

Kryptologie

Johannes Köbler



Institut für Informatik
Humboldt-Universität zu Berlin

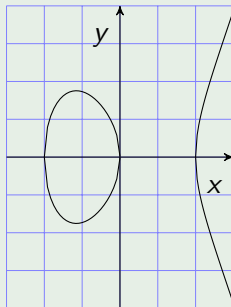
WS 2020/21

Definition

- Seien $a, b \in \mathbb{R}$
- Eine elliptische Kurve E über \mathbb{R} enthält alle Lösungen $(x, y) \in \mathbb{R}^2$ der Gleichung $y^2 = x^3 + ax + b$ und zusätzlich den Punkt \mathcal{O} (Punkt im Unendlichen; siehe Übungen)
- Im Fall $4a^3 + 27b^2 = 0$ heißt E **singulär**, sonst **nicht-singulär**

Beispiel

- Betrachte die durch $y^2 = x^3 - 4x$ definierte elliptische Kurve E :



Punkte: $(-2, 0)$, $(0, 0)$, $(2, 0)$, $(-1, \sqrt{3})$, $(-1, -\sqrt{3})$, $(3, \sqrt{15})$, $(3, -\sqrt{15})$

- Auf den nicht-singulären Punkten von E lässt sich eine additive Gruppenoperation $+$ definieren
- Die Idee dabei ist, dass die Addition von 3 beliebigen Punkten von E , die auf einer Geraden liegen, das neutrale Element \mathcal{O} ergeben soll
- Hierbei werden Tangentialpunkte doppelt und Wendepunkte dreifach gezählt und den parallel zur y -Achse verlaufenden Geraden wird zusätzlich noch der Punkt \mathcal{O} hinzugerechnet
- D.h. alle Geraden, die parallel zur y -Achse verlaufen, schneiden sich im Punkt \mathcal{O} und es werden nur solche Geraden g betrachtet, auf denen bei dieser Zählweise 3 Punkte von E liegen

Berechnung von $P + Q$

- Um nun die Summe $R = P + Q$ von zwei gegebenen Punkten $P = \{x_1, y_1\}$ und $Q = \{x_2, y_2\}$ zu berechnen, bestimmen wir zuerst die Gerade g , auf denen P und Q liegen, wobei g im Fall $P = Q$ die Tangente an E im Punkt P ist
- Falls g parallel zur y -Achse verläuft, ist $x_1 = x_2$ und $y_1 = -y_2$ (also $Q = (x_1, -y_1)$)
- Da in diesem Fall zudem der Punkt \mathcal{O} auf g liegt, erhalten wir die Gleichung $P + Q(+\mathcal{O}) = \mathcal{O}$ bzw. $-P = Q = (x_1, -y_1)$

Berechnung von $P + Q$

Falls g nicht parallel zur y -Achse verläuft, können wir $P + Q$ wie folgt berechnen

- Im Fall $P \neq Q$ gilt $x_1 \neq x_2$
- Zudem ist $g = \{(x, y) \in \mathbb{R}^2 \mid y = \lambda x + \mu\}$ mit $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ und $\mu = y_1 - \lambda x_1 = y_2 - \lambda x_2$
- Wir zeigen zuerst, dass es einen Punkt $R = (x_3, y_3) \in \mathbb{R}^2$ gibt mit

$$E \cap g = \{P, Q, R\}$$

- Für alle $(x, y) \in E \cap g$ gilt

$$(\lambda x + \mu)^2 = x^3 + ax + b$$

$$\rightsquigarrow \underbrace{x^3 - \lambda^2 x^2 + (a - 2\mu\lambda)x + b - \mu^2}_{p(x)} = 0$$

- p lässt sich in \mathbb{C} vollständig in Linearfaktoren zerlegen:

$$p(x) = (x - x_1)(x - x_2)(x - x_3)$$

Berechnung von $P + Q$ im Fall $P \neq Q$

- p lässt sich in \mathbb{C} vollständig in Linearfaktoren zerlegen:

$$p(x) = (x - x_1)(x - x_2)(x - x_3)$$

- Da sich der Koeffizient $-\lambda^2$ von x^2 aus der linearen Zerlegung von $p(x)$ zu

$$-\lambda^2 = -x_1 - x_2 - x_3$$

berechnet, muss $x_3 = \lambda^2 - x_1 - x_2$ sein

- Da R auch auf g liegt, ist zudem $y_3 = \lambda(x_3 - x_1) + y_1$
- Folglich ist $P + Q = -R = (x_3, -y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$

