Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K21: Schnelle Arithmetik auf elliptischen Kurven

Stichworte: • Varianten projektiver Koordinaten • Jakobinische Koordinaten
• Rechnerischer Vorteil bei Punktaddition/-verdopplung auf $E(k)$

21.1. Einleitung: Wir diskutieren die Machbarkeit der schnellen Punktaddition am Computer, d.h. schnelle Arithmetik auf elliptischen Kurven:
Die Gruppenoperation "+" auf einer Elliptischen Kurve $E(k)$ soll rechnerisch praktisch mit den expliziten Formeln Satz 19.17 / 19.18 auf den Computer umgesetzt werden.

21.2. Bem.: Ein Blick auf die expliziten Formeln zeigt:
- Bei kurzer Weierstraßform $y^2 = x^3 + ax + b$ spielt der Koeffizient b keine Rolle. Also ist es rechnerisch günstig, Kurven mit kleinem a und großem b zu benutzen.
- Für Kurven mit $\mathrm{char}\, k = 2$ ergeben sich mit Satz 19.17 Formeln für "+", die sich besonders gut für Hardwareimplementierungen eignen.
- sowohl bei der Addition "+" als auch bei der Punktverdopplung $P \rightsquigarrow 2 \cdot P$ (affin) wird eine Division in k benötigt. Das ist z.B. für $k = \mathbb{R}$ unpässlich bzw. zu ungenau. Das Problem lässt sich mit projektiven Koordinaten beheben: Ist $P = (\frac{x}{r}, \frac{y}{s}) \in A^2(k)$ mit $r, s \in k \setminus \{0\}$, ist $P = [xs : yr : rs]$ ohne Division berechenbar, aber es müssen mehr Multiplikationen durchgeführt werden. Durch die Einführung einer Variante von projektiven Koordinaten – den sogenannten Jakobinischen Koordinaten – kann man in Vergleich dazu Multiplikationen einsparen, was den Rechenaufwand vermindert. Wir besprechen dies in diesem Abschnitt zur schnellen Punktaddition.

21.3. **Def.:** Sei k ein Körper und $c,d \in \mathbb{N}$, dann definieren wir die Relation $\sim$ auf $k^3 \setminus \{(0,0,0)\}$ durch

$$(x,y,z) \sim (x',y',z') \quad :\Leftrightarrow \quad \exists\, \sigma \in k \setminus \{0\}:$$
$$x = \sigma^c x',\ y = \sigma^d y',\ z = \sigma z'$$

21.4. **Bem.:** • $\sim$ ist eine Äquivalenzrelation auf $k^3 \setminus \{(0,0,0)\}$, ihre Äquivalenzklassen bezeichnen wir mit

$$(x:y:z) := \{(x',y',z') \in k^3 \setminus \{(0,0,0)\};\ (x',y',z') \sim (x,y,z)\}.$$

• Im Fall $c=d=1$ erhalten wir unsere bisherige Definition für einen projektiven Punkt $[x:y:z]$ zurück. Auch hier nennen wir $(x:y:z)$ einen projektiven Punkt.

21.5. **Bem.:** • Wenn $z \neq 0$, gilt durch Normierung $(x/z^c,\ y/z^d,\ 1) \sim (x,y,z)$, vermöge $\sigma = \frac{1}{z}$, damit kann man in der Menge

$$\mathbb{P}^2_{(c,d)}(k) := \{(x:y:z);\ (x,y,z) \in k^3 \setminus \{(0,0,0)\}\}$$

die Punkte mit $z \neq 0$ wieder mit $\mathbb{A}^2(k)$ identifizieren.

• Die Punkte mit $z=0$ bilden wieder die unendlich ferne Gerade.

• Die projektive Form der Weierstraßgleichung erhält man durch Einsetzen von $\frac{x}{z^c}$ und $\frac{y}{z^d}$ in die Gleichung und Entfernung der Nenner durch Multiplikation:

$$y^2 - x^3 - ax - b = 0 \ \rightsquigarrow \ \left(\frac{y}{z^d}\right)^2 - \left(\frac{x}{z^c}\right)^3 - a\frac{x}{z^c} - b = 0$$
$$\rightsquigarrow y^2 - x^{3-3c+2d} - a x z^{2d-c} - b z^{2d} = 0, \quad \text{falls etwa } 2d \geq 3c,$$

was offenbar i.a. nicht mehr homogen sein muss.

• In der Kryptographie verwendet man folgende projektive Darstellungen:
- Standard-projektive Koordinaten: $c=d=1$
- Jakobinische Koordinaten: $c=2,\ d=3$
- Chudnovski-Koordinaten: ein jakobinischer Punkt wird als $(x:y:z:z^2:z^3)$ dargestellt.

Schnelle Punkteaddition mit Jakobimischen Koordinaten:

21.6. Sei $E(K): y^2 = x^3 + ax + b$ gegeben mit $4a^3 + 27b^2 \neq 0$.
Anhand der affinen Version für die explizite Punkteverdopplung zeigen wir nun, dass man Rechenaufwand sparen kann, wenn man mit Jakobimischen Koordinaten $c=2$, $d=3$ arbeitet.
Ist $P=(u,v)$, $P \neq -P$, ist $2P = P+P = (\underbrace{\lambda^2 - 2u}_{=:x}, \underbrace{\lambda(u-x)-v}_{=:y})$, wo

$\lambda := \frac{3u^2+a}{2v}$, die affine Version der expliziten Formel in Standard-Darstellung.

