"Sapienza" University of Rome
Faculty of Information Engineering, Informatics and Statistics
Department of Computer Science

Discrete Mathematics

Lecture notes integrated with the book "TODO",
Author TODO, ...

Author
Alessio Bandiera

March 7, 2024

Contents

Information and Contacts

Personal notes and summaries collected as part of the *Discrete Mathematics* course offered by the degree in Computer Science of the University of Rome "La Sapienza".

Further information and notes can be found at the following link: **https://github.com/aflaag-notes**. Anyone can feel free to report inaccuracies, improvements or requests through the Issue system provided by GitHub itself or by contacting the author privately:

- Email: **alessio.bandiera02@gmail.com**
- LinkedIn: **Alessio Bandiera**

The notes are constantly being updated, so please check if the changes have already been made in the most recent version.

Suggested prerequisites:

- Differential Calculus
- Integral Calculus

Licence:

1

TODO

1.1 TODO

1.1.1 TODO

Definition 1.1.1.1: Peano's axioms

The **Peano's axioms** are 5 axioms which define the set $\mathbb{N}$ of the **natural numbers**, and they are the following:

i) $0 \in \mathbb{N}$

ii) $\exists\, \mathrm{succ} : \mathbb{N} \to \mathbb{N}$, or equivalently, $\forall x \in \mathbb{N} \quad \mathrm{succ}(x) \in \mathbb{N}$

iii) $\forall x, y \in \mathbb{N} \quad x \neq y \implies \mathrm{succ}(x) \neq \mathrm{succ}(y)$

iv) $\nexists x \in \mathbb{N} \mid \mathrm{succ}(x) = 0$

v) $\forall S \subseteq \mathbb{N} \quad (0 \in S \land (\forall x \in S \quad \mathrm{succ}(x) \in S)) \implies S = \mathbb{N}$

Note: inside this notes, it will be assumed that $0 \in \mathbb{N}$.

Principle 1.1.1.1: Induction principle

Let P be a property which is true for $n = 0$, thus $P(0)$ is true; also, for every $n \in \mathbb{N}$ we have that $P(n) \implies P(n+1)$; then $P(n)$ is true for every $n \in \mathbb{N}$.

Using symbols, using the formal logic notation, we have that

$$\frac{P(0) \quad P(n) \implies P(n+1)}{\forall n \quad P(n)}$$

Observation 1.1.1.1: The fifth Peano's axiom

Note that the fifth Peano's axiom is equivalent to the induction principle, since, it states that for every subset S of $\mathbb{N}$ containing 0 and closed under succ must be equal to $\mathbb{N}$ itself.

Definition 1.1.1.2: Integers

The set of **integers** is defined as follows:

$$\mathbb{Z} := \mathbb{N} \cup \{-x \mid x \in \mathbb{N}\}$$

Definition 1.1.1.3: Divisor

Given two numbers a, b, we say that a **divides** b – therefore a is called **divisor** of b – if and only if there exists an integer $k \in \mathbb{Z}$ such that $b = a \cdot k$ – therefore b is called **multiple** of a. Using symbols

$$a \mid b \iff \exists k \in \mathbb{Z} \mid b = a \cdot k$$

Example 1.1.1.1 (Divisors)**.** Given the numbers 15 and 5, we can say that $5 \mid 15$ because $3 \cdot 5 = 15$.

Definition 1.1.1.4: $\mathbb{P}$

A number x is said to be **prime** if no number between 2 and $x-1$ divides it. Note that 0 and 1 are not considered prime numbers by convention. The set of **prime** numbers is defined as follows:

$$\mathbb{P} = \{x \in \mathbb{N} - \{0, 1\} \mid \nexists d \in [2, x-1] : d \mid x\}$$

