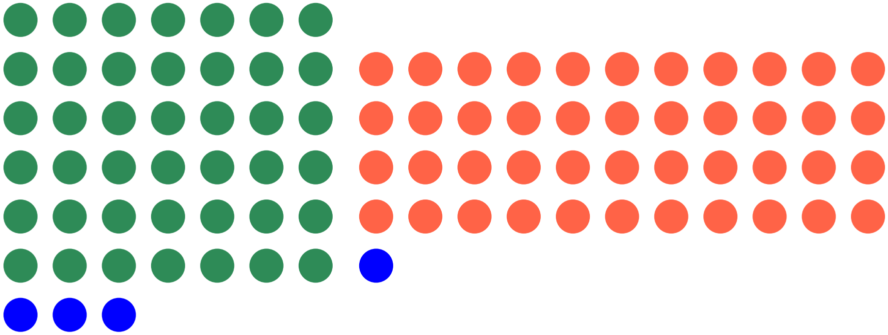
What is...the Chinese remainder theorem?

Or: Arranging rectangles

A puzzle à la Sun-tzu



Puzzle. What is the smallest $n \in \mathbb{N}$ such that we can arrange n into $7 \times a$ and $11 \times b$ rectangles with leftovers 3 and 1?

45 **of course! But why?**

The puzzle asks to solve the congruences:

$$\text{Given. } \begin{cases} n \equiv 3 \bmod 7 \\ n \equiv 1 \bmod 11 \end{cases} \quad \text{Task. Find minimal } n$$

- System of congruences

$$\text{Given. } \begin{cases} n \equiv r_1 \bmod m_1 \\ \vdots \\ n \equiv r_k \bmod m_k \end{cases} \quad \text{Task. Find minimal } n$$

  are analogs of systems of linear equations
- How can one solve these systematically?
- Can this be generalized?

Here what we can do

0	1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43
44	45	46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63	64	65
66	67	68	69	70	71	72	73	74	75	76

- Write down a numbered $11 \cdot 7$ square
- Mark the second column, and every seventh entry starting at 3
- The intersection of the markers is the unique solution

For completeness: The formal statement

For coprime moduli $m_1, \ldots, m_k$ and remainders $r_1, \ldots, r_k$, there is $n \in \mathbb{N}$ such that:

(a) $n < N = m_1 \cdot \ldots \cdot m_k$

(b) n satisfies the congruences Existence

$$n \equiv r_1 \bmod m_1$$
$$\vdots$$
$$n \equiv r_k \bmod m_k$$

(c) n is unique Uniqueness

(d) The assignment

$$n \bmod N \mapsto (n \bmod m_1, \ldots, n \bmod m_k)$$

is a group isomorphism

$$\mathbb{Z}/N\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$$

The restriction “coprime” is necessary, otherwise the statement will look different

Generalization? Sure!

Fix a ring R

(a) Two ideals I, J are coprime if $I + J = R$ Bézout in rings

(b) For (two-sided) ideals $I_1, ..., I_k$ let be I their intersection

(c) The assignment

$$n \bmod I \mapsto (n \bmod I_1, ..., n \bmod I_k)$$

is a group isomorphism

$$R/I \xrightarrow{\cong} R/I_1 \times ... \times R/I_k$$

Existence Uniqueness

(d) If R is commutative, then $I = I_1 \cdot ... \cdot I_k$

This applies, for example, to polynomial rings

Thank you for your attention!

I hope that was of some help.