Crittografia

Indice

1 Lezione 1 - 26/09/2023

1.1 Una suddivisione approssimativa della Matematica

Matematica delle grandezze continue

- Analisi
- Geometria
- Meccanica

Matematica delle grandezze discrete

- Aritmetica
- Algebra
- Combinatoria

1.2 Gruppi ciclici finiti: l'equazione $z^n = 1$

Sia n un intero positivo fissato. Consideriamo l'insieme $\mathcal{U}_n$ delle soluzioni complesse dell'equazione $z^n = 1$. È facile vedere che le radici sono distinte.

Teorema 1

Un polinomio ha radici distinte sse è primo con la sua derivata

$f(z) = z^n - 1 \implies f'(z) = nz^{n-1}$ e quindi i polinomi f ed f' non hanno fattori comuni.

Per il Teorema fondamentale dell'algebra, $|\mathcal{U}_n| = n$

Gli elementi di $\mathcal{U}_n$ sono disposti ai vertici del poligono regolare con n lati, il centro nell'origine ed un vertice in $z = 1$.

Poniamo

$$\delta_n = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i\,\sin\left(\frac{2\pi}{n}\right) = \cos(\theta_n) + i\,\sin(\theta_n)$$

dove

$$i^2 = -1 \quad \text{e} \quad \theta_n = \frac{2\pi}{n}$$

Osserviamo che:

$$\delta_n^n = e^{2\pi i} = 1$$

Le n soluzioni dell'equazione sono

$$z_j = \delta_n^j = e^{2\pi ij/n} \qquad \text{per } j = 0, \ldots, n-1$$

$$\delta_n^j \cdot \delta_n^k = \begin{cases} \delta_n^{j+k} & \text{se } j+k < n \\ \delta_n^{j+k-n} & \text{se } j+k \geq n \end{cases}$$

$$\delta_n^{-j} = (\overline{\delta_n})^j = \begin{cases} \delta_n^{n-j} & \text{se } j \neq 0 \\ \delta_n^0 = 1 & \text{se } j = 0 \end{cases}$$

Se $m = q \cdot n + r$ dove $0 \leq r < n$ allora

$$\delta_n^m = \delta_n^{qn+r} = (\delta_n^n)^q \cdot \delta_n^r = 1^q \cdot \delta_n^r = \delta_n^r$$

Le soluzioni si possono classificare a seconda di quale sia il più piccolo poligono regolare su cui giacciono, cioè il loro periodo (la potenza da applicare per ottenere 1).

Es. δ_{12}^8 è di ordine 3. Infatti $(\delta_{12}^8)^3 = \delta_{12}^{24} = \delta_{12}^0 = 1$

Alcune soluzioni di $z^n = 1$ soddisfano anche $z^k = 1$ per qualche k intero positivo con $k < n$

1.3 Ordine di un elemento di $\mathcal{U}_n$

L'ordine di $z \in \mathcal{U}_n$ è il minimo intero positivo m per cui $z_m = 1$

E' il minimo periodo della successione

$$1, z, z^2, z^3, \dots, z^{n-1}, z^n = 1, z^{n+1} = z, \dots$$

m non può superare n.

Definizione 1

Diciamo che un intero m divide un intero n se esiste un intero a t.c. $n = m \cdot a$. In questo caso scriviamo $m|n$

Esempio 1

Con questa definizione si ha:

$$\begin{cases} 1|n & \forall n \in \mathbb{Z} \\ n|0 & \forall n \in \mathbb{Z} \\ 0|n & \iff n = 0 \end{cases}$$

L'ordine m di $z \in \mathcal{U}_n$ è un divisore di n: se $z^n = 1$ e $z^m = 1$, allora $n = q \cdot m + r$ con $0 \leq r < m$ da cui

$$z^n = z^{qm+r} = (z^m)^q \cdot z^r = z^r = 1$$

che è assurdo se $r > 0$. L'unica possibilità è che $r = 0$.

Se l'ordine di $z \in \mathcal{U}_n$ è n, si dice che z è un generatore poiché le sue potenze successive sono distinte e forniscono tutti gli elementi di $\mathcal{U}_n$.

Infatti, se esistessero j e k con $0 \leq j < k < n$ t.c.

$$z^j = z^k \implies z^{k-j} = 1 \quad \text{ma } 1 \leq k - j < n$$

che è assurdo.

Dunque gli n elementi indicati sono tutti e soli gli elementi di $calU_n$.

Se z non è un generatore, questo non accade.

Definizione 2: Sottogruppo di un elemento di $\mathcal{U}_n$

Dato $z \in \mathcal{U}_n$ indicheremo con $\langle z \rangle$ il sottoinsieme $\{1, z, z^2, z^3, \dots\} \subseteq \mathcal{U}_n$ e lo chiameremo sottogruppo generato da z.

