

Math 784
Homework 5

Due Thursday, May 8.

Problems:

1. Marcus §5, #28 a,b.
2. Marcus §5, #35 a,b,c.
3. Do at least one of Marcus §5, #36, #37.
4. Let p be prime. In this problem, we will use Minkowski's Convex Body Theorem to show that there exists $(a, b, c, d) \in \mathbb{Z}^4$ with $p = a^2 + b^2 + c^2 + d^2$. It follows from basic facts on Hamilton's quaternions that this statement continues to hold with p replaced by an arbitrary integer $n > 0$. This is Lagrange's Four Squares Theorem.

(a) Let p be an odd prime number. Show that there exists $(u, v) \in \mathbb{Z}^2$ with

$$u^2 + v^2 \equiv -1 \pmod{p}.$$

(Compare the sizes of $\{u^2 : u \in \mathbb{Z}/p\mathbb{Z}\}$ and $\{-1 - v^2 : v \in \mathbb{Z}/p\mathbb{Z}\}$).

(b) Fix u and v as in (a). Let

$$L = \{(a, b, c, d) \in \mathbb{Z}^4 : c \equiv ua + vb \pmod{p}, d \equiv ub - va \pmod{p}\}.$$

Show that L is a rank 4 lattice in \mathbb{R}^4 with $\text{vol}(\mathbb{R}^4/L) = p^2$. It may help to rewrite L as

$$L = \{(a, b, ua + vb + pk, ub - va + pl) : a, b, k, l \in \mathbb{Z}\}.$$

- (c) Let $r > 0$. Compute the volume of a sphere $S_r = \{(w, x, y, z) \in \mathbb{R}^4 : w^2 + x^2 + y^2 + z^2 < r^2\}$ in \mathbb{R}^4 or radius $r > 0$. Note that S is bounded, symmetric, and convex.
 - (d) Use parts (a), (b), and (c) together with Minkowski's Convex Body Theorem to show that there exists $(a, b, c, d) \in \mathbb{Z}^4$ with $p = a^2 + b^2 + c^2 + d^2$. (Choose an appropriate value of r in terms of p in part (c) so that you can easily compare $\text{vol}(S_r)$ with $2^4 \text{vol}(\mathbb{R}^4/L)$. What does this tell you?)
5. Do at least one of Marcus, §8, #21, #24a, #24b. (Problems on Hilbert class fields).