Der Algorithmus von Schoof

Simone Deppert

Technische Universität Kaiserslautern
Sommersemester 2011

29. Juli 2011

Inhaltsverzeichnis

Betrachte eine elliptische Kurve E:

$$y^2 = x^3 + Ax + B \text{ über } \mathbb{F}_q$$

Nach dem Satz von Hasse gilt:

$$\#E[\mathbb{F}_q] = q + 1 - a \text{ mit } |a| \leq 2\sqrt{q}$$

Wie bestimmen wir a?

Der Algorithmus

- Wähle eine Menge von Primzahlen S (mit $p \notin S$), so dass $\prod_{\ell \in S} \ell > 4\sqrt{q}$
- Berechne $a \mod \ell$
  - Betrachte $\ell = 2$:
    Es gilt $a \equiv 0 \mod 2$ gdw. $ggt(x^3 + AX + B, x^q - x) \neq 1$
  - Betrachte $\ell \in S, \ell \neq 2$:
    Durchlaufe den „Unteralgorithmus“.
- Wir kennen nun $a \mod \ell$ für alle $\ell \in S$ und berechnen daraus $a \mod \prod_{\ell \in S} l$. Suche nun ein a, dass diese Gleichung erfüllt und für das gilt: $|a| \leq 2\sqrt{q}$

„Unteralgorithmus“

Für $\ell \in S, \ell \neq 2$

- Sei $q_\ell \equiv q \mod \ell$ mit $|q_\ell| < \frac{\ell}{2}$
- Berechne die x-Koordinate von $(x', y') = (x^{q^2}, y^{q^2}) + q_\ell(x, y)$ $\mod \psi_\ell$
- Für alle $j = 1, 2, \cdots, \frac{\ell-1}{2}$:
  - Berechne die x-Koordinate von $(x_j, y_j) = j(x, y)$
  - Falls $x' \not\equiv 0 \mod \psi_\ell$, versuche das nächste j.
  - Berechne y' und y_j. Wenn $\frac{y' - y_j^q}{y} \equiv 0 \mod \psi_\ell$, dann $a \equiv j \mod \ell$. Wenn nicht, dann gilt: $a \equiv -j \mod \ell$
- Falls alle $1 \leq j \leq \frac{\ell-1}{2}$ ohne Erfolg ausprobiert wurden, dann sei $w^2 \equiv q \mod \ell$. Wenn w nicht existiert, dann gilt: $a \equiv 0 \mod \ell$
- Falls gilt, dass der $ggt(\text{Zähler}(x^q - x_w), \psi_\ell) = 1$ ist, dann folgt: $a \equiv 0$ $\mod \ell$. Ansonsten berechne den $ggt(\text{Zähler}(\frac{y^q - y_w}{y}), \psi_\ell)$. Falls der ggt nicht 1 ist, dann gilt $a \equiv 2w \mod \ell$, ansonsten: $a \equiv -2w \mod \ell$

Die Menge S

Sei die Menge $S = \{2, 3, 5, ..., L\}$ eine Menge von Primzahlen, so dass $\prod_{\ell \in S} \ell > 4\sqrt{q}$

Annahmen

Wähle $\ell \in S$, der Einfachheit wegen soll gelten: $\ell \neq p$ wobei p die Charakteristik von $\mathbb{F}_q$.
Sei q im Folgenden ungerade.

1. Fall: $\ell = 2$

- Wenn $x^3 + Ax + B$ eine Wurzel $e \in \mathbb{F}_q$ hat, dann gilt $(e, 0) \in E[2]$ und $(e, 0) \in E(\mathbb{F}_q)$. Daraus folgt $E(\mathbb{F}_q)$ hat eine gerade Ordnung. In diesem Fall gilt $q + 1 - a \equiv 0 \mod 2 \Rightarrow a$ gerade
- Wenn $x^3 + Ax + B$ keine Wurzel in $\mathbb{F}_q$ hat, dann hat $E(\mathbb{F}_q)$ keine Punkte von der Ordnung 2 $\Rightarrow a$ ungerade.

