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

Discrete Mathematics

Lecture notes integrated with the book "Discrete Mathematics",
Norman L. Biggs

Author
Simone Bianco

March 6, 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/Exyss/university-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: **bianco.simone@outlook.it**
- LinkedIn: **Simone Bianco**

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

Suggested prerequisites:

Preventive learning of material related to the *Algebra* course is recommended

Licence:

1

Introduction to number theory

1.1 Prime numbers

Observation 1: Natural numbers

In every following statement, we assume that $0 \notin \mathbb{N}$.

Definition 1: Divisor

Given two numbers $n, m \in \mathbb{N}$ we say that m **divides** n, noted with $m \mid n$, if and only if $\exists k \in \mathbb{N}$ such that $n = mk$.

$$m \mid n \iff \exists k \in \mathbb{N} : n = mk$$

Problem 1: Partial order of divisors

The relation of divisibility, that being $m \mid n$, is a **partial order over** $\mathbb{N}$, meaning that it's *reflective*, *anti-symmetric* and *transitive*.

Proof.

- For each number $n \in \mathbb{N}$, we have that $n = n \cdot 1$, so we conclude that $\forall n \in \mathbb{N};\ n \mid n$ and thus that the relation is *reflexive*.
- Suppose that we have $n \mid m$ and $m \mid n$, implying that $\exists k, h \in \mathbb{N}$ such that $n = mk$ and $m = nh$. Then, we have that:

  $$n = mk = (nh)k = nhk \iff k, h = 1$$

  concluding that $n = m$ and thus that the relation is *anti-symmetric*.

- Suppose that we have $n \mid m$ and $m \mid k$, implying that $\exists a, b \in \mathbb{N}$ such that $n = ma$ and $k = mb$. Then, we have that $k = mb = (na)b = nab \implies n \mid k$, thus the relation is *transitive*.

$\square$

Definition 2: Set of prime numbers

We define the **set of prime numbers**, noted with $\mathbb{P}$, as the set of natural numbers that have exactly two factors, that being the number 1 and itself.

$$\mathbb{P} = \{n \in \mathbb{N} \mid \nexists a, b \in \mathbb{N} - \{1, n\} : n = ab\}$$

Definition 3: Gratest Common Divisor

Given $n, m \in \mathbb{N}$, we define the **greatest common divisor** of n and m as the greatest number $d \in \mathbb{N}$ such that $d \mid n$ and $d \mid m$.

In other words, we have that:

$$\gcd(n, m) = d \iff \forall k \in \mathbb{N} : k \mid n, k \mid m \implies k \mid d$$

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

Examples:

- Given 15 and 63, we have that $\gcd(15, 63) = 3$.
- Given 15 and 62, we have that $\gcd(15, 62) = 1$, so 15 and 62 are coprime.

Algorithm 1: Eclid's algorithm

Given $n, m \in \mathbb{N}$, the following algorithm computes $\gcd(n, m)$.

function GCD(n, m)
    $a = n$
    $b = m$
    Find $q, r \in \mathbb{N}$ such that $a = bq + r$
    while $r \neq 0$ **do**
        $a = b$
        $b = r$
        Find $q, r \in \mathbb{N}$ such that $a = bq + r$
    end while
    return b
end function

(*proof omitted*)

Example:

We compute $\gcd(341, 527)$ using the algorithm:

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

Hence, we conclude that $\gcd(341, 527) = 31$

Lemma 1: Bézout's identity

Given $n, m \in \mathbb{N}$, it holds that:

$$\exists x, y \in \mathbb{Z} : ax + by = \gcd(n, m)$$

(*proof omitted*)

Example:

Through the computations of the previous example, we can find the values that satisfy Bézout's identity for 341 and 527:

$$\begin{aligned} 31 &= 186 - 155 \\ &= 186 - (341 - 186) \\ &= 2 \cdot 186 - 341 \\ &= 2 \cdot (527 - 341) - 341 \\ &= 2 \cdot 527 - 3 \cdot 341 \end{aligned}$$

Corollary 1: Prime divisors

Given $n \in \mathbb{N}$ and $p \in \mathbb{P}$, it holds that:

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

Proof.

First implication. Let $d := \gcd(n, p)$ and suppose that $d \neq 1$. Since $d \in \mathbb{N}$, if $d \neq 1$ then it must hold that $d > 1$.

By definition of gcd we have that $d \mid n$ and $d \mid p$. Then, since $p \in \mathbb{P}$, in order for $d \mid p$ to hold it must be true that $d = 1$ or $d = p$. However, since we assumed that $d > 1$, the only possibility is that $d = p$ and thus that $p \mid n$.

