# Crittografia - Appunti su RSA

Salvatore D'Asta

October 15, 2022

## 1 Congruenze modulo p: precisazioni:

### 1.1 Classi resto modulo n

Dati due numeri $a, b \in \mathbb{Z} = \{insieme\ dei\ numeri\ interi\}$ si dicono congrui modulo $n \in \mathbb{Z}$:

$$a \equiv b \mod n \qquad (\textbf{a}\ congruo\ \textbf{b}\ modulo\ \textbf{n})$$

se $\exists k \in \mathbb{Z}$ tale che $a = b + k \cdot n$ con $k \in \mathbb{Z}$ La congruenza modulo n è una relazione di equivalenza[1] che *partiziona* l'insieme $\mathbb{Z}$ creando l'insieme quoziente:

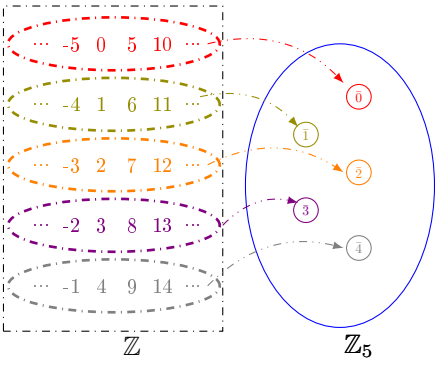
$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{(n-1)}\}$$

dove l'elemento $\bar{t} \in \mathbb{Z}_n$ rappresenta tutti i $k \in \mathbb{Z}$ per i quali vale $k \equiv t \mod n$
Nella pratica per trovare a quale classe appartiene il numero $s \in \mathbb{Z}$ basta calcolare il resto della divisione intera: $s = k \cdot n + r$ in tal caso $s \in \bar{r}$
In $\mathbb{Z}_n$ possiamo definire le stesse operazioni definite in $\mathbb{Z}$
A titolo d'esempio prendiamo l'elevazione a potenza in $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$$\overline{3^2} \equiv \bar{2} \mod 7$$

infatti $3^2 = 9 = 7 \cdot 1 + \boxed{\mathbf{2}}$ .
Per convenzione come rappresentante di una classe resto modulo n si prende il più piccolo dei suoi elementi maggiore di zero.

**Esempio** $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$**:**




[1] https://it.wikipedia.org/wiki/Relazione_di_equivalenza

## 1.2 Strutture Algebriche: gruppi, anelli e campi.

Dato un insieme $A$ e un'operazione $+$ definita in $A \times A \longmapsto A$ in modo tale che $\forall a, b \in A$ sia $a + b = c \in A$ un operazione che ha questa proprietà viene detta *legge di composizione interna* in $A$.

**Definizione 1.1 (gruppo)** *Un insieme $(A, +)$ dotato di legge di composizione interna $+$ da $A \times A \longrightarrow A$ è un* ***gruppo*** *abeliano se:*

- $\forall a, b, c \in A \qquad (a + b) + c = a + (b + c)$ *(associativa)*
- $\exists e \in A$ *tale che* $\forall a \in A \qquad a + e = e + a = a$ *(elemento neutro)*
- $\forall a \in A \qquad \exists a^{-1}$ *tale che* $a + a^{-1} = a^{-1} + a = e$ *(esistenza del reciproco)*
- $\forall a, b \in A \quad a + b = b + a$ *( commutativa)*

**Definizione 1.2 (anello)** *Se $(A, +)$ è un gruppo abeliano e se è definita una operazione $\cdot$ da $A \times A \longrightarrow A$ per la quale valgano le seguenti leggi distributive:*

$$\forall a, b, c \in A \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad (a \cdot b) + c = (a + c) \cdot (b + c)$$

*allora $(A, +, \cdot)$ è un* ***anello***

**Definizione 1.3 (campo)** *Sia $(A, +, \cdot)$ un* ***anello*** *e sia $A^* = A - \{0\}$. Se $(A^*, \cdot)$ è un gruppo abeliano allora è anche un* ***campo***

*Quindi un* ***campo*** *è un anello nel quale $A^*$ con l'operazione $\cdot$ è un gruppo abeliano*

## 1.3 L'algoritmo RSA

Alice vuole consentire a Bob di inviarle un messaggio $M$ segreto.

