-8)} = G_0^{(12)} = G_0^{(54)} = G_0^{(6)} = G_0^{(-50)} = G_0^{(-968)} = G_0^{(-722)} = -2;$$
$$G_0^{(-2)} = G_0^{(3)} = G_0^{(-242)} = -1;$$
$$G_0^{(108)} = G_0^{(-72)} = G_0^{(-450)} = 6;$$
$$G_0^{(27)} = G_0^{(-18)} = 3;$$
$$G_0^{(24)} = G_0^{(216)} = G_0^{(-200)} = G_0^{(-2888)} = -4;$$
$$G_0^{(2700)} = G_0^{(3468)} = -50;$$
$$G_0^{(300)} = -18;$$
$$G_0^{(75)} = -9;$$
$$G_0^{(675)} = -25;$$
$$G_0^{(-1352)} = -1250;$$
$$G_0^{(-338)} = -625;$$
$$G_0^{(-1800)} = 12;$$
$$G_0^{(31212)} = 150.$$

4.1.2 Effizienzvergleich

Wie man am Code der Funktion `EllipticMersenne` (vgl. Anhang B.2.1) sieht, gibt es zumindest theoretisch einen Vorteil der Tests mit elliptischen Kurven gegenüber dem LUCAS-LEHMER-Test. Während für den LUCAS-LEHMER-Test stets $p-2$ Neuberechnungen von `L` nötig sind, kann es sein, dass die Tests mit elliptischen Kurven die Schleife nicht unbedingt $p-1$-mal durchlaufen müssen, was einen Geschwindigkeitsgewinn bedeuten würde. Allerdings ist die Berechnung bei den Tests mit elliptischen Kurven in jedem einzelnen Schritt viel aufwendiger (LUCAS-LEHMER benötigt pro Iteration 2 Multiplikationen und eine Division, die anderen Tests jeweils 5 Multiplikationen und eine Division). Zum Vergleich der Geschwindigkeit der jeweiligen Tests wurde die Funktion `Velocity(a)` geschrieben (vgl. Anhang B.2.1), die für jede Primzahl $p \leq 10\,000$ den Test zu der elliptischen Kurve mit WEIERSTRASS-Gleichung $y^2 = x^3 - ax$ bzw. für `a=0` den LUCAS-LEHMER-Test und eine Liste aller $p \leq 10\,000$ zurückgibt, für die M_p prim ist. Die Funktion `EllipticMersenne` gibt hierbei auch diejenigen p aus, für die tatsächlich der Fall eintritt, dass $G_{p-1}^{(a)}$ nicht existiert. Die benötigte Zeit wurde durch den Befehl

```
time Velocity(a);
```

gemessen.
Die folgende Tabelle stellt in die benötigte Zeit für den Aufruf von `Velocity(a)` für jedes

a	$G_0^{(a)}$	Abbruch bei	Zeit
0	-	-	71.480
-8	-2	-	3565.760
-2	-1	-	3567.560
12	-2	23	3556.030
108	6	23	3555.150
3	-1	23	3554.900
27	3	23	3554.020
54	-2	-	3553.410
6	-2	11, 37, 47, 191	3551.710
-72	6	-	3573.630
24	-4	11, 37, 47, 191	3654.720
216	-4	-	3644.640
-18	3	-	3672.360
-200	-4	37, 47, 191	3670.280
-50	-2	11, 37, 191	3661.970
2700	-50	37	3607.860
300	-18	37	3570.660
75	-9	37	3580.410
675	-25	37	3579.150
-968	-2	-	3577.110
-242	-1	-	3580.260
-1352	-1250	11, 37, 3359, 7823	3569.170
-338	-625	11, 37, 3359, 7823	3563.180
-1800	12	11, 37, 191	3590.890
-450	6	11, 37, 191	3575.780
3468	-50	29, 79, 1103	3571.380
31212	150	29, 79, 1103	3567.520
-2888	-4	11, 23, 179	3572.820
-722	-2	11, 23, 179	3571.850

