Übungen zu Elementare Zahlentheorie — Blatt 4

Prof. Dr. Ulrich Thiel, TU Kaiserslautern — Sommersemester 2021
Abgabetermin: Montag, 14.06.2021, 10:00 Uhr — Dr. Tommy Hofmann

---

Mit Primzahl ist im Folgenden stets eine positive Primzahl gemeint.

Aufgabe 1. Es sei $p \in \mathbb{P}$ eine ungerade Primzahl und a eine Primitivwurzel modulo p. Zeigen Sie:

(i) Es gilt $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

(ii) Genau dann ist $-a$ ebenfalls eine Primitivwurzel modulo p, wenn $p \equiv 1 \bmod 4$ gilt.

Aufgabe 2.

(i) Es sei $p \in \mathbb{P}$ eine ungerade Primzahl, $k \in \mathbb{N}$ und $a \in \mathbb{Z}$ eine Primitivwurzel modulo p^k. Zeigen Sie:

  (a) Ist a ungerade, so ist a eine Primtivwurzel modulo $2p^k$.

  (b) Ist a gerade, so ist $a + p^k$ eine Primitivwurzel modulo $2p^k$.

(ii) Bestimmen Sie eine Primitivwurzel modulo $n = 98$.

Aufgabe 3. Zeigen Sie: Lässt sich eine natürliche Zahl n auf zwei verschiedene Arten als Summe zweier Quadratzahlen schreiben, das heißt, gilt $n = x^2 + y^2 = z^2 + w^2$ mit $x, y, z, w \in \mathbb{Z}$ und $\{x^2, y^2\} \neq \{z^2, w^2\}$, so ist n keine Primzahl. Hinweis: Es ist hilfreich zunächst folgende Behauptungen zu zeigen:

(i) Ohne Einschränkung kann man $x \equiv z \bmod 2$ und $y \equiv w \bmod 2$ voraussetzen.

(ii) Das Gleichungssystem

$$\frac{x+z}{2} = ac,\ \frac{z-x}{2} = bd,\ \frac{y+w}{2} = cb,\ \frac{y-w}{2} = ad$$

besitzt eine ganzzahlige ganzzahlige Lösung $(a, b, c, d) \in \mathbb{Z}^4$.

(iii) Es gilt $n = (a^2 + b^2)(c^2 + d^2)$.

Aufgabe 4.

(i) Zeigen Sie, dass auch die folgende Umkehrung des Satzes von Wilson gilt: Eine natürliche Zahl $p \geq 2$ ist genau dann eine Primzahl, wenn $(p-1)! \equiv -1 \bmod p$ gilt.

(ii) Beweisen Sie, dass für eine natürliche Zahl $p \geq 2$ das Paar $(p, p+2)$ genau dann ein Primzahlzwilling ist, wenn

$$4((p-1)! + 1) + p \equiv 0 \bmod p(p+2).$$