E. Dummit's Math 3527 ~ Number Theory 1, Spring 2026 ~ Homework 9, due Fri Mar 27th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly and submit via Gradescope, making sure to select page submissions for each problem. Use of generative AI in any manner is not allowed on this or any other course assignments.

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 briefly 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) $m = 32^{2026}$.
   (d) $m = 33^{2026}$.
   (e) $m = 5^{2026}$.
   (f) $m = 2 \cdot 5^{2026}$.

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

5. Give an explicit construction for each of the following things, making sure to include full justification that your example has the required property:
   (a) A field having exactly 49 elements.
   (b) An integral domain that is not a Euclidean domain.
   (c) An integral domain R with exactly 125 elements in which $r^{125} = r$ for every $r \in R$.

---

6. Let $r \in \mathbb{Z}[\sqrt{D}]$ be nonzero and not a unit. Prove that r has at least one factorization as a product of irreducibles: namely, $r = r_1 \cdots r_k$ for some irreducible elements $r_1, \ldots, r_k$. [Hint: Induct on $|N(r)|$.]

---

7. Suppose p and q are distinct odd primes. The goal of this problem is to give another approach to show that there is no primitive root modulo pq.

   (a) Suppose a is a unit modulo pq, and that its order is d_p modulo p and d_q modulo q. Show that the order of a modulo pq divides $\text{lcm}(d_p, d_q)$.

   (b) Show that the order of any unit modulo pq divides $\text{lcm}(p-1, q-1)$ and that this lcm is at most $\frac{1}{2}\varphi(pq)$. Deduce that there is no primitive root modulo pq.

---

8. Let $n \geq 3$. We have seen that there are no primitive roots modulo 2^n for $n \geq 3$, so there exists no element of order $\varphi(2^n) = 2^{n-1}$. The goal of this problem is to show that there does exist an element of the next largest possible order, namely 2^{n-2}, modulo 2^n, and to show every unit is a power of this element up to a $\pm$ sign.

   (a) Prove that $5^{2^{n-3}} - 1$ is divisible by 2^{n-1} but not by 2^n for all integers $n \geq 3$. [Hint: Induct on n, using the factorization $5^{2a} - 1 = (5^a - 1)(5^a + 1)$, and count the factors of 2 in each term.]

   (b) Deduce that $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ for $n \geq 3$.

   (c) Show that 5 has order 2^{n-2} modulo 2^n for $n \geq 3$.

   (d) Show that there is no solution to $5^a \equiv -1 \pmod{2^n}$ for $n \geq 3$.

   (e) Show that every unit modulo 2^n is of the form 5^a or -5^a for some $1 \leq a \leq 2^{n-2}$. [Hint: Show that all these elements are distinct units.]
