Gregor Leander
7.07.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Lösungsvorschläge zum Übungsblatt 7

Aufgabe 1 *Rechnen auf Elliptischen Kurven I*
Betrachte die über $\mathbb{F}_{19}$ durch folgende Gleichung definierte Kurve

$$E : y^2 = x^3 + x + 9 \ .$$

1. Zeige, dass E eine elliptische Kurve ist. (2 Punkte)
2. Bestimme alle Punkte auf E über $\mathbb{F}_{19}$. (4 Punkte)
3. Bestimme die Punkte der Ordnung 2 auf E. (2 Punkte)
4. Sei $P = (1, 12) \in E$. Berechne $445 \cdot P$. (2 Punkte)

Lösung

1. Da $char\,(E(\mathbb{F}_{19})) = 19 \neq 2, 3$ gilt, muss

   $$\Delta = 4a^3 + 27b \neq 0$$

   gelten. Dies ist für $a = 1$ und $b = 9$ erfüllt und somit ist $E(\mathbb{F}_{19})$ nicht singulär und erfüllt alle Anforderungen an eine elliptische Kurve.

2. $$\begin{aligned} E(\mathbb{F}_{19}) \quad = \quad & \{(0,3),(0,16),(1,7),(1,12) \\ & (2,0),(3,1),(3,18),(4,1) \\ & (4,18),(5,5),(5,14),(7,6) \\ & (7,13),(8,4),(8,15),(9,5) \\ & (9,14),(12,1),(12,18),(15,6) \\ & (15,13),(16,6),(16,13),(18,8) \\ & (18,11),\emptyset\} \end{aligned}$$

3. Da $E(\mathbb{F}_{19})$ eine Gruppe der Kardinalität 26 ist und $2 \mid 26$ gilt, weiß man, dass es Elemente (bzw. Punkte) der Ordnung 2 in $E(\mathbb{F}_{19})$ gibt. Da für alle Elemente der Ordnung 2 $2Y \equiv 0 \bmod 17$ gelten muss, folgt dass $(2, 0)$ der gesuchte Punkt ist.

4. Es gibt zwei mögliche Lösungswege für diese Aufgabe. Entweder man berechnet den „Double-and-Add“- Algorithmus vollständig für 445 oder man bedenkt, dass

$$max(ord_{E(\mathbb{F}_{19})}(P)) = 26$$

gilt und das somit

$$445P \equiv (445 \bmod 26)P \equiv 3P$$

gilt.

□

Aufgabe 2 *Rechnen auf Elliptischen Kurven II*
Betrachte die Kurve

$$E_{p,k} : y^2 + x\,y = x^3 - 2\,x^2 + x + 3$$

über $\mathbb{F}_{p^k}$, wobei p eine Primzahl ist und k eine natürliche Zahl ist.

1. Für welche Werte von p und k ist die Kurve $E_{p,k}$ singulär? (4 Punkte)
2. Für alle andere Werte von p und k bestimme die Weierstraß-Form von $E_{p,k}$. (3 Punkte)

Lösung

1. Wenn ein Punkt (x_P, y_P) ein singulärer Punkt von $E/\mathbb{F}_p$ ist, dann muss er auch ein singulärer Punkt von $E/\mathbb{F}_p^k$ sein. Aus dem Isomorphismus $\mathbb{F}_p^k \cong \mathbb{F}_{p^k}$ folgt dann, dass er auch für $E/\mathbb{F}_{p^k}$ ein singulärer Punkt ist. Es reicht also aus, alle p zu bestimmen, für die die Kurve singulär ist. Es gibt hier drei Lösungswege:

   - **Berechnung mit Hilfe einer expliziten Formel:** Man kann beispielsweise die Formel

   $$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \bmod p$$

   aus [**?**] verwenden, wobei

   $$\begin{aligned} y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6 \\ b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

   gelten. Wenn man nun die Werte $a_1 = 1$, $a_2 = -2$, $a_3 = 0$, $a_4 = 1$ und $a_6 = 3$ einsetzt, erhält man:

   $$\Delta = -4386 \bmod p = (-1) \cdot 2 \cdot 3 \cdot 17 \cdot 43 \bmod p$$

   Die Kurve ist also genau für $p \in \{2, 3, 17, 43\}$ singulär.

- **Verwendung der Definition des singulären Punktes:** Alternativ kann man testen, wann die Kurve einen singulären Punkt enthält. Aus der Definition des singulären Punktes müssen gleichzeitig

$$\begin{aligned} f(x,y) = &\quad y^2 + xy - x^3 + 2x - x - 3 &&= 0 \quad (1)\\ \frac{\partial f(x,y)}{\partial x} = &\quad y - 3x^2 + 4x - 1 &&= 0 \quad (2)\\ \frac{\partial f(x,y)}{\partial y} = &\quad 2y + x &&= 0 \quad (3) \end{aligned}$$

gelten. Nun löst man (3) nach x auf, erhält $x = -2y$ und setzt dies in (1) und (2) ein:

$$\begin{aligned} f(-2y,y) = &\quad p(y) = 8y^3 + 7y^2 + 2y - 3 &&= 0\\ \frac{\partial f(-2y,y)}{\partial x} = &\quad q(y) = -12y^2 - 7y - 1 &&= 0 \end{aligned}$$

Die Idee für das weitere Vorgehen besteht darin, eine Linearkombination aus $p(y) = 0$ und $q(y) = 0$ zu berechnen und zu prüfen, wann diese zu 0 wird. Dabei stören aber der kubische Term in $p(y)$ und die quadratischen Terme in beiden Gleichungen.

