Elliptische Kurven

1. Motivation

Die Sicherheit einiger Public-Key-Kryptosysteme, z.B. Diffie-Hellman-Schlüsselaustausch, ElGamal-Verschlüsselung, beruht auf zwei Tatsachen:

- Man kann schnell $g^b \bmod p$ berechnen (square-and-multiply-Methode).
- Es ist schwer, die Gleichung $g^x \equiv a \bmod p$ zu lösen (DLP - discrete logarithm problem).

Für die Verfahren wird im Wesentlichen nur benutzt, dass $\mathbb{F}_p^*$ eine Gruppe ist. Daher liegt es nahe, andere endliche Gruppen auf kryptographische Verwendungsmöglichkeiten hin zu untersuchen.
1985 haben Neal Koblitz und Victor Miller unabhängig voneinander die Verwendung elliptischer Kurven über endlichen Körpern der Gestalt $\mathbb{F}_p$ oder $\mathbb{F}_{2^n}$ vorgeschlagen.

Elliptische Kurven treten in der Mathematik an verschiedenen Stellen auf:

- in der Algebraischen Geometrie als glatte projektive Kurven vom Geschlecht 1 und als einfachstes Beispiel einer projektiven Varietät mit Gruppenstruktur,
- in der Funktionentheorie beim Studium doppeltperiodischer Funktionen,
- in der Zahlentheorie als eine wichtige Klasse diophantischer Gleichungen (Elliptische Kurven spielten beim Beweis der Fermatschen Vermutung durch Wiles 1994 eine entscheidende Rolle).

Im folgenden soll eine kurze Einführung in die elliptischen Kurven gegeben werden. Dann folgen kryptographische Anwendungen. Der Einfachkeit halber beschränken wir uns auf elliptische Kurven über Körpern der Charakteristik $\neq 2, 3$.

2. Ein Beispiel zur Sekanten- und Tangentenmethode

Die Suche nach ganzzahligen oder rationalen Lösungen von Gleichungen der Form

$$y^2 = x^3 + ax + b$$

mit vorgegebenen $a, b \in \mathbb{Z}$ hat eine lange Geschichte. So bemerkte schon Bachet 1621, dass bei der Gleichung $y^2 = x^3 - 2$ aus der Lösung $(x, y) = (3, 5)$ weitere rationale Lösungen durch die sogenannte Tangentenmethode gewonnen werden können.

Bemerkung: Ist eine ebene Kurve implizit durch eine Gleichung $f(x, y) = 0$ gegeben, und ist $P = (x_0, y_0)$ ein Punkt der Kurve, d.h. $f(x_0, y_0) = 0$, so definiert der lineare Teil der Taylorentwicklung von f in P die **Tangente an die Kurve im Punkt** $P = (x_0, y_0)$:

$$\frac{\partial f}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial f}{\partial y}(x_0, y_0)(y - y_0) = 0,$$

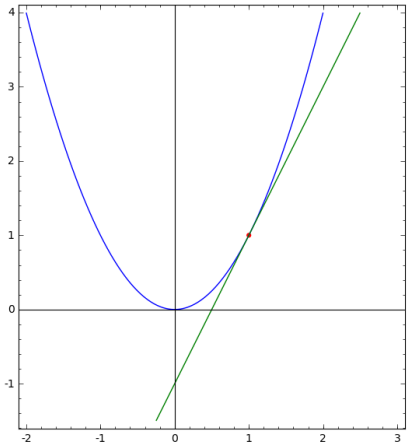
sofern $(\frac{\partial f}{\partial x}(x_0, y_0), \frac{\partial f}{\partial y}(x_0, y_0)) \neq (0, 0)$ gilt. Ist $\frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0$, so sagen wir, die Kurve besitzt keine Tangente im Punkt (x_0, y_0).

Beispiel: Die Parabel $y = x^2$ lässt sich auch durch $f(x, y) = x^2 - y = 0$ beschreiben. Die Tangente im Punkt $(1, 1)$ wird dann durch die Gleichung

$$\frac{\partial f}{\partial x}(1, 1)(x - 1) + \frac{\partial f}{\partial y}(1, 1)(y - 1) = 0 \quad \text{bzw.} \quad 2(x - 1) - (y - 1) = 0, \quad \text{bzw.} \quad y = 2x - 1$$

Datei: kii_ek.tex. Version vom 7.3.2019

beschrieben.

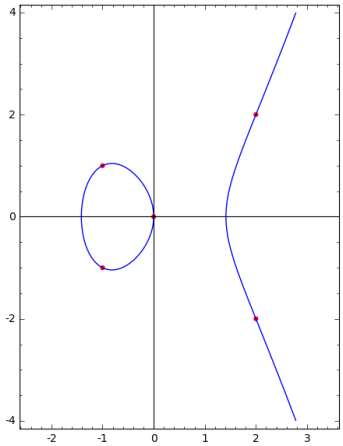


Wir geben zunächst ein Beispiel für das sogenannte Sekanten- und Tangentenverfahren, mit dem man aus bekannten rationalen Lösungen einer diophantischen Gleichung des Typs $y^2 = x^3 + ax + b$ auf geometrischem Weg neue rationale Lösungen konstruieren kann.

Beispiel: Wir suchen rationale Lösungen der Gleichung $y^2 = x^3 - 2x$. Durch Probieren findet man schnell die Lösungen

$$(x, y) = (0, 0), (-1, \pm 1), (2, \pm 2).$$

Reell stellt die Gleichung $y^2 = x^3 - 2x$ eine ebene Kurve dar, die in etwa so aussieht:



Wir wollen jetzt Sekanten und Tangenten bilden und mit der Kurve schneiden:

- Wir beschreiben die Kurve durch $f(x, y) = x^3 - 2x - y^2 = 0$. Die Tangente in einem Punkt (x_0, y_0) wird dann durch die Gleichung

  $$\frac{\partial f}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial f}{\partial y}(x_0, y_0)(y - y_0) = 0, \text{ d.h. } (3x_0^2 - 2)(x - x_0) - 2y_0(y - y_0) = 0$$

  beschrieben, was sich auch in der folgenden Form schreiben lässt:

  $$y = y_0 + \frac{3x_0^2 - 2}{2y_0}(x - x_0).$$

- Die Verbindungsgerade von $(-1, 1)$ und $(2, 2)$ ist

  $$y = \frac{1}{3}x + \frac{4}{3}.$$

Wir bestimmen die Schnittpunkte der Geraden mit der Kurve, indem wir die Geradengleichung in die Kurvengleichung $f(x,y)=0$ einsetzen:

$$f(x,\frac{1}{3}x+\frac{4}{3}) = x^3-2x-(\frac{1}{3}x+\frac{4}{3})^2 = (x+1)(x-2)(x+\frac{8}{9}).$$

Die Schnittpunkte von Kurve und Gerade sind also:

$$(-1,1), \quad (2,2), \quad (-\frac{8}{9},\frac{28}{27}),$$

also haben wir eine neue rationale Lösung $x=-\frac{8}{9}, y=\frac{28}{27}$ der Gleichung $y^2=x^3-2x$ gefunden.

- Die Tangente im Punk $(-1,1)$ berechnet sich mit obiger Formel zu

$$y=\frac{1}{2}x+\frac{3}{2}.$$

Wir schneiden die Kurve mit der Tangente, indem wir die Tangentengleichung in die Kurvengleichung einsetzen:

$$f(x,\frac{1}{2}x+\frac{3}{2}) = x^3-2x-(\frac{1}{2}x+\frac{3}{2})^2 = (x+1)^2(x-\frac{9}{4}),$$

als zusätzlichen Punkt erhalten wir also

$$(x,y)=(\frac{9}{4},\frac{21}{8}),$$

was eine neue Lösung der diophantischen Gleichung $y^2=x^3-2x$ ergibt.

- Die Tangente im Punkt $(2,2)$ ist

$$y=\frac{5}{2}x-3.$$

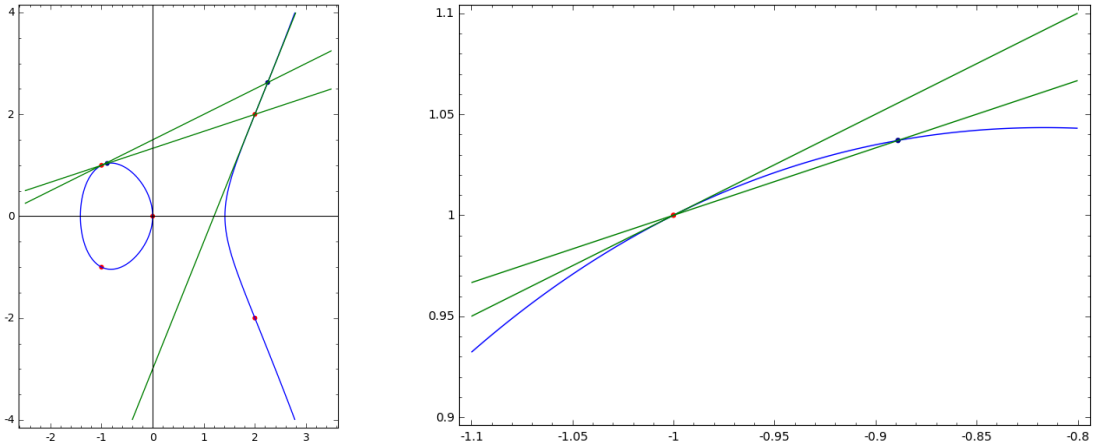
Wir setzen die Tangentengleichung in die Kurvengleichung ein:

$$f(x,\frac{5}{2}x-3) = x^3-2x+(\frac{5}{2}x-3)^2 = (x-2)^2(x-\frac{9}{4}).$$

Die Tangente schneidet die Kurve in dem weiteren Punkt $(\frac{9}{4},\frac{21}{8})$, den wir aber bereits kennen.

- Mit den vorgestellten Verfahren kann man leicht weitere rationale Lösungen der Gleichung $y^2=x^3-2x$ bestimmen.

Das linke Bild zeigt die Kurve mit den beschriebenen Geraden und Punkten, das rechte Bild zeigt eine Vergrößerung um $(-1,1)$, da die Punkte $(-1,1)$ und $(-\frac{8}{9},\frac{28}{27})$ nahe beieinander liegen:



3. Elliptische Kurven und das Additionsgesetz

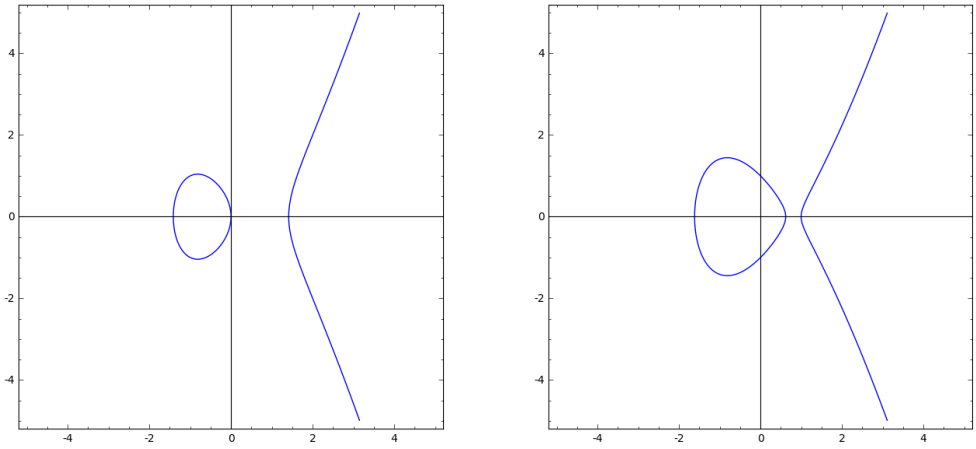
DEFINITION. *Sei K ein Körper der Charakteristik $\neq 2, 3$. Eine elliptische Kurve E über K wird gegeben durch eine Gleichung*

$$y^2 = x^3 + ax + b$$

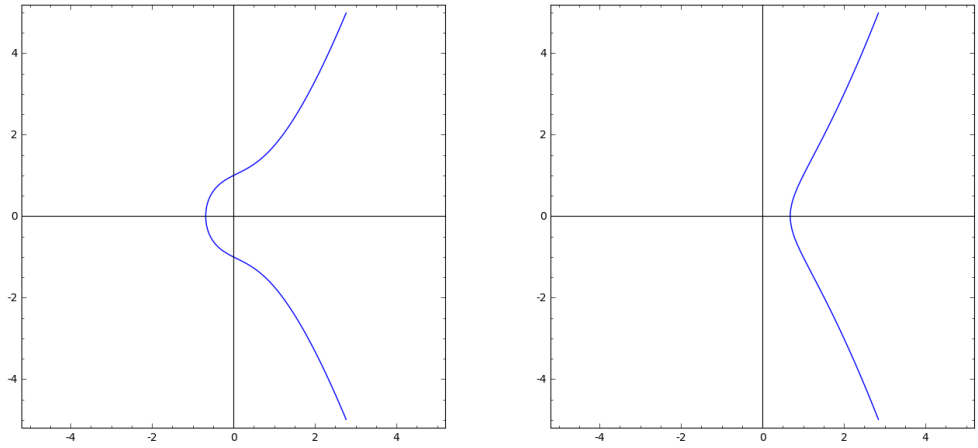
mit $a, b \in K$, wobei außerdem $\Delta = 4a^3 + 27b^2 \neq 0$ gelten muss. (Die angegebene Gleichung wird auch als Weierstraß-Gleichung für E bezeichnet.)

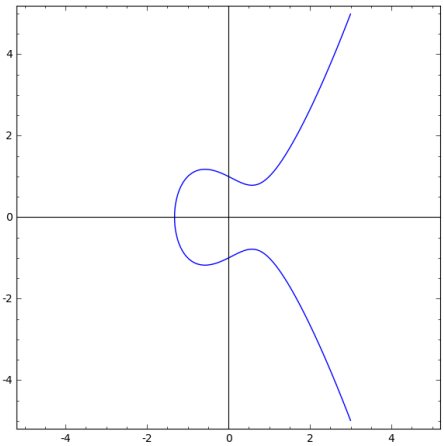
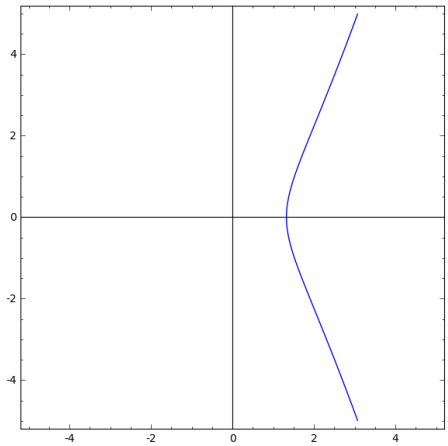
Bemerkungen:

(1) Wenn man elliptische Kurven skizzieren will, zeichnet man meist reelle Bilder: Hier sind Zeichnungen für $y^2 = x^3 - 2x$ und $y^2 = x^3 - 2x + 1$:



Eine Kurve des Typs $y^2 = x^3 + ax + b$ muss reell nicht besonders interessant aussehen: Hier sind Bilder für $y^2 = x^3 + x + 1$, $y^2 = x^3 + x - 1$, $y^2 = x^3 - x + 1$, $y^2 = x^3 - x - 1$:



(2) Wir beschränken uns hier auf elliptische Kurven über Körpern der Charakteristik $\neq 2, 3$. Will man beliebige Charakteristiken zulassen, startet man mit Gleichungen der Gestalt

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

Für kryptographische Anwendungen ist allerdings auch Charakteristik 2 interessant.

Die Bedingung $\Delta = 4a^3 + 27b^2 \neq 0$ in der Definition einer elliptischen Kurve bedeutet, dass die Kurve $y^2 = x^3 + ax + b$ in jedem Punkt eine Tangente besitzt, wie das folgende Lemma zeigt:

LEMMA. *Sei K ein Körper der Charakteristik $\neq 2, 3$ und $a, b \in K$.*

(1) *Ist $f(x, y) = x^3 + ax + b - y^2 \in K[x, y]$ und $x_0, y_0 \in K$, so ist die Taylorentwicklung von f in (x_0, y_0)*

$$\begin{aligned} f(x,y) &= f(x_0,y_0) + \Big((3x_0^2 + a)(x - x_0) - 2y_0(y - y_0)\Big) + \\ &\quad + \Big(3x_0(x - x_0)^2 - (y - y_0)^2\Big) + (x - x_0)^3. \end{aligned}$$

(2) *Sind $x_0, y_0 \in K$ mit $y_0^2 = x_0^3 + ax_0 + b$, so ist die Tangente an die Kurve $y^2 = x^3 + ax + b$ im Punkt (x_0, y_0) gegeben durch die Gleichung*

$$(3x_0^2 + a)(x - x_0) - 2y_0(y - y_0) = 0,$$

falls $(3x_0^2 + a, 2y_0) \neq (0, 0)$ ist.

(3) *Ist $4a^3 + 27b^2 \neq 0$, so gilt für alle $x_0, y_0 \in K$ mit $y_0^2 = x_0^3 + ax_0 + b$*

$$3x_0^2 + a \neq 0 \quad \textit{oder} \quad 2y_0 \neq 0,$$

d.h. die Tangente an $y^2 = x^3 + ax + b$ in (x_0, y_0) existiert und ist gegeben durch die Gleichung

$$(3x_0^2 + a)(x - x_0) - 2y_0(y - y_0) = 0.$$

(4) *Sei nun $4a^3 + 27b^2 = 0$.*
   (a) *Ist $a = 0$, so ist auch $b = 0$. Die Kurve $y^2 = x^3$ besitzt keine Tangente in $(0, 0)$.*
   (b) *Ist $a \neq 0$, definiert man*

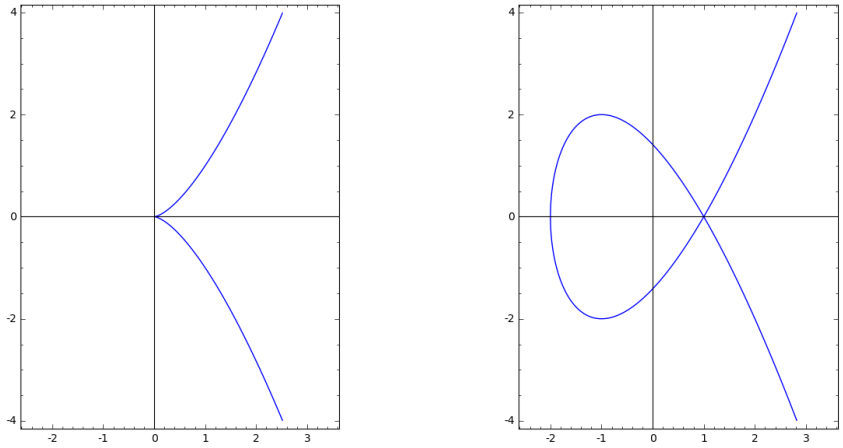
$$x_0 = -\frac{3b}{2a}, \quad y_0 = 0,$$

so gilt

$$y_0^2 = x_0^3 + ax_0 + b, \quad 3x_0^2 + a = 0, \quad 2y_0 = 0,$$

d.h. (x_0, y_0) ist ein Punkt der Kurve $y^2 = x^3 + ax + b$, in dem die Tangente nicht existiert.

Das linke Bild zeigt die Kurve $y^2 = x^3$, das rechte die Kurve $y^2 = x^3 - 3x + 2$:



Beweis:

(1) Die Taylorentwicklung kann man einfach nachrechnen.

(2) Die Kurve $y^2 = x^3 + ax + b$ lässt sich durch die Gleichung $f(x, y) = 0$ beschreiben. Die Tangente in einem Kurvenpunkt (x_0, y_0) ist durch

$$(3x_0^2 + a)(x - x_0) - 2y_0(y - y_0) = 0$$

gegeben, falls dieses lineare Polynom von 0 verschieden ist.

(3) Wir nehmen an, es gilt $3x_0^2 + a = 0$ und $2y_0 = 0$, also $y_0 = 0$. Dann gilt

$$a = -3x_0^2$$

und wegen $y_0^2 = x_0^3 + ax_0 + b$ und $y_0 = 0$

$$b = y_0^2 - x_0^3 - ax_0 = -x_0^3 - (-3x_0^2)x_0 = -x_0^3 + 3x_0^3 = 2x_0^3.$$

Es folgt

$$4a^3 + 27b^2 = 4(-3x_0^2)^3 + 27(2x_0^3)^2 = -4 \cdot 27x_0^6 + 27 \cdot 4x_0^6 = 0.$$

Da dies ausgeschlossen war, stimmt die Annahme nicht. Die Behauptung ist also richtig.

(4) (a) Klar.

(b) Es gilt

$$\begin{aligned} x_0^3 + ax_0 + b &= \frac{-27b^3}{8a^3} + a\frac{-3b}{2a} + b = \frac{-27b^3 - 4a^3 \cdot 3b + 8a^3 b}{8a^3} = \\ &= \frac{-b(27b^2 + 4a^3)}{8a^3} = 0 = y_0^2 \end{aligned}$$

und

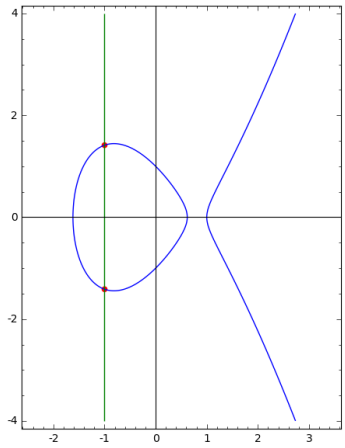
$$3x_0^2 + a = 3\frac{9b^2}{4a^2} + a = \frac{27b^2 + 4a^3}{4a^2} = 0, \quad 2y_0 = 0.$$

Mit dem Sekanten- und Tangentenverfahren wollen wir jetzt eine Verknüpfung auf elliptischen Kurven definieren.

Schnitte elliptischer Kurven mit Sekanten und Tangenten: Sei die elliptische Kurve E gegeben durch die Gleichung $y^2 = x^3 + ax + b$, die wir auch in der Form $f(x, y) = 0$ mit $f(x, y) = x^3 + ax + b - y^2$ schreiben können.

(1) **Sekantenschnitte:** Seien Kurvenpunkte $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, d.h. $y_i^2 = x_i^3 + ax_i + b$, gegeben mit $P_1 \neq P_2$. Es gibt 2 Fälle:

(a) $x_1 = x_2$. Wegen $P_1 \neq P_2$ gilt dann $y_1 = -y_2$. Die Verbindungsgerade von P_1 und P_2 ist dann $x = x_1$ und schneidet die Kurve nur in den Punkten P_1 und P_2.



(b) $x_1 \neq x_2$. Die Verbindungsgerade ist

$$y = m(x - x_1) + y_1 \quad \text{mit} \quad m = \frac{y_1 - y_2}{x_1 - x_2}.$$

Wir setzen dies in $f(x, y)$ ein und bilden

$$\begin{aligned} g(x) &= f(x, m(x - x_1) + y_1) = x^3 + ax + b - (m(x - x_1) + y_1))^2 = \\ &= x^3 - m^2x^2 + (a + 2m^2x_1 - 2my_1)x + (b - m^2x_1^2 + 2mx_1y_1 - y_1^2). \end{aligned}$$

$g(x)$ ist ein normiertes kubisches Polynom mit

$$g(x_1) = f(x_1, y_1) = 0 \quad \text{und} \quad g(x_2) = f(x_2, m(x_2 - y_1) + y_1) = f(x_2, y_2) = 0,$$

sodass ein $x_3 \in K$ existiert mit

$$g(x) = (x - x_1)(x - x_2)(x - x_3).$$

Es ist

$$g(x) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3.$$

Vergleicht man die Koeffizienten bei x^2, so erhält man

$$x_1 + x_2 + x_3 = m^2, \quad \text{also} \quad x_3 = m^2 - x_1 - x_2.$$

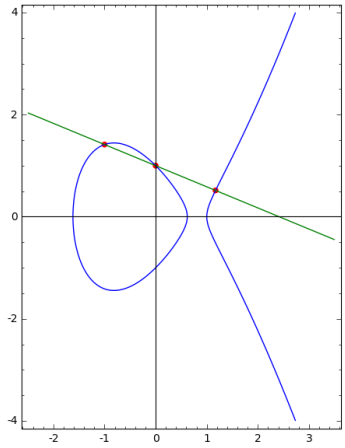
Definiert man dazu

$$y_3 = m(x_3 - x_1) + y_1,$$

so ist wegen $f(x_3, y_3) = f(x_3, m(x_3 - x_1) + y_1) = g(x_3) = 0$

$$(x_3, y_3)$$

ein Kurvenpunkt, der auf der Geraden liegt.

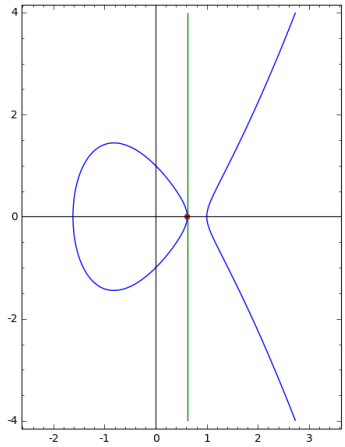


(2) **Tangentenschnitte:** Sei $P_1 = (x_1, y_1)$ ein Kurvenpunkt, d.h. $y_1^2 = x_1^3 + ax_1 + b$. Die Tangentengleichung lautet

$$(3x_1^2 + a)(x - x_1) - 2y_1(y - y_1) = 0.$$

Es gibt wieder 2 Fälle:

(a) **Fall $y_1 = 0$:** Die Tangentengleichung ist $x = x_1$, die Tangente schneidet die Kurve nur im Punkt $P_1 = (x_1, y_1)$.



