Lauschen zwecklos!

Teilnehmer:

Andrea Birth	Andreas-Oberschule
Nikolai Bobenko	Herder-Oberschule
Jonas Gätjen	Immanuel-Kant-Oberschule
Holger Hesse	Heinrich-Hertz-Oberschule
Julian Risch	Heinrich-Hertz-Oberschule
Sophie Spirkl	Evangelische Schule Frohnau

Gruppenleiter:

Jürg Kramer	Humboldt-Universität zu Berlin, Mitglied im DFG-Forschungszentrum MATHEON „Mathematik für Schlüsseltechnologien“
Anna v. Pippich	Humboldt-Universität zu Berlin, Mitglied im DFG-Forschungszentrum MATHEON „Mathematik für Schlüsseltechnologien“

Abhörsicheres Telefonieren mit dem Mobiltelefon oder die Sicherheit beim Einsatz von Chipkarten sind zwei von unzähligen Beispielen aus dem Alltagsleben, bei denen das sichere Verschlüsseln von Daten eine entscheidende Rolle spielt. Dabei sollte das Verschlüsseln dieser Daten so clever sein, dass ein Abhören durch Unbefugte wertlos ist, also: Lauschen zwecklos! Dies ist mit Mathematik möglich.
In unserem Sommerschul-Kurs haben wir ein 350 Jahre altes Resultat aus der Zahlentheorie hergeleitet, welches für das 1977 von R. Rivest, A. Shamir und L. Adleman erfundene Verschlüsselungsverfahren, das sogenannte *RSA-Verfahren*, die Grundlage bildet. Dies ist ein asymmetrisches Verschlüsselungsverfahren, das zwei verschiedene Schlüssel zum Ver- und Entschlüsseln verwendet. Weiter haben wir uns mit dem sogenannten *Faktorisierungsproblem* beschäftigt, auf welchem die Sicherheit des RSA-Verfahren beruht.
Ein moderneres Verfahren, das bei gleicher Sicherheitsleistung eine geringere Schlüssellänge benötigt, benutzt *elliptische Kurven*. Dabei verstehen wir unter einer elliptische Kurve eine kubische Kurve, die durch eine Gleichung der Form $y^2 = x^3 + a \cdot x^2 + b \cdot x + c$ mit $a, b, c \in \mathbb{Q}$ gegeben ist. Wir haben untersucht, wie elliptische Kurven zur Verschlüsselung herangezogen werden können. Schließlich haben wir die von uns erarbeiteten Verschlüsselungsverfahren programmiert.

1 Zahlentheoretische Grundlagen

1.1 Der größte gemeinsame Teiler

Definition 1.1. Die natürliche Zahl $d \in \mathbb{N}$ heißt größter gemeinsamer Teiler von $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$, falls gilt:

(1) $d|a$ und $d|b$;

(2) Für alle $c \in \mathbb{Z}$ mit $c|a$ und $c|b$ gilt auch $c|d$.

Bezeichnung. (a, b):= größter gemeinsamer Teiler von a und b.

Beispiel. Die Zahlen $a = 30$ und $b = 12$ haben die gemeinsamen Teiler $1, 2, 3$ und 6. Weiter gilt $1|6$, $2|6$, $3|6$ und $6|6$. Damit ist der größte gemeinsame Teiler von 30 und 12 gleich $(a, b) = (30, 12) = 6$.

1.2 Euklidischer Algorithmus

Normalerweise liefert die Primfaktorenzerlegung der Zahlen a und b auf einfache Weise den größten gemeinsamen Teiler. Zum Beispiel erhalten wir mit Hilfe der eindeutigen Zerlegungen $a = 30 = 2 \cdot 3 \cdot 5$ und $b = 12 = 2 \cdot 2 \cdot 3$ sofort den größten gemeinsamen Teiler $(a, b) = (30, 12) = 2 \cdot 3 = 6$.
Dieses Verfahren ist jedoch für große Zahlen für den Computer sehr aufwendig zu berechnen. Deshalb führen wir den Euklidischen Algorithmus ein.

Satz 1.1 (Euklidischer Algorithmus)**.** *Seien $a, b \in \mathbb{Z}$ mit $a > b$ und $b \neq 0$. Wir betrachten dann die fortgesetzte Division mit Rest, welche zu dem Schema*

$$\begin{aligned}
a &= q_1 \cdot b + r_1 && (0 < r_1 < |b|)\\
b &= q_2 \cdot r_1 + r_2 && (0 < r_2 < r_1)\\
r_1 &= q_3 \cdot r_2 + r_3 && (0 < r_3 < r_2)\\
&\vdots\\
r_{n-2} &= q_n \cdot r_{n-1} + r_n && (0 < r_n < r_{n-1})\\
r_{n-1} &= q_{n+1} \cdot r_n + 0
\end{aligned}$$

führt. Dieses Verfahren bricht nach endlich vielen Schritten ab, d.h. es findet sich ein $n \in \mathbb{N}$ derart, dass $r_{n+1} = 0$ ist. Überdies ist der letzte nicht verschwindende Rest r_n ein größter gemeinsamer Teiler von a und b, d.h. es gilt

$$(a, b) = r_n.$$

Beweis. Da es nur endlich viele natürliche Zahlen $r_1, \ldots, r_n$ mit

$$0 \leq r_n < \ldots < r_2 < r_1 < |b|$$

gibt, ist klar, dass die fortgesetzte Division mit Rest nach endlich vielen Schritten abbrechen muss. Sei r_n der letzte nicht verschwindende Rest. Wir zeigen zunächst, dass r_n die Eigenschaft (1) aus Definition 1.1 besitzt, wobei wir die Gleichheiten des obigen Schemas benutzen. Auf Grund der letzten Gleichung $r_{n-1} = q_{n+1} \cdot r_n$ dieses Schemas gilt

$$r_n | r_{n-1}. \tag{1.1}$$

Wegen $r_{n-2} = q_n \cdot r_{n-1} + r_n$ folgt mit (1.1), dass auch

$$r_n | r_{n-2}$$

gilt. Durch Fortsetzung dieses Verfahrens können wir damit sukzessiv die Eigenschaft (1) aus Definition 1.1 für r_n beweisen.
Nun zeigen wir, dass r_n die Eigenschaft (2) aus Definition 1.1 besitzt. Dazu beweisen wir, dass es $x, y \in \mathbb{Z}$ gibt, so dass

$$r_n = x \cdot a + y \cdot b \tag{1.2}$$

gilt. Dazu rollen wir das Schema der fortgesetzten Division mit Rest aus Satz 1.1 wie folgt rückwärts auf

$$\begin{aligned}
r_n &= r_{n-2} - q_n \cdot r_{n-1} \\
r_n &= r_{n-2} - q_n \cdot (r_{n-3} - q_{n-1} \cdot r_{n-2}) \\
&= r_{n-2} \cdot (1 + q_n \cdot q_{n-1}) - r_{n-3} \cdot q_n \\
r_n &= (r_{n-4} - q_{n-2} \cdot r_{n-3}) \cdot (1 + q_n \cdot q_{n-1}) - r_{n-3} \cdot q_n \\
&= r_{n-4} \cdot (1 + q_n \cdot q_{n-1}) - r_{n-3} \cdot (q_{n-2} + q_n \cdot q_{n-1} \cdot q_{n-2} - q_n) \\
&\vdots \\
r_n &= x \cdot a + y \cdot b
\end{aligned}$$

mit ganzen Zahlen $x, y \in \mathbb{Z}$, was (1.2) beweist. Sei nun $c \in \mathbb{Z}$ mit $c|a$ und $c|b$. Dann gilt auch

$$c | (x \cdot a + y \cdot b)$$

und somit wegen der Gleichheit (1.2) auch $c|r_n$. Insgesamt erhalten wir somit

$$(a, b) = r_n,$$

wie behauptet. □

Hierbei haben wir auch den für das Folgende wichtigen Satz bewiesen.

