Final Review

We've covered a lot of content in the course. Here's a breakdown of what's important to know for the final exam. This list is not a guarantee that these are the things/are the only things that will appear on your final exam – it's meant to be a guide to help you understand what the important things to takeaway from the course are. Of course, I expect that you look over the homework solutions so that you know how to solve your homework problems, too, and that you take a look at the key results on Canvas and understand what they say/how they might get used in a problem. If there are problems on the worksheets that you don't know how to do (most of them should be answerable by now, either from a key results, a HW problem, etc.), you should look over those, too.

Computations

- Finding integer solutions to linear Diophantine equations (HW 3). More generally, the idea of finding rational/integer points on curves and how this can help you solve equations (Week 10/HW 9).
- Computing the gcd and lcm of integers. You should understand how this can be done either using the Euclidean algorithm, or via prime factorization. (HW3/4).
- Basic modular arithmetic computations. This means being able to add, multiply, divide (i.e. compute inverses), and use Euler's theorem to help you do exponentiation (HW 5/7).
- Solving congruence equations mod n. There are a lot of problems about this, both on the worksheets and on your homework! You should be able to solve linear congruences mod n (HW 5), exponential congruences mod p (HW 8), and find k-th roots mod n (HW 7,8). You should understand how to use Hensel's lemma to solve polynomial congruences modulo prime powers (HW 8), and be able to use the Chinese remainder theorem to solve systems of congruences (HW 6). You should also understand the procedure for solving general polynomial congruences mod n (HW 8).
- You should understand how to compute orders mod n and be able to check if something is a generator mod n or not (Week 7/8/HW 7).
- You should understand how to compute $\varphi(n)$ and how to solve equations involving $\varphi(n)$ (HW 6).
- You should be able to determine (with proof) if a function is injective/surjective/bijective (Week 6/HW 6).
- Polynomial arithmetic (Week 8).

Theory

- Here are the big theorems that we have proven that tend to have theoretical applications:
  - Division algorithm
  - Bezout's lemma
  - Fundamental theorem of arithmetic
  - Chinese remainder theorem
  - Euler's theorem

- Hensel's lemma
- Existence of a generator mod p.

You should understand what all these theorems say, and how they can be used to help you prove results (e.g. on your homework). With the exception of the existence of a generator mod p, you should be able to explain in a few sentences (without giving a full proof!) what the ideas that went into proving these theorems were. For example, using WOP on the set of positive linear combinations of a and b and showing the smallest element is $\gcd(a, b)$ proves Bezout's lemma.

- You should be comfortable with induction (used throughout the course).
- You should understand basic properties of divisibility, the gcd/lcm, and prime numbers (used throughout the course, but most of this was done up to and including on the midterm).
- You should understand the basic properties of $\mathrm{ord}_n(a)$ and how this can help you prove results about divisibility (e.g. HW 7).
- You should be comfortable translating between divisibility statements in $\mathbb{Z}$ and congruences. Also, you should be comfortable translating between the language of equations in $\mathbb{Z}/n\mathbb{Z}$ and congruences mod n (again used throughout the course, but some examples are HW 5/6).
- You should understand the main philosophies of number theory, and how this can help you prove things in $\mathbb{Z}$ or in $\mathbb{Z}/n\mathbb{Z}$. This means the "gluing" philosophy (used frequently, but the big examples: HW4/6/7/Week 9) and the "lifting" philosophy (HW6/Week 9).