Elementare Zahlentheorie

Blatt 7 — 28.05.2015

Aufgabe 25. (Struktur der Einheitengruppe, 4 Punkte)

(a) Sei $n \in \mathbb{N}$. Zeigen Sie: Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ist genau dann zyklisch, wenn $n = 2, 4, p^m$ oder $2p^m$ für eine ungerade Primzahl p und $m \in \mathbb{N}$ ist.

(b) Bestimmen Sie eine Primitivwurzel modulo $338 = 2 \cdot 13^2$ (d.h. einen zyklischen Erzeuger von $(\mathbb{Z}/338\mathbb{Z})^\times$).

Aufgabe 26. (Potenzreste, 2+2 Punkte)

(a) Sei p eine ungerade Primzahl und $n \in \mathbb{N}$. Weiter sei $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, $m \in \mathbb{N}$ und $d := (m, \varphi(p^n))$. Zeigen Sie:

(i) Ist $d = 1$, so hat die Kongruenz $x^m \equiv a \pmod{p^n}$ immer genau eine Lösung in $\mathbb{Z}/p^n\mathbb{Z}$.

(ii) Ist $d > 1$, so hat die Kongruenz $x^m \equiv a \pmod{p^n}$ entweder genau d verschiedene oder gar keine Lösungen in $\mathbb{Z}/p^n\mathbb{Z}$.

Hinweis: Primitivwurzeln.

(b) Bestimmen Sie alle Lösungen der Kongruenz $\quad x^3 \equiv 5 \mod 143$.

Aufgabe 27. (Quadratische Kongruenzen, 2+2 Punkte)

(a) Sei p eine ungerade Primzahl. Weiter seien $a, b, c \in \mathbb{N}$ mit $p \nmid a$. Zeigen Sie: Die Kongruenz

$$ax^2 + bx + c \equiv 0 \mod p$$

besitzt genau $\left(\frac{b^2-4ac}{p}\right) + 1$ viele Lösungen in $\mathbb{Z}/p\mathbb{Z}$.

(b) Untersuchen Sie, wieviele Lösungen in $\mathbb{Z}/n\mathbb{Z}$ folgende Kongruenzen besitzen:

(i) $2x^2 + 3x - 1 \equiv 0 \mod n,\quad$ wobei $n = 133$.

(ii) $5x^2 + 3x + 1 \equiv 0 \mod n,\quad$ wobei $n = 235$.

— bitte wenden —

Aufgabe 28. (Weiterer Spezialfall des Dirichlet'schen Primzahlsatzes, 4 Punkte)

Zeigen Sie:

(a) Ist p ein Primteiler einer Zahl der Form $2N^2+1$ mit $N \in \mathbb{N}$, so ist $p \equiv 1$ oder $3 \bmod 8$.

(b) Sind $p_1, \dots, p_k$ ungerade Primzahlen, so besitzt $P := 2(p_1 \cdots p_k)^2 + 1$ einen Primteiler der Form $8n+3$ mit $n \in \mathbb{N}_0$.

(c) Es gibt unendlich viele Primzahlen p mit $p \equiv 3 \bmod 8$.

Abgabe: Am kommenden **Mittwoch, den 03.06.2015, bis 14 Uhr** in den Kasten im 3. Stock, Institut für Mathematik, Robert-Mayer-Straße 6-8. Downloads von Übungsblättern und Informationen zur Vorlesung unter

`http://www.uni-frankfurt.de/54089776/Elementare_Zahlentheorie`
