

Der Schoof Algorithmus

Seminar von
Anton Betten
Institut für Algorithmen
und Kognitive Systeme
Prof. Dr. Th. Beth
Fakultät für Informatik
Universität Karlsruhe

15.Mai 1992

1 Einleitung

In jüngster Zeit spielen elliptische Kurven eine große Rolle in der Kryptographie. Aus der Zahlentheorie und algebraischen Geometrie stammend, sind sie jetzt beliebt in Anwendungen, wo man sich ihre reichhaltige abelsche Gruppenstruktur zu Nutze macht. Hier sind sie den herkömmlichen Methoden, die mit der multiplikativen Gruppe endlicher Körper arbeiten, an Flexibilität weit überlegen.

Wir wollen hier nur die grundlegenden Definitionen aus diesem Gebiet geben und uns im Weiteren auf elliptische Kurven über endlichen Körpern beschränken. Die allgemeinsten Definitionen wollen wir dennoch für beliebige Körper fassen.

Unser Ziel soll es sein, den Schoof Algorithmus zu erörtern, dessen Nutzen darin besteht, die Gruppenordnung einer elliptischen Kurve über einem endlichen Körper modulo Primzahl zu bestimmen. Wenn man dies für genügend viele Primzahlen tut, kann man die wahre Gruppenordnung dann durch chinesische Restetechnik zusammensetzen (eine Größenabschätzung ist auch vorhanden).

2 Elliptische Kurven - Einführung

Sei \mathbf{K} ein Körper der Charakteristik $\neq 2, 3$. Sei $p(X) = X^3 + AX + B$ (mit $A, B \in \mathbf{K}$) ein kubisches Polynom ohne doppelte Nullstellen.

Def.: Eine elliptische Kurve über \mathbf{K} ist die Menge der Punkte $(x, y) \in \mathbf{K}^2$, die die Gleichung

$$Y^2 = X^3 + AX + B \quad (1)$$

erfüllen zusammen mit einem speziellen Element 0, genannt *Punkt im Unendlichen*.

Bem. 1: Die Gleichung $Y^2 = X^3 + AX + B$ wird auch als *Weierstraß Gleichung* bezeichnet und ist die *affine* Form der Gleichung einer elliptischen Kurve.

Bem. 2: Die Diskriminante von $p(X)$ ist (bis auf das Vorzeichen) $4A^3 + 27B^2$. Wir wollen hier also voraussetzen, daß sie $\neq 0$ ist und $p(X)$ somit keine doppelte Nullstelle hat.

Bem. 3: Sei $F(x, y) = 0$ die implizite Gleichung für y als Funktion von x aus (1). Einen Kurvenpunkt nennen wir *singulär*, wenn beide partiellen Ableitungen $\partial F/\partial x$ und $\partial F/\partial y$ in ihm verschwinden (formale Ableitungen können nach den bekannten Formeln in jedem Körper gebildet werden). Man kann leicht einsehen (siehe Anhang), daß die Diskriminantenbedingung (s. Bem. 2) gleichwertig zur Forderung ist, daß alle Kurvenpunkte nichtsingulär sind.

Bem. 4: Die allgemeine Form einer Ellipsengleichung für beliebige Körper lautet $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Sie kann in char $\mathbf{K} \neq 2, 3$ durch Substitution von

$$X = x + \frac{a_1^2 + 4a_2}{12}, \quad Y = y + \frac{a_1x + a_3}{2}$$

auf die Form (1) gebracht werden.

Bem. 5: Mit der *projektiven Ebene* über einem Körper \mathbf{K} meint man die Menge der Tripel $(X, Y, Z) \in \mathbf{K}^3$ (nicht alle Komponenten Null) wobei zwei Tripel äquivalent sein sollen, wenn sie ein skalares Vielfaches voneinander sind, d.h. $(\lambda X, \lambda Y, \lambda Z) \sim (X, Y, Z)$. Solch eine Klasse nennt man *Projektiven Punkt*. Für $Z \neq 0$ kann man sich beispielsweise auf $(x, y, 1)$ mit $x = X/Z$ und $y = Y/Z$ als kanonischen Vertreter einigen. Wir erhalten also die gewöhnliche (*affine*) Ebene und die Punkte mit $Z = 0$. Sie sind genau die projektive Gerade (wende obigen Faktorisierungsprozeß \mathbf{K}^3/\sim auf \mathbf{K}^2 an). Diese Punkte mit $Z = 0$ sind sozusagen die Gerade im Unendlichen oder auch der Horizont der Ebene. Für unsere Kurve $F(x, y) = 0$ erhalten wir $\tilde{F}(X, Y, Z) = 0$ durch Substitution von $x = X/Z, y = Y/Z$:

$$\begin{aligned} y^2 &= x^3 + Ax + B \\ \Leftrightarrow Y^2Z &= X^3 + AXZ^2 + BZ^3 \end{aligned}$$

