RUHR UNIVERSITÄT BOCHUM

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

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 13 / 5. Juli 2013 / Abgabe bis spätestens 15. Juli 2013, 12:00 Uhr in dem Kasten auf NA 02 oder am Anfang der Vorlesung

Geben Sie bitte die Aufgaben zur Vereinfachung der Korrektur folgendermassen nach Aufgaben getrennt ab:

- Aufgaben 1,2 in Kasten A
- Aufgaben 3,4 in Kasten B
- Aufgabe 5 in Kasten C

Die Kästen auf NA 02 sind entsprechend beschriftet. Wenn Sie in der Vorlesung abgeben, machen sie einfach 3 getrennte Stapel. Schreiben Sie auf alle 3 Abgaben jeweils Ihre(n) Namen und/oder Matrikelnummer(n).
Bitte schreiben Sie auf Ihre Abgaben eine Sollrückgabestelle (Übungsgruppe, Zentralübung, persönlich in NA5/74).

AUFGABE 1 (4 Punkte)**:**
Sei $p > 2$ Primzahl und $a \in \mathbb{F}_p^*$ mit $\left(\frac{a}{p}\right) = +1$. Zeigen Sie, dass es *genau* $\frac{1}{2}(p-1)$ Elemente $b \in \mathbb{F}_p$ gibt, für die $\left(\frac{b^2-a}{p}\right) = -1$ gilt.

AUFGABE 2 (4 Punkte)**:**
Zeigen Sie, dass William's $p+1$ - Methode korrekt ist, falls $\left(\frac{D}{p}\right) = -1$.

Hinweis(e):
Machen Sie geeignete Annahmen ähnlich wie bei Pollard's $p-1$-Methode. Nehmen Sie vereinfachend an, dass die zu faktorisierende Zahl n von der Form $n = pq$, mit $p \neq q$ ungerade Primzahlen ist. $p+1$ soll dabei b-glatt sein und für den anderen Primteiler q von n sollen weder $q-1$ noch $q+1$ b-blatt sein.
Beachten Sie, dass der Algorithmus im Ring $R = \mathbb{Z}/(n)[X]/(X^2-D)$ rechnet und zerlegen Sie R sowie die Norm-Abbildung $N : R \to \mathbb{Z}/(n)$ mit dem chinesichen Restsatz (bzgl. $n = pq$).
Sie werden eine Fallunterscheidung benötigen, je nachdem was $\left(\frac{D}{q}\right)$ ist. Versuchen Sie sich zunächst/nur an dem (einfacheren) Fall $\left(\frac{D}{q}\right) = -1$.
Beachten Sie ausserdem, dass für den Primteiler q von n gilt, dass $\mathbb{Z}/(q)[X]/(X^2-D) \cong \mathbb{F}_{q^2}$ ist, wenn D kein Quadrat modulo q ist.

Wenn D hingegen ein Quadrat modulo q ist, etwa $D = \gamma^2 \bmod q$, so gilt $\phi_q : \mathbb{Z}/(q)[X]/(X^2 - D) \cong \mathbb{F}_q \times \mathbb{F}_q$, wobei der Isomorphismus ϕ_q gegeben ist durch $\phi_q(f) = (f(\gamma), f(-\gamma))$ (d.h. man wertet das Polynom $f \in \mathbb{Z}/(q)[X]/(X^2 - D)$ an $\pm\gamma$ aus). Weiterhin gilt in diesem Fall für $\omega \in \mathbb{Z}/(n)[X]/(X^2 - D)$, dass $N(\omega) \equiv \omega(\gamma)\omega(-\gamma) \mod q$.

AUFGABE 3 (4 Punkte)**:**
Sei p prim. Sei $(x_k) \in \mathbb{Z}_p$ ganze p-adische Zahl mit Potenzreihendarstellung $\sum_{k=0}^{\infty} c_k p^k$ mit $0 \leq c_i < p$. Zeigen Sie, dass die folgenden beiden Aussagen äquivalent sind:

(a) Es gibt ein $x \in \mathbb{Z}$ mit $\epsilon_p(x) = (x_k)$, wobei $\epsilon_p : \mathbb{Z} \to \mathbb{Z}_p$ die Einbettung von $\mathbb{Z}$ in $\mathbb{Z}_p$ mit $\epsilon_p(x) = (x, x, x, x, x, \ldots)$ wie in der Vorlesung ist.

(b) Es gibt ein k_0, so dass für alle $k > k_0$ gilt: $c_k = 0$ oder für alle $k > k_0$ gilt $c_k = p - 1$.

AUFGABE 4 (5 Punkte)**:**
Bestimmen Sie die Lösungsmenge der Gleichung $20x^2 - 9x + 4 \equiv 0 \mod 45$ mittels Chinesischem Restsatz und Hensel-Lifting.

AUFGABE 5 (7 Punkte)**:**
Berechnen Sie alle Lösungen der Gleichung $(x-1)^2(x-2)^2 + 5(x-1) + 25 \equiv 0 \mod 5^i$ für $i = 1, 2, 3$, indem Sie für $i = 2, 3$ Hensel's Lemma verwenden.