Questo fascicolo contiene
la lezione di martedì 14 maggio 2019

Gli argomenti sono:

- Considerazioni generali sulle congruenze ed i gruppi di resti
- Esercizi (R.S.A. ed El Gamal, del tipo di quelli che avrete nel compito d'esame)

R.S.A.

$p = 31, \quad q = 47$

$n = pq = 31 \cdot 47 = 1457$

$$\begin{array}{r} 47 \\ 31 \\ \hline 47 \\ 141 \\ \hline 1457 \end{array}$$

$\varphi(n) = 30 \cdot 46 = 1380 = 6 \cdot 5 \cdot 2 \cdot 23 = 2^2 \cdot 3 \cdot 5 \cdot 23$

$e = 17$. Chi è d?

$ed \equiv 1 \ (\varphi(n))$, per noi $17d \equiv 1 (1380)$

$1380 = 17 \cdot 81 + 3$

$17 = 3 \cdot 5 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$ da cui

$$\begin{array}{r|l} 1380 & 17 \\ \hline 020 & 81 \\ 3 & \end{array}$$

$$\begin{array}{r} 17 \\ 81 \\ \hline 17 \\ 136 \\ \hline 1377 \end{array}$$

$1 = 3 - 2 = 3 - (17 - 3 \cdot 5) =$

$= 3 \cdot 6 - 17 = (1380 - 17 \cdot 81)6 - 17 =$

$= (1380) \cdot 6 - 17(6 \cdot 81 + 1) = (1380) \cdot 6 - 17(486 + 1)$

$= (1380) \cdot 6 - 17(487)$

verifica

$$\begin{array}{r} 1380 \\ 6 \\ \hline 8280 \end{array} \qquad \begin{array}{r} 487 \\ 17 \\ \hline 3409 \\ 487 \\ \hline 8279 \end{array}$$

giusto

dunque $d \equiv -487 \equiv 1380 - 487 = 893 \pmod{1380}$

$$\boxed{d = 893}$$

– decryption – key minima

$$\varphi_1(n) = \frac{(p-1)(q-1)}{(p-1,q-1)} = \frac{30\cdot 46}{(30,46)} = \frac{30\cdot 46}{2} =$$

$$= 30\cdot 23 = 690$$

$e d_1 \equiv 1\,(\varphi_1(n))$, per noi $17 d_1 \equiv 1\,(690)$

$690 = 17\cdot 40 + 10$

$17 = 10\cdot 1 + 7$

$10 = 7\cdot 1 + 3$

$7 = 3\cdot 2 + 1$ da cui

$3 = 1\cdot 3 + 0$

$$\begin{array}{r|l} 690 & 17 \\ \hline 10 & 40 \end{array}$$

$$1 = 7 - 3\cdot 2 = 7 - 2(10-7) = 3\cdot 7 - 2\cdot 10 =$$

$$= 3(17-10) - 2\cdot 10 = 3\cdot 17 - 5\cdot 10 =$$

$$= 3\cdot 17 - 5(690 - 17\cdot 40) =$$

$$= 17(3 + 5\cdot 40) - 5\cdot 690 =$$

$$= 17\cdot(203) - 5\cdot 690$$

Verifica

$$\begin{array}{r} 203 \\ 17 \\ \hline 1421 \\ 203 \\ \hline 3451 \end{array} \qquad \begin{array}{r} 690 \\ 5 \\ \hline 3450 \end{array}$$

giusto, quindi $\boxed{d_1 = 203}$

– Cifrate il messaggio $M=7$.