1. - Sceglie due numeri primi $p$ e $q$ e calcola $N = p \times q$. (scelti in modo che $M < N$ )
   - Calcola $\varphi(N) = (p - 1) \times (q - 1)$.
   - Trova $0 < e < \phi(N)$ in modo che $MCD(e, \varphi(N)) = 1$ (cioè siano coprimi).
     La coppia $\boxed{(e, N)}$ costituisce la chiave pubblica e viene inviata a Bob.
   - Alice poi crea la sua chiave privata $\boxed{(d, N)}$ trovando $d$ tale che $\boxed{e \times d \equiv 1 \mod \varphi(N)}$.
2. Bob ricevuto $(e, N)$ calcola:

   $$M^e \mod N = C$$

   e lo invia a Alice. Quest'ultima per decifrare il messaggio eseguirà:

   $$C^d \mod N = M$$

### 1.3.1 Perchè RSA funziona?

Ciò accade perchè:

$$C^d \mod N = M^{e \cdot d} \mod N = M \mod N \tag{1}$$

e ciò è vero perché avendo scelto $e$ e $d$ in modo che $e \cdot d = k \cdot \phi(N) + 1$ allora posso riscrivere la (1) in questo modo:

$$M^{e \cdot d} \mod N = M^{k \cdot \phi(N)+1} \mod N = M^{k \cdot \phi(N)} \cdot M^1 \mod N \tag{2}$$

per ottenere la tesi è necessario che nella (2) valga $M^{\phi(N)} = 1$ in $\mathbb{Z}_N$.
Il teorema di **Eulero-Fermat** afferma proprio quanto richiesto:

**Teorema 1.1 (Eulero-Fermat)** *Se M è coprimo con N (cioè $MCD(M, N) = 1$) allora:*

$$\boxed{M^{\phi(N)} \equiv 1 \mod N} \tag{3}$$

Essendo $M < N$ allora $MCD(M, N) = 1$ e quindi soddisfa le ipotesi del teorema. [2]

### 1.3.2 Perchè RSA è sicuro?

Per poter decifrare un messaggio ($C = M^e \mod N$) bisogna disporre della chiave privata $d$ ($M = C^d \mod N$) ma per ricavare la chiave privata $d$ bisogna conoscere $\phi(N) = (p-1) \cdot (q-1)$ che equivale a trovare i fattori $p$ e $q$ che generano $N$. Per i numeri $N$ molto grandi (rappresentabili con centinaia di cifre), non sono stati ancora trovati degli algoritmi che ne consentano la fattorizzazione in tempi accettabili.
Esistono diversi algoritmi di fattorizzazione, il più semplice consiste nel provare a dividere il numero per tutti i numeri $n \in \mathbb{Z}$ con $1 < n < \sqrt{N}$. Questo metodo per numeri molto grandi non risulta efficiente dato che, nel caso pessimo, si potrebbe essere costretti ad effettuare $\sqrt{(}N)$ operazioni. In questo caso si dice che l'algoritmo ha complessità $O\sqrt{N}$ (ordine di radice di N).
Un altro algoritmo, la fattorizzazione di Fermat, sfrutta l'idea che se $N$ è un numero dispari ed è ottenuto come prodotto di due numeri $p$ e $q$, anch'essi dispari, allora si possono trovare due interi $a$ e $b$ tali che:

$$N = (a - b)(a + b)$$

Questo perché:

$$N = pq = \left(\frac{p-q}{2}\right)^2 - \left(\frac{p+q}{2}\right)^2$$

[2] Il teorema di **EULERO-Fermat** prevede che se N è coprimo con M allora vale la 3
Il piccolo teorema di Fermat afferma che se $p$ è un numero primo allora $t^p \equiv t \mod p$ da cui si ottiene, dividendo entrambi i membri per $t$,

$$t^{p-1} \equiv 1 \mod p \tag{4}$$

ma la funzione **toziente di Eulero** $\phi(p) = \{$*numero di valori minori di p che non sono divisori di n*$\}$ essendo $p$ primo sarà $\phi(p) = (p-1)$ e sostituendo nella (4) ottengo

$$t^{\phi(p)} \equiv 1 \mod p \tag{5}$$

Infatti:

$$\left(\frac{p-q}{2}\right)^2 - \left(\frac{p+q}{2}\right)^2 = \frac{1}{4}(p^2+2pq+q^2) - \frac{1}{4}(p^2-2pq+q^2) = pq$$

Quindi posto:

$$\left(\frac{p-q}{2}\right) = a$$

e

$$\left(\frac{p+q}{2}\right) = b$$

ottengo che $N = a^2 - b^2 = (a+b)(a-b)$. *(Si asservi che $p-q$ e $p+q$ sono numeri pari perché la somma e la differenza di due numeri dispari dà un numero pari, questo ci assicura che $a$ e $b$ sono interi).*
Il problema di trovare i fattori di $N$ si può ricondurre a trovare $a$ per il quale si abbia:

$$a^2 - N = b^2$$

La ricerca dei fattori consiste nel trovare $\sqrt{N} < a < N$ in modo che $a^2 - N$ sia intero.