Proposition 1.1.1.1: $\mathbb{P}$ is infinite

There are infinitely many primes. Using symbols

$$|\mathbb{P}| = +\infty$$

Proof. By way of contradiction, assume that $\mathbb{P}$ is finite, thus

$$\exists n \in \mathbb{N} \mid \mathbb{P} = \{p_1, \ldots, p_n\}$$

and let $x = p_1 \cdot \ldots \cdot p_n$. Since $x \neq p_1, \ldots, p_n$, then $x \notin \mathbb{P}$, so x is not a prime number; but x can't be divided by any of the $p_1, \ldots, p_n$ either, because the remainder will always be 1. This means that x is neither prime nor non-prime, which is a contradiction $\lightning$. □

Definition 1.1.1.5: gcd

The **gcd** (*Greatest Common Divisor*) of two given numbers a, b is the greatest of the divisors which a and b have in common. Using symbols, we say that

$$d = \gcd(a, b) \iff \forall f \in \mathbb{N} : f \mid a \land f \mid b \quad f \mid d$$

If the gcd of two numbers is 1, they are said to be **coprime**.

Example 1.1.1.2 (gcd)**.** Given 15 and 63, we have that $\gcd(15, 63) = 3$.

Algorithm 1.1.1.1: Euclid's algorithm

Input: Two natural numbers a, b.
Output: $\gcd(a, b)$.

---

function GCD(a, b)
    $r_0 := b$
    $r_1 := a$
    $r_{i-1} := r_1$
    $r_i : r_1 \mid r_i - r_0$
    $r_{i+1} : r_i \mid r_{i+1} - r_{i-1}$
    while $r_{i+1} \neq 0$ **do**
        $r_{i-1} = r_i$
        $r_i = r_{i+1}$
        $r_{i+1} : r_i \mid r_{i+1} - r_{i-1}$
    end while
    return r_i
end function

Idea. TODO

Example 1.1.1.3 (Euclid's algorithm)**.** To compute the $\gcd(341, 527)$, using the Algorithm 1.1.1.1, we get the following:

$$\begin{aligned} 527 &= 341 \cdot 1 + 186 \\ 341 &= 186 \cdot 1 + 155 \\ 186 &= 155 \cdot 1 + 31 \\ 155 &= 31 \cdot 5 + 0 \end{aligned}$$

hence we have that

$$\gcd(341, 527) = 31$$

Lemma 1.1.1.1: Bézout's identity

Given a pair of numbers $a, b \in \mathbb{Z}$, there exists $x, y \in \mathbb{Z}$ such that the $\gcd(a, b)$ is a linear combination of a and b. Using symbols

$$\forall a, b \in \mathbb{Z} \quad \exists x, y \in \mathbb{Z} \mid \gcd(a, b) = ax + by$$

Proof. Omitted. □

Example 1.1.1.4 (Bézout's identities)**.** Using the Example 1.1.1.3, in order to compute the Bézout's identity of 341 and 527, we need to do the following:

$$31 = 186 - 155 \cdot 1 = 186 - (341 - 186 \cdot 1) = 2 \cdot 186 - 341 = 2 \cdot (527 - 341) - 341 = 2 \cdot 527 - 3 \cdot 341$$

thus the Bézout's identity is

$$31 = 2 \cdot 527 - 3 \cdot 341$$

Corollary 1.1.1.1: Prime divisors

Given a natural number $n \in \mathbb{N}$ and a prime number $p \in \mathbb{P}$, it holds that

$$p \nmid n \iff \gcd(p, n) = 1$$

Proof.

First implication. Instead of proving that $p \nmid n \implies \gcd(p, n) = 1$, we will prove the contrapositive, namely that $\gcd(p, n) > 1 \implies p \mid n$. Hence, since $\gcd(p, n) \mid p$ by definition, because $p \in \mathbb{P}$ then $\gcd(p, n)$ must be either 1 or p itself, and we assumed that $\gcd(p, n) > 1$, $\gcd(p, n)$ must be 1, which means that $p \mid n$.

Second implication. Note that $\gcd(p, n) = 1 \implies \exists x, y \in \mathbb{Z} \mid 1 = px + ny$ by the Lemma 1.1.1.1, hence if $p \mid a$ then $p \mid 1$ by the Definition 1.1.1.5, which is impossibile because $p \in \mathbb{P}$ by the Definition 1.1.1.4.

