Elementare Zahlentheorie

Blatt 8 — 04.06.2015

Aufgabe 29. (Kreisgleichung über $\mathbb{Z}/p\mathbb{Z}$ und die Ergänzungssätze des quadratischen Reziprozitätsgesetzes, 2+1+2+2+1+1 Punkte)

Es sei $p > 2$ eine Primzahl. Für $a \in \mathbb{Z}$ mit $p \nmid a$ definieren wir

$$K_a := \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \ : \ x^2 + y^2 \equiv a \mod p\}.$$

Ziel dieser Aufgabe ist es, $\#K_a$ zu bestimmen und daraus einen weiteren Beweis der Ergänzungssätze des quadratischen Reziprozitätsgesetzes herzuleiten. Gehen Sie wie folgt vor:

(a) Zeigen Sie: $\displaystyle\sum_{j=0}^{p-1} \left(\frac{j(j-a)}{p}\right) = -1.$

Hinweis: Zeigen Sie zunächst für $j \neq 0$, dass $\left(\frac{j^{-1}}{p}\right) = \left(\frac{j}{p}\right)$, wobei $j^{-1} \in \mathbb{Z}/p\mathbb{Z}$ das multiplikative Inverse von j modulo p bezeichnet. Benutzen Sie auch die aus der Vorlesung bekannte Relation $\sum_{j=0}^{p-1}\left(\frac{j}{p}\right) = 0$.

(b) Zeigen Sie: $\displaystyle\#K_a = \sum_{j=0}^{p-1} \left(1 + \left(\frac{j}{p}\right)\right)\left(1 + \left(\frac{a-j}{p}\right)\right).$

Hinweis: Überlegen Sie hierzu, dass $\#\{x \in \mathbb{Z}/p\mathbb{Z} \mid x^2 \equiv j \mod p\} = 1 + \left(\frac{j}{p}\right)$ gilt.

(c) Folgern Sie: $\displaystyle\#K_a = p - \left(\frac{-1}{p}\right).$

Wir kommen nun zum Beweis der Ergänzungssätze. Folgende Teilaufgaben sind unabhängig von den vorherigen. Lediglich das Resultat von (c) wird für die Teile (e) und (f) benötigt.

— bitte wenden —

(d) Zeigen Sie: $\#K_2 \equiv 4 + 2\left(\left(\frac{2}{p}\right) + 1\right) \mod 8$.

Hinweis: Betrachten Sie die Gruppenwirkung von $D_4 = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = (\sigma\tau)^4 = 1 \rangle$ *auf* K_2*, die für* $(x, y) \in K_2$ *gegeben ist durch*

$$\sigma(x, y) := (x, -y) \quad \textit{und} \quad \tau(x, y) := (y, x).$$

Sie dürfen davon ausgehen, dass es sich hier um eine wohldefinierte Gruppenwirkung handelt. Für welchen Punkt $(x, y) \in K_2$ *hat die Bahn unter dieser Gruppenwirkung die Länge* 8*? Welche Bahnlänge haben dann die restlichen Punkte?*

(e) Folgern Sie den ersten Ergänzungssatz: $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \mod 4, \\ -1, & p \equiv 3 \mod 4. \end{cases}$

(f) Folgern Sie den zweiten Ergänzungssatz: $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \mod 8, \\ -1, & p \equiv \pm 3 \mod 8. \end{cases}$

Aufgabe 30. (Nochmals Primitivwurzeln, 2+2 Punkte)

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 $q \equiv 1 \mod 4$.
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 31. (Pépins Primzahltest, 3 Punkte)

Für $n \in \mathbb{N}$ sei $F_n := 2^{(2^n)} + 1$ eine Fermat-Zahl. Zeigen Sie:

$$F_n \text{ ist eine Primzahl} \quad \Leftrightarrow \quad 3^{(F_n - 1)/2} \equiv -1 \mod F_n.$$

Hinweis für die Rückrichtung: Zeigen Sie zunächst, dass für jeden Primteiler q *von* F_n *die Ordnung von* 3 *modulo* q *gleich* $2^{(2^n)}$ *sein muss.*

Abgabe: Am kommenden Donnerstag, den 11.06.2015, 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`