Chinese Remainder Theorem (CRT)

$$\begin{aligned} n &\equiv r_1 \pmod{m_1} \\ &\equiv r_2 \pmod{m_2} \\ &\quad\bullet\ \bullet\ \bullet \\ &\equiv r_k \pmod{m_k} \end{aligned}$$

$\gcd(m_i, m_j) = 1$

Chinese Remainder Theorem (CRT)

$n \equiv r_1 \pmod{m_1}$
$\equiv r_2 \pmod{m_2}$
$\bullet \bullet \bullet$
$\equiv r_k \pmod{m_k}$

$\gcd(m_i, m_j) = 1$

- solution:

$m = m_1 m_2 \cdot \cdot \cdot m_k$

$z_i = m / m_i$

$\exists!\ z_i^{-1} \in Z^*_{mi}$ s.t. $z_i \cdot z_i^{-1} \equiv 1 \pmod{m_i}$ (since $\gcd(z_i, m_i) = 1$)

$$n \equiv \sum_{i=1}^{k} z_i \cdot z_i^{-1} \cdot r_i \pmod{m}$$

Chinese Remainder Theorem (CRT)

$$n \equiv r_1 \pmod{m_1}$$
$$\equiv r_2 \pmod{m_2}$$
$$\cdots$$
$$\equiv r_k \pmod{m_k}$$

$\gcd(m_i, m_j) = 1$

- solution:

  $m = m_1 m_2 \cdots m_k$

  $z_i = m / m_i$

  $\exists!\ z_i^{-1} \in Z_{mi}^{*}$ s.t. $z_i \cdot z_i^{-1} \equiv 1 \pmod{m_i}$ (since $\gcd(z_i, m_i) = 1$)

  $$n \equiv \sum_{i=1}^{k} z_i \cdot z_i^{-1} \cdot r_i \pmod{m}$$

- ex: $r_1=1$, $r_2=2$, $r_3=3$

  $m_1=3$, $m_2=5$, $m_3=7$ $\qquad m = 3 \cdot 5 \cdot 7$

Chinese Remainder Theorem (CRT)

$$n \equiv r_1 \pmod{m_1}$$
$$\equiv r_2 \pmod{m_2}$$
$$\cdots$$
$$\equiv r_k \pmod{m_k}$$

$\gcd(m_i, m_j) = 1$

- solution:

$$m = m_1 m_2 \cdots m_k$$

$$z_i = m / m_i$$

$$\exists!\ z_i^{-1} \in Z^*_{mi} \text{ s.t. } z_i \cdot z_i^{-1} \equiv 1 \pmod{m_i} \text{ (since } \gcd(z_i, m_i) = 1)$$

$$n \equiv \sum_{i=1}^{k} z_i \cdot z_i^{-1} \cdot r_i \pmod{m}$$

- ex: $r_1=1$, $r_2=2$, $r_3=3$

$m_1=3$, $m_2=5$, $m_3=7$ $\qquad m = 3 \cdot 5 \cdot 7$

$z_1=35$, $z_2=21$, $z_3=15$

Chinese Remainder Theorem (CRT)

$$n \equiv r_1 \pmod{m_1}$$
$$\equiv r_2 \pmod{m_2}$$
$$\cdots$$
$$\equiv r_k \pmod{m_k}$$

$\gcd(m_i, m_j) = 1$

✧ solution:

$$m = m_1 m_2 \cdots m_k$$

$$z_i = m / m_i$$

$$\exists!\ z_i^{-1} \in Z^*_{mi} \ \text{ s.t. } \ z_i \cdot z_i^{-1} \equiv 1 \pmod{m_i} \ (\text{since } \gcd(z_i, m_i) = 1)$$

$$n \equiv \sum_{i=1}^{k} z_i \cdot z_i^{-1} \cdot r_i \pmod{m}$$

✧ ex: $r_1=1, \quad r_2=2, \quad r_3=3$

$m_1=3, m_2=5, m_3=7$ $\qquad m = 3 \cdot 5 \cdot 7$

$z_1=35, z_2=21, z_3=15$

$z_1^{-1}=2, z_2^{-1}=1, z_3^{-1}=1$ $\qquad 35 \cdot 2 + 3\,(-23) = 1$

Chinese Remainder Theorem (CRT)

$n \equiv r_1 \pmod{m_1}$
$\equiv r_2 \pmod{m_2}$
$\cdots$
$\equiv r_k \pmod{m_k}$

$\gcd(m_i, m_j) = 1$

- solution:

  $m = m_1 m_2 \cdots m_k$

  $z_i = m / m_i$

  $\exists!\ z_i^{-1} \in Z^*_{mi}$ s.t. $z_i \cdot z_i^{-1} \equiv 1 \pmod{m_i}$ (since $\gcd(z_i, m_i) = 1$)

  $$n \equiv \sum_{i=1}^{k} z_i \cdot z_i^{-1} \cdot r_i \pmod{m}$$

- ex: $r_1=1$, $r_2=2$, $r_3=3$

  $m_1=3$, $m_2=5$, $m_3=7$ $\qquad m = 3 \cdot 5 \cdot 7$

  $z_1=35$, $z_2=21$, $z_3=15$

  $z_1^{-1}=2$, $z_2^{-1}=1$, $z_3^{-1}=1$

  $n \equiv 35\cdot2\cdot1 + 21\cdot1\cdot2 + 15\cdot1\cdot3 \equiv 157 \equiv 52 \pmod{105}$

CRT, $\gcd(m_1, m_2)=1$

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

$\gcd(m_1, m_2) = 1$

CRT, $\gcd(m_1, m_2)=1$

- $n \equiv r_1 \pmod{m_1}$ $\quad\quad$ $\gcd(m_1, m_2) = 1$
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

CRT, $\gcd(m_1, m_2)=1$

- $n \equiv r_1 \pmod{m_1}$ $\quad\quad$ $\gcd(m_1, m_2) = 1$
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

CRT, $\gcd(m_1, m_2)=1$

- $n \equiv r_1 \pmod{m_1}$ $\quad\quad\quad\quad$ $\gcd(m_1, m_2) = 1$
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

  (m_1^{-1} is taken) $\pmod{m_2}$

CRT, $\gcd(m_1, m_2)=1$

- $n \equiv r_1 \pmod{m_1}$ $\quad\quad\quad$ $\gcd(m_1, m_2) = 1$
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

  (m_1^{-1}: $\pmod{m_2}$) $\quad$ (m_2^{-1}: $\pmod{m_1}$)

CRT, $\gcd(m_1, m_2)=1$

- $n \equiv r_1 \pmod{m_1}$ $\gcd(m_1, m_2) = 1$

  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

- $n \equiv r_1 (m_2 m_2^{-1}) + r_2 (m_1 m_1^{-1}) \pmod{m_1 m_2}$

CRT, gcd(m_1, m_2)=1

- $n \equiv r_1 \pmod{m_1}$ gcd(m_1, m_2) = 1
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

- $n \equiv r_1 (m_2 m_2^{-1}) + r_2 (m_1 m_1^{-1}) \pmod{m_1 m_2}$

CRT, $\gcd(m_1, m_2)=1$

- $n \equiv r_1 \pmod{m_1}$ $\qquad\qquad$ $\gcd(m_1, m_2) = 1$
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

