The Chinese Remainder Theorem

Chinese Remainder Theorem: If $m_1, m_2, .., m_k$ are pairwise relatively prime positive integers, and if $a_1, a_2, .., a_k$ are any integers, then the simultaneous congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_k \pmod{m_k}$$

have a solution, and the solution is unique modulo m, where $m = m_1 m_2 \cdots m_k$.

Proof that a solution exists: To keep the notation simpler, we will assume $k = 4$. Note the proof is constructive, i.e., it shows us how to actually construct a solution.

Our simultaneous congruences are

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad x \equiv a_3 \pmod{m_3}, \quad x \equiv a_4 \pmod{m_4}.$$

Our goal is to find integers w_1, w_2, w_3, w_4 such that:

	value mod m_1	**value mod m_2**	**value mod m_3**	**value mod m_4**
w_1	1	0	0	0
w_2	0	1	0	0
w_3	0	0	1	0
w_4	0	0	0	1

Once we have found w_1, w_2, w_3, w_4, it is easy to construct x:

$$x = a_1 w_1 + a_2 w_2 + a_3 w_3 + a_4 w_4.$$

Moreover, as long as the moduli (m_1, m_2, m_3, m_4) remain the same, we can use the same w_1, w_2, w_3, w_4 with any a_1, a_2, a_3, a_4.

First define:

$$\begin{aligned} z_1 &= m / m_1 = m_2 m_3 m_4 \\ z_2 &= m / m_2 = m_1 m_3 m_4 \\ z_3 &= m / m_3 = m_1 m_2 m_4 \\ z_4 &= m / m_4 = m_1 m_2 m_3 \end{aligned}$$

Note that

i) $z_1 \equiv 0 \pmod{m_j}$ for $j = 2, 3, 4$.

ii) $\gcd(z_1, m_1) = 1$. (If a prime p dividing m_1 also divides $z_1 = m_2 m_3 m_4$, then p divides m_2, m_3, or m_4.)

and likewise for z_2, z_3, z_4.

Next define:

$$\begin{aligned} y_1 &\equiv z_1^{-1} \pmod{m_1} \\ y_2 &\equiv z_2^{-1} \pmod{m_2} \\ y_3 &\equiv z_3^{-1} \pmod{m_3} \\ y_4 &\equiv z_4^{-1} \pmod{m_4} \end{aligned}$$

The inverses exist by (ii) above, and we can find them by Euclid's extended algorithm. Note that

iii) $y_1 z_1 \equiv 0 \pmod{m_j}$ for $j = 2, 3, 4$. (Recall $z_1 \equiv 0 \pmod{m_j}$)

iv) $y_1 z_1 \equiv 1 \pmod{m_1}$

and likewise for $y_2 z_2$, $y_3 z_3$, $y_4 z_4$.

Lastly define:

$$\begin{aligned} w_1 &\equiv y_1 z_1 \pmod{m} \\ w_2 &\equiv y_2 z_2 \pmod{m} \\ w_3 &\equiv y_3 z_3 \pmod{m} \\ w_4 &\equiv y_4 z_4 \pmod{m} \end{aligned}$$

Then w_1, w_2, w_3, and w_4 have the properties in the table on the previous page.

Example: Solve the simultaneous congruences

$$x \equiv 6 \pmod{11}, \quad x \equiv 13 \pmod{16}, \quad x \equiv 9 \pmod{21}, \quad x \equiv 19 \pmod{25}.$$

Solution: Since 11, 16, 21, and 25 are pairwise relatively prime, the Chinese Remainder Theorem tells us that there is a unique solution modulo m, where $m = 11\cdot16\cdot21\cdot25 = 92400$.

We apply the technique of the Chinese Remainder Theorem with

$$k = 4, \quad m_1 = 11, \quad m_2 = 16, \quad m_3 = 21, \quad m_4 = 25,$$
$$a_1 = 6, \quad a_2 = 13, \quad a_3 = 9, \quad a_4 = 19,$$

to obtain the solution.

We compute

$$z_1 = m / m_1 = m_2 m_3 m_4 = 16\cdot21\cdot25 = 8400$$
$$z_2 = m / m_2 = m_1 m_3 m_4 = 11\cdot21\cdot25 = 5775$$
$$z_3 = m / m_3 = m_1 m_2 m_4 = 11\cdot16\cdot25 = 4400$$
$$z_4 = m / m_4 = m_1 m_3 m_3 = 11\cdot16\cdot21 = 3696$$

$$y_1 \equiv z_1^{-1} \pmod{m_1} \equiv 8400^{-1} \pmod{11} \equiv 7^{-1} \pmod{11} \equiv 8 \pmod{11}$$
$$y_2 \equiv z_2^{-1} \pmod{m_2} \equiv 5775^{-1} \pmod{16} \equiv 15^{-1} \pmod{16} \equiv 15 \pmod{16}$$
$$y_3 \equiv z_3^{-1} \pmod{m_3} \equiv 4400^{-1} \pmod{21} \equiv 11^{-1} \pmod{21} \equiv 2 \pmod{21}$$
$$y_4 \equiv z_4^{-1} \pmod{m_4} \equiv 3696^{-1} \pmod{25} \equiv 21^{-1} \pmod{25} \equiv 6 \pmod{25}$$

$$w_1 \equiv y_1 z_1 \pmod{m} \equiv 8\cdot8400 \pmod{92400} \equiv 67200 \pmod{92400}$$
$$w_2 \equiv y_2 z_2 \pmod{m} \equiv 15\cdot5775 \pmod{92400} \equiv 86625 \pmod{92400}$$
$$w_3 \equiv y_3 z_3 \pmod{m} \equiv 2\cdot4400 \pmod{92400} \equiv 8800 \pmod{92400}$$
$$w_4 \equiv y_4 z_4 \pmod{m} \equiv 6\cdot3696 \pmod{92400} \equiv 22176 \pmod{92400}$$