1. Fall: $\ell = 2$

Wie bestimmen wir ob $x^3 + Ax + B$ eine Wurzel in $\mathbb{F}_q$ hat?

1. Fall: $\ell = 2$

Wie bestimmen wir ob $x^3 + Ax + B$ eine Wurzel in $\mathbb{F}_q$ hat?

Ausprobieren!

1. Fall: $\ell = 2$

Betrachtet man die Wurzeln von $x^q - x$, so erhält man nach Definition die Elemente von $\mathbb{F}_q$

$\Rightarrow x^3 + Ax + B$ hat eine Wurzel in $\mathbb{F}_q \Leftrightarrow ggt(x^3 + Ax + B, x^q - x) \neq 1$

1. Fall: $\ell = 2$

Effizienter:
Betrachte $x_q \equiv x^q \mod (x^3 + Ax + B)$ bei fortlaufendem Quardrieren.

Dadurch lässt sich der ggt berechnen als:
$ggt(x^3 + Ax + B, x^q - x) = ggt(x^3 + Ax + B, x_q - x)$

Fallunterscheidung:

- $ggt(\cdots) = 1 \rightarrow$ keine gemeinsame Wurzel $\rightarrow$ a ist ungerade
- $ggt(\cdots) \neq 1 \rightarrow$ a ist gerade

2. Fall: $\ell \in S$, $\ell \neq 2$

Im Folgenden werden ebenfalls Ausdrücke wie x^q und x^{q^2} benutzt. Sie werden so berechnet wie im Fall $\ell = 2$.

2. Fall: $\ell \in S$, $\ell \neq 2$

Betrachte nun ψ_n. Falls n ungerade ist, dann ist ψ_n ein Polynom in x und für $(x, y) \in E(\overline{\mathbb{F}}_q)$ gilt: $(x, y) \in E[n] \Leftrightarrow \psi_n = 0$

2. Fall: $\ell \in S$, $\ell \neq 2$

Betrachten: $\phi_q^2 - a\phi_q + q = 0$

Sei nun (x, y) ein Punkt der Ordnung ℓ, dann gilt:
$(x^{q^2}, y^{q^2}) + q(x, y) = a(x^q, y^q)$

Mit $q_\ell \equiv q \mod \ell, |q_\ell| < \frac{\ell}{2}$ folgt:
$(x^{q^2}, y^{q^2}) + q_\ell(x, y) = a(x^q, y^q)$

$$(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y)$$

Falls für einige $(x, y) \in E[\ell]$ gilt, dass: $(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y)$, dann definiere: $(x', y') := (x^{q^2}, y^{q^2}) + q_\ell(x, y) \neq \infty$, so dass $a \not\equiv 0 \mod \ell$

$$(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y)$$

Dann gilt, dass die x-Koordinaten von (x^{q^2}, y^{q^2}) und $q_\ell(x, y)$ eindeutig sind. Wir betrachten die Summe durch die beiden Punkte.
$j(x, y) = (x_j, y_j)$ mit $x_j = r_{1,j}(x), y_j = r_{2,j}(x)y$

$$(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y)$$

Betrachten wir:

$$x' = \left(\frac{y^{q^2} - y_{q_\ell}}{x^{q^2} - x_{q_\ell}}\right)^2 - x^{q^2} - x_{q_\ell}$$

So ergibt sich:

$$\begin{aligned}\left(y^{q^2} - y_{q_\ell}\right)^2 &= y^2 \left(y^{q^2-1} - r_{2,q_\ell}(x)\right)^2 \\ &= \left(x^3 + Ax + B\right) \left(\left(x^3 + Ax + B\right)^{\frac{q^2-1}{2}} - r_{2,q_\ell}(x)\right)^2\end{aligned}$$

Dadurch ergibt sich, dass x' eine rationale Funktion von x wird.

$$(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y)$$

Wir suchen nun j, für die gilt:
$(x', y') = (x_j^q, y_j^q)$

Wir betrachten primär die x-Koordinate!

