Review for Midterm 2 (Math 2200, Spring 2023)

1 Sample Problems

On the problems requiring computations, feel free to use a calculator if you would like. The point of the problem is to understand how to do the computation.

1. Let m be a positive integer. Prove, from the definitions, that if a and b are integers and $a \equiv b \pmod{m}$, then for any integer k we have $a + k \equiv b + k \pmod{m}$ and $ak \equiv bk \pmod{m}$.
2. Let p be a prime number. Let k be an integer which is not divisible by p. Prove, from the definitions, that if a and b are integers and $ak \equiv bk \pmod{p}$, then $a \equiv b \pmod{p}$ (in other words, we can "divide by k" modulo m).
3. Find an example of a positive integer m, an integer k which is not divisible by m, and integers a, b such that $ak \equiv bk \pmod{m}$ but $a \not\equiv b \pmod{m}$. (This shows that the previous problem is false if you drop the assumption that p is prime. In general, you can "divide by k" modulo m if k is coprime to m).
4. Solve $5x \equiv 2 \pmod{17}$ for x by using the Euclidean algorithm.
5. Solve $5x \equiv 2 \pmod{17}$ by using Fermat's Little Theorem (**Hint**: Fermat's Little Theorem shows that $5^{16} \equiv 1 \pmod{17}$, so $5 \cdot 5^{15} \equiv 1 \pmod{17}$, and therefore 5^{15} is the multiplicative inverse of 5 modulo 17).
6. Solve $x^7 \equiv 2 \pmod{23}$ for x.
7. How many strings of 0's and 1's are there of length 7? For example, here are three of them:
$$0110100, 1111111, 1001001$$
8. How many strings of 0's and 1's are there which have length 7 and exactly three 1's? Try to find the answer without actually listing all of them.
9. Find the coefficient of x^2 in the expansion of
$$\left(\sqrt{x} - \frac{2}{x^2}\right)^9$$
10. Say you have a group of 20 people. You need to select 8 of these people to form a sports team, and also designate one of the people on the team to be the captain. In how many ways can you do this?
11. Using the formula for binomial coefficients, prove that
$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

12. Reprove the identity in the previous problem by using a counting argument. (without using the formula for binomial coefficients) **Hint**: in problem (10), we can count the number of teams in two ways: by first picking a team, and then designating a captain, or by first picking the captain, and then picking the other people on the team.

13. Prove that, for all integers $n \geq 0$ and $0 \leq k \leq n$, we have

$$\binom{n+1}{k+1} = \binom{k}{k} + \binom{k+1}{k} + \cdots + \binom{n}{k}$$

Hint: the left hand side is the number of $k+1$–element subsets of $\{1, \ldots, n+1\}$. Show that the right hand side is also equal to this number by grouping these subsets according to their largest element.

2 Review topics by chapter

Chapter §12

- Understand the proof of Theorem 12.1.

Chapter §13

- Know the definition of the notation $a \equiv b \pmod{m}$.
- Understand how to use the method of repeated squaring to compute $x^n \pmod{m}$ (see Example 13.3).
- Know when you can divide modulo m (see Proposition 13.5).
- Know how to tell when $ax \equiv b \pmod{m}$ has a solution, and how to find this solution.

Chapter §14

- Know the statement of Fermat's Little Theorem (Theorem 14.1).
- Know how to tell when $x^k \equiv b \pmod{p}$ has a solution, and how to find the solution (Proposition 14.2).

Chapter §15

- Know the encoding and decoding process behind RSA.

Chapter §16

- Understand the "multiplication principle" (Theorem 16.1).
- Know why $n!$ is the number of arrangements of n things.
- Know the definition of the binomial coefficients $\binom{n}{k}$.
- Know the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, and why it is true (Proposition 16.2)
- Know the statement of the binomial theorem (Theorem 16.2)
- Multinomial coefficients will not be on midterm 2.