□

Lemma 1.1.1.2: Prime divisors

Given a pair of numbers $a, b \in \mathbb{N}$, and a prime number $p \in \mathbb{P}$ such that $p \mid ab$, then either $p \mid a$ or $p \mid b$. Using symbols

$$\forall a, b \in \mathbb{N} \quad \exists p \in \mathbb{P} : p \mid ab \implies p \mid a \lor p \mid b$$

Proof. Without loss of generality, assume that $p \nmid a$, thus $\gcd(p, a) = 1$ by the Corollary 1.1.1.1; hence, for the Lemma 1.1.1.1, we have that

$$\exists x, y \in \mathbb{Z} \mid 1 = px + ay \iff b = bpx + bay$$

Note that $p \mid ab \iff \exists k \in \mathbb{Z} \mid pk = ab$ which means that

$$b = bpx + pky = p(bx + ky) \iff p \mid b$$

The same argument can be used to show that $p \nmid b \implies p \mid a$. □

Theorem 1.1.1.1: Fundamental theorem of arithmetic

The **fundamental theorem of arithmetic**, also known as the **UPF** theorem (*Unique Prime Factorization*) states that for every natural number $n \in \mathbb{N}$ there exists a unique prime factorization for n. Using symbols

$$\forall n \in \mathbb{N} \quad \exists! p_1, \ldots, p_k \in \mathbb{P}, e_1, \ldots, e_k \in \mathbb{N} \mid n = {p_1}^{e_1} \cdot \ldots \cdot {p_k}^{e_k}$$

Proof. Omitted. □

1.1.2 Continued fractions

Definition 1.1.2.1: Continued fraction

A **continued fraction** is an expression obtained through an iterative process of representing a number as the sum of its *integer part*, and the reciprocal of another number. Continued fractions can be both **finite** and **infinite**, and are represented with the following notation:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} = [a_0; a_1, a_2, \ldots, a_n]$$

for finite continued fractions, and

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} = [a_0; a_1, a_2, \ldots]$$

for infinite continued fractions.

Example 1.1.2.1 (Finite continued fractions)**.** Consider the Example 1.1.1.3; note that the Euclid algorithm can be used to derive the finite continued fraction of $\dfrac{527}{341}$, as follows:

$$\begin{aligned} \tfrac{527}{341} &= 1 + \tfrac{186}{341} \\ \tfrac{341}{186} &= 1 + \tfrac{155}{186} \\ \tfrac{186}{155} &= 1 + \tfrac{31}{155} \\ \tfrac{155}{31} &= 5 \end{aligned}$$

and then, rearranging

$$\frac{527}{341} = 1 + \cfrac{1}{1 + \cfrac{155}{186}} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{31}{155}}} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{5}}} = [1; 1, 1, 5]$$

Example 1.1.2.2 (Infinite continued fractions)**.** Assume that there exists an x such that

$$\sqrt{2} = 1 + \frac{1}{x}$$

then rearrange as follows:

$$\sqrt{2} = 1 + \frac{1}{x} \iff \sqrt{2} - 1 = \frac{1}{x} \iff x = \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)} = \sqrt{2}+1$$

and now we can substitute $\sqrt{2}$ with $1 + \frac{1}{x}$, yielding the following:

$$x = 1 + \frac{1}{x} + 1 = 2 + \frac{1}{x}$$

Finally, this equation can be used to construct the infinite continued fraction of $\sqrt{2}$, like this:

$$x = 2 + \frac{1}{x} = 2 + \cfrac{1}{2 + \cfrac{1}{x}} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}$$

implying that

$$\sqrt{2} = 1 + \frac{1}{x} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}} = [1; 2, 2, 2] = [1; \overline{2}]$$

Algorithm 1.1.2.1: Continued fractions

Given a continued fraction $[a_0; a_1, \ldots, a_n]$, the corresponding number can be computed by constructing the following table (note that $N_0 := 1$ and $D_0 := 0$, meaning that a and N, D differ by 1 position at each column)

