Rechnen mit Punkten einer elliptischen Kurve

von Ralph-Hardo Schulz, Helmut Witten und Bernhard Esslinger

Einleitung

In diesem Beitrag führen wir in die Theorie der endlichen elliptischen Kurven ein. Diese spielen eine wichtige Rolle in der Public-Key-Kryptografie (vgl. BSI, 2013):

Zwei bekannte asymmetrische Verschlüsselungsverfahren sind das RSA-Verfahren (benannt nach den Erfindern Rivest, Shamir, Adleman) und die Klasse der Elgamal-Verfahren. Zu letzteren gehören auch die auf Elliptischen Kurven basierenden Verschlüsselungsverfahren.

Mit Punkten einer Kurve kann man rechnen? Dies mag wohl zunächst in Erstaunen zu versetzen. Doch denkt man an Ortsvektoren in der analytischen Geometrie, so ist das Rechnen mit Punkten nicht ungewöhnlich. Bei Punkten einer elliptischen Kurve besteht dieses Rechnen aus der Addition von Punkten, insbesondere der mehrfachen Summation desselben Punktes (entsprechend der Multiplikation mit einem Skalar).

Anwendung finden die Rechnungen auf elliptischen Kurven u.a. in der Elliptische-Kurven-Kryptografie (ECC – ***E**lliptic **C**urve **C**ryptography*). Zum Beispiel lässt sich das sogenannte Elgamal-Verschlüsselungsverfahren (vgl. Witten u.a., 2015, Seite 97ff., in diesem Heft) oder der Diffie-Hellman-Schlüsselaustausch in einfacher Weise auf elliptische Kurven übertragen. Dieses Prinzip wurde von Victor S. Miller und Neal Koblitz 1986 bzw. 1987 unabhängig voneinander vorgeschlagen (vgl. Wikipedia – Stichwort „Elliptic Curve Cryptography“).

Quelle: Esslinger u. a., [11] 2013, S. 234 (nach Lenstra/Verheul)

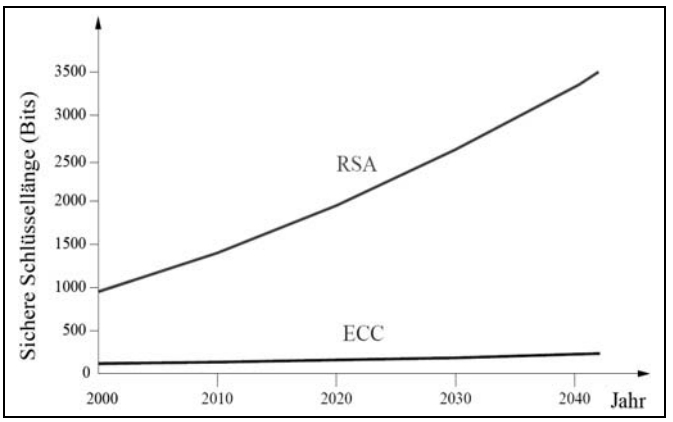


Bild 1: Prognose für die Entwicklung als sicher betrachteter Schlüssellängen bei RSA und bei elliptischen Kurven (ECC).

Für die Sicherheit beim Verschlüsseln mittels elliptischer Kurven spielt eine entscheidende Rolle, dass in der zugrunde liegenden Gruppe der Exponent einer gegebenen Potenz nicht in sinnvoller Zeit bestimmt werden kann (Problem des diskreten Logarithmus), das Potenzieren also eine Einwegfunktion ist. Die Public-Key-Verfahren, die solche Kurven benutzen, liefern Alternativen zum RSA-Verfahren; sie kommen mit Schlüsseln wesentlich geringerer Länge als RSA aus und können damit durch Hardware (in Smartcards ohne Koprozessoren) billiger implementiert werden. Laut Arjen K. Lenstra und Eric R. Verheul (vgl. Lenstra/Verheul, 1999) ist eine gute elliptische Kurve mit dem Parameter p einer Bitlänge von 139 Bit (für die Größenordnung des erzeugenden Punktes P aus einer elliptischen Kurve) genauso sicher wie ein RSA-Modul von 1024 Bit Länge. Auch die Prognosen für die Entwicklung als sicher betrachteter Schlüssellängen (siehe Bild 1) zeigen den diesbezüglichen Vorteil der Elliptischen-Kurven-Kryptografie.

Die oberste europäische Sicherheitsbehörde (ENISA – *European Union Agency for Network and Information Security*; Europäische Agentur für Netz- und Informationssicherheit) empfiehlt inzwischen den Einsatz der Elliptischen-Kurven-Kryptografie mit 160 Bit (für den größten Prim-Teiler der Gruppenordnung), für mittelfristige Speicherung mit 256 Bit und langfristig mit 512 Bit Länge, während bei RSA für mittelfristig gespeicherte Daten mindesten 3072 Bit und für langfristige Sicherheit sogar nur Systeme mit 15360 Bit langen Schlüsseln angeraten werden (vgl. ENISA, 2013, und Brenner, 2013).

Schon lange mehren sich die Experten-Warnungen vor möglichen Geheimdienst-Angriffen auf Systeme mit zu geringen Sicherheitsspielräumen oder versteckten Hintertüren (vgl. z.B. Schneier, 2013, Weis, 2013,

und Ermert, 2014). Empfohlen wird daher u.a. von Bruce Schneier (2013):

> […] I think we need to 1) make sure we know where our curves come from, and 2) build in a hefty security margin.

Neben der Anwendung von elliptischen Kurven im Elgamal-Verschlüsselungsverfahren findet man ihren Einsatz auch in dem Faktorisierungsalgorithmus (ECM – ***E**lliptic **C**urve **M**ethod*) von Hendrik Wilhelm Lenstra (vgl. Lenstra, 1987), einem Bruder des oben erwähnten Arjen K. Lenstra, und bei der Erzeugung von Pseudozufallszahlen (siehe dazu aber die Anmerkung 5 am Schluss dieses Beitrags über Hintertüren und Schwächen gewisser Standards, Seite 113).

Elliptische Kurven sind übrigens nicht ellipsenförmig, sondern lassen sich durch sogenannte elliptische Funktionen parametrisieren, die bei der Berechnung der Bogenlängen von Ellipsen auftreten: Bereits der italienische Mathematiker Giulio Carlo Fagnano dei Toschi (1682–1766) zeigte, dass diese Berechnung auf sogenannte elliptische Integrale führt (vgl. Brown, 2000), deren Integrand von der Form $(x^3 + ax^2 + bx + c)^{-½}$ ist. Solche Integrale wurden u.a. von Leonhard Euler und Adrien-Marie Legendre im 18. sowie von Niels Henrik Abel und Carl Gustav Jacob Jacobi im 19. Jahrhundert untersucht.

Zum ersten Verstehen des Gebiets der elliptischen Kurven benötigen wir die Anfänge der affinen und der algebraischen Geometrie; diese wollen wir im Folgenden ebenfalls bereitstellen.

Affine Ebene über einem Körper

Um elliptische Kurven betrachten zu können, erinnern wir zunächst an die Geometrie, in der solche Kurven „leben“, die sogenannten affinen Ebenen.

Anmerkung: Als Modell der Zeichenebene nimmt man meist die reelle euklidische Ebene. Jeder Punkt lässt sich dabei nach Festlegung eines Koordinatensystems durch zwei reelle Koordinaten (x_1, y_1), also als Element von $\mathbb{R}^2$, beschreiben. In Verallgemeinerung lassen wir nun (statt $\mathbb{R}$) einen beliebigen Körper K zu, z.B. auch den endlichen Körper $K = \mathbb{Z}_p$ für eine Primzahl p, also den Körper mit den Elementen $0, 1, \ldots, p–1$, bei dem modulo p gerechnet wird. Winkel und Abstände spielen dabei keine Rolle mehr. Man beschränkt sich bei der sogenannten affinen Ebene auf die Begriffe „Punkt“, „Gerade“, „(ein Punkt) liegt auf (einer Geraden)“ und „Parallelität von Geraden“. Wir vereinbaren:

Definition

Punkte der affinen Ebene $\mathcal{A} = \mathrm{AG}(2, K)$ über dem Körper K (d.h. die ***A**ffine **G**eometrie* AG der Dimension 2 über K) sind definitionsgemäß die Paare $(x, y) \in K^2$.

Beispiel einer endlichen affinen Ebene

Die Punkte der affinen Ebene $\mathcal{A}$ über dem Körper $K = \mathbb{Z}_3$ sind die folgenden 9 Paare:

$(0,0),\ (0,1),\ (0,2),$
$(1,0),\ (1,1),\ (1,2),$
$(2,0),\ (2,1),\ (2,2).$

Geraden von $\mathcal{A}$ sind die folgenden 12 Punktmengen:

$(0,0) + K(1,0) = \{(0,0), (1,0), (2,0)\}$ (x-Achse)
$(0,1) + K(1,0) = \{(0,1), (1,1), (2,1)\}$ (Parallele zur x-Achse)
$(0,2) + K(1,0) = \{(0,2), (1,2), (2,2)\}$ (Parallele zur x-Achse)

$(0,0) + K(0,1) = \{(0,0), (0,1), (0,2)\}$ (y-Achse)
$(1,0) + K(0,1) = \{(1,0), (1,1), (1,2)\}$ (Parallele zur y-Achse)
$(2,0) + K(0,1) = \{(2,0), (2,1), (2,2)\}$ (Parallele zur y-Achse)

$(0,0) + K(1,1) = \{(0,0), (1,1), (2,2)\}$
$(1,0) + K(1,1) = \{(1,0), (2,1), (0,2)\}$
$(2,0) + K(1,1) = \{(2,0), (0,1), (1,2)\}$

$(0,0) + K(2,1) = \{(0,0), (2,1), (1,2)\}$
$(1,0) + K(2,1) = \{(1,0), (0,1), (2,2)\}$
$(2,0) + K(2,1) = \{(2,0), (1,1), (0,2)\}.$

Im Bild 2 werden die 9 Punkte und 12 Geraden (als Punkte bzw. Strecken und gekrümmte Linien in der Zeichenebene) dargestellt.

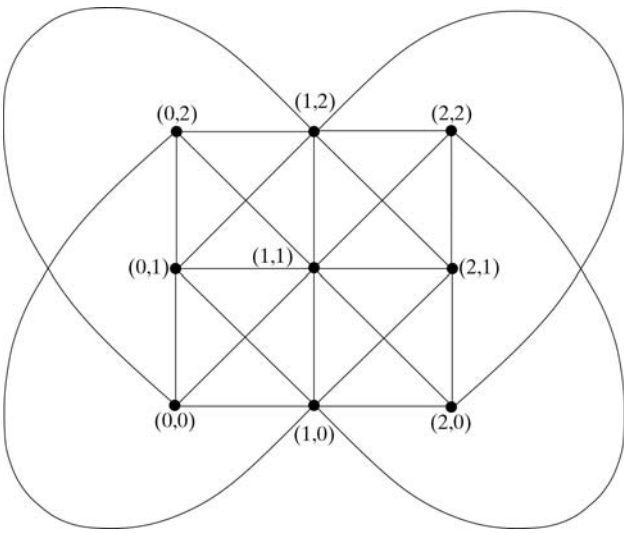


Bild 2: Die affine Ebene $\mathcal{A} = \mathrm{AG}(2, \mathbb{Z}_3)$.

