Kryptographie

Studienbrief 7

universität wien

Elliptische Kurven

Gerald und Susanne Teschl

Druckfehler/Feedback bitte an:
gerald.teschl@univie.ac.at

SS 23

Version:
2023-06-30

Studienbrief 7

Elliptische Kurven

Inhalt

Unter [NSA09] wurde im Jänner 2009 von der NSA empfohlen, auf Elliptic Curve Cryptography (ECC) umzusteigen. Seit 2015 ist diese Seite nicht mehr online. Im August 2015 veröffentlichte die NSA die Empfehlung, nicht mehr unbedingt auf ECC umzusteigen sondern sich auf die Post-Quantencomputer-Zeit vorzubereiten [NSA15]. Für eine Diskussion dazu siehe [KM15] oder [She17].

Elliptische Kurven in der Kryptographie zu verwenden wurde 1985 unabhängig voneinander von Neal Koblitz [Kob87] und Victor Miller [Mil86] vorgeschlagen.

7.1 Elliptische Kurven über $\mathbb{R}$

Was ist eine elliptische Kurve? Wir kennen bereits andere Kurven. Die Kreisgleichung

$$x^2 + y^2 = r^2$$

beschreibt alle Punkte, deren Koordinaten $(x, y) \in \mathbb{R}^2$ auf einem Kreis mit Radius r liegen. Die Gleichung

$$b^2x^2 + a^2y^2 = a^2b^2$$

beschreibt eine Ellipse mit Hauptachse a und Nebenachse b.

Eine **elliptische Kurve** in Weierstraß-Normalform besteht aus allen Punkten, deren Koordinaten $(x, y) \in \mathbb{R}^2$ die Gleichung

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

erfüllen.

Die allgemeinste Form einer elliptischen Kurve ist $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Durch die lineare Transformation $x \to x - \frac{a_2}{3} + \frac{a_1^2}{12}$ und $y \to y - \frac{a_1}{2}x - \frac{a_3}{2} + \frac{a_1^3+4a_1a2}{24}$ erhält man obige Normalform mit $a = -\frac{a_1^4}{48} - \frac{a_1^2a_2}{6} + \frac{a_1a_3}{2} - \frac{a_2^2}{3} + a_4$ und $b = \frac{a_1^6}{864} + \frac{a_1^4a_2}{72} - \frac{a_1^3a_3}{24} + \frac{a_1^2a_2^2}{18} - \frac{a_1^2a_4}{12} - \frac{a_1a_2a_3}{6} + \frac{2a_2^3}{27} - \frac{a_2a_4}{3} + \frac{a_3^2}{4} + a_6$.

Falls Sie in der Kurve keine Ellipse erkennen können: Der Name kommt daher, dass diese Kurven zuerst im Zusammenhang mit elliptischen Integralen untersucht wurden. Das sind jene Integrale, die bei der Berechnung der Bogenlänge einer Ellipse auftreten.

Beispiel 7.1 Gegeben ist die elliptische Kurve $y^2 = x^3 - 3x + 5$. Stellen Sie eine Wertetabelle auf, indem Sie einige x-Werte vorgeben und die zugehörigen y-Werte ermitteln. Finden Sie weiters heraus, ob es einen Punkt gibt, für den die y-Koordinate gleich 0 ist. Zeichnen Sie die berechneten Punkte in einem Koordinatensystem ein und zeichnen Sie danach die gesamte Kurve mit einem Computeralgebrasystem.

Lösung zu 7.1 Wir machen eine Wertetabelle mit einigen Punkten:
$x = 0$: $y^2 = 0^3 - 3 \cdot 0 + 5 = 5$, daher $y_{1,2} = \pm\sqrt{5} = \pm 2.2$.
$x = 1$: $y^2 = 1^3 - 3 \cdot 1 + 5 = 3$, daher $y_{1,2} = \pm\sqrt{3} = \pm 1.7$.
$x = 2$: $y^2 = 2^3 - 3 \cdot 2 + 5 = 7$, daher $y_{1,2} = \pm\sqrt{7} = \pm 2.6$.
$x = 3$: $y^2 = 3^3 - 3 \cdot 3 + 5 = 23$, daher $y_{1,2} = \pm\sqrt{23} = \pm 4.8$.
$x = -1$: $y^2 = (-1)^3 - 3 \cdot (-1) + 5 = 7$, daher $y_{1,2} = \pm\sqrt{7} = \pm 2.6$.
$x = -2$: $y^2 = (-2)^3 - 3 \cdot (-2) + 5 = 3$, daher $y_{1,2} = \pm\sqrt{3} = \pm 1.7$.
$x = -3$: $y^2 = (-3)^3 - 3 \cdot (-3) + 5 = -13$, daher gibt es keinen Punkt mit x-Koordinate -3.
Für welches x ist $y = 0$? Dazu ist die kubische Gleichung $0 = x^3 - 3x + 5$ zu lösen (wir tun dies einfach mithilfe eines Computeralgebrasystems). Es ergibt sich: $x = -2.3$.
Wir sehen: Da die y-Werte immer in Paaren mit entgegengesetztem Vorzeichen auftreten, ist die elliptische Kurve spiegelsymmetrisch zur x-Achse. Für zu kleine negative x-Werte gibt es keinen Punkt der elliptischen Kurve. In Abbildung 7.1 ist die Kurve im ersten Bild dargestellt. ■

Abbildung 7.1 zeigt weitere typische Graphen von elliptischen Kurven. Eine elliptische Kurve ist immer spiegelsymmetrisch zur x-Achse. Wenn also $P = (x, y)$ ein Punkt der elliptischen Kurve ist, so ist auch $P^* = (x, -y)$ ein Punkt der elliptischen Kurve. Weiters sehen wir, dass eine elliptische Kurve entweder aus einer

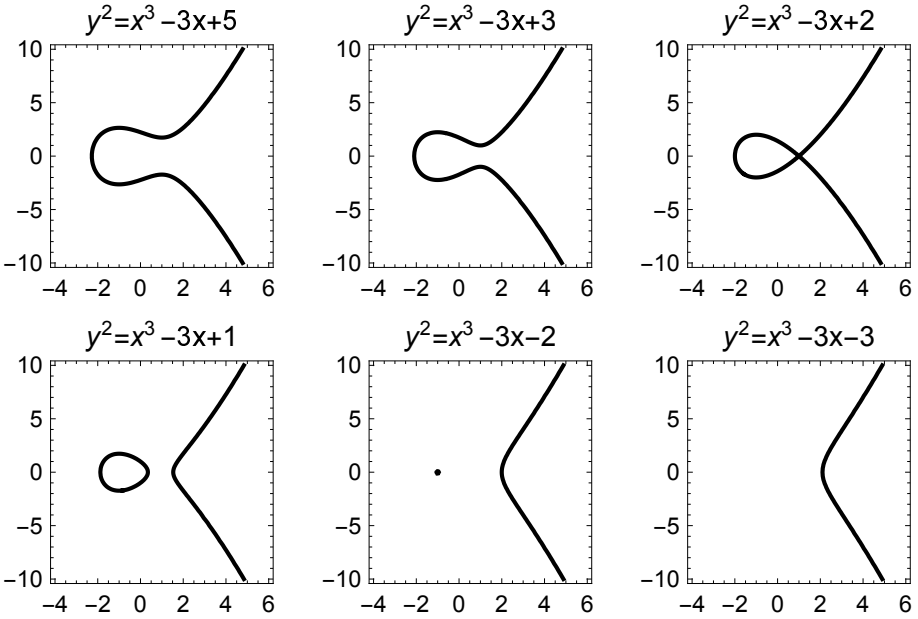

Abbildung 7.1: Verschiedene elliptische Kurven

oder aus zwei Teilkurven besteht. Dies hängt davon ab, ob das kubische Polynom $p(x) = x^3 + ax + b$ eine oder drei reelle Nullstellen besitzt.

Das kann man sich so überlegen: Grundsätzlich gibt es nur Punkte der elliptischen Kurve für $p(x) \geq 0$ (denn jeder Kurvenpunkt erfüllt $y^2 = p(x)$.) Weiters wissen wir, dass ein kubisches Polynom der Form $p(x) = x^3 + ax + b$ „von links unten“ (von $-\infty$) „nach rechts oben“ ($+\infty$) verläuft, entweder mit einer oder mit drei reellen Nullstellen dazwischen. Gibt es nur eine reelle Nullstelle x_1, so gilt $p(x) > 0$ für $x > x_1$ (und $p(x) < 0$ für $x < x_1$). Die Kurve besteht dann aus den zwei spiegelsymmetrischen Ästen $y = \pm\sqrt{p(x)}$ für $x \geq x_1$. Gibt es drei reelle Nullstellen $x_1 \leq x_2 \leq x_3$, so gilt $p(x) > 0$ für $x_1 < x < x_2$ und $x_3 < x$ und die Kurve besteht daher aus zwei Teilen. Fallen zwei Nullstellen zusammen, so gibt es im Fall $x_2 = x_3$ eine Selbstüberschneidung bei $x_2 = x_3$ (drittes Bild mit $x_2 = x_3 = 1$ und $x_1 = -2$) und im Fall $x_1 = x_2$ hier einen isolierten Punkt (fünftes Bild mit $x_1 = x_2 = -1$ und $x_3 = 2$). Fallen alle drei Nullstellen zusammen, $x_1 = x_2 = x_3 = 0$, so ist die Kurve $y^2 = x^3$ und hat bei $x = 0$ einen Knick.

Eine reelle Nullstelle ist übrigens immer durch die Formel von Cardano

$$x = \sqrt[3]{-\frac{b}{2} + c} + \sqrt[3]{-\frac{b}{2} - c}, \qquad c = \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}$$

gegeben.

Fallen Nullstellen zusammen, so ist es nicht möglich, an diesen zusammenfallenden Nullstellen eine (eindeutige) Tangente an die Kurve zu legen (Bild 3 und 5 in Abbildung 7.1). Das wird sie für uns unbrauchbar machen und wir werden diese Fälle daher ausschließen, indem wir ab nun fordern, dass die Parameter a und b die Bedingung $4a^3 + 27b^2 \neq 0$ erfüllen.

Wie kommt man auf diese Bedingung? Ist x_0 eine (mindestens) doppelte Nullstelle von $p(x) = x^3 + ax + b$, so gilt nicht nur $p(x_0) = x_0^3 + ax_0 + b = 0$, sondern auch $p'(x_0) = 3x_0^2 + a = 0$. Aus

der zweiten Gleichung folgt $x_0 = \pm(-\frac{a}{3})^{1/2}$ und Einsetzen in die erste ergibt $\mp 2(-\frac{a}{3})^{3/2} + b = 0$ oder, indem man beide Bedingungen multipliziert, $4a^3 + 27b^2 = 0$.

Unser Ziel ist nun, aus den Punkten der elliptischen Kurve eine kommutative Gruppe zu erhalten. Dazu brauchen wir eine Gruppenverknüpfung. Wir müssen also zwei Punkten P und Q einer elliptischen Kurve einen weiteren Punkt R der elliptischen Kurve zuordnen, so, dass alle notwendigen Gruppeneigenschaften (kommutativ, assoziativ, neutrales Element, inverse Elemente) erfüllt sind.

Nun gibt es zwei geometrische Möglichkeiten um aus gegeben Punkten auf der Kurve neue Punkte auf der Kurve zu erhalten. Die einfachste Möglichkeit, den Punkt $P = (x, y)$ an der x-Achse zu spiegeln, $P^* = (x, -y)$, kennen wir bereits. Hat man zwei Punkte P und Q, so kann man durch diese eine Gerade legen und erhält (im Allgemeinen) einen dritten Schnittpunkt R mit der Kurve. Allerdings gibt es zwei Grenzfälle in denen es keine drei Schnittpunkte gibt. Der erste Fall tritt ein, wenn wir den Grenzfall $Q \to P$ betrachten, dann wird die Gerade von einer Sekante zur Tangente und es liegt nahe den Schnittpunkt $P = Q$ in diesem Fall doppelt zu zählen. Der zweite Fall tritt ein, wenn wir den Grenzfall $Q \to P^*$ betrachten, dann verschwindet der dritte Schnittpunkt R im Unendlichen. Es liegt also nahe, einen „**Punkt im Unendlichen**“, nennen wir ihn $\mathcal{O}$, zu ergänzen, damit wir in jedem Fall drei Schnittpunkte haben. Diese drei Fälle sind in Abbildung 7.2

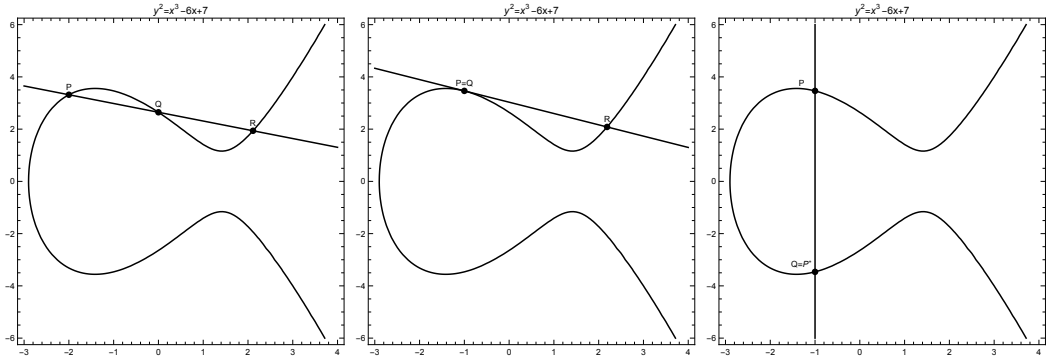

Abbildung 7.2: Addition auf einer elliptischen Kurve für den Fall $P \neq Q, P^*$ (links), $P = Q$ (mitte) und $P = P^*$ (rechts). Im letzten Fall passt der dritte Schnittpunkt $R = \mathcal{O}$ nicht aufs Bild. Die Addition ist durch $P + Q + R = \mathcal{O}$ definiert.

veranschaulicht.

Kommen wir nun zur Gruppenverküpfung, die wir mit „+“ bezeichnen werden. Eine erste naive Idee wäre es, $P + Q = R$ zu definieren. Da die drei Schnittpunkte aber untereinander austauschbar sind, führt das unmittelbar auf Widersprüche.

Es gilt dann ja auch $P + R = Q$ und daraus folgt $Q = P + R = 2P + Q$ also $2P = 0$. Für $P = Q$ folgt dann aber $0 = 2P = R$ und verschiedene P würden verschiedene neutrale Elemente liefern, was in einer Gruppe nicht möglich ist.

