Modular arithmetic

Number theory

Application of discrete models

1 Residue classes

Definition 1.1. $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ are *congruent modulo* $m \in \mathbb{N}^+$ if $m \mid a - b$.
Notation: $a \equiv b \pmod{m}$, or simply $a \equiv b\ (m)$. Notation of negation: $a \not\equiv b \pmod{m}$.
Further names: m is the *modulus*, and the statement $a \equiv b \pmod{m}$ is a *congruence*.
For example, $34 \equiv 14 \pmod{10}$, because $10 \mid 34 - 14$. We can guess from this that $a \equiv b \pmod{10}$ if and only if the last digit of a and b are the same (at least if $a, b \in \mathbb{N}$). In general, it can be shown that $a \equiv b \pmod{m}$ if and only if the remainder of a and b by m are equal, i.e. $a \bmod m = b \bmod m$. (Note: "mod" has two 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" (congruence), as defined above.)
The congruence relation ($\equiv$) has the following properties (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: $\forall a, b, c \in \mathbb{Z} : a \equiv b\ (m) \wedge b \equiv c\ (m) \implies a \equiv c\ (m)$.

By the above three properties, the congruence relation is an *equivalence relation* (see e.g. Discrete mathematics I). We know that every equivalence relation defines a partition of the base set. The equivalence classes of $\mathbb{Z}$ defined by the congruence relation $a \equiv b \pmod{m}$ are the following:

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

It can be seen that exactly those numbers are in the same class that have the same remainder when divided by m. For example for $m = 5$, the classes 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 1.2. The equivalence classes defined by a congruence relation are called *congruence class*es or *residue class*es. Notation: $\overline{a}$ is the residue class that contains a. (If the modulus m is not implied from the context, then the notation is $\overline{a}_m$.)

For example, for $m = 5$, the residue class $\overline{3} = \{5k + 3 \mid k \in \mathbb{Z}\}$. The definition of $\overline{a}$ is valid because each $a \in \mathbb{Z}$ is in exactly one residue class. But the notation is not unique, for example $\overline{3} = \overline{8} = \overline{28} = \overline{-2}$.

Definition 1.3. $\mathbb{Z}_m$ is the set of all residue classes modulo m, i.e. $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

(Warning: $\mathbb{Z}_m \not\subseteq \mathbb{Z}$, and the elements of $\mathbb{Z}_m$ are not numbers, but sets (residue classes). So for example $\overline{2} \neq 2$, but $2 \in \overline{2}$. This distinction will be important for the arithmetic operations.)

We can refer to residue classes uniquely by fixing one element in each class, and using only that element for reference. So we need the following:

Definition 1.4. A set of integers that contains exactly one element from each residue class modulo m is called a *complete residue system modulo m*.

There are infinitely many complete residue systems for any m. For example, for $m = 5$, all these sets are complete residue systems: $\{0, 1, 2, 3, 4\}$, $\{1, 2, 3, 4, 5\}$, $\{-2, -1, 0, 1, 2\}$, $\{10, 6, -3, 23, -6\}$ etc. Any complete residue system modulo m contains exactly m elements. One of the most common complete residue system is: $\{0, 1, 2, \ldots, m-1\}$.

2 Modular arithmetic

There are many kinds of calculations with numbers where we are only really interested in the remainder of the result (for a certain divisor m). For example if it's currently 18 o'clock, then 10 hours later it will not be 28 o'clock, but $28 \bmod 24 = 4$ o'clock.

This can be formalized by calculating with residue classes. But how can we do arithmetic with sets? First, let's see addition: the sum of two sets can be calculated by adding all elements of one set to all elements of the other set, and putting the result into a set. E.g. if $A = \{3, 5\}$ and $B = \{10, 20\}$, then $A + B = \{13, 15, 23, 25\}$. It can be proven that if we add two residue classes, then the result will also be a residue class. For example: $\{24k + 18 \mid k \in \mathbb{Z}\} + \{24k + 10 \mid k \in \mathbb{Z}\} = \{24k + 4 \mid k \in \mathbb{Z}\}$ (i.e. $\overline{18} + \overline{10} = \overline{4}$, where $m = 24$). The same is true for subtraction and multiplication, i.e.:

Theorem 2.1. $\forall m \in \mathbb{N}^+, a, b \in \mathbb{Z}$:

1. $\overline{a} + \overline{b} = \overline{a + b}$,
2. $\overline{a} - \overline{b} = \overline{a - b}$,
3. $\overline{a} \cdot \overline{b} = \overline{ab}$,
4. $-\overline{a} = \overline{-a}$.

