MA357, Spring 2020 — Problem Set 5

This assignment is due on **Friday, March 13**. It's a bit shorter than usual because you also have a writing assignment due that day.

1. NTG, Exercise 4.7.41.

2. NTG, Exercise 4.7.42. (Experiment first!)

3. Do any numbers satisfy the equation $\varphi(n) = 2n$?

4. Do any numbers satisfy the equation $\varphi(n) = n/2$?

5. NTG, Exercise 5.6.21.

6. In the previous assignment you showed that if $n > 4$ is not prime then $(n-1)! \equiv 0 \pmod{n}$. This problem shows what happens when n is prime.

Let p be a prime. Use the fact that every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ has an inverse (mod p) to show that

$$(p-1)! \equiv -1 \pmod{p}.$$

This is called *Wilson's Theorem*.

7. Suppose $m \in \mathbb{N}$ and let a be an integer such that $\gcd(a, m) = 1$. In the last problem set you showed that there exists an integer k such that $a^k \equiv 1 \pmod{m}$. Of course, then we also have $a^{2k} \equiv 1 \pmod{m}$, so there will be many such exponents.

Let $e \geqslant 1$ be the *smallest* exponent such that $a^e \equiv 1 \pmod{m}$. This is called the *order* of a mod m. Show that

a. If n is a multiple of e, then $a^n \equiv 1 \pmod{m}$.

b. Conversely, if $a^n \equiv 1 \pmod{m}$, then e is a divisor of n. (Consider the remainder when we divide n by e.)

To Explore: Suppose we want to decide whether there exists a non-trivial solution in integers for the quadratic equation $ax^2 + by^2 + cz^2 = 0$. (Non-trivial here means that we don't want the solution $x = y = z = 0$.) To avoid degenerate cases, let's assume that a, b, and c are squarefree, i.e., they do not have any square divisors, and that they do not all have the same sign.

a. Show that if such a solution exists, then for every m the congruence $ax^2 + by^2 + cz^2 \equiv 0 \pmod{m}$ has a non-trivial solution. (Be careful! After all, a nonzero integer x might be zero mod m.)

b. Explain why it follows that if the congruence mod m fails to have a non-trivial solution for some m, then there is no non-trivial integer solution.

c. Is that the only obstruction? In other words, is it true that if the congruences mod m have solutions for every m, we can conclude that there are integer solutions as well?

To Explore: A point in the plane with integer coordinates (a, b) is called *visible* if the line segment connecting $(0, 0)$ to (a, b) does not contain any other points with integer coordinates.

a. Show that (a, b) is visible if and only if $\gcd(a, b) = 1$.

b. Let $V(n)$ be the number of visible points (a, b) in the square defined by the conditions $1 \leqslant a \leqslant n$, $1 \leqslant b \leqslant n$. Compute $V(n)$ for $n = 10, 20, 30, 40, 50$. (You'll probably need a computer to do this.)

c. For each of those values of n, compute $V(n)/n^2$, i.e., the fraction of points in the square that are visible.

d. Make a guess as to whether the ratio $V(n)/n^2$ has a limit as $n \to \infty$.

e. Prove your guess.

To Explore: Let $a_1, a_2, \dots, a_n$ be positive integers. Study the theory of diophantine equations of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b.$$

If we restrict the solutions to *positive* integers, i.e., we assume $x_i \geqslant 0$, this is sometimes known as the postage stamp problem: think of a_1, a_2, etc. as the values of the stamps you have, and of b as the amount of postage you want to put onto an envelope.

To Explore: In calculus, you may have seen a proof that the series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n} + \dots$$

diverges. What happens if we take only the reciprocals of the primes? Does the series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p} + \dots$$

converge?

If you can settle that one, what if we select subsets of the primes to work with? For example, how about summing over all p such that $p + 2$ is also prime? Does that series converge?