Für $Z = 0$ ergibt sich: $0 = X^3$. D.h. einzig der projektive Punkt $(0, 1, 0)$ kommt für $Z = 0$ in Frage. Das ist der oben erwähnte Punkt O oder Punkt im Unendlichen.

3 Das Gruppengesetz

Wir wollen nun eine Addition einführen und dabei gleich Körpererweiterungen im Auge behalten. Seien also jetzt $A, B \in \mathbf{k}$ wie oben, $\mathbf{K} \supseteq \mathbf{k}$ ein Erweiterungskörper von \mathbf{k} und $E(\mathbf{K})$ die Menge der Punkte $(x, y) \in \mathbf{K}^2$ die (1) erfüllen und 0 . Der Punkt 0 soll die Rolle des Neutralelements spielen. Das Inverse zu $P = (x, y)$ soll $-P = (x, -y)$ sein. Zwei von 0 verschiedene Punkte $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2) \in E(\mathbf{K})$ mit $P_1 + P_2 \neq 0$ addieren sich wie folgt: Für $P_1 \neq P_2$ haben wir $x_1 \neq x_2$ und setzen $\lambda = (y_2 - y_1)/(x_2 - x_1)$. Andernfalls ist $y_1 \neq 0$ und wir nehmen $\lambda = (3x_1^2 + A)/(2y_1)$. Dann ist $P_3 = P_1 + P_2 = (x_3, y_3)$ mit:

$$x_3 = -x_1 - x_2 + \lambda^2, \quad y_3 = -y_1 - \lambda(x_3 - x_1). \quad (2)$$

Veranschaulichen kann man sich den Vorgang im Fall $\mathbf{K} = \mathbf{R}$: Hier ist die elliptische Kurve eine gewöhnliche Kurve in der Ebene (plus 0 im Unendlichen). Zwei Punkte $\neq 0$ zu addieren heißt (für $P_1 + P_2 \neq 0$) eine Sekante durch die Kurvenpunkte zu legen (bzw. Tangente falls $P_1 = P_2$) und den dritten Schnittpunkt mit der Kurve als $-P_3$ zu nehmen. So ist die Summe der Schnittpunkte - und doppelt gezählt der Berührungspunkte - einer Geraden mit der elliptischen Kurve immer gerade 0 .

Diese Setzung ergibt eine abelsche Gruppe (o. Bew.). Für Körpererweiterungen $\mathbf{K} \leq \mathbf{L}$ hat man: $E(\mathbf{K})$ ist Untergruppe von $E(\mathbf{L})$ (klar - die Koordinaten werden ja nur durch die Grundrechenarten miteinander verknüpft).

4 Elliptische Kurven über endlichen Körpern

Von nun an sei $\mathbf{k} = \mathbf{F}_q$ der endliche Körper mit $q = p^r$ Elementen und $p = \text{char } \mathbf{k}$. Erzeugt durch die Polynome in einer Unbestimmten über \mathbf{F}_p modulo einem über \mathbf{F}_p irreduziblen Polynom $m(X)$ vom Grad r : $\mathbf{F}_q \cong \mathbf{F}[X]/(m(X))$.

Für $\mathbf{k} = \mathbf{F}_p$ gibt es folgende explizite Formel für die Gruppenordnung von $E(\mathbf{F}_p)$:

$$\#E(\mathbf{F}_p) = 1 + \sum_{x \bmod p} \left(\left(\frac{x^3 + Ax + B}{p} \right) + 1 \right)$$

Dabei sei $\left(\frac{a}{p} \right)$ das Legendre Symbol, welches 1 liefert, wenn a ein Quadrat modulo p ist, -1 wenn es keines ist und 0 wenn $a \equiv 0 \pmod{p}$ ist. Die Zählung der Punkte läuft folgendermaßen: Untersuche alle Restklassen $x \bmod p$; wenn

