Chapter 3

Date: Feb 23 Made by Eric

Definitions and Theorems

Definition 1. *Let* $a, b, n \in \mathbb{Z}$. $a \equiv_n b \iff n|a-b$

Lemma 1. $\equiv_n$ *is an equivalence relation.*

Proof. $\forall a \in \mathbb{Z}, n|0 = a - a \implies a \equiv_n a$

$a \equiv_n b \implies n|a-b \implies n|b-a \implies b \equiv_n a$

$a \equiv_n b$ and $b \equiv_n c \implies n|a-b$ and $n|b-c \implies n|a-c \implies a \equiv_n c$ ■

From now on, we call the cosets of $n\mathbb{Z}$ containing a, which is an equivalent class given by $\equiv_n$, congruent class $[a]$

Lemma 2. *Let* $a \equiv_n b$

$$-a \equiv_n -b \text{ and } c \equiv_n d \implies a + c \equiv_n b + d \text{ and } c \equiv_n d \implies ac \equiv_n bd$$

Proof. $a \equiv_n b \implies [a] = [b]$

$[-a] = -[a] = -[b] = [-b] \implies -a \equiv_n -b$

$c \equiv_n d \implies [c] = [d]$

$[a + c] = [a] + [c] = [b] + [d] = [b + d] \implies a + c \equiv_n b + d$

$[ac] = [a][c] = [b][d] \implies ac \equiv_n bd$

■

Lemma 3. *Let* $a, b, c, n \in \mathbb{Z}$

$$ac \equiv_{nc} bc \iff a \equiv_n b$$

Proof. $nc|bc - ac \iff n|b - a$ ■

Lemma 4. *Let* $a \equiv_n b$, *and* $f(x) \in \mathbb{Z}[x]$

$$f(a) \equiv_n f(b)$$

Proof. $f(a) = \sum c_i a^i \equiv_n \sum c_i b^i = f(b)$ ■

Lemma 5. *Let* n *have the prime factorization* $n = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$

$$a \equiv_n b \iff \forall 1 \leq i \leq n, a \equiv_{p_i^{c_i}} b$$

Proof. $(\longrightarrow)$

$\forall 1 \leq i \leq n, p_i^{c_i} | n$ and $n | a - b \implies p_i^{c_i} | a - b$

$(\longleftarrow)$

Denote $a - b$ with r

We prove by induction.

Base step: $p_1^{c_1} p_2^{c_2} | r$

$p_1^{c_1} | r$ and $p_2^{c_2} | r$ and $gcd(p_1^{c_1}, p_2^{c_2}) = 1 \implies p_1^{c_1} p_2^{c_2} | r$

Induction step: $p_1^{c_1} p_2^{c_2} \cdots p_{k-1}^{c_{k-1}} | r \longrightarrow p_1^{c_1} p_2^{c_2} \cdots p_{k-1}^{c_{k-1}} p_k^{c_k} | r$

$p_1^{c_1} p_2^{c_2} \cdots p_{k-1}^{c_{k-1}} | r$ and $p_k^{c_k} | r$ and $gcd(p_1^{c_1} p_2^{c_2} \cdots p_{k-1}^{c_{k-1}}, p_k^{c_k}) = 1 \implies p_1^{c_1} p_2^{c_2} \cdots p_{k-1}^{c_{k-1}} p_k^{c_k} | r$ ■

Theorem 6. *Let $d = gcd(a, n)$, where $d = \alpha a + \beta n$*

$ax \equiv_n b$ have solution of x only if $d | b$, where $b = cd$, and the solution is $x = c\alpha + \frac{n}{d} t, \forall t \in \mathbb{Z}$

Proof. We now prove $d | b \implies x = c\alpha + \frac{n}{d} t, \forall t \in \mathbb{Z}$

$b = cd = c\alpha a + c\beta n$

$ax \equiv_n b = c\alpha a + c\beta n \iff n | c\alpha a + c\beta n - ax \iff n | a(c\alpha - x) \iff \frac{n}{d} | \frac{a}{d}(c\alpha - x)$

$gcd(\frac{n}{d}, \frac{a}{d}) = 1$ and $\frac{n}{d} | \frac{a}{d}(c\alpha - x) \implies \frac{n}{d} | c\alpha - x \implies c\alpha - x = \frac{n}{d} t, \forall t \in \mathbb{Z} \implies x = c\alpha + \frac{n}{d} t, \forall t \in \mathbb{Z}$

