Modular Arithmetic

The Chinese Remainder Theorem:

Let $n_1, \ldots, n_k$ be pairwise coprime integers: gcd(n_i, n_j)=1 whenever $i \neq j$. Then the system of k equations

$$x = a1 \pmod{n_1}$$

.....

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

has a unique solution x modulo $n \coloneqq n_1 n_2 \ldots n_k$.

Alternative formulation:

For any integer n, we denote by $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ the set of all classes (mod n).
Let $n_1, \ldots, n_k$ be pairwise coprime integers: gcd(n_i, n_j)=1 whenever $i \neq j$. Then we can identify $\mathbb{Z}_{n_1 n_2 \ldots n_k}$ with $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ as follows:

$$F : \mathbb{Z}_{n_1 n_2 \ldots n_k} \rightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

$$x \pmod{n_1 n_2 \ldots n_k} \rightarrow (x \pmod{n_1}, x \pmod{n_2}, \ldots, x \pmod{n_k}).$$

We can think of $a_i = x \pmod{n_i}$ as the (mod n_i) "coordinate" of the number x.

Conversely, knowing the coordinates $(a_1 \pmod{n_1}, a_2 \pmod{n_2}, \ldots, a_k \pmod{n_k})$ of an unknown number x, we can recover:

$$x \pmod{n_1 n_2 \ldots n_k} \leftarrow (a_1 \pmod{n_1}, a_2 \pmod{n_2}, \ldots, a_k \pmod{n_k})$$

as a sum of numbers:

$$x_1 \pmod{n_1 n_2 \ldots n_k} \leftarrow (a_1 \pmod{n_1}, 0 \pmod{n_2}, \ldots, 0 \pmod{n_k})$$

$$+ \qquad\qquad +$$

$$x_2 \pmod{n_1 n_2 \ldots n_k} \leftarrow (0 \pmod{n_1}, a_2 \pmod{n_2}, \ldots, 0 \pmod{n_k})$$

$$+ \qquad\qquad +$$

.....

$$x_k \pmod{n_1 n_2 \ldots n_k} \leftarrow (0 \pmod{n_1}, 0 \pmod{n_2}, \ldots, a_k \pmod{n_k})$$

Each x_i is easy to calculate, for example:

$$x_1 = a_1 \pmod{n_1}, \quad x_1 = 0 \pmod{n_2}, \ldots, \quad x_1 = 0 \pmod{n_k}$$

means that $x_1 = c_1 n_2 \ldots n_k$ where $c_1 = a_1 n_2^{-1} \ldots n_k^{-1} \pmod{n_1}$. Hence by a slight abuse of notation:

$$x = n_2 n_3 \ldots n_k \left(\frac{a_1}{n_2 n_3 \ldots n_k} \ (mod\ n_1) \right) + n_1 n_3 \ldots n_k \left(\frac{a_2}{n_1 n_3 \ldots n_k} \ (mod\ n_2) \right) + \cdots$$
$$+ \ n_1 n_2 \ldots n_{k-1} \left(\frac{a_k}{n_1 n_2 \ldots n_{k-1}} \ (mod\ n_k) \right)$$

where $(mod\ n_i)$ within a bracket signifies that only the quotient within that bracket is to be calculated $(mod\ n_i)$.

Example: In ancient China generals counted soldiers remaining after a battle by lining them up in rows of different lengths and calculating the total from these remainders using what we now call the Chinese Remainder Theorem. If a general had 1200 soldiers at the start of a battle and if at the end there were 3 left over when they lined up 5 at a time, 3 left over when they lined up 6 at a time, 1 left over when they lined up 7 at a time, and none left over when they lined 11 at a time, how many soldiers survived the battle?

Euler's Numbers:

$\varphi(n)$ = how many positive numbers smaller than n are relatively prime with n

In other words $\varphi(n) = |U_n|$ where $U_n = \{ a \in \mathbb{Z}_n; \quad \gcd(a, n) = 1 \}$ is the group of elements in $\mathbb{Z}_n$ which admit inverse $a^{-1} \ (mod\ n)$.

Exercise:

Given a prime number p prove $\varphi(p^k) = p^{k-1}(p-1)$.

Corollary of the Chinese Remainder Theorem:

The following sets can be identified by the bijection:

$$F : U_{n_1 n_2 \ldots n_k} \quad \rightarrow \quad U_{n_1} \quad \times \quad U_{n_2} \quad \times \ \ldots \ \times \quad U_{n_k}$$

$$x \pmod{n_1 n_2 \ldots n_k} \rightarrow (x \pmod{n_1}, \ x \pmod{n_2}, \ldots, x \pmod{n_k}).$$

Exercise:

If $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ is the prime factorization of n, then Euler's number for n is

$$\varphi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_s - 1) p_1^{k_1 - 1} p_2^{k_2 - 1} \cdots p_s^{k_s - 1}.$$

Euler's Theorem: If a is not divisible by any of these primes, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Exercise: Find the last 3 digits of $i)\ 11^{500}$; $ii)\ 2014^{2014}$.

Hint: Use Euler's theorem to reduce the exponents to smaller numbers, and then also the binomial formula (for 11=10+1, 14=10+4) to deal with the remaining powers.

The RSA encryption protocol:

- Bob releases the public key data n and k. (positive integers with $\gcd(\varphi(n), k) = 1$).
- Alice wants to send her secret number x to Bob. She knows $\gcd(x, n) = 1$. She encrypts x by calculating $b = x^k \pmod{n}$.

  Alice $\rightarrow$ Bob

  $x \rightarrow b = x^k \pmod{n}$.

- Knowing b, Bob finds x by solving the simultaneous equations:
  $x^k = b \pmod{n}$ and $x^{\varphi(n)} = 1 \pmod{n}$

Main Trick: Even though n and k may be known by the general public, in special cases only Bob can solve the decryption problem above because only he might know $\varphi(n)$.

For example, if $n = pq$ where p and q are extremely large primes, then the public will know n but won't be able to find p and q and hence neither $\varphi(n) = (p-1)(q-1)$.

Exercise:

a) Find x knowing that $x^{17} = 82$ (mod 91).

b) Decrypt *b* = 2790, knowing that the **public key** is (*n* = 3233, *k* = 17).