Berechnung von $P + Q$ im Fall $P = Q$

- Im Fall $P = Q$ gilt $x_1 = x_2$ und $y_1 = y_2 \neq 0$
- Sei g die Tangente durch P an E
- Wir zeigen, dass es einen Punkt $R = (x_3, y_3) \in \mathbb{R}^2$ gibt mit

$$g \cap E = \{P, R\}$$

- Die Steigung λ von g erhalten wir durch implizites Differenzieren:

$$\lambda = \frac{-\frac{\partial F}{\partial x}(x_1, y_1)}{\frac{\partial F}{\partial y}(x_1, y_1)} = \frac{3x_1^2 + a}{2y_1},$$

wobei $F(x, y) = y^2 - x^3 - ax - b$ ist

- Zur Begründung sei

$$T(x, y) = c(x - x_1) + d(y - y_1)$$

die Tangentialebene an die Fläche $F(x, y)$ im Punkt

$$(x_1, y_1, F(x_1, y_1)) = (x_1, y_1, 0)$$

Berechnung von $P + Q$ im Fall $P = Q$

- Zur Begründung sei

$$T(x, y) = c(x - x_1) + d(y - y_1)$$

die Tangentialebene an die Fläche $F(x, y)$ im Punkt $(x_1, y_1, F(x_1, y_1)) = (x_1, y_1, 0)$

- Dann gilt

$$c = \frac{\partial F}{\partial x}(x_1, y_1) = -3x_1^2 - a$$

und

$$d = \frac{\partial F}{\partial y}(x_1, y_1) = 2y_1$$

- Da die Tangente g sowohl in der Tangentialebene T als auch in der x, y -Ebene verläuft, folgt

$$\begin{aligned}(x, y) \in g &\Leftrightarrow T(x, y) = 0 \\ &\Leftrightarrow y - y_1 = -\frac{c}{d}(x - x_1),\end{aligned}$$

woraus sich $\lambda = -\frac{c}{d}$ ergibt

Berechnung von $P + Q$ im Fall $P = Q$

- Genau wie im Fall $P \neq Q$ erhalten wir nun

$$P + Q = P + P = 2P = -R = (x_3, -y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$$

$$\text{mit } \lambda = \frac{3x_1^2 + a}{2y_1}$$

Satz

E bildet mit \mathcal{O} als neutralem Element und $+$ als Addition eine abelsche Gruppe, d.h.

- $+$ ist abgeschlossen auf E
- $+$ ist kommutativ
- Jeder Punkt hat ein Inverses $-P$
- P ist selbstinvers, falls $P = -P$ ist;
dies gilt für $P = \mathcal{O}$ und alle Kurvenpunkte der Form $P = (x, 0)$
- $+$ ist assoziativ (ohne Beweis!)

Definition

- Sei \mathbb{F}_q ein endlicher Körper mit $q = p^n$ für eine Primzahl $p > 3$ (der Fall $p = 2$ wird in den Übungen betrachtet)
- Für $a, b \in \mathbb{F}_q$ mit $4a^3 + 27b^2 \neq 0$ heißt

$$E = \{(x, y) \in \mathbb{F}_q \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

elliptische Kurve über \mathbb{F}_q

- Die Gruppenoperation $+$ ist auf E wie folgt definiert:
 - \mathcal{O} ist neutrales Element, d.h. $\forall P \in E - \{\mathcal{O}\} : P + \mathcal{O} = \mathcal{O} + P = P$
 - Das Inverse zu $P = (x, y) \in E \setminus \{\mathcal{O}\}$ ist $-P = \bar{P} = (x, -y)$
 - Für $P, Q \in E \setminus \{\mathcal{O}\}$ ist

$$P + Q = \begin{cases} \mathcal{O}, & P = \bar{Q} \\ R, & \text{sonst} \end{cases}$$

Definition

- Die Gruppenoperation $+$ ist auf E wie folgt definiert:
 - \mathcal{O} ist neutrales Element, d.h. $\forall P \in E - \{\mathcal{O}\} : P + \mathcal{O} = \mathcal{O} + P = P$
 - Das Inverse zu $P = (x, y) \in E \setminus \{\mathcal{O}\}$ ist $-P = \bar{P} = (x, -y)$
 - Für $P, Q \in E \setminus \{\mathcal{O}\}$ ist

$$P + Q = \begin{cases} \mathcal{O}, & P = \bar{Q} \\ R, & \text{sonst} \end{cases}$$

- Dabei wird $R = (x_3, y_3)$ wie folgt aus $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ berechnet:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned} \quad \text{mit } \lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1}, & P = Q \end{cases}$$

Elliptische Kurven über endlichen Körpern

Satz

$(E, \mathcal{O}, +)$ bildet eine abelsche Gruppe (ohne Beweis)

