E. Dummit's Math 4527 ~ Number Theory 2, Spring 2025 ~ Homework 7, due Tue Feb 25th.

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. Find the prime ideal factorizations of each ideal in the given quadratic integer ring:
   (a) The ideals (2), (3), (5), and (7) in $\mathcal{O}_{\sqrt{-5}} = \mathbb{Z}[\sqrt{-5}]$.
   (b) The ideals (2), (3), (5), and (7) in $\mathcal{O}_{\sqrt{6}} = \mathbb{Z}[\sqrt{6}]$.
   (c) The ideals (2), (3), (5), and (7) in $\mathcal{O}_{\sqrt{-11}} = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$.

---

2. Solve the following problems related to factorization:
   (a) Find prime factorizations of $12+31i$, $183-12i$, $75-11i$, and $28-4i$ in $\mathbb{Z}[i]$.
   (b) Find representations of the primes 2909 and 8161 as the sum of two squares of integers.
   (c) Find prime factorizations for $70+60\sqrt{-2}$, $49-46\sqrt{-2}$, and 193 in $\mathbb{Z}[\sqrt{-2}]$.
   (d) Find prime factorizations for $70+60\sqrt{-3}$, $48+46\sqrt{-3}$, and 193 in $\mathcal{O}_{\sqrt{-3}}$.
   (e) Determine whether the integers 117, 263, and 950 can be written in the form a^2+b^2 for integers a, b.
   (f) Determine whether the integers 117, 263, and 950 can be written in the form a^2+2b^2 for integers a, b.
   (g) Determine whether the integers 117, 263, and 950 can be written in the form a^2+3b^2 for integers a, b.

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

3. Let $R = \mathbb{Z}[\sqrt{-14}]$, and let $I_3 = (3, 1+\sqrt{-14})$, $I_3' = (3, 1-\sqrt{-14})$, $I_5 = (5, 1+\sqrt{-14})$, and $I_5' = (5, 1-\sqrt{-14})$.
   (a) Show that the elements 3, 5, and $1 \pm \sqrt{-14}$ are nonassociate irreducible elements of R, and that 15 has two inequivalent factorizations into irreducible elements in R. Deduce that R is not a UFD or a PID.
   (b) Show that I_3 and I_3' are both prime ideals of R and that $I_3 I_3'$ is the principal ideal (3). [Hint: Show that R/I_3 and R/I_3' both have 3 residue classes and then invoke problem 3 of homework 6.]
   (c) Show that I_5 and I_5' are both prime ideals of R and that $I_5 I_5'$ is the principal ideal (5).
   (d) Show that $I_3 I_5 = (1+\sqrt{-14})$ and $I_3' I_5' = (1-\sqrt{-14})$. Conclude that the two factorizations of 15 from part (a) yield the same factorization of the ideal (15) as a product of prime ideals.
   (e) Repeat (a)-(d) with the factorization $14 = 2 \cdot 7 = \sqrt{-14} \cdot (-\sqrt{-14})$ by showing that $I_2 = (2, \sqrt{-14})$ and $I_7 = (7, \sqrt{-14})$ are both prime, that $I_2^2 = (2)$, $I_2 I_7 = (\sqrt{-14})$, $I_7^2 = (7)$, and that $(14) = I_2^2 I_7^2$.

---

4. Let D be a squarefree integer not equal to 1. The discriminant of the quadratic integer ring $\mathcal{O}_{\sqrt{D}}$ is defined to be the discriminant of the minimal polynomial $m(x)$ of the generator of $\mathcal{O}_{\sqrt{D}}$. Recall that for a quadratic polynomial ax^2+bx+c, the discriminant is b^2-4ac.
   (a) Find the discriminant of $\mathcal{O}_{\sqrt{D}}$ in terms of D (note that there will be two cases, depending on whether $D \equiv 1 \pmod 4$ or not).
   (b) Show that the integer prime p is ramified in $\mathcal{O}_{\sqrt{D}}$ (i.e., its prime ideal factorization has a repeated factor) if and only if p divides the discriminant of $\mathcal{O}_{\sqrt{D}}$. [Hint: When does a quadratic have a repeated root?]
   (c) Identify the ramified primes in $\mathcal{O}_{\sqrt{D}}$ for $D = -1$, -2, 5, 6, -10, and 21, and give their prime ideal factorizations.

---

5. Recall that you proved on homework 6 that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain, hence also a PID and a UFD. Recall also that the Legendre symbol $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, so that 2 is a quadratic residue modulo an odd prime p precisely when $p \equiv 1$ or 7 (mod 8).

   (a) Show that every nonzero element in $\mathbb{Z}[\sqrt{2}]$ is associate to one having positive norm.

   (b) Prove that the prime elements in $\mathbb{Z}[\sqrt{2}]$, up to associates, are as follows:

      i. The element $2 + \sqrt{2}$, of norm 2.

      ii. The primes p congruent to 3 or 5 modulo 8, of norm p^2.

      iii. The two conjugate factors $a + b\sqrt{2}$ and $a - b\sqrt{2}$ where $p = a^2 - 2b^2$ is a prime congruent to 1 or 7 modulo 8, of norm p.

   (c) Find the irreducible factorizations of $10 + \sqrt{2}$ and of $345 + 15\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$.

   (d) Let n be a positive integer, and write $n = 2^k p_1^{n_1} \cdots p_k^{n_k} q_1^{m_1} \cdots q_d^{m_d}$, where $p_1, \cdots, p_k$ are distinct primes congruent to 1 or 7 modulo 8 and $q_1, \cdots, q_d$ are distinct primes congruent to 3 or 5 modulo 8. Prove that n can be written in the form $a^2 - 2b^2$ for some integers a and b if and only if all of the m_i are even.

---

6. [Challenge] The goal of this problem is to formulate the notions of gcd and lcm for ideals. Let R be an integral domain and A, B be ideals of R. We say an ideal K is a common divisor of A and B when $K|A$ and $K|B$, and K is a greatest common divisor when any other common divisor of A, B also divides K. We say an ideal E is a common multiple of A and B when $A|E$ and $B|E$, and E is a least common multiple when any other common multiple of A, B is also divisible by E.

   (a) If R is a PID, show that (d) is a greatest common divisor of (a) and (b) if and only if d is a gcd of a and b. Deduce that the greatest common divisor of ideals I and J is the sum $I + J$.

   (b) If R is a PID, show that (l) is a least common multiple of (a) and (b) if and only if l is an lcm of a and b. Deduce that the least common multiple of ideals I and J is the intersection $I \cap J$.

   The goal now is to show that the formulas $\gcd(I, J) = I + J$ and $\mathrm{lcm}(I, J) = I \cap J$ also hold in quadratic integer rings. So let $R = \mathcal{O}_{\sqrt{D}}$ be a quadratic integer ring and I and J be ideals of R.

   (c) Show that an ideal K is a common divisor of I and J if and only if K contains both I and J. Deduce that $\gcd(I, J) = I + J$.

   (d) Show that an ideal K is a common multiple of I and J if and only if K is contained in both I and J. Deduce that $\mathrm{lcm}(I, J) = I \cap J$.

   (e) Suppose I and J have prime ideal factorizations $I = P_1^{i_1} \cdots P_k^{i_k}$ and $J = P_1^{j_1} \cdots P_k^{j_k}$ for distinct prime ideals $P_1, \ldots P_k$. Show that $I + J = P_1^{\min(i_1, j_1)} \cdots P_k^{\min(i_k, j_k)}$ and $I \cap J = P_1^{\max(i_1, j_1)} \cdots P_k^{\max(i_k, j_k)}$.
