Mathematisches Institut
Abt. für Reine Mathematik
Dr. K. Halupczok

01.06.2006

Übungen zur Vorlesung

Elementare Zahlentheorie

SoSe 2006

Blatt 5

Abgabe: Bitte die Lösungen bis spätestens Freitag, den 16.06.2006, 11 Uhr, ins Postfach von K. Halupczok im 3. Stock der Eckerstr. 1 legen.

Aufgabe 1.

Sei $N = a_m 10^m + \cdots + a_2 10^2 + a_1 10 + a_0$ mit $0 \le a_k \le 9$ die Dezimaldarstellung einer Zahl $N \in \mathbb{N}$.

(a) Zeige, daß die Zahlen 7, 11 *und* 13 die Zahl N genau dann teilen, wenn sie allesamt die Zahl

$$M := (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - \dots$$

teilen. [Hinweis: Betrachte den Modul 1001.]

(b) Zeige, daß 6 die Zahl N genau dann teilt, wenn sie die Zahl $M := a_0 + 4a_1 + 4a_2 + \cdots + 4a_m$ teilt.

(c) Stelle fest, ob die Zahl 1.010.908.899 durch 7, 11 und 13 teilbar ist, ohne die Divisionen durchzuführen.

Aufgabe 2.

Zeige, daß für jede ungerade Primzahl p die Kongruenz

$$1^n + 2^n + 3^n + \cdots + (p-1)^n \equiv \begin{cases} 0\ (p) & \text{für } (p-1) \nmid n \\ -1\ (p) & \text{für } (p-1) \mid n \end{cases}$$

erfüllt ist. [Hinweis: Betrachte eine Primitivwurzel r mod p.]

Aufgabe 3.

Sei $m \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$, $(a, m) = 1$, und $\{x_1, \dots, x_m\}$ sei ein vollständiges Restsystem mod m. Für $\alpha \in \mathbb{R}$ bezeichnet $\{\alpha\} := \alpha - [\alpha]$ den „gebrochenen Teil von α“. Zeige:

$$\text{(a)} \quad \sum_{j=1}^{m} \left\{ \frac{ax_j + b}{m} \right\} = \frac{1}{2}(m-1),$$

$$\text{(b)} \quad \sum_{j=1}^{m} \exp\left(2\pi i \frac{cx_j}{m}\right) = \begin{cases} m, & \text{falls } m \mid c, \\ 0, & \text{sonst.} \end{cases}$$

Aufgabe 4. Zum RSA-Verfahren

Die Buchstaben des Alphabets A bis Z werden mit den Zahlen 0 bis 25 identifiziert, das Leerzeichen mit der Zahl 26. Klartexte werden zu Blöcken aus je drei Zahlen von 0 bis 26 zusammengefaßt, also z. B. „KLARTEXT_“= $10, 11, 0/17, 19, 4/23, 19, 26$. Jedem Block k_1, k_2, k_3 wird die Zahl $k = k_1 \cdot 27^2 + k_2 \cdot 27 + k_3$ zugeordnet, die beim RSA-Verfahren gemäß $k \mapsto v(k) = k^t \ (N)$ verschlüsselt wird. Die Zahl $v(k)$ wird durch $v(k) = v_1 \cdot 29^2 + v_2 \cdot 29 + v_3$ mit einen Geheimtextblock aus drei Zeichen $v_1, v_2, v_3 \in \{0, \ldots, 28\}$ beschrieben, die auch die zusätzlichen Zeichen „.“= 27 und „,“= 28 sein können.

(a) Sei $N = 22499$, $t = 1291$. Verschlüssle damit die Klartextnachricht „ZAHLEN“.

(b) Knack den Code: Faktorisiere N und berechne den Schlüssel s, für den $st \equiv 1 \ (\varphi(N))$ gilt. Entschlüssle damit den Geheimtext „JI.FTJ“.

(c) Warum ist $N = 22499$ – abgesehen davon, daß N sehr klein gewählt ist – eine besonders schlechte Wahl für N? Welche N sind generell eher ungeeignet?

(d) (freiwillig) Hier kann $(k, N) > 1$ sein. Warum arbeitet das angegebene RSA-Verfahren trotzdem korrekt?