Math 417 **Homework 10** **Due Friday, April 19, 2019**

It's ok to work together, but don't copy without comprehension. The symbol ($\mathcal{E}$) means that at least part of this problem is a former or potential exam question. This is the final homework of the semester.

Ungraded. *Fraleigh* § IV.23 (p.218) – 1, 3, 5, 9

---

1. *Fraleigh* § IV.23 (p. 218) – 4, 6, 12.

2a. ($\mathcal{E}$) Suppose $p = 2m + 1$ is prime, and a is a primitive root mod p and let $b = a^m$. Prove that $b \equiv -1 \mod p$. Hint: first show that $b^2 \equiv 1 \mod p$, and then see what that says about b.

2b. Wolfram|Alpha tells you that 2 is a primitive root mod 101. Using this information alone, determine whether the following are also primitive roots mod 101:

$$4 \equiv 2^2, \quad 8 \equiv 2^3, \quad 32 \equiv 2^5, \quad 27 \equiv 2^7.$$

(Hint: this is really a group theory question!)

3. ($\mathcal{E}$) Let $F = \mathbb{Z}/7\mathbb{Z}$. Suppose $f(x) = x^3 + 2x + 1$ and $g(x) = x^2 + 3$. (That is, $f(x) = [1]_7x^3 + [0]_7x^2 + [2]_7x + [1]_7$ and $g(x) = [1]_7x^2 + [0]_7x + [3]_7$ are elements of $F[x]$.) Write

$$f(x) = g(x)q(x) + r(x),$$

where $q(x), r(x) \in F[x]$ and either $r(x) = 0$ or the degree of $r(x)$ is strictly less than the degree of $g(x)$. You do *not* have to use the $[a]_7$ notation in your answer, but you should do all arithmetic mod 7.

4. ($\mathcal{E}$) Compute $11^{35} \mod 36$ using theorems from the class. (Note: $36 = 2^2 \cdot 3^2$ is not prime!)

5. ($\mathcal{E}$) Let $p(x) = x^4 + 9x^3 + 20x^2 + x - 1$. By following the general argument of Example 23.14, show that p does not have any linear factors in $\mathbb{Z}[x]$ and also write p as a product of two quadratic factors. To make the grader's life easier, please write these factors as $(x^2 + ax + b)(x^2 + cx + d)$.) Your first decision should be determining b and d.

6. Find integers $A \neq 0$ and $B \neq 0$ so that $f(x) = x^4 + Ax + B$ has no linear factors, but is reducible over $\mathbb{Z}[x]$ as a product of two quadratics. As a hint, repeat the argument of the last problem by finding conditions on a, b, c, d so that the coefficients of x^3 and x^2 in $(x^2 + ax + b)(x^2 + cx + d)$ are each equal to zero. There are infinitely many correct answers, but make sure that the one you come up with doesn't have linear factors! (The condition $A \neq 0$ is designed so you won't present something like $(x^2 + 2)(x^2 - 2) = x^4 - 4$.)