Congruences

Application of discrete models

1 Definition and properties

Definition 1.1. $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ are **congruent** modulo $m \in \mathbb{N}^+$ if $m \mid b - a$.
Notation: $a \equiv b \pmod{m}$, or simply $a \equiv b\ (m)$. Notation of negation: $a \not\equiv b \pmod{m}$.
Terminology: m is the **modulus** (plural: *moduli*), and "$a \equiv b \pmod{m}$" is a **congruence**.

Example. $14 \equiv 34 \pmod{10}$ ("14 and 34 are congruent modulo 10"), because $10 \mid 34 - 14$.

As we can see, $a \equiv b \pmod{10}$ if and only if the last digit of a and b are the same (at least for nonnegative a and b). In general, $a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m, i.e. $a \bmod m = b \bmod m$. Roughly speaking, we could say that "congruent" = "having the same remainder".

Example. $9 \equiv 23\ (7)$, because $7 \mid 23 - 9$, and indeed: both 9 and 23 have the remainder 2 when divided by 7.

(Note: "mod" has two different meanings: in the expression "$a \bmod m$", it means the remainder of the integer division, e.g. $34 \bmod 10 = 4$; but in "$a \equiv b \pmod{m}$", it refers to the whole "equation" (more precisely *congruence*), as defined above. In the latter case, the right-hand side is not necessarily the remainder, e.g. $14 \equiv 34 \pmod{10}$ doesn't contain 4 on either side.)

Congruences are useful in calculations where we are only interested in the remainder (for a certain divisor m). For example, we do this with clocks: if it is currently 18 o'clock, then 10 hours later it is not 28 o'clock, but $28 \bmod 24 = 4$ o'clock. This can also be written as $18 + 10 \equiv 4\ (24)$.

Theorem 1.2 (properties of congruence)**.** *For any $m \in \mathbb{N}^+$:*

1. *reflexive:* $\forall a \in \mathbb{Z} : a \equiv a\ (m)$;
2. *symmetric:* $\forall a, b \in \mathbb{Z} : a \equiv b\ (m) \implies b \equiv a\ (m)$;
3. *transitive:* $\forall a, b, c \in \mathbb{Z} : a \equiv b\ (m) \land b \equiv c\ (m) \implies a \equiv c\ (m)$.
4. *addition:* $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z} : a_1 \equiv b_1\ (m) \land a_2 \equiv b_2\ (m) \implies a_1 + a_2 \equiv b_1 + b_2\ (m)$.
5. *subtraction:* $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z} : a_1 \equiv b_1\ (m) \land a_2 \equiv b_2\ (m) \implies a_1 - a_2 \equiv b_1 - b_2\ (m)$.
6. *multiplication:* $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z} : a_1 \equiv b_1\ (m) \land a_2 \equiv b_2\ (m) \implies a_1 a_2 \equiv b_1 b_2\ (m)$.
7. *exponentiation:* $\forall a, b \in \mathbb{Z}, n \in \mathbb{N} : a \equiv b\ (m) \implies a^n \equiv b^n\ (m)$.

2 Congruence classes

The above theorem says that the congruence relation ($\equiv$) is reflexive, symmetric and transitive – in other words, it is an *equivalence relation* (see e.g. Discrete mathematics I). And we know that an equivalence relation *partitions* the base set, i.e. it splits it into disjoint sets called *classes*. The congruence relation $a \equiv b \pmod{m}$ partitions $\mathbb{Z}$ into the following classes:

$$\{km \quad \mid k \in \mathbb{Z}\},$$
$$\{km+1 \mid k \in \mathbb{Z}\},$$
$$\{km+2 \mid k \in \mathbb{Z}\},$$
$$\ldots,$$
$$\{km+m-1 \mid k \in \mathbb{Z}\}.$$

Two numbers are in the same class if and only if they have the same remainder when divided by m. For example, the classes for $m = 5$ are the following:

$$\{5k \quad \mid k \in \mathbb{Z}\} = \{\ldots, -10, -5, 0, 5, 10, \ldots\},$$
$$\{5k+1 \mid k \in \mathbb{Z}\} = \{\ldots, -9, -4, 1, 6, 11, \ldots\},$$
$$\{5k+2 \mid k \in \mathbb{Z}\} = \{\ldots, -8, -3, 2, 7, 12, \ldots\},$$
$$\{5k+3 \mid k \in \mathbb{Z}\} = \{\ldots, -7, -2, 3, 8, 13, \ldots\},$$
$$\{5k+4 \mid k \in \mathbb{Z}\} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}.$$

Definition 2.1. For a given m, the equivalence classes defined by the congruence relation are called **congruence class**es (or **residue class**es) modulo m. Notation: $\overline{a}$ is the congruence class that contains $a \in \mathbb{Z}$. (Or if the modulus m is not implied from the context, then $\overline{a}_m$.)