Satz 1.2 (Erweiterter Euklidischer Algorithmus)**.** *Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann gibt es $x, y \in \mathbb{Z}$, so dass gilt:*

$$(a, b) = x \cdot a + y \cdot b.$$

Sind speziell a und b teilerfremd, dann gilt

$$1 = x \cdot a + y \cdot b.$$

Beispiel. Für $a = 925$ und $b = 65$ berechnen wir

$$\begin{aligned} 925 &= 14 \cdot 65 + 15 \\ 65 &= 4 \cdot 15 + 5 \\ 15 &= 3 \cdot 5. \end{aligned}$$

Damit folgt, dass

$$(925, 65) = 5$$

gilt. Rollen wir das obige Schema rückwärts auf, erhalten wir

$$\begin{aligned} 5 &= 65 - 4 \cdot 15 \\ 5 &= 65 - 4 \cdot (925 - 14 \cdot 65) \\ 5 &= -4 \cdot 925 + 57 \cdot 65. \end{aligned}$$

Damit gilt

$$(925, 65) = -4 \cdot 925 + 57 \cdot 65.$$

1.3 Rechnen modulo p

Definition 1.2. Für a, $b \in \mathbb{Z}$ und eine natürliche Zahl $m > 0$ definieren wir die Operationen $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ und $\odot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ gemäß

$$\begin{aligned} a \oplus b &= R_m(a + b), \\ a \odot b &= R_m(a \cdot b); \end{aligned}$$

hierbei bezeichnet $R_m(n)$ den Rest der ganzen Zahl n nach Division durch m.

Beispiel. Ist $m = 5$, so gelten für $a = 5$ und $b = 3$ die Gleichheiten

$$\begin{aligned} 5 \oplus 3 &= R_5(5 + 3) = 3, \\ 5 \odot 3 &= R_5(5 \cdot 3) = 0. \end{aligned}$$

Definition 1.3. Wir definieren

$$a \equiv b \mod m \iff R_m(a) = R_m(b),$$

in Worten: a heißt kongruent zu b modulo m, genau dann, wenn a und b nach Division durch m den gleichen Rest lassen.

Beispiel. Ist $m = 5$, so gilt für $a = 17$ und $b = 7$ die Äquivalenz

$$17 \equiv 7 \mod 5 \iff R_5(17) = 2 = R_5(7),$$

d.h. 17 ist kongruent zu 7 modulo 5.

Bemerkung. Man kann bei einer Kongruenz modulo m fast wie bei echter Gleichheit rechnen. Zum Beispiel gilt für $a \equiv b \mod m$ und $c \equiv d \mod m$:

$$(1)\ a \pm c \equiv b \pm d \mod m,$$
$$(2)\ a \cdot c \equiv b \cdot d \mod m.$$

Beispiel. Wir erklären nun an Hand eines Beispiels, dass man die Gleichung

$$a \cdot x \equiv 1 \mod m,$$

modulo m lösen kann, d.h. wir suchen nach einer Lösung $x \in \mathbb{N}$ mit $0 \leq x < m$, vorausgesetzt, dass $(a, m) = 1$ ist. Dies ist grundlegend für die folgenden Kapitel. Sei dazu $a = 23$ und $m = 56$. Dann gilt

$$\begin{aligned} & 23 \cdot x \equiv 1 \mod 56 \\ \iff \quad & 23 \cdot x + y \cdot 56 \equiv 1 \mod 56, \end{aligned}$$

wobei $y \in \mathbb{Z}$ beliebig ist. Nun wird der Euklidische Algorithmus angewendet.

$$\begin{aligned} 56 &= 2 \cdot 23 + 10 \\ 23 &= 2 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Nun rollen wir den Euklidischen Algorithmus rückwärts auf.

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 \\ 1 &= 10 - 3 \cdot (23 - 2 \cdot 10) \\ 1 &= 10 - 3 \cdot 23 + 6 \cdot 10 \\ 1 &= (56 - 2 \cdot 23) - 3 \cdot 23 + 6 \cdot (56 - 2 \cdot 23) \\ 1 &= 7 \cdot 56 - 17 \cdot 23. \end{aligned}$$

Damit gilt

$$\begin{aligned} & 23 \cdot (-17) + 7 \cdot 56 \equiv 1 \mod 56 \\ \iff \quad & 23 \cdot (-17) + 23 \cdot 56 \equiv 1 \mod 56 \\ \iff \quad & 23 \cdot (-17 + 56) \equiv 1 \mod 56 \\ \iff \quad & 23 \cdot 39 \equiv 1 \mod 56. \end{aligned}$$

Damit ist $x = 39$ eine Lösung der Gleichung $23 \cdot x \equiv 1 \mod 56$ mit $0 \leq x < 56$.

Bemerkung. Im Folgenden bezeichnen wir die Zahl $x \in \mathbb{N}$ mit $0 \leq x < m$ und $a \cdot x \equiv 1 \mod m$ mit dem Symbol a^{-1}.

Bemerkung. Ist p eine Primzahl, dann ist die Menge $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ der Reste modulo p ein Körper mit p Elementen.

1.4 Die Sätze von Fermat und Euler

Satz 1.3 (Satz von Fermat)**.** *Es sei p eine Primzahl. Dann gilt für alle $a \in \mathbb{Z}$, die nicht Vielfache von p sind:*

$$a^{p-1} \equiv 1 \mod p.$$

Beweis. Es sei nun p eine Primzahl und $a \in \mathbb{N}$ kein Vielfaches von p. Zunächst bemerken wir, dass sich die Vielfachen

$$a, 2a, 3a, \ldots, (p-1)a$$

bis auf die Reihenfolge als

$$1 + k_1 p, 2 + k_2 p, 3 + k_3 p, \ldots, (p-1) + k_{p-1} p$$

darstellen lassen, wobei $k_1, \ldots k_{p-1} \in \mathbb{N}$ sind. Bilden wir das Produkt dieser Vielfachen, erhalten wir somit die Gleichheit

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a = (1 + k_1 p) \cdot (2 + k_2 p) \cdot (3 + k_3 p) \cdot \ldots \cdot (p - 1 + k_{p-1} p),$$

welche man für ein $l \in \mathbb{Z}$ in der folgenden Form schreiben kann

$$\begin{aligned} & (p-1)! \cdot a^{p-1} = (p-1)! + l \cdot p \\ \iff & (p-1)! \cdot a^{p-1} \equiv (p-1)! \mod p. \end{aligned} \tag{1.3}$$

Wegen $((p-1)!, p) = 1$ gibt es nach dem Satz vom erweiterten Euklidischen Algorithmus zwei Zahlen $x, y \in \mathbb{Z}$ mit $1 = x \cdot (p-1)! + y \cdot p$, d.h. mit

$$x \cdot (p-1)! \equiv 1 \mod p. \tag{1.4}$$

Multiplizieren wir nun (1.3) mit x, so erhalten wir wegen (1.4) die Äquivalenz

$$\begin{aligned} & x \cdot (p-1)! \cdot a^{p-1} \equiv x \cdot (p-1)! \mod p \\ \iff & a^{p-1} \equiv 1 \mod p. \end{aligned}$$

Dies beweist die Behauptung. □

Der Schweizer Mathematiker Euler hat den kleinen Satz von Fermat wie folgt verallgemeinert.

