Problem Set 4

Due: February 27th, 5pm

1 Formal proofs

For each problem in this section, you must give a complete and rigorous proof. Your arguments should be clear, logically ordered, and written in full sentences.

In particular, state all assumptions explicitly and define all notation. Justify every nontrivial step.

1. (1 point) Binomial Coefficients

   (a) For integers $n \geq 0$ and $0 \leq k \leq n$, the binomial coefficient is defined by

   $$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

   Compute $\binom{4}{0}$, $\binom{4}{1}$, $\binom{4}{2}$, $\binom{4}{3}$, and $\binom{4}{4}$.

   (b) Prove that for all $0 \leq k \leq n$, $\binom{n}{k} = \binom{n}{n-k}$.

   (c) Let $n \geq 1$. Prove that for $1 \leq k \leq n-1$, the binomial coefficients satisfy Pascal's identity: $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. Look up Pascal's triangle, and write down the first 5 lines.

2. (2 points) The Binomial Theorem.

   (a) Expand $(x+y)^2$, $(x+y)^3$, and $(x+y)^4$ by direct multiplication. Rewrite your expansions so that the coefficients appear as binomial coefficients.

   (b) Prove by induction on n the Binomial Theorem

   $$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

   (c) Let p be prime and $x, y \in \mathbb{Z}$. Prove that $(x+y)^p \equiv x^p + y^p \pmod{p}$.

2 Demonstrations

For problems in this section, you still need to give complete mathematical reasoning to support your answers. I should be able to follow and understand your work, but it doesn't have to be organized into a formal proof.

3. (1 point) Solve the simultaneous congruence equations

$$\begin{cases} 3x \equiv 4 & \pmod{17} \\ 8x + 11 \equiv 5 & \pmod{31} \end{cases}$$

4. (1 point) Solve the simultaneous congruence equations

$$\begin{cases} x \equiv 2 & \pmod{5}, \\ x \equiv 3 & \pmod{7}, \\ x \equiv 4 & \pmod{9}. \end{cases}$$

5. (1 point) How many units are there in $\mathbb{Z}_{2600}$?

6. (2 points) If a is a positive integer, we can write a uniquely as

$$a = \sum_{i=0}^{n} d_i 2^i = d_n \cdot 2^n + d_{n-1} \cdot 2^{n-1} + \cdots + d_1 \cdot 2 + d_0 \cdot 2^0 \qquad d_i \in \{0, 1\}.$$

The digits $d_n \cdots d_0$ are the **binary digits** of a, and we write $(a)_2$ for the binary digits. For example $(11)_2 = 1011$ since

$$11 = 8 + 2 + 1 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0.$$

(a) Find the binary expansion of 1345.

(b) Find $7^{2^i} \pmod{81}$ for $i = 0, 1 \ldots, 10$.

(c) Use your results from parts (a) and (b) to compute $7^{1345} \pmod{81}$ efficiently.

3 Explorations

In this section, I'm looking for answers that are supported by evidence, but you don't have to prove your answers.

7. (2 points) Let n be a positive integer, and let $\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n : x \text{ is a unit modulo } n\}$. Let
$$O_n = \{k : k = \operatorname{ord}_n(a) \text{ for some } a \in \mathbb{Z}_n^\times\}.$$
   (a) Write down the sets O_n for $n = 1, \ldots, 100$. (*You are of course welcome to do this problem by hand, but I wouldn't recommend it ☺. Instead, I recommend that you use SageMath, in which case you need to provide screen shots of both your code and the results you have found.*)

   (b) Give an upper bound for the biggest possible value in O_n, and provide some explanation of why this is an upper bound.

   (c) For which values of n from part (a) does O_n achieve the upper bound you have given in part (b)?

   (d) Write down some observations about the sets O_n. Do you have any conjectures about the structure of this sets? E.g., are there cases where you can determine exactly which numbers appear in O_n based on just n alone?