(b) **Fall $y_1 \neq 0$:** Die Taylorentwicklung von $f(x, y)$ in (x_1, y_1) ist

$$f(x, y) = (3x_1^2 + a)(x - x_1) - 2y_1(y - y_1) + 3x_1(x - x_1)^2 - (y - y_1)^2 + (x - x_1)^3,$$

die Tangente

$$y = m(x - x_1) + y_1 \text{ mit } m = \frac{3x_1^2 + a}{2y_1}.$$

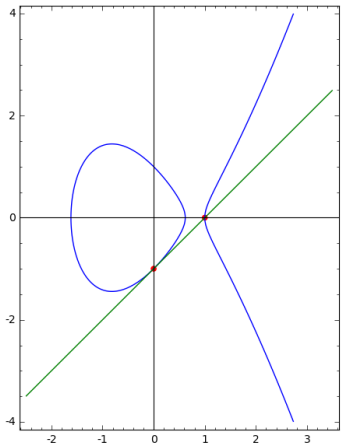
Wir setzen die Tangentengleichung in $f(x, y)$ ein:

$$\begin{aligned} g(x) &= f(x, y_1 + m(x - x_1)) = \\ &= (3x_1^2 + a)(x - x_1) - 2y_1 \cdot m(x - x_1) + \\ &\quad +3x_1(x - x_1)^2 - (m(x - x_1))^2 + (x - x_1)^3 = \\ &= 3x_1(x - x_1)^2 - m^2(x - x_1)^2 + (x - x_1)^3 = \\ &= (x - x_1)^2(3x_1 - m^2 + x - x_1) = (x - x_1)^2(x - (m^2 - 2x_1)). \end{aligned}$$

Definiert man also

$$x_3 = m^2 - 2x_1 \quad \text{und} \quad y_3 = m(x_3 - x_1) + y_1,$$

so ist (x_3, y_3) ein weiterer Schnittpunkt der Tangente mit der Kurve.



Hat man zwei Punkte auf einer elliptischen Kurve gegeben, so schneidet die Verbindungsgerade die Kurve im Allgemeinen in einem weiteren Punkt. Dies legt die Einführung einer Verknüpfung nahe. Da es aber nicht immer einen weiteren Schnittpunkt gibt, führen wir einen zusätzlichen Punkt ein:

DEFINITION. *Sei E eine elliptische Kurve über K, gegeben durch eine Gleichung $y^2 = x^3 + ax + b$. Die Menge der K-rationalen Punkte von E oder die Menge der über K definierten Punkte von E wird definiert als*

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{O\},$$

wo O ein zusätzlicher Punkt ist, der sogenannte unendlich ferne Punkt oder der Punkt im Unendlichen. Ist L ein Erweiterungskörper von K, also $K \subseteq L$, so ist die elliptische Kurve natürlich auch über L definiert. Die Menge der L-rationalen Punkte ist dann ganz analog

$$E(L) = \{(x, y) \in L \times L : y^2 = x^3 + ax + b\} \cup \{O\}.$$

Bemerkung: Nimmt man den projektiven Abschluß einer elliptischen Kurve in der projektiven Ebene $¶^2$, so kommt ein unendlich ferner Punkt hinzu, der hier mit O bezeichnet wird.

Bemerkungen: Wie beschreibt man elliptische Kurven und Punkt mit dem Computer?

(1) Sage: Mit `E=EllipticCurve(GF(p),[a,b])` führt man eine elliptische Kurve E über $\mathbb{F}_p$ ein. Ist $P = (x, y) \in E(\mathbb{F}_p)$ so lautet der Sage-Befehl `P=E(x,y)` oder `P=E([x,y])`. P gibt den Punkt als $(x : y : 1)$ aus. Alternativ: `P=E([2,0,1])` oder `P=E(2,0,1)` oder .... Der Punkt O ist in Sage $(0 : 1 : 0)$, den man in der Form `P=E(0,1,0)` oder auch `P=E(0)` einführen kann.
(2) In unseren Python3-Programmen geben wir eine elliptische Kurve als Tripel `[p,a,b]` an. Punkte schreiben wir in der Form `[x,y]`, den Punkt O als leere Liste `[]`.

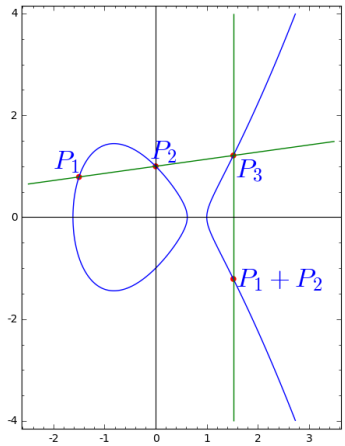
Beispiel: Sei E über $\mathbb{F}_{11}$ gegeben durch $y^2 = x^3 + x + 1$. Dann ist

$$E(\mathbb{F}_{11}) = \{O, (0, 1), (0, 10), (1, 5), (1, 6), (2, 0), (3, 3), (3, 8), (4, 5), (4, 6), (6, 5), (6, 6), (8, 2), (8, 9)\}.$$

Die elliptische Kurve E hat also 14 Punkte über $\mathbb{F}_5$.

Wir wollen jetzt auf einer elliptischen Kurve E über K eine Verknüpfung einführen. Die Idee ist folgende: Sind $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ zwei Punkte der Kurve, so schneidet die Verbindungsgerade der beiden Punkte (bzw. die Tangente im Fall $P_1 = P_2$) die Kurve im Allgemeinen in einem weiteren Kurvenpunkt $P_3 = (x_3, y_3)$. Die Summe der Punkte P_1 und P_2 ist der an der x-Achse gespiegelte Punkt:

$$P_1 + P_2 = (x_3, -y_3),$$



Gibt es keinen weiteren Schnittpunkt, so lösen wir das Problem mit Hilfe des unendlich fernen Punktes O.

Vollständig und mit Formeln ergibt sich folgendes Bild:

DEFINITION. *Sei E eine über einem Körper K der Charakteristik $\neq 2, 3$ durch $y^2 = x^3 + ax + b$ definierte elliptische Kurve. Wir definieren eine Verknüpfung $+$ auf der Menge der K-rationalen Punkte $E(K)$ wie folgt:*

- *Für alle $P \in E(K)$ sei $P + O = O + P = P$.*
- *Gilt für $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K)$ die Beziehung $x_1 = x_2$ und $y_1 + y_2 = 0$, so sei $P_1 + P_2 = O$.*
- *Gilt für $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K)$ die Beziehung $x_1 \neq x_2$ oder ($x_1 = x_2$ und $y_1 = y_2 \neq 0$), so sei $P_1 + P_2 = (x_3, y_3)$ mit*

$$m = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & \text{falls } x_1 \neq x_2, \\ \frac{3x_1^2 + a}{2y_1} & \text{falls } x_1 = x_2, y_1 = y_2 \neq 0 \end{cases}$$

und

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1.$$

Hier ist eine algorithmische Darstellung der Addition:

Addition auf einer elliptischen Kurve:

Eingabe: Eine über einem Körper K ($\mathrm{char}(K) \neq 2, 3$) durch $y^2 + x^3 + ax + b$ definierte elliptische Kurve E und Punkte $P_1, P_2 \in K(E)$

Ausgabe: $P_1 + P_2 \in E(K)$

if $P_1 = O$ **then**
    return P_2
end if
if $P_2 = O$ **then**
    return P_1
end if
$(x_1, y_1) = P_1$, $(x_2, y_2) = P_2$
if $x_1 = x_2$ **then**
    if $y_1 + y_2 = 0$ **then**
        return O
    end if
    $m \leftarrow \frac{3x_1^2 + a}{2y_1}$
else
    $m \leftarrow \frac{y_1 - y_2}{x_1 - x_2}$
end if

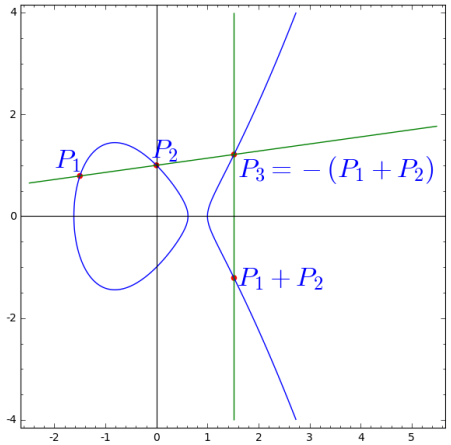
16: $x_3 \leftarrow m^2 - x_1 - x_2$, $y_3 \leftarrow m(x_1 - x_3) - y_1$
17: **return** (x_3, y_3)

Das fundamentale Ergebnis, das wir hier nicht beweisen werden, ist nun:

SATZ. *Ist E eine elliptische Kurve über K, so ist $(E(K), +)$ eine abelsche Gruppe mit neutralem Element O. Das Inverse von $P = (x, y)$ ist $-P = (x, -y)$.*

Bemerkung: Schneidet die Gerade (bzw. Tangente) durch Kurvenpunkte P_1, P_2 in einem dritten Punkt P_3, so gilt also

$$P_3 = -(P_1 + P_2).$$



Mit dem folgenden kleinen Python3-Programm kann man Punkte aus $E(\mathbb{F}_p)$ addieren. Der Vollständigkeit halber ist auch eine Funktion zum Invertieren modulo n angegeben:

```
def invmod(a,n): # Berechnung des Inversen von a modulo n
  u,v,y,yy=n,a%n,0,1
  while v>0:
    q=u//v
    u,v,y,yy=v,u-q*v,yy,y-q*yy
  return y%n

def ek_add(P1,P2,pab):
  p,a,b=pab
  if P1==[]:
    return P2
  if P2==[]:
    return P1
  x1,y1=P1
  x2,y2=P2
  if x1==x2:
    if (y1+y2)%p==0:
      return []
    m=((3*x1**2+a)*invmod(2*y1,p))%p
  else:
    m=((y1-y2)*invmod(x1-x2,p))%p
  x3=(m**2-x1-x2)%p
  y3=(m*(x1-x3)-y1)%p
  return [x3,y3]
```

Bei den folgenden Beispielen wurde das Programm benutzt:

Beispiel: Wir wählen $K = \mathbb{F}_5$ und die Kurve $E : y^2 = x^3 + x + 2$ (Es ist $\Delta = 4 \cdot 1^3 + 27 \cdot 2^2 = 2 \neq 0$.) Man findet

$$E(\mathbb{F}_5) = \{O, P_1 = (1, 2), P_2 = (1, 3), P_3 = (4, 0)\}.$$

Durch Benutzung der Formeln erhalten wir folgende Verknüpfungstabelle:

$+$	O	P_1	P_2	P_3
O	O	P_1	P_2	P_3
P_1	P_1	P_3	O	P_2
P_2	P_2	O	P_3	P_1
P_3	P_3	P_2	P_1	O

$E(\mathbb{F}_5)$ ist also eine zyklische Gruppe der Ordnung 4, erzeugt z.B. von P_1: $2P_1 = P_3$, $3P_1 = P_2$, $4P_1 = O$.

Bemerkung: Ist A eine additiv geschriebene abelsche Gruppe, so ist bekanntlich für $n \in \mathbb{Z}$ und $a \in A$ das Produkt $n \cdot a$ durch

$$n \cdot a = \underbrace{a + \cdots + a}_{n \text{ Summanden}} \text{ für } n \geq 1,$$

$$0 \cdot a = 0 \quad \text{und} \quad n \cdot a = |n| \cdot (-a) \text{ für } n < 0$$

definiert.

Für $a \in \mathbb{Z}$, $d \in \mathbb{N}$, $n \in \mathbb{N}$ gibt es einige „square-and-multiply“-Methoden, um die Potenz

$$a^d \bmod n$$

schnell zu berechnen. Wir beschreiben eine additive Variante:

Überlegung: Ist A eine additiv geschriebene abelsche Gruppe, $n \in \mathbb{N}$ und

$$n = \sum_{i=0}^{r} n_i \cdot 2^i \text{ mit } n_i \in \{0, 1\}$$

die Binärzerlegung von n, so gilt

$$n \cdot a = \sum_{i=0}^{r} (n_i \cdot 2^i) \cdot a = \sum_{i=0}^{r} n_i \cdot (2^i a) = \sum_{\substack{0 \leq i \leq r \\ n_i = 1}} 2^i a.$$

Zur Berechnung von $n \cdot a$ muss man also nur Verdoppeln:

$$a, \quad 2a, \quad 2^2 a = 2 \cdot 2a, \quad 2^3 a = 2 \cdot 2^2 a, \quad 2^4 a = 2 \cdot 2^3 a, \quad \ldots$$

und die Terme $2^i a$ mit $n_i = 1$ aufaddieren. Man erhält daraus leicht algorithmische Varianten:

Berechnung von $n \cdot a$ für $n \in \mathbb{N}_0$ und $a \in A$ mit einer additiv geschriebenen abelschen Gruppe A (double-and-add-Verfahren, d.h. additives square-and-multiply-Verfahren):
Eingabe: Additiv geschriebene abelsche Gruppe A, $a \in A$, $n \in \mathbb{N}_0$
Ausgabe: $n \cdot a$

```
1: b ← 0, c ← a
2: while n > 0 do
3:     if n ≡ 1 mod 2 then
4:         b ← b + c
5:     end if
6:     c ← c + c
7:     n ← ⌊n/2⌋
8: end while
9: return b
```

Wir schreiben das Verfahren nochmals für elliptische Kurven auf:

Berechnung von $n \cdot P$ für $P \in E(K)$ für eine elliptische Kurve E über K:
Eingabe: Elliptische Kurve E, definiert über einem Körper K, $P \in E(K)$, $n \in \mathbb{N}_0$
Ausgabe: $n \cdot P$
1: $Q \leftarrow O$, $R \leftarrow P$
2: **while** $n > 0$ **do**
3: **if** $n \equiv 1 \bmod 2$ **then**
4: $Q \leftarrow Q + R$
5: **end if**
6: $R \leftarrow R + R$
7: $n \leftarrow \lfloor \frac{n}{2} \rfloor$
8: **end while**
9: **return** Q

Hier ist eine zugehörige Python3-Funktion:

```
def ek_mult(n,P,pab):
  Q,R=[],P[:]
  while n>0:
    if n%2==1:
      Q=ek_add(Q,R,pab)
    R=ek_add(R,R,pab)
    n=n//2
  return Q
```

Bemerkung: Mit obigem Verfahren kann man $n \cdot P$ für $n \in \mathbb{N}_0$ und $P \in E(\mathbb{F}_p)$ auf einer über $\mathbb{F}_p$ definierten elliptischen Kurve E schnell berechnen. Dies ist von zentraler Bedeutung für die Anwendung elliptischer Kurven in der Kryptographie.

Wir geben noch ein paar ganz einfache Beispiele elliptischer Kurven an.

Beispiel: E werde über $\mathbb{F}_5$ durch $y^2 = x^3 + x + 1$ definiert. (Wegen $\Delta = 4 \cdot 1^3 + 27 \cdot 1^2 = 1 \neq 0$ ist E eine elliptische Kurve.) Es ist

$$E(\mathbb{F}_5) = \{O, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}.$$

Mit den Formeln und $P = (0,1)$ findet man

$$P = (0,1), 2P = (4,2), 3P = (2,1), 4P = (3,4), 5P = (3,1), 6P = (2,4), 7P = (4,3), 8P = (0,4), 9P = O,$$

also ist $E(\mathbb{F}_5)$ eine zyklische Gruppe der Ordnung 9.

Beispiel: $y^2 = x^3 + 4x$ definiert über $\mathbb{F}_5$ wegen $4 \cdot 4^3 + 27 \cdot 0^2 \neq 0 \in \mathbb{F}_5$ eine elliptische Kurve. Man findet

$$E(\mathbb{F}_5) = \{O, (0,0), (1,0), (2,1), (2,4), (3,2), (3,3), (4,0)\}$$

und

$$2 \cdot E(\mathbb{F}_5) = \{O, (0,0)\} \quad \text{und} \quad 4 \cdot E(\mathbb{F}_5) = \{O\},$$

insbesondere ist $E(\mathbb{F}_5)$ eine nichtzyklische Gruppe der Ordnung 8.

Bemerkung: Ist A eine additiv geschriebene abelsche Gruppe und $n \in \mathbb{N}$, so schreibt man

$$A[n] = \{a \in A : n \cdot a = 0\}$$

für die Untergruppe der n-Torsionselemente.

DEFINITION. *Ist E eine über dem Körper K definierte elliptische Kurve und $n \in \mathbb{N}$, so nennt man $P \in E(\overline{K})$ einen* n**-Teilungspunkt** *oder* n**-Torsionspunkt**, *falls gilt*

$$n \cdot P = O.$$

Der Untergruppe der n-Teilungspunkte ist

$$E(\overline{K})[n] = \{P \in E(\overline{K}) : n \cdot P = O,$$

die auch kurz $E[n]$ geschrieben wird. Die über K definierten n-Teilungspunkte sind

$$E(K)[n] = \{P \in E(K) : n \cdot P = O\}$$

und bilden natürlich ebenfalls eine Untergruppe.

Wir geben eine geometrische Charakterisierung der 2-Teilungspunkte an:

SATZ. *Sei E eine durch die Gleichung $y^2 = x^3 + ax + b$ über einem Körper K der Charakteristik $\neq 2, 3$ definierte elliptische Kurve. Dann gilt:*

(1) *$P = (x, y) \in E(K) \setminus \{O\}$ ist genau dann ein 2-Teilungspunkt, wenn $y = 0$ (und damit $x^3 + ax + b = 0$) gilt.*
(2) *Es gibt genau drei Möglichkeiten:*
   - *Hat das Polynom $x^3 + ax + b$ keine Nullstelle in K, so ist*
   $$E(K)[2] = \{O\}.$$
   - *Hat das Polynom $x^3 + ax + b$ genau eine Nullstelle c in K, so ist*
   $$E(K)[2] = \{O, (c, 0)\}.$$
   - *Hat das Polynom $x^3 + ax + b$ genau drei Nullstellen c_1, c_2, c_3 in K, so ist*
   $$E(K)[2] = \{O, (c_1, 0), (c_2, 0), (c_3, 0)\} \simeq Z_2 \times Z_2.$$

Beweis:

(1) Für einen Punkt $P = (x, y)$ gilt:
$$\begin{aligned} P \text{ ist 2-Teilungspunkt} \quad &\iff \quad 2P = O \quad \iff P = -P \quad \iff \\ &\iff \quad (x, y) = (x, -y) \quad \iff \quad y = 0. \end{aligned}$$

(2) Natürlich ist O wegen $2O = O$ ein 2-Teilungspunkt. Mit (1) erhält man nun:
   - Hat $x^3 + ax + b$ keine Nullstelle in K, so ist O der einzige 2-Teilungspunkt in $E(K)$.
   - Hat $x^3 + ax + b$ genau eine Nullstelle c in K, so ist $\{O, (c, 0)\} \simeq Z_2$ die Menge der 2-Teilungspunkte.
   - Hat $x^3 + ax + b$ (mindestens) zwei verschiedene Nullstellen c_1, c_2 in K, so erhält man durch Polynomdivision eine weitere Nullstelle $c_3 \in K$:
   $$x^3 + ax + b = (x - c_1)(x - c_2)(x - c_3).$$
   Wäre $c_3 \in \{c_1, c_2\}$, also o.E. $c_3 = c_1$, so würde aus
   $$x^3 + ax + b = (x - c_1)^2(x - c_3) = x^3 - (2c_1 + c_2)x^2 + (c_1^2 + 2c_1c_2)x - c_1^2c_2$$
   zunächst $c_2 = -2c_1$ und damit dann
   $$x^3 + ax + b = (x - c_1)(x + 2c_1) = x^3 - 3c_1^2x + 2c_1^3,$$
   also
   $$a = -3c_1^2, \quad b = 2c_1^3$$
   folgen. Dann wäre aber
   $$4a^3 + 27b^2 = 4(-3c_1^2)^3 + 27(2c_1^3) = -4 \cdot 27c_1^6 + 27 \cdot 4c_1^6 = 0,$$
   was aber ausgeschlossen war. Daher hat $x^3 + ax + b$ die 3 verschiedenen Nullstellen c_1, c_2, c_3, und damit ist $\{O, (c_1, 0), (c_2, 0), (c_3, 0)\}$ die Menge der 2-Teilungspunkte.

Wir werden uns später auf elliptische Kurven E über Körpern $\mathbb{F}_p$ mit einer Primzahl $p \geq 5$ beschränken. Einige naheliegende Fragen sind:

- Welche Gruppenstruktur hat $E(\mathbb{F}_p)$?
- Was ist $\#E(\mathbb{F}_p)$?
- Wie findet man einen Punkt $P \in E(\mathbb{F}_p) \setminus \{0\}$?

4. Wie findet man Punkte in $E(\mathbb{F}_p)$?

Wir werden uns ab jetzt auf elliptische Kurven $E : y^2 = x^3 + ax + b$ über einem Körper $\mathbb{F}_p$ mit einer Primzahl $p \geq 5$ beschränken. Zu $x_0 \in \mathbb{F}_p$ suchen wir nach Punkten $(x_0, *) \in E(\mathbb{F}_p)$:

LEMMA. *Sei $p \geq 5$ eine Primzahl und E eine durch $y^2 = x^3 + ax + b$ über $\mathbb{F}_p$ definierte elliptische Kurve. Sei $x_0 \in \mathbb{F}_p$.*

- *Gilt $\left(\frac{x_0^3+ax_0+b}{p}\right) = -1$, so gibt es keinen Punkt aus $E(\mathbb{F}_p)$ mit x-Koordinate x_0.*
- *Gilt $\left(\frac{x_0^3+ax_0+b}{p}\right) = 0$, so gibt es genau einen Punkt mit x-Koordinate x_0 in $E(\mathbb{F}_p)$, nämlich*

$$(x_0, 0).$$

- *Gilt $\left(\frac{x_0^3+ax_0+b}{p}\right) = 1$, so gibt es genau zwei Punkte mit x-Koordinate x_0 in $E(\mathbb{F}_p)$: Ist $w \in \mathbb{F}_p$ eine Quadratwurzel aus $x_0^3 + ax_0 + b$, so sind dies die Punkte*

$$(x_0, w) \quad \text{und} \quad (x_0, p - w).$$

Insbesondere ist die Anzahl der Punkte aus $E(\mathbb{F}_p)$ mit x-Koordinate x_0

$$\left(\frac{x_0^3 + ax_0 + b}{p}\right) + 1.$$

Beweis: Die Punkte der Gestalt $(x_0, *) \in E(\mathbb{F}_p)$ sind genau die Punkte (x_0, y) mit

$$y^2 = x_0^3 + ax_0 + b.$$

Man muss also untersuchen, ob $x_0^3 + ax_0 + b$ ein Quadrat in $\mathbb{F}_p$ ist und gegebenfalls die Quadratwurzel ziehen. Dabei ergibt sich die angegebene Fallunterscheidung und der Rest. ■

Man kann also also Punkte aus $E(\mathbb{F}_p)$ auslisten, was natürlich nur für kleine p sinnvoll ist:

Bestimmung von $E(\mathbb{F}_p)$:
Eingabe: Elliptische Kurve E über $\mathbb{F}_p$ durch Gleichung $y^2 = x^3 + ax + b$
Ausgabe: $E(\mathbb{F}_p)$

```
M ← {O}
for x = 0, ..., p − 1 do
    z ← x^3 + ax + b
    if z = 0 then
        M ← M ∪ {(x, 0)}
    else if (z/p) = 1 then
        Bestimme mit einem Quadratwurzelalgorithmus ein y ∈ F_p mit y^2 = z
        M ← M ∪ {(x, y), (x, p − y)}
    end if
end for
return M als E(F_p)
```

Hier ist eine zugehörige Python3-Funktion:

```
# Auflistung aller Punkte der elliptischen Kurve pab - nur fuer kleine p
# sinnvoll
def ek_punkte(pab):
  p,a,b=pab
  M=[]
  M.append([])
  for x in range(p):
    z=(x**3+a*x+b)%p
    if z==0:
      M.append([x,0])
    elif jac(z,p)==1:
      y=sqrtp(z,p)
      M.append([x,y])
      M.append([x,p-y])
  return M
```

Das Lemma liefert auch sofort eine Formel für die Anzahl $\#E(\mathbb{F}_p)$:

SATZ. *Ist E eine über $\mathbb{F}_p$ durch $y^2 = x^3 + ax + b$ definierte elliptische Kurve, so gilt für die Anzahl der $\mathbb{F}_p$-rationalen Punkte*

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right).$$

Beweis: Wir haben gesehen, dass es zu $x \in \mathbb{F}_p$ genau $\left(\frac{x^3+ax+b}{p}\right)+1$ Punkte $(x, *) \in E(\mathbb{F}_p)$ gibt. Außerdem gibt es noch den Punkt O. Insgesamt folgt

$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} (\left(\frac{x^3 + ax + b}{p} \right) + 1) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right),$$

was zu zeigen war. ■

Eine zugehörige Python3-Funktion könnte so aussehen:

```
# Bestimmung der Anzahl #E(F_p) mit der Anzahlformel - nur fuer kleine p
# sinnvoll
def ek_anzahl(pab):
  p,a,b=pab
  n=p+1
  for x in range(p):
    n+=jac(x**3+a*x+b,p)
  return n
```

Beispiele: Für die ersten Primzahlen bestimmen wir alle Zahlen $\#E_{a,b}(\mathbb{F}_p)$ (für die Kurven $y^2 = x^3 + ax + b$). Ein $-$ bedeutet, dass $4a^3 + 27b^2 = 0$ in $\mathbb{F}_p$ ist, dass also keine elliptische Kurve vorliegt.

