E. Dummit's Math 4527 ~ Number Theory 2, Fall 2022 ~ Homework 6, due Fri Oct 21st.

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. In each given quadratic integer ring, determine which of the given elements are units, which are irreducible, and which are reducible. Also, for the units, compute their multiplicative inverses, and for the reducible elements find a nontrivial factorization.

   (a) $R = \mathbb{Z}[i]$, elements $4 - i$, $3 + i$, $3 - 2i$, 7.

   (b) $R = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$, elements $\dfrac{1+\sqrt{-3}}{2}$, $2 + \sqrt{-3}$, $3 + \sqrt{-3}$, $\dfrac{5+\sqrt{-3}}{2}$.

   (c) $R = \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, elements $2 + \sqrt{5}$, $3 - 2\sqrt{5}$, $7 + 5\sqrt{5}$, $1 + \sqrt{5}$.

   (d) $R = \mathcal{O}_{\mathbb{Q}(\sqrt{7})}$, elements $2 - \sqrt{7}$, $3 + \sqrt{7}$, $1 + \sqrt{7}$, $8 - 3\sqrt{7}$.

---

2. For each pair of elements a, b in the given Euclidean domain R, find a greatest common divisor d and write it in the form $d = ax + by$ for some $x, y \in R$. (You may wish to work through problems 5 and 6 before doing parts (c), (d), and (e).)

   (a) $R = \mathbb{Z}[i]$, $a = 57 + 17i$, $b = 26 + 22i$.

   (b) $R = \mathbb{Z}[i]$, $a = 9 + 43i$, $b = 22 + 10i$.

   (c) $R = \mathbb{Z}[\sqrt{-2}]$, $a = 33 + 5\sqrt{-2}$, $b = 8 + 11\sqrt{-2}$.

   (d) $R = \mathbb{Z}[\sqrt{2}]$, $a = 31 + 15\sqrt{2}$, $b = 10 + \sqrt{2}$.

   (e) $R = \mathcal{O}_{\sqrt{-3}}$, $a = 19 + \sqrt{-3}$, $b = 14 + 7\sqrt{-3}$.

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

3. Suppose R is a finite ring with $1 \neq 0$. If R has a prime number of elements p, show that R is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a ring. [Hint: Use Lagrange's theorem on the additive group of R to show 1 has additive order p, then use the first isomorphism theorem.]

---

4. Show that the rings $(\mathbb{Z}/15\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$ and $(\mathbb{Z}/24\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ are isomorphic.

---

5. Let $R = \mathbb{Z}[\sqrt{-2}]$, and let $a + b\sqrt{-2}$ and $c + d\sqrt{-2}$ be elements of R with $c + d\sqrt{-2} \neq 0$.

   (a) Show that $\dfrac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = x + y\sqrt{-2}$ for rational x, y. Then let s be the closest integer to x and t be the closest integer to y, and set $q = s + t\sqrt{-2}$ and $r = (a + b\sqrt{-2}) - (s + t\sqrt{-2})(c + d\sqrt{-2})$. Prove also that $N(r) \leq \dfrac{3}{4} N(c + d\sqrt{-2})$.

   (b) Show that R is a Euclidean domain.

   (c) Show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are also Euclidean domains under the absolute value of the field norm $\left|N(a + b\sqrt{D})\right| = \left|a^2 - Db^2\right|$.

---

6. The goal of this problem is to prove that $\mathcal{O}_{\sqrt{-D}}$ is a Euclidean domain for $-D = -3$, -7, and -11, which extends the result of problem 4 (establishing this fact for $-D = -2$, 2, and 3).

   (a) Suppose ABC is a triangle. Show that the point P inside ABC that maximizes the distance to the nearest vertex of ABC is the circumcenter (i.e., the center of the circle through the vertices of ABC, or equivalently, the point O such that $OA = OB = OC$).

   (b) Suppose that $-D = -3$, -7, or -11. Prove that any complex number $z \in \mathbb{C}$ differs from an element in $\mathcal{O}_{\sqrt{-D}}$ by a complex number whose norm (i.e., the square of its absolute value) is at most $\frac{(1+D)^2}{16D}$. [Hint: The elements of $\mathcal{O}_{\sqrt{-D}}$ form a lattice Λ in the complex plane. Identify a fundamental region for this lattice and then use symmetry to reduce the minimal distance calculation to part (a).]

   (c) Prove that $\mathcal{O}_{\sqrt{-D}}$ is a Euclidean domain for $-D = -3$, -7, and -11. [Hint: Adapt the proof in 5b.]

---

7. [Challenge] Let F be a field and define $R = F[\epsilon]/(\epsilon^2)$, a ring known as ring of dual numbers over F. Intuitively, one can think of the element $\epsilon \in R$ as being like an "infinitesimal": a number so small that its square is zero.

   (a) Show that the zero divisors in R are the elements of the form $b\epsilon$ with $b \neq 0$, and the units in R are the elements of the form $a + b\epsilon$ with $a \neq 0$.

   (b) Find all the ideals of R. (There are three.)

   (c) Let $p(x) \in F[x]$. Show that $p(x + \epsilon) = p(x) + \epsilon p'(x)$ in $R[x]$, where $p'(x)$ denotes the derivative of $p(x)$.

   (d) Let $p(x), q(x) \in F[x]$ and set $P(x) = p(x)q(x)$. Show that $P'(x) = p'(x)q(x) + p(x)q'(x)$. [Hint: Use (c).]

   - Remark: Part (c) shows how to use dual numbers to give a purely algebraic way to compute the derivative of a polynomial (in fact, some computer systems actually do differentiation this way), and (d) illustrates that they yield a formal proof of the product rule. In fact, the dual numbers are essentially the same object used in the construction of cotangent spaces in differential geometry.
