Review:

Def: A congruence of the form

(*) $$ax \equiv c \pmod{n}$$

is called a LINEAR CONGRUENCE in the variable x.

Ex: $$17x \equiv 1 \pmod{30}$$

Prop 3.53: The linear congruence (*) has a solution $x = x_0$, if and only if the linear Diophantine equation

(**) $$ax + ny = c$$

has a solution $(x, y) = (x_0, y_0)$, for some integer y_0.

Ex: $17x_0 \equiv 1 \pmod{30}$ if and only if

$17x_0 + 30y_0 = 1$, for some $y_0 \in \mathbb{Z}$.

Thm 2.31: (i) The linear Diophantine eq (**) has a solution if and only if $\gcd(a, n) \mid c$.

(ii) Set $d := \gcd(a, n)$. If (x_0, y_0) is a particular solution of (**), then the general solution is

$$(x, y) = \left(x_0 + k\frac{n}{d}, y_0 - k\frac{a}{d}\right), \quad k \in \mathbb{Z}.$$

Thm: (i) The linear congruence

$$\circledast \quad ax \equiv c \pmod{n}$$

has a solution, if and only if $\gcd(a, n) \mid c$.

(ii) Set $d := \gcd(a, n)$. If $x_0 \in \mathbb{Z}$ is a particular solution of $\circledast$, then the general solution is

$$x \equiv x_0 \pmod{\frac{n}{d}}.$$

I.e. the set of sol'n of $[a][x] = [c]$ in $\mathbb{Z}_n$ is

$$[x_0], \left[x_0 + \frac{n}{d}\right], \ldots, \left[x_0 + (d-1)\frac{n}{d}\right].$$

There are precisely d solutions.

Ex: Solve (+) $17x \equiv 1 \pmod{30}$

We will solve

$$17x + 30y = 1. \qquad 30y_i + 17x_i = r_i$$

y_i	x_i	r_i	q_i
1	0	30	
0	1	17	
1	-1	13	1
-1	2	4	1

4	-7	1	3
		0	

gcd(30, 17)

$$\underbrace{30\cdot 4}_{120} + \underbrace{(-7)17}_{-119} = 1 \quad \checkmark$$

Particular Sol'n to $17x \equiv 1 \pmod{30}$ is

$$x_0 = -7 \equiv 23 \pmod{30}.$$

$$[17]^{-1} = [23] \pmod{30}$$

There is a unique sol'n in $\mathbb{Z}_{30}$ to $[17][x] = [1]$,

because $d = \gcd(17, 30) = \underline{1}$.

Ex: Find all sol'n of

$$(\#) \qquad \overbrace{51}^{a} x \equiv \overbrace{3}^{c} \pmod{\overbrace{30}^{n}}$$

$x_0 \equiv 23$ is a particular sol'n to (#) since it is a sol'n of (+).

Set $d = \gcd(a, n) = \gcd(\underbrace{51}_{3\cdot 17}, 30) = 3$

The general sol'n of (#) is

$x \equiv 23 \quad (\bmod \frac{30}{3} = 10)$

$\qquad\qquad\qquad\qquad\qquad\qquad \overset{\shortparallel}{\frac{n}{d}}$

In $\mathbb{Z}_{30}$

$[x_0] = 23, \quad [x_1] = [3], \quad [x_2] = [\underset{\underset{23}{\shortparallel}}{x_0} + 2 \cdot \frac{30}{3}] = [13].$

There are precisely 3 solution to

$$[51][x] = [3] \quad \text{in } \mathbb{Z}_{30}.$$

<u>Cor (of the above Thm)</u> Let n be a positive integer. Then $[a]$ has a multiplicative inverse in $\mathbb{Z}_n$, if and only if $\gcd(a, n) = 1$.

<u>Ex</u>: $[17]$ has a mult inverse in $\mathbb{Z}_{30}$

$[3]$ does not have a mult inverse in $\mathbb{Z}_{30}$, since $\gcd(3, 30) = 3 \neq 1$.

Ex: Find all the solutions to

$$x^2 - 9 \equiv 0 \pmod{17}.$$

$$[x]^2 - [9] = [0] \text{ in } \mathbb{Z}_{17}.$$

Answer:

$$x^2 - 9 = x^2 - 3^2 = (x-3)(x+3) \overset{\text{want}}{\equiv} 0 \pmod{17}.$$

So $17 \mid (x-3)(x+3)$.

This means that $17 \mid x-3$ <u>OR</u> $17 \mid x+3$, since is prime. So

$x \equiv 3 \pmod{17}$ OR $x \equiv -3 \pmod{17}$.

There are precisely two sol'ns in $\mathbb{Z}_{17}$. $\square$

Ex: Find all solutions of

$$(**) \quad \underbrace{x^{12}}_{\equiv x^2 \pmod{11}} + \overbrace{x^{11}}^{\equiv x \pmod{11}} - x - 4 \equiv 0 \pmod{11}.$$

11 is a prime. Fermat's Little Theorem implies that if $[x] \neq [0] \pmod{11}$, then $[x]^{10} = [1] \pmod{11}$.

More generally, $[x]^{11} = [x] \pmod{11}$

So *** is equivalent to

$$x^2 - 4 \equiv 0 \pmod{11}.$$

2^2

$$(x-2)(x+2) \equiv 0 \pmod{11}$$

So $11 \mid x-2$ or $11 \mid x+2$.

