Numbers

Math 170: Ideas in Mathematics (Section 001)
University of Pennsylvania. Fall, 2015.
Monday 19th October, 2015

Instructor: Subhrajit Bhattacharya
(email: subhrabh@math.upenn.edu)

The Set of Natural Numbers and the Addition Operation

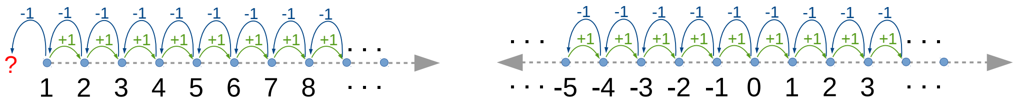
The set of of Natural Numbers, $\mathbb{N}$, by itself, contains the elements $1,2,3,\ldots$. As a set, these elements are nothing more than symbols. But when we define the addition operation (in particular, the operation of adding '1' to any natural number), we establish a relationship between these elements. Thus, $1+1=2$, $2+1=3$, $3+1=4$, and so on. The addition operation is also naturally defined between any two natural numbers: for example, $5+3=8$, can be interpreted as repetition of the operation of '+1' on 5 three times: $5+3=5+(2+1)=5+((1+1)+1)=((5+1)+1)+1$. Thus, the natural number, as we know it, is not just the set $\mathbb{N}$, but the set along with the defined operation '+'. Formally, it is said that the operation of addition, '+', gives the set of natural numbers a *structure*. Thus the natural numbers is really defined by the pair of entities, $(\mathbb{N},+)$.

The operation of subtraction is a natural consequence of the operation of addition: The operation of subtracting '1' from a natural number, n, is defined as the operation that gives answer to the question *"What is the natural number, to which when we add '1', do we get n?"* The operation is written as "$n-1$". In general we have, like for addition, $n-m=((\ldots((n-1)-1)\ldots)-1)$ (where there are m counts of open and close brackets).

Quite obviously subtraction is called the *inverse* of the operation of addition, and they go hand-in-hand. When we refer to the natural numbers $(\mathbb{N},+)$, the existence of the operator '$-$', the inverse of '+', is implied by default.

However, there is an unsettling fact about $(\mathbb{N},+)$: While we can apply the '+1' (and in fact'$+m$') operation on any natural number and get a natural number, we cannot apply its inverse, '-1' (respectively '$-m$'), on any natural number and still get something in the set $\mathbb{N}$ (Figure 1(a)). For example, '-1' operated on $1\in\mathbb{N}$ is not defined within the natural numbers. Likewise, -8 operated on $5\in\mathbb{N}$, *i.e.,* $5-8$, is not defined within the natural numbers.

In a relatively formal language, we say that the natural numbers is *incomplete* with respect to the '+' (addition) operation since the set of natural numbers is *not closed* (*i.e.*, not self-contained) under the inverse of the addition operation, *i.e.,* '$-$'.



(a) $(\mathbb{N},+)$.

(b) $(\mathbb{Z},+)$.

Figure 1: Natural number and integers.

This leads us to construct a set that is complete under addition by introducing the "*missing*" elements into the set of natural numbers, thus giving us the set of integers.

Integers and Modular Arithmetic

The set of integers, $\mathbb{Z}$, contains the natural numbers, as well as the ones that would make the operation of addition, along with subtraction, closed in the set (Figure 1(b)). Thus, $\mathbb{Z} = \{\dots,-3,-2,-1,0,1,2,\dots\}$, along with the addition operation, gives it a structure (establishes relationships between its elements). As before, we write $(\mathbb{Z},+)$ to denote the set along with the addition operation (and its inverse).

A few important properties of $(\mathbb{Z},+)$ (some of which were missing in $(\mathbb{N},+)$) are as follows:

i. There exists an element, $0 \in \mathbb{Z}$, called the *additive identity*, such that for any $a \in \mathbb{Z}$, $a+0 = 0+a = a$ (*existence of identity element*),

ii. For every element $a \in \mathbb{Z}$, there exists an element $-a \in \mathbb{Z}$ (called the *additive inverse of* a) such that $a+(-a) = 0$ (*existence inverse elements*),

iii. For any $a,b \in \mathbb{Z}$, the element $a+b \in \mathbb{Z}$ (*closure under addition*),

The property 'ii.' encodes the operation of subtraction, where instead of talking about inverse of the '$+$' operation, we present the same concept in terms of inverse of the elements themselves. These properties, along with one more (the property that $a+(b+c) = (a+b)+c$, which is called *associativity*), gives $(\mathbb{Z},+)$ a specific type of structure known as a *group*.