Satz 1.4 (Satz von Euler)**.** *Seien p, q verschiedene Primzahlen, $m = p \cdot q$ und $n = (p-1)(q-1)$. Dann gilt für alle $a \in \mathbb{Z}$, die teilerfremd zu m sind:*

$$a^n = a^{(p-1)(q-1)} \equiv 1 \mod m.$$

Bemerkung. Es ist möglich, den Beweis analog zum Beweis des Satzes von Fermat zu führen. Wir verzichten allerdings darauf, den Beweis hier anzugeben.

2 Das RSA-Verfahren

Im folgenden Abschnitt wird gezeigt, wie das RSA-Verfahren funktioniert, und es wird bewiesen, dass es korrekt ist, d.h. dass der Empfänger die Nachricht des Senders immer richtig liest. Dieses Verfahren ist ein Public-Key-Kryptosystem, bei dem asymmetrisch chiffriert wird, das bedeutet, dass Absender A und Empfänger B verschiedene Schlüssel benutzen. Hierbei müssen sich A und B weder kennen, noch sich zu einem Schlüsselaustausch treffen.

Bevor der Austausch der Nachricht erfolgen kann, müssen folgende Vorbereitungen erfolgen: Der Empfänger B wählt zwei „große“ Primzahlen, d.h. zur Zeit etwa 200-stellige Primzahlen p und q, welche geheim gehalten werden müssen. Daraufhin berechnet er $m = p \cdot q$. Nun bestimmt B eine natürliche Zahl k, die zu $n = (p-1) \cdot (q-1)$ teilerfremd ist. Die Zahlen m und k bilden den öffentlichen Schlüssel, d.h. sie werden öffentlich an A übermittelt.

Der Absender A wandelt nun seine zu übermittelnde Nachricht in eine natürliche Zahl a $(1 < a < m)$ um, z.B. mit Hilfe des ASCII-Codes. Danach verschlüsselt A die Nachricht a als

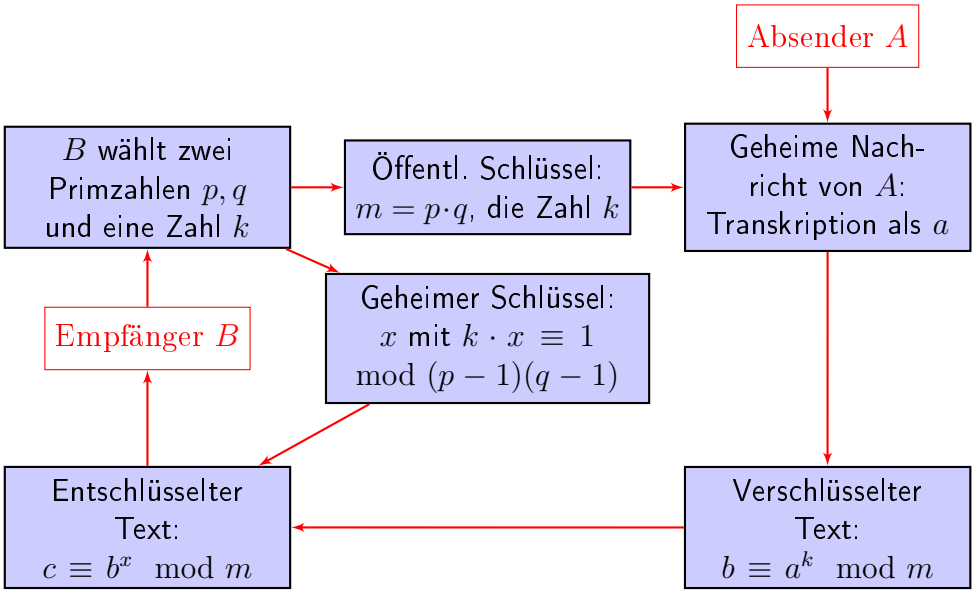
$$b \equiv a^k \mod m$$

und sendet b öffentlich an B.

Damit der Empfänger B die Nachricht von A entschlüsseln kann, muss er zunächst eine ganze Zahl x bestimmt, die die Kongruenz $k \cdot x \equiv 1 \mod n$ erfüllt. Mit dem so gewonnenen geheimen Schlüssel x berechnet er

$$c \equiv b^x \mod m.$$

Damit ist die Nachricht entschlüsselt, denn es gilt $c = a$.



Nun wird gezeigt, dass das RSA-Verfahren korrekt ist. Dazu formulieren wir folgenden Satz:

Satz 2.1. *Seien p, q verschiedene Primzahlen und k eine natürliche Zahl, die zu $n = (p-1) \cdot (q-1)$ teilerfremd ist. Desweiteren seien a, b, c, m und x Zahlen entsprechend dem oben beschriebenen Vorgehen. Dann gilt $a \equiv c \mod m$.*

Beweis. Aus $b \equiv a^k \mod m$ und $c \equiv b^x \mod m$ folgt

$$c \equiv (a^k)^x \equiv a^{kx} \mod m.$$

Da $kx \equiv 1 \mod n$ mit $n = (p-1) \cdot (q-1)$, existiert ein $y \in \mathbb{Z}$ mit

$$kx = 1 + yn.$$

Damit ergibt sich $a^{kx} = a^{1+yn} = a \cdot a^{yn} = a \cdot (a^n)^y$ und somit

$$c \equiv a \cdot (a^n)^y \mod m.$$

Da a teilerfremd zu $m = p \cdot q$ ist, gilt nach Satz 1.4, dem Satz von Euler, dass $a^n \equiv 1 \mod m$ gilt und damit

$$c \equiv a \cdot (a^n)^y \equiv a \cdot 1^y \equiv a \mod m,$$

d.h. $a \equiv c \mod m$, wie behauptet. □

Beispiel. Zum besseren Verständnis betrachten wir ein kleines Beispiel. Der Empfänger B wählt die Primzahlen $p = 229$ und $q = 389$. Damit erhält er

$$n = (p-1) \cdot (q-1) = 228 \cdot 389 = 88464.$$

Nun wählt B beispielsweise $k = 43$. Da 43 eine Primzahl ist und n kein Vielfaches von 43 ist, ist k teilerfremd zu n, wie gewünscht. B gibt nun die Zahlen

$$\begin{aligned} m &= p \cdot q = 229 \cdot 389 = 89081, \\ k &= 43 \end{aligned}$$

öffentlich bekannt. Der Absender A transkribiert die Nachricht „PI“ mit Hilfe des ASCII-Codes als $a = 8073$ und übermittelt die verschlüsselte Nachricht

$$b \equiv 8073^{43} \equiv 30783 \mod 89081.$$

Wärenddessen bestimmt B den geheimen Schlüssel x, indem er die Gleichung $k \cdot x \equiv 1 \mod n$ löst. So erhält er die Lösung

$$x = 67891.$$

Nun kann der Empfänger B die Nachricht entschlüsseln, indem er $c \equiv b^x \mod m$ berechnet; er erhält $c \equiv 30783^{67891} \equiv 8073 \mod 89081$, also die Nachricht „PI“.