$a = x^3 + Ax + B$ ein Quadrat ist ($(\frac{a}{p}) = 1$), so erhalten wir aus (1) genau zwei Kurvenpunkte: (x, y) und $(x, -y)$. Also $(\frac{a}{p}) + 1$. Für a kein Quadrat gibt es auch keinen Punkt auf der Kurve, also wieder $(\frac{a}{p}) + 1$. Für $a \equiv 0 \pmod p$ kommt als Lösung von (1) nur $y = 0$ in Frage, also genau ein Kurvenpunkt; wieder $(\frac{a}{p}) + 1$. Die führende 1 zählt die 0.

Sei $\bar{\mathbf{F}}_q$ der algebraische Abschluß von \mathbf{F}_q , d.h. der Körper, in dem alle Polynome über \mathbf{F}_q zerfallen. Die Gruppe $E(\bar{\mathbf{F}}_q)$ ist eine unendliche Torsionsgruppe. Warum unendlich? Offenbar gibt es über \mathbf{F}_q jedenfalls irreduzible Polynome beliebig hohen Grades. Dies zeigt der analoger Schluß wie man über den ganzen Zahlen die Unendlichkeit der Primzahlmenge zeigt: Das Produkt aller endlich vielen plus 1 muß als Teiler eine bislang noch nicht bekannte Primzahl haben. Damit haben wir also jedenfalls schon einmal unendlich viele irreduzible Polynome. Weil \mathbf{F}_q abzählbar ist und damit auch die Polynome vom Grad $\leq n$, folgt alles weitere. Deswegen gibt auch beliebig viele Körpererweiterungen $\mathbf{F}_q = \mathbf{k} \leq \mathbf{K}_1 \leq \mathbf{K}_2 \leq \mathbf{K}_3 \dots$. So können wir uns immer neue Elemente für x verschaffen, die wir in (1) einsetzen. Die resultierende rechte Seite ist dann entweder bereits ein Quadrat oder gegebenenfalls erst nach einer erneuten Körpererweiterung vom Grade 2. Wir haben damit eine Folge von immer neuen Elementen in $E(\bar{\mathbf{F}}_q)$ konstruiert. Warum Torsionsgruppe? Nun, jedes feste Element, das wir hernehmen, ist in einem endlichen Körper enthalten. Als solches hat es auch nur endliche Ordnung.

Mit $E[n]$ wollen wir die Untergruppe der n -Torsionselemente bezeichnen, d.h. die Punkte P mit $\underbrace{P + P + \dots + P}_{n \text{ mal}} = 0$. Für $n \not\equiv 0 \pmod p$ ist $E[n] \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ (o. Bew.).

5 Der Frobenius Endomorphismus

Es sei Φ der Frobenius Endomorphismus einer elliptischen Kurve über \mathbf{F}_q ; er operiere auf $E(\bar{\mathbf{F}}_q)$ durch

$$(x, y) \xrightarrow{\Phi} (x^q, y^q).$$

Wir wollen uns vergewissern, daß Φ zuerst einmal eine Selbstabbildung ist:

$$y^2 = x^3 + Ax + B$$

$$\Leftrightarrow \Phi y^2 = \Phi x^3 + \Phi A \Phi x + \Phi B$$

$$\Phi|_{\mathbf{F}_q} = \text{id}_{\mathbf{F}_q}$$

$$\Leftrightarrow (\Phi y)^2 = (\Phi x)^3 + A \Phi x + B$$

D.h. $(\Phi x, \Phi y) \in E(\bar{\mathbf{F}}_q)$. Die anderen Bedingungen für *Operation von Gruppe auf Menge* sind offensichtlich erfüllt.