One can also define multiplication on the integers using the addition operation quite naturally: $m \times n = m+m+\cdots m$ (n counts of m summed up), for $n,m \in \mathbb{Z}, n \geq 0$. If n is negative, we simply add $-n$ counts of m, and then finally flip the sign of the number. This is how we define multiplication on integers. The definition of *divisibility* in integers is actually given in terms of multiplication (and not division, since we have not yet defined what division is):

> **Divisibility:** An integer $p \in \mathbb{Z}$ is said to be divisible by $n \in \mathbb{Z}$ (or $p \lfloor n$, where the symbol "$\lfloor$" reads out as "*is divisible by*") if there exists a $m \in \mathbb{Z}$ such that $n \times m = p$.
>
> **Summary:** The integers are defined by the pair $(\mathbb{Z}, +)$. $0 \in \mathbb{Z}$ is called the *additive* identity for integers. For every $a \in \mathbb{Z}$, $-a$ is called the *additive inverse* of a such that $a + (-a) = 0$. Multiplication can be defined in terms of a sequence of additions, and divisibility is defined in terms of multiplication.

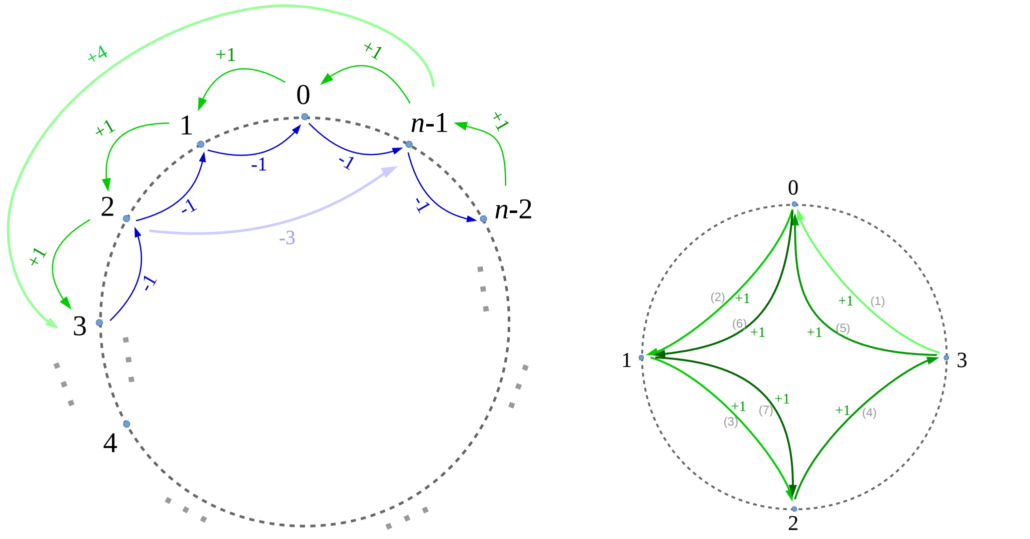
However, there is a different structure that one can impart to a finite set of n elements, $\{0, 1, 2, \cdots, n-1\}$ (the elements of which, once again, as a set, are nothing but n different symbols), such that all the properties of a *group* still hold – thus letting us define addition, additive identity and additive inverse on this finite set. The key difference between this structure and the Natural numbers or the Integers is that instead of arranging the elements on a line, as we did in Figure 1, we arrange them on a circle (Figure 2(a)). Then the operation of '$+1$' is defined to be one that takes us one step counterclockwise to the next number, while its inverse operation, '-1' takes us one step clockwise to the previous number. This system behaves almost like the usual addition and subtraction, except that when we add 1 to $n-1$, we get back to 0, and when we subtract 1 from zero, we get to $n-1$. Operations of '$+m$' or '$-m$', as before, can be considered as m consecutive operations of '$+1$' or '-1' respectively.

This kind of arithmetic is called a *modular arithmetic* (or *clock arithmetic*). The finite set of elements is written as $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$. This set, along with the described addition operation, describes the modular arithmetic (in particular, "mod-n arithmetic"), and is referred to using the pair $(\mathbb{Z}_n, +)$. Note that this operation '$+$' is fundamentally different from the '$+$' operation in integers, $(\mathbb{Z}, +)$. It may have been appropriate to use a different symbol for the addition operator acting on elements of $\mathbb{Z}_n$ (say, '$\oplus$' instead of '$+$), but it's convenient to use the same symbol, '$+$', whenever the context is clear.

As an example, if $n = 4$, then the set of elements in the mod-4 arithmetic is $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ (see Figure 2(b)). In this modular arithmetic, one would have $3 + 1 = 0$. But that equation would look odd and it is not obvious that we mean addition in mod-4 arithmetic. So the usual way of writing equations in a modular arithmetic is as follows:

$$3 + 1 \equiv 0 \pmod 4$$

The " mod 4" in brackets and the equivalent sign (instead of '$=$') indicates that we are doing a modular arithmetic. Likewise, one has $3 + 7 \equiv 2 \pmod 4$, since if one goes 7 steps counterclockwise on the mod-4 system, starting at 3, one gets to 2.



