Universität Karlsruhe (TH)
Mathematisches Institut II
Prof. Dr. H.-W. Leopoldt

Karlsruhe, 8.6.1990

Elementare Zahlentheorie — Übungsblatt 7

Aufgabe 30 (4 Punkte)
Bestimmen Sie für die folgenden Werte von m alle Lösungen der Kongruenz $x^4 - 8x + 12 \equiv 0 \pmod m$:
(a) $m = 128$,
(b) $m = 81$,
(c) $m = 125$,
(d) $m = 49$.

Aufgabe 31 (4 Punkte)
Sei A die abelsche Gruppe
(a) $A = \left(\mathbb{Z}/\mathbb{Z}p^n\right)^\times$ $(p \in \mathbb{P},\, n \in \mathbb{N})$
bzw. allgemeiner
(b) $A = \left(\mathbb{Z}/\mathbb{Z}m\right)^\times$ $(m \in \mathbb{N})$.
Bestimmen Sie die Anzahl der Quadrate (Elemente der Form $a = b^2$ mit $b \in A$) in A.
(Hinweis: Benutzen Sie die Darstellung als direktes Produkt zyklischer Gruppen.)

Aufgabe 32 (7=3+2+2 Punkte)
Eine natürliche Zahl n heißt *Carmichaelzahl* oder *Pseudo-Primzahl*, falls $n > 1$ und für jedes $a \in \mathbb{Z}$ mit $(a, n) = 1$ die Kongruenz $a^{n-1} \equiv 1 \pmod n$ gilt und n dennoch keine Primzahl ist.
Zeigen Sie:
(a) n ist genau dann eine Carmichaelzahl, wenn n die Primfaktorzerlegung $n = p_1 \cdot p_2 \cdot \ldots \cdot p_t$ mit $t \geq 2$ und paarweise verschiedenen p_i besitzt, für die $p_i - 1 \mid n - 1 \quad (i = 1, \ldots, t)$ gilt.
(b) Jede Carmichaelzahl ist ungerade und hat mindestens 3 Primfaktoren.
(c) Die kleinste Carmichaelzahl ist 561.

Aufgabe 33 (5 Punkte)
Für $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ sei

$$\left(\frac{a,b}{m}\right) = \sum_{x \in \left(\mathbb{Z}/\mathbb{Z}m\right)^\times} e^{2\pi i \cdot \frac{ax + bx^{-1}}{m}}$$

wobei x^{-1} die Inverse von x in $\left(\mathbb{Z}/\mathbb{Z}m\right)^\times$ sei.
Zeigen Sie:
(a) $\left(\frac{a,b}{m}\right)$ hängt nur von den Restklassen $a \bmod m$ und $b \bmod m$ ab.
(b) $\left(\frac{a,b}{m}\right) \in \mathbb{R}$.
(c) $\left(\frac{a,b}{m}\right) = \left(\frac{b,a}{m}\right)$.
(d) Für $h \in \left(\mathbb{Z}/\mathbb{Z}m\right)^\times$ gilt $\left(\frac{ah,b}{m}\right) = \left(\frac{a,bh}{m}\right)$.
(e) Sei $m = m_1 \cdot \ldots \cdot m_r$ mit paarweise teilerfremden $m_i \in \mathbb{N}$. Wie üblich sei $\widetilde{m_i} = \frac{m}{m_i}$. Zeigen Sie:

$$\left(\frac{a_1, 1}{m_1}\right) \cdot \ldots \cdot \left(\frac{a_r, 1}{m_r}\right) = \left(\frac{\widetilde{m_1}^2 a_1 + \ldots + \widetilde{m_r}^2 a_r, 1}{m}\right)$$

Aufgabe 34 (7 Punkte)

Bestimmen Sie alle Lösungen der Gleichung $2x^2 + 2x + 1 = 5^n$ mit $x \in \mathbb{Z}$ und $n \in \mathbb{N}_0$.

Anleitung: Sei (x, n) eine Lösung. Zeigen Sie:

(a) In $\Gamma = \mathbb{Z}[i]$ gilt $x \pm (x+1)i = u \cdot (1+2i)^n$ mit einer Einheit $u \in \Gamma^\times$.

(b) Definiert man $a_n, b_n \in \mathbb{Z}$ durch $a_n + 2b_n \cdot i = (1+2i)^n$, so gelten für $n = 2^t \cdot s$ mit ungeradem $s \in \mathbb{N}$ und $t \geq 2$ die Kongruenzen

$$a_n \equiv 1 - 2^{t+1} \cdot s \pmod{2^{t+4}} ,$$
$$2b_n \equiv 2^{t+1} \cdot 5 \cdot s \pmod{2^{t+4}} .$$

(c) Es ist $n \in \{0, 1, 2\}$.

Abgabe: Bis spätestens Freitag, 15.6.1990, 11.15 Uhr in den Kasten bei Zi. 308 des Mathematikgebäudes oder in der Vorlesung im Hörsaal Hauptbau.