gefundene `a` und das zugehörige $G_0^{(a)}$ gemäß Satz 4.1, sowie diejenigen Exponenten `p` dar, für die der Test vorzeitig abbricht. Man sieht also, dass das Phänomen des vorzeitigen Abbruchs nur sporadisch auftritt, sodass der Lucas-Lehmer-Test wohl stets schneller ist als jeder der Tests mit elliptischen Kurven, hier ist der Lucas-Lehmer-Test etwa 50-mal so schnell, wie die gefundenen Tests mit elliptischen Kurven. Der Unterschied zwischen den einzelnen Tests mit elliptischen Kurven ist nach der Tabelle offenbar hinreichend gering, so dass sie als etwa gleich effizient gelten können. Die Differenz zwischen dem schnellsten (für $a = 6$) und langsamsten (für $a = 18$) Durchgang beträgt 120.650 s, das entspricht etwa $3,3\%$ der im Mittel benötigten Zeit. Außerdem ist nicht erkennbar, dass diejenigen Tests schneller liefen, die oft vorzeitig abbrachen, sodass die Abweichungen andere Ursachen haben müssen.

4.2 Primzahltest für verallgemeinterte Thabit-Zahlen

Die bisher vorgestellten Tests für MERSENNE-Primzahlen basierten wesentlich darauf, dass man zumindest ab einer gewissen Schranke sagen kann, dass 3 modulo M_p kein Quadrat ist für eine MERSENNE-Primzahl M_p. Auch der Test von DENOMME und SAVIN für FERMAT-Zahlen benutzt, dass ab einem gewissen Exponenten n 5 kein Quadrat modulo F_n ist, falls F_n eine Primzahl ist. Für verallgemeinerte THABIT-Zahlen $K(h,n) = h \cdot 2^n - 1$ funktioniert dies nicht mehr unbedingt. Zwar gilt für $h \equiv 1 \pmod 3$, $n \geq 2$ und $K(h,n) \in \mathbb{P}$ (also notwendigerweise n ungerade)

$$\left(\frac{3}{K(h,n)}\right) \overset{1.9}{=} -\left(\frac{h \cdot 2^n - 1}{3}\right) = -\left(\frac{2^n - 1}{3}\right) = -1$$

und für $h \equiv 0 \pmod 3$, $n \geq 2$ und $K(h,n) \in \mathbb{P}$ (also notwendigerweise n gerade)

$$\left(\frac{3}{K(h,n)}\right) \overset{1.9}{=} -\left(\frac{h \cdot 2^n - 1}{3}\right) = -\left(\frac{2^{n+1} - 1}{3}\right) = -1,$$

aber für $h \equiv 0 \pmod 3$ ist

$$\begin{aligned}
&\left(\frac{2}{K(h,n)}\right) \overset{1.8}{=} 1 \\
&\left(\frac{3}{K(h,n)}\right) \overset{1.9}{=} -\left(\frac{K(h,n)}{3}\right) = 1 \\
&\left(\frac{5}{K(h,n)}\right) \overset{1.9}{=} \left(\frac{K(h,n)}{5}\right) = \begin{cases} 1 & \text{, falls } n \equiv 2 \pmod 4 \\ -1 & \text{, falls } n \equiv 0,\, 3 \pmod 4 \end{cases} \\
&\left(\frac{7}{K(h,n)}\right) \overset{1.9}{=} -\left(\frac{K(h,n)}{7}\right) = \begin{cases} -\left(\frac{5}{7}\right) = 1 & \text{, falls } n \equiv 1 \pmod 3 \\ -1 & \text{sonst} \end{cases}
\end{aligned}$$

Man sieht, dass es wohl keine Primzahl gibt, die modulo jeder verallgemeinerten THABIT-Primzahl für $h \equiv 0 \pmod 3$ ein Nichtquadrat ist, mit anderen Worten wird man daher keine globale Kurve finden kann, die stets einen geeigneten Primzahltest liefert.
Die entscheidende Idee, im Fall $h \equiv 0 \pmod 3$ eine lokale Kurve zu konstruieren, lautet wie folgt:
Man beschränkt sich auf Kurven E_ε mit einer WEIERSTRASS-Gleichung von der Form

$$y^2 = x^3 - \varepsilon x.$$

In Abhängigkeit des zu prüfenden Exponenten n und Faktors h der verallgemeinerten THABIT-Zahl $K(h,n)$ wählt man nun ein geeignetes ε.
Auf dieser Idee basiert auch der LUCAS-LEHMER-RIESEL[2]-Test für verallgemeinerte THABIT-Zahlen. Dieser arbeitet mit der in Abschnitt 3.1.1 definierten Rekursion, nur muss der Anfangswert jeweils in Abhängigkeit von h und n geeignet gewählt werden. Für $h = 3$ und $n \equiv 0 \pmod 4$ oder $n \equiv 3 \pmod 4$ wählt man beispielsweise als Anfangswert der Rekursion $L_0 := 5778$. Für eine detaillierte Diskussion dieses Tests sei auf [Rie69] verwiesen.
Wir behandeln die beiden relevanten Fälle separat:

[2]HANS RIESEL, geboren 1929, schwed. Mathematiker, algorithmische Zahlentheorie

4.2.1 Der Fall $h \not\equiv 0 \pmod 3$

In diesem Abschnitt sei stets $h \not\equiv 0 \pmod 3$.
Wie oben gesehen, ist in diesem Fall 3 ein Nichtquadrat modulo $K(h,n)$, falls $K(h,n)$ eine Primzahl ist und $n \geq 2$ gilt. Dann ist auch -1 kein Quadrat modulo $K(h,n)$. Man sieht genau wie in Lemma 1.2, dass $K(h,n) \equiv 7 \pmod{24}$, falls $K(h,n) \in \mathbb{P}$ und $n \geq 3$. Dies ist auch die entscheidende Eigenschaft von MERSENNE-Primzahlen, die für die Tests in Abschnitt 4.1.1 verwendet wurde, so dass wir hier sofort das Analogon zu Satz 4.1 erhalten:

Satz 4.2.
Es sei $h \not\equiv 0 \pmod 3$, $n \in \mathbb{N}, n \geq \max\{3, \lceil \log_2(h) \rceil + 2$ und $K(h,n)$ die zugehörige verallgemeinerte THABIT*-Zahl. Weiter seien $a, x_0^{(a)} \in \mathbb{Z}$ mit den Eigenschaften 1.-3. aus Abschnitt 4.1.1 beliebig und E_a die elliptische Kurve mit* WEIERSTRASS*-Gleichung $y^2 = x^3 - ax$. Dann existiert ein $\mathbb{F}_{K(h,n)}$-rationaler Punkt $P = (x_0^{(a)}, y_0^{(a)})$ von $\widehat{E}_a$. Definiere*

$$T_0^{(a)} := x(h \cdot P) \text{ und } T_{k+1}^{(a)} := \frac{(T_k^{(a)^2} + a)^2}{4 \cdot T_k^{(a)} \cdot (T_k^{(a)^2} - a)},$$

wobei ψ_k das k-te Divisionspolynom gemäß Satz 2.10 bezeichnet.
Dann ist $K(h,n)$ genau dann eine Primzahl, wenn $T_{n-1}^{(a)}$ existiert und es gilt

$$T_{n-1}^{(a)} \equiv 0 \pmod{K(h,n)}.$$

BEWEIS. Nach Wahl von a und $x_0^{(a)}$ ist die Existenz von P garantiert.
Sei nun $K(h,n)$ eine Primzahl. Dann folgt mit Lemma 2.37, dass $h \cdot P$ die 2-SYLOW[3]gruppe von $E(K(h,n))$ erzeugt, da P nach Satz 2.38 nicht durch 2 teilbar ist. Insbesondere hat also $h \cdot P$ Ordnung 2^n, also ist $2^{n-1} \cdot (h \cdot P) = (0,0)$, denn $(0,0)$ ist auch der einzige $\mathbb{F}_{K(h,n)}$-rationale 2-Torsionspunkt von $\widehat{E}_a$ und $2^k \cdot (h \cdot P) \neq Q$ für jedes $k \in \{0, ..., n-2\}$. Nach Konstruktion ist nun $T_k^{(a)} = x\left(2^k \cdot (h \cdot P)\right)$. Demnach ist also $T_{n-1}^{(a)} \equiv 0 \pmod{K(h,n)}$ und $T_k^{(a)} \not\equiv 0 \pmod{K(h,n)}$ für $0 \leq k \leq n-2$, also ist $T_k^{(a)}$ in $\mathbb{Z}/K(h,n)\mathbb{Z}$ invertierbar, da $K(h,n)$ nach Voraussetzung eine Primzahl ist. Entsprechendes gilt für $T_k^{(a)^2} - a$, denn a ist kein Quadrat in $\mathbb{F}_{K(h,n)}$.
Sei nun umgekehrt $T_{n-1}^{(a)} \equiv 0 \pmod{K(h,n)}$ und $T_k^{(a)^2} - a$ in $\mathbb{Z}/K(h,n)\mathbb{Z}$ invertierbar für alle $k \in \{0, ..., n-2\}$. Weiterhin sei $q \in \mathbb{P}$ mit $q < \sqrt{K(h,n)}$ ein Primteiler von $K(h,n)$. Dann hat $2^{n-1} \cdot (h \cdot P)$ in $E_a(q)$ Ordnung 2, demnach hat $h \cdot P$ Ordnung $2^n = \frac{K(h,n)+1}{h}$. Mit der HASSEschen Ungleichung folgt aber

