E. Dummit's Math 3527 ~ Number Theory I, Spring 2022 ~ Homework 9, due Fri 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. Submit scans of your responses via Canvas.

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

1. 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 $11-14i$.

---

2. For each polynomial $p(x)$ in the given polynomial rings $F[x]$, either find a nontrivial factorization or explain why it is irreducible:
   (a) $p(x)=x^2+2$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$.
   (b) $p(x)=x^3+x^2+2$ in $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{F}_7[x]$.
   (c) $p(x)=x^4+1$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{R}[x]$. [Hint: This polynomial factors in each case.]

---

3. For each p and $F[x]$ (note that these are the same as in problem 2), determine whether or not $F[x]$ modulo p is a field.
   (a) $p(x)=x^2+2$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$.
   (b) $p(x)=x^3+x^2+2$ in $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{F}_7[x]$.
   (c) $p(x)=x^4+1$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{R}[x]$.

---

4. Solve the following problems:
   (a) Verify Euler's theorem for each unit in R/pR for $R=\mathbb{F}_3[x]$ and $p=x^2+x$. [Hint: Use the multiplication table from problem 2 of homework 8.]
   (b) Verify Fermat's little theorem for the elements $\overline{x}$ and $\overline{x+1}$ in R/pR for $R=\mathbb{F}_2[x]$ and $p=x^3+x+1$. [Hint: Use the multiplication table from problem 3 of homework 8.]
   (c) Solve the simultaneous congruences $p\equiv 1 \pmod{x+2}$ and $p\equiv 7 \pmod{x-1}$ in $\mathbb{Q}[x]$.
   (d) Solve the simultaneous congruences $z\equiv 1 \pmod{2+2i}$ and $z\equiv -i \pmod{4+5i}$ in $\mathbb{Z}[i]$.
   (e) Give an explicit construction for a field having exactly 49 elements.
   (f) Find the number of monic irreducible polynomials in $\mathbb{F}_3[x]$ of degrees 5, 6, 7, 8, 9, and 10.

---

5. Let $p(x)=x^{2022}$.
   (a) Find the remainder when $p(x)$ is divided by $x-4$ in $\mathbb{R}[x]$.
   (b) Find the remainder when $p(x)$ is divided by $x-2$ in $\mathbb{R}[x]$.
   (c) Find the remainder when $p(x)$ is divided by x^2-6x+8 in $\mathbb{R}[x]$. [Hint: Use the Chinese Remainder Theorem and the results of (a) and (b).]

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

6. If R/pR has finitely many units, then we can use successive squaring and the same order-calculation procedure we used in $\mathbb{Z}/m\mathbb{Z}$ to find the order of an arbitrary unit residue class $\overline{s}$. 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 $p = 3 + 5i$.

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

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

   (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?