Die Geraden sind definiert als die Punktmengen der Gleichung $y = mx+d$ bzw. $x = c$ (mit $m, d, c \in K$); vektoriell geschrieben sind das die Mengen

$$g = \{(q_1, q_2) + k(m_1, m_2) \mid k \in K\} =: (q_1, q_2) + K(m_1, m_2)$$

für einen (nicht eindeutig bestimmten) „Aufpunkt“ $(q_1, q_2) \in K^2$ und die eindeutig bestimmte „Richtung“ $K(m_1, m_2) := \{k(m_1, m_2) \mid k \in K\}$ mit $(m_1, m_2) \neq (0, 0)$. Zwei Geraden der Ebene heißen dann *parallel*, wenn sie gleich sind oder sich nicht schneiden (bzw. die gleiche Richtung haben).

Als Beispiel einer affinen Ebene ist im Kasten „Beispiel einer endlichen affinen Ebene“ (siehe oben) die-

jenige über dem endlichen Körper $\mathbb{Z}_3$ angegeben und im Bild 2 (vorige Seite) dargestellt. Die Gleichungen der Geraden der affinen Ebene über $\mathbb{Z}_5$ und einige ihrer Punkte sind in den Tabellen 2 und 3 aufgeführt (siehe Seite 109).

Elliptische Kurve

Wir betrachten als Zahlbereich $K = (\mathbb{Z}_p, +, \cdot)$ für p prim, $p \neq 2$, $K = \mathbb{R}$ oder $K = \mathbb{Q}$. (Zur Behandlung des Falles eines Körpers mit 2^m Elementen vgl. z.B. Esslinger u.a., [11]2013, Kapitel 7 „Elliptische Kurven".)

Definition

Eine elliptische Kurve ist definiert als die Menge $\mathscr{C} = \mathscr{C}(K)$ der Lösungen $(x, y) \in K^2$ einer kubischen Gleichung in zwei Variablen x und y mit einer auf der Kurve definierten Addition; zu diesen Kurven gehören – eventuell nach affiner Koordinatentransformation – die Kurven mit der sogenannten kurzen Weierstraß-Gleichung

$$y^2 = x^3 + bx + c \qquad (*)$$

mit festen $b, c \in K$. (Im Fall $p = 3$ wird neben (*) auch $y^2 = x^3 + ax^2 + b$ betrachtet.) Es handelt sich hierbei um sogenannte *Weierstraß-Kurven*. Weitere elliptische Kurven sind die *Edwards-Kurven* und die *Montgomery-Kurven* (siehe dazu die Anmerkung 6, Seite 113 f.).

Bild 3 (unten): Beispiele kubischer Kurven im Reellen mit Gleichung $y^2 = f(x)$, wobei $f(x)$ ein Polynom vom Grad 3 mit a) einer reellen Nullstelle und b) drei reellen Nullstellen ist.

Die Kurve mit Gleichung (*) heißt *nicht-singulär*, falls $D \neq 0$ für $D = -4b^3 - 27c^2$ gilt. (Für $p = 3$ wird D anders definiert.) Mit der Anforderung an D soll ausgeschlossen werden, dass $\mathscr{C}$ sich selbst schneidet oder Spitzen oder isolierte Punkte hat. Wir beschränken uns hier auf nicht-singuläre Kurven der Gleichung (*), oft auf den Spezialfall $b = c = 1$.

Beispiele mit $K = \mathbb{R}$ werden im Bild 3 veranschaulicht. Im reellen Fall heißt $\mathscr{C}(\mathbb{Q}) := \mathscr{C}(\mathbb{R}) \cap \mathbb{Q}^2$ die Menge der *rationalen Punkte* der Kurve $\mathscr{C}$. Auch die Punkte einer elliptischen Kurve über $\mathbb{Z}_p$ mit p prim können als Teil einer elliptischen Kurve über einem Oberkörper von $\mathbb{Z}_p$ aufgefasst werden; daher nennt man sie ebenfalls „rational".

Beispiele elliptischer Kurven

Sei $\mathscr{C}_p$ die (Weierstraß-)Kurve mit Gleichung

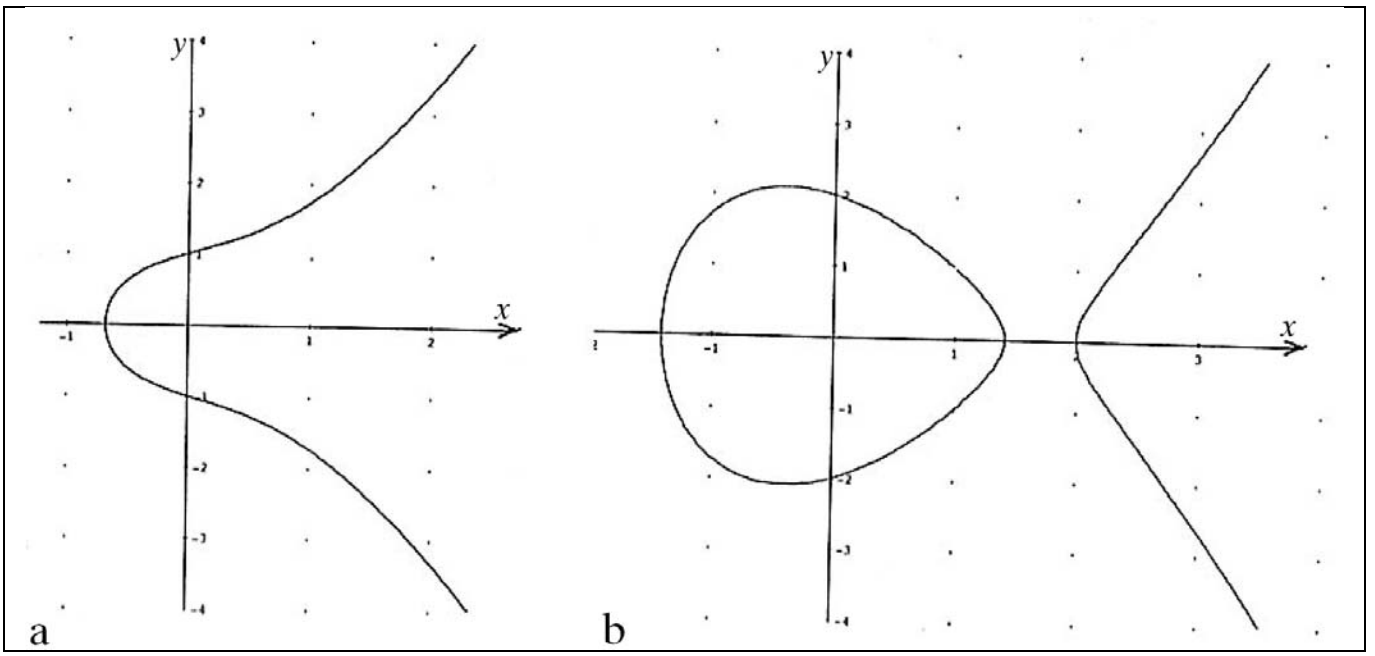
$$y^2 = x^3 + x + 1 \qquad (*1)$$

in der affinen Ebene über $K = \mathbb{Z}_p$.

Zur Bestimmung von $\mathscr{C}_p$ kann man allgemein wie folgt vorgehen:

1. Man erzeugt eine Tabelle der Quadrate y^2 der Elemente y von $\mathbb{Z}_p$.
2. In einer weiteren Tabelle listet man den Wert von $f(x) = x^3 + x + 1$ für jedes $x \in \mathbb{Z}_p$!
3. Durch Vergleich der Tabellenwerte bestimmt man diejenigen Paare (x, y), für die y^2 und $f(x)$ übereinstimmen!

Zum besseren Verständnis behandeln wir im Folgenden hauptsächlich das Beispiel $p = 5$, das für die Praxis der Kryptografie natürlich viel zu klein ist. Wir vergleichen folgende beiden Tabellen 1a und 1b (nächste Seite).



y	0	1	2	3	4
y^2 (mod 5)	0	1	4	4	1

Tabelle 1a (oben): Quadrate in $\mathbb{Z}_5$.

Tabelle 1b (unten): Werte von $f(x) := x^3 + x + 1$ in $\mathbb{Z}_5$.

x	0	1	2	3	4
$x^3 + x + 1$ (mod 5)	**1**	3	**1**	**1**	**4**

Ist $f(x) := x^3 + x + 1$ (siehe untere Zeile von Tabelle 1b) für $x \in \mathbb{Z}_p$ ein Quadrat in $\mathbb{Z}_p$, kommt also in der unteren Zeile von Tabelle 1a vor, so erhält man „rationale“ Punkte der Form (x, y) von $\mathscr{C}_5$ (d.h. mit $x, y \in \mathbb{Z}_5$ und $y^2 = f(x)$).

Da $f(1) = 3$ kein Quadrat in $\mathbb{Z}_5$ ist, folgt (unter Beachtung von $4 \equiv -1$ und $3 \equiv -2$):

$$\mathscr{C}_5 = \{(0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}$$
$$= \{(0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}.$$

$\mathscr{C}_5$ ist im Bild 4 grafisch dargestellt. Als weiteres kleines Beispiel wird im Bild 5 die Kurve $\mathscr{C}_{17}$ gezeigt, die noch per Hand und Taschenrechner berechnet werden kann. Ein Bild von $\mathscr{C}_{23}$ findet man z.B. bei Beutelspacher u.a. (^{2}2010).

Um elliptische Kurven $\mathscr{C}_p$ für etwas größere Primzahlen p zu berechnen und zu plotten, kann man – angeregt durch das Buch von William Stein (2011) – z.B. das EllipticCurve-Kommando von SageMath benutzen:

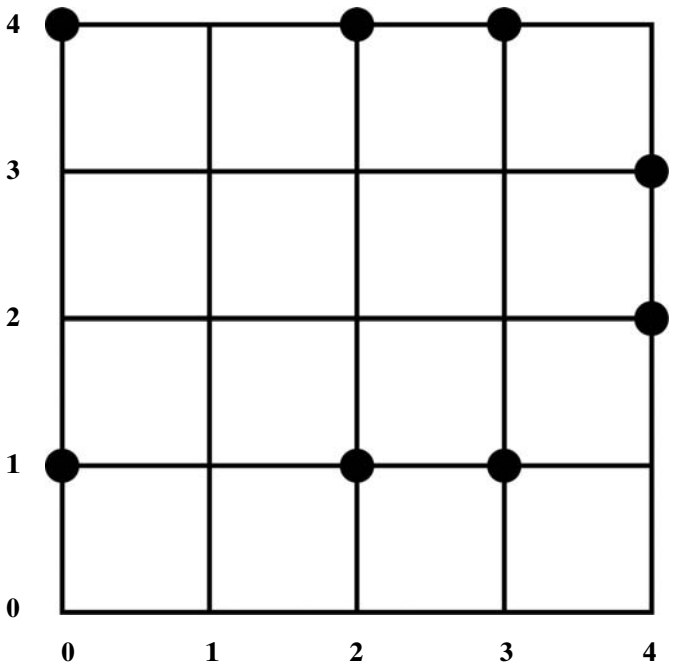


Bild 4: Elliptische Kurve über $\mathbb{Z}_5$; die Elemente von $\mathscr{C}_5$ sind durch die dicken Punkte markiert. (Nicht alle Geraden der Ebene sind dargestellt.)

