MATH 7230 Homework 7 - Fall 2018

Due Wednesday, Nov. 7 at 1:30

https://www.math.lsu.edu/~mahlburg/teaching/2018F-MATH7230.html

You are required to turn in at least **one** of the following problems, and must complete a total of **20** by semester's end. Group work is allowed, but your solutions must be written up individually.

The notation "Ash A.B.C" means Problem C from Section A.B in the textbook.

Problems 1–3 illustrate another application of Minkowski's Convex Body Theorem. In particular, you will prove Fermat and Lagrange's theorems for primes representable as the sum of two or four squares.

1. Recall that if $p \equiv 1 \pmod 4$, then there is an integer a such that $a^2 \equiv -1 \pmod p$ (e.g. by Wilson's Theorem, or the fact that finite fields have cyclic multiplicative groups). Define the lattice $H := \langle (1,a),(0,p) \rangle_{\mathbb{Z}} \subset \mathbb{Z}^2$, or equivalently (following the slight abuse notation from lecture), $H = \mathbb{Z}^2 \cdot C$, where
$$C := \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix}.$$
   (a) Calculate $v(H)$ (i.e., the area of the fundamental parallelogram).
   (b) Show that if $(x,y) \in C$, then $x^2 + y^2 \equiv 0 \pmod p$.
   (c) For $t > 0$, define the ball
$$B_t := \left\{ (x,y) \in \mathbb{R}^2 \ \mid \ \sqrt{x^2+y^2} < t \right\}.$$
   Show that with $t = \sqrt{2p}$, $\mu(B_t) > v(H)$.
   (d) Finally, apply Minkowski's Convex Body Theorem (why does it apply?) to obtain the existence of a point $0 \neq (x,y) \in B_t \cap H$. Argue that this point must satisfy $x^2 + y^2 = p$!

2. Now consider the primes p representable as the sum of four squares. Without loss of generality, let p be odd (why?). Note that for sums of two squares, Problem 1 began from one specially chosen square modulo p. Here you will began with **two** specially chosen squares.
   (a) Let $S := \{a^2 \bmod p \ \mid \ a \in \mathbb{Z}\}, S' := \{-1 - b^2 \bmod p \ \mid \ b \in \mathbb{Z}\}$. Show that S and S' both contain exactly $\frac{p+1}{2}$ residues. Conclude that $S \cap S' \neq \emptyset$, so that there are integers a and b such that $a^2 + b^2 \equiv -1 \pmod p$.
   (b) Now define the lattice $H := Z^4 \cdot C$, where
$$C := \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ a & b & 1 & 0 \\ b & -a & 0 & 1 \end{pmatrix}.$$
   Prove that if $(x_1,x_2,x_3,x_4) \in H$, then $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod p$.

(c) Calculate the volume $v(H)$.

3. (a) For $t > 0$, define the ball

$$B_t := \{\vec{x} = (x_1, x_2, x_3, x_4) \in \mathbb{R}_4 \mid \|\vec{x}\| < t\},$$

where $\|\cdot\|$ is the usual Euclidean norm. Explain why B_t is symmetric and convex.

(b) Find the volume of B_t (a four-dimensional hypersphere). You may use any references that you like, but if you have never derived the volume of an n-dimensional hypersphere, I encourage you to try!

(c) With $t = \sqrt{2p}$, show that $\mu(B_t) > 16v(H)$

(d) Apply Minkowski's Theorem, and conclude that there is an integer 4-tuple such that $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$.

4. Bell 6.3.1. Do only the cases with $m \leq 13$.