(a) $(\mathbb{Z}_n, +)$.

(b) $(\mathbb{Z}_4, +)$. Note how $3 + 7 \equiv 2 \pmod 4$

Figure 2: Modular arithmetic.

So, in general, how to figure out what is $a+b$ in a mod-n arithmetic? The answer to that lies in the observation that starting at 0 on the circle, we get back to 0 every time we move n steps clockwise or counterclockwise. Thus, if we consider a general integer, say $c \in \mathbb{Z}$, the corresponding number in $\mathbb{Z}_n$ is the remainder that one obtains when c is divided by n. The phrase *"remainder that one obtains when c is divided by n"* is often itself written as "$c \mod n$". Thus, in our previous example, $3+7 = 10 \in \mathbb{Z}$. Thus, to obtain the value of $3+7$, or 10, in mod-4, we compute $10 \mod 4 = 2$ (*i.e.*, the remainder that one obtains when one divides 10 by 4). A few more examples:

i. $98 + 5 \equiv 3 \pmod{100}$

ii. $55 + 41 \equiv 16 \pmod{20}$ [since, $55 + 44 = 96$, and $96 \mod 20 = 16$]

A few important remarks:

1. The following statements are equivalent (saying the same thing in different ways):

$$a \equiv b \pmod n$$

$$a \mod n = b \mod n$$

The first statement is saying that a and b are the same numbers in mod-n arithmetic (*e.g.*, from our previous example $10 \equiv 2 \pmod 4$), while the later is explicitly describing what it means: That is, the remainders that one obtain when one divdes either a or b by n are the same (*e.g.*, in our earlier example, $10 \bmod 4 \ = \ 2 \ = \ 2 \bmod 4$).

2. Due to the *division algorithm*, for any $a, n \in \mathbb{Z}$, one can write a as

$$a = qn + r$$

for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. Here, q is the quotient and r is the remainder that one obtains when one divides a by n. Thus, $a \mod n = r$. For example, since $38 = 5 \times 7 + 3$ we have $38 \bmod 7 = 3$.

3. If $a \lfloor n$ (*i.e.*, a is divisible by n), then by definition, $a = qn$ for some $q \in \mathbb{Z}$, and thus, $a \mod n = 0$ (*i.e.*, the remainder that one obtains when one divides a by n is zero).

4. In the system $(\mathbb{Z}_n, +)$, the *additive identity* is still 0, which corresponds to taking no step either clockwise or anticlockwise. For any $a \in \mathbb{Z}_n$, its *additive inverse* is $(n-a) \in \mathbb{Z}_n$, since $a + (n-a) = n \equiv 0 \pmod n$.

5. It's often convenient to remember the following:

$$(a+b) \mod n \quad = \quad ((a \mod n) + (b \mod n)) \mod n$$

An example problem using the above basic principles:

Q: Compute $(5 + 31^2) \bmod 29$.

Solution: The most important thing to do in problems as this is to be able to make use of the division algorithm by expressing the quantity $(5 + 31^2)$ as $29q + r$. The problematic term in this question is the 31^2. So we simply express 31 as $29 + 2$. Thus we have,

$$\begin{aligned} 5 + 31^2 &= 5 + (29+2)^2 \\ &= 5 + 29^2 + 4 \times 29 + 4 \\ &= 29(29+4) + 9 \\ &= 29q + 9 \end{aligned}$$

where $q = 33$.

Thus, $(5 + 31^2) \bmod 29 \ = \ (29 \times 33 + 9) \bmod 29 \ = \ 9$.

Practice problems:

1. Compute $(25^2 + 32^3) \bmod 29$.
2. Compute $15! \bmod 7$.
3. If $12 \equiv 7 \pmod{n}$, what can be a possible value of n?

Prime Numbers

> **Definition of Prime Numbers:** Prime numbers are natural numbers that have exactly two positive divisors: 1 and itself.

Example of the first few prime numbers: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots$. 1 is not a prime number since its two positive divisors, 1 and itself, are not distinct.

> **Prime Counting Function:** The prime counting function, π, is defined as follows: $\pi(n)$ is equal to the *number of prime numbers less than or equal to n*, for some $n \in \mathbb{N}$.

