E. Dummit's Math 4527 ~ Number Theory 2, Fall 2022 ~ Homework 7, due Fri Oct 28th.

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. The goal of this problem is to prove that for any squarefree integer $D \geq 3$, the ring $\mathbb{Z}[\sqrt{-D}]$ is not a unique factorization domain, generalizing the technique used for $D = 5$.
   (a) Show that $\sqrt{-D}$, $1 + \sqrt{-D}$, $1 - \sqrt{-D}$, and 2 are irreducible elements in $\mathbb{Z}[\sqrt{-D}]$. [Hint: For the first three, show that the only elements of norm less than D are integers.]
   (b) Show that either D (if D is even) or $D+1$ (if D is odd) has two different factorizations into irreducibles in $\mathbb{Z}[\sqrt{-D}]$, and deduce that $\mathbb{Z}[\sqrt{-D}]$ is not a unique factorization domain.
   (c) What goes wrong if you try to use the proof to show that $\mathbb{Z}[\sqrt{D}]$ is not a UFD for squarefree $D \geq 3$?

---

4. 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 $(14) = I_2^2 I_7^2$.

---

5. 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.

---

6. [Challenge] Let $R = \mathbb{Z}[\sqrt{-3}]$ and let $I = (2, 1 + \sqrt{-3})$ in R.

   (a) Show that $I^2 = (2)I$ in R but that $I \neq (2)$.

   (b) Show that there are two residue classes in R/I and deduce that I is a prime ideal.

   (c) Show that I is the unique proper ideal of R properly containing (2) and also the unique prime ideal of R containing (2). [Hint: Consider the ideals of $R/(2)$ and use the correspondence between ideals of R containing J and ideals of R/J.]

   (d) Show that (2) cannot be written as a product of prime ideals of R.

   - Remark: This problem illustrates that factorization into prime ideals can fail if we do not work in the full quadratic integer ring. Working in the correct ring $\mathcal{O}_{\sqrt{-3}} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ will solve the issues that arise in this example, since in fact $I = (2)$ is a prime ideal inside $\mathcal{O}_{\sqrt{-3}}$ because 2 and $1 + \sqrt{-3}$ are now associates.
