

## Elementare Zahlentheorie

### Übungsblatt 9

#### 9.1 (4 Punkte)

Es seien  $p$  eine Primzahl und  $N \in \mathbb{N} \setminus p\mathbb{N}$ . Weiter sei  $m$  ein irreduzibler Teiler des Kreisteilungspolynoms  $\Phi_N$  in  $\mathbb{F}_p[X]$ .

Welchen Grad hat  $m$ ?

Bestimmen Sie die irreduziblen Teiler von  $\Phi_{13}$  über  $\mathbb{F}_3$ .

#### 9.2 (4 Punkte)

a) Finden Sie primitive Elemente in  $\mathbb{F}_p^\times$  für  $p \in \{31, 47\}$ .

b) Berechnen Sie die Legendre-Symbole

$$\left(\frac{22}{17}\right), \left(\frac{13}{47}\right).$$

#### 9.3 (4 Punkte)

Es seien  $p$  eine ungerade Primzahl und  $\zeta = \cos\left(\frac{2\pi}{p}\right) + i \cdot \sin\left(\frac{2\pi}{p}\right) \in \mathbb{C}$ .

Zeigen Sie die Gleichheit

$$\left[ \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \cdot \zeta^a \right]^2 = \left(\frac{-1}{p}\right) p.$$

Lust auf mehr? Bitte wenden!

#### 9.4 (4 Punkte)

Es seien  $p$  eine ungerade Primzahl und  $f, g \in R := \mathbb{F}_p[X]$  zwei verschiedene irreduzible und normierte Polynome. Wir definieren

$$\left(\frac{f}{g}\right) := \left(\frac{f + gR}{R/gR}\right).$$

Die Grade von  $f$  bzw.  $g$  seien  $d$  bzw.  $e$ . Weiter seien  $\alpha$  bzw.  $\beta$  jeweils eine Nullstelle von  $f$  bzw.  $g$  in  $\mathbb{F}_{p^d} = R/fR$  bzw.  $\mathbb{F}_{p^e} = R/gR$ .

Zeigen Sie:

a)

$$\left(\frac{f}{g}\right) = \left(\frac{f(\beta)}{\mathbb{F}_{p^e}}\right) = f(\beta)^{\frac{p^e-1}{2}}.$$

b)

$$\left(\frac{f}{g}\right) = \left[f(\beta) \cdot f(\beta^p) \cdot \dots \cdot f(\beta^{p^{e-1}})\right]^{(p-1)/2}.$$

c)

$$\left(\frac{f}{g}\right) = \prod_{a=0}^{d-1} \prod_{b=0}^{e-1} (\beta^{p^b} - \alpha^{p^a})^{(p-1)/2}.$$

d)

$$\left(\frac{f}{g}\right) \cdot \left(\frac{g}{f}\right) = (-1)^{de \frac{p-1}{2}}.$$

Wie besprochen wird die **Klausur zur Vorlesung Elementare Zahlentheorie** am Donnerstag, den 9. Oktober 2008 von 10:00 bis 12:00 Uhr in Hörsaal 37 stattfinden.

Diese Klausur ist entweder als Prüfung im Ergänzungsfach für das Informatikstudium oder als studienbegleitende Prüfung in den mathematischen Diplomstudiengängen verwendbar.

Die Anmeldung zur Klausur findet in Zimmer 308 bei Frau Hoffmann statt.

**Abgabe:** Bis Mittwoch, den 18. Juni um 13.00 Uhr in den dafür vorgesehenen Briefkasten bei Zimmer 308 im Fakultätsbau Mathematik oder in der Übung.