Chinese remainder theorem

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Setting

Given a system of k congruences

$$\begin{aligned} x &\equiv r_1 \bmod n_1, \\ x &\equiv r_2 \bmod n_2, \\ &\vdots \\ x &\equiv r_k \bmod n_k \end{aligned}$$

we want to find x.

Setting

Given a system of k congruences

$$\begin{aligned} x &\equiv r_1 \bmod n_1, \\ x &\equiv r_2 \bmod n_2, \\ &\vdots \\ x &\equiv r_k \bmod n_k \end{aligned}$$

we want to find x.
This might not be possible:

$$\begin{aligned} x &\equiv 1 \bmod 2, \\ x &\equiv 2 \bmod 4, \end{aligned}$$

Setting

Given a system of k congruences

$$\begin{aligned} x &\equiv r_1 \bmod n_1, \\ x &\equiv r_2 \bmod n_2, \\ &\vdots \\ x &\equiv r_k \bmod n_k \end{aligned}$$

we want to find x.
This might not be possible:

$$\begin{aligned} x &\equiv 1 \bmod 2, \\ x &\equiv 2 \bmod 4, \end{aligned}$$

has x odd by the first congruence and even by the second.

Setting

Given a system of k congruences

$$\begin{aligned} x &\equiv r_1 \bmod n_1, \\ x &\equiv r_2 \bmod n_2, \\ &\vdots \\ x &\equiv r_k \bmod n_k \end{aligned}$$

we want to find x.
This might not be possible:

$$\begin{aligned} x &\equiv 1 \bmod 2, \\ x &\equiv 2 \bmod 4, \end{aligned}$$

has x odd by the first congruence and even by the second.

Theorem (Chinese remainder theorem)

If the moduli are pairwise coprime then the system of congruences has a solution and the solution is unique modulo $N = \prod_{i=1}^{k} n_i$.

How to compute CRT

`In` system of k congruences as $(r_1, n_1), (r_2, n_2), \ldots (r_k, n_k)$
with pairwise coprime n_i

`Out` smallest positive solution to system

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $x \leftarrow 0$
3. for $i = 1$ to k:
   - 3.1 $M \leftarrow N/n_i$
   - 3.2 $v \leftarrow (M^{-1} \bmod n_i)$ (use XGCD)
   - 3.3 $e \leftarrow vM$
   - 3.4 $x \leftarrow x + r_i e$
4. $x \leftarrow x \bmod N$

Example

$$\begin{aligned} x &\equiv 1 \bmod 3, \\ x &\equiv 2 \bmod 5, \\ x &\equiv 5 \bmod 7. \end{aligned}$$

$N = 3 \cdot 5 \cdot 7 = 105.$
$i = 1, M = 35$
$v^{-1} \equiv 35 \equiv 2 \bmod 3$

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $x \leftarrow 0$
3. for $i = 1$ to k:
   - 3.1 $M \leftarrow N/n_i$
   - 3.2 $v \leftarrow (M^{-1} \bmod n_i)$
   - 3.3 $e \leftarrow vM$
   - 3.4 $x \leftarrow x + r_i e$
4. $x \leftarrow x \bmod N$

Example

$$\begin{aligned} x &\equiv 1 \bmod 3, \\ x &\equiv 2 \bmod 5, \\ x &\equiv 5 \bmod 7. \end{aligned}$$

$N = 3 \cdot 5 \cdot 7 = 105.$
$i = 1, M = 35$
$v^{-1} \equiv 35 \equiv 2 \bmod 3 \Rightarrow v \equiv 2 \bmod 3$
$e = 2 \cdot 35 = 70, x = 0 + 1 \cdot 70 = 70$

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $x \leftarrow 0$
3. for $i = 1$ to k:
   - 3.1 $M \leftarrow N/n_i$
   - 3.2 $v \leftarrow (M^{-1} \bmod n_i)$
   - 3.3 $e \leftarrow vM$
   - 3.4 $x \leftarrow x + r_i e$
4. $x \leftarrow x \bmod N$

Example

$$\begin{aligned} x &\equiv 1 \bmod 3, \\ x &\equiv 2 \bmod 5, \\ x &\equiv 5 \bmod 7. \end{aligned}$$

$N = 3 \cdot 5 \cdot 7 = 105.$
$i = 1, M = 35$
$v^{-1} \equiv 35 \equiv 2 \bmod 3 \Rightarrow v \equiv 2 \bmod 3$
$e = 2 \cdot 35 = 70, x = 0 + 1 \cdot 70 = 70$

$i = 2, M = 21$
$v^{-1} \equiv 21 \equiv 1 \bmod 5$

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $x \leftarrow 0$
3. for $i = 1$ to k:
   - 3.1 $M \leftarrow N/n_i$
   - 3.2 $v \leftarrow (M^{-1} \bmod n_i)$
   - 3.3 $e \leftarrow vM$
   - 3.4 $x \leftarrow x + r_i e$
4. $x \leftarrow x \bmod N$

Example

$$\begin{aligned} x &\equiv 1 \bmod 3, \\ x &\equiv 2 \bmod 5, \\ x &\equiv 5 \bmod 7. \end{aligned}$$

