$$f(x) \equiv 0 \pmod{m}$$

$$m = \prod_{i=1}^{r} p_i^{a_i}$$

Solve each sub-congruence

$$f(x) \equiv 0 \pmod{p_i^{a_i}} \quad i = 1, \ldots, r$$

For every possible combination of sols. to these

$$x \equiv b_i \quad i = 1, \ldots, r$$

apply the C.R.T. will generate a unique congruence class x modulo m that simultaneously satisfies all these

i.e. $p_i^{a_i} \mid f(x)$ for each $i = 1, \ldots, r$.

$$\Rightarrow \left(\prod_{i=1}^{r} p_i^{a_i} \right) \Big| f(x),$$

i.e. $f(x) \equiv 0 \pmod{m}$

Ex 6.1 Solve $34x \equiv 60 \pmod{98}$.

Q7. (should be handled theorem 6.3)

Get the gcd.

$$d = \gcd(34, 98) = 2 \quad \text{and } 2 \mid 60$$

So by Th 6.3 there are two solutions

given by $x \equiv t,\ t+49 \pmod{98}$

where t is the unique solution to the reduced congruence

$$17x \equiv 30 \pmod{49}$$

which is

$$t \equiv 17^{-1} \cdot 30 \pmod{49}$$

?

Can compute 17^{-1} by obtaining a Bezout's identity $17m + 49n = 1$

$$\iff 17m = -n \cdot 49 + 1 \equiv 1 \mod 49$$

$$\iff m \equiv 17^{-1} \pmod{49}$$

B.I. obtained from Euclidean Algorithm for $\gcd(17, 49) = 1$

$$49 = 2 \cdot 17 + 15$$
$$17 = 1 \cdot 15 + 2$$
$$15 = 7 \cdot 2 + 1$$

$$\begin{aligned} 1 &= 15 - 7 \cdot 2 \\ &= 15 - 7 \cdot (17 - 15) \\ &= 8 \cdot 15 - 7 \cdot 17 \\ &= 8 \cdot (49 - 2 \cdot 17) - 7 \cdot 17 \\ &= 8 \cdot 49 - 23 \cdot 17 \end{aligned}$$

So $17^{-1} \equiv -23 \pmod{49}$
$\equiv 26 \pmod{49}$.

So $t \equiv 26 \cdot 30 \pmod{49}$
$\equiv 45$.

So we have the two sols

$$x \equiv 45, \cancel{84}\ 94 \pmod{98}$$

to $34x \equiv 60 \pmod{98}$

Ex 6.2.

Q4. Let x be the number of eggs in the basket.

$$\cancel{x \equiv 1 \pmod 2}$$

$$\cancel{x \equiv 2 \pmod 3}.$$

$$\cancel{x \equiv 3 \pmod 4} \quad *$$

$$x \equiv 4 \pmod 5$$

$$\cancel{x \equiv 5 \pmod 6} \quad *$$

$$x \equiv 0 \pmod 7.$$

$x \equiv 11 \pmod{12}$

Can we apply the CRT straight away? No, as the pairwise coprime condition is not met.

$$x \equiv 3 \pmod 4$$

$$\Rightarrow x = 4 \cdot q + 3$$

$$= 2 \cdot 2q + 2 + 1$$

$$= (2q+1)2 + 1$$

$\Rightarrow x \equiv 1 \pmod 2$

If $x \equiv 5 \pmod 6$

$\Rightarrow x = 6q + 5$

$= 3(2q+1) + 2. \equiv 2 \pmod 3$

$x \equiv 3 \pmod 4$ AND $x \equiv 5 \pmod 6$

Can we ~~re~~ replace these with a single congruence, $\equiv -1 \bmod 4$ $\equiv -1 \bmod 6$

