1 Chinese Remainder Theorem Practice

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

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 4 \pmod{7}$$  \hspace{1cm} (1)

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

$$a \equiv 2 \pmod{3} ; a \equiv 0 \pmod{5} ; a \equiv 0 \pmod{7}, \hspace{1cm} (2)$$
$$b \equiv 0 \pmod{3} ; b \equiv 3 \pmod{5} ; b \equiv 0 \pmod{7}, \hspace{1cm} (3)$$
$$c \equiv 0 \pmod{3} ; c \equiv 0 \pmod{5} ; c \equiv 4 \pmod{7}. \hspace{1cm} (4)$$

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 $5 \times 7$ modulo 3. What do you see when you compute $(5 \times 7) \times a^* \pmod{3, 5, 7}$? 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 $c \equiv 4 \pmod{7}$.

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

In this problem we will find \(3^{302} \mod 385\).

(a) Write 385 as a product of prime numbers in the form \(385 = p_1 \times p_2 \times p_3\).

(b) Use Fermat’s Little Theorem to find \(3^{302} \mod p_1\), \(3^{302} \mod p_2\), and \(3^{302} \mod p_3\).

(c) Let \(x = 3^{302}\). Use part (b) to express the problem as a system of congruences (modular equations \(\mod 385\)). Solve the system using the Chinese Remainder Theorem. What is \(3^{302} \mod 385\)?

3 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. 

\textbf{(Hint:} Consider the Pigeonhole Principle.\textbf{)}

(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 \(j\)?