In $\text{End}_{\mathbf{F}_q} E$ genügt der Frobenius Endomorphismus einer eindeutigen Relation

$$\Phi^2 - t\Phi + q = 0 \quad (t \in \mathbf{Z}) \quad (3)$$

Wir nennen t die *Spur* des Frobenius Endomorphismus. Es gilt

$$|t| \leq 2\sqrt{q} \quad (\text{Riemannsche Vermutung}) \quad (4)$$

und das

$$\#E(\mathbf{F}_q) = q + 1 - t. \quad (5)$$

6 Die Teilungspolynome

Wir führen Polynome $\Psi_n(X, Y) \in \mathbf{F}_q[X, Y]$ für $n \in \mathbf{Z}_{\geq -1}$ ein:

$$\Psi_{-1}(X, Y) = -1, \quad \Psi_0(X, Y) = 0, \quad \Psi_1(X, Y) = 1, \quad \Psi_2(X, Y) = 2Y,$$

$$\Psi_3(X, Y) = 3X^4 + 6AX^2 + 12BX - A^2,$$

$$\Psi_4(X, Y) = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3),$$

$$\Psi_{2n}(X, Y) = \Psi_n(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)/2Y \quad (n \in \mathbf{Z}_{\geq 1}),$$

$$\Psi_{2n+1}(X, Y) = \Psi_{n+2}\Psi_n^3 - \Psi_{n+1}^3\Psi_{n-1} \quad (n \in \mathbf{Z}_{\geq 1}).$$

Auf E verschwinden diese Polynome genau an den n -Torsionspunkten. Relation (1) gestattet es uns, Y^2 Terme durch $X^3 + AX + B$ zu ersetzen und damit den Y -Grad auf ≤ 1 zu beschränken. Wir behaupten weiter, daß das resultierende Polynom $\Psi'_n(X, Y)$ in $\mathbf{F}_q[X]$ (für n ungerade) oder in $Y\mathbf{F}_q[X]$ (für n gerade) liegt. Der anstehende Induktionsbeweis sei hier exemplarisch für den ersten der vier Fälle vorgeführt: Fall 1: $2n \equiv 0 \pmod{4}$ ($n \geq 1$)

$$\Psi'_{2n}(X, Y) = \underbrace{\Psi'_n}_{\in Y\mathbf{F}_q[X]} \left(\underbrace{\Psi'_{n+2}}_{\in Y\mathbf{F}_q[X]} \underbrace{\Psi_{n-1}^2}_{\in \mathbf{F}_q[X]^2} - \underbrace{\Psi'_{n-2}}_{\in Y\mathbf{F}_q[X]} \underbrace{\Psi_{n+1}^2}_{\in \mathbf{F}_q[X]^2} \right) / 2Y \in Y\mathbf{F}_q[X]$$

$$\underbrace{\hspace{15em}}_{\in Y\mathbf{F}_q[X]}$$

Diese Beobachtung wird man sich bei den später folgenden Rechnungen zunutze machen, um die Polynomarithmetik in $\mathbf{F}_q[X, Y]$ durch die in $\mathbf{F}_q[X]$ zu ersetzen. Man wird sich bei jedem Polynom merken, ob ihm ein Y hinzuzustellen ist. Wenn man zwei Polynome multipliziert, die beide ein Y mitführen, so wird man das Ergebnis anschliessend noch mit $(X^3 + AX + B)$ multiplizieren.

Für alles weitere wollen wir nun die Ψ' -Polynome einfach Ψ nennen.

Für den X -Grad der Ψ -Polynome erhalten wir folgende Abschätzungen:

$$\deg_X \Psi_n = \frac{1}{2}(n^2 - 1) \quad \text{für } n \text{ ungerade, } n \not\equiv 0 \pmod{p},$$

$$\deg_X \Psi_n = \frac{1}{2}(n^2 - 4) \quad \text{für } n \text{ gerade, } n \not\equiv 0 \pmod{p}.$$

Proposition 1 (o. Bew.): Sei $P = (x, y) \in E(\bar{\mathbf{F}}_q)$ mit $P \neq 0$ und $n \in \mathbf{Z}_{\geq -1}$; dann

$$nP = 0 \Leftrightarrow \Psi_n(x, y) = 0.$$

Proposition 2 (o. Bew.): Sei $P = (x, y) \in E(\bar{\mathbf{F}}_q)$; sei $n \in \mathbf{Z}_{\geq -1}$ mit $nP \neq 0$; dann

$$nP = \left(x - \frac{\Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2}{4Y\Psi_n^3} \right). \quad (6)$$

Wir wollen den Frobenius Endomorphismus nun nur auf l -Torsionspunkten betrachten (mit primem $l \neq q$). Offensichtlich ist er auch dort Selbstabbildung. Wir haben eine Abbildung

$$\text{End}_{\mathbf{F}_q} E \rightarrow \text{End}_{\text{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)} E[l].$$

Es sei Φ_l das Bild von Φ in der Gruppe auf der rechten Seite. Aus (3) wird folgende Relation auf $E[l]$:

$$\Phi_l^2 - t'\Phi_l + q = 0 \quad (t' \pmod{l}). \quad (7)$$

Das bedeutet, daß wir die Spur des Frobenius Endomorphismus mod l bestimmen können, indem wir prüfen, für welches t' die Relation (7) auf $E[l]$ gilt.

