CS 70 Discrete Mathematics and Probability Theory
Fall 2021 HW 4

Due: Friday 9/24, 10:00 PM
Grace period until Friday 9/24 11:59 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) $7^{21} \equiv x \pmod{11}$.

(f) $x \equiv 5 \pmod{7}$, $x \equiv 3 \pmod{9}$, $x \equiv 3 \pmod{11}$. What is the smallest possible value for x?

2 Check Digits: ISBN

In this problem, we'll look at a real-world applications of check-digits.

International Standard Book Numbers (ISBNs) are 10-digit codes ($d_1 d_2 \ldots d_{10}$) which are assigned by the publisher. These 10 digits contain information about the language, the publisher, and the number assigned to the book by the publisher. Additionally, the last digit d_{10} is a "check digit" selected so that $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \pmod{11}$. (*Note that the letter X is used to represent the number 10 in the check digit.*)

(a) Suppose you have a very worn copy of the (recommended) textbook for this class. You want to list it for sale online but you can only read the first nine digits: 0-07-288008-? (the dashes are only there for readability). What is the last digit? Show your work.

(b) Wikipedia says that you can determine the check digit by computing $\sum_{i=1}^{9} i \cdot d_i \pmod{11}$. Show that Wikipedia's description is equivalent to the above description.

(c) Prove that changing any single digit of the ISBN will render the ISBN invalid. That is, the check digit allows you to *detect* a single-digit substitution error.

(d) Can we ever switch two distinct digits in an ISBN number and get another valid ISBN number? For example, could 012345678X and 015342678X both be valid ISBNs? Explain.

3 Divisible or Not

(a) Prove that for any number n, the number formed by the last two digits of n are divisible by 4 if and only if n is divisible by 4. (For example, '23xx' is divisible by 4 if and only if the number 'xx' is divisible by 4.)

(b) Prove that for any number n, the sum of the digits of n are divisible by 3 if and only if n is divisible by 3.

4 Just Can't Wait

Joel lives in Berkeley. He mainly commutes by public transport, i.e., bus and BART. He hates waiting while transferring, and he usually plans his trip so that he can get on his next vehicle immediately after he gets off the previous one (zero transfer time, i.e. if he gets off his previous vehicle at 7:00am he gets on his next vehicle at 7:00am). Tomorrow, Joel needs to take an AC Transit bus from his home stop to the Downtown Berkeley BART station, then take BART into San Francisco.

(a) The bus arrives at Joel's home stop every 22 minutes from 6:05am onwards, and it takes 10 minutes to get to the Downtown Berkeley BART station. The train arrives at the station every 8 minutes from 4:25am onwards. What time is the earliest bus he can take to be able to transfer to the train immediately? Show your work. (Find the answer without listing all the schedules. Hint: derive an equation relating the bus number and train number and then work in modular arithmetic to get rid of one of the variables to give a set of possible train numbers.)

(b) Joel has to take a Muni bus after he gets off the train in San Francisco. The commute time on BART is 33 minutes, and the Muni bus arrives at the San Francisco BART station every 17 minutes from 7:12am onwards. What time is the earliest bus he could take from Berkeley to ensure zero transfer time for both transfers? If all bus/BART services stop just before midnight, is it the only bus he can take that day? Show your work.

5 Fermat's Little Theorem

Fermat's Little Theorem states that for any prime p and any $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$. Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

6 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 $x+1; x+2; x+3;$ $: : : x+k$ 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.

7 Unique Prime Factorization

We proved in lecture that every positive integer has a factorization into primes. Using the techniques in this course, we can show that this factorization is unique, up to reordering the factors!

Recall from lecture that we defined a prime number p to be a positive integer whose only positive factors are 1 and p.

In this problem, you should not assume that the positive integers have unique prime factorization.

(a) Let p and q be distinct primes. Show that $p \nmid q$.

(b) Prove that if a and b are positive integers such that $p \mid ab$, then $p \mid a$ or $p \mid b$. (Hint: Use the Extended Euclidean algorithm: There are integers x, y such that $ax + py = \gcd(a, p)$.)

(c) Show that the prime factorization of a positive integer n is unique up to reordering the factors. (Hint: Suppose that there were two prime factorizations of n. Use the previous parts to show that the factorizations are the same.)

8 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 $(p-1)! = 1 \cdot 2 \ldots \cdot p-1$ 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 $(p-1)! \pmod{q}$?