Study guide

- (§8) Practice switching between divisibily statements and congruence statements. Each can be used to prove theorems about the other.
- Review earlier study items and techniques. Several problems on this set are designed to synthesize older techniques together.
- (§9) Know the statement of Fermat's little theorem, and how it can be used to rewrite large powers in modular arithmetic.
- (§9) Understand the proof from class (to be done on Friday 2/21) of Fermat's little theorem.

1. Find three positive integers a, b, c with no common factors such that $a^2 + b^2 = c^4$, and describe a systematic method you could use to find more (besides guessing and checking).

   Hint Try combining some techniques from some earlier problem sets.

2. Let m be a positive integer, and a be an integer such that $\gcd(a, m) = 1$. We showed in class that there must exist some exponent $e > 0$ such that $a^e \equiv 1 \pmod{m}$. Call the smallest such value e the *multiplicative order* of a modulo m.

   (a) For each a between 1 and 12 inclusive, find the multiplicative order of a modulo 13.

   (b) For each a between 1 and 14 inclusive such that $\gcd(a, 15) = 1$, find the multiplicative order of a modulo 15.

3. Let a and b be two positive integers such that $\gcd(a, b) = 1$. Suppose that x, y are two other integers such that $x \equiv y \pmod{a}$ and $x \equiv y \pmod{b}$. Prove that $x \equiv y \pmod{ab}$.

4. We've mentioned in class that the two main "cancel a factor" operations we use while manipulating congruences are in fact not just logical implications; their converses are true as well. In this problem, we will fill in that gap, so that we can write these operations as ⇔ in the future.

   (a) Suppose that $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{N}$. Further, assume that $c \mid m$. Prove that

   $$ca \equiv cb \pmod{m} \quad \text{if and only if} \quad a \equiv b \pmod{\frac{m}{c}}.$$

   (We have proved the ⇒ implication in class, but you should write it out for completeness, and to make sure you understand it. Then be sure to also prove the ⇐ implication.)

   (b) Suppose that $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{N}$, and now assume that $\gcd(c, m) = 1$. Prove that

   $$ca \equiv cb \pmod{m} \quad \text{if and only if} \quad a \equiv b \pmod{m}.$$

   (Again, you should prove both implications, though we have proved one in class.)

   (c) Prove the following convenient mutual generalization of (a) and (b). It is possible to prove this directly, or by deducing it from (a) and (b). If you prove it direclty, it is fine to prove this part first and then simply deduce parts (a) and (b) from it; just clearly indicate that this is what you are doing.

Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{N}$. This time, make no assumptions about common divisors of c and m. Prove that

$$ca \equiv cb \pmod{m} \quad \text{if and only if} \quad a \equiv b \pmod{\frac{m}{\gcd(c,m)}}.$$

5. One thousand gnomes have been imprisoned by an evil wizard. The wizard informs the gnomes that the following day they will line up, facing forward, and that he will place a hat on each gnome. Each hat will be one of 41 possible colors. Starting from the back of the line, each gnome will then be permitted to guess their own hat color. After all the gnomes have finished guessing, the gnomes that guessed correctly will be freed. Determine a strategy for the gnomes guaranteeing that at most one of them will not be freed. Each gnome can see all of the hats in front of them, and hear all of the guesses made by gnomes behind them, but they cannot see their own hat color.[1]

6. Determine the largest integer n such that $n + 10$ divides $n^3 + 100$.

   Hint Use congruences.

7. Determine the remainder when 19^{5085} is divided by 43.

[1] Don't worry: once these 999 gnomes are free they will be powerful enough to come back and rescue the last one.