- $n \equiv r_1 (m_2 m_2^{-1}) + r_2 (m_1 m_1^{-1}) \pmod{m_1 m_2}$

Verification

CRT, gcd(m_1, m_2)=1

- $n \equiv r_1 \pmod{m_1}$ gcd(m_1, m_2) = 1
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

- $n \equiv r_1 (m_2 m_2^{-1}) + r_2 (m_1 m_1^{-1}) \pmod{m_1 m_2}$

$n \bmod m_1 =$

Verification

CRT, gcd(m_1, m_2)=1

- $n \equiv r_1 \pmod{m_1}$ gcd(m_1, m_2) = 1

  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

- $n \equiv r_1 (m_2 m_2^{-1}) + r_2 (m_1 m_1^{-1}) \pmod{m_1 m_2}$

$n \bmod m_1 =$

$n \bmod m_2 =$

Verification

CRT, gcd(m_1, m_2)=1

- $n \equiv r_1 \pmod{m_1}$ $\qquad$ $\gcd(m_1, m_2) = 1$
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

mod m_1

- $n \equiv r_1 (m_2 m_2^{-1}) + r_2 (m_1 m_1^{-1}) \pmod{m_1 m_2}$

n mod m_1 = r_1

Verification

CRT, gcd(m_1, m_2)=1

- $n \equiv r_1 \pmod{m_1}$ $\quad$ $\gcd(m_1, m_2) = 1$
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

- $n \equiv r_1 (m_2 m_2^{-1}) + r_2 (m_1 m_1^{-1}) \pmod{m_1 m_2}$

$n \bmod m_1 = r_1 + 0$

Verification

CRT, $\gcd(m_1, m_2)=1$

- $n \equiv r_1 \pmod{m_1}$ $\quad\quad$ $\gcd(m_1, m_2) = 1$
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

  mod m_2

- $n \equiv r_1 (m_2 m_2^{-1}) + r_2 (m_1 m_1^{-1}) \pmod{m_1 m_2}$

$n \bmod m_1 = r_1 + 0$

$n \bmod m_2 = 0 + r_2$

Verification

CRT, $\gcd(m_1, m_2)=1$

- $n \equiv r_1 \pmod{m_1}$ $\qquad$ $\gcd(m_1, m_2) = 1$
  $\equiv r_2 \pmod{m_2}$

- $\exists$ s, t such that $m_1 s + m_2 t = 1$

  i.e. $m_1 m_1^{-1} + m_2 m_2^{-1} = 1$

- $n \equiv r_1 (m_2 m_2^{-1}) + r_2 (m_1 m_1^{-1}) \pmod{m_1 m_2}$

$n \bmod m_1 =$	r_1	+	0	**Verification**
$n \bmod m_2 =$	0		r_2	

Manually Incremental Calculation

$$
\begin{aligned}
n &\equiv \mathbf{1} \pmod{3} \\
  &\equiv \mathbf{2} \pmod{5} \\
  &\equiv \mathbf{3} \pmod{7}
\end{aligned}
$$

Manually Incremental Calculation

$$n \equiv 1 \pmod 3$$
$$\equiv 2 \pmod 5$$
$$\equiv 3 \pmod 7$$

① $\hat{n}_1 \equiv \underset{r_1}{1} \pmod 3$ … satisfying the 1st eq.

Manually Incremental Calculation

$$\begin{aligned} n &\equiv \mathbf{1} \pmod 3 \\ &\equiv \mathbf{2} \pmod 5 \\ &\equiv \mathbf{3} \pmod 7 \end{aligned}$$

$$\begin{aligned} n &\equiv \mathbf{1} \pmod 3 \\ &\equiv \mathbf{2} \pmod 5 \end{aligned}$$

① $\hat{n}_1 \equiv \mathbf{1} \pmod 3$ … satisfying the 1st eq.

Manually Incremental Calculation

$$
\begin{aligned}
n &\equiv 1 \pmod 3)\\
&\equiv 2 \pmod 5)\\
&\equiv 3 \pmod 7)
\end{aligned}
\qquad\qquad
\begin{aligned}
n &\equiv 1 \pmod 3)\\
&\equiv 2 \pmod 5)
\end{aligned}
$$

① $\hat{n}_1 \equiv 1 \pmod 3$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

Manually Incremental Calculation

$$n \equiv \mathbf{1} \pmod 3$$
$$\equiv \mathbf{2} \pmod 5$$
$$\equiv \mathbf{3} \pmod 7$$

$$n \equiv \mathbf{1} \pmod 3$$
$$\equiv \mathbf{2} \pmod 5$$

① $\hat{n}_1 \equiv \mathbf{1} \pmod 3$ … satisfying the 1st eq.

inverse of 3 (mod 5)

② $3 \cdot (-3) + 5 \cdot 2 = 1$

Manually Incremental Calculation

$n \equiv 1 \pmod{3}$
$\equiv 2 \pmod{5}$
$\equiv 3 \pmod{7}$

$n \equiv 1 \pmod{3}$
$\equiv 2 \pmod{5}$

① $\hat{n}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

inverse of 3 (mod 5)

inverse of 5 (mod 3)

Manually Incremental Calculation

$n \equiv 1 \pmod 3$
$\equiv 2 \pmod 5$
$\equiv 3 \pmod 7$

$n \equiv 1 \pmod 3$
$\equiv 2 \pmod 5$

① $\hat{n}_1 \equiv 1 \pmod 3$ … satisfying the 1st eq.

inverse of 3 (mod 5)

② $3 \cdot (-3) + 5 \cdot 2 = 1$

inverse of 5 (mod 3)

③ $\hat{n}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2$

$\hat{n}_1$

Manually Incremental Calculation

$$n \equiv 1 \pmod 3$$
$$\equiv 2 \pmod 5$$
$$\equiv 3 \pmod 7$$

$$n \equiv 1 \pmod 3$$
$$\equiv 2 \pmod 5$$

① $\hat{n}_1 \equiv 1 \pmod 3$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

inverse of 3 (mod 5)

inverse of 5 (mod 3)

③ $\hat{n}_2 \equiv \underbrace{2}_{r_2} \cdot 3 \cdot (-3) + \underbrace{1}_{\hat{n}_1} \cdot 5 \cdot 2$

Manually Incremental Calculation

$n \equiv 1 \pmod{3}$
$\equiv 2 \pmod{5}$
$\equiv 3 \pmod{7}$

$n \equiv 1 \pmod{3}$
$\equiv 2 \pmod{5}$

① $\hat{n}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{n}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

Manually Incremental Calculation

$n \equiv 1 \pmod 3$
$\equiv 2 \pmod 5$
$\equiv 3 \pmod 7$

$n \equiv 7 \pmod{15}$
$\equiv 3 \pmod 7$

① $\hat{n}_1 \equiv 1 \pmod 3$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{n}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

Manually Incremental Calculation

$n \equiv 1 \pmod{3}$
$\equiv 2 \pmod{5}$
$\equiv 3 \pmod{7}$

$n \equiv 7 \pmod{15}$
$\equiv 3 \pmod{7}$

① $\hat{n}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{n}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

