Crittografia e Combinatoria

Amati Pierluigi

27 febbraio 2020

Indice

1 Introduzione **2**

2 Teoria dei numeri **4**

2.1 Divisibilità 4

2.2 Teorema dei numeri primi 4

2.3 Teorema fondamentale dell'aritmetica 4

2.3.1 Algoritmo Euclideo 5

2.3.2 Identità di Bezout 5

3 Aritmetica Modulare **7**

3.1 Congruenze 7

3.2 Divisione in $\mathbb{Z}_N$ 8

3.3 Gruppi 8

Capitolo 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.

$$\begin{tikzcd}
& \boxed{\text{Crittologia}} \arrow[dl] \arrow[dr] & \\
\boxed{\text{Crittografia}} & & \boxed{\text{Crittanalisi}}
\end{tikzcd}$$

In generale in una comunicazione un messaggio $\mathbf{m}$ viene cifrato all'origine attraverso un algoritmo di cifratura ENC e una chiave di cifratura $\boldsymbol{k}$ e viene decifrato alla destinazione con un algoritmo di decifratura DEC (idealmente ENC^{-1}) e una chiave di decifratura $\boldsymbol{k}$. 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).

Capitolo 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[1])

- $a \mid a$;
- $a \mid 0$;
- $1 \mid b$;
- 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 $\Pi(x) \simeq \frac{x}{\ln(x)}$,

$$\Rightarrow \lim_{x \to \infty} \frac{\Pi(x) \ln(x)}{x} = 1.$$

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.

[1] [Trappe p.64]

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* $gcd(a,b) = 1$.

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 $r_{n+1} \neq 0$:

$$y_0 = 0$$
$$y_1 = 1$$
$$y_n = -q_{n-1} \cdot y_{n-1} + y_{n-1}$$

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 $x, y : 1234x + 1111y = gcd(1234, 1111)$.

Capitolo 3

Aritmetica Modulare

3.1 Congruenze

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

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

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

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

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

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

$$a - b = kN \Rightarrow a \equiv b \equiv r \mod N$$

Definizione *Si denota con $\mathbb{Z}_N$ l'insieme di tutti i possibili resti in una divisione per N*

$$\mathbb{Z}_N = \{0, 1, 2, \cdots, N - 1\}$$

Lemma *Siano* $a, b, c, d \in \mathbb{Z}, N \in \mathbb{N} \setminus \{0\} : a \equiv b, c \equiv d \mod N$

$$\Rightarrow a + c \equiv b + d, \quad a - c \equiv b - d, \quad a \cdot c \equiv b \cdot d \mod N$$

per dimostrarlo si utilizzi la definizione di congruenza $a = b + kN$.

Vale inoltre, dalla regola della moltiplicazione $a \cdot c \equiv b \cdot d \mod N$*,*

$$a^k \equiv b^k \mod N.$$

3.2 Divisione in $\mathbb{Z}_N$

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

- $ab \equiv ac \mod aN \Rightarrow b \equiv c \mod N$, poiché se

$$ab \equiv ac \mod aN \Rightarrow \exists k \in \mathbb{Z} : ab = kaN + ac \Rightarrow b = kN + c$$

$$\Rightarrow b \equiv c \mod N$$

- $ab \equiv ac \mod N, gcd(a, N) = 1 \Rightarrow b \equiv c \mod N$, poiché se

$$gcd(a, N) = 1 \Rightarrow \exists x, y \in \mathbb{Z} : ax + Ny = 1,$$

  si moltiplichi l'equazione per $(b - c)$, ottenendo:

$$(ab - ac)y + n(b - c)y = b - c$$

  dato che per ipotesi $(ab-ac)$ è un multiplo di N, e osservando che $N(b-c)y$ è un multiplo di N, si deduce che anche $b - c$ è un multiplo di N.

$$\Rightarrow b \equiv c \mod N.$$

3.3 Gruppi

Definizione *Definito un insieme* $\mathbb{G} \neq \{\emptyset\}$ *e un'operazione* $*$ *tale che* $\forall a, b \in \mathbb{G} \Rightarrow a * b \in \mathbb{G}$*, la struttura* $(\mathbb{G}, *)$ *si dice* ***gruppo*** *se:*

- $\exists e \in \mathbb{G} : a * e = e * a = a, \quad \forall a \in \mathbb{G};$
- $\exists b \in \mathbb{G} : a * b = b * a = e, \quad \forall a \in \mathbb{G};$
- $(a * b) * c = a * (b * c), \quad \forall a, b, c \in \mathbb{G}.$

Definizione *Un gruppo* $(\mathbb{G}, *)$*, si dice* ***Abeliano****, o* ***commutativo*** *se:*

- $a * b = b * a, \quad \forall a, b \in \mathbb{G}.$

Lemma $(\mathbb{Z}_N, +)$ *è un gruppo Abeliano.*

Lemma $(\mathbb{Z}_N \setminus \{0\}, \cdot)$ *è un gruppo* $\Leftrightarrow N$ *è primo.*

Esempi Per verificare se una struttura $(\mathbb{G}, *)$ sia un gruppo, è sufficiente applicare l'operazione considerata a tutte le possibili combinazioni degli elementi appartenenti all'insieme $\mathbb{G}$.

N.B. Nel caso di insiemi $\mathbb{Z}_N$ tutte le operazioni vanno effettuate in $\mod N$.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Nella tabella si è scelto $\mathbb{Z}_6$ con l'operazione di addizione $\mod 6$, con $e = 0$. Per ogni a appartenente all'insieme, esiste b tale che $a + b = b + a = e = 0$, e inoltre $a + e = e + a = a$.

$$\Rightarrow (\mathbb{Z}_6, +) \text{ \emph{è un gruppo.}}$$

·	1	2	3
1	1	2	3
2	2	1	3
3	3	3	3

In questo caso si è scelta la struttura $(\mathbb{Z}_4 \setminus \{0\}, \cdot)$, dove $N = 4$ non è primo. Il valore e tale che $a \cdot e = e \cdot a = a$ è 1. La seconda proprietà invece non è rispettata, poiché non esiste nessun numero appartenente all'insieme che moltiplicato per 3, dà come risultato $e = 1$.

$$\Rightarrow (\mathbb{Z}_4 \setminus \{0\}, \cdot) \text{ \emph{non è un gruppo.}}$$