Universität Tübingen
Mathematisches Institut Tübingen, den 18.11.2007

Übungen zur Elementaren Zahlentheorie (6)

(21) Man gebe die kleinste natürliche Zahl an, deren Restklasse modulo 31 die multiplikative Gruppe von $\mathbb{F}_{31} = \mathbb{Z}/31\mathbb{Z}$ erzeugt.

(22) Für jede ungerade Primzahl p gilt

$$[(\frac{p-1}{2})!]^2 \equiv (-1)^{(p-1)/2} \,(\mathrm{mod}\, p).$$

Für $p \equiv 1 \,(\mathrm{mod}\, 4)$ ist also $x = (\frac{p-1}{2})!$ eine Quadratwurzel von -1 mod p.

(23) Mit Hilfe des Schubfachprinzips ("shoe box principle") zeige man, dass für jede ungerade Primzahl p die Kongruenz $X^2 + Y^2 \equiv -1 \,(\mathrm{mod}\, p)$ in $\mathbb{Z}^{(2)}$ lösbar ist.

(24) Sei K ein endlicher Körper der Ordnung q. Sei $r \in \mathbb{N}$.
Man zeige:
(a) $\sum_{x \in K} x^r = -1$, falls $r \geq 1$ durch $q-1$ teilbar ist.
(b) $\sum_{x \in K} x^r = 0$ in jedem anderen Fall.