Universität Tübingen
Mathematisches Institut Tübingen, den 4.12.2007

Übungen zur Elementaren Zahlentheorie (8)

(29) Für ungerade Primzahlen p gilt:
(a) $(\frac{3}{p}) = 1 \iff p \equiv \pm 1 \,(\mathrm{mod}\, 12)$
(b) $(\frac{-3}{p}) = 1 \iff p \equiv 1, 7 \,(\mathrm{mod}\, 12)$
(c) $(\frac{5}{p}) = 1 \iff p \equiv \pm 1, \pm 11 \,(\mathrm{mod}\, 20)$
(d) $(\frac{6}{p}) = 1 \iff p \equiv \pm 1, \pm 5 \,(\mathrm{mod}\, 24)$.

(30) Sei $b \in \mathbb{N}_{\geq 3}$ ungerade mit Primfaktorzerlegung $b = p_1 \cdots p_r$. Für zu b teilerfremde ganze Zahlen a definiere das *Jacobi-Symbol* durch $(\frac{a}{b}) = \prod_{i=1}^{r} (\frac{a}{p_i})$. Man zeige, dass dies nur von der Restklasse von $a \,\mathrm{mod}\, b$ abhängt und ein Charakter (Homomorphismus) auf den primen Restklassen mod b ist (mit Werten in $\{\pm 1\}$). Ferner zeige man:
(a) $(\frac{-1}{b}) = (-1)^{(b-1)/2}$
(b) $(\frac{2}{b}) = (-1)^{(b^2-1)/8}$.
(Auch das Quadratische Reziprozitätsgesetz gilt entsprechend.)

(31) Sei $p \neq 2, 3$ eine Primzahl.
(a) Ist die Kongruenz $X^4 \equiv -1 \,(\mathrm{mod}\, p)$ lösbar in $\mathbb{Z}$, so ist $p \equiv 1 \,(\mathrm{mod}\, 8)$.
(b) Ist $X(X+1) \equiv -1 \,(\mathrm{mod}\, p)$ lösbar in $\mathbb{Z}$, so ist $p \equiv 1 \,(\mathrm{mod}\, 6)$.
Gilt in (a) oder (b) auch die Umkehrung ? - Man präzisiere gegebenfalls die Aussagen.

(32) Sei $p \equiv 1 \,(\mathrm{mod}\, 4)$ eine Primzahl. Man zeige, dass die Darstellung von p als Summe von 2 Quadraten in $\mathbb{N}$ eindeutig ist, d.h., aus $p = a^2 + b^2 = a_0^2 + b_0^2$ mit natürlichen Zahlen a, b, a_0, b_0 folgt $\{a, b\} = \{a_0, b_0\}$.