Elliptic Curve Cryptography

Valentin Dietrich

19.05.2021

Abstract

In diesem Vortrag werden wir uns mit elliptischen Kurven und ihren Anwendungen in der Kryptographie beschäftigen. Hierzu werden zunächst Laufzeitbetrachtungen für Lösungsalgorithmen zur Primfaktorzerlegung und des herkömmlichen diskreten Logarithmusproblems, wo sich bei elliptischen Kurven Vorteile ergeben, als Motivation vorgestellt. Danach schauen wir uns nach einer Definition des Begriffs an, wie man auf elliptischen Kurven Gruppenoperationen ausführen kann, und betrachten ein paar einfache Rechenbeispiele. Zuletzt folgen noch ein paar Überlegungen dazu, welche Eigenschaften konkret vonnöten sind, um Gruppen über elliptischen Kurven als Grundlage kryptographischer Verfahren nutzen zu können.

1 Motivation

Gängige Verschlüsselungsverfahren wie RSA oder Elgamal bauen auf der Härte der Primfaktorzerlegung bzw. des diskreten Logarithmusproblems (DLP) auf. Obwohl es für diese in der Tat im allgemeinen nur Algorithmen mit exponentieller Laufzeit gibt, stellt zB. das sogenannte Zahlkörpersieb dennoch eine deutliche Verbesserung gegenüber Brute-Force Verfahren dar:

- Brute-Force Faktorisierung einer Zahl N mit n Bits:
  Probiere $2, \ldots, \sqrt{N}$ als mögliche Faktoren durch,
  jede solche Division kostet $\mathcal{O}(n^2)$

$\rightarrow$ Laufzeit von $\mathcal{O}(2^{\frac{n}{2}} \cdot n^2)$

- Zahlkörpersieb:
$$\mathcal{O}\left(e^{c\cdot\ln(n)^{\frac{1}{3}}\cdot(\ln\ln(n))^{\frac{2}{3}}}\right) \subset \mathcal{O}\left(n^{c\cdot(\ln\ln(n))}\right)$$
  wobei $c \approx 1.9$ im generellen Fall

- Schnellster Algorithmus für diskreten Logarithmus auf elliptischen Kurven: $\mathcal{O}(2^{\frac{n}{2}})$

Da das Zahlkörpersieb zwar auf Primfaktorzerlegung und das herkömmliche DLP, jedoch nicht zum Lösen des DLPs auf elliptischen Kurven angewendet werden kann, sind zyklische Gruppen über elliptischen Kurven als Grundlage kryptographischer Verfahren eine interessante Alternative.

2 Elliptische Kurven

2.1 Definition

Falls E die Kurve einer Gleichung

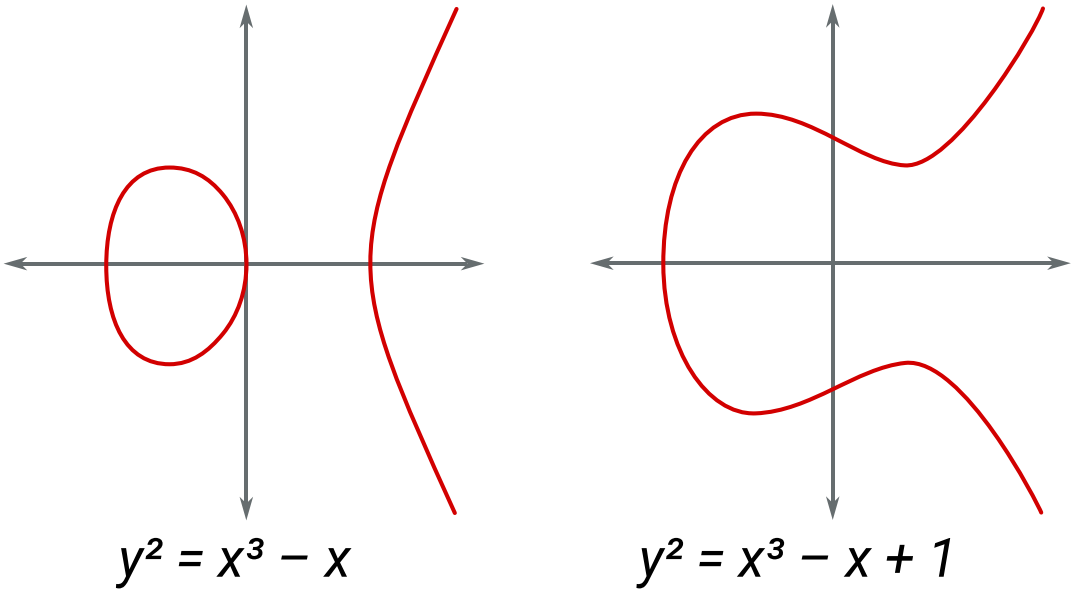
$$y^2 + y(mx + n) = x^3 + px^2 + qx + r$$

