E. Dummit's Math 3527 ~ Number Theory 1, Spring 2024 ~ Homework 8, due Tue Mar 26th.

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?
   (e) 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. (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?
   (e) Verify Fermat's little theorem for the elements $\overline{x}$ and $\overline{x+1}$ in R/pR.

---

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 $11 - 14i$.

---

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

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

6. 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.]

---

7. We can use successive squaring and the same order-calculation procedure we used in $\mathbb{Z}/m\mathbb{Z}$ to establish the order of an arbitrary unit residue class $\overline{s}$ in R/rR: explicitly, $\overline{s}$ has order n if and only if $\overline{s}^n = \overline{1}$ and $\overline{s}^{n/p} \neq \overline{1}$ for any integer prime p dividing n.

   (a) Show that the element $2+i$ has order 8 in $\mathbb{Z}[i]$ modulo $r = 3+5i$.

   (b) Show that the element $\overline{x}$ has order 6 in $\mathbb{F}_7[x]$ modulo $r = x^2+x+5$.

   (c) Show that $R = \mathbb{F}_5[x]$ modulo $r = x^2+2$ is a field with 25 elements, and deduce that the order of any nonzero residue class in R/rR divides 24.

   (d) Find the orders of $\overline{2}$, $\overline{x}$, and $\overline{x+1}$ in $\mathbb{F}_5[x]$ modulo x^2+2. Are any of them primitive roots? [Hint: By (c), the order of each element divides 24, so search among divisors of 24.]

   (e) Show that $R = \mathbb{F}_5[x]$ modulo $p = x^2$ is not a field, and in fact that there are 20 units in R/rR.

   (f) Find the orders of $\overline{2}$, $\overline{x+1}$ and $\overline{x+2}$ in $\mathbb{F}_5[x]$ modulo x^2. Are any of them primitive roots? [Hint: The orders divide 20.]
