To further reduce the amount of computations in solving congruences it is important to realise that if $m = m_1 m_2 \dots m_s$ where the m_i are pairwise coprime, then $a \equiv b \pmod{m}$ if and only if $a \equiv b \pmod{m_i}$ for every i, $1 \le i \le s$. This leads to the question of simultaneous solution of a system of congruences.

Theorem 1 (Chinese Remainder Theorem)**.** *Let $m_1, m_2, \dots, m_s$ be pairwise coprime integers ≥ 2, and $b_1, b_2, \dots, b_s$ arbitrary integers. Then, the s congruences $x \equiv b_i \pmod{m_i}$ have a simultaneous solution that is unique modulo $m = m_1 m_2 \dots m_s$.*

Proof. Let $n_i = m/m_i$; note that $(m_i, n_i) = 1$. Every n_i has an inverse $\bar{n}_i \bmod m_i$ (lecture 2). We show that $x_0 = \sum_{1 \le j \le s} n_j \bar{n}_j b_j$ is a solution of our system of s congruences. Since m_i divides each n_j except for n_i, we have $x_0 = \sum_{1 \le j \le s} n_j \bar{n}_j b_j \equiv n_i \bar{n}_i b_j \pmod{m_i} \equiv b_i \pmod{m_i}$. Uniqueness: If x is any solution of the system, then $x - x_0 \equiv 0 \pmod{m_i}$ for all i. This implies that $m | (x - x_0)$ i.e. $x \equiv x_0 \pmod{m}$. □

Exercise 1. Find all solutions of the system $4x \equiv 2 \pmod 6$, $3x \equiv 5 \pmod 7$, $2x \equiv 4 \pmod{11}$.

Exercise 2. Using the Chinese Remainder Theorem (CRT), solve $3x \equiv 11 \pmod{2275}$.

Systems of linear congruences in one variable can often be solved efficiently by combining inspection (I) and Euclid's algorithm (EA) with the Chinese Remainder Theorem (CRT).

Example. Consider the congruence $13x \equiv 71 \pmod{380}$. Using (CRT) we obtain an equivalent system $13x \equiv 71 \pmod m$ where $m = 4, 5, 19$, which, finding multiplicative inverses by (EA) or (I), can be simplified to $x \equiv 3 \pmod 4$, $x \equiv 2 \pmod 5$, and $x \equiv 4 \pmod{19}$. All solutions of the 3rd congruence have the form $4 + 19s$ for $s \in Z$. By (EA) or by (I) we see that for $s = 2$ we *also* obtain a solution 42 of the 2nd congruence, and by (CRT) this solution is unique $\pmod{95}$. It remains to look for solutions of the 1st congruence among the integers $42 + 95t$ for $t \in Z$; by (EA) or (I) we find that $t = -1$ works. Invoking (CRT) again, we have a unique solution $x \equiv -53 \pmod{380}$.

An extension of the CRT to arbitrary moduli was described in full detail by Qin Jiushao in the 13th century AD (parts of it were known to Yih-Hing in the 7th century AD).

Theorem 2. *Let $m_1, m_2, \dots, m_s$ be integers ≥ 2 and let $b_1, b_2, \dots, b_s$ be any integers. Then the s congruences $x \equiv b_i \pmod{m_i}$ have a simultaneous solution if and only if $\gcd(m_i, m_j)$ divides $b_i - b_j$ whenever $i \ne j$. When this is satisfied, the solution is unique mod $\operatorname{lcm}(m_1, m_2, \dots, m_s)$.*

Proof. Necessity and uniqueness are easy. Sufficiency: For each i replace $x_i \equiv b_i \pmod{m_i}$ with an equivalent set of congruences $x_i \equiv b_i \pmod q$), where q are the prime power factors in the factorisation of m_i. For a given prime p, let e be the largest integer such that p^e divides some m_i. If now p^k divides an m_j with $j \ne i$, then $k \le e$ and hence p^k divides $b_i - b_j$ since $\gcd(m_i, m_j)$ does. In this case $x \equiv b_i \pmod{p^e}$ implies $x \equiv b_j \pmod{p^k}$. Thus, from the new set of congruences we may discard, for a given p, all congruences except for the one with the highest power of p. Apply CRT. □

Structure of the ring $\mathbb{Z}_m$. As in Theorem 1, let $m_1, m_2, \dots, m_s$ be pairwise coprime integers ≥ 2, and $m = m_1 m_2 \cdots m_s$.
The mapping $f \colon \mathbb{Z} \to R = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s}$ given by

$$n \mapsto (n \bmod m_1,\ n \bmod m_2, \dots,\ n \bmod m_s)$$

is a ring homomorphism (easy exercise). Its kernel consists of all multiples of $m = \operatorname{lcm}(m_1, \dots, m_s)$. By the first isomorphism theorem, the image of f is therefore isomorphic to $\mathbb{Z}_m$. Counting the number of elements in R and in $\mathbb{Z}_m$ (there are m elements in each of them), we see that f is *onto*. This provides an alternative proof of Theorem 1.

The numbers $e_i = n_i \bar{n}_i$ in the proof of Theorem 1 have the property that $e_i \equiv 1 \pmod{m_i}$ and $e_i \equiv 0 \pmod{m_j}$ for $j \ne i$. Moreover, $e_i^2 \equiv e_i \pmod m$ for all i and $\sum_i e_i \equiv 1 \pmod m$.

Theorem 1 reduces the study of the rings $\mathbb{Z}_n$ for arbitrary $n \in \mathbb{N}$ to the study of the rings $\mathbb{Z}_{p^k}$ where p is a prime number.

GAP Commands:

`ChineseRem([55,17],[1,0]);` finds an integer $x \in [0, \operatorname{lcm}(55, 17))$ which satisfies $x \equiv 1 \pmod{55}$ and $x \equiv 0 \pmod{17}$.

Similarly: `ChineseRem([13,101,59,54,77],[1,2,3,4,5]);` for 5 simultaneous congruences.

If you say `ChineseRem([55,33],[0,1]);` GAP will complain, because it is only a computer program and cannot perform the impossible (see Theorem 2).