By contrapositive, we get that $p \nmid n \implies \gcd(n, p) = 1$.

Second implication. Let $d := \gcd(n, p)$ and suppose that $d = 1$. By definition of gcd we have that $d \mid n$ and $d \mid p$. Moreover, by reflexivity we have that $p \mid p$.

Suppose now by absurd that $p \mid n$. Then, since $p \mid n$ and $p \mid p$, by definition of gcd it must hold that $p \mid d = 1$. However, since $1 \mid p$ and $p \mid 1$, by anti-symmetry it must hold that $p = 1$, giving us the contradiction $1 \in \mathbb{P}$. Thus, it must be impossible that $p \mid n$.

$\square$

Lemma 2: Prime divisors

Given $n, m \in \mathbb{N}$ and $p \in \mathbb{P}$, it holds that:

$$p \mid nm \implies p \mid n \lor p \mid m$$

Proof.

Suppose that $p \mid nm$. If $p \mid n$ or $p \mid m$, we trivially conclude the result.

Consider now the case where $p \nmid n$, by the previous corollary and Bézout's identity, we have that:

$$p \nmid n \iff \gcd(n, p) = 1 \implies \exists x, y \in \mathbb{Z} : nx + py = 1 \iff mnx + mpy = m$$

Since $p \mid nm$, we know that $\exists k \in \mathbb{N} : nm = pk$, implying that:

$$m = mnx + mpy = pkx + mpy = p(x + my)$$

so we get that $p \mid m$.

By the same argument, if $p \nmid m$ we can conclude that $p \mid n$, so it holds that p must divide n or m in all cases.

$\square$

1.1.1 Unique prime factorization

Theorem 1: Fundamental Theorem of Arithmetic

Given $n \in \mathbb{N}$ such that $n \geq 2$, there exists an **unique prime factorization (UPF)** of n.

$$\exists! p_1, \ldots, p_k \in \mathbb{P} : p_1 \cdot \ldots \cdot p_k = n$$

Proof of existance.

We procede by strong induction on n

Base case. Given $n = 2$, we trivially have that $2 \in \mathbb{P}$, so n is its own prime factorization.

Strong inductive hypothesis. $\forall m \in \mathbb{N}$ such that $m \leq n$ it holds that:

$$\exists p_1, \ldots, p_k \in \mathbb{P} : p_1 \cdot \ldots \cdot p_k = m$$

Inductive step. Given $n+1$, if $n+1 \in \mathbb{P}$ then $n+1$ is its own prime factorization.

Suppose now that $n+1 \notin \mathbb{P}$. Then, by definition, there exists $a, b \in \mathbb{N} - \{1, n+1\}$ such that $n+1 = ab$. Since $a \mid n+1$ and $b \mid n+1$, it must hold that $a, b \leq n+1$. In particular, since $a, b \in \mathbb{N} - \{1, n+1\}$, we have that $a, b < n+1$, implying that $a, b \leq n$.

Then, by inductive hypothesis, we have that $\exists p_1, \ldots, p_k, q_1, \ldots, q_h \in \mathbb{P}$ such that $a = p_1 \ldots p_k$ and $b = q_1 \ldots q_h$. Thus, we conclude that $p_1 \ldots p_k q_1 \ldots q_h$ is the prime factorization of n.

□

Proof of uniqueness.

By way of contradiction, suppose that n has two prime factorizations $p_1 \ldots p_k$ and $q_1 \ldots q_h$:

$$p_1 \ldots p_k = n = q_1 \ldots q_h$$

Then, through the Lemma 2, for all $i \in [1, k]$ we have that:

$$p_i \mid p_1 \ldots p_k = q_1 \ldots q_h \implies p_i \mid q_1 \vee \ldots \vee p_i \mid q_h$$

Let $j \in [1, h]$ be the index such that $p_i \mid q_j$. Since $q_j \in \mathbb{P}$, it can hold that $p_i \mid q_j$ only if $p_i = q_j$. So, we conclude that $\forall i \in [1, k] \;\; \exists j \in [1, h] : p_i = q_j$.

By applying the same argument, we can show that $\forall j \in [1, h] \;\; \exists i \in [1, k] : q_j = p_i$, giving us a bijection between the two factorizations where, without loss of generality, we can assume that $p_1 = q_1, \ldots, p_k = q_h$.

□

Theorem 2: Euclid's theorem

The set of prime numbers is infinite, meaning that $|\mathbb{P}| = +\infty$.