We now prove $d \not| b \implies$ equation $ax \equiv_n b$ have no solutions

Assume $ax \equiv_n b$

$b - ax = tn, \exists t \in \mathbb{Z} \implies b = ax - tn, \exists t \in \mathbb{Z} \implies d | ax - tn = b$ CaC ■

Notice $x = [c\alpha]$ given by $\equiv_{\frac{n}{d}}$

Theorem 7. ***(Chinese Remainder Theorem)****Let $n_1, n_2, \ldots, n_k \in \mathbb{Z}$ satisfy $\forall 1 \leq i, j \leq k, gcd(n_i, n_j) = 1$. Let $n = n_1 n_2 \cdots n_k$, and $c_i = \frac{n_1 n_2 \cdots n_k}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k$. Let $\{d_i | i \in I\}$ satisfy $c_i d_i \equiv_{n_i} 1$*

The solutions set of the equation set $\{a_1 \equiv_{n_1} x, a_2 \equiv_{n_2} x, \ldots, a_k \equiv_{n_k} x\}$ is $[a_1 c_1 d_1 + a_2 c_2 d_2 + \cdots + a_k c_k d_k]$ given by $\equiv_n$

Proof. We first prove $a_1c_1d_1 + a_2c_2d_2 + \cdots + a_kc_kd_k$ is a solution

Notice $\forall 1 \leq j \leq k, \forall i \neq j, c_i = n_1n_2 \cdots n_{i-1}n_{i+1} \cdots n_k \implies \forall 1 \leq j \leq k, \forall i \neq j, n_j | c_i$

$\forall 1 \leq j \leq k, \forall i \neq j, c_id_i \equiv_{n_i} 1 \implies a_1 \equiv_{n_1} a_ic_id_i$

$\forall 1 \leq j \leq k, \forall i \neq j, n_j | c_i \implies \forall 1 \leq j \leq k, \forall i \neq j, 0 \equiv_{n_j} a_ic_id_i$

Adding the two equations above, we have $\forall 1 \leq j \leq k, a_j \equiv_{n_j} a_1c_1d_1 + a_2c_2d_2 + \cdots + a_kc_kd_k$

We now prove $[a_1c_1d_1 + a_2c_2d_2 + \cdots a_kc_kd_k]$ is contained by the solutions set

$\forall m \in [a_1c_1d_1 + a_2c_2d_2 + \cdots a_kc_kd_k], m = a_1c_1d_1 + a_2c_2d_2 + \cdots a_kc_kd_k + nt, \exists t \in \mathbb{Z}$

$\forall 1 \leq i \leq k, n_i | n_1n_2 \cdots n_k = n \implies \forall t \in \mathbb{Z}, \forall 1 \leq i \leq k, 0 \equiv_{n_i} nt \implies a_i \equiv_{n_i} a_1c_1d_1 + a_2c_2d_2 + \cdots a_kc_kd_k + nt = m$ (done)

We now prove $[a_1c_1d_1 + a_2c_2d_2 + \cdots a_kc_kd_k]$ contains the solution set

Let $x = a_1c_1d_1 + a_2c_2d_2 + \cdots + a_kc_kd_k$, and y be another solution.

$\forall 1 \leq i \leq k, x \equiv_{n_i} a_i \equiv_{n_i} y \implies \forall 1 \leq i \leq k, n_i | y - x$

Because $\forall 1 \leq i, j \leq k, gcd(n_i, n_j) = 1$, so $n = n_1n_2 \cdots n_k | y - x$

So $y = x + nt \in [a_1c_1d_1 + a_2c_2d_2 + \cdots a_kc_kd_k]$ (done)

■

Theorem 8. *Let $n = n_1n_2 \cdots n_k$, where the integer n_i are mutually coprime, and $f(x) \in \mathbb{Z}[x]$. Let N_i be the amount of congruence classes $x \in \mathbb{Z}_{n_i}$ satisfy $f(x) \equiv_{n_i} 0$*

There exists $N_1N_2 \cdots N_k$ amount of congruence classes $x \in \mathbb{Z}_n$ satisfy $f(x) \equiv_n 0$

