

Einführung in Algebra und Zahlentheorie – Übungsblatt 13 – finito

Aufgabe 1 (4 Punkte)

Sei $p \geq 3$ eine Primzahl. Zeige:

- Jede natürliche Zahl a mit $\left(\frac{a}{p}\right) = -1$ besitzt mindestens einen Primfaktor $q|a$ mit $\left(\frac{q}{p}\right) = -1$.
- Es gibt unendlich viele Primzahlen, die kein Quadrat modulo p sind.

Aufgabe 2 (4 Punkte)

Sei $R = \mathbb{Z}/524\mathbb{Z}$.

- Wie viele Quadrate gibt es in R ?
- Wie viele $x \in R$ gibt es mit der Eigenschaft $x^2 = 20$? Wie viele $y \in R$ erfüllen $y^2 = 443$?

(Hinweis: Der chinesische Restsatz könnte helfen.)

Aufgabe 3 (4 Punkte)

Seien p, q zwei ungerade Primzahlen mit $p = q + 9a$ für ein $a \in \mathbb{Z}$. Zeige die folgenden Aussagen:

- $\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right)$ und $\left(\frac{-q}{p}\right) = \left(\frac{a}{p}\right)$.
- Für $a \equiv 0$ modulo 4 gilt $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
- Finde einen Zusammenhang zwischen den Legendresymbolen $\left(\frac{a}{p}\right), \left(\frac{a}{q}\right)$ für $a \equiv 2$ modulo 4.
(Hinweis: Der Zusammenhang ist abhängig von p .)

Aufgabe 4 (4 Punkte)

In dieser Aufgabe zeigen wir, dass für eine Primzahl $p \in \mathbb{P}$ das Polynom $\Phi_p(X) := \frac{X^p-1}{X-1} \in \mathbb{Z}[X]$ irreduzibel in $\mathbb{Q}[X]$ ist.

- Zunächst zeigen wir folgenden Spezialfall des „Lemmas von Gauß“:
Sei $f \in \mathbb{Z}[X]$ normiert und irreduzibel in $\mathbb{Z}[X]$. Dann ist f auch irreduzibel in $\mathbb{Q}[X]$.
(Hinweis: Den größten gemeinsamen Teiler der Koeffizienten eines Polynoms $f \in \mathbb{Z}[X]$ bezeichnen wir als *Inhalt* $\text{Inh}(f)$. Du darfst ohne Rechnung benutzen, dass der *Inhalt* multiplikativ ist, dass also $f = g \cdot h \Rightarrow \text{Inh}(f) = \text{Inh}(g) \cdot \text{Inh}(h)$ gilt.)
- Zeige nun, dass Φ_p irreduzibel über $\mathbb{Q}[X]$ ist.
(Hinweis: Betrachte $\Phi_p(X+1)$ und erinnere dich an eine alte Übungsaufgabe.)

Nächste Woche lernen wir Φ_p als p -tes *Kreisteilungspolynom* kennen.

Abgabe der Übungsblätter:

Bitte wirf deine Lösung zu diesem Übungsblatt bis Donnerstag, 18. Juli 2013, 11:30 Uhr in den entsprechenden Abgabekasten im 1C-Teil des Allianzgebäudes oder gib sie deinem Übungsleiter direkt vor der großen Übung.