So $x \equiv 2 \pmod{11}$ or $x \equiv -2 \pmod{11}$

In $\mathbb{Z}_{11}$ there are precisely two solutions to

$$[x]^2 - [4] = [0] \quad (\text{in } \mathbb{Z}_{11})$$

Sec 3.6 The Chinese Remainder Theorem:

Ex: Solve the simultaneous linear congruence

$$x \equiv 3 \pmod 5 \qquad (1)$$

$$x \equiv 4 \pmod 7 \qquad (2).$$

Answer:

$(1) \Leftrightarrow (1')$ $\quad x = 3 + 5y.$

Plug the above into eq (2) to get

$$3 + 5y \equiv 4 \pmod 7$$

$$5y \equiv 4 - 3 = 1 \pmod 7.$$

$y_0 = 3$ is a particular sol'n.

$$y = \underbrace{y_0}_{3} + 7z, \qquad z \in \mathbb{Z}$$

So in $(1')$ we get that

$$x = 3 + 5(3 + 7z) = 18 + 35z, \quad z \in \mathbb{Z}.$$

So $\boxed{x \equiv 18 \pmod{\underbrace{5 \cdot 7}_{N}}}.$

Observe: If $n \mid N$, n, N are positive integers then we have a well defined function

$$g: \mathbb{Z}_N \longrightarrow \mathbb{Z}_n$$

$$\boxed{\begin{array}{l} \text{sending } [x]_N \text{ to } [x]_n \\ \text{For example} \\ \quad g: \mathbb{Z}_{35} \longrightarrow \mathbb{Z}_5 \\ \qquad [18]_{35} \longmapsto [18]_5 = [3]_5 \\ \text{or} \\ \quad g: \mathbb{Z}_{35} \longrightarrow \mathbb{Z}_7 \\ \qquad [18]_{35} \longmapsto [18]_7 = [4]_7 \end{array}}$$

The function g is well defined, since if $[x_1]_N \overset{\text{In } \mathbb{Z}_N.}{=} [x_2]_N$, then $N \mid x_2 - x_1$. So $n \mid (x_2 - x_1)$ (because $n \mid N$).

So $[x_1]_n = [x_2]_n$ in $\mathbb{Z}_n$.

Con: We have a well defined function $\mathbb{Z} \xrightarrow{\tilde{f}}$

$f : \mathbb{Z}_{35} \longrightarrow \underbrace{\mathbb{Z}_5 \times \mathbb{Z}_7}_{\{([a]_5, [b]_7) : \text{ such that } [a]_5 \in \mathbb{Z}_5 \text{ and } [a]_7 \in \mathbb{Z}_7\}}$

sending $[x]_{35}$ to $\underbrace{([x]_5, [x]_7)}_{\overset{\text{def}}{=} f([x]_{35})}$.

Question: Is $([3]_5, [4]_7)$ a value of f?

$\Leftrightarrow$ Is there $[x]_{35} \in \mathbb{Z}_{35}$ such that

$f([x]_{35}) = ([x]_5, [x]_7) = ([3]_5, [4]_7)$?

$\Leftrightarrow$ Is there x, such that

$x \equiv 3 \pmod 5$

$x \equiv 4 \pmod 7$.

Answer: Yes $[x] = [18] \in \mathbb{Z}_{35}$ is a sol'n, as we saw above.

Theorem: (3.62) Let n_1, n_2 be positive integers.

(a) If $\gcd(n_1, n_2) = 1$, then the simultaneous congruences

(1) $x \equiv a_1 \pmod{n_1}$

(2) $x \equiv a_2 \pmod{n_2}$

have a solution for every $a_1, a_2 \in \mathbb{Z}$.

(b) If $x = x_0$ is a particular sol'n, then the general solution is

$x \equiv x_0 \pmod{n_1 \cdot n_2}$.

Proof: (a)

(1) $x \equiv a_1 \pmod{n_1}$

$$x = a_1 + y n_1, \quad y \in \mathbb{Z}.$$

Substitute into (2)

$$a_1 + y n_1 \equiv a_2 \pmod{n_2}. \quad \text{So}$$

$$a_1 + y n_1 = a_2 + n_2 z, \quad z \in \mathbb{Z}.$$

$$y n_1 = (a_2 - a_1) + n_2 z$$

$\Longleftrightarrow$

$$[y][n_1] = [a_2 - a_1] \pmod{n_2}.$$

We assumed that $\gcd(n_1, n_2) = 1$, so $[n_1]^{-1}$ exists in $\mathbb{Z}_{n_2}$. So

$$[y] = [n_1]^{-1}[a_2 - a_1] \text{ in } \mathbb{Z}_{n_2}.$$

So a particular sol'n y_0 exists.

It satisfies that

$$y_0 n_1 = (a_2 - a_1) + n_2 z, \quad z \in \mathbb{Z}.$$

So $\underbrace{a_1 + y_0 n_1}_{x =} = a_2 + n_2 z, \quad z \in \mathbb{Z}.$

(##)

Note that setting $x = a_2 + y_0 n_2$ we get that

$$x \equiv a_1 \pmod{n_1}$$ and

by (H) $x \equiv a_2 \pmod{n_2}$.

So $x = a_2 + y_0 n_1$ is a sol'n.