Number Theory Cheatsheet

3.AB PreIB Math

Adam Klepáč and Jáchym Löwenhöffer

Natural Numbers

Natural numbers (denoted $\mathbb{N}$) are defined basically as 'sets containing so many elements'. This means that the number 0 is a set with no elements, 1 is a set with one element and so on. Formally, we construct them in the following way ($\emptyset$ is the empty set):

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} &&= \{\emptyset\} \\ 2 &= \{0,1\} &&= \{\emptyset, \{\emptyset\}\} \\ 3 &= \{0,1,2\} &&= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\ &\vdots \end{aligned}$$

In general, the next natural number after a number n is defined as the set $\{0, \ldots, n\}$.

Observe that we can find a formula for the next number after n. Since $n = \{0, \ldots, n-1\}$ and the next number is $\{0, \ldots, n\}$, we can construct the next number after n as a union of two sets: $n \cup \{n\}$. We call this number, the successor of n, and write it as $\mathrm{succ}(n)$. For example, $1 = \{0\} = 0 \cup \{0\} = \mathrm{succ}(0)$ or $3 = \{0,1,2\} = \{0,1\} \cup \{2\} = 2 \cup \{2\} = \mathrm{succ}(2)$.

Addition of natural numbers (not examined)

We can define the operation of addition on natural numbers using two simple rules. For two natural numbers $n, m \in \mathbb{N}$,

(1) $n + 1 = \mathrm{succ}(n)$,
(2) $\mathrm{succ}(n+m) = n + \mathrm{succ}(m)$.

Rule (1) simply states that $n+1$ is the next number after n. Rule (2) is harder to decode. It literally says that by adding the two numbers together and then taking the next number one reaches the same answer as by first taking the next number and then performing addition. It's visualised on the picture below.

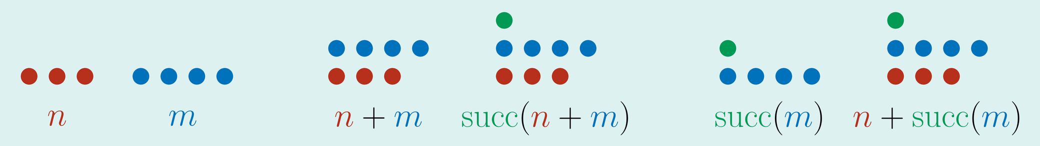


Figure 1. Visualisation of rule (2) of addition. Both $\mathrm{succ}(n+m)$ and $n+\mathrm{succ}(m)$ feature the same number of dots.

Rules (1) and (2) combine to give a simple algorithm of computing the sum $n+m$ for any two numbers $n, m \in \mathbb{N}$. It goes like this:

- Using rule (1), calculate $n + 1 = \mathrm{succ}(n) = n \cup \{n\}$.
- Now that we have calculated $n+1$, we can calculate $n+2$ because $n + 2 = n + \mathrm{succ}(1)$ and by rule (2) this equals $n + \mathrm{succ}(1) = \mathrm{succ}(n+1)$, so just take the next number after $n+1$.
- Continue like this until you calculate $n + m = n + \mathrm{succ}(m-1)$.

For example, to compute $4+2$, we calculate $4+1 = \mathrm{succ}(4)$ and then $4+2 = 4+\mathrm{succ}(1) = \mathrm{succ}(4+1) = \mathrm{succ}(\mathrm{succ}(4))$ so $4+2$ is just the next number after the next number after 4.

Integers (Whole Numbers)

We have defined addition on natural numbers, but in order to perform subtraction, we must move to a 'larger' set of numbers – the integers. This is because subtraction is **not** an operation on natural numbers as its result needn't be a natural number itself.

The idea behind the definition of integers (labelled $\mathbb{Z}$) is to take pairs of natural numbers. Fundamentally, we want the pair $(a,b) \in \mathbb{N} \times \mathbb{N}$ to represent the result of the operation '$a - b$' (which we can't yet perform because we need to define the integers **before** defining subtraction).

To this end, we define an equivalence on $\mathbb{N} \times \mathbb{N}$ (i.e. on pairs of natural numbers) that makes two pairs equivalent if they represent the same integer. For example, the pair $(4,6)$ should represent the number -2 (as $4 - 6 = -2$) and so should the pairs $(8,10)$, $(3,5)$ or just about any pair $(a, a+2)$ for $a \in \mathbb{N}$. The integers will then be the classes of equivalence of this equivalence relation.