Proof.

By way of contradiction, we suppose that $\mathbb{P} = \{p_1, \ldots, p_n\}$, meaning that there are a finite amount of prime numbers.

Consider the number $n = p_1 \cdot \ldots p_n + 1$. Since $n \notin \mathbb{P}$, meaning that it's a composite number. Then by the Fundamental Theorem of Arithmetic, there exists $q_1, \ldots, q_k \in \mathbb{P}$ such that $n = q_1 \ldots q_h$.

Given $i \in [1, h]$, we know that $q_i \in \mathbb{P}$, so $q_i \mid p_1 \ldots p_k$, implying that $\exists a \in \mathbb{N}$ such that $p_1 \ldots p_k = q_i a$. Then, we get that:

$$1 = p_1 \ldots p_k - n = q_i a - q_1 \ldots q_h = q_i(a - q_1 \ldots q_{i-1} q_{i+1} \ldots q_h)$$

so we get that $q_i \mid 1$. However, this can only be possible if $q_i = 1$, which would imply that $1 \in \mathbb{P}$, which is a contradiction. So, it must hold that $|\mathbb{P}| = +\infty$.

$\square$

1.2 Solved exercises

Problem 2

Let $S = \{4n - 3 \mid n \in \mathbb{N}\}$ and let $S_{\mathbb{P}} \subseteq S$ be the set of S-prime numbers, that being the numbers in S that have exactly two factors (1 and itself) in S.

1. Prove that S is closed under multiplication.
2. Are there infinitely many S-prime numbers?
3. Prove that $1617 \in S$ and find two different factorizations of 1617 into S-primes.
4. Find a few more examples of S-integers with more than one factorization.

Solution:

First, we formally define $S_{\mathbb{P}}$ as $S_{\mathbb{P}} = \{x \in S \mid \nexists a, b \in S - \{1, x\} : x = ab\}$. It's easy to notice that $\mathbb{P} \cap S \subseteq S_{\mathbb{P}}$, meaning that if a prime number is also in S then it's an S-prime number.

1. Given $(4a-3), (4b-3) \in S$, we show that:

$$(4a-3)(4b-3) = 16ab - 12a - 12b + 9 =$$
$$16ab - 12a - 12b + 12 - 3 = 4(4ab - 3a - 3b + 4) - 3$$

   Since $ab - 3a - 3b + 4 \in \mathbb{N}$, we conclude that $(4a-3)(4b-3) \in S$.

2. By way of contradiction, we suppose that $S_{\mathbb{P}}$ is finite, meaning that $S_{\mathbb{P}} = \{p_1, \dots, p_n\}$.

   Consider the number $q := 4p_1 \dots p_n - 3$. It's easy to see that $q \in S - S_{\mathbb{P}}$, meaning that q is S-composite and thus that $\exists p_i, p_j \in S_{\mathbb{P}}$ such that $p_i \mid q$ and $p_j \mid q$.

   Without loss of generality, we procede with p_i. By reflection, we have that $p_i \mid p_i$, which implies that $p_i \mid 4p_1 \dots p_n$. Then, since $p_i \mid 4p_1 \dots p_n$ and $p_i \mid q$, it must also divide their difference, which equals 3, implying that $p_i \mid 3$.

   Finally, since $p_i \mid 3$, it must hold that $p_i \leq 3$, implying that $p_i \in \{1, 2, 3\}$. However, if $p_i = 2$ or $p_i = 3$, that would imply that $2 \in S$ or $3 \in S$, which is a contradiction. By the same reasoning, p_i can't be equal to 1 since that would imply that $p_j = 3$ and that $3 \in S$, which is a contradiction. Thus, the set $S_{\mathbb{P}}$ must be infinite.

   Another way to prove this result is by showing that $\forall k \in \mathbb{N}$ it holds that $4 \cdot 2^k - 3 \in S_{\mathbb{P}}$. This can be easily done by way of contradiction. Moreover, this generator of infinite S-prime numbers can be extended to all primes, meaning that $\forall p \in \mathbb{P}$ and $\forall k \in \mathbb{N}$ it holds that $4p^k - 3 \in S_{\mathbb{P}}$.

3. It's easy to see that $1617 = 4 \cdot 405 - 3$, thus $1617 \in S$. We now consider the prime factorization $1617 = 3 \cdot 11 \cdot 7^2$, we notice that $1617 = 33 \cdot 49$ and $1617 = 21 \cdot 77$.