Beispiel. Nun ein etwas realistischeres Beispiel. Der Empfänger B wählt die Primzahlen

$$\begin{aligned} p &= 153249554086588885835834702715030918361873935752883763 3, \\ q &= 153249554086588885835834702715030918361897446794836651 3. \end{aligned}$$

Damit erhält er

$$\begin{aligned} n &= (p-1)(q-1) \\ &= 234854258277383322788948059678933702737604357590890678 8 \\ &\quad 406607163597747756552746892633980748733486828474179584. \end{aligned}$$

Nun wählt B wieder $k = 43$. Da 43 eine Primzahl ist und n kein Vielfaches von 43 ist, ist k teilerfremd zu n, wie gewünscht. B gibt nun die Zahlen

$$\begin{aligned} m &= p \cdot q \\ &= 234854258277383322788948059678933702737604357590890679 1 \\ &\quad 471598245329525473269440946934599115971200653951383729, \\ k &= 43 \end{aligned}$$

öffentlich bekannt. Der Absender A transkribiert die Nachricht „MATHEMATIK“ mit Hilfe des ASCII-Code als

$$a = 77658472697765847375$$

und übermittelt die verschlüsselte Nachricht

$$\begin{aligned} b &\equiv 77658472697765847375^{43} \\ &\equiv 217819882953579407544224571425479958308096036559243448 \\ &\quad 980351224602119873496097431290450386913902399435406279 \mod m. \end{aligned}$$

Währenddessen bestimmt B den geheimen Schlüssel x, indem er die Gleichung $k \cdot x \equiv 1 \mod n$ löst. So erhält er

$$\begin{aligned} x &= 491555424301499977930356403979163563869404469376282816 \\ &\quad 178127080753016972301737721714088993920962359448084099. \end{aligned}$$

Nun kann der Empfänger B die Nachricht entschlüsseln, indem er $c \equiv b^x \mod m$ bestimmt; er erhält

$$c \equiv 77658472697765847375 \mod m,$$

also wieder die Nachricht „MATHEMATIK“.

Die Sicherheit des RSA-Verfahrens beruht auf dem Faktorisierungsproblem. Da bisher kein Algorithmus zur Faktorisierung großer Zahlen allgemein bekannt ist, kann eine Person C, die die Kommunikation mitschreibt und somit die Zahlen m, k und b erhält, die Nachricht nicht entschlüsseln, da sie dafür m in seine Primfaktoren p und q zerlegen muss, um n und dann x, den Schlüssel, den sie zum Entschlüsseln benötigt, zu berechnen. Da sich die Leistung der Computer nach dem Mooreschen Gesetz, welches laut Intel bis 2029 Bestand haben soll, ständig verbessert und man somit immer größere Zahlen in annehmbarer Zeit zerlegen kann und dadurch auch früher abgefangene Nachrichten leichter lesen kann, werden zur Verschlüsselung meist sehr viel höhere Primzahlen als eigentlich nötig wären benutzt. In Kapitel 4 haben wir uns mit verschiedenen Faktorisierungsmethoden beschäftigt.

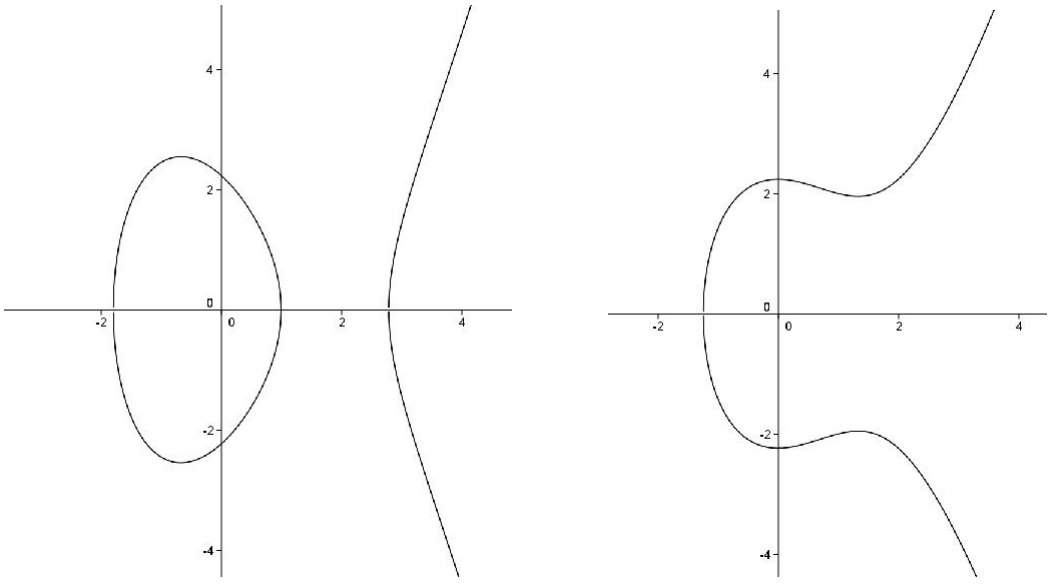
3 Elliptische Kurven

3.1 Definition

Definition 3.1. Eine kubische Kurve C, die durch die Gleichung

$$y^2 = x^3 + a \cdot x^2 + b \cdot x + c \tag{3.1}$$

festgelegt ist, heißt elliptische Kurve, falls das kubische Polynom auf der rechten Seite drei verschiedene Nullstellen hat (zwei dieser Nullstellen können auch komplex sein). Falls die Koeffizienten a, b, c rationale Zahlen sind, sagen wir, dass die elliptische Kurve C über den rationalen Zahlen $\mathbb{Q}$ definiert ist.



3.2 Gruppenstruktur

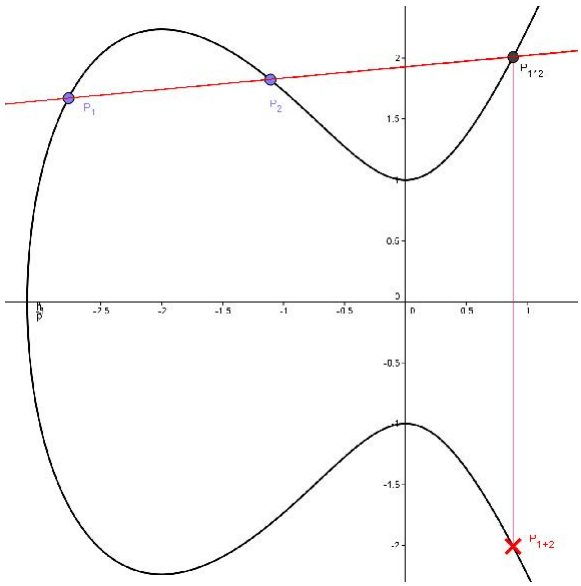
Definition 3.2. Die Menge der rationalen Punkte der elliptischen Kurve (3.5) ist gegeben durch die Menge

$$C(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \,|\, y^2 = x^3 + a \cdot x^2 + b \cdot x + c\} \cup \{O\},$$

wobei O der unendlich ferne Punkt mit den Koordinaten (∞, ∞) ist; dieser ist von allen anderen Punkten der Kurve unendlich weit entfernt und, wenn man sich von einem Punkt in eine beliebige Richtung unendlich weit weg bewegt, dann landet man im unendlich fernen Punkt.

Die Besonderheit der Menge der rationalen Punkte $C(\mathbb{Q})$ liegt in der Existenz einer additiven Struktur, wodurch diese Menge zu einer abelschen Gruppe wird.