Si ha $C \equiv M^e (n)$, per noi $C \equiv 7^{17} (1457)$

Si ha

$7^1 \equiv 7 \ (1457)$

$7^2 \equiv 49$

$7^4 \equiv 2401 \equiv 944 \equiv -513 \ (1457)$

$7^8 \equiv (513)^2 \equiv 909 \ (1457)$

$7^{16} \equiv (909)^2 \equiv 162 \ (1457)$

$7^{17} \equiv 162 \cdot 7 = 1134 \ (1457)$

Dunque

$\boxed{C = 1134}$

El Gamal

Bob ha un crittosistema di El Gamal con

$$p = 53,\quad g = 2,\quad \beta \equiv g^a = 2^{17} \equiv 3 \ (53)$$

con $a = 17$ come chiave segreta

$$\left(\begin{array}{l} 2^1 \equiv 2 \ (53) \\ 2^2 \equiv 4 \\ 2^4 \equiv 16 \\ 2^8 \equiv 256 \equiv 44 \equiv -9 \ (53) \\ 2^{16} \equiv 81 \equiv 28 \equiv -25 \ (53) \\ 2^{17} \equiv 56 \equiv 3 \ (53) \end{array}\right)$$

$$\begin{array}{r|l} 256 & 53 \\ \hline 44 & 4 \end{array}$$

$(p, g, \beta) = (53, 2, 3)$ chiave pubblica El Gamal di Bob

$a = 17$ chiave segreta

Alice manda a Bob il messaggio $M = 13$ con parametro di mascheratura $k = 9$. Qual è il cifrato $(\gamma, \delta) = C$ che Alice riceve?

Ricordiamo che

$(p, g, \beta) = (53, 2, 3)$ chiave pubblica di Bob.

e $\begin{cases} \gamma \equiv g^k \ (p) \\ \delta \equiv M \beta^k \ (p) \end{cases}$ per noi $\begin{array}{l} \gamma \equiv 2^9 \ (53) \\ \delta \equiv 13 \cdot 3^9 \ (53) \end{array}$

Calcoliamo γ.

Si ha $2^8 \equiv 44 \equiv -9 \ (53)$ e quindi $2^9 \equiv 88 \equiv 35 \ (53)$

$$\boxed{\gamma = 35}$$

Calcoliamo δ. Si ha

$3^1 \equiv 3\ (53)$

$3^2 \equiv 9$

$3^4 \equiv 81 \equiv 28\ (53)$

$3^8 \equiv 784 \equiv 42 \equiv -11\ (53)$

$3^9 \equiv -33 \equiv 20\ (53)$

$\boxed{\beta^k = 20}$

$$\begin{array}{l|l} 28 \cdot 28 = 784 & 53 \\ 254 & 14 \\ 42 & \end{array}$$

$\delta \equiv 13 \cdot 20 \equiv 260 \equiv -5 \equiv 48\ (53)$

Dunque Bob riceve $(\gamma, \delta) = (35, 48) = C$

Decifriamo

Siccome $\gamma \equiv g^k\ (p)$ e $\delta \equiv M\beta^k \equiv m g^{ak}\ (p)$

si tratta di calcolare $(g^{ak})^{-1}\ (\mathrm{mod}\ p)$.

Dato che per noi $g=2, a=17, k=9$ e $p=53$, dobbiamo calcolare l'inverso moltiplicativo di $2^{(17)(9)} = 2^{153}\ (\mathrm{mod}\ 53)$.

Ma $2^{52} \equiv 1\ (\mathrm{mod}\ 53)$ (Eulero-Fermat) e quindi $2^{156} \equiv 1\ (\mathrm{mod}\ 53)$. Ma $2^{156} = 2^{153} \cdot 2^3 \equiv 1\ (\mathrm{mod}\ 53)$.

Basta quindi calcolare $(2^3)^{-1} = (8^{-1})\ \mathrm{mod}\ 53$.

Si ha $53 = 8 \cdot 6 + 5$ da cui segue

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$1 = 3 - 2 = 3 - (5-3) = 2 \cdot 3 - 5 =$

$= 2(8-5) - 5 = 2 \cdot 8 - 3 \cdot 5 =$

$= 2 \cdot 8 - 3(53 - 8 \cdot 6) =$

$= 20 \cdot 8 - 3 \cdot 53$

e quindi $2^{153} \equiv 20\ (\mathrm{mod}\ 53)$ e $(2^{153})^{-1} \equiv 8\ (\mathrm{mod}\ 53)$.