For example, if $m = 10$, then $\overline{7} + \overline{3} \cdot \overline{6} = \overline{7} + \overline{8} = \overline{5}$. The same can be calculated using numbers (as opposed to residue classes), by taking the remainder after each step: $(7 + 3 \cdot 6) \bmod 10 = (7 + (3 \cdot 6 \bmod 10)) \bmod 10 = (7 + 8) \bmod 10 = 5$. Or we could take the remainder only at the end, but the former method has the advantage that the intermediate results are smaller.

The main properties of the operations in $\mathbb{Z}_m$ (like in $\mathbb{Z}$):

1. commutativity (+ and $\cdot$): $\forall \overline{a}, \overline{b} \in \mathbb{Z}_m : \overline{a} + \overline{b} = \overline{b} + \overline{a} \ \wedge \ \overline{a}\overline{b} = \overline{b}\overline{a}$;
2. associativity (+ and $\cdot$): $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m : \overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c} \ \wedge \ \overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}$;
3. distributivity (of $\cdot$ over +): $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m : \overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{a}\overline{c}$;
4. zero: $\forall \overline{a} \in \mathbb{Z}_m : \overline{a} + \overline{0} = \overline{a} \ \wedge \ \overline{a} \cdot \overline{0} = \overline{0}$;
5. one: $\forall \overline{a} \in \mathbb{Z}_m : \overline{a} \cdot \overline{1} = \overline{a}$;
6. opposite: $\forall \overline{a} \in \mathbb{Z}_m : \overline{a} + \overline{-a} = \overline{0}$.

In Sage, there are multiple ways to calculate modularly. We can take remainders manually:

```
sage: (7 + (3*6)%10) % 10
5
```

Or we can use the $\mathbb{Z}_m$ structure, which is called `Zmod(m)` in Sage:

```
sage: Zmod(10)
Ring of integers modulo 10
sage: Z10 = Zmod(10)
sage: Z10(3)       # convert the integer "3" to the residue class of 3
3
sage: Z10(3) * 6   # "6" is converted automatically
8
sage: 7 + Z10(3) * 6
5
sage: type(Z10(3))
<class 'sage.rings.finite_rings.integer_mod.IntegerMod_int'>
sage: type(3)
<class 'sage.rings.integer.Integer'>
```

The elements of $\mathbb{Z}_m$ can be enumerated in the usual way:

```
sage: for a in Zmod(4):
....:     print(a, a^2)
0 0
1 1
2 0
3 1
```

Another way to create a residue class is the `mod(a, m)` function, which can do so without creating $\mathbb{Z}_m$ first. It does the same calculation as `a % m`, but its result is not an integer, but the residue class:

```
sage: mod(34, 10)
4
sage: _ ^ 2
6
sage: type(mod(34, 10))
<class 'sage.rings.finite_rings.integer_mod.IntegerMod_int'>
sage: type(34 % 10)
<class 'sage.rings.integer.Integer'>
```

3 Linear congruences

An important operation is still missing: the division. Can we divide in $\mathbb{Z}_m$, and if so, how?
Naively, one could think that we can do division in the same way as addition, subtraction and multiplication (as discussed above), e.g. for $m = 10$, we would have $\overline{6}/\overline{2} = \overline{3}$, and $\overline{8}/\overline{3}$ would not exist. But this is not so simple. In fact, both statements are false!

Instead, first let's see what divison means elsewhere, e.g. in $\mathbb{Z}$: division is the inverse of multiplication, i.e. if $a, b \in \mathbb{Z}$, then b/a is the unique $x \in \mathbb{Z}$ number for which $ax = b$. For example:

- $6/2 = 3$, because $2 \cdot 3 = 6$, and $x = 3$ is the only such number;
- $8/3$ doesn't exist in $\mathbb{Z}$, because there is no $x \in \mathbb{Z}$ for which $3x = 8$ (but it does exist in $\mathbb{Q}$);
- $5/0$ doesn't exist either, because $0x = 0 \neq 5$;
- neither does $0/0$, but for a different reason: there exists x such that $0x = 0$, but it is not unique (in fact, all x works).

Apply this approach of division for $\mathbb{Z}_m$:

Definition 3.1. For $\overline{a}, \overline{b} \in \mathbb{Z}_m$, $\overline{b}/\overline{a}$ is the unique $\overline{x} \in \mathbb{Z}_m$ for which $\overline{a}\overline{x} = \overline{b}$.

