

**ARITMETICA MODULARE****Introduzione**

L'aritmetica modulare, chiamata anche finita o circolare, studia i resti  $R$  delle divisioni aritmetiche fra numeri interi. E' chiamata finita in quanto utilizza un insieme limitato di numeri e circolare perché una volta raggiunto l'ultimo numero si ritorna al primo. Come esempio, si consideri un orologio le cui ore si susseguono da 1 a 12 (dove il 12 è il punto di partenza, quindi lo 0), una volta passate le dodici scocca nuovamente l'una.

Nell'aritmetica modulare è del tutto irrilevante la conoscenza del quoziente  $Q$  della divisione fra dividendo  $X$  e divisore  $m$ ; pertanto, si usa una diversa notazione rispetto a quella impiegata per la divisione fra numeri reali:  $X(\text{mod } m) = R$  e si legge:  $X$  modulo  $m$  è uguale a  $R$ .

Degli esempi banali possono essere:

$$30(\text{mod } 4) = 2; \quad 74(\text{mod } 7) = 4; \quad 45(\text{mod } 45) = 0; \quad 11(\text{mod } 35) = 11;$$

Vediamo adesso le proprietà relative alla notazione  $X(\text{mod } m) = R$ :

- È sempre  $R < m$ ;
- Tutti i possibili resti sono pari ad  $m$  e sono cifre comprese tra 0 e  $m - 1$ ;
- Se  $X < m$  allora il resto  $R$  è uguale a  $X$ , cioè  $X(\text{mod } m) = X$ ;
- Se  $X = m$  il resto è  $R = 0$ ;
- Se  $X$  è un multiplo di  $m$  il resto è  $R = 0$ ;
- $0(\text{mod } m) = 0$ ;
- $X(\text{mod } 1) = 0$ ;
- $X(\text{mod } (X - 1)) = 1$  ovvero  $(m+1)(\text{mod } m) = 1$ .

Alcune equivalenze, che adesso mostreremo, sono di notevole importanza:

- $(X + Y)(\text{mod } m) = X(\text{mod } m) + Y(\text{mod } m)$ , ciò vuol dire che il resto di una somma è uguale alla somma dei resti;

**ARITMETICA MODULARE**

- $(X \cdot Y)(\text{mod } m) = X(\text{mod } m) \cdot Y(\text{mod } m)$ , ciò vuol dire che il resto di un prodotto è uguale al prodotto dei resti.

Essendo dei resti, è chiaro che se uno dei due membri di una equivalenza è maggiore o uguale a  $m$ , vuol dire che non è un resto, e pertanto occorre ancora dividerlo per  $m$ .

Vediamo un esempio:

- $15(\text{mod } 6) = 3 = (12 + 3)(\text{mod } 6) = 12(\text{mod } 6) + 3(\text{mod } 6) = 0 + 3 = 3$ ;
- $15(\text{mod } 6) = 3 = (10 + 5)(\text{mod } 6) = 10(\text{mod } 6) + 5(\text{mod } 6) = 4 + 5 = 9 = 9(\text{mod } 6) = 3$ ;

L'equivalenza sul prodotto è estremamente importante quando  $X$  e  $Y$  sono uguali (quadrato). Infatti, in questo caso risulta che il resto di un quadrato è pari al quadrato del resto. Infatti, come esempio si ha :  $X^2(\text{mod } m) = (X \cdot X)(\text{mod } m) = X(\text{mod } m) \cdot X(\text{mod } m) = R \cdot R = R^2$ .

Questa proprietà relativa al resto di un quadrato è il motivo del nostro studio dell'aritmetica modulare. Infatti, è utilizzata fondamentalmente nell'ambito della crittografia a chiave pubblica (RSA)<sup>1</sup> con numeri primi. E sarà grazie a questa proprietà che sarà possibile determinare i resti di divisioni tra numeri con un incalcolabile numero di cifre.