The solution, which is unique modulo 92400, is

$$\begin{aligned} x &\equiv a_1 w_1 + a_2 w_2 + a_3 w_3 + a_4 w_4 \pmod{92400} \\ &\equiv 6\cdot67200 + 13\cdot86625 + 9\cdot8800 + 19\cdot22176 \pmod{92400} \\ &\equiv 2029869 \pmod{92400} \\ &\equiv \mathbf{51669} \pmod{92400} \end{aligned}$$

Example: Find all solutions of $x^2 \equiv 1 \pmod{144}$.

Solution: $144 = 16\cdot9 = 2^4 3^2$, and $\gcd(16,9) = 1$.

We can replace our congruence by two simultaneous congruences:

$$\boxed{x^2 \equiv 1 \pmod{16} \quad \text{and} \quad x^2 \equiv 1 \pmod{9}}$$

$x^2 \equiv 1 \pmod{16}$ has 4 solutions: $x \equiv \pm1$ or $\pm7 \pmod{16}$

$x^2 \equiv 1 \pmod{9}$ has 2 solutions: $x \equiv \pm1 \pmod{9}$

There are 8 alternatives:

i)	$x \equiv 1 \pmod{16}$	and	$x \equiv 1 \pmod{9}$
ii)	$x \equiv 1 \pmod{16}$	and	$x \equiv -1 \pmod{9}$
iii)	$x \equiv -1 \pmod{16}$	and	$x \equiv 1 \pmod{9}$
iv)	$x \equiv -1 \pmod{16}$	and	$x \equiv -1 \pmod{9}$
v)	$x \equiv 7 \pmod{16}$	and	$x \equiv 1 \pmod{9}$
vi)	$x \equiv 7 \pmod{16}$	and	$x \equiv -1 \pmod{9}$
vii)	$x \equiv -7 \pmod{16}$	and	$x \equiv 1 \pmod{9}$
viii)	$x \equiv -7 \pmod{16}$	and	$x \equiv -1 \pmod{9}$

By the Chinese Remainder Theorem with $k = 2$, $m_1 = 16$ and $m_2 = 9$, each case above has a unique solution for x modulo 144.

We compute: $z_1 = m_2 = 9$, $\quad z_2 = m_1 = 16$,

$y_1 \equiv 9^{-1} \equiv 9 \pmod{16}$, $\quad y_2 \equiv 16^{-1} \equiv 4 \pmod{9}$,

$w_1 \equiv 9\cdot9 = 81 \pmod{144}$, $\quad w_2 \equiv 16\cdot4 \equiv 64 \pmod{144}$.

The 8 solutions are:

i)	$x \equiv 1\cdot81 + 1\cdot64$	$\equiv$	145	$\equiv$	$\mathbf{1} \pmod{144}$
ii)	$x \equiv 1\cdot81 + (-1)\cdot64$	$\equiv$	17	$\equiv$	$\mathbf{17} \pmod{144}$
iii)	$x \equiv (-1)\cdot81 + 1\cdot64$	$\equiv$	-17	$\equiv$	$\mathbf{-17} \pmod{144}$
iv)	$x \equiv (-1)\cdot81 + (-1)\cdot64$	$\equiv$	-145	$\equiv$	$\mathbf{-1} \pmod{144}$
v)	$x \equiv 7\cdot81 + 1\cdot64$	$\equiv$	631	$\equiv$	$\mathbf{55} \pmod{144}$
vi)	$x \equiv 7\cdot81 + (-1)\cdot64$	$\equiv$	503	$\equiv$	$\mathbf{71} \pmod{144}$
vii)	$x \equiv (-7)\cdot81 + 1\cdot64$	$\equiv$	-503	$\equiv$	$\mathbf{-71} \pmod{144}$
viii)	$x \equiv (-7)\cdot81 + (-1)\cdot64$	$\equiv$	-603	$\equiv$	$\mathbf{-55} \pmod{144}$

$M_1 = N_1^{-1} \bmod n_1$

$8400 \equiv 7 \bmod 11$ Suche Lösung zu

$7 M_1 + m_1 11 = 1$

$11 = 1\cdot7 + 4$

$7 = 4 + 3$

$4 = 3 + 1$

$4 - 3 = 1$

$4 = 11 - 7$

$3 = 7 - (11 - 7)$

$3 = 2\cdot7 - 11$

$1 = 4 - 3$

$1 = (11 - 7) - (2\cdot7 + 11)$

$1 = -11 - 3\cdot7$

$[-3] = [7]^{-1} \bmod 11$

$[8]$