Perciò $M \equiv \delta (g^{ak})^{-1} \equiv (48) \cdot (8) = 384 \equiv 13\ (\mathrm{mod}\ 53)$

ed abbiamo decifrato. (Oppure metodo standard.)

Considerazioni matematiche generali sulle congruenze

La relazione di congruenza (modulo m) su $\mathbb{Z}$ è una "relazione d'equivalenza", cioè gode delle proprietà seguenti:

i) è riflessiva, $a \equiv a\,(m)$

ii) è simmetrica, $a \equiv b\,(m) \Rightarrow b \equiv a\,(m)$

iii) è transitiva, $a \equiv b\,(m)$ e $b \equiv c\,(m) \Rightarrow a \equiv c\,(m)$

Per dimostrare le tre proprietà basta ricordare la definizione di congruenza, che è la seguente "per m fissato, $m \in \mathbb{N}$, si dice che a è congruo b modulo m se $m \mid (a-b)$, cioè se $\exists k \in \mathbb{Z}$ tale che

$a-b=mk$".

Quindi la i) è ovvia, infatti $a-a=0=0\cdot m$; anche ii) è facile da provare, infatti $a-b=km$ implica $b-a=(-k)m$ e $k,-k \in \mathbb{Z}$. Per dimostrare iii) basta osservare che $a-b=mk$ e $b-c=mh$ implicano, sommando membro a membro,

$a-c=m(k+h)$, dove h,k e $k+h \in \mathbb{Z}$.

Ciò consente di ripartire $\mathbb{Z}$ in "classi d'equivalenza", dove la "classe d'equivalenza di a", che indicheremo con $\hat{a}$, è definita come

$$\hat{a} = \{x \in \mathbb{Z} : x \equiv a\,(m)\}$$

o, equivalentemente, $\hat{a} = \{a + mk,\ k \in \mathbb{Z}\}$. (2)

È facile convincersi del fatto che, modulo m, ci sono in tutto m classi d'equivalenza, precisamente $\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{m-1}$: infatti ogni numero $a \in$ diviso per m può dare resto $0, 1, 2, \ldots, m-1$ e quindi può essere scritto in modo unico sotto la forma $a = mq + r$ con $q \in \mathbb{Z}$ e $0 \leq r < m$. (vedi fascicolo "Prerequisiti aritmetici", pag 13). Tali classi sono disgiunte e la loro unione dà $\mathbb{Z}$ (dimostrarlo per esercizio).

Sull'insieme delle classi d'equivalenza modulo m possono essere definite due operazioni di somma e prodotto, denotate rispettivamente + e ·, nel modo seguente

$$1) \qquad \hat{a} + \hat{b} = \widehat{a+b}$$

$$2) \qquad \hat{a} \cdot \hat{b} = \widehat{a \cdot b}$$

Le due eguaglianze che abbiamo scritto sono, in effetti, due definizioni: inoltre, a voler essere rigorosi, i due segni + e · non hanno, a sinistra e a destra di 1) e 2), lo stesso significato. Infatti a sinistra indicano un'operazione tra due classi e a destra un'operazione (in $\mathbb{Z}$) tra i due rappresentanti di tali classi.

Tale "abuso di notazione" (come dicono i matematici) può essere tollerato a patto di dimostrare che le due definizioni 1) e 2) sono ben poste, nel senso che il risultato dell'operazione tra le classi $\hat{a}$ e $\hat{b}$ è indipendente dai rappresentanti a e b. Ciò per fortuna è vero, infatti

$$\begin{cases} a_1 \equiv a \ (m) \\ b_1 \equiv b \ (m) \end{cases} \Longrightarrow \begin{matrix} a_1+b_1 \equiv a+b \ (m) \\ a_1 \cdot b_1 \equiv a \cdot b \ (m) \end{matrix}$$

e quindi $\widehat{a_1+b_1} = \widehat{a+b}$ e $\widehat{a_1 b_1} = \widehat{a \cdot b}$

Dunque le due definizioni 1) e 2) sono "ben poste", cioè corrette.

