



SAPIENZA
UNIVERSITÀ DI ROMA

“SAPIENZA” UNIVERSITÀ DI ROMA
INGEGNERIA DELL'INFORMAZIONE,
INFORMATICA E STATISTICA
DIPARTIMENTO DI INFORMATICA

Discrete Mathematics

TODO non so se scriverò qualcosa qui idk

Author
Alessio Bandiera

1 marzo 2024

Indice

Informazioni e Contatti	1
1 Number Theory	2
1.1 TODO	2
1.1.1 TODO	2

Informazioni e Contatti

Segnalazione errori ed eventuali migliorie:

Per segnalare eventuali errori e/o migliorie possibili, si prega di utilizzare il **sistema di Issues fornito da GitHub** all'interno della pagina della repository stessa contenente questi ed altri appunti (link fornito al di sotto), utilizzando uno dei template già forniti compilando direttamente i campi richiesti.

Gli appunti sono in continuo aggiornamento, pertanto, previa segnalazione, si prega di controllare se l'errore sia ancora presente nella versione più recente.

Licenza di distribuzione:

These documents are distributed under the [GNU Free Documentation License](#), a form of copyleft intended to be used on manuals, textbooks or other types of document in order to assure everyone the effective freedom to copy and redistribute it, with or without modifications, either commercially or non-commercially.

Contatti dell'autore e ulteriori link:

- Github: <https://github.com/aflaag>
- Email: alessio.bandiera02@gmail.com
- LinkedIn: [Alessio Bandiera](#)

1

Number Theory

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) $\exists \text{succ} : \mathbb{N} \rightarrow \mathbb{N}$, or equivalently, $\forall x \in \mathbb{N} \quad \text{succ}(x) \in \mathbb{N}$
- iii) $\forall x, y \in \mathbb{N} \quad x \neq y \implies \text{succ}(x) \neq \text{succ}(y)$
- iv) $\nexists x \in \mathbb{N} \mid \text{succ}(x) = 0$
- v) $\forall S \subseteq \mathbb{N} \quad (0 \in S \wedge (\forall x \in S \quad \text{succ}(x) \in S)) \implies S = \mathbb{N}$

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.

Problem 1.1.1.1: Cardinality of the power set

Show that for every given set S such that $n := |S|$ it holds true 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. $n = 0 \implies S = \emptyset \implies \mathcal{P}(S) = \mathcal{P}(\emptyset) = \{\emptyset\} \implies |\mathcal{P}(S)| = 1 = 2^0 = 2^n$.

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

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

□

Definition 1.1.1.2: Integers

TODO

Definition 1.1.1.3: Divisor

TODO

Esempio 1.1.1.1 (Divisors). TODO

Definition 1.1.1.4: \mathbb{P}

TODO

Proposition 1.1.1.1: \mathbb{P} is infinite

There are infinitely many primes. Using symbols

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

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

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

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

Problem 1.1.1.2: $n^2 + n$ is even

Show that $\forall n \in \mathbb{N} \quad n^2 + n$ is an even number.

Dimostrazione. 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 1.1.1.3: $4n - 1$ is not prime

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

Dimostrazione. 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:

$$f : \mathbb{N} \rightarrow \mathbb{N} : x \mapsto x^2$$

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

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

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

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

Esempio 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: $\gcd(a, b)$.

```

1: function GCD( $a, b$ )
2:   TODO
3: end function

```

Esempio 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

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

Dimostrazione. Omitted. □

Esempio 1.1.1.4 (Bézout's identities). Using the [Esempio 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 true that

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

Proof.

First direction. 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 p , which means that $p \mid n$.

Second direction. 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 impossible 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

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

Dimostrazione. 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

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

Dimostrazione. Omitted.

□

Problem 1.1.1.4: 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

Dimostrazione.

1. To show that S is closed under multiplication, it suffices to show that

$$\forall a, b \in \mathbb{N} \quad (4a - 3)(4b - 3) = 16ab - 12a - 12b + 9 = 4(ab - 3a - 3b + 3) - 3 \in S$$

2. TODO

□