Teorema 2: Teorema (Lagrange)

La cardinalità di $\langle z \rangle$ è uguale all'ordine di z ed è un divisore della cardinalità di $\mathcal{U}_n$ che è n

Gli insiemi $\mathcal{U}_n$ con n primo sono speciali!

Infatti, in questo caso l'ordine di un elemento $z \in \mathcal{U}_n$ può essere solamente 1 o n stesso

Ma solo $z = 1$ ha ordine 1, dunque tutti gli altri elementi di $\mathcal{U}_n$ hanno ordine n e sono perciò generatori di $\mathcal{U}_n$

Esempio 2

Dato che $z_7^{12} = 1$, le potenze successive di z_7 sono invece

$$\begin{array}{cccc} z_7^0 = z_0 & z_7^1 = z_7 & z_7^2 = z_2 & z_7^3 = z_9 \\ z_7^4 = z_4 & z_7^5 = z_{11} & z_7^6 = z_6 & z_7^7 = z_1 \\ z_7^8 = z_8 & z_7^9 = z_3 & z_7^{10} = z_{10} & z_7^{11} = z_5 \end{array}$$

cioè abbiamo trovato un modo per rimescolare gli elementi di $\mathcal{U}_n$

Osserviamo che tutti gli elementi di $\mathcal{U}\backslash\{1\}$ sono generatori e dunque la successione $(\delta_{11}^a)^n$ ha periodo 11 per ogni $a \in \{1, 2, \ldots, 10\}$. Cioè, i resti di $a, 2a, 3a, \ldots$ divisi per 11 hanno periodo 11

1.4 L'algoritmo di Euclide

Definizione 3

Dati due interi n ed m non entrambi nulli, indichiamo con (n, m) il loro massimo comune divisore.

$$(n, m) = max\{d \in \mathbb{N} : d|n \quad \wedge \quad d|m\}$$

Se $z \in \mathcal{U}_n \cap \mathcal{U}_m$ (cioè se $z^n = z^m = 1$) allora

$$z^{\lambda n + \mu m} = (z^n)^\lambda \cdot (z^m)^\mu = 1 \qquad \forall \lambda, \mu \in \mathbb{Z}$$

Quindi $z^{(n,m)} = 1$

Questo fatto segue dall'algoritmo di Euclide: dati due interi n e m, dimostreremo che l'insieme $\{\lambda n + \mu m : \lambda, \mu \in \mathbb{Z}\}$ coincide con l'insieme dei multipli di $d = (n, m)$

Esempio 3

Se $z^{51} = z^{120} = 1$ allora

$$\begin{aligned} 120 &= 2 \cdot 51 + 18 \quad &\Longrightarrow \quad 1 = z^{120} = (z^{51})^2 \cdot z^{18} = z^{18} \\ 51 &= 2 \cdot 18 + 15 \quad &\Longrightarrow \quad 1 = z^{51} = (z^{18})^2 \cdot z^{15} = z^{15} \\ 18 &= 1 \cdot 15 + 3 \quad &\Longrightarrow \quad 1 = z^{18} = (z^{15})^1 \cdot z^3 = z^3 \\ 15 &= 5 \cdot 3 + 0 \end{aligned}$$

Come ricavare i coefficienti 3 e -7 per cui $(51, 120) = 3 = 3 \cdot 120 - 7 \cdot 51$?

$$\begin{aligned} 18 = 1 \cdot 15 + 3 \quad &\Longrightarrow \quad 3 = 18 - 15 \\ 51 = 2 \cdot 18 + 15 \quad &\Longrightarrow \quad 3 = 18 - (51 - 2 \cdot 18) \\ 120 = 2 \cdot 51 + 18 \quad &\Longrightarrow \quad 3 = (120 - 2 \cdot 51) - (51 - 2 \cdot (120 - 2 \cdot 51)) \\ &\qquad\qquad\quad = 120 - 2 \cdot 51 - 51 + 2 \cdot 120 - 4 \cdot 51 \\ &\qquad\qquad\quad = 3 \cdot 120 - 7 \cdot 51 \end{aligned}$$

Mio codice Python che implementa l'algoritmo di Euclide.

Domanda 1: Quali sono i generatori di $\mathcal{U}_n$?

I generatori di $\mathcal{U}_n$ sono gli elementi di ordine n, cioè quegli elementi $z \in \mathcal{U}_n$ tali che le loro potenze successive $z^0, z^1, z^2, \ldots, z^{n-1}$ sono tutte distinte e coincidono con tutti gli elementi di $\mathcal{U}_n$.