$$2^n \leq |E_a(q)| \leq q + 1 + 2\sqrt{q} \leq (2^{(n+2)/4} + 1)^2,$$

und das kann nach Wahl von n nicht sein. Also muss $K(h,n)$ eine Primzahl sein und das war zu zeigen. □

4.2.2 Der Fall $h \equiv 0 \pmod 3$

In diesem Anschnitt sei stets $h \equiv 0 \pmod 3$. Das folgende Lemma gibt eine Konstruktion eines geeigneten ε an:

[3]PETER LUDWIG MEJDELL SYLOW, 1832-1918, norw. Mathematiker, Gruppentheorie

Lemma 4.3.
Sei $n \geq 3$ und $K(h,n) = h \cdot 2^n - 1$ die zugehörige verallgemeinerte Thabit*-Zahl. Dann existiert eine kleinste Primzahl $p \in \mathbb{P}$, $p \geq 5$, die kein Quadrat modulo $K(h,n)$ ist und $\varepsilon := -p + 4$ ist ebenfalls kein Quadrat modulo $K(h,n)$.*

Beweis. Dass es ein $p \in \mathbb{P}$ geben muss, das modulo $K(h,n)$ kein Quadrat ist, ist klar, ansonsten wäre jede ganze Zahl ein Quadrat modulo $K(h,n)$ und das kann offenbar nicht sein. Wähle also das minimale solche p. Dann muss aber $p-4$ ein Quadrat modulo $K(h,n)$ sein, denn sei o.B.d.A. $p > 5$ (für $p = 5$ ist nichts zu zeigen) und $q \in \mathbb{P}$ ein Primteiler von $p-4$. Dann ist insbesondere $q < p$, also nach Wahl von p ist q ein Quadrat modulo $K(h,n)$. Da dies für jeden Primfaktor von $p-4$ gilt, ist auch $p-4$ ein Quadrat. Nun ist -1 kein Quadrat modulo $K(h,n)$, also ist auch $\varepsilon = -p+4$ kein Quadrat modulo $K(h,n)$. □

Bemerkung 4.4. *Das in Lemma 4.3 konstruierte ε ist als ganze Zahl aufgefasst stets negativ, also kein Quadrat in $\mathbb{Q}$. Damit ist $Q = (0,0)$ der einzige $\mathbb{Q}$-rationale Punkt von E_ε von Ordnung 2.*

Mit diesem gerade bestimmten ε erhält man, dass für die Diskriminante von E_ε gilt

$$\Delta(E_\varepsilon) = -2^6 \cdot \varepsilon^3.$$

Nach Konstruktion ist ε teilerfremd zu $K(h,n)$, also hat E_ε gute Reduktion modulo $K(h,n)$, wobei wir die üblichen Bezeichnungen beibehalten. Es sei also $\widehat{E}_\varepsilon$ die Reduktion von E_ε modulo einer Primzahl $p \in \mathbb{P}$ und abkürzend sei $\widehat{E}_\varepsilon(\mathbb{F}_p) = E_\varepsilon(p)$.
Mit Lemma 2.36 erhält man wieder sofort, dass für $n \geq 2$ und $K(h,n) \in \mathbb{P}$ die Reduktion von E_ε modulo $K(h,n)$ mit ε aus Lemma 4.3 supersingulär ist, denn dann ist $K(h,n) \equiv -1 \pmod 4$.
Wir haben die

Proposition 4.5.
Seien $n \in \mathbb{N}$, $n \geq 3$ und $h \in \mathbb{N}$, $h > 1$ ungerade so, dass die zugehörige verallgemeinerte Thabit*-Zahl $K(h,n)$ eine Primzahl ist und ε gemäß Lemma 4.3 gewählt. Dann ist $E_\varepsilon(K(h,n))$ zyklisch, also*

$$E_\varepsilon(K(h,n)) \cong C_{K(h,n)+1} \cong C_h \times C_{2^n}.$$

Weiterhin existiert ein $y \in \mathbb{F}_{K(h,n)}$, so dass $P = (-2, y)$ ein $\mathbb{F}_{K(h,n)}$-rationaler Punkt von $\widehat{E}_\varepsilon$ ist. Dann erzeugt $h \cdot P$ die 2-Sylow*gruppe von $E_\varepsilon(K(h,n))$.*