Der Ausweg ist es, die Gruppenverküpfung so zu definieren, dass

$$P + Q + R = \mathcal{O}$$

gilt, wobei wir $\mathcal{O}$ die Rolle des neutralen Elements zugeordnet haben. Dann folgt im Fall $Q = P^*$ (und somit $R = \mathcal{O}$)

$$P + P^* = \mathcal{O},$$

dass $P^* = -P$ das inverse Element ist.

Die Gruppenverknüpfung lautet also $P+Q = R^*$ mit R dem dritte Schnittpunkt der Geraden durch P und Q mit der Kurve (wobei, wie zuvor beschrieben, im Fall $P = Q$ die Gerade durch P und Q als Tangente an P zu verstehen ist und im Fall $P = P^*$ der dritte Schnittpunkt gleich $\mathcal{O}$ ist).

Bis auf das Assoziativgesetzt ist klar, dass damit die Menge der Punkte auf unserer elliptischen Kurve erweitert um $\mathcal{O}$ zu einer kommutativen Gruppe wird.

Definition 7.2 Es seien $a, b \in \mathbb{R}$ mit $4a^3 + 27b^2 \neq 0$. Eine elliptische Kurve $\mathcal{E}$ über $\mathbb{R}$ ist die Menge der Punkte $(x, y) \in \mathbb{R}^2$, die

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

erfüllen, gemeinsam mit einem Punkt $\mathcal{O}$, genannt **Punkt im Unendlichen**.

Die Addition kann durch Berechnen der Schnittpunkte leicht explizit angegeben werden:

Definition 7.3 (Punktaddition) Seien $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ Punkte der elliptischen Kurve $y^2 = x^3 + ax + b$ mit $Q \neq P^*$. Dann ist $P + Q = (x_3, y_3)$ mit

$$\begin{aligned} x_3 &= s^2 - x_1 - x_2, \\ y_3 &= s(x_1 - x_3) - y_1, \end{aligned}$$

und

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & P \neq Q, \\ \frac{3x_1^2 + a}{2y_1}, & P = Q. \end{cases}$$

Die Gleichung der Sekante durch P und Q ist $y = y_1 + s(x - x_1)$ mit $s = \frac{y_2 - y_1}{x_2 - x_1}$. Setzen wir dies in die elliptische Kurvengleichung ein, so erhalten wir ein kubisches Polynom $x^3 - s^2x^2 + \alpha x + \beta$ (es gilt $\alpha = a + 2s^2x_1 - 2sy_1$ und $\beta = b - s^2x_1^2 + 2sx_1y_1 - y_1^2$, aber das werden wir nicht mehr brauchen). Da wir die Nullstellen dieses Polynoms kennen, können wir es alternativ in der Form $(x-x_1)(x-x_2)(x-x_3) = x^3-(x_1+x_2+x_3)x^2+(x_1x_2+x_1x_3+x_2x_3)x-x_1x_2x_3$ schreiben. Durch

Koeffizientenvergleich erhalten wir $x_3 = s^2 - x_1 - x_2$ und Einsetzen in die Sekantengleichung liefert $y_3 = y_1 + s(x_3 - x_1)$.

Im Fall $P = Q$ erhalten wir für die Steigung der Tangente $s = \frac{p'(x_1)}{2y_1} = \frac{3x_1^2+a}{2y_1}$ und der Rest folgt wie zuvor.

Mit dieser Addition wird $\mathcal{E}$ zu einer kommutativen Gruppe:

Satz 7.4 Eine elliptische Kurve $\mathcal{E}$: $y^2 = x^3 + ax + b$ über $\mathbb{R}$ mit $4a^3 + 27b^2 \neq 0$ bildet mit der Punktaddition eine kommutative Gruppe mit neutralem Element $\mathcal{O}$ und inversem Element $-P = P^*$.

Das einzige was noch zu überprüfen ist, ist das Assoziativgesetzt. Gibt es eine (eindeutige) Tangente an die Kurve (hier verwenden wir die Bedingung $4a^3 + 27b^2 \neq 0$), so geht die Sekantensteigung im Grenzwert in die Tangentensteigung über und die Formeln für die Addition sind in diesem Sinn stetig. Deshalb reicht es den generischen Fall, wenn alle drei Punkte verschieden sind, zu überprüfen. Das ist eine zwar mühsame, aber im Prinzip elementare Rechnung. Am besten überlässt man sie einem Computeralgebrasystem.

Im Fall $4a^3 + 27b^2 = 0$ gibt es am Punkt $P = (\text{sign}(b)\sqrt{-a/3}, 0) = P^*$ der Selbstüberscheidung ein Problem: Dort gilt für jeden Punkt $Q \neq P$ die Gleichung $Q + P = P$, was in einer Gruppe unmöglich ist. In diesem Fall kann also das Assoziativgesetz nicht gelten. In der Tat haben wir $(Q + P) + P = P + P = \mathcal{O}$ und $Q + (P + P) = Q + \mathcal{O} = Q$.

Abkürzend schreibt man für $n \in \mathbb{N}$:

$$\underbrace{P + \cdots + P}_{n \text{ mal}} = n \cdot P \text{ oder } nP$$

(sprich: „n mal P“) beziehungsweise $0 \cdot P = \mathcal{O}$ und $(-n) \cdot P = n \cdot (-P)$. In der Praxis berechnet man diese Operation wieder mit „Square-and-Multiply“, wobei hier die Bezeichnung „Double-and-Add“ treffender ist.

Unsere Darstellung der Punkte als (x, y) wird auch als **affine Koordinaten** bezeichnet. Daneben gibt es noch die Möglichkeit der **projektiven Koordinaten** $[x : y : z]$, wobei die Punkte nun als Äquivalenzklassen zu verstehen sind, d.h., jede Skalierung aller drei Koordinaten mit dem gleichen Faktor $t \neq 0$ beschreibt den gleichen Punkt: $[tx : ty : tz] = [x : y : z]$. Die Umwandlung erfolgt also mittels $(x, y) \mapsto [x : y : 1]$ und $[x : y : z] \mapsto (x/z, y/z)$ solange $z \neq 0$. Der Fall $z = 0$ ist besonders, denn $[0 : 1 : 0]$ entspricht $\mathcal{O}$. Es gibt auch noch modifizierte projektive Koordinate, wobei die Umwandlung nun $\langle x : y : z \rangle \mapsto (x/z^2, y/z^3)$ lautet. Der Vorteil der letzteren ist, dass sich die Addition in diesen Koordinaten gut ohne Division beschreiben läßt, was bei der Implementation am Computer Geschwindigkeitsvorteile bringen kann.

7.2 Wurzelziehen in $\mathbb{Z}_p$

Um den letzten Abschnitt von $\mathbb{R}$ auf $\mathbb{Z}_p$ zu übertragen, müssen wir uns noch Gedanken darüber machen, wie man in $\mathbb{Z}_p$ Wurzeln berechnen kann.

Das führt uns auf die Frage der quadratischen Reste, also welche Zahlen in $\mathbb{Z}_p$ sich als Quadrate schreiben lassen. Indem wir in $\mathbb{Z}$ die ersten Quadratzahlen

1, 4, 9, 16, 25, 36, 49, 64, 81, 100 berechnen, so sehen wir, dass als letzte Ziffer einer Quadratzahl nur die Werte 0, 1, 4, 5, 6 und 9 in Frage kommen. Mit anderen Worten, das sind die einzigen quadratischen Reste in $\mathbb{Z}_{10}$. Im Prinzip kann man auf diese Weise natürlich immer die quadratischen Reste (und die zugehörigen Wurzeln) durch Probieren aller Möglichkeiten bestimmen. Für große Zahlen ist das aber unpraktikabel und wir fragen uns daher, wie man es besser machen kann.

Es sei also p eine Primzahl. Wir benutzen, dass $\mathbb{Z}_p^*$ zyklisch ist und damit einen Generator g besitzt. Jedes Element $a \in \mathbb{Z}_p^*$ können wir damit als

$$a = g^j, \qquad 1 \leq j \leq p-1$$

schreiben. Insbesondere sind die Quadratzahlen genau jene mit geraden j. Es gibt also genau $\frac{p-1}{2}$ Quadratzahlen. Wie können wir sie aber erkennen? Dazu definieren wir

Definition 7.5 Das **Legendre-Symbol** von a bezüglich einer Primzahl p ist

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p.$$

Beispiel 7.6 Es gilt immer

$$\left(\frac{0}{p}\right) = 0, \qquad \left(\frac{1}{p}\right) = 1$$

und für $p = 2$ deckt das schon alle Möglichkeiten ab. Der Fall $p = 2$ ist also nicht besonders spannend. Für $p = 3$ gilt

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

und für $p = 5$

$$\left(\frac{1}{5}\right) = 1, \qquad \left(\frac{2}{5}\right) = -1, \qquad \left(\frac{3}{5}\right) = -1, \qquad \left(\frac{4}{5}\right) = 1.$$

Es fällt auf, dass für $a \in \mathbb{Z}_p^*$ nur die Werte ± 1 angenommen werden. Und zwar $+1$ genau für die Quadratzahlen.

Versuchen wir nun das Legendre-Symbol allgemein zu berechnen. Aus den Potenzregeln folgt sofort

Satz 7.7 Das Legendre-Symbol ist multiplikativ:

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

Es reicht somit das Legendre-Symbol von g zu berechnen. Wegen $(g^{(p-1)/2})^2 = g^{p-1} = 1$ muss $g^{(p-1)/2} = +1$ oder $g^{(p-1)/2} = -1$ gelten. Der Fall $g^{(p-1)/2} = +1$ ist aber nicht möglich, da sonst $\mathrm{ord}(g) = (p-1)/2$ wäre. Damit erhalten wir

$$\left(\frac{g^j}{p}\right) = (-1)^j$$

und das Legendre-Symbol sagt uns, wann wir es mit einer Quadratzahl zu tun haben:

Satz 7.8 Sei p eine Primzahl. Das Legendre-Symbol ist

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{falls } a = b^2 \pmod p \\ 0, & \text{falls } a = 0 \pmod p, \\ -1 & \text{sonst.} \end{cases}$$

Insbesondere hat die Gleichung $x^2 = a$ in $\mathbb{Z}_p$ genau $\left(\frac{a}{p}\right) + 1$ Lösungen. Ist $x \in \mathbb{Z}_p^*$ eine Lösung, so ist $-x$ die zweite Lösung.

Der klassische Zugang verwendet den letzten Satz als Definition und unsere Definition ist dann als Satz von Euler bekannt.

Man beachte auch, dass man diese Probleme in einer Gruppe mit ungerader Ordnung m (z.B. in $GF(2^k)^*$ mit $k > 1$) nicht hat, denn da ist die Wurzel eindeutig und durch $a^{(m+1)/2}$ gegeben.

Das Legendre-Symbol beantwortet also die Frage nach der Lösbarkeit, nicht aber wie wir die Lösung finden. Wir beginnen mit dem (einfachen) Fall, wenn $(p+1)/2$ gerade ist.

Satz 7.9 Es sei $p \geq 3$ eine Primzahl mit $(p+1)/2$ gerade. Ist $a \in \mathbb{Z}_p^*$ eine Quadratzahl, dann ist eine Wurzel durch

$$b = a^{(p+1)/4}$$

gegeben.

Gilt $a = b^2$, so folgt $a^{(p-1)/2} = b^{p-1} = 1$. Multiplizieren wir diese Gleichung mit a, so folgt $a^{(p+1)/2} = a$. Nach unserer Voraussetzung ist $(p+1)/2$ gerade und somit ist $b = a^{(p+1)/4}$ eine Zahl mit $b^2 = a^{(p+1)/2} = a$, wie gewünscht.

Beispiel 7.10 Berechnen Sie (wenn möglich) die Wurzeln von:
a) $a = 2$ in $\mathbb{Z}_3$ b) $a = 2$ in $\mathbb{Z}_7$

Lösung zu 7.10 a) Da $\left(\frac{2}{3}\right) = -1$ gibt es keine Wurzel von 2 in $\mathbb{Z}_3$.
b) Da $\left(\frac{2}{7}\right) = 1$ gibt es zwei Wurzeln in $\mathbb{Z}_7$. Diese sind gegeben durch $b = 2^2 = 4$ und $-b = -4 = 3$. ■

Der Fall wenn $(p+1)/2$ ungerade ist, ist um einiges schwieriger und benötigt Körpererweiterungen.

In diesem Fall kann es keine so einfache Formel geben. Denn in diesem Fall ist $(p-1)/2$ gerade und damit ist -1 eine Quadratzahl. Aber wir können die Wurzel offensichtlich nicht als Potenz $(-1)^j$ darstellen, da uns diese Potenzen nur die Werte $+1$ und -1 liefern.

Satz 7.11 Es sei $p \geq 3$ eine Primzahl mit $(p+1)/2$ ungerade. Ist $a \in \mathbb{Z}_p^*$ eine Quadratzahl, dann ist eine Wurzel durch

$$b = (c + \sqrt{c^2 - a})^{(p+1)/2}$$

gegeben ist, wobei $c \in \mathbb{Z}_p^*$ so gewählt wurde, dass $c^2 - a$ keine Quadratzahl ist (diese Bedingung ist für mindestens $\frac{p-1}{2}$ Elemente erfüllt).

Bemerkung: Die Rechenoperationen sind in $\mathbb{Z}_p(\sqrt{c^2-a})$ auszuführen, das Ergebnis ist aber in $\mathbb{Z}_p$. Die benötigte Zahl c wird zufällig gewählt, solange bis die Bedingung erfüllt ist (da die Wahrscheinlichkeit dafür $\geq \frac{1}{2}$ ist, wird das in der Regel nur wenige Versuche benötigen).