Example. For $m = 5$, a congruence class is $\overline{3} = \{5k+3 \mid k \in \mathbb{Z}\} = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$.

The definition of $\overline{a}$ is valid, because each $a \in \mathbb{Z}$ is contained in exactly one congruence class. But one class has multiple notations, e.g. for $m = 5$: $\overline{3} = \overline{8} = \overline{28} = \overline{-2} = \ldots$.

Definition 2.2. The set of all congruence classes modulo m is denoted by $\mathbb{Z}_m$ (alternative notations: $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\langle m \rangle$), i.e. $\mathbb{Z}_m := \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

(Note: the elements of $\mathbb{Z}_m$ are not numbers, but sets (congruence classes), e.g. $2 \neq \overline{2}$, but $2 \in \overline{2}$.)

To make the congruence class notation unique, we can select one element from each class, and use only that element for referencing the class. That is, we need the following:

Definition 2.3. A set of integers that contains exactly one element from each congruence class is called a **complete residue system** (modulo m).

Example. All of the following sets are complete residue systems modulo 5:
$\{0, 1, 2, 3, 4\}$, $\{1, 2, 3, 4, 5\}$, $\{-2, -1, 0, 1, 2\}$, $\{34, 35, 36, 37, 38\}$, $\{10, 6, -3, 23, -6\}$ etc.

There are infinitely many complete residue systems for any m. All complete residue systems modulo m contain exactly m elements. A very common complete residue system is $\{0, 1, \ldots, m-1\}$.

We can do operations between congruence classes:

Definition 2.4. For a given modulus $m \in \mathbb{N}^+$ and any $a, b \in \mathbb{Z}$:

- $\overline{a} + \overline{b} := \overline{a+b}$,
- $\overline{a} - \overline{b} := \overline{a-b}$,
- $\overline{a} \cdot \overline{b} := \overline{ab}$.

Example. For $m = 10$: $\overline{7} + \overline{3} \cdot \overline{6} = \overline{7} + \overline{18} = \overline{7} + \overline{8} = \overline{15} = \overline{5}$. This can also be written equivalently using congruences: $7 + 3 \cdot 6 \equiv 7 + 8 \equiv 5 \ (10)$.

Calculating with congurence classes is called **modular arithmetic**.

3 Linear congruences

We have seen above, at the properties of congruences, that they can be added, subtracted, multiplied and exponentiated. But there was no mention about division – and for good reason. For example, we can't just divide the congruence $4 \equiv 14\ (10)$ by 2, because then we would break it: $2 \not\equiv 7\ (10)$. But then, what can we do with division?

First: what does division mean at all? In the set of real numbers, b/a means the unique $x \in \mathbb{R}$ for which $ax = b$. (E.g. $6/2 = 3$ is the solution of $2x = 6$.) That is, division is just solving a linear equation. So it is worth examining the modular analogue of linear equations:

Definition 3.1. A congruence of the form $ax \equiv b\ \pmod{m}$, where $a, b \in \mathbb{Z}$ are known parameters and $x \in \mathbb{Z}$ is the unknown, is called a **linear congruence**.

Example. $2x \equiv 6\ \pmod{10}$ is a linear congruence, and $x = 3$ is *one* of its solutions.

In this section, we examine how to solve linear congruences, i.e. how to find all solutions.

First of all, notice that if x is a solution, then $x + m$, $x + 2m$ etc. are also solutions, since we calculate "modulo m", i.e. only the remainder by m is relevant. For example, if $x = 3$ is a solution of $2x \equiv 6\ (10)$, then $x = 13$, $x = 23$, $x = -7$ etc. are also solutions. These infinitely many solutions can be summarized as $x \equiv 3\ (10)$.