Proof. Let $S_i = \{[a_{i,1}], \ldots [a_{i,N_i}]\}$ be the cogruence classes $x \in \mathbb{Z}_{n_i}$ satisfy $f(x) \equiv_{n_i} 0$ for each $1 \leq i \leq k$

Let $U = \{[c_1], \ldots [c_L]\}$ be the congruence classes $x \in Z_n$ satisfy $f(x) \equiv_n 0$

We now prove $\forall \{j_1, \ldots j_k | \forall 1 \leq i \leq k, 1 \leq j_i \leq N_i\}, \bigcap_{1 \leq i \leq k} [a_{i,j_i}]$ is a congruence class $x \in \mathbb{Z}_n$

$\forall x \in \bigcap_{1 \leq i \leq k} [a_{i,j_i}], x \equiv_{n_i} a_{i,j_i} \iff x \in [a_{1,j_1}c_1d_1 + \cdots + a_{k,j_k}c_kd_k]$ given by $\equiv_{n=n_1 \cdots n_k}$, where $\forall 1 \leq i \leq k, c_i = \frac{n_1 \cdots n_k}{n_i}$ and $\forall 1 \leq i \leq k, c_id_i \equiv_{n_i} 1$, by **(Chinese Remainder Theorem)**

So, $\bigcap_{1 \leq i \leq k} [a_{i,j_i}] = [a_{1,j_1}c_1d_1 + \cdots + a_{k,j_k}c_kd_k]$ given by $\equiv_n$ (done)

Let $K = \{\bigcap_{1\le i\le k}[a_{i,j_i}] | \forall 1 \le i \le k, 1 \le j_i \le N_i\}$

We now prove $\{\bigcap_{1\le i\le k}[a_{i,j_i}] | \forall 1 \le i \le k, 1 \le j_i \le N_i\} = K = U$

We notice $x \in \bigcap_{1\le i\le k}[a_{i,j_i}] \iff \forall 1 \le i \le k, x \in [a_{i,j_i}] \iff \forall 1 \le i \le k, f(x) \equiv_{n_i} 0 \iff f(x) \equiv_{n=n_1\cdots n_k} 0 \iff x \in [c], \exists [c] \in U$

And $\forall [c] \in U, x \in [c] \iff f(x) \equiv_{n=n_1\cdots n_k} 0 \iff \forall 1 \le i \le k, f(x) \equiv_{n_i} 0 \iff \exists \{j_1, \dots j_k | \forall 1 \le i \le k, 1 \le j_i \le N_i\}, \forall 1 \le i \le k, x \in [a_{i,j_i}] \iff x \in \bigcap_{1\le i\le k}[a_{i,j_i}] \in K$

Then $\forall \bigcap_{1\le i\le k}[a_{i,j_i}] \in K, \forall x \in \bigcap_{1\le i\le k}[a_{i,j_i}], x \in [c], \exists [c] \in U \implies \forall \bigcap_{1\le i\le k}[a_{i,j_i}] \in K, \exists [c] \in U, \bigcap_{1\le i\le k}[a_{i,j_i}] \subseteq [c]$

And $\forall [c] \in U, \forall x \in [c], x \in \bigcap_{1\le i\le k}[a_{i,j_i}], \exists \bigcap_{1\le i\le k}[a_{i,j_i}] \in K \implies \forall [c] \in U, \exists \bigcap_{1\le i\le k}[a_{i,j_i}] \in K, [c] \subseteq \bigcap_{1\le i\le k}[a_{i,j_i}]$

Because both $\bigcap_{1\le i\le k}[a_{i,j_i}]$ and $[c]$ are congruence classes $x \in \mathbb{Z}_n$, so $\bigcap_{1\le i\le k}[a_{i,j_i}] \subseteq [c]$ or $[c] \subseteq \bigcap_{1\le i\le k}[a_{i,j_i}] \implies \bigcap_{1\le i\le k}[a_{i,j_i}] = [c]$

$\forall [c] \in U, \exists \bigcap_{1\le i\le k}[a_{i,j_i}] \in K, [c] \subseteq \bigcap_{1\le i\le k}[a_{i,j_i}] \implies U \subseteq K$

$\forall [c] \in U, \exists \bigcap_{1\le i\le k}[a_{i,j_i}] \in K, [c] \subseteq \bigcap_{1\le i\le k}[a_{i,j_i}] \implies K \subseteq U$ (done)

We now prove $\bigcap_{1\le i\le k}[a_{i,j_i}] = \bigcap_{1\le i\le k}[a_{i,j'_i}] \iff \forall 1 \le i \le k, j_i = j'_i$, which says $U = K$ have $N_1 N_2 \cdots N_k$ distinct elements, congruence classes $x \in \mathbb{Z}_n$.