7 Der Schoof Algorithmus

Sei l eine Primzahl $\neq 2, p$. Unser Ziel soll es sein, das τ zu bestimmen, so daß die folgende Relation auf $E[l]$ gilt:

$$\Phi_l^2 + k = \tau\Phi_l \quad (\tau \in \mathbf{Z}/l\mathbf{Z}; k \equiv q \pmod{l}). \quad (8)$$

Sei $0 \neq P = (x, y) \in E[l]$. Nach Proposition 2 ist die Relation (8) für (x, y) genau dann erfüllt, wenn gilt

$$\begin{aligned} & (x^{q^2}, y^{q^2}) + \left(x - \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2}, \frac{\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2}{4Y\Psi_k^3} \right) \\ &= \begin{cases} 0 & \text{für } \tau \equiv 0 \pmod{l}, \\ \left(x^q - \left(\frac{\Psi_{r-1}\Psi_{r+1}}{\Psi_r^2} \right)^q, \left(\frac{\Psi_{r+2}\Psi_{r-1}^2 - \Psi_{r-2}\Psi_{r+1}^2}{4y\Psi_r^3} \right)^q \right) & \text{sonst} \end{cases} \end{aligned} \quad (9)$$

Um die Additionsformeln (2) für die Punkte auf der linken Seite anwenden zu können, müssen wir die Fälle unterscheiden, ob sie verschieden sind oder nicht. Dazu testen wir zuerst, ob es einen von Null verschiedenen Punkt $P = (x, y)$ in $E[l]$ gibt, für den $\Phi_l^2 P = \pm kP$ gilt (also gleiche X-Koordinaten). Es muß also gelten

$$x^{q^2} = x - \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2}(x, y) \quad (10)$$

oder

$$x^{q^2} = \begin{cases} x - \frac{\Psi_{k-1}\Psi_{k+1}}{(\Psi_k^2/y)^2(x^3+Ax+B)} & (\text{für } k \text{ gerade}) \\ x - \frac{(\Psi_{k-1}/y)(\Psi_{k+1}/y)(x^3+Ax+B)}{\Psi_k^2} & (\text{für } k \text{ ungerade}) \end{cases} \quad (11)$$

$$\Leftrightarrow (x^{q^2} - x)(\Psi_k/y)^2(x^3 + Ax + B) + \Psi_{k-1}\Psi_{k+1} = 0 \quad (\text{für } k \text{ gerade})$$

$$(x^{q^2} - x)\Psi_k^2 + (\Psi_{k-1}/y)(\Psi_{k+1}/y)(x^3 + Ax + B) = 0 \quad (\text{für } k \text{ ungerade}) \quad (12)$$

Wir können testen, ob ein solcher Punkt P in $E[l]$ existiert, indem wir berechnen (in $\mathbf{F}_q[X]$):

$$\text{ggT}((X^{q^2} - X)(\Psi_k/Y)^2(X^3 + AX + B) + \Psi_{k-1}\Psi_{k+1}, \Psi_l/Y)$$

$$\text{ggT}((X^{q^2} - X)\Psi_k^2 + (\Psi_{k-1}/Y)(\Psi_{k+1}/Y)(X^3 + AX + B), \Psi_l/Y) \quad (13)$$

(Für k gerade bzw. ungerade). Wenn sich dieser ggT als eins herausstellt, folgt $\tau \neq 0$ in (8) und wir können beim Berechnen von $\Phi_l^2 P + kP$ die Formel (2) anwenden und verschiedene X-Koordinaten annehmen. Mehr dazu unter *Fall 2*.

