Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix

Elementare Zahlentheorie

Sommersemester 2017

Übungsblatt 8 12. Juni 2017

Aufgabe 36. (Nochmals Primitivwurzeln)

Sei $q \in \mathbb{N}$ eine ungerade Primzahl, so dass $p := 2q + 1$ wieder eine Primzahl ist.

(a) Zeigen Sie: 2 ist genau dann eine Primitivwurzel modulo p, wenn $q \equiv 1 \pmod 4$.
Hinweis: Welche Ordnung kann 2 modulo p haben?

(b) Finden Sie eine notwendige und hinreichende Bedingung an q dafür, daß 5 eine Primitivwurzel modulo p ist.

Aufgabe 37. (Parametrisierung Pythagoräischer Tripel)

Ziel dieser Aufgabe ist es, die Parametrisierung Pythagoräischer Tripel, das sind $a, b, c \in \mathbb{N}$ mit

$$a^2 + b^2 = c^2,$$

mit einer geometrischen Methode herzuleiten, und zwar wie folgt:

(a) Zeigen Sie: Ist (a, b, c) ein Pythagoräisches Tripel, so ist $(x, y) := (\frac{a}{c}, \frac{b}{c})$ ein rationaler Punkt auf dem Einheitskreis

$$x^2 + y^2 = 1.$$

Außerdem ist die Steigung der Geraden durch die Punkte $(-1, 0)$ und (x, y) eine rationale Zahl $t \in (0, 1)$.

(b) Bestimmen Sie für $t \in (0, 1) \cap \mathbb{Q}$ die Schnittpunkte der Geraden der Steigung t durch den Punkt $(-1, 0)$ mit dem Einheitskreis.

(c) Folgern Sie: Ist (a, b, c) ein *primitives* Pythagoräisches Tripel, d.h. ein Pythagoräisches Tripel mit $\mathrm{ggT}(a, b, c) = 1$, so gibt es $u, v \in \mathbb{N}$ teilerfremd mit $u \not\equiv v \pmod 2$, so daß

$$a = u^2 - v^2, \quad b = 2uv \quad \text{und} \quad c = u^2 + v^2.$$

Hinweis: Schreiben Sie für t aus Teil (b) $t = \frac{v}{u}$ für $u, v \in \mathbb{N}$ teilerfremd mit $u > v$. Was passiert, wenn u und v beide ungerade sind?

Aufgabe 38.

Sei $\zeta \in \mathbb{C}$, $\zeta \neq 1$ eine Einheitswurzel mit $\zeta^n = 1$. Zeigen Sie $\sum_{k=1}^{n} \zeta^k = 0$.

Aufgabe 39. (Gauß-Summe)

Sei p eine ungerade Primzahl und sei $\zeta = e^{2\pi i/p}$. Wir definieren die **Gauß-Summe** als

$$\tau = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a.$$

Zeigen Sie $\tau^2 = (-1)^{\frac{p-1}{2}} p$.

Abgabe: Am kommenden Dienstag, den **20. Juni 2017**, bis zur Vorlesung 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/65113368/17_SS_Elementare-Zahlentheorie`