RUHR UNIVERSITÄT BOCHUM

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

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 13 / 8.–10. Juli 2013

AUFGABE 1:
Faktorisieren sie $n = 77$ mittels William's $p + 1$ - Methode, wobei Sie D als quadratischen Nicht-Rest wählen. Nehmen Sie an, dass n einen Primteiler $p \leq 15$ besitzt, für den $p + 1$ 2-glatt ist.

AUFGABE 2:
Lösen Sie die quadratische Gleichung $x^2 - 4x + 2 \equiv 0 \mod 49$.

Bemerkung: Um Lösungen modulo 7 nach Lösungen modulo 49 fortzusetzen, können Sie Hensels Lemma benutzen. Wenn Sie dies noch nicht kennen, setzen Sie $x = x_0 + 7 \cdot x_1$ in die Gleichung ein, wobei x_0 eine Lösung modulo 7 ist.

AUFGABE 3:
Sei $p > 2$ prim und $x = (x_k) \in \mathbb{Z}_p$ ganze p-adische Zahl. Zeigen Sie, dass x eine Potenzreihendarstellung der Form $x = \sum_{i=0}^{\infty} c_i p^i$ mit $-\frac{p-1}{2} < c_i < \frac{p-1}{2}$ besitzt.

Bemerkung: $x = \sum_{i=0}^{\infty} c_i p^i$ bedeutet, dass $x \equiv \sum_{i=0}^{k-1} c_i p^i \mod p^k$ für alle $k \geq 0$ gilt.

AUFGABE 4:
Berechnen Sie $2^{-1} \mod 3^4$ mittels Hensels Lemma. Es kann hilfreich sein, dies als Potenzreihe wie in Aufgabe 3 oben zu entwickeln.
Ist 2 in $\mathbb{Z}_3$ invertierbar? Was ist ggf. die Inverse (geschrieben als Potenzreihe).

Bemerkung: Erinnern Sie sich an die geometrische Reihe.