ist, nennen wir $E \cup \{\mathcal{O}\}$ eine *elliptische Kurve*.
$\mathcal{O}$ bezeichnet hierbei den '*point at infinity*', bekannt aus der projektiven algebraischen Geometrie.
Oft schreibt man auch nur E statt explizit $E \cup \{\mathcal{O}\}$.

Diese Gleichung lässt sich durch Koordinatentransformationen vereinfachen, man erhält (je nach unterliegendem Körper) die 4 *Weierstraß*-Gleichungen

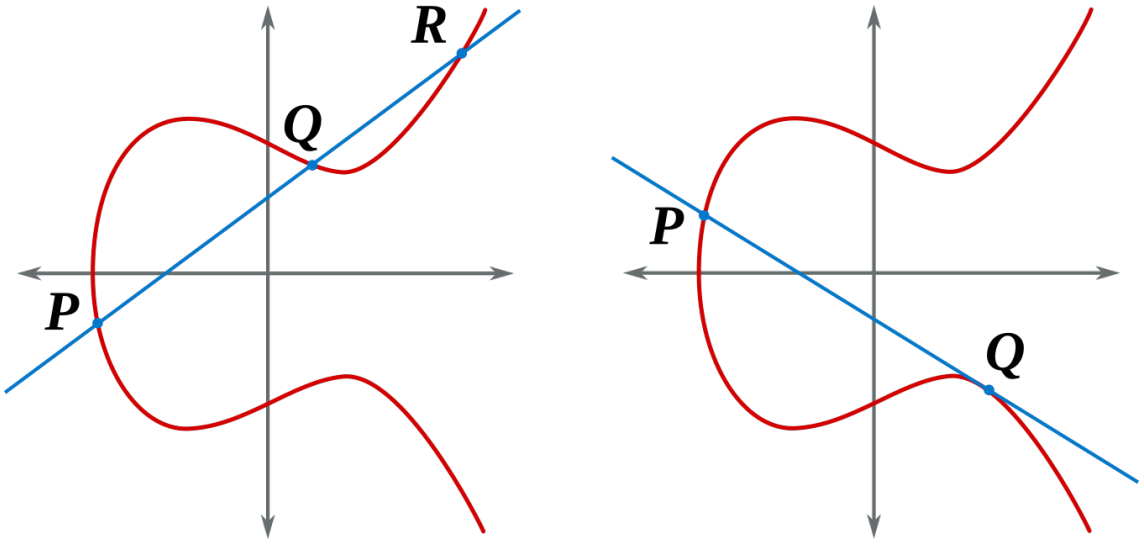
$$\begin{aligned} y^2 &= x^3 + ax + b \\ y^2 &= x^3 + ax^2 + bx + c \\ y^2 + cy &= x^3 + ax + b \\ y^2 + xy &= x^3 + ax^2 + b \end{aligned}$$

Im folgenden werden wir hauptsächlich Gleichungen der ersten Form betrachten, wie in diesen 2 Beispielen aus Wikipedia:



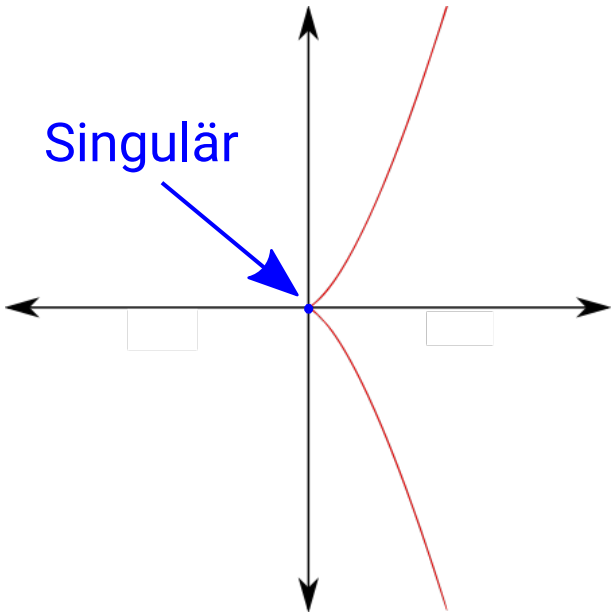
2.2 Eigenschaften

Man sieht recht direkt, dass elliptische Kurven symmetrisch zur x-Achse sind.
Eine weitere wichtige Eigenschaft, auf welcher die später definierte Gruppenoperation aufbaut, ist die, dass im Allgemeinen eine Gerade durch zwei Punkte der Kurve diese in einem weiteren schneidet:



Wir fordern zuletzt noch *Regularität* der Kurve, also das Abhandensein von Punkten, an denen sich keine eindeutige Tangente finden lässt. Hierzu reicht es, $27b^2 + 4a^3 \neq 0$ (bzw. je nach unterliegendem Körper $b \neq 0$)

zu fordern, was ungünstige Vielfachheiten von Nullstellen verhindert. Ein Beispiel für eine Kurve mit singulärem Punkt ist die Kurve $y^2 = x^3$:



3 Gruppenoperationen auf Elliptischen Kurven

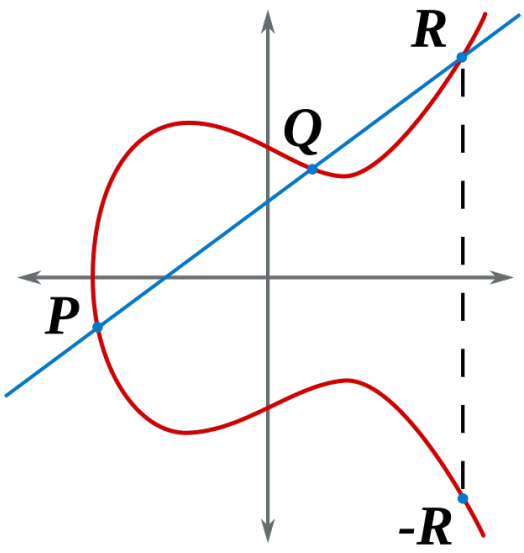
Wie vorher schon vorweggenommen, nutzen wir hier die Eigenschaft, dass Geraden durch zwei Punkte einer elliptischen Kurve sich bis auf Spezialfälle in einem dritten Punkt mit der Kurve schneiden.

3.1 Definition

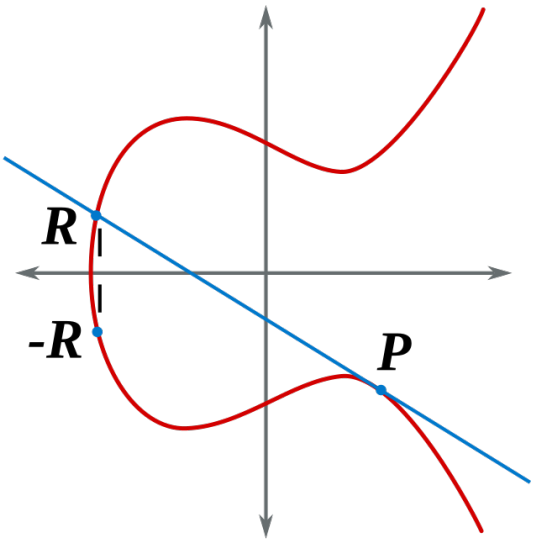
Für eine elliptische Kurve $E \cup \{\mathcal{O}\}$, definiere

$$\begin{aligned} + : E \times E &\to E \\ (P, Q) &\mapsto -R \end{aligned}$$

wobei R der dritte Schnittpunkt der Geraden $\overline{PQ}$ ist, und $-R$ dessen Spiegelung an der x-Achse. Falls $P = Q$ gilt, wählen wir hierbei statt $\overline{PQ}$ die Tangente der Kurve am Punkt P; an dieser Stelle ist die Regularität wichtig, da die Tangente sonst nicht zwingend eindeutig existiert.
Diese Gruppenoperation ist im folgenden (leicht abgewandelt aus Wikipedia) illustriert:



P + Q = -R

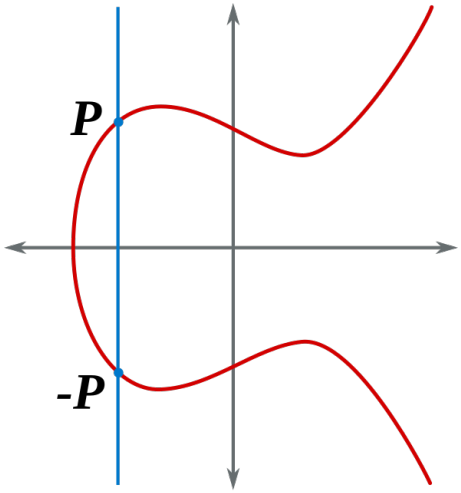


P + P = -R

Falls die Gerade durch P und Q senkrecht zur x-Achse steht, also im affinen Raum kein dritter Schnittpunkt existiert, so definieren wir $P + Q := \mathcal{O}$. Insbesondere sei

$$P + \mathcal{O} = P$$
$$P - P = \mathcal{O}$$

Damit wird $\mathcal{O}$ zum neutralen Element der Gruppe $(E, +)$. Man schreibt daher auch 0 für $\mathcal{O}$. Auch hierzu eine Illustration:



P - P = 0

Im Folgenden werden wir noch anhand eines Beispiels die Berechnung des dritten Schnittpunktes demonstrieren.

3.2 Berechnung des dritten Schnittpunkts

Grundsätzlich handelt es sich hierbei nur um simple Geometrie.

Sei also $y^2 = x^3 + ax + b$ regulär und P, Q Punkte $\neq \mathcal{O}$ mit $Q \neq -P$.

Die Gerade $\overline{PQ}$ hat nun die Form $y = mx + n$ mit Steigung $m = \frac{y_Q - y_P}{x_Q - x_P}$, es ergibt sich also durch Einsetzen von P direkt $n = y_P - mx_P$.
Um alle Schnittpunkte zu erhalten, kann man dies nun mit der Kurvengleichung gleichsetzen:

$$x^3 - (mx + n)^2 + ax + b = 0$$

Es stellt sich heraus, dass die Bedingung $Q \neq -P$ garantiert, dass wir tatsächlich genau 3 Nullstellen für x erhalten. Diese sind x_P, x_Q, x_R, also jeweils die x-Koordinate der Schnittpunkte, wobei R der gesuchte dritte Schnittpunkt ist.
Nun können wir dieses Polynom auch als seine Zerlegung

$$(x - x_P)(x - x_Q)(x - x_R) = x^3 + x^2(-x_P - x_Q - x_R) + x(x_P x_Q + x_P x_R + x_Q x_R) - x_p x_Q x_R$$

schreiben. Vergleicht man jetzt die Koeffizienten des Monoms x^2, so sieht man, dass

$$m^2 = x_P + x_Q + x_R$$

gelten muss. Hierraus ergeben sich dann schlussendlich die Koordinaten des Punktes R:

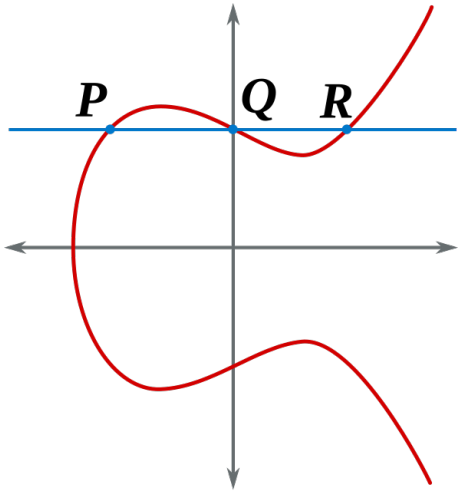
$$x_R = m^2 - x_P - x_Q, \quad y_R = mx_R + n$$

Spiegelt man diesen noch an der x-Achse, indem man die y-Koordinate negativiert, entspricht das Resultat dem Punkt $P + Q$.