Wir betrachten die Körpererweiterung $\mathbb{Z}_p(\sqrt{c^2-a})$. Die Abbildung $F(x) = x^p$ ist als Frobenius Automorphismus bekannt. Es gilt also $F(x \cdot y) = F(x)F(y)$ und $F(x+y) = F(x) + F(y)$. Die erste Formel folgt aus den Potenzgesetzten und die zweite aus

$$F(x+y) = (x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j} = x^p + y^p = F(x) + F(y)$$

da $\binom{p}{j} = 0 \pmod p$ für $1 < j < p$. Aus dem kleinen Satz von Fermat folgt $F(a) = a$ für $a \in \mathbb{Z}_p$ und da die Gleichung $x^p = x$ im Körper $\mathbb{Z}_p(\sqrt{c^2-a})$ maximal p Nullstellen haben kann, haben wir alle Werte in $\mathbb{Z}_p(\sqrt{c^2-a})$ mit dieser Eigenschaft gefunden. Wegen $F(\sqrt{c^2-a})^2 = F(c^2-a) = c^2 - a$ gilt $F(\sqrt{c^2-a}) = \pm\sqrt{c^2-a}$ und da $F(x) = +x$ nur für Werte aus $\mathbb{Z}_p$ auftreten kann, gilt $F(\sqrt{c^2-a}) = -\sqrt{c^2-a}$. Insgesamt folgt

$$(d + e\sqrt{c^2-a})^p = d - e\sqrt{c^2-a}.$$

Daraus folgt

$$(c+\sqrt{c^2-a})^{p+1} = (c-\sqrt{c^2-a})(c+\sqrt{c^2-a}) = a$$

und damit die Behauptung. Auf den ersten Blick ist nur $b = d + e\sqrt{c^2-a} \in \mathbb{Z}_p(\sqrt{c^2-a})$ klar. Wegen

$$b^2 = d^2 + e^2(c^2-a) + 2de\sqrt{c^2-a} = a$$

folgt aber $d^2 + e^2(c^2-a) = a$ und $2de = 0$. Wäre $d = 0$ so ist $b = e\sqrt{c^2-a}$ und $b^2 = e^2(c^2-a)$ im Widerspruch dazu, dass $c^2 - a$ keine Quadratzahl ist. Also ist $e = 0$ und somit $b \in \mathbb{Z}_p$.

Beispiel 7.12 Berechnen Sie (wenn möglich) die Wurzeln von:
a) $a = 2$ in $\mathbb{Z}_5$ b) $a = 3$ in $\mathbb{Z}_{13}$

Lösung zu 7.12 a) Da $\left(\frac{2}{5}\right) = -1$ gibt es keine Wurzel von 2 in $\mathbb{Z}_5$.
b) Da $\left(\frac{3}{13}\right) = 1$ gibt es zwei Wurzeln in $\mathbb{Z}_{13}$. Wir benötigen also ein $c \in \mathbb{Z}_{13}^*$ mit $\left(\frac{c^2-a}{13}\right) = -1$. Wir versuchen der Reihe nach $c = 1, 2, \ldots$ und werden gleich bei $c = 1$ (und $c^2 - a = 11$) fündig: $\left(\frac{11}{13}\right) = -1$. Somit ist

$$b = (1+\sqrt{11})^7 = 13784 + 4264\sqrt{11} = 4 \pmod{13}$$

und die zweite Wurzel ist $-b = -4 = 9$. ■

Wir erwähnen noch, dass das Legendre-Symbol besonders effizient mit dem **Quadratischen Reziprozitätzgesetz** von Gauß

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

für zwei verschiedene ungerade Primzahlen und den beiden Ergänzungssätzen

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

berechnet werden kann. Ist $n = p_1 \cdots p_k$ eine ungerade Zahl und sind p_j (nicht notwendigerweise verschiedene) Primzahlen, so kann man das Legendre-Symbol zum **Jacobi-Symbol**

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right)$$

erweitern. Die Multiplizität erbt das Jacobi-Symbol vom Legendre-Symbol und man kann zeigen, dass auch das Reziprozitätzgesetz sowie die beiden Ergänzungssätze dabei gültig bleiben. Allerdings gilt nicht mehr, dass $\left(\frac{a}{n}\right)$ genau dann 1 ist, wenn a ein quadratischer Rest in $\mathbb{Z}_n$ ist. Wir wollen hier aber nicht weiter darauf eingehen.

Wollen wir in $\mathbb{Z}_n$ Wurzeln ziehen, so können wir das mithilfe des Chinesischen Restsatz auf den Fall eines Körpers zurückführen. Betrachten wir einfachheisthalber den Fall bei dem $n = p_1p_2$ das Produkt zweier Primzahlen ist. Dann kann die

Wurzel aus $a \in \mathbb{Z}_n$ wie folgt gezogen werden: Ist a ein quadratischer Rest, also $a = b^2$ in $\mathbb{Z}_n$, so gilt auch $a = b_j^2 \pmod{p_j}$ mit $b_j = b \bmod p_j$. Also ist a auch ein quadratischer Rest bezüglich p_1 und p_2. Ist umgekehrt $a = b_j^2 \pmod{p_j}$ ein quadratischer Rest bezüglich p_1 und p_2, so können wir mithilfe des Chinesischen Restsatz ein $b \in \mathbb{Z}_n$ bestimmen mit $b_j = b \bmod p_j$. Dann gilt auch $b_j^2 = b^2 \bmod p_j$ und damit ist $b^2 = a \pmod{n}$. Da wir, im Allgemeinen je zwei Möglichkeiten für b_j haben, gibt es im Allgemeinen vier Möglichkeiten für b.

Beispiel 7.13 Bestimmen Sie die Quadratwurzel von $a = 3$ in $\mathbb{Z}_{91}$.

Lösung zu 7.13 Die Quadratwurzeln von $16 \bmod 7 = 2$ in $\mathbb{Z}_7$ sind $b_{11} = 4$ und $b_{12} = 3$ (Beispiel 7.10 b). Die Quadratwurzeln von $16 \bmod 13 = 3$ in $\mathbb{Z}_{13}$ sind $b_{21} = 4$ und $b_{22} = 9$ (Beispiel 7.12 b). Mit $(b_{11}, b_{21}) = (4, 4)$ liefert der Chinesischen Restsatz $b = 4$. Die anderen Kombinationen ergeben $b = 74, 17, 87$. ■

Ist $n = pq$ das Produkt zweier Primzahlen und kennt man eine Lösung von $a = b^2 \pmod{n}$, so sind die anderen durch a, σa, $-\sigma a$, $-a$ gegeben, wobei 1, σ, $-\sigma$, -1 die vier Quadratwurzeln von 1 sind. Es gilt also, dass σ die Lösung von $1 = \sigma \bmod p$, $-1 = \sigma \bmod q$ ist und das Auffinden von σ ist genauso schwer wie das Faktorisieren von n (denn es gilt ja $p = \mathrm{ggT}(\sigma - 1, n)$ und $q = \mathrm{ggT}(\sigma + 1, n)$). Können wir also zwei verschiedene Quadratwurzeln b, $\tilde{b}$ mit $b \neq -\tilde{b}$ finden, so können wir n faktorisieren. Auf dieser Tatsache beruht die Idee des **Rabin-Kryptosystem**

$$y = x^2 \pmod{n}.$$

Das ist RSA mit $e = 2$, da aber e nicht teilerfremd zu $\varphi(n)$ ist, gibt es keinen geheimen Schlüssel d, der die Verschlüsselung umkehrt.

Der Nachteil ist, dass Alice beim Entschlüsseln der Nachricht von Bob (im Allgemeinen) vier mögliche Klartexte erhält. Alice und Bob müssen sich also auf ein Nachrichtenformat einigen, anhand von dem Alice erkennen kann, welche der vier Möglichkeiten die richtige ist. Z.B. könnte man die Nachrichten Bits (oder einen Teil davon) verdoppeln. Dann ist es extrem unwahrscheinlich, dass mehr als eine der möglichen vier Nachrichten diese Bedingung erfüllt. Mit zu viel Struktur im Klartext hat man aber bei RSA schon schlechte Erfahrungen gemacht.

Eine andere Möglichkeit ist es, für n eine **Blum-Zahl** (nach dem amerikanischen Informatiker Manuel Blum (*1936)) zu wählen, also ein Produkt aus zwei Primzahlen die beide die Bedingung aus Satz 7.9 erfüllen. Ist x eine Quadratzahl bezüglich n, dann kann man leicht mit $y^{((p-1)(q-1)+4)/8} = x$ entschlüsseln und x ist die einzige Wurzel von $y = x^2$ mit dieser Eigenschaft (Aufgabe 6). Man könnte also die Nachricht mit Zufallsbits auffüllen bis eine Quadratzahl entsteht.

7.3 Elliptische Kurven über $\mathbb{Z}_p$

Die Überlegungen aus Abschnitt 7.1 lassen sich ohne Probleme auf endliche Körper $\mathbb{K}$ übertragen. Wir werden hier nur den Fall $\mathbb{K} = \mathbb{Z}_p$ (p Primzahl) betrachten, man kann im Prinzip aber beliebige endliche Körper $\mathbb{K} = GF(p^k)$ betrachten.

Definition 7.14 Sei $p > 2$ eine Primzahl und $a, b \in \mathbb{Z}_p$ mit $4a^3 + 27b^2 \neq 0 \pmod p$. Eine elliptische Kurve $\mathcal{E}$ über $\mathbb{Z}_p$ ist die Menge der Punkte (x, y) mit $x, y \in \mathbb{Z}_p$, die

$$y^2 = x^3 + ax + b \,(\mathrm{mod}\, p)$$

erfüllen, gemeinsam mit einem Punkt $\mathcal{O}$, genannt **Punkt im Unendlichen**.

Im Fall $p = 2, 3$ kann man sich nicht ohne Beschränkungen der Allgemeinheit auf Kurven in der obigen Normalform $y^2 = x^3 + ax + b \,(\mathrm{mod}\, p)$ einschränken (da wir bei der Transformation auf Normalform das multiplikative Inverse von 2 und 3 benötigen), sondern es gibt noch weitere Möglichkeiten. Da wir uns hier für sehr große Werte von p interessieren, gehen wir nicht näher darauf ein.

Definition 7.15 (Punktaddition) Seien $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ Punkte einer elliptischen Kurve $\mathcal{E} : y^2 = x^3 + ax + b \,(\mathrm{mod}\, p)$ mit $Q \neq P^*$. Dann definiert man die Summe $R = P + Q = (x_3, y_3)$ mit

$$\begin{aligned} x_3 &= s^2 - x_1 - x_2 \,(\mathrm{mod}\, p), \\ y_3 &= s(x_1 - x_3) - y_1 \,(\mathrm{mod}\, p), \end{aligned}$$

wobei

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \,(\mathrm{mod}\, p), & P \neq Q, \\ \frac{3x_1^2 + a}{2y_1} \,(\mathrm{mod}\, p), & P = Q. \end{cases}$$

Außerdem definiert man $P + \mathcal{O} = \mathcal{O} + P = P$ und $P + P^* = \mathcal{O}$. Wenn aus der Angabe klar ist, dass über dem Körper $\mathbb{Z}_p$ gerechnet wird, so wird oft der Zusatz „mod p“ bei den Gleichungen gar nicht angeschrieben.

Man beachte, dass die Formel für s im Fall $P = Q$ nur für $p \neq 2$ wohldefiniert ist.

Wie zuvor definieren wir für $n \in \mathbb{Z}_p$ das **Vielfache** als

$$n \cdot P = \underbrace{P + \cdots + P}_{n \text{ mal}}.$$

Satz 7.16 $(\mathcal{E}, +)$ bildet gemeinsam mit der oben definierten Punktaddition eine kommutative Gruppe. Das neutrale Element der Gruppe ist $\mathcal{O}$, der zu $P = (x, y)$ negative Punkt ist $-P = (x, -y)$.

Beispiel 7.17 Gegeben ist die elliptischen Kurve $\mathcal{E} : y^2 = x^3 - 3x + 1$ über $\mathbb{Z}_{11}$.
a) Überprüfen Sie, ob die Bedingung $4a^3 + 27b^2 \neq 0 \,(\mathrm{mod}\, p)$ erfüllt ist.
b) Geben Sie alle Punkte von $\mathcal{E}$ an. Wie viele Punkte hat $\mathcal{E}$?
c) Skizzieren Sie die elliptische Kurve als Punktwolke.

Lösung zu 7.17 a) Es gilt $4a^3 + 27b^2 = 7 \neq 0 \pmod p$.
b) Wir berechnen zu allen möglichen x-Koordinaten (alle Werte aus $\mathbb{Z}_{11}$) die zugehörigen y-Koordinaten der Punkte. Um die Wurzel von y zu ermitteln berechnen wir vorab alle Möglichkeiten für y^2 in einer Hilfstabelle:

y	0	1	2	3	4	5	6	7	8	9	10
$y^2 \bmod 11$	0	1	4	9	5	3	3	5	9	4	1

Nun setzen wir nacheinander für $x = 0, 1, 2, \ldots, 10$ in die Kurvengleichung ein:
$x = 0$: $y^2 = 1$ ergibt $y_1 = 1$ und $y_2 = 10 \pmod{11}$.
$x = 1$: $y^2 = 1^3 - 3 \cdot 1 + 1 = -1 = 10 \pmod{11}$. Aus der Hilfstabelle sehen wir, dass es kein y mit $y^2 = 10$ gibt, somit keinen Punkt mit x-Koordinate 1 der elliptischen Kurve.
$x = 2$: $y^2 = 2^3 - 3 \cdot 2 + 1 = 3 \pmod{11}$. Aus der Hilfstabelle entnehmen wir $y_1 = 5$ und $y_2 = 6$.
...
Insgesamt berechnen wir folgende Punkte:

x	y_1	y_2
0	1	10
1	–	–
2	5	6
3	–	–
4	3	8
5	1	10
6	1	10
7	2	9
8	4	7
9	–	–
10	5	6

Somit hat $\mathcal{E}$, wenn wir noch den Punkt $\mathcal{O}$ hinzunehmen, insgesamt 17 Punkte.
c) Siehe Abbildung 7.3. Wir sehen, dass die elliptische Kurve eine Punktwolke ist, die symmetrisch ist bezüglich einer gedachten Linie $\frac{p}{2} = \frac{11}{2} = 5.5$. Das kommt daher, dass es zu jedem Punkt $P = (x, y)$ auf $\mathcal{E}$ auch den Punkt $-P = (x, -y)$ auf $\mathcal{E}$ gibt. ■

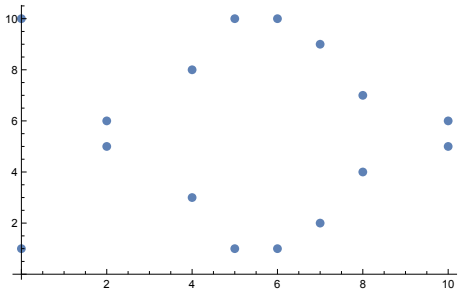

Abbildung 7.3: Die elliptische Kurve $\mathcal{E} : y^2 = x^3 - 3x + 1$ über $\mathbb{Z}_{11}$.

Beispiel 7.18 Gegeben ist wieder die elliptischen Kurve $\mathcal{E} : y^2 = x^3 - 3x + 1$ über $\mathbb{Z}_{11}$. Berechnen Sie:
a) $(2, 5) + (4, 8)$ b) $2 \cdot (2, 5)$ c) $(4, 3) + (4, 8)$

Lösung zu 7.18 Wir wenden die Formeln aus Definition 7.15 an:
a) $(10, 5)$ b) $(2, 5) + (2, 5) = (0, 10)$ c) $(4, 3) + (4, 8) = \mathcal{O}$, da $(4, 8) = -(4, 3)$ ■

Die y-Koordinate eines Punktes ist bis auf das Vorzeichen durch $y = \pm\sqrt{x^3 + ax + b}$ bestimmt. Da p ungerade ist, ist (falls $y \neq 0$) genau eine der beiden Wurzeln gerade und die andere ist ungerade. Wenn man Punkte auf der Kurve angibt, reicht also die x Koordinate und der Wert von $y \bmod 2$.