Manually Incremental Calculation

$n \equiv 1 \pmod{3}$
$\equiv 2 \pmod{5}$
$\equiv 3 \pmod{7}$

$n \equiv 7 \pmod{15}$
$\equiv 3 \pmod{7}$

① $\hat{n}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{n}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

inverse of 15 (mod 7)

inverse of 7 (mod 15)

Manually Incremental Calculation

$n \equiv 1 \pmod 3$
$\equiv 2 \pmod 5$
$\equiv 3 \pmod 7$

$n \equiv 7 \pmod{15}$
$\equiv 3 \pmod 7$

① $\hat{n}_1 \equiv 1 \pmod 3$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{n}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

inverse of 15 (mod 7)

inverse of 7 (mod 15)

⑤ $\hat{n}_3 \equiv 3 \cdot 15 \cdot 1 + 7 \cdot 7 \cdot (-2)$

$\hat{n}_2$

Manually Incremental Calculation

$n \equiv 1 \pmod 3$
$\equiv 2 \pmod 5$
$\equiv 3 \pmod 7$

$n \equiv 7 \pmod{15}$
$\equiv 3 \pmod 7$

① $\hat{n}_1 \equiv 1 \pmod 3$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{n}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

inverse of 15 (mod 7)

inverse of 7 (mod 15)

⑤ $\hat{n}_3 \equiv 3 \cdot 15 \cdot 1 + 7 \cdot 7 \cdot (-2)$

r_3 $\hat{n}_2$

Manually Incremental Calculation

$n \equiv 1 \pmod 3$
$\equiv 2 \pmod 5$
$\equiv 3 \pmod 7$

$n \equiv 7 \pmod{15}$
$\equiv 3 \pmod 7$

① $\hat{n}_1 \equiv 1 \pmod 3$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{n}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

⑤ $\hat{n}_3 \equiv 3 \cdot 15 \cdot 1 + 7 \cdot 7 \cdot (-2) \equiv -53 \equiv \mathbf{52} \pmod{105}$
… satisfying all 3 eqs.

Manually Incremental Calculation

$n \equiv 1 \pmod{3}$
$\equiv 2 \pmod{5}$
$\equiv 3 \pmod{7}$

① $\hat{n}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{n}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

⑤ $\hat{n}_3 \equiv 3 \cdot 15 \cdot 1 + 7 \cdot 7 \cdot (-2) \equiv -53 \equiv \mathbf{52} \pmod{105}$
… satisfying all 3 eqs.

CRT, gcd(m_1, m_2)=d

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

CRT, gcd(m_1, m_2)=d

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = \mathbf{d} > 1$

CRT, gcd(m_1, m_2)=d

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

gcd(m_1, m_2) = **d** > 1

- $n \equiv 1 \pmod{6}$
  $\equiv 3 \pmod{10}$

CRT, $\gcd(m_1, m_2)=d$

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

- $n \equiv 1 \pmod{6}$
  $\equiv 3 \pmod{10}$

$3 \cdot (-3) + 5 \cdot 2 = 1$

CRT, $\gcd(m_1, m_2)=d$

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

- $n \equiv 1 \pmod 6$
  $\equiv 3 \pmod{10}$

$3 \cdot (-3) + 5 \cdot 2 = 1$

$3^{-1} \equiv -3 \pmod 5$, $5^{-1} \equiv 2 \pmod 3$

CRT, gcd(m_1, m_2)=d

✧ $n \equiv r_1 \pmod{m_1}$
$\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

✧ $n \equiv 1 \pmod{6}$
$\equiv 3 \pmod{10}$

$3 \cdot (-3) + 5 \cdot 2 = 1$

$3^{-1} \equiv -3 \pmod{5}$, $5^{-1} \equiv 2 \pmod{3}$

CRT, $\gcd(m_1, m_2)=d$

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

- $n \equiv 1 \pmod{6}$
  $\equiv 3 \pmod{10}$

$3 \cdot (-3) + 5 \cdot 2 = 1$ $3^{-1} \equiv -3 \pmod{5}$, $5^{-1} \equiv 2 \pmod{3}$

$n \equiv 3 \cdot 6 \cdot (-3) + 1 \cdot 10 \cdot 2$

CRT, $\gcd(m_1, m_2)=d$

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

- $n \equiv 1 \pmod{6}$
  $\equiv 3 \pmod{10}$

$\mathbf{3}\cdot(-3) + \mathbf{5}\cdot 2 = 1$ $\quad 3^{-1} \equiv -3 \pmod{\mathbf{5}}$, $5^{-1} \equiv 2 \pmod{\mathbf{3}}$

$n \equiv \mathbf{3} \cdot 6\cdot(-3) + \mathbf{1} \cdot 10\cdot 2 \equiv -34 \equiv \mathbf{26} \pmod{60}$

CRT, gcd(m_1, m_2)=d

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = \mathbf{d} > 1$

- $n \equiv 1 \pmod{6}$
  $\equiv 3 \pmod{10}$

$\mathbf{3}\cdot(-3) + \mathbf{5}\cdot 2 = 1$ $\quad 3^{-1} \equiv -3 \pmod{\mathbf{5}}$, $5^{-1} \equiv 2 \pmod{\mathbf{3}}$

$n \equiv \mathbf{3} \cdot 6\cdot(-3) + \mathbf{1} \cdot 10\cdot 2 \equiv -34 \equiv \mathbf{26} \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6**

CRT, gcd(m_1, m_2)=d

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

- $n \equiv 1 \pmod{6}$
  $\equiv 3 \pmod{10}$

$3 \cdot (-3) + 5 \cdot 2 = 1$ $\quad 3^{-1} \equiv -3 \pmod{5}$, $5^{-1} \equiv 2 \pmod{3}$

$n \equiv 3 \cdot 6 \cdot (-3) + 1 \cdot 10 \cdot 2 \equiv -34 \equiv 26 \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

CRT, gcd(m_1, m_2)=d

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

- $n \equiv 1 \pmod 6$
  $\equiv 3 \pmod{10}$

$3\cdot(-3) + 5\cdot 2 = 1$ $3^{-1} \equiv -3 \pmod 5$, $5^{-1} \equiv 2 \pmod 3$

$n \equiv 3 \cdot 6\cdot(-3) + 1 \cdot 10\cdot 2 \equiv -34 \equiv 26 \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

- $n \equiv 1 \pmod 6 \equiv 3 \pmod{10}$, $\gcd(6,10)=2$

CRT, gcd(m_1, m_2)=d

✧ $n \equiv r_1 \pmod{m_1}$
$\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

✧ $n \equiv 1 \pmod{6}$
$\equiv 3 \pmod{10}$

$3 \cdot (-3) + 5 \cdot 2 = 1$ $3^{-1} \equiv -3 \pmod{5}$, $5^{-1} \equiv 2 \pmod{3}$

$n \equiv 3 \cdot 6 \cdot (-3) + 1 \cdot 10 \cdot 2 \equiv -34 \equiv 26 \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

✧ $n \equiv 1 \pmod{6} \equiv 3 \pmod{10}$, $\gcd(6,10)=2$

$n \equiv 1 \pmod{6} \overset{CRT}{\Leftrightarrow} n \equiv 1 \pmod{2} \equiv 1 \pmod{3}$

