E. Dummit's Math 4527 $\sim$ Number Theory 2, Spring 2024 $\sim$ Homework 9, due Fri Mar 22nd.

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. (a) Express 46, 57, 88, and 114 as the sum of three squares.
   (b) Express 87, 135, 2023, and 2024 as the sum of four squares.

---

2. 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.

3. The goal of this problem is to discuss runs of consecutive integers none of which are the sum of 2 or 3 squares.
   (a) For any positive integer k, show that there exist k consecutive positive integers none of which are the sum of two squares. [Hint: Take $N \equiv 3 \pmod 9$, $N + 1 \equiv 7 \pmod{49}$, etc.]
   (b) Show that of any 3 consecutive positive integers, at least one is the sum of three squares.
   (c) Find an example of 2 consecutive positive integers neither of which is the sum of three squares.

---

4. 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.

---

5. 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 r.

---

6. 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) 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 $\mathbb{Z}[i]/(\beta)$.

   (c) 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.]

   (d) 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.]

   (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.]

---

7. The goal of this problem is to show that $\mathcal{O}_{\sqrt{-19}}$ is a PID that is not Euclidean. If R is an integral domain, we say an element $u \in R$ is a universal side divisor if it is not zero, not a unit, and every $x \in R$ can be written in the form $x = qu + z$ where z is either zero or a unit. Equivalently, u is a universal side divisor when every nonzero residue class modulo u is represented by a unit of R.

   (a) Suppose R is a Euclidean domain that is not a field. If u is a nonzero nonunit of R having minimal norm among nonzero nonunits in R (with respect to the norm function on R), show that u is a universal side divisor.

   (b) If u is a universal side divisor in $\mathcal{O}_{\sqrt{-19}}$, show that u must divide one of $x-1$, x, $x+1$ for any $x \in R$.

   (c) Show that $\mathcal{O}_{\sqrt{-19}}$ has no universal side divisors and conclude that $\mathcal{O}_{\sqrt{-19}}$ is not Euclidean. [Hint: Apply (b) when $x = 2$ and $x = (1+\sqrt{-19})/2$, and compute norms.]

   (d) Show that $\mathcal{O}_{\sqrt{-19}}$ has trivial class group. Deduce that $\mathcal{O}_{\sqrt{-19}}$ is a PID that is not Euclidean.

---

8. [Challenge] The goal of this problem is to give a proof using Minkowski's theorem of the Diophantine approximation theorem we established using continued fractions: that for any irrational real number α there exist infinitely many rationals p/q with $|\alpha - p/q| < \frac{1}{2}q^{-2}$.

   (a) Suppose $A = \{a_{i,j}\}_{1 \le i,j \le n}$ is a real $n \times n$ matrix whose determinant is not zero. If $\lambda_1, \lambda_2, \ldots, \lambda_n$ are positive real numbers such that $\lambda_1 \lambda_2 \cdots \lambda_n \ge |\det A|$, prove that there exist integers $x_1, x_2, \ldots, x_n$, not all zero, such that $|a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n| \le \lambda_1$, $|a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n| \le \lambda_2$, ... , and $|a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,n}x_n| \le \lambda_n$.

   (b) Suppose that a, b, c, d are real numbers such that $ad - bc \ne 0$. Show that there exist integers p, q not both zero such that $|ap + bq| \cdot |cp + dq| \le \dfrac{1}{2}|ad - bc|$ and $|ap + bq|, |cp + dq| \le \sqrt{2\,|ad - bc|}$. [Hint: Apply (a) to the forms $(ax + by) \pm (cx + dy)$, then use the triangle inequality and the arithmetic-geometric mean inequality.]

   (c) Let α be a real number and fix a positive real number t. Show that there exist integers p, q not both zero such that $\left|pq - \alpha q^2\right| \le \dfrac{1}{2}$ and with $|tp - \alpha tq| \le \sqrt{2}$. [Hint: Use (b) with $a = t$, $b = -\alpha t$.]

   (d) Let α be an irrational real number. Show that there exist infinitely many rational numbers p/q such that $|\alpha - p/q| < \dfrac{1}{2}q^{-2}$. [Hint: For any finite N, choose t large enough so that $|p - \alpha q| > \sqrt{2}/t$ whenever $q \le N$.]
