Wolfgang K. Seiler
Tel. 2515

A5, C201

16. Oktober 2008

6. Übungsblatt Computeralgebra

Aufgabe 1: (*10 Punkte)*

$f \in \mathbb{Z}[x]$ sei ein Swinnerton-Dyer-Polynom, d.h. es gibt n verschiedene Primzahlen $p_1, \ldots, p_n$, so daß f die 2^n Nullstellen $\pm\sqrt{p_1} \pm \cdots \pm \sqrt{p_n}$ und höchsten Koeffizienten eins hat. Zeigen Sie, daß in f nur gerade x-Potenzen auftreten!

b) Bestimmen Sie das Swinnerton-Dyer-Polynom f mit Nullstellen $\pm\sqrt{2} \pm \sqrt{3}$ explizit!

c) Faktorisieren Sie f mod 2 und f mod 3 !

d) $p > 3$ sei eine Primzahl. Zeigen Sie: Falls 2 und 3 Quadrate in $\mathbb{F}_p$ sind, zerfällt f mod p in Linearfaktoren, ansonsten in zwei quadratische Faktoren.

e) Im letzteren Fall gibt es ein $a \in \mathbb{F}_p$, so daß die Faktorisierung von f mod p in $\mathbb{F}_p[x]$ folgende Gestalt hat:

$$f = \begin{cases} (x^2+1)(x^2+a^{-1}) & \text{falls weder 2 noch 3 ein Quadrat in } \mathbb{F}_p \text{ ist} \\ (x^2+ax+1)(x^2-ax+1) & \text{falls 2 ein Quadrat in } \mathbb{F}_p \text{ ist, nicht aber 3} \\ (x^2+ax-1)(x^2-ax-1) & \text{falls 3 ein Quadrat in } \mathbb{F}_p \text{ ist, nicht aber 2} \end{cases}$$

Hinweis: Es gibt stets einen Erweiterungskörper von $\mathbb{F}_p$, in dem Quadratwurzeln von 2 und 3 existieren; Sie können also auch modulo p mit den Symbolen $\sqrt{2}$ und $\sqrt{3}$ rechnen. Überlegen Sie sich, wie Sie Nullstellen so kombinieren können, daß Faktoren mit Koeffizienten aus $\mathbb{F}_p$ entstehen. Für den ersten Fall kann es auch nützlich sein, f als quadratische Gleichung für x^2 zu betrachten und diese zu lösen.

f) Faktorisieren Sie f über $\mathbb{F}_7$, $\mathbb{F}_{11}$ und $\mathbb{F}_{13}$!

g) In $\mathbb{F}_{23}$ ist $5^2 = 2$ und $7^2 = 3$. Faktorisieren Sie f mod 23 !

Aufgabe 2: (*6 Punkte)*

a) Berechnen Sie eine Orthogonalbasis des von $\vec{b}_1 = \begin{pmatrix} 2 \\ 4 \\ 2 \\ -1 \end{pmatrix}$, $\vec{b}_2 = \begin{pmatrix} 4 \\ 3 \\ 4 \\ 3 \end{pmatrix}$ und $\vec{b}_3 = \begin{pmatrix} 5 \\ 3 \\ 3 \\ 3 \end{pmatrix}$ aufgespannten Untervektorraums U von $\mathbb{R}^4$!

b) Ergänzen Sie diese zu einer Orthogonalbasis von $\mathbb{R}^4$!

Aufgabe 3: (*4 Punkte)*

a) Zeigen Sie: Für zwei beliebige teilerfremde ganze Zahlen $p, q \in \mathbb{Z}$ gibt es stets eine Gitterbasis von $\mathbb{Z} \oplus \mathbb{Z}$, die den Vektor $\binom{p}{q}$ enthält.

b) Für jede reelle Zahl λ gibt es eine Gitterbasis von $\mathbb{Z} \oplus \mathbb{Z}$, deren Basisvektoren beide mindestens die Länge λ haben.

c) Ist $\vec{v}, \vec{w}$ eine beliebige Gitterbasis von $\mathbb{Z} \oplus \mathbb{Z}$, so hat das von $\vec{v}$ und $\vec{w}$ aufgespannte Dreieck die Fläche $\frac{1}{2}$.

Abgabe bis zum Donnerstag, dem 23. Oktober 2008, um 15.30 Uhr