CRT - Chinese Remainder Theorem

N=p*q with p and q prime. You want to solve some kind of function in mod N, with the Chinese Remainder Theorem you can solve it instead in mod p and mop q.

$$x = x_p * q * (q^{-1} \ mod \ p) + x_q * p * (p^{-1} \ mod \ q)$$

The chinese remainder theorem can also be used to solve systems of simultaneous congruences (withall m_i are relative prime) of the form:

$x \ = \ a_1 \ mod \ m_1$
...
$x \ = \ a_i \ mod \ m_i$
...
$x \ = \ a_k \ mod \ m_k$

This can be solved (if there is at least one solution) by:

$$x = \sum_{i=1}^{k} a_i * M_i * (M_i^{-1} \ mod \ m_i)$$

with:

$$M_i = \prod_{n \in [1,..,k]/i} m_i$$