C.F.		a_0	a_1	a_2	$\ldots$	a_n
N	1	a_0	$a_1 \cdot N_1 + N_0$	$a_2 \cdot N_2 + N_1$	$\ldots$	$a_n \cdot N_n + N_{n-1}$
D	0	1	$a_1 \cdot D_1 + D_0$	$a_2 \cdot D_2 + D_1$	$\ldots$	$a_n \cdot D_n + D_{n-1}$

then, the answer is

$$[a_0; a_1, \ldots, a_n] = \frac{N_{n+1}}{D_{n+1}}$$

Idea. TODO

Example 1.1.2.3. To compute the number corresponding to the continued fraction $[2; 1, 3, 1, 5, 4]$, the following table can be constructed:

C.F.		2	1	3	1	5	4
N	1	2	3	11	14	81	338
D	0	1	1	4	5	29	121

meaning that

$$[2; 1, 3, 1, 5, 4] = \frac{338}{121}$$

Definition 1.1.2.2: The golden ratio

The **golden ratio** is defined as the positive solution of the following equation:

$$x^2 - x - 1 = 0 \iff x = \frac{1 \pm \sqrt{5}}{2} \implies \varphi := \frac{1 \pm \sqrt{5}}{2}$$

and it's commonly denoted with the greek letter φ.

Observation 1.1.2.1: Continued fraction of φ

Given the Definition 1.1.2.2, we have that

$$\varphi^2 - \varphi - 1 = 0 \iff \varphi^2 = \varphi + 1 \iff \varphi = 1 + \frac{1}{\varphi}$$

and then from this equation we can repeatedly substitute φ as follows:

$$\varphi = 1 + \frac{1}{\varphi} = 1 + \cfrac{1}{1 + \cfrac{1}{\varphi}} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}$$

which means that

$$\varphi = [1; \overline{1}]$$

Definition 1.1.2.3: The Fibonacci sequence

The **Fibonacci sequence** is recursively defined as follows:

$$F_n = \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ F_{n-1} + F_{n-2} & n \geq 2 \end{cases}$$

Observation 1.1.2.2: Continued fraction of φ

Consider the following table of the continued fraction of the golden ratio, constructed via the Algorithm 1.1.2.1 by using the result discussed inside the Observation 1.1.2.1:

C.F.		1	1	1	1	1	...
N	1	1	2	3	5	8	...
D	0	1	1	2	3	5	...

we can spot that the pattern this table reveals is exactly the Fibonacci sequence, and this fact can be easily proved by letting

$$x = \lim_{n \to +\infty} \frac{F_{n+1}}{F_n} = \lim_{n \to +\infty} \frac{F_n}{F_{n-1}}$$

note that, clearly, $x > 0$ – and then, by using the Definition 1.1.2.3, we get the following

$$F_{n+1} = F_n + F_{n-1} \iff \frac{F_{n+1}}{F_n} = 1 + \frac{F_{n-1}}{F_n} = 1 + \frac{1}{\frac{F_n}{F_{n-1}}}$$

thus for $n \to +\infty$ we get that

$$x = 1 + \frac{1}{x}$$

which is the same equation that we derived inside Observation 1.1.2.1.

1.1.3 Series

Definition 1.1.3.1: The harmonic series

The harmonic series is defined as follows:

$$\sum_{k=1}^{+\infty} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \dots$$

Proposition 1.1.3.1: Divergence of the harmonic series

The harmonic series diverges.

Proof. Suppose that the harmonic series converges, thus

$$\exists S \mid \sum_{k=1}^{+\infty} \frac{1}{k} = S$$

then we have that

$$
\begin{aligned}
S = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} \ldots = \\
= \left(1 + \frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6}\right) + \ldots > \\
> \left(\frac{1}{2} + \frac{1}{2}\right) + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{6} + \frac{1}{6}\right) + \ldots = \\
= 1 + \frac{1}{2} + \frac{1}{3} + \ldots = S
\end{aligned}
$$

implying that $S > S$ ↯. □

Definition 1.1.3.2: Geometric series

A **geometric series** is commonly written as

$$\sum_{k=0}^{n} ar^k$$

where $a \in \mathbb{R}$ is a coefficient and $r \in \mathbb{R}$ is the *ration between adjacent terms*.

