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.

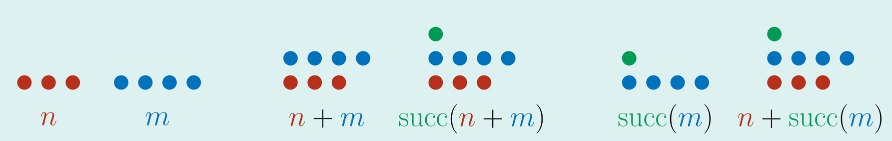


Figure 1. Visualisation of rule (2) of addition. Both $\mathrm{succ}(n+m)$ and $n+\mathrm{succ}(m)$ feature the same number of dots.

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.

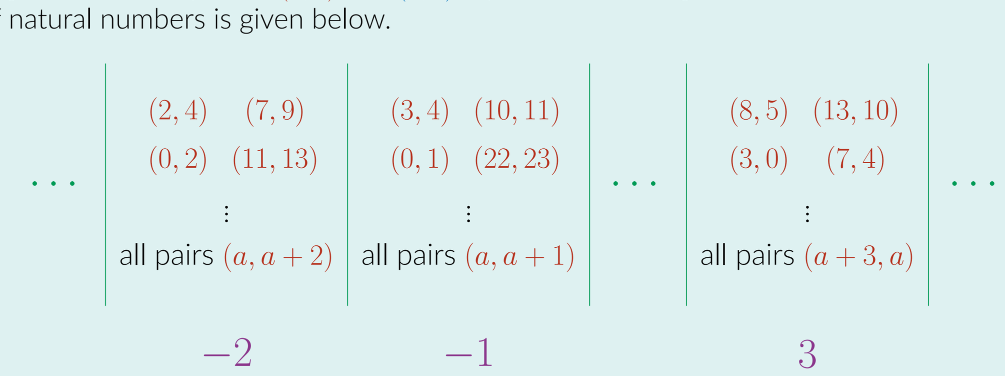


Figure 2. Integers as classes of equivalence of natural numbers.

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,

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

Divisibility

There are two more interesting operations on integers – integer division and modulus. You've learnt about them in elementary school and they are basically 'a way to do division on integers'.

Given two integers: $a, b \in \mathbb{Z}$, we can ask '**How many times does b fit into a?**'. This number is called the quotient (of a by b) and denoted $a \operatorname{div} b$. For example, $7 \operatorname{div} 2 = 3$ because 2 fits 3 times into 7 or $10 \operatorname{div} 8 = 1$ because 8 fits only once into 10. This operation can also be used with integers, for instance $-5 \operatorname{div} 2 = -2$ because 2 'fits' -2 times into -5.

The quantity that is 'left after integer division' is called the remainder and denoted $a \bmod b$. In our first example, $7 \bmod 2 = 1$ because $7 \operatorname{div} 3 = 2$ and $2 \cdot 3 = 6$, so the number 1 is left after performing the division. Similarly, $10 \bmod 8 = 2$ since $10 \operatorname{div} 8 = 1$ and $8 \cdot 1 = 8$ and $10 - 8 = 2$. In the last example, we get $-5 \bmod 2 = -1$ as $-5 \operatorname{div} 2 = -2$ and $2 \cdot (-2) = -4$.

Notice that the remainder must always be smaller (in absolute value) than the divisor because it's the quantity that's left after the divisor no longer fits into the dividend. We may thus formalise the idea of integer division as such: for any two numbers $a, b \in \mathbb{Z}$ there are **unique** numbers $q, r \in \mathbb{Z}$ (called quotient and remainder) such that

$$a = b \cdot q + r$$

and $0 \le |r| < |b|$. We write $q = a \operatorname{div} b$ and $r = a \bmod b$.

The operation of integer division gives birth to the idea of divisibility. We say that a number b divides the number a (and write $b \mid a$) if $a \bmod b = 0$ or, equivalently, $a = b \cdot q$ for some integer $q \in \mathbb{Z}$.

If $b \mid a$, we say that b is a divisor of a. A number that has exactly two divisors (the number 1 and itself) is said to be prime. If two numbers $x, y \in \mathbb{Z}$ share no divisors, they are called *coprime*.

Prime Decomposition

Each integer $a \in \mathbb{Z}$ has a unique prime decomposition, meaning, it can be written as a product of prime numbers.