For example, let's see the following multiplication table for $m = 10$ (the first row contains the elements, x, the second row $2x$, and the third row $3x$):

```
sage: matrix([[b*x for x in Zmod(10)] for b in Zmod(10) if b >= 1 and b <= 3])
[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]
```

From this, we can see that:

- the equation $\overline{3}\overline{x} = \overline{8}$ has exactly one solution (the third row contains exactly one 8): $\overline{3} \cdot \overline{6} = \overline{8}$, i.e. $\overline{8}/\overline{3} = \overline{6}$ (this result might be surprising from $\mathbb{Z}$'s perspective);
- furthermore, any $\overline{b}/\overline{3}$ exists, since the third row contains each element exactly once;
- the equation $\overline{2}\overline{x} = \overline{6}$ however has *two* solutions: $\overline{2} \cdot \overline{3} = \overline{6}$ (this was expected) and $\overline{2} \cdot \overline{8} = \overline{6}$, so $\overline{6}/\overline{2}$ doesn't exist modulo 10!

But how can we perform division efficiently, without a table (i.e. without trying out m elements)? First, write the equation $\overline{a}\overline{x} = \overline{b}$ (from the division's definition) as a congruence: $ax \equiv b \pmod{m}$, and try to solve that first.

Definition 3.2. A congruence of the form $ax \equiv b \pmod{m}$, where x is the unknown, is called a *linear congruence.*

From the definition of the congruence, $ax \equiv b \pmod{m}$ is equivalent to $m \mid b - ax$, which means (from the divisor's definition) that $\exists y \in \mathbb{Z} : my = b - ax$, or equivalently: $ax + my = b$. This is a linear Diophantine equation, which we already know how to solve (see the previous topic: Greatest common divisor). Note that we only need to find x. 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, and they can be written as $x = x_0 - k \cdot m/\gcd(a, m)$, where k is an arbitrary integer. But for our congruence, it's enough to find solutions in $x \in \{0, 1, \ldots, m-1\}$, where there are only finitely many. But how many exactly? We can calculate this from the distance between adjacent solutions, which is $m/\gcd(a, m)$, so there are exactly $\gcd(a, m)$ solutions between 0 and $m-1$.

So the congruence $ax \equiv b \pmod{m}$ can be solved as follows:

1. Using the extended Euclidean algorithm (EEA), calculate $g := \gcd(a, m)$ and the corresponding x_0, y_0 Bézout coefficients (or in this case, y_0 is not necessary).
2. If $\gcd(a, m) \nmid b$, then there is no solution.
3. Otherwise, there are exactly $\gcd(a, m)$ solutions between 0 and $m-1$:
   (a) The first solution is $x_0 \cdot b/g \bmod m/g$.
   (b) Each subsequent solution is m/g more than the previous one.

For example for $2x \equiv 6 \pmod{10}$, we have $g = \gcd(2, 10) = 2$, and the Bézout coefficient is $x_0 = 1$ (and $y_0 = 0$). Since $\gcd(2, 10) \mid 6$, 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).

Now return to the division $\overline{b}/\overline{a}$. This is different from solving the corresponding congruence in that for division, the solution must be unique. This means the following:

Theorem 3.3. *The quotient $\overline{b}/\overline{a}$ (modulo m) exists if and only if a and m are coprime (i.e. $\gcd(a, m) = 1$).*

So $\overline{b}/\overline{a}$ can be calculated as follows:

1. Using EEA, calculate $\gcd(a, m)$ and the Bézout coefficient x_0 for a.
2. If $\gcd(a, m) \neq 1$, then there is no solution.
3. Otherwise the solution is $x_0 \cdot b \bmod m$.

For example, for $\overline{8}/\overline{3}$ (modulo 10), $\gcd(3, 10) = 1$ and $x_0 = -3$, so there is a solution: $\overline{x} = \overline{-3} \cdot \overline{8} = \overline{6}$.

Division has a useful special case when $\overline{b} = \overline{1}$:

Definition 3.4. The *multiplicative inverse* of the element $\overline{a}$ (modulo m) is $\overline{1}/\overline{a}$. Notation: $\overline{a}^{-1}$. If it exists, then we say that $\overline{a}$ is *invertible*.

