CSL 105: Discrete Mathematical Structures
Instructor: Ragesh Jaiswal

This file may get updated. So, please refresh your browser.

1. Give an example of two increasing functions $f(n)$ and $g(n)$ from the set of positive integers to the set of positive integers such that neither $f(n)$ is $O(g(n))$ nor $g(n)$ is $O(f(n))$.

2. Show that we can easily factor N when we know that N is the product of two primes, p and q, and we know the value of $(p-1)(q-1)$.

3. (a) Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.

   (b) Use part (a) to show that $10! \equiv -1 \ (mod\ 11)$.

4. Show that if p is prime, the only solutions of $x^2 \equiv 1 \ (mod\ p)$ are integers x such that $x \equiv 1 \ (mod\ p)$ or $x \equiv -1 \ (mod\ p)$.

5. (a) Generalize the result in part (a) of problem 2; that is, show that if p is a prime, the positive integers less than p, except 1 and $p-1$, can be split into $(p-3)/2$ pairs of integers such that each pair consists of integers that are inverses of each other.

   (b) From part (a) conclude that $(p-1)! \equiv -1 \ (mod\ p)$ whenever p is prime. This result is known as *Wilson's theorem*.

   (c) What can we conclude if n is a positive integer such that $(n-1)! \not\equiv -1 \ (mod\ n)$?

6. Prove that an integer $(a_{n-1}, ..., a_0)$ is divisible by 11 if and only if $a_0 + a_2 + a_4 + ... \equiv a_1 + a_3 + ... \ (mod\ 11)$.

7. If m is a positive integer, the integer a is a quadratic residue of m if $gcd(a, m) = 1$ and the congruence $x^2 \equiv a \ (mod\ m)$ has a solution. In other words, a quadratic residue of m is an integer relatively prime to m that is a perfect square modulo m. If a is not a quadratic residue of m and $gcd(a, m) = 1$, we say that it is a quadratic non-residue of m. For example, 2 is a quadratic residue of 7 because $gcd(2, 7) = 1$ and $3^2 \equiv 2 \ (mod\ 7)$ and 3 is a quadratic non-residue of 7 because $gcd(3, 7) = 1$ and $x^2 \equiv 3 \ (mod\ 7)$ has no solution.

   Show that if p is an odd prime, then there are exactly $(p-1)/2$ quadratic residues of p among the integers $1, 2, ..., p-1$.

8. Problems 58 to 64 of section 4.4 (International version). Please try to attempt these problems on your own even if we do not get time to discuss them in the tutorial.