

Extending the Chinese Remainder Theorem

Example. Suppose we have three congruences to solve simultaneously:

$$(1) \quad x \equiv 3 \pmod{5}$$

$$(2) \quad x \equiv 7 \pmod{8}$$

$$(3) \quad x \equiv 5 \pmod{7}$$

“ONE AT A TIME” METHOD I

Process congruence (1). Congruence (1) is solved by

$$(4) \quad x = 5q_1 + 3.$$

Process congruence (2). Plugging equation (4) into congruence (2) gives

$$5q_1 + 3 \equiv 7 \pmod{8}$$

or

$$5q_1 \equiv 4 \pmod{8}.$$

Since $5 \cdot 5 \equiv 1 \pmod{8}$,

$$5 \cdot 5q_1 \equiv 5 \cdot 4 \pmod{8}$$

or

$$1 \cdot q_1 \equiv 20 \pmod{8}$$

or

$$q_1 \equiv 4 \pmod{8}$$

or

$$q_1 = 8q_2 + 4$$

Plugging into (4) gives

$$(5) \quad x = 5(8q_2 + 4) + 3 = 40q_2 + 23.$$

Process congruence (3). Plugging equation (5) into congruence (3):

$$40q_2 + 23 \equiv 5 \pmod{7}$$

or

$$40q_2 \equiv -18 \pmod{7}$$

or

$$5q_2 \equiv 3 \pmod{7}$$

Since $3 \cdot 5 \equiv 1 \pmod{7}$,

$$3 \cdot 5q_2 \equiv 3 \cdot 3 \pmod{7}$$

2

or

$$q_2 \equiv 2 \pmod{7}$$

or

$$q_2 = 7q_2 + 2$$

Thus, plugging into (5),

$$(6) \quad x = 40(7q_2 + 2) + 23 = 280q_2 + 103,$$

that is,

$$x \equiv 103 \pmod{280}.$$

Check:

$$103 = 20(5) + 3$$

$$103 = 12(8) + 7$$

$$103 = 14(7) + 5$$

“VECTOR” METHOD II

Step 1. Solve POW with 5 and $8 \times 7 = 56$:

$$\left(\begin{array}{cc|c} 1 & 0 & 56 \\ 0 & 1 & 5 \\ 1 & -11 & 1 \end{array} \right)$$

So

$$1 \cdot 56 + (-11) \cdot 5 = 1.$$

Set

$$(7) \quad i = 1 \cdot 56 = 56.$$

Step 2. Solve POW with 8 and $5 \times 7 = 35$:

$$\left(\begin{array}{cc|c} 1 & 0 & 35 \\ 0 & 1 & 8 \\ 1 & -4 & 3 \\ -2 & 9 & 2 \\ 3 & -13 & 1 \end{array} \right)$$

So

$$3 \cdot 35 + (-13) \cdot 8 = 1.$$

Set

$$(8) \quad j = 3 \cdot 35 = 105.$$

Step 3. Solve POW with 7 and $5 \times 8 = 40$:

$$\left(\begin{array}{cc|c} 1 & 0 & 40 \\ 0 & 1 & 7 \\ 1 & -5 & 5 \\ -1 & 6 & 2 \\ 3 & -17 & 1 \end{array} \right)$$

So

$$3 \cdot 40 + (-17) \cdot 7 = 1.$$

Set

$$(9) \quad k = 3 \cdot 40 = 120.$$

The solution to

$$x \equiv a \pmod{5}$$

$$x \equiv b \pmod{8}$$

$$x \equiv c \pmod{7}$$

is

$$(10) \quad x \equiv ai + bj + ck \pmod{5 \cdot 8 \cdot 7}.$$

In particular, for $a = 3$, $b = 7$, $c = 5$,

$$\begin{aligned} x &\equiv 3 \cdot 56 + 7 \cdot 105 + 5 \cdot 120 \pmod{280} \\ &= 1503 \pmod{280} \\ &\equiv 103 \pmod{280} \end{aligned}$$

The reason why this works is because i , j , and k have been carefully chosen so that

$$\begin{aligned} i &\equiv 1 \pmod{5} & j &\equiv 0 \pmod{5} & k &\equiv 0 \pmod{5} \\ i &\equiv 0 \pmod{8} & j &\equiv 1 \pmod{8} & k &\equiv 0 \pmod{8} \\ i &\equiv 0 \pmod{7} & j &\equiv 0 \pmod{7} & k &\equiv 1 \pmod{7}. \end{aligned}$$

Hence

$$\begin{aligned} ai + bj + ck &\equiv a \cdot 1 + b \cdot 0 + c \cdot 0 = a \pmod{5} \\ ai + bj + ck &\equiv a \cdot 0 + b \cdot 1 + c \cdot 0 = b \pmod{8} \\ ai + bj + ck &\equiv a \cdot 0 + b \cdot 0 + c \cdot 1 = c \pmod{7}. \end{aligned}$$