Das wollen wir nun einmal anhand eines einfachen Beispiels durchrechnen.
Wir betrachten die schon oft illustrierte Kurve der Gleichung $y^2 = x^3 - x + 1$, wählen uns auf dieser zwei Punkte, $P = (-1, 1)$ und $Q = (0, 1)$, und verfahren wie eben.

Wir berechnen also zunächst die Geradengleichung der Gerade $\overline{PQ}$. Es gilt $y = mx + n$ mit $m = \frac{y_Q - y_P}{x_Q - x_P} = 0$, $n = y_P - mx_P = 1$, insgesamt erhalten wir also $y = 1$. Mit den nun bekannten Werten $m = 0, n = 1$ können wir direkt unseren dritten Punkt berechnen, und erhalten $x_R = m^2 - x_P - x_Q = 1$ und $y_R = mx_R + n = 1$, also $R = (1, 1)$.

Schaut man sich dies geometrisch an, sieht man, dass dies in der Tat dem gesuchten Punkt zu entsprechen scheint:



P + Q + R = 0

4 Anwendung in der Kryptographie

4.1 Gewünschte Eigenschaften

Welche Eigenschaften müssen wir nun noch fordern, damit die so definierten Gruppen über elliptischen Kurven in der Kryptographie anwendbar sind?

- Wir wollen zugrundeliegende Rechnungen bestehender kryptographischer Verfahren direkt wie gewohnt anwenden können, und hierbei ähnlich effizient (bezüglich Laufzeiten von Ver-/Entschlüsselung) sein. Wir hätten also zB. gerne, dass die Gruppen **zyklisch** sind, sodass wir in Verfahren wie dem Diffie-Hellman Schlüsselaustausch ein erzeugendes Element auswählen können.
- Von extremer Wichtigkeit ist, dass wir die Gruppenelemente, also Punkte der elliptischen Kurve, eindeutig im Binärsystem darstellen können. Das läuft insbesondere darauf hinaus, dass die Gruppen **endlich** sind.
- Es muss nach wie vor garantiert sein, dass es eine Einwegfunktion gibt, also eine Funktion deren Rückrichtung schwer zu lösen ist.

Wir werden sehen, dass wir diese Eigenschaften durch korrekte Wahl des unterliegenden Körpers, sowie der konkreten elliptischen Kurve selbst, erhalten können.

4.2 Wahl des Körpers

Zunächst können wir als unterligenden Körper direkt $\mathbb{R}$ oderund $\mathbb{C}$ ausschließen, denn über beiden sind die Kurven kontinuierlich und damit nicht endlich.

Ist E eine elliptische Kurve über $\mathbb{Q}$, so gilt nach dem Satz von Mordell-Weil

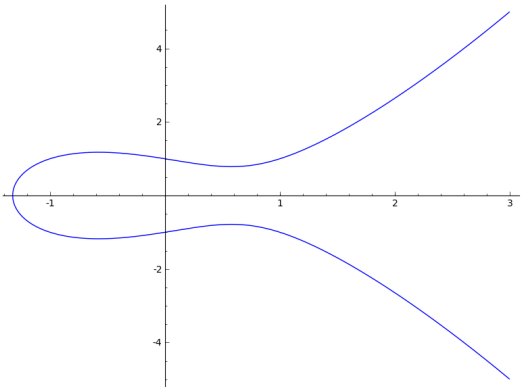
$$E \simeq Tors(E) \oplus \mathbb{Z}^r$$

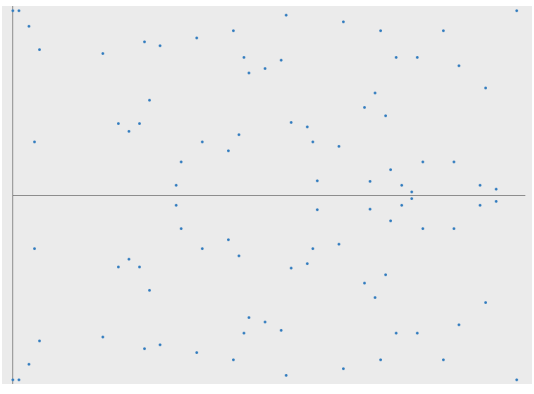
für ein $r \in \mathbb{N}_0$. Für $r > 0$ ist dies wieder nicht endlich; für $r = 0$ bleiben nur noch Torsionselemente übrig, sodass die Gruppe nicht mehr zyklisch ist.
Es bleiben noch die endlichen Körper $\mathbb{F}_q$. Diese liefern das Gewünschte, denn es gibt nur endlich viele $x \in \mathbb{F}_q$, und höchstens 2 Lösungen der Gleichung $y^2 = x^3 + ax + b$ für jedes fixe solche x. Zusammen mit dem Punkt $\mathcal{O}$ ergibt sich für $|E/\mathbb{F}_q|$, die Anzahl der Gruppenelemente der elliptischen Kurve E über dem Körper $\mathbb{F}_q$, die Ungleichung

