Übungen zur **Blatt 6**
Elementaren Zahlentheorie 21.11.2014

Falko Lorenz, Karin Halupczok WiSe 2014/15

Abgabetermin: Freitag, 28. November 2014, bis 10:10 Uhr in die Briefkästen

---

Aufgabe 21:

(a) Löse die Kongruenz $163x \equiv 13 \bmod 261$ in $\mathbb{Z}$.

(b) Man bestimme alle $x \in \mathbb{Z}$ mit $x \equiv 4 \bmod 25$, $x \equiv 2 \bmod 64$, $x \equiv 3 \bmod 59$.

Aufgabe 22:

Es sei $n = a_0 10^0 + a_1 10^1 + a_2 10^2 + \dots$ die Darstellung der natürlichen Zahl n im Dezimalsystem; mit s_n werde ihre Quersumme $\sum a_i$ und mit t_n die Summe $\sum (-1)^i a_i$ bezeichnet. Man zeige:

(a) $n \equiv s_n \bmod 9$, $n \equiv t_n \bmod 11$. Welche Regeln folgen hieraus hinsichtlich der Teilbarkeit durch 3, 9, 11?

(b) Für $p \in \{7, 11, 13\}$ gilt genau dann $p \mid n$, wenn

$$p \mid (a_0 + a_1 10 + a_2 10^2) - (a_3 + a_4 10 + a_5 10^2) + (a_6 + a_7 10 + a_8 10^2) - \dots$$

(Tip: $7 \cdot 11 \cdot 13 = 1001$). Welche Primzahlen teilen 3.702.294.323?

Aufgabe 23:

Es sei p eine Primzahl, $F := \mathbb{Z}/p\mathbb{Z}$; $F[X]$ bezeichne den Polynomring in einer Unbestimmten über dem Körper F.

(a) Mittels Grad- und Nullstellenvergleich zeige man, daß in $F[X]$ gelten:

$$X^{p-1} - 1 = (X+1)(X+2)\cdots(X+(p-1)), \qquad (X+1)^p - (X+1) = X^p - X.$$

(b) Aus der ersten Relation in a) folgere man den *Satz von Wilson*, aus der zweiten die Gültigkeit von

$$\binom{p}{j} \equiv 0 \bmod p \text{ für } 1 \le j \le p-1.$$

(c) Zeige: Für $m, n \in \mathbb{N}$ und für $k \in \mathbb{N}_0$ mit $0 \le k \le m$ gilt

$$\binom{mp^n}{kp^n} \equiv \binom{m}{k} \bmod p.$$

(Hinweis: Warum ist $(X+1)^{p^n m} = (X^{p^n} + 1)^m$ in $F[X]$?)

Aufgabe 24:

(a) Man berechne die Ordnungen der Restklassen 6 mod 31 und 5 mod 108.

(b) Für $m, a, c \in \mathbb{N}$ mit $m > 1$ gelte $a^c \equiv 1 \bmod m$. Man zeige: Genau dann ist c die Ordnung von a mod m, wenn gilt: Für jeden Primteiler q von c ist $a^{c/q} \not\equiv 1 \bmod m$.