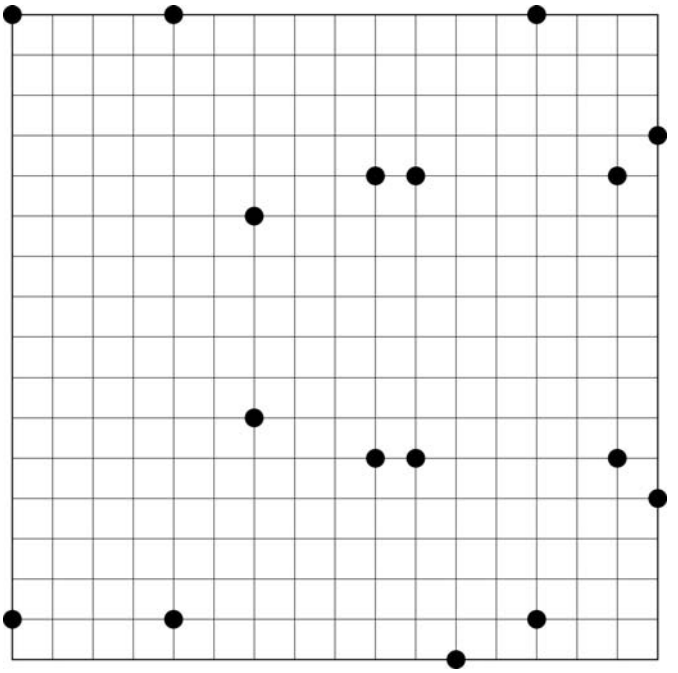


Bild 5: Elliptische Kurve über $\mathbb{Z}_{17}$ (wieder sind nur zwei Parallelenscharen von Geraden der Ebene abgebildet).

Die elliptische Kurve $\mathscr{C}_p$ mit Gleichung $y^2 = x^3 + bx + c$ über dem Körper $\mathbb{Z}_p = \mathrm{GF}(p) = \mathbb{F}_p$ berechnet man mit SageMath mittels des Befehls

```
E = EllipticCurve(GF(p), [b,c])
```

Ein Beispiel findet man im Kasten „SageMath-Beispiel zu $\mathscr{C}_{127}$“, nächste Seite. Die Kontrolle, ob ein Punkt auf der Kurve $\mathscr{C}_p$ liegt oder nicht, kann dann durch die Eingabe von

```
R = E([d; e])
```

erfolgen. Im Falle R $\notin \mathscr{C}_p$ erfolgt die Meldung:

```
Coordinates [d, e, 1] do not define a point on
Elliptic Curve defined by y^2 = x^3 + bx + c over
Finite Field of size p
```

Auch elliptische Kurven über $\mathbb{Q}$ kann man mit SageMath veranschaulichen (siehe Kasten „SageMath-Programmier-Beispiel zu elliptischen Kurven über $\mathbb{Q}$“, nächste Seite).

Verwiesen sei auch auf die interaktiven Notebooks von Maike Massierer (vgl. Massierer, 2011).

Symmetrie von $\mathscr{C}$

Wegen $(-y)^2 = y^2$ ist mit jedem Punkt $Q = (x, y)$ aus $\mathscr{C}$ auch $Q' = (x, -y)$ ein Punkt von $\mathscr{C}$. Letzterer liegt in gewissem Sinne symmetrisch zur x-Achse (bzw. zu einer gedachten Parallelen zur x-Achse, wenn mod p re-

SageMath-Beispiel zu $\mathscr{C}_{127}$

Das Beispiel ist analog zu einem Vorschlag von William Stein (2011, S. 125) konstruiert (siehe auch Bild 6).

```
sage: E = EllipticCurve(GF(127), [1,1])
sage: E
Elliptic Curve defined by y^2 = x^3 + x + 1
         over Finite Field of size 127
sage: P = E.plot(pointsize=20)
```

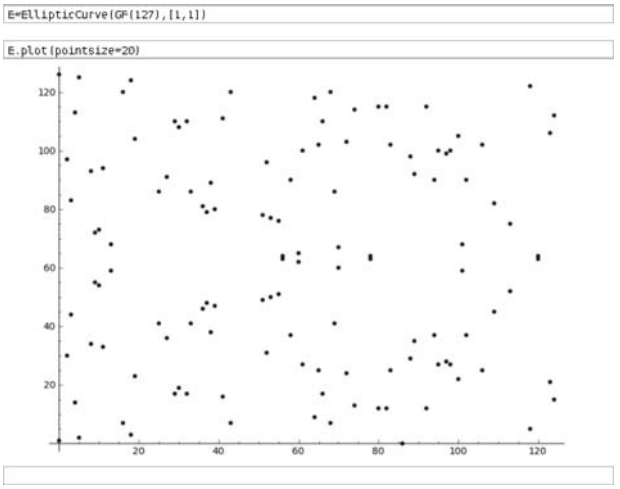


Bild 6: Elliptische Kurve über $\mathbb{Z}_{127}$ (erstellt mithilfe von SageMath).

SageMath-Programmier-Beispiel zu elliptischen Kurven über $\mathbb{Q}$

Das Beispiel ist analog zu einem weiteren Vorschlag von William Stein (2011, S. 124) konstruiert.

```
sage: E = EllipticCurve([-5, 4])
sage: E
Elliptic Curve defined by y^2 = x^3 - 5*x + 4
         over Rational Field
sage: P = E.plot(thickness=4, rgbcolor=(0.1,0.7,0.1))
sage: P.show(figsize=[4,6])
```

duziert wird): Die x-Koordinaten von Q und Q' sind gleich, die y-Koordinate von Q wird zu $-y$ (d.h. im Fall $K = \mathbb{Z}_p$ zu $p - y$) bei Q'.

Der uneigentliche Punkt von $\mathscr{C}$

Es erweist sich als zweckmäßig, noch einen (gedachten) Punkt $\mathbb{O}$ zu $\mathscr{C}$ hinzuzunehmen, der nicht in $\mathscr{A}$ liegt und um den wir die Ebene $\mathscr{A}$ erweitern:

$\overline{\mathscr{C}} := \mathscr{C} \cup \{\mathbb{O}\}$.

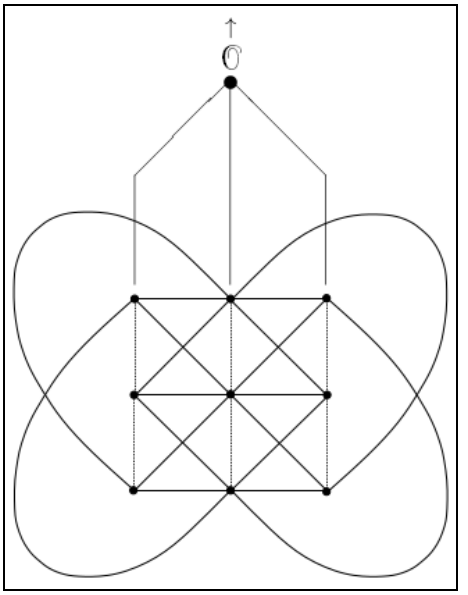


Bild 7: AG(2, $\mathbb{Z}_3$) mit uneigentlichem Punkt $\mathbb{O}$ in y-Richtung (die Geraden sind wieder als Strecken und gekrümmte Linien dargestellt).

Dieser Punkt ist der „uneigentliche Punkt in Richtung der y-Achse“: Analog zum fiktiven Schnittpunkt von parallelen Geraden auf der Horizontlinie nimmt man im vorliegenden Fall an, dass alle Parallelen zur y-Achse aus $\mathscr{A}$ durch diesen im „Unendlichen“ liegenden Punkt $\mathbb{O}$ gehen (siehe dazu die Beispiele zu AG(2, $\mathbb{Z}_3$) und AG(2, $\mathbb{Z}_5$) in Bild 7 und in Bild 8, nächste Seite).

Mit Mitteln der projektiven Geometrie kann man zeigen, dass die Hinzunahme von $\mathbb{O}$ zu $\mathscr{C}$ nicht willkürlich ist, sondern sich auf natürliche Weise aus der vorliegenden Situation ergibt. (Für die Leserinnen oder Leser, die sich etwas mit projektiver Geometrie, insbesondere mit projektiven Koordinaten, auskennen, zeigen wir dies im Kasten „Zum uneigentlichen Punkt $\mathbb{O}$“, nächste Seite.) Wir werden weiter unten sehen, dass der Punkt $\mathbb{O}$ für die zu definierende Gruppenstruktur der Kurve wichtig ist.

Schnitt von $\overline{\mathscr{C}}$ mit Geraden

Will man Schnittpunkte einer Geraden h mit der Kurve $\overline{\mathscr{C}}$ berechnen, so kann man die Gleichung $y = mx + d$ bzw. $x = k$ von h in die Gleichung (*) der Kurve einsetzen. Man erhält dann (gemäß der Berechnung im Kasten „Schnitt von $\mathscr{C}$ mit Geraden“, nächste Seite) als Ergebnis:

Die Verbindungsgerade zweier Punkte $P, Q \in \overline{\mathscr{C}}$ schneidet die Kurve in einem dritten Punkt. (Dieser kann bei entsprechender Vielfachheit des Punktes gleich P oder Q sein.)

Wir vermerken noch, dass man zeigen kann: In jedem Punkt von $\mathscr{C}$ existiert eine lokale Tangente (zur Definition siehe den Kasten „Schnitt von $\mathscr{C}$ mit Geraden“, nächste Seite). Mit einem ähnlichen Argument wie in diesem Kasten sieht man wieder: Diese Tangente schneidet $\overline{\mathscr{C}}$ in genau einem weiteren Punkt.

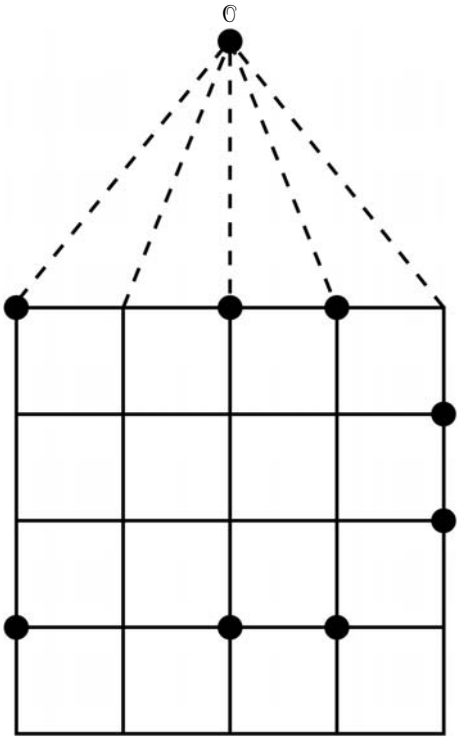


Bild 8: Elliptische Kurve in AG(2, $\mathbb{Z}_5$) mit uneigentlichem Punkt $\mathbb{O}$ in y-Richtung (wieder sind nicht alle Geraden der Ebene eingezeichnet; die durch $\mathbb{O}$ gehenden Geraden sind außerhalb des „affinen Teils“ gestrichelt).

