Kryptographie *WS 2012/13*
Barbara Baumeister

13. Übungsblatt

Abgabe: Donnerstag, 24.1.2013

Aufgabe 1 Faktorisieren Sie $n = 138277151$ mit der $p-1$-Methode von Pollard.

Aufgabe 2 Faktorisieren Sie mit der elliptischen Kurven-Methode von Lenstra $n = 2773$.
Hinweis: Wählen Sie $P = (1, 3)$ und $a = 4$.

Aufgabe 3 Finden Sie mit dem quadratischen Sieb einen echten Teiler von $n = 2773$.

Aufgabe 4
(a) Bestimmen Sie eine elliptische Kurve über $K = \mathbb{F}_5$, die kleinste Ordung hat und eine weitere, die größte Ordnung hat.
(b) Bestimmen Sie die Gruppenstrukturen dieser Kurven. (Diese ist unabhängig von der speziellen Wahl).

Zusatzaufgabe Sei p eine Primzahl, die kongruent 1 modulo 4 ist. Weiter sei a ein Quadrat in $\mathbb{Z}_p$ und u eine Zahl, die kein Quadrat in $\mathbb{Z}_p$ ist (z.B. falls $p \equiv 5 \bmod 8$, dann können wir $u = 2$ wählen). Zeigen Sie, wie wir mit Hilfe von a und u die Wurzel von a bestimmen können.
Hinweis: Betrachten Sie die Zerlegung $p - 1 = 2^s t$, wobei t ungerade ist.