(1) $p = 5$

$\#E_{a,b}(\mathbb{F}_5)$	0	1	2	3	4
0	-	6	6	6	6
1	4	9	4	4	9
2	2	7	-	-	7
3	10	-	5	5	-
4	8	8	3	3	8

Als Anzahlen $\#E(\mathbb{F}_5)$ kommen die Zahlen

$$2, 3, 4, 5, 6, 7, 8, 9, 10$$

vor.

(2) $p = 7$

$\#E_{a,b}(\mathbb{F}_7)$	0	1	2	3	4	5	6
0	-	12	9	13	3	7	4
1	8	5	-	6	10	-	11
2	8	5	-	6	10	-	11
3	8	12	9	6	10	7	4
4	8	5	-	6	10	-	11
5	8	12	9	6	10	7	4
6	8	12	9	6	10	7	4

Als Anzahlen $\#E(\mathbb{F}_7)$ kommen die Zahlen

$$3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13$$

vor.

(3) $p = 11$

$\#E_{a,b}(\mathbb{F}_{11})$	0	1	2	3	4	5	6	7	8	9	10
0	-	12	12	12	12	12	12	12	12	12	12
1	12	14	16	18	9	11	13	15	6	8	10
2	12	16	9	-	17	10	14	7	-	15	8
3	12	18	13	8	14	9	15	10	16	11	6
4	12	9	6	14	11	8	16	13	10	18	15
5	12	11	10	9	8	18	6	16	15	14	13
6	12	-	14	15	16	17	7	8	9	10	-
7	12	15	7	10	-	16	8	-	14	17	9
8	12	17	-	16	10	15	9	14	8	-	7
9	12	8	15	11	18	14	10	6	13	9	16
10	12	10	8	17	15	-	-	9	7	16	14

Als Anzahlen $\#E(\mathbb{F}_{11})$ kommen die Zahlen

$$6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18$$

vor.

(4) $p = 13$

$\#E_{a,b}(\mathbb{F}_{13})$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	-	12	19	9	21	16	7	7	16	21	9	19	12
1	20	18	12	-	14	9	13	13	9	14	-	12	18
2	10	8	15	18	17	12	16	16	12	17	18	15	8
3	20	18	12	-	14	9	13	13	9	14	-	12	18
4	8	19	-	16	15	10	14	14	10	15	16	-	19
5	10	8	15	18	17	12	16	16	12	17	18	15	8
6	10	8	15	18	17	12	16	16	12	17	18	15	8
7	18	16	10	13	12	20	11	11	20	12	13	10	16
8	18	16	10	13	12	20	11	11	20	12	13	10	16
9	20	18	12	-	14	9	13	13	9	14	-	12	18
10	8	19	-	16	15	10	14	14	10	15	16	-	19
11	18	16	10	13	12	20	11	11	20	12	13	10	16
12	8	19	-	16	15	10	14	14	10	15	16	-	19

Als Anzahlen $\#E(\mathbb{F}_{13})$ kommen die Zahlen

$$7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21$$

vor.

(5) $p = 17$

$\#E_{a,b}(\mathbb{F}_{17})$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	-	18	18	18	18	18	18	18	18	18	18	18	18	18	18	18	18
1	16	18	24	17	14	15	20	12	25	25	12	20	15	14	17	24	18
2	20	24	19	22	16	18	11	12	21	21	12	11	18	16	22	19	24
3	26	15	16	12	20	23	21	14	-	-	14	21	23	20	12	16	15
4	16	24	14	20	25	12	15	17	18	18	17	15	12	25	20	14	24
5	26	-	15	14	16	21	12	23	20	20	23	12	21	16	14	15	-
6	10	22	24	16	15	21	-	20	13	13	20	-	21	15	16	24	22
7	10	24	15	-	13	20	21	16	22	22	16	21	20	13	-	15	24
8	20	19	16	11	21	12	18	22	24	24	22	18	12	21	11	16	19
9	20	21	24	12	19	11	22	18	16	16	18	22	11	19	12	24	21
10	10	13	22	20	24	-	16	21	15	15	21	16	-	24	20	22	13
11	10	15	13	21	22	16	20	-	24	24	-	20	16	22	21	13	15
12	26	16	20	21	-	14	23	12	15	15	12	23	14	-	21	20	16
13	16	25	18	12	24	20	17	15	14	14	15	17	20	24	12	18	25
14	26	20	-	23	15	12	14	21	16	16	21	14	12	15	23	-	20
15	20	16	21	18	24	22	12	11	19	19	11	12	22	24	18	21	16
16	16	14	25	15	18	17	12	20	24	24	20	12	17	18	15	25	14

Als Anzahlen $\#E(\mathbb{F}_{17})$ kommen die Zahlen

$$10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26$$

vor.

Durch die Beispiele motiviert, erwähnen wir zwei wichtige Sätze:

Satz (Hasse). *Ist E eine über $\mathbb{F}_p$ definierte elliptische Kurve, so gilt*

$$p + 1 - 2\sqrt{p} < \#E(\mathbb{F}_p) < p + 1 + 2\sqrt{p},$$

was auch in der Form

$$|\#E(\mathbb{F}_p) - (p + 1)| < 2\sqrt{p}$$

geschrieben werden kann.

Satz (Deuring). *Ist $p \geq 5$ eine Primzahl, so gibt es zu jeder natürlichen Zahl N mit*

$$p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p}$$

eine über $\mathbb{F}_p$ definierte elliptische Kurve E, für die

$$\#E(\mathbb{F}_p) = N$$

gilt.

Mit dem Lemma können wir natürlich auch einfach Punkte auf einer elliptischen Kurve konstruieren, auch wenn p groß ist:

Eingabe: Elliptische Kurve $E : y^2 + ax + b$ über $\mathbb{F}_p$, $x_0 \in \mathbb{F}_p$
Ausgabe: $(x, y) \in E(\mathbb{F}_p)$ mit $x = x_0 + \delta$ und δ „minimal ≥ 0“

1: $x \leftarrow x_0$
2: **while** $\left(\frac{x^3+ax+b}{p}\right) = -1$ **do**
3: $\quad x \leftarrow x + 1$
4: **end while**
5: $y \leftarrow \sqrt{x^3 + ax + b}$, d.h. y erfüllt $y^2 = x^3 + ax + b$
6: **return** (x, y)

Hier ist eine mögliche Python3-Funktion dazu:

```
# Zu x0 wird x minimal mit x>=x0 bestimmt, sodass [x,*] ein Kurvenpunkt
# ist. Ausgegeben wird der gefundene Kurvenpunkt [x,*].
def ek_nxtpkt(x,pab):
  p,a,b=pab
  x=x%p
  while jac(x**3+a*x+b,p)==-1:
    x=x+1
  y=sqrtp(x**3+a*x+b,p)
    return [x,y]
```

Bemerkung: Wir überlegen naiv: Die Hälfte aller Zahlen in $\mathbb{F}_p$ ist ein Quadrat, also sollte die Wahrscheinlichkeit, dass bei Vorgabe von x die Gleichung $y^2 = x^3 + ax + b$ lösbar ist, ungefähr $\frac{1}{2}$ sein. Mit obigem Algorithmus sollte man also schnell einen Kurvenpunkt finden.

Beispiel: Wir haben für $p = 2^{63}+29$ (kleinste Primzahl mit 64 Bits) und die elliptischen Kurven $E_{a,b}$ mit $b = 2a - 1$, $1 \leq a \leq 10^6$ jeweils die ersten 10 Punkte $(x_1, y_1), \ldots, (x_{10}, y_{10})$ mit $0 \leq x_1 < x_2 < \cdots < x_{10}$ bestimmt und geschaut, wie groß die Lücken zwischen aufeinanderfolgenden Punkten sind. Die größte Lücke $x_{i+1} - x_i$ war 27 und trat bei folgendem Beispiel auf:

$$p = 9223372036854775837, \quad a = 598559, \quad b = 1197117$$

mit den aufeinanderfolgenden Punkten

$$(4, 1748577092592839446)$$
$$(6, 1768796861020725752)$$
$$(9, 938004650129235389)$$
$$(10, 3403621942798732139)$$
$$(37, 3890818200182748697)$$
$$(38, 4151293106323329339)$$
$$(39, 2582428572206569044)$$
$$(41, 437031169802445950)$$
$$(42, 4486032537256344212)$$
$$(43, 943360154636082863)$$

Punktkompression: Sei E eine durch $y^2 = x^3 + ax + b$ über $\mathbb{F}_p$ definierte elliptische Kurve. Ist $P = (x, y) \in E(\mathbb{F}_p)$, so hat auch

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

die gleiche x-Koordinate. Wie kann man P von $-P$ unterscheiden, wenn man nur die x-Koordinate kennt? Denken wir uns y repräsentiert durch eine Zahl aus $\{0, 1, \ldots, p\}$, so gilt

$$(y \bmod 2) \neq ((p - y) \bmod 2).$$

Wenn wir also y mod 2 angeben, ist P dadurch eindeutig bestimmt.

5. Diffie-Hellman-Schlüsselaustausch, ElGamal-Verschlüsselung und ein Signaturverfahren mit elliptischen Kurven

Wir sind nun in der Lage, einfache Public-Key-Verfahren auf elliptische Kurven zu übertragen.
Wir haben gesehen: Ist E eine über $\mathbb{F}_p$ definierte elliptische Kurve und $P \in E(\mathbb{F}_p)$, so lässt sich für $n \in \mathbb{N}$ der Punkt $n \cdot P \in E(\mathbb{F}_p)$ schnell (mit einer additiven Variante des square-and-multiply-Verfahrens) berechnen. Ist $Q \in E(\mathbb{F}_p)$ gegeben, so nennt man $x \in \mathbb{Z}$ einen **diskreten Logarithmus** von Q zur Basis P in der Gruppe $E(\mathbb{F}_p)$, wenn gilt

$$Q = x \cdot P.$$

Die Berechnung von diskreten Logarithmen ist im Allgemeinen schwierig. Sie ist für die Sicherheit der nachfolgenden Verfahren wesentlich.

Diffie-Hellman-Schlüsselaustausch mit elliptischen Kurven:

(1) Zugrunde liegt eine Primzahl p, eine elliptische Kurve $E : y^2 = x^3 + ax + b$ über $\mathbb{F}_p$, ein Punkt $P \in E(\mathbb{F}_p)$.
(2) Als privaten Schlüssel wählt sich Teilnehmer A eine Zahl e_A und berechnet $Q_A = e_A \cdot P \in E(\mathbb{F}_p)$. Genauso wählt Teilnehmer B eine Zahl $e_B \in \mathbb{N}$ und berechnet $Q_B = e_B \cdot P \in E(\mathbb{F}_p)$. Veröffentlicht werden Q_A und Q_B.
(3) Der gemeinsame Schlüssel ist nun der Punkt
$$(x_k, y_k) = e_A e_B \cdot P = e_A \cdot Q_B = e_B \cdot Q_A,$$
den sich A als $e_A \cdot Q_B$ und B als $e_B \cdot Q_A$ berechnen kann.

Vorbemerkungen zur ElGamal-Verschlüsselung:

(1) Bei der klassischen ElGamal-Verschlüsselung liegt eine Primzahl p und eine Zahl $g \in \mathbb{F}_p^*$ zugrunde. A hat einen geheimen Schlüssel $e_A \in \mathbb{N}$ und berechnet dann seinen öffentlichen Schlüssel f_A als
$$f_A = g^{e_A} \in \mathbb{F}_p^*.$$
Zur Verschlüsselung eines Texts wird dieser in eine Zahlenfolge $a_i \in \mathbb{F}_p$ umgewandelt. Nach Wahl von Zufallszahlen z_i wird mit dem öffentlichen Schlüssel von A
$$b_i = g^{z_i}, \quad c_i = a_i f_A^{z_i}$$
berechnet. Der Chiffretext ist das Zahlenpaar (b_i, c_i).
Für die Entschlüsselung benutzt A die Beziehung
$$b_i^{e_A} = g^{z_i e_A} = f_A^{z_i}$$
und erhält damit sofort
$$a_i = \frac{c_i}{b_i^{e_A}}.$$
Hier spielt alles in der Gruppe $\mathbb{F}_p^*$. Statt $\mathbb{F}_p^*$ könnte man die Formeln auch in einer anderen multiplikativ geschriebenen Gruppe lesen. (Ist die Gruppe nicht kommutativ, sollte man die letzte Formel besser in der Form $a_i = c_i (b_i^{e_A})^{-1}$ schreiben.)
(2) Man kann die vorangegangenen Formeln auch additiv für eine additiv geschriebene, abelsche Gruppe E aufschreiben: Zugrunde liegt also eine abelsche Gruppe E und ein Element $g \in E$. Teilnehmer A wählt geheim $e_A \in \mathbb{N}$ und berechnet in E
$$f_A = e_A \cdot g \in E.$$
Will jemand verschlüsselt eine Nachricht an A schicken, wandelt er sie nach einem vereinbarten Schema in eine Folge $a_i \in E$ um, wählt Zufallszahlen $z_i \in \mathbb{N}$ und berechnet
$$b_i = z_i \cdot g \in E \quad \text{und} \quad c_i = a_i + z_i \cdot f_A \in E.$$
Der Chiffretext besteht aus den Paaren (b_i, c_i). Wegen
$$z_i \cdot f_A = z_i \cdot e_A \cdot g = e_A \cdot z_i \cdot g = e_A \cdot b_i$$
entschlüsselt A die Nachricht leicht über die Formel
$$a_i = c_i - e_A \cdot b_i.$$
Eine wesentliche Frage ist hier, wie man Text in eine Folge $a_i \in E$ umwandeln kann.
(3) Es ist bei elliptischen Kurven überhaupt nicht klar, wie man einen Text in eine Punktfolge aus $E(\mathbb{F}_p)$ übersetzen soll: Nicht zu jeder Zahl $a_i \in \mathbb{F}_p$ gibt es einen Punkt $(a_i, \dots) \in E(\mathbb{F}_p)$. Es gibt Ideen, wie man dies bewerkstelligen kann, wir werden es aber einfacher machen.

ElGamal-Verschlüsselung mit elliptischen Kurven: (Eine mögliche Variante)

(1) **Schlüsselerzeugung:**
   (a) Man einigt sich auf eine Primzahl $p > 3$, eine elliptische Kurve E über $\mathbb{F}_p$, gegeben durch eine Gleichung $y^2 = x^3 + ax + b$, einen Punkt $P \in E(\mathbb{F}_p)$.
   (b) Jeder Teilnehmer A wählt sich geheim eine natürliche Zahl e_A und berechnet $Q_A = e_A P \in E(\mathbb{F}_p)$. Der öffentliche Schlüssel von A ist Q_A, der geheime Schlüssel ist e_A.

(2) **Verschlüsselung:**
   (a) Will B eine Nachricht geheim an A schicken, besorgt er sich den öffentlichen Schlüssel Q_A von A und übersetzt die Nachricht nach einem festgelegten Verfahren in eine Folge von Zahlen $a_i \in \mathbb{F}_p$.
   (b) Für jede Zahl a_i wählt B eine Zufallszahl $z_i \in \mathbb{N}$ und berechnet nacheinander in $E(\mathbb{F}_p)$ bzw. $\mathbb{F}_p$

$$R_i = z_i \cdot P = (x_{R_i}, y_{R_i}), \quad S_i = z_i \cdot Q_A = (x_{S_i}, y_{S_i}), \quad t_i = a_i + x_{S_i}.$$

   Die verschlüsselte Nachricht besteht dann aus der Tripeln

$$(x_{R_i}, y_{R_i}, t_i)$$

   bzw. mit Punktkompression

$$(x_{R_i}, y_{R_i} \bmod 2, t_i).$$

(3) **Entschlüsselung:** A setzt bzw. berechnet

$$R_i = (x_{R_i}, y_{R_i}), \quad S_i = e_A \cdot R_i = (x_{S_i}, y_{S_i}), \quad a_i = t_i - x_{S_i}$$

   und erhält nach Umwandlung von a_i den Ausgangstext.

Überlegung: Wie kann ein Außenstehender C an die Nachricht a_i kommen, wenn er außer P und Q_A auch R_i und t_i kennt? Die Kenntnis von a_i ist äquivalent mit der Kenntnis von x_{S_i}, also (Punktkompression) mit $S_i = z_i e_A \cdot P$. Wie kann C aus $z_i \cdot P$ und $e_A \cdot P$ den Punkt $z_i e_A \cdot P$ berechnen? Dies ist das Diffie-Hellman-Problem. Zwei Möglichkeiten sind: C kommt an z_i oder an e_A.

- e_A ist der diskrete Logarithmus von Q_A zur Basis P in $E(\mathbb{F}_p)$, der aber praktisch nicht zu berechnen sein sollte bei geeigneter Parameterwahl.
- z_i ist der diskrete Logarithmus von R_i zur Basis P in $E(\mathbb{F}_p)$, der auch praktisch nicht zu berechnen sein sollte.
- Eine andere Möglichkeit ergibt sich, wenn C die Zufallszahl z_i erraten kann, z.B. bei schlechter Wahl des Zufallszahlengenerators.

Das Verschlüsselungssystem ist also (nach heutigem Stand) sicher, wenn man die entsprechenden diskreten Logarithmen praktisch nicht berechnen kann und wenn die verwendeten Zufallszahlen gut sind.

Bemerkung: Die folgende Kurve (NIST-Kurve P-256 (aus FIPS 186-4)) wird zur Zeit bei kryptographischen Anwendungen eingesetzt: $y^2 = x^3 + ax + b$ über $\mathbb{F}_p$ mit Basispunkt (G_x, G_y).

$$\begin{aligned}
p &= 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1 = \\
&= 115792089210356248762697446949407573530086143415290314195533631308867097853951 = \\
&= \texttt{0xffffffff00000001000000000000000000000000ffffffffffffffffffffffff} \\
a &= -3 \\
b &= 41058363725152142129326129780047268409114441015993725554835256314039467401291 = \\
&= \texttt{0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b} \\
G_x &= 48439561293906451759052585252797914202762949526041747995844080717082404635286 \\
&= \texttt{0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296} \\
G_y &= 36134250956749795798585127919587881956611106672985015071877198253568414405109 \\
&= \texttt{0x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5} \\
n &= 115792089210356248762697446949407573529996955224135760342422259061068512044369 = \\
&= \texttt{0xffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551}
\end{aligned}$$

Dabei ist n die Gruppenordnung $\#E(\mathbb{F}_p)$. Die Zahl n ist eine Primzahl.

Das folgende ECDSA-Signierverfahren ist ein Signierfahren, dessen Verwendung von NIST gebilligt wurde. In FIPS 186-4 wird es beschrieben, auch werden dort einige elliptische Kurven zur Verwendung vorgeschlagen.

ECDSA (Elliptic Curve Digital Signature Algorithm): Als systemweite Parameter wählt man eine elliptische Kurve E über $\mathbb{F}_p$ und einen Punkt $P \in E(\mathbb{F}_p)$ der Ordnung q, wo q eine Primzahl ist. (q sollte ungefähr die gleiche Größe wie p haben.) Außerdem benutzt man noch eine festgewählte Hashfunktion h, z.B. SHA-256.

(1) **Schlüsselerzeugung:** Jeder Teilnehmer A wählt sich eine (zufällige) Zahl e_A mit $1 < e_A < q-1$ und berechnet $Q_A = e_A P$. Der öffentliche Schlüssel von A ist Q_A, der private e_A.

(2) **Signatur-Erzeugung:** A unterschreibt ein (digital vorliegendes) Dokument M folgendermaßen:
   (a) A wählt eine Zufallszahl z mit $1 < z < q-1$.
   (b) A berechnet (auf der elliptischen Kurve)
   $$z \cdot P = (x_1, y_1) \text{ mit } 0 \le x_1 \le p-1 \text{ und } r = x_1 \bmod q \text{ mit } 0 \le r \le q-1.$$
   Ist $r = 0$, wählt A eine andere Zufallszahl z.
   (c) A berechnet den Hashwert $h(M)$ des Dokuments M und damit
   $$s = \frac{1}{z}(h(M) + e_A r) \bmod q.$$
   Im Fall $s = 0$, wählt A eine andere Zufallszahl.
   (d) Die Signatur von A für das Dokument M ist das Paar (r, s).

(3) **Signatur-Überprüfung:** Will eine Person B überprüfen, ob die Signatur (r, s) für das Dokument M tatsächlich von A stammt, geht er so vor:
   (a) B überprüft zunächst, ob
   $$1 \le r, s \le q-1$$
   gilt. Ist dies nicht der Fall, wird die Signatur nicht akzeptiert.
   (b) B bestimmt den Hashwert $h(M)$ des Dokuments M und berechnet dann nacheinander
   $$u_1 = \frac{h(M)}{s} \bmod q, \quad u_2 = \frac{r}{s} \bmod q, \quad (x_0, y_0) = u_1 P + u_2 Q_A, \quad v = x_0 \bmod q.$$
   (c) B akzeptiert die Unterschrift nur dann, falls $v = r$ gilt.

Bemerkung: Warum gilt $v = r$, wenn alles richtig gelaufen ist? Unter Beachtung der Tatsache, dass $\operatorname{ord}(P) = q$ und damit die Implikation $a \equiv b \bmod q \Longrightarrow a \cdot P = b \cdot P$ gilt, erhält man

$$(x_0, y_0) = u_1 P + u_2 Q_A = \frac{h(M)}{s} \cdot P + \frac{r e_A}{s} \cdot P = \frac{h(M) + e_A r}{s} \cdot P = z \cdot P = (x_1, y_1),$$

also $x_0 = x_1$ und damit $r = v$.

Beispiel: Wir legen die in FIPS 186-4 vorgeschlagene Kurve P-192 zugrunde. Die Kurve hat folgende Parameter:

$$\begin{aligned}
p &= \text{FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFF} = \\
&= 6277101735386680763835789423207666416083908700390324961279, \\
a &= -3 = \\
&= \text{FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFC} = \\
&= 6277101735386680763835789423207666416083908700390324961276, \\
b &= \text{64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1} = \\
&= 2455155546008943817740293915197451784769108058161191238065, \\
N &= \#E(\mathbb{F}_p) = q = \text{ (Primzahl)} \\
&= \text{FFFFFFFFFFFFFFFFFFFFFFFF99DEF836146BC9B1B4D22831} = \\
&= 6277101735386680763835789423176059013767194773182842284081, \\
P_x &= \text{188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF1012} = \\
&= 6020462823756886567582134805875261119166989766368846848 18, \\
P_y &= \text{7192B95FFC8DA78631011ED6B24CDD573F977A11E794811} = \\
&= 1740503322936220314048575522802194103640234889273866506 41.
\end{aligned}$$

Wir haben nachgeprüft, dass p und q (wahrscheinliche) Primzahlen sind, und dass $P \in E(\mathbb{F}_p)$ und $k \cdot P = O$ gilt.
Als privaten Schlüssel wählen wir ein zufälliges e und berechnen damit den öffentlichen Schlüssel $Q = e \cdot P$:

$$\begin{aligned} e &= 79888162211721479494675401361434501920004307248303240022 0, \\ Q_x &= 24696554746320021036802553270030880325813375039594445648 94, \\ Q_y &= 47136307991050723856972590431112384893762734393157846164 63. \end{aligned}$$

Wir wollen ein Dokument M mit folgendem SHA-1-Hashwert h signieren:

$$\begin{aligned} h &= (83a67d1760ef5ef6adbdff1a00009dd8124d872c)_{16} = \\ &= 75159061167196374296339533259994854548174677790 0. \end{aligned}$$

Als Zufallszahl wählen wir

$$z = 44435801450156040444515434650633281125849996798520723370 16.$$

Damit erhalten wir

$$\begin{aligned} (x_1, y_1) &= z \cdot P, \\ x_1 &= 48978500792397967822752284705760479817319613163170324909 86, \\ y_1 &= 14688451539084342785959083711486329996520342784042300567 99, \\ r &= x_1 \bmod q = \\ &= 48978500792397967822752284705760479817319613163170324909 86 = \\ &= \text{C7BFF0D8DC7D258FF02E48728E94A092DF0F5529FE2E27EA}, \\ s &= (h + er/z \bmod q = \\ &= 49523752462458269376345905681713450020759285384766672404 16 = \\ &= \text{C9F935CA0F907B80126F032FEC11D472D1FF8CD7E6947FE0}. \end{aligned}$$

Die Signatur ist also

C7BFF0D8DC7D258FF02E48728E94A092DF0F5529FE2E27EAC9F935CA0F907B80126F032FEC11D472D1FF8CD7E6947FE0

mit 96 Zeichen in Hexadezimaldarstellung.
Zum Überprüfen der Signatur bilden wir nacheinander

$$\begin{aligned} u_1 &= \frac{h}{s} \bmod q = 42186846984231057983192699795952791815354611815085043061 57, \\ u_2 &= \frac{r}{s} \bmod q = 23780256756827482628325781396536395927030237575954276765 24, \\ (x_0, y_0) &= u_1 P + u_2 Q = (48978500792397967822752284705760479817319613163170324909 86, \\ &\quad 14688451539084342785959083711486329996520342784042300567 99), \\ v &= x_0 \bmod q = 48978500792397967822752284705760479817319613163170324909 86. \end{aligned}$$

Die Signatur ist gültig, da $r = v$ gilt.