Expressed formally, for every number $a \in \mathbb{Z}$, we can find **prime** numbers $p_1, \ldots, p_n \in \mathbb{Z}$ and powers $k_1, \ldots, k_n \in \mathbb{N}$ satisfying

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot \ldots \cdot p_n^{k_n}$$

where $n \in \mathbb{N}$ is an adequate natural number.

A very important assumption of modern cryptography is that decomposition into primes is a very slow process for which no fast algorithm is known. This is the basis for several cryptographic methods including the RSA system we shall discuss in class.

Greatest Common Divisor

We ask the question: 'What's the largest number that divides both a and b?' Such number is called the greatest common divisor of a and b and written $\gcd(a,b)$.

There is a nice algorithmic way to compute this number: the algorithm is called Euclid's Algorithm. It uses the following equality: for every two numbers, $a, b \in \mathbb{Z}$, it holds that

$$\gcd(a,b) = \gcd(a \bmod b, b).$$

Since $a \bmod b$ is always smaller than both a and b, we keep taking the remainder after division of the larger number by the smaller until we reach the number 0. Once we do, we have found the greatest common divisor as $\gcd(d,0) = d$ (0 is divided by every number).

Let's showcase the algorithm. Suppose we want to calculate $\gcd(3312, 448)$. We first calculate $3312 \bmod 448 = 176$. Therefore

$$\gcd(3312,448) = \gcd(176,448).$$

Next, we compute $448 \bmod 176 = 96$ and thus

$$\gcd(176,448) = \gcd(176,96).$$

We are almost done. Computing $176 \bmod 96 = 80$ and $96 \bmod 80 = 16$ gives

$$\gcd(176,96) = \gcd(80,96) = \gcd(80,16).$$

Because $80 \bmod 16 = 0$, we have reached the conclusion that $\gcd(3312,448) = 16$.

Congruence

Now that we have defined the remainder after division, we want to express the idea that two integers (say, x and y) have the same remainder (r) when divided by some $m \in \mathbb{Z}$. Mathematically, we write this as

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

In other words, this means

$$x = k \cdot m + r \quad\text{and}\quad y = l \cdot m + r$$

for some numbers $k, l \in \mathbb{Z}$. Said 'naturally', both x and y are greater by r than some multiple of m. For example, 13 and 25 are the same modulo 12 because they share the remainder 1 when divided by 12 (formally written as $13 \equiv 25 \pmod{12}$). So, 13 is greater by 1 than 12 (a multiple of 12) and so is 25 than 24 (also a multiple of 12).

This, of course, implies that a number x is divisible by m if it is congruent to 0 modulo m. This alludes to our previous definition where we said that m divides x only if there is no remainder after the division of x by m.

This idea of congruence might sound unintuitive and artificial at first, yet it is all around us. If we, for example, consider 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-hour format which describes current time modulo 12.

Congruence is very similar to normal equation (it is also an equivalence relation, try to prove it!). We can manipulate it as we would an equation. More specifically, if we know that $x \equiv y \pmod{m}$, then both of the following congruences hold.

- $x + a \equiv y + a \pmod{m}$ – **adding** (also works for subtracting, so $a \in \mathbb{Z}$)
- $c \cdot x \equiv c \cdot y \pmod{m}$ – **multiplying**

for any $c, k \in \mathbb{N}$.

One can also simplify a congruence, but this one is trickier. If

$$n \cdot a \equiv n \cdot b, \quad \pmod{m}$$

then it is also true that $a \equiv b \pmod{m}$ only in the case that n and m are coprime, i.e. $\gcd(m,n) = 1$. Let's make an example: if $35 \equiv 15 \pmod{4}$, then we can 'divide' both sides by 5 and get $7 \equiv 3 \pmod{4}$ because $\gcd(4,5) = 1$. However, $10 \equiv 2 \pmod{8}$ but $5 \not\equiv 1 \pmod{8}$ since we have divided by 4 which is **not** coprime to 8.

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

Solving Congruences

We now attempt to solve the congruence $7 \cdot x \equiv 5 \pmod{10}$. Solving a congruence means a similar thing as solving an equation. We're looking for a number $n \in \mathbb{Z}$ such that $x \equiv n \pmod{10}$.

