RUHR UNIVERSITÄT BOCHUM
RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 8 / 7. Dezember 2011

AUFGABE 1:
Sei g ein Generator von $\mathbb{Z}_q^*$ und $a \bmod q = g^i$ für ein $i \in [1, \dots, q-1]$. Zeigen Sie,

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

AUFGABE 2:
Sei $f(x) = x^3 + ax + b \in \mathbb{Z}_p[x]$. 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.

AUFGABE 3:
Beweisen Sie: Die Anzahl aller elliptischen Kurven E modulo p beträgt $p^2 - p$.

AUFGABE 4:
Sei $E : y^2 = x^3 + 1$ eine Kurve über $\mathbb{Z}_{12}$. Zeigen Sie, dass E nicht abgeschlossen bzgl. der Addition ist. Bestimmen Sie dazu zunächst alle Punkte auf der Kurve. Können Sie mittels der ECM-Methode faktorisieren?