Nun zeigen wir, dass die Menge der rationalen Punkte $C(\mathbb{Q})$ zusammen mit einer von uns noch zu definierenden Operation $+$ eine abelsche Gruppe bildet. Um diese Addition zweier Punkte $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$ zu definieren, wird als erstes eine Gerade an diese beiden Punkte angelegt. Es entsteht immer ein dritter Schnittpunkt mit der elliptischen Kurve; diesen nennen wir $T = (x_T, y_T)$. Die Summe $R := P + Q$ von P und Q erhält man geometrisch, wenn der eben ermittelte Punkt T an der x-Achse gespiegelt wird, d.h. die Koordinaten (x_R, y_R) von $R = P + Q$ sind gegeben durch $x_R = x_T$ und $y_R = -y_T$.



Um mit algebraischen Methoden auf die Koordinaten des Punktes T zu kommen, betrachten wir die Gerade

$$y = \lambda x + \nu \tag{3.2}$$

mit Steigung λ und Achsenabschnitt ν, welche durch die Formeln

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \quad \text{und} \quad \nu = y_P - \lambda x_P = y_Q - \lambda x_Q$$

gegeben sind. Nun setzt man die Geradengleichung (3.2) in die Gleichung der elliptischen Kurve (3.5) ein. Es ergibt sich eine Polynomgleichung vom Grad 3 in x, welche x_P und x_Q als Nullstellen besitzt. Mit Hilfe des Vietaschen Wurzelsatzes lässt sich dann x_T berechnen. Wir haben nämlich:

$$\begin{aligned}(\lambda x + \nu)^2 = y^2 = x^3 + a \cdot x^2 + b \cdot x + c, \text{ d.h.}\\ x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0.\end{aligned}$$

Der Vietasche Wurzelsatz für letztere kubische Gleichung besagt, dass die Summe der drei Nullstellen gleich (-1) mal der Koeffizient des quadratischen Terms ist, d.h.

$$\begin{aligned}x_P + x_Q + x_T = -(a - \lambda^2), \text{ d.h.}\\ x_T = \lambda^2 - a - x_P - x_Q.\end{aligned} \tag{3.3}$$

Die y-Koordinate y_T von T berechnet sich wie folgt. Man setzt (3.3) in (3.2) ein und erhält

$$y_T = \lambda x_T + \nu. \tag{3.4}$$

Nach Spiegelung an der x-Achse ergeben sich die Koordinaten von $R = P + Q$ zu (x_R, y_R) mit $x_R = x_T$ und $y_R = -y_T$.

Ein Spezialfall stellt die Addition eines Punktes $P = (x_P, y_P)$ mit sich selbst, also die Verdoppelung dar, weil hierbei die Tangente in P angelegt wird, deren zweiter Schnittpunkt mit der elliptischen Kurve T ist. Wenn man diesen so erhaltenen Punkt spiegelt, ergibt sich die Summe $P + P = 2P$. Hierbei wird die Steigung der Tangente an P durch

$$\left.\frac{dy}{dx}\right|_{(x,y)=(x_P,y_P)} = \frac{f'(x_P)}{2y_P}$$

gegeben.

Satz 3.1. *Die Menge der rationalen Punkte $C(\mathbb{Q})$ der elliptischen Kurve* (3.5) *bildet zusammen mit der oben definierten Addition $+$ eine abelsche Gruppe.*

Beweis. Die Tatsache, dass bei der Addition $+$ zweier beliebiger Punkte aus der Menge der rationalen Punkte einer elliptischen Kurve, die Summe wieder durch einen rationalen Punkt repräsentiert wird, ist aus der Gleichung (3.3) ersichtlich: Da sowohl die Steigung λ, der Koeffizient vor dem quadratischen Teil, sowie die

x-Koordinaten der Punkte P und Q rational sind, muss auch x_R rational sein. Daraus folgt, dass auch y_R rational ist und es sich bei der Summe um einen rationalen Punkt handelt. Somit ist $(C(\mathbb{Q}), +)$ abgeschlossen.
Auf den Beweis der Assoziativität der Operation + soll hier verzichtet werden. Durch dynamische Geometriesoftware kann diese jedoch veranschaulicht werden.
Das neutrale Element bezüglich der Operation + ist der unendlich ferne Punkt O, da für alle Punkte P in $C(\mathbb{Q})$ die Gleichung $P + O = P = O + P$ gilt.
Das inverse Element bezüglich der Operation + für den Punkt $P = (x_P, y_P)$ ist der Punkt $-P := (x_P, -y_P)$, da $P + (-P) = O = (-P) + P$ für alle P in $C(\mathbb{Q})$ gilt.
Wie aus den Gleichungen schließlich ersichtlich ist, gilt auch das Kommutativgesetz für $(C(\mathbb{Q}), +)$, da es irrelevant ist, ob man $P + Q$ oder $Q + P$ berechnet, das Ergebnis ist gleich.

3.3 Elliptische Kurven über endlichen Körpern

Unser Ziel ist es, elliptische Kurven in kryptographischen Verfahren einzusetzen. Dafür muss das Ergebnis der Entschlüsselung eines zuvor verschlüsselten Textes eindeutig sein. Dazu bietet sich das Rechnen mit elliptischen Kurven modulo p an. Wir führen dazu den Körper mit p Elementen ein.

Der endliche Körper $\mathbb{F}_p$ wird als Menge dargestellt durch die Zahlen $\{0, \ldots, p-1\}$, wobei p eine Primzahl ist. Addition, Subtraktion und Multiplikation werden dabei modulo p gerechnet, wie es im Abschnitt 1.3 beschrieben wurde; die Division durch von 0 verschiedene Zahlen wird auch wie im Abschnitt 1.3 vorgestellt mit Hilfe des Erweiterten Euklidischen Algorithmus durchgeführt.

Eine elliptische Kurve C über dem endlichen Körper $\mathbb{F}_p$ wird durch die Kongruenz

$$y^2 \equiv x^3 + a \cdot x^2 + b \cdot x + c \mod p \tag{3.5}$$

definiert, wobei das kubische Polynom rechter Hand drei verschiedene Nullstellen modulo p haben muss; die Koeffizienten a, b, c sind hierbei im Körper $\mathbb{F}_p$ zu wählen. Die $\mathbb{F}_p$-rationalen Punkte von C sind gegeben durch die Menge

$$C(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 \,|\, y^2 \equiv x^3 + a \cdot x^2 + b \cdot x + c \mod p\} \cup \{O\}.$$

Beispiel. Wir betrachten die elliptische Kurve C über dem Körper $\mathbb{F}_{23}$, welche durch die Kongruenz

$$y^2 \equiv x^3 + x \mod 23$$

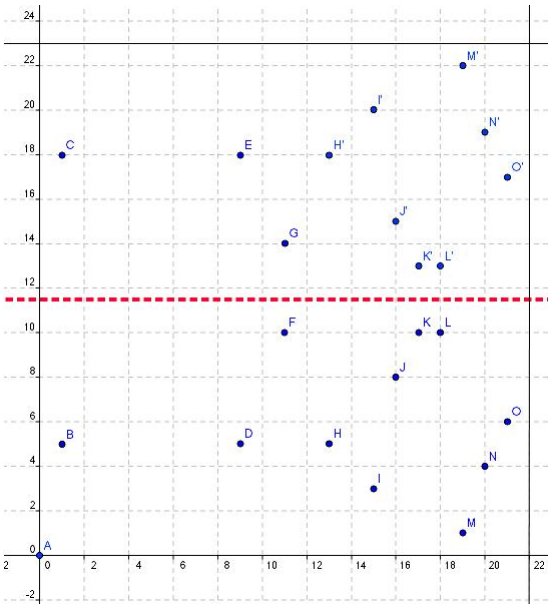
gegeben ist. Die Menge der $\mathbb{F}_{23}$-rationalen Punkte ist gegeben durch

$$\begin{aligned} C(\mathbb{F}_{23}) = \{&O, (0,0), (1,5), (1,18), (9,5), (9,18), (11,10), (11,13), (13,5), \\ &(13,18), (15,3), (15,20), (16,8), (16,15), (17,10), (17,13), (18,10), \\ &(18,13), (19,1), (19,22), (20,4), (20,19), (21,6), (21,17)\}. \end{aligned}$$

Beispielsweise gilt $(9,5) \in C(\mathbb{F}_{23})$, da

$$5^2 \equiv 25 \equiv 738 \equiv 9^3 + 9 \mod 23$$

gilt.