This is useful because if we need to calculate many divisions by the same divisor, then it's enough to calculate $\overline{a}^{-1}$ once:

Theorem 3.5. *$\overline{b}/\overline{a}$ exists if and only if $\overline{a}$ is invertible, and then $\overline{b}/\overline{a} = \overline{b} \cdot \overline{a}^{-1}$.*

As we discussed above, exactly those elements are invertible that are coprime with m. For some m, this makes the situation trivial:

Theorem 3.6. *If m is prime, then all $\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ elements are invertible.*

This means that for a prime modulus, we can divide by any element except $\overline{0}$ (just like e.g. in $\mathbb{Q}$).

Of course, Sage can calculate all of this:

```
sage: Z10 = Zmod(10)
sage: Z10(8) / 3
6
sage: Z10(6) / 2
...
ZeroDivisionError: inverse of Mod(2, 10) does not exist
sage: Z10(3).inverse()
7
sage: _ * 3
1
```

Congruences can be solved by `solve_mod()`:

```
sage: solve_mod(2*x == 6, 10)
[(8,), (3,)]
sage: (_[0][0] * 2, _[1][0] * 2)
(6, 6)
```

4 Chinese remainder theorem (CRT)

Finally, let's see how we can solve multiple congruences with different moduli at the same time ("moduli" = plural of "modulus"):

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

where $m, n \in \mathbb{N}^+$, $a, b, x \in \mathbb{Z}$, and x is the unknown. This is called a *simultaneous congruence system.*

Theorem 4.1 (Chinese remainder theorem)**.** *The above simultaneous congruence system has a solution if and only if* $\gcd(m,n) \mid b-a$*, and it is unique modulo* $\operatorname{lcm}(m,n)$ *(i.e. the set of solutions is exactly a residue class modulo* $\operatorname{lcm}(m,n)$*).*

But we still don't know how the calculate a solution.

The above simultaneous congruence system is equivalent to the following two equations (by the definitions of congruence and divisibility):

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

where $u, v \in \mathbb{Z}$. By cancelling x, we get a linear Diophantine equation for u and v:

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

which we already know how to solve. By this, we can easily prove the above theorem, and derive a formula for x (we omit the derivation).

The solution of the above system is as follows:

1. Using EEA, calculate $g := \gcd(m,n)$ and the Bézout coefficients u_0 and v_0.
2. If $g \nmid b-a$, then there is no solution.
3. Otherwise, the solution is: $x \equiv (av_0n + bu_0m)/g \pmod{mn/g}$. (Note: $mn/g = \operatorname{lcm}(m,n)$.)

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

First example:

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

EEA for 5 and 7 gives $(1, 3, -2)$, i.e. the moduli are coprime. Then we always have a solution, and here $x \equiv 3 \cdot (-2) \cdot 7 + 2 \cdot 3 \cdot 5 \pmod{5 \cdot 7}$, i.e. $x \equiv 23 \pmod{35}$.

Second example:

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

EEA for 6 and 4 gives $(2, 1, -1)$. Since $2 \mid 3-1$, we have a solution, namely: $x \equiv (1\cdot(-1)\cdot 4 + 3\cdot 1\cdot 6)/2 \pmod{6 \cdot 4/2}$, i.e. $x \equiv 7 \pmod{12}$.

Third example:

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

The moduli are the same as in the previous one, but now $2 \nmid 3-2$, so there is no solution. But we can know this by just looking at them, since the two congruences are contradictory: from the first one, x must be even, but from the second one, it must be odd.

The Chinese remainder theorem can stated not just for two, but for any number of 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, which is the solution. If, at any point, the current two congruences have no common solution, then the whole simultaneous congruence system has no solutions.

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?"

We can write this as a simultaneous congruence system:

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

First solve two of these congruences. We have already solved the last two (see the first example above): $x \equiv 23 \pmod{35}$. Write 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: $x \equiv 23 \pmod{105}$.

Sage can solve simultaneous linear congruence systems by the `crt()` function. This can be used in two ways: if there are only two congruences, then the four parameters can be given directly: `crt(a, b, m, n)`, and for any number of congruences, it expects two lists, one for the right-hand side constants of the congruences, and one for the moduli: `crt([a, b, ...], [m, n, ...])`. In both cases, it returns one solution as an integer (it doesn't give the common modulus). For example:

```
sage: crt(1,3, 6,4)   # second example above
7
sage: crt(2,3, 6,4)   # third example 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
```

5 Author

These lecture notes were written by Uray M. János, partially using Nagy Ádám's notes in Hungarian: https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa

Please report errors and suggestions here: uray.janos@inf.elte.hu.