$$|E/\mathbb{F}_q| \leq 2q + 1$$

womit die Gruppe endlich ist.

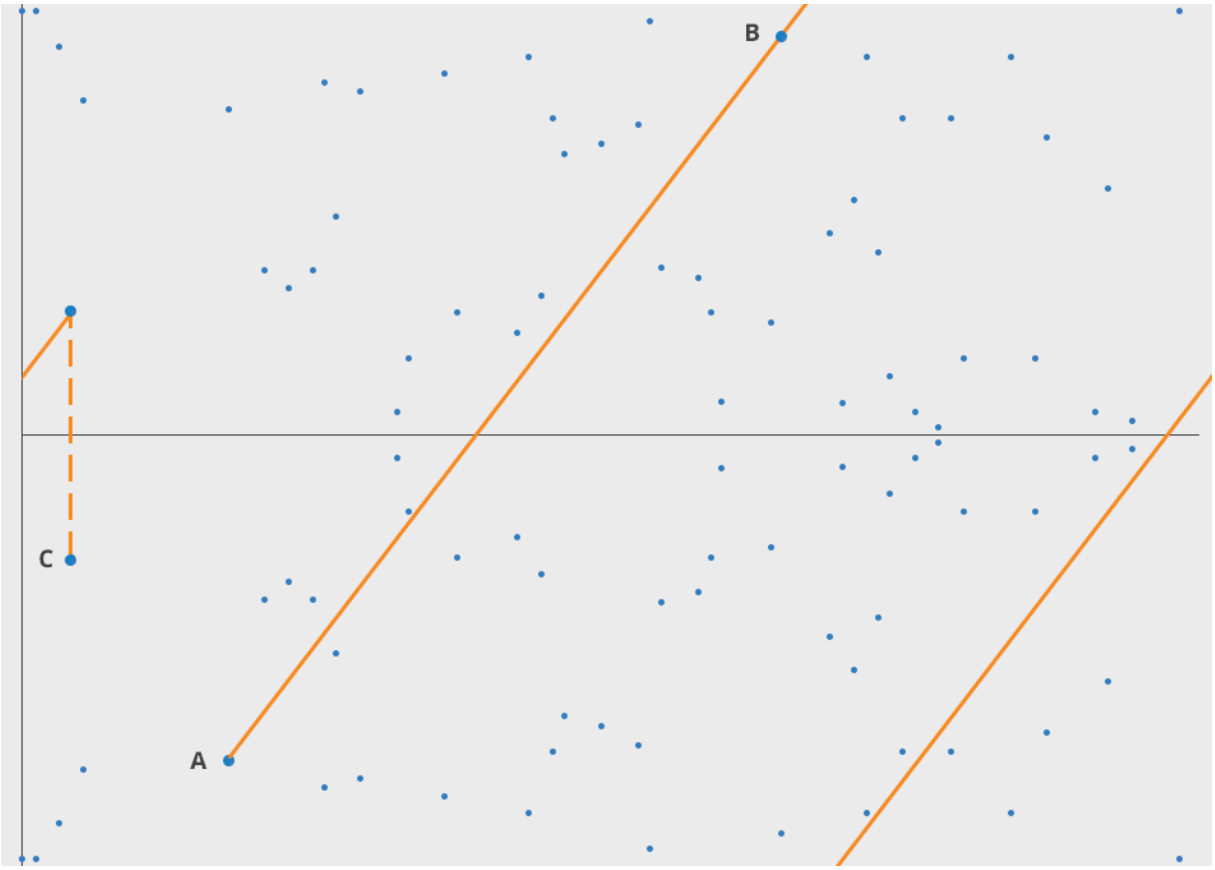
Graphisch entsprechen Kurven dieser Art genau den Punkten mit ganzzahligen Koordinaten, wobei man zusätzlich das Koordinatensystem periodisch bei q 'umklappt'. Man betrachte zum Beispiel[1] wieder die Kurve $y^2 = x^3 - x + 1$, einmal über $\mathbb{R}$ und einmal über $\mathbb{F}_{97}$:





[1] Diese zwei Bilder, sowie das nächste Bild, stammen aus folgendem Artikel:
`https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/`

Das 'Umklappen' wird besonders deutlich, indem wir eine Gruppenoperation $A + B = C$ zeigen:



Man sieht, dass die Gerade durch A und B einfach solange (mit Umklappen) fortgesetzt wird, bis wir wieder auf einen ganzzahligen Punkt stoßen.

4.3 Wahl der Kurve

Neben der Wahl des Körpers ist auch die Wahl der elliptischen Kurve selbst interessant. Hierbei ergeben sich nämlich Unterschiede was die Berechnungen der Gruppenoperationen, sowie bestimmte Sicherheitsfaktoren (zB. Robustheit gegen Timing-Attacken) angeht. Zum Beispiel sind Kurven über $\mathbb{F}_{2^n}$ besonders gut im Binärsystem darstellbar, allerdings erleichtern diese auch das Lösen des diskreten Logarithmusproblems.
Aus diesem Grund gibt es Datenbanken ausgiebig erforschter, kryptographisch sicherer elliptischer Kurven, die insbesondere auch performante Berechnungen zulassen.

4.4 Beispiel Elliptic Curve Diffie-Hellman

Zuletzt zeigen wir noch kurz, wie sich Gruppen über elliptischen Kurven beim Diffie-Hellman Schlüsselaustausch anwenden lassen, um zu demonstrieren, dass sich am eigentlichen Verfahren in der Tat nichts ändert:

1. Alice und Bob einigen sich auf Kurve E, einen zugrundeliegenden Körper K, und einen erzeugenden Punkt P auf der Kurve. Diese Informationen sind auch einem Angreifer bekannt.

2. Alice und Bob wählen jetzt jeweils eine zufällige Zahl $< |E/K|$ als privaten Schlüssel, wir nennen diese p_A und p_B.

3. Nun berechnen beide jeweils $p_A \cdot P$ und $p_B \cdot P$, addieren (im Sinne der Gruppenoperation über elliptischen Kurven) also P so oft zu sich selbst wie ihr jeweiliger privater Schlüssel angibt, und senden den Ergebnispunkt zum jeweils anderen.

4. Nun können beide den erhaltenen Punkt nochmals wie oben mit ihrem eigenen privaten Schlüssel multiplizieren; $p_A \cdot (p_B \cdot P) = p_B \cdot (p_A \cdot P)$ ist das gemeinsame Geheimnis.

5 Fazit

Wir haben gesehen, dass wir mit elliptischen Kurven über endlichen Körpern zyklische endliche Gruppen bilden können, über wüelchen sich viele kryptographische Verfahren wie gewohnt anwenden lassen. Wie anfangs in der Motivation erwähnt sind jedoch gewisse Lösungsalgorithmen für das herkömmliche DLP wie das Zahlkörpersieb nicht für das ECDLP anwendbar. Die besten existierenden Algorithmen wie Baby-Step-Giant-Step haben deutlich größere Laufzeiten, sodass bei ECC schon deutlich kürzere Schlüssellängen ausreichen, um ähnliche Sicherheitsstufen zu erreichen, wie die folgende Tabelle[2] zeigt.

Security level	Symmetric key length (bits)	ECC key length (bits)	RSA/DH/DSA key length (bits)	ECC/RSA key size ratio	MIPS years time to break key
2^{80}	80	160	1024	1/6	10^{12}
2^{112}	112	224	2048	1/9	10^{24}
2^{128}	128	256	3072	1/12	10^{28}
2^{192}	192	384	7680	1/20	10^{47}
2^{256}	256	512	15360	1/30	10^{66}

[2] https://www.researchgate.net/figure/Comparison-of-key-length-for-ECC-and-RSA_tbl1_50282876