If this were 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 care about the idea more than about the result). Even though congruence is a relation between integers and we mustn't use rational numbers, the idea is still useful.

The number $n \in \mathbb{Z}$ that satisfies $7 \cdot n \equiv 1 \pmod{10}$ is called inverse of 7 modulo 10. There is no straightforward way to find an inverse. To calculate it, we try multiplying 7 by increasing integers and see which result is 1 modulo 10.

$$\begin{aligned} 2 \cdot 7 &\equiv 4 \pmod{10} \\ 3 \cdot 7 &\equiv 1 \pmod{10} \end{aligned}$$

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

$$\begin{aligned} 7 \cdot x &\equiv 5 &&\pmod{10} \\ 3 \cdot 7 \cdot x &\equiv 3 \cdot 5 &&\pmod{10} \\ 21 \cdot x &\equiv 15 &&\pmod{10} \\ x &\equiv 5 &&\pmod{10} \end{aligned}$$

We got the fourth congruence from the third by calculating $21 \bmod 10 = 1$ and $15 \bmod 10 = 5$.

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 modulo 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 $a \cdot x \equiv 1 \pmod{m}$) exists if and only if a and m are coprime.

Chinese Remainder Theorem

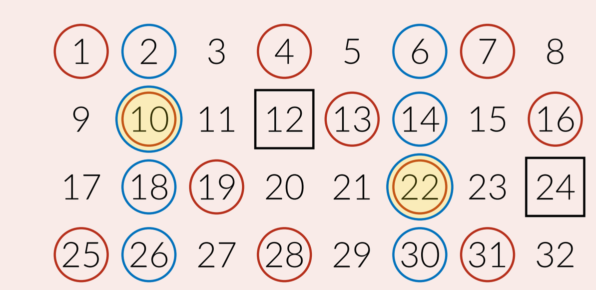
Imagine we have the system of linear congruences

$$\begin{aligned} x &\equiv r_1 &&\pmod{m_1} \\ x &\equiv r_2 &&\pmod{m_2} \\ &\vdots \\ x &\equiv r_n, &&\pmod{m_n} \end{aligned}$$

where all the numbers are natural and $m_1, \ldots, m_n$ are pairwise coprime. Then the Chinese Remainder Theorem tells us that there is unique solution smaller than the product $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ of all the numbers we divide by.

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

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



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

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

By the Chinese Remainder Theorem, we are only guaranteed a unique solution up to M. But the system itself has infinitely many solutions. To find all of them, we have to start with the smallest solution x (the one smaller than M), and then keep adding multiples of M. More precisely, all solutions are of the form $x + k \cdot M$ for any $k \in \mathbb{N}$.

Solving Congruence Systems

Now, to showcase a more scalable but less intuitive method, we shall solve the system

$$\begin{aligned} x &\equiv 3 &&\pmod{7} \\ x &\equiv 5 &&\pmod{9} \\ x &\equiv 4. &&\pmod{11} \end{aligned}$$

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

$$\begin{aligned} 7 \cdot k + 3 &\equiv 5 \pmod{9} && \text{\# Substituting} \\ 7 \cdot k &\equiv 2 \pmod{9} && \text{\# Subtracting 3} \\ k &\equiv 8 \pmod{9} && \text{\# Multiplying by the inverse of 7 modulo 9, which is 4.} \end{aligned}$$

Now we know that $k = 9 \cdot l + 8$ for some $l \in \mathbb{N}$. This expression is now used to express x in terms of l as $x = 7 \cdot (9 \cdot l + 8) + 3 = 63 \cdot l + 59$. There is still one equation that we have not used. We calculate $63 \bmod 11 = 8$ and $59 \bmod 11 = 4$. Hence, $x \equiv 8 \cdot l + 4 \pmod{11}$. Substituting to the last congruence gives us

$$\begin{aligned} 8 \cdot l + 4 &\equiv 4 &&\pmod{11} && \text{\# Substituting} \\ l &\equiv 0. &&\pmod{11} \end{aligned}$$

With this we can express $l = 11 \cdot m$ in terms of some other variable m and finally see the answer

$$x = 63 \cdot (11 \cdot m) + 59 = 693 \cdot l + 59.$$

Notice that the coefficient before m is equal to $693 = 7 \cdot 9 \cdot 11$. The CRT tells us that this will be the case for every system where the divisors are coprime.