Dijana Kreso (kreso@math.tugraz.at)

Exercises in Number Theory MAT.413

Due: November 30, 2015

Graz University of Technology

Note that there are two pages of this exercise sheet!

1. Recall that for any $a \in \mathbb{Q} \setminus \{0\}$, the number of solutions of the equation $u_1 + u_2 + \cdots + u_k = a$ in S-units u_i's, such that no zero subsum of $u_1 + u_2 + \cdots + u_k$ exists, is bounded by a constant independent of a.

   An n-tuple of distinct rational numbers $(a_1, a_2, \ldots, a_n)$ with $n > 2$ is said to be an S-cycle of size n if $a_i - a_j$ is an S-unit exactly when either i and j are consecutive integers, or $\{i, j\} = \{1, n\}$.

   (a) (1 point) Show that if $2 \notin S$, for odd n no S-cycle of size n exists.

   (b) (2 points) Show that there exists an S-cycle of size 4, and if $2 \in S$ an S-cycle of size 3 exists.

   (c) (2 points) Show that if $2 \in S$, then for any $n > 2$ there exists an S-cycle of size n, and if $2 \notin S$, then for any even $n > 2$ there exists an S-cycle of size n, by showing that we may always extend an S-cycle by 2.

2. Let $f(x) = \zeta_0 x^n + \cdots + \zeta_{n-1} x + \zeta_n = \zeta_0 (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \in \mathbb{C}[x]$. Let $M(f) = |\zeta_0| \cdot \prod_{i=1}^{n} \max\{1, |\alpha_i|\}$ be the Mahler measure of f (here $|\cdot|$ denotes the usual absolute value on $\mathbb{C}$).

   (a) (1 point) Show that $M(f) \geq 2^{-n} \max\{|\zeta_0|, \ldots, |\zeta_n|\}$.

   (b) (2 points) Show that for real $x \geq 1$

   $$\#\left\{\alpha \in \overline{\mathbb{Q}} : \deg \alpha \leq d, H(\alpha) \leq x\right\} \leq \sum_{n=1}^{d} n(5x)^{n(n+1)} \leq (8x)^{d(d+1)},$$

   that is, the number of algebraic numbers of degree at most d and of height at most x is bounded above by $(8x)^{d(d+1)}$.

   (Here for an algebraic number α of degree d, $H(\alpha)$ denotes the d-th root of the Mahler measure of the minimum polynomial of α).

3. Suppose $S \subseteq \mathbb{N}_0$, $\psi : \mathbb{N} \to \mathbb{N}_0$ and $Q_0 \in \mathbb{N}$ are such that

   $$\#\{s \in S : s \leq Q\} > \psi(Q) > 0 \quad \text{for} \quad Q \geq Q_0.$$

   Let $A = S - S := \{s_1 - s_2 : s_1, s_2 \in S\}$.

   (a) (2 points) Let $\alpha \in \mathbb{R}$ and $Q \in \mathbb{N}$ with $Q \geq Q_0$. Show that there exists $p \in \mathbb{Z}$ and $q \in A$ such that

   $$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\psi(Q) \cdot q} \quad \text{and} \quad 0 < q \leq Q.$$

   Hint: Split the interval $[0, 1]$ into $\psi(Q)$ intervals and apply Pigeonhole principle.

   (b) (1 point) Show that if $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and ψ is monotone increasing and unbounded, then

   $$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\psi(q) \cdot q}$$

   has infinitely many solutions $(p, q) \in \mathbb{Z} \times A$ with $q > 0$.

4. Let p be a prime number such that $p \equiv 1 \pmod 4$.

   (a) (1 point) Show that there exists an integer a such that $a^2 \equiv -1 \pmod p$.

   (b) (2 points) Use Minkowski's First theorem to show that there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

5. **(2 extra points)** Let $n \in \mathbb{N}$ and $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{R}$ and $Q > 1$. Use Minkowski's First Theorem to show that there exist $q, p_1, \ldots, p_n \in \mathbb{Z}$ such that

$$0 < q \leq Q \quad \& \quad |q\alpha_i - p_i| \leq Q^{-1/n} \quad \text{for } i = 1, 2, \ldots, n.$$