Dijana Kreso (kreso@math.tugraz.at)

Exercises in Number Theory MAT.413

Due: December 14, 2015

Graz University of Technology

1. A nonnegative integer n is a sum of two integer squares if and only if the prime divisors of n which are congruent to 3 modulo 4 have an even exponent in the prime factorization of n.

   Show that the above theorem holds by showing that:

   (a) (2 points) For a prime p such that $p \equiv 3 \pmod 4$, there does not exist $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \pmod p$, i.e. -1 is not a quadratic residue modulo p when $p \equiv 3 \pmod 4$.

   (b) (2 points) If n is a sum of two squares, then the prime divisors of n which are congruent to 3 modulo 4 have an even exponent in the prime factorization of n.

   (c) (2 points) If the prime divisors of n which are congruent to 3 modulo 4 have an even exponent in the prime factorization of n, then n is a sum of two squares.

   (Recall that in the fourth exercise sheet one of the problems was to prove that a prime $p \equiv 1 \pmod 4$ is a sum of two squares using Minkowski's first theorem).

2. (2 points) Using Minkowski's first theorem, show that Dirichlet's theorem holds, i.e. that for a real number α and a positive integer Q, there are integers p and q such that $0 < q \leq Q$ and

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}.$$

3. Let Δ be a lattice in $\mathbb{R}^n$ and $C \subseteq \mathbb{R}^n$ convex, closed, bounded, with 0 in its interior, and symmetric with respect to 0. For $\lambda \geq 0$ let $\lambda C := \{\lambda \mathbf{x} \colon \mathbf{x} = (x_1, \ldots, x_n) \in C\}$. Let $\|\mathbf{x}\|_C := \inf\{\lambda \in \mathbb{R}_{\geq 0} \colon \mathbf{x} \in \lambda C\}$.

   Minkowski's first theorem for convex bodies states that if $\mathrm{vol}(C) \geq 2^n \det(\Delta)$, then C contains a nonzero point of Δ. Minkowski's second theorem for convex bodies states that if $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the successive minima of C with respect to Δ (i.e. λ_i is the minimum of all $\lambda > 0$ s.t. λC contains at least i linearly independent vectors of Δ), then

$$\frac{2^n}{n!} \cdot \frac{\det \Delta}{\mathrm{vol}\, C} \leq \lambda_1 \lambda_2 \cdots \lambda_n \leq 2^n \frac{\det \Delta}{\mathrm{vol}\, C}.$$

   (a) (1 point) Show that $\lambda C = \{\mathbf{x} \in \mathbb{R}^n \colon \|\mathbf{x}\|_C \leq \lambda\}$ for $\lambda \geq 0$.

   (b) (2 points) Show that $\|\mathbf{x} + \mathbf{y}\|_C \leq \|\mathbf{x}\|_C + \|\mathbf{y}\|_C$ for $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, and conclude that $\|\cdot\|_C$ defines a norm on $\mathbb{R}^n$.

   (c) (2 points) Show that Minkowski's second theorem for convex bodies implies Minkowski's first theorem for convex bodies.

   Solve Problem 5 (a)–(d) of the third exercise sheet (that was due 16.11.) for extra points!

   Solve Problem 1 (c) of the fourth exercise sheet (that was due 30.11.) to earn the 2 points (crosses inserted into the table on 30.11. for the Problem 1 (c) do not count!).

   Please send the solutions of the above mentioned problems from earlier homeworks (not of this homework!) via e-mail, until December 13, 23:59 h.