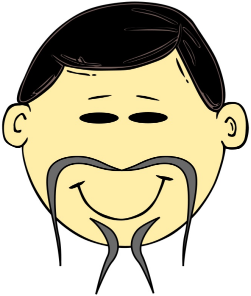
The Chinese Remainder Theorem (CRT)

We will present only a special case of the Chinese Reminder Theorem *[Sun Zi, ca 300 AD]*.



The Chinese Remainder Theorem (CRT)

Chinese Remainder Theorem (simplified version)

Let p and q be distinct primes and $N = p \cdot q$.
Let $a \in \mathbb{Z}_p$ and $b \in \mathbb{Z}_q$.

Then the system of congruences:

$$\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases}$$

is always solvable.

Moreover, if $s, r \in \mathbb{Z}$ are two integers satisfying $sp + rq = 1$ (Bézout identity), a solution of the system of congruences is

$$x = a\lambda_q + b\lambda_p$$

where $\lambda_p = sp$ and $\lambda_q = rq$.

NOTE: 'The' solution x is *unique* $\bmod N$ (otherwise there are infinitely many solutions, all possible multiple of N).

Elementary Problem $->$ Advanced Solution

At Alice's birthday party there will be either 7 or 11 guests. How many slices of cake shall Alice cut in order to be sure that in the first case there will be just 1 slice left, and in the second case only 3?

Elementary Problem $->$ Advanced Solution

Translated into math the problem becomes:

Let x be the number of slices of cake, then

$$\begin{cases} x \equiv 1 \bmod 7 \\ x \equiv 3 \bmod 11 \end{cases}$$

Find the solution x.

We need to compute the coefficients of Bézout identity: $11(2) + 7(-3) = 22 - 21 = 1$.

Now, by the CRT we have $\mathbf{x} = 1(22) + 3(518) \equiv \mathbf{36} \bmod \mathbf{77}$.

Indeed:

$$36 = 7(5) + 1, \text{ thus } 36 \equiv 1 \bmod 7$$

and

$$36 = 11(3) + 3, \text{ thus } 36 \equiv 3 \bmod 11.$$

RSA and CRT

FACT

The Chinese Remainder Theorem is extremely useful for **modular exponentiation**:

$$(x^s \bmod N)_{CRT} = (x_1^s \bmod p, x_2^s \bmod q) = (x_1^{s \bmod (p-1)} \bmod p, x_2^{s \bmod (q-1)} \bmod q).$$

We reduce the size of both the **basis** and of the **exponent** (Fermat's Little Theorem)

Applications of the CRT to Cryptography

- **In RSA**: calculations in $\mathbb{Z}_N$ (time-consuming) can be reduced to computations in $\mathbb{Z}_p$ and $\mathbb{Z}_q$ (recall $N = pq$). Since p and q are normally of about the same size (that is about $\sqrt{N}$), calculations in the *smaller* rings are much faster!
- **Secret sharing**: distributing a set of data (shares) among a certain number of people who, all together (but no one alone), can recover a certain secret from the given set of data. In this case, each of the *shares* is represented in a congruence, and the solution of the system of congruences is the secret to be recovered.
- **Parallel computations**: suppose you have a huge computation to do that involves adding, multiplying. You can choose primes $p_1, p_2, \ldots, p_k$ such that $p_1 p_2 \cdots p_k$ is surely larger than your answer, and split the computation over k processors.