We label this equivalence by the letter E. Since we want (a,b) to be equivalent to (c,d) if '$a-b = c-d$' but we can't use subtraction yet, we simply rewrite the equation above to use only addition, like this: $a + d = c + b$. Thus, we say that $(a,b)E(c,d)$ if $a + d = c + b$. This defines an equivalence on $\mathbb{N} \times \mathbb{N}$ and we let $\mathbb{Z}$ be the classes of equivalence of all pairs of natural numbers:

$$\mathbb{Z} = \{[(a,b)]_E \mid a, b \in \mathbb{N}\}.$$

To give an example, the pair $(3,5)$ is equivalent to $(7,9)$ because $3+9 = 7+5$ and they both represent the integer -2. Similarly, both $(6,2)$ and $(8,4)$ represent the integer 4. The visualisation of integers as pairs of natural numbers is given below.

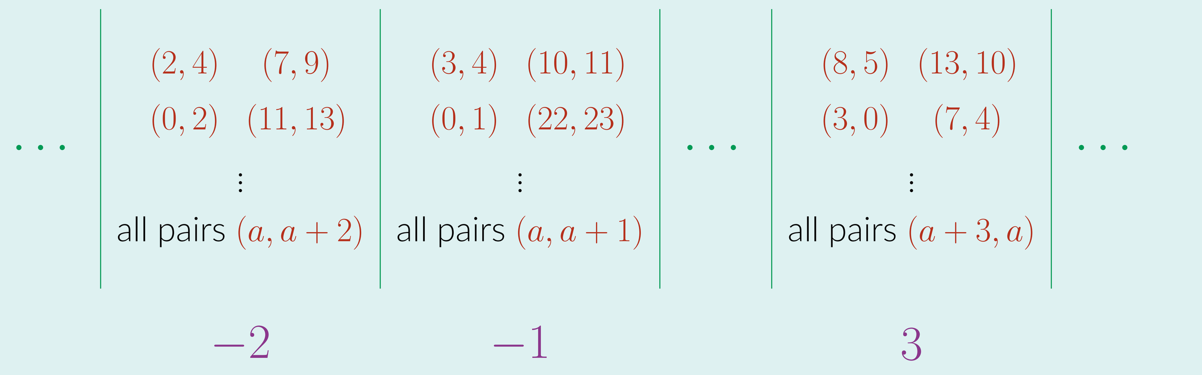


Figure 2. Integers as classes of equivalence of natural numbers.

The addition of integers is defined using the addition of natural numbers. Given two classes of equivalence $[(a,b)]_E, [(c,d)]_E \in \mathbb{Z}$, we let

$$[(a,b)]_E + [(c,d)]_E = [(a+c, b+d)]_E.$$

Finally, we define the opposite number to $[(a,b)]_E$ as $-[(a,b)]_E = [(b,a)]_E$ (this is because $-(a-b) = b - a$). The subtraction of two integers is now just a sum of the first and the opposite of the second, that is

$$[(a,b)]_E - [(c,d)]_E = [(a,b)]_E + (-[(c,d)]_E) = [(a,b)]_E + [(d,c)]_E = [(a+d, b+c)]_E.$$

For example,

$$[(3,1)]_E - [(5,2)]_E = [(3,1)]_E + [(2,5)]_E = [(3+2, 1+5)]_E = [(5,6)]_E,$$

which is the same as writing

$$2 - 3 = 2 + (-3) = -1.$$

Multiplication

In a way similar to addition, we can define multiplication on natural numbers by the following two rules.

(1) $n \cdot 1 = n$,
(2) $n \cdot \mathrm{succ}(m) = n \cdot m + m$,

for $n, m \in \mathbb{N}$. They carry the idea behind an algorithmic way to compute the product $n \cdot m$ for any two natural numbers n, m. It goes like this:

- Using rule (1), calculate $n \cdot 1 = n$.
- Using rule (2), calculate $n \cdot 2 = n \cdot \mathrm{succ}(1) = n \cdot 1 + n = n + n$.
- Continue like this until you calculate

$$n \cdot m = n \cdot \mathrm{succ}(m-1) = n \cdot (m-1) + n = \underbrace{n + n + \ldots + n}_{(m-1)\text{ times}} + n.$$

For example, to calculate $4 \cdot 3$, we first multiply $4 \cdot 1 = 4$, then $4 \cdot 2 = 4 \cdot \mathrm{succ}(1) = 4 \cdot 1 + 4 = 4 + 4$, and finally $4 \cdot 3 = 4 \cdot \mathrm{succ}(2) = 4 \cdot 2 + 4 = (4+4) + 4$. As you've been taught: 'multiplication is just repeated addition'.

