Kryptographie Letztes Blatt 13

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 29.1.2024, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Zur Punkteanzahl elliptischer Kurven über $\mathbb{F}_p$

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:

(a) Gilt $p \equiv 3 \bmod 4$, folgt $\#E_1(\mathbb{F}_p) + \#E_2(\mathbb{F}_p) = 2p + 2$.

(b) Sei $p \equiv 3 \bmod 4$ und $E(\mathbb{F}_p)$ elliptische Kurve mit affiner Gleichung $y^2 = x^3 + ax$. Für jede ganze Zahl $0 < x < p/2$ ist entweder x oder $p - x$ die x-Koordinate eines Punktes von $E(\mathbb{F}_p)$.

Aufgabe 2: Mögliche Gruppenstruktur einer elliptischen Kurve ermitteln

Bestimmen Sie das Hasse-Intervall für $\#E(\mathbb{F}_{73})$.

Wir betrachten die elliptische Kurve $E : y^2 = x^3 - 2x + 2$ über $\mathbb{F}_{73}$. Der Punkt $(-36, 24)$ hat Ordnung 23. Bestimmen Sie $\#E(\mathbb{F}_{73})$ und die mögliche Gruppenstruktur von E.

Aufgabe 3: Kryptographisch sichere elliptische Kurven

Über die Webseite `http://safecurves.cr.yp.to/`
mit den Titel "SafeCurves: choosing safe curves for elliptic-curve cryptography"
können Informationen zur Sicherheit bestimmter elliptischer Kurven abgerufen werden.
Wählen Sie eine bestimmte davon aus und geben Sie ihre zugehörige Kurvengleichung an.
Inwiefern schätzen Sie diese Kurve als kryptographisch sicher ein (im Sinne der Vorlesung)?