Ein weiteres Beispiel

Wieder sei $\overline{\mathscr{C}}$ die Kurve mit Gleichung

$y^2 = x^3 + x + 1$ (*1)

in der affinen Ebene $\mathscr{A}$ über $K = \mathbb{Z}_5$ und uneigentlichem Punkt $\mathbb{O}$ (siehe Bild 8). In den Tabellen 2 und 3 (nächste Seite) listen wir die Schnittpunkte der Geraden von $\mathscr{A}$ mit $\overline{\mathscr{C}}$ auf. (Die Geraden mit den Gleichungen $y = 0$, $y = x$, bzw. $y = 4x$ schneiden $\overline{\mathscr{C}}$ nicht; sie sind „Passanten“.)

Addition von rationalen Punkten

Wir betrachten wieder elliptische Kurven über $\mathbb{Q}$ oder $\mathbb{Z}_p$ für $p > 3$. Sei $\overline{\mathscr{C}}$ die Menge der Punkte der nicht-singulären Kurve der Gleichung

$y^2 = x^3 + bx + c$

einschließlich des uneigentlichen Punktes $\mathbb{O}$ in y-Richtung. Dann kann man auf $\overline{\mathscr{C}}$ eine Addition definieren. Wir beschreiben das Verfahren zunächst anschaulich geometrisch, danach geben wir Formeln und Beispiele an.

Zuvor aber noch einige *historische Anmerkungen* (nach Brown, 2000, S.166): Schon Isaac Newton (vgl. Brown, 2000, mit Hinweis auf Knapp, 1992) hatte erkannt, dass – gegeben einige Punkte einer elliptischen Kurve – man „neue“ Punkte der Kurve als Schnitte der Kurve mit einer Sekante durch zwei bekannte Punkte der Kurve oder mit einer Tangente an einen bekannten Punkt gewinnen konnte. Carl Gustav J. Jacobi stellte den Zusammenhang mit elliptischen Integralen her, und Karl Weierstraß fand die Verbindung der Addition von elliptischen Funktionen mit der Sekanten- und

Schnitt von $\mathscr{C}$ mit Geraden

Sind $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ mit $x_1 \neq x_2$ Punkte der Geraden h der Gleichung $y = mx + d$, die auf der Kurve $\mathscr{C}$ der Gleichung (*) liegen, so liefert Einsetzen von $y_i = mx_i + d$ in $y^2 = x^3 + bx + c$ eine Beziehung der Form

$x_i^3 - m^2x_i^2 + (b - 2md)x_i + c - d^2 = 0$ $(i = 1, 2)$.

Umgekehrt sind die Lösungen von

$x^3 + jx^2 + kx + l = 0$ (◊)

(mit $j = -m^2$, $k = b - 2md$, $l = c - d^2$) in K die x-Koordinaten der Schnittpunkte von h mit $\mathscr{C}$. Als Gleichung dritten Grades besitzt (◊) höchstens 3 Lösungen; zu jeder Lösung a ist $(x - a)$ ein Teiler der linken Seite. Ist keine höhere Potenz von $(x - a)$ Teiler, so handelt es sich um einen einfachen Schnittpunkt; wenn aber auch $(x - a)^2$ Teiler ist, so spricht man von einem mehrfachen Schnittpunkt oder von einem *Tangentialpunkt von h* und von h als *lokaler Tangente* an $\mathscr{C}$ im Punkt mit x-Koordinate a.
In einem geeigneten Oberkörper von K zerfällt das Polynom der linken Seite von (◊) in $(x - x_1)(x - x_2)(x - x_3)$. Mit x_1 und x_2 muss (wegen der rationalen Koeffizienten des Polynoms) auch x_3 aus K sein.
Die Gerade durch P und Q schneidet also $\mathscr{C}$ in einem dritten Schnittpunkt: Dieser kann auch mit P oder Q übereinstimmen. Zu vermerken ist noch, dass keine der Geraden mit Gleichung $y = mx + d$ durch $\mathbb{O}$ geht.
Setzt man die Gleichung $x = d$ einer Parallelen zur y-Achse in (*) ein, so erhält man $y^2 = l$ mit $l = d^3 + bd + c$; wenn l ein Quadrat ist, so ergeben sich 2 Lösungen. Die fraglichen Geraden gehen alle außerdem durch den uneigentlichen Punkt $\mathbb{O}$, schneiden also ebenfalls $\overline{\mathscr{C}}$ in 3 Punkten.

Zum uneigentlichen Punkt $\mathbb{O}$

Sei (x, y) Punkt von $\mathscr{A}$; dann heißen $\zeta_0, \zeta_1, \zeta_2$ die homogenen Koordinaten des Punktes, falls gilt:

$x = \frac{\zeta_1}{\zeta_0}$ und $y = \frac{\zeta_2}{\zeta_0}$ mit $\zeta_0 \neq 0$.

Einsetzen von x und y in (*), die Gleichung von $\mathscr{C}$ (siehe Seite 105), und Multiplikation mit ζ_0^3 ergibt die Gleichung

$\zeta_2^2\,\zeta_0 = \zeta_1^3 + b\,\zeta_1\,\zeta_0^2 + c\,\zeta_0^3$, (*')

die für die affinen Punkte äquivalent zu (*) ist. Für einen „uneigentlichen Punkt“, also solchen mit Koordinate $\zeta_0 = 0$, ist (*') genau dann erfüllt, wenn $\zeta_1 = 0$ ist, d.h. für den uneigentlichen Punkt $K(0, 0, 1)$, den wir mit $\mathbb{O}$ bezeichnen. $\mathbb{O}$ liegt auf den Geraden der Gleichungen $\zeta_1 - c\zeta_0 = 0$, also den Geraden mit affinen Gleichungen $x = c$, den Parallelen zur y-Achse von $\mathscr{A}$. Daher ist $\mathbb{O}$ der Fernpunkt in y-Richtung und erfüllt (*'), die „projektive Version“ der Gleichung (*).

Geraden-gleichung	Schnittpunkte mit $\overline{\mathscr{C}}$	Bemerkungen (Rechnungen mod 5)
$y = 1$	(0, 1), (2,1), (3,1)	
$y = 2$	(4, 2)	4 ist einfache Nullstelle Einsetzen von $y = 2$ in (*1) ergibt $4 = x^3 + x + 1$. Division von $x^3 + x + 2$ durch $(x - 4)$ liefert $x^2 + 4x + 2$, sodass (*1) zu $(x^2 + 4x + 2)(x - 4) = 0$ führt. Da für jedes $x \in \mathbb{Z}_5$ der quadratische Term ungleich 0 ist (d. h. $x^2 + 4x + 2$ irreduzibel), gibt es keine Nullstelle außer $x = 4$; und diese ist eine einfache Nullstelle. Die Gerade $y = 2$ ist keine Tangente.
$y = x + 1$	(0, 1), <u>(3, 4)</u>	Tangente in (3, 4) Denn $y^2 = (x + 1)^2 = x^3 + x + 1$ ist äquivalent zu $x^3 - x^2 - x = 0$; das Polynom der linken Seite hat die einfache Nullstelle $x = 0$ und die doppelte Nullstelle $x = 3$.
$y = x + 2$	<u>(2, 4)</u>	dreifache Nullstelle wegen $x^3 + 4x^2 + 2x + 2 = (x - 2)^3$
$y = x + 3$	(3, 1), <u>(4, 2)</u>	Tangente in (4, 2) wegen $x^3 + 4x^2 + 2 = (x - 4)^2(x - 3)$
$y = 2x$	(2, 4), (3, 1), (4, 3)	
$y = 2x + 1$	(0, 1)	einfach, denn $(2x + 1)^2 = x^3 + x + 1$ ergibt $x^3 + x^2 + 2x = 0$; es ist wieder $x = 0$ einfache Nullstelle; Einsetzen aller $x \in \mathbb{Z}_5$ in $x^2 + x + 2$ zeigt, dass es keine weitere Nullstelle gibt.
$y = 2x + 2$	(2, 1)	einfach, da $x^2 + 3x + 4$ ohne Nullstelle in $\mathbb{Z}_5$.
$y = 2x + 3$	(3, 4)	einfach, da $x^2 + 4x + 1$ irreduzibel.
$y = 3x + 1$	(4, 3), <u>(0, 1)</u>	Tangente in (0, 1)
$y = 4x + 1$	(0, 1), (2, 4), (4, 2)	
$x = 0$	(0, 1), (0, 4), $\mathbb{O}$	y-Achse
$x = 1$	<u>$\mathbb{O}$</u>	Parallele zur y-Achse
$x = 2$	(2, 1), (2, 4), $\mathbb{O}$	Parallele zur y-Achse
$x = 3$	(3, 1), (3, 4), $\mathbb{O}$	Parallele zur y-Achse
$x = 4$	(4, 2), (4, 3), $\mathbb{O}$	Parallele zur y-Achse
$y = 0$	kein Schnittpunkt	Passante
$y = x$	kein Schnittpunkt	Passante

Tabelle 2:
Schnittpunkte der Geraden mit der Kurve $\overline{\mathscr{C}}$ über $\mathbb{Z}_5$ (1. Teil); unterstrichen sind die jeweiligen Tangentialpunkte.

Geraden-gleichung	Schnittpunkte mit $\overline{\mathscr{C}}$
$y = 4$	(0, 4), (2, 4), (3, 4)
$y = 3$	(4, 3)
$y = 4x + 4$	(0, 4), <u>(3, 1)</u>
$y = 4x + 3$	<u>(2, 1)</u>
$y = 4x + 2$	(3, 4), <u>(4, 3)</u>
$y = 3x$	(2, 1), (3, 4), (4, 2)
$y = 3x + 4$	(0, 4)
$y = 3x + 3$	(2, 4)
$y = 3x + 2$	(3, 1)
$y = 2x + 4$	(4,2), <u>(0, 4)</u>
$y = x + 4$	(0, 4), (2, 1), (4, 3)
$y = 4x$	keiner (Passante)

Tabelle 3: Schnittpunkte der Geraden mit der Kurve $\overline{\mathscr{C}}$ über $\mathbb{Z}_5$ (2. Teil) – gespiegelte Geraden aus Tabelle 2 und deren Schnittpunkte mit $\overline{\mathscr{C}}$; unterstrichen sind die jeweiligen Tangentialpunkte.

Tangenten-Methode der Erzeugung von neuen aus gegebenen Punkten. Schließlich verband Henri Poincaré 1901 alle diese Ideen in der Beschreibung arithmetischer Eigenschaften algebraischer Kurven.

Geometrische Beschreibung:
Sehnen- und Tangenten-Addition

Wir führen eine Verknüpfung „+“ wie folgt ein:

▷ Sind P und Q mit $P \neq Q$ Punkte der Kurve $\overline{\mathscr{C}}$, so schneiden wir zunächst die Gerade g durch diese Punkte mit der Kurve; falls der nach Kapitel „Schnitt von $\overline{\mathscr{C}}$ mit Geraden“, Seite 107 f., existierende dritte Schnittpunkt (x_3, y_3) von g mit $\overline{\mathscr{C}}$ ungleich $\mathbb{O}$ ist, „spiegeln“ wir ihn an der x-Achse zu $(x_3, -y_3) =: P + Q$; andernfalls sei $P + Q = \mathbb{O}$ (siehe Bild 9a, nächste Seite).

