Universität Bielefeld

Peter Zeiner
Fakultät für Mathematik

Bielefeld, 31.10.2013

Wintersemester 2013/14

Elementare Zahlentheorie

Übungszettel 3

Aufgabe 14: Zeigen Sie, dass Kongruenz modulo m eine Äquivalenzrelation ist, d.h. für alle $a, b, c \in \mathbb{Z}$ gilt

(a) $a \equiv a \pmod{m}$ (Reflexivität)

(b) $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$ (Symmetrie)

(c) $(a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \Longrightarrow a \equiv c \pmod{m}$ (Transitivität).

(1+1+2 Punkte)

Aufgabe 15: Sei $n = \sum_{i=0}^{\ell} 10^i a_i$ die Dezimaldarstellung einer Zahl $n \in \mathbb{N}$, $Q'(n) = \sum_{i=0}^{\ell} (-1)^i a_i$ ihre alternierende Ziffernsumme, $Q_2(n) = \sum_i (a_{2i} + 10a_{2i+1})$ ihre Ziffernsumme zweiter Stufe und $Q_k(n) = \sum_i (a_{ki} + 10a_{ki+1} + \ldots 10^{k-1} a_{ki+k-1})$ ihre Ziffernsumme k-ter Stufe.

(a) Zeigen Sie $11 \mid n \Longleftrightarrow 11 \mid Q'(n)$.

(b) Zeigen Sie $11 \mid n \Longleftrightarrow 11 \mid Q_2(n)$.

(c) Bestimmen Sie eine gewichtete Ziffernsumme $Q_{(g)}(n) = \sum_{i=0}^{\ell} g_i a_i$ so, dass $37 \mid n \Longleftrightarrow 37 \mid Q_{(g)}(n)$ gilt.

(d) Bestimmen Sie das kleinste k, für das $37 \mid n \Longleftrightarrow 37 \mid Q_k(n)$ gilt.

(1+1+2+1 Punkte)

Aufgabe 16: Betrachten Sie den euklidischen Algorithmus $r_{-1} = a$, $r_0 = b$, $r_{k-2} = c_{k-1} r_{k-1} + r_k$, $0 \leq r_k < r_{k-1}$ für zwei natürliche Zahlen $a, b \in \mathbb{N}$ mit $b < a$. Sei $g = \mathrm{ggT}(a, b) = r_\ell$, d.h. $r_{\ell+1} = 0$. Definieren Sie $p_0 := 1, p_1 := 1$ und $p_{i+2} := p_i - c_{\ell-i} p_{i+1}$ für $i \geq 2$. Zeigen Sie, dass $a p_{\ell+1} + b p_{\ell+2} = g$ gilt, d.h. $ax + by = g$ besitzt die Lösung $x = p_{\ell+1}, y = p_{\ell+2}$.

Hinweis: Zeigen Sie induktiv, dass $p_i r_{\ell-i} + p_{i+1} r_{\ell-i+1} = r_\ell = g$ für alle $i = 0, \ldots, \ell + 1$ gilt.

(3 Punkte)

Aufgabe 17: Sei $a \in \mathbb{Z}$, $m \in \mathbb{N}$. Betrachten Sie die Folge $(a^i)_{i \in \mathbb{N}}$ modulo m.

(a) Zeigen Sie, dass es $n_1, n_2 \in \mathbb{N}$ mit $n_2 > n_1$ gibt, so dass $a^{n_1} \equiv a^{n_2} \pmod{m}$ gilt.

(b) Zeigen Sie, dass es $n, k \in \mathbb{N}$ gibt, so dass $a^{i+k} \equiv a^i \pmod{m}$ für alle $i \geq n$ gilt, d.h., dass $(a^i)_{i \in \mathbb{N}}$ ab einem n periodisch mit Periode k ist.

(c) Sei $\mathrm{ggT}(a, m) = 1$. Zeigen Sie, dass es ein $k \in \mathbb{N}$ gibt, sodass $a^k \equiv 1 \pmod{m}$ ist.

(1+1+1 Punkte)

Aufgabe 18*: In der Vorlesung haben wir Kongruenzen $a \equiv b \pmod{m}$ nur für $m \in \mathbb{N}$ definiert. Ist die Definition auch für $m = 0$ sinnvoll? Falls ja:

(a) Wie lauten die Restklassen modulo 0?

(b) Was ist $\mathbb{Z}/0\mathbb{Z}$? Ist dies ein kommutativer Ring?

(c) Falls $\mathbb{Z}/0\mathbb{Z}$ ein Ring ist, hat er die Charakteristik 0? Ist er nullteilerfrei?
Hinweis: Ein Ring hat Charakteristik 0, falls es kein $m \in \mathbb{N}$ mit $m \cdot 1 = 0$ gibt.

(bis zu 4 Bonuspunkte)

Abgabe bis zum 7.11.2013!