Evaluation of the prime counting function on the first 20 natural numbers is listed in the table below:

n	$\pi(n)$	The prime numbers less than or equal to n
1	0	
2	1	2
3	2	2, 3
4	2	2, 3
5	3	2, 3, 5
6	3	2, 3, 5
7	4	2, 3, 5, 7
8	4	2, 3, 5, 7
9	4	2, 3, 5, 7
10	4	2, 3, 5, 7
11	5	2, 3, 5, 7, 11
12	5	2, 3, 5, 7, 11
13	6	2, 3, 5, 7, 11, 13
14	6	2, 3, 5, 7, 11, 13
15	6	2, 3, 5, 7, 11, 13
16	6	2, 3, 5, 7, 11, 13
17	7	2, 3, 5, 7, 11, 13, 17
18	7	2, 3, 5, 7, 11, 13, 17
19	8	2, 3, 5, 7, 11, 13, 17, 19
20	8	2, 3, 5, 7, 11, 13, 17, 19

Note how $\pi(n)$ remains unchanged between 3 & 4, between 5 & 6, between 7 & 10, between 11 & 12, between 13 & 16, etc. Of course as the value of n increases, the value of $\pi(n)$ increases as well. But as n becomes larger and larger, the *rate* at which $\pi(n)$ increases become smaller and smaller. That means the intervals of n in which $\pi(n)$ remain unchanged, on an average, become longer and longer. This is illustrated in the plot of $\pi(n)$ against n in Figure 3.

So the question that we will investigate next is, *"for large values of n, how does $\pi(n)$ increase as we increase n?"* The answer is given by the *Prime Number Theorem*:

Prime Number Theorem: For large values of n, the following holds:

$$\pi(n) \simeq \frac{n}{\ln(n)}$$

where, ln is the *natural logarithm* function.

That means, as n becomes very large, the number of prime numbers less than or equal to n is approximately $\frac{n}{\ln(n)}$. This of course will give incorrect results for small values of n. But let's consider an example of large n, say, $n = 10^9$. For

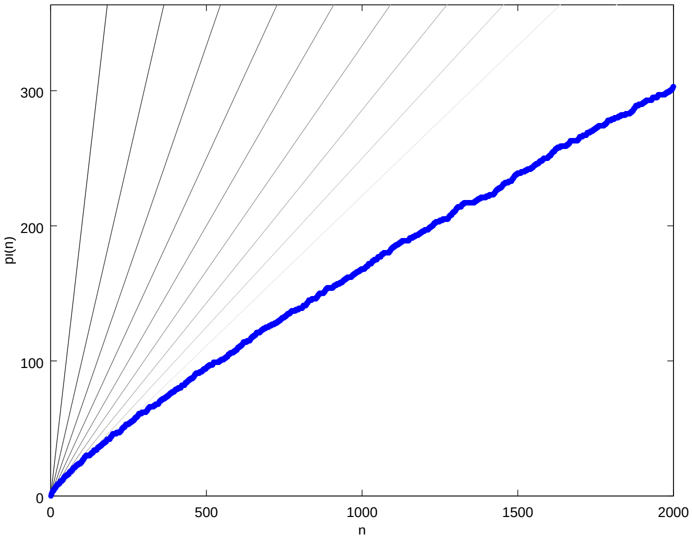


Figure 3: $\pi(n)$ plotted against n, for n from 1 to 2000. Note how the curve "bends" downwards as the value of n increases.

this value, $\ln(10^9) \simeq 20.723$. Thus, by the prime number theorem, we should have $\pi(10^9) \simeq \frac{10^9}{20.723} \simeq 48,300,000$. This number is in fact quite close to the actual value of $\pi(10^9) = 50,847,534$ in relative terms (the error is about $\frac{50{,}847{,}534-48{,}300{,}000}{50{,}847{,}534} \simeq$ 5% of the actual value). As we make n even higher, this relative error becomes even smaller.

Historic note: This theorem was first conjectured by C. F. Gauss in early 1800's, and later proven near the end of the same century due to the effort of multiple mathematicians.

Practice problems:

1. If $\pi(1000) = 168$ and $\pi(100) = 25$, how many 3-digit prime numbers are there?
2. If $\ln(4.9 \times 10^8) \simeq 20$, estimate the number of prime numbers less than 4.9×10^8.

We will discuss a few other interesting theorems involving prime numbers:

Fermat's Little Theorem: If p is a prime number and $a \in \mathbb{Z}$ is an integer that is not divisible by p, then the following is always true:

$$a^{p-1} \equiv 1 \pmod{p}$$

Or in other words, $a^{p-1} \bmod p = 1$.

It is easy to test this theorem for small values of a and p: Let's say $p = 5$ be the prime number o choice, and $a = 6$ be the integer which is not divisible by p. Then $a^{p-1} = 6^4 = 1296$. Now, if we divide 1296 by $p = 5$, the remainder that we get is 1. Thus, $6^4 \equiv 1 \pmod{5}$, just as Fermat's little theorem predicted. However, one may now use this theorem to arbitrary prime numbers, p, and numbers n that are not divisible by p. For example, one can ask what is 21^{12} mod 13? Choosing $p = 13$, $a = 21$ and applying the Fermat's little theorem, one can immediately say that 21^{12} mod $13 = 1$.

Practice problems:

1. Compute: $24^{10} \bmod 11$, $49^6 \bmod 7$, $11^{22} \bmod 23$.
2. Compute: $12^{24} \bmod 7$, $(16^{18} + 21^2) \bmod 19$.