Anmerkung: Von Nick Sullivan (2013) wird übrigens versucht, die Operation mithilfe eines bizarren Billard-Spiels zu veranschaulichen: Eine Billard-Kugel im Punkt P wird in Richtung von Punkt Q gestoßen; wenn sie die Kurve dann zum dritten Mal trifft, springt sie entweder senkrecht nach oben (falls unterhalb der x-Achse) oder nach unten (falls oberhalb der x-Achse), bis sie die Kurve ein weiteres Mal trifft.

▷ Ist $R \in \mathscr{C}$, so erhält man $R + R$, indem man die (lokale) Tangente in R an die Kurve, d. h. die Gerade, die R als Schnittpunkt mindestens doppelter Vielfachheit besitzt (siehe Kasten „Schnitt von $\mathscr{C}$ mit Geraden“, vorige Seite), mit der Kurve $\mathscr{C}$ schneidet und den so erhaltenen weiteren Punkt an der x-Achse spiegelt (siehe Bild 9b, nächste Seite).

▷ Schließlich definiert man $\mathbb{O} + \mathbb{O} = \mathbb{O}$.

Es stellt sich heraus:

$(\overline{\mathscr{C}}, +)$ ist eine kommutative Gruppe.

Beweis-Andeutung: $\mathbb{O}$ ist das neutrale Element, denn nach Konstruktion ist der dritte Punkt der Geraden $\mathbb{O}P$ spiegelsymmetrisch zu P; daher gilt: $P + \mathbb{O} = P = \mathbb{O} + P$ für jeden Punkt $P \in \overline{\mathscr{C}}$; das Kommutativgesetz ist klar, da für die Verbindungsgerade zweier Punkte P, Q gilt: $PQ = QP$; die Inverse zu S erhält man durch Spiegelung von S wie in Bild 10 (nächste Seite) veranschaulicht. Den aufwendigen Beweis des Assoziativgesetzes übergehen wir hier und verweisen z. B. auf Silverman/Tate (1992) oder Silverman (^{2}2009).

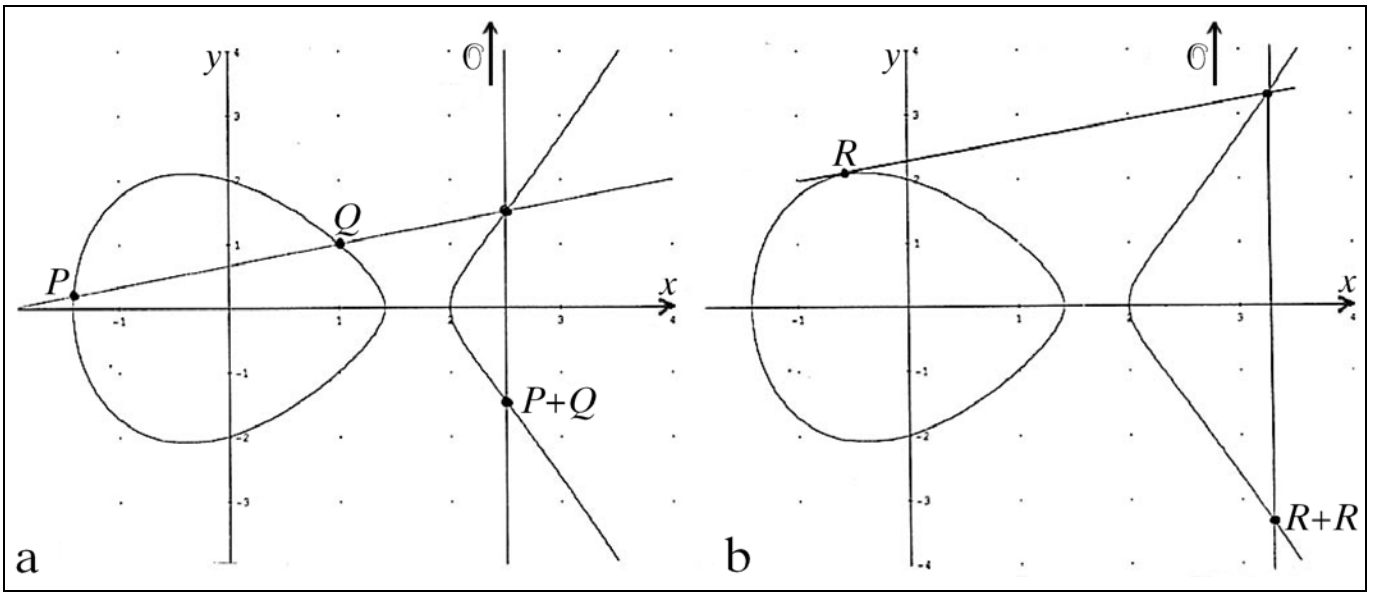


Bild 9: Zur Verknüpfung rationaler Punkte von elliptischen Kurven.

Wie schon in der Einleitung erwähnt, benutzt man in der Kryptografie mit elliptischen Kurven (EC-Kryptografie) Gruppen aus Punkten einer elliptischen Kurve unter anderem für ein (verallgemeinertes) Elgamal-Verfahren (vgl. Esslinger u.a., [11]2013, Stein, 2011, Schulz, [2]2003, oder Witten u.a., 2015, Seite 85 ff. in diesem Heft).

Algebraische Beschreibung

Jetzt kommen wir zur algebraischen Darstellung (vgl. hierzu auch z.B. Buchmann, [5]2010, S.194 f., oder Stein, 2011, S.126), die man durch Einsetzen der entsprechenden Geradengleichung in die Kurvengleichung erhält; alternativ kann man das Folgende auch als Definition nehmen:

▷ $(x, y) + (x, -y) := \mathbb{O}$ (d.h. $P + (-P) = \mathbb{O}$) und
▷ $P + \mathbb{O} := P =: \mathbb{O} + P$

für alle Punkte (x, y) und P aus $\mathscr{C}$. Sind $P,Q \in \mathscr{C}$ mit $Q \neq -P$, und gilt $P = (p_1, p_2)$, $Q = (q_1, q_2)$, so setzt man

▷ $P + Q := (s_1, s_2)$ mit $s_1 = \lambda^2 - p_1 - q_1$ und $s_2 = \lambda p_1 - p_2 - \lambda s_1$

für

$$\lambda = \begin{cases} \frac{q_2 - p_2}{q_1 - p_1} & \text{falls } P \neq Q, -Q \\ \frac{3p_1^2 + b}{2p_2} & \text{falls } P = Q \quad \text{(mit dem } b \text{ aus Gleichung(*))}. \end{cases}$$

Anmerkung: Wie man zeigen kann, ist hierbei $y = \lambda x + (p_2 - \lambda p_1)$ im Falle $p_1 \neq q_1$ die Gleichung der Geraden PQ durch P und Q und $(s_1, -s_2) \in PQ$ bzw. im Falle $P = Q$ und $p_2 \neq 0$ die Gleichung der Tangenten in P.

Fortsetzung der Beispiele

Im Fall der Kurve der Gleichung $y^2 = x^3 + x + 1$ über $K = \mathbb{Z}_5$ (siehe Kapitel „Schnitt von $\overline{\mathscr{C}}$ mit Geraden“ und „Addition von rationalen Punkten“) erhält man aus $\overline{\mathscr{C}}$ (einschließlich des uneigentlichen Punktes $\mathbb{O}$) eine Gruppe mit 9 Elementen. Ist diese zyklisch (also von einem Element erzeugt)? Wir zeigen, dass die Summen („Potenzen“ oder „skalare Vielfache“) des Punktes $P = (0, 1)$ alle Elemente von $\overline{\mathscr{C}}$ ergeben: Aus Bild 11 (nächste Seite) sowie Tabelle 2 sieht man $2P := P + P = (4, 2)$. Ähnlich ergibt sich $3P := 2P + P = (2, 1)$, nämlich wie folgt: Die Gerade durch $P = (0, 1)$ und $2P = (4, 2)$ hat die Gleichung $y = 4x + 1$ (siehe Tabelle 2, vorige Seite) und schneidet $\mathscr{C}$ auch in $(2, 4)$; durch Spiegelung von $(2, 4)$ ergibt sich $3P = (2, 1)$.

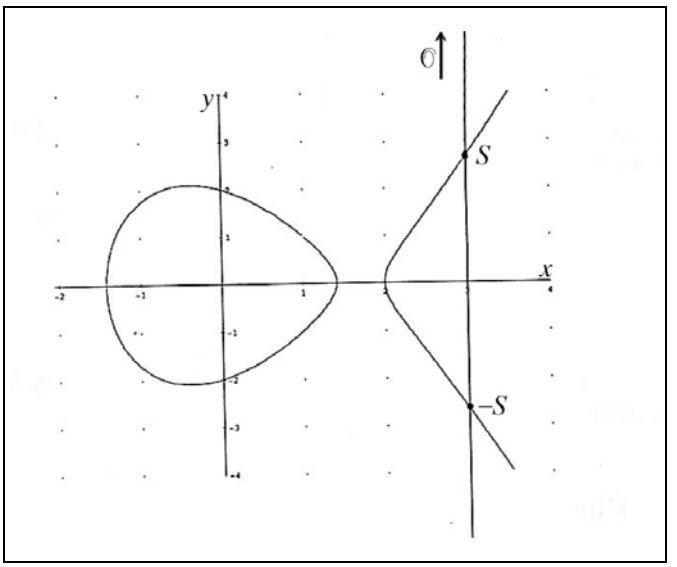


Bild 10: Zur Inversenbildung.

Q	(0, 1)	(0, 4)	(2, 1)	(2, 4)	(3, 1)	(3, 4)	(4, 2)	(4, 3)	$\mathbb{O}$
$a = \log_P Q$	1	8	3	6	5	4	2	7	0

Tabelle 4: Die Logarithmusfunktion $\log_P Q$ des Beispiels.

Addition auf elliptischen Kurven mit SageMath

Beispiel

```
E = EllipticCurve(GF(5);[1,1])
P = E([0; 1]);Q = E([2; 1])
P + P
     (4:2:1)
P + Q
     (3:4:1)
P + P + P + P + P + P + P
     (4:3:1)
```

Dies lässt sich auch aus den zitierten Formeln herleiten: Mit $\lambda = \frac{3\cdot 0+1}{2\cdot 1} \equiv 3 \pmod 5$ erhält man wieder $P + P = (3^2–0–0, 3\cdot 0–1–3s_1) = (4, 2) \neq -P$ sowie (mit $\lambda = \frac{1–2}{0–4} \equiv 4 \pmod 5$) die Beziehung $2P + P = 3P = (2, 1) \neq \mathbb{O}$. Damit erzeugt P eine Untergruppe mit mehr als 3 Punkten (nämlich mindestens mit $\mathbb{O}$, P, $2P$, $3P$). Es ist $(\overline{\mathscr{C}}, +)$ daher nach einem gruppentheoretischen Satz („Die Ordnung $|U|$ jeder Untergruppe U einer endlichen Gruppe G ist Teiler der Ordnung $|G|$ von G“) eine zyklische Gruppe mit $|\overline{\mathscr{C}}| = 9$ Elementen. Dies sieht man auch aus den Werten der Logarithmusfunktion, die in Tabelle 4 (mit $Q = aP \mapsto a$) angegeben sind bzw. aus der Darstellung in Bild 12a. Man beachte z. B. $8P = –P$, $7P = –2P$, $6P = –3P$, $5P = –4P$ und $4P = (3, –1)$.