6. Isomorphie elliptischer Kurven

Für elliptische Kurven führt man einen Isomorphiebegriff ein, der sich wie folgt charakterisieren lässt:

DEFINITION. *Zwei über einem Körper K der Charakteristik $\neq 2, 3$ definierte elliptische Kurven $E : y^2 = x^3 + ax + b$ und $E' : y^2 = x^3 + a'x + b'$ heißen isomorph über K, wenn ein $u \in K^*$ existiert mit*

$$a' = u^4 a \quad \text{und} \quad b' = u^6 b.$$

Eine unmittelbare Auswirkung der Definition ist folgender Satz:

SATZ. *Sind $E : y^2 = x^3 + ax + b$ und $E' : y^2 = x^3 + a'x + b'$ über K isomorphe elliptische Kurven mit $a' = u^4 a$, $b' = u^6 b$ für ein $u \in K^*$, so liefert*

$$E(K) \to E'(K), \quad (x, y) \mapsto (u^2 x, u^3 y)$$

einen Gruppenisomorphismus.

Beweis: Ist $(x,y) \in E(K)$, so gilt $y^2 = x^3 + ax + b$ und damit $(u^3y)^2 = (u^2x)^3 + au^4(u^2x) + bu^6$, d.h. $(u^2x, u^3y) \in E'(K)$. Die angegebene Abbildung ist also sinnvoll definiert. Die Bijektivität ist klar, da die Umkehrabbildung die gleiche Gestalt hat, aber mit dem Parameter $\frac{1}{u}$. Mit den expliziten Formeln für die Addition sieht man, daß die Abbildung ein Gruppenhomomorphismus ist. ■

Beispiel: Wir betrachten alle elliptischen Kurven über $K = \mathbb{F}_5$. Es ist

$$\{(u^4, u^6) : u \in K^*\} = \{(1,1),(1,4)\} = \{(1,1),(1,-1)\}.$$

Wollen wir also die Kurven $y^2 = x^3 + ax + b$ bis auf Isomorphie klassifizieren, so können wir $0 \le a \le 4$ und $0 \le b \le 2$ voraussetzen. Durch die Bedingung $4a^3 + 27b^2 \neq 0$ werden die Fälle $(0,0)$, $(2,2)$, $(3,1)$ ausgeschlossen. Die Isomorphieklassen elliptischer Kurven über $\mathbb{F}_5$ werden also durch die Kurven $y^2 = x^3 + ax + b$ mit

$$(a,b) \in \{(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(3,0),(3,2),(4,0),(4,1),(4,2)\}$$

repräsentiert.

(a,b)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(3,0)	(3,2)	(4,0)	(4,1)	(4,2)
$\#E_{a,b}(\mathbb{F}_5)$	6	6	4	9	4	2	7	10	5	8	8	3
$E_{a,b}(\mathbb{F}_5)$	Z_6	Z_6	$Z_2 \times Z_2$	Z_9	Z_4	Z_2	Z_7	Z_{10}	Z_5	$Z_2 \times Z_4$	Z_8	Z_3

DEFINITION. *Sei E eine durch $y^2 = x^3 + ax + b$ über K definierte elliptische Kurve. Dann heißt*

$$j = j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

die j-Invariante von E. ($1728 = 12^3$.)

Beispiele: Genau die Kurven $y^2 = x^3 + b$ (mit $b \neq 0$) haben j-Invariante 0, genau die Kurven $y^2 = x^3 + ax$ (mit $a \neq 0$) haben j-Invariante 1728.

SATZ. *Seien E und E' zwei über einem Körper K definierte elliptische Kurven. Dann gilt:*

1. *Sind E und E' isomorph über K, so ist $j(E) = j(E')$. (Sind E und E' isomorph über K, so natürlich auch über jedem Oberkörper L von K.)*
2. *Gilt $j(E) = j(E')$, so sind E und E' isomorph über dem algebraischen Abschluss $\overline{K}$ von K.*

Beweis: E sei durch $y^2 = x^3 + ax + b$, E' durch $y^2 = x^3 + a'x + b'$ definiert.

(1) Sind E und E' isomorph über K, so gibt es ein $u \in K^*$ mit $a' = u^4a$, $b' = u^6b$, woraus sofort

$$j(E') = 1728\frac{4a'^3}{4a'^3 + 27b'^2} = 1728\frac{4u^{12}a^3}{4u^{12}a^3 + 27u^{12}b^2} = 1728\frac{4a^3}{4a^3 + 27b^2} = j(E)$$

folgt.

(2) Sei nun $j(E) = j(E')$.

- Ist $j(E) = 0 = j(E')$, so ist $a = a' = 0$. Wählt man ein $u \in \overline{K}^*$ mit $u^6 = \frac{b'}{b}$, so hat man $a' = u^4a$, $b' = u^6b$, E und E' sind also isomorph über $\overline{K}$.
- Ist $j(E) = 1728 = j(E')$, so ist $b = b' = 0$. Die Wahl von $u \in \overline{K}^*$ mit $u^4 = \frac{a'}{a}$ führt wegen $a' = u^4a$, $b' = u^6b$ zu einem Isomorphismus von E und E' über $\overline{K}$.
- Sei jetzt $j(E) = j(E') \neq 0, 1728$. Dann sind $a, a', b, b' \neq 0$. Die Gleichung $j(E) = j(E')$ führt zu $a^3(4a'^3 + 27b'^2) = a'^3(4a^3 + 27b^2)$, was sofort

$$a^3b'^2 = a'^3b^2$$

ergibt. Wählt man $u \in \overline{K}^*$ mit

$$u^2 = \frac{ab'}{a'b},$$

so folgt unter Verwendung obiger Gleichung

$$u^4 = \frac{a^2b'^2}{a'^2b^2} = \frac{a^3b'^2}{aa'^2b^2} = \frac{a'^3b^2}{aa'^2b^2} = \frac{a'}{a}$$

und

$$u^6 = \frac{a^3 {b'}^3}{{a'}^3 b^3} = \frac{a^3 {b'}^2 b'}{{a'}^3 b^2 b} = \frac{b'}{b},$$

was die Isomorphie von E und E' über $\overline{K}$ zeigt. ■

Der folgende Satz beschreibt die $\mathbb{F}_p$-Isomorphieklassen elliptischer Kurven $\mathbb{F}_p$ in Abhängigkeit von der j-Invariante:

SATZ. *Sei $p \geq 5$ eine Primzahl. Für $a, b \in \mathbb{F}_p$ (mit $4a^3+27b^2 \neq 0$) bezeichne $E_{a,b}$ die durch $y^2 = x^3+ax+b$ über $\mathbb{F}_p$ definierte elliptische Kurve.*

(1) $j \neq 0, 1728$.
   (a) *Es gilt: $j(E_{a,b}) \neq 0, 1728 \iff a, b \neq 0$. (Genau die Kurven $y^2 = x^3 + ax + b$ mit $a, b \neq 0$ und $4a^3 + 27b^2 \neq 0$ haben also eine j-Invariante $\neq 0, 1728$.)*
   (b) *Gilt $j(E_{a,b}) = j(E_{\widetilde{a},\widetilde{b}}) \neq 0, 1728$, so gibt es ein $u \in \mathbb{F}_p^*$ mit*

$$\widetilde{a} = au^2, \quad \widetilde{b} = bu^3.$$

   Die Zahl u ist durch diese Eigenschaft eindeutig bestimmt, es ist

$$u = \frac{\widetilde{b}a}{\widetilde{a}b}.$$

   (c) *Ist $j(E_{a,b}) \neq 0, 1728$ und $u \in \mathbb{F}_p^*$, so gilt*

$$j(E_{a,b}) = j(E_{au^2,bu^3}).$$

   Weiter gilt

$$E_{a,b} \text{ ist über } \mathbb{F}_p \text{ isomorph zu } E_{au^2,bu^3} \quad \iff \quad \left(\frac{u}{p}\right) = 1.$$

   (d) *Ist $j \in \mathbb{F}_p \setminus \{0, 1728\}$, setzt man*

$$c = \frac{j}{j - 1728},$$

   so gilt

$$j(E_{-3c,2c}) = j.$$

   (e) *Für $j \neq 0, 1728$ gibt es genau zwei $\mathbb{F}_p$-Isomorphieklassen elliptischer Kurven über $\mathbb{F}_p$ mit j-Invariante j. Gilt $j(E_{a,b}) = j$ und $\left(\frac{u}{p}\right) = -1$, so repräsentieren*

$$E_{a,b} \quad \text{und} \quad E_{au^2,bu^3}$$

   diese Isomorphieklassen.

(2) $j = 1728$.
   (a) *Es gilt: $j(E_{a,b}) = 1728 \iff a \neq 0, b = 0$. (Genau die Kurven $y^2 = x^3 + ax$ (mit $a \neq 0$) haben j-Invariante 1728.)*
   (b) *Im Fall $p \equiv 1 \bmod 4$ sind $E_{a,0}$ und $E_{\widetilde{a},0}$ genau dann isomorph über $\mathbb{F}_p$, wenn gilt*

$$a^{\frac{p-1}{4}} = \widetilde{a}^{\frac{p-1}{4}}.$$

   Es gibt vier $\mathbb{F}_p$-Isomorphieklassen elliptischer Kurven mit j-Invariante 1728. Wählt man vier Zahlen

$$a_1, a_2, a_3, a_4 \in \mathbb{F}_p^* \quad \text{mit} \quad \#\{a_1^{\frac{p-1}{4}}, a_2^{\frac{p-1}{4}}, a_3^{\frac{p-1}{4}}, a_4^{\frac{p-1}{4}}\} = 4,$$

   so bilden $E_{a_1,0}, E_{a_2,0}, E_{a_3,0}, E_{a_4,0}$ ein Repräsentantensystem der Isomorphieklassen.
   (c) *Im Fall $p \equiv 3 \bmod 4$ sind $E_{a,0}$ und $E_{\widetilde{a},0}$ genau dann isomorph über $\mathbb{F}_p$, wenn gilt*

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

   Es gibt in diesem Fall zwei $\mathbb{F}_p$-Isomorphieklassen elliptischer Kurven mit j-Invariante 1728. Repräsentanten sind beispielsweise $y^2 = x^3 + x$ und $y^2 = x^3 - x$.

(3) $j = 0$.

(a) *Es gilt:* $j(E_{a,b}) = 0 \iff a = 0, b \neq 0$. *(Genau die Kurven* $y^2 = x^3 + b$ *(mit* $b \neq 0$*) haben* j*-Invariante* 0*.)*

(b) *Im Fall* $p \equiv 1 \bmod 3$ *sind die Kurven* $E_{0,b}$ *und* $E_{0,\widetilde{b}}$ *genau dann isomorph über* $\mathbb{F}_p$*, wenn gilt*

$$a^{\frac{p-1}{6}} = \widetilde{a}^{\frac{p-1}{6}}.$$

Da $\{x^{\frac{p-1}{6}} : x \in \mathbb{F}_p^*\}$ *genau sechs Elemente enthält - die 6-ten Einheitswurzeln von* $\mathbb{F}_p$ *-, gibt es genau sechs* $\mathbb{F}_p$*-Isomorphieklassen elliptischer Kurven mit* j*-Invariante* 0*.*

(c) *Im Fall* $p \equiv 2 \bmod 3$ *sind die Kurven* $E_{0,b}$ *und* $E_{0,\widetilde{b}}$ *genau dann isomorph über* $\mathbb{F}_p$*, wenn gilt*

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

Es gibt genau zwei $\mathbb{F}_p$*-Isomorphieklassen elliptischer Kurven mit* j*-Invariante* 0*. Ist* $u \in \mathbb{F}_p^*$ *mit* $\left(\frac{u}{p}\right) = -1$*, so repräsentieren* $y^2 = x^3 + 1$ *und* $y^2 = x^3 + u$ *die Isomorphieklassen.*

Beweis:

(1) $j \neq 0, 1728$.

(a) Es gilt

$$\begin{aligned} j(E_{a,b}) = 0 \quad &\iff \quad 1728 \cdot \frac{4a^3}{4a^3 + 27b^2} = 0 \quad \iff \quad a = 0, \\ j(E_{a,b}) = 1728 \quad &\iff \quad 1728 \cdot \frac{4a^3}{4a^3 + 27b^2} = 1728 \quad \iff \quad \frac{4a^3}{4a^3 + 27b^2} = 1 \quad \iff \\ &\iff \quad 4a^3 = 4a^3 + 27b^2 \quad \iff \quad 27b^2 = 0 \quad \iff \quad b = 0. \end{aligned}$$

Daraus folgt sofort

$$j(E_{a,b}) \neq 0, 1728 \quad \iff \quad a, b \neq 0,$$

was zu zeigen war.

(b) Es gilt:

$$\begin{aligned} j(E_{a,b}) = j(E_{\widetilde{a},\widetilde{b}}) \quad &\iff \quad 1728 \cdot \frac{4a^3}{4a^3 + 27b^2} = 1728 \cdot \frac{4\widetilde{a}^3}{4\widetilde{a}^3 + 27\widetilde{b}^2} \quad \iff \\ &\iff \quad \frac{a^3}{4a^3 + 27b^2} = \frac{\widetilde{a}^3}{4\widetilde{a}^3 + 27\widetilde{b}^2} \quad \iff \\ &\iff \quad 4a^3\widetilde{a}^3 + 27a^3\widetilde{b}^2 = 4a^3\widetilde{a}^3 + 27\widetilde{a}^3b^2 \quad \iff \\ &\iff \quad a^3\widetilde{b}^2 = \widetilde{a}^3b^2 \quad \iff \quad (\frac{\widetilde{a}}{a})^3 = (\frac{\widetilde{b}}{b})^2. \end{aligned}$$

Definieren wir u durch

$$u = \frac{\widetilde{b}a}{\widetilde{a}b} = \frac{\frac{\widetilde{b}}{b}}{\frac{\widetilde{a}}{a}},$$

so folgt mit obiger Relation

$$u^2 = \frac{(\frac{\widetilde{b}}{b})^2}{(\frac{\widetilde{a}}{a})^2} = \frac{(\frac{\widetilde{a}}{a})^3}{(\frac{\widetilde{a}}{a})^2} = \frac{\widetilde{a}}{a} \quad \text{und} \quad u^3 = \frac{(\frac{\widetilde{b}}{b})^3}{(\frac{\widetilde{a}}{a})^3} = \frac{(\frac{\widetilde{b}}{b})^3}{(\frac{\widetilde{b}}{b})^2} = \frac{\widetilde{b}}{b},$$

also

$$\widetilde{a} = au^2 \quad \text{und} \quad \widetilde{b} = bu^3.$$

Gilt für $\widetilde{u} \in \mathbb{F}_p^*$

$$\widetilde{a} = a\widetilde{u}^2 \quad \text{und} \quad \widetilde{b} = b\widetilde{u}^3,$$

so folgt

$$\widetilde{u} = \frac{\frac{\widetilde{b}}{b}}{\frac{\widetilde{a}}{a}} = u,$$

die Zahl u ist also eindeutig bestimmt.

(c) Es ist

$$j(E_{au^2,bu^3}) = 1728 \cdot \frac{4(au^2)^3}{4(au^2)^3 + 27(bu^3)^2} = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2} = j(E_{a,b}).$$

Weiter gilt unter Benutzung von $a \neq 0$ und $b \neq 0$:

$$\begin{aligned} E_{a,b} \overset{\mathbb{F}_p}{\simeq} E_{au^2,bu^3} &\iff au^2 = av^4 \text{ und } bu^3 = bv^6 \text{ für ein } v \in \mathbb{F}_p^* \iff \\ &\iff u^2 = v^4 \text{ und } u^3 = v^6 \text{ für ein } v \in \mathbb{F}_p^* \iff \\ &\iff u = v^2 \text{ für ein } v \in \mathbb{F}_p^* \iff \left(\frac{u}{p}\right) = 1. \end{aligned}$$

(Dabei bedeutet $\overset{\mathbb{F}_p}{\simeq}$ „isomorph über $\mathbb{F}_p$“.)

(d) Mit $c = \frac{j}{j-1728}$ gilt

$$\begin{aligned} j(E_{-3c,2c}) &= 1728 \cdot \frac{4(-3c)^3}{4(-3c)^3 + 27(2c)^2} = 1728 \cdot \frac{-c^3}{-c^3 + c^2} = 1728 \cdot \frac{c}{c-1} = \\ &= 1728 \cdot \frac{\frac{j}{j-1728}}{\frac{j}{j-1728} - 1} = 1728 \cdot \frac{j}{j - (j - 1728)} = j. \end{aligned}$$

(e) Dies folgt sofort aus (b) und (c).

(2) $j = 1728$.

(a) Die Aussage wurde bereits in (1)(a) bewiesen.

(b) Sei $p \equiv 1 \bmod 4$.

- Sind $E_{a,0}$ und $E_{\widetilde{a},0}$ isomorph über $\mathbb{F}_p$, so gibt es ein $u \in \mathbb{F}_p^*$ mit

$$\widetilde{a} = au^4.$$

Es folgt

$$\widetilde{a}^{\frac{p-1}{4}} = a^{\frac{p-1}{4}} (u^4)^{\frac{p-1}{4}} = a^{\frac{p-1}{4}} u^{p-1} = a^{\frac{p-1}{4}}.$$

- Es gelte nun umgekehrt

$$\widetilde{a}^{\frac{p-1}{4}} = a^{\frac{p-1}{4}}, \quad \text{also} \quad (\frac{\widetilde{a}}{a})^{\frac{p-1}{4}} = 1.$$

Ist $g \in \mathbb{F}_p^*$ eine Primitivwurzel, so gibt es ein $k \in \mathbb{N}_0$ mit $\frac{\widetilde{a}}{a} = g^k$. Es folgt

$$1 = (\frac{\widetilde{a}}{a})^{\frac{p-1}{4}} = (g^k)^{\frac{p-1}{4}} = g^{k \cdot \frac{p-1}{4}}.$$

Wegen $\operatorname{ord}(g) = p-1$ folgt $p-1 \mid k \cdot \frac{p-1}{4}$, also $4 \mid k$. Definiert man $u = g^{\frac{k}{4}}$, so ergibt sich

$$u^4 = g^k = \frac{\widetilde{a}}{a}, \quad \text{also} \quad \widetilde{a} = au^4,$$

d.h. $E_{a,0}$ und $E_{\widetilde{a},0}$ sind isomorph über $\mathbb{F}_p$.

- Ist $g \in \mathbb{F}_p^*$ eine Primitivwurzel, so sieht man wie eben, dass gilt

$$\#\{(g^0)^{\frac{p-1}{4}}, (g^1)^{\frac{p-1}{4}}, (g^2)^{\frac{p-1}{4}}, (g^3)^{\frac{p-1}{4}}\} = 4.$$

Die angegebenen Zahlen sind genau die 4-ten Einheitswurzeln in $\mathbb{F}_p^*$. Deshalb lassen sich auch leicht Zahlen a_1, a_2, a_3, a_4 mit den angegebenen Eigenschaften finden.

(c) Sei $p \equiv 3 \bmod 4$.

- Sind $E_{a,0}$ und $E_{\widetilde{a},0}$ isomorph über $\mathbb{F}_p$, so gibt es ein $u \in \mathbb{F}_p^*$ mit

$$\widetilde{a} = au^4.$$

Es folgt

$$\left(\frac{\widetilde{a}}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{u^4}{p}\right) = \left(\frac{a}{p}\right).$$

- Sei umgekehrt $\left(\frac{\widetilde{a}}{p}\right) = \left(\frac{a}{p}\right)$. Dann gibt es ein $t \in \mathbb{F}_p^*$ mit $\widetilde{a} = at^2$. Wegen $\left(\frac{-1}{p}\right) = -1$ gilt $\left(\frac{t}{p}\right) = -\left(\frac{-t}{p}\right)$. Daher können wir o.E. $\left(\frac{t}{p}\right) = 1$ annehmen. Es gibt also ein $u \in \mathbb{F}_p$ mit $t = u^2$. Es folgt $\widetilde{a} = au^4$, d.h. $E_{a,0}$ und $E_{\widetilde{a},0}$ sind isomorph über $\mathbb{F}_p$. Der Rest ist dann klar.

(3) $j = 0$.

(a) Dies wurde bereits in (1)(a) gezeigt.

(b) Wir betrachten den Fall $p \equiv 1 \bmod 3$.

- Sind $E_{0,b}$ und $E_{0,\widetilde{b}}$ isomorph über $\mathbb{F}_p$, so gibt es ein $u \in \mathbb{F}_p^*$ mit $\widetilde{b} = bu^6$. Es folgt mit $u^{p-1} = 1$ sofort
$$\widetilde{b}^{\frac{p-1}{6}} = b^{\frac{p-1}{6}}.$$
- Es gelte umgekehrt $\widetilde{b}^{\frac{p-1}{6}} = b^{\frac{p-1}{6}}$. Dann gilt
$$(\frac{\widetilde{b}}{b})^{\frac{p-1}{6}} = 1.$$
Ist $g \in \mathbb{F}_p^*$ eine Primitivwurzel, so gibt es ein $k \in \mathbb{N}_0$ mit $\frac{\widetilde{b}}{b} = g^k$. Dann folgt
$$1 = (\frac{\widetilde{b}}{b})^{\frac{p-1}{6}} = (g^k)^{\frac{p-1}{6}} = g^{k \cdot \frac{p-1}{6}},$$
also $p-1 \mid k \cdot \frac{p-1}{6}$ und damit $6 \mid k$. Für $u = g^{\frac{k}{6}}$ ergibt sich
$$u^6 = g^k = \frac{\widetilde{b}}{b}, \quad \text{also} \quad \widetilde{b} = bu^6,$$
d.h. $E_{0,b}$ und $E_{0,\widetilde{b}}$ sind isomorph über $\mathbb{F}_p$.
- Wie eben sieht man, dass für eine Primitivwurzel g
$$\#\{(g^0)^{\frac{p-1}{6}}, (g^1)^{\frac{p-1}{6}}, (g^2)^{\frac{p-1}{6}}, (g^3)^{\frac{p-1}{6}}, (g^4)^{\frac{p-1}{6}}, (g^5)^{\frac{p-1}{6}}\} = 6$$
gilt, die Elemente sind gerade die 6-ten Einheitswurzeln in $\mathbb{F}_p$. Daher gibt es auch sechs $\mathbb{F}_p$ Isomorphieklassen elliptischer Kurven über $\mathbb{F}_p$ mit j-Invariante 0.

(c) Wir betrachten den Fall $p \equiv 2 \bmod 3$.

- Wir bemerken zunächst, dass $\mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto x^3$ bijektiv ist. Denn $d = \frac{1+2(p-1)}{3}$ ist eine natürliche Zahl und $x \mapsto x^d$ die zu $x \mapsto x^3$ inverse Abbildung.
- Sind $E_{0,b}$ und $E_{0,\widetilde{b}}$ isomorph über $\mathbb{F}_p$, so gibt es ein $u \in \mathbb{F}_p^*$ mit
$$\widetilde{b} = bu^6,$$
was sofort
$$\left(\frac{\widetilde{b}}{p}\right) = \left(\frac{b}{p}\right)$$
impliziert.
- Es gelte umgekehrt $\left(\frac{\widetilde{b}}{p}\right) = \left(\frac{b}{p}\right)$. Dann gibt es ein $t \in \mathbb{F}_p^*$ mit $\widetilde{b} = bt^2$. Da $x \mapsto x^3$ hier bijektiv ist, gibt es ein $u \in \mathbb{F}_p^*$ mit $t = u^3$. Es folgt
$$\widetilde{b} = bt^2 = bu^6,$$
d.h. $E_{0,b}$ und $E_{0,\widetilde{b}}$ sind isomorph über $\mathbb{F}_p$.
- Der Rest ist klar. ■

Bemerkung: Mit dem vorangegangenen Satz kann man auch abzählen, wieviele elliptische Kurven es über $\mathbb{F}_p$ bis auf $\mathbb{F}_p$-Isomorphie gibt.

p mod 12	p mod 4	p mod 3	Kurven mit $j \neq 0, 1728$	Kurven mit $j = 0$	Kurven mit $j = 1728$	insgesamt
1	1	1	$2(p-2)$	6	4	$2p+6$
5	1	2	$2(p-2)$	2	4	$2p+2$
7	3	1	$2(p-2)$	6	2	$2p+4$
11	3	2	$2(p-2)$	2	2	$2p$

Wir fassen das Ergebnis nochmals zusammen:

SATZ. *Sei p eine Primzahl ≥ 5. Die Anzahl der $\mathbb{F}_p$-Isomorphieklassen elliptischer Kurven über $\mathbb{F}_p$ ist*

$$2p + \begin{cases} 6 & \text{für } p \equiv 1 \bmod 12, \\ 2 & \text{für } p \equiv 5 \bmod 12, \\ 4 & \text{für } p \equiv 7 \bmod 12, \\ 0 & \text{für } p \equiv 11 \bmod 12. \end{cases}$$

Die folgende Satz macht eine Aussage über die Isomorphie elliptischer Kurven bei allgemeinem Körper K.

