# CS2214B - Assignment 2

Ali Al-Musawi

04/02/2020

## Question 1

We first show that if $p$ is a prime number and $a$ is an integer not divisible by $p$, then there exists a multiplicative inverse $b$ such that $ab \equiv 1 \pmod{p}$. Note that by indivisibility, we know that $a$ and $p$ are co-primes. From here, we proceed into the proof:

*Proof.*

$$\gcd(a, p) = 1 \text{ (Co-Primes)}$$
$$\Rightarrow \exists b, c \in \mathbb{Z} : ab + pc = 1 \text{ (Bezout's Identity)}$$
$$\Rightarrow ab - 1 = -pc \equiv 0 \mod p \text{ (multiple of p)}$$
$$\therefore ab - 1 \equiv 0 \mod p$$
$$\Rightarrow ab \equiv 1 \mod p$$

As such, we have proven that for every integer $a$ not divisible by $p$, there exists a multipliative inverse. Next, we prove given the above result, for every non-zero integer in modulo $p$, there exists a multiplicative inverse. Note that since $p$ is a prime, all non-zero integers $a$ in $\mathbb{Z}_p$ are co-primes with $p$, so $\gcd(a, p) = 1$. By universal generalization, for all non-zero integers in $\mathbb{Z}_p$, the above result holds. $\square$

## Question 2

In this question, we have a linear system of congruences:

$$x = 3 \mod 5$$

$$x = 7 \mod 12$$

$$x = 8 \mod 13$$

Using, this system, we need to find the number $r \in \mathbb{Z}_{780}$ such that $x \equiv r \mod 780$. We start out by solving the system above. Using the *Chinese Remainder Theorem* for three equations, n = 3:

$$x = \sum_{i=1}^{n} r_i M_i y_i$$

and $r_i$ is the ith remainder, $M_i$ is the product of modulos divided by the ith modulo $m_i$, and $y_i$ is the inverse of $M_i$ in the ith modulo $m_i$. The first two factors are easy to compute. The following table outlines what we need to find:

| $i$ | $r_i$ | $m_i$ | $M_i$ | $y_i$ |
|---|---|---|---|---|
| 1 | 3 | 5 | $\frac{5\times12\times13}{5} = 156$ | ? |
| 2 | 7 | 12 | $\frac{5\times12\times13}{12} = 65$ | ? |
| 3 | 8 | 13 | $\frac{5\times12\times13}{13} = 60$ | ? |

Table 1: Variables of Interest in Applying CRT

Applying the *Extended Euclidean Algorithm*, we find the inverses of each $M_i$:

- $y_1 \in \mathbb{Z}_5$:

$$\gcd(156, 5) : -$$

$$156 = 30 \times 5 + 6 \Rightarrow 6 = 156 - 30 \times 5$$

$$5 = 0 \times 6 + 5$$

$$6 = 1 \times 5 + 1 \Rightarrow 1 = 6 - 5 \times 1$$

since $\gcd(156, 5) = 1$, then 156 has an inverse. Using back-substitution:

$$\therefore 1 = 1 \times 156 - 30 \times 5 \Rightarrow y_1 = 1 \text{ (Question 1 Result)}$$

- $y_2 \in \mathbb{Z}_{12}$:

$$\gcd(65, 12) : -$$

$$65 = 5 \times 12 + 5 \Rightarrow 5 = 65 - 12 \times 5$$

$$12 = 2 \times 5 + 2 \Rightarrow 2 = 12 - 2 \times 5$$

$$5 = 2 \times 2 + 1 \Rightarrow 1 = 5 - 2 \times 2$$

since $\gcd(65, 12) = 1$, then 65 has an inverse. Using back-substitution:

$$\therefore 1 = 1 \times 5 - 2 \times (12 - 2 \times 5) = 5 \times 5 - 2 \times 12$$

$$1 = 5 \times (65 - 12 \times 5) - 2 \times 12 = 5 \times 65 - 27 \times 12$$

$$\therefore y_2 = 5 \text{ (Question 1 Result)}$$

- $y_3 \in \mathbb{Z}_{13}$:

$$\gcd(60, 13) : -$$

$$60 = 4 \times 13 + 8 \Rightarrow 8 = 60 - 4 \times 13$$

$$13 = 1 \times 8 + 5 \Rightarrow 5 = 13 - 1 \times 8$$

$$8 = 1 \times 5 + 3 \Rightarrow 3 = 8 - 1 \times 5$$

$$5 = 1 \times 3 + 2 \Rightarrow 2 = 5 - 1 \times 3$$

$$3 = 1 \times 2 + 1 \Rightarrow 1 = 3 - 1 \times 2$$

since $\gcd(60, 13) = 1$, then 60 has an inverse. Using back-substitution:

$$\therefore 1 = 1 \times 3 - 1 \times (5 - 1 \times 3) = 2 \times 3 - 1 \times 5$$

$$\therefore 1 = 2 \times (8 - 1 \times 5) - 1 \times 5 = 2 \times 8 - 3 \times 5$$