Coprime Numbers

Two integers are called *coprime* or *relatively prime* if they do not have any common factor other than 1. Thus, 15 and 28 are coprime integers (relative to each other), since upon factorization, $15 = 3 \times 5$ and $28 = 2 \times 2 \times 7$, do not have any common factor other than 1. On the other hand, $12 = 2 \times 2 \times 3$ and $15 = 3 \times 5$ are not coprime since they have the common factor of '3'.

Chinese Remainder Theorem: Suppose $n_1, n_2, \cdots, n_k$ are pairwise coprime integers and $a_1, a_2, \cdots, a_k$ are any integers. Then the following set of k equations in the variable x has a simultaneous integer solution.

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\cdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

For example, given $n_1 = 3, n_2 = 4, n_3 = 5$, which are pairwise coprime, and $a_1 = 2, a_2 = 3, a_3 = 1$, the following set of equations

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 1 \pmod{5} \end{aligned}$$

has a solution of $x = 11$ (Exercise: Verify that's indeed true.)

Open Problems and General Discussions on Prime Numbers

The Twin Prime Conjecture: Two prime numbers are called *twin primes* if their difference is 2. For example, 2 and 3 are twin primes, 3 and 5 are twin primes, 17 and 19 are twin primes, etc. Interestingly, even if we go higher and higher in the natural number, we keep finding such twin prime numbers. However it is not known if there are infinitely many twin prime pairs. That is, whether or not there exists a number, however large, above which there does not exist any twin primes. People have used computers to search for twin primes, and have found very large twin primes. For example, as of 2009, the largest known twin primes are $65516468355 \times 2^{333333} - 1$ and $65516468355 \times 2^{333333} + 1$. However a proof or disproof for the claim that there exits arbitrarily large twin primes (and thus infinitely many of them) is still an unsolved problem in mathematics, and is known as the *twin prime conjecture*.

Goldbach's conjecture: Consider an even natural number, say 12. One can write it as sum of two prime numbers, $12 = 5+7$. A few more examples are $18 = 7+11 = 5+13$, $76 = 73+3 = 29+47$, $100 = 3+97 = 11+89 = 17+83 = 29+71 = 41+59 = 47+53$, etc. Thus the natural question is, *"can every even natural number be written as sum two prime numbers?"* Although this question is deceptively simple, finding a definitive "yes" or "no" answer to it has remained illusive. As of 2013, computers have been used to check even natural numbers up to 4×10^{17}, and each and every of them can be written as sum of two prime numbers at least in one way. But weather every arbitrarily large even natural number can be written as sum of two prime numbers is an unanswered question in mathematics, and the claim that it can be, is known as the *Goldbach's conjecture*.

Cryptography: Refer to class lecture notes for details.

Rational Numbers

In the previous section we saw how we went from $\mathbb{N}$ to $\mathbb{Z}$ in order to be able to complete a structure, namely a *group* structure, which involved closure of the set under the operation of '$+$' (addition) and its inverse.

Recall that on the integers, $(\mathbb{Z},+)$, one can define multiplication using addition quite naturally: By definition, $m \times n = m+m+\cdots m$ (n counts of m summed up), for $n,m \in \mathbb{Z}, n \geq 0$. If n is negative, we simply add $-n$ counts of m, and then finally flip the sign of the number.

Now, just as we defined subtraction as the inverse operation of multiplication, *division* can be defined as the inverse operation of multiplication: The answer to the question *"What is the integer, to which when we multiply 'n', do we get p?"* is defined as $\frac{p}{n}$. For example, with $p = 15$ and $n = 5$, the integer $\frac{15}{5} = 3$ is the integer to which when we multiply 5 we get 15. However, for arbitrary pairs of integers, the answer to this question may not lie in the integers. For example, what is the integer, to which when we multiply '$n = 7$', do we get $p = 18$? There is no answer to this question in the set of integers. Thus, we insert the *"missing"* numbers to create a new set of numbers, such that it will be *closed* under division, the inverse operation of multiplication. This is the set of *rational numbers*:

> **Rational Numbers:** In set builder notation, the set of rational numbers is defined as,
>
> $$\mathbb{Q} = \left\{ \frac{p}{q} \;\middle|\; p, q \in \mathbb{Z} \right\}$$
>
> The rational numbers are equipped with two operations, '$+$' (addition) and '$\times$' (multiplication). So one may write the rational numbers as $(\mathbb{Q}, +, \times)$.