Wir haben uns in Studienbrief 5 mit zyklischen Gruppen beschäftigt, insbesondere mit der Ordnung eines Elementes und mit erzeugenden Elementen. Wir wiederholen diese Begriffe im Zusammenhang mit elliptischen Kurven:

Die Ordnung eines Punktes P einer elliptischen Kurve $\mathcal{E}$ ist die kleinste natürliche Zahl k mit $k \cdot P = \mathcal{O}$. Als Ordnung eines Punktes sind nur Teiler der Gruppenordnung $|\mathcal{E}|$ möglich (Satz von Lagrange). Eine elliptische Kurve ist zyklisch, wenn es zumindest einen Punkt mit maximaler Ordnung, also mit $\mathrm{ord}(P) = |\mathcal{E}|$, gibt. Solch ein Punkt heißt Generator oder erzeugender Punkt von $\mathcal{E}$. Wenn eine elliptische Kurve mit m Punkten zyklisch ist, so besitzt sie $\varphi(m)$ Generatoren. Insbesondere ist bei einer elliptischen Kurve mit primer Ordnung jeder Punkt bis auf $\mathcal{O}$ erzeugender Punkt. Ein Punkt mit Ordnung q erzeugt eine zyklische Untergruppe von $\mathcal{E}$ mit q Elementen.

Beispiel 7.19 Wie wir in Beispiel 7.17 gesehen haben, hat die elliptische Kurve $\mathcal{E}$: $y^2 = x^3 - 3x + 1$ über $\mathbb{Z}_{11}$ die Ordnung 17. Da 17 eine Primzahl ist, ist jeder endliche Punkt (also jeder Punkt außer $\mathcal{O}$) ein Generator.

Wir haben in Beispiel 7.17 alle Punkte der elliptischen Kurve berechnet. Auf diese Weise haben wir insbesondere die Punktanzahl $|\mathcal{E}|$ erhalten. Für kryptographische Anwendungen ist es wesentlich zu wissen, wie viele Punkte eine elliptische Kurve hat. Mithilfe des Legendre-Symbols können wir diese Anzahl wie folgt schreiben:

Satz 7.20 Die Anzahl der Elemente einer elliptischen Kurve $\mathcal{E}$ über $\mathbb{Z}_p$ ist gegeben durch

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

Da das Legendre-Symbol nur die Werte ± 1 annimmt, wird $|\mathcal{E}|$ typischerweise in der Nähe von $p+1$ liegen. In der Tat kann man die maximale Abweichung abschätzen:

Satz 7.21 (Satz von Hasse) Für die Anzahl der Punkte einer elliptischen Kurve $\mathcal{E}$ über $\mathbb{Z}_p$ gilt:

$$p + 1 - 2\sqrt{p} \leq |\mathcal{E}| \leq p + 1 + 2\sqrt{p}$$

Nach einem Resultat von M. Deuring gilt, dass es umgekehrt zu jeder Primzahl p und jeder natürlichen Zahl N, die $p + 1 - 2\sqrt{p} \leq N \leq p + 1 + 2\sqrt{p}$ erfüllt, auch zugehörige elliptische Kurven mit N Punkten gibt.

Für eine große Primzahl p kann man daher grob sagen: $|\mathcal{E}| \approx p + O(\sqrt{p})$. Benötigt man also eine elliptische Kurve mit $|\mathcal{E}| \approx 2^{256}$ Punkten, so wählt man $p \approx 2^{256}$, also p mit 256 binären Stellen.

Mit der Hasse-Schranke kann man den Baby-Step-Giant-Step-Algorithmus adaptieren um $|\mathcal{E}|$ zu berechnen (**Shanks–Mestre Algorithmus**, siehe [CP05]). Der Algorithmus ist aber von der Ordnung $O(p^{1/4})$ und damit für Anwendungen in der Kryptographie unbrauchbar. Es gibt aber eine effiziente Methode, den **Schoof–Elkies–Atkin–Algorithmus**, auf die wir hier aber nicht weiter eingehen.

Es gibt auch spezielle Fälle in denen die Ordnung einfach berechnet werden kann. Siehe [Kob93].

Um Kryptographie auf elliptischen Kurven betreiben zu können, übertragen wir den **Diffie–Hellman Schlüsselaustausch** (und alle daraus abgeleiteten Verfahren wie z.B. Elgamal und DSA) auf die Punktegruppe einer elliptischen Kurve (ECDH):

- Gegeben sei eine elliptische Kurve $\mathcal{E}$ und ein Punkt $G \in \mathcal{E}$ mit einer primen Ordnung $m = \text{ord}(G)$. Die elliptische Kurve (also a, b, p) sowie der Punkt G und seine Ordnung sind öffentlich bekannt.

- Alice wählt eine geheime Zahl $a \in \mathbb{Z}_m^*$ und Bob eine geheime Zahl $b \in \mathbb{Z}_m^*$.
- Alice schickt $A = a \cdot G \in \mathcal{E}$ an Bob. Bob schickt $B = b \cdot G \in \mathcal{E}$ an Alice.
- Alice berechnet $a \cdot B \in \mathcal{E}$, Bob berechnet $b \cdot A \in \mathcal{E}$. Wegen

$$a \cdot B = (b \cdot a) \cdot G = (a \cdot b) \cdot G = b \cdot A \in \mathcal{E}$$

  sind beide Punkte gleich und können als geheimer Schlüssel (z.B. die x-Koordinate des Punktes für AES) verwendet werden.

Wird am Ende nur die x-Koordinate verwendet, so reicht es wenn auch nur die x-Koordinaten der Punkte übertragen werden. Wählt Alice eine y-Koordinate, dann hat sie entweder B oder $-B$ und somit $(a \cdot b) \cdot G$ oder $-(a \cdot b) \cdot G$. Die x-Koordinate ist in beiden Fällen die gleiche. Analoges gilt für Bob.

Wie schon im klassischen Fall (also für die Gruppe $\mathbb{Z}_p^*$) basiert die Sicherheit des Diffie Hellman Schlüsselaustausches auf:

Definition 7.22 (Diskretes Logarithmusproblem auf ellipt. Kurven)
Gegeben ist eine elliptische Kurve $\mathcal{E}$, ein erzeugender Punkt P von $\mathcal{E}$ (oder einer möglichst großen Untergruppe von $\mathcal{E}$) und ein beliebiger Punkt T von $\mathcal{E}$ (bzw. der Untergruppe). Die Aufgabe, jenes $d \in \mathbb{N}$, $1 \leq d \leq |\mathcal{E}|$ zu finden mit

$$d \cdot P = T$$

wird als das **Problem des diskreten Logarithmus auf der elliptischen Kurve $\mathcal{E}$** bezeichnet (Elliptic Curve Discrete Logarithm Problem, ECDLP).

Falls Sie in der Definition weit und breit keinen Logarithmus erkennen können, dann erinnern Sie sich daran, dass man die Gruppenverknüpfung der elliptischen Kurve willkürlich als Addition bezeichnet hat. Hätte man sie Multplikation genannt, und demnach mit dem Symbol $\cdot$ statt $+$ geschrieben, so würde der gemeinsame geheime Punkt von Alice und Bob $T = P \cdot \ldots \cdot P = P^d$ anstelle von $T = P + \cdots + P = d \cdot P$ geschrieben werden. Und dann wäre das von Mallory gesuchte d die Hochzahl, also der Logarithmus von T zur Basis P.

Der Unterschied zum klassischen DLP in $\mathbb{Z}_p^*$ ist, dass für den Fall von elliptischen Kurven der Index Calculus zur Lösung des DLP ineffizient ist, da es in unsere Gruppe keine Primzahlen gibt. Der derzeit beste allgemeine Algorithmus zur Lösung des DLP ist damit der Pollard-Rho bzw. der Baby-Step-Giant-Step-Algorithmus (zusammen mit einer Pohlig-Hellman Reduktion). Das bedeutet, dass man mit kleinerer Schlüssellänge die gleiche Sicherheit erhalten kann (vgl. Tabelle 2.2). Aber Achtung, es gibt einige spezielle Kurven, für die effektivere Algorithmen bekannt sind [Men01].

Unter gewissen Bedingungen kann das ECDLP auf einer Kurve über $\mathbb{Z}_p$ auf ein DLP in $\mathbb{Z}_{p^k}$ zurückgeführt werden (**MOV-Algorithmus**, Weil/Tate-Paarung). Damit dieser Angriff nicht erfolgreich ist, muss sicher gestellt werden, dass $\mathrm{ord}(P) \nmid p^k - 1$ für kleine k. Kurven auf denen der Angriff funktioniert, sind **supersinguläre elliptische Kurven**, das sind Kurven mit $|\mathcal{E}| = p+1$, und Kurven mit $|\mathcal{E}| = p-1$. Ausserdem ist es auf **anormalen elliptischen Kurven** (das sind Kurven mit $|\mathcal{E}| = p$) möglich, das ECDLP effektiv zu lösen. Siehe [Men01].

Diese Kurven sind für kryptographische Anwendungen natürlich ungeeignet. Von diversen Organisationen gibt es Listen mit sicheren Kurven. Teilweise sind das Kurven mit speziellen mathematischen Eigenschaften oder auch zufällig erzeugte Kurven.

Analog kann man das Elgamal-Verschlüsselungsverfahren und den Digital Signature Algorithm (DSA) auf elliptische Kurven übertragen. Das liefert den **ECDSA**:

- Gegeben sei eine elliptische Kurve $\mathcal{E}$ und ein Punkt $G \in \mathcal{E}$ mit einer primen Ordnung $m = \mathrm{ord}(G)$. H sei eine kryptographische Hashfunktion, auf die sich Bob und Alice geeinigt haben. Es sei a bzw. $A = a \cdot G$ der private bzw. öffentliche Schlüssel von Alice. Alice möchte das Dokument x signieren.

- Alice wählt eine (geheime) Zufallszahl $r \in \mathbb{Z}_m^*$ (**Nonce**), berechnet $R = r \cdot G$ und betrachtet die x-Koordinate modulo m: $\rho = R_1 \bmod m$. Ist $\rho = 0$, so muss ein neues r gewählt werden. Ansonsten berechnet Alice $h = H(x)$ und $s = r^{-1}(h + a\rho) \pmod m$. Ist $s \neq 0$ so wird x gemeinsam mit (ρ, s) als Signatur bekanntgegeben. Ansonsten wird der Vorgang mit einem neuen r wiederholt.

- Bob berechnet $v_1 = s^{-1}H(x) \pmod m$ und $v_2 = s^{-1}\rho \pmod m$. Ist die x-Koordinate von $(v_1 \cdot G + v_2 \cdot A)_1$ modulo m gleich ρ, so ist die Signatur echt.

Wegen $v_1 = s^{-1}H(x) = r(h-a\rho)^{-1}h$ und $v_2 = r(h-a\rho)^{-1}\rho$ gilt $v_1 \cdot G + v_2 \cdot A = (r(h+a\rho)^{-1}h + r(h+a\rho)^{-1}\rho) \cdot G = r \cdot G = R$, also ist der Algorithmus korrekt. Da wir nur die x-Koordinate überprüfen, ist auch $(\rho, -s)$ eine gültige Signatur.

Die Details sind in [FIPS186-5] zu finden. Insbesondere wird im Standard der Hashwert von x (falls notwendig) auf die Bitlänge von m gekürzt.

Im Laufe der Zeit gab es eine Reihe von Versuchen die Gruppenoperationen besonders effektiv auszuwerten. Eine wichtige Beobachtung dazu kam vom amerikanischen Mathematiker Peter Montgomery (1947–2020), der Kurven in der Form

$$Dy^2 = x^3 + Cx^2 + Ax + B$$

betrachtet hat. Das D wird dabei als **quadratischer Twist** (quadratische Verdrehung) der Kurve bezeichnet und wenn man $y \to Ey$ ersetzt, dann folgt $D \to DE^2$. Die Fälle D und DE^2 führen also auf äquivalente Kurven und es gibt somit, bis

auf Äquivalenz nur zwei Möglichkeiten, nämlich wenn D eine Quadratzahl ist und wenn D keine Quadratzahl ist (Aufgabe 13). Montgomery erkannte, dass, wenn man es geschickt anstellt, zur Berechnung der x-Koordinate von nP nur die x-Koordinate von P notwendig ist und, dass die Formeln besonders einfach werden, wenn man $B = 0$ wählt (wir benötigen ja bei Schlüsseltausch/Signatur nur die x-Koordinate). Der Wert von D wird dabei überhaupt nicht benötigt. Man nennt daher eine Kurve der Form

$$Dy^2 = x^3 + Cx^2 + x$$

auch **Montgomery-Kurve**.

Die Transformation $y = DY$, $x = DX - 3^{-1}C$ bringt sie auf unsere Standardform $Y^2 = X^3 + aX + b$ mit $a = 3^{-1}D^{-2}(3 - C^2)$, $b = 27^{-1}D^{-3}(2C^3 - 9C)$.

Die nächste Idee kam vom amerikanischen Mathematiker Harold Edwards (1936–2020), der Kurven der Form

$$cx^2 + y^2 = 1 + dx^2y^2, \qquad a \neq d \in \mathbb{Z}_p^*$$

betrachtete. Das sieht zwar auf den ersten Blick nicht wie eine elliptische Kurve aus, ist aber mithilfe der Transformation

$$(x, y) \mapsto \left(\frac{1+y}{1-y}, \frac{1}{x}\frac{1+y}{1-y}\right)$$

äquivalent zu einer Montgomery Kurve mit $D = \frac{4}{c-d}$, $C = \frac{2(c+d)}{c-d}$. Die Addition kann auf der **Edwards-Kurve** mit

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - cx_1x_2}{1 - dx_1x_2y_1y_2}\right)$$

besonders leicht durchgeführt werden. Ausserdem benötigt man keinen Punkt im Unendlichen, da das neutrale Element gleich $(0, 1)$ ist. Das inverse Element ist $(-x, y)$. Ist c ein quadratischer Rest und d kein quadratischer Rest, so verschwinden auch die Nenner nicht.

Während die Zuordnung zwischen Montgomery- und Edwards-Kurven bijektiv ist, sind nicht alle elliptischen Kurven von dieser Form.