Proposition 1.1.3.2: Convergence of geometric series

For $r \in \mathbb{R}$ such that $|r| < 1$, it holds that

$$\sum_{k=0}^{+\infty} ar^k = \frac{a}{1-r}$$

Proof. Omitted. □

Theorem 1.1.3.1: Reciprocal of primes

The sum of the reciprocal of the prime numbers diverges. Using symbols

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = +\infty$$

Proof. Consider the following inequality:

$$\forall n \in \mathbb{N} \quad \prod_{p \in \mathbb{P} | p \leq n} \frac{p}{p-1} > \sum_{k=1}^{n} \frac{1}{k}$$

We can prove it with as follows:

- for any given $p \in \mathbb{P}$, the fraction $\dfrac{p}{p-1}$ can be rewritten as follows, by using the Proposition 1.1.3.2:

$$\forall p \in \mathbb{P} \mid p \leq n \quad \frac{p}{p-1} = \frac{1}{\frac{p-1}{p}} = \frac{1}{1-\dfrac{1}{p}} = \sum_{k=0}^{+\infty} \frac{1}{p^k} = 1 + \frac{1}{p} + \frac{1}{p^2} + \dots$$

  where $a = 1$ and $r = \dfrac{1}{p^k} : \dfrac{1}{p^{k-1}} = \dfrac{1}{p}$ – which is the infinite sum of the reciprocal of the powers of some prime number p

- this means that

$$\exists p_1, \dots, p_j \in \mathbb{P} \mid \prod_{p \in \mathbb{P} \mid p \leq n} \frac{p}{p-1} = p_1 \cdot \dots \cdot p_j \implies \prod_{p \in \mathbb{P} \mid p \leq n} \frac{p}{p-1} = \sum_{k=0}^{+\infty} \frac{1}{p_1^k} \cdot \dots \cdot \sum_{k=0}^{+\infty} \frac{1}{p_j^k}$$

- thus, thanks to the Theorem 1.1.1.1 this product expands to the sum of the reciprocal of every natural number that contains $p_1, \dots, p_j$ in his prime factorization, namely

$$\exists e_1, \dots, e_j \in \mathbb{N} \mid \sum_{k=0}^{+\infty} \frac{1}{p_1^k} \cdot \dots \cdot \sum_{k=0}^{+\infty} \frac{1}{p_j^k} = \sum_{k=0}^{+\infty} \frac{1}{p_1^{e_1} \cdot \dots \cdot p_j^{e_j}}$$

- finally, since $p_1, \dots, p_j <= n$ this summation must contain at least every term contained inside $\displaystyle\sum_{k=1}^{n} \frac{1}{k}$, which proves the inequality.

$\square$

Now consider the following:

$$\sum_{k=1}^{+\infty} \frac{1}{k} < \prod_{p \in \mathbb{P} \mid p \leq n} \frac{p}{p-1} \iff$$
$$\iff \log\left(\sum_{k=1}^{+\infty} \frac{1}{k}\right) < \left(\prod_{p \in \mathbb{P} \mid p \leq n} \frac{p}{p-1}\right) =$$
$$= \sum_{p \in \mathbb{P} \mid p \leq n} \log\left(\frac{p}{p-1}\right) = \sum_{p \in \mathbb{P} \mid p \leq n} (\log p - \log(p-1)) = \sum_{p \in \mathbb{P} \mid p \leq n} \int_{p-1}^{p} \frac{1}{x} \mathrm{d}x$$

and consider the area under the curve $\dfrac{1}{x}$ within the $[p-1, p]$ interval, for some prime number p:

