Einführung in die Algebra und Zahlentheorie
Übungsblatt 14

Abgabetermin Donnerstag, den 10.02.2010 vor der Vorlesung.

0. Wiederholen Sie Abschnitt 6.8 – 7 im Vorlesungsmanuskript.

1. Wieviele Elemente $a \in \mathbb{F}_{4096}$ gibt es, sodass $\mathbb{F}_{4096} = \mathbb{F}_2[a]$?

2. Sei $K = \mathbb{F}_3$, $L = \mathbb{F}_3[x] / \langle x^3 - x + 1 \rangle$ und $a = \overline{x}^2 + \overline{x} + 1 \in L$. Bestimmen Sie das Minimalpolynom von a über K, und geben Sie für alle Automorphismen von L über K das Bild von a an.

3. Bestimmen Sie das Jacobisymbol
$$\left(\frac{455}{1236}\right)$$
und entscheiden Sie, ob die Gleichung $x^2 \equiv 455 \mod 1236$ lösbar ist. Beachten Sie: $1236 = 2^2 \cdot 3 \cdot 103$.

4. (a) Berechnen Sie per Hand:
$$\left(\frac{3}{97}\right), \left(\frac{5}{389}\right), \left(\frac{2003}{11}\right), \left(\frac{5!}{7}\right)$$
(b) Zeigen Sie
$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{falls} \quad p \equiv 1 \mod 3 \\ -1 & \text{falls} \quad p \equiv -1 \mod 3 \end{cases}$$

5. (4 Zusatzpunkte) Sei p eine ungerade Primzahl und
$$S = \left\{-\frac{p-1}{2}, -\frac{p-1}{2} + 1, ..., -1, 1, ..., \frac{p-1}{2} - 1, \frac{p-1}{2}\right\}$$
Zu jedem $a \in \mathbb{Z}$ mit $p \nmid a$ gibt es genau ein $s \in S$ mit $a \equiv s \mod p$.
Ist $a \in \mathbb{Z}$ mit $p \nmid a$, dann sind ε_n und s_n für $n = 1, ..., \frac{p-1}{2}$ definiert durch
$$na \equiv \varepsilon_n s_n \mod p$$
mit $s_n \in S$, $s_n > 0$ und $\varepsilon_n \in \{1, -1\}$.
(a) Bestimmen Sie $\varepsilon_1, ..., \varepsilon_5$ und $s_1, ..., s_5$ für $p = 11$ und $a = 2$.
(b) Zeigen Sie:
$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot ... \cdot \varepsilon_{(p-1)/2}$$
(c) Implementieren Sie damit die Berechnung des Legendre-Symbols, und überprüfen Sie Ihr Programm an den Beispielen aus Aufgabe 3 und 4.