E. Dummit's Math 3527 ~ Number Theory I, Spring 2020 ~ 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 clearly identify all problem numbers. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

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. Solve the following problems:
   (a) Find the number of monic irreducible polynomials in $\mathbb{F}_3$ of degrees 5, 6, 7, 8, 9, and 10.
   (b) Give an explicit construction for a field having exactly 49 elements.
   (c) Find a primitive root modulo 17^{2020} and the total number of primitive roots modulo 17^{2020}, or explain why there are none.
   (d) Find a primitive root modulo 32^{2020} and the total number of primitive roots modulo 32^{2020}, or explain why there are none.
   (e) Find a primitive root modulo 33^{2020} and the total number of primitive roots modulo 33^{2020}, or explain why there are none.
   (f) Find a primitive root modulo $2 \cdot 5^{2020}$ and the total number of primitive roots modulo $2 \cdot 5^{2020}$, or explain why there are none.

---

4. Let $p(x) = x^{2020}$.
   (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 $x + 1$ in $\mathbb{R}[x]$.
   (c) Find the remainder when $p(x)$ is divided by $x^2 - 3x - 4$ in $\mathbb{R}[x]$. [Hint: Use the Chinese Remainder Theorem.]

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

5. If R/rR has finitely many units, then we can use the same order-calculation algorithm 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 prime p dividing n.

   (a) 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.

   (b) 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?

---

6. The goal of this problem is to give some examples of R/rR for $R = \mathbb{F}_5[x]$ where there do and do not exist primitive roots.

   (a) In $\mathbb{F}_5[x]$ modulo the irreducible polynomial $x^2 + x + 1$, show that the element $\overline{x+2}$ is a primitive root.

   (b) In $\mathbb{F}_5[x]$ modulo the reducible polynomial x^2, show that there are 20 units and and that $\overline{x+3}$ has order 20 (and thus is a primitive root).

   (c) In $\mathbb{F}_5[x]$ modulo the reducible polynomial $x^2 + x$, show that there are 16 units but that all of them have order dividing 4. Deduce that there are no primitive roots in this case. [Hint: Show that $u^4 \equiv 1 \bmod x$ and $u^4 \equiv 1 \bmod x+1$ for each possible unit, and then use the Chinese Remainder Theorem.]

   (d) Based on the results of parts (a)-(c), and in analogy with the case for $\mathbb{Z}/m\mathbb{Z}$, can you conjecture when there will be a primitive root in R/rR when $R = \mathbb{F}_5[x]$?