Osserviamo anche che si può parlare di classe $\hat{a}$ "relativamente prima" con il modulo m.

Infatti $a \equiv a_1 \ (m) \Rightarrow (a,m) = (a_1,m)$: questa implicazione è facile da dimostrare osservando che la relazione $a = a_1 + mk$ implica che l'insieme dei divisori comuni ad a ed m coincide con l'insieme dei divisori comuni ad a_1 ed m (provarlo per esercizio), e quindi anche i massimi dei due insiemi coincidono. Perciò (se) $(a,m) = 1$ si ha anche $(a_1,m) = 1$, per ogni $a_1 \equiv a \ (m)$ e la proprietà di "relativamente primo" è indipendente dal rappresentante della classe. Ne segue che le classi relativamente prime con m sono in

numero di $\varphi(m)$ (dove φ è la funzione di Eulero).
Alla luce di queste proprietà possiamo dire che un "sistema completo di resti mod m" si costruisce scegliendo un elemento da ogni classe $\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{m-1}$ e che un "sistema ridotto di resti mod m" si costruisce scegliendo un elemento da ogni classe relativamente prima con m.

Diamo ora una definizione fondamentale.

Definizione di gruppo

Sia G un insieme con un'operazione binaria denotata $*$. Se l'operazione $*$ è tale che

i) è associativa, cioè $a*(b*c) = (a*b)*c$
$\forall a, b, c \in G$

ii) esiste l'elemento neutro, denotato $e \in G$, tale che $a*e = e*a$, $\forall a \in G$

iii) esiste l'inverso per ogni elemento, cioè
$\forall a \in G \; \exists a^{-1} \in G$ tale che
$$a*a^{-1} = a^{-1}*a = e$$

allora $G, *$ si dice gruppo.

Se poi $*$ è anche commutativa, cioè
$$a*b = b*a, \quad \forall a, b \in G$$
il gruppo si dice commutativo (o abeliano)

La struttura di gruppo si presenta continuamente in Matematica: ad esempio sono gruppi abeliani $\mathbb{Q},+$ (numeri razionali dotati dell'operazione di somma, $\mathbb{R},+$ (numeri reali), $\mathbb{C},+$ (numeri complessi) (la verifica è immediata: l'elemento neutro è lo zero e l'inverso è l'opposto additivo di ogni elemento, cioè $a^{-1}=-a$). Anche $\mathbb{Q}/\{0\},\cdot$ $\mathbb{R}/\{0\},\cdot$ e $\mathbb{C}/\{0\},\cdot$ sono gruppi abeliani (anche in questo caso la verifica è immediata: l'elemento neutro è 1 e $a^{-1}=\frac{1}{a}$, trattandosi dell'operazione di moltiplicazione.)

Possiamo aggiungere <u>due esempi interessanti</u> riguardanti le classi di resto. Le classi di resto mod m, cioè $G=\{\hat{0},\hat{1},\hat{2},\dots,\widehat{m-1}\}$ dotate dell'operazione 1) (di somma) cioè $\hat{a}+\hat{b}=\widehat{a+b}$, sono un gruppo abeliano (verifica facile, $e=\hat{0}$, $\hat{a}^{-1}=\widehat{-a}$

Un secondo esempio (<u>importante</u>) è dato dalle classi <u>ridotte</u> di resto mod m (cioè delle classi <u>relativamente prime con m</u>) dotate dell'operazione 2) di prodotto, cioè $\hat{a}\cdot\hat{b}=\widehat{a\cdot b}$. In questo caso l'operazione tra le classi è certamente associativa e commutativa perché tale è tra gli interi, e $\hat{1}$ è l'elemento neutro. Per provare che ogni elemento $\hat{a}$ ha inverso occorre invece ricordare che la congruenza $ax \equiv 1 \pmod{m}$ ha una sola soluzione mod m, se $(a,m)=1$. Questo è il Teorema 3) del fascicolo "Prerequisiti aritmetici" (pag 14). Quindi se indichiamo con $G',\cdot$ l'insieme delle classi ridotte (cioè relativamente prime con m) modulo m dotato dell'operazione $\cdot$, possiamo dire che $G',\cdot$ è un gruppo abeliano.

