MAT315 - HW3

Quentin Vilchez – 1002562586

March 5, 2018

1. (a) $3x \equiv 1 \pmod{11}$, we know that $(11, 3) = 1$
   This equation is soluble.
   $\exists x, y \in Z$ such that $3x - 11y = 1$.
   $(4, 1)$ are solutions. Therefore $3x \equiv 1 \pmod{11} \iff x \equiv 4 \pmod{11}$.

   (b) $2x \equiv 1 \pmod{11}$, we know that $(11, 2) = 1$
   This equation is soluble.
   $\exists x, y \in Z$ such that $2x - 11y = 1$.
   $(6, 1)$ are solutions. Therefore $2x \equiv 1 \pmod{11} \iff x \equiv 6 \pmod{11}$.

   (c) $37x \equiv 2 \pmod{145}$, we know that $(145, 35) = 1$
   This equation is soluble.
   $\exists x, y \in Z$ such that $37x - 145y = 2$.
   $(-94, -24)$ are solutions. Therefore $37x \equiv 2 \pmod{145} \iff x \equiv 51 \pmod{145}$.

   (d) $15x \equiv 5 \pmod{305}$, we know that $(305, 15) = 5$
   This equation is soluble.
   $\exists x, y \in Z$ such that $15x - 305y = 5$.
   $(-20, -1)$ are solutions. Therefore $15x \equiv 5 \pmod{305} \iff x \equiv 285 \pmod{305}$.

   (e) $18x \equiv 6 \pmod{45}$, we know that $(45, 18) = 9$
   This equation is not soluble.

2. (a)
   $$x \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 \pmod{13}$$
   Then,
   $$x^2 \equiv 0, 1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1 \pmod{13}$$
   So the residue classes of $x^2 \pmod{13}$ are $0, 1, 4, 9, 3, 12, 10$.

   (b) $2x^2 \equiv 1 \pmod{13}$, we have $(13, 2) = 1$, so the equation seems soluble.
   $(-6, -1)$ is a solution. $2x^2 \equiv 1 \pmod{13} \iff x^2 \equiv 7 \pmod{13}$. But in (a) we saw that $x^2 \not\equiv 7 \pmod{13}$. Therefore the equation is not soluble.

(c) Suppose there exists $x, y \in Z$ such that $13x^3 - 11y^2 = 1$. Then we must have,

$$\begin{aligned} -11y^2 &\equiv 1 \pmod{13} \\ 11y^2 &\equiv 12 \pmod{13} \end{aligned} \tag{1}$$

Now $(12, 13) = 1$. Therefore, $\exists k, l \in Z$ such that $11k - 13l = 12$.
$(72, 60)$ is a solution. Hence, $11y^2 \equiv 12 \pmod{13} \iff y^2 \equiv 7 \pmod{13}$. But in (a) we saw that $y^2 \not\equiv 7 \pmod{13}$. Therefore this equation has no solutions in $\mathbb{Z}$.

(d) It is easy (but tedious) to check that the residue classes for $x^3 \pmod{11}$ are $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$.

$$13x^3 - 11y^2 \equiv 1 \pmod{11} \iff 13x^3 \equiv 1 \pmod{11}$$

This equation is soluble since $(13, 11) = 1$ and the residue classes for $x^3 \pmod{13}$ are the same as $x \pmod{13}$.

