RUHR
UNIVERSITÄT
BOCHUM

RUB

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

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 4 / 26. April 2013 / Abgabe bis spätestens 06. Mai 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 1,2,3 Kasten A
- Aufgaben 4,5,6 in Kasten B
- (Kasten C bleibt dieses Mal leer)

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 (5 Punkte)**:**
Bestimmen Sie die Lösungsmenge folgenden Gleichungssystems über $\mathbb{Z}$:

$$\begin{aligned} 2x &\equiv 10 \mod 63 \\ 10x &\equiv 5 \mod 15 \\ 5x &\equiv 4 \mod 14 \end{aligned}$$

AUFGABE 2 (4 Punkte)**:**
Geben Sie alle Lösungen (aus $\mathbb{Z}/93\mathbb{Z}$) der Gleichung

$$x^2 = \overline{31} \qquad \text{in } \mathbb{Z}/93\mathbb{Z}$$

an. Begründen Sie dabei, warum die von Ihnen gefundenen Lösungen alle Lösungen sind.

— bitte wenden —

AUFGABE 3 (3 Punkte)**:**
Seien $n_1, n_2, \ldots, n_k > 0$ paarweise teilerfremd. Setze $N := n_1 n_2 \cdots n_k$ und $M_i := \frac{N}{n_i}$.
Seien x_i, y_i so, dass $1 = x_i M_i + y_i n_i$.
Zeigen Sie, dass $x \in \mathbb{Z}$ das Gleichungssystem

$$\begin{aligned} x &\equiv c_1 \mod n_1 \\ x &\equiv c_2 \mod n_2 \\ &\ldots \\ x &\equiv c_k \mod n_k \end{aligned}$$

genau dann löst, wenn $x \equiv c_1(x_1 M_1) + c_2(x_2 M_2) + \ldots + c_k(x_k M_k) \mod N$

AUFGABE 4 (2 Punkte)**:**
Geben Sie $m, a_1, \ldots, a_m, c_1, \ldots, c_m, n_1, \ldots, n_m$ mit folgenden Eigenschaften an:

- $m > 0, n_i > 0$ für alle i.
- $\mathrm{ggT}(a_i, n_i) = 1$ für alle i
- $\mathrm{ggT}(n_1, \ldots, n_m) = 1$
- Das Gleichungssystem

$$\begin{aligned} a_1 \cdot x &= c_1 \mod n_1 \\ a_2 \cdot x &= c_2 \mod n_2 \\ &\ldots \\ a_m \cdot x &= c_m \mod n_m \end{aligned}$$

  hat für diese $m, a_1, \ldots, a_m, c_1, \ldots, c_m, n_1, \ldots, n_m$ *keine* Lösung in $\mathbb{Z}$.

AUFGABE 5 (2 Punkte)**:**
Sei $n \in \mathbb{Z}, n > 0$ und $\overline{a}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$, und $d = \mathrm{ggT}(a, n) > 0$, wobei $d \mid c$. Zeigen Sie, dass die Gleichung

$$\overline{a}x = \overline{c}$$

genau d Lösungen für $x \in \mathbb{Z}/n\mathbb{Z}$ hat.

AUFGABE 6 (4 Punkte)**:**
Sei $n = p^2 \cdot q$, wobei $p \neq q \in \mathbb{Z}$ ungerade Primzahlen gleicher Bitlänge
(d.h. $\lfloor \log_2(p) \rfloor + 1 = \lfloor \log_2(q) \rfloor + 1$).
Zeigen Sie: $\mathrm{ggT}(n, \phi(n)) = p$, wobei ϕ die Eulersche ϕ-Funktion ist.