RUHR UNIVERSITÄT BOCHUM

RUB

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

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 7 / 10. Mai 2013 / Abgabe bis spätestens 03. Juni 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:

- Aufgabe 1 in Kasten A
- Aufgabe 2 in Kasten B
- Aufgaben 3,4 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).

Beachten Sie, dass die Blätter 6 und 7 zeitgleich online gestellt wurden. Dieses Blatt ist nicht das Blatt, das über die Pfingstwoche zu bearbeiten ist!

AUFGABE 1 (7 Punkte)**:**

(a) Bestimmen Sie die Ordnung von $\overline{2}$ in U_{1961}

(b) Berechnen Sie die Lösungsmenge von $2^x \equiv 1950 \mod 1961$

Hinweis: $1961 = 53 \cdot 37$. Verwenden Sie einen Taschenrechner (der idealerweise Modulo-Rechnung kann). Probieren Sie bitte nicht alle Möglichkeiten durch, sondern versuchen Sie, die Rechnung so weit es geht zu verkürzen (CRT und Baby-Step-Giant-Step). Beachten Sie, dass U_{1961} nicht zyklisch ist.

AUFGABE 2 (6 Punkte)**:**
Sei $p \in \mathbb{N}$ eine ungerade Primzahl. Zeigen Sie:

(a) Wenn $p = x^2 + y^2$ Summe von 2 Quadraten mit $x, y \in \mathbb{Z}$, so ist $p \equiv 1 \mod 4$.

(b) Wenn $p \equiv 1 \mod 4$ ist, so lässt sich p als Summe $p = x^2 + y^2$ von 2 Quadraten mit $x, y \in \mathbb{Z}$ schreiben.

Hinweis zu (b): Sie können z.B. wie folgt vorgehen. Betrachten Sie $z = 1 + \zeta i \in \mathbb{Z}[i]$, wobei $\zeta^2 \equiv -1 \mod p$ mit $0 < \zeta < p$. Versuchen Sie $N(z)$ zu faktorisieren. Was folgt für die Primfaktorzerlegung von z in $\mathbb{Z}[i]$? Folgern Sie, dass $\mathrm{ggT}(z, p) = x + iy$ in $\mathbb{Z}[i]$ mit $x^2 + y^2 = p$.

— bitte wenden —

AUFGABE 3 (4 Punkte)**:**
Sei $n \in \mathbb{N}$ beliebig. Zeigen Sie, dass

$$\mathrm{QR}_n = \{a \in U_n \mid a \text{ ist quadratischer Rest}\}$$

eine Untergruppe von U_n ist.
Bemerkung: Wir fordern *nicht*, dass n prim ist. Die Definition von quadratischen Resten für nicht-prime n ist genauso wie für n prim:
$a \in U_n$ ist quadratischer Rest, wenn $a = b^2$ in $\mathbb{Z}/n\mathbb{Z}$.

AUFGABE 4 (3 Punkte)**:**
Berechnen Sie alle Lösungen von $\overline{1+X}^t = \overline{2-2X}$ in $\mathbb{F}_9 \cong \mathbb{F}_3[X]/(X^2+1)$ in der Unbekannten t.