$$(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y)$$

Wähle ein $(x, y) \in E[\ell]$, dann gilt $(x', y') = \pm(x_j^q, y_j^q) \Leftrightarrow x' = x_j^q$
Da die Wurzeln von ψ_ℓ die x-Koordinaten der Punkte in $E[\ell]$ sind, folgt daraus: $x' - x_j^q \equiv 0 \mod \psi_\ell$. Die Wurzeln von ψ_ℓ sind einfach.

$$(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y)$$

Angenommen wir haben ein j gefunden, so dass $x' - x_j^q \equiv 0 \mod \psi_\ell$ gilt.
Dann folgt:
$(x', y') = \pm(x_j^q, y_j^q) = (x_j^q, \pm y_j^q)$

$$(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y)$$

Sowohl $\frac{y'}{y}$ als auch $\frac{y_j^q}{y}$ können als Funktionen von x geschrieben werden.

Wenn gilt, dass $\left(\frac{y' - y_j^q}{y}\right) \equiv 0 \mod \psi_\ell \Rightarrow a \equiv j \mod \ell$

Anderenfalls gilt: $a \equiv -j \mod \ell$

$$(x^{q^2}, y^{q^2}) = \pm q_\ell(x, y)$$

Angenommen $(x^{q^2}, y^{q^2}) = \pm q(x, y)$ gilt für alle $(x, y) \in E[\ell]$

$$\begin{aligned} \phi_q^2(x, y) &= \left(x^{q^2}, y^{q^2}\right) = q(x, y) \\ \Rightarrow a\phi_q(x, y) &= \phi_q^2(x, y) + q(x, y) = 2q(x, y) \\ \Rightarrow a^2 q(x, y) &= a^2 \phi_q^2(x, y) = (2q)^2(x, y) \end{aligned}$$

$$(x^{q^2}, y^{q^2}) = \pm q_\ell(x, y)$$

$a^2 q \equiv 4q^2 \mod \ell \Rightarrow q$ ist ein Quadrat $\mod \ell$.
Wenn q ein Quadrat $\mod \ell$ ist, dann sei $w^2 \equiv q \mod \ell$.
Daraus folgt: $(\phi_q + w)(\phi_q - w)(x, y) = \left(\phi_q^2 - q\right)(x, y) = \infty$ für alle $(x, y) \in E[\ell]$

$$(x^{q^2}, y^{q^2}) = \pm q_\ell(x, y)$$

Sei nun P ein beliebiger Punkt in $E[\ell]$.
Entweder es gilt $(\phi_q - w)P = \infty, \phi_q P = wP$ oder
$P' = (\phi_q - w)P, (\phi_q + w)P' = \infty$ ist ein endlicher Punkt.
Folglich gibt es in jedem Fall einen Punkt $P \in E[\ell]$ mit $\phi_q P = \pm wP$.

$$(x^{q^2}, y^{q^2}) = \pm q_\ell(x, y)$$

- $\phi_q P = wP$
  Dann folgt mit $\infty = (\phi_q^2 - a\phi_q + q)P = (q - aw + q)P$, dass $aw \equiv 2q \equiv 2w^2 \mod \ell$. Also gilt: $a \equiv 2w \mod \ell$
- $\phi_q P = -wP$
  Dann gilt analog zu oben: $a \equiv -2w \mod \ell$

$$(x^{q^2}, y^{q^2}) = \pm q_\ell(x, y)$$

Um zu überprüfen ob wir in diesem Fall sind, betrachten wir ob folgendes für einige $(x, y) \in E[\ell]$ gilt:
$(x^q, y^q) = \pm w(x, y) = \pm(x_w, y_w) = (x_w, \pm y_w)$

Hierfür berechnen wir $x^q - x_w$. Wenn gilt, dass $ggt(Zaehler(x^q - x_w), \psi_\ell) \neq 1$, dann existieren einige $(x, y) \in E[\ell]$, so dass $\phi_q(x, y) = \pm(x, y)$. Zur Bestimmung des Vorzeichens betrachten wir die y-Koordinate.

Das gesuchte a

Wir kennen nun $a \mod \ell$ für alle $\ell \in S$ und berechnen daraus $a \mod \prod_{\ell \in S} \ell$. Suche nun ein a, dass diese Gleichung erfüllt und für das gilt: $|a| \leq 2\sqrt{q}$