

Abgabetermin: Freitag, 18.06.2004, vor Beginn der Vorlesung

25. (a) *Leiten Sie* die Darstellung von 114 bezüglich der Basis 4 (4-adische Darstellung von 114) her, d.h. bestimmen Sie $\alpha_i \in \{0, 1, 2, 3\}$ mit

$$114 = \sum_{i \in \mathbb{N}_0} \alpha_i 4^i.$$

Folgen Sie hierzu dem Beweis von Satz 2.1.10 der Vorlesung.

- (b) Die Übertragung einer ISBN wird so gestört, daß exakt zwei aufeinanderfolgende gleiche Ziffern aa zu bb verändert werden (Zwillingsfehler). Kann der Empfänger aufgrund der erhaltenen Ziffernfolge erkennen, daß es sich nicht um eine ISBN handelt?
 (c) Zeigen Sie, daß für $x \in \mathbb{Z}$ stets

$$x^2 \equiv 0 \pmod{4} \quad \text{oder} \quad x^2 \equiv 1 \pmod{4}$$

gilt. Warum ist 17654326203 nicht Summe von 2 Quadratzahlen?

26. (a) Sei p eine Primzahl und $a \in \mathbb{Z}$. Zeigen Sie $a^p \equiv a \pmod{p}$.
 (b) Sei f ein Polynom mit Koeffizienten in \mathbb{Z} . Sei p prim. Zeigen Sie für $x \in \mathbb{Z}$:

$$(f(x))^p \equiv f(x^p) \pmod{p}.$$

Ist die Voraussetzung “ p prim” entbehrlich?

27. (a) Seien $a, b \in \mathbb{Z}$ und $m_1, m_2 \in \mathbb{N}$. Weisen Sie nach, daß das System von Kongruenzen

$$x \equiv a \pmod{m_1} \quad \text{und} \quad x \equiv b \pmod{m_2}$$

genau dann eine Lösung $x \in \mathbb{Z}$ besitzt, wenn $(m_1, m_2) \mid (b - a)$ gilt.

- (b) Aus einem alten Rechenbuch: 17 Räuber stehlen einen Sack mit Goldstücken. Beim Versuch, die Beute gerecht aufzuteilen, bleiben drei Goldstücke übrig. Es kommt zum Streit. Ein Räuber wird erschlagen. Beim Versuch, unter den verbleibenden 16 die Beute gerecht aufzuteilen, bleiben 10 Goldstücke übrig. Wieder wird ein Räuber im Streit erschlagen. Nun geht die Teilung der Beute auf. Bestimmen Sie die kleinste Anzahl von Goldstücken, auf die die Geschichte zutrifft.

28. (a) Kodieren Sie wie in der Vorlesung (für den Text “IM”) beschrieben den Text

GEHEIM

mit dem RSA-Verfahren, wobei $n = 2773$ und $k = 17$ gewählt wird. Ersetzen Sie dazu zunächst jeden Buchstaben gemäß A=01, B=02, ..., Z=26 durch zwei Ziffern und kodieren Sie dann je vier aufeinander folgende Ziffern mit dem RSA-Verfahren.

- (b) Beim RSA-Verfahren (Notation wie in der Vorlesung) sind n, k publik. Falls eine der beiden Primzahlen p, q mit $n = pq$ ermittelt werden kann, dann können sofort auch $\varphi(n)$ und ℓ berechnet werden. Erklären Sie dies. Umgekehrt erhält man aus der Kenntnis von n und $\varphi(n)$ leicht die Primfaktorzerlegung von n .