8 Der Fall 1

Hier müssen wir zwei Unterfälle unterscheiden. Im Fall 1 α) existiert ein $0 \neq P$ in $E[l]$ mit $\Phi_l^2 P = -qP$. Mit (3) gilt dann $t\Phi_l P = 0$. Wegen $\Phi_l P \neq 0$ folgt: $t \equiv 0 \pmod{l}$. Im Fall 1 β) gilt: $\exists 0 \neq P \in E[l] : \Phi_l^2 P = qP$.

$$\stackrel{(3)}{\Rightarrow} \underbrace{2qP}_{\neq 0} = t \underbrace{\Phi_l P}_{\neq 0} \quad (14)$$

Wegen $q = p^r$ und $l \neq 2, p$ folgt $t \not\equiv 0 \pmod{l}$.

$$\Leftrightarrow \Phi_l P = \frac{2q}{t} P \quad (t \in (\mathbf{Z}/l\mathbf{Z})^\times)$$

$$\Leftrightarrow \Phi_l^2 P = \frac{4q^2}{t^2} P$$

$$\Leftrightarrow 4q^2 P = t^2 \Phi_l^2 P = t^2 q P$$

$$\begin{aligned} &\Leftrightarrow t^2 P = 4qP \\ &\Leftrightarrow t^2 \equiv 4q \pmod{l} \end{aligned} \tag{15}$$

Beachte: $q = p^r, l \neq q \Rightarrow q \not\equiv 0 \pmod{l}; l \neq 2 \Rightarrow 4q \not\equiv 0 \pmod{l}$. Sei jetzt $w \in (\mathbf{Z}/l\mathbf{Z})^\times$ eine Quadratwurzel von $q \pmod{l}$ ($t \equiv \pm 2w \pmod{l}$). Mit (3) haben wir in $E[l]$:

$$\begin{aligned} &\Phi_l^2 - t\Phi_l + q = 0 \\ &\Leftrightarrow \Phi_l^2 - t\Phi_l + \frac{t^2}{4} = 0 \\ &\Leftrightarrow \left(\Phi_l - \underbrace{\frac{1}{2}t}_{\equiv \pm w \pmod{l}} \right)^2 = 0 \end{aligned} \tag{16}$$

D.h. für Φ_l kommen als Eigenwerte nur $\pm w$ in Frage. Da wir also noch nicht wissen, welcher Unterfall vorliegt, testen wir zuerst, ob $\left(\frac{q}{l}\right) = -1$ ist. Dann nämlich sind wir in Fall 1 α) und $t \equiv 0 \pmod{l}$. Ansonsten berechnen wir obige Quadratwurzel w von q und schauen, welcher Eigenwert vorliegt. Dies kann durch eine analoge ggT-Berechnung geschehen wie in (13) - ersetze X^{q^2} durch X und k durch w . Wir haben drei Möglichkeiten:

$$\begin{aligned} &\exists 0 \neq P \in E[l] : \Phi_l P = wP = \frac{1}{2}tP \quad \Rightarrow t \equiv 2w \pmod{l} \\ &\exists 0 \neq P \in E[l] : \Phi_l P = -wP = \frac{1}{2}tP \quad \Rightarrow t \equiv -2w \pmod{l} \\ &\forall 0 \neq P \in E[l] : \Phi_l P \neq \pm wP \quad \Rightarrow \text{Fall 1}\alpha); t \equiv 0 \pmod{l} \end{aligned}$$

Um uns zwischen $+w$ und $-w$ zu entscheiden, müssen wir eine erneute ggT-Berechnung ansetzen, diesmal für die Y -Koordinaten. Mit Proposition 2 gilt:

$$Y^q = \frac{\Psi_{w+2}\Psi_{w-1}^2 - \Psi_{w-2}\Psi_{w+1}^2}{4Y\Psi_w^3} \tag{17}$$

$$\Leftrightarrow Y^q = \begin{cases} \frac{(\Psi_{w+2}/Y)\Psi_{w-1}^2 - (\Psi_{w-2}/Y)\Psi_{w+1}^2}{4\Psi_w^3} & \text{(für } w \text{ gerade)} \\ \frac{(\Psi_{w+2}(\Psi_{w-1}/Y)^2 - \Psi_{w-2}(\Psi_{w+1}/Y)^2)Y^2}{4Y\Psi_w^3} & \text{(für } w \text{ ungerade)} \end{cases} \tag{18}$$

Und in $\mathbf{F}_q[X]$:

$$\begin{aligned} &\text{ggT}(4(X^3 + AX + B)^{\frac{q+3}{2}}(\Psi_w/Y)^3 - (\Psi_{w+2}/Y)\Psi_{w-1}^2 + (\Psi_{w-2}/Y)\Psi_{w+1}^2, \Psi_l) \\ &\text{ggT}(4(X^3 + AX + B)^{\frac{q-1}{2}}\Psi_w^3 - \Psi_{w+2}(\Psi_{w-1}/Y)^2 + \Psi_{w-2}(\Psi_{w+1}/Y)^2, \Psi_l) \end{aligned} \tag{19}$$

(Für w gerade bzw. ungerade). Ist dieser ggT 1, so haben wir $t \equiv -2w \pmod{l}$, ansonsten $t \equiv 2w \pmod{l}$.