Beispiel

- Sei E definiert durch $y^2 = x^3 + x + 6$ über \mathbb{Z}_p , $p = 11$
- Im Fall $p \equiv_4 3$ lassen sich die Wurzeln y von quadratischen Resten $z \in QR_p = \{y^2 \bmod p \mid y \in \mathbb{Z}_p^*\}$ durch $\pm z^{\frac{p+1}{4}} \bmod p$ bestimmen

x	0	1	2	3	4	5	6	7	8	9	10
$z = x^3 + x + 6$	6	8	5	3	8	4	8	4	9	7	4
$y = \pm\sqrt{z} \bmod 11$	–	–	4; 7	5; 6	–	2; 9	–	2; 9	3; 8	–	2; 9

- Da die Gruppe $(E, +, \mathcal{O})$ die Größe $\|E\| = 13$ hat und 13 prim ist, ist die Ordnung jedes Elements der Kurve 1 oder 13
- Da nur das neutrale Element \mathcal{O} die Ordnung 1 haben kann, haben alle anderen Elemente die Ordnung 13 und sind Erzeuger der Gruppe
- Folglich ist $(E, +, \mathcal{O})$ zyklisch und somit isomorph zu $(\mathbb{Z}_{13}, +, 0)$

Beispiel (Fortsetzung)

- Untenstehende Tabelle zeigt die Vielfachen des Punktes $P = (2, 7) \in E$
- Berechnung von $2P = (2, 7) + (2, 7) = (5, 2)$:

$$\lambda = (3 \cdot 2^2 + 1)(2 \cdot 7)^{-1} \bmod 11 = 2 \cdot 3^{-1} = 2 \cdot 4 \bmod 11 = 8$$

$$x_3 = 8^2 - 2 - 2 \bmod 11 = 5$$

$$y_3 = 8(2 - 5) - 7 \bmod 11 = 2$$

- Berechnung von $3P = 2P + P = (5, 2) + (2, 7) = (8, 3)$:

$$\lambda = (7 - 2)(2 - 5)^{-1} \bmod 11 = 5 \cdot (-3)^{-1} \bmod 11 = 2$$

$$x_3 = 2^2 - 5 - 2 \bmod 11 = 8$$

$$y_3 = 2 \cdot (5 - 8) - 2 \bmod 11 = 3$$

m	1	2	3	4	5	6	7	8	9	10	11	12	13
mP	(2,7)	(5,2)	(8,3)	(10,2)	(3,6)	(7,9)	(7,2)	(3,5)	(10,9)	(8,8)	(5,9)	(2,4)	\mathcal{O}

Satz (Hasse)

Für die Anzahl $\|E\|$ von Punkten einer elliptischen Kurve über einem endlichen Körper \mathbb{F}_q gilt

$$q + 1 - 2\sqrt{q} \leq \|E\| \leq q + 1 + 2\sqrt{q} \quad (\text{ohne Beweis})$$

Bemerkung

Es gibt einen effizienten Algorithmus (von Schoof) mit Zeitkomplexität $O(\log^8 q)$, der $\|E\|$ bei Eingabe von a, b und q berechnet

Satz

Sei E eine elliptische Kurve über \mathbb{F}_q . Dann ist $(E, \mathcal{O}, +)$ isomorph zu $(\mathbb{Z}_{n_1}, 0, +) \times (\mathbb{Z}_{n_2}, 0, +)$, wobei $n_1, n_2 \in \mathbb{N}^+$ sind und n_1 Teiler von n_2 und von $q - 1$ ist (ohne Beweis)

Satz

Sei E eine elliptische Kurve über \mathbb{F}_q . Dann ist $(E, \mathcal{O}, +)$ isomorph zu $(\mathbb{Z}_{n_1}, 0, +) \times (\mathbb{Z}_{n_2}, 0, +)$, wobei $n_1, n_2 \in \mathbb{N}^+$ sind und n_1 Teiler von n_2 und von $q - 1$ ist (ohne Beweis)

Bemerkung

- Falls n_1 ein Teiler von n_2 ist, ist die (additive) Gruppe $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ genau dann zyklisch, wenn $n_1 = 1$ (und somit $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cong \mathbb{Z}_{n_2}$) ist
- Eine hinreichende Bedingung hierfür ist, dass $\|E\|$ quadratfrei (also das Produkt von paarweise verschiedenen Primzahlen) ist
- Im Fall $n_1 > 1$ ist E dagegen nicht zyklisch, hat aber eine nicht-triviale zyklische Untergruppe, die zu \mathbb{Z}_{n_2} isomorph ist und für kryptografische Anwendungen benutzt werden kann

Bemerkung

- Für den Fall, dass sich Quadratwurzeln effizient in \mathbb{F}_q berechnen lassen, gibt es eine einfache Möglichkeit, Punkte auf einer elliptischen Kurve über \mathbb{F}_q kompakter darzustellen
- Ist zum Beispiel $q = p$ prim mit $p \equiv_4 3$, so lassen sich die Wurzeln $\pm\sqrt{z} \bmod p$ von $z \in QR_p = \{x^2 \bmod p \mid x \in \mathbb{Z}_p^*\}$ effizient mittels $\pm z^{(\rho+1)/4} \bmod p$ berechnen
- Folgende Funktion liefert dann eine kompakte Darstellung:
PointCompress: $E - \{\mathcal{O}\} \rightarrow \mathbb{Z}_p \times \mathbb{Z}_2$ mit $(x, y) \mapsto (x, y \bmod 2)$