As with the integers, the rational numbers are closed under addition (for every $u, v \in \mathbb{Q}$ there exists $u + v \in \mathbb{Q}$), has an additive identity element ($0 = \frac{0}{1}$), and has additive inverses (for every $w \in \mathbb{Q}$, there exists $-w \in \mathbb{Q}$ such that $w + (-w) = 0$). However, in addition, it also has the following properties:

a. There exists an element, $1 \in \mathbb{Q}$, called the *multiplicative identity*, such that for any $a \in \mathbb{Q}$, $a \times 1 = 1 \times a = a$ (*multiplicative identity element*),

b. For every element $a \in \mathbb{Q}$, $a \neq 0$ (where 0 is the additive identity), there exists an element $\frac{1}{a} \in \mathbb{Q}$ (called the *multiplicative inverse of* a) such that $a \times \frac{1}{a} = 1$ (*existence multiplicative inverse elements*),

c. For any $a, b \in \mathbb{Q}$, the element $a \times b \in \mathbb{Q}$ (*closure under multiplication*),

As before, the property 'b.' above encodes the operation of division, where instead of talking about inverse of the '$\times$' operation, we present the same concept in terms of *multiplicative inverse* of the elements themselves.

Addition, subtraction, multiplication and division of rational numbers can be summarized in the following formulae: For $p, q, u, v \in \mathbb{Z}$,

1. $\frac{p}{q} + \frac{u}{v} = \frac{pv+qu}{qv}$

2. $\frac{p}{q} - \frac{u}{v} = \frac{pv-qu}{qv}$

3. $\frac{p}{q} \times \frac{u}{v} = \frac{pu}{qv}$

4. $\frac{p}{q} / \frac{u}{v} = \frac{pv}{qu}$

Rational Numbers As Ratio of Coprime Integers

A rational number does not have an unique representation as ratio of two integers. For a rational number $\frac{p}{q} \in \mathbb{Q}$, where $p, q \in \mathbb{Z}$, it may be possible to cancel the common factors of p and q to obtain a *reduced form* of the same rational number. For example, $\frac{12}{18} = \frac{2\times2\times3}{2\times3\times3} = \frac{2}{3}$, where in the last step we divided the numerator and the denominator by the factor $2 \times 3 = 6$, that is common to 12 and 18. Note that in the final form, the numerator, 2, and the denominator, 3, do not have any more common factors, and thus are *coprime integers*. As a matter of fact, given any rational number as ratio of two integers, one can always "*cancel out*" the common factors from the numerator and the denominator so that the final form of the number is expressed as ratio of two coprime integers. This form of a rational number we will refer to as its *reduced form*.

Irrational Numbers

Irrational numbers are those which cannot be expressed as ratio of two integers (*i.e.*, not rational). For example, the solution to the equation $x^2 - 2 = 0$, as we know, is $x = \pm\sqrt{2}$. It can be shown that this number is not a rational number:

> **Proposition:** $\sqrt{2}$ is an irrational number.
>
> *Proof:* We prove this by contradiction. If possible, supposed $\sqrt{2}$ is rational. Thus, we can write it as a ratio of two coprime integers, $\sqrt{2} = \frac{p}{q}$, where $p, q \in \mathbb{Z}$ are coprime (recall that any rational number can be written as a ratio of two coprime integers). Thus,
>
> $$\begin{aligned} \sqrt{2} &= \frac{p}{q} \\ \Rightarrow \quad 2 &= \frac{p^2}{q^2} \\ \Rightarrow \quad p^2 &= 2\,q^2 \end{aligned}$$
>
> Thus p^2 is even (divisible by 2). p being an integer, and 2 being not a square integer, the only way p^2 can be divisible by 2 is if p itself is divisible by 2. Thus, $p = 2a$, for some $a \in \mathbb{Z}$. Plugging this into the equation above,
>
> $$\begin{aligned} (2a)^2 &= 2\,q^2 \\ \Rightarrow \quad q^2 &= 2\,a^2 \end{aligned}$$
>
> Once again, by similar argument as before, the only way q^2 can be even is if q itself is even. Thus, $q = 2b$.

Thus we have shown that both p and q have to be divisible by 2. This is in direct contradiction to our initial assumption that p and q are coprime integers. Thus we have ended up with a contradiction! Hence $\sqrt{2}$ cannot be written as a ratio of two coprime integers, and hence it's irrational.

Practice problems:

1. Using the method of contradiction, prove that the following numbers are irrational: $\sqrt[3]{4}$, $\sqrt[5]{7}$, $\sqrt[2]{8}$.

2. Which of the following numbers are irrational and which are rational: $\sqrt{\frac{4}{9}}$, $\sqrt{5}$, $2+\sqrt[3]{3}$, $\frac{1}{2}-\sqrt[3]{8}$? Explain your answers.

Algebraic Numbers

The set of (real) algebraic number, $\mathbb{A}$, consist of numbers that are (real) solutions to polynomial equations with rational coefficients.

Note that rational numbers are algebraic as well since $\frac{p}{q}$ is a solution to the polynomial equation $qx-p=0$.

Refer to class lecture notes for details.

Transcendental Numbers

The real numbers that are not algebraic numbers (*e.g.*, π, e, π^{π}, etc.). One cannot write down a pilynomial equation with rational coefficients whose solution is a transcendental numbers.

Refer to class lecture notes for details.

