Prof. Dr. M. Kreuzer
H. Bluhm

Abgabe: Mo, 22.05.2006, 12h

Algebra I
Übungsblatt 7

Aufgabe 31:
Seien $x_1, \ldots, x_r, m_1, \ldots, m_r \in \mathbb{Z}$ mit paarweise verschiedenen Zahlen $m_1, \ldots, m_r \geq 2$ und sei $n_i = m_1 \cdots m_{i-1}$ für $i = 1, \ldots, r+1$.

a) Zeigen Sie, dass für jedes $i \in \{1, \ldots, r\}$ ein Zahl $a_i \in \mathbb{Z}$ existiert mit $1 \leq a_i < m_i$ und $a_i n_i \equiv 1 \mod m_i$.
b) Für $i = 1, \ldots, r$ sei $b_i \in \mathbb{Z}$ mit $0 \leq b_i < m_i$ und $b_i \equiv (x_i - \sum_{k=1}^{i-1} b_k n_k) a_i \mod m_i$. Zeigen Sie, dass die Zahl $x = b_1 n_1 + \cdots + b_r n_r$ simultane Lösung der Kongruenzen

$$\begin{aligned} x &\equiv x_1 \mod m_1 \\ x &\equiv x_2 \mod m_2 \\ &\vdots \\ x &\equiv x_r \mod m_r \end{aligned}$$

ist.
c) Berechnen Sie eine simultane Lösung der Kongruenzen

$$x \equiv 1 \mod 2, \quad x \equiv 2 \mod 3, \quad x \equiv 4 \mod 5.$$

Aufgabe 32: (Polynomfaktorisierung nach Kronecker)
Sei $f \in \mathbb{Z}[x]$ ein primitives Polynom vom Grad n und $g \in \mathbb{Z}[x]$ ein Teiler von f. Betrachten Sie die folgenden Instruktionen:

1) Sei $s = \lfloor \frac{n}{2} \rfloor + 1$. Wähle paarweise verschiedene Zahlen $a_0, \ldots, a_s \in \mathbb{Z}$.
2) Setze $X = \{(d_0, \ldots, d_s) \in \mathbb{Z}^{s+1} \mid d_i \text{ teilt } f(a_i) \text{ für } i = 0, \ldots, s\}$.
3) Bestimme für jedes Tupel $d = (d_0, \ldots, d_s) \in X$ das Polynom

$$g_d(x) = \sum_{i=0}^{s} d_i \prod_{j \neq i} \frac{x - a_j}{a_i - a_j}.$$

Zeigen Sie, dass es ein Tupel $d \in X$ gibt mit $g = g_d$.

Aufgabe 33:
Faktorisieren Sie die folgenden Polynome:

a) $x^{100} - x^{200} \in \mathbb{Z}/_{5\mathbb{Z}}[x]$,
b) $x^{12} + x^8 + x^7 + x^6 + x^2 + x + 1 \in \mathbb{Z}/_{2\mathbb{Z}}[x]$,
c) $x^4 + 4x^3 + x^2 - 4x + 1 \in \mathbb{Z}[x]$,
d) $x^5 + 3x^4 - 6x^2 + 1 \in \mathbb{Z}[x]$.

Aufgabe 34:
Sei p eine Primzahl, sei $q = p^e$ für ein $e > 0$ und sei $r \geq 1$. Zeigen Sie:

a) Es ist $x^{q^r} - x = \prod_{a \in \mathbb{F}_{q^r}} (x - a)$.
b) Das Polynom $x^{q^r} - x \in \mathbb{F}_q[x]$ ist quadratfrei.
c) Ein irreduzibles normiertes Polynom $f \in \mathbb{F}_q[x]$ ist genau dann ein Teiler von $x^{q^r} - x$, wenn $\deg(f)$ ein Teiler von r ist.
d) Das Polynom $x^{q^r} - x \in \mathbb{F}_q[x]$ ist das Produkt aller irreduziblen normierten Polynome in $\mathbb{F}_q[x]$, deren Grad ein Teiler von r ist.
e) Ist r eine Primzahl, so existieren in $\mathbb{F}_q[x]$ genau $(q^r - q)/r$ irreduzible normierte Polynome vom Grad r.

Aufgabe 35: (Magische Momente)
Als cleverer Algebraiker bist du an folgendem Glücksspiel interessiert: Ein Kartenspiel bestehe aus 56 verschiedenen Karten, die mit den Zahlen $\{1, \ldots, 56\}$ nummeriert sind. Die Karten werden zeilenweise in Form eines Rechtecks mit 7 Zeilen ausgelegt. Du wirst gebeten, dir eine Karte auszuwählen und die Spalte zu nennen, in der diese liegt (in diesem Fall die Zweite). Anschließend werden die Karten wieder so eingesammelt, dass sie sich in derselben Reihenfolge wie zu Beginn des Spiels befinden. Dann werden sie wiederum zeilenweise in Form eines Rechtecks ausgelegt, diesmal aber in 8 Zeilen. Erneut wirst du gefragt in welcher Spalte sich deine Karte befindet (nun in der Vierten). Dein Gegenüber behauptet nun, er würde deine Karte kennen und verspricht, falls er sich irrt, dir das 1,5-fache deines Einsatzes auszuzahlen.
Spielst du mit ? Und welche Karte hast du dir eigentlich ausgesucht ?