Elliptische Kurven modulo N

Definition Elliptische Kurve über $\mathbb{Z}_n$

Sei $N \in \mathbb{N}$ mit

$\text{ggT}(6, N) = 1$, $f(x) = x^3 + ax + b \in \mathbb{Z}_N[x]$ und $\text{ggT}(4a^3 + 27b^2, N) = 1$.

Wir definieren die Punktemenge auf einer *elliptischen Kurve* als

$$E[N] = \{(x, y) \in \mathbb{Z}_N \mid y^2 \equiv f(x) \bmod N\} \cup \{\mathbf{O}\},$$

wobei **O** der Punkt im Unendlichen heißt.

- **Vorsicht:** Die Punkte von E bilden mit der zuvor definierten Addition **keine** Gruppe.
- Bsp: Sei $N = 55$ und E definiert durch $f(x) = x^3 + 1$.
- Dann liegt $P = (10, 11)$ auf E.
- Die Berechnung von $2P$ erfordert $(2y)^{-1} = 22^{-1} \bmod 55$.
- Wegen $\text{ggT}(22, 55) = 11$ existiert dieses Inverse in $\mathbb{Z}_{55}$ nicht.
- D.h. E ist nicht abgeschlossen bezüglich der Addition.

Addition von Punkten auf $E[N]$

Algorithmus Addition von Punkten auf $E[N]$

EINGABE: N, $P = (x_1, y_1)$, $Q = (x_2, y_2)$ auf $E[N]$ mit $P, Q \neq \mathbf{O}$

1. Falls $x_1 \equiv x_2 \bmod N$ und $y_1 \equiv -y_2 \bmod N$, Ausgabe $\mathbf{O}$.
2. Berechne $d = \mathrm{ggT}(x_1 - x_2, N)$. Falls $d \notin \{1, N\}$, Ausgabe d.
3. Falls $x_1 \equiv x_2 \bmod N$, berechne $d = \mathrm{ggT}(y_1 + y_2, N)$.
   Falls $d > 1$, Ausgabe d.
4. Setze $\alpha := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{für } x_1 \not\equiv x_2 \\ \frac{3x_1^2 + a}{y_1 + y_2} & \text{für } x_1 \equiv x_2 \end{cases}$. Setze $\beta \equiv y_1 - \alpha x_1 \bmod N$.
5. Berechne $x_3 \equiv \alpha^2 - x_1 - x_2 \bmod N$ und $y_3 \equiv -(\alpha x_3 + \beta) \bmod N$.

AUSGABE: $P + Q = (x_3, y_3)$ oder nicht-trivialer Teiler d von N

Reihenfolge der Addition auf $E[N]$

Vorsicht: Es hängt von der Berechnungsvorschrift der Addition von Punkten auf $E[N]$ ab, ob ein Teiler ausgegeben wird.

Definition Reihenfolge der Addition auf $E[N]$

Sei P ein Punkt auf E modulo N. Für $m \in \mathbb{N}$ definieren wir

$$mP = \begin{cases} (m-1)P + P & \text{für } m \text{ ungerade} \\ \frac{m}{2}P + \frac{m}{2}P & \text{für } m \text{ gerade, } m > 0 \\ \mathbf{O} & \text{für } m = 0. \end{cases}$$

Anmerkung:

- mP kann in Zeit $\mathcal{O}(\log m \log^2 N)$ berechnet werden.

Addition verträglich mit zuvor definierter Addition

Satz Verträglichkeit der Additionsdefinitionen

Sei P, Q auf $E[N]$, so dass nicht für genau einen Teiler $p \mid N$ gilt $P + Q = \mathbf{O}$ auf $E \bmod p$. Dann ist $P + Q$ auf $E[N]$ identisch mit der Addition auf $E[p]$, $E[q]$ oder liefert einen Teiler von N.

Beweis:

- Sei $P = (x_1, y_1)$ und $Q = (x_2, y_2)$.
- **Fall 1:** Sei $P + Q = \mathbf{O}$ auf $E[p]$ und $E[q]$.
- Dann gilt $\left| \begin{array}{l} x_1 \equiv x_2 \\ y_1 \equiv -y_2 \end{array} \right| \bmod p$ und $\bmod q$ und damit auch $\bmod N$.
- Es folgt $P + Q = \mathbf{O}$ auf $E[p]$ und $E[q]$.
- Unser Algorithmus berechnet analog $P + Q = \mathbf{O}$ auf $E[N]$.

Addition verträglich mit zuvor definierter Addition

Beweis: (Fortsetzung)

- **Fall 2:** Sei $P + Q \neq \mathbf{O}$ auf $E[p]$ und $E[q]$.
- **Fall 2a:** $x_1 \not\equiv x_2 \bmod p$ und $x_1 \not\equiv x_2 \bmod q$.
- Die Additionsformel ist identisch auf $E[p]$ und $E[N]$. (analog für $E[q]$ und $E[N]$)
- **Fall 2b:** $x_1 \not\equiv x_2 \bmod p$ und $x_1 \equiv x_2 \bmod q$ (und vice versa).
- Es folgt $\mathrm{ggT}(x_1 - x_2, N) = q$ in Schritt 2.
- **Fall 2c:** $\left| \begin{array}{ll} x_1 \equiv x_2 & \bmod N \\ y_1 \not\equiv -y_2 & \bmod p \end{array} \right|$ (analog $y_1 \not\equiv y_2 \bmod q$).
- Die Gleichung $y^2 \equiv x_1^3 + ax_1 + b$ besitzt genau 2 Lösungen $y_{1,2} \equiv \pm y \bmod p$ mit $y_1 \not\equiv -y_2 \bmod p$. Damit gilt $y_1 \equiv y_2 \bmod p$.
- Es folgt $y_1 + y_2 = 2y_1 \bmod p$, d.h. die Additionsformel ist identisch. (analog modulo q)

ECM Faktorisierungssatz

Satz ECM Faktorisierungssatz

Sei $P + Q = \mathbf{O}$ auf $E[p]$ und $P + Q \neq \mathbf{O}$ auf $E[q]$. Dann liefert die Addition $P + Q$ auf $E[N]$ einen Teiler von N.