$x = 4q + 3 = 6r + \boxed{5}$

we can bring these together as a single congruence class modulo $12 = \text{lcm}(4,6)$

as

$x \equiv \underline{\ 11\ } \pmod{12}$ $\equiv -1 \bmod 12$

I.e. $x = 12s + 11$

$= 4 \cdot 3s + 2 \cdot 4 + 3$

$= 6 \cdot 2s + 6 + \boxed{5}$

If $x \equiv 3 \pmod 4$

then $x \equiv 3, 7, 11 \pmod{12}$

$x \equiv 5 \pmod 6 \implies x \equiv 5$ or $11 \pmod{12}$

Our problem has become.

$$\underline{b_i}$$

$$x \equiv 4 \pmod 5$$

$$x \equiv 0 \pmod 7$$

$$x \equiv 11 \pmod{12}$$

and 5, 7, 12 <u>are</u> pairwise-coprime.

so the CRT can be applied.

$M = 420$, $M_1 = 84$, $M_2 = 60$, $M_3 = 35$

$$M_1' \equiv 84^{-1} \pmod 5$$
$$\equiv 4^{-1} \pmod 5$$
$$\equiv 4$$

$$M_2' \equiv 60^{-1} \pmod 7$$
$$\equiv 4^{-1} \pmod 7$$
$$\equiv 2. \pmod 7$$

$$M_3' \equiv 35^{-1} \pmod{12}$$
$$\equiv 11^{-1} \pmod{12}$$

$\equiv 11 \pmod{12}$

So by the CRT. the number of eggs x must satisfy

$$x \equiv 4 \cdot 84 \cdot 4 + 0 \cdot 60 \cdot 2 + 11 \cdot 35 \cdot 11 \pmod{420}$$

$$\equiv 5579 \pmod{420}$$

$$\equiv 119 \pmod{420}$$

Q5 Generalisation of the C.R.T. ~~for~~ to non pairwise coprime moduli.

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

Claim: this has a simultaneous solution iff $d \mid a-b$, $d = \gcd(n, m)$.

Moreover, the simulteneous solutions make up a unique congruence class modulo $\operatorname{lcm}(n, m)$.

<u>Thinking</u> If $d = \gcd(n, m)$

then $\exists\ r, s \in \mathbb{Z}$ such that

$$\boxed{d = rn + sm}$$

Well

$\boxed{d \mid a-b}$ means $a - b = qd$. for some $q \in \mathbb{Z}$.

$a \equiv qd + b$ $\qquad$ $b = a - qd$.

$\iff a - b = q(rn + sm)$.

$\iff \boxed{a - qrn} = \boxed{b + qsm}$

$\equiv a \pmod{n}$ $\qquad$ $\equiv b \pmod{m}$

So we've identified a simultaneous solution. $x = a - qrn = b + qsm$

to $x \equiv a \pmod{n}$, $b \pmod{m}$

<u>Second part</u>

Suppose we have <u>two</u>

simultaneous solutions. x, y.

$x \equiv y \equiv a \pmod{n}$, $x \equiv y \equiv b \pmod{m}$

we want $x \equiv y \pmod{\operatorname{lcm}(n, m)}$

$\iff \underline{\operatorname{lcm}(m, n) \mid x - y}$ goal.

$y = q_1 n + a = q_2 m + b$.

$x = r_1 n + a = r_2 m + b$.

So clearly

$x - y = r_1 n + a - (q_1 n + a) = (r_1 - q_1) n$

so $x - y$ is a multiple of n.

<u>AND</u>

$x - y = r_2 m + b - (q_2 m + b) = (r_2 - q_2) m$

so $x - y$ is a multiple of m.

So $x - y$ is a <u>common multiple</u> <u>of n, m.</u>

$\Rightarrow \operatorname{lcm}(n, m) \mid x - y$, by Q13 of Exercises in chapt 2.

$u \mid v \qquad v = q\,u$

A negative example.

$x \equiv 1 \pmod 4$ $\qquad$ $x \equiv 4 \pmod 6$

$\gcd(4,6) = 2$ but $2 \nmid 4-1$

$x \equiv 1 \pmod 4 \Rightarrow x \equiv 1, 5, 9 \pmod{12}$

$x \equiv 4 \pmod 6 \Rightarrow x \equiv 4, 10 \pmod{12}$