CS 70 Discrete Mathematics and Probability Theory
Spring 2021

DIS 3B

1 Baby Fermat

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions. (**Hint:** Consider the Pigeonhole Principle.)

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

2 Euler's Totient Function

Euler's totient function is defined as follows:

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

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof:

For m, n such that $\texttt{gcd}(m,n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

(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) Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod{p}$? *(Hint: use Fermat's Little Theorem.)*

(d) Let b be a positive integer whose prime factors are $p_1, p_2, \ldots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

Show that for any a relatively prime to b, the following holds:

$$\forall i \in \{1, 2, \ldots, k\}, \; a^{\phi(b)} \equiv 1 \pmod{p_i}$$

3 Chinese Remainder Theorem Practice

In this question, you will solve for a natural number x such that,

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned} \tag{1}$$

(a) Suppose you find 3 natural numbers a, b, c that satisfy the following properties:

$$a \equiv 2 \pmod 3 \; ; \; a \equiv 0 \pmod 5 \; ; \; a \equiv 0 \pmod 7, \tag{2}$$

$$b \equiv 0 \pmod 3 \; ; \; b \equiv 3 \pmod 5 \; ; \; b \equiv 0 \pmod 7, \tag{3}$$

$$c \equiv 0 \pmod 3 \; ; \; c \equiv 0 \pmod 5 \; ; \; c \equiv 4 \pmod 7. \tag{4}$$

Show how you can use the knowledge of a, b and c to compute an x that satisfies (1).

In the following parts, you will compute natural numbers a, b and c that satisfy the above 3 conditions and use them to find an x that indeed satisfies (1).

(b) Find a natural number a that satisfies (2). In particular, an a such that $a \equiv 2 \pmod 3$ and is a multiple of 5 and 7. It may help to approach the following problem first:

(b.i) Find a^*, the multiplicative inverse of 5×7 modulo 3. What do you see when you compute $(5 \times 7) \times a^*$ modulo 3, 5 and 7? What can you then say about $(5 \times 7) \times (2 \times a^*)$?

(c) Find a natural number b that satisfies (3). In other words: $b \equiv 3 \pmod 5$ and is a multiple of 3 and 7.

(d) Find a natural number c that satisfies (4). That is, c is a multiple of 3 and 5 and $\equiv 4 \pmod 7$.

(e) Putting together your answers for Part (a), (b), (c) and (d), report an x that indeed satisfies (1).