CRT, $\gcd(m_1, m_2)=d$

- $n \equiv r_1 \pmod{m_1}$ **moduli are not relative prime**
  $\equiv r_2 \pmod{m_2}$ $\gcd(m_1, m_2) = \mathbf{d} > 1$

- $n \equiv 1 \pmod 6$ $\mathbf{3}\cdot(-3) + \mathbf{5}\cdot 2 = 1$ $3^{-1} \equiv -3 \pmod{\mathbf{5}}$, $5^{-1} \equiv 2 \pmod{\mathbf{3}}$
  $\equiv 3 \pmod{10}$ $n \equiv \mathbf{3} \cdot 6\cdot(-3) + \mathbf{1} \cdot 10\cdot 2 \equiv -34 \equiv \mathbf{26} \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

- $n \equiv 1 \pmod 6 \equiv 3 \pmod{10}$, $\gcd(6,10)=\mathbf{2}$

$\gcd(2,3)=1$

$$n \equiv 1 \pmod 6 \overset{\text{CRT}}{\Leftrightarrow} n \equiv \mathbf{1} \pmod{\mathbf{2}} \equiv 1 \pmod 3$$

CRT, gcd(m_1, m_2)=d

✧ $n \equiv r_1 \pmod{m_1}$
$\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

✧ $n \equiv 1 \pmod{6}$
$\equiv 3 \pmod{10}$

$3\cdot(-3) + 5\cdot 2 = 1$ $\quad 3^{-1} \equiv -3 \pmod{5}$, $5^{-1} \equiv 2 \pmod{3}$

$n \equiv 3 \cdot 6\cdot(-3) + 1 \cdot 10\cdot 2 \equiv -34 \equiv 26 \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

✧ $n \equiv 1 \pmod{6} \equiv 3 \pmod{10}$, $\gcd(6,10)=2$

$\gcd(2,3)=1$

$n \equiv 1 \pmod{6} \overset{CRT}{\Leftrightarrow} n \equiv 1 \pmod{2} \equiv 1 \pmod{3}$

$n \equiv 3 \pmod{10} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 3 \pmod{5}$

CRT, gcd(m_1, m_2)=d

✧ $n \equiv r_1 \pmod{m_1}$ **moduli are not relative prime**

$\equiv r_2 \pmod{m_2}$ $\gcd(m_1, m_2) = \mathbf{d} > 1$

✧ $n \equiv 1 \pmod{6}$ $\mathbf{3}\cdot(-3) + \mathbf{5}\cdot 2 = 1$ $3^{-1} \equiv -3 \pmod{\mathbf{5}}$, $5^{-1} \equiv 2 \pmod{\mathbf{3}}$

$\equiv 3 \pmod{10}$ $n \equiv \mathbf{3} \cdot 6\cdot(-3) + \mathbf{1} \cdot 10\cdot 2 \equiv -34 \equiv \mathbf{26} \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

✧ $n \equiv 1 \pmod{6} \equiv 3 \pmod{10}$, $\gcd(6,10)=\mathbf{2}$

$\gcd(2,3)=1$

$n \equiv 1 \pmod{6} \overset{\text{CRT}}{\Leftrightarrow} n \equiv \mathbf{1} \pmod{\mathbf{2}} \equiv 1 \pmod{3}$

$n \equiv 3 \pmod{10} \Leftrightarrow n \equiv \mathbf{1} \pmod{\mathbf{2}} \equiv 3 \pmod{5}$

$\gcd(2,5)=1$

CRT, gcd(m_1, m_2)=d

✧ $n \equiv r_1 \pmod{m_1}$
$\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = \mathbf{d} > 1$

✧ $n \equiv 1 \pmod{6}$
$\equiv 3 \pmod{10}$

$\mathbf{3}\cdot(-3) + \mathbf{5}\cdot 2 = 1$ $3^{-1} \equiv -3 \pmod{\mathbf{5}}$, $5^{-1} \equiv 2 \pmod{\mathbf{3}}$

$n \equiv \mathbf{3} \cdot 6\cdot(-3) + \mathbf{1} \cdot 10\cdot 2 \equiv -34 \equiv \mathbf{26} \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

✧ $n \equiv 1 \pmod{6} \equiv 3 \pmod{10}$, $\gcd(6,10)=\mathbf{2}$

CRT

$n \equiv 1 \pmod{6} \iff n \equiv \mathbf{1} \pmod{\mathbf{2}} \equiv 1 \pmod{3}$ gcd(2,3)=1

$n \equiv 3 \pmod{10} \iff n \equiv \mathbf{1} \pmod{\mathbf{2}} \equiv 3 \pmod{5}$ gcd(2,5)=1

consistent

CRT, $\gcd(m_1, m_2)=d$

✧ $n \equiv r_1 \pmod{m_1}$
$\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

✧ $n \equiv 1 \pmod{6}$
$\equiv 3 \pmod{10}$

$3 \cdot (-3) + 5 \cdot 2 = 1$ $3^{-1} \equiv -3 \pmod{5}$, $5^{-1} \equiv 2 \pmod{3}$

$n \equiv 3 \cdot 6 \cdot (-3) + 1 \cdot 10 \cdot 2 \equiv -34 \equiv 26 \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6**   Incorrect!!!

✧ $n \equiv 1 \pmod{6} \equiv 3 \pmod{10}$, $\gcd(6,10)=2$

$n \equiv 1 \pmod{6} \overset{CRT}{\Leftrightarrow} n \equiv 1 \pmod{2} \equiv 1 \pmod{3}$

$n \equiv 3 \pmod{10} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 3 \pmod{5}$

$n \equiv 1 \pmod{2}$
$\equiv 1 \pmod{3}$
$\equiv 3 \pmod{5}$

CRT, $\gcd(m_1, m_2)=d$

- ✧ $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

- ✧ $n \equiv 1 \pmod{6}$
  $\equiv 3 \pmod{10}$

$3 \cdot (-3) + 5 \cdot 2 = 1$ $\quad 3^{-1} \equiv -3 \pmod{5}$, $5^{-1} \equiv 2 \pmod{3}$

$n \equiv 3 \cdot 6 \cdot (-3) + 1 \cdot 10 \cdot 2 \equiv -34 \equiv 26 \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

- ✧ $n \equiv 1 \pmod{6} \equiv 3 \pmod{10}$, $\gcd(6,10)=2$

CRT

$n \equiv 1 \pmod{6} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 1 \pmod{3}$

$n \equiv 3 \pmod{10} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 3 \pmod{5}$

$n \equiv 1 \pmod{2}$
$\equiv 1 \pmod{3}$ $\Rightarrow$ $n \equiv 1 \pmod{6}$
$\equiv 3 \pmod{5}$ $\quad \equiv 3 \pmod{5}$

CRT, gcd(m_1, m_2)=d

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

- $n \equiv 1 \pmod{6}$
  $\equiv 3 \pmod{10}$

$3 \cdot (-3) + 5 \cdot 2 = 1$ $\quad 3^{-1} \equiv -3 \pmod{5}$, $5^{-1} \equiv 2 \pmod{3}$

$n \equiv 3 \cdot 6 \cdot (-3) + 1 \cdot 10 \cdot 2 \equiv -34 \equiv 26 \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

