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

Karlsruhe, 25.5.1990

**Elementare Zahlentheorie — Übungsblatt 5**

* **Aufgabe 19** (5 Punkte)

Zeigen Sie folgende Verallgemeinerung des *Fermat*schen Satzes:
Für $n \in \mathbb{N}$, $a \in \mathbb{Z}$ gilt $n \mid \sum_{d \mid n} \mu(d) \cdot a^{\frac{n}{d}}$.

**Aufgabe 20** (3 Punkte)

(a) Sei $p \in \mathbb{P}$. Zeigen Sie:
$\bar{g} \in \mathbb{F}_p^{\times}$ ist genau dann Primitivwurzel modulo $p$, wenn für alle Primteiler $q$ von $p-1$ gilt $\bar{g}^{\frac{p-1}{q}} \neq \bar{1}$.

(b) Bestimmen Sie alle Primitivwurzeln modulo 31.

**Aufgabe 21** (4 Punkte)

Beweisen Sie das folgende Primzahlkriterium für $n \in \mathbb{N}$: $n$ ist Primzahl $\iff$
$n > 1$, zu jedem Primteiler $p$ von $n-1$ gibt es ein $a \in \mathbb{Z}$ mit $a^{n-1} \equiv 1 \pmod{n}$ und $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$.

**Aufgabe 22** (4 Punkte)

Sei $p \in \mathbb{P}$, $p > 2$. Zeigen Sie die folgenden Kongruenzen:

(a) $h! \cdot k! + (-1)^h \equiv 0 \pmod{p}$ für $h, k \in \mathbb{N}$ mit $h + k = p - 1$ ,

(b) $((\frac{p-1}{2})!)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ ,

(c) $2^2 \cdot 4^2 \cdot 6^2 \cdot \ldots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ ,

(d) $1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ .

**Aufgabe 23** (7 Punkte)

Sei $p \in \mathbb{P}$. Für $F \in \mathbb{Z}[X_1, \ldots, X_n]$ sei $N(F)$ die Anzahl der Lösungen in ${\mathbb{F}_p}^n$ der Kongruenz $F(X_1, \ldots, X_n) \equiv 0 \pmod{p}$.

(a) Zeigen Sie: Für $F(X_1, X_2) = aX_1 + bX_2$ $(a, b \in \mathbb{Z})$ gilt $N(F) \equiv 0 \pmod{p}$.

(b) Sei $p$ ungerade. Zeigen Sie: Für $F_a(X_1) = X_1^2 - a$ $(a \in \mathbb{Z})$ gilt $N(F_a) \equiv 1 + a^{\frac{p-1}{2}} \pmod{p}$.

* (c) Sei $p$ ungerade. Geben Sie ein Polynom $P(\lambda)$ an, so daß für $F_\lambda(X_1, X_2) = X_2^2 - X_1(X_1 - 1)(X_1 - \lambda)$ $(\lambda \in \mathbb{Z})$ gilt $N(F_\lambda) \equiv P(\lambda) \pmod{p}$.

(Hinweis: Betrachten Sie – wie beim Beweis des Satzes von *Waring/Chevalley* – die Monome des Polynoms $1 - F^{p-1}$.)

**Aufgabe 24** (4 Punkte)

Für $n \in \mathbb{N}$ sei $\operatorname{guT}(n)$ der größte ungerade Teiler von $n$. Zeigen Sie: $\displaystyle\sum_{n=1}^{\infty} \frac{\operatorname{guT}(n)}{n^s} = \frac{1 - 2^{1-s}}{1 - 2^{-s}} \cdot \zeta(s-1)$.

**Abgabe:** Bis spätestens Donnerstag, 31.5.1990, 15.30 Uhr in den Kasten bei Zi. 308 des Mathematikgebäudes oder in der Übung im Hörsaal Hauptbau.