SATZ. *Sei K ein Körper der Charakteristik $\neq 2, 3$. Folgende Kurven ergeben ein Repräsentantensystem aller elliptischen Kurven über K bis auf K-Isomorphie:*

- *$j = 0$: $y^2 = x^3 + b$, wobei b ein Repräsentantensystem von K^*/K^{*6} durchläuft.*
- *$j = 1728$: $y^2 = x^3 + ax$, wobei a ein Repräsentantensystem von K^*/K^{*4} durchläuft.*
- *$j \neq 0, 1728$: $y^2 = x^3 - 3cu^2x + 2cu^3$ mit $c = \frac{j}{j-1728}$, wobei u ein Repräsentantensystem von K^*/K^{*2} durchläuft.*

Beweis: Wir betrachten den Fall $j \neq 0, 1728$.

- Zunächst rechnet man nach, dass jede Kurve $y^2 = x^3 - 3cu^2x + 2cu^3$ wirklich j-Invariante j hat.
- Ist E eine elliptische Kurve über K mit der Gleichung $y^2 = x^3 + ax + b$ und j-Invariante j, so gibt es also ein $\lambda \in \overline{K}^*$ mit

  $$a = -3c\lambda^4 \quad \text{und} \quad b = 2c\lambda^6.$$

  Also folgt $\lambda^4, \lambda^6 \in K$ und damit $\lambda^2 \in K$. Setzt man $u = \lambda^2 \in K$, so hat E die gewünschte Form.
- Sei E gegeben durch $y^2 = x^3 - 3cu^2x + 2cu^3$ und E' durch $y^2 = x^3 - 3cu'^2x + 2cu'^3$. Dann gilt:

  $$\begin{aligned} E \simeq_K E' &\iff -3cu^2 \cdot v^4 = -3cu'^2, \quad 2cu^3 \cdot v^6 = 2cu'^3 \text{ für ein } v \in K \\ &\iff u'^2 = u^2 \cdot v^4, u'^3 = u^3 \cdot v^6 \text{ für ein } v \in K \\ &\iff u' = u \cdot v^2 \text{ für ein } v \in K^*, \end{aligned}$$

  woraus sofort die Behauptung folgt.

Die Fälle $j = 0$ und $j = 1728$ funktionieren analog. ■

Beispiele: Sei K ein Körper der Charakteristik $\neq 2, 3$.

(1) Ist K algebraisch abgeschlossen, so ist $K^* = K^{*2} = K^{*4} = K^{*6}$, zu jedem $j \in K$ gibt es also bis auf Isomorphie genau eine elliptische Kurve mit j-Invariante j.
(2) Für $K = \mathbb{R}$ sind $K^{*2} = K^{*4} = K^{*6} = \mathbb{R}_{>0}$ die positiven reellen Zahlen, als Repräsentanten von $K^*/K^{*2\ell}$ kann man also 1 und -1 wählen. Zu jedem $j \in \mathbb{R}$ gibt es also genau zwei elliptische Kurven über $\mathbb{R}$ mit j-Invariante j.

Beispiel: Wir wollen nochmals alle elliptischen Kurven E über $\mathbb{F}_5$ angeben zusammen mit $j = j(E)$ und $N = E(\mathbb{F}_5)$.

$$\begin{aligned} j = 0: &\quad y^2 = x^3 + 1 \quad (N = 6), \quad y^2 = x^3 + 2 \quad (N = 6) \\ j = 1: &\quad y^2 = x^3 + x + 2 \quad (N = 4), \quad y^2 = x^3 + 4x + 1 \quad (N = 8) \\ j = 2: &\quad y^2 = x^3 + x + 1 \quad (N = 9), \quad y^2 = x^3 + 4x + 2 \quad (N = 3) \\ j = 3: &\quad y^2 = x^3 + x \quad (N = 4), \quad y^2 = x^3 + 2x \quad (N = 2), \\ &\quad y^2 = x^3 + 3x \quad (N = 10), \quad y^2 = x^3 + 4x \quad (N = 8) \\ j = 4: &\quad y^2 = x^3 + 2x + 1 \quad (N = 7), \quad y^2 = x^3 + 3x + 2 \quad (N = 5) \end{aligned}$$

7. Faktorisieren mit elliptischen Kurven — ECM

7.1. Erinnerung. Will man die Primfaktorzerlegung einer natürlichen Zahl n bestimmen, geht man heutzutage algorithmisch in etwa so vor:

Eingabe: Eine natürliche Zahl n. Eine obere Grenze M für die „kleinen“ Primteiler.
Ausgabe: Primfaktorzerlegung von n

1: Lege Listen P und T an.
2: **for** t mit $2 \leq t \leq M$ **do**
3: **while** $n\%t = 0$ **do**
4: Hänge t an P an
5: $n \leftarrow \frac{n}{t}$
6: **end while**
7: **end for**
8: **if** $n > 1$ **then**
9: Hänge n an T an.
10: **while** T ist nicht leer **do**
11: Sei m das letzte Element von T. Streiche das letzte Element von T.
12: **if** m ist prim **then**
13: Hänge m an P an.
14: **else**
15: Bestimme einen nichttrivialen Teiler d von m, d.h. $d \mid m$ mit $1 < d < m$. ▷ Dies ist der schwierige Teil
16: Hänge d und $\frac{m}{d}$ an T an.
17: **end if**
18: **end while**
19: **end if**
20: Sortiere P. Erstelle die Primfaktorzerlegung $p_1^{e_1} \dots p_r^{e_r}$ und gibt sie aus.

Die schwierige Aufgabe ist, einen nichttrivialen Teiler d einer zusammengesetzten Zahl m (ohne kleine Teiler) zu finden. Dafür gibt es verschiedene Methoden. Wir werden ein Verfahren mit elliptischen Kurven skizzieren.

7.2. Die $(p-1)$-Methode von Pollard. Sei $n > 1$ eine ungerade natürliche Zahl und $K \in \mathbb{N}$. Ist p ein Primteiler von n, sodass für die Primfaktorzerlegung von $p-1$

$$p - 1 = q_1^{e_1} \dots q_r^{e_r} \quad \text{und} \quad q_i^{\alpha_i} \leq K \text{ für } i = 1, \dots, r$$

gilt, so folgt $q_1^{e_1} \dots q_r^{e_r} \mid \mathrm{kgV}(1, \dots, K)$, also

$$p - 1 \mid \mathrm{kgV}(1, \dots, K).$$

Nach dem kleinen Satz von Fermat gilt $2^{p-1} \equiv 1 \bmod p$ und damit auch

$$2^{\mathrm{kgV}(1,\dots,K)} \equiv 1 \bmod p,$$

also

$$p \mid \mathrm{ggT}(2^{\mathrm{kgV}(1,\dots,K)} - 1, n).$$

Auf der rechten Seite kommt p nicht vor. Daher kann man K wählen und

$$\mathrm{ggT}(2^{\mathrm{kgV}(1,\dots,K)} - 1, n)$$

berechnen. Eventuell findet man so einen nichttrivialen Teiler von n.

Beispiel: Für $n = 5353 = 53 \cdot 101$ findet man

$$\mathrm{ggT}(2^{\mathrm{kgV}(1,\dots,20)} - 1, n) = 53.$$

(Es ist $\mathrm{kgV}(1, \dots, 20) = 232792560$.)

Das Verfahren funktioniert, wenn die Gruppenordnung $p-1 = \#\mathbb{F}_p^*$ nur Primteilerpotenzen $q_i^{\alpha_i} \leq K$ hat, hängt also wesentlich von der Struktur der Gruppe $\mathbb{F}_p^*$ ab.

Die Idee von Lenstra: Ersetze in obigem Verfahren die Gruppe $\mathbb{F}_p^*$ durch elliptische Kurven $E_{a,b}(\mathbb{F}_p)$ (mit der Gleichung $y^2 = x^3 + ax + b$). Der erhoffte Vorteil: Während es bei festem p nur eine multiplikative Gruppe $\mathbb{F}_p^*$ gibt, deren Struktur dann eindeutig bestimmt ist, gibt es viele elliptische Kurven $E_{a,b}(\mathbb{F}_p)$, sodass man die Parameter a, b variieren kann, bis die Struktur von $E_{a,b}(\mathbb{F}_p)$ so ist, dass das Faktorisierungsverfahren funktioniert.

7.3. Nochmals Addition auf elliptischen Kurven. Gegeben sei eine natürliche Zahl $n > 1$ mit $\mathrm{ggT}(n, 6) = 1$. Sei p ein Primteiler von n. Wenn wir modulo n rechnen, gelten die Ergebnisse natürlich auch in $\mathbb{F}_p$. Sei eine elliptische Kurve über $\mathbb{F}_p$ durch die Gleichung $y^2 = x^3 + ax + b$ mit $a, b \in \mathbb{Z}$ (und $\mathrm{ggT}(4a^3 + 27b^2, n) = 1$) gegeben. Seien weiter Punkte

$$P_1 = (x_1, y_1) \quad \text{und} \quad P_2 = (x_2, y_2)$$

aus $E(\mathbb{F}_p)$ gegeben durch Zahlen $x_1, y_1, x_2, y_2 \in \mathbb{Z}$, für die gilt

$$y_1^2 \equiv x_1^3 + ax_1 + b \bmod n \quad \text{und} \quad y_2^2 \equiv x_2^3 + ax_2 + b \bmod n.$$

Wir berechnen zunächst

$$d_1 = \mathrm{ggT}(n, x_1 - x_2)$$

und unterscheiden drei Fälle:

- **Fall** $1 < d_1 < n$**:** Dann ist n keine Primzahl und d_1 ein nichttrivialer Teiler von n. (Wir haben also einen nichttrivialen Teiler von n gefunden und hören auf.)
- **Fall** $d_1 = n$**:** Dann ist $x_1 \equiv x_2 \bmod n$ und

  $$y_1^2 \equiv x_1^3 + ax_1 + b \equiv x_2^3 + ax_2 + b \equiv y_2^2 \bmod n,$$

  also

  $$y_1^2 \equiv y_2^2 \bmod n, \quad \text{also} \quad n \mid (y_1 - y_2)(y_1 + y_2).$$

  Wir berechnen nun

  $$d_2 = \mathrm{ggT}(n, y_1 + y_2)$$

  und unterscheiden wieder drei Fälle:
  - **Fall** $1 < d_2 < n$**:** Dann ist d_2 ein nichttrivialer Teiler von n. (Wir hören auf.)
  - **Fall** $d_2 = n$**:** Dann ist $y_1 + y_2 \equiv 0 \bmod n$, also $P_1 + P_2 = O$.
  - **Fall** $d_2 = 1$**:** Dann gilt $y_1 \equiv y_2 \bmod n$ und $\mathrm{ggT}(n, 2y_1) = 1$. Wir können also die Steigung berechnen:

    $$m = \frac{3x_1^2 + a}{2y_1} \bmod n, \quad x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1 \bmod n.$$

    Es ist $P_1 + P_2 = (x_3, y_3)$.
- **Fall** $d_1 = 1$**:** Wegen $\mathrm{ggT}(n, x_1 - x_2) = 1$ ist $x_1 - x_2$ invertierbar modulo n und wir können berechnen

  $$m = \frac{y_1 - y_2}{x_1 - x_2} \bmod n, \quad x_3 = m^2 - x_1 - x_2 \bmod n, \quad y_3 = m(x_1 - x_3) - y_1 \bmod n.$$

  Es ist $P_1 + P_2 = (x_3, y_3)$.

Was ist das Ergebnis?

- Entweder finden wir einen nichttrivialen Teiler d von n oder
- das Ergebnis $P_1 + P_2$ gilt in $E(\mathbb{F}_p)$ für jeden Primteiler p von n.

Beispiele: $n = 5353 = 53 \cdot 101$.

(1) $y^2 = x^3 + 70x + 1$. Für

$$P_1 = (38, 3224), \quad P_2 = (3371, 4856)$$

gilt

$$d_1 = \mathrm{ggT}(n, x_1 - x_2) = 101.$$

Das Ergebnis kann man auch in $E(\mathbb{F}_p)$ für $p \in \{53, 101\}$ sehen:

$$P_1 \equiv (38, 44) \bmod 53, \quad P_2 \equiv (32, 33) \bmod 53$$

und

$$P_1 \equiv (38, 93) \bmod 101, \quad P_2 \equiv (38, 8) \bmod 101.$$

(2) $y^2 = x^3 + 71x + 1$. Für

$$P_1 = P_2 = (775, 1919)$$

gilt

$$d_1 = \mathrm{ggT}(n, x_1 - x_2) = n \quad \text{und} \quad d_2 = \mathrm{ggT}(n, y_1 + y_2) = 101.$$

Wegen

$$P_1 \equiv (33, 11) \bmod 53 \quad \text{und} \quad P_1 \equiv (68, 0) \bmod 101$$

ist das Ergebnis auch klar.

Hier ist eine algorithmische Variante:

Addition auf einer elliptischen Kurve modulo n:

Eingabe: $n \in \mathbb{N}_>$ mit $\mathrm{ggT}(n, 6) = 1$, $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(n, 4a^3 + 27b^2) = 1$, $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ mit $y_1^2 \equiv x_1^3 + ax_1 + b \bmod n$, $y_2^2 \equiv x_2^3 + ax_2 + b \bmod n$

Ausgabe: Entweder ein nichttrivialer Teiler von d von n oder $P_1 + P_2 \in E(\mathbb{F}_p)$, das für jeden Primteiler p von n gilt

$d_1 \leftarrow \mathrm{ggT}(n, x_1 - x_2)$
if $1 < d_1 < n$ **then**
  return d_1 (nichttrivialer Teiler von n)
else if $d_1 = n$ **then**
  $d_2 \leftarrow \mathrm{ggT}(n, y_1 + y_2)$
  if $1 < d_2 < n$ **then**
    return d_2 (nichttrivialer Teiler von n)
  else if $d_2 = n$ **then**
    return $P_1 + P_2 = O$
  else
    $m \leftarrow \frac{3x_1^2 + a}{2y_1} \bmod n$
  end if
else
  $m \leftarrow \frac{y_1 - y_2}{x_1 - x_2} \bmod n$
end if
$x_3 \leftarrow m^2 - x_1 - x_2 \bmod n$, $y_3 \leftarrow m(x_1 - x_3) - y_1 \bmod n$
return (x_3, y_3) als $P_1 + P_2$

Hier ist eine mögliche Python3-Funktion:

```
# Addition P1+P2 auf der 'elliptischen' Kurve y^2=x^3+ax+b modulo n.
# Fuer die Rueckgabe gibt es drei Moeglichkeiten:
# [] - O=P1+P2
# [d] - d ist nichttrivialer Teiler von n
# [x,y] - P1+P2=(x,y)
def ek_ecm_add(P1,P2,nab):
  n,a,b=nab
  if P1==[]:
    return P2
  if P2==[]:
    return P1
  x1,y1=P1
  x2,y2=P2
  d1=ggT(n,x1-x2)
  if 1<d1<n:
    return [d1]
  elif d1==n:
    d2=ggT(n,y1+y2)
```

```
    if 1<d2<n:
      return [d2]
    elif d2==n:
      return []
    else:
      m=((3*x1**2+a)*invmod(2*y1,n))%n
  else:
    m=((y1-y2)*invmod(x1-x2,n))%n
  x3=(m**2-x1-x2)%n
  y3=(m*(x1-x3)-y1)%n
  return [x3,y3]
```

Nun brauchen wir noch die Multiplikation mit $k \in \mathbb{N}$ auf unseren Kurven:

Berechnung von $k \cdot P$ auf einer „elliptischen Kurve“ modulo n:

Eingabe: $n \in \mathbb{N}_{>1}$ mit $\mathrm{ggT}(n, 6) = 1$, $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(n, 4a^3 + 27b^2) = 1$, $x, y \in \mathbb{Z}$ mit $y^2 \equiv x^3 + ax + b \bmod n$, $k \in \mathbb{N}_0$

Ausgabe: Entweder ein nichttrivialer Teiler d von n oder $k \cdot P \in E(\mathbb{F}_p)$, das für jeden Primteiler p von n gilt

$Q \leftarrow O$, $R \leftarrow P$
while $k > 0$ **do**
  if $k \equiv 1 \bmod 2$ **then**
    $Q \leftarrow Q + R$ (mit dem vorangegangenen Verfahren)
    if Q ist eine Zahl d **then**
      return d (nichttrivialer Teiler von n)
    end if
  end if
  $R \leftarrow R + R$ (mit dem vorangegangenen Verfahren)
  if R ist eine Zahl d **then**
    return d (nichttrivialer Teiler von n)
  end if
  $k \leftarrow \left\lfloor \frac{k}{2} \right\rfloor$
end while
return Q

Hier ist eine zugehörige Python3-Funktion:

```
# Berechnung von k*P auf der 'elliptischen' Kurve y^2=x^3+ax+b modulo n
# Fuer die Rueckgabe gibt es drei Moeglichkeiten:
# [] - O=k*P
# [d] - d ist nichttrivialer Teiler von n
# [x,y] - k*P=(x,y)
def ek_ecm_mult(k,P,nab):
  Q,R=[],P[:]
  while k>0:
    if k%2==1:
      Q=ek_ecm_add(Q,R,nab)
      if len(Q)==1:
        return Q
    R=ek_ecm_add(R,R,nab)
    if len(R)==1:
      return R
    k=k//2
  return Q
```

Wir sind jetzt in der Lage, ein Faktorisierungsverfahren mit elliptischen Kurven vorzustellen, zunächst eine grobe Version:

Faktorisierungsverfahren mit elliptischen Kurven: Sei $n > 1$ eine zusammengesetzte natürliche Zahl mit $\mathrm{ggT}(n, 6) = 1$. Wir suchen einen nichttrivialer Teiler von n.

(1) Wähle eine natürliche Zahl K.
(2) Wähle $a, x, y \in \mathbb{Z}$, berechne $b = (y^2 - x^3 - ax) \bmod n$. (Damit haben wir eine Kurve $y^2 = x^3 + ax + b$ mit einem Punkt $P = (x, y)$.)
(3) Versuche, mit obigen Formeln auf der Kurve $y^2 = x^3 + ax + b$ den Punkt
$$\mathrm{kgV}(1, \ldots, K) \cdot P$$
zu berechnen.
(4) Wurde bei der Berechnung ein nichttrivialer Teiler von n gefunden, ist man fertig. Andernfalls kann man eine andere Kurve, d.h. a, x, y, oder ein anderes K wählen.

Beispiel: $n = 20702018498844294793$ ist zusammengesetzt. Wir wählen die Kurven $y^2 = x^3 + ax + 1$ mit dem Punkt $P = (0, 1)$ für $a = 0, 1, 2, 3, \ldots$. Wir versuchen, auf der Kurve $\mathrm{kgV}(1, \ldots, 100) \cdot P$ zu berechnen. (Es ist $\mathrm{kgV}(1, \ldots, 100) = 69720375229712477164533808935312303556800$.) Bei $a = 43$ haben wir Erfolg. Wir erhalten den Teiler 3645782639. Tatsächlich hat man so schon die Primfaktorzerlegung:
$$n = 20702018498844294793 = 3645782639 \cdot 5678346887.$$

Bemerkungen:

(1) Ist K gegeben, sind $p_1, \ldots, p_r$ die Primzahlen $\leq K$, ist e_j maximale mit $p_j^{e_j} \leq K$, so gilt
$$\mathrm{kgV}(1, \ldots, K) = \prod_{j=1}^{r} p_j^{e_j}.$$
Statt
$$\mathrm{kgV}(1, \ldots, K) \cdot P$$
zu berechnen, kann man dann
$$\sum_{j=1}^{r} \sum_{k=1}^{e_j} p_j \cdot P$$
berechnen, wodurch die Zahlen etwas kleiner bleiben.
(2) In den folgenden Beispielen haben wir die Kurven $y^2 = x^3 + ax + 1$ (für $a = 1, 2, 3, \ldots$) mit dem Punkt $P = (1, 1)$ benutzt.

Faktorisierung mit elliptischen Kurven:

Eingabe: Eine natürliche Zahl $n > 1$ mit $\mathrm{ggT}(n, 6) = 1$, eine natürliche Zahl K, eine Liste von Zahlen a_i, x_i, y_i für $i = 1, \ldots, m$ für 'elliptische Kurven' $y^2 = x^3 + a_i x + b_i$ und Punkte $P = (x_i, y_i)$
Ausgabe: Ein nichttrivialer Teiler d von n oder 'False'

```
Erzeuge (mit dem Sieb des Eratosthenes) eine Liste p_1, ..., p_r der Primzahlen ≤ K.
Bestimme Exponenten e_1, ..., e_r, sodass e_j maximal mit p_j^{e_j} ≤ K ist
for i = 1, ..., m do
    b_i ← (y_i^2 − x_i^3 − a_i x_i) mod n
    g ← ggT(n, 4a_i^3 + 27b_i^2)
    if 1 < g < n then
        return g
    else if g = 1 then
        P ← (x_i, y_i)
        for j = 1, ..., r do
            for k = 1, ..., e_j do
                P ← p_j · P auf der Kurve y^2 = x^3 + a_i x + b_i mit obigen Formeln
                if P ist Zahl then
                    return d = P als nichttrivialer Teiler von n
```

15: **end if**
16: **end for**
17: **end for**
18: **end if**
19: **end for**

Eine zugehörige Python3-Funktion könnte so aussehen:

```
# ECM - Faktorisierung mit elliptischen Kurven
# Eingabe:
# (a) n - zu faktorisierende Zahl
# (b) K - fuer kgV(1,...,K)
# axy - Liste von Kurven und Punkten in der Form
# [[a_1,x_1,y_1],[a_2,x_2,y_2],...], wobei b_i als
# b_i=(y_i^2-x_i^3-a_ix_i) mod n berechnet wird
# Ausgabe: ein nichttrivialer Teiler von n oder 'False'
def ecm(n,K,axy=False):
  if ggT(n,6)>1:
    print("ggT(n,6)>1",sep="")
    return ggT(n,6)
  if axy==False:
    axy=[]
    for a in range(1000):
      axy.append([a,0,1]) # y^2=x^3+ax+1 und P=(0,1)
  p=eratosthenes(K)
  e=len(p)*[1]
  for j in range(len(p)):
    e_j=0
    while p[j]**(e_j+1)<=K:
      e_j=e_j+1
    e[j]=e_j
  # Dann ist kgV(1,...,K)=prod(p_j^e_j)
  for axy_i in axy:
    a,x,y=axy_i
    P=[x,y]
    b=(y**2-x**3-a*x)%n
    print("a=",a," b=",b," P=(",x,",",y,")",sep="")
    g=ggT(n,4*a**3+27*b**2)
    if 1<g<n:
      print("1<ggT(n,4a^3+27b^2)<n",sep="")
      return g
    elif g==n:
      print("4a^3+27b^2=0 mod n",sep="")
    else:
      nab=[n,a,b]
      for j in range(len(p)):
        for k in range(e[j]):
          P=ek_ecm_mult(p[j],P,nab)
          if len(P)==1:
            return P[0] # Teiler gefunden
  return False
```

7.4. Warum funktioniert das Verfahren? Seien p und $\widetilde{p}$ zwei verschiedene Primteiler der Zahl n (ohne kleine Teiler) und $E_{a,1}$ die durch $y^2 = x^3 + ax + 1$ definierte Kurve.

- Hat der Punkt $P = (0,1)$ als Element der Gruppe $E_{a,1}(\mathbb{F}_p)$ die Ordnung $q_1^{\alpha_1} \dots q_r^{\alpha_r}$ und ist $q_i^{\alpha_i} \leq K$, (d.h. die Ordnung ist K-potenzglatt), so gilt
$$\mathrm{kgV}(1..K) \cdot (0,1) = O \text{ in } E_a(\mathbb{F}_p).$$
- Ist die Ordnung von P als Element von $E_{a,1}(\mathbb{F}_{\widetilde{p}})$ kein Teiler von $\mathrm{kgV}(1..K)$, so ist
$$\mathrm{kgV}(1..K) \cdot (0,1) \neq O \text{ in } E_{a,1}(\mathbb{F}_{\widetilde{p}}).$$
- Versucht man also $\mathrm{kgV}(1..K) \cdot (0,1)$ modulo n zu berechnen, muss etwas schief gehen, und man stößt auf einen nichttrivialen Teiler von n.

Beispiel: Wir betrachten nochmals die zusammengesetzte Zahl $n = 20702018498844294793$. Mit $a = 43$ und $K = 100$ erhielten wir die Primfaktorzerlegung
$$n = 20702018498844294793 = 3645782639 \cdot 5678346887.$$
- Für $p = 3645782639$ und $P = (0,1) \in E_{a,1}(\mathbb{F}_p)$ gilt
$$\#E(\mathbb{F}_p) = 3645808283 = 13 \cdot 29 \cdot 37 \cdot 47 \cdot 67 \cdot 83 \quad \text{und} \quad \mathrm{ord}\,(P) = \#E(\mathbb{F}_p).$$
Daher gilt natürlich hier $\mathrm{kgV}(1, \dots, 100) \cdot P = O$.
- Für $q = 5678346887$ und $P = (0,1) \in E_{a,1}(\mathbb{F}_q)$ gilt
$$\#E(\mathbb{F}_q) = 5678426381 \text{ (Primzahl)} \quad \text{und} \quad \mathrm{ord}\,(P) = \#E(\mathbb{F}_q).$$
Damit gilt natürlich $\mathrm{kgV}(1, \dots, 100) \cdot P \neq O$.