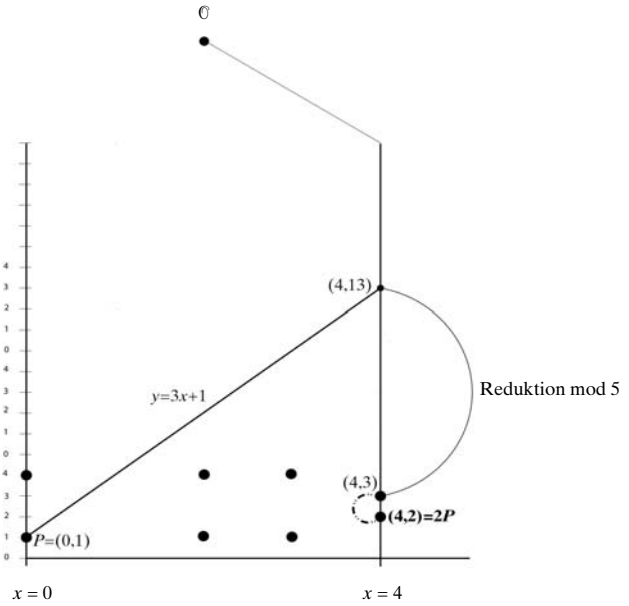


Bild 11: Bestimmung von $P + P$ bei $\overline{\mathscr{C}}_5$: Die Tangente an $\overline{\mathscr{C}}$ durch $P = (0, 1)$ hat die Gleichung $y = 3x + 1$ (siehe auch Tabelle 2); der weitere Schnittpunkt ist (4, 3), sein Spiegelbild $P + P = (4, 2)$. Dick eingezeichnete Punkte sind die Elemente von $\overline{\mathscr{C}}$.

Um „skalare Vielfache“ des Basispunktes P bei größeren Beispielen zu berechnen, kann man eine zur binären Exponentiation (*square and multiply*) analoge Methode benutzen, indem man entsprechend der binären Darstellung von $a = \sum_i a_i 2^i$ (mit $a_i \in \{0, 1\}$) die Punkte 2^iP sukzessive berechnet und dann $\sum_i a_i 2^i P$ bildet. Zum Beispiel: Man berechnet $2P$ und $4P = 2P + 2P$ und dann $7P = P + 2P + 4P$. Einfacher ist es allerdings, die Rechnungen mit SageMath auszuführen (siehe Kasten „Addition auf elliptischen Kurven mit SageMath“, diese Seite). Die Ausgabe erfolgt wohl in homogenen Koordinaten (siehe Kasten „Zum uneigentlichen Punkt $\mathbb{O}$“, Seite 108).

Beispiel: $P + P$ ergibt (4 : 2 : 1), d. h. $2P = (4, 2)$ (siehe Tabelle 4, oben).

Ordnet man die Punkte lexikografisch, wie in Tabelle 4 geschehen, so sieht man, dass $\log_P Q$ (anders als der reelle Logarithmus) schwer vorhersagbar ist (siehe Bild 12b).

Beispiele mit CrypTool

CrypTool 1 (CT1) und JCrypTool (JCT) sind unterschiedliche Lernprogramme aus dem Open-Source-Projekt *CrypTool*. In CT1 findet sich unter dem Menü „Einzelverfahren → Zahlentheorie interaktiv“ das Programm „Punktaddition auf elliptischen Kurven“. Dieses visualisiert verschiedene elliptische Kurven und ermöglicht es, Punktadditionen auf diesen durchzuführen. Die Kurven können entweder über dem Zahlenraum der reellen Zahlen oder über der endlichen Grup-

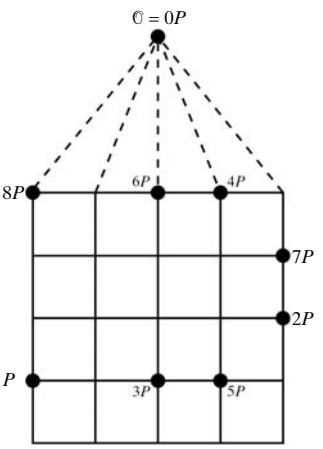


Bild 12a: Elemente der Gruppe $(\overline{\mathscr{C}}_5, +)$ als Vielfache des Punktes P.

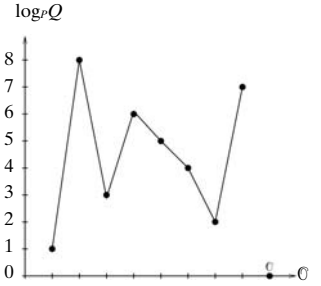


Bild 12b: Schwer vorherzusagender Logarithmus a von $Q = aP$ zum Basispunkt P (Punkte in lexikografischer Ordnung).

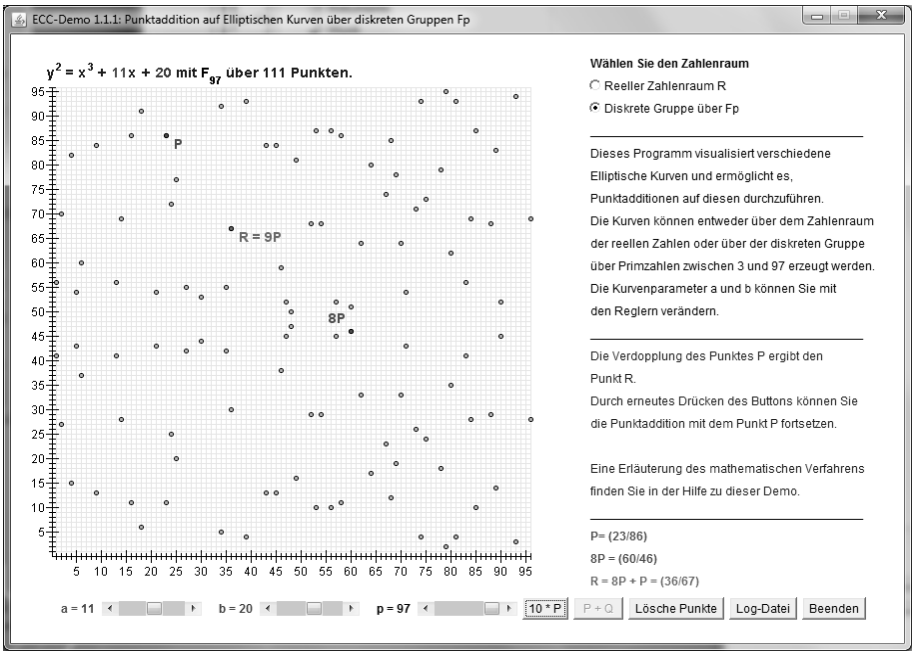


Bild 13:
Bildschirmkopie einer elliptischen Kurve über $\mathbb{Z}_{97}$, erstellt mit CrypTool 1 (CT1).

pe modulo einer Primzahl zwischen 3 und 97 erzeugt werden. Wenn man das nicht-modale Fenster mit den Log-Ausgaben öffnet, kann man seine Aktionen (z.B. fortgesetzte Additionen) parallel verfolgen. Bildschirmkopien von elliptischen Kurven über $\mathbb{Z}_{97}$ bzw. über $\mathbb{R}$ werden in den Bildern 13 und 14 wiedergegeben.

Mit JCT kann man Kryptografie auf den drei Plattformen Linux, MacOS und Windows umfassend ausprobieren. Dabei lassen sich nicht nur Kurven über den reellen Zahlen und Kurven über dem Körper $\mathbb{F}_p = \mathbb{Z}_p$, sondern auch Kurven über dem Körper $\mathbb{F}_{2m} = \mathrm{GF}(2^m)$ berechnen und visualisieren. Im Bild 15 (nächste Seite) ist hierzu eine Bildschirmkopie wiedergegeben.

Anmerkungen

(1) Bei der Anwendung der Gruppe der rationalen Punkte einer elliptischen Kurve in der Kryptologie ist nicht so sehr die abstrakte Gruppe selbst, sondern ihre Darstellung von Bedeutung. Im Gegensatz zur ebenfalls zyklischen Gruppe $(\mathbb{Z}_p, +)$, in der die Gleichung $xg = m$ durch Division zu lösen ist $(x = m/g)$, oder der Berechnung des Logarithmus (also bei gegebenen g und m die Bestimmung eines x mit $g^x = m$) in der multiplikativen Gruppe $(\mathbb{Z}_p^*, \cdot)$, für die ein Algorithmus mit subexponentieller Laufzeit bekannt ist, kennt man bis heute für die Berechnung des diskreten Logarithmus in Gruppen elliptischer Kurven (also bei gegebenem Punkt Q und bekanntem Basispunkt P die Ermittlung von a mit $Q = aP$) nur Algorithmen exponentieller Laufzeit.
Beim öffentlichen Verschlüsselungssystem RSA (vgl z.B. Witten/Schulz, 2011/2012) wird übrigens die Halbgruppe $(\mathbb{Z}_{pq}^*, \cdot)$ für Primzahlen p und q verwendet. Zum Entschlüsseln einer Botschaft c $(= m^e)$ ohne Hintertür wäre die Berechnung der e-ten Wurzel aus c nötig.

(2) Wieviele Punkte enthält eine elliptische Kurve? Dazu zitieren wir den Satz von Helmut Hasse (vgl. Hasse, 1933): Für die Anzahl der Elemente (Ordnung) der Gruppe einer nicht-singulären elliptischen Kurve über $\mathbb{Z}_p$ gilt
$|\overline{\mathcal{C}}| = p + 1 + t$ mit $|t| \leq 2\sqrt{p}$.
Der Satz stellt damit für große p sicher, dass die

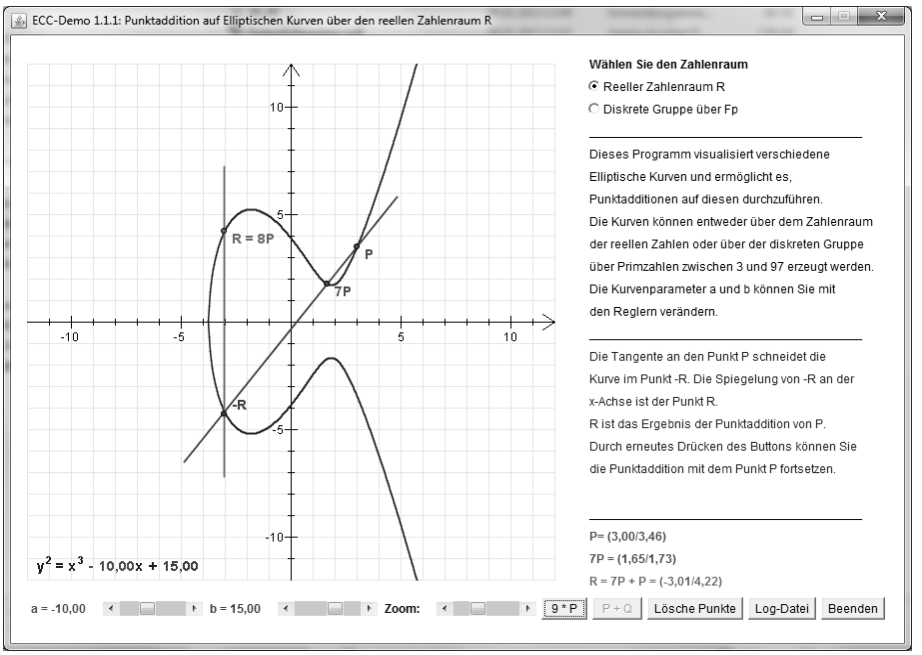


Bild 14:
Bildschirmkopie einer elliptischen Kurve über $\mathbb{R}$, erstellt mit CrypTool 1 (CT1).