- Für die Rekonstruktion können wir folgende Prozedur benutzen
- Sei E eine elliptische Kurve $y^2 = x^3 + ax + b$ über \mathbb{F}_p und sei $p(x) = x^3 + ax + b$

Prozedur PointDeCompress(x, b)

```
1   $z := p(x) \bmod p$ 
2   $y := z^{(p+1)/4} \bmod p$ 
3  if  $y^2 \equiv_p z$  then
4    if  $y \not\equiv_2 b$  then  $y := p - y$ 
5    output( $x, y$ )
6  else output(" error ")
```

- In \mathbb{Z}_m^* berechnen wir Potenzen $a^e \bmod m$ durch 'wiederholtes Quadrieren und Multiplizieren'
- Ähnlich können wir in einer elliptischen Kurve E die Vielfachen mP eines Punktes P durch 'wiederholtes Verdoppeln und Addieren' berechnen
- Da in E additive Inverse sehr leicht zu berechnen sind, kann mP durch 'wiederholtes Verdoppeln, Addieren und Subtrahieren' noch effizienter berechnet werden
- Hierzu repräsentieren wir m in NAF-Darstellung (Non Adjacent Form)

Definition

- Eine Folge $(c_{l-1}, \dots, c_0) \in \{-1, 0, 1\}^l$ heißt **SBR-Darstellung** (Signed Binary Representation) einer Zahl $c \in \mathbb{Z}$, falls

$$\sum_{i=0}^{l-1} c_i 2^i = c$$

ist

- Ist von je zwei benachbarten Ziffern c_i mindestens eine 0, so heißt (c_{l-1}, \dots, c_0) **NAF-Darstellung** (Non-Adjacent Form) von c

Beispiel

Sowohl $(0, 1, 0, 1, 1)$ als auch $(1, 0, -1, 0, -1)$ sind SBR-Darstellungen von $c = 1 + 2 + 8 = 11 = -1 - 4 + 16$ ◀

Satz

Jede Zahl $c \in \mathbb{Z}$ hat eine eindeutige NAF-Darstellung
(Beweis siehe Übungen)

Berechnung einer NAF-Darstellung aus der Binärdarstellung

- Ersetze jeden Teilstring der Form $(0, 1, \dots, 1)$ von rechts beginnend durch den Teilstring $(1, 0, \dots, 0, -1)$
- Um z.B. die NAF-Darstellung von $c = 47$ zu berechnen, bestimmen wir zuerst die Binärdarstellung von c
- Es gilt $47_{10} = 101111_2$
- Mit obiger Transformationsregel ergibt sich

$$\begin{aligned} & (0, 1, \underbrace{0, 1, 1, 1, 1}) \\ \rightsquigarrow & (\underbrace{0, 1, 1}, 0, 0, 0, -1) \\ \rightsquigarrow & (1, 0, -1, 0, 0, 0, -1) \end{aligned}$$

- Sei (c_s, \dots, c_0) eine SBR-Darstellung einer Zahl $c \in \mathbb{Z}$
- Zur effizienten Berechnung von $Q = cP$ benutzen wir das Horner-Schema

$$c = \sum_{j=0}^s c_j 2^j = (\dots (\dots (c_s 2 + c_{s-1}) 2 + \dots + c_i) 2 + \dots + c_1) 2 + c_0$$

d_i

- Dieses führt auf das folgende iterative Schema zur Berechnung der Punkte $Q_i = d_i P = \sum_{j=i}^s c_j 2^{j-i} P$:

$$Q_i = \begin{cases} \mathcal{O}, & i = s + 1 \\ 2Q_{i+1} + c_i P, & i = s, \dots, 0 \end{cases}$$

- Damit erhalten wir folgenden Algorithmus zur Berechnung von $Q = Q_0 = cP$:

Prozedur DoubleAddSub(P, c_s, \dots, c_0)

```
1    $Q := \mathcal{O}$ 
2   for  $i := s$  downto 0 do
3      $Q := 2Q + c_i P$ 
4   output( $Q$ )
```

- Da eine $(s + 1)$ -Bitzahl im Durchschnitt $s/2$ Nullen in Binärdarstellung und $(2/3)s$ Nullen in NAF-Darstellung enthält (siehe Übungen), benötigt DoubleAddSub bei Verwendung von NAF ca. $(4/3)s$ Additionen/Subtraktionen im Vergleich zu ca. $(3/2)s$ Additionen im Binärfall
- Dies entspricht einer Beschleunigung um ca. 11 Prozent