Beweis. Die Zyklizität der Punktgruppe folgt wieder unmittelbar mit Lemma 2.37. Es ist $(-2)^3 + 2\varepsilon = 2(\varepsilon - 4)$. Nach Konstruktion von ε ist $\varepsilon - 4$ ein Quadrat in $\mathbb{F}_{K(h,n)}$, ebenso ist 2 ein Quadrat, also gibt es ein $y \in \mathbb{F}_{K(h,n)}$ mit $y^2 = 2 \cdot (\varepsilon - 4)$. Demnach hat also P die Koordinaten $(-2, y)$ und ist damit $\mathbb{F}_{K(h,n)}$-rational.
Da -2 kein Quadrat in $\mathbb{F}_{K(h,n)}$ ist, ist P nach Satz 2.38 nicht durch 2 teilbar, muss also die 2-Sylow-Gruppe von $E(K(h,n))$ erzeugen. □

Man beachte hierbei, dass der oben gewählte Punkt P sich nicht zu einem $\mathbb{Q}$-rationalen Punkt von E_ε liften lässt, denn sonst müsste die Gleichung $y^2 = -8 + 2\varepsilon$ in $\mathbb{Q}$ lösbar sein, was aber nicht sein kann, da $\varepsilon < 0$.
Mit diesen Vorüberlegungen lässt sich nun der gesuchte Primzahltest für verallgmeinerte Thabit-Zahlen formulieren, wobei er im Wesentlichen genau so zu beweisen ist, wie der entsprechende Satz 3.8:

Satz 4.6.
Es sei $n \in \mathbb{N}$ mit $n \geq \lceil \log_2(h) \rceil + 2$ und $K(h,n)$ die zugehörige Thabit*-Zahl. Sei außerdem ε wie in Lemma 4.3 und $P = (-2, y)$ ein Punkt in $E_\varepsilon(K(h,n))$. Dann ist $K(h,n)$ genau dann eine Primzahl, wenn $T_{n-1} \equiv 0 \pmod{K(h,n)}$ und $T_k(T_k^2 - \varepsilon)$ eine Einheit in $\mathbb{Z}/K(h,n)\mathbb{Z}$ für jedes $k \in \{1, ..., n-2\}$ ist, wobei*

$$T_0 := x(h \cdot P) = \quad \text{und } T_{k+1} := \frac{(T_k^2 + \varepsilon)^2}{4T_k(T_k^2 - \varepsilon)}.$$

Beweis. Analog zum Beweis von Satz 4.2. □

Zum Abschluss geben wir noch einen Algorithmus an, der basierend auf Satz 4.6 und für $h = 3$ feststellt, ob zu gegebenem $n \geq 4$ die Thabit-Zahl $K(h,n)$ prim ist oder nicht. Eine Implementierung in `Magma` findet sich in Anhang B.2.3. Die Funktion `eps` berechnet zu gegebenem n ein ε wie in Lemma 4.3 und die Funktion `ThabitTest` führt den Test durch, wobei die Initialisierung von `T` direkt aus Korollar 2.9.2.

Algorithmus 4.7.

EINGABE : $n \in \mathbb{N}$, $n \geq 4$
ALGORITHMUS : `Bestimme` ε.
$T \leftarrow 16 * (\varepsilon - 4) * (\varepsilon^3 + 20 * \varepsilon^2 - 80 * \varepsilon - 64)/(\varepsilon^2 - 24 * \varepsilon - 64)^2 - 2$
`Falls` T `nicht existiert: Abbruch`
`Für` k `zwischen` 1 `und` $n-1$ `berechne`
$T \leftarrow (T^2 + \varepsilon)^2/(4T(T^2 - \varepsilon)) \pmod{K(h,n)}$
`Falls` T `nicht existiert: Abbruch`
AUSGABE : K_n `ist zusammengesetzt, falls Abbruch oder` $T \neq 0$
K_n `ist prim, falls` $T = 0$.

