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.

 $x \equiv 1 \pmod{3}$ $x \equiv 3 \pmod{7}$ $x \equiv 4 \pmod{11}$.

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



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

$$c \equiv 0 \pmod{3}$$
 $c \equiv 0 \pmod{7}$ $c \equiv 1 \pmod{11}$. (3)

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

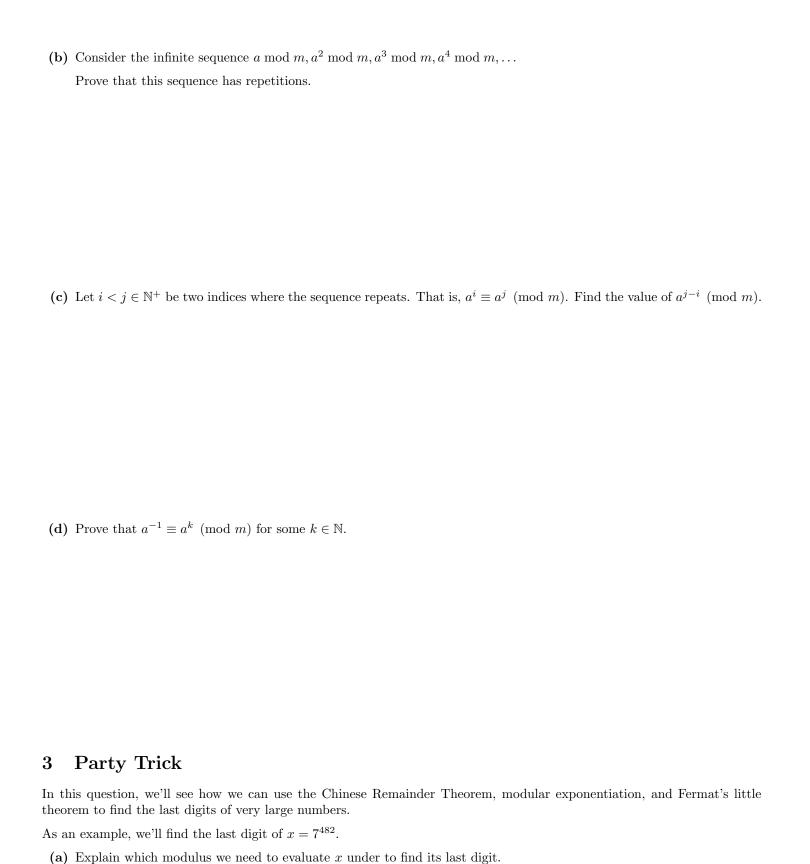
(b) In this part and the following parts, we will construct the numbers a, b, and c satisfying these properties.

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 $k \ge 0$.	
(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)	Find $x \mod 2$.
(c)	Find $x \mod 5$.
(d)	Use parts (a), (b), (c) to find the last digit of x .