TODO METTI GRAFICO

since

$$\forall x_1, x_2 \in \mathbb{R} \quad x_1 < x_2 \iff \frac{1}{x_1} > \frac{1}{x_2}$$

the function $\frac{1}{x}$ is monotonically decreasing, and in particular

$$\forall p \in \mathbb{P} \mid p \leq n \quad p - 1 < p \implies \frac{1}{p-1} > \frac{1}{p}$$

whic implies that the area under the curve $\frac{1}{x}$ within the $\frac{[}{p} - 1, p]$ must be smaller than the area of the rectangle that has a base of of $p - (p-1) = p - p + 1 = 1$ and an height of $\frac{1}{p-1}$, namely an area of $1 \cdot \frac{1}{p-1} = \frac{1}{1-p}$. This implies that

$$\sum_{p \in \mathbb{P} | p \leq n} \int_{p-1}^{p} \frac{1}{x} \mathrm{d}x < \sum_{p \in \mathbb{P} | p \leq n} \frac{1}{p-1}$$

Suppose that

$$\frac{1}{p-1} > \frac{2}{p}$$

then we have that

$$\frac{1}{p-1} > \frac{2}{p} \iff p > 2 \cdot (p-1) \iff p > 2p - 2 \iff 2 > 3p$$

which is not possibile because $p \in \mathbb{P} \mid p \leq n$. This implies that

$$\frac{1}{p-1} < \frac{2}{p} \implies \sum_{p \in \mathbb{P} | p \leq n} \frac{1}{p-1} < \sum_{p \in \mathbb{P} | p \leq n} \frac{2}{p}$$

and finally, this means that

$$\log\left(\sum_{k=1}^{+\infty} \frac{1}{k}\right) < \sum_{p \in \mathbb{P} | p \leq n} \frac{2}{p} \iff \frac{1}{2} \log\left(\sum_{k=1}^{+\infty} \frac{1}{k}\right) < \sum_{p \in \mathbb{P} | p \leq n} \frac{1}{p}$$

and because $\sum_{k=1}^{+\infty} \frac{1}{k}$ diverges, the left-hand side of the inequality diverges, thus the right-hand side must diverge too. This proves the statement, because the primes $p \in \mathbb{P}$ such that $p \leq n$ form a subset of $\mathbb{P}$.

1.2 Solved exercises

1.2.1 Number theory

Problem 1.2.1.1: $n^2 + n$ is even

Show that for every $n \in \mathbb{N}$, $n^2 + n$ is an even number.

Proof. Note that $n^2 + n = n \cdot (n+1)$, hence:

- if n is even, then
$$\exists k \in \mathbb{N} \mid n = 2k \implies n(n+1) = 2k(2k+1) = 4k^2 + 2k = 2(k^2 + k)$$
which is an even number;
- if n is odd, then
$$\exists k \in \mathbb{N} \mid n = 2k+1 \implies n(n+1) = (2k+1)(2k+2) = 4k^2+6k+2 = 2(2k^2+3k+1)$$
which is an even number.

$\square$

Problem 1.2.1.2: $4n - 1$ is not prime

Show that there are infinitely many numbers of the form $4n-1$ that are not prime.

Proof. Note that
$$\forall x^2 \in \mathbb{N} - \{0\} \quad 4x^2 - 1 = (2x+1)(2x-1)$$
which is a proper factorization of $4x^2 - 1$, hence every perfect square yields a number of the form $4n - 1$ which is not a prime number. Note that the number of perfect squares is infinite since the set of perfect square has the same cardinality of $\mathbb{N}$ since it's possibile to construct a bijective function as follows:
$$f : \mathbb{N} \to \mathbb{N} : x \mapsto x^2$$
Also, note that this proof does not show *every non-prime number of the form* $4n - 1$, since that is outside the scope of the problem. $\square$

Problem 1.2.1.3: The $4n - 3$ set

Consider the following set:
$$S := \{4n - 3 \mid n \in \mathbb{N}\}$$

1. Show that S closed under multiplication.
2. A number p is said to be *S-prime* if and only if p is the product of exactly two factors of S; for example, even though $3^2 = 9 \notin \mathbb{P}$ we have that $9 = 1 \cdot 9$, and since $1 = 4 \cdot 1 - 3 \in S$ and $9 = 4 \cdot 3 - 3 \in S$, then 9 is S-prime. Is the set of S-prime numbers infinite?
3. TODO

Proof.