## 1.4 Come calcolare l'esponente privato $d$ noti $\phi(N)$ ed $e$

### 1.4.1 Metodo di Eulero esteso

Indicando con l'operatore *div* la parte intera della divisione tra due interi ad esempio $5\ div\ 2 = 2$ e indicando con mod l'operatore modulo che fornisce il resto della divisione tra due interi ad esempio $5 \mod 2 = 1$

| | | |
|---|---|---|
| $\phi(N)$ | 0 (a) | |
| e | 1 (b) | $\phi(N)\ div\ e$ (c) |
| $\phi(N) \mod e$ | $a - b \cdot c$ | |

Ad esempio siano $p = 37, q = 43$ allora $N = 37 \cdot 43 = 1591$ e $\phi(N) = 36 \cdot 42 = 1512$ e scegliamo $e = 23$ calcoliamo $d$ con l'algoritmo precedente:

| | | |
|---|---|---|
| 1512 | 0 | |
| 23 | 1 | 65 |
| 17 | -65 | 1 |
| 6 | 66 | 2 |
| 5 | -197 | 1 |
| 1 | 263 | |

ed infatti posto $M = 24$ ottengo $C = M^e \mod N = 24^{23} \mod 1591 = 146$ ed elevando $C$ per $d$ ottengo $C^d \mod N = 146^{263} \mod 1591 = 24$

| Indice | Quoziente | resto | x | y |
|---|---|---|---|---|
| | | 20 | 1 | 0 |
| | | 7 | 0 | 1 |
| | 20//7 = 2 | 6 | | |
| | | | | |
| | | | | |

# 2 Dimostrazione del teorema di Eulero-Fermat

## 2.1 Prima parte - I coefficenti binomiali

Il **coefficiente binomiale** è definito come:

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \qquad \forall p, i \in \mathbb{N} \quad i \leq p$$

e $\forall n \in \mathbb{N} \quad n! = n \cdot (n-1) \cdot (n-2) \cdots 1$
possiamo usare il coefficiente binomiale per calcolare la potenza di un binomio:

$$(A+B)^p = \sum_{i=0}^{p} \binom{p}{i} A^{(p-i)} B^i$$

quindi ad esempio:

$$(A+B)^3 = \binom{3}{0} A^3 B^0 + \binom{3}{1} A^2 B^1 + \binom{3}{2} A^1 B^2 + \binom{3}{3} A^0 B^3 =$$

$$= A^3 + 3A^2B + 3AB^2 + B^3$$

Tutto questo vale se si sta operando nell'insieme degli interi, cioè in $\mathbb{Z}$, se invece operiamo nell'insieme $\mathbb{Z}_3 = \{0, 1, 2\}$ (l'insieme delle classi resto modulo 3) la situazione cambia infatti dalla precedente espressione scompaiono i termini intermedi poiché

$$\binom{3}{1} = \binom{3}{2} = 3 \equiv 0 \mod 3$$

Quindi si avrà:

$$(A+B)^3 \mod 3 \equiv A^3 + B^3 \mod 3$$

ed in generale $\forall p \in \mathbb{Z}$ accade che in $\mathbb{Z}_p$ :

$$(A+B)^p = A^p + B^p$$

Si può osservare che la proprietà può estendersi ad un trinomio:

$$(A+B+C)^3 = (A+(B+C))^3 = A^3 + (B+C)^3 = A^3 + B^3 + C^3$$

quindi in generale ad un qualsiasi polinomio.
Operando come abbiamo fatto con il trinomio, e sostituendo 3 con un qualsiasi esponente $p \in \mathbb{Z}$, *a patto che p sia un numero primo*, possiamo estendere la proprietà alla somma di t valori elevati a p:

$$\underbrace{(A_1 + A_2 + A_3 + \ldots A_t)^p}_{t} \mod p \equiv \underbrace{A_1^p + A_2^p + A_3^p + \ldots A_t^p}_{t} \mod p \qquad (6)$$

Tutto ciò e possibile osservando che in generale per $0 < i < p$ (e $p$ numero primo)