$$\therefore 1 = 2 \times 8 - 3 \times (13 - 1 \times 8) = 5 \times 8 - 3 \times 13$$

$$\therefore 1 = 5 \times (60 - 4 \times 13) - 3 \times 13 = 5 \times 60 - 15 \times 23$$

$$\therefore y_3 = 5 \text{ (Question 1 Result)}$$

We have completed the table:

| $i$ | $r_i$ | $m_i$ | $M_i$ | $y_i$ |
|---|---|---|---|---|
| 1 | 3 | 5 | $\frac{5\times12\times13}{5} = 156$ | 1 |
| 2 | 7 | 12 | $\frac{5\times12\times13}{12} = 65$ | 5 |
| 3 | 8 | 13 | $\frac{5\times12\times13}{13} = 60$ | 5 |

Table 2: Variables of Interest in Applying CRT

Therefore, using *Chinese Remiander Theorem*, we have:

$$x = 3 \times 156 \times 1 + 7 \times 65 \times 5 + 8 \times 60 \times 5 = 5143$$

Now, we answer the question: for which $r$ is $5143 \equiv r \mod 780$? This is a matter of division:

$$5143 = 6 \times 780 + 463 \Rightarrow r = 463$$

## Question 3

We will prove the contrapositive instead. That is, if $\mathbb{P}$ is the set of prime integers, then our claim is as follows:

$$n \notin \mathbb{P} \Rightarrow 2^n - 1 \notin \mathbb{P}$$

It immediately follows that $\exists a, b \in \mathbb{Z} : n = ab, a > 1, b > 1$. From here, we proceed into the proof:

*Proof.*

$$2^a - 1 \equiv 0 \mod 2^a - 1 \text{ (Definition of Modulo)}$$

$$2^a \equiv 1 \mod 2^a - 1 \text{ (Adding 1 to both sides)}$$

$$(2^a)^b \equiv 1^b = 1 \mod 2^a - 1 \text{ (Exponentiation)}$$

$$(2^a)^b - 1 \equiv 0 \mod 2^a - 1 \text{ (Re-Writing)}$$

$$2^a - 1 | (2^a)^b - 1 \text{ (Congruency to 0)}$$

$$a > 1, b > 1 \Rightarrow (2^a)^b - 1 > 2^a - 1 > 1$$

$$\therefore (2^a)^b - 1 = 2^{ab} - 1 = 2^n - 1 \notin \mathbb{P} \text{ (Existence of a factor other than 1)}$$

$$2^n - 1 \in \mathbb{P} \Rightarrow n \in \mathbb{P} \text{ (By Contrapositive)}$$

□

## Question 4

To prove that no such pair of integer coefficients $(a, b)$ exists, we first reduce the problem. Note if this pair exists, then $b = 1$ becasue:

$$p(mb) = m^2b^2 + mba + b = b(m^2b + ma + 1), m \in \mathbb{Z}, m > 0$$

Thus if $b \neq 1$, then $p(mb)$ is composite. Note $b \neq -1$ because if it were, then either $m^2b + ma + 1 < 0$ or $m^2b + ma + 1 \geq 0$. In the first case, the two negatives cancel, and it reduces to the case $b = 1$. In the second case, the product results in a zero or a negative, which is not a prime. Below, we prove that $p(n)$ is not a prime-generating function.

*Proof.* First, assume that p(n) is a prime-generating function. Then, we must have $p(n) = n^2 + an + 1$ is a prime for all $n > 0$. Let us examine the function in two cases:

- $a \geq 0$: Note that:

$$p(1) = 1^2 + (1)a + 1 = a + 2$$

$$p(2) = 2^2 + (2)a + 1 = 2a + 5$$

  By our assumption, $p(1)$ and $p(2)$ are primes. Therefore, $p(1) \times p(2)$ is a composite number. But note:

$$p(1) \times p(2) = (a + 2)(2a + 5) = (a + 3)^2 + a(a + 3) + 1 = p(a + 3)$$

  But by our assumption, $p(n)$ is a prime for all $n > 0$, hence a contradiction.

- $a < 0$: Note that:

$$p(1 - a) = (1 - a)^2 + a(1 - a) + 1 = 2 - a$$

$$p(2 - a) = (2 - a)^2 + a(2 - a) + 1 = 5 - 2a$$

  By our assumption, $p(1 - a)$ and $p(2 - a)$ are primes. Therefore, $p(1 - a) \times p(2 - a)$ is a composite number. But note:

$$p(1 - a) \times p(2 - a) = (2 - a)(5 - 2a) = (3 - 2a)^2 + a(3 - 2a) + 1 = p(3 - 2a)$$

  But by our assumption, $p(n)$ is a prime for all $n > 0$, hence a contradiction.

Assuming $p(n)$ is a prime generating function for all $n > 0$, we have reached a contradiction for all integers $a$. By contradiction, we conclude there does not exists $a$ (and hence $b$) such that $p(n)$ is a prime-generating function. □