Die Punkte $(\pm c^{-1/2}, 1)$ sind von der Ordnung 4 (man rechnet leicht $4(\pm c^{-1/2}, 1) = 2(0, -1) = (0, 1)$ nach) und man kann zeigen, dass eine elliptische Kurve genau dann äquivalent zu einer Edwards-Kurve ist, wenn sie einen Punkt der Ordnung 4 hat. Das und mehr findet man in [Ber+08].

Beim **Edwards-Curve Digital Signature Algorithm** wird die Edwards-Kurve

$$-x^2 + y^2 = 1 + \frac{121665}{121666}x^2y^2, \qquad p = 2^{255} - 19$$

verwendet. Wie oben beschrieben, ist sie äquivalent zur Montgomery-Kurve **Curve25519**

$$y^2 = x^3 + 486662x^2 + x, \qquad p = 2^{255} - 19.$$

Diese Kurve wurde 2005 vom deutsch-amerikanischen Mathematiker Daniel J. Bernstein (*2005) vorgeschlagen und wurde 2013 populär, als Vermutungen aufkamen, die NSA könnte Hintertüren in die vom NIST veröffentlichten Kurven eingebaut haben (vgl. auch [KM15]).

Die Signatur basiert auf SHA-512 als Hashfunktion zusammen mit einer Variante des Schnorr-Signatur-Algorithmus.

7.3.1 Ausblick: Die elliptische Kurven-Methode zur Faktorisierung

Da wir nun elliptische Kurven kennen, können wir auch verstehen wie man damit Faktorisieren kann. Die Idee des Algorithmus won H. Lenstra ist ganz einfach, ist n keine Primzahl, so ist $\mathbb{Z}_n$ kein Körper und wenn wir für einen zufälligen Punkt P die Vielfachen $k \cdot P$ betrachten, dann wird die Berechnung irgendwann fehlschlagen, sobald wir auf ein Element stoßen, das in $\mathbb{Z}_n$ nicht invertierbar ist. In dem Fall wissen wir auch warum: Es muss dann ein Teiler von n in der Zahl stecken, die wir nicht invertieren können, und wir sind fertig. Wann passiert dieser Fall? Angenommen p sei der kleinste Primfaktor von $n = pq$ und der Rest q (der nicht notwendigerweise prim sein muss) sei zumindest teilerfremd zu p. Dann können wir unseren Punkt in die Komponenten P_p modulo p und P_q modulo q zerlegen (und mithilfe des Chinesischen Restsatztes auch wieder zu P zusammensetzten). Diese Punkte leben dann auf den entsprechend reduzierten Kurven über $\mathbb{Z}_p$ bzw. $\mathbb{Z}_q$. Wir interessieren uns nur für P_p (wenn bei P_q auch etwas schief gehen sollte, kann uns das natürlich auch recht sein). Sobald k die Ordnung von P_p (oder eine Vielfaches der Ordnung) erreicht, wird P_p ins Unendliche geschickt, das bedeutet, dass die Steigung s (aus der Definition 7.15) gleich 0 modulo p wird und das erkennen wir auch, wenn wir modulo n rechnen, weil dann $s \notin \mathbb{Z}_n^*$ ist. Wir brauchen also nur vor der Berechnung von s^{-1} den $\mathrm{ggT}(s, n)$ berechnen und erhalten einen Teiler von n sobald $s = 0 \pmod{p}$.

Woher bekommen wir nun die Ordnung von P_p, wenn wir p doch nicht kennen? So wie bei der $p-1$ Faktorisierungsmethode in Abschnitt 5.5.3: Wir setzten k als Produkt kleiner Primfaktoren an und hoffen, dass die Teiler der Gruppenordnung der verwendeten elliptischen Kurve über $\mathbb{Z}_p$ darunter sind. Der entscheidende Vorteil gegenüber der $p-1$ Methode ist, dass die Gruppenordnung (und damit die Primfaktoren) nicht nur von p, sondern auch von den Parametern a und b der Kurve abhängen. Hat man also mit einer Kurve kein Glück, so kann man einfach eine andere versuchen. Auf diese Weise können Primfaktoren bis zu einer bestimmten Größe (abhängig von der zur Verfügung stehenden Rechenleistung) mit hoher Wahrscheinlichkeit gefunden werden.

Falls man zuerst a, b und dann P wählt, so hat man das Problem, dass man zur Berechnung der y-Komponente von P die Wurzel in $\mathbb{Z}_n$ ziehen müsste. Das geht aber nur, wenn wir die Faktorisierung von n kennen. Der Ausweg ist es, zuerst a und P zu wählen. Der Wert von b folgt dann leicht (genaugenommen benötigen wir b gar nicht, da es in den Formeln für die Punktaddition nicht explizit aufscheint).

Beispiel 7.23 Faktorisieren Sie die **Mersenne-Zahl** $M_{59} = 2^{59} - 1$ mit der Methode von Lenstra.

Lösung zu 7.23 Wir wählen (zufällig) $a = 3$ und $P = (1, 1)$ (daraus ergibt sich $b = -3$) und wählen als Schranke für die Primzahlpotenzen 80:

$$k = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdots 73 \cdot 79.$$

Damit folgt (Berechnung der Punktaddition in $\mathbb{Z}_{M_{59}}$)

$$kP = (212568097514436876, 67587308435643608)$$

und wir finden keinen Faktor.

Da die Zahlen klein genug sind, können wir auch verstehen warum: Der kleinste Primfaktor von M_{59} ist $p = 179951$ und die Ordnung von P in der elliptischen Kurve über $\mathbb{Z}_p$ ist $7 \cdot 67 \cdot 383$. Die Ordnung unseres Punktes ist gleich der Gruppenordnung und der größte Faktor 383 ist von unserer Schranke nicht abgedeckt. Die Methode wird also erst Erfolg haben, wenn die Schranke bei 383 ist. Natürlich könnten wir den Punkt wechseln und auf eine kleinere Ordnung hoffen, das ist aber unwahrscheinlich.

Alternativ können wir aber nun auch die Kurve wechseln. Z.B. $a = 3$ und $P = (1, 1)$ (daraus ergibt sich $b = -4$). Damit scheitert die Berechnung von kP und liefert den kleinsten Primfaktor p. Die Gruppenordnung ist übrigens in diesem Fall $2^3 \cdot 3^2 \cdot 41 \cdot 61$ und das erkärt warum es nun geklappt hat (die Ordnung von P ist wieder gleich der Gruppenordnung). ■

Weitere Details zur Implementierung dieser Idee finden sich in [CP05; For15].

7.4 Anwendung: Bitcoin

Die ursprüngliche Idee hinter **Bitcoin** war es ein Geldsystem zu entwickeln, das ohne zentrale Kontrolle auskommt [Sat08]:
Bei einem klassischen System wird diese Kontrolle durch die Banken übernommen (wir interessieren uns hier nur für die Funktion als Zahlungsdienstleister, der über die korrekte Abwicklung von Zahlungen zwischen den Teilnehmern wacht). Gehen wir von einem rein digitalen Szenario aus und überlegen wir uns, welche Aufgaben die Bank, der alle Teilnehmer vertrauen, in diesem System hat:

Um Zahlungen abwickeln zu können, vereinbart jeder Teilnehmer mit der Bank eine öffentliche Kontonummer und einen privaten PIN, mit dem er sich gegenüber der Bank authentifizieren kann. Das könnten zum Beispiel der öffentliche und der private Schlüssel eines Signaturalgorithmus sein.

Indem man den öffentlichen Schlüssel (oder eine daraus abgeleitete Größe) als Kontonummer nimmt, spart man sich das Buchführen darüber welcher Schlüssel zu welchem Konto gehört. Bei Bitcoin ist die Kontonummer (genannt **Bitcoinadresse**) der Hashwert des öffentlichen Schlüssels plus eine Prüfziffer.

Möchte nun Alice an Bob Geld überweisen, so erzeugt sie eine Transaktion mit Auftraggeberkonto, Empfängerkonto, Überweisungsbetrag und signiert sie mit ihrem privaten Schlüssel, um die Transaktion zu autorisieren.

Die Bank überprüft die Signatur und ob das Auftraggeberkonto gedeckt ist. Ist die Überprüfung erfolgreich, so akzeptiert sie die Transaktion und trägt sie in ihr Kassabuch ein. Mit diesem Schritt ist die Transaktion abgeschlossen und Bob kann über den Betrag verfügen. Schlägt die Überprüfung fehl (ungültige Signatur oder ungedecktes Konto), so wird die Transaktion zurückgewiesen. Da die Bank die Kontrolle über das Kassabuch hat, müssen alle Teilnehmer der Bank vertrauen.

Stecken Mallory und die Bank unter einer Decke, so könnte Mallory bei Bob einkaufen und per Überweisung bezahlen. Bob überprüft seinen Kontostand und übergibt die Waren. Mallory mach sich aus dem Staub und die Bank löscht die Überweisung aus dem Kassabuch und behauptet Bob hätte sich beim Überprüfen seines Kontostands geirrt.

Die Frage ist nun, wie man die Rolle der Bank (zentral das Kassabuch zu führen) vermeiden könnte. Man könnte das Kassabuch öffentlich führen: Jeder Teilnehmer hat eine Kopie und alle Transaktionen wären transparent für alle Teilnehmer nachvollziehbar (die Kommunikation zwischen den Teilnehmern erfolgt dabei als Peer-to-Peer-Netzwerk).

Eigentlich würde man nicht das ganze Kassabuch brauchen und es würden nur die Kontostände reichen. Ein Kassabuch mit allen Transaktionen zu führen erhöht aber die Nachvollziehbarkeit und damit das Vertrauen ins System. Außerdem müssen bei einem potentiellen Angriff ganze Teile des Kassabuchs gefälscht werden, was den Aufwand für eine Angriff wesentlich erhöht.

Durch die Verwendung von Public-Key-Kryptographie kann jeder Teilnehmer die Korrektheit der einzelnen Transaktionen selbst prüfen. Damit keine Transaktion nachträglich hinzugefügt oder entfernt werden kann, wird jede Transaktion kryptographisch mit der vorhergehenden verkettet. So entsteht eine Kette von Transaktionen (die **Blockchain**) die im Nachhinein (praktisch) nicht mehr manipulierbar ist. Dass es nicht Transaktionskette, sondern Blockkette heißt, erklärt sich dadurch, dass aus Gründen der Effizienz Transaktionen nicht einzeln verarbeitet werden sondern zu Blöcken zusammen gefaßt werden. Wir werden also von nun an, dem allgemeinen Sprachgebrauch folgend, nicht mehr von Transaktionen sondern von Blöcken sprechen, die an die Kette gehängt werden.

Würde man die Blöcke nur nummerieren, so kann man zwar nicht unbemerkt einen Block löschen, man kann aber einen Block durch einen andere ersetzten. Um das zu verhindern und die Blöcke

bildlich aneinanderzuketten wird ein Hashwert des vorhergehenden Blocks zum nächsten dazugeschrieben. Möchte ein Angreifer also einen Block ändern, so muss er zwangsläufig auch alle nachfolgenden Blöcke ändern.

Nun bleibt nur noch ein einziges Problem: Wenn zwei Teilnehmer zwei verschiedene Blöcke an die Kette hängen (d.h. ins Kassabuch eintragen), welche der beiden Ketten ist nun die gültige? Dieses Problem ergibt sich insbesondere, wenn Mallory versucht, ihr Geld (gleichzeitig) mehrfach an verschiedene Empfänger auszugeben!

Es muss also irgendwie bestätigt werden, dass ein Block nun Teil der Kette ist (und somit jede weitere Transaktion die dieser widerspricht — weil das Geld schon ausgegeben ist — als ungültig zurückgewiesen wird). Eine naive Hoffnung wäre es dieses Problem durch die zeitliche Reihenfolge zu lösen, in der die Transaktionen von den Teilnehmern empfangen werden. Während bei einer zentralen Bank die Reihenfolge in der Tat eindeutig ist, so kann man bei lauter gleichberechtigten Teilnehmern nicht mehr davon ausgehen, dass alle die Transaktionen in der selben Reihenfolge erhalten. Dadurch könnten verschiedene Kassabücher entstehen, die sich gegenseitig widersprechen. Wir brauchen also eine Art von *Signatur* mit der jeder aufgenommene Block versehen wird (wodurch auch gleich sichergestellt wird, dass Blöcke nachträglich nicht mehr verändert werden können). Wer aber soll diese *Signatur* erstellen wenn es keine zentrale Stelle gibt, der alle vertrauen?

Übrigens hätte dieses Vorgehen bereits den Vorteil, dass auch eine zentrale Bank keine Transaktionen mehr löschen kann, da sie aufgrund der Transparenz eine einmal gegebene Signatur auf einen Block nicht mehr zurückziehen kann. Ein Manipulationsversuch der Bank würde also zumindest auffliegen und das erforderliche Vertrauen in die Bank kann weit geringer ausfallen. Trotzdem wäre eine böswillige Bank in der Lage das ganze System zu stören und im schlimmsten Fall damit sogar zu Fall zu bringen.

Der Lösungsansatz von Bitcoin ist es, dass diese Signatur kollektiv in Form von Arbeit ("**proof-of-work**") erbracht wird. Solange die Mehrheit mehr Arbeitsleistung (=Rechenleistung) zur Verfügung stellen kann als Mallory, hat Mallory keine Möglichkeit mehr das System zu manipulieren!

Eine anderer Möglichkeit wäre es die Signatur durch einen Mehrheitsentscheid zu erbringen: Wenn die Mehrheit der Teilnehmer einen Block akzeptiert (bestätigt durch ihre Signaturen), dann gilt er als in die Kette eingetragen. Da die Anzahl der Teilnehmer aber nicht bekannt ist (mehr noch, ein Teilnehmer kann im Prinzip beliebig viele Konten erstellen), müsste man die Unterschriften mit der Geldmenge gewichten über die sie verfügen ("**proof-of-stake**"). Bei einer großen Anzahl von Teilnehmern ist das schwierig.

Konkret wird das bei Bitcoin wie folgt umgesetzt: Neben den *Kontoinhabern* gibt es noch weitere Teilnehmer, die Arbeitsleistung zur Verfügung stellen, die sogenannten Schürfer ("miner"). Natürlich kann jeder Teilnehmer beide Rollen einnehmen. Jeder Schürfer sammelt alle zu verarbeitenden Transaktionen in einem Pool, aus dem er sich eine gewisse Anzahl auswählt um einen neuen Block zu erstellen. Nun verknüpft er den Hashwert des letzten (ihm bekannten) Blocks mit dem Hashwert der ausgewählten Transaktionen und hängt noch einen kleinen Zufallsblock (Nonce) dran. Davon berechnet er einen weiteren Hashwert und ändert den Zufallsblock

so lange, bis das Ergebnis eine vorgegebene Anzahl von führenden Nullen hat.