(For simplicity, we will not differentiate between these congruent solutions, i.e. we will say that the linear congruence has a *unique solution* if all solutions are congruent modulo m; or we will say that it has *two solutions* if the solutions are from two different congruence classes; and so on.)

Therefore, to solve the congruence $ax \equiv b\ \pmod{m}$, we only need to check $x = 0, 1, 2, \ldots, m-1$, since any other number is congruent to some of these x's. (In other words, we need to check exactly the elements of a complete residue system.) So in the above example, we only need to check 10 numbers. To do this, we can calculate the following fraction of a modular times table (where the first row is x, the second row is $2x$ mod 10, and the thrid row is $3x$ mod 10):

```
sage: matrix([[a*x % 10 for x in range(10)] for a in range(1,4)])
[0 1 2 3 4 5 6 7 8 9]
[0 2 4 6 8 0 2 4 6 8]
[0 3 6 9 2 5 8 1 4 7]
```

With that, we can observe the following:

- The congruence $2x \equiv 6\ (10)$ has *two* solutions:
  - $x \equiv 3\ (10)$ (which we already knew from $6/2 = 3$);
  - $x \equiv 8\ (10)$ (which is less obvious).

  Or, since their distance is exactly 5, we can combine them into a single congruence: $x \equiv 3\ (5)$.
- Now consider the linear congruence $3x \equiv 8\ (10)$. The table says that it has exactly one solution: $x \equiv 6\ (10)$. (This is also not obvious, because $8/3$ is not an integer. To understand this, we need to replace 8 with 18: $18/3 = 6$.)
- In general, congruences of the form $3x \equiv b\ (10)$ are all uniquely solvable, because the third row of the table contains each remainder exactly once.
- And what about congruences of the form $2x \equiv b\ (10)$? Since the second row contains only even numbers, odd b's have no solution. But since all even remainders occur twice, every even b gives two solutions.

For a small modulus like $m = 10$, the above *brute force* method, i.e. trying out m numbers to find a solution, works perfectly well. But for bigger m's, we need a more efficient method.

For that, let's unpack the linear congruence $ax \equiv b \pmod{m}$ using the definition:

$$\begin{aligned} ax &\equiv b \pmod{m} \\ &\Downarrow \quad \text{(definition of congruence)} \\ m &\mid b - ax \\ &\Downarrow \quad \text{(definition of divisibility)} \\ \exists y \in \mathbb{Z} &: my = b - ax \\ &\Downarrow \quad \text{(rearrangement)} \\ \exists y \in \mathbb{Z} &: ax + my = b \end{aligned}$$

This is a linear Diophantine equation, which we already know how to solve from the previous document (Greatest common divisor). And we only need to find x, not y. We know that this equation has a solution if and only if $\gcd(a, m) \mid b$, and if x_0 is a solution for x, then there are infinitely many solutions, which can be written as $x = x_0 + k \cdot m \,/\, \gcd(a, m)$, where k is an arbitrary integer. So the distance between adjacent solutions is $m \,/\, \gcd(a, m)$, which means that there are exactly $\gcd(a, m)$ solutions between 0 and $m-1$. In particular, if $\gcd(a, m) = 1$, i.e. a and m are coprime, then it has a unique solution. Putting this together:

Solving a linear congruence:

Input: $a, b \in \mathbb{Z}, m \in \mathbb{N}^+$, the parameters of the congruence $ax \equiv b \pmod{m}$
Output: all solutions between 0 and $m-1$
$(g, x_g, y_g) :=$ Extended Euclidean algorithm(a, m) *(y_g is not needed)*
if $g \nmid b$ **then** $\rightarrow$ *no solution*
One solution: $x_0 := x_g \cdot b/g \bmod m/g$
All solutions: $x_0,\ x_0 + m/g,\ x_0 + 2m/g,\ \ldots,\ x_0 + (g-1)m/g$
(or: $x = x_0 + k \cdot m/g \quad (k = 0, 1, \ldots, g-1)$)
(or: $x \equiv x_0 \pmod{m/g}$)

Example. For $2x \equiv 6 \pmod{10}$, we have $g = \gcd(2, 10) = 2$, and the Bézout coefficient is $x_g = 1$ (and $y_g = 0$, but that we don't need). Since $g \mid 6$, it has solutions, and exactly two ($g = 2$): the first one is $1 \cdot 6/2 \bmod 10/2 = 3 \bmod 5 = 3$, and the second one is $3 + 10/2 = 8$ (as we have seen above).