   Since $33 = 4 \cdot 9 - 3$, we get that $33 \in S$. However, since $33 = 3 \cdot 11$ and $3, 7 \notin S$, the number 33 must be S-prime. By the same reasoning, we can show that $49, 21, 77 \in S_{\mathbb{P}}$, giving us two different S-prime factorizations of 1617.

4. Following the structure of the previous example, we can simply replace one of the numbers that form the prime factorization of 1617 with another prime number that isn't in S:
   - The number $441 = 3 \cdot 3 \cdot 7^2 \in S$ can be rewritten as $441 = 9 \cdot 49 = 21 \cdot 21$, where $9, 21, 49 \in S_{\mathbb{P}}$.
   - The number $2789 = 3 \cdot 19 \cdot 7^2 \in S$ can be rewritten as $1029 = 57 \cdot 49 = 21 \cdot 133$, where $21, 57, 133 \in S_{\mathbb{P}}$.

Problem 3

Given the sequence $a_n := [2; 1, 4, n]$, where $n \in \mathbb{N}$, find the limit of the sequence as $n \to +\infty$.

Solution:

We show that:

		2	**1**	**4**	**n**
Num	1	2	3	14	$14n + 3$
Den	0	1	1	5	$5n + 1$

So we conclude that $[2; 1, 4, n] = \frac{14n+3}{5n+1}$. Thus, for $n \to +\infty$ we get that:

$$\lim_{n \to +\infty} a_n = \lim_{n \to +\infty} \frac{14n + 3}{5n + 1} = \lim_{n \to +\infty} \frac{n(14 + \frac{3}{n})}{n(5 + \frac{1}{n})} = \frac{14}{5}$$

Problem 4

Compute the continued fractions equivalent to the following expressions:

1. $\frac{25}{16}$
2. $\frac{49}{36}$
3. $\frac{81}{64}$
4. $\frac{11}{100}$

Can you spot the pattern in the continued fractions? What is the limit of this sequence? Does $\frac{9}{4}$ fit into that pattern too?

Solution:

First, we procede by computing the continued fractions of the given sequence:

1. Through Euler's algorithm we get that:

$$\begin{aligned} 25 &= 16 \cdot 1 + 9 \\ 16 &= 9 \cdot 1 + 7 \\ 9 &= 7 \cdot 1 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

   implying that $\frac{25}{16} = [1; 1, 1, 3, 2]$

2. Through Euler's algorithm we get that:

$$\begin{aligned} 49 &= 36 \cdot 1 + 13 \\ 36 &= 13 \cdot 2 + 10 \\ 13 &= 7 \cdot 1 + 2 \\ 10 &= 2 \cdot 3 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

   implying that $\frac{49}{36} = [1; 2, 1, 3, 3]$

3. Through Euler's algorithm we get that:

$$\begin{aligned} 81 &= 64 \cdot 1 + 17 \\ 64 &= 17 \cdot 3 + 13 \\ 17 &= 13 \cdot 1 + 4 \\ 13 &= 4 \cdot 3 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

   implying that $\frac{81}{64} = [1; 3, 1, 3, 4]$

4. Through Euler's algorithm we get that:

$$\begin{aligned} 121 &= 100 \cdot 1 + 21 \\ 100 &= 21 \cdot 4 + 16 \\ 21 &= 16 \cdot 1 + 5 \\ 16 &= 5 \cdot 3 + 1 \\ 5 &= 1 \cdot 5 + 0 \end{aligned}$$

   implying that $\frac{121}{100} = [1; 4, 1, 3, 5]$

The pattern of the computed continued fractions clearly seems to be $[1; n, 1, 3, n+1]$. In fact, it's easy to see that:

		1	**n**	**1**	**3**	**n + 1**
Num	1	1	$n+1$	$n+2$	$4n+7$	$(2n+3)^2$
Den	0	1	n	$n+1$	$4n+3$	$(2n+1)^2$

implying that $\forall n \in \mathbb{N}$ it holds that $[1; n, 1, 3, n+1] = \frac{(2n+3)^2}{(2n+2)^2}$. In particular, with the values $n = 1, 2, 3, 4$ we get exactly the results previously computed.

However, we cannot apply this patter to $\frac{9}{4} = [1; 0, 1, 3, 1]$ since 0 can't be a valid continued fraction value. In fact, we notice that:

$$\begin{aligned} 9 &= 4 \cdot 2 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

implying that $\frac{9}{4} = [2; 4]$, confirming that the pattern doesn't hold for $n = 0$.

In conclusion, we show that the limit of the sequence is equal to $\lim_{n \to +\infty} \frac{(2n+3)^2}{(2n+2)^2} = 1$.