

# Crittografia e Combinatoria

Amati Pierluigi

26 febbraio 2020

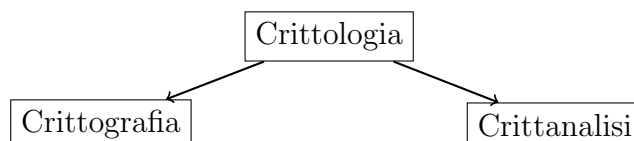
## Indice

<b>1</b>	<b>Introduzione</b>	<b>1</b>
<b>2</b>	<b>Teoria dei numeri</b>	<b>2</b>
2.1	Divisibilità . . . . .	2
2.2	Teorema dei numeri primi . . . . .	3
2.3	Teorema fondamentale dell'aritmetica . . . . .	3
2.3.1	Algoritmo Euclideo . . . . .	4
2.3.2	Identità di Bezout . . . . .	4
<b>3</b>	<b>Aritmetica Modulare</b>	<b>6</b>
3.1	Congruenze . . . . .	6

## 1 Introduzione

La **crittologia** è lo studio dei metodi per mantenere sicure le comunicazioni che avvengono in un canale *non sicuro*.

Essa si suddivide in **crittografia**, che studia la progettazione di tali metodi, e **crittanalisi**, che invece si occupa di infrangerli.



In generale in una comunicazione un messaggio  $\mathbf{m}$  viene cifrato all'origine attraverso un algoritmo di cifratura  $ENC$  e una chiave di cifratura  $\mathbf{k}$  e viene decifrato alla destinazione con un algoritmo di decifratura  $DEC$  (idealmente  $ENC^{-1}$ ) e una chiave di decifratura  $\mathbf{k}$ . L'algoritmo di cifratura è solitamente noto a tutte le parti, ma è la chiave ad essere segreta.

$$ENC(m, k) = c$$

$$DEC(c, k) = m$$

Ipotizzando una comunicazione tra Alice e Bob, dove entrambi possiedono le chiavi di cifratura, un soggetto esterno malintenzionato, Eve (a.k.a. Evil), potrebbe:

- leggere il messaggio;
- trovare la chiave e quindi decifrare tutti i messaggi scambiati tra Alice e Bob;
- alterare un messaggio in modo tale da far sembrare che sia effettivamente spedito da una delle due parti;
- fingersi una delle due parti.

**Tipologie di cifratura** Esistono principalmente due tipologie di cifratura:

- la cifratura **simmetrica**, in cui la chiave di cifratura è identica alla chiave di decifratura;
- la cifratura **asimmetrica**, in cui la chiave di cifratura (generalmente pubblica) è differente dalla chiave di decifratura (privata).

## 2 Teoria dei numeri

### 2.1 Divisibilità

**Definizione** Siano  $a, b \in \mathbb{Z}$ , con  $a \neq 0$ , si dice che  $a$  divide  $b$  ( $a \mid b$ ) se esiste  $k \in \mathbb{Z}$  tale che  $b = ak$ . In altre parole,  $b$  è un multiplo di  $a$ .

**Proprietà** (dimostrazioni<sup>1</sup>)

- $a \mid a$ ;
- $a \mid 0$ ;
- $1 \mid b$ ;
- se  $a \mid b$  e  $b \mid c$ , allora  $a \mid c$ ;
- se  $a \mid b$  e  $a \mid c$ , allora  $a \mid (sb + tc)$ , con  $s, t \in \mathbb{Z}$ .

**Esempi**

$$15 \mid 60, \quad 2 \mid 8, \quad 4 \nmid 15$$

## 2.2 Teorema dei numeri primi

Sia  $\Pi(x)$  la quantità di numeri primi  $< x$ , definita  $\Pi(x) \simeq \frac{x}{\ln(x)}$ ,

$$\Rightarrow \lim_{x \rightarrow \infty} \frac{\Pi(x) \ln(x)}{x}.$$

## 2.3 Teorema fondamentale dell'aritmetica

**Enunciato** Ogni numero  $n \in \mathbb{Z}$  è un prodotto di numeri primi.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

Si dice **fattorizzazione** la ricerca di tale insieme di numeri primi.

**Definizione** Si dice Massimo Comun Divisore tra  $a$  e  $b$ , il più grande numero intero che divide  $a$  e  $b$   $[\gcd(a, b)]$ .

**Definizione** Dati  $a, b \in \mathbb{Z}$ , essi si dicono **co-primi** se e solo se  $\gcd(a, b) = 1$ .

---

<sup>1</sup>[Trappe p.64]

### 2.3.1 Algoritmo Euclideo

Oltre al classico metodo di scomposizione in fattori primi, la ricerca del massimo comun divisore tra due numeri interi è possibile attraverso il cosiddetto Algoritmo Euclideo, di natura iterativa.