Der Graphik kann man entnehmen, dass auch über dem Körper $\mathbb{F}_p$ eine Achsensymmetrie besteht.

Analog den über den rationalen Zahlen angestellten Betrachtungen wollen wir im folgenden auch die (endliche) Menge der $\mathbb{F}_p$-rationalen Punkte als abelsche Gruppe erkennen. Dazu adaptieren wir die für die Addition hergeleiteten Formeln (3.3) und (3.4) an das Rechnen auf elliptischen Kurven modulo p. Für die Koordinaten (x_R, y_R) der „Summe“ $R = P + Q$ der beiden Punkte $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$ mit $x_P \not\equiv x_Q \mod p$ gilt

$$x_R \equiv \lambda^2 - a - x_P - x_Q \mod p, \tag{3.6}$$
$$y_R \equiv -\lambda x_R - \nu \mod p, \tag{3.7}$$

wobei

$$\lambda \equiv (y_P - y_Q) \cdot (x_P - x_Q)^{-1} \mod p,$$
$$\nu \equiv y_P - \lambda x_P \mod p.$$

Der negative Punkt $-P$ eines Punktes $P = (x_P, y_P) \in C(\mathbb{F}_p)$ ist durch $-P = (x_P, -y_P)$ gegeben.

Für den Spezialfall, dass $x_P \equiv x_Q \mod p$ und $y_P \not\equiv y_Q \mod p$ gilt $P + Q = O$; andernfalls ziehen wir die Verdoppelungsformeln für den Punkt $P + P = 2P$ mit den Koordinaten (x_R, y_R) heran, d.h. wir verwenden die Formeln

$$x_R \equiv \lambda^2 - a - 2x_P \mod p, \tag{3.8}$$
$$y_R \equiv -\lambda x_R - \nu \mod p, \tag{3.9}$$

wobei

$$\lambda \equiv (3x_P^2 + 2ax_P + b) \cdot (2y_P)^{-1} \mod p,$$
$$\nu \equiv y_P - \lambda x_P \mod p.$$

3.4 Analogon zum Diffie-Hellman Schlüsselaustausch

Alice und Bob einigen sich auf einen Punkt Q einer elliptischen Kurve C über dem endlichen Körper $\mathbb{F}_p$. Nun wählt Alice im Geheimen ein n und schickt Bob den Punkt $A = n \cdot Q = Q + \ldots + Q \in C(\mathbb{F}_p)$ (Q wird n-mal zu sich selbst addiert). Analog dazu wählt Bob im Geheimen ein m und schickt Alice $B = m \cdot Q \in C(\mathbb{F}_p)$. Alice und Bob berechnen beide den geheimen Schlüssel

$$S := (n \cdot m) \cdot Q = n \cdot B = m \cdot A.$$

Auch wenn Charly Alice und Bob belauscht hat und somit A, B und Q kennt, kann er daraus nicht so einfach auf S, den geheimen Schlüssel, schließen. Das Problem für Charlie besteht darin, dass er zwar die Produkte $A = n \cdot Q$ und $B = m \cdot Q$, den Punkt Q und die Primzahl p kennt, daraus jedoch nicht so leicht auf m oder n schließen kann. Dies führt uns zum diskreten Logarithmus Problem:

Diskretes Logarithmus Problem für elliptische Kurven über $\mathbb{F}_p$:
Gegeben sind die Punkte $P, Q \in C(\mathbb{F}_p)$ mit der Eigenschaft $Q = k \cdot P$.
Gesucht ist k, welches der diskrete Logarithmus von Q zur Basis P genannt wird.

Diskretes Logarithmus Problem für die multiplikative Gruppe $\mathbb{F}_p^\times$:
Gegeben sind die zur Primzahl p teilerfremden ganzen Zahlen a, b mit der Eigenschaft $b \equiv a^k \mod p$.
Gesucht ist k, welches der diskrete Logarithmus von b zur Basis a genannt wird.

Es gibt bis heute noch keine schnellen Algorithmen zur Lösung dieses Problems. Eine Möglichkeit ist die Berechnung der Vielfachen von P, bis Q erreicht wird, bzw. der Potenzen von a, bis b erreicht wird. Einige der gegenwärtig existierenden Algorithmen sind: der Babystep-Giantstep-Algorithmus, der Pohlig-Hellman-Algorithmus, der Index-Calculus-Algorithmus und die Pollard-Rho-Methode. Diese sind jedoch aufgrund ihrer langen Rechenzeit nicht praxisrelevant.

4 Faktorisierung

Das Faktorisierungsproblem ist eine klassische Aufgabe aus der Zahlentheorie. Die Aufgabe lautet, zu einer gegebenen Zahl alle Primfaktoren zu ermitteln. Für große Zahlen ist diese Aufgabe nur schwer zu lösen, insbesondere, wenn es sich um sogenannte schwere Zahlen handelt, d.h. Zahlen, die nur große Primfaktoren besitzen. Beispielsweise benötigten 600 Mitarbeiter und 1600 Rechner für die Faktorisierung einer 129-stelligen Dezimalzahl im Jahr 1994 ganze acht Monate. Im diesem Kapitel wollen wir einige Methoden zur Faktorisierung vorstellen.

4.1 Faktorisierung nach Fermat

Satz 4.1. *Es sei n eine ungerade, positive, natürliche Zahl. Dann kann man n faktorisieren, indem man für $t = [\sqrt{n}] + 1, [\sqrt{n}] + 2, \ldots$ prüft, ob $t^2 - n$ eine Quadratzahl ist. Falls dem so ist, sind $t + \sqrt{t^2 - n}$ und $t - \sqrt{t^2 - n}$ Teiler von n.*

Beweis. Die Fermat-Faktorisierung beruht auf der zweiten bzw. dritten binomischen Formel. Es gilt nämlich

$$(t - \sqrt{t^2 - n})(t + \sqrt{t^2 - n}) = t^2 - (t^2 - n) = n.$$

□

Diese Methode funktioniert besonders gut, falls die Teiler von n relativ nahe beieinander liegen, da dann ihre Differenz, d.h.

$$(t + \sqrt{t^2 - n}) - (t - \sqrt{t^2 - n}) = 2\sqrt{t^2 - n},$$

relativ klein ist und somit $t^2 - n$ verhältnismäßig schnell als Quadratzahl erkannt wird, womit dann die gesuchte Faktorisierung gefunden ist.