Es ist klar, dass dann bei der Berechnung von $\mathrm{kgV}(1, \dots, 100) \cdot (0,1)$ modulo n etwas schief gehen muss.

Bemerkung: Es gibt (viele) a's, sodass die Ordnung von $P = (0,1)$ in $E_{a,1}(\mathbb{F}_p)$ ein Teiler von $\mathrm{kgV}(1, \dots, K)$ ist. Nun gilt natürlich auch:
$$\mathrm{ord}_{E_{a,1}(\mathbb{F}_p)}(P) | \#E_{a,1}(\mathbb{F}_p).$$
Es reicht also, wenn wir (viele) a's finden mit
$$\#E_{a,1}(\mathbb{F}_p) | \mathrm{kgV}(1, \dots, K).$$
Jetzt weiß man aber:
$$p + 1 - 2\sqrt{p} < \#E(\mathbb{F}_p) < p + 1 + 2\sqrt{p}.$$
Außerdem kommt auch jede Zahl dieses Intervalls als Mächtigkeit einer elliptischen Kurve über $\mathbb{F}_p$ vor. Die Zahl
$$w_K(p) = \frac{\#\{N \in \mathbb{N} : p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p} \text{ und } N | \mathrm{kgV}(1, \dots, K)\}}{\#\{N \in \mathbb{N} : p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p}\}}$$
gibt also in etwa die Wahrscheinlichkeit an, durch Variation von a auf eine Kurve zu treffen, für die das Faktorisierungsverfahren funktioniert.
Es ist verständlich, dass bei festem K die Wahrscheinlichkeit $w_K(p)$ kleiner wird, wenn p größer wird. Also wird man mit dem Faktorisierungsverfahren eher die kleineren Primteiler der Zahl n finden.

7.5. Beispiele. Wir wollen die 256-Bit-Zahlen $2^{255} + i$, $i = 1, \dots, 10$, faktorisieren. Zunächst werden die kleinen Teiler bis 100000 herausgeteilt, dann wird die Faktorisierung mit den elliptischen Kurven $y^2 = x^3 + ax + 1$ und dem Punkt $(0,1)$ versucht, wobei der Reihe nach $K = 100, 1000, 10000, 100000$ und $a = 1, \dots, 999$ probiert wird. (Bei $2^{255} + 6$ und $2^{255} + 7$ wurden Ausnahmen gemacht.)

$$\begin{aligned} 2^{255} + 1 &= 57896044618658097711785492504343953926634992332820282019728792003956564819969 = \\ &= 3^2 \cdot 11 \cdot 307 \cdot 331 \cdot 2857 \cdot 6529 \cdot 12241 \cdot 43691 \cdot \quad \text{(kleine Teiler)} \\ &\quad \cdot 418562986357561 \quad (\text{prim}, K = 1000, a = 46) \\ &\quad \cdot 51366149455494753931 \quad (\text{prim}, K = 10000, a = 179) \\ &\quad \cdot 26831423036065352611 \quad (\text{prim - Rest}) \end{aligned}$$

$$
\begin{aligned}
2^{255}+2 &= 57896044618658097711785492504343953926634992332820282019728792003956564819970 = \\
&= 2 \cdot 5 \cdot 509 \cdot 18797 \cdot 26417 \cdot \quad \text{(kleine Teiler)} \\
&\quad \cdot 72118729 \quad (\text{prim}, K = 100, a = 66) \\
&\quad \cdot 140385293 \quad (\text{prim}, K = 100, a = 515) \\
&\quad \cdot 8988357880501 \quad (\text{prim}, K = 1000, a = 42) \\
&\quad \cdot 2792688414613 \quad (\text{prim}, K = 1000, a = 117) \\
&\quad \cdot 90133566917913517709497 \quad (\text{prim - Rest})
\end{aligned}
$$

$$
\begin{aligned}
2^{255}+3 &= 57896044618658097711785492504343953926634992332820282019728792003956564819971 = \\
&= \quad \text{(kleine Teiler)} \\
&\quad \cdot 9663703905367 \quad (\text{prim}, K = 1000, a = 624) \\
&\quad \cdot 599108221708903554595341427309377510241603132709327340702349061 3 \quad (\text{prim - Rest})
\end{aligned}
$$

$$
\begin{aligned}
2^{255}+4 &= 57896044618658097711785492504343953926634992332820282019728792003956564819972 = \\
&= 2^2 \cdot 3 \cdot 683 \cdot 4049 \cdot 85009 \cdot \quad \text{(kleine Teiler)} \\
&\quad \cdot 2796203 \quad (\text{prim}, K = 100, a = 1) \\
&\quad \cdot 31797547 \quad (\text{prim}, K = 100, a = 24) \\
&\quad \cdot 81776791273 \quad (\text{prim}, K = 1000, a = 55) \\
&\quad \cdot 28225515294603308476042620861490152426 89 \quad (\text{prim - Rest})
\end{aligned}
$$

$$
\begin{aligned}
2^{255}+5 &= 57896044618658097711785492504343953926634992332820282019728792003956564819973 = \\
&= 13 \cdot \quad \text{(kleine Teiler)} \\
&\quad \cdot 44306302815072318101196 1 \quad (\text{prim}, K = 10000, a = 940) \\
&\quad \cdot 10051711857636436790242983745690155971833605671259361 \quad (\text{prim - Rest})
\end{aligned}
$$

$$
\begin{aligned}
2^{255}+6 &= 57896044618658097711785492504343953926634992332820282019728792003956564819974 = \\
&= 2 \cdot 7 \cdot \quad \text{(kleine Teiler)} \\
&\quad \cdot 14308487864574132496998414325 21 \quad (\text{prim}, K = 100000, a = 74830) \\
&\quad \cdot 28901948253486270216231618660631549620329002 21 \quad (\text{prim - Rest})
\end{aligned}
$$

(Zuerst wurde die Zahl mit anderen Methoden faktorisiert, dann wurde ein passender Wert für a berechnet.)

$$
\begin{aligned}
2^{255}+7 &= 57896044618658097711785492504343953926634992332820282019728792003956564819975 = \\
&= 3\cdot 5^2\cdot \quad \text{(kleine Teiler)} \\
&\quad \cdot 87852564226769798471 \quad (\text{prim, } K=100000,\ a=300) \\
&\quad \cdot 10684679205312774729813 1 \quad (\text{prim, } K=100000,\ a=1129) \\
&\quad \cdot 82237841198580158205446139566833 \quad (\text{prim - Rest})
\end{aligned}
$$

(Hier wurde als Möglichkeit $1 \le a \le 2000$ zugelassen.)

$$
\begin{aligned}
2^{255}+8 &= 57896044618658097711785492504343953926634992332820282019728792003956564819976 = \\
&= 2^3\cdot 17\cdot 241\cdot 433\cdot 1009\cdot 3361\cdot 21169\cdot 38737\cdot \quad \text{(kleine Teiler)} \\
&\quad \cdot 2627857 \quad (\text{prim, } K=100,\ a=2) \\
&\quad \cdot 269389009 \quad (\text{prim, } K=100,\ a=50) \\
&\quad \cdot 15790321 \quad (\text{prim, } K=100,\ a=260) \\
&\quad \cdot 88959882481 \quad (\text{prim, } K=1000,\ a=32) \\
&\quad \cdot 1475204679190128571777 \quad (\text{prim - Rest})
\end{aligned}
$$

$$
\begin{aligned}
2^{255}+9 &= 57896044618658097711785492504343953926634992332820282019728792003956564819977 = \\
&= 761\cdot \quad \text{(kleine Teiler)} \\
&\quad \cdot 102523 \quad (\text{prim, } K=100,\ a=6) \\
&\quad \cdot 164863869064627 \quad (\text{prim, } K=100000,\ a=4) \\
&\quad \cdot 92688479535572441677859 \quad (\text{prim, } K=100000,\ a=618) \\
&\quad \cdot 485614544676997703586082690871 63 \quad (\text{prim - Rest})
\end{aligned}
$$

$$
\begin{aligned}
2^{255}+10 &= 57896044618658097711785492504343953926634992332820282019728792003956564819978 = \\
&= 2\cdot 3^2\cdot 3229\cdot 7547\cdot 8803\cdot \quad \text{(kleine Teiler)} \\
&\quad \cdot 1499350926460804658260882311524773407724343014407075566800701 6689 \quad (\text{prim - Rest})
\end{aligned}
$$

Beispiel: Wir betrachten $2^{255}+9$. Als „kleine Teiler“ $\le 10^6$ findet man 761 und 102523, dann gibt es noch drei Primteiler

$$
\begin{aligned}
p_1 &= 164863869064627, \\
p_2 &= 92688479535572441677859, \\
p_3 &= 485614544676997703586082690871 63,
\end{aligned}
$$

sodass insgesamt gilt

$$2^{255}+9 = 761\cdot 102523\cdot p_1\cdot p_2\cdot p_3.$$

Die folgenden Tabellen zeigen, warum man für $K=100000$ und $a=4$ bzw. $a=618$ einen Teiler findet:

$a=4$	$\#E_{a,1}(\mathbb{F}_p)$	$\operatorname{ord}((0,1))$
p_1	$11^3\cdot 1223\cdot 3833\cdot 26423$	$11^3\cdot 1223\cdot 3833\cdot 26423\ *$
p_2	$2^3\cdot 13\cdot 29663\cdot 30707251\cdot 978444977$	$2^3\cdot 13\cdot 29663\cdot 30707251\cdot 978444977$
p_3	$2^3\cdot 13\cdot 821\cdot 4793\cdot 11941\cdot 78601849\cdot 126425389339$	$2^2\cdot 13\cdot 821\cdot 4793\cdot 11941\cdot 78601849\cdot 126425389339$

$a = 618$	$\#E_{a,1}(\mathbb{F}_p)$	$\operatorname{ord}((0,1))$
p_1	$2^3 \cdot 3^4 \cdot 59 \cdot 241 \cdot 17892929$	$2^2 \cdot 3^3 \cdot 59 \cdot 241 \cdot 17892929$
p_2	$11^2 \cdot 13 \cdot 17 \cdot 23 \cdot 67 \cdot 2293 \cdot 8693 \cdot 9629 \cdot 11719$	$11^2 \cdot 13 \cdot 17 \cdot 23 \cdot 67 \cdot 2293 \cdot 8693 \cdot 9629 \cdot 11719 *$
p_3	$2^4 \cdot 3^2 \cdot 7 \cdot 23 \cdot 20946106999525435218338202 13$	$2^2 \cdot 3^2 \cdot 7 \cdot 23 \cdot 20946106999525435218338202 13$

8. Elliptische Kurven über $\mathbb{C}$

Das Studium elliptischer Kurven über dem Körper $\mathbb{C}$ der komplexen Zahlen ist in mancher Hinsicht einfacher als der Allgemeinfall, da man hier Mittel der Funktionentheorie zur Verfügung hat. Im Folgenden soll ein kurzer Überblick (ohne Beweise) gegeben werden[1].

Gitter: Ein Gitter in $\mathbb{C}$ ist eine Untergruppe der additiven Gruppe von $\mathbb{C}$ der Gestalt

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{z_1\omega_1 + z_2\omega_2 \in \mathbb{C} : z_1, z_2 \in \mathbb{Z}\} \subseteq \mathbb{C},$$

wo ω_1, ω_2 eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist. (Dies ist gleichwertig mit $\omega_1 \neq 0$, $\omega_2 \neq 0$ und $\frac{\omega_2}{\omega_1} \notin \mathbb{R}$.) ω_1, ω_2 nennt man dann eine Gitterbasis von Λ. Die folgende Äquivalenz zeigt, wie Gitterbasen eines Gitters auseinander hervorgehen:

$$\mathbb{Z}\omega_1' + \mathbb{Z}\omega_2' = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \iff \text{es gibt } a,b,c,d \in \mathbb{Z} \text{ mit } ad - bc = \pm 1 \text{ und } \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Zwei Gitter Λ, Λ' nennt man ähnlich ($\Lambda \sim \Lambda'$), wenn es ein $\mu \in \mathbb{C}^*$ gibt mit $\Lambda' = \mu\Lambda$. Jedes Gitter ist dann ähnlich einem Gitter der Gestalt

$$\Lambda = \mathbb{Z} + \mathbb{Z}\tau \quad \text{mit} \quad \operatorname{Im}(\tau) > 0.$$

Da ein Gitter $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subseteq \mathbb{C}$ eine Untergruppe der additiven Gruppe von $\mathbb{C}$ ist, kann man die Faktorgruppe $\mathbb{C}/\Lambda$ bilden:

$$\mathbb{C}/\Lambda = (\mathbb{R}\omega_1 + \mathbb{R}\omega_2)/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \simeq \mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}.$$

Topologisch ist $\mathbb{C}/\Lambda$ ein Torus.

Doppeltperiodische Funktionen: Eine meromorphe komplexe Funktion $f(z)$ heißt doppeltperiodisch bzgl. eines Gitters Λ, wenn

$$f(z+\omega) = f(z) \text{ für alle } \omega \in \Lambda$$

gilt. Gleichwertig damit ist die Bedingung $f(z+\omega_1) = f(z+\omega_2) = f(z)$, wenn $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ ist. Welche doppeltperiodischen Funktionen (bzgl. Λ) gibt es?

- Ist f doppeltperiodisch und holomorph, so ist f nach dem Satz von Liouville konstant.
- Die (historisch) wichtigste doppeltperiodische Funktion ist die Weierstraßsche $\wp$-Funktion, die durch
$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$
definiert wird. $\wp(z)$ hat in allen Punkten $\omega \in \Lambda$ einen Pol zweiter Ordnung und ist sonst holomorph.
- Die Ableitung der Weierstraßschen $\wp$-Funktion
$$\wp'(z) = -2 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^3}$$
ist ebenfalls doppeltperiodisch bzgl. Λ.
- Man kann zeigen, dass jede doppeltperiodische Funktion die Gestalt
$$\frac{f(\wp(z), \wp'(z))}{g(\wp(z), \wp'(z))} \text{ mit Polynomen } f(x,y), g(x,y) \in \mathbb{C}[x,y]$$
hat. Die Menge aller bzgl. Λ doppeltperiodischen Funktionen bildet einen Körper.

[1] Eine funktionentheoretische Einführung findet sich in Kapitel V von „E. Freitag, R. Busam. Funktionentheorie 1. 4. Auflage. Springer, 2006“.

Der Zusammenhang mit elliptischen Kurven: Definiert man für ein Gitter Λ

$$s_m = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^m},$$

so erhält man für die Laurentreihenentwicklungen von $\wp$ und $\wp'$ in $z = 0$:

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + 3s_4 z^2 + 5s_6 z^4 + \cdots = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) s_{2n+2} z^{2n}, \\ \wp'(z) &= -\frac{2}{z^3} + 6s_4 z + 20 s_6 z^3 + \ldots \end{aligned}$$

Da es keine nichtkonstanten holomorphen doppeltperiodischen Funktionen gibt, erhält man daraus schnell die Relation

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3 \quad \text{mit} \quad g_2 = 60 s_4 \quad \text{und} \quad g_3 = 140 s_6,$$

wobei außerdem die Bedingung $g_2^3 - 27 g_3^2 \neq 0$ erfüllt ist.
Definiert man nun eine ebene Kurve E über $\mathbb{C}$ durch die Gleichung

$$y^2 = x^3 - \frac{1}{4} g_2 x - \frac{1}{4} g_3,$$

so ist

$$4(-\frac{1}{4} g_2)^3 + 27(-\frac{1}{4} g_3)^2 = -\frac{1}{16}(g_2^3 - 27 g_3^2) \neq 0,$$

d.h. E ist eine elliptische Kurve. Für $z \in \mathbb{C} \setminus \Lambda$ gilt dann

$$(\wp(z), \frac{1}{2}\wp'(z)) \in E(\mathbb{C}).$$

Man kann dann zeigen, dass durch die Zuordnung

$$z \mapsto (\wp(z), \frac{1}{2}\wp'(z)), \quad \omega \mapsto O \text{ für } \omega \in \Lambda$$

sogar ein Gruppenisomorphismus

$$\mathbb{C}/\Lambda \simeq E(\mathbb{C})$$

definiert wird.

Umgekehrt gilt, dass sich jede elliptische Kurve E über $\mathbb{C}$ auf obige Weise darstellen lässt, d.h. ist E gegeben durch $y^2 = x^3 + ax + b$, so gibt es ein Gitter Λ mit $a = -\frac{1}{4} g_2(\Lambda)$, $b = -\frac{1}{4} g_3(\Lambda)$, $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, etc. Wir geben daher eine elliptische Kurve über $\mathbb{C}$ oft in der Gestalt $\mathbb{C}/\Lambda$ an. Damit kann man Fragen nach Eigenschaften elliptischer Kurven über $\mathbb{C}$ auf Fragen über den Quotienten $\mathbb{C}/\Lambda$ zurückführen.

Isomorphie: Sind Λ_1 und Λ_2 Gitter in $\mathbb{C}$, sind E_1 und E_2 die zugehörigen elliptischen Kurven, so gilt

$$j(E_1) = j(E_2) \quad \Longleftrightarrow \quad E_1 \simeq E_2 \quad \Longleftrightarrow \quad \Lambda_1 \sim \Lambda_2.$$

Ist E_τ die zu $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ (mit $\operatorname{Im}(\tau) > 0$) gehörige elliptische Kurve, so gilt für die j-Invariante

$$j(E_\tau) = \frac{1}{q} + 744 + 196884 q + 21493760 q^2 + \ldots \quad \text{mit} \quad q = e^{2\pi i \tau}.$$

Gruppenstruktur: Gehört die elliptische Kurve E zum Gitter $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, so haben wir jetzt die Gruppenisomorphien

$$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda = (\mathbb{R}\omega_1 \times \mathbb{R}\omega_2)/(\mathbb{Z}\omega_1 \times \mathbb{Z}\omega_2) \simeq \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}.$$

Ist A eine abelsche Gruppe und $m \in \mathbb{N}$, so definiert man die Untergruppe der m-Torsionspunkte durch

$$A[m] = \{a \in A : ma = 0\}.$$

Für eine elliptische Kurve über $\mathbb{C}$ ergibt sich dann

$$E(\mathbb{C})[m] \simeq (\mathbb{C}/\Lambda)[m] = \frac{1}{m}\Lambda/\Lambda \simeq Z_m \times Z_m.$$

Endomorphismen: Ein Endomorphismus einer elliptischen Kurve $\mathbb{C}/\Lambda$ ist eine holomorphe Abbildung der elliptischen Kurve auf sich selbst. Man kann zeigen, dass die Menge der Endomorphismen $\mathrm{End}(\mathbb{C}/\Lambda)$ durch

$$\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$$

beschrieben wird, wobei zu $\alpha \in \mathrm{End}(\Lambda)$ der Endomorphismus $z \mapsto \alpha z$ gehört, d.h.

$$\mathrm{End}(\mathbb{C}/\Lambda) = \{(z \mapsto \alpha z) : \alpha \in \mathrm{End}(\Lambda)\}.$$

Wir werden uns daher einen Endomorphismus als komplexe Zahl vorstellen, wobei eigentlich die Multiplikation mit dieser komplexen Zahl gemeint ist, also $\mathrm{End}(\mathbb{C}/\Lambda) \simeq \mathrm{End}(\Lambda)$. Ist $m \in \mathbb{Z}$, so gilt $m\Lambda \subseteq \Lambda$, also liefert $z \mapsto mz$ einen Endomorphismus von $\mathbb{C}/\Lambda$. Wir haben

$$\mathbb{Z} \subseteq \mathrm{End}(\Lambda) \subseteq \mathbb{C}.$$

Die Endomorphismen bilden offensichtlich einen Ring, den Endomorphismenring $\mathrm{End}(\mathbb{C}/\Lambda) \simeq \mathrm{End}(\Lambda)$ von $\mathbb{C}/\Lambda$. Man kann folgenden Satz zeigen:

SATZ. *Für ein Gitter $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ und zugehörige elliptische Kurve E_τ gibt es folgende Möglichkeiten:*

1. $\mathrm{End}(\mathbb{C}/\Lambda) = \mathbb{Z}$.
2. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{C}/\Lambda) \subseteq \mathbb{Q}(\sqrt{-d})$ *mit $d \in \mathbb{N}$ quadratfrei und $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{-d})$. Man sagt in diesem Fall, dass E_τ komplexe Multiplikation hat.*

Komplexe Multiplikation: Den letzten Satz kann man noch genauer formulieren: Hat $\mathbb{C}/\Lambda$ komplexe Multiplikation, d.h. ist $\mathrm{End}(\mathbb{C}/\Lambda) \neq \mathbb{Z}$, dann ist $\mathrm{End}(\mathbb{C}/\Lambda)$ eine Ordnung in einem imaginärquadratischen Körper, d.h. es gibt $d \in \mathbb{N}$ quadratfrei, $f \in \mathbb{N}$ mit

$$\mathrm{End}(E) \simeq \begin{cases} \mathbb{Z}[f\frac{1+\sqrt{-d}}{2}] & d \equiv 3 \bmod 4, \\ \mathbb{Z}[f\sqrt{-d}] & d \equiv 1, 2 \bmod 4. \end{cases}$$

Elliptische Kurven über $\mathbb{Q}$ mit komplexer Multiplikation: Ist E eine über $\mathbb{Q}$ definierte elliptische Kurve mit komplexer Multiplikation, so gibt es genau 13 mögliche j-Invarianten und Endomorphismenringe. Diese sind in der folgenden Tabelle zusammengestellt. Eine Kurve E ist durch $j(E)$ natürlich nur bis auf $\overline{\mathbb{Q}}$-Isomorphie bestimmt. (Ist $E : y^2 = x^2 + ax + b$ und $j \neq 0, 1728$, so erhält man die anderen Kurven durch $y^2 = x^3 + au^2x + bu^3$, wo u ein Repräsentantensystem von $\mathbb{Q}^*/\mathbb{Q}^{*2}$ durchläuft.)

$\mathrm{End}(E)$	$j(E)$	Beispiel für E
$\mathbb{Z}[\sqrt{-1}]$	$2^6 \cdot 3^3$	$y^2 = x^3 - x$
$\mathbb{Z}[2\sqrt{-1}]$	$2^3 \cdot 3^3 \cdot 11^3$	$y^2 = x^3 - 11x - 14$
$\mathbb{Z}[\sqrt{-2}]$	$2^6 \cdot 5^3$	$y^2 = x^3 - 30x - 56$
$\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$	0	$y^2 = x^3 - 1$
$\mathbb{Z}[\sqrt{-3}]$	$2^4 \cdot 3^3 \cdot 5^3$	$y^2 = x^3 - 15x - 22$
$\mathbb{Z}[\frac{1+3\sqrt{-3}}{2}]$	$-2^{15} \cdot 3 \cdot 5^3$	$y^2 = x^3 - 120x - 506$
$\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$	$-3^3 \cdot 5^3$	$y^2 = x^3 - 35x - 98$
$\mathbb{Z}[\sqrt{-7}]$	$3^3 \cdot 5^3 \cdot 17^3$	$y^2 = x^3 - 595x - 5586$
$\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$	-2^{15}	$y^2 = x^3 - 264x - 1694$
$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$	$-2^{15} \cdot 3^3$	$y^2 = x^3 - 152x - 722$
$\mathbb{Z}[\frac{1+\sqrt{-43}}{2}]$	$-2^{18} \cdot 3^3 \cdot 5^3$	$y^2 = x^3 - 3440x - 77658$
$\mathbb{Z}[\frac{1+\sqrt{-67}}{2}]$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	$y^2 = x^3 - 29480x - 1948226$
$\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	$y^2 = x^3 - 8697680x - 9873093538$

9. Wie bestimmt man $\#E(\mathbb{F}_p)$?

Wir haben bereits zuvor den Satz von Hasse erwähnt, der eine grundlegende Abschätzung für $\#E(\mathbb{F}_p)$ angibt:

Satz (Hasse). *Für eine elliptische Kurve E über $\mathbb{F}_p$ gilt*

$$p+1-2\sqrt{p} < \#E(\mathbb{F}_p) < p+1+2\sqrt{p} \quad \textit{oder anders geschrieben} \quad |\#E(\mathbb{F}_p)-(p+1)| < 2\sqrt{p}.$$

Bemerkungen:

(1) Tatsächlich gibt es auch zu jeder natürlichen Zahl N mit $|N-(p+1)| < 2\sqrt{p}$ eine elliptische Kurve E über $\mathbb{F}_p$ mit $N = \#E(\mathbb{F}_p)$, d.h. alle durch den Satz von Hasse zugelassenen Zahlen für $\#E(\mathbb{F}_p)$ kommen auch vor. Zu vorgegebenem N allerdings eine elliptische Kurve zu finden, ist nicht so leicht.

(2) Ist E eine elliptische Kurve über $\mathbb{F}_p$, so kommen für die Struktur der Gruppe $E(\mathbb{F}_p)$ nur zwei Möglichkeiten in Frage:

$$E(\mathbb{F}_p) \simeq Z_d \quad \text{oder} \quad E(\mathbb{F}_p) \simeq Z_{d_1} \oplus Z_{d_2}.$$

(3) Wichtig für kryptographische Anwendungen ist, dass bei großer Primzahl p auch $\#E(\mathbb{F}_p)$ in der Größenordnung von p ist.