Anhang A

Magma-Code

A.1 Für Mersenne-Primzahlen

A.1.1 Komplexe Multiplikation

```
DB:=CremonaDatabase();
L:=[];
L:=[E : E in DB | HasComplexMultiplication(E)];
# DB;
847550
# L;
2524
M:=L;
```

Unter diesen Kurven Sind natürlich nur diejenigen relevant, die gute Reduktion modulo M_p besitzen.

A.1.2 Gute Reduktion

```
for E in L do
  d:=Factorization(Floor(Discriminant(E)));
  if exists(t){x[1]: x in d | x[1] mod 24 eq 7} then
    Exclude(~M,E);
  end if;
end for;
L:=M;
# L;
1854
```

Als nächstes sortiert man diejenigen Kurven aus, deren Reduktion nicht supersingulär ist. Hierzu kann man zum Beispiel die Reduktionen modulo M_p für $p \leq 100$ testen. Der entsprechende Magma-Code liefert dies:

A.1.3 Supersingularität

```
for E in L do
  for p in [3,5,7,13,17,19,31,61,89] do
    Mp:=2^p-1;
```

```
    F:=ChangeRing(E,GF(Mp));
    if IsOrdinary(F) then
      Exclude(~M,E);
      break;
    end if;
  end for;
end for;

L:=M;
# L;
540
```

Nach Möglichkeit sollte die Gruppen der $\mathbb{F}_{M_p}$-rationalen Punkte der gesuchten Kurven zyklisch sein. Das kann man wie folgt erreichen:

A.1.4 Zyklizität der Punktgruppe

```
for E in L do
  CurveList:=[ChangeRing(E,GF(2^p-1)) :p in [3,5,7,13,17,19,31,61,89]];
  if not forall(t){F: F in CurveList | IsCyclic(AbelianGroup(F))} then
    Exclude(~M,E);
  end if;
end for;

L:=M;
# L;
81
```

A.1.5 Bestimmung von x_0

```
A:=[-Floor(aInvariants(E)[4]) : E in L];
X:=[];
P:=[p : p in PrimesUpTo(10^5) | p mod 24 eq 7];
# P;
1205

for a in A do
  X1:=exists(x1){2^l*3*n^2 : l in [0..100], n in [1..100] | forall{p : p in P |
      LegendreSymbol    ((2^l*3*n^2)^2-a,p) eq -1}};
  X2:=exists(x2){-2^l*n^2 : l in [0..100], n in [1..100] | forall{p : p in P |
      LegendreSymbol((-2^l*n^2)^2-a,p) eq -1}};
  if X1 and X2 then
    if -x2 gt x1 then
      Append(~X,<a,x1>);
    else
      Append(~X,<a,x2>);
    end if;
  elif X1 then
    Append(~X,<a,x1>);
```

```
  elif X2 then
    Append(~X,<a,x2>);
  else
    Exclude(~L, EllipticCurve([-a,0]));
  end if;
end for;
```

Anhang B

Implementierung der Tests in Magma

B.1 Klassische Tests

B.1.1 Lucas-Lehmer-Test für Mersenne-Zahlen

```
LucLeh:=function(p)
  Mp:=2^p-1;
  L:=Integers(Mp)!4;
    for k in [1..p-2] do
    L:= (L^2-2);
  end for;
  return L eq 0;
end function;
```

B.1.2 Pépin-Test für Fermat-Zahlen

```
Pepin:=function(n)
  Fn:=2^(2^n)+1;
  return Modexp(3,(Fn-1) div 2, Fn) eq Fn-1;
end function;
```

Der Magma-Operator ^ funktioniert nicht für beliebig große Exponenten. Das hat zur Folge, dass die Funktion Pepin nur für n$\leq$ 29 funktioniert.

B.2 Tests mit elliptischen Kurven

B.2.1 Tests für Mersenne-Zahlen

```
EllipticMersenne:=function(p,a)
  Mp:=2^p-1;
  R:=ResidueClassRing(Mp);
  case a:
  when -8,12,54,6,-50,-968,-722:
  G:=R!-2;
  when -2,3,-242:
  G:=R!-1;
  when 108, -72 ,-450:
  G:=R!6;
  when 27,-18:
  G:=R!3;
  when 24, 216, -200, -2888:
  G:=R!-4;
  when 2700,3468:
  G:=R!-50;
  when 300:
  G:=R!-18;
  when 75:
  G:=R!-9;
  when -1352:
  G:=R!-1250;
  when -338:
  G:=R!-625;
  when -1800:
  G:=R!12;
  when 31212:
  G:=R!150;
  else
  error "Ungueltige Eingabe";
  end case;
  for k in [1..p-1] do
    G2:=G^2;
    ok, u:=IsInvertible(4*G*(G2-a));
    if not ok then
      print p;
      return false;
    end if;
    G:=(G2+a)^2*u;
  end for;
  return G eq 0;
end function;
```

