RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

**Präsenzübungen zur Vorlesung**

# Kryptanalyse

**WS 2012/2013**

Blatt 8 / 4. Dezember 2011

**AUFGABE 1:**
Sei $g$ ein Generator der multiplikativen Gruppe $\mathbb{Z}_q^*$. Sei $a \in \mathbb{Z}_q^*$. Schreibe $a = g^i$ für ein eindeutig bestimmtes $i \in \{1, \ldots, q-1\}$. Zeigen Sie,

$$\mathrm{ord}_{\mathbb{Z}_q^*}(a) = \frac{q-1}{\mathrm{ggT}(i, q-1)} \ .$$

**AUFGABE 2:**
Sei $f(x) = x^3 + ax + b \in \mathbb{Z}_p[x]$ für $p > 3$ prim. Zeigen Sie, dass die Bedingung $4a^3 + 27b^2 \neq 0 \bmod p$ äquivalent zu der Forderung ist, dass $f(x)$ keine mehrfachen Nullstellen besitzt.

Bemerkung: Im Allgemeinen hat ein Polynom vom Grad 3 keine 3 Nullstellen in $\mathbb{Z}_p$, sondern die 3 Nullstellen liegen ggf. in einem Erweiterungskörper. Es gilt allerdings, dass, falls $f(x)$ mehrfache Nullstellen besitzt und $p > 3$, alle Nullstellen automatisch in $\mathbb{Z}_p$ liegen müssen. Ihr Beweis wird diese Zusatzaussage unter Umständen mitliefern.

**AUFGABE 3:**
Sei $p > 3$ prim. Beweisen Sie: Die Anzahl der Paare $a, b$, für die die Weierstrass-Gleichung $y^2 = x^3 + ax + b$ eine elliptischen Kurven $E$ über $\mathbb{Z}_p$ definiert beträgt genau $p^2 - p$.

**AUFGABE 4:**
Seien $p, q > 3$ verschiedene Primzahlen, $N = pq$ und $a, b \in \mathbb{Z}_N$ mit $\mathrm{ggT}(4a^3 + 27b^2, N) = 1$. Seien $E_p, E_q, E_N$ elliptische Kurven über $\mathbb{Z}_p, \mathbb{Z}_q, \mathbb{Z}_N$, definiert durch die Gleichung $y^2 = x^3 + ax + b$ (modulo $p$,$q$, bzw. $N$).
Wir definieren $f : E_N \to E_p \times E_q$ durch

$$f(x, y) = ((x \bmod p, y \bmod p), (x \bmod q, y \bmod q)) \qquad \text{(chin. RS)} \tag{1}$$
$$f(\mathcal{O}) = (\mathcal{O}, \mathcal{O}) \tag{2}$$

Zeigen Sie: $f$ ist wohldefiniert und injektiv, aber nicht surjektiv und es gilt $f(P + Q) = f(P) + f(Q)$, wann immer definiert, wobei $+$ die Addition der elliptischen Kurven bezeichnet.