Beweis:

- Wegen $P + Q = \mathbf{O}$ auf $E[p]$ gilt
$$x_1 \equiv x_2 \bmod p \text{ und } y_1 \equiv -y_2 \bmod p.$$
- Aus $P + Q \neq \mathbf{O}$ auf $E[q]$ folgt
$$x_1 \not\equiv x_2 \bmod q \text{ oder } y_1 \not\equiv -y_2 \bmod q.$$
- **Fall 1:** $x_1 \not\equiv x_2 \bmod q$. Dann liefert Schritt 2 $\mathrm{ggT}(x_1 - x_2, N) = p$.
- **Fall 2:** $y_1 \not\equiv -y_2 \bmod q$. Dann liefert Schritt 3 $\mathrm{ggT}(y_1 + y_2, N) = q$.

ECM Faktorisierung

Algorithmus ECM Faktorisierung

EINGABE: $N = pq$ mit p, q gleicher Bitgröße

1. Wähle Schranken $B_1, B_2 \in \mathbb{N}$.
2. Wähle $(a, x, y) \in_R \mathbb{Z}_N^3$ und berechne $b = y^2 - x^3 - ax \bmod N$.
3. Falls $\mathrm{ggT}(4a^3 + 27b^2, N) = \begin{cases} 1 & \text{Setze } P = (x, y). \\ N & \text{Gehe zu Schritt 2.} \\ \text{sonst} & \text{Ausgabe } p, q. \end{cases}$
4. Für alle Primzahlen $p_i \leq B_1$, berechne $P := p_i^{e_i} P$ auf $E \bmod N$, wobei e_i maximal mit $p_i^{e_i} \leq B_2$.
   Falls eine der Berechnungen scheitert, Ausgabe p, q.
5. Sonst zurück zu Schritt 2 oder Ausgabe *Kein Faktor gefunden.*

AUSGABE: p, q oder *Kein Faktor gefunden*.

Man beachte:

In Schritt 2 wird eine zufällige Kurve E mit zufälligem P auf E gewählt.

Korrektheit der ECM Faktorisierung

Satz Korrektheit der ECM Faktorisierung

Sei $N = pq$ und E eine elliptische Kurve über $\mathbb{Z}_N$, so dass $|E[p]|$ B_1-glatt und $|E[q]|$ nicht B_1-glatt ist. Dann liefert ECM die Faktorisierung von N in Zeit $\mathcal{O}(B_1 \log^3 N)$ mit Erfolgsws mind. $1 - \frac{1}{B_1}$.

Beweis:

- Wir definieren $k := \prod_{\text{Primzahlen } p_i \leq B_1} p_i^{e_i}$.
- Da $|E[q]|$ nicht B_1-glatt, gilt $r \mid |E[q]|$ für ein primes $r > B_1$.
- Falls $r \mid \text{ord}_{E[q]}(P)$, so folgt $kP \neq \mathbf{O}$ auf $E[q]$.
- Andererseits ist k ein Vielfaches von $|E[p]|$.
- Damit gilt $kP = \mathbf{O}$ auf $E[p]$.
- D.h. wir erhalten bei Berechnung von kP auf $(E[N])$ P', Q' mit

$$P' + Q' = \mathbf{O} \text{ auf } E[p] \text{ und } P' + Q' \neq \mathbf{O} \text{ auf } E[q].$$

- Mit ECM Faktorisierungssatz liefert dies die Faktorisierung von N.
- Laufzeitanalyse und Erfolgws sind analog zur $p-1$-Methode.

Wahl der Schranken B_1, B_2 und Laufzeit

Laufzeit von ECM:

- Tradeoff: Kleine B_1 führen zu kleiner Laufzeit einer ECM-Iteration.
- Große B_1 erhöhen die Ws, dass $E \bmod p$ B_1-glatt ist. D.h. für große B_1 müssen weniger ECM-Iterationen durchlaufen werden.
- Optimale Wahl: $B_1 \approx L_p[\frac{1}{2}, \frac{1}{\sqrt{2}}] = e^{\frac{1}{\sqrt{2}}\sqrt{\log p \log\log p}}$.
- Unter einer Annahme für die Glattheit von Zahlen in $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ erhalten wir Gesamtlaufzeit $L_p[\frac{1}{2}, \sqrt{2}]$.
- Besser als Laufzeit $L_N[\frac{1}{2}, 1]$ für Quadratisches Sieb falls $p < \sqrt{N}$:
  $L_p[\frac{1}{2}, \sqrt{2}] = e^{\sqrt{2 \ln p \ln\ln p}} < e^{\sqrt{2\frac{1}{2} \ln N \ln\ln N}} = L_N[\frac{1}{2}, 1]$.
- ECM ist die beste Methode, um kleine Primfaktoren zu finden.