Diese Funktion lässt den Benutzer sowohl den zu testenden Exponenten `p` als auch eine der neun gefundenen Kurven über den Koeffizienten `a` ihrer Weierstrass-Gleichung $y^2 = x^3 - a \cdot x$ auswerten. Die Wahl `a:=12` liefert genau den Test von Gross. Im Fall, dass die

Schleife nicht vollständig durchlaufen wird, wird zur Unterscheidung zusätzlich der Exponent p ausgegeben.

```
PrimeList:=PrimesUpTo(10^4);

Velocity:=function(a)
  if a eq 0 then
    return [2] cat [p: p in PrimeList | p ne 2 and LucLeh(p)];
  else
    return [2] cat [p: p in PrimeList | p ne 2 and EllipticMersenne(p,a)];
  end if;
end function;
```

B.2.2 Test für Fermat-Zahlen

```
DenSav:=function(n)
  K<i>:=QuadraticField(-1);
  R:=Integers(K);
  f:=2^(2^(n-1))+i;
  Res:=quo<R|f>;
  D:=Res!5;
  I:=Res!(R!i);
  z:=(Res!2)^(-1);
  for k in [1..2^n-1] do
    ok, u:= IsInvertible(D);
    if not ok then
      return false;
    end if;
    D:=z*(D/I+I*u);
  end for;
  return Res!D eq 0;
end function;
```

Wie bei der Funktion Pepin ist auch hier die Funktionalität auf n$\leq$ 30 eingeschränkt.

B.2.3 Test für Thabit-Zahlen

```
eps:=function(n)
  if n mod 4 ne 2
    then return -1;
  end if;
  if n mod 3 ne 1
    then return -3;
  end if;
  p:= 5;
  repeat
    p:= NextPrime(p);
    u:= p mod 4 eq 1 select -1 else 1;
  until LegendreSymbol( 3*Modexp(2, n, p)-1, p) eq u;
  return -p+4;
```

```
end function;

ThabitTest:=function(n)
  e:=eps(n);
  Kn:=3*2^n-1;
  R:=ResidueClassRing(Kn);
  r:=R!(e^2 - 24*e - 64)^2;
  ok, l:=IsInvertible(r);
  if not ok then
    return false;
  end if;
  T:=R!16*(e - 4)*(e^3 + 20*e^2 - 80*e - 64)*l - 2;
  for k in [1..n-1] do
    T2:=T^2;
    ok, u:=IsInvertible(4*T*(T2-e));
    if not ok then
      return false;
    end if;
    T:=(T2+e)^2*u;
  end for;
  return T eq 0;
end function;
```

Symbolverzeichnis

$[m]$ Multiplikation mit $m \in \mathbb{Z}$ auf einer elliptischen Kurve als Isogenie

$\bar{}$ nichttrivialer Körperautomorphismus eines quadratischen Zahlkörpers

$\Delta(E_f)$ Diskriminante einer elliptischen Kurve E_f

$\mathbb{F}_q$ endlicher Körper mit q Elementen

$\mathrm{Grad}(\phi)$ Grad einer Isogenie ϕ

$\left(\frac{a,b}{K}\right)$ Quaternionenalgebra über einem Körper K

$\left(\frac{a}{p}\right)$ LEGENDRE-Symbol, ist 1, falls $a \in \mathbb{F}_p^*$ ein Quadrat ist, -1 sonst

$\mathcal{A}_n(K)$ affiner Raum der Dimension n über dem Körper K

$\mathcal{P}_n(K)$ projektiver Raum der Dimension n über dem Körper K

$\mathfrak{p}$ Primideal im Ganzheitsring eines quadratischen Zahlkörpers

$\mathbb{N}$ Menge der natürlichen Zahlen $\{1, 2, 3, 4, ...\}$

$\mathbb{N}_0$ Menge der natürlichen Zahlen und 0

$\nu(\alpha)$ Norm von α, $\nu(\alpha) = \alpha \cdot \overline{\alpha}$

$\mathcal{O}$ Neutrales Element der Punktgruppe einer elliptischen Kurve, unendlich ferner Punkt