Vediamo qualche esempio di chiarimento:

- $12^2(\text{mod } 11) = 144(\text{mod } 11) = 1 = (12(\text{mod } 11))^2 = 1 \cdot 1 = 1$ ;
- $16^2(\text{mod } 7) = 256(\text{mod } 7) = 4 = (16(\text{mod } 7))^2 = 2 \cdot 2 = 4$ ;
- $20^2(\text{mod } 9) = 400(\text{mod } 9) = 4 = (20(\text{mod } 9))^2 = 2 \cdot 2 = 4$ .

**Resti di divisioni impossibili**

Esistono alcuni calcoli che anche con il processore più veloce richiederebbero tempi enormi ed in alcuni casi i resti di divisioni particolare potrebbero essere addirittura impossibili.

---

<sup>1</sup> Vedi capitolo sulla crittografia.

**ARITMETICA MODULARE**

Ad esempio il resto della divisione:

$$327^{1033} \pmod{1827}$$

è obiettivamente impossibile da calcolare con le tecniche finora conosciute.

Ebbene, vi assicuro che utilizzando le proprietà dell'aritmetica modulare, il resto è pari a 432.

Per ottenerlo è necessario implementare un algoritmo che, appunto, sfrutta la proprietà sul resto di un quadrato.

Vediamo, adesso, il procedimento di come si giunge al risultato richiesto, ricordando che esso è ovviamente del tutto generalizzabile ed implementabile, anche quando sia l'esponente della potenza sia il modulo hanno un numero di cifre superiori.

Per prima cosa si deve effettuare la decomposizione binaria dell'esponente della potenza. Si scrivono a partire da destra tutte le potenze di 2 (binario) fino a quella precedente all'esponente:

$$2^n \quad 2^{n-1} \quad 2^{n-2} \quad 2^{n-3} \dots 2^0.$$

Nel nostro caso  $n = 10$  e, quindi, si sommano quelle potenze che daranno il valore di partenza:

$$1033 = 1024 + 8 + 1.$$

Applichiamo ora la proprietà sul resto di un prodotto, scrivendo:

$$327^{1033} \pmod{1827} = (327 \cdot 327^8 \cdot 327^{1024}) \pmod{1827} = 327 \pmod{1827} \cdot 327^8 \pmod{1827} \cdot 327^{1024} \pmod{1827}.$$

Se si applica le proprietà generali dell'aritmetica modulare ed in particolare la proprietà sul resto di un quadrato, è possibile determinare i singoli resti. Infatti, si ottiene:

$$327 \pmod{1827} = 327$$

$$327^2 \pmod{1827} = 327^2 = 106929 = 106929 \pmod{1827} = 963$$

$$327^4 \pmod{1827} = 963^2 = 927369 = 927369 \pmod{1827} = 1080$$

$$327^8 \pmod{1827} = 1080^2 = 1166400 = 1166400 \pmod{1827} = 774$$

$$327^{16} \pmod{1827} = 774^2 = 599076 = 599076 \pmod{1827} = 1647$$

**ARITMETICA MODULARE**

$$327^{32}(\text{mod}1827) = 1647^2 = 2712609 = 2712609(\text{mod}1827) = 1341$$

$$327^{64}(\text{mod}1827) = 1341^2 = 1798281 = 1798281(\text{mod}1827) = 513$$

$$327^{128}(\text{mod}1827) = 513^2 = 263169 = 263169(\text{mod}1827) = 81$$

$$327^{256}(\text{mod}1827) = 81^2 = 6561 = 6561(\text{mod}1827) = 1080$$

$$327^{512}(\text{mod}1827) = 1080^2 = 1166400 = 1166400(\text{mod}1827) = 774$$

$$327^{1024}(\text{mod}1827) = 774^2 = 599076 = 599076(\text{mod}1827) = 1647$$

I resti in rosso sono quelli che devono essere utilizzati; infatti:

$$327^{1033}(\text{mod}1827) = (327 \cdot 774 \cdot 1647)(\text{mod}1827) = 416852406(\text{mod}1827) = 228162(\text{mod}1827) = 432.$$

In definitiva, il metodo è ricorsivo e facilmente implementabile con un qualunque linguaggio di programmazione contenente l'istruzione "mod" (che permette di determinare il resto di una divisione fra numeri interi).