- $n \equiv 1 \pmod{6} \equiv 3 \pmod{10}$, $\quad \gcd(6,10)=2$

$n \equiv 1 \pmod{6} \overset{\text{CRT}}{\Leftrightarrow} n \equiv 1 \pmod{2} \equiv 1 \pmod{3}$

$n \equiv 3 \pmod{10} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 3 \pmod{5}$

$n \equiv 1 \pmod{2}$, $\equiv 1 \pmod{3}$, $\equiv 3 \pmod{5}$ $\Rightarrow$ $n \equiv 1 \pmod{6}$, $\equiv 3 \pmod{5}$

i.e. $n \equiv r_1 \pmod{m_1}$, $\equiv r_2 \pmod{m_2/d}$

CRT, gcd(m_1, m_2)=d

- $n \equiv r_1 \pmod{m_1}$
  $\equiv r_2 \pmod{m_2}$

moduli are not relative prime

$\gcd(m_1, m_2) = d > 1$

- $n \equiv 1 \pmod{6}$
  $\equiv 3 \pmod{10}$

$3\cdot(-3) + 5\cdot 2 = 1$ $3^{-1} \equiv -3 \pmod{5}$, $5^{-1} \equiv 2 \pmod{3}$

$n \equiv 3 \cdot 6\cdot(-3) + 1 \cdot 10\cdot 2 \equiv -34 \equiv 26 \pmod{60}$

Verification: 26 mod 6 = **2**, 26 mod 10 = **6** Incorrect!!!

- $n \equiv 1 \pmod{6} \equiv 3 \pmod{10}$, $\gcd(6,10)=2$

CRT

$n \equiv 1 \pmod{6} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 1 \pmod{3}$

$n \equiv 3 \pmod{10} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 3 \pmod{5}$

note: CRT works only when gcd(d,m_2/d)=1

$n \equiv 1 \pmod{2}$
$\equiv 1 \pmod{3}$
$\equiv 3 \pmod{5}$
$\Rightarrow$
$n \equiv 1 \pmod{6}$
$\equiv 3 \pmod{5}$

i.e.

$n \equiv r_1 \pmod{m_1}$
$\equiv r_2 \pmod{m_2/d}$

CAVEAT

- $n \equiv 3 \pmod{10}$
  $\equiv 11 \pmod{12}$

CAVEAT

$10 = 2 \cdot 5$, $12 = 2^2 \cdot 3$

- $n \equiv 3 \pmod{10}$

  $\equiv 11 \pmod{12}$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3 \qquad \gcd(10,12)=2$

- $n \equiv 3 \pmod{10}$
  $\equiv 11 \pmod{12}$

CAVEAT

$10=2\cdot5,\ 12=2^2\cdot3 \qquad \gcd(10,12)=2$

- $n \equiv 3 \pmod{10}$
  $\equiv 11 \pmod{12}$

  ⇨ $n \equiv 3 \pmod{10}$
  $\equiv 5 \pmod{6}$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3$ $\gcd(10,12)=2$ $\gcd(10,6)=2$

- $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ $\Rightarrow$ $n \equiv 3 \pmod{10}$, $\equiv 5 \pmod{6}$ $\Rightarrow$ $n \equiv 3 \pmod{10}$, $\equiv 2 \pmod{3}$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3$ $\quad gcd(10,12)=2$ $\quad gcd(10,6)=2$

- $n \equiv 3 \pmod{10}$
  $\equiv 11 \pmod{12}$

$\Rightarrow$ $n \equiv 3 \pmod{10}$
$\equiv 5 \pmod{6}$

$\Rightarrow$ $n \equiv 3 \pmod{10}$
$\equiv 2 \pmod{3}$

$\Rightarrow$ $n \equiv 23 \pmod{30}$

CAVEAT

$10 = 2 \cdot 5,\ 12 = 2^2 \cdot 3$ gcd(10,12)=2 gcd(10,6)=2

- $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ ⇒ $n \equiv 3 \pmod{10}$, $\equiv 5 \pmod{6}$ ⇒ $n \equiv 3 \pmod{10}$, $\equiv 2 \pmod{3}$ ⇒ $n \equiv 23 \pmod{30}$

~~53~~

CAVEAT

$10 = 2\cdot 5,\ 12 = 2^2\cdot 3$ gcd(10,12)=2 gcd(10,6)=2

- $n \equiv 3 \pmod{10}$
  $\equiv 11 \pmod{12}$

⇒ $n \equiv 3 \pmod{10}$
~~$\equiv 5 \pmod{6}$~~

⇒ $n \equiv 3 \pmod{10}$
$\equiv 2 \pmod{3}$

~~53~~

⇒ $n \equiv 23 \pmod{30}$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3$ $\quad \gcd(10,12)=2$ $\quad \gcd(10,6)=2$

✧ $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ ⇒ $n \equiv 3 \pmod{10}$, ~~$\equiv 5 \pmod{6}$~~ ⇒ $n \equiv 3 \pmod{10}$, $\equiv 2 \pmod{3}$ ⇒ $n \equiv 23 \pmod{30}$

~~53~~

$12=2^2\cdot 3$

$\gcd(4,3)=1$

$n \equiv 11 \pmod{12}$ $\overset{\text{CRT}}{\Longleftrightarrow}$ $n \equiv 3 \pmod{4} \equiv 2 \pmod{3}$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3$ gcd(10,12)=2   gcd(10,6)=2

- $n \equiv 3 \pmod{10}$
  $\equiv 11 \pmod{12}$
  $\Rightarrow$ $n \equiv 3 \pmod{10}$
  ~~$\equiv 5 \pmod{6}$~~
  $\Rightarrow$ $n \equiv 3 \pmod{10}$
  $\equiv 2 \pmod{3}$
  $\Rightarrow$ $n \equiv 23 \pmod{30}$

~~53~~

$12=2^2\cdot 3$

CRT

$n \equiv 11 \pmod{12} \Leftrightarrow n \equiv 3 \pmod{4} \equiv 2 \pmod{3}$ **gcd(4,3)=1**

$n \equiv 11 \pmod{12}$ ~~$\Leftrightarrow$~~ $n \equiv 1 \pmod{2} \equiv 5 \pmod{6}$ **gcd(2,6)≠1**

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3$ $\gcd(10,12)=2$ $\gcd(10,6)=2$

✧ $n \equiv 3 \pmod{10}$
$\equiv 11 \pmod{12}$

$\Rightarrow$ $n \equiv 3 \pmod{10}$
~~$\equiv 5 \pmod{6}$~~

$\Rightarrow$ $n \equiv 3 \pmod{10}$
$\equiv 2 \pmod{3}$

$\Rightarrow$ $n \equiv 23 \pmod{30}$

~~53~~

$12=2^2\cdot 3$

$n \equiv 11 \pmod{12}$ $\overset{\text{CRT}}{\Leftrightarrow}$ $n \equiv 3 \pmod{4} \equiv 2 \pmod{3}$

$n \equiv 11 \pmod{12}$ ~~$\Leftrightarrow$~~ $n \equiv 1 \pmod{2} \equiv 5 \pmod{6}$

$n \equiv 1 \pmod{2} \equiv 5 \pmod{6}$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3$ gcd(10,12)=2 gcd(10,6)=2

