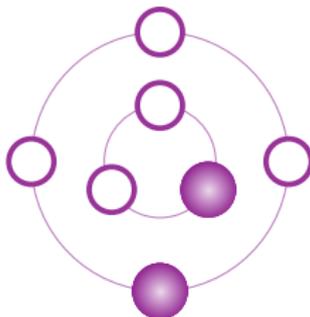


Chinese Remainder Theorem explained with rotations



Reference: Antonella Perucca, *The Chinese Remainder Clock*,
The College Mathematics Journal, 2017, Vol. 48, No. 2, pp. 82-89.

One step-wise rotation

Consider a circle with one marked point on it.

- ▶ Fix some positive integer m . At every time unit, let the point move $\frac{1}{m}$ -th of the circle clockwise.
- ▶ This phenomenon is periodic, the fundamental period is m .
- ▶ We identify the positions with the integers from 0 to $m - 1$. For convenience, we set the initial position and 0 at the top.

Example: $m = 3$, the position at time 0

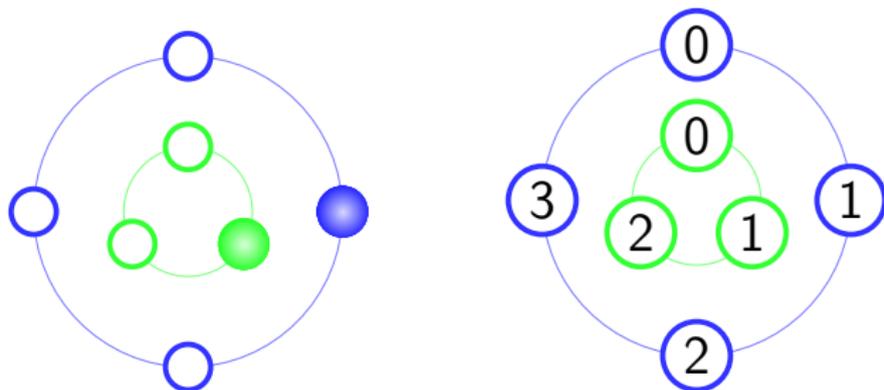


Two simultaneous rotations

Consider two simultaneous rotations with m_1 and m_2 steps.

- ▶ There are $m_1 \cdot m_2$ configurations for the pair of points.

Example: $m_1 = 3$ and $m_2 = 4$, the configuration at time 1

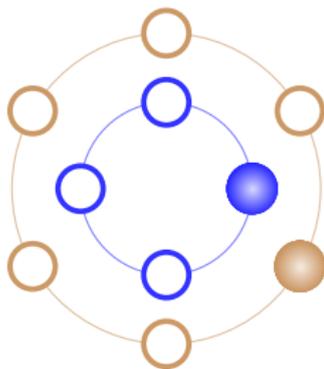
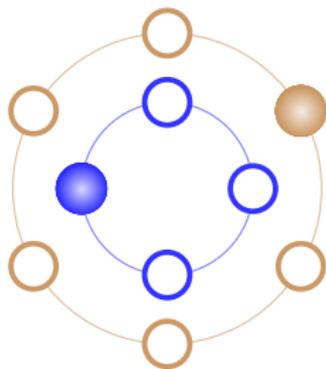


Impossible configurations

Consider two simultaneous rotations with m_1 and m_2 steps.

- ▶ In general, not all of configurations occur because the rotations are simultaneous (this is evident if $m_1 = m_2$).

Example: $m_1 = 4$ and $m_2 = 6$, the configuration at time 7 and an impossible configuration



Fundamental period for two rotations

- ▶ **The fundamental period is the least common multiple of the single periods.**

Indeed, the fundamental period is the smallest positive time at which both points are back to the initial position, namely the least common multiple of m_1 and m_2 .

- ▶ Each configuration occurs at most once in every fundamental period (because getting the same configuration implies that both points did full turns).

We deduce:

- ▶ **The fundamental period is the number of occurring configurations.**
- ▶ Special case m_1 and m_2 coprime:
The fundamental period is $m_1 \cdot m_2$, every configuration occurs.

Generalisation to several rotations

Consider simultaneous rotations with $m_1, m_2 \dots, m_n$ steps.

- ▶ **The fundamental period is the least common multiple of the single periods.**

Namely, the least common multiple of $m_1, m_2 \dots, m_n$.

- ▶ Each configuration occurs at most once in every fundamental period.
- ▶ **The fundamental period is the number of occurring configurations.**
- ▶ Special case $m_1, m_2 \dots, m_n$ pairwise coprime:
The fundamental period is the product $m_1 \cdots m_n$, every configuration occurs.

CRT for rotations

We have thus proven:

Chinese Remainder Theorem for rotations

Let m_1, \dots, m_n be pairwise coprime positive integers. For each integer m in this set, consider a circle with one marked point on it, which at every time unit rotates of $\frac{1}{m}$ -th of the circle clockwise. The fundamental period for this phenomenon is $m_1 \cdots m_n$, and every configuration for the n -tuple of marked points occurs exactly once in the fundamental period.

Remark: Even if the integer parameters are not coprime, the configuration of the marked points determines the time inside a fundamental period because it occurs at most once.

CRT for cyclic periodic phenomena

Consider a cyclic periodic phenomenon, where finitely many distinct situations repeat cyclically. This can be seen as a rotation with as many steps as the fundamental period, so we have proven:

Chinese Remainder Theorem for cyclic periodic phenomena

If m_1, \dots, m_n are pairwise coprime positive integers, then a cyclic periodic phenomenon with fundamental period $m_1 \cdots m_n$ amounts to the collection of simultaneous cyclic periodic phenomena whose fundamental periods are m_1 to m_n .

Corollary: A cyclic periodic phenomenon with fundamental period m can be described by cyclic periodic phenomena whose fundamental periods are the prime powers appearing in the factorization of m .

CRT for lists of remainders

Chinese Remainder Theorem for lists of remainders

Let m_1, \dots, m_n be pairwise coprime positive integers. For every integer consider the n -tuple of its remainders after division by m_1 to m_n . We then have:

- ▶ Two integers produce the same n -tuple if and only if they leave the same remainder after division by the product $m_1 \cdots m_n$.
- ▶ All n -tuples consisting of remainders after division by m_1 to m_n are produced.

Proof: The result can be deduced from the CRT for rotations. A list of remainders can be identified (in an obvious way) with a configuration of marked points. □

The usual CRT

Chinese Remainder Theorem

Let m_1, \dots, m_n be pairwise coprime positive integers. An integer in the range from 0 to $m_1 \cdots m_n - 1$ is uniquely determined by the n -tuple of its remainders after division by m_1 to m_n .

Proof: This is a reformulation of the previous result. □

Generalisation of the usual CRT

Generalized Chinese Remainder Theorem

Let m_1, \dots, m_n be positive integers. An integer in the range from 0 to $\text{lcm}(m_1, \dots, m_n) - 1$ is uniquely determined by the n -tuple of its remainders after division by m_1 to m_n .

Proof: The result can be deduced from the corresponding result about simultaneous step-wise rotations. \square

Remark that an impossible n -tuple of remainders corresponds to an impossible configuration for the n -tuple of marked points.

**Thank you
for your attention!**