4.2 Faktorisierung nach Pollard

Die Idee der Faktorisierung nach Pollard besteht darin, eine Zahl zu finden, die ein Vielfaches von einem Primteiler der vorgelegten natürlichen Zahl n ist, aber nicht von n selbst. Durch Bestimmung des größten gemeinsamen Teilers dieser Zahl mit n erhält man einen nichttrivialen Teiler von n. Indem man annimmt, dass n einen Primfaktor p besitzt, so dass $(p-1)$ relativ kleine Primfaktoren hat, kann man n mit der $(p-1)$-Methode nach Pollard wie folgt faktorisieren.

Algorithmus. Wir wählen zunächst ein beliebiges $B \in \mathbb{N}$ und ein dazu passendes $k \in \mathbb{N}$, so dass k ein Vielfaches aller natürlichen Zahlen kleiner gleich B ist.

Die Zahl k könnte beispielsweise als das Produkt aller echten Teiler von $(p-1)$ gewählt werden. Man hofft nun, dass $(p-1)|k$ gilt. Außerdem wählt man ein $a \in \mathbb{N}$ mit $2 \leq a \leq (n-2)$ und bestimmt $a^k \mod n$. Mit Hilfe des Euklidischen Algorithmus bestimmt man nun den größten gemeinsamen Teiler $(a^k - 1, n)$. Da aufgrund des Kleinen Satzes von Fermat wegen $(p-1)|k$ die Kongruenz

$$a^k \equiv 1 \mod p$$

besteht, ergibt sich $p|(a^k - 1)$. Da voraussetzungsgemäß $p|n$ gilt, folgt $p|(a^k - 1, n)$, d.h., falls nicht $a^k \equiv 1 \mod n$ ist, liefert diese Methode mit dem größten gemeinsamen Teiler $(a^k - 1, n)$ einen nichttrivialen Teiler von n.

4.3 Faktorisierung mit elliptischen Kurven

Im Jahr 1987 entwickelte H. W. Lenstra einen Faktorisierungsalgorithmus, welcher elliptische Kurven benutzt. Dieser ist von großer praktischer Bedeutung, weil er kleine Primfaktoren von n besonders schnell entdeckt.

In diesem Abschnitt sei n eine große natürliche Zahl, die nicht durch 2 und 3 teilbar ist und einen (noch unbekannten) Primfaktor $p > 3$ besitzt. Zuerst wählt man eine beliebige elliptische Kurve C, welche durch die Gleichung

$$y^2 = x^3 + b \cdot x + c$$

mit $b, c \in \mathbb{Z}$ gegeben ist, und einen beliebigen Punkt $P = (x_P, y_P) \in C(\mathbb{Q})$.

Da die Primzahl p unbekannt ist, kann die Kurve C nicht über dem endlichen Körper $\mathbb{F}_p$ betrachtet werden. Stattdessen rechnen wir modulo n, weswegen wir mit der folgenden Definition beginnen.

Definition 4.1 (Modulorechnung auf $\mathbb{Q}$)**.** Es seien $n \in \mathbb{N}$ und $x_1, x_2 \in \mathbb{Q}$, derart, dass die Nenner von x_1 und x_2 teilerfremd zu n sind, d.h., derart, dass sie keine echten gemeinsamen Teiler mit n besitzen. Dann schreiben wir

$$x_1 \equiv x_2 \mod n,$$

falls der Zähler des gekürzten Bruches $x_1 - x_2$ durch n teilbar ist.

Beispiel. Es sei $x_1 = 1/3$ und $x_2 = 11/5$. Für $n = 4$ gilt $(3, 4) = (5, 4) = 1$ und $x_1 - x_2 = 4/15$, also

$$\frac{1}{3} \equiv \frac{11}{5} \mod 4.$$

Satz 4.2 (Kleinster nicht-negativer Rest)**.** *Es sei n eine positive natürliche Zahl. Für alle $x \in \mathbb{Q}$ mit zu n teilerfremdem Nenner exisitiert genau ein $m \in \mathbb{N}$ mit $0 \leq m \leq (n-1)$ derart, dass*

$$x \equiv m \mod n \tag{4.1}$$

gilt.

Bezeichnung. Die eindeutige Zahl m aus Satz 4.2 wird als „kleinster nicht-negativer Rest“ von x modulo n oder kurz als $x \mod n$ bezeichnet.

Beweis. Existenz: Es sei r/q die gekürzte Bruchdarstellung von x; hierbei ist der Nenner q teilerfremd zu n. Wegen $(n, q) = 1$ existieren $a, b \in \mathbb{Z}$ mit

$$a \cdot n + b \cdot q = 1.$$

Multiplikation dieser Gleichung mit r und Umstellung liefert die Kongruenz

$$r - (b \cdot r) \cdot q \equiv 0 \mod n.$$

Indem wir nun $m \in \mathbb{N}$ mit $0 \leq m \leq (n-1)$ und $m \equiv b \cdot r \mod n$ wählen, erhalten wir die Kongruenz

$$r - m \cdot q \equiv 0 \mod n.$$

Wir haben

$$\frac{r}{q} - m = \frac{r - m \cdot q}{q};$$

diesen Bruch kann man nicht weiter kürzen, da $m \cdot q$ offensichtlich ein Vielfaches von q ist, r und q aber teilerfremd zueinander sind. Konstruktionsgemäß gilt für den Zähler $r - m \cdot q$ die Kongruenz

$$r - m \cdot q \equiv 0 \mod n,$$

womit der Existenzbeweis geführt ist.

Eindeutigkeit: Angenommen, es existieren verschiedene $m_1 \in \mathbb{N}$ und $m_2 \in \mathbb{N}$ mit $0 \leq m_1, m_2 \leq (n-1)$, welche (4.1) erfüllen, dann gilt mit $x = r/q$ wie oben:

$$\begin{aligned} & r - m_1 \cdot q \equiv r - m_2 \cdot q \mod n \\ \Leftrightarrow\, & r - m_1 \cdot q = r - m_2 \cdot q + \lambda \cdot n \\ \Leftrightarrow\, & m_2 - m_1 = \frac{\lambda \cdot n}{q} \end{aligned}$$

mit einem $\lambda \in \mathbb{Z}$. Da m_1 und m_2 natürliche Zahlen, und n und q teilerfremd sind, muss also λ ein Vielfaches von q sein, d.h. $|m_2 - m_1| \geq n$, im Widerspruch zu $0 \leq m_1, m_2 \leq n - 1$. Damit ist auch die Eindeutigkeit bewiesen. □

Beispiel. Es sei $x_1 = 1/3$ und $x_2 = 11/5$. Für $n = 4$ gilt

$$\frac{1}{3} \equiv \frac{11}{5} \equiv 3 \mod 4.$$

Bei der Methode von Lenstra berechnen wir schrittweise das Vielfache kP ($k \in \mathbb{N}$) des gewählten Punktes $P \in C(\mathbb{Q})$ modulo n. Dies ist jedoch nur möglich, falls die auftretenden Nenner in jedem Rechenschritt zu n teilerfremd sind. Es gilt der folgende Satz.

Satz 4.3. *Seien n und C wie oben, wobei zusätzlich $(4b^3 + 27c^2, n) = 1$ gelte. Außerdem seien $P = (x_P, y_P), Q = (x_Q, y_Q) \in C(\mathbb{Q})$ mit $P \neq -Q$ und die rationalen Koordinaten x_P, y_P und x_Q, y_Q besitzen zu n teilerfremde Nenner. Dann sind die folgenden Aussagen äquivalent:*

(a) Die Summe $R := P + Q \in C(\mathbb{Q})$ besitzt rationale Koordinaten x_R, y_R mit zu n teilerfremdem Nenner.