- $n \equiv 3 \pmod{10}$
  $\equiv 11 \pmod{12}$
  $\Rightarrow$ $n \equiv 3 \pmod{10}$
  ~~$\equiv 5 \pmod{6}$~~
  $\Rightarrow$ $n \equiv 3 \pmod{10}$
  $\equiv 2 \pmod{3}$
  ~~53~~
  $\Rightarrow$ $n \equiv 23 \pmod{30}$

$12=2^2\cdot 3$

CRT

$n \equiv 11 \pmod{12} \Leftrightarrow n \equiv 3 \pmod{4} \equiv 2 \pmod{3}$

$n \equiv 11 \pmod{12}$ ~~$\Leftrightarrow$~~ $n \equiv 1 \pmod{2} \equiv 5 \pmod{6}$

$n \equiv 1 \pmod{2} \equiv 5 \pmod{6} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 1 \pmod{2} \equiv 2 \pmod{3}$

CAVEAT

$10=2\cdot5,\ 12=2^2\cdot3$ $\quad gcd(10,12)=2$ $\quad gcd(10,6)=2$

- $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ ⇨ $n \equiv 3 \pmod{10}$, ~~$\equiv 5 \pmod 6$~~ ⇨ $n \equiv 3 \pmod{10}$, $\equiv 2 \pmod 3$ ⇨ $n \equiv 23 \pmod{30}$ ~~53~~

$12=2^2\cdot3$

$n \equiv 11 \pmod{12}$ $\overset{CRT}{\Leftrightarrow}$ $n \equiv 3 \pmod 4 \equiv 2 \pmod 3$

$n \equiv 11 \pmod{12}$ ~~$\Leftrightarrow$~~ $n \equiv 1 \pmod 2 \equiv 5 \pmod 6$

$n \equiv 1 \pmod 2 \equiv 5 \pmod 6 \Leftrightarrow n \equiv 1 \pmod 2 \equiv 1 \pmod 2 \equiv 2 \pmod 3$

$\Leftrightarrow n \equiv 1 \pmod 2 \equiv 2 \pmod 3$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3 \qquad \gcd(10,12)=2 \qquad \gcd(10,6)=2$

- $n \equiv 3 \pmod{10}$
  $\equiv 11 \pmod{12}$
  $\Rightarrow n \equiv 3 \pmod{10}$
  ~~$\equiv 5 \pmod 6$~~
  $\Rightarrow n \equiv 3 \pmod{10}$
  $\equiv 2 \pmod 3$
  $\Rightarrow n \equiv 23 \pmod{30}$
  ~~53~~

$12=2^2\cdot 3$

CRT

$n \equiv 11 \pmod{12} \Leftrightarrow n \equiv 3 \pmod 4 \equiv 2 \pmod 3$

$n \equiv 11 \pmod{12}$ ~~$\Leftrightarrow$~~ $n \equiv 1 \pmod 2 \equiv 5 \pmod 6$

$n \equiv 1 \pmod 2 \equiv 5 \pmod 6 \Leftrightarrow n \equiv 1 \pmod 2 \equiv 1 \pmod 2 \equiv 2 \pmod 3$

$\Leftrightarrow n \equiv 1 \pmod 2 \equiv 2 \pmod 3$

$\Leftrightarrow n \equiv 5 \pmod 6$

CAVEAT

$10=2\cdot5,\ 12=2^2\cdot3$ $\quad \gcd(10,12)=2$ $\quad \gcd(10,6)=2$

✧ $n \equiv 3 \pmod{10}$
$\equiv 11 \pmod{12}$

$\Rightarrow$ $n \equiv 3 \pmod{10}$
~~$\equiv 5 \pmod{6}$~~

$\Rightarrow$ $n \equiv 3 \pmod{10}$
$\equiv 2 \pmod{3}$

~~53~~

$\Rightarrow$ $n \equiv 23 \pmod{30}$

$12=2^2\cdot3$

CRT

$n \equiv 11 \pmod{12} \Leftrightarrow n \equiv 3 \pmod{4} \equiv 2 \pmod{3}$

$n \equiv 11 \pmod{12}$ ~~$\Leftrightarrow$~~ $n \equiv 1 \pmod{2} \equiv 5 \pmod{6}$

$n \equiv 1 \pmod{2} \equiv 5 \pmod{6} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 1 \pmod{2} \equiv 2 \pmod{3}$

$\Leftrightarrow n \equiv 1 \pmod{2} \equiv 2 \pmod{3}$

$\Leftrightarrow n \equiv 5 \pmod{6}$

✧ $n \equiv 3 \pmod{10}$
$\equiv 11 \pmod{12}$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3$ $\quad \gcd(10,12)=2$ $\quad \gcd(10,6)=2$

✧ $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ $\Rightarrow$ $n \equiv 3 \pmod{10}$, ~~$\equiv 5 \pmod{6}$~~ $\Rightarrow$ $n \equiv 3 \pmod{10}$, $\equiv 2 \pmod{3}$ $\Rightarrow$ $n \equiv 23 \pmod{30}$ ~~53~~

$12=2^2\cdot 3$

$$n \equiv 11 \pmod{12} \overset{\text{CRT}}{\Leftrightarrow} n \equiv 3 \pmod{4} \equiv 2 \pmod{3}$$

$$n \equiv 11 \pmod{12} \not\Leftrightarrow n \equiv 1 \pmod{2} \equiv 5 \pmod{6}$$

$$n \equiv 1 \pmod{2} \equiv 5 \pmod{6} \Leftrightarrow n \equiv 1 \pmod{2} \equiv 1 \pmod{2} \equiv 2 \pmod{3}$$
$$\Leftrightarrow n \equiv 1 \pmod{2} \equiv 2 \pmod{3}$$
$$\Leftrightarrow n \equiv 5 \pmod{6}$$

✧ $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ $\Rightarrow$ $n \equiv 1 \pmod{2}$, $\equiv 3 \pmod{5}$, $\equiv 3 \pmod{4}$, $\equiv 2 \pmod{3}$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3$ $\gcd(10,12)=2$ $\gcd(10,6)=2$

✧ $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ ⇒ $n \equiv 3 \pmod{10}$, ~~$\equiv 5 \pmod 6$~~ ⇒ $n \equiv 3 \pmod{10}$, $\equiv 2 \pmod 3$ ⇒ $n \equiv 23 \pmod{30}$ ~~53~~

$12=2^2\cdot 3$

$n \equiv 11 \pmod{12}$ $\overset{\text{CRT}}{\Leftrightarrow}$ $n \equiv 3 \pmod 4 \equiv 2 \pmod 3$

$n \equiv 11 \pmod{12}$ ~~$\Leftrightarrow$~~ $n \equiv 1 \pmod 2 \equiv 5 \pmod 6$

$n \equiv 1 \pmod 2 \equiv 5 \pmod 6 \Leftrightarrow n \equiv 1 \pmod 2 \equiv 1 \pmod 2 \equiv 2 \pmod 3$

$\Leftrightarrow n \equiv 1 \pmod 2 \equiv 2 \pmod 3$

$\Leftrightarrow n \equiv 5 \pmod 6$

✧ $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ ⇒ $n \equiv 1 \pmod 2$, $\equiv 3 \pmod 5$, $\equiv 3 \pmod 4$, $\equiv 2 \pmod 3$ ⇒ $n \equiv 3 \pmod 5$, $\equiv 3 \pmod 4$, $\equiv 2 \pmod 3$

