Logic & Set Theory Cheatsheet

3.AB PreIB Math

Adam Klepáč

Natural Numbers

Logic is the language of mathematics. It uses propositions to talk about sets.

Propositions are sentences which can be either true or false. For example

- '**Cats are black.**' is a proposition;
- '**How are you?**' is *not* a proposition;
- '**We will have colonised Mars by 2500.**' is also a proposition.

As the third example suggests, we need not necessarily know whether a proposition is true or false – it remains a proposition anyway.

Whole numbers

Propositions can be joined together using logical conjunctions. They pretty much correspond to the conjunctions of natural language. Let us consider two propositions:

$p =$ 'It's raining outside.'
$q =$ 'I'll stay at home.'

($\wedge$) Logical and forms a proposition that is only true if both of its constituents are also true. In natural language, the proposition $p \wedge q$ can be expressed as

$$p \wedge q = \text{'It's raining outside and I'll stay at home.'}$$

($\vee$) Logical or forms a proposition that is true if at least one of its constituents is true. In natural language, the proposition $p \vee q$ can be expressed as

$$p \vee q = \text{'It's raining outside or I'll stay at home.'}$$

In mathematical logic, or is **not exclusive**! This means that $p \vee q$ is true even if both p and q are true.

($\neg$) Logical not isn't strictly speaking a conjunction but I include it anyway. It reverses the truth value of a proposition. For example, the proposition $\neg p$ can be read as

$$\neg p = \text{'It's not raining outside.'}$$

It follows that $\neg p$ is true exactly when p is false and vice versa.

($\Rightarrow$) Logical implication is a conjunction that makes the first proposition into an *assumption* or *premise* and the second one into a *conclusion*. The proposition $p \Rightarrow q$ is read in multiple ways, to list a few:

$p \Rightarrow q =$ 'If it's raining outside, then I'll stay at home.'
$p \Rightarrow q =$ 'It raining outside implies that I'll stay at home.'
$p \Rightarrow q =$ 'Assuming it's raining outside, I'll stay at home.'

The implication is tricky. It's true if both p and q are true and false if p is true but q is false. However, it is always true if p is false. That is because, in mathematical logic, whatever follows from a lie is automatically true.

($\Leftrightarrow$) Logical equivalence is true only if both propositions have the same truth value – they're both true or both false. In natural language, it is typically read like this:

$$p \Leftrightarrow q = \text{'It's raining if and only if I stay at home.'}$$

Equivalence is basically just a two-way implication. The proposition p is both a premise and a conclusion to q and q is both a premise and a conclusion to p. If it's raining outside, I stay at home and if I stay at home, then it's raining outside.

Rational numbers

Toto je o racionalnich cislech.

Divisibility

A conjunction of propositions being true or false based on whether its constituent propositions are true or false can be summarized using so-called truth table. It is basically just a table that lists all the possibilities of p and q being true or false and the resulting truth value of their conjunctions.

For the basic logical conjunctions from above, it can look like this (we represent true by 1 and false by 0):

p	q	$\neg p$	$\neg q$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
0	0	1	1	0	0	1	1
0	1	1	0	0	1	1	0
1	0	0	1	0	1	0	0
1	1	0	0	1	1	1	1

Prime decomposition

Sets are the 'stuff' that makes up the world of mathematics. Their basic characteristics and properties are described using logic.

Sets cannot be defined inside set theory but we interpret them as *groups of things*.

There's only one foundational *proposition* related to set theory – the proposition 'An object is an element of a set.' If we label the object in question x and the set A, this proposition is written as $x \in A$ (the symbol $\in$ is just the letter 'e' in 'element'). Combining these propositions using logical conjunctions allows for various set-theoretic constructions.

If a set A has, for example, exactly three elements – $\square$, $\triangle$ and $\bigcirc$, I can write it as a list of these three elements inside curly brackets $\{\}$. In this case,

$$A = \{\square, \triangle, \bigcirc\}.$$

A few warnings about sets:

- **Sets are not ordered**. There is nothing like a 'first', 'second' or 'last' element of a set. Either an object **is** inside a set or it **isn't**. Nothing else. For example, the three sets below are exactly the same, only written differently.
$$\{\square, \triangle, \bigcirc\} = \{\bigcirc, \triangle, \square\} = \{\triangle, \square, \bigcirc\}$$
- **Elements of sets have no frequency**. Again, an element either is inside a set or not. It cannot be twice in a set, for example. The three sets below are exactly the same.
$$\{\square, \triangle, \bigcirc\} = \{\square, \triangle, \bigcirc, \triangle, \bigcirc\} = \{\triangle, \square, \square, \triangle, \bigcirc, \triangle\}$$

Euler's algorithm

Congruence

Now that we have defined the remainder after division we want to express the idea that two numbers (x and y) **have the same remainder** (r) **when divided by some** m**.** Mathematically we write this as

$$x \equiv y \pmod{m}.$$

In other words this means

$$x = km + r \qquad \text{and} \qquad y = lm + r$$

for some numbers $l, k \in \mathbb{N}$. This way we can for example say that 13 and 25 are the same modulo 12, because they share the remainder 1 when divided by 12 (formally written as $13 \equiv 25 \pmod{12}$).

This of course implies that each number divisible by m is congruent to 0 $\bmod m$. This makes sense because we said that a divides b only if there is no remainder after the division.

This idea of congruence might sound unintuitive and artificial at first, yet it is all around us. If we for example take the regular old clock. Looking only at the clock and seeing both hands up tells us that it is either noon or midnight. This is because we use the 12 hours format which gives the time $\bmod 12$.