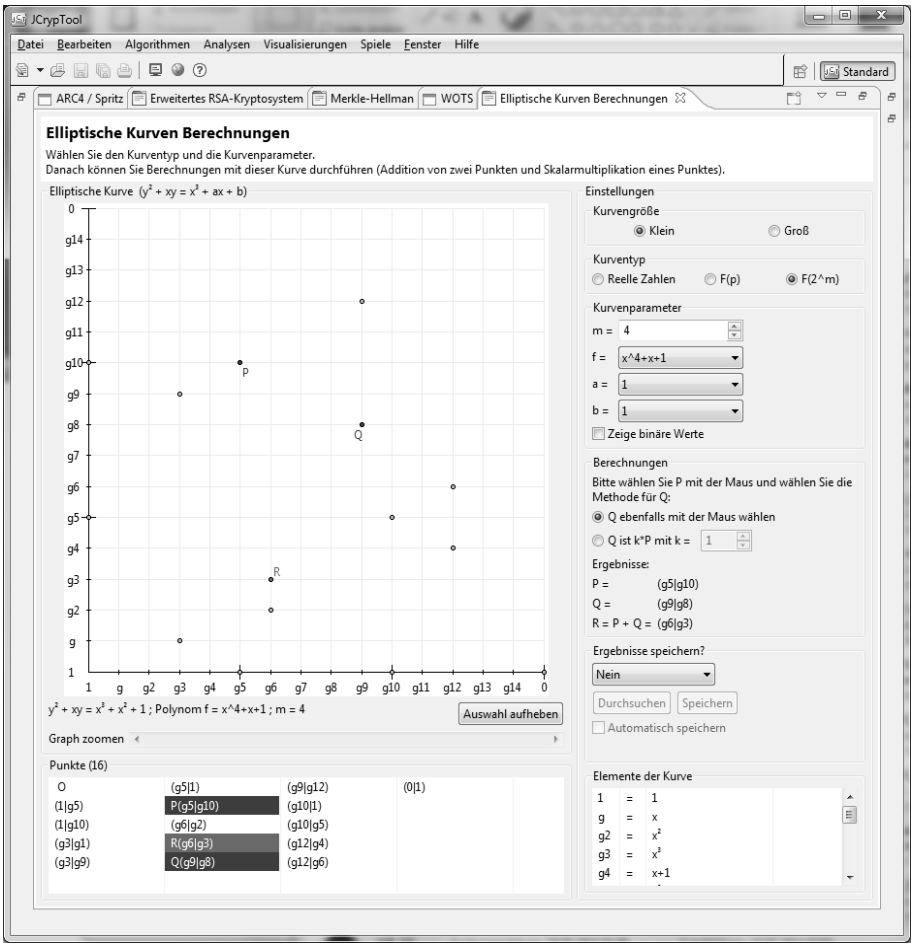


Bild 15: Bildschirmkopie einer elliptischen Kurve über $\mathbb{F}_4$, erstellt mit JCrypTool (JCT).

Anzahl der Punkte einer elliptischen Kurve über $\mathbb{Z}_p$ in der Größenordnung von p liegt. Aber gibt es denn auch genügend elliptische Kurven? Eine Antwort gibt der Satz von Waterhouse/Deuring (vgl. Waterhouse, 1969): Für jede natürliche Zahl n aus dem Intervall $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ existiert eine Gruppe $\mathcal{C}$ einer elliptischen Kurve mit $|\mathcal{C}| = n$. Dabei sind die Ordnungen nahezu gleichverteilt.

(3) Wie schon anfangs erwähnt, hat Hendrik Willem Lenstra 1987 (vgl. Lenstra, 1987) einen Algorithmus zur Faktorisierung von ganzen Zahlen vorgeschlagen, der elliptische Kurven benutzt, insbesondere die Addition auf deren Punkten (vgl. z. B. Stein, 2011, S. 133 f.). Bis zu welcher Größe man natürliche Zahlen faktorisieren kann, ist eine wichtige Frage für die Kryptoanalyse, z. B. des RSA-Systems (vgl. z. B. Witten/Schulz, 2011/2012).

(4) Auch die Primzahl-Tests von Shafi Goldwasser und Joe Kilian (vgl. Goldwasser/Kilian, 1981) sowie von Arthur Atkin und François Morain (vgl. Atkin/Morain, 1993) benutzen elliptische Kurven.

(5) Wie ebenfalls schon erwähnt, garantiert die Verwendung elliptischer Kurven nicht unbedingt die Sicherheit eines kryptografischen Verfahrens. So wurden (laut einem Artikel der *New York Times*) in dem Standard SP 800-90A (der US-Standardisierungsorganisation ***N**ational **I**nstitute of **S**tandards and **T**echnology* – NIST) durch den amerikanischen Geheimdienst NSA vorsätzlich Schwächen eingebaut (vgl. Fischlin, 2014; vgl. auch Ermert, 2014). Der erwähnte Standard beschreibt dabei verschiedene Pseudozufallsgeneratoren. Zum Beispiel werden beim Generator *Dual EC DRBG* (siehe Kasten „Zu einem Pseudozufallsgenerator mit Hintertür“, nächste Seite) eine Folge von Punkten einer elliptischen Kurve generiert und deren Projektionswerte auf die x-Achse als Pseudozufallsfolgen ausgegeben. Obwohl die gewählten Punkte der Kurve uniform verteilt sind, sind es die x-Koordinaten der Punkte nicht, da ein erheblicher Anteil der infrage kommenden Zeichenketten aus $\{0, 1\}^{240}$ nicht von Kurvenpunkten getroffen und daher nicht generiert wird. Ein möglicher Angriff ist ebenfalls in Kasten „Zu einem Pseudozufallsgenerator mit Hintertür“, nächste Seite, beschrieben.

(6) In dem Online-Artikel von Monika Ermert und den darin zitierten Artikeln (vgl. Ermert, 2014) findet man eine Zusammenfassung zum gegenwärtigen Stand der Vertrauenswürdigkeit der Elliptischen-Kurven-Verschlüsselung und die Aufforderung, statt der von der NIST empfohlenen elliptischen Kurven neue Kurvenvarianten mit einfacheren Kurvengleichungen zu verwenden. Laut einer Analyse von Tanja Lange und Dan Bernstein nutzen nämlich die Attacken bei bisherigen Standardkurven gerade nicht Schwächen im Logarithmus der Kurve, sondern die Fehleranfälligkeit der auf sehr komplexen Rechenregeln beruhenden Implementierungen (vgl. Bernstein/Lange, 2014).
Eine von Dan Bernstein als Alternative propagierte „Curve 25519“ hat die Gleichung
$y^2 = x^3 + 486662x^2 + x$,
über dem Körper mit p^2 Elementen (und auf $\mathbb{Z}_p$ eingeschränkter x-Koordinate) für $p = 2^{255} - 19$ (vgl. Bernstein, 2006). Diese *Bernstein-Kurve* ist inzwischen auf dem Weg zum Standard für TLS (dem Nachfolger von SSL) und wird bereits von OpenSSH und GnuPG benutzt (vgl. Schmidt, 2015).
Weitere empfohlene Typen von elliptischen Kurven (mit leichter zu implementierender Addition) sind die *Montgomery-Kurven*, zu denen die Bernstein-

Zu einem Pseudozufallsgenerator mit Hintertür

Die folgende Beschreibung basiert auf dem Artikel von Marc Fischlin (vgl. Fischlin, 2014).
Beim Generator ***Dual Elliptic Curve Deterministic Random Bit Generator*** (Dual EC DRBG) werden eine Primzahl p (z. B. $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} + 1$) sowie Konstanten a und b spezifiziert und die elliptische Kurve

$$E_{a,b}(\mathbb{F}_p) = \{(x, y) \in (\mathbb{F}_p)^2 \mid y^2 = x^3 + ax + b\}$$

herangezogen. Im Standard werden dann zusätzlich zwei (vom unendlichen Punkt verschiedene) Kurvenpunkte $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$ gewählt; dabei wird P als Erzeuger der additiven Gruppe genommen.
Beginnend mit einem zufälligen Startwert $s_0 \in \mathbb{F}_p$ generiert das Verfahren in jeder Runde zunächst 240 Pseudozufallsbits, indem es ausgehend von s_i den Kurvenpunkt s_iP bestimmt und die untersten 240 der 256 Bits der x-Koordinate dieses Punktes (in der üblichen Binärdarstellung) als s_{i+1} speichert. Dann berechnet es $s_{i+1}Q$ und gibt die untersten 240 Bits der 256 Bits der x-Koordinate dieses Punktes aus.
Bereits kurz nach Erscheinen des Standards zeigten die ersten Analysen, dass die Ausgaben nicht die übliche Sicherheit bieten. Dan Shumow und Niels Ferguson konnten schließlich im Jahr 2007 zeigen, wie man aus der Kenntnis von e mit $P = eQ$ und der Ausgabe $r \in \{0, 1\}^{240}$ der i-ten Iteration die weiteren Ausgaben vorhersagen kann (vgl. Shumow/Ferguson, 2007). Dabei berechnet man u. a. alle möglichen 2^{16} Bitfolgen der Länge 256, die auf r enden, und prüft, welche dieser Bitfolgen die x-Koordinaten eines Kurvenpunkts sind. Der „richtige" Punkt $s_{i+1}Q$ ist dann unter den maximal $2 \cdot 2^{16}$ so gefundenen Punkten $R_1, R_2, \ldots$ enthalten und $s_{i+1}P = s_{i+1}(eQ) = e(s_{i+1}Q)$ unter $eR_1, eR_2, \ldots$. Damit sind die möglichen nächsten Zustandsvektoren bekannt, und nach weiteren Iterationsrunden lassen sich die potenziellen Kandidaten auf ein Element reduzieren.

kurve gehört, mit einer Gleichung der Form $By^2 = x^3 + Ax^2 + x$ und (in einer Erweiterung des Begriffs „elliptische Kurve") auch die *Edwards-Kurven* mit einer Gleichung der Form $ax^2 + y^2 = 1 + dx^2y^2$.

(7) Für eine elementare Vorbereitung (durch die Addition auf der Uhr) und Einführung in die ECC empfehlen wir das YouTube-Video *ECCHacks – A gentle introduction to elliptic-curve cryptography* (und die zugehörigen PYTHON-Skripte) von Bernstein und Lange (2014).

