Discussion 3B

CS 70, Summer 2024

1 Chinese Remainder Theorem

Consider a natural number which is one more than a multiple of 3, three more than a multiple of 7, and four more than a multiple of 11. In this question we'll find the smallest such number satisfying these conditions.

The above conditions can be written as the following system of linear congruences, where x is our unknown number.

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 3 \pmod 7 \\ x &\equiv 4 \pmod{11}. \end{aligned}$$

(a) Suppose that you have three natural numbers a, b, and c such that the following are true.

$$a \equiv 1 \pmod 3 \qquad a \equiv 0 \pmod 7 \qquad a \equiv 0 \pmod{11} \tag{1}$$
$$b \equiv 0 \pmod 3 \qquad b \equiv 1 \pmod 7 \qquad b \equiv 0 \pmod{11} \tag{2}$$
$$c \equiv 0 \pmod 3 \qquad c \equiv 0 \pmod 7 \qquad c \equiv 1 \pmod{11}. \tag{3}$$

Use a, b, and c to construct a solution x to the system of linear congruences.

(b) In this part and the following parts, we will construct the numbers a, b, and c satisfying these properties.

Find a natural number a satisfying (1). That is, find a such that $a \equiv 1 \pmod 3$ and a is a multiple of 7 and 11.

(*Hint*: Start with a number which is a multiple of both 7 and 11. Find a number to multiply this number by so that it becomes equivalent to 1 modulo 3.)

(c) Find a natural number b satisfying (2). That is, find b such that $b \equiv 1 \pmod 7$ and b is a multiple of 3 and 11.

(d) Find a natural number c satisfying (3). That is, find c such that $c \equiv 1 \pmod{11}$ and c is a multiple of 3 and 7.

(e) Use your a, b, and c, as well as your work in part **(a)**, to find the smallest positive integer x which satisfies the system of linear congruences.

2 Fermat's Littler Theorem

In lecture, we proved Fermat's Little Theorem. Here, we'll prove a slightly weaker version. In particular, we'll prove that if a has a multiplicative inverse modulo m, then it can be written in the form a^k for some $k \geq 0$.

(a) Prove that for any $n \in \mathbb{N}$, if a^{-1} exists modulo m, then $(a^n)^{-1} \equiv (a^{-1})^n \pmod{m}$. We will write such an element as a^{-n}. You may assume that the standard exponent rules continue to hold with negative exponents.

(b) Consider the infinite sequence $a \bmod m, a^2 \bmod m, a^3 \bmod m, a^4 \bmod m, \ldots$

Prove that this sequence has repetitions.

(c) Let $i < j \in \mathbb{N}^+$ be two indices where the sequence repeats. That is, $a^i \equiv a^j \pmod{m}$. Find the value of $a^{j-i} \pmod{m}$.

(d) Prove that $a^{-1} \equiv a^k \pmod{m}$ for some $k \in \mathbb{N}$.

3 Party Trick

In this question, we'll see how we can use the Chinese Remainder Theorem, modular exponentiation, and Fermat's little theorem to find the last digits of very large numbers.

As an example, we'll find the last digit of $x = 7^{482}$.

(a) Explain which modulus we need to evaluate x under to find its last digit.

(b) Find $x \bmod 2$.

(c) Find $x \bmod 5$.

(d) Use parts **(a)**, **(b)**, **(c)** to find the last digit of x.