(b) Für jede Primzahl q mit der Eigenschaft $q|n$ gilt:

$$R := P + Q \not\equiv O \mod q$$

auf der elliptischen Kurve $C(\mathbb{F}_q)$.

Beweis. (a) $\Rightarrow$ (b): Seien P, Q und $R = P + Q \in C(\mathbb{Q})$ mit rationalen Koordinaten, deren Nenner relativ prim zu n sind, gegeben. Weiter sei q ein beliebiger Primfaktor von n.
Falls $x_P \not\equiv x_Q \mod q$ gilt, dann folgt sofort aus den Formeln (3.6) und (3.7) für die Addition modulo q, wobei $a = 0$ ist, dass $R \not\equiv O \mod q$ ist.
Falls $x_P \equiv x_Q \mod q$ gilt, unterscheiden wir folgende zwei Fälle: Falls $P = Q$ gilt, dann ist $R = 2P$, und die Koordinaten von R sind modulo q gegeben durch die Formeln (3.8), bzw. (3.9), wobei $a = 0$ ist. Wir müssen also zeigen, dass der Nenner von $2y_P$ nicht durch q teilbar ist. Angenommen, q teilt den Nenner von $2y_P$, dann muss q auch den Zähler von $3x_P^2 + b$ teilen, da der Nenner von x_R nicht durch q teilbar ist. Daraus folgt, dass das kubische Polynom der elliptischen Kurve C an der Stelle x_P eine doppelte Nullstelle modulo q besitzt, da Funktion und erste Ableitung dort den Wert 0 annehmen, im Widerspruch zu unserer Voraussetzung $(4b^3 + 27c^2, n) = 1$. Damit kann q nicht den Nenner von $2y_P$ teilen, was (b) beweist. Falls $P \neq Q$ gilt, kann man auf ähnliche Weise einen Widerspruch herbeiführen.

(b) $\Rightarrow$ (a): Es sei (b) erfüllt. Wir müssen zeigen, dass die Koordinaten x_R, y_R Nenner teilerfremd zu n besitzen, d.h., dass jeder Primteiler q von n diese Nenner nicht teilt. Sei nun ein Primteiler q von n fixiert.
Falls $x_P \not\equiv x_Q \mod q$ gilt, dann folgt sofort aus den Formeln (3.6) und (3.7) für die Addition modulo q, dass hier offensichtlich sind alle Nenner teilerfremd zu q sind, was (a) beweist.
Falls $x_P \equiv x_Q \mod q$ gilt, dann folgt aus der Voraussetzung $R \not\equiv O \mod q$, dass $y_P \equiv y_Q \not\equiv 0 \mod q$ gelten muss. Ist nun $P = Q$, dann folgt damit wieder

aus den Additionsformeln (3.8), bzw. (3.9), dass die Koordinaten x_R, y_R Nenner besitzen, welche nicht durch q teilbar sind, d.h. Nenner, welche teilerfremd zu n sind, was (a) beweist. Falls $P \neq Q$ gilt, so verfahren wir auf ähnliche Weise. $\square$

Algorithmus (*Methode von Lenstra*). Sei n eine große natürliche Zahl, die nicht durch 2 und 3 teilbar ist und einen Primfaktor $p > 3$ besitzt. Zuerst wählt man eine beliebige elliptische Kurve C, welche durch die Gleichung

$$y^2 = x^3 + b \cdot x + c$$

mit $b, c \in \mathbb{Z}$ gegeben ist, und einen beliebigen Punkt $P = (x_P, y_P) \in C(\mathbb{Q})$.
Daraufhin prüft man, ob $(4b^3 + 27c^2, n) = 1$ gilt, d.h. ob das kubische Polynom $x^3 + b \cdot x + c$ drei verschiedene Nullstellen modulo q für jeden Primfaktor q von n besitzt. Im Falle $1 < (4b^3 + 27c^2, n) < n$ hat man bereits einen Teiler von n gefunden und ist fertig. Im Falle $(4b^3 + 27c^2, n) = n$ wählt man eine neue elliptische Kurve und beginnt von vorne.
Als nächstes wählt man sich zwei Grenzen B und C und ein

$$k = q_1^{\alpha_1} \cdot \ldots \cdot q_r^{\alpha_r} \in \mathbb{N}$$

als Produkt aller Primzahlpotenzen $q_j^{\alpha_j} \leq C$, wobei q_j eine Primzahl und $\alpha_j \in \mathbb{N}$ $(j = 1, \ldots, r)$ ist. B soll dabei eine obere Grenze für die Primteiler q_j von k sein, d.h. es gilt $q_j \leq B$ für $j = 1, \ldots, r$. Falls B sehr groß ist, ist die Wahrscheinlichkeit höher, das $kP \equiv O \mod p$ für ein p mit $p|n$, allerdings wird mehr Zeit für die Berechnung von kP benötigt. Falls man einen Primfaktor der Größe $q \sim \sqrt{n}$ sucht, so wählt man C (nach dem Satz von Hasse) so, dass $q + 1 + 2\sqrt{q} < C$ gilt. Mit diesem k berechnet man nun schrittweise das Vielfache kP des Punktes P modulo n. Zuerst berechnet man $q_1 P$, $q_1(q_1 P)$, $\ldots$, $q_1^{\alpha_1} P$, danach $q_2(q_1^{\alpha_1} P)$, $q_2(q_2 \cdot q_1^{\alpha_1} P)$, $\ldots$, $q_2^{\alpha_2} q_1^{\alpha_1} P$, und so fort. Wenn nun die Berechnung eines dieser Vielfachen fehlschlägt, dann liegt eine rationle Koordinate mit einem Nenner vor, welcher nicht teilerfremd zu n ist. Mit der Bestimmung des größten gemeinsamen Teilers dieses Nenners und n erhält man also entweder einen echten Teiler von n und man ist fertig, oder man erhält n selbst. In diesem Fall wiederholt man den Algorithmus mit einer neuen elliptischen Kurve und einem neuen Punkt. Genauso verfährt man, falls die Berechnung von kP in keinem der Schritte fehlschlägt.

Beispiel. Sei $n = 5429$. Zuerst wählen wir die elliptische Kurve C, welche durch die Gleichung $y^2 = x^3 + 2 \cdot x - 2$ gegeben ist, und den Punkt $P = (1, 1) \in C(\mathbb{Q})$. Da $4 \cdot 2^3 + 27 \cdot 2^2 = 140 = 2^2 \cdot 5 \cdot 7$, gilt $(4 \cdot 2^3 + 27 \cdot 2^2, 5429) = 1$. Wir wählen $B = 3$. Suchen wir einen Primfaktor der Größe $\sqrt{n} \sim 73$, so wählen wir wegen $73 + 1 + 2\sqrt{73} < 92$ die Schranke $C = 92$. Damit ist $k = 2^6 3^4$. Berechnen wir nun schrittweise die Vielfachen $2P$, $2(2P)$, $\ldots$, $2^6 P$, $3(2^6 P)$, und so fort, so schlägt die Berechnung bei $3^2 2^6 P$ fehl, d.h. wir erhalten einen Nenner welcher nicht teilerfremd zu n ist, sondern mit n den größten gemeinsamen Teiler 61 besitzt.