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

è divisibile per $p$:
Poiché $\binom{p}{i}$ è intero[3], la fattorizzazione del suo denominatore:

$$i!(p-i)! = n_1 n_2 \dots n_k$$

sarà composta da fattori che necessariamente figureranno nella fattorizzazione del numeratore, perché se così non fosse allora il coefficiente binomiale non sarebbe un intero in quanto la frazione avrebbe denominatore diverso da 1. Ora poiché $p$ è fattore del numeratore ($p! = p(p-1)\cdots 2$) e poiché $p$ è primo non è divisibile per nessuno de i fattori del denominatore, allora $p$ sarà un divisore di $\binom{p}{i}$ cioè:

$$\binom{p}{i} = p\frac{(p-1)!}{i! \cdot (p-i)!}$$

e $\frac{(p-1)!}{i!\cdot(p-i)!}$ sarà un intero
quindi:

$$\binom{p}{i} \equiv 0 \mod p$$

## 2.2 Seconda parte – Il teorema di Eulero-Fermat

Scelti $p\ q \in \mathbb{P}$ e posto $N = pq$, $\phi(N) = (p-1)(q-1)$, scelto $t \in \mathbb{Z}$ e ponendo nella (6) $A_1 = A_2 = A_3 = \cdots = A_t = 1$ otteniamo:

$$(\underbrace{1+1+1+1\dots}_{t\ volte})^p \mod p \equiv \underbrace{1^p + 1^p \dots 1^p}_{t\ volte} \mod p \equiv t \mod p$$

cioè:

$$t^p \mod p \equiv t \mod p$$

Dividendo entrambi i membri per $t$ ottengo:

$$\boxed{t^{p-1} \equiv 1 \mod p} \tag{8}$$

Elevando entrambi i membri per $q-1$ ottengo:

$$t^{(p-1)(q-1)} \equiv 1 \mod p \tag{9}$$

[3] La dimostrazione che $\binom{p}{i}$ è intero deriva per induzione dalla seguente proprietà:

$$\binom{n+1}{k+1} = \frac{(n+1)!}{(k+1)!(n+1-k-1)!} = \binom{n}{k+1} + \binom{n}{k} \tag{7}$$

Supposto che $\binom{n}{k}$ sia intero $\forall n \in \mathbb{N}$ e $0 \le k \le n$ dimostriamolo per $n+1$.
La dimostrazione risulta evidente dalla (7) e dalla definizione di coefficiente binomiale

Si osservi che nel caso $k = n$ allora $\binom{n}{k+1} = 0$ e $\binom{n+1}{k+1} = 0 + \binom{n}{k} = \binom{n}{n} = 1$

La dimostrazione della (7) deriva da:

$$\binom{n}{k+1} + \binom{n}{k} = \frac{n!}{(k+1)!(n-k-1)!} + \frac{n!}{k!(n-k)!}$$

e poiché $(k+1)! = (k+1)k!$ e $(n-k)! = (n-k)(n-k-1)$ sostituendo:

$$\binom{n}{k+1} + \binom{n}{k} = \frac{n!}{(k+1)k!(n-k-1)!} + \frac{n!}{(n-k)k!(n-k-1)!} =$$

$$= \frac{(n-k)n!}{(k+1)k!(n-k)(n-k-1)!} + \frac{(k+1)n!}{(k+1)k!\cdot(n-k)(n-k-1)!} =$$

$$= \frac{(n-k+k+1)n!}{(k+1)k!(n-k)(n-k-1)!} = \frac{(n+1)!}{(k+1)!(n-k)!} = \binom{n+1}{k+1}$$

e ripetendo per q lo stesso ragionamento fatto per p ottengo:

$$t^{(p-1)(q-1)} \equiv 1 \mod q \tag{10}$$

La (9) e la (10) ci portano ad osservare che $\exists h\ k$ tali che:

$$t^{(p-1)(q-1)} = 1 + kq \tag{11}$$

$$t^{(p-1)(q-1)} = 1 + hp \tag{12}$$

cioè $hp = kq$ quindi $k = \frac{h}{q}p$ ed allora posto $l = \frac{h}{q}$ ottengo che $k = lp$ e quindi sostituendo $k$ nella (11) e ponendo $N = p \cdot q$ e $\phi(N) = (p-1)(q-1)$ otteniamo il **teorema di Eulero-Fermat**:

$$t^{(p-1)(q-1)} = 1 + lpq \Longrightarrow \boxed{t^{\phi(N)} \equiv 1 \mod N} \tag{13}$$