Elementare Zahlentheorie

Blatt 9 — 11.06.2015

Aufgabe 32. (Berechnung der Jacobi-Symbole, 4 Punkte)
Berechnen Sie $\left(\frac{2017}{5843}\right)$ und $\left(\frac{13259}{35671}\right)$.

Aufgabe 33. (Jacobi-Symbole, 4 Punkte)

Seien $m, n \in \mathbb{N}$ ungerade und $a \in \mathbb{Z}$, so dass $(a, mn) = 1$.

(a) Zeigen Sie: Ist $m \equiv n \bmod 4|a|$, so gilt: $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$

(b) Zeigen Sie anhand eines Beispiels mit $a \in \mathbb{N}$ ungerade, dass die Bedingung $m \equiv n \bmod 2a$ nicht ausreicht.

Aufgabe 34. (Quadratische Erweiterung von $\mathbb{F}_p$, 4 Punkte)

Sei p eine ungerade Primzahl und $a \in \mathbb{F}_p^\times$ eine quadratische Nichtrest. Wie in der Vorlesung bezeichne $\bar{\mathbb{F}}_p \supseteq \mathbb{F}_p$ eine algebraisch abgeschlossene Erweiterung. Sei $\alpha \in \bar{\mathbb{F}}_p$ so fest gewählt, dass $\alpha^2 = a$. Ferner Sei

$$\mathbb{F}_p(\alpha) := \{x + y\alpha \mid x, y \in \mathbb{F}_p\}.$$

Zeigen Sie:

(a) $\mathbb{F}_p(\alpha)$ ist ein Körper der Charakteristik p mit p^2 Elementen. Diesen werden wir deshalb im folgenden mit $\mathbb{F}_{p^2}$ bezeichnet.

(b) Für den Frobenius-Automorphismus $F : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2},\ z \mapsto z^p$ aus der Vorlesung gilt:

$$F(x + y\alpha) = x - y\alpha \quad \text{für alle } x, y \in \mathbb{F}_p.$$

(c) Die *Normabbildung*

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p} : \mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times,\ z = x + y\alpha \mapsto z \cdot F(z) \stackrel{!}{=} x^2 - y^2 a$$

ist ein surjektiver Gruppenhomomorphismus.

— **bitte wenden** —

Aufgabe 35. (Parametrisierung Pythagoräischer Tripel, 4 Punkte)

Ziel dieser Aufgabe ist es, die Parametrisierung Pythagoräischer Tripel (Vgl. Aufgabe 15 Blatt 4) 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 $u \not\equiv v \bmod 2$, 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?*

Abgabe: Am kommenden Donnerstag, den 18.06.2015, 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/54089776/Elementare_Zahlentheorie`