RUHR UNIVERSITÄT BOCHUM

RUB

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

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 8 / 31. Mai 2013 / Abgabe bis spätestens 10. 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:

- Aufgaben 1,2 in Kasten A
- Aufgaben 3,5 in Kasten B
- Aufgabe 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).

AUFGABE 1 (2 Punkte)**:**
Zeigen Sie, dass 3 ein Erzeuger von U_{400277} ist.

Hinweis: 100069 und 400277 sind ist prim. Man muss in dieser Aufgabe (fast) nicht rechnen.

AUFGABE 2 (2 Punkte)**:**
Sei $p > 2$ ungerade Primzahl. Zeigen Sie, dass $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ gilt.

AUFGABE 3 (9 Punkte)**:**
Berechnen Sie die folgenden Jacobi-Symbole $\left(\frac{a}{b}\right)$. Geben Sie jeweils die Lösungsmenge der Gleichung $x^2 \equiv a \mod b$ an.

(a) $\left(\frac{101}{133}\right)$

(b) $\left(\frac{114}{133}\right)$

(c) $\left(\frac{84}{133}\right)$

(d) $\left(\frac{130}{133}\right)$

(e) $\left(\frac{31}{133}\right)$

Bemerkung: $133 = 19 \cdot 7$

– bitte wenden –

AUFGABE 4 (3 Punkte)**:**
Bestimmen Sie die Lösungsmenge folgender Gleichung:

$$3x^2 + 94x + 65 \equiv 0 \mod 253$$

Bemerkung: $253 = 11 \cdot 23$

AUFGABE 5 (4 Punkte)**:**
Sei $p > 2$ Primzahl und $\text{ggT}(a, p) = 1$ Zeigen Sie:

(a) Die Gleichung $x^2 \equiv a \mod p^2$ hat entweder keine oder genau 2 Lösungen in $\mathbb{Z}/(p^2)$

(b) Die Gleichung $x^2 \equiv a \mod p^2$ hat eine Lösung $\Leftrightarrow \left(\frac{a}{p}\right) = +1$.

Hinweise: Für (a) empfiehlt es sich, zu zeigen, dass wenn x_0, x_1 Lösungen sind, dass dann $x_0 \equiv \pm x_1 \mod p^2$ gelten muss. Argumentieren Sie direkt mit der Definition von Modulo.
Zeigen Sie in (b) zunächst die Richtung $\Longrightarrow$. Für die andere Richtung gibt es 2 Lösungsmöglichkeiten:
Sie können zum einen versuchen, eine Wurzel zu konstruieren.
Zum anderen können Sie sich überlegen, dass die Mengen $\{b \in U_{p^2} \mid x^2 \equiv b \text{ lösbar}\}$ und $\{b \in U_{p^2} \mid \left(\frac{b}{p}\right) = +1\}$ gleich viele Elemente haben. Teil (a) ist dabei hilfreich.