1. To show that S is closed under multiplication, it suffices to show that
$$\forall a, b \in \mathbb{N} \quad (4a-3)(4b-3) = 16ab - 12a - 12b + 9 = 4(4ab - 3a - 3b + 3) - 3 \in S$$
2. TODO

$\square$

1.2.2 Induction

Problem 1.2.2.1: Cardinality of the power set

Show that for every given set S such that $n := |S|$ it holds that $|\mathcal{P}(S)| = 2^n$.

Proof. The statement will be shown by induction over n, the number of elements contained into S.

Base case. $n = 0 \implies S = \varnothing \implies \mathcal{P}(S) = \mathcal{P}(\varnothing) = \{\varnothing\} \implies |\mathcal{P}(S)| = 1 = 2^0 = 2^n$.

Inductive hypothesis. Assume that the statement is true for some fixed integer n.

Inductive step. It must be shown that, for a given set of elements S such that $|S| = n + 1$, it holds true that $|\mathcal{P}(S)| = 2^{n+1}$. Consider a subset $S' \subseteq S$ such that $|S'| = |S| - 1 = n + 1 - n = n$, hence for the inductive hypothesis we have that $|\mathcal{P}(S')| = 2^n$. Thus, to get the cardinality of $\mathcal{P}(S)$ the $(n + 1)$-th element inside $S - S'$ must be paired with every of the sets contained inside $\mathcal{P}(S')$, hence

$$\mathcal{P}(S) = 2 \cdot \mathcal{P}(S') = 2 \cdot 2^n = 2^{n+1}$$

$\square$

1.2.3 Continued fractions

Problem 1.2.3.1: Limits of continued fractions

1. What is the value that the following limit approaches?

$$\lim_{n \to +\infty} [2; 1, 4, n]$$

2. Consider the following sequence:

$$\frac{25}{16}, \frac{49}{36}, \frac{81}{64}, \frac{121}{100}, \ldots$$

Compute the continued fractions of these ratios; what is the limit of this sequence?

Proof.

1. By using the Algorithm 1.1.2.1, we get the following table:

C.F.		2	1	4	n
N	1	2	3	14	$14 \cdot n + 3$
D	0	1	1	5	$5 \cdot n + 1$

which means that

$$[2;1,4,n] = \frac{14n+3}{5n+1} \implies \lim_{n\to+\infty} \frac{14n+3}{5n+1} = \frac{14}{5}$$

2. We can convince ourselves that the sequence is

$$\left(\frac{2k+1}{2k}\right)^2$$

for some $k \in \mathbb{N}$. Thus, by following the Example 1.1.2.1, we can compute the continued fractions of the given ratios (calculations omitted) and get the following results:

$$\begin{aligned}
k = 2 &\implies \left(\frac{2\cdot 2+1}{2\cdot 2}\right)^2 = \left(\frac{5}{4}\right)^2 = \frac{25}{16} = [1;1,1,3,2] \\
k = 3 &\implies \left(\frac{2\cdot 3+1}{2\cdot 3}\right)^2 = \left(\frac{7}{6}\right)^2 = \frac{49}{36} = [1;2,1,3,3] \\
k = 4 &\implies \left(\frac{2\cdot 4+1}{2\cdot 4}\right)^2 = \left(\frac{9}{8}\right)^2 = \frac{81}{64} = [1;3,1,3,4] \\
k = 5 &\implies \left(\frac{2\cdot 5+1}{2\cdot 5}\right)^2 = \left(\frac{11}{10}\right)^2 = \frac{121}{100} = [1;4,1,3,5]
\end{aligned}$$

and we can easily prove that

$$\left(\frac{2k+1}{2k}\right)^2 = [1;k-1,1,3,k]$$

by using the Algorithm 1.1.2.1 and constructing the following table:

C.F.		1	$k-1$	1	3	k
N	1	1	k	$k+1$	$4k+3$	$4k^2+4k+1$
D	0	1	$k-1$	k	$4k-1$	$4k^2$

Ultimately, the limit approaches

$$\lim_{k\to+\infty} \frac{4k^2+4k+1}{4k^2} = \frac{4}{4} = 1$$

□

Definition 1.2.3.1: Relation

Given a set S, a **relation** R over S is a subset $R \subseteq S \times S$. Two members $a, b \in S$ are said to be **related** if and only if $(a,b) \in R$, also noted as

$$a \sim b$$

Definition 1.2.3.2: Equivalence relation

Given a set S and a relation R over it, R is said to be **equivalence relation** if and only if the following properties hold:

- **reflexive property**, i.e.
$$\forall x \in S \quad x \sim x$$
- **symmetric property**, i.e.
$$\forall x, y \in S \quad x \sim y \implies y \sim x$$
- **transitive property**, i.e.
$$\forall x, y, z \in S \quad x \sim y \wedge y \sim z \implies x \sim z$$

Definition 1.2.3.3: Congruence class

TODO

Definition 1.2.3.4: Modulus congruence

Given two numbers $a, b \in \mathbb{Z}$ and some $n \in \mathbb{N} - \{0\}$, we say that a **is congruent with** b **modulo** n if and only if n divides $a - b$. Using symbols

$$a \equiv b \pmod{n} \iff n \mid a - b \iff \exists k \in \mathbb{Z} \mid nk = a - b$$

Proposition 1.2.3.1: Modulus congruence equivalence relation

The modulus congruence is an equivalence relation.

Proof. Let $n \in \mathbb{N} - \{0\}$, to prove the statement, the following properties must hold:

- reflexive property, thus
$$\forall a \in \mathbb{Z} \quad a \equiv a \pmod{n} \iff n \mid a - a = 0 \iff \exists k \in \mathbb{Z} \mid nk = 0 \iff k = 0$$
and note that $0 \in \mathbb{Z}$;
- symmetric property, thus
$$\begin{gathered} \forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{n} \iff n \mid a - b \iff \\ \iff \exists k \in \mathbb{Z} \mid nk = a - b \iff -nk = b - a \iff n(-k) = b - a \iff \\ \exists - k \in \mathbb{Z} : n \mid b - a \iff b \equiv a \pmod{n} \end{gathered}$$
and note that $\forall k \in \mathbb{Z} \quad -k \in \mathbb{Z}$;

- transitive property, thus

$$\forall a,b,c \in \mathbb{Z} \quad \begin{cases} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{cases} \iff \begin{cases} n \mid a-b \\ n \mid b-c \end{cases} \iff \begin{cases} \exists k \in \mathbb{Z} \mid nk = a-b \\ \exists h \in \mathbb{Z} \mid nh = b-c \end{cases} \iff$$
$$\iff \begin{cases} b = a - nk \\ nh = a - nk - c \end{cases} \implies nh + nk = a - c \iff n(h+k) = a - c \iff$$
$$\iff \exists (k+h) \in \mathbb{Z} : n \mid a - c \iff a \equiv c \pmod{n}$$

□

Definition 1.2.3.5: Partition

Given a set S, a **partition** of S is a set of *mutually disjoint subsets of* S i.e. the subsets are non-empty and such that every element $x \in S$ is exactly in one of the subsets. Using symbols, given a set of indices I we have that

$$S = \bigsqcup_{i \in I} S_i \iff \forall i,j \in I \quad \begin{cases} S_i = S_j & i = j \\ S_i \cap S_j = \varnothing & i \neq j \end{cases}$$

Example 1.2.3.1 (Partitions)**.** TODO

Theorem 1.2.3.1: Equivalence relations and partitions

A partition induces an equivalence relation, and viceversa. Using symbols