Domanda 2: Quanti sono i generatori di $\mathcal{U}_n$?

Il numero di generatori di $\mathcal{U}_n$ è uguale al numero di interi k con $1 \leq k \leq n-1$ tali che $(k, n) = 1$, cioè $\phi(n)$ dove ϕ è la funzione di Eulero.

Domanda 3: Dato un generatore di $\mathcal{U}_n$, come si trovano tutti gli altri?

Se g è un generatore di $\mathcal{U}_n$, allora tutti i generatori sono esattamente gli elementi della forma g^k dove $1 \leq k \leq n-1$ e $(k, n) = 1$.

1.5 Gruppi

Definizione 4

L'insieme G si dice gruppo rispetto all'operazione $\circ$ se

- $\forall g, h \in G : g \circ h \in G$
- $\exists e \in G : \forall g \in G : g \circ e = e \circ g = g$
- $\forall g \in G : \exists h \in G : g \circ h = h \circ g = e$
- $\forall g, h, j \in G : (g \circ h) \circ j = g \circ (h \circ j)$

L'elemento e si dice elemento neutro o unità di G.
L'elemento h si dice inverso o reciproco di g e si indica con g^{-1}.
Un sottoinsieme $H \subseteq G$ che sia a sua volta un gruppo rispetto all'operazione $\circ$ si dice sottogruppo di G.

Definizione 5

Sia G un gruppo rispetto all'operazione $\circ$

- se $g \circ h = h \circ g \forall g, h \in G$ il gruppo si dice abeliano o commutativo
- se $\exists g \in G : G = \langle g \rangle$ allora G si dice ciclico

In questo caso definiamo $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$
La definizione alternativa è necessaria quando G è infinito

L'insieme $\mathcal{U}_n$ è un gruppo abeliano ciclico rispetto alla moltiplicazione, ed è generato da δ_n

L'insieme $\mathcal{U}_m$ ne è un sottogruppo sse $m|n$, ed è generato da $\delta_n^{n/m} = \delta_m$

Esempio 4

L'insieme $\mathbb{Z}$ è un gruppo ciclico infinito generato da $g \in \{\pm 1\}$

Problema:

Se $G = \langle g \rangle$ e $card(G) = n$, quante soluzioni ha $x^d = 1$? (d *fissato*)

Se x è una soluzione, sia $x = g^m$ per un intero $m \in \{0, \dots, n-1\}$
L'equazione diventa $g^{md} = 1$ e da questo segue che $n|md$
Dividendo per (n, d) si ha $\frac{n}{(n,d)}|m$ e il numero di $m \in \{0, \dots, n-1\}$ che la soddisfano è (n, d).

Esempio 5

Risolvere $x^4 = 1$ in $\mathcal{U}_{12}$.

$$\begin{cases} m \in \{0, 1, \dots, 11\} \\ g^{4m} = 1 \\ g^{12} = 1 \end{cases} \implies 12|4m \implies 3|m \implies m \in \{0, 3, 6, 9\}$$

Risolvere $x^4 = 1$ in $\mathcal{U}_6$.

$$\begin{cases} m \in \{0, 1, \dots, 5\} \\ g^{4m} = 1 \\ g^{6} = 1 \end{cases} \implies 6|4m \implies 3|2m \implies m \in \{0, 3\}$$

1.6 Isomorfismi fra gruppi

Definizione 6

Siano G e G' due gruppi, con operazione $\circ$ e $*$ rispettivamente.
Un'applicazione biiettiva $\phi : G \to G'$ si dice isomorfismo se

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \forall x, y \in G$$

Esempio 6

Posto $G = \mathbb{R}^+$ con l'operazione di moltiplicazione e $G' = \mathbb{R}$ con l'operazione di addizione, un isomorfismo è la funzione $\phi(x) = log(x)$. Infatti: $log(x \cdot y) = log(x) + log(y)$

Un isomorfismo non è un'uguaglianza e ciò ha delle conseguenze computazionali. Certi insiemi non sono adatti alla crittografia, ma degli insiemi a loro isomorfi sì.

Gli isomorfismi sono invertibili, ma ciò non significa che le operazioni coinvolte abbiano la stessa complessità computazionale.

Esempio 7

Dato $\phi : \mathbb{R}^+ \to \mathbb{R}$ dell'esempio precedente, l'inverso $\psi : \mathbb{R} \to \mathbb{R}^+$ è l'esponenziale.
$\phi \circ \psi$ è l'identità su $\mathbb{R}$ e $\psi \circ \phi$ è l'identità su $\mathbb{R}^+$

2 Lezione 2 - 27/09/2023