CAVEAT

$10 = 2\cdot 5,\ 12 = 2^2\cdot 3$ $\gcd(10,12)=2$ $\gcd(10,6)=2$

✧ $n \equiv 3 \pmod{10}$
$\equiv 11 \pmod{12}$
$\Rightarrow$ $n \equiv 3 \pmod{10}$
~~$\equiv 5 \pmod 6$~~
$\Rightarrow$ $n \equiv 3 \pmod{10}$
$\equiv 2 \pmod 3$
$\Rightarrow$ $n \equiv 23 \pmod{30}$ ~~53~~

$12 = 2^2\cdot 3$

CRT

$n \equiv 11 \pmod{12} \Leftrightarrow n \equiv 3 \pmod 4 \equiv 2 \pmod 3$

$n \equiv 11 \pmod{12}$ ~~$\Leftrightarrow$~~ $n \equiv 1 \pmod 2 \equiv 5 \pmod 6$

$n \equiv 1 \pmod 2 \equiv 5 \pmod 6 \Leftrightarrow n \equiv 1 \pmod 2 \equiv 1 \pmod 2 \equiv 2 \pmod 3$
$\Leftrightarrow n \equiv 1 \pmod 2 \equiv 2 \pmod 3$
$\Leftrightarrow n \equiv 5 \pmod 6$

✧ $n \equiv 3 \pmod{10}$
$\equiv 11 \pmod{12}$
$\Rightarrow$ $n \equiv 1 \pmod 2$
$\equiv 3 \pmod 5$
$\equiv 3 \pmod 4$
$\equiv 2 \pmod 3$
$\Rightarrow$ $n \equiv 3 \pmod 5$
$\equiv 3 \pmod 4$
$\equiv 2 \pmod 3$
$\Rightarrow$ $n \equiv 3 \pmod{20}$
$\equiv 2 \pmod 3$

CAVEAT

$10=2\cdot 5,\ 12=2^2\cdot 3$ $\quad \gcd(10,12)=2$ $\quad \gcd(10,6)=2$

✧ $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ ⇨ $n \equiv 3 \pmod{10}$, ~~$\equiv 5 \pmod 6$~~ ⇨ $n \equiv 3 \pmod{10}$, $\equiv 2 \pmod 3$ ⇨ $n \equiv 23 \pmod{30}$ ~~53~~

$12=2^2\cdot 3$

$n \equiv 11 \pmod{12} \overset{\text{CRT}}{\Leftrightarrow} n \equiv 3 \pmod 4 \equiv 2 \pmod 3$

$n \equiv 11 \pmod{12}$ ~~⇔~~ $n \equiv 1 \pmod 2 \equiv 5 \pmod 6$

$n \equiv 1 \pmod 2 \equiv 5 \pmod 6 \Leftrightarrow n \equiv 1 \pmod 2 \equiv 1 \pmod 2 \equiv 2 \pmod 3$

$\Leftrightarrow n \equiv 1 \pmod 2 \equiv 2 \pmod 3$

$\Leftrightarrow n \equiv 5 \pmod 6$

✧ $n \equiv 3 \pmod{10}$, $\equiv 11 \pmod{12}$ ⇨ $n \equiv 1 \pmod 2$, $\equiv 3 \pmod 5$, $\equiv 3 \pmod 4$, $\equiv 2 \pmod 3$ ⇨ $n \equiv 3 \pmod 5$, $\equiv 3 \pmod 4$, $\equiv 2 \pmod 3$ ⇨ $n \equiv 3 \pmod{20}$, $\equiv 2 \pmod 3$ ⇨ **$n \equiv 23 \pmod{60}$**

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

$$
\begin{aligned}
\mathbf{n} &\equiv r_1 \pmod{m_1} \\
&\equiv r_2 \pmod{m_2} \\
&\quad \cdots \\
&\equiv r_k \pmod{m_k}
\end{aligned}
$$

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

$$\begin{aligned} \mathbf{n} &\equiv r_1 \pmod{m_1} \\ &\equiv r_2 \pmod{m_2} \\ &\cdots \\ &\equiv r_k \pmod{m_k} \end{aligned}$$

$\gcd(m_i, m_j) = 1$

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

  there exists a unique integer $n \in Z_{m_1 \cdots m_k}$ satisfying the set of k congruence equations

$$\begin{aligned} n &\equiv r_1 \pmod{m_1} \\ &\equiv r_2 \pmod{m_2} \\ &\cdots \\ &\equiv r_k \pmod{m_k} \end{aligned}$$

$\gcd(m_i, m_j) = 1$

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

  there exists a unique integer

  n $\in Z_{m_1 \cdots m_k}$ satisfying the

  set of k congruence equations

$$\begin{aligned} \mathbf{n} &\equiv r_1 \pmod{m_1} \\ &\equiv r_2 \pmod{m_2} \\ &\cdots \\ &\equiv r_k \pmod{m_k} \end{aligned}$$

$\gcd(m_i, m_j) = 1$

note: each tuple $(r_1, r_2 \cdots, r_k)$ maps to one of $m_1 m_2 \cdots m_k$ distinct integers, which are members of the field $Z_{m_1 \cdots m_k}$

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

  there exists a unique integer
  $\mathbf{n} \in Z_{m_1 \cdots m_k}$ satisfying the
  set of k congruence equations

$$\begin{aligned} \mathbf{n} &\equiv r_1 \pmod{m_1} \\ &\equiv r_2 \pmod{m_2} \\ &\cdots \\ &\equiv r_k \pmod{m_k} \end{aligned}$$

$\gcd(m_i, m_j) = 1$

note: each tuple $(r_1, r_2 \cdots, r_k)$ maps to one of $m_1 m_2 \cdots m_k$ distinct integers, which are members of the field $Z_{m_1 \cdots m_k}$

- **Prime power moduli**: $n \equiv r \pmod{p^c}$

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

  there exists a unique integer

  $n \in Z_{m_1 \cdots m_k}$ satisfying the

  set of k congruence equations

$$
\begin{aligned}
n &\equiv r_1 \pmod{m_1} \\
&\equiv r_2 \pmod{m_2} \\
&\cdots \\
&\equiv r_k \pmod{m_k}
\end{aligned}
$$

$\gcd(m_i, m_j) = 1$

note: each tuple $(r_1, r_2 \cdots, r_k)$ maps to one of $m_1 m_2 \cdots m_k$ distinct integers, which are members of the field $Z_{m_1 \cdots m_k}$

- **Prime power moduli**: $n \equiv r \pmod{p^c}$

  $\Rightarrow n \equiv r' \pmod{p^{c'}}, \forall c' < c, r' \equiv r \pmod{p^{c'}}$

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

  there exists a unique integer
  n $\in Z_{m_1 \cdots m_k}$ satisfying the
  set of k congruence equations

$$\begin{aligned} \mathbf{n} &\equiv r_1 \pmod{m_1} \\ &\equiv r_2 \pmod{m_2} \\ &\bullet \bullet \bullet \\ &\equiv r_k \pmod{m_k} \end{aligned}$$

$\gcd(m_i, m_j) = 1$

note: each tuple $(r_1, r_2 \cdots, r_k)$ maps to one of $m_1 m_2 \cdots m_k$ distinct integers, which are members of the field $Z_{m_1 \cdots m_k}$

