Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2013/14
15. Januar 2014

Endliche Körper

Übungsblatt 6

Aufgabe 21

Sei p eine ungerade Primzahl und K ein Körper, in dem eine primitive p-te Einheitswurzel ζ existiert. Dann ist die Gaußsche Summe

$$S(p,\zeta) := \sum_{x\in(\mathbb{Z}/p)^*} \left(\frac{x}{p}\right)\zeta^x \in K$$

definiert. Für eine ganze Zahl ℓ mit $p \nmid \ell$ ist ζ^ℓ ebenfalls eine primitive p-te Einheitswurzel. Man berechne den Quotienten $S(p,\zeta^\ell)/S(p,\zeta)$.

Aufgabe 22

Sei p eine ungerade Primzahl, $n \geq 1$ und $\mathrm{N} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ die Norm-Abbildung. Man beweise:

$$x \in \mathbb{F}_{p^n}^* \text{ ist ein Quadrat in } \mathbb{F}_{p^n} \quad\Longleftrightarrow\quad \left(\frac{\mathrm{N}(x)}{p}\right) = 1.$$

Aufgabe 23

a) Sei $a \neq 0$ eine ganze Zahl und seien p, p' ungerade Primzahlen mit $p \equiv p' \bmod 4|a|$ bzw. $p \equiv p' \bmod 2|a|$, falls $a \equiv 1 \bmod 4$. Man zeige:

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p'}\right).$$

b) Bekanntlich gilt

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv \pm 1 \bmod 8, \\ -1, & \text{falls } p \equiv \pm 3 \bmod 8. \end{cases}$$

Man stelle analoge Regeln für $\left(\frac{3}{p}\right)$ und $\left(\frac{5}{p}\right)$ auf.

Aufgabe 24

Sei p eine ungerade Primzahl und a eine ganze Zahl mit $\left(\frac{a}{p}\right) = 1$. Man beweise:

a) Falls $p \equiv 3 \bmod 4$, so ist $x := a^{(p+1)/4}$ eine Lösung der Kongruenz $x^2 \equiv a \bmod p$.

b) Falls $p \equiv 5 \bmod 8$, so gilt für $x := a^{(p+3)/8}$ entweder $x^2 \equiv a \bmod p$ oder $x^2 \equiv -a \bmod p$. Im zweiten Fall ist $\tilde{x} := 2^{(p-1)/4}x$ eine Lösung der Kongruenz $\tilde{x}^2 \equiv a \bmod p$.