Multiplication is easily extended to integers by the formula

$$[(a,b)]_E \cdot [(c,d)]_E = [(a \cdot c + b \cdot d, b \cdot c + a \cdot d)]_E.$$

The formula is based on the calculation

$$(a - b) \cdot (c - d) = a \cdot c - b \cdot c - a \cdot d + b \cdot d = (a \cdot c + b \cdot d) - (b \cdot c + a \cdot d).$$

For example,

$$[(5,3)]_E \cdot [(1,5)]_E = [(5 \cdot 1 + 3 \cdot 5, 3 \cdot 1 + 5 \cdot 5)]_E = [(20, 28)]_E.$$

This is the same calculation as

$$2 \cdot (-4) = -8.$$

Rational Numbers

Being able to multiply integers, we'd like to divide them as well. As was the case with natural numbers and subtraction, division is not an operation on integers because its result needn't be an integer.

The idea behind the definition of rational numbers (labelled $\mathbb{Q}$) is pretty much the same as the one behind the definition of integers – rational numbers are really just pairs of integers. And again, multiple pairs of integers represent the same rational number. Therefore, given pairs (a,b) and (c,d) with $a, b, c, d \in \mathbb{Z}$, we must make sure that (a,b) is equivalent to (c,d) if 'the fraction a/b is the same as the fraction c/d'.

As we couldn't have defined division yet, we must rewrite the last equation in terms of multiplication only. This is easy to do because $a/b = c/d$ if $a \cdot d = c \cdot b$. This directly leads to the definition of an equivalence Q on pairs of integers: $(a,b)Q(c,d)$ if

$$a \cdot d = c \cdot b.$$

This is indeed an equivalence on $\mathbb{Z} \times \mathbb{Z}$ and we define $\mathbb{Q}$ as

$$\mathbb{Q} = \{[(a,b)]_Q \mid a, b \in \mathbb{Z}\}.$$

We tend to write elements of $\mathbb{Q}$ as **fractions**, that is, instead of $[(a,b)]_Q$, we write a/b. We shall adopt this notation henceforth.

It only remains to extend addition and multiplication to rational numbers. This is easily done using formulae you already know. For example, the product of two rational numbers $a/b, c/d \in \mathbb{Q}$ is defined as such:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

The sum of rational numbers as

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}.$$

For example,

$$\frac{2}{5} \cdot \frac{3}{4} = \frac{2 \cdot 3}{5 \cdot 4} = \frac{6}{20} \quad \text{and} \quad \frac{2}{5} + \frac{3}{4} = \frac{2 \cdot 4 + 3 \cdot 5}{5 \cdot 4} = \frac{23}{20}.$$

Finally, we're ready to define division on rational numbers. We first define the inverse of a rational numbers a/b as b/a. We write $b/a = (a/b)^{-1}$. The operation of division on rational numbers is defined as multiplication by the inverse element, that is

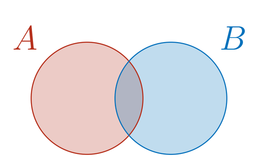
$$\frac{a}{b} : \frac{c}{d} = \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1} = \frac{a}{b} \cdot \frac{d}{c} = \frac{a \cdot d}{b \cdot c}.$$

For example,

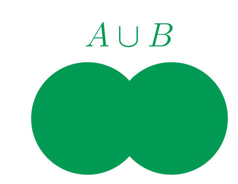
$$\frac{2}{5} : \frac{3}{4} = \frac{2}{5} \cdot \left(\frac{3}{4}\right)^{-1} = \frac{2}{5} \cdot \frac{4}{3} = \frac{2 \cdot 4}{5 \cdot 3} = \frac{8}{15}.$$

Drawing Sets

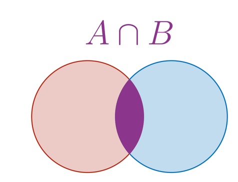
Set operations can be visualized using so-called *Venn diagrams*. This just means using circles to represent the sets in questions. For example, two sets – A and B – can be drawn like this:



In these pictures, one can easily visualize the operations of union and intersection. The union $A \cup B$ is the entire area covered by A and B. It looks like this:



The intersection $A \cap B$ is the 'strip' in the middle, the area which is shared between both A and B. It can be depicted like this:



Products of Sets & Relations

Before introducing *products* of sets, we must define a *pair*. Simply said, a pair of objects (a,b) is just a set containing a and b **with ordering**, that is, a is the **first** element of (a,b) and b is **second**. This means that $(a,b) \neq (b,a)$ because the order is not the same.

