The Chinese Remainder Theorem

Suppose we wish to solve

$$x = 2 \pmod{5}$$

$$x = 3 \pmod{7}$$

for x. If we have a solution y, then $y + 35$ is also a solution. So we only need to look for solutions modulo 35. By brute force, we find the only solution is $x = 17 \pmod{35}$.

For any system of equations like this, the Chinese Remainder Theorem tells us there is always a unique solution up to a certain modulus, and describes how to find the solution efficiently.

Theorem: Let p, q be coprime. Then the system of equations

$$x = a \pmod{p}$$

$$x = b \pmod{q}$$

has a unique solution for x modulo pq.

The reverse direction is trivial: given $x \in \mathbb{Z}_{pq}$, we can reduce x modulo p and x modulo q to obtain two equations of the above form.

Proof: Let $p_1 = p^{-1} \pmod{q}$ and $q_1 = q^{-1} \pmod{p}$. These must exist since p, q are coprime. Then we claim that if y is an integer such that

$$y = aqq_1 + bpp_1 \pmod{pq}$$

then y satisfies both equations:

Modulo p, we have $y = aqq_1 = a \pmod{p}$ since $qq_1 = 1 \pmod{p}$. Similarly $y = b \pmod{q}$. Thus y is a solution for x.

It remains to show no other solutions exist modulo pq. If $z = a \pmod{p}$ then $z - y$ is a multiple of p. If $z = b \pmod{q}$ as well, then $z - y$ is also a multiple of q. Since p and q are coprime, this implies $z - y$ is a multiple of pq, hence $z = y \pmod{pq}$. ∎

This theorem implies we can represent an element of $\mathbb{Z}_{pq}$ by one element of $\mathbb{Z}_p$ and one element of $\mathbb{Z}_q$, and vice versa. In other words, we have a bijection between $\mathbb{Z}_{pq}$ and $\mathbb{Z}_p \times \mathbb{Z}_q$.

Examples: We can write $17 \in \mathbb{Z}_{35}$ as $(2,3) \in \mathbb{Z}_5 \times \mathbb{Z}_7$. We can write $1 \in \mathbb{Z}_{pq}$ as $(1,1) \in \mathbb{Z}_p \times \mathbb{Z}_q$.

In fact, this correspondence goes further than a simple relabelling. Suppose $x, y \in \mathbb{Z}_{pq}$ correspond to $(a,b), (c,d) \in \mathbb{Z}_p \times \mathbb{Z}_q$ respectively. Then a little thought shows $x + y$ corresponds to $(a + c, b + d)$, and similarly xy corresponds to (ac, bd).

A practical application: if we have many computations to perform on $x \in \mathbb{Z}_{pq}$ (e.g. RSA signing and decryption), we can convert x to $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_q$ and do all the computations on a and b instead before converting back. This is often cheaper because for many algorithms, doubling the size of the input more than doubles the running time.

Example: To compute $17 \times 17 \pmod{35}$, we can compute $(2 \times 2, 3 \times 3) = (4,2)$ in $\mathbb{Z}_5 \times \mathbb{Z}_7$, and then apply the Chinese Remainder Theorem to find that $(4,2)$ is $9 \pmod{35}$.

Let us restate the Chinese Remainder Theorem in the form it is usually presented.

For Several Equations

Theorem: Let $m_1, \ldots, m_n$ be pairwise coprime (that is $\gcd(m_i, m_j) = 1$ whenever $i \neq j$). Then the system of n equations

$$x = a_1 \pmod{m_1}$$

$$\ldots$$

$$x = a_n \pmod{m_n}$$

has a unique solution for x modulo M where $M = m_1 \ldots m_n$.

Proof: This is an easy induction from the previous form of the theorem, or we can write down the solution directly.

Define $b_i = M / m_i$ (the product of all the moduli except for m_i) and $b'_i = b_i^{-1} \pmod{m_i}$. Then by a similar argument to before,

$$x = \sum_{i=1}^{n} a_i b_i b'_i \pmod{M}$$

is the unique solution. ∎

Prime Powers First

An important consequence of the theorem is that when studying modular arithmetic in general, we can first study modular arithmetic a prime power and then appeal to the Chinese Remainder Theorem to generalize any results. For any integer n, we factorize n into primes $n = p_1^{k_1} \ldots p_m^{k_m}$ and then use the Chinese Remainder Theorem to get

$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}}$$

To prove statements in $\mathbb{Z}_{p^k}$, one starts from $\mathbb{Z}_p$, and inductively works up to $\mathbb{Z}_{p^k}$. Thus the most important case to study is $\mathbb{Z}_p$.

Ben Lynn *blynn@cs.stanford.edu*