Complex Numbers

Imaginary Numbers

The set of real algebraic numbers, $\mathbb{A}$, consists of the real numbers that are solution to polynomial equations with rational coefficients.
Examples:

i. $\sqrt{2} \in \mathbb{A}$ since it is a solution to the polynomial equation $x^2-2=0$.

ii. $-2+\sqrt{3} \in \mathbb{A}$ since it is a solution to the polynomial equation $x^2+4x+1=0$.

However, there are many polynomial equations whose solutions cannot be found anywhere in the set of real numbers. For example, consider the simple polynomial equation $x^2+2=0$. A solution to this, x, should be such that $x^2=-2$. However the square of any real number cannot be negative. So we introduce new numbers in our number system:

> We take the simplest of such polynomial equations, $x^2+1=0$, and for a solution to this equation define a new number: $i=\sqrt{-1}$.

This new number, i, that we just defined is called *imaginary* due to historic reasons. However, in the light of modern mathematics this is no more "imaginary" than the rational numbers, real algebraic numbers or the transcendental numbers — each of which were introduced in our number system in order to *complete* some structure, operation or properties on the number system. For example, when we introduced the rationals, we saw that some ratio of integers, such as $\frac{6}{3}, \frac{-21}{7}$, etc. do lie in the set of integers themselves. But the ratios like $\frac{3}{2}, \frac{7}{9}, \frac{20}{6}$, etc do not find a place in $\mathbb{Z}$. So we introduced new numbers in the system – every number of the form $\frac{p}{q}$ for $p,q\in\mathbb{Z}$ – and called this new set of numbers *rational numbers*, $\mathbb{Q}$. Likewise, now we introduce new numbers for solution to polynomial equations that clearly do not have solution on the real line, $\mathbb{R}$.

Since it is clear that this number, i, does not lie on $\mathbb{R}$, we place it somewhere outside the number line. It is also clear that if a solution to the equation of $x^2+1=0$ is written as i, then there will be polynomial equations whose solutions will be multiples of i. For example, for the polynomial equation $x^2+4=0$, a solution is $x=\sqrt{-4}=\sqrt{4}\sqrt{-1}=2i$. As another example, a solution to $x^2+\frac{2}{9}$ is $x=-\sqrt{-\frac{2}{9}}=-\frac{\sqrt{2}}{3}i$. These multiples of i are called "*imaginary numbers*", although as mentioned earlier, there is absolutely nothing "imaginary" about them. It's just a name given to these numbers.

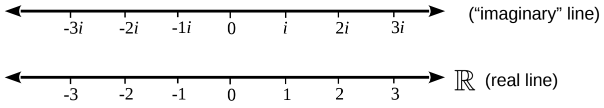


Figure 4: The real and imaginary number lines.

Thus, now we have two number lines in our number system: one is our usual real number line, $\mathbb{R}$, and the other is the *imaginary line* containing the multiples of i (Figure 4).

Complex numbers

However, the next thing that we observe is that the solutions to some polynomial equations come in form of a sum of a real number and an imaginary number. For example, consider the polynomial equation $x^2 - 2x + 3 = 0$, which can be re-written as $(x-1)^2 + 2 = 0$. Thus, a solution to this equation is given by $x - 1 = \sqrt{-2} = \sqrt{2}i \;\Rightarrow\; x = 1 + \sqrt{2}i$. Thus, the number $1 + \sqrt{2}i$ is a solution to a polynomial equation. In general, one can get arbitrary numbers of the form $a + bi$, where $a, b \in \mathbb{R}$, as solutions to polynomial equations. These numbers are essentially made up of two real numbers, a and b (the later being the coefficient of i), and are called *complex numbers*.

We emphasize once again that complex numbers are numbers that are made up of nothing but pairs of real numbers, (a, b), written in the peculiar form $a + bi$. Thus complex numbers an be represented as points on a plane, which by definition, is $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, consisting pairs of real numbers as its elements (recall the definition of a Cartesian product). This plane of the complex numbers is called the *complex plane*, $\mathbb{C}$, and just as we mentioned, this is nothing but $\mathbb{R}^2$. So the complex number $a + bi$ can be drawn as point on the complex plane with a projection of a on the horizontal axis (called the *real axis*) and a projection of b on the vertical axis (called the *imaginary* axis). This is illustrated in Figure 5.