Deswegen bildet man zuerst eine Linearkombination bei der geschickterweise die kubischen Terme wegfallen:

$$\begin{aligned} g(y) &= 3(8y^3 + 7y^2 + 2y - 3) + 2y(-12y^2 - 7y - 1)\\ &= 7y^2 + 4y - 9 \end{aligned}$$

Nun berechnet man die nächste Linearkombination, bei der geschickterweise die quadratischen Terme wegfallen:

$$\begin{aligned} 12g(y) + 7p(y) &= 12(7y^2 + 4y - 9) + 7(-12y^2 - 7y - 1)\\ &= -y - 115 \stackrel{!}{=} 0 \end{aligned}$$

Somit muss also der Fall $y = -115$ näher betrachtet werden. Es gilt:

$$\begin{aligned} g(-115) = &\quad 7 \cdot 115^2 - 4 \cdot 115 - p &&= 2 \cdot 3^2 \cdot 7 \cdot 17 \cdot 43\\ p(-115) = &\quad -8 \cdot 115^3 + 7 \cdot 115^2 - 2 \cdot 115 - 3 &&= (-1) \cdot 2 \cdot 3 \cdot 17 \cdot 43 \cdot 2753 \end{aligned}$$

Die Lösung besteht aus den $\underline{p = \{2, 3, 17, 43\}}$, die in beiden Ergebnissen vorkommen.

- **Variablensubstitution:** Diese Lösung ist die charmanteste, da sie gleichzeitig die Weierstrassform der Kurve liefert. Nach Lockhart ersetzt man

$$(x, y) \mapsto (s^{-2}\tilde{x} + b, s^{-3}\tilde{y} + A(\tilde{x}))$$

wobei $A(\tilde{x}) = A_1\tilde{x} + A_0$ gilt. Somit ändert sich der Grad der Kurve nicht und man erhält:

$$(s^{-3}\tilde{y}+A(\tilde{x}))^2+(s^{-2}\tilde{x}+b)(s^{-3}\tilde{y}+A(\tilde{x})) = \left[(s^{-2}\tilde{x}+b)^3 - 2(s^{-2}\tilde{x}+b)^2 + (s^{-2}\tilde{x}+b) + 3\right]$$

Wenn man dies nun ausmultipliziert und auf beiden Seiten mit s^6 multipliziert erhält man auf der linken Seite:

$$\begin{aligned} s^6\left[(s^{-3}\tilde{y}+A(\tilde{x}))^2 + (s^{-2}\tilde{x}+b)(s^{-3}\tilde{y}+A(\tilde{x}))\right] &= \\ s^6\left[s^{-6}\tilde{y}^2 + 2s^{-3}\tilde{y}A(\tilde{x}) + A^2(\tilde{x}) + s^{-5}\tilde{x}\tilde{y} + s^{-2}\tilde{x}A(\tilde{x}) + s^{-3}b\tilde{y} + bA(\tilde{x})\right] &= \\ s^6(A^2(\tilde{x}) + bA(\tilde{x})) + s^4\tilde{x}A(\tilde{x}) + s^3(b\tilde{y} + 2\tilde{y}A(\tilde{x})) + s\tilde{x}\tilde{y} + \tilde{y}^2 &= \end{aligned}$$

Und auf der rechten Seite:

$$\begin{aligned} &= \left[(s^{-2}\tilde{x}+b)^3 - 2(s^{-2}\tilde{x}+b)^2 + (s^{-2}\tilde{x}+b) + 3\right] s^6 \\ &= \left[s^{-6}\tilde{x}^3 + 3s^{-4}\tilde{x}^2 b + 3s^{-2}\tilde{x}b^2 + b^3 - 2s^{-4}\tilde{x}^2 - 4s^{-2}\tilde{x}b - 2b^2 + s^{-2}\tilde{x} + b + 3\right] s^6 \\ &= s^6(b^3 - 2b^2 + b + 3) + s^4(3\tilde{x}b^2 - 4\tilde{x}b + \tilde{x}) + s^2(3\tilde{x}^2 b - 2\tilde{x}^2) + \tilde{x}^3 \end{aligned}$$