Supponendo di voler calcolare  $\gcd(r_0, r_1)$ , con  $r_0 > r_1$ , si può scrivere iterativamente:

$$r_0 = r_1 \cdot q_1 + r_2$$

$$r_1 = r_2 \cdot q_2 + r_3$$

$$r_2 = r_3 \cdot q_3 + r_4$$

$$\vdots$$

dove  $r_n$  e  $q_n$  sono rispettivamente il resto e il quoziente della divisione tra  $r_{n-1}$  e  $r_{n-2}$ .

$$\gcd(r_0, r_1) = r_n \Leftrightarrow r_{n+1} = 0$$

**Esempio** Si calcoli  $\gcd(1180, 482)$ :

$$1180 = 482 \cdot 2 + 216$$

$$482 = 216 \cdot 2 + 50$$

$$216 = 50 \cdot 4 + 16$$

$$50 = 16 \cdot 3 + 2$$

$$16 = 2 \cdot 8 + 0$$

Il resto appena precedente a  $r = 0$  è  $r = 2$ , quindi  $\gcd(1180, 482) = 2$ .

### 2.3.2 Identità di Bezout

**Enunciato** Siano  $a, b \in \mathbb{Z}$ , dove almeno uno tra  $a$  e  $b$  è diverso da 0  $\Rightarrow \exists x, y \in \mathbb{Z} : ax + by = \gcd(a, b)$ .

Per individuare i valori  $x, y$  che soddisfano l'identità di Bezout, si scrivono le espressioni dei resti a partire dalle iterazioni dell'algoritmo Euclideo

$$r_n = r_{n-2} - r_{n-1} \cdot q_{n-1}$$

e si sostituiscono a ritroso, svolgendo i calcoli, fino ad arrivare alla prima iterazione. In riferimento al  $\gcd(1180, 482)$ , bisogna trovare i valori  $x, y$  :  $1180x + 482y = \gcd(1180, 482) = 2$ :

$$216 = 1180 - 482 \cdot 2$$

$$50 = 482 - 216 \cdot 2$$

$$16 = 216 - 50 \cdot 4$$

$$2 = 50 - 16 \cdot 3$$

Si parte quindi dall'ultima identità  $2 = 50 - 16 \cdot 3$ , con l'obiettivo di ottenere nel membro di destra un'espressione del tipo  $1180x + 482y$ , sostituendo i valori delle costanti note dalle iterazioni precedenti:

$$2 = 50 - 3 \cdot (216 - 50 \cdot 4) = 50 - 3 \cdot 216 + 12 \cdot 50 = 13 \cdot 50 - 3 \cdot 216$$

$$2 = 13 \cdot (482 - 216 \cdot 2) - 3 \cdot 216 = 13 \cdot 482 - 26 \cdot 216 - 3 \cdot 216 = 13 \cdot 482 - 29 \cdot 216$$

$$2 = 13 \cdot 482 - 29 \cdot (1180 - 482 \cdot 2) = 13 \cdot 482 - 29 \cdot 1180 + 58 \cdot 482$$

$$\Rightarrow -1180 \cdot 29 + 482 \cdot 71 = 2$$

$$\Rightarrow (x, y) = (-29, 71)$$

In alternativa è possibile utilizzare il seguente algoritmo iterativo, dove  $q_n$  è l' $n$ -esimo quoziente dell'algoritmo Euclideo con  $r_{n+1} \neq 0$ :

$$y_0 = 0$$

$$y_1 = 1$$

$$y_n = -q_{n-1} \cdot y_{n-1} + y_{n-2}$$

da cui si ottiene, nell'esercizio in esame:

$$y_0 = 0$$

$$y_1 = 1$$

$$y_2 = -2$$

$$y_3 = -2 \cdot (-2) + 1 = 5$$

$$y_4 = -4 \cdot 5 - 2 = -22$$

$$y_5 = -3 \cdot (-22) + 5 = 71$$

$$\Rightarrow y = 71$$

Si ha quindi  $1180 \cdot x + 482 \cdot 71 = 2$ , da cui si ricava  $x = -29$ .

**Esercizio** Individuare  $x, y : 1234x + 1111y = \gcd(1234, 1111)$ .

## 3 Aritmetica Modulare

### 3.1 Congruenze

**Teorema** Siano  $a, b \in \mathbb{Z}, N \in \mathbb{N} \setminus \{0\}$ , si dice che  $a \equiv b \pmod{N} \Leftrightarrow \exists k \in \mathbb{Z} : a - b = kN$ , cioè se e solo se  $a - b$  è un multiplo di  $N$ .

**Proprietà** Siano  $a, b, c \in \mathbb{Z}, N \in \mathbb{N} \setminus \{0\}$ :

- $a \equiv 0 \pmod{N} \Leftrightarrow N \mid a$ , cioè se  $a = kN$ ;
- $a \equiv a \pmod{N}$ , cioè per  $k = 0$ ;
- $a \equiv b \pmod{N} \Leftrightarrow b \equiv a \pmod{N}$ , cioè per  $k_1 = -k_2$ ;
- $a \equiv b \pmod{N}, b \equiv c \pmod{N} \Rightarrow a \equiv c \pmod{N}$ , cioè per  $k_3 = k_1 - k_2$ .

In altre parole, sia  $a \in \mathbb{Z}$  un numero divisibile per  $N$ , esso si può scrivere come:

$$a = kN + r$$

con  $k \in \mathbb{Z}$ , dove  $0 \leq r < N$  è il resto della divisione per  $N$ . Si dice quindi che due numeri  $a, b$  sono congruenti se e solo se hanno lo stesso resto se divisi per  $N$ .

$$a = q_1 \cdot N + r$$

$$b = q_2 \cdot N + r$$

$$a - b = (q_1 - q_2) \cdot N$$

$$a - b = kN \Rightarrow a \equiv b \equiv r \pmod{N}$$