Die passende Nonce übernimmt also die Rolle der *Signatur* für den Block. Solange die guten Teilnehmer mehr Rechenleistung als Mallory zur Verfügung stellen, können sie Signaturen schneller erzeugen als Mallory und, da die längste Kette gewinnt, ist Mallory chancenlos.

Bei Verwendung einer kryptographischen Hashfunktion ist das ein rechenaufwendiges Problem das nur mit Brute-Force gelöst werden kann. Durch die Anzahl der Nullen, die man fordert, kann die Schwierigkeit dieses Problem der Anzahl der Schürfer angepasst werden, sodass durchschnittlich alle 10 Minuten irgendein Schürfer eine Lösung findet.

Bei einer kryptographischen Hashfunktion produziert jeder Eingangswert eine (praktisch) unvorhersehbare Folge von Ausgangsbits. Die Ausgangsbits können in diesem Sinn also als Zufallsbits betrachtet werden. Die Wahrscheinlichkeit, dass die ersten n Bits gleich Null sind, ist somit 2^{-n} und man braucht im Mittel 2^n Versuche um dieses Ergebnis zu erreichen

Sobald ein Schürfer eine Lösung findet, hängt er seinen Block an die Kette und teilt allen anderen Teilnehmern die neue Kette mit und das Spiel beginnt von vorne. Als Belohnung für seine Arbeit hat er seinem Block auch noch eine Transaktion hinzugefügt, die seinem Konto eine definierte Menge an Bitcoins gutschreibt. Die anderen Schürfer gehen leer aus und hoffen auf mehr Glück in der nächsten Runde. Im Prinzip ist es möglich (wenn auch sehr unwahrscheinlich), dass zwei Schürfer gleichzeitig zwei verschiedene Blöcke validieren und damit zwei gültige Ketten entstehen, die sich im letzten Block unterscheiden. In diesem Fall kann sich jeder Schürfer aussuchen, mit welcher Kette er weiterarbeitet. Sobald er aber von einer längeren Kette erfährt, muss er seine Arbeit einstellen und mit der längsten ihm bekannten weitermachen. Solange sich die Mehrheit der Teilnehmer an diese Regel hält, wird es bald wieder nur eine gültige Kette geben. In der Praxis betrachtet man eine Transaktion daher erst dann als endgültig eingetragen, wenn sie mindestens 6 Blöcke tief in der Kette ist (also nach ca. einer Stunde). Das Prinzip des Schürfens übernimmt übrigens auch die Funktion der Gelderzeugung (die als Belohnung ausgezahlten Bitcoins hat es vorher nicht gegeben). Die Höhe der Belohnung ist im Protokoll festgelegt und nimmt im Laufe der Zeit ab (irgendwann sinkt sie auf Null und ab diesem Zeitpunkt gibt es keine neuen Bitcoins mehr). Außerdem kann man bei jeder Transaktion auch ein *Trinkgeld* für den Schürfer lassen (damit die eigene Transaktion bevorzug aus dem Pool gewählt wird) damit das System auch noch funktioniert, wenn die festgelegte Maximalzahl an Bitcoins erreicht ist (und somit keine weiteren Belohnungen an Schürfer ausgezahlt werden).

Im ersten Block wurden 50 Bitcoins ausgezahlt und dieser Wert wird alle 210 000 Blöcke halbiert (bei 10 Minuten pro Block also ca. alle vier Jahre). Nach 32 Halbierungen (also voraussichtlich im Jahr $2009 + 33 * 4 - 1 = 2140$) fällt dieser Wert unter die kleinste Einheit von 10^{-8} Bitcoin (genannt ein Satoshi) und somit kann keine Belohnung mehr ausgezahlt werden. Zu diesem Zeitpunkt ist die theoretische Maximalzahl von $210\,000 \sum_{j=0}^{32} 10^{-8} \lfloor 10^8 \frac{50}{2^j} \rfloor = 20999999.9769$ an Bitcoins erreicht. Die Anzahl der im Umlauf befindlichen Bitcoins ist natürlich kleiner, denn wann immer jemand seinen privaten Schlüssel verliert sind die zugehörigen Bitcoins für immer verloren. Aber auch wenn ein Schürfer vergißt sein Trinkgeld zu kassieren (was schon vorgekommen ist),

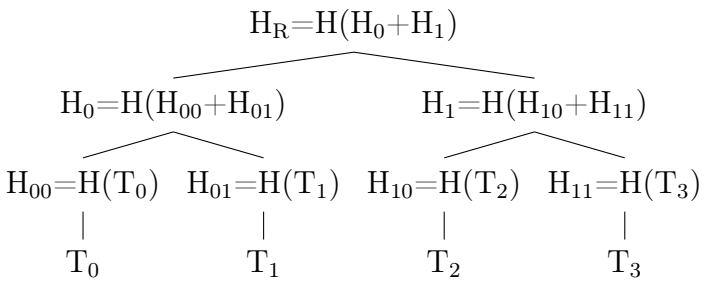

Abbildung 7.4: Hashbaum

so ist dieses ebenfalls für immer verloren.

Dadurch, dass alle Transaktionen öffentlich sind gibt das natürlich ein Problem mit der Privatsphäre. Dieses wird gelöst, da die Anzahl der Kontonummern praktisch unbegrenzt ist. Bob kann also für jeden Betrag, den er erhalten möchte, ein neues Konto erzeugen.

Es ist aber zu beachten, dass bei Bitcoin die Anonymität spätestens an den Schnittstellen mit der realen Welt zu Ende ist. Wenn sich jemand seine illegalen Machenschaften in Bitcoins bezahlen läßt, so kann man den Weg dieser Bitcoins verfolgen bis sie in *normales* Geld getauscht werden und in diesem Moment können dann die Handschellen klicken.

Natürlich braucht man dann eine passende Software um den Überblick nicht zu verlieren! In der Praxis erzeugt man einen privaten Masterschlüssel und daraus dann weitere private Unterschlüssel. Das erzeugt allerdings viele Konten, die nur einmalig verwendet werden. Um Speicherplatz zu sparen würde man die zugehörigen Transaktionen gerne löschen können, sobald sie obsolet sind (d.h. zu einem inzwischen geleerten Konto gehören). Daten aus der Kette zu löschen ist aber gerade nicht möglich. Deshalb werden zusätzlich zu den Transaktionen auch deren Hashwerte als **Hashbaum** (Merkel Tree; die Hashwerte der Transaktionen sind die Blätter des Baums und der Hashwert an jedem Knoten ist der Hashwert aus den beiden Nachfolgern — vgl. Abbildung 7.4) zur Verifikation gespeichert. Für jede nicht mehr benötigte Transaktion reicht es also, den zugehörigen Hashwert zu speichern und dank der Baumstruktur reicht es sogar, den darüberliegenden Hash zu kennen wenn alle darunterliegenden Transaktionen nicht mehr relevant sind. Sind z.B. alle Transaktionen in einem Block nicht mehr relevant, reicht es einen einzelnen Hashwert (den der Wurzel des Hashbaums) zu behalten. Dieser Hashwert steht im Blockheader und es reicht also in diesem Fall nur den Blockheader zu behalten. Das können aber nur einzelne Teilnehmer für sich machen, da man nur mithilfe des gesamten Blocks sicherstellen kann, dass dieser in der Tat keine relevanten Transaktionen mehr enthält.

Nun noch einige technische Details [BCWiki]: Als Signaturalgorithmus wird der Elliptic Curve Digital Signature Algorithm (ECDSA) auf der Kurve secp256k1 verwendet:

$y^2 = x^3 + 7$ über $\mathbb{Z}_p$ mit $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
Generator $G =$ 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798.

Das "02" am Anfang bedeutet, dass der Generator in komprimierter Form angegeben ist. D.h. es ist nur die x-Koordinate des Generators als Hexadezimalzahl angegeben. Für die y-Koordinate gibt es ja nur zwei Möglichkeiten, die sich nur durch das Vorzeichen unterscheiden. Die zwei Möglichkeiten sind also von der Form y bzw. $-y = p - y$ und da p ungerade ist, ist eine der Zahlen gerade und die andere ungerade. Das 02 sagt uns, dass wir die gerade y-Koordinate nehmen müssen (ein 03 würde uns anweisen, die ungerade zu nehmen). Steht am Anfang 04, so ist die Hexadezimalzahl dahinter doppelt so lang und die erste Hälfte ist die x-Koordinate und die zweite die y-Koordinate.

Das ist eine vom NIST standardisierte Kurve mit speziellen mathematischen Eigenschaften (eine sogenannte Koblitz-Kurve), die eine effiziente Implementierung der Rechenoperationen erlaubt. Die Ordnung kann ebenfalls explizit ausgerechnet werden und G erzeugt die ganze Gruppe.

Der private Schlüssel ist eine Zufallszahl $r \in \mathbb{Z}_p$ und der öffentliche Schlüssel ist $r \cdot G$. Der private Schlüssel muss unbedingt kryptographisch sicher erzeugt werden (Teilnehmer, die sich dabei auf die Dienste von Webseiten verlassen, haben dieses "Service" in der Vergangenheit schon mit dem Totalverlust ihres digitalen Vermögens bezahlt).

Die öffentliche Bitcoin-Adresse (Kontonummer) mit der man digitale Coins empfangen kann wird aus dem öffentlichen Schlüssel als Hashwert gebildet (als Hashfunktionen kommen SHA-256 und RIPEMD160 zum Einsatz) und Transaktionen werden mit dem ECDSA signiert.

Jeder Block beginnt mit einer *Magic number*, der Blockgröße, dem Blockheader und der Anzahl der Transaktionen, gefolgt von den eigentlichen Transaktionen. Der Blockheader enthält die Protokollversion, den Hashwert des Headers des Vorgängerblocks, den Hashwert der Wurzel des Hashbaums der Transaktionen, einen Zeitstempel, den Zielwert, den ein gültiger Hashwert für den Block unterschreiten muss (also die Zahl über die die Schwierigkeit des Problems gesteuert wird), und die Zufallszahl (Nonce), die vom Schürfer variiert werden kann, um den vorgegebenen Zielwert zu unterschreiten. Alle 2016 Blöcke (also ca. alle 2 Wochen) wird der Zielwert neu berechnet, um die Schwierigkeit an die Rechenleistung der Schürfer anzupassen.

Normale Transaktionen bestehen aus einer Anzahl von Eingängen und einer Anzahl von Ausgängen. Die Eingänge sind Verweise auf Ausgänge vorangegangener Transaktionen (dadurch wird sichergestellt, dass man die Coins, die man ausgibt, auch irgendwann eingenommen hat). Die Summe der Eingänge steht als Ausgang zur Verfügung und die Ausgänge verteilen diese Summe auf beliebige weitere Adressen. Eine digitale Signatur mit ECDSA stellt sicher, dass die Transaktion

4 Bytes	0xD9B4BEF9 (Magic number)
4 Bytes	Blockgröße
80 Bytes	Blockheader
	4 Bytes Protokollversion
	32 Bytes Hashwert des Headers des Vorgängerblocks
	32 Bytes Hashwert der Wurzel des Hashbaums
	4 Bytes Zeitstempel
	4 Bytes Zielwert
	4 Bytes Nonce
1–9 Bytes	Anzahl der Transaktionen
max 1 MB	ca. 2000 Transaktionen zu je ca. 300–400 Bytes

Tabelle 7.1: Struktur eines Blocks bei Bitcoin

vom rechtmäßigen Besitzer der Coins erzeugt wurde. Zusätzlich gibt es in jedem Block noch eine **Coinbase-Transaktion** ohne Eingänge, in der der Schürfer seine Belohnung für das Schürfen des Blocks und die etwaige Differenzen zwischen Ein- und Ausgängen aus weiteren Transaktionen (sein Trinkgeld) beanspruchen kann. Wenn jemand also vergisst, das Restgeld wieder einer seiner Adressen zuzuschreiben, freut sich ein Schürfer.

Mathematisch gibt es hier noch viele interessante Fragestellungen. Z.B. was ist die Wahrscheinlichkeit, dass ein Versuch von Mallory, sein Geld zweimal auszugeben erfolgreich ist, wenn Mallory ein vorgegebener Prozentsatz der Rechenleistung aller Schürfer zur Verfügung steht? Vgl. dazu [GP17]. Aber wir können hier leider nicht näher darauf eingehen.

Zum Schluss noch einige (nichtmathematische) Bemerkungen:

Das Prinzip der Blockchain ist natürlich auch für beliebige andere Anwendungen nützlich, wo sich mehrere Teilnehmer (ohne zentrale Stelle, der alle vertrauen) darauf einigen müssen, welche Einträge in ein gemeinsam geführtes Transaktionsbuch gemacht werden.

Zum Beispiel könnte man Buch über Verträge führen. Das findet z.B. bei Non-Fungible Tokens (**NFT**) Anwendung, wo in einer Blockchain ein Vertrag hinterlegt wird, in dem ein Urheber die Rechte an einem Objekt (z.B. ein digitales Kunstwerk) verkauft. Wer das NTF besitzt, besitzt also juristisch gesehen (und vorausgesetzt, der hinterlegte Vertrag ist juristisch gültig) das Objekt (auch wenn das Objekt, wie bei einem digitalen Kunstwerk, beliebig oft kopiert werden kann und es technisch gesehen kein Original gibt das man besitzen kann). Der Hauptvorteil ist, dass man ein NTF leicht und schnell über das Internet handeln kann.

Man könnte sogar den Speicher (Programme und ihre Daten) eines virtuellen Computers auf diese Art verwalten. Das klingt zunächst vielleicht absurd, ermöglicht aber sogenannte "**Smart Contracts**", also Verträge die dynamisch auf gewisse zukünftige Ergeignisse reagieren können. Das ist z.B. bei **Ethereum** im-

plementiert. Da ein Smart Contract ein Programm ist, kann es natürlich Fehler enthalten, was dazu führen kann, dass Geld unwiederbringlich verloren geht oder an die falschen Personen verteilt wird.

Einer der Hauptkritikpunkte an Bitcoin ist die große Resourcenverschwendung durch das Schürfen. Deshalb gibt es inzwischen Alternativen um bei einer Blockchain zu einem Konsenz über den nächsten gültige Block zu gelangen. Dies erfolgt meist über Teilnehmer (*Validators*), die durch ein Verfahren, dass die Anzahl und das Alter der gehaltenen Coins berücksichtigt ("**proof-of-stake**"), ausgewählt werden. Bei Ethereum erfolgte diese Umstellung 2022. Wer am Konsenzprozess mitwirken will, muss eine bestimmte Anzahl an Coins hinterlegen, und darf dann an der Wahl des nächsten Blocks teilnehmen. Dieser wird mit Zweidrittelmehrheit bestimmt und wer seinen Pflichten nicht zeitgerecht nachkommt, oder sich nicht an die Regeln hält, der verliert seine Belohnung bzw. es werden die hinterlegten Coins eingezogen.