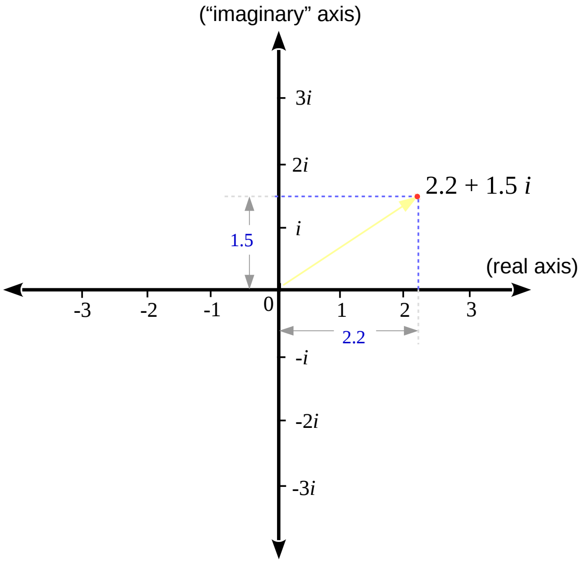


Figure 5: The complex plane.

The Fundamental Theorem of Algebra

So far we have defined $i = \sqrt{-1}$ (a solution to the polynomial equation $x^2 + 1 = 0$) and saw that solution to some polynomial equations can be written in the form of $a + ib$, where $(a, b) \in \mathbb{R}^2$. But what is so special about $\sqrt{-1}$? What about the polynomial equation $x^4 + 1 = 0$? A solution to this equation seems to be $\sqrt[4]{-1}$. Do we have to define another new number, say $j = \sqrt[4]{-1}$, for a solution to this polynomial?

It turns out that we need not define any more new numbers for writing solution to polynomial equations with any real coefficients. It can in fact be shown that a solution to the aforesaid equation, $x^4 + 1 = 0$, is actually $x = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i$ (a complex number). We can verify that very easily: If $x = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i$, then,

$$x^2 = \left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i\right)^2 = \left(\frac{1}{\sqrt{2}}\right)^2 + 2\left(\frac{1}{\sqrt{2}}\right)\left(\frac{1}{\sqrt{2}} i\right) + \left(\frac{1}{\sqrt{2}} i\right)^2 = \frac{1}{2} + 2\frac{1}{2} i - \frac{1}{2} = i$$

Thus we have, $x^4 = (x^2)^2 = i^2 = -1$. This means $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i$ is a solution to the polynomial equation $x^4 + 1 = 0$. In fact any polynomial equation with real or complex coefficients have solutions that are complex numbers (*i.e.* are of the form $a + bi$). This is formally known under the name of *The Fundamental Theorem of Algebra*.

> **The Fundamental Theorem of Algebra** *(semi-formal statement)*: Every polynomial equation in x, with real or complex coefficients, have one or more solutions which are complex numbers.

Complex Algebra

In this section we will describe the rules for addition, multiplication and division of complex numbers:

Addition: $(a + bi) + (p + qi) = (a + p) + (b + q)i.$
Example: $(2 + 3i) + (1 - 1.4i) = 3 + 1.6i.$

Subtraction: $(a + bi) - (p + qi) = (a - p) + (b - q)i.$
Example: $(2 + 3i) - (1 - 1.4i) = 1 + 4.4i.$

Multiplication: $(a + bi)(p + qi) = ap + bpi + aqi + (bi)(qi) = (ap - bq) + (bp + aq)i.$
Example: $(2 + 3i)(1 - 1.4i) = 6.2 + 0.2i.$

Multiplication: $\frac{a+bi}{p+qi} = \frac{(a+bi)(p-qi)}{(p+qi)(p-qi)} = \frac{(ap+bq)+(bp-aq)i}{p^2+q^2}.$
Example: $\frac{2+3i}{1-2i} = \frac{-5+7i}{5} = -1 + \frac{7}{5} i.$

Summary: The following relationships are important:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{A} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Note that $\mathbb{A}$ refers to only the real algebraic numbers (in general, one can talk about complex algebraic numbers as well). The Transcendental numbers is thus the set $\mathbb{R} - \mathbb{A}$.

Cardinality

The way we compare cardinality of two infinite sets is by establishing one-to-one correspondence between the elements of the sets. If such a correspondence exists, then they have the same cardinality.

Cardinality of countably infinite sets is $\aleph_0$. Thus, $|\mathbb{N}| = |\mathbb{Z}| = \aleph_0$. **Refer to class lecture notes for** details.

Using the *"spiral"* argument, one can also show that $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Q}| = \aleph_0$. It is also possible to show that $|\mathbb{A}| = \aleph_0$. **Refer to class lecture notes for** details.

However, using the *Cantor's Diagonal Argument*, one can show that $|\mathbb{R}| > |\mathbb{N}| = \aleph_0$. Thus we write $|\mathbb{R}| = \aleph_1$, and call it the *cardinality of the continuum*. **Refer to class lecture notes for** details.

Relationship between $\aleph_0$ and $\aleph_1$: It can be shown that there exists a one-to-one correspondence between the elements of $\mathbb{R}$ and $\mathscr{P}(\mathbb{N})$ (the power set of $\mathbb{N}$). Thus, $\aleph_1 = |\mathbb{R}| = |\mathscr{P}(\mathbb{N})| = 2^{\aleph_0}$. **Refer to class lecture notes for** details.