9 Der Fall 2

Wir wissen also, daß die Punkte auf der linken Seite von (9) unterschiedliche X-Koordinaten haben (also das $\Phi_l^2 P \neq \pm k P \quad \forall 0 \neq P \in E[l]$). Wir wenden die Additionsformeln (2) für $P = (x, y)$ an:

$$\begin{aligned} \lambda(X, Y) &:= \alpha(X, Y)/\beta(X, Y) \\ \alpha(X, Y) &:= \Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2 - 4Y^{q^2+1}\Psi_k^3 \\ \beta(X, Y) &:= 4\Psi_k Y((X - X^{q^2})\Psi_k^2 - \Psi_{k-1}\Psi_{k+1}) \\ \Phi_l^2 P + kP &= \left(-x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2, \right. \\ &\quad \left. -y^{q^2} - \lambda \left(-2x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2 \right) \right) \end{aligned} \quad (20)$$

Auf der rechten Seite ergibt sich nach (9) in diesem Fall:

$$\tau\Phi_l P = \left(x^q - \left(\frac{\Psi_{\tau-1}\Psi_{\tau+1}}{\Psi_\tau^2} \right)^q, \left(\frac{\Psi_{\tau+2}\Psi_{\tau-1}^2 - \Psi_{\tau-2}\Psi_{\tau+1}^2}{4y\Psi_\tau^3} \right)^q \right) \quad (21)$$

Wir formen um: X-Bedingung mal $\Psi_k^2\beta^2\Psi_\tau^{2q}$:

$$\underbrace{\left[\left(\Psi_{k-1}\Psi_{k+1} - (X^{q^2} + X^q + X)\Psi_k^2 \right) \beta^2 + \Psi_k^2\alpha^2 \right]}_{=:\text{pxC0}} \Psi_\tau^{2q} + \Psi_{\tau-1}^q \Psi_{\tau+1}^q \underbrace{\beta^2\Psi_k^2}_{=:\text{pxC1}} = 0 \quad (22)$$

Y-Bedingung mal $4\Psi_k^2 Y^q \Psi_\tau^{3q} \beta^3$:

$$\begin{aligned} \Psi_\tau^{3q} 4Y^q \left[\alpha \left[\left((2X^{q^2} + X)\Psi_k^2 - \Psi_{k-1}\Psi_{k+1} \right) \beta^2 - \alpha^2\Psi_k^2 \right] - \Psi_k^2\beta^3 Y^{q^2} \right] \\ \underbrace{\hspace{10em}}_{=:\text{pxC2}} \\ \underbrace{-\Psi_k^2\beta^3}_{=:\text{pxC3}} (\Psi_{\tau+2}\Psi_{\tau-1}^2 - \Psi_{\tau-2}\Psi_{\tau+1}^2)^q = 0 \end{aligned} \quad (23)$$

Die eingeführten Konstanten-Ausdrücke sind von τ unabhängig und können nach der Wahl von l sofort berechnet werden.

A Die Diskriminantenbedingung

Gegeben seien eine Matrix $M \in \mathbf{K}^{n \times n}$ (\mathbf{K} algebraisch abgeschlossen), ihr charakteristisches Polynom $f(X)$:

$$f(X) = \det(XI - M) = \prod_{i=1}^n (X - \lambda_i)$$

und ein beliebiges Polynom $g(X)$:

$$g(X) = \prod_{j=1}^m (X - \gamma_j)$$

Dann gilt:

$$\begin{aligned} \det(g(M)) &= \det \left(\prod_{j=1}^m (M - \gamma_j I) \right) = \prod_{j=1}^m \det(M - \gamma_j I) \\ &= (-1)^{m \cdot n} \prod_{j=1}^m \det(\gamma_j I - M) = (-1)^{m \cdot n} \prod_{j=1}^m f(\gamma_j) \\ &= (-1)^{m \cdot n} \prod_{j=1}^m \prod_{i=1}^n (\gamma_j - \lambda_i) = \prod_{i=1}^n \prod_{j=1}^m (\lambda_i - \gamma_j) = \prod_{i=1}^n g(\lambda_i) \end{aligned}$$

Sei jetzt das Polynom $f(X)$ vorgegeben.

