Übungen zur Vorlesung
Elliptische Kurven und Kryptographie
keine Abgabe, nur zur Besprechung

29.06.2015

PD Dr. K. Halupczok
Dipl.–Math. A. Juhas

SoSe 2015

Aufgabe 1:

(a) Bestimmen Sie die Hasse–Intervalle für $N_{73} = \#E(\mathbb{F}_{73})$ und $N_{101} = \#E(\mathbb{F}_{101})$.
(b) Wir betrachten die elliptische Kurve $E_1 : y^2 = x^3 - 2x + 2$ über $\mathbb{F}_{73}$. Der Punkt $(-36, 24)$ hat Ordnung 23. Bestimmen Sie N_{73} und die mögliche Gruppenstruktur von E_1.
(c) Wir betrachten die elliptische Kurve $E_2 : y^2 = x^3 - 33x - 22$ über $\mathbb{F}_{101}$. Der Punkt $(36, -20)$ hat Ordnung 11 und der Punkt $(32, -28)$ hat Ordnung 9. Bestimmen Sie N_{101} und die mögliche Gruppenstruktur von E_2.

Aufgabe 2:

(a) Wir betrachten die Lösungsmenge $E \subset \mathbb{F}_p^2$ der Gleichung $y^2 = x^3 + x + 9$. Für welche $p \in \{2, 3, 5, 7, 19\}$ ist E eine elliptische Kurve?
(b) Seien E_1, E_2 elliptische Kurven über $\mathbb{F}_p$, $p > 2$, mit affinen Gleichungen $E_1 : y^2 = x^3 + ax + b$, $E_2 : y^2 = x^3 + ax - b$. Zeigen Sie: Gilt $p \equiv 3 \bmod 4$, folgt $\#E_1(\mathbb{F}_p) + \#E_2(\mathbb{F}_p) = 2p + 2$.
(c) Sei $p \equiv 3 \bmod 4$ prim und $E(\mathbb{F}_p)$ elliptische Kurve mit affiner Gleichung $Y^2 = X^3 + aX$. Zeigen Sie: Für jede ganze Zahl $0 < x < \frac{p}{2}$ ist entweder x oder $p - x$ die X–Koordinate eines Punktes von $E(\mathbb{F}_p)$.

Aufgabe 3:

(a) Berechnen Sie $3^{1000003} \bmod 101$ sowie $81^{27} \bmod 100$.
(b) Ermitteln Sie eine Zahl, die bei Division durch $3, 4, 5$ und 6 den Rest $2, 3, 4$ bzw. 5 lässt.
(c) Seien $a, b \in \mathbb{Z}, p \in \mathbb{P}$. Zeigen Sie: Aus $a^p \equiv b^p \bmod p$ folgt $a \equiv b \bmod p$ sowie $a^p \equiv b^p \bmod p^2$.
(d) Berechnen Sie $\mathrm{ggT}(11760, 8932)$ und stellen Sie den ggT als Linearkombination der beiden Zahlen dar.

Aufgabe 4:

Wir betrachten die Gruppe $(\mathbb{Z}_n, +)$, $n \in \mathbb{N}$.

(a) Sei $g \in \mathbb{Z}_n$. Definieren Sie die Abbildung $\exp_g$ über $\mathbb{Z}_n$.
(b) Sei $n = 42$ und $g = 5$. Bestimmen Sie $\mathrm{ord}(g)$ sowie $\log_5(1)$.
(c) Sei $g \in \mathbb{Z}_n^*$. Wie lässt sich $\log_g(y)$ berechnen? Wäre $\mathbb{Z}_n$ in diesem Fall eine gute Wahl für einen Diffie–Hellmann Schlüsselaustausch?

Aufgabe 5:

Beschreiben Sie (in jeweils 1–2 Sätzen) das Diffie–Hellmann–Schlüsselaustauschverfahren:

(a) Was ist der öffentliche Schlüssel?
(b) Was ist Alices geheimer Schlüssel und welchen Wert schickt sie an Bob?
(c) Was ist Bobs geheimer Schlüssel und welchen Wert schickt er an Alice?
(d) Was ist der gemeinsame Schlüssel? Warum ist das Verfahren sicher?

Aufgabe 6:

Sei k ein algebraisch abgeschlossener Körper mit $\mathrm{char}\, k \neq 2, 3$ und $k_0 \subset k$ ein Teilkörper. Zeigen Sie:

(a) Sei $f \in k_0[x]$ ein Polynom dritten Grades. Hat f eine mehrfache Nullstelle x_0 in k, so liegt x_0 schon in k_0.
(b) Sei $\mathcal{C}$ eine projektive Kurve mit affiner Gleichung $y^2 = x^3 + ax + b$, $a, b \in k_0$. Hat $\mathcal{C}$ einen singulären Punkt P in $\mathbb{P}^2(k)$, so liegt P schon in $\mathbb{P}(k_0)$.