Wolfgang K. Seiler
Tel. 2515

B6, B4.08

4. Mai 2023

10. Übungsblatt Computeralgebra

Aufgabe 1:

a) Zeigen Sie, daß die Swinnerton-Dyer-Polynome nur X-Potenzen mit geraden Exponenten enthalten!

b) q und r seien zwei verschiedene Primzahlen. Bestimmen Sie das Swinnerton-Dyer-Polynom f mit den Nullstellen $\pm\sqrt{q} \pm \sqrt{r}$ mit möglichst geringem Aufwand explizit!

c) p sei eine weitere, von q und r verschiedene Primzahl. Zeigen Sie: Wenn $f^{(p)}$ in $\mathbb{F}_p$ eine Nullstelle hat, zerfällt es in $\mathbb{F}_p[X]$ in ein Produkt von Linearfaktoren.

d) Dies ist genau dann der Fall, wenn sowohl q als auch r modulo p Quadrate sind.

e) Falls weder q noch r modulo p Quadrate sind, läßt sich $f^{(p)}$ als ein Produkt der Form $(X^2 + a)(X^2 + b)$ schreiben.

f) Falls genau eine der beiden Primzahlen q und r modulo p ein Quadrat ist, läßt sich $f^{(p)}$ als ein Produkt der Form $(X^2 + aX + b)(X^2 - aX + b)$ schreiben.

Aufgabe 2:

Das Untergitter Γ von $\mathbb{Z}^2$ wird aufgespannt von den Vektoren $\binom{28}{6}$ und $\binom{13}{3}$.

a) Berechnen sie die Determinante $d(\Gamma)$!

b) Welche Schranke liefert die Ungleichung von Hadamard für $d(\Gamma)$?

c) Zeigen Sie, daß es in Γ keinen Vektor der Länge eins gibt!

d) Bestimmen Sie alle Vektoren aus Γ mit Länge höchstens drei!

e) Finden Sie eine Gitterbasis aus möglichst kurzen Vektoren, und wenden Sie die Ungleichung von Hadamard darauf an!

f) Zeigen Sie, daß es keine Gitterbasis aus aufeinander senkrecht stehenden Vektoren gibt!

Aufgabe 3:

a) Finden Sie eine Basis des Gitters $\Gamma = \left\{ \binom{x}{y} \in \mathbb{Z}^2 \;\middle|\; x \equiv y \bmod 2 \right\}$!

b) Finden Sie eine Basis des Gitters $\Lambda = \left\{ \binom{x}{y} \in \mathbb{Z}^2 \;\middle|\; x \equiv y \bmod 3 \right\}$!

c) Berechnen Sie die Determinanten $d(\Gamma)$ und $d(\Lambda)$!

Aufgabe 4:

a) Zeigen Sie: Für zwei beliebige teilerfremde ganze Zahlen $p, q \in \mathbb{Z}$ gibt es stets eine Gitterbasis von $\mathbb{Z}^2$, die den Vektor $\binom{p}{q}$ enthält.

b) Bilden $\binom{p}{q}$ und $\binom{p'}{q'}$ eine Gitterbasis von $\mathbb{Z}^2$, so ist $ggT(p, q) = ggT(p', q') = 1$.

c) Für jede reelle Zahl λ gibt es eine Gitterbasis von $\mathbb{Z}^2$, deren Basisvektoren beide mindestens die Länge λ haben.

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

Abgabe bis zum Mittwoch, dem 10. Mai 2023, um 15.30 Uhr