Prof. Friedrich Eisenbrand
Alfonso Cevallos

Discussions from: May 19, 2015

Computer Algebra

Spring 2015

Assignment Sheet 7

Exercises marked with a $\star$ can be handed in for bonus points. Because of the upcoming end of the semester, due date is May 26. *Remark:* If you hand in the homework by e-mail, make sure to type as subject "Computer Algebra HW7".

You can assume as known the following characterization of lattices: $\Lambda \subset \mathbb{R}^n$ is a lattice is and only if:

- It is an *additive subgroup* of $\mathbb{R}^n$: $0 \in \Lambda$, and for each $x, y \in \Lambda$, we have $x - y \in \Lambda$; and
- It is *discrete*: $\exists \epsilon > 0$ such that, for each $x \in \Lambda$, the ball centered at x with radius ϵ contains no lattice point other than x.

Exercise 1
Let $\Lambda \subset \mathbb{R}^n$ be a full-dimensional lattice and define the *dual lattice* $\Lambda^* = \{y \in \mathbb{R}^n \mid y^T x \in \mathbb{Z} \text{ for all } x \in \Lambda\}$.

1. Prove that Λ^* is a lattice, and that $(\Lambda^*)^* = \Lambda$.
2. Let B a basis of Λ. Prove that $(B^{-1})^T$ is a basis of Λ^*.
3. Let $y \in \Lambda^*$ be arbitrary, and consider the affine hyperplanes $H_k = \{x \in \mathbb{R}^n \mid y^T x = k\}$ for all $k \in \mathbb{Z}$. Prove that $\Lambda \subset \cup_{k \in \mathbb{Z}} H_k$.

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

1. Show that the equation $q^2 \equiv -1 \mod p$ has a solution.
2. Let Λ be the lattice generated by $\begin{pmatrix} 1 & 0 \\ q & p \end{pmatrix}$. Show that for each $v \in \Lambda$, $\|v\|^2$ is divisible by p.
3. Consider the disk centered at the origin of radius $\sqrt{2p - \epsilon}$, for some small $\epsilon > 0$. Show that that there exists a $v \in \Lambda \setminus \{0\}$ with $\|v\|^2 = p$.
4. Conclude that p is the sum of two squares.
5. Is there a prime $p \geq 3$, with $p \not\equiv 1 \mod 4$, that can be written as a sum of two squares?

Exercise 3
Let $K \subset \mathbb{R}^n$ be a convex and centrally-symmetric body of volume $\text{vol}(K) \geq k \cdot 2^n$. Prove that K contains at least $2k$ nonzero integer points.

Exercise 4
The Earth revolves around the sun in about $\alpha = 365.2422$ days. For a calendar to be synchronous with the seasons, it cannot define every year to have the same number of years: some years will have 365 days, and some 366, according to some rule (which should be simple enough). For instance, approximating α by $365 + 1/4$ gives the following rule: every year that is divisible by 4 has 366 days, every other year has 365 days. With this rule, the calendar will be off by one day in roughly 130 days. Can we do better, with a rule that is not too complicated?

1. Find the best fractional approximation p/q for α, such that $q \leq 40$. This is, find the positive numbers p and q that minimize the difference $|\alpha - p'/q'|$ over all numbers p', q' with $q' \leq 40$.

2. Describe a corresponding rule for an accurate calendar, and estimate the time it will take for the calendar to be off by one day.

3. The *k-convergent* of a positive irrational number $\beta > 1$ is a sequence of k positive integers, defined recursively as: an empy sequence if $k = 0$, and otherwise $\lfloor \beta \rfloor$ followed by the $k-1$ convergent of $\frac{1}{\beta - \lfloor \beta \rfloor}$. Prove that the 4-convergent of α is $(365, 4, 7, 1)$. What's the relation of this sequence with the approximation found in the first part?

Exercise 5
Let λ be the lattice generated by the basis B with columns $b_1 = (1\ 0\ 0)^T$, $b_2 = (4\ 2\ 15)^T$ and $b_3 = (0\ 0\ 3)^T$. Peform the LLL algorithm by hand. Hint: The final basis should be quite simple, with only non-negative entries of value at most 3.