E. Dummit's Math 4527 ~ Number Theory 2, Spring 2021 ~ Homework 11, due Thu Apr 8th.

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. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

---

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

1. Do:
   (a) Find prime factorizations for $70 + 60\sqrt{-2}$, $49 - 46\sqrt{-2}$, and 193 in $\mathbb{Z}[\sqrt{-2}]$.
   (b) Find prime factorizations for $70 + 60\sqrt{-3}$, $48 + 46\sqrt{-3}$, and 193 in $\mathcal{O}_{\sqrt{-3}}$.
   (c) Determine whether the integers 117, 263, and 950 can be written in the form $a^2 + 2b^2$ for integers $a, b$.
   (d) Determine whether the integers 117, 263, and 950 can be written in the form $a^2 + 3b^2$ for integers $a, b$.

---

2. 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 $\mathcal{O}_{\sqrt{D}}$.
   (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.

---

3. Find all solutions to the Diophantine equation $x^2 + y^2 = z^7$ where $x$ and $y$ are relatively prime.

---

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

4. Recall that you proved on homework 9 that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain, hence also a PID and a UFD. Recall also that $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
   (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.

---

5. The goal of this problem is to explore some results about integers of the form $x^2 + Dy^2$.

   (a) Prove that if an integer $n$ can be written in the form $x^2 + y^2$ for rational numbers $x, y$ then it can be written in that form for integers $x, y$. (For example, $5 = (22/13)^2 + (19/13)^2 = 2^2 + 1^2$.)

   (b) Prove that the result of part (a) also holds for integers that are of the form $x^2 + 2y^2$ or of the form $x^2 + 3y^2$.

   (c) Give a counterexample to the result of part (a) for integers that are of the form $x^2 + 14y^2$.

---

6. Prove that the only solution to the Diophantine equation $y^2 = x^3 - 8$ is $(x, y) = (0, 2)$. [Hint: There are two different cases according to whether $y$ is even or odd.]

---

7. 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 $I$.

---