9.1. Elementare Bestimmung von $\#E(\mathbb{F}_p)$. Wir haben früher die Anzahlformel

$$\#E(\mathbb{F}_p) = p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right)$$

kennengelernt. Ist p relativ klein, kann man damit die Gruppenordnung $\#E(\mathbb{F}_p)$ eine über $\mathbb{F}_p$ durch $y^2 = x^3+ax+b$ definierten elliptischen Kurve bequem bestimmen.

9.2. Die Kurven $y^2 = x^3+ax$. Wir betrachten diese Kurven als Beispiel für Kurven, die man aus der Theorie der komplexen Multiplikation erhält.

Sei E über $\mathbb{F}_p$ gegeben durch $y^2 = x^3+ax$, $a \neq 0$. Ist $i \in \overline{\mathbb{F}}_p$ mit $i^2 = -1$, so folgt aus $y^2 = x^3+ax$ sofort $(iy)^2 = (-x)^3 + a(-x)$, d.h.

$$E(\mathbb{F}_p) \to E(\mathbb{F}_p), \quad (x,y) \mapsto (-x, iy)$$

ist eine Abbildung, ein sogenannter Endomorphismus. Durch das Studium der Endomorphismen elliptischer Kurven erhält man dann folgenden Satz:

Satz. *Sei $E : y^2 = x^3+ax$ eine elliptische Kurve über $\mathbb{F}_p$.*

(1) *Ist $p \equiv 3 \bmod 4$, so gilt $\#E(\mathbb{F}_p) = p+1$.*

(2) *Ist $p \equiv 1 \bmod 4$, so gibt es $m,n \in \mathbb{N}$ mit $p = m^2+n^2$. Dann ist*

$$\#E(\mathbb{F}_p) \in \{p+1-2m, p+1+2m, p+1-2n, p+1+2n\}.$$

Beweis für (1): Da mit x auch $-x$ ganz $\mathbb{F}_p$ durchläuft, erhalten wir mit der Anzahlformel und $\left(\frac{-1}{p}\right) = -1$ (wegen $p \equiv 3 \bmod 4$)

$$\begin{aligned}
\#E(\mathbb{F}_p) &= p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax}{p}\right) = p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{(-x)^3+a(-x)}{p}\right) = \\
&= p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{-1}{p}\right)\left(\frac{x^3+ax+b}{p}\right) = p+1-\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right) = \\
&= 2(p+1)-\left(p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right)\right) = 2(p+1)-\#E(\mathbb{F}_p),
\end{aligned}$$

woraus sofort $\#E(\mathbb{F}_p) = p+1$ folgt. ■

Überlegung: Wir betrachten eine elliptische Kurve E über $\mathbb{F}_p$ mit $p \equiv 1 \bmod 4$, die durch eine Gleichung $y^2 = x^3 + ax$ definiert wird. Mit dem Cornacchia-Algorithmus können wir schnell $m, n \in \mathbb{N}$ mit $p = m^2 + n^2$ bestimmen. Dann gilt

$$\#E(\mathbb{F}_p) \in M = \{p + 1 + 2m, p + 1 - 2m, p + 1 - 2n, p + 1 + 2n\}.$$

Sei nun $P \in E(\mathbb{F}_p)$ und $N \in M$.

- Es gilt $\#E(\mathbb{F}_p) \cdot P = O$.
- Ist $N \cdot P \neq O$, so gilt $N \neq \#E(\mathbb{F}_p)$. (Die Zahl N kann also als $\#E(\mathbb{F}_p)$ ausgeschlossen werden.)
- Ist $N \cdot P = O$, so kann $N = \#E(\mathbb{F}_p)$ oder $N \neq \#E(\mathbb{F}_p)$ gelten.

Die Hoffnung ist, dass man durch Wahl von verschiedenen Punkten $P \in E(\mathbb{F}_p)$ die Möglichkeit für $\#E(\mathbb{F}_p)$ schnell auf eine Möglichkeit reduziert. Damit erhalten wir dann folgenden Algorithmus:

Verfahren zur Bestimmung von $\#E(\mathbb{F}_p)$ für Kurven $y^2 = x^3 + ax$, also mit $j(E) = 1728$:
Eingabe: Elliptische Kurve E mit Gleichung $y^2 = x^3 + ax$ über $\mathbb{F}_p$
Ausgabe: $\#E(\mathbb{F}_p)$

if $p \equiv 3 \bmod 4$ **then**
  return $p + 1$
else ▷ $p \equiv 1 \bmod 4$
  Bestimme mit dem Cornacchia-Algorithmus $m, n \in \mathbb{N}$ mit $p = m^2 + n^2$
  $M \leftarrow \{p + 1 + 2m, p + 1 - 2m, p + 1 + 2n, p + 1 - 2n\}$
  while $\#M > 1$ **do**
    Wähle einen zufälligen Punkt $P \in E(\mathbb{F}_p)$
    for $N \in M$ **do**
      if $N \cdot P \neq O$ **then**
        Streiche N aus M heraus.
      end if
    end for
  end while
  return N mit $M = \{N\}$
end if

Hier ist eine zugehörige Python3-Funktion:

```
# Bestimmung der Anzahl #E(F_p) fuer Kurven y^2=x^3+ax, also mit
# j-Invariante 1728
def ek_anzahl_j1728(pab):
  p,a,b=pab
  if b!=0:
    return False
  if p%4==3:
    return p+1
  m,n=cornacchi(p,1)
  M=[p+1+2*m,p+1-2*m,p+1+2*n,p+1-2*n]
  while len(M)>1:
    import random
    P=ek_nxtpkt(random.randint(1,p),pab)
    for N in M:
      if ek_mult(N,P,pab)!=[]:
        M.remove(N)
  return M[0]
```

Beispiel: Wir haben (zufällig) eine 1024-Bit-Primzahl $p \equiv 1 \bmod 4$ gewählt:

$$\begin{aligned} p \;=\; & 12992049545115601262948309175391701214599999472616331442835542856864287020412901 \\ & 76985939768666159087425339274439266522040959065503182777802241322903094442052589 \\ & 66854033404961750508280783260503769853285716183548574490149549854605144323132879 \\ & 69813527363868157238298018395293340922341997738944004318330208643149 7. \end{aligned}$$

Mit dem Cornacchia-Algorithmus haben mir m, n mit $p = m^2 + n^2$ bestimmt:

$$\begin{aligned} m \;=\; & 10365365408709527263145071991523984306074033498186021622275991964779232510215297 \\ & 4641394147670832470118163623081515163698370356720265077812755574267558272 96, \\ n \;=\; & 47412757138858722424946233213841018138040698661781471122373712527819916790939500 \\ & 84098735478311751008920838740037398503438484139774576020890549904911413891. \end{aligned}$$

N	a mit $1 \le a \le 99$ und $\#E_{a,0}(\mathbb{F}_p) = N$
$p+1+2m$	5, 7, 10, 14, 15, 20, 21, 28, 30, 37, 40, 41, 42, 43, 45, 47, 56, 59, 60, 63, 65, 74, 80, 82, 84, 86, 90, 91, 94, 95
$p+1-2m$	55, 67, 77, 85, 97
$p+1+2n$	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 19, 23, 24, 26, 27, 32, 36, 38, 39, 46, 48, 52, 53, 54, 57, 64, 69, 72, 73, 76, 78, 79, 81, 89, 92, 96
$p+1-2n$	11, 17, 22, 25, 29, 31, 33, 34, 35, 44, 49, 50, 51, 58, 61, 62, 66, 68, 70, 71, 75, 83, 87, 88, 93, 98, 99

Bemerkungen:

(1) Das dargestellte Verfahren für die Kurven $y^2 = x^3 + ax$ ist sehr schnell. Ähnliches kann man es für Kurven machen, die über $\mathbb{Q}$ definiert sind und sogenannte komplexe Multiplikation haben.
(2) Das Verfahren ist gut zu Testzwecken geeignet, wenn man für große Primzahlen p elliptische Kurven E und die zugehörige Gruppenordnung $\#E(\mathbb{F}_p)$ braucht.
(3) Im Anhang wird gezeigt, dass für $p > 233$ der Algorithmus immer funktioniert. Für kleine Primzahlen kann es passieren, dass die while-Schleife im Algorithmus unendlich oft durchlaufen wird.

9.3. Der Schoof-Algorithmus und SEA-Algorithmus zur Bestimmung von $\#E(\mathbb{F}_p)$. Dies ist das zur Zeit schnellste Verfahren, um für eine allgemeine elliptische Kurve E über $\mathbb{F}_p$ die Gruppenordnung $\#E(\mathbb{F}_p)$ zu bestimmen. Da in der Vorlesung die dazu nötige Theorie nicht gemacht wurden, gehen wir nicht näher darauf ein. Das Computeralgebrasystem Sagemath verwendet das Verfahren:

```
E=EllipticCurve(GF(p),[a,b])
E.count_points()
```

10. Diskrete Logarithmenberechnung auf elliptischen Kurven

Ist E eine elliptische Kurve über einem Körper K, sind $P, Q \in E(K)$, so heißt eine Zahl x mit $xP = Q$ ein **diskreter Logarithmus von Q zur Basis P in $E(K)$**. Die Berechnung diskreter Logarithmen auf (allgemeine) elliptischen Kurven ist schwierig, weshalb sie für kryptographische Zwecke benutzt werden können.

10.1. Naive Logarithmenberechnung. Sei E eine über $\mathbb{F}_p$ definierte elliptische Kurve und $P, Q \in E(\mathbb{F}_p)$. Wir suchen ein $x \in \mathbb{N}_0$ mit $xP = Q$ oder wollen sehen, dass kein solches x existiert. Natürliche kann man einfach die Zahlen $x = 0, 1, 2, \ldots$ durchprobieren und schauen, ob irgendwann $xP = Q$ gilt. Ein naiver Algorithmus ist folgender:

Naive Logarithmenberechnung:
Eingabe: Elliptische Kurve E über $\mathbb{F}_p$, $P, Q \in E(\mathbb{F}_p)$

Ausgabe: x mit $xP = Q$ oder 'False', falls kein solches x existiert
1: $x \leftarrow 0$, $P_x \leftarrow O$
2: **while** $P_x \neq Q$ **do**
3: $x \leftarrow x + 1$, $P_x \leftarrow P + P_x$
4: **if** $P_x = O$ **then**
5: **return** 'False'
6: **end if**
7: **end while**
8: **return** x

Eine mögliche Python3-Funktion dazu könnte so aussehen:

```
# Berechnung des diskreten Logarithmus von Q zur Basis P auf einer
# elliptischen Kurve pab mit der naiven Methode.
def ek_log_naiv(Q,P,pab):
  x,xP=0,[]
  while xP!=Q:
    x,xP=x+1,ek_add(P,xP,pab)
    if xP==[]:
      return False
  return x
```

10.2. Das Silver-Pohlig-Hellman-Verfahren - Logarithmenberechnung bei glatter Gruppenordnung. Sei E eine elliptische Kurve über $\mathbb{F}_p$ und $P, Q \in E(\mathbb{F}_p)$. Wir wollen die Gleichung

$$xP = Q$$

untersuchen bzw. lösen. Wir nehmen an, wir können die Gruppenordnung berechnen und faktorisieren

$$N = \#E(\mathbb{F}_p) = d_1 d_2 \dots d_r$$

mit paarweise teilerfremden Zahlen d_i. Gilt $xP = Q$, so auch

$$x \cdot \frac{N}{d_i} P = \frac{N}{d_i} Q.$$

Wegen $d_i \cdot \frac{N}{d_i} P = NP = O$ gilt

$$\{x \cdot \frac{N}{d_i} P : x \in \mathbb{Z}\} = \{x \cdot \frac{N}{d_i} P : 0 \leq x \leq d_i - 1\}.$$

Ist d_i klein, so kann man also durch Probieren ein x_i mit

$$x_i \cdot \frac{N}{d_i} P = \frac{N}{d_i} Q \quad \text{und} \quad 0 \leq x_i < d_i$$

finden oder feststellen, dass die Gleichung keine Lösung hat. Es gibt nun zwei Fälle:

- Gibt es ein i, so dass $x_i \cdot \frac{N}{d_i} P = \frac{N}{d_i} Q$ nicht lösbar ist, so existiert auch keine Lösung der Gleichung $xP = Q$.
- Findet man für alle i Zahlen x_i mit $x_i \cdot \frac{N}{d_i} P = \frac{N}{d_i} Q$, berechnet sich dann mit dem chinesischen Restsatz ein $\widetilde{x}$ mit $\widetilde{x} \equiv x_i \bmod d_i$ für alle i, so ist

  $$\widetilde{x} P = Q,$$

  d.h. wir haben eine Lösung der Gleichung gefunden.

Das Verfahren funktioniert also, wenn man die Gruppenordnung $N = d_1 \dots d_r$ faktorisieren kann mit paarweise teilerfremden kleinen Zahlen d_i. Man sagt dann auch, E hat glatte Gruppenordnung.

Eine Python3-Funktion könnte so aussehen:

```
# Berechnung des diskreten Logarithmus von Q zur Basis P auf einer
# elliptischen Kurve pab, wo die Gruppenordnung sich faktorisieren laesst
# und nur kleine Primteiler hat: N=q_1^e_1*...*q_r^e_r.
def ek_log_glatt(Q,P,pab,N):
  F=factor(N)
  x=[]
  qe=[]
  for q,e in F:
    qe_i=q**e
    x_i=ek_log_naiv(ek_mult(N//qe_i,Q,pab),ek_mult(N//qe_i,P,pab),pab)
    if x_i==False:
      return False
    qe.append(qe_i)
    x.append(x_i)
  return crs(x,qe)[0]
```

Beispiel: Die Kurve $E : y^2 = x^3 + ax + b$ über $\mathbb{F}_p$ mit

$$p = 100000000000000140431, \quad a = -152, \quad b = -722$$

hat (glatte) Gruppenordnung

$$N = 100000000014721958125 = 625 \cdot 169 \cdot 17 \cdot 23 \cdot 367 \cdot 647 \cdot 2417 \cdot 4219.$$

Wir wollen $xP = Q$ für die Kurvenpunkte

$$P = (2, 19029769932505619219) \quad \text{und} \quad Q = (68009693572155891 86, 74352320581165835102)$$

lösen. Nun findet man durch einfaches Probieren:

Die Gleichung	wird gelöst von
$x \cdot (N/625)P = (N/625)Q$	$x \equiv 2 \bmod 625$
$x \cdot (N/169)P = (N/169)Q$	$x \equiv 7 \bmod 169$
$x \cdot (N/17)P = (N/17)Q$	$x \equiv 8 \bmod 17$
$x \cdot (N/23)P = (N/23)Q$	$x \equiv 22 \bmod 23$
$x \cdot (N/367)P = (N/367)Q$	$x \equiv 47 \bmod 367$
$x \cdot (N/647)P = (N/647)Q$	$x \equiv 139 \bmod 647$
$x \cdot (N/2417)P = (N/2417)Q$	$x \equiv 922 \bmod 2417$
$x \cdot (N/4219)P = (N/4219)Q$	$x \equiv 2064 \bmod 4219$

woraus man mit dem chinesischen Restsatz sofort die Lösung

$$x = 19350540357117144377$$

erhält.

Bemerkungen: Soll die Berechnung diskreter Logarithmen schwierig sein, muss man auf jeden Fall Kurven mit glatter Gruppenordnung vermeiden. Allerdings sind solche Kurven auch eher selten.

10.3. Die Pollardsche ρ-Methode zur Logarithmenberechnung auf elliptischen Kurven. Wir übertragen die Pollardsche ρ-Methode zur Logarithmenberechnung in $\mathbb{F}_p^*$ auf elliptische Kurven.

Gegeben sei eine Primzahl $p \geq 5$, eine über $\mathbb{F}_p$ definierte elliptische Kurve E und zwei Punkte $P, Q \in E(\mathbb{F}_p)$. Wir setzen außerdem voraus, dass die Ordnung $\operatorname{ord}(P)$ des Punktes P bekannt ist. Außerdem sollte ein $x \in \mathbb{N}_0$ existieren mit $Q = xP$. Eine notwendige Bedingung dafür ist $\operatorname{ord}(P) \cdot Q = O$. Ein solches x soll bestimmt werden.

1. Schritt: Wir konstruieren rekursiv eine Folge R_i von Punkten in $E(\mathbb{F}_p)$ wie folgt:

$$R_0 = O \quad \text{und} \quad R_{i+1} = \begin{cases} P + R_i, & \text{falls } R_i = O \text{ oder } x_{R_i} \equiv 0 \bmod 3, \\ 2R_i, & \text{falls } x_{R_i} \equiv 1 \bmod 3, \\ Q + R_i, & \text{falls } x_{R_i} \equiv 2 \bmod 3. \end{cases}$$

Dabei ist x_{R_i} die x-Koordinate von R_i, also $R_i = (x_{R_i}, y_{R_i})$, die durch eine Zahl zwischen 0 und $p-1$ repräsentiert werden soll. R_i lässt sich aus P und Q linear kombinieren

$$R_i = e_i P + f_i Q,$$

wenn wir rekursiv definieren

$$(e_0, f_0) = (0,0) \quad \text{und} \quad (e_{i+1}, f_{i+1}) = \begin{cases} ((e_i + 1) \bmod \operatorname{ord}(P), f_i) & \text{falls } R_i = O \text{ oder} \\ & \quad x_{R_i} \equiv 0 \bmod 3, \\ (2e_i \bmod \operatorname{ord}(P), 2f_i \bmod \operatorname{ord}(P)), & \text{falls } x_{R_i} \equiv 1 \bmod 3, \\ (e_i, (f_i + 1) \bmod \operatorname{ord}(P)), & \text{falls } x_{R_i} \equiv 2 \bmod 3. \end{cases}$$

Wenn sich R_i wie eine Zufallsfolge in $E(\mathbb{F}_p)$ verhält, dann kann man erwarten, dass nach $O(\sqrt{\operatorname{ord}(P)})$ Schritten ($O(\sqrt{p})$ Schritten) ein Index $i > 0$ vorkommt mit

$$R_i = R_{2i}.$$

In diesem Fall erhalten wir eine Relation

$$e_i P + f_i Q = e_{2i} P + f_{2i} Q.$$

Wir rechnen also rekursiv $(R_i, e_i, f_i, R_{2i} e_{2i}, f_{2i})$ aus und testen dann, ob $R_i = R_{2i}$ gilt. Wenn ja, haben wir eine obige Relation gefunden. Dann gilt also

$$(f_{2i} - f_i) Q = (e_i - e_{2i}) P.$$

Dies ist das Ergebnis des 1. Schritts.

Beispiele:

(1) Wir betrachten die Kurve $y^2 = x^3 + x + 1$ über $\mathbb{F}_{1009}$, die die Ordnung $N = 1034$ hat.

i	R_i	e_i	f_i	R_{2i}	e_{2i}	f_{2i}
0	O	0	0	O	0	0
1	$(1, 149)$	1	0	$(672, 465)$	2	0
2	$(672, 465)$	2	0	$(46, 103)$	6	0
3	$(727, 882)$	3	0	$(416, 892)$	24	0
4	$(46, 103)$	6	0	$(324, 525)$	24	2
5	$(556, 832)$	12	0	$(864, 140)$	25	3
6	$(416, 892)$	24	0	$(743, 228)$	27	3
7	$(542, 935)$	24	1	$(181, 78)$	54	8
8	$(324, 525)$	24	2	$(235, 719)$	216	32
9	$(107, 15)$	25	2	$(549, 179)$	864	128
10	$(864, 140)$	25	3	$(925, 724)$	696	256
11	$(669, 805)$	26	3	$(934, 282)$	358	513
12	$(743, 228)$	27	3	$(841, 733)$	716	1027
13	$(478, 164)$	27	4	$(368, 871)$	796	1006
14	$(181, 78)$	54	8	$(11, 873)$	558	980
15	$(970, 424)$	108	16	$(925, 724)$	82	928
16	$(235, 719)$	216	32	$(934, 282)$	164	823
17	$(130, 219)$	432	64	$(841, 733)$	328	613
18	$(549, 179)$	864	128	$(368, 871)$	278	384
19	$(841, 733)$	865	128	$(11, 873)$	556	770
20	$(925, 724)$	696	256	$(925, 724)$	78	508

Es ist $R_{20} = R_{40}$, woraus die Relation

$$696P + 256Q = 78P + 508Q$$

folgt, und damit

$$252Q = 618P.$$

(2) Für $p = 10007$ und die über $\mathbb{F}_p$ durch $y^2 = x^3 + 2x + 3$ definierte elliptische Kurve E mit $N = \#E(\mathbb{F}_p) = 9846$ mit den Punkten

$$P = (4, 7385) \text{ (mit ord}\,(P) = N), \quad Q = (6497, 694)$$

findet man $R_{180} = R_{360} = (8474, 3593)$ und die Relation

$$6892P + 3614Q = 178P + 8573Q,$$

was zu

$$4959Q = 6714P$$

führt.

(3) Für $p = 10^{10} + 19$ und die über $\mathbb{F}_p$ durch $y^2 = x^3 + 5x + 7$ definierte elliptische Kurve E mit den Punkten

$$P = (1, 6243000782), \quad Q = (622744699, 4426807157),$$

den Ordnungen

$$N = 10000113575 = 5^2 \cdot 17 \cdot 23529679, \quad \operatorname{ord}(P) = N$$

haben wir gefunden

$$R_{166068} = R_{2\cdot 166068} = (7526285112, 3111113166)$$

und damit

$$6808636796P + 5624888777Q = 5201685566P + 2317088397Q,$$

was zur Beziehung

$$-3307800380Q = 1606951230P,$$

also

$$6692313195Q = 1606951230P$$

führt.

2. Schritt: Wir nehmen an, wir haben eine Relation

$$(f_{2i} - f_i)Q = (e_i - e_{2i})P$$

gefunden, wir nehmen auch an, dass ein x existiert mit $Q = xP$. Dann folgt $(f_{2i} - f_i)xP = (e_i - e_{2i})P$, also

$$(f_{2i} - f_i)x \equiv e_i - e_{2i} \bmod \operatorname{ord}(P).$$

Dies Gleichung haben wir früher behandelt. Ist die Gleichung lösbar, hat sie

$$\operatorname{ggT}(f_{2i} - f_i, \operatorname{ord}(P))$$

Lösungen x_i zwischen 0 und $\operatorname{ord}(P) - 1$, die man einfach bestimmen kann. Wir testen nun durch, für welches x_i die Beziehung

$$Q = x_i P$$

gilt. Hierfür müssen wir auch $\operatorname{ord}(P)$ kennen.

Beispiele:

(1) Wir setzen das obige 1. Beispiel fort (mit $p = 1009$ und $N = 1034$). Wir haben die Beziehung

$$252Q = 618P$$

gefunden. Nun ist $\operatorname{ord}(P) = N = 1034$, woraus mit dem Ansatz $Q = xP$ die Gleichung

$$252x \equiv 618 \bmod 1034$$

folgt. Mit dem üblichen Verfahren (zur Gleichung $ax \equiv b \bmod m$) finden wie die zwei Lösungen

$$x_1 = 64, \quad x_2 = 581.$$

$$64P = (589, 173) \quad \text{und} \quad 581P = (9, 235),$$

sodass $x = 581$ der gesuchte Logarithmus ist.

(2) Im 2. Beispiel mit $p = 1007$, $N = 9846$ und der Relation

$$4959Q = 6714P$$

erhalten wir wegen $\operatorname{ord}(P) = N = 9846$ mit dem Ansatz $Q = xP$ die Gleichung

$$4959x \equiv 6714 \bmod 9846,$$

die die Lösungen (zwischen 0 und 9845)

$$460, 1554, 2648, 3742, 4836, 5930, 7024, 8118, 9212$$

hat. Durch Durchprobieren findet man, dass

$$x = 2648$$

$Q = xP$ löst.