- **Prime power moduli**: $n \equiv r \pmod{p^c}$

  $\Rightarrow n \equiv r' \pmod{p^{c'}}, \forall c' < c, r' \equiv r \pmod{p^{c'}}$

- **CRT** with **prime modulus**: $n \equiv r \pmod{m}$

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

  there exists a unique integer $\mathbf{n} \in Z_{m_1 \cdots m_k}$ satisfying the set of k congruence equations

$$\mathbf{n} \equiv r_1 \pmod{m_1}$$
$$\equiv r_2 \pmod{m_2}$$
$$\cdots$$
$$\equiv r_k \pmod{m_k}$$

$\gcd(m_i, m_j) = 1$

note: each tuple $(r_1, r_2 \cdots, r_k)$ maps to one of $m_1 m_2 \cdots m_k$ distinct integers, which are members of the field $Z_{m_1 \cdots m_k}$

- **Prime power moduli**: $n \equiv r \pmod{p^c}$

  $\Rightarrow n \equiv r' \pmod{p^{c'}}$, $\forall c' < c$, $r' \equiv r \pmod{p^{c'}}$

- **CRT** with **prime modulus**: $n \equiv r \pmod{m}$

$$m = p_1^{c1} p_2^{c2} \cdots p_k^{ck}$$

Unique Prime Factorization Theorem

CRT w/ Moluli not Relative Prime

- **Chinese Remainder** Theorem:

  there exists a unique integer $\mathbf{n} \in Z_{m_1 \cdots m_k}$ satisfying the set of k congruence equations

$$\begin{aligned} \mathbf{n} &\equiv r_1 \pmod{m_1} \\ &\equiv r_2 \pmod{m_2} \\ &\cdots \\ &\equiv r_k \pmod{m_k} \end{aligned}$$

$\gcd(m_i, m_j) = 1$

note: each tuple $(r_1, r_2 \cdots, r_k)$ maps to one of $m_1 m_2 \cdots m_k$ distinct integers, which are members of the field $Z_{m_1 \cdots m_k}$

- **Prime power moduli**: $n \equiv r \pmod{p^c}$

$$\Rightarrow n \equiv r' \pmod{p^{c'}},\ \forall c' < c,\ r' \equiv r \pmod{p^{c'}}$$

- **CRT** with **prime modulus**: $n \equiv r \pmod{m}$ $\Longleftrightarrow$

$$\begin{aligned} n &\equiv r_1 \pmod{p_1^{c_1}} \\ &\equiv r_2 \pmod{p_2^{c_2}} \\ &\cdots \\ &\equiv r_k \pmod{p_k^{c_k}} \end{aligned}$$

$$m = p_1^{c1} p_2^{c2} \cdots p_k^{ck}$$

Unique Prime Factorization Theorem

CRT w/ Moluli not Relative Prime

CRT w/ Moluli not Relative Prime

- **CRT** with **moduli not relative prime**:

CRT w/ Moluli not Relative Prime

✧ **CRT** with **moduli not relative prime**:

$n \equiv r_1 \pmod{m_1}$

CRT w/ Moluli not Relative Prime

- ✧ **CRT** with **moduli not relative prime**:

$n \equiv r_1 \pmod{m_1} \quad m_1 = p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s}$

CRT w/ Moluli not Relative Prime

- **CRT** with **moduli not relative prime**:

$$\begin{cases} n \equiv r_1 \pmod{m_1} & m_1 = p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s} \\ n \equiv r_2 \pmod{m_2} & \end{cases}$$

CRT w/ Moluli not Relative Prime

- **CRT** with **moduli not relative prime**:

$$\begin{cases} n \equiv r_1 \pmod{m_1} & m_1 = p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s} \\ n \equiv r_2 \pmod{m_2} & m_2 = q_1^{d_1} q_2^{d_2} \cdots\cdots q_t^{d_t} \end{cases}$$

CRT w/ Moluli not Relative Prime

- **CRT** with **moduli not relative prime**:

$$\begin{cases} n \equiv r_1 \pmod{m_1} & m_1 = p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s} \\ n \equiv r_2 \pmod{m_2} & m_2 = q_1^{d_1} q_2^{d_2} \cdots\cdots q_t^{d_t} \end{cases}$$

$\exists$ i, j, such that $p_i = q_j$

i.e. mululi share common factors

CRT w/ Moluli not Relative Prime

- **CRT** with **moduli not relative prime**:

$$\left\{\begin{array}{ll} n \equiv r_1 \pmod{m_1} & m_1 = p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s} \\ n \equiv r_2 \pmod{m_2} & m_2 = q_1^{d_1} q_2^{d_2} \cdots\cdots q_t^{d_t} \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} n \equiv r_{11} \pmod{p_1^{c_1}} \\ \quad \equiv r_{12} \pmod{p_2^{c_2}} \\ \quad \cdots \\ \quad \equiv r_{1s} \pmod{p_s^{c_s}} \end{array}\right.$$

$\exists$ i, j, such that $p_i = q_j$
i.e. mululi share common factors

CRT w/ Moluli not Relative Prime

✧ **CRT** with **moduli not relative prime**:

$$\begin{cases} n \equiv r_1 \pmod{m_1} & m_1 = p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s} \\ n \equiv r_2 \pmod{m_2} & m_2 = q_1^{d_1} q_2^{d_2} \cdots\cdots q_t^{d_t} \end{cases} \Leftrightarrow \begin{cases} n \equiv r_{11} \pmod{p_1^{c_1}} \\ \quad \equiv r_{12} \pmod{p_2^{c_2}} \\ \quad \cdots \\ \quad \equiv r_{1s} \pmod{p_s^{c_s}} \\ \\ n \equiv r_{21} \pmod{q_1^{d_1}} \\ \quad \equiv r_{22} \pmod{q_2^{d_2}} \\ \quad \cdots \\ \quad \equiv r_{2t} \pmod{q_t^{d_t}} \end{cases}$$

$\exists$ i, j, such that $p_i = q_j$

i.e. mululi share common factors

CRT w/ Moluli not Relative Prime

✧ **CRT** with **moduli not relative prime**:

$$\begin{cases} n \equiv r_1 \pmod{m_1} & m_1 = p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s} \\ n \equiv r_2 \pmod{m_2} & m_2 = q_1^{d_1} q_2^{d_2} \cdots\cdots q_t^{d_t} \end{cases} \iff \begin{cases} n \equiv r_{11} \pmod{p_1^{c_1}} \\ \quad \equiv r_{12} \pmod{p_2^{c_2}} \\ \quad \cdots \\ \quad \equiv r_{1s} \pmod{p_s^{c_s}} \\ n \equiv r_{21} \pmod{q_1^{d_1}} \\ \quad \equiv r_{22} \pmod{q_2^{d_2}} \\ \quad \cdots \\ \quad \equiv r_{2t} \pmod{q_t^{d_t}} \end{cases}$$

$\exists$ i, j, such that $p_i = q_j$

i.e. mululi share common factors

solution exists if $\mathbf{r_{1i} \equiv r_{2j} \pmod{p_i^k}}$, for $p_i = q_j$, $\mathbf{k}=\min(c_i,d_j)$