$(\longleftarrow)$

$\forall 1 \le i \le k, j_i = j'_i \implies \forall \le i \le k, [a_{i,j_i}] = [a_{i,j'_i}] \implies \bigcap_{1\le i\le k}[a_{i,j_i}] = \bigcap_{1\le i\le k}[a_{i,j'_i}]$

$(\longrightarrow)$

Assume $\exists 1 \le r \le k, j_r \ne j'_r$

Then $[a_{r,j_r}] \ne [a_{r,j'_r}]$

So $a_{r,j_r} \not\equiv_{n_r} a_{r,j'_r}$

$x \in \bigcap_{1\le i\le k}[a_{i,j_i}] \implies x \in [a_{r,j_r}] \implies x \equiv_{n_r} a_{r,j_r} \implies x \not\equiv_{n_r} a_{r,j'_r} \implies x \notin [a_{r,j'_r}] \implies x \notin \bigcap_{1\le i\le k}[a_{i,j'_i}]$ CaC (done)

■

Exercises

3.8

Solve $x \equiv_4 1, x \equiv_3 2, x \equiv_5 3$

Proof. $x \in [3 * 15 + 20 + 4 * 12]$ given by $\equiv_{4*3*5}$ ■

3.9

Solve $x \equiv_7 2, x \equiv_9 7, x \equiv_4 3$

Proof. $x \in [2 * 36 + 7 * 28 + 1 * 63]$ given by $\equiv_{7*9*4}$ ■

3.10

Solve $3x \equiv_{12} 6, 2x \equiv_7 5, 3x \equiv_5 1$

Proof. $3x \equiv_{12} 6 \iff x \equiv_4 2$

$2x \equiv_7 5 \iff x \equiv_7 6$

$3x \equiv_5 1 \iff x \equiv_5 2$

$x \in [35 * 2 + 20 + 28 * 12]$ given by $\equiv_{4*7*5}$ ■

3.11

Solve $91x \equiv_{440} 419$

Proof. $91x \equiv_{440} 419 \iff 91x \equiv_5 419$ and $91x \equiv_8 419$ and $91x \equiv_{11} 419$

$91x \equiv_5 419 \iff x \equiv_5 4$

$91x \equiv_8 419 \iff 3x \equiv_8 3 \iff x \equiv_8 1$

$91x \equiv_{11} 419 \iff 3x \equiv_{11} 1 \iff x \equiv_{11} 4$

$x \in [88 * 3 + 55 * 7 + 40 * 10]$ given by 440 ■

3.12

Solve $x^2 + 2x + 2 \equiv_5 0, 7x \equiv_{11} 3$

Proof. $x^2 + 2x + 2 \equiv_5 0 \iff x \equiv_5 1$ or 2

$7x \equiv_{11} 3 \iff x \equiv_{11} 2$ **($\mathbb{Z}_{11}$ is a field)**

$x \equiv_5 1$ and $x \equiv_{11} 2 \iff x \in [1 * 11 + 7 * 5]$

$x \equiv_5 2$ and $x \equiv_{11} 2 \iff x \in [2 * 11 + 7 * 5]$

So $x^2 + 2x + 2 \equiv_5 0$ and $7x \equiv_1 13 \iff x \in [1 * 11 + 7 * 5] \cup [2 * 11 + 7 * 5]$ given by $\mathbb{Z}_{55}$ ■

3.13

How many classes of solutions are there for each of the following cogruence?

(a) $x^2 - 1 \equiv_{168} 0$

(b)$x^2 + 1 \equiv_{70} 0$

(c)$x^2 + x + 1 \equiv_{91} 0$

(d)$x^3 + 1 \equiv_{140} 0$

(a)

Proof. $(x-1)(x+1) = x^2 - 1 \equiv_{168} 0 \iff (x-1)(x+1) \equiv_3 0$ and $(x-1)(x+1) \equiv_8 0$ and $(x-1)(x+1) \equiv_7 0$

$\mathbb{Z}_3$ and $\mathbb{Z}_7$ are fields, so they are integral domains.