Nun bringt man alle Terme, die nicht $\tilde{y}$ enthalten auf die rechte Seite, erhält

$$\begin{aligned} \tilde{y}^2 + \tilde{y}\left[s^3(b + 2A(\tilde{x})) + s\tilde{x}\right] &= \\ &= s^6(b^3 - 2b^2 + b + 3 - A^2(\tilde{x}) - bA(\tilde{x})) \\ &\quad + s^4(3\tilde{x}b^2 - 4\tilde{x}b + \tilde{x} - \tilde{x}A(\tilde{x})) \\ &\quad + s^2(3\tilde{x}^2 b - 2\tilde{x}^2) + \tilde{x}^3 \end{aligned}$$

und setzt $A(\tilde{x}) = A_1\tilde{x} + A_0$ ein und erhält auf der linken Seite

$$\tilde{y}^2 + \tilde{y}s\left[(2s^2A_1 + 1)\tilde{x} + s^2(b + 2A_0)\right] =$$

und auf der rechten Seite:

$$\begin{aligned} &= s^6(b^3 - 2b^2 + b + 3 - A_1^2\tilde{x}^2 - 2A_0A_1\tilde{x} - A_0^2 - bA_1\tilde{x} - bA_0) \\ &\quad + s^4(3\tilde{x}b^2 - 4\tilde{x}b + \tilde{x} - A_1\tilde{x}^2 - A_0\tilde{x}) \\ &\quad + s^2(3\tilde{x}^2 b - 2\tilde{x}^2) + \tilde{x}^3 \end{aligned}$$

Nun sortiert man auf der rechten Seite nach Potenzen von $\tilde{x}$:

$$\begin{aligned} \tilde{y}^2 + \tilde{y}s\left[(2s^2A_1 + 1)\tilde{x} + s^2(b + 2A_0)\right] &= \\ &= \tilde{x}^3 - s^2(s^4A_1^2 + s^2A_1 - 3b + 2)\tilde{x}^2 \\ &\quad - s^4(2s^2A_0A_1 + s^2bA_1 - 3b^2 + 4b - 1 + A_0)\tilde{x} \\ &\quad + s^6(b^3 - 2b^2 + b - bA_0 + 3 - A_0^2) \end{aligned}$$

Da die Koeffizienten des $\tilde{x}\tilde{y}$-Terms und des $\tilde{y}$-Terms gleich 0 sein sollen, setzt man

$$\begin{aligned} 2s^2A_1 + 1 &= 0 \\ 2A_0 + b &= 0 \end{aligned}$$

und erhält $b = -2A_0$ und $A_1 = \frac{-1}{2s^2}$. Da auch der Koeffizient des $\tilde{x}^2$-Terms gleich 0 sein soll, setzt man diese beiden Werte nun den Koeffizienten ein:

$$s^4 A_1^2 + s^2 A_1 - 3b + 2 = \frac{7}{4} + 6A_0$$

und erhält somit $A_0 = \frac{-7}{24}$ und $b = \frac{14}{24}$. Dies setzt man nun in die Kurvengleichung ein und erhält:

$$\begin{aligned} \tilde{y}^2 &= \tilde{x}^3 \\ &\quad -(\frac{7}{24} - \frac{14}{48} - \frac{588}{576} + \frac{56}{24} - 1 - \frac{7}{24})s^4\tilde{x} \\ &\quad +(\frac{2744}{13824} - \frac{392}{576} + \frac{14}{24} + \frac{98}{576} + 3 - \frac{49}{576})s^6 \\ &= \tilde{x}^3 - \frac{1}{48}s^4\tilde{x} + \frac{2753}{864}s^6 \end{aligned}$$

Da $48 = 2^4 \cdot 3$ und $864 = 2^5 \cdot 3^3$ gilt, schließt diese Umformung bereits $p \in \{2, 3\}$ aus. Nun kann man sich ein geeignetes s der Form $2^{e_1} \cdot 3^{e_2}$ wählen.
Sei $s = \sqrt{12}$. Dann ist die Weierstrassform der Kurve gegeben durch

$$\tilde{y}^2 = \tilde{x}^3 - 3\tilde{x} + 5506$$

und die Kurve ist für

$$4 \cdot 3^3 - 27 \cdot 5506^2 = (-1) \cdot 2^9 \cdot 3^7 \cdot 17 \cdot 43 \not\equiv 0 \bmod p$$

eine elliptische Kurve. Damit ist die Kurve für $p \in \{2, 3, 17, 43\}$ singulär. Alternativ sei $s = 6$. Dann ist die Weierstrassform der Kurve gegeben durch

$$\tilde{y}^2 = \tilde{x}^3 - 27\tilde{x} + 148662$$

und die Kurve ist für

$$4 \cdot 27^3 - 27 \cdot 148662^2 = (-1) \cdot 2^9 \cdot 3^{13} \cdot 17 \cdot 43 \not\equiv 0 \bmod p$$

eine elliptische Kurve. Damit ist sie (wie erwartet) für die selben $p \in \{2, 3, 17, 43\}$ singulär.

2. Wie man für die letzte Lösung bereits gesehen hat, sind zwei mögliche Weierstrassformen der Kurve gegeben durch

$$\underline{\tilde{y}^2 = \tilde{x}^3 - 3\tilde{x} + 5506}$$

und

$$\underline{\tilde{y}^2 = \tilde{x}^3 - 27\tilde{x} + 148662}$$

□