Prof. Friedrich Eisenbrand
Nicolai Hähnle

Discussions from: May 10, 2011

Computer Algebra

Spring 2011

Assignment Sheet 6

Exercises marked with a $\star$ can be handed in for bonus points. Due date is May 24.

Exercise 1

Let $f, g \in \mathbb{Z}[x]$ be two polynomials with $\|f\|_\infty, \|g\|_\infty \leq 2^s$ of degree at most d. Let $n = \max\{d, s\}$. Show that $fg \in \mathbb{Z}[x]$ can be computed in time $O(M(n) \cdot d \log d)$ using the Fast Fourier Transform, where $M(n)$ is the time required to multiply two n-bit numbers.

Exercise 2 ($\star$)

Let

$$B = (b_1, \ldots, b_{i-1}, b_i, b_{i+1}, b_{i+2}, \ldots, b_n)$$

and

$$C = (b_1, \ldots, b_{i-1}, b_{i+1}, b_i, b_{i+2}, \ldots, b_n)$$

be two lattice bases. Notice that C originates from B via swapping the i-th and $i+1$-st column. Prove that B^* and C^* only differ in the i-th and $i+1$-st column. Show further that $\|b_i^*\| \cdot \|b_{i+1}^*\| = \|c_i^*\| \cdot \|c_{i+1}^*\|$ holds. What does this imply for $\det(B)$ and $\det(C)$?

Exercise 3

Let $K \subseteq \mathbb{R}^n$ be a convex body of volume $\mathrm{vol}(K) \geq 2^n$ that is symmetric about the origin. Prove that K contains a nonzero integer point.

Exercise 4

Let $K \subseteq \mathbb{R}^n$ be a convex body of volume $\mathrm{vol}(K) \geq k \cdot 2^n$ that is symmetric about the origin. Prove that K contains at least $2k$ nonzero integer points.

Exercise 5

Let p be an odd prime. Prove that $(p-1)! \equiv -1 \pmod{p}$.

Exercise 6 ($\star$)

In this exercise you will prove that every prime number p with $p \equiv 1 \pmod 4$ can be written as the sum of two square numbers $p = a^2 + b^2$, for $a, b, \in \mathbb{N}$.

a) Show that the equation $q^2 \equiv -1 \pmod{p}$ has a solution.

   Hint: You can use the result of the previous exercise by contradiction, or you can look at the group structure in detail.

b) Consider the lattice Λ generated by $\left(\begin{smallmatrix} 1 & 0 \\ q & p \end{smallmatrix}\right)$ and the disk of radius $\sqrt{p \cdot 2 - \varepsilon}$ around 0 for a small $\varepsilon > 0$.

i) Show that $\|v\|^2$ is divisible by p for each $v \in \Lambda$.

ii) Show that there exists a $v \in \Lambda \setminus \{0\}$ with $\|v\|^2 = p$.

iii) Conclude that p is the sum of two squares.

c) Is there a prime p with $p \equiv 3 \pmod 4$ that can be written as the sum of two squares?