**Funzioni modulari ed inverse**

Le funzioni ordinarie sono troppo regolari e, quindi, estremamente prevedibili nel loro andamento. Pertanto, quando si vuole introdurre un elevato fattore di difficoltà (sicurezza in rete) nel calcolo dei valori ignoti per estrapolazione a partire da quelli noti, ci vengono in aiuto le funzioni modulari.

Una generica funzione modulare ha la seguente struttura:

$$C = E_K \cdot P(\text{mod } m),$$

dove:

- $E_K$  e  $m$  sono due costanti numeriche;
- $E_K$  è la chiave di codifica (Encode Key) che mi cripta il messaggio;

**ARITMETICA MODULARE**

- $P$  è la variabile indipendente e rappresenta il messaggio che deve essere trasmesso;
- $C$  è la variabile dipendente e rappresenta il messaggio criptato, cioè reso intellegibile.

$C$  è ovviamente un resto e, supponendo di voler utilizzare la funzione modulare inversa per riottenere il messaggio di partenza, anche  $P$  è un resto. Quindi, sia  $C$  sia  $P$  sono numeri naturali compresi tra  $0$  e  $m - 1$ .

E' importante sottolineare che la funzione modulare  $C = E_k \cdot P(\text{mod } m)$  è invertibile solo nel caso in cui  $E_k$  e  $m$  sono **primi tra loro**<sup>2</sup>.

Vediamo adesso alcuni esempi semplici di funzioni modulari invertibili con la relativa tabella di valori:

1.  $C = 11 \cdot P(\text{mod } 7)$ ;
2.  $C = 6 \cdot P(\text{mod } 7)$ ;
3.  $C = 11 \cdot P(\text{mod } 9)$ .

Nel primo caso, ricordando che  $P$  è compreso tra  $0$  e  $(7 - 1) = 6$  avremo questa tabella, dove i valori di  $C$  sono calcolati in funzione dei corrispondenti valori di  $P$  sfruttando tutte le possibili proprietà delle funzioni modulari:

P	0	1	2	3	4	5	6
C	0	4	1	5	2	6	3

con  $E_k = 11$  e  $m = 7$ .

Nel secondo caso effettuando lo stesso svolgimento si ottiene un'altra tabella:

P	0	1	2	3	4	5	6
C	0	6	5	4	3	2	1

con  $E_k = 6$  e  $m = 7$ .

---

<sup>2</sup> Due numeri si dicono primi tra loro se il loro massimo comune divisore è 1, ovvero non hanno alcun fattore in comune. Esempi di coppie di numeri primi fra loro: 2 e 3, 5 e 7, 15 e 2, etc. Invece, un numero è primo quando è divisibile solo per 1 e per se stesso.

**ARITMETICA MODULARE**

Nel terzo esempio, essendo  $m = 9$ , sia P sia C andranno dallo 0 all'8, ed avremo:

P	0	1	2	3	4	5	6	7	8
C	0	2	4	6	8	1	3	5	7

con  $E_k = 11$  e  $m = 9$ .

Si nota immediatamente il tipico andamento *disordinato* delle funzioni modulari.

La funzione modulare inversa che troveremo avrà la stessa tabella ma letta al contrario; ovvero C diventa la variabile indipendente e P quella dipendente.

Si è detto che se  $E_k$  e  $m$  sono primi tra loro, la conoscenza della forma esplicita di una data funzione modulare generale:  $C = E_k \cdot P(\text{mod } m)$ , rende sempre possibile la determinazione di un'unica funzione modulare inversa:  $P = D_k \cdot C(\text{mod } m)$ , dove l'unica costante da calcolare è  $D_k$  (decoder Key).

Sono