1. The Sun Ze Theorem

The Sun Ze Theorem is often called the Chinese Remainder Theorem. Here is an example to motivate it. Suppose that we want to solve the equation

\[ 13x = 23 \mod 2310. \]

(Note that 2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11.) Since gcd(13, 2310) = 1, we can solve the congruence using the extended Euclidean algorithm, but we want to think about it in a different way now. The idea is that

\[ 13x = 23 \mod 2310 \iff 13x = 23 (2), \ 13x = 23 (3), \ 13x = 23 (5), \ 13x = 23 (7), \ 13x = 23 (11) \]

\[ \iff x = 1 (2), \ x = 2 (3), \ 3x = 3 (5), \ 6x = 2 (7), \ 2x = 1 (11) \]

\[ \iff x = 1 (2), \ x = 2 (3), \ x = 1 (5), \ x = 5 (7), \ x = 6 (11). \]

The process has reduced one linear congruence with a large modulus to a system of linear congruences with smaller moduli. Furthermore, the moduli are pairwise coprime.

In general, given pairwise coprime positive integers \( n_1, \ldots, n_k \), compute the integers

\[ e_i = \left( \prod_{j \neq i} n_j \right) \times \left( \prod_{j \neq i} n_j \right)^{-1} \mod n_i, \quad i = 1, \ldots, k. \]

These numbers satisfy the conditions

\[ e_i = \begin{cases} 1 \mod n_i, \\ 0 \mod n_j \quad \text{for } j \neq i. \end{cases} \]

That is, they are rather like the standard basis of \( \mathbb{R}^n \) in that each \( e_i \) lies one unit along the \( i \)th direction and is orthogonal to the other directions. But in this context, direction refers to a modulus.

With the \( e_i \) in hand, we can solve the system of congruences

\[ x = a_1 (n_1), \quad x = a_2 (n_2), \quad \cdots, \quad x = a_k (n_k). \]

A solution is simply the obvious linear combination,

\[ x = a_1 e_1 + a_2 e_2 + \cdots + a_k e_k. \]
Returning to the example, a solution is
\[ x = 1 \cdot (3 \cdot 5 \cdot 7 \cdot 11) \cdot 1 + 2 \cdot (2 \cdot 5 \cdot 7 \cdot 11) \cdot 2 + 1 \cdot (2 \cdot 3 \cdot 7 \cdot 11) \cdot 3 \\
+ 5 \cdot (2 \cdot 3 \cdot 5 \cdot 11) \cdot 1 + 6 \cdot (2 \cdot 3 \cdot 5 \cdot 7) \cdot 1 \\
= 8531 \\
= 1601 \mod 2310. \\
\]
(It is easy to verify that \(13 \cdot 1601 = 23 \mod 2310\).)

2. The Sun Ze Theorem Structurally

Again let \(n_1, \ldots, n_k\) be pairwise coprime positive integers, and let \(n\) be their product. The map
\[
\mathbb{Z} \longrightarrow \prod_i \mathbb{Z}/n_i \mathbb{Z}, \quad x \longmapsto (x \mod n_1, \ldots, x \mod n_k)
\]
is a ring homomorphism. Its kernel is \(n\mathbb{Z}\). So the map descends to an injection
\[
\mathbb{Z}/n\mathbb{Z} \longrightarrow \prod_i \mathbb{Z}/n_i \mathbb{Z}, \quad x \mod n \longmapsto (x \mod n_1, \ldots, x \mod n_k)
\]
But this injection surjects as well. One can see this either by counting (both sides are finite rings with \(n\) elements) or by noting that in fact we have constructed the inverse map,
\[
\prod_i \mathbb{Z}/n_i \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad (x_1 \mod n_1, \ldots, x_k \mod n_k) \longmapsto \sum x_i e_i \mod n.
\]
For example, the inverse of
\[
\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \quad x \mod 12 \longmapsto (x \mod 4, x \mod 3)
\]
is
\[
\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}, \quad (x_1 \mod 4, x_2 \mod 3) \longmapsto 9x_1 + 4x_2 \mod 12.
\]
Especially, the the \(n_i\) are prime powers, we have an isomorphism
\[
\mathbb{Z}/(p_1^{e_1} \cdots p_k^{e_k})\mathbb{Z} \cong (\mathbb{Z}/p_1^{e_1} \mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{e_k} \mathbb{Z}),
\]
or
\[
\mathbb{Z}/(\prod_p p^{e_p})\mathbb{Z} \cong \prod_p \mathbb{Z}/p^{e_p} \mathbb{Z}.
\]

3. The Miller–Rabin Test Again

Suppose that an odd integer \(n\) factors as \(n = \prod p^{e_p}\). By the Sun Ze Theorem, the condition
\[
x^2 = 1 \mod n
\]
is equivalent to the simultaneous conditions
\[
x^2 = 1 \mod p^{e_p} \quad \text{for all } p \mid n,
\]
which in turn is equivalent to the simultaneous conditions
\[
x = \pm 1 \mod p^{e_p} \quad \text{for all } p \mid n,
\]
with all the “±” signs independent of each other. Thus, if \(n\) is divisible by \(k\) distinct primes then there are \(2^k\) square roots of 1 modulo \(p\).
Of these $2^k$ square roots of 1 modulo $n$, only one is $-1$ modulo $n$. The Miller–Rabin test returns the result that $n$ could be prime if it finds the particular square root $-1$ of 1 modulo $n$. The odds of finding $-1$ rather than some other square root of 1 are $1/2^k$, so they are at most $1/4$.

4. A Simple Threshold Scheme Based on the Sun Ze Theorem

Let $n_1, \ldots, n_k$ be pairwise coprime integers, all large. Define

\[ N = \text{the product of all the } n_i, \]
\[ n = \text{the product of all the } n_i \text{ except } n_k. \]

Thus
\[ N/n = n_k. \]

Consider a secret number
\[ x: 0 \leq x < N. \]

Let $a_i = x \% n_i$ for $i = 1, \ldots, k$. Then:

\[ \text{All } k \text{ of the } a_i \text{ determine } x, \text{ but the first } k-1 \text{ of them do not.} \]

Indeed, given $a_1$ through $a_k$, the Sun Ze Theorem shows how the congruences
\[ \tilde{x} = a_i \mod n_i, \quad i = 1, \ldots, k, \]
give us a value $\tilde{x}$ in $\{0, \cdots, N-1\}$ that agrees with $x$ modulo $N$. But also $x$ lies in the same range as $\tilde{x}$, so they are equal.

On the other hand, given only $a_1$ through $a_{k-1}$, we can solve the congruences
\[ \tilde{x} = a_i \mod n_i, \quad i = 1, \ldots, k-1, \]
and so we have a value $\tilde{x} \in \{0, \cdots, n-1\}$ that agrees with $x$ modulo $n$. But also $\tilde{x}$ plus any multiple of $n$ is a candidate for $x$ until we reach $N$. Thus there are $N/n = n_k$ candidates for $x$ based on $\tilde{x}$. 