(8) Die Verwendung elliptischer Kurven in der Kryptografie ist trotz der angedeuteten Schwächen (auch laut Werner, [4]2013) „ein Beispiel für die verblüffende Nützlichkeit der reinen Mathematik". Dieses Lob steht im Gegensatz zur Ansicht von Godfrey Harold Hardy (1877–1947): „Die schönste Mathematik für Hardy war die reine Mathematik, die keine Anwendungen in der Außenwelt findet, insbesondere sein eigener spezieller Bereich, die Zahlentheorie. Er begründet das Streben nach der reinen Mathematik mit dem Argument, dass ihre Nutzlosigkeit bedeute, dass sie niemals missbraucht werden könne, um Schaden anzurichten" (Wikipedia – Stichwort „Apologie eines Mathematikers"). Schon vor Hardy hatte Carl Gustav Jacobi (1804–1851) als „einziges Ziel der Wissenschaft die Ehre des menschlichen Geistes" genannt, auf den von Jean Baptiste Joseph Fourier (1978–1830) u. a. propagierten „Gemeinnutzen" antwortend (vgl. dazu Siegmund-Schultze, 2013).

(9) Aber es gibt auch bedeutende (zurzeit) nur innermathematische Anwendungen, z. B. (vgl. Brown, 2000): die Lösung des (vorher z. B. von Diophant, Fermat und Euler behandelten) Problems der „kongruenten Zahl" (d. h. der Größe des Flächeninhalts eines rechtwinkligen Dreiecks mit rationalen Seitenlängen) durch Jerrold Tunnell 1983 und die Transformation des Großen Satzes von Fermat in ein Problem über elliptische Kurven durch Gerhard Frey 1986, die dann 1995 zum Beweis des Großen Satzes von Fermat durch Andrew Wiles und Richard Taylor führte.

Prof. Dr. Ralph-Hardo Schulz
Freie Universität Berlin
Fachbereich Mathematik und Informatik
Institut für Mathematik
Arnimallee 3
14195 Berlin

E-Mail: schulz@math.fu-berlin.de

Helmut Witten
Brandenburgische Straße 23
10707 Berlin

E-Mail: helmut@witten-berlin.de

Prof. Bernhard Esslinger
Universität Siegen
Institut für Wirtschaftsinformatik
Hölderlinstraße 3
57076 Siegen

E-Mail: bernhard.esslinger@uni-siegen.de

Literatur und Internetquellen

Atkin, A. O. L.; Morain, F.: Elliptic curves and primality proving. In: Mathematics of Computation, Band 61 (1993), Nr. 203, S. 29-68.
http://www.ams.org/journals/mcom/1993-61-203/S0025-5718-1993-1199989-X/S0025-5718-1993-1199989-X.pdf

Bernstein, D. J.: Curve25519 – new Diffie-Hellman speed records. 09.02. 2006.
http://cr.yp.to/ecdh/curve25519-20060209.pdf
http://cr.yp.to/ecdh.html#curve25519-paper.html

Bernstein, D. J.; Lange, T.: ECCHacks – A gentle introduction to elliptic-curve cryptography. 28.12. 2014.
Video mit Vortrag:
https://www.youtube.com/watch?v=l6jTFxQaUJA
Gliederung und PYTHON-Skripte:
http://ecchacks.cr.yp.to/

Beutelspacher, A.; Neumann, H.; Schwarzpaul, Th.: Kryptografie in Theorie und Praxis – Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld. Reihe „Studium“. Wiesbaden: Vieweg+Teubner, [2]2010.

Brenner, M.: ENISA-Empfehlungen zu Krypto-Verfahren. heise Security, 11.11.2013.
http://www.heise.de/security/artikel/ENISA-Empfehlungen-zu-Krypto-Verfahren-2043356.html

Brown, E.: Three Fermat Trails to Elliptic Curves. In: The College Mathematics Journal, Band 31 (2000), Nr. 3, S. 162–172.
http://www.math.vt.edu/people/brown/doc/ellip.pdf

BSI – Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzkataloge – M 3.23 Einführung in kryptographische Grundbegriffe. 2013.
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03023.html

Buchmann, J.: Einführung in die Kryptographie. Heidelberg u. a.: Springer, [5]2010.

CrypTool 1 (CT 1):
http://www.cryptool.org/de/cryptool1

ENISA – European Union Agency for Network and Information Security: Algorithms, Key Sizes and Parameters Report. 2013 recommendations. October 2013.
http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

Ermert, M.: Nach Snowden – Wenig Schlaf für Kryptoforscher. heise Security im Gespräch mit der Kryptologin Tanja Lange. heise Security, 17.09.2014.
http://www.heise.de/security/artikel/Nach-Snowden-Wenig-Schlaf-fuer-Kryptoforscher-2392236.html

Esslinger, B. u. a.: Das CrypTool-Skript – Kryptographie, Mathematik und mehr. Hintergrundmaterial und Zusatzinformationen zum freien E-Learning-Programm CrypTool (mit Code-Beispielen zur Zahlentheorie, geschrieben in Sage). [11]2013.
https://www.cryptool.org/images/ctp/documents/CrypToolScript-de-draft.pdf

Fischlin, M.: Hintertüren und Schwächen im kryptographischen Standard SP 800-90A. In: Mitteilungen der Deutschen Mathematiker-Vereinigung, Band 22 (2014), Heft 1, S. 18–22.
http://www.degruyter.com/view/j/dmvm.2014.22.issue-1/dmvm-2014-0012/dmvm-2014-0012.xml?format=INT

Goldwasser, Sh.; Kilian, J.: Almost all primes can be quickly certified. In: J. Hartmanis (Hrsg.): STOC '86 – Eighteenth Annual ACM Symposium on Theory of Computing, Berkeley, CA, USA – May 28–30, 1986. New York: ACM,1986, S. 316–329.
http://groups.csail.mit.edu/cis/pubs/shafi/1986-stoc-gk.pdf

Hasse, H.: Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. In: Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, 40. Jg. (1933); Band 1933, S. 253–262.
http://gdz.sub.uni-goettingen.de/dms/load/img/?PPN=GDZPPN002509288&IDDOC=64289

JCrypTool (JCT):
https://www.cryptool.org/de/jcryptool

Knapp, A. W.: Elliptic Curves. Princeton (NJ, USA): Princeton University Press, 1992.

Lenstra, A. K.; Verheul, E. R.: Selecting Cryptographic Key Sizes. In: H. Imai, Y. Zheng (Hrsg.): Public Key Cryptography – Third International Workshop on Practice and Theory in Public Key Cryptosystems – PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000 – Proceedings.. Reihe „LNCS – Lecture Notes in Computer Science“, Band 1751. Berlin u. a.: Springer, 2000, S. 446–465.
http://link.springer.com/chapter/10.1007%2F978-3-540-46588-1_30

Lenstra, H. W.: Factoring integers with elliptic curves. In: Annals of Mathematics, Second Series, Band 126 (1987), Heft 3, S. 649–673.
http://wstein.org/edu/2010/414/refs/lenstra_factor.pdf

Massierer, M.: ECC Notebook – An Interactive Introduction to Elliptic Curve Cryptography. 2011.
http://webloria.loria.fr/~mmassier/ecc-notebook/

Schmidt, J.: Konkurrenz für die NIST – Bernsteins Elliptische Kurven auf dem Weg zum Standard. heise Security, 27.02.2015.
http://www.heise.de/security/meldung/Konkurrenz-fuer-die-NIST-Bernsteins-Elliptische-Kurven-auf-dem-Weg-zum-Standard-2560881.html

Schneier, B.: Elliptic Curve Crypto Primer. Schneier on Security (Blog), 06.11.2013.
https://www.schneier.com/blog/archives/2013/11/elliptic_curve.html

Schulz, R.-H.: Codierungstheorie – Eine Einführung. Wiesbaden: Vieweg, [2]2003.

Shumow, D.; Ferguson, N.: On the Possibility of a Back Door in the NIST SP800-90 Dual EC PRNG. In: CRYPTO 2007 Rump Session. 21.08.2007.
http://rump2007.cr.yp.to/15-shumow.pdf

Siegmund-Schultze, R.: Für die Ehre des menschlichen Geistes – Ein neuer Blick auf die bekannte Kontroverse zwischen Fourier und Jacobi über die Rolle der Anwendungen der Mathematik. Mitteilungen der Deutschen Mathematiker-Vereinigung, Band 21 (2013), Heft 2, S. 112–118.
http://www.degruyter.com/view/j/dmvm.2013.21.issue-2/dmvm-2013-0042/dmvm-2013-0042.xml?format=INT

Silverman, J. H.: The Arithmetic of Elliptic Curves. Reihe „Graduate Texts in Mathematic“. Dordrecht; Heidelberg u. a.: Springer, [2]2009.

Silverman, J. H.; Tate, J.: Rational Points on Elliptic Curves. Reihe „Undergraduate Texts in Mathematic“. New York: Springer, 1992.
http://link.springer.com/book/10.1007%2F978-1-4757-4252-7

Stein, W.: Elementary Number Theory – Primes, Congruences, and Secrets. 16.11.2011.
http://wstein.org/ent/ent.pdf

Sullivan, N.: A (relatively easy to understand) primer on elliptic curve cryptography – Everything you wanted to know about the next generation of public key crypto. 24.10.2013.
http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

Waterhouse, W. Ch.: Abelian varieties over finite fields. In: Annales scientifiques de l'École Normale Supérieure, (4) 2. Jg. (1969), Heft 4, S. 521–560.

Weis, R.: Kryptographie nach Snowden. In: M. Beckedahl, A. Meister (Hrsg.): Überwachtes Netz – Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications in Kooperation mit epubli GmbH, 2013, S. 260–268.
https://netzpolitik.org/wp-upload/Ueberwachtes-Netz-Markus-Beckedahl-Andre-Meister.pdf

Werner, A.: Elliptische Kurven in der Kryptographie. Berlin u. a.: Springer, [4]2013.

Wikipedia – Stichwort „Apologie eines Mathematikers“:
http://de.wikipedia.org/wiki/Apologie_eines_Mathematikers

Wikipedia – Stichwort „Elliptic Curve Cryptography“:
http://de.wikipedia.org/wiki/Elliptic_Curve_Cryptography

Witten, H.; Schulz, R.-H.: RSA & Co. in der Schule – Moderne Kryptologie, alte Mathematik, raffinierte Protokolle. Neue Folge – Teil 6: Das Faktorisierungsproblem oder: Wie sicher ist RSA? In: LOG IN, 31. Jg. (2011/2012), Heft 172/173, S. 59–69.

Witten, H.; Schulz, R.-H.; Esslinger, B.: RSA & Co. in der Schule – Moderne Kryptologie, alte Mathematik, raffinierte Protokolle. Neue Folge – Teil 7: Alternativen zu RSA oder: Diskreter Logarithmus statt Faktorisierung. In: LOG IN, 35. Jg. (2015), Heft 181/182, S. 85–102 *(in diesem Heft)*.

Alle Internetquellen wurden zuletzt am 15. September 2015 geprüft und können auch aus dem Service-Bereich des LOG IN Verlags (http://www.log-in-verlag.de/) heruntergeladen werden.