Chinese Remainder Theorem Practice

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

$$\underline{x \equiv 2 \pmod{3}}$$

$$\underline{x \equiv 3 \pmod{5}}$$

$$\underline{x \equiv 4 \pmod{7}}$$
(1)

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

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

$$\chi = a + b + c \mod (3.5.7)$$
 at $b + c \mod 3 \equiv 2 \mod 3$

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 = 2 mod3 35 mod 3 = 2
 - (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 $(5 \times 7) \times (2 \times a^*)$? $5x7 = 35 = 0 \mod 5$ $0 \mod 7$ $35a^{+} = 1 \mod 3 = 2a^{+} = 1 = 2 \mod 3$ $2x70 \mod 3 = 2 \mod 3$ $2x70 \mod 5 = 0 \mod 5$ $2x70 \mod 5 = 0 \mod 5$ $2x70 \mod 5 = 0 \mod 5$ 2×70 mod 3 = 2mod 3
- (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. The world $a \equiv 1 \pmod{5}$ 21 mod 5 =1 mod 5 3 and 7. 2.7.0 = 210 = | mod5
- (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* = 1 mod 7 => a* =1 mod 7 => ua* = u mod7
- (e) Putting together your answers for Part (a), (b), (c) and (d), report an x that indeed satisfies (1). = 263 mod 105 = 53 mod 105

CS 70, Fall 2020, DIS 04A
$$53 = 2 \mod 3$$
 $53 = 3 \mod 5$ $53 = 4 \mod 7$

$$x \equiv b_1 \mod m_1$$

$$x \equiv b_2 \mod m_2$$

$$y - x = 1$$

$$x \equiv b_1 \mod m_2$$

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

$$D \mod m_{i}$$

(Notes switch a: & b;

$$2c \text{ Contd.}$$

$$\alpha_{1} = \left(\frac{385}{5}\right) \alpha_{1}^{*} \equiv 77.3 \equiv 231$$

$$\alpha_{2} = \left(\frac{385}{7}\right) \alpha_{2}^{*} \equiv 55.6 \equiv 330$$

$$\alpha_{3} = \left(\frac{385}{11}\right) \alpha_{3}^{*} \equiv 35.6 \equiv 210$$

$$2c \text{ Contd.}$$

$$2d \text{ DON'T DO THIS!}$$

$$\equiv 2.4 \equiv 3 \text{ mod 5}$$

$$\equiv 6.6 \equiv 1 \text{ mod 7}$$

$$\equiv 2.6 \equiv 1 \text{ mod II}$$

$$\therefore x = b_1 a_1 + b_2 a_2 + b_3 a_3 = 4.231 + 2.330 + 9.210 \mod{385}$$

$$= 154 + 275 + 350 \mod{385}$$

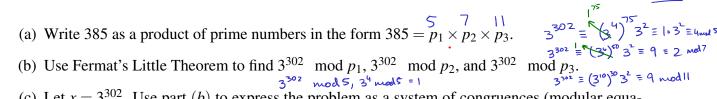
$$= 779 \mod{385}$$

$$= 9 \mod{385}$$

$$= 9 \mod{385}$$

CRT Decomposition

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



(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? M = 385

Baby Fermat
$$a_2 = \frac{385}{5}$$
 mod $5 = 77$ $= 2$ $= 3$ mod 5 $= 9$ mod $=$

can be written as $a^k \pmod{m}$ for some k > 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?

CS 70, Fall 2020, DIS 04A