$N = 3 \cdot 5 \cdot 7 = 105.$
$i = 1, M = 35$
$v^{-1} \equiv 35 \equiv 2 \bmod 3 \Rightarrow v \equiv 2 \bmod 3$
$e = 2 \cdot 35 = 70, x = 0 + 1 \cdot 70 = 70$

$i = 2, M = 21$
$v^{-1} \equiv 21 \equiv 1 \bmod 5 \Rightarrow v \equiv 1 \bmod 5$
$e = 1 \cdot 21 = 21, x = 70 + 2 \cdot 21 = 112$

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $x \leftarrow 0$
3. for $i = 1$ to k:
   - 3.1 $M \leftarrow N/n_i$
   - 3.2 $v \leftarrow (M^{-1} \bmod n_i)$
   - 3.3 $e \leftarrow vM$
   - 3.4 $x \leftarrow x + r_i e$
4. $x \leftarrow x \bmod N$

Example

$$\begin{aligned} x &\equiv 1 \bmod 3, \\ x &\equiv 2 \bmod 5, \\ x &\equiv 5 \bmod 7. \end{aligned}$$

$N = 3 \cdot 5 \cdot 7 = 105.$
$i = 1, M = 35$
$v^{-1} \equiv 35 \equiv 2 \bmod 3 \Rightarrow v \equiv 2 \bmod 3$
$e = 2 \cdot 35 = 70, x = 0 + 1 \cdot 70 = 70$

$i = 2, M = 21$
$v^{-1} \equiv 21 \equiv 1 \bmod 5 \Rightarrow v \equiv 1 \bmod 5$
$e = 1 \cdot 21 = 21, x = 70 + 2 \cdot 21 = 112$

$i = 3, M = 15$
$v^{-1} \equiv 15 \equiv 1 \bmod 7$

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $x \leftarrow 0$
3. for $i = 1$ to k:
   - 3.1 $M \leftarrow N/n_i$
   - 3.2 $v \leftarrow (M^{-1} \bmod n_i)$
   - 3.3 $e \leftarrow vM$
   - 3.4 $x \leftarrow x + r_i e$
4. $x \leftarrow x \bmod N$

Example

$$\begin{aligned} x &\equiv 1 \bmod 3, \\ x &\equiv 2 \bmod 5, \\ x &\equiv 5 \bmod 7. \end{aligned}$$

$N = 3 \cdot 5 \cdot 7 = 105.$
$i = 1, M = 35$
$v^{-1} \equiv 35 \equiv 2 \bmod 3 \Rightarrow v \equiv 2 \bmod 3$
$e = 2 \cdot 35 = 70, x = 0 + 1 \cdot 70 = 70$

$i = 2, M = 21$
$v^{-1} \equiv 21 \equiv 1 \bmod 5 \Rightarrow v \equiv 1 \bmod 5$
$e = 1 \cdot 21 = 21, x = 70 + 2 \cdot 21 = 112$

$i = 3, M = 15$
$v^{-1} \equiv 15 \equiv 1 \bmod 7 \Rightarrow v \equiv 1 \bmod 7$
$e = 1 \cdot 15 = 15, x = 112 + 5 \cdot 15 = 187$

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $x \leftarrow 0$
3. for $i = 1$ to k:
   - 3.1 $M \leftarrow N/n_i$
   - 3.2 $v \leftarrow (M^{-1} \bmod n_i)$
   - 3.3 $e \leftarrow vM$
   - 3.4 $x \leftarrow x + r_i e$
4. $x \leftarrow x \bmod N$

Example

$$\begin{aligned} x &\equiv 1 \bmod 3, \\ x &\equiv 2 \bmod 5, \\ x &\equiv 5 \bmod 7. \end{aligned}$$

$N = 3 \cdot 5 \cdot 7 = 105.$
$i = 1, M = 35$
$v^{-1} \equiv 35 \equiv 2 \bmod 3 \Rightarrow v \equiv 2 \bmod 3$
$e = 2 \cdot 35 = 70, x = 0 + 1 \cdot 70 = 70$

$i = 2, M = 21$
$v^{-1} \equiv 21 \equiv 1 \bmod 5 \Rightarrow v \equiv 1 \bmod 5$
$e = 1 \cdot 21 = 21, x = 70 + 2 \cdot 21 = 112$

$i = 3, M = 15$
$v^{-1} \equiv 15 \equiv 1 \bmod 7 \Rightarrow v \equiv 1 \bmod 7$
$e = 1 \cdot 15 = 15, x = 112 + 5 \cdot 15 = 187$

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $x \leftarrow 0$
3. for $i = 1$ to k:
   - 3.1 $M \leftarrow N/n_i$
   - 3.2 $v \leftarrow (M^{-1} \bmod n_i)$
   - 3.3 $e \leftarrow vM$
   - 3.4 $x \leftarrow x + r_i e$
4. $x \leftarrow x \bmod N$

$x \equiv 187$
$\equiv 82 \bmod 105$
Indeed

$$\begin{aligned} 82 &\equiv 1 \bmod 3, \\ 82 &\equiv 2 \bmod 5, \\ 82 &\equiv 5 \bmod 7. \end{aligned}$$