Man muss sich auch darüber im Klaren sein, dass, auch wenn die Erzeugung eines Bitcoins durch Schürfen erhebliche Kosten (Hardware und Strom) verursacht, der *reale* Wert eines Bitcoins einzig und alleine durch das Vertrauen der Teilnehmer in das System bestimmt ist. Sinkt das Vertrauen, sinkt auch der Wert. Im Prinzip ist das natürlich bei den heutigen Geldsystemen ebenso, allerdings gibt es hier eine Nationalbank, die versucht, den Wert innerhalb bestimmter Grenzen zu halten. Dadurch wurde Bitcoin zum reinen Spekulationsobjekt und die ursprüngliche Idee, ein günstiges Zahlungsmittel, das nicht zentral kontrolliert wird, zur Verfügung zu stellen, ist in weite Ferne gerückt.

7.5 Kontrollfragen

Fragen zu Abschnitt 7.1: Elliptische Kurven über $\mathbb{R}$

Erklären Sie folgende Begriffe: Elliptische Kurve, Addition, Punkt im Unendlichen

1. Welche Gleichung beschreibt eine elliptische Kurve?
   a) $y^2 = x^3 - 3x + 5$ b) $y^2 = x^2 + 4x - 7$ c) $y = x^2 + 2x + 1$
   d) $y = x^3 - 8x - 6$ e) $y^2 = x^3 + 2x$ f) $y^2 = x^3 - 5$

   (Lösung zu Kontrollfrage 1)

2. Warum wird für elliptische Kurven $\mathcal{E} : y^2 = x^3 + ax + b$ die Bedingung $4a^3 + 27b^2 \neq 0$ verlangt?
   a) Damit es in jedem Punkt von $\mathcal{E}$ eine Tangente gibt.
   b) Damit die elliptische Kurve keine doppelten Nullstellen hat.
   c) Damit $p(x) = x^3 + ax + b$ keine doppelten Nullstellen besitzt.
   d) Damit die elliptische Kurve keine Punkte mit senkrechter Tangente hat.

   (Lösung zu Kontrollfrage 2)

3. Was trifft für jede elliptische Kurve $\mathcal{E}$ über $\mathbb{R}$ zu?
   a) $\mathcal{E}$ ist spiegelsymmetrisch zur x-Achse.
   b) $\mathcal{E}$ ist spiegelsymmetrisch zur y-Achse.
   c) Zu jedem $y \in \mathbb{R}$ gibt es zumindest einen Punkt $(x, y) \in \mathcal{E}$.
   d) Zu jedem $x \in \mathbb{R}$ gibt es zumindest einen Punkt $(x, y) \in \mathcal{E}$.
   e) $\mathcal{E}$ ist eine einzige geschlossene Kurve.

   (Lösung zu Kontrollfrage 3)

4. Wie kann man die Addition von zwei unterschiedlichen Punkte P und Q einer elliptischen Kurve über $\mathbb{R}$ geometrisch (also graphisch) veranschaulichen? Man legt eine Gerade durch P und Q.

   a) Diese Gerade schneidet die elliptische Kurve in genau einem weiteren Punkt. Der Schnittpunkt wird an der x-Achse gespiegelt und man erhält so wieder einen Punkt der elliptischen Kurve. Dieser ist $P + Q$.

   b) Diese schneidet die elliptische Kurve in genau einem weiteren Punkt. Dieser ist $P + Q$.

   c) Der Schnittpunkt dieser Geraden mit der x-Achse ist $P + Q$.

   d) Der Schnittpunkt dieser Geraden mit der y-Achse ist $P + Q$.

   (Lösung zu Kontrollfrage 4)

5. Wozu benötigt man den Punkt im Unendlichen $\mathcal{O}$?

   (Lösung zu Kontrollfrage 5)

6. $\mathcal{E}$ sei die elliptische Kurve $y^2 = x^3 + 3x$ und $P = (3, 6)$ und $Q = (3, -6)$ Punkte von $\mathcal{E}$. Was trifft zu?
   a) $-P = (-3, -6)$ b) $P + Q = (6, 0)$ c) $P + Q = (0, 0)$
   d) $P + Q = \mathcal{O}$ e) $-P = Q$

   (Lösung zu Kontrollfrage 6)

7. $\mathcal{E}$ sei die elliptische Kurve $y^2 = x^3 + 3x$ über $\mathbb{R}$ und $P = (3, 6)$ und $Q = (1, 2)$ Punkte von $\mathcal{E}$. Was trifft zu?
   a) $P + Q = (4, 8)$ b) $P + Q = (0, 0)$ c) $R = (4, 8)$ liegt auf $\mathcal{E}$.
   d) Die Sekante durch P und Q hat die Steigung $s = 2$.

   (Lösung zu Kontrollfrage 7)

8. Was trifft zu?
   a) Der Parameter s in der Formel für die Punktaddition ist die Steigung der Sekante bzw. Tangente.
   b) Wenn man zwei verschiedene Punkte addiert, die spiegelsymmetrisch sind zur x-Achse, so ist die Formel nicht verwendbar, denn dabei würde 0 im Nenner von s stehen.

c) Wenn man zwei verschiedene Punkte addiert, die spiegelsymmetrisch sind zur x-Achse, so ist ihre Summe $\mathcal{O}$, also der Punkt im Unendlichen.
d) Wenn man zwei verschiedene Punkte addiert, die spiegelsymmetrisch sind zur x-Achse, so ist $s = 0$.

(Lösung zu Kontrollfrage 8)

9. Gegeben ist die elliptische Kurve $\mathcal{E} : y^2 = x^3 + 5x - 2$ über $\mathbb{R}$. Was trifft zu?
a) Es gibt mindestens einen Punkt mit $x = 0$.
b) $P = (2, 4)$ liegt auf $\mathcal{E}$.
c) Es gibt mindestens einen Punkt mit $y = 0$.
d) Es gibt mindestens einen Punkt mit $y = -3$.

(Lösung zu Kontrollfrage 9)

10. Gibt es auf einer elliptischen Kurve $\mathcal{E}$ ausser $\mathcal{O}$ Punkte mit der Eigenschaft $P = -P$? Wenn ja wie viele?

(Lösung zu Kontrollfrage 10)

Fragen zu Abschnitt 7.2: Wurzelziehen in $\mathbb{Z}_p$

Erklären Sie folgende Begriffe: Quadratischer Rest, Legendre-Symbol

1. Wann verschwindet das Legendre-Symbol $\left(\frac{a}{p}\right)$?

(Lösung zu Kontrollfrage 1)

2. Es sei $a \in \mathbb{Z}_p$ eine Quadratzahl. Wann ist $-a$ auch eine Quadratzahl?

(Lösung zu Kontrollfrage 2)

Fragen zu Abschnitt 7.3: Elliptische Kurven über $\mathbb{Z}_p$

Erklären Sie folgende Begriffe: Diskrete Elliptische Kurve, Ordnung, Generator, Diskretes Logarithmusproblem

1. Richtig oder falsch? Auf jeder elliptischen Kurve gilt $|\mathcal{E}| \cdot P = \mathcal{O}$.

(Lösung zu Kontrollfrage 1)

2. Wieviele Elemente hat eine elliptische Kurve über $\mathbb{Z}_5$ maximal?

(Lösung zu Kontrollfrage 2)

3. In welchem Sinn ist das DLP auf elliptischen Kurven schwieriger?

(Lösung zu Kontrollfrage 3)

Lösungen zu den Kontrollfragen

Lösungen zu Abschnitt 7.1

1. a) richtig b) falsch c) falsch d) falsch e) richtig f) richtig
2. a) richtig b) falsch c) richtig d) falsch
3. a) richtig b) falsch c) richtig d) falsch e) falsch
4. a) richtig b) falsch c) falsch d) falsch
5. Er übernimmt die Rolle des neutralen Elements bei der Addition.
6. a) falsch b) falsch c) falsch d) richtig e) richtig
7. a) falsch b) richtig c) falsch d) richtig
8. a) richtig b) richtig c) richtig d) falsch
9. a) falsch b) richtig c) richtig d) richtig
10. Aus $P = -P = P^*$ folgt, dass diese Punkte von der Form $(x, 0)$ sind. x muss also eine Nullstelle von $x^3 + ax + b$ sein. Denmnach gibt es entweder einen oder drei solcher Punkte.

Lösungen zu Abschnitt 7.2

1. Genau dann, wenn $a = 0 \pmod{p}$.
2. Es gilt $\left(\frac{-a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Also genau dann, wenn $(p-1)/2$ gerade ist.

Lösungen zu Abschnitt 7.3

1. Ja, das gilt in jeder Gruppe und folgt aus dem Satz von Lagrange.
2. Nach dem Satz von Hasse höchstens $\lfloor 6 + 2\sqrt{5} \rfloor = 10$.
3. Weil es keine so guten Algorithmen wie für $\mathbb{Z}_p^*$ gibt.

7.6 Übungen

Aufwärmübungen

1. Gegeben ist die elliptische Kurve $E : y^2 = x^3 - 2x + 4$ über $\mathbb{R}$.
   a) Überprüfen Sie die Bedingung $4a^3 + 27b^2 \neq 0$ für diese Kurve. Was wird durch diese Bedingung garantiert?
   b) Skizzieren Sie die elliptische Kurve (zuerst kleine Wertetabelle und dann z.B. mithilfe Wolfram Alpha oder Geogebra).
   c) Zeichnen Sie das kubische Polynom $p(x) = x^3 - 2x + 4$ und die elliptische Kurve gemeinsam in eine Skizze. Warum hat die elliptische Kurve nur Punkte $P = (x, y)$ für jene x, für die $p(x) \geq 0$ gilt?

2. Gegeben ist die elliptische Kurve $y^2 = x^3 - 2x + 4$ über $\mathbb{R}$ und der Punkt $B = (3, 5)$.
   a) Zeigen Sie, dass B auf der elliptischen Kurve liegt.
   b) Ermitteln Sie $P = 2B$ sowohl geometrisch als auch rechnerisch.

3. Gegeben ist die elliptische Kurve $y^2 = x^3 - 2x + 4$ über $\mathbb{R}$ und die Punkte $A = (0, 2)$ und $B = (3, 5)$.
   Ermitteln Sie $R = A + B$ sowohl geometrisch als auch rechnerisch.

4. Wie groß muss p gewählt werden, damit eine elliptische Kurve über $\mathbb{Z}_p$ mindestens 30 Punkte hat?

5. Gegeben ist die elliptische Kurve $\mathcal{E} : y^2 = x^3 + x$ über $\mathbb{Z}_3$.
   a) Überprüfen Sie die Bedingung $4a^3 + 27b^2 \neq 0 \pmod 3$.
   b) Bestimmen Sie alle Punkte der elliptischen Kurve. Wie viele Punkte hat $\mathcal{E}$?
   c) Stellen Sie die Additionstabelle auf.

6. Gegeben ist die elliptischen Kurve $E : y^2 = x^3 + x + 6 \bmod 11$.
   a) Berechnen Sie alle Punkte von E.
   b) Skizzieren Sie die elliptische Kurve.
   c) Ist E zyklisch? Begründen Sie kurz.
   d) Verifizieren Sie die Abschätzung von Hasse für diese elliptische Kurve.

7. Gegeben ist die elliptische Kurve $E : y^2 = x^3 + 5x + 2 \bmod 7$. Mittels Wertetabelle kann man berechnen, dass $E = \{\mathcal{O}, (0, 3), (0, 4), (1, 1), (1, 6), (3, 3), (3, 4), (4, 3), (4, 4)\}$.
   a) Bestimmen Sie die Ordnung des Punktes $P = (4, 4)$.
   b) Warum ist E zyklisch?
   c) Wie viele Generatoren gibt es in E?

8. Wie könnte man die Punkte, die auf einem Einheitskreis $x^2 + y^2 = 1$ liegen zu einer Gruppe machen? Klappt das auch mit einer Ellipse?

Weiterführende Aufgaben

1. Gegeben ist die elliptische Kurve $y^2 = x^3 - 3x + 1$ über $\mathbb{R}$.
   a) Skizzieren Sie die elliptische Kurve (kleine Wertetabelle und z.B. mithilfe Wolfram Alpha oder Geogebra).
   b) Ermitteln Sie zum Punkt $A = (0, 1)$ der elliptischen Kurve den Punkt $2A$ sowohl geometrisch als auch rechnerisch.

2. Gegeben ist die elliptische Kurve $y^2 = x^3 - 3x + 1$ über $\mathbb{R}$ und die Punkte $A = (0, 1)$ und $B = (\frac{9}{4}, \frac{19}{8})$. Ermitteln Sie den Punkt $A + B$ sowohl geometrisch als auch rechnerisch.

3. Gegeben ist die elliptische Kurve $y^2 = x^3 - 3x + 5$ über $\mathbb{R}$ und einer ihrer Punkte $P = (1, \sqrt{3})$.
   a) Ermitteln Sie $R = 2P$ rechnerisch und geometrisch.
   b) Ermitteln Sie $Q = P + (-R)$ rechnerisch und geometrisch.

4. Um das Vielfache nP auf einer elliptischen Kurve effizient zu berechnen, wird der **Double-and-Add-Algorithmus** verwendet. Er funktioniert analog zum **Square-and-Multiply-Algorithmus**, es muss nur „Quadrieren“ durch „Verdopplung“ und „Multiplizieren“ durch „Addition“ ersetzt werden: Beispiel: Um $23P$ zu berechnen, ermitteln wir wieder die Binärdarstellung, $23 = (10111)_2$; von links nach rechts gelesen wird für jeden 1 verdoppelt und addiert, für jede 0 wird nur verdoppelt. Initialisiert wird nun mit $\mathcal{O}$:

   $$23P = 2(2(2(2(2 \cdot \mathcal{O} + P)) + P) + P) + P$$

   Geben Sie mithilfe des Double-and-Add-Algorithmus an:
   a) $17P$ b) $20P$

5. Berechnen Sie (wenn möglich) die Wurzeln von:
   a) $a = 3$ in $\mathbb{Z}_{11}$ b) $a = -1$ in $\mathbb{Z}_{13}$

6. Betrachten Sie das Rabin-Kryptosystem mit n einer Blum-Zahl, also ein Produkt aus zwei Primzahlen die Rest 3 bei Division mit 4 ergeben. Zeigen Sie: Ist x eine Quadratzahl bezüglich n, dann kann man leicht mit $y^{((p-1)(q-1)+4)/8} = x$ entschlüsseln und x ist die einzige Wurzel von $y = x^2$ mit dieser Eigenschaft. (Hinweis: Verwenden Sie das Legendresymbol in $\mathbb{Z}_p$ und $\mathbb{Z}_q$.)