So $(x-1)(x+1) \equiv_3 0 \iff x \equiv_3 1$ or 2

And $(x-1)(x+1) \equiv_7 0 \iff x \equiv_7 1$ or 6

$(x-1)(x+1) \equiv_8 0 \iff x \equiv_8 1$ or 7 or 3 or 5

By Theorem 8, we know there are $(2)(2)(4)$ congruence classes of solution. ■

(b)

Proof. $x^2 + 1 \equiv_{70} 0 \implies x^2 + 1 \equiv_4 0$ and $x^2 + 1 \equiv_3 0$ and $x^2 + 1 \equiv_5 0$

$x_1^2 \equiv_4 0 \iff x \equiv_4 3$

$x^2 + 1 \equiv_3 0$ have no solution.

$x^2 + 1 \equiv_5 0 \iff x \equiv_5 2$ or 3

By Theorem 8, we know there are $(1)(0)(2)$ congruence classes of solution. ■

(c)

Proof. $x^2+x+1 \equiv_{91} 0 \iff x^2+x+1 \equiv_7 0$ and $x^2+x+1 \equiv_{13} 0$

$x^2+x+1 \equiv_7 0 \iff x \equiv_7 2$ or 4

$x^2+x+1 \equiv_{13} 0 \iff x \equiv_{13} 3$ or 9

By Theorem 8, we know there are $(2)(2)$ congruence classes of solution. ■

(d)

Proof. $x^3+1 \equiv_{140} 0 \iff x^3+1 \equiv_4 0$ and $x^3+1 \equiv_5 0$ and $x^3+1 \equiv_7 0$

$x^3+1 \equiv_4 0 \iff x \equiv_4 3$

$x^3+1 \equiv_5 0 \iff x \equiv_5 4$

$x^3+1 \equiv_7 0 \iff x \equiv_7 3$ or 5 or 6

By Theorem 8, we know there are $(1)(1)(3)$ congruence clases of slution. ■

3.14

Solve the following congruence equations

(a) $x \equiv_6 1$ **and** $x \equiv_{14} 5$ **and** $x \equiv_{21} 4$
(b) $x \equiv_6 1$ **and** $x \equiv_{14} 5$ **and** $x \equiv_{21} -2$
(c) $x \equiv_{40} 13$ **and** $x \equiv_{44} 5$ **and** $x \equiv_{275} 38$
(d)$x^2 \equiv_{10} 9$ **and** $7x \equiv_{24} 19$ **and** $2x \equiv_{45} -1$

(a)

Proof. $x \equiv_6 1 \iff x \equiv_2 1$ and $x \equiv_3 1$

$x \equiv_{14} 5 \iff x \equiv_2 1 \equiv_2 5$ and $x \equiv_7 5$

$x \equiv_{21} 4 \iff x \equiv_3 1 \equiv_3 4$ and $x \equiv_7 4$

$x \equiv_7 5 \not\equiv_7 4 \equiv_7 x$ CaC

So no solution ■

(b)

Proof. $x \equiv_6 1 \iff x \equiv_2 1$ and $x \equiv_3 1$

$x \equiv_{14} 5 \iff x \equiv_2 1 \equiv_2 5$ and $x \equiv_7 5$

$x \equiv_{21} -2 \iff x \equiv_3 1 \equiv_3 -2$ and $x \equiv_7 5 \equiv_7 -2$

So $x \equiv_6 1$ and $x \equiv_{14} 5$ and $x \equiv_{21} -2 \iff x \equiv_2 1$ and $x \equiv_3 1$ and $x \equiv_7 5$

The solution is $[1 * 21 + 2 * 14 + (-5) * 6]$ given by $\equiv_{42=(2)(3)(7)}$ ■

(c)

Proof. $x \equiv_{40} 13 \iff x \equiv_8 5 \equiv_8 13$ and $x \equiv_5 3 \equiv_5 13$

$x \equiv_{44} 5 \iff x \equiv_4 1 \equiv_4 5$ and $x \equiv_{11} 5$

$x \equiv_{275} 38 \iff x \equiv_5 3$ and $x \equiv_{11} 5$

So $x \equiv_{40} 13$ and $x \equiv_{44} 5$ and $x \equiv_{275} 38 \iff x \equiv_8 5$ and $x \equiv_5 3$ and $x \equiv_4 1$ and $x \equiv_{11} 5$

