E. Dummit's Math 3527 ~ Number Theory I, Spring 2023 ~ Homework 8, due Fri Mar 24th.

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. Submit scans of your responses via Canvas.

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. (You may omit the bars in the residue class notation.)

   (b) Construct the addition and multiplication tables for R/pR.

   (c) Identify all of the units and zero divisors in R/pR.

   (d) Find the order of each unit in R/pR. Are there any primitive roots?

---

2. Let $R = \mathbb{F}_2[x]$ and $p = x^3 + x + 1$.

   (a) List the 8 residue classes in R/pR. (You may omit the bars in the residue class notation.)

   (b) Construct the addition and multiplication tables for R/pR.

   (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) Find the order of each unit in R/pR. Are there any primitive roots?

---

3. Let $R = \mathbb{Z}[i]$ and $p = 2 + 2i$. You are given that there are 8 residue classes modulo p, represented by 0, 1, 2, -1, $1 - i$, i, $1 + i$, and $-i$.

   (a) Construct the addition and multiplication tables for R/pR. (Please leave the elements in the order given above: when you work out the tables you will see they are given in that order for a reason!)

   (b) Identify all of the units and zero divisors in R/pR.

   (c) Find the order of each unit in R/pR. Are there any primitive roots?

---

4. Find the following multiplicative inverses:

   (a) The multiplicative inverse of $x + 3$ inside $\mathbb{Q}[x]$ modulo $x^2 + 1$.

   (b) The multiplicative inverse of $1 - 2i$ inside $\mathbb{Z}[i]$ modulo $8 + 7i$.

   (c) The multiplicative inverse of $x^2 + 1$ inside $\mathbb{F}_3[x]$ modulo $x^4 + 2x + 1$.

   (d) The multiplicative inverse of $4 + 8i$ inside $\mathbb{Z}[i]$ modulo $11 - 14i$.

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

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 $x^2 + 4x + 5$ is irreducible and prime in $\mathbb{R}[x]$.

   (c) Show that the element $x^2 + 4x + 5$ is neither irreducible nor prime in $\mathbb{C}[x]$ by finding a factorization.

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

   (e) 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 the ring $R = \mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain under its norm function $N(a + b\sqrt{-2}) = a^2 + 2b^2$ using a similar argument to the one used to show $\mathbb{Z}[i]$ is Euclidean.

   (a) Suppose that $c + d\sqrt{-2}$ is not zero. Write $\dfrac{a + b\sqrt{-2}}{c + d\sqrt{-2}}$ in the form $x + y\sqrt{-2}$ for rational numbers x and y. [Hint: Rationalize the denominator.]

   (b) With notation from part (a), let s be the closest integer to x and t be the closest integer to y. Set $q = s + t\sqrt{-2}$ and $r = (a + b\sqrt{-2}) - (s + t\sqrt{-2})(c + d\sqrt{-2})$. Prove that $N(r) \leq \frac{3}{4}N(c + d\sqrt{-2})$.

   (c) Deduce that R is a Euclidean domain.

   (d) Use the Euclidean algorithm in R to find the greatest common divisor of $33 + 5\sqrt{-2}$ and $8 + 11\sqrt{-2}$ in R, and then write the gcd as a linear combination of these elements.

   Remark: By a similar argument, one may show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are also Euclidean domains.