Osserviamo che nel contesto delle classi di resto modulo m, cioè $\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{m-1}$ la congruenza lineare $ax \equiv b \pmod{m}$ diviene un'equazione di primo grado, cioè $\hat{a} \cdot \hat{x} = \hat{b}$, che può avere una, nessuna o più soluzioni (vedi teorema 3 dei "Prerequisiti aritmetici"). Sempre in quest'ottica il teorema di Eulero-Fermat, cioè l'implicazione

$$(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

diviene

$$(a,m)=1 \Rightarrow (\hat{a})^{\varphi(m)} = \hat{1}$$

Anche il concetto di ordine di a modulo m, per $(a,m)=1$, riguarda la classe di resto di a, cioè $\hat{a}$. Infatti $a_1 \equiv a \pmod{m} \Rightarrow a_1^h \equiv a^h \pmod{m}$ e quindi a_1 ed a hanno lo stesso ordine modulo m (vedi sempre "Prerequisiti aritmetici" pag. 22 e 23

Quindi, in questo contesto, una "radice primitiva" mod m è una classe $\hat{a}$ di ordine $\varphi(m)$, che quindi "genera" con le sue potenze tutto il gruppo G'.
(Ricordiamo che questo accade se e solo se $m=1, 2, 4, p^\alpha$ e $2p^\alpha$ con p primo dispari, vedi i soliti "Prerequisiti", pag 2?)
Se c'è una radice primitiva il gruppo G' si dice ciclico e la radice primitiva è un "generatore" del gruppo.

Gruppi e quadrati latini

Un quadrato latino di ordine n è una matrice $n \times n$ nella quale n simboli distinti compaiono tutti in ogni riga ed in ogni colonna.
Ad esempio

$$\begin{vmatrix} A & B & C \\ B & C & A \\ C & A & B \end{vmatrix}$$

è un quadrato latino di ordine 3.

È interessante notare che la tavola delle operazioni su un gruppo $G, *$ è sempre un quadrato latino.
Consideriamo, ad esempio, il gruppo $\mathbb{Z}_6, +$: la sua tavola operativa è

+	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

Tavola di $\mathbb{Z}_{6,+}$
(quadrato latino di ordine 6)
(congruenza modulo 6)

Consideriamo ora $\mathbb{Z}^*_{12,\cdot}$ (gruppo (moltiplicativo) del sistema ridotto di resti mod 12, cioè 1, 5, 7, 11)

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Tavola di $\mathbb{Z}^*_{12,\cdot}$
(quadrato latino di ordine 4)
(congruenza modulo 12)

Per quale motivo la tavola dell'operazione $*$ di un gruppo $G, *$ ($G=\{g_1, g_2, \dots, g_n\}$) è sempre un quadrato latino? Il motivo è nell'esistenza degli inversi (assioma iii) di pag 4), che implica la legge di cancellazione, cioè

$a*c=b*c \Rightarrow a=b$ (basta moltiplicare a destra
$c*a=c*b \Rightarrow a=b$ e a sinistra per c^{-1}).

Ciò implica che nella riga i-esima della tabella operativa di $G,*$ compaiano tutti gli elementi di G: infatti gli elementi che compaiono sono effettivamente $g_i * g_1, g_i * g_2, g_i * g_3, \dots, g_i * g_n$, (9)

ma $g_i * g_h = g_i * g_k \Rightarrow g_h = g_k$. Lo stesso discorso vale per la colonna j-esima. Quindi si tratta effettivamente di un quadrato latino di ordine n.