Notice $x \equiv_8 5$ and $x \equiv_4 1 \implies x \equiv_8 5$

So $x \equiv_{40} 13$ and $x \equiv_{44} 5$ and $x \equiv_{275} 38 \iff x \equiv_8 5$ and $x \equiv_5 3$ and $x \equiv_{11} 5$

The solution is $[(-5) * 55 + 1 * 88 + 7 * 40]$ given by $\equiv_{440}$

■

(d)

Proof. $x^2 \equiv_{10} 9 \iff x \equiv_{10} 3$ or $x \equiv_{10} 7 \iff (x \equiv_2 1$ and $x \equiv_5 3)$ or $(x \equiv_2 1$ and $x \equiv_5 2)$

$7x \equiv_{24} 19 \iff 7x \equiv_8 3$ and $7x \equiv_3 1 \iff x \equiv_8 5$ and $x \equiv_3 1$

$2x \equiv_{45} -1 \iff 2x \equiv_9 8$ and $2x \equiv_5 4 \iff x \equiv_9 4$ and $x \equiv_5 2$

So $x^2 \equiv_{10} 9$ and $7x \equiv_{24} 19$ and $2x \equiv_{45} -1 \iff x \equiv_2 1$ and $x \equiv_5 2$ and $x \equiv_8 5$ and $x \equiv_3 1$ and $x \equiv_9 4$ and $x \equiv_5 2 \iff x \equiv_8 5$ and $x \equiv_9 4$ and $x \equiv_5 2$

The solution is $[1 * 45 + 1 * 40 + 1 * 72]$ given by $\equiv_{360}$ ■

3.16

Solve the following set of simultaneous congruence

(a) $x \equiv_4 1$ **and** $x \equiv_3 2$ **and** $x \equiv_5 3$

(b) $3x \equiv_{12} 6$ **and** $2x \equiv_7 5$ **and** $3x \equiv_5 1$

(c) $x^2 \equiv_6 3$ **and** $x^3 \equiv_5 3$

(a)

Proof. The solution is $[(-1) * 15 + 1 * 20 + 4 * 12]$ given by $\equiv_{60}$ ■

(b)

Proof. $3x \equiv_{12} 6 \iff x \equiv_4 2$

$2x \equiv_7 5 \iff x \equiv_7 6$

$3x \equiv_5 1 \iff x \equiv_5 2$

The solution is $[2 * 35 + 1 * 20 + 4 * 28]$ given by $\equiv_{140}$ ■

(c)

Proof. $x^2 \equiv_6 3 \iff x \equiv_6 3$

$x^3 \equiv_5 3 \iff x \equiv_5 2$

The solution is $[(-3) * 5 + 2 * 6]$ given by $\equiv_{30}$ ■

3.17

Solve $x^3 + 3x - 8 \equiv_{33} 0$

Proof. $x^3 + 3x - 8 \equiv_{33} 0 \iff x^3 + 3x \equiv_3 2$ and $x^3 + 3x \equiv_{11} 8$

$x^3 + 3x \equiv_3 2 \iff x \equiv_3 2$

$x^3 + 3x \equiv_{11} 8 \iff x \equiv_{11} 8$ or 9

The solution set is $[1 * 11 + 10 * 3] \cup [1 * 11 + 14 * 3]$ ■

3.18 (This is probably not gonna take place in test, I made a mistake)

Seven thieves try to share a hoard of gold bars equally between them- selves. Unfortunately, six bars are left over, and in the fight over them, one thief is killed. The remaining six thieves, still unable to share the bars equally since two are left over, again fight, and another is killed. When the remaining five share the bars, one bar is left over, and it is only after yet another thief is killed that an equal sharing is possible. What is the minimum number of bars which allows this to happen?

Proof. Let x be the number of bars.

