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

SS 2006
21. Juni 2006

Endliche Körper, Übungsblatt 5

Aufgabe 17

Sei p eine ungerade Primzahl und K ein Körper, der eine primitive p-te Einheitswurzel ζ_p enthält. Der Wert der Gaußsche Summe

$$S(p) = \sum_{x=1}^{p-1} \Big(\frac{x}{p}\Big)\zeta_p^x \in K$$

hängt von der Wahl der primitiven Einheitswurzel ab. Wie ändert sich $S(p)$, wenn man ζ_p durch eine andere primitive p-te Einheitswurzel in K ersetzt?

Aufgabe 18

Man beweise folgende Regel für das Legendre-Symbol: Sei $a \neq 0$ eine ganze Zahl und seien p, q ungerade Primzahlen mit $p \equiv \pm q \bmod 4a$. Dann gilt

$$\Big(\frac{a}{p}\Big) = \Big(\frac{a}{q}\Big)$$

Aufgabe 19

a) Für welche Primzahlen p ist folgende Kongruenz lösbar?

$$x^2 - x - 1 \equiv 0 \bmod p.$$

b) Man löse die obige Kongruenz für $p = 11$ und* (mit Computerhilfe) für

$$p = \frac{10^{19} - 1}{9} = 1111\,11111\,11111\,11111.$$

Aufgabe 20

Man zeige die Korrektheit des folgenden Algorithmus für das Wurzelziehen im Körper $\mathbb{F}_p$, wobei p eine Primzahl der Gestalt $p = 8k + 5$ sei.

Sei $a \in \mathbb{F}_p^*$ mit $(\frac{a}{p}) = 1$. Man setze $x := a^{k+1}$. Dann gilt $x^2 = \pm a$. Falls das Pluszeichen zutrifft, ist man fertig. Andernfalls setze man $y := 2^{2k+1}x$. Dann gilt $y^2 = a$.

Abgabetermin: Mittwoch, 28. Juni 2006, 14 Uhr