3. (a)

$$x^2 \equiv 1 \pmod{p} \Leftrightarrow (x-1)(x+1) \equiv 0 \pmod{p}$$
$$\Leftrightarrow p \mid (x-1)(x+1) \Rightarrow p \mid (x-1) \text{ or } (x+1)$$

$$\begin{aligned} x - 1 &\equiv 0 \pmod{p} & \qquad x + 1 &\equiv 0 \pmod{p} \\ x &\equiv 1 \pmod{p} & x &\equiv -1 \pmod{p} \end{aligned}$$

(b) This is true.

i. *Existence:*
We have $a \equiv a \pmod{p}$ and $(a, p) = 1$.
Therefore there exists x and y such that $ax - py = 1 \Rightarrow ax \equiv 1 \pmod{p}$.
We may simply take $b = x \pmod{p}$.

ii. *Uniqueness:*
Suppose there exists $1 \leq b_1, b_2 \leq p-1$ such that $ab_i \equiv 1 \pmod{p}$ for $i = 1, 2$.
Then, $a(b_1 - b_2) \equiv 0 \pmod{p}$. So $p \mid (b_1 - b_2)$ hence $b_1 \equiv b_2 \pmod{13} \Rightarrow b_1 = b_2$.

(c) We will first show that $(p-2)! \equiv 1 \pmod{p}$.
We first note that there is an even number of terms in the product $(p-2)!$ (since we may neglect the term 1).
By (a), we know that $x^2 \equiv 1 \pmod{p} \Leftrightarrow x \equiv \pm 1 \pmod{p}$, therefore (by (b)) for each term in the product , we can find a unique term (not itself) such that $ab \equiv 1 \pmod{p}$, adding this to the fact that there are an even number of terms in the product $(p-2)!$, we get $(p-2)! \equiv 1 \pmod{p}$.
Now $(p-2)!(p-1) \equiv p - 1 \pmod{p} \equiv -1 \pmod{p}$.

(d) i. Let $R = \{r_1, r_2, \cdots, r_{\phi(p^c)}\}$ be a complete set of residues prime to p_c. Then for each r_i there exists a unique r_j such that $r_j r_i \equiv 1 \pmod{p^c}$ since $(r_i, p^c) = 1$.

ii. Now for $x \in R$, $x^2 \equiv 1 \pmod{p^c} \Leftrightarrow p^c \mid (x+1)(x-1) \Leftrightarrow x = 1$ or $p^c - 1 \Leftrightarrow x \equiv \pm 1 \pmod{p^c}$.

iii. So now we consider $K = r_1 r_2 \cdots r_{\phi(p^c)}$, where $r_1 = 1$ and $r_{\phi(p^c)} = p^c - 1$. It is easy to see that $K' = r_2 \cdots r_{\phi(p^c)-1} \equiv 1 \pmod{p^c}$ since K' has an even number of terms ($\phi(p^c) = p^c - p^{c-1}$ which is even) and by (ii). Therefore $K \equiv r_{\phi(p^c)} \pmod{p^c} \equiv -1 \pmod{p^c}$.

(e) A complete set of residues prime to 15 is $\{1, 2, 4, 7, 8, 11, 13, 14\}$
$1 \times 2 \times 4 \times 7 \times 8 \times 11 \times 13 \times 14 = 896896$ and

$$192192 \equiv 1 \pmod{15}$$

4. (a) $\phi(n) = \frac{1}{3}n \Leftrightarrow n = 2^{c_1}3^{c_2}$ where $c_i \geq 1$. Indeed,

$$\phi(n) = n \prod_{p|n}(1 - \frac{1}{p}) = n \times \frac{1}{2} \times \frac{2}{3} = \frac{1}{3}n$$

(b) $\phi(n) = \frac{1}{24}n$ is not possible.
Write
$$\phi(n) = n \prod_{p|n}(1 - \frac{1}{p}) = n \times \frac{(p_1 - 1)(p_2 - 1)\cdots(p_k - 1)}{p_1 \cdots p_k}$$
where p_i are the prime divisors of n.
Let $A = \frac{(p_1-1)(p_2-1)\cdots(p_k-1)}{p_1 \cdots p_k}$
Now we know that all prime numbers greater than 2 are odd.
So if n is odd our numerator in A cannot be 1 since $(p_i - 1, p_1 \cdots p_k) = 1$ for all $i = 1, \cdots k$ (except in the case of (a)).
If n is even, then our numerator can be written as $2k$ where $k \geq 1$ and even, and the denominator can be written as $2l$ with $l \geq 1$ and odd. So we would get $A = \frac{2k}{2l} = \frac{k}{l} \neq \frac{1}{24}$.