We know $x \equiv_7 6$ and $x \equiv_6 2$ and $x \equiv_5 1$ and $x \equiv_4 0$

$x \equiv_6 2 \iff x \equiv_2 0$ and $x \equiv_3 2$

$x \equiv_7 6$ and $x \equiv_6 2$ and $x \equiv_5 1$ and $x \equiv_4 0 \iff x \equiv_4 0$ and $x \equiv_3 2$ and $x \equiv_5 1$ and $x \equiv_7 6$

The solution is $[4 * 105 + 1 * 140 + (-1) * 84 + 5 * 60]$ given by $\equiv_{420}$

356 is the minimum positive x ■

3.19

For each $k \in \mathbb{N}$, find $x \in \mathbb{N}$, such $\forall u \in \mathbb{N} : 1 \leq u \leq k, x + u$ can not be expressed as a product of two distinct primes.

Proof. Let $\{p_1, \dots p_k\}$ be a set of distinct primes.

We know the equation set$\{x \equiv_{p_1^2} -1, x \equiv_{p_2^2} -2, \dots, x \equiv_{p_k^2} -k\}$ have some solution y by **Chinese Remainder Theorem**

$\forall 1 \leq i \leq k, y + i \equiv_{p_i^2} 0 \implies \forall 1 \leq i \leq k, p_i^2 | x + i$

Then if $\exists c, d \in \mathbb{N} : cd = y + i, (p_i | c$ and $p_i | d)$ or $p_i^2 | c$ or $p_i^2 | d$

Assume $\exists 1 \leq u \leq k, y + u$ can be expressed as a product of two distinct primes

Let $y + u = cd, \exists c, d$ two primes.

$p_u^2 | y + u \implies (p_u | c$ and $p_u | d)$ or $p_u^2 | c$ CaC or $p_u^2 | d$ CaC

Because the last two statement CaC, we now have $p_u | c$ and $p_u | d$

Because both c and d are primes, so $c = p_u = d$ CaC

■

3.21

Let $n = n_1 \cdots n_k$, where $n_1, \dots, n_k$ are mutually coprime. For each $1 \leq i \leq k$, let $\{a_{i,1}, \dots, a_{i,n_i}\}$ satisfy $\forall u \in \mathbb{N}, \exists 1 \leq s \leq n_i, a_{i,s} \equiv_{n_i} u$

Show $\forall r \in \mathbb{N}, \exists \{j_1, \dots j_k | \forall 1 \leq i \leq k, 1 \leq j_i \leq n_i\}, r \equiv_n a_{1,j_1} + a_{2,j_2} n_1 + a_{3,j_3} n_1 n_2 + \cdots + a_{k,j_k} n_1 \cdots n_{k-1}$

Proof. For each r

Let j_1 satisfy $a_{1,j_1} \equiv_{n_1} r$

Let j_2 satisfy $n_1 a_{2,j_2} \equiv_{n_2} r - a_{1,j_1}$

Let j_3 satisfy $n_1 n_2 a_{3,j_3} \equiv_{n_3} r - a_{1,j_1} - n_1 a_{2,j_2}$

For each $3 < i \leq k$, pick the j_i satisfy $n_1 \cdots n_{i-1} a_{i,j_i} \equiv_{n_i} r - a_{1,j_1} + a_{2,j_2} n_1 + \cdots + a_{i,j_{i-1}} n_1 n_2 \cdots n_{i-2}$

Such j_i must exists, because $\{a_{i,1}, \ldots, a_{i,n_i}\}$ satisfy $\forall u \in \mathbb{N}, \exists 1 \leq s \leq n_i, a_{i,s} \equiv_{n_i} u$ and $\forall 1 \leq i \leq k, gcd(n_1 \cdots n_{i-1}, n_i) = 1$

We see $\forall 1 \leq i \leq k, r \equiv_{n_i} a_{1,j_1} + a_{2,j_2} n_1 + a_{3,j_3} n_1 n_2 + \cdots + a_{i,j_i} n_1 \cdots n_{i-1}$

This give us $\forall 1 \leq i \leq k, r \equiv_{n_i} a_{1,j_1} + a_{2,j_2} n_1 + a_{3,j_3} n_1 n_2 + \cdots + a_{i,j_i} n_1 \cdots n_{i-1} + a_{i+1,j_{i+1}} n_1 \cdots n_i + a_{k,j_k} n_1 \cdots n_{i-1} n_i n_{i+1} \cdots n_{k-1}$

So $r \equiv_{n=n_1 \cdots n_k} a_{1,j_1} + a_{2,j_2} n_1 + a_{3,j_3} n_1 n_2 + \cdots + a_{k,j_k} n_1 \cdots n_{k-1}$ ■