CS 70 Discrete Mathematics and Probability Theory
Fall 2022 Satish Rao and Babak Ayazifar

HW 04

Due: Saturday, 9/24, 4:00 PM
Grace period until Saturday, 9/24, 6:00 PM

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Modular Practice

Solve the following modular arithmetic equations for x and y.

(a) $9x+5 \equiv 7 \pmod{11}$.

(b) Show that $3x+15 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $3x+2y \equiv 0 \pmod{7}$ and $2x+y \equiv 4 \pmod{7}$.

(d) $13^{2019} \equiv x \pmod{12}$.

(e) $7^{21} \equiv x \pmod{11}$.

2 Nontrivial Modular Solutions

(a) What are all the possible perfect cubes modulo 7?

(b) Show that any solution to $a^3+2b^3 \equiv 0 \pmod{7}$ must satisfy $a \equiv b \equiv 0 \pmod{7}$.

(c) Using part (b), prove that $a^3+2b^3 = 7a^2b$ has no non-trivial solutions (a,b) in the integers. In other words, there are no integers a and b, that satisfy this equation, except the trivial solution $a = b = 0$.

[*Hint:* Consider some nontrivial solution (a,b) with the smallest value for $|a|$ (why are we allowed to consider this?). Then arrive at a contradiction by finding another solution (a',b') with $|a'| < |a|$.]

3 Wilson's Theorem

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?

4 Fermat's Little Theorem

Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

5 Euler's Totient Function

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \leq i \leq n, \gcd(n,i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. We develop a general formula to compute $\phi(n)$.

(a) Let p be a prime number. What is $\phi(p)$?

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

(c) Show that if $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. (Hint: Use the Chinese Remainder Theorem.)

(d) Argue that if the prime factorization of $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then

$$\phi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.$$

6 Euler's Totient Theorem

Euler's Totient Theorem states that, if n and a are coprime,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n)$ (known as Euler's Totient Function) is the number of positive integers less than or equal to n which are coprime to n (including 1).

(a) Let the numbers less than n which are coprime to n be $m_1, m_2, \ldots, m_{\phi(n)}$. Argue that the set

$$\{am_1, am_2, \ldots, am_{\phi(n)}\}$$

is a permutation of the set

$$\{m_1, m_2, \ldots, m_{\phi(n)}\}.$$

In other words, prove that

$$f : \{m_1, m_2, \ldots, m_{\phi(n)}\} \to \{m_1, m_2, \ldots, m_{\phi(n)}\}$$

is a bijection, where $f(x) \coloneqq ax \pmod{n}$.

(b) Prove Euler's Theorem. (Hint: Recall the FLT proof.)

7 Sparsity of Primes

A prime power is a number that can be written as p^i for some prime p and some positive integer i. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

Hint: This is a Chinese Remainder Theorem problem. We want to find x such that $x+1, x+2, \ldots, x+k$ are all not powers of primes. We can enforce this by saying that $x+1$ through $x+k$ each must have two distinct prime divisors.