1 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:

$x = a + b + c$

$x \bmod 3 \equiv 2 = a \bmod 3 + b \bmod 3 + c \bmod 3$

$x \bmod 5 \equiv 3 = a \bmod 5 + b \bmod 5 + c \bmod 5 \equiv 3 \bmod 5$

$x \bmod 7 \equiv 4$

2 mod 3

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

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

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

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

$x = a + b + c \mod (3 \cdot 5 \cdot 7)$ $\qquad a + b + c \bmod 3 \equiv 2 \bmod 3$

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:

$35 \bmod 3 = 2$ $\qquad 35 \equiv 2 \bmod 3$

(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 $(5 \times 7) \times (2 \times a^*)$?

$5 \times 7 = 35 \equiv 0 \bmod 5$, $\equiv 0 \bmod 7$

$35 a^* \equiv 1 \bmod 3 \Rightarrow 2a^* \equiv 1 \Rightarrow a^* \equiv 2^{-1} \equiv \boxed{2} \bmod 3$

$2 \times 70 \bmod 3 \equiv 2 \bmod 3$
$2 \times 70 \bmod 5 \equiv 0 \bmod 5$
$2 \times 70 \bmod 7 \equiv 0 \bmod 7$

(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.

$21 \bmod 5 \equiv 1 \bmod 5$ $\qquad 3 \cdot 7 \cdot a^* \equiv 21 a^* \equiv 1 \bmod 5$

$\boxed{63} \bmod 5 \equiv 3 \bmod 5$ $\qquad 3 \cdot 7 \cdot 3a^* \equiv 3 \cdot 7 \cdot 3 = 63$ $\qquad a^* \equiv (21)^{-1} \equiv (1)^{-1} \equiv 1 \bmod 5$ $\Rightarrow 3 \cancel{3a^*} \equiv 3 \bmod 5$

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

$15 a^* \equiv 1 \bmod 7 \Rightarrow a^* \equiv 1 \bmod 7$
$\Rightarrow 4a^* \equiv 4 \bmod 7$ $\qquad \boxed{60}$

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

$35 + 63 + 60 = 263 \bmod 105 \equiv 53 \bmod 105$

$53 \equiv 2 \bmod 3$
$53 \equiv 3 \bmod 5$
$53 \equiv 4 \bmod 7$

$$\begin{aligned} x &\equiv b_1 \mod m_1 \\ x &\equiv b_2 \mod m_2 \\ &\vdots \\ x &\equiv b_n \mod m_n \end{aligned}$$

$$x + 3y = 4$$
$$y - x = 1$$

$$M = \prod_{i=1}^{n} m_i$$

$$\sum_{i=1}^{n} \left[b_i \underbrace{\left(\frac{M}{m_i}\right)\left(\left(\frac{M}{m_i}\right)^{-1} \mod m_i\right)}_{\substack{a_i \equiv 1 \mod m_i \\ \equiv 0 \mod m_{j \neq i}}} \right]$$

$b_1 \mod m_1$, $0 \mod m_2$, $\vdots$, $0 \mod m_n$

$0 \mod m_1$, $b_2 \mod m_2$, $0 \mod m_3$, $\vdots$, $0 \mod m_n$

$0 \mod m_1$, $\vdots$, $0 \mod m_{i-1}$, $1 \mod m_i$, $0 \mod m_{i+1}$, $\vdots$, $0 \mod m_n$

(*) Notes switch a_i & b_i

$\cancel{4}, \cancel{11}, \cancel{18}, \cancel{25}, \cancel{32}, \cancel{39}, \cancel{46}, 53, \cancel{59},$

2c Contd.

$$a_1 = \left(\frac{385}{5}\right) a_1^* \equiv 77 \cdot 3 \equiv 231$$

$$a_2 = \left(\frac{385}{7}\right) a_2^* \equiv 55 \cdot 6 \equiv 330$$

$$a_3 = \left(\frac{385}{11}\right) a_3^* \equiv 35 \cdot 6 \equiv 210$$

154
275
350
779

DON'T DO THIS!

$\equiv 2 \cdot 4 \equiv 3 \mod 5$

$\equiv 6 \cdot 6 \equiv 1 \mod 7$

$\equiv 2 \cdot 6 \equiv 1 \mod 11$

$$\therefore\ x = b_1 a_1 + b_2 a_2 + b_3 a_3 = 4 \cdot 231 + 2 \cdot 330 + 9 \cdot 210 \mod 385$$
$$\equiv 154 + 275 + 350 \mod 385$$
$$\equiv 779 \mod 385$$
$$\equiv \boxed{9 \mod 385}$$

SCRATCH WORK

924
770
154

1890
1540
350

770
385
1155

660
385
275

2 CRT Decomposition

$2 \cdot 3 \equiv 6 \equiv 5+1 \equiv 1 \bmod 5$

2^{-1}

$$\begin{array}{r} 50 \\ 6\,\overline{)302} \\ 300 \\ \hline 2 \end{array}$$

In this problem we will find $3^{302} \pmod{385}$.

(a) Write 385 as a product of prime numbers in the form $385 = \overset{5}{p_1} \times \overset{7}{p_2} \times \overset{11}{p_3}$.

$3^{302} \equiv (\overset{1^{75}}{\cancel{3^4}})^{75} 3^2 \equiv 1 \cdot 3^2 \equiv 4 \bmod 5$

$3^{302} \overset{1}{\equiv} (\cancel{3^6})^{50} 3^2 \equiv 9 \equiv 2 \bmod 7$

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

$3^{302} \bmod 5$, $3^4 \bmod 5 = 1$

$3^{302} \equiv (3^{10})^{30} 3^2 \equiv 9 \bmod 11$

55
$= 56 - 1$

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

$x = \sum a_i b_i \pmod M$
$= 4 \cdot 3 + 2 \cdot 6 + 9 \cdot 6 \bmod 385$
$= 12 + 12 + 54$
$= 78 \bmod 385$ WRONG

$x \equiv 4 \bmod 5$

$x \equiv 2 \bmod 7$

$x \equiv 9 \bmod 11$

$a_1^* \equiv \left(\frac{385}{5}\right)^{-1} \bmod 5 \equiv 77^{-1} \equiv 2^{-1} \equiv 3 \bmod 5$

55^{-1}
$\equiv 6^{-1}$
$\equiv 6$
$6 \cdot 6$
$= 36$
$\equiv 1 \bmod 7$

3 Baby Fermat

$a_2^* \equiv \left(\frac{385}{7}\right)^{-1} \bmod 7 \equiv 55^{-1} \equiv (-1)^{-1} \equiv -1 \equiv 6 \bmod 7$

$a_3^* \equiv 35^{-1} \bmod 11 \equiv 2^{-1} \equiv 6 \bmod 11$ (CONTINUED ABOVE)

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?