(3) Im 3. Beispiel mit $p = 10^{10} + 19$, $N = \operatorname{ord}(P) = 10000113575$ hatten wir die Relation

$$6692313195Q = 1606951230P$$

gefunden, die mit dem Ansatz $Q = xP$ zu

$$6692313195x \equiv 1606951230 \bmod 10000113575$$

führt. Die Lösungen dieser Kongruenzgleichung sind (modulo $\operatorname{ord}(P)$)

$$733879119, 2733901834, 4733924549, 6733947264, 8733969979.$$

Indem wir die fünf Möglichkeiten durchprobieren, erhalten wir für $Q = xP$ die Lösung

$$x = 4733924549.$$

Eine mögliche Python3-Funktion kann so aussehen:

```
# Berechnung des diskreten Logarithmen von Q zur Basis P auf einer
# elliptischen Kurve pab mit der Pollardschen rho-Methode. Eingegeben
# werden mus auch die Ordnung des Punktes P, also ord(P).
def ek_log_rho(Q,P,pab,ordP):
  def nachfolger(R,e,f):
    if R==[] or R[0]%3==0:
      return ek_add(P,R,pab),(e+1)%ordP,f
    if R[0]%3==1:
      return ek_add(R,R,pab),(2*e)%ordP,(2*f)%ordP
    return ek_add(Q,R,pab),e,(f+1)%ordP
  R_i,e_i,f_i,R_2i,e_2i,f_2i=[],0,0,[],0,0
  i=0
  while True:
    i+=1
    R_i,e_i,f_i=nachfolger(R_i,e_i,f_i)
    R_2i,e_2i,f_2i=nachfolger(R_2i,e_2i,f_2i)
    R_2i,e_2i,f_2i=nachfolger(R_2i,e_2i,f_2i)
    if R_i==R_2i: # Nun gilt e_i*P+f_i*Q=e_2i*P+f_2i*Q
      x=axbmodm(f_2i-f_i,e_i-e_2i,ordP)
      for x_i in x:
        if ek_mult(x_i,P,pab)==Q:
          return x_i
```

10.4. Rekorde. Um zu illustrieren, wie schwierig die Berechnung diskreter Logarithmen in den Gruppen $E(\mathbb{F}_p)$ ist, erwähnen wir einen Rekord aus dem Jahr 2012: Gegeben ist die elliptische Kurve „secp112r1“[2], die über $\mathbb{F}_p$ mit

$$p = \frac{2^{128} - 3}{11 \cdot 6949} = 4451685225093714772084598273548427$$

durch die Gleichung $y^2 = x^3 + ax + b$ mit

$$a = -3 \quad \text{und} \quad b = 2061118396808653202902996166388514$$

gegeben ist. $\#E(\mathbb{F}_p)$ hat Primzahlordnung mit

$$N = \#E(\mathbb{F}_p) = 4451685225093714776491891542548933,$$

der Punkt

$$P = (1882814650579725348922237787137 52, 3419875491033170827167861896082688)$$

erzeugt die Gruppe.
Bos, Kaihara, Kleinjung, Lenstra, Montgomery wählten

$$x_Q = \lfloor (\pi - 3) \cdot 10^{34} \rfloor$$

[2]Die Kurve „secp112r1“ findet sich in SEC 2: Recommended Elliptic Curve Domain Parameters

und dazu den Punkt

$$Q = (1415926535897932384626433832795028, 3846759606494706724286139623885544).$$

Es gelang ihnen dann, den diskreten Logarithmus von Q zur Basis P in $E(\mathbb{F}_p)$ mit der Pollardschen ρ-Methode zu berechnen: Die Zahl

$$x = 312521636014772477161767351856699$$

erfüllt die Gleichung $Q = xP$.
(Quelle: J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, P. L. Montgomery. Solving a 112-bit Prime Elliptic Curve Discrete Logarithme Problem on Game Consoles using Sloppy Reduction. International Journal of Applied Cryptography. Volume 2, Issue 3, February 2012. Pages 212-228.)

11. Anhang: Anmerkungen zur Bestimmung von $\#E(\mathbb{F}_p)$ für elliptische Kurven mit j-Invariante 1728

Der vorliegende Abschnitt setzt Grundkenntnisse über Endomorphismen elliptischer Kurven voraus, die aber in der Vorlesung nicht besprochen wurden. Wir erinnern noch daran, dass für $p \geq 5$ jede über $\mathbb{F}_p$ definierte elliptische Kurve mit j-Invariante 1728 durch eine Gleichung $y^2 = x^3 + ax$ mit $a \in \mathbb{F}_p^*$ definiert wird.

Bemerkung: Wird für $p \geq 5$ eine elliptische Kurve E durch $y^2 = x^3 + ax$ definiert, und ist $i \in \overline{\mathbb{F}}_p$ mit $i^2 = -1$, so gilt:

$$(x, y) \in E(\overline{\mathbb{F}}_p) \quad \Longrightarrow \quad y^2 = x^3 + ax \boxed{???}$$

Daher definiert

$$\phi : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p), \quad (x, y) \mapsto (-x, iy)$$

einen Endomorphismus $\phi \in \mathrm{End}(E)$. Es gilt

$$\phi^2((x, y)) = \phi(\phi((x, y))) = \phi((-x, iy)) = (-(-x), i(iy)) = (x, -y) = -(x, y),$$

sodass im Endomorphismenring

$$\phi^2 = -1$$

gilt.

LEMMA. *Ist E eine über $\mathbb{F}_p$ mit $p \geq 5$ durch $y^2 = x^3 + ax$ definierte elliptische Kurve, $i \in \overline{\mathbb{F}}_p$ mit $i^2 = -1$ und $\pi, \phi \in \mathrm{End}(E)$ mit $\pi((x, y)) = (x^p, y^p)$ und $\phi((x, y)) = (-x, iy)$, so gilt:*

(1) *Im Fall $p \equiv 1 \bmod 4$ ist $\mathrm{End}(E) = \mathbb{Z}[\phi]$ mit $\phi^2 = -1$, es gibt $m, n \in \mathbb{Z}$ mit*

$$\pi = m + n\phi \quad \text{und} \quad p = m^2 + n^2 \quad \text{und} \quad \#E(\mathbb{F}_p) = p + 1 - 2m.$$

(2) *Im Fall $p \equiv 3 \bmod 4$ ist E supersingulär, es gilt $\pi^2 = -p$ und*

$$\#E(\mathbb{F}_p) = p + 1.$$

Beweis:

(0) Vorbemerkung: Es gilt

$$\begin{aligned}(\pi\phi)((x, y)) &= \pi(\phi((x, y))) = \pi((-x, iy)) = ((-x)^p, (iy)^p) = (-x^p, (i^2)^{\frac{p-1}{2}} iy^p) = \\ &= (-x^p, (-1)^{\frac{p-1}{2}} iy^p) = (-x^p, \left(\frac{-1}{p}\right) iy^p), \\ (\phi\pi)((x, y)) &= \phi((x^p, y^p)) = (-x^p, iy^p),\end{aligned}$$

also

$$\pi\phi = \begin{cases} \phi\pi & \text{im Fall } p \equiv 1 \bmod 4, \\ -\phi\pi & \text{im Fall } p \equiv 3 \bmod 4. \end{cases}$$

(1) Sei $p \equiv 1 \bmod 4$. Dann ist also $\pi\phi = \phi\pi$.

- Wäre E supersingulär, so würde $\pi^2 = -p$ und damit
$$(\pi\phi)^2 = \pi\phi\pi\phi = \pi\pi\phi\phi = (-p)(-1) = p$$
folgen. So etwas ist aber in einer definiten Quaternionenalgebra nicht möglich. Daher ist E nicht supersingulär.
- Aus $\phi \in \mathrm{End}(E)$ folgt $\mathbb{Z}[\phi] \subseteq \mathrm{End}(E)$. Da aber $\mathbb{Z}[\phi]$ die Maximalordnung von $\mathbb{Q}(\phi) \simeq \mathbb{Q}(\sqrt{-1})$ ist, folgt $\mathrm{End}(E) \subseteq \mathbb{Z}[\phi]$, und damit
$$\mathrm{End}(E) = \mathbb{Z}[\phi].$$
Daher gibt es $m, n \in \mathbb{Z}$ mit
$$\pi = m + n\phi.$$
Aus $p = \mathrm{N}(\pi)$ folgt $p = m^2 + n^2$, aus $E(\mathbb{F}_p) = \mathrm{Kern}(\pi - 1)$ und der Separabilität von $\pi - 1$
$$\begin{aligned} \#E(\mathbb{F}_p) &= \mathrm{N}(\pi - 1) = \mathrm{N}((m-1) + n\phi) = (m-1)^2 + n^2 = \\ &= m^2 - 2m + 1 + n^2 = p + 1 - 2m. \end{aligned}$$

(2) Sei $p \equiv 3 \bmod 4$. Dann ist $\pi\phi = -\phi\pi$. Daher ist $\mathrm{End}(E)$ nicht kommutativ, also ist E supersingulär und damit gilt $\pi^2 = -p$. Es folgt $\mathrm{Sp}(\pi) = 0$ und damit
$$\#E(\mathbb{F}_p) = p + 1 - \mathrm{Sp}(\pi) = p + 1.$$

LEMMA. *Sei E eine über $\mathbb{F}_p$ definierte elliptische Kurve, $\pi \in \mathrm{End}(E)$ der Frobenius-Endomorphismus und $M \in \mathbb{Z}$. Wegen $\pi \neq 1$ kann man $\frac{M}{\pi-1}$ als Element von $\mathbb{Q} \otimes \mathrm{End}(E)$ betrachten. Dann gilt:*
$$E(\mathbb{F}_p) \subseteq E[M] \quad \Longleftrightarrow \quad \frac{M}{\pi - 1} \in \mathrm{End}(E).$$

Beweis:

- Betrachten wir $\pi - 1$ und M als Endomorphismen, so ist
$$E(\mathbb{F}_p) = \{P \in E(\overline{\mathbb{F}}_p) : \pi(P) = P\} = \{P \in E(\overline{\mathbb{F}}_p) : (\pi - 1)(P) = O\} = \mathrm{Kern}(\pi - 1)$$
und
$$E[M] = \{P \in E(\overline{\mathbb{F}}_p : M \cdot P = O\} = \mathrm{Kern}(M),$$
sodass wir die Äquivalenz
$$E(\mathbb{F}_p) \subseteq E[M] \quad \Longleftrightarrow \quad \mathrm{Kern}(\pi - 1) \subseteq \mathrm{Kern}(M)$$
erhalten.
- $\Longrightarrow$ Wir setzen also
$$\mathrm{Kern}(\pi - 1) \subseteq \mathrm{Kern}(M)$$
voraus. Nun ist $\pi - 1$ separabel. Nach Silverman, The Arithmetic of Elliptic Curves, 2nd Edition, Corollary 4.11 existiert ein Endomorphismus $\mu \in \mathrm{End}(E)$ mit
$$M = \mu \cdot (\pi - 1).$$
Dann ist aber
$$\mu = \frac{M}{\pi - 1} \in \mathrm{End}(E).$$
- $\Longleftarrow$ Ist $\frac{M}{\pi-1} \in \mathrm{End}(E)$, so gibt es einen Endomorphismus $\mu \in \mathrm{End}(E)$ mit $M = \mu \cdot (\pi - 1)$. Daraus folgt aber sofort
$$\mathrm{Kern}(\pi - 1) \subseteq \mathrm{Kern}(M), \quad \text{also} \quad E(\mathbb{F}_p) \subseteq E[M],$$
wie behauptet. ■

LEMMA. (1) *Für $m, n \in \mathbb{Z}$ gilt die Relation*

$$(m-1)^2 + n^2 \mid 4m \cdot \mathrm{ggT}(m-1, n)$$

genau dann, wenn $m = 0$ ist oder einer der folgenden Fälle vorliegt:

m^2+n^2	m	n	$(m-1)^2+n^2$	$\mathrm{ggT}(m-1,n)$
1	-1	0	4	2
1	1	0	0	0
2	1	± 1	1	1
4	2	0	1	1
5	-1	± 2	8	2
5	1	± 2	4	2
5	2	± 1	2	1
9	-3	0	16	4
9	3	0	4	2
13	3	± 2	8	2
17	1	± 4	16	4
25	5	0	16	4
29	-5	± 2	40	2
29	5	± 2	20	2
89	5	± 8	80	4
233	13	± 8	208	4
305	17	± 4	272	4

(2) *Für $m, n \in \mathbb{Z}$ gilt die Relation*

$$(m-1)^2 + n^2 \mid 2(m-n) \cdot \mathrm{ggT}(m-1, n)$$

genau dann, wenn $m = n$ ist oder einer der folgenden Fälle vorliegt:

m^2+n^2	m	n	$(m-1)^2+n^2$	$\mathrm{ggT}(m-1,n)$
1	-1	0	4	2
1	0	-1	2	1
1	0	1	2	1
1	1	0	0	0
2	1	-1	1	1
4	2	0	1	1
5	1	2	4	2
5	1	-2	4	2
5	2	-1	2	1
5	2	1	2	1
9	3	0	4	2
13	-3	2	20	2
13	2	-3	10	1
17	-1	4	20	2
17	4	-1	10	1

Beweis:

(1) In den Fällen $m = 0$ und $(m,n) = (1,0)$ ist die Beziehung offensichtlich erfüllt, sodass die dies im Folgenden ausschließen können. Dann ist sowohl die linke als auch die rechte Seite von 0 verschieden. Wir betrachten $\mathrm{ggT}(m-1,n)$:
- Gibt es eine ungerade Primzahl ℓ mit $\ell \mid \mathrm{ggT}(m-1,n)$ und ist dann $e \geq 1$ maximal mit $\ell^e \mid \mathrm{ggT}(m-1,n)$, so folgt aus $\ell^{2e} \mid (m-1)^2$ und $\ell^{2e} \mid n^2$ sofort $\ell^{2e} \mid (m-1)^2+n^2$ und damit $\ell^{2e} \mid 4m \cdot \mathrm{ggT}(m-1,n)$. Wegen $\ell \mid m-1$ gilt $\mathrm{ggT}(m,\ell) = 1$, und damit $\ell^{2e} \mid \mathrm{ggT}(m-1,n)$. Dies widerspricht aber der Wahl von e. Daher wird $\mathrm{ggT}(m-1,n)$ von keiner ungeraden Primzahl geteilt, es ist also $\mathrm{ggT}(m-1,n) = 2^e$ mit $e \in \mathbb{N}_0$.
- Gilt $2 \mid \mathrm{ggT}(m-1,n)$ und ist $e \geq 1$ maximal mit $2^e \mid \mathrm{ggT}(m-1,n)$, so gilt $2^{2e} \mid (m-1)^2+n^2$, und damit $2^{2e} \mid 4m \cdot \mathrm{ggT}(m-1,n)$. Wegen $2 \nmid m$ folgt durch Vergleich der Exponenten bei 2 die Ungleichung $2e \leq 2+e$, also $e \leq 2$.

Damit haben wir gezeigt, dass gilt

$$\mathrm{ggT}(m-1,n) \in \{1,2,4\}.$$

Die Beziehung impliziert dann

$$(m-1)^2+n^2 \mid 16m.$$

Dies impliziert $(m-1^2)+n^2 \leq 16|m|$, was wir weiter umformen:

$$\begin{aligned}
(m-1)^2+n^2 \leq 16|m| &\implies m^2-2m+1+n^2 \leq 16|m| \implies \\
&\implies m^2+n^2+1 \leq 18|m| \implies \\
&\implies (m^2-2\cdot 9|m|+81)+n^2 \leq 80 \implies \\
&\implies (|m|-9)^2+n^2 \leq 80 \implies \\
&\implies (|m|-9)^2 \leq 80 \text{ und } n^2 \leq 80 \implies \\
&\implies (|m|-9)^2 \leq 8^2 \text{ und } n^2 \leq 8^2 \implies \\
&\implies ||m|-9| \leq 8 \text{ und } |n| \leq 8 \implies \\
&\implies |m| \leq 17 \text{ und } |n| \leq 8.
\end{aligned}$$

Wir haben also Schranken für m und n bestimmt. Die Tabelle wurde gefunden durch Überprüfen der endlich vielen in Frage kommenden Fälle.

(2) In den Fällen $m = n$ und $(m, n) = (1, 0)$ ist die Beziehung offensichtlich erfüllt, sodass wir diese Fälle im Folgenden ausschließen können. Dann sind linke und rechte Seite von 0 verschieden. Wir betrachten $\mathrm{ggT}(m-1, n)$:
- Gibt es eine ungerade Primzahl ℓ mit $\ell \mid \mathrm{ggT}(m-1, n)$, so folgt $\ell \nmid m - n$. Ist $e \geq 1$ maximal mit $\ell^e \mid \mathrm{ggT}(m-1, n)$, so würde $\ell^{2e} \mid (m-1)^2 + n^2$ und damit ein Widerspruch folgen. Also teilt keine ungerade Primzahl $\mathrm{ggT}(m-1, n)$. Daher bleibt nur die Möglichkeit $\mathrm{ggT}(m-1, n) = 2^e$ mit $e \in \mathbb{N}_0$.
- Gilt $2 \mid \mathrm{ggT}(m-1, n)$, so gilt $2 \nmid m - n$. Ist $e \geq 1$ maximale mit $2^e \mid \mathrm{ggT}(m-1, n)$, so gilt $2^{2e} \mid (m-1)^2 + n^2$, woraus dann $2e \leq 1 + e$, also $e \leq 1$ folgt. Wir erhalten $\mathrm{ggT}(m-1, n) = 2$.

Damit haben wir gezeigt, dass gilt

$$\mathrm{ggT}(m-1, n) \in \{1, 2\}.$$

Die vorausgesetzte Beziehung impliziert daher

$$(m-1)^2 + n^2 \mid 4(m-n).$$

Es folgt

$$(m-1)^2 + n^2 \leq 4|m-n|,$$

und damit nacheinander:

$$\begin{aligned}
(m-1)^2 + n^2 \leq 4|m-n| &\implies m^2 - 2m + 1 + n^2 \leq 4|m| + 4|n| \implies \\
&\implies m^2 + n^2 + 1 \leq 6|m| + 4|n| \implies \\
&\implies (m^2 - 2 \cdot 3|m| + 9) + (n^2 - 2 \cdot 2|n| + 4) \leq 12 \implies \\
&\implies (|m| - 3)^2 + (|n| - 2)^2 \leq 12 \implies \\
&\implies (|m| - 3)^2 \leq 12 \text{ und } (|n| - 2)^2 \leq 12 \implies \\
&\implies (|m| - 3)^2 \leq 3^2 \text{ und } (|n| - 2)^2 \leq 3^2 \implies \\
&\implies ||m| - 3| \leq 3 \text{ und } ||n| - 2| \leq 3 \implies \\
&\implies |m| \leq 6 \text{ und } |n| \leq 5.
\end{aligned}$$

Indem man nun alle Möglichkeiten mit $|m| \leq 6$ und $|n| \leq 5$ durchprobiert, erhält man obige Tabelle. ■

Satz. *Sei $p \geq 5$ eine Primzahl mit $p \equiv 1 \bmod 4$ und E eine über $\mathbb{F}_p$ definierte elliptische Kurve mit $j(E) = 1728$. Dann lässt sich E durch eine Weierstraß-Gleichung $y^2 = x^3 + ax$ beschreiben. Der Endomorphismenring ist $\mathrm{End}(E) = \mathbb{Z}[i]$. Ist π der Frobenius-Endomorphismus, so gibt es $m, n \in \mathbb{Z}$ mit*

$$\pi = m + ni,$$

wobei wir o.E. $n \in \mathbb{N}$ annehmen können. Es gilt dann

$$p = \mathrm{N}(\pi) = m^2 + n^2 \quad \text{und} \quad \#E(\mathbb{F}_p) = p + 1 - \mathrm{Sp}(\pi) = p + 1 - 2m$$

und insbesondere

$$(p + 1 - 2m) \cdot P = O \text{ für alle } P \in E(\mathbb{F}_p).$$

(1) *Genau dann gilt* $(p+1+2m)\cdot P = O$ *für alle* $P \in E(\mathbb{F}_p)$*, wenn einer der folgenden Fälle vorliegt:*

$p = m^2+n^2$	m	n	$\#E(\mathbb{F}_p) = p+1-2m$	$p+1+2m$
5	-1	2	8	4
5	1	2	4	8
5	2	1	2	10
13	3	2	8	20
17	1	4	16	20
29	-5	2	40	20
29	5	2	20	40
89	5	8	80	100
233	13	8	182	260

(2) *Genau dann gilt* $(p+1-2n)\cdot P = O$ *für alle* $P \in E(\mathbb{F}_p)$*, wenn einer der folgenden Fälle vorliegt:*

$p = m^2+n^2$	m	n	$\#E(\mathbb{F}_p) = p+1-2m$	$p+1-2n$
5	1	2	4	2
5	2	1	2	4
13	-3	2	20	10
17	-1	4	20	10

(3) *Genau dann gilt* $(p+1+2n)\cdot P = O$ *für alle* $P \in E(\mathbb{F}_p)$*, wenn einer der folgenden Fälle vorliegt:*

$p = m^2+n^2$	m	n	$\#E(\mathbb{F}_p) = p+1-2m$	$p+1+2n$
5	1	2	4	10
5	2	1	2	8
13	2	3	10	20
17	4	1	10	20

Beweis:

(0) Die Grundidee für das nachfolgende Vorgehen steht in einem früheren Lemma: Für $M \in \mathbb{Z}$ gilt

$$E(\mathbb{F}_p) \subseteq E[M] \quad \Longleftrightarrow \quad \mu = \frac{M}{\pi - 1} \in \mathbb{Z}[i],$$

wobei $\frac{M}{\pi-1}$ zunächst als Element von $\mathbb{Q}(i)$ aufzufassen ist.

(1) Es gilt (wegen $(p+1-2m)\cdot P = O$ für alle $P \in E(\mathbb{F}_p)$):

$$\begin{aligned}
(p+1+2m)\cdot P = O \text{ für alle } P \in E(\mathbb{F}_p) \quad &\Longleftrightarrow \quad 4m \cdot P = O \text{ für alle } P \in E(\mathbb{F}_p) \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad E(\mathbb{F}_p) \subseteq E[4m] \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad \mathrm{Kern}(\pi - 1) \subseteq \mathrm{Kern}(4m) \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad 4m = \mu \cdot (\pi - 1) \text{ für ein } \mu \in Z[i].
\end{aligned}$$

μ ist durch $4m$ und $\pi - 1$ bestimmt. Wir rechnen nun im Quotientenkörper $\mathbb{Q}(i)$:

$$\mu \quad = \quad \frac{4m}{\pi - 1} = \frac{4m}{(m-1)+ni} = \frac{4m((m-1)-ni)}{((m-1)+ni)((m-1)-ni)} = \frac{4m(m-1)-4mni}{(m-1)^2+n^2}.$$

Damit gilt:

$$\begin{aligned}\mu \in \mathbb{Z}[i] &\iff \frac{4m(m-1)}{(m-1)^2+n^2} \in \mathbb{Z} \text{ und } \frac{4mn}{(m-1)^2+n^2} \in \mathbb{Z} \iff \\ &\iff (m-1)^2+n^2 \mid 4m(m-1) \text{ und } (m-1)^2+n^2 \mid 4mn \iff \\ &\iff (m-1)^2+n^2 \mid 4m \cdot \mathrm{ggT}(m-1,n).\end{aligned}$$

Damit erhalten wir:

$$(p+1+2m)\cdot P = O \text{ für alle } P \in E(\mathbb{F}_p) \iff (m-1)^2+n^2 \mid 4m \cdot \mathrm{ggT}(m-1,n).$$

Nun schaut man in der Liste des vorangegangenen Lemmas nach.

(2) Es gilt:

$$\begin{aligned}(p+1-2n)\cdot P = O \text{ für alle } P \in E(\mathbb{F}_p) &\iff 2(m-n)\cdot P = O \text{ für alle } P \in E(\mathbb{F}_p) \iff \\ &\iff E(\mathbb{F}_p) \subseteq E[2(m-n)] \iff \\ &\iff \mathrm{Kern}(\pi-1) \subseteq \mathrm{Kern}(2(m-n)) \iff \\ &\iff 2(m-n) = \mu\cdot(\pi-1) \text{ für ein } \mu \in \mathbb{Z}[i].\end{aligned}$$

Die Zahl μ kann zunächst im Quotientenring berechnet werden:

$$\mu = \frac{2(m-n)}{\pi-1} = \frac{2(m-n)}{(m-1)+ni} = \frac{2(m-n)((m-1)-ni)}{(m-1)^2+n^2}.$$

Es gilt:

$$\begin{aligned}\mu \in \mathbb{Z}[i] &\iff (m-1)^2+n^2 \mid 2(m-n)(m-1) \text{ und } (m-1)^2+n^2 \mid 2(m-n)n \iff \\ &\iff (m-1)^2+n^2 \mid 2(m-n)\cdot \mathrm{ggT}(m-1,n).\end{aligned}$$

Der Rest folgt aus der Liste des vorangegangenen Lemmas.

(3) Es gilt:

$$\begin{aligned}(p+1+2n)\cdot P = O \text{ für alle } P \in E(\mathbb{F}_p) &\iff 2(m+n)\cdot P = O \text{ für alle } P \in E(\mathbb{F}_p) \iff \\ &\iff E(\mathbb{F}_p) \subseteq E[2(m+n)] \iff \\ &\iff \mathrm{Kern}(\pi-1) \subseteq \mathrm{Kern}(2(m+n)) \iff \\ &\iff 2(m+n) = \mu\cdot(\pi-1) \text{ für ein } \mu \in \mathbb{Z}[i].\end{aligned}$$

Die Zahl μ kann zunächst im Quotientenring berechnet werden:

$$\mu = \frac{2(m+n)}{\pi-1} = \frac{2(m+n)}{(m-1)+ni} = \frac{2(m+n)((m-1)-ni)}{(m-1)^2+n^2}.$$

Es gilt:

$$\begin{aligned}\mu \in \mathbb{Z}[i] &\iff (m-1)^2+n^2 \mid 2(m+n)(m-1) \text{ und } (m-1)^2+n^2 \mid 2(m+n)n \iff \\ &\iff (m-1)^2+n^2 \mid 2(m+n)\cdot \mathrm{ggT}(m-1,n).\end{aligned}$$

Der Rest folgt aus der Liste des vorangegangenen Lemmas. ■

FOLGERUNG. *Ist $p > 233$ eine Primzahl mit $p \equiv 1 \bmod 4$ und E eine durch $y^2 = x^3 + ax$ über $\mathbb{F}_p$ definierte elliptische Kurve, so gibt es $m, n \in \mathbb{N}$ mit $p = m^2 + n^2$. Dann gilt:*

$$\{M \in \{p+1-2m, p+1+2m, p+1-2n, p+1+2n\} : M\cdot P = O \text{ für alle } P \in E(\mathbb{F}_p)\} = \{\#E(\mathbb{F}_p)\}.$$

Die Folgerung zeigt, dass der zuvor angegebene Algorithmus zur Bestimmung von $\#E(\mathbb{F}_p)$ die while-Schleife nicht unendlich oft durchläuft.