Für die Koordinaten x,y von $2P = (x:y:1) = [x:y:1]$ bei $P = [u:v:z]$ erhält man durch Einsetzen von $\frac{u}{z^2}$ für u und $\frac{v}{z^3}$ für v dann

$$x = \left(\frac{3\left(\frac{u}{z^2}\right)^2 + a}{2\left(\frac{v}{z^3}\right)}\right)^2 - 2\frac{u}{z^2} = \frac{\left(3\frac{u^2}{z^4}+a\right)^2 z^6}{4v^2} - 2\frac{u}{z^2} = \frac{(3u^2+az^4)^2 - 8uv^2}{4v^2z^2}$$

und $$y = \frac{3\left(\frac{u}{z^2}\right)^2 + a}{2\frac{v}{z^3}}\left(\frac{u}{z^2} - x\right) - \frac{v}{z^3} = \frac{3u^2+az^4}{2vz}\left(\frac{u}{z^2} - x\right) - \frac{v}{z^3}.$$

Setzen wir $v := 2vz$, damit wird $x_0 = v^2 x$, $y_0 = v^3 y$, $z_0 = v$

und somit $x_0 = (3u^2+az^4)^2 - 8uv^2$, $z_0 = 2vz$

und $$y_0 = \frac{3u^2+az^4}{2vz} \cdot 8v^3z^3 \cdot \left(\frac{u}{z^2} - x\right) - \frac{v}{z^3} \cdot 8v^3z^3$$

$$= (3u^2+az^4) \cdot 4v^2 \cdot (u - z^2x) - 8v^4$$

$$= (3u^2+az^4) \cdot (4uv^2 - x_0) - 8v^4.$$

} explizite Formeln zur Punkteverdopplung in jakobimischen Koordinaten

21.7. Eine Umsetzung der Berechnung von $(x_0 : y_0 : z_0) = 2P = (x : y : 1)$ ist somit wie folgt möglich: (2 Quadrierungen)

$$A := v^2, \quad B := 4u \cdot A, \quad C := 8A^2, \quad D := 3u^2 + a \cdot z^4,$$
$$x_0 := D^2 - 2B, \quad y_0 := D \cdot (B - x_0) - C, \quad z_0 := 2v \cdot z$$

Das sind insg. 6 Quadrierungen und 4 Multiplikationen im Basiskörper k, es sind keine Divisionen nötig! (Die Skalaren Vielfachen mit 2, 3, 4, 8 zählen wie Additionen: $2 \cdot s = s + s$ usw.)

Analog gewinnt man die folgenden effizienten, expliziten Formeln zur Punktaddition $P + Q$ mit $P = (u, v)$, $Q = (r, s)$ in jakobinischen Koordinaten:

$$x_0 = (sz^3 - v)^2 - (rz^2 - u)^2 (u + rz^2)$$
$$y_0 = (sz^3 - v)(u(rz^2 - u)^2 - x_0) - v(rz^2 - u)^3$$
$$z_0 = (rz^2 - u)z$$

Als Rechenverfahren dient dann:

$$A := z^2, \quad B := z \cdot A, \quad C := r \cdot A, \quad D := s \cdot B, \quad E := C - u,$$
$$F := D - v, \quad G := E^2, \quad H := G \cdot E, \quad I := u \cdot G,$$
$$x_0 := F^2 - (H + 2I), \quad y_0 := F \cdot (I - x_0) - v \cdot H, \quad z_0 := z \cdot E$$

21.8. Das sind insg. 3 Quadrierungen und 8 Produkte in k, keine Divisionen!

Aufstellung des Rechenaufwands für eine elliptische Kurve $y^2 = x^3 - 3x + b$:

[Idee: Ausdruck $3u^2 + a \cdot z^4$ in expl. Formel bei Punktverdopplung braucht 3Q, 1M und wird mit $a = -3$ zu $3u^2 - 3z^4 = 3 \cdot (u - z^2) \cdot (u + z^2)$ mit 1Q, 1M]

	Punkteverdopplung $2P = P+P$	Punkteaddition $P+Q$
affin	1 D, 2 M, 2 Q	1 D, 2 M, 1 Q
standard-projektiv	7 M, 3 Q	12 M, 2 Q
Jakobinische Koordinaten	4 M, 4 Q	12 M, 4 Q
Chudnovski-Koordinaten	5 M, 4 Q	11 M, 3 Q

D = Divisionen, M = Multiplikationen, Q = Quadrierungen

21.9. Fazit: Arbeitet man mit jakobinischen Koordinaten, können bei der Punkteverdopplung Multiplikationen eingespart werden, was dann am Computer zu einem schnelleren Verfahren bei der Berechnung von $2 \cdot P$ bzw. $m \cdot P$ führt.

21.10. Erinnerung: Wie bei der schnellen Potenzierung zur Berechnung von x^m kann bei additiver Schreibweise einer Gruppe die Berechnung von $m \cdot P$ analog durchgeführt werden, was man "schnelle Vervielfachung" nennen könnte, engl. "dual-and-add-algorithm". Schritte des Verfahrens:

1.) Sei $d = \lfloor \frac{\log m}{\log 2} \rfloor$, berechne durch sukzessives Verdoppeln: $P, 2P, 4P, 8P, \ldots, 2^d P$

2.) Schreibe m als Binärzahl: $m = \sum_{i=0}^{d} c_i 2^i$, $c_i \in \{0,1\}$.

3.) Berechne $m \cdot P = (c_0 P) + (c_1 \cdot 2P) + (c_2 \cdot 4P) + \ldots + (c_d \cdot 2^d P)$ mit maximal d weiteren Additionen von Punkten auf $E(k)$.