

and then must solve the system

$$\begin{aligned} x &\equiv a_1 \pmod{p_1} \\ x &\equiv a_2 \pmod{p_2} \\ &\vdots \\ x &\equiv a_n \pmod{p_n} \end{aligned}$$

The system is solved using the Chinese remainder theorem and we have, uniquely mod $\prod_{i=1}^n p_i$ ✓

$$x = \sum_{i=1}^n a_i \left(\prod_{j=1, j \neq i}^n p_j \right) m_i$$

where m_i is the inverse of $\prod_{j=1, j \neq i}^n p_j$ ✓

(mod p). If one of the congruences $f(x) \equiv 0 \pmod{p_i}$ has no solution, there are in general more than one solution to each congruence.

If there are $s(1)$ solutions to the 1st, $s(2)$ solutions to 2, ..., $s(n)$ solutions to (n) then we will be able to form $s(1)s(2) \dots s(n)$ n-tuples of solutions, and this will be the number of solutions mod $m (= \prod p_i)$ ✓

How to extend the method to an arbitrary modulus?

We write $m = \prod p_i^{\alpha_i}$, and take our system to solve as

$$\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_n^{\alpha_n}} \end{aligned}$$

If we can find solutions to each of these congruences, then by the Chinese remainder theorem, we can ✓