Universität Tübingen
Mathematisches Institut Tübingen, den 18.12.2007

Übungen zur Elementaren Zahlentheorie (10)

(37) Sei p eine ungerade Primzahl und seien a, b ganze Zahlen. Man gebe notwendige und hinreichende Bedingungen dafür an, dass die Kongruenz $X^2 + aX + b \equiv 0 \pmod{p}$ in $\mathbb{Z}$ lösbar ist.

(38) Sei X^2+aX+b ein ganzzahliges Polynom. Man beschreibe, wann die Reduktion von f modulo 2 folgende Eigenschaften hat:
(a) $f \bmod 2 = X^2$ oder $(X+1)^2$.
(b) $f \bmod 2 = X(X+1)$.
(c) $f \bmod 2$ ist irreduzibel in $\mathbb{F}_2[X]$.

(39) Die Aufgabe von Sun-Tse (50 v. Chr.): "Es soll eine Anzahl von Dingen gezählt werden. Zählt man sie zu je dreien, dann bleiben zwei übrig. Zählt man sie zu je fünf, so bleiben drei übrig. Zählt man sie zu je sieben, so bleiben zwei übrig. Wie viele sind es (mindestens) ?"

(40) Seien $m_1, \cdots, m_r$ paarweise teilerfremde natürliche Zahlen, $m = m_1 \cdots m_r$ und $m_i' = \frac{m}{m_i}$, und seien $x_1, \cdots, x_r$ irgendwelche ganzen Zahlen ($r \in \mathbb{N}_{\geq 2}$). Seien $m_i'' \in \mathbb{Z}$ mit $m_i'' m_i' \equiv 1 \pmod{m_i}$ für jedes i, und sei

$$x = x_1(m_i'' m_i') + \cdots + x_r(m_r'' m_r').$$

Man zeige, dass $x \equiv x_i \pmod{m_i}$ gilt für alle $i = 1, \cdots, r$ *simultan*, und dass dadurch die Restklasse von $x \bmod m$ eindeutig bestimmt ist. Die Zuordnung $x \mapsto (x_1 + m_1\mathbb{Z}, \cdots, x_r + m_r\mathbb{Z})$ ist also ein Ringepimorphismus von $\mathbb{Z}$ auf das direkte Produkt $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ mit Kern $m\mathbb{Z}$.
Zusatz: Warum folgt $\varphi(m) = \varphi(m_1) \cdots \varphi(m_r)$?