Wir konstruieren seine Begleitmatrix

$$M = \begin{pmatrix} 0 & & & -\lambda_0 \\ 1 & & & -\lambda_1 \\ & 1 & & -\lambda_2 \\ & & \ddots & \vdots \\ & & & 1 & -\lambda_{n-1} \end{pmatrix}$$

mit $\det(XI - M) = f(X)$.

Als $g(X)$ wählen wir speziell die formale Ableitung $f'(X)$:

$$g(X) := f'(X) = \sum_{k=1}^n \prod_{\substack{i=1 \\ i \neq k}}^n (X - \lambda_i)$$

Dann gilt:

$$\begin{aligned} \det(f'(M)) &= \prod_{j=1}^n f'(\lambda_j) = \prod_{j=1}^n \sum_{k=1}^n \prod_{\substack{i=1 \\ i \neq k}}^n (\lambda_j - \lambda_i) \\ &= \prod_{j=1}^n \prod_{\substack{i=1 \\ i \neq j}}^n (\lambda_j - \lambda_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i < j} (\lambda_i - \lambda_j)^2 = \begin{cases} 0 & \exists i, j \text{ mit } i \neq j : \lambda_i = \lambda_j \\ \neq 0 & \text{sonst} \end{cases} \end{aligned}$$

Wir haben damit also einen Ausdruck gefunden, der genau dann verschwindet, wenn zwei der Nullstellen von f zusammenfallen.

In unserem Falle:

$$f(X) = X^3 + AX + B$$

$$\begin{aligned}
g(X) &:= f'(X) = 3X^2 + A \\
M &= \begin{pmatrix} 0 & 0 & -B \\ 1 & 0 & -A \\ 0 & 1 & 0 \end{pmatrix}, \quad M^2 = \begin{pmatrix} 0 & -B & 0 \\ 0 & -A & -B \\ 1 & 0 & -A \end{pmatrix} \\
f'(M) = 3M^2 + AI &= \begin{pmatrix} 0 & -3B & 0 \\ 0 & -3A & -3B \\ 3 & 0 & -3A \end{pmatrix} + \begin{pmatrix} A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & A \end{pmatrix} \\
&= \begin{pmatrix} A & -3B & 0 \\ 0 & -2A & -3B \\ 3 & 0 & -2A \end{pmatrix}
\end{aligned}$$

Dann gilt:

$$\det(f'(M)) = A(-2A)(-2A) + 27B^2 = 4A^3 + 27B^2$$

B Singuläre Punkte

Äquivalent zur Diskriminantenbedingung kann man die Singularität einer elliptischen Kurve über die Existenz von singulären Punkten definieren. Singulär ist ein Kurvenpunkt genau dann, wenn beide partiellen Ableitungen in diesem Punkt verschwinden.

$$\begin{aligned}
F(X, Y) &= X^3 + AX + B - Y^2 = 0 \\
\frac{\partial F}{\partial x} &= 3x_0^2 + A = 0 \Leftrightarrow x_0^2 = -\frac{1}{3}A \\
\frac{\partial F}{\partial y} &= -2y_0 = 0 \Leftrightarrow y_0 = 0
\end{aligned}$$

Einsetzen ergibt:

$$\begin{aligned}
F(x_0, y_0) &= x_0^2 x_0 + Ax_0 + B = 0 \\
&\Leftrightarrow -\frac{1}{3}Ax_0 + Ax_0 + B = 0 \\
&\Leftrightarrow \frac{2}{3}Ax_0 + B = 0 \\
&\Leftrightarrow \frac{4}{9}A^2 \underbrace{x_0^2}_{=-\frac{1}{3}A} = B^2 \\
&\Leftrightarrow -\frac{4}{27}A^3 = B^2 \\
&\Leftrightarrow 4A^3 + 27B^2 = 0
\end{aligned}$$

Literatur:

R. Schoof; *Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p*; Math. Of Comp., Vol. 44, No. 170, 1985, pp 483-494