

HOMEWORK ASSIGNMENT # 6  
Due Tuesday, October 22

In this exercise set, you should use the following theorem of Minkowski, which we will prove in class:

**Theorem:** Let  $K$  be a number field. Then every ideal class in  $\mathcal{O}_K$  contains a nonzero ideal of norm at most  $M_K$ , where

$$M_K := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}.$$

is *Minkowski's constant*.

1. Let  $K = \mathbf{Q}(\sqrt{-6})$ . Determine which rational primes  $p$  split, ramify, and remain inert in  $K$ . Your answer should be expressed in terms of congruence conditions on  $p$ . (**Hint:** Use quadratic reciprocity.)
2. Let  $p$  be an odd prime number. Use Minkowski's Convex Body Theorem to give a proof of Fermat's theorem that  $p$  can be written in the form  $a^2 + b^2$  for some integers  $a, b$  if and only if  $p \equiv 1 \pmod{4}$ . (**Hint:** Suppose  $p \equiv 1 \pmod{4}$ , and fix an integer  $u$  such that  $u^2 \equiv -1 \pmod{p}$ . Let  $L \subset \mathbf{Z}^2$  be the subset of  $\mathbf{R}^2$  consisting of all pairs  $(a, b)$  of integers such that  $b \equiv ua \pmod{p}$ . Show that  $L$  is a lattice, and determine its covolume. Now prove Fermat's theorem by showing that there exists a nonzero point  $(a, b) \in L$  for which  $a^2 + b^2 < 2p$ .)
3. Our goal in this problem is to use geometry of numbers to prove the theorem of Lagrange which says that every positive integer can be written as the sum of four integer squares.
  - a. Let  $p$  be an odd prime number. Show that the congruence  $u^2 + v^2 \equiv -1 \pmod{p}$  has a solution in integers  $u, v$ .
  - b. Fix  $u, v$  as in part (a). Let  $L$  be the subset of  $\mathbf{Z}^4$  consisting of all  $(a, b, c, d)$  such that  $c \equiv ua + vb \pmod{p}$  and  $d \equiv ub - va \pmod{p}$ . Show that  $L$  is a lattice in  $\mathbf{R}^4$  and compute its volume.

- c. Compute the volume of a sphere of radius  $r$  in  $\mathbf{R}^4$ .
  - d. Prove that  $p$  can be written as a sum of 4 integer squares.
  - e. A *quaternion* is an expression of the form  $a + bi + cj + dk$ , where  $i, j, k$  are formal symbols satisfying  $i^2 = j^2 = k^2 = -1$  and  $ij = -k$ . Quaternions can be added componentwise (like complex numbers). They can also be multiplied, but unlike with complex numbers, multiplication of quaternions is associative but not commutative. If  $z = a + bi + cj + dk$  is a quaternion, its conjugate  $\bar{z}$  is given by  $a - bi - cj - dk$ . Show that  $z\bar{z}$  is always a positive real number, so that we can define the norm of  $z$  to be  $\sqrt{z\bar{z}}$ . Prove that the norm of a product of two quaternions is the product of their norms.
  - f. Use parts (d) and (e) to show that every integer can be written as a sum of four squares.
4. Prove that  $\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$  is a PID which is not a Euclidean domain.
  5. Determine the ideal class group of  $\mathbf{Z}[\sqrt[3]{2}]$ .
  6. Determine the ideal class groups (not just their orders) of:
    - a.  $\mathbf{Z}[\sqrt{-14}]$ .
    - b.  $\mathbf{Z}[\sqrt{-21}]$ .