$\mathcal{O}_K$ Ganzheitsring eines algebraischen Zahlkörpers K

$\mathbb{P}$ Menge der positiven ganzen Primzahlen

Φ_r Frobenius-Endomorphismus, $x \mapsto x^{p^r}$, wo $p \in \mathbb{P}$

$\mathbb{Q}$ Körper der rationalen Zahlen

$\mathbb{Q}(\sqrt{m})$ quadratischer Zahlkörper

$\mathrm{Spur}(\alpha)$ Spur von α, $\mathrm{Spur}(\alpha) = \alpha + \overline{\alpha}$

φ EULERsche φ-Funktion, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$

$\widehat{\phi}$ duale Abbildung zur Isogenie ϕ

$\mathbb{Z}$ Ring der ganzen Zahlen $\{0, \pm 1, \pm 2, \pm 3, ...\}$

C_n zyklische Gruppe der Ordnung n

E_f elliptische Kurve über einem Körper K mit WEIERSTRASS-Polynom f

$E_f(L)$ Gruppe der L-rationalen Punkte einer elliptischen Kurve E_f für einen Erweiterungskörper L des Grundkörpers

$e_m(S,T)$ WEIL-Paarung der Punkte S und T

F_n FERMAT-Zahl $2^{2^n}+1$ für eine natürliche Zahl n oder 0

$j(E_f)$ j-Invariante einer elliptischen Kurve E_f

$K(E_f)$ Funktionenkörper der elliptischen Kurve E_f

K_n THABIT-Zahl $3 \cdot 2^n - 1$ für $n \in \mathbb{N}_0$

M_p MERSENNE-Zahl $2^p - 1$ für eine Primzahl p

R^* Gruppe der multiplikativ invertierbaren Elemente eines Ringes R

Literaturverzeichnis

[Bor72] Borho, Walter: *On Thabit ibn Kurrah's Formula for Amicable Numbers.* Mathematics of Computation, 26(118):571–578, 1972.

[Deu41] Deuring, Max: *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem. Hansischen Univ., 14:197–272, 1941.

[DS08] Denomme, Robert und Gordan Savin: *Elliptic curve primality tests for Fermat and related primes.* Journal of Number Theory, 128:2398–2412, 2008.

[Gro05] Gross, Benedict H.: *An elliptic curve test for Mersenne primes.* Journal of Number Theory, 110:114–119, 2005.

[Har77] Hartshorne, Robin: *Algebraic Geometry.* Springer-Verlag, 1977.

[Hus87] Husemöller, Dale: *Elliptic Curves.* Springer-Verlag, 1987.

[IR82] Ireland, Kenneth und Michael Rosen: *A classical Introduction to Modern Number Theory.* Springer-Verlag, 1982.

[Kne02] Kneser, Martin: *Quadratische Formen.* Springer-Verlag, 2002.

[Lan78] Lang, Serge: *Elliptic Curves - Diophantine Analysis.* Springer-Verlag, 1978.

[Neu07] Neukirch, Jürgen: *Algebraische Zahlentheorie.* Springer-Verlag, 2007.

[Rie69] Riesel, Hans: *Lucasian Criteria for the Primality of $N = h \cdot 2^n - 1$.* Mathematics of Computation, 23(108):869–875, 1969.

[RPB91] R. P. Brent, G. L. Cohen, H. J. J. te Riele: *Improved techniques for lower bounds of odd perfect numbers.* Mathematics of Computation, 57:857–868, 1991.

[RU07] Remmert, Reinhold und Peter Ullrich: *Elementare Zahlentheorie.* Birkhäuser-Verlag, 2007.

[Sil86] Silverman, Joseph H.: *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[ST92] Silverman, Joseph H. und John Tate: *Rational Points on Elliptic Curves.* Springer-Verlag, 1992.

[Str98] Stroth, Gernot: *Algebra - Einführung in die Galoistheorie.* Walter de Gruyter, 1998.

[Wer01] Werner, Annette: *Elliptische Kurven in der Kryptographie.* Springer-Verlag, 2001.

Eigenständigkeitserklärung

Hiermit versichere ich, Michael Helmut Mertens, geboren am 16. Juli 1989 in Viersen, dass die vorliegende Arbeit von mir selbstständig und ausschließlich unter Zuhilfenahme der angegebenen Quellen und Hilfsmittel verfasst wurde.

Aachen, den 28. März 2011

_____

Michael H. Mertens