Now, the product of sets A and B, denoted $A \times B$, is the set of all pairs (a,b) where $a \in A$ and $b \in B$. For example, if

$$A = \{\bigcirc, \triangle\} \quad \text{and} \quad B = \{\triangle, \times, \sim\},$$

then

$$A \times B = \{(\bigcirc, \triangle), (\bigcirc, \times), (\bigcirc, \sim), (\triangle, \triangle), (\triangle, \times), (\triangle, \sim)\}.$$

Notice that $A \times B \neq B \times A$ because the **order** of elements in a pair **matters**. In this case,

$$B \times A = \{(\triangle, \bigcirc), (\triangle, \triangle), (\times, \bigcirc), (\times, \triangle), (\sim, \bigcirc), (\sim, \triangle)\}.$$

As another example, consider the *real plane* – the set of all points with two coordinates. That is simply the set of pairs of real numbers, $\mathbb{R} \times \mathbb{R}$.

The mathematical way to define a relation between two sets is to simply **list all the elements that are related**. Said formally, a relation R is a subset $R \subseteq A \times B$. For example,

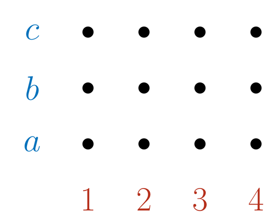
$$\{(\triangle, \times), (\triangle, \sim)\} \subseteq \{\bigcirc, \triangle\} \times \{\triangle, \times, \sim\}$$

is a relation between the sets A and B from above. It literally says that $\triangle$ is related to $\times$ and $\sim$. Instead of writing $(\triangle, \times) \in R$, we write $\triangle R \times$ because it's more natural. Typical examples of relations include $\leq$ and $=$ and we don't write $(2,3) \in \leq$ but $2 \leq 3$.

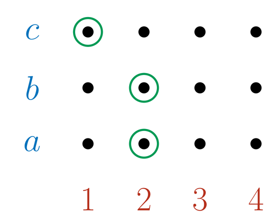
Drawing Products And Relations

One can draw the product $A \times B$ similarly to the way we draw Cartesian coordinates – by distributing the elements of A horizontally and those of B vertically. Each point in the resulting grid represents an element of $A \times B$.

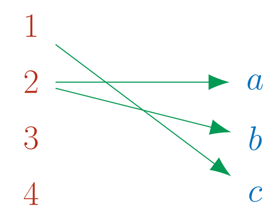
Take, for example, $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. We can depict the set $A \times B$ like this:



Any relation $R \subseteq A \times B$ can now be easily drawn into the grid just by marking certain dots. For example, the relation $R = \{(1,c), (2,b), (2,a)\} \subseteq A \times B$ looks like this:



There is another way to draw relations – as arrows from A to B. This style of drawing emphasises the 'one-way' nature of relations. The same relation $R \subseteq A \times B$ is drawn using arrows like this:



Equivalence & Equivalence Classes

A relation $E \subseteq A \times A$ (do note that it's a relation **on a set**) is called an equivalence if it behaves **something like 'equals'**, that is,

(R) it's reflexive, i.e. aEa for every $a \in A$ (every element is equivalent to itself);
(S) it's symmetric, i.e. if $a_1 E a_2$, then also $a_2 E a_1$ (all elements are **mutually** equivalent);
(T) it's transitive, i.e. if $a_1 E a_2$ and $a_2 E a_3$, then $a_1 E a_3$ (it **propagates** through a middle element).

A good example of equivalence to keep in mind is the relation '**being the same age**' on the set of all people. It's reflexive because I'm as old as me. It's symmetric because if I'm as old as you, then you are as old as me. And finally, it's transitive because if I'm as old as you and you are as old as someone else, then I'm as old as that someone. This example also drives home the idea of equivalence 'being like equals'. It's not that two people of the same age are *equal*, they are *equal by some criterion*. This is exactly what equivalence is, the relation of being equal by some criterion.

With an equivalence $E \subseteq A \times A$, we can divide the set A into 'packets' of elements – each packet consisting of elements which are **equivalent** by E. For example, I can divide the set of all people by putting equally old people to the same packet. Formally, we write

$$[a]_E = \{b \in A \mid aEb\},$$

in other words, $[a]_E$ is the set of all elements from A that are $equivalent$ to a. We call it an equivalence class. The element a is then called a representative.