Università' degli studi di Roma "Tor Vergata"
Teoria della sicurezza e crittografia
Lezione 03

Authors: Angelo Silvestri, Marcello Politi, Samir Salman

Ottobre 2019

1 Numeri primi

Si definisce **numero primo** un numero intero > 1 tale che sia divisibile solamente per 1 e per se stesso.

2 Teorema fondamentale dell'aritmetica

Il teorema fondamentale dell'aritmetica afferma che:

Ogni numero naturale maggiore di 1 o è un numero primo o si può esprimere come prodotto di numeri primi. Tale rappresentazione è unica, se si prescinde dall'ordine in cui compaiono i fattori.

2.1 dimostrazione:

1 Dimostrimao l'esistenza di una fattorizzazione in numeri primi. Vogliamo dimostrare che ogni numero naturale maggiore di 1 o è un numero primo o si può esprimere come prodotto di numeri primi.

Procediamo *per induzione*.

Passo base: sia n=2, poichè 2 è primo l'enunciato è vero.

Passo induttivo: supponiamo che la tesi sia vera per numeri da 2 ...n. n+1 può essere primo o viceversa. Se n+1 primo allora abbiamo la tesi. Se n+1 non è primo allora n+1 è divisibile per un primo p (come dimostrato nella prima parte); in quest'ultimo caso il numero m=(n+1)/p è minore di n+1, e quindi verifica l'ipotesi induttiva, ovvero esiste una fattorizzazione di m. Ma allora n+1=mp cioè n+1 è fattorizzabile (è il prodotto di m e p). Quindi l'esistenza di una fattorizzazione è dimostrata per ogni numero naturale n.

2 Dimostriamo l'unicità: Dimostriamo che se un numero ammette una fattorizzazione in numeri primi questa è unica.

Per assurdo: Si supponga che esistano dei numeri scomponibili in fattori primi in più di un modo, e si chiami m il più piccolo (che esiste per il principio del buon ordinamento).

Innanzitutto si dimostra che, date due fattorizzazioni di m, i numeri primi che si presentano nella prima fattorizzazione sono tutti distinti da quelli della seconda fattorizzazione. Siano infatti le seguenti due diverse fattorizzazioni di m

$$m = p1p2p3 \ldots ps \tag{1}$$

$$m = q1q2q3 \ldots qt \tag{2}$$

dove i pi e qi sono primi ma differenti tra loro, ovvero per ogni i,j $pi <> qj$. A questo punto sappiamo che p 1 è diverso da q 1 ; senza perdita di generalità possiamo supporre che p 1 ¡ q 1 Poniamo allora

$$n = (q1p1)q2q3 \ldots qt \tag{3}$$

Evidentemente, n ¡ m, dato che la [3]si può scrivere come

$$n = q1q2q3 \ldots qtp1q2q3 \ldots qt = mp1q2q3 \ldots qt < m \tag{4}$$

Dimostriamo ora che n ammette almeno due fattorizzazioni distinte.

Iniziamo considerando il primo fattore di n ,$q1p1$. Esso può essere primo o meno; nel caso non lo fosse lo fattorizzeremo e la nuova fattorizzazione di n così ottenuta non ammetterebbe p 1 tra i suoi fattori. Infatti, per la prima parte della dimostrazione sappiamo che p 1 è diverso da q 2 , q 3 , ... q t e non può comparire nella eventuale fattorizzazione di q 1 p 1, poiché se ciò accadesse significherebbe che

$q1p1 = p1bq1 = p1(1 + b)$

e quindi q 1 sarebbe divisibile per p 1, il che non è possibile in quanto q 1 è un numero primo.

Prendendo ora l'ultima uguaglianza della [4] e sostituendo m con la [1]otteniamo

$$n = p1p2p3 \ldots psp1q2q3 \ldots qtn = p1(p2p3 \ldots psq2q3 \ldots qt) \tag{5}$$

In qualunque modo sia fattorizzabile il secondo fattore nella [5] , avremo ottenuto una fattorizzazione di n che contiene p 1 e che pertanto è diversa da quella nella [3] , contrariamente all'ipotesi che m sia il numero più piccolo che ammette più di una fattorizzazione.

L'unicità è pertanto dimostrata.

3 Algoritmo di Euclide

L'algoritmo di Euclide permette di calcolare il massimo comune divisore tra due numeri, anche se questi sono molto grandi, senza aver bisogno di fattorizzarli come prodotto di fattori primi.

3.1 MCD

Il massimo comune divisore dati dati due numeri naturali non nulli a e bè un intero positivo d > 0 tale che

1. d divide a e d divide b (divisore comune)
2. d è il numero più grande con tale proprietà.

Se a e b non sono entrambi nulli, l'insieme dei loro divisori comuni è non vuoto (contenendo almeno 1) e finito (perchè i divisori di unnumero non nullo non possono essere maggiori del numero stesso). Poichè i numeri naturali formano un insieme ordinato, il massimo comune divisore esiste sempre, ed è unico: esso viene indicato con il simbolo MCD (a; b). Se a = b = 0, si dice che 0 è il loro massimo comune divisore. Se solo uno tra a e b, è non nullo, esso coincide con il massimo comune divisore. Se d0 divide sia a che b allora d0 divide d.

4 Piccolo teorema di Fermat

Il piccolo teorema di Fermat dice che se p è un numero primo, allora per ogni intero a:

$$a^p = a(modp) \tag{6}$$

Questo significa che se si prende un qualunque numero a, lo si moltiplica per se stesso p volte e si sottrae a, il risultato è divisibile per p . Nella forma equivalente: se p è primo e a è un intero coprimo con p, allora:

$$a^{p-1} = 1(modp) \tag{7}$$

Per dimostrare il piccolo teorema di fermat usiamo il teorema di Eulero detto anche teorema di **Fermat-Eulero** che afferma che

> se n è un intero positivo ed a è coprimo rispetto ad n, allora: $a^{\phi(n)} \equiv 1(modn)$ dove $\phi(n)$ indica la funzione phi di Eulero

Per arrivare alla tesi del teorema di Fermat osserviamo che,poichè p è primo abbiamo, $\phi(p) = p - 1 \rightarrow a^{\phi p)} = 1(modp)$ quindi $a^{p-1} = 1(modp)$ e moltiplicando i membri per a $a^p = a(modp)$