7. Bestimmen Sie alle Punkte der elliptischen Kurve $y^2 = x^3 + 3x + 2$ über $\mathbb{Z}_7$.

8. Gegeben ist die elliptischen Kurve $\mathcal{E} : y^2 = x^3 + x + 6 \bmod 11$. Man kann zeigen (Aufgabe 6), dass $|\mathcal{E}| = 13$ (inklusive dem Punkt $\mathcal{O}$). Betrachten Sie den Punkt $P = (2, 4)$.

a) Zeigen Sie, dass $P \in \mathcal{E}$.
b) Ist P ein erzeugendes Element? (Begründen Sie ohne Rechnung!)
c) Berechnen Sie $2P$ und $3P$.
d) Geben Sie (ohne lange Rechnung) an: $-P$, $13P$, $12P$, $26P$, $25P$.

9. Gegeben ist die elliptische Kurve $\mathcal{E} : y^2 = x^3 + 3x + 6$ über $\mathbb{Z}_7$, die aus folgenden vier Punkten besteht: $\mathcal{E} = \{\mathcal{O}, (3,0), (6,3), (6,4)\}$.
a) Geben Sie zu jedem Punkt dessen Ordnung an.
b) Geben Sie zu jedem Punkt die von ihm erzeugte Untergruppe an.

10. **ECDH:** Gegeben ist die elliptischen Kurve $\mathcal{E} : y^2 = x^3 + x + 6 \bmod 11$ und der Punkt $G = (2,4)$. Alice wählt $a = 6$ und Bob wählt $b = 3$. Wie gehen Alice und Bob beim Diffie Hellman Schlüsselaustausch vor (geben Sie die einzelnen Schritte an) und welchen gemeinsamen geheimen Punkt C vereinbaren sie?
(Tipp: Sobald Sie die Punktaddition mit der Hand beherrschen, können Sie die Rechenarbeit auslagern z.B. mithilfe http://www.christelbach.com/eccalculator.aspx).

11. Geben Sie alle Elemente der Ordnung 2 einer elliptischen Kurve $\mathcal{E}$ an. Wie erhält man daraus eine notwendige Bedingung dafür das $\mathcal{E}$ zyklisch ist? Finden Sie eine elliptische Kurve die nicht zyklisch ist.

12. Die Punkte
$$\mathcal{E}[m] = \{P \in \mathcal{E} | mP = \mathcal{O}\}$$
heißen m-**Torsionspunkte**. Zeigen Sie, dass $\mathcal{E}[m]$ eine Untergruppe bildet.

13. Es seien $A, B, C \in \mathbb{Z}_p$ fest. Für $D \in \mathbb{Z}_p^*$ wird die Montgommery-Kurve $\mathcal{E}_D$
$$Dy^2 = x^3 + Cx^2 + Ax + B$$
als quadratischer Twist der Kurve $\mathcal{E} = \mathcal{E}_1$
$$y^2 = x^3 + Cx^2 + Ax + B$$
bezeichnet. Man zeige, dass $\mathcal{E}_{D'}$ und $\mathcal{E}_D$ genau dann isomorph sind, wenn $\left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right)$. Wie hängen $|\mathcal{E}_D|$ und $|\mathcal{E}|$ zusammen, wenn $\left(\frac{D}{p}\right) = -1$?

14. **Digital Signature Standard (DSS):** Recherchieren Sie im FIPS 186-4 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf zur **Curve P-256**:
a) Welche Bedeutung hat die angegebene Zahl 256?
b) Welchen Wert hat der Parameter a bei dieser Kurvengleichung?
c) Was erfährt man über die Anzahl der Punkte der Kurve?
d) Welche Ordnung hat der angegebene *base point* G?
e) Ist die Kurve zyklisch? Warum?

15. Recherchieren Sie:
    a) Welche elliptische Kurve spielt bei **Bitcoin** eine Rolle?
    b) Wozu wird sie gebraucht?
    c) Welches „mathematische Rätsel“ muss ein „Miner“ lösen? Welche kryptographische Hashfunktion ist dabei im Spiel?

16. **Bitcoin Mining**:
    a) Wie groß ist die Wahrscheinlichkeit, bei einer kryptographischen Hashfunktion einen Hashwert mit n führenden Nullen zu erzeugen (unter der Annahme einer Gleichverteilung für die Hashwerte)?
    b) Gegeben ist eine kryptographische Hashfunktion. Ein „Miner“ probiert zufällig und „mit Zurücklegen“ einen Hashwert mit 4 führenden Nullen zu erzeugen. X = Anzahl der Versuche, bis der Miner Erfolg hat. Bestimmen Sie die Verteilung von X! (Tipp: Ist es eine Gleichverteilung, eine Binomialverteilung oder eine geometrische Verteilung?).
    c) Wie viele Hashwerte muss der Miner im Schnitt probieren? (Tipp: Erwartungswert).

17. **Doublespending bei Bitcoin** Da gültige Hashwerte für einen Block durch zufälliges Probieren gefunden werden, kann man davon ausgehen, dass die Zeit bis zu deren Auffinden exponentialverteilt ist:

    $$T_1 \sim \mathcal{E}(\alpha).$$

    Hierbei ist α die durchschnittliche Zeit, die zum Auffinden benötigt wird.
    a) Wie ist die Zeit T_n zum Auffinden von n-Blöcken verteilt?
    b) Wenn Mallory mit einer Rate β Hashwerte finden kann, was ist die Wahrscheinlichkeit, dass Mallory n-Blöcke schneller findet, als der Rest? (Hinweis: Integrale dürfen gerne mit CAS/Tabellen berechnet werden.)

Lösungen zu den Aufwärmübungen

1. a) $4 \cdot (-2)^3 + 27 \cdot 4^2 \neq 0$
   b) und c) Abbildung 7.5. Weil für x mit $p(x) < 0$ die Gleichung $y^2 = p(x)$ keine reelle Lösung hat.

2. $2B = (\frac{1}{4}, \frac{15}{8})$

3. $R = A + B = (-2, 0)$

4. Nach dem Satz von Hasse müssen wir p so wählen, dass $p+1-2\sqrt{p} \geq 30$ gilt. Setzen wir $x = \sqrt{p}$, so folgt $x^2 - 2x - 29 \geq 0$. Die Nullstellen dieses Polynoms sind $1 \pm \sqrt{30}$ und die Ungleichung ist somit für alle $|x - 1| \geq \sqrt{30}$ erfüllt. Also muss in unserem Fall $\sqrt{p} \geq 1 + \sqrt{30}$ gelten, also $p \geq \lceil (1 + \sqrt{30})^2 \rceil = \lceil 31 + 2\sqrt{30} \rceil = 42$.

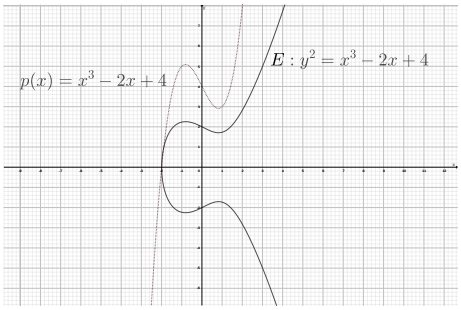

Abbildung 7.5: Die elliptische Kurve $E : y^2 = x^3 - 2x + 4$ und das kubische Polynom $p(x) = x^3 - 2x + 4$

5. a) $4a^3 + 27b^2 = 4 = 1 \neq 0 \pmod 3$
   b) Analog zu Beispiel 7.17 erhalten wir $\mathcal{E} = \{\mathcal{O}, (0,0), (2,1), (2,2)\}$. Die Ordnung (= Anzahl der Punkte) von $\mathcal{E}$ ist somit 4.
   c) Die Additionstabelle lautet (Formeln aus Definition 7.15 anwenden):

$+$	$\mathcal{O}$	$(0,0)$	$(2,1)$	$(2,2)$
$\mathcal{O}$	$\mathcal{O}$	$(0,0)$	$(2,1)$	$(2,2)$
$(0,0)$	$(0,0)$	$\mathcal{O}$	$(2,2)$	$(2,1)$
$(2,1)$	$(2,1)$	$(2,2)$	$(0,0)$	$\mathcal{O}$
$(2,2)$	$(2,2)$	$(2,1)$	$\mathcal{O}$	$(0,0)$

6. a) $|E| = 13$
   c) E ist zyklisch, da $|E| = 13$ prim.
   d) $p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$ liefert hier: $5.4 \leq 13 \leq 18.6$

7. a) Als Ordnung für P kommt nur 3 oder 9 in Frage. Wir berechnen $2P, 3P$. Da $3P \neq \mathcal{O}$, muss P die Ordnung 9 haben.
   b) Da es ein Element maximaler Ordnung (9) gibt.
   c) $\varphi(9) = (3^2 - 3^1) = 6$.

8. Hinweis: Betrachten Sie die Punkte in der Ebene als komplexe Zahlen! Wie transfomeirt man einen Kreis auf eine Ellipse?

Lösungen zu ausgewählten Aufgaben

1. $B = 2P = (\frac{9}{4}, \frac{19}{8})$
2. $A + B = (-\frac{152}{81}, \frac{107}{729})$
3. a) $R = 2P = (-2, -\sqrt{3})$
   b) $Q = -P$
4. a) $17P = 2(2(2(2(2 \cdot \mathcal{O} + P)))) + 1$ b) ...

5. a) $5, 6$ b) $5, 8$

6. –

7. Es gilt $\mathcal{E} = \{\mathcal{O}, (0,3), (0,4), (2,3), (2,4), (4,1), (4,6), (5,3), (5,4)\}$ und die Ordnung ist 9. Die Bedingung $4 \cdot 3^3 + 27 \cdot 2^2 = 6 \neq 0 \pmod 7$ ist erfüllt.

8. a) – b) $\mathcal{E}$ ist zyklisch c) $2P = (5,9)$; $3P = (8,8)$
   d) Verwende, dass $13P = \mathcal{O}$ (warum?)

9. a) $\mathcal{O}$ hat Ordnung 1; $(3,0)$ hat Ordnung 2; $(6,3)$ und $(6,4)$ haben Ordnung 4
   b) $\{\mathcal{O}\}$; $\{\mathcal{O}, (3,0)\}$; $\mathcal{E}$

10. $T = (3,5)$

11. $\{P \in \mathcal{E} | \text{ord}(P) = 2\} = \{(x,0) \in \mathcal{E} | x^3 + ax + b = 0\}$. Z.B. $x^3 + 2x$ über $\mathbb{Z}_3$.

12. –

13. Der Isomorphismus ist $\psi : \mathcal{E}_{D'} \to \mathbb{K}_D$, $(x,y) \mapsto (x, hy)$ mit $h^2 = D^{-1}D'$ und es gilt $|\mathcal{E}_D| + |\mathcal{E}| = 2(p+1)$ wenn $\left(\frac{D}{p}\right) = -1$.

14. –

15. –

16. a) $p = (\frac{1}{2})^n$
    b) –
    c) Erwartungswert: 16

17. a) Gammaverteilung $T_n \sim \mathcal{G}(n, \alpha)$.
    b) $P_1 = \frac{\gamma}{1+\gamma}$, $P_2 = \frac{\gamma^2(3+\gamma)}{(1+\gamma)^3}$, ...

Literatur

[BCWiki] *Bitcoin Wiki*. URL: https://en.bitcoin.it/wiki/ (besucht am 20. 02. 2018).

[Ber+08] D. J. Bernstein u. a. „Twisted Edwards Curves“. In: *Progress in Cryptology – AFRICACRYPT 2008*. Hrsg. von S. Vaudenay. Bd. 209. Lecture Notes in Comput. Sci. Berlin: Springer, 2008, S. 389–405. DOI: 10.1007/978-3-540-68164-9_26.

[CP05] R. Crandall und C. Pomerance. *Prime Numbers, A Computational Perspective*. 2. Aufl. New York: Springer, 2005.

[FIPS186-5] NIST. „Digital Signature Standard (DSS)“. In: *Federal Information Processing Standards Publication (FIPS)* 186-5 (2023). URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.

[For15] O. Forster. *Algorithmische Zahlentheorie*. 2. Aufl. Wiesbaden: Springer Spektrum, 2015.

[GP17] C. Grunspan und R. Perez-Marco. „The Mathematics Behind Bitcoin“. 2017. URL: https://webusers.imj-prg.fr/~ricardo.perez-marco/blockchain/BitcoinP7.pdf (besucht am 19. 02. 2018).

[KM15] N. Koblitz und A. J. Menezes. „A Riddle wrapped in an enigma“. In: *Cryptology ePrint Archive Listing 2015/1018* (Aug. 2015). URL: https://eprint.iacr.org/2015/1018.pdf.

[Kob87] N. Koblitz. „Elliptic curve cryptosystems“. In: *Math. Comp.* 48.177 (1987), S. 203–209. URL: https://doi.org/10.2307/2007884.

[Kob93] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. 2. Aufl. New York: Springer, 1993.

[Men01] A. Menezes. *Evaluation of Security Level of Cryptography: The Elliptic Curve Discrete Logarithm Problem (ECDLP)*. Techn. Ber. 2001. URL: https://www.cryptrec.go.jp/exreport/cryptrec-ex-1028-2001.pdf.

[Mil86] V. S. Miller. „Use of elliptic curves in cryptography“. In: *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*. Bd. 218. Lecture Notes in Comput. Sci. Springer, Berlin, 1986, S. 417–426. URL: https://doi.org/10.1007/3-540-39799-X_31.

[NSA09] National Security Agency. *The Case for Elliptic Curve Cryptography*. 2009. URL: http://web.archive.org/web/20150627183730/https://www.nsa.gov/business/programs/elliptic_curve.shtml (besucht am 27. 06. 2015).

[NSA15] National Security Agency. *Cryptography Today*. URL: https://web.archive.org/web/20151123081120/https://www.nsa.gov/ia/programs/suiteb_cryptography (besucht am 23. 11. 2015).

[Sat08] N. Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Techn. Ber. 2008. URL: https://bitcoin.org/bitcoin.pdf.

[She17] T. R. Shemanske. *Modern Cryptography and Elliptic Curves*. Bd. 83. Student Mathematical Library. A beginner's guide. Providence, RI: American Mathematical Society, 2017, S. xii+250.