E. Dummit's Math 4527 ∼ Number Theory 2, Fall 2022 ∼ Homework 9, due Sun Nov 13th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Identify all pages containing each problem when submitting the assignment.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. For each quadratic integer ring (i) identify the value given by the Minkowski bound, (ii) find the splitting of all prime ideals up to the Minkowski bound, and (iii) determine the structure of the ideal class group:
   (a) $\mathbb{Z}[\sqrt{3}]$.
   (b) $\mathcal{O}_{\sqrt{13}}$.
   (c) $\mathbb{Z}[\sqrt{-6}]$.
   (d) $\mathbb{Z}[\sqrt{14}]$.
   (e) $\mathcal{O}_{\sqrt{-163}}$.
   (f) $\mathcal{O}_{\sqrt{-23}}$. [Hint: Show I_2^3 and $I_2 I_3$ are both principal.]

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

2. The goal of this problem is to prove the slightly sharper version of Minkowski's theorem for closed sets.
   (a) Suppose S is a closed subset of n-measure 1 inside $[0,1]^n$. Prove that $S = [0,1]^n$. [Hint: Consider the complement of S.]
   (b) Suppose S is a closed, bounded, measurable set in $\mathbb{R}^n$ whose n-measure is equal to 1. Show that there exist two points x and y in S such that $x - y$ has integer coordinates.
   (c) Suppose B is a convex closed set in $\mathbb{R}^n$ that is symmetric about the origin and whose n-measure is $\geq 2^n$. Prove that B contains a nonzero point all of whose coordinates are integers.

---

3. Suppose that α and β are real numbers and that N is a positive integer.
   (a) Find the volume of the region $(x, y, z) \in \mathbb{R}^3$ with $|x| \leq N$, $|\alpha x - y| \leq 1/\sqrt{N}$, $|\beta x - z| \leq 1/\sqrt{N}$.
   (b) Show there exist integers p, q, r with $1 \leq r \leq N$ such that $|\alpha - p/r|$ and $|\beta - q/r|$ are both at most $\dfrac{1}{r^{3/2}}$.
   - Remark: The idea of (b) is that we can provide simultaneous approximations to the real numbers α and β using a shared denominator r such that the approximation error is small relative to the shared denominator r.

---

4. Suppose $A = \{a_{i,j}\}_{1 \leq i,j \leq n}$ is a real $n \times n$ matrix whose determinant is not zero.
   (a) If $\lambda_1, \lambda_2, \ldots, \lambda_n$ are positive real numbers such that $\lambda_1 \lambda_2 \cdots \lambda_n \geq |\det A|$, prove that there exist integers $x_1, x_2, \ldots, x_n$, not all zero, such that $|a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n| \leq \lambda_1$, $|a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n| \leq \lambda_2$, ... , and $|a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,n}x_n| \leq \lambda_n$.
   (b) Show that there exist nonzero integers a and b such that $\left|a\sqrt{3} + b\sqrt{22}\right|$ and $\left|a\sqrt{23} + 13b\right|$ are both less than $\dfrac{1}{\sqrt[4]{2024}}$. [Hint: Use (a).]

---

5. The goal of this problem is to give a geometric method for analyzing $\mathbb{Z}[i]/(\beta)$ for a nonzero $\beta \in \mathbb{Z}[i]$.

   (a) Show that the ideal (β) forms a sublattice of the Gaussian integer lattice inside $\mathbb{C}$, and compute the area of its fundamental domain. [Hint: It is spanned by β and $i\beta$.]

   (b) Show that the number of residue classes in $\mathbb{Z}[i]/(\beta)$ is equal to the total number of interior points I, plus half of the number of boundary points B, minus one, inside the fundamental domain. [Hint: The boundary points come in pairs, except for the four corners.]

   (c) Deduce that the number of distinct residue classes in $\mathbb{Z}[i]$ modulo β is equal to $N(\beta)$. [Hint: Use Pick's theorem to put (a) and (b) together.]

   (d) Let $\beta = 3 + i$. Draw a fundamental region for $\mathbb{Z}[i]/(\beta)$, and use it to find an explicit list of residue class representatives for $\mathbb{Z}[i]/(\beta)$.

   (e) Does this method also work for $\mathcal{O}_{\sqrt{D}}/I$ for a general nonzero ideal I of $\mathcal{O}_{\sqrt{D}}$? [Hint: Yes, with the right way to view I as a lattice.]

---

6. Suppose D is a squarefree integer congruent to 2 or 3 modulo 4. As you showed on homework 7, the prime 2 ramifies in $\mathcal{O}_{\sqrt{D}}$, so that $(2) = P^2$ for a prime ideal P.

   (a) Suppose $D < -2$. Show that P is not a principal ideal. [Hint: Consider the norm of a generator.]

   (b) Suppose $D < -2$. Show that the class number of $\mathcal{O}_{\sqrt{D}}$ is even.

   (c) Now suppose that $D > 2$ and that D is divisible by a prime congruent to 5 modulo 8. Show again that the class number of $\mathcal{O}_{\sqrt{D}}$ is even.

---

7. [Challenge] Suppose I is a nonzero ideal of $R = \mathcal{O}_{\sqrt{D}}$. The goal of this problem is to show that R/I is finite and its cardinality is $N(I)$. (Indeed, $N(I)$ is often just defined to be the cardinality of R/I, rather than as the principal generator of $I \cdot \overline{I}$.)

   (a) Suppose I has prime ideal factorization $I = P_1^{a_1} \cdots P_n^{a_n}$. Show that R/I is isomorphic to $(R/P_1^{a_1}) \times \cdots \times (R/P_n^{a_n})$ and that $N(I) = N(P_1^{a_1}) \cdots N(P_n^{a_n})$.

   (b) Suppose a is any positive integer. Show that the cardinality of $R/(a)$ is a^2.

   (c) Suppose $Q = P^n$ is a power of a prime ideal. If $P = (p)$ for a prime integer p, show that $\#(R/Q) = N(Q)$.

   (d) Suppose $Q = P^n$ for some prime ideal P with $P\overline{P} = (p)$ and p prime; note that we are *not* assuming that $\overline{P} \neq P$. Show that all of the quotients R/P, P/P^2, ... , P^{n-1}/P^n, $P^n/(P^n\overline{P})$, ... , $(P^n\overline{P}^{n-1})/(P^n\overline{P}^n)$ have cardinality greater than 1, and that the product of their cardinalities is the cardinality of $R/(P^n\overline{P}^n)$. Conclude that all of these cardinalities must equal p and deduce that $\#(R/Q) = N(Q)$.

   (e) Show that R/I has cardinality $N(I)$ for any nonzero ideal I.
