E. Dummit's Math 3527 ~ Number Theory 1, Spring 2024 ~ Homework 9, due Tue Apr 2nd.

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. 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.]

---

2. For each p and $F[x]$ (note that these are the same as in problem 1), 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 $\mathbb{R}[x]$.

---

3. Find the number of monic irreducible polynomials in $\mathbb{F}_2[x]$ and $\mathbb{F}_3[x]$ of degrees 4, 5, 6, 7, 8, 9, and 10.

---

4. For each integer m, either find a primitive root modulo m and the total number of primitive roots modulo m, or explain briefly why there are none:

   (a) $m = 13$. (b) $m = 13^3$. (c) $m = 32^{2024}$. (d) $m = 33^{2024}$. (e) $m = 5^{2024}$. (f) $m = 2 \cdot 5^{2024}$.

---

5. For each Gaussian integer α, find (i) the number of residue classes in $\mathbb{Z}[i]$ modulo α, and (ii) the prime factorization of α in $\mathbb{Z}[i]$:

   (a) $\alpha = 19 + 48i$. (b) $\alpha = 28 - 4i$. (c) $\alpha = 20 + 7i$. (d) $\alpha = 60 - 11i$. (e) $\alpha = 2023$. (f) $\alpha = 2024$.

---

6. Let $R = \mathbb{Z}[i]$ and $r = 4 + 2i$.

   (a) Find the prime factorization of r in $\mathbb{Z}[i]$.
   (b) Given that there are 8 units modulo r, verify Euler's Theorem for the element $x = 1 + 2i$ in R/rR.
   (c) Determine the total number of residue classes in R/rR.
   (d) Draw a fundamental region for R/rR, and use it to find an explicit list of residue class representatives.

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

7. Give an explicit construction for a field having exactly 49 elements (make sure to prove that your construction does yield a field and that it does have exactly 49 elements).

---

8. We have given a geometric description for finding residue class representatives for $\mathbb{Z}[i]$ modulo α. In certain cases, we can give a more direct description.

   (a) If $\alpha = n$ is an integer (in $\mathbb{Z}$), show that the residue classes modulo α are represented by the elements $c + di$, with $0 \le c \le n - 1$ and $0 \le d \le n - 1$. [Hint: Draw the fundamental region.]
   (b) If $\pi = a + bi$ is a prime element with $N(\pi) = p$ a prime congruent to 1 modulo 4 (e.g., such as $\pi = 2 + i$ or $\pi = 3 - 2i$), show that the residue classes modulo π are represented by the elements 0, 1, ... , $p - 1$. [Hint: Count the residue classes and then show the given ones are distinct.]
