E. Dummit's Math 3527 ~ Number Theory I, Spring 2020 ~ Homework 8, due Wed Mar 18th.

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. Let $R = \mathbb{F}_3[x]$ and $p = x^2 + x$.
   (a) List the 9 residue classes in R/pR.
   (b) Construct the addition and multiplication tables for R/pR. (You may omit the bars in the residue class notation for efficiency.)
   (c) Identify all of the units and zero divisors in R/pR.
   (d) Verify Euler's theorem for each unit in R/pR.

---

2. Let $R = \mathbb{F}_2[x]$ and $p = x^3 + x + 1$.
   (a) List the 8 residue classes in R/pR.
   (b) Construct the addition and multiplication tables for R/pR. (You may omit the bars in the residue class notation for efficiency.)
   (c) Show that R/pR is a field by explicitly identifying the inverse of every nonzero element. [Hint: Use the multiplication table from (b).]
   (d) Verify Fermat's little theorem for the elements $\overline{x}$ and $\overline{x+1}$ in R/pR.

---

3. For each of the following quotient rings R/pR, show that the given element u is a unit and find its multiplicative inverse in R/pR:
   (a) $R = \mathbb{Q}[x]$, $p(x) = x^2 + 1$, $u = x + 3$.
   (b) $R = \mathbb{Z}[i]$, $p = 8 + 7i$, $u = 1 - 2i$.
   (c) $R = \mathbb{F}_3[x]$, $p(x) = x^4 + 2x + 1$, $u = x^2 + 1$.
   (d) $R = \mathbb{Z}[i]$, $p = 11 - 14i$, $u = 4 + 8i$.

---

4. Solve the following systems of congruences:
   (a) $p \equiv 1 \pmod{x+2}$ and $p \equiv 7 \pmod{x-1}$ in $\mathbb{Q}[x]$.
   (b) $z \equiv 1 \pmod{2+2i}$ and $z \equiv -i \pmod{4+5i}$ in $\mathbb{Z}[i]$.

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

5. Show the following things:

   (a) Show that the element $4 + 5i$ is irreducible and prime in $\mathbb{Z}[i]$.

   (b) Show that the element $x^2 + 1$ is irreducible and prime in $\mathbb{R}[x]$.

   (c) Show that the element $3 + 5i$ is neither irreducible nor prime in $\mathbb{Z}[i]$ by finding a factorization.

   (d) Show that the element $2 + \sqrt{-10}$ is irreducible but not prime in $\mathbb{Z}[\sqrt{-10}]$. [Hint: Show it divides 14 and that there are no elements of norm 2 or 7.]

---

6. The goal of this problem is to prove that for any integer $D > 3$, 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 positive $D > 3$?

   - Remark: When combined with our previous results (showing $\mathbb{Z}[i]$ is Euclidean in class, and that $\mathbb{Z}[\sqrt{-2}]$ is Euclidean and $\mathbb{Z}[\sqrt{-3}]$ is not on homework 7), this problem completes the characterization of the rings $\mathbb{Z}[\sqrt{-D}]$ that are Euclidean when D is a positive integer.
