

15-251: Great Theoretical Ideas In Computer Science

Homework 8 (due Thursday, October 22)

Directions: Write up carefully argued solutions to the following problems. The first task is to be complete and correct. The more subtle task is to keep it simple and succinct. Your solution should be clear enough that it should explain to someone who does not already understand the answer why it works. You may use any results proven in lecture without proof. Anything else must be argued rigorously. Unless otherwise specified, all answers are expected to be in closed form.

0. Warmup (0 points)

1. Let n be a positive integer. Prove that $3^{2^n} + 1$ is divisible by 2, but not by 4.
2. Show that $(ab)^{-1} = b^{-1}a^{-1}$ for any group.
3. What is the units digit in the decimal representation of $3^{1001}7^{1002}13^{1003}$.

1. Binomial Congruence (15 points)

Let p be a prime, and let k be an integer such that $0 \leq k \leq p-1$. Prove that $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$.

2. YATAG (10 points)

Brad, who still hasn't gotten sick of playing with take-away games, is proposing yet another take-away game. In this game, each player can remove x chips only if x is a perfect square. (E.g., one can remove 1, 4, 9, 16, 25, ..., 10^6 , ..., but not 2 or 12 or 127 chips.)

Prove that there are infinitely many P -positions under normal rules.

3. Divide and Conquer (20 points)

Prove the following statements assuming that p is a prime.

1. (7 points) Prove that $p \mid (ab^p - ba^p)$ for all integers a, b .
2. (13 points) Prove that there are infinitely many positive integers n such that $p \mid (2^n - n)$.

4. Euler Totient Function (20 points)

1. (6 points) Find the sum of positive integers less than n and relatively prime to n .
2. (14 points) Find the smallest integer $n \geq 0$ such that n^3 written in decimal ends in 888.

5. Order! Order! (15 points)

1. (5 points) Prove that ab and ba have the same order.
2. (10 points) If a group G has only one element a of order 2, show that for every x in G , $xa = ax$.

6. You're the One, Neo. (20 points)

Let G be a group with order $|G| = m \times p$, where p is a prime and $p > m$. Show that if A and B are two subgroups of G of order $|A| = |B| = p$, then $A = B$.