(c) $\phi(2n) = \phi(n) \Leftrightarrow n$ is odd. Take n odd,

$$\phi(2n) = 2n \prod_i \frac{1}{2} \times (1 - \frac{1}{p_i}) = n \prod_{p|n}(1 - \frac{1}{p}) = \phi(n)$$

where p_i are the prime divisors of n.

5. (a) Suppose f is multiplicative. Consider $n_1, n_2 \in \mathbb{Z}$ such that $(n_1, n_2) = 1$.
If $d \mid n_1 n_2$, then d can be uniquely written as $d = k_1 k_2$ whenr $k_i \mid n_i$, since n_1

and n_2 are coprime.

$$\begin{aligned} g(n_1 n_2) &= \sum_{d|n_1 n_2} f(d) = \sum_{k_1|n_1, k_2|n_2} f(k_1 k_2) \\ &= \sum_{k_1|n_1, k_2|n_2} f(k_1) f(k_2) = \sum_{k_1|n_1} f(k_1) \sum_{k_2|n_2} f(k_2) = g(n_1) g(n_2) \end{aligned} \tag{2}$$

(b) We know that the identity function is multiplicative. Therefore, by (a) $\sigma(n) = \sum_{d|n} d$ is multiplicative.

(c) The divisors of p^c are $\{1, 2, \cdots, p^{c-1}, p^c\}$. So,

$$\sigma(p^c) = \sum_{d|p^c} d = \sum_{n=0}^{c} p^n$$

(d) Let $p_1^{c_1} \cdots p_k^{c_k}$ be the prime decomposition of n. We get,

$$\sigma(n) = \sigma(p_1^{c_1} \cdots p_k^{c_k}) = \sigma(p_1^{c_1}) \cdots \sigma(p_k^{c_k}) = \prod_{i=1}^{k} \left[\sum_{n=0}^{c_i} p_i^n \right]$$

6. (a) If x_0, x_1 both are solutions, then $x_0 \equiv x_1 \pmod{n_i}$ for all i. We know that $(n_i, n_j) = 1$ for $i \neq j$. Hence, by theorem 53 of Hardy-Wright,

$$x_0 \equiv x_1 \pmod{n_i n_j}$$

and since $(\prod_{i \neq j} n_i, n_j) = 1$, we have

$$x_0 \equiv x_1 \pmod{N}$$

(b) i. $N_i x_i \equiv ci \pmod{n_i}$, $(N_i, n_i) = 1$, therefore this equation is soluble and has a unique solution $\pmod{n_i}$.

ii. $N_j x_j \equiv 0 \pmod{n_i}$ since $N_j = \prod_{i \neq j} n_i$, so $\forall i \neq j \; n_i \mid N_j$.

iii. $x = \sum N_i x_i$, by (i) there exists x_i such that $N_i x_i \equiv ci \pmod{n_i}$, and by (ii) we have

$$x \equiv N_i x_i \pmod{n_i} \equiv ci \pmod{n_i}$$

So x is a solution to the system of congruences.

(c)

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases}$$

Define $N_1 = 4 \times 3$, $N_2 = 4 \times 5$, $N_3 = 3 \times 5$. We get

$$\begin{cases} N_1 x_1 \equiv 1 \pmod 5 \Leftrightarrow x_1 \equiv 3 \pmod 5 \\ N_2 x_2 \equiv 2 \pmod 3 \Leftrightarrow x_2 \equiv 1 \pmod 3 \\ N_3 x_3 \equiv 3 \pmod 4 \Leftrightarrow x_3 \equiv 1 \pmod 4 \end{cases}$$

So $x = 20 \times 1 + 15 \times 1 + 12 \times 3 = 71$ is a solution.