Exercises and Investigations: Set 3

The "Exercises and Investigations" sets for this class are designed both to reinforce mathematical concepts and to lead you to think creatively about problems. You should clearly explain what you tried and how approached each item, even if you do not get to a final solution. Also, it often happens that you gain new insight into an old problem as time goes on and you are thinking about things from a new angle. So, as weeks go on, you may choose to go back and re-explore old problems in place of new ones.

1. Several times in class, we have used the following fact: If a polynomial whose coefficients are integers does not have a zero $\mod n$ for some n, then it does not have a zero in the integers. Explain why this fact is true. [Hint: Show that if a polynomial with integer coefficients has a zero in the integers, then it also has a zero $\mod n$.]

2. Give a specific example of a polynomial with integer coefficients that does not have any zeros in the integers but that has a zero $\mod n$ for some n. [Hint: Try $x^2 + 1$ as your polynomial and $n = 5$.] So the converse of the statement from the first problem is not necessarily true.

3. Fix a prime number p. Fermat's little Theorem says that if a is an integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$. In other words, $a^{p-1} - 1 = pk$ for some integer k. Often Fermat's little Theorem is proved using *group theory*, a topic we have not discussed in this course. Instead, we are going to find a more elementary reason for Fermat's little Theorem. (If you've taken a proofs course before, you'll notice that what we end up doing is a *proof by induction*, but we won't assume that you are familiar with that terminology or approach here.)

   (a) Verify that Fermat's little Theorem holds in the simplest case possible, namely when $a = 1$.

   (b) By our beginning exercises on congruences, it suffices to prove Fermat's little Theorem for $a = 1, \ldots, p - 1$. Explain why it is also sufficient to show the following: If we know Fermat's little Theorem holds for a number a, then we also know Fermat's little Theorem also holds for $a + 1$.

   (c) Now, suppose Fermat's little Theorem holds for a number a (for example $a = 1$). Show that $(a + 1)^p \equiv a + 1 \mod p$ [Hint: You may use, without proof, the Binomial Theorem, which says that for any integers x and y and any positive integer n, $(x + y)^n = \sum_{j=0}^{n} \frac{n!}{j!(n-j)!} x^j y^{n-j}$, i.e. the when we expand $(x + y)^n$, the coefficient of the term $x^j y^{n-j}$ is $\frac{n!}{j!(n-j)!}$. For a *prime* number p and $0 < j < p$, why is this number divisible by p?]

   (d) Put the previous parts of the exercise together to conclude that Fermat's little Theorem holds.

   (e) What would go wrong if we tried to replace p by a non-prime number in the statement of Fermat's little Theorem?

4. We have already covered the fact that a polynomial with complex coefficients has a zero in the complex numbers (for example, by Gauss's proof). We also can easily come up with polynomials with integer coefficients that don't have zeroes in the

integers. (For example x^2+1 can't have a zero in the integers, since $a^2+1 \geq 1 > 0$ for all real numbers a). In this problem, we'll use modular arithmetic to find more examples of polynomials that do not have zeroes in the integers.

(a) Show that the polynomial $x^4 + 5x^3 - 15x^2 - 10x + 2$ has no zeroes in the integers. [Hint: Work mod 5, and don't forget Fermat's little Theorem.]

(b) Show that the polynomial $2x^{12} + 21x^{11} - 7x^{10} - x^6 + 7x^5 + 14x^4 + 3$ has no zeroes in the integers. [Hint: Work mod 7, and don't forget Fermat's little Theorem.]

(c) Produce a family of infinitely many polynomials with integer coefficients that don't have zeroes in the integers. [Hint: Try to generalize the ideas you used in the previous two parts. There are lots of different possibilities that work here.]