Study guide

- Understand the strategy of "reducing the exponent," and some of the problems it is applicable to.
- (§11) How do you compute $\phi(m)$ quickly if you know the prime factorization of m?
- (§11) Understand the main statement of the *Chinese Remainder Theorem*.
- (§11) Know how to "merge" pairs of congruences in practice.

1. (Textbook 10.1, on a quantity arising in the proof of Euler's theorem)

2. (Textbook 10.3, on *Carmichael numbers*.)

Note For the following two problems, you may, and probably should, use a computer or calculator to aid in the arithmetic. Feel free to ask me for tips on what tools to use to do this. There are some ways to make it more efficient to the point doing it by hand is feasible, which I am happy to discuss at office hours and which we'll likely discuss in class soon, but for now it's fine to use a computer.

3. Determine the last two digits (tens digit and units digit) of $3^{13^{2015}}$. (Problem 5 may be useful, and you can assume the result of it is true in this problem.)

4. Find the smallest positive integer n such that the last two digits of n^3 are "77."

5. Let m be positive integer, and a an integer with $\gcd(a, m) = 1$. Prove that if $e, f \in \mathbb{N}$ satisfy

$$e \equiv f \pmod{\phi(m)},$$

then

$$a^e \equiv a^f \pmod{m}.$$

This is a precise version of the claim I made in class that you can use $\phi(m)$ as a modulus when working with exponents.

Note The remaining problems rely on the Chinese remainder theorem, so you should save them until after Friday's class, or read §11 in advance.

6. (Textbook 11.5, solving several sets of simultaneous congruences)

7. (a) Find a solution to the following problem, from Sun Tzu's Mathematical Manual (circa 300 C.E.): "We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?"
   (b) Find a solution between 100 and 200 to the problem in part (a).

8. Compute $\phi(97)$ and $\phi(8800)$, where $\phi(n)$ denotes Euler's phi function.