Congruence is very similar to normal equation (it is also equivalence, try to prove it!). Similar to equations we can manipulate it. More specifically if i have $x \equiv y \pmod{m}$ then all the oncoming congruences hold.

- $x + a \equiv y + a \pmod{m}$ - **adding** also works for subtracting so $a \in \mathbb{Z}$
- $x^k \equiv y^k \pmod{m}$ - **exponentiation**
- $cx \equiv cx \pmod{m}$ - **simplification**

for any $k, c \in \mathbb{N}$ and $GCD(m, c) = 1$.

The last operation better be explained by an example. If we take $1 \equiv 6 \pmod{5}$ and multiply it by 2, we get $2 \equiv 12 \bmod 5$. Notice that multiplying the modulus is optional and the congruence holds in both cases (because obviously $2 \equiv 12 \bmod 10$). This is because $GCD(2, 5) = 1$.

An interesting thing to note about the equivalence classes created by some congruence $\bmod m$ is that there will be m of them. This is because all the possible remainders after diving by m are numbers $0, \ldots, m-1$.

Solving congruences

With this we can now attempt to solve the congruence $7x \equiv 5 \pmod{10}$.

If this was just a normal equation how would we solve it? Well we would multiply both sides by such a number that 7 times that number gives us 1 (that would obviously be $1/7$ but we want the idea more then the result). Even though that we are working $\bmod 10$ and cannot use rational numbers, the idea is still useful.

The number that satisfies $7x \equiv 1 \pmod{10}$ is called **inverse** of $7 \bmod 10$. To calculate the **inverse** we try to multiply 7 by increasing integers and see which result is $1 \bmod 10$.

$$2 \cdot 7 \equiv 4 \pmod{10}$$
$$3 \cdot 7 \equiv 1 \pmod{10}$$

This concludes that 3 is the **inverse** to $7 \bmod 10$. Now we multiply the whole equation by 3 and get the final result.

$$21x \equiv x \equiv 15 \equiv 5 \pmod{10}$$

One unfortunate thing about inverses is that they are not guaranteed to exist for every number. If for example we try to find the inverse of $2 \bmod 4$ we have to conclude that there is no such a number. The inverse for a modulo some m (this can be written as: the solution to the congruence $ax \equiv 1 \pmod{m}$) exists **if and only if** a and m are **coprime**.

Now that we can solve an congruence there is nothing stoping us from solving more of them.

Chineese remainder theorem

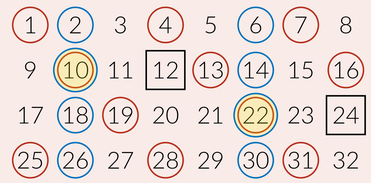
Imagine we have a system of linear congruences:

$$x \equiv r_1 \pmod{m_1}$$
$$x \equiv r_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv r_n \pmod{m_n}$$

Where all the numbers are natural and $m_1, \ldots m_n$ are mutually coprime. Then the CRT tells us that there is unique solution x smaller then the product of all the numbers we divide by $M = m_1 \cdot m_2 \ldots m_n$.

Each congruence limits the possible solutions radically. For example the congruence $x \equiv r \pmod{m}$ has solutions in the form: $km + r$ for any $k \in \mathbb{N}$. To solve the whole system, one can write down all the solutions for all the congruences and then find their intersection.

We can do this process also graphically. If we circle solutions to the individual congruences the number with n circles is the solution to the whole system. If, for example, we have the linear congruences $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, we can draw



Where every circle shows a solution to one of the congruence based on their color. The overall solution has two circles and is tinted yellow. The box around 12 and 24 indicates on what intervals are we guaranteed to have a unique solution. This is because $M = m_1 \cdot m_2 = 3 \cdot 4 = 12$.

To draw all the solution to the congruence $x \equiv r \pmod{m}$ it is useful to note that the first (or the smallest) solution will always be x and then the solutions always jump by m. So the next will be $x+m$, the next will be $x + 2m$ and so on.

From the formulation of CFT we are only guaranteed an unique solution up to M. But the system itself has infinitely many of them in similar to congruences. To find them all we have to start with the smallest solution x (the one smaller then M), then all of them are in the form of $x + kM$ for any $k \in \mathbb{N}$.

Solving congruence systems

Now, to showcase more scalable but less intuitive method, the system

$$x \equiv 3 \pmod{7}$$
$$x \equiv 5 \pmod{9}$$
$$x \equiv 4 \pmod{11}$$

is solved. From the first congruence we know that $x = 7k + 3$ for some $k \in \mathbb{N}$. We can now substitute for x to the second congruence and solve it.

$$7k + 3 \equiv 5 \pmod{9} \quad \text{\# Substituting}$$
$$7k \equiv 2 \pmod{9} \quad \text{\# Subtracting 3}$$
$$k \equiv 8 \pmod{9} \quad \text{\# Multiplying by inverse of 7 mod 9 which is 4.}$$

Now we know that $k = 9l + 8$ for some $l \in \mathbb{N}$. This expression is now used to express x in terms of l as $x = 7(9l + 8) + 3 = 63l + 59$. There is still one equation that we have not used. Substituting to the last congruence gives us.

$$8l + 4 \equiv 4 \pmod{11} \quad \text{\# Substituting}$$
$$l \equiv 0 \pmod{11}$$

With this we can express l in terms of some other constant and finally see the answer

$$x = 210m + 59.$$

Notice how the coefficient before m is the same $7 \cdot 9 \cdot 11$. The CRT tell us that this will be the case for every system where the module are coprime.