Example. For $3x \equiv 8\ (10)$, we have $g = \gcd(3, 10) = 1$, and the Bézout coefficient is $x_g = -3$. Since $g \mid 8$ and $g = 1$, it has exactly one solution: $x := -3 \cdot 8/1 \bmod 10/1 = -24 \bmod 10 = 6$.

Note: according to the note in the previous document at the linear Diophantine equations, we can simplify the calculation by dividing the congruence by $\gcd(a, m)$ (along with the modulus), because then we get $g = 1$ in the algorithm above, so we have exactly one solution (with respect to the new modulus). For example, dividing $2x \equiv 6\ (10)$ by 2 gives $x \equiv 3\ (5)$, which is already the solution itself. Other example: $4x \equiv 6\ (10) \longrightarrow 2x \equiv 3\ (5)$, which can be solved in the above way to get $x \equiv 4\ (5)$, which corresponds to $x \equiv 4\ (10)$ and $x \equiv 9\ (10)$.

Naturally, Sage can solve linear congruences, using the `solve_mod()` function:

```
sage: solve_mod(2*x == 6, 10)
[(8,), (3,)]
sage: _[1][0]   # the second solution
3
sage: for (xx,) in solve_mod(2*x == 6, 10):
....:     assert xx*2 % 10 == 6   # checking the result
```

4 Modular inverse

There is an important special case of linear congruences, when the right-hand side is 1:

Definition 4.1. The **modular inverse** of $a \in \mathbb{Z}$ modulo m is the solution of the linear congruence $ax \equiv 1 \pmod{m}$. Notation: $a^{-1} \bmod m$. If it exists, we say that a is **invertible** modulo m.

Example. The modular inverse of 3 modulo 10 is 7, because $3x \equiv 1\ (10)$ has the solution $x = 7$.

Example. 2 is not invertible modulo 10, because the congruence $2x \equiv 1\ (10)$ has no solution.

Similarly to how the linear congruence corresponds to division, the modular inverse corresponds to the reciprocal $(1/x)$: for example, the inverse of 3 in $\mathbb{R}$ (i.e. its reciprocal) is $1/3$, and its modular inverse is 7 (modulo 10), as multiplying either of them by 3 (in the appropriate way) gives 1.

If the inverse exists, it is always unique: the condition above for solving a linear congruence is $\gcd(a, m) \mid b$, where now $b = 1$, so the inverse exists if and only if $\gcd(a, m) = 1$, in which case we have already seen that there is exactly one solution. Again:

Theorem 4.2. *$a \in \mathbb{Z}$ is invertible modulo m if and only if a and m are coprime, i.e.* $\gcd(a, m) = 1$.

Example. For $m = 10$, only 1, 3, 7 and 9 are invertible (because the others are divisible by 2 or 5).

Theorem 4.3. *If m is prime, then all $a \not\equiv 0 \pmod{m}$ numbers are invertible modulo m.*

So for a prime modulus, all remainders except $a = 0$ are invertible. This is similar to $\mathbb{R}$, where we can divide by any number except 0.

For small m, the brute force method still works, i.e. to check all x between 1 and $m-1$ whether $ax \equiv 1 \pmod{m}$, and if so, then that x is the inverse.

For big m, we can use a simplified version of solving a linear congruence:

Modular inverse(a, m):

> **Input:** $a \in \mathbb{Z}, m \in \mathbb{N}^+$
> $(g, x_g, y_g) :=$ Extended Euclidean algorithm(a, m) *(y_g is not needed)*
> **if** $g \neq 1$ **then** $\rightarrow$ *not invertible*
> **Output:** $x_g \bmod m$

Notice that if the inverse exists, then it coincides with the Bézout coefficient for a (at least modulo m).

Why is the modular inverse interesting? For example, if we need to solve linear congruences of the form $3x \equiv b\ (10)$ for many different b's, then we only need to solve one: $3x \equiv 1\ (10)$, i.e. calculate the inverse of 3 modulo 10 (which is 7), and then we get the solution of all such congruences by multiplying the solution $3 \cdot 7 \equiv 1\ (10)$ by b: $3 \cdot 7b \equiv b\ (10)$, i.e. $x \equiv 7b\ (10)$. In general:

Theorem 4.4. *The solution of $ax \equiv b\ (m)$ is $x \equiv a^{-1}b\ (m)$, where a^{-1} is the inverse of a.*

(This is like calculating b/a in $\mathbb{R}$ by multiplying b by $1/a$.)

Sage can calculate the modular inverse by the `inverse_mod()` function:

```
sage: inverse_mod(3, 10)
7
sage: inverse_mod(2, 10)
[...]
ZeroDivisionError: inverse of Mod(2, 10) does not exist
```

5 Bank account numbers

A Hungarian bank account number is 3×8 or 2×8 digits, for example:

10402166-50526765-81771006.

The first 8 digits identify the bank, and the rest 16 or 8 digits are created by the bank to identify the customer.

To prevent errors, a correct bank account number must satisfy the following rule (*checksum*): if the digits are multiplied by $1, 3, 7, 9, 1, 3, 7, 9, \ldots$ respectively, then the sum of these products must be a multiple of 10. (In fact, this must also be true independently for the first 8 digits and the rest 16 or 8 digits, but we ignore this here.)

Denote the digits of the bank account number by b_i (from b_1 to b_{24}, filling it with zeros at the end if it has only 16 digits), and the check digits by c_i ($c_1 = 1$, $c_2 = 3$, $c_3 = 7$, $c_4 = 9$, …, $c_{24} = 9$). Then the above rule can be expressed by the following congruence:

$$\sum_{i=1}^{24} b_i c_i \equiv 0 \pmod{10}.$$

What does this rule achieve, and why are the check digits 1, 3, 7 and 9? The goal is that if one of the digits is mistyped, then the incorrect account number is detected by the checksum. Let's say that the digit b_j was mistyped as b'_j, then in the above sum, the term $b_j c_j$ is replaced by $b'_j c_j$, so the sum changes by $(b'_j - b_j)c_j$. In order for the incorrect number to pass the test, the change needs to be divisible by 10, i.e. $(b'_j - b_j)c_j \equiv 0 \pmod{10}$. This is a linear congruence with the unknown $x := (b'_j - b_j)$, i.e. $c_j x \equiv 0 \pmod{10}$. A trivial solution is $x = 0$, i.e. that $b'_j = b_j$, meaning that the number is correct. What we need is that $x = 0$ is the *only* one-digit solution. We have seen that for a congruence like this to have a *unique* solution, we need c_j and 10 to be coprime. There are four such c_j numbers: 1, 3, 7 and 9, so the use of these check digits makes sure that all single-digit errors are caught. (Other check digits wouldn't work, e.g. if $c_j = 4$, and a digit 3 were changed to 8, then the sum would change by $(8 - 3) \cdot 4 = 20$, i.e. it wouldn't be detected by the checksum.)

But this method has its limitations too. For example, it cannot detect two or more incorrect digits (only by chance, in 90% of the cases). Also, just from the checksum being incorrect, we don't know which digit is wrong (so this is an *error detection*, but not an *error correction* method). Note: but if we somehow happen to know which digit is wrong, then we can fix it by solving a linear congruence, because the coefficient (1, 3, 7 or 9) makes sure that the solution is unique. This is also used by the bank when creating a new bank account number: they first create the first 23 digits, and then calculate the last digit by solving the congruence.

6 Chinese remainder theorem

Now consider the problem of solving multiple congruences at the same time, with different moduli:

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n}, \end{cases}$$

where $m, n \in \mathbb{N}^+$, $a, b, x \in \mathbb{Z}$, and x is the unknown. This is called a *simultaneous congruence system*. That is, if we know the remainder of x by two different divisors, then how can we find x?

Theorem 6.1 (Chinese remainder theorem (CRT))**.**
The above simultaneous congruence system has a solution if and only if $\gcd(m,n) \mid a-b$*, and the solution is unique modulo* $\operatorname{lcm}(m,n)$ *(i.e. the solutions repeat by* $\operatorname{lcm}(m,n)$*).*

But how can we find a solution?

The above simultaneous congruence system is equivalent to the following two equations (by the definitions of congruence and divisibility – see above at the solution of linear congruences):

$$um = a - x,$$
$$vn = b - x,$$

where $u, v \in \mathbb{Z}$. Subtracting these from each other gives a linear Diophantine equation for u and v:

$$um - vn = a - b,$$

which we already know how to solve. Thus, we can easily prove the above theorem, and derive a formula for x (the derivation is omitted):

Chinese remainder theorem:

Input: $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}^+$, the parameters of the two congruences
$(g, u_g, v_g) :=$ Extended Euclidean algorithm(m, n)
if $g \nmid a - b$ **then** $\rightarrow$ *no solution*
Output: $x \equiv (av_g n + bu_g m)/g \pmod{mn/g}$ (note: $mn/g = \operatorname{lcm}(m,n)$)
(or: $x \equiv a + (b-a)u_g m/g \pmod{mn/g}$)
(or: $x \equiv b + (a-b)v_g n/g \pmod{mn/g}$)

Note: if we know that m and n are coprime, then the calculation is simpler, because we always have a solution, and we don't need to divide by g. And the common modulus is simply mn.

Example 1.

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

The extended Euclidean algorithm (EEA) for 5 and 7 gives $(1, 3, -2)$, i.e. the moduli are coprime. So the system is solvable, and we have $x \equiv 3 \cdot (-2) \cdot 7 + 2 \cdot 3 \cdot 5 \pmod{5 \cdot 7}$, i.e. $x \equiv 23 \pmod{35}$.

Example 2.

$$\begin{cases} x \equiv 1 \pmod 6 \\ x \equiv 3 \pmod 4 \end{cases}$$

The EEA for 6 and 4 gives $(2, 1, -1)$. Since $2 \mid 3 - 1$, the system is solvable, and the solution is $x \equiv (1 \cdot (-1) \cdot 4 + 3 \cdot 1 \cdot 6)/2 \pmod{6 \cdot 4/2}$, i.e. $x \equiv 7 \pmod{12}$.

Example 3.

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 3 \pmod 4 \end{cases}$$

We start similarly as above, but now $2 \nmid 3 - 2$, so there is no solution. Which is not a surprise if we notice that the first congruence implies that x is even, but the second one implies that it is odd.

The Chinese remainder theorem can be extended to more than two congruences. They can be solved by repeatedly applying the above method for two congruences: first solve only two of the congruences, and replace them in the original system by their result as a new congruence. This

reduces the number of congruences by one, and it can be repeated until only one congruence remains, and then that is the solution. If, at any point, the current two congruences have no common solution, then the whole simultaneous congruence system has no solution either.

Let's see an example: the ancient Chinese mathematician Sunzi (from whom the theorem got its name), posed the following problem:

> *"There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?"*

Writing this as a simultaneous congruence system, we get:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7. \end{cases}$$

First solve two of these congruences. We have already solved the last two (see Example 1. above): $x \equiv 23 \pmod{35}$. Writing this into the above system:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 23 \pmod{35}. \end{cases}$$

Solving this, the EEA for 3 and 35 gives $(1, 12, -1)$, and the solution can be calculated from the above formula: $x \equiv 2 \cdot (-1) \cdot 35 + 23 \cdot 12 \cdot 3 \equiv 23 \pmod{105}$.

Sage implements the chinese remainder theorem by the `crt()` function. For two congruences, the four parameters can be given as `crt(a, b, m, n)`, otherwise it expects two lists, one for the right-hand side constants and one for the moduli: `crt([a, b, ...], [m, n, ...])`. In both cases, it returns the smallest nonnegative solution (it doesn't give the common modulus). For example:

```
sage: crt(1,3, 6,4)     # Example 2. above
7
sage: crt(2,3, 6,4)     # Example 3. above
[...]
ValueError: no solution to crt problem since gcd(6,4) does not divide 2-3
sage: crt([2,3,2], [3,5,7])   # Sunzi's problem
23
```

7 Author

This document was written by Uray M. János, partly using the following sources:

[1] https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa (Hungarian)

[2] https://en.wikipedia.org/wiki/Modular_arithmetic

[3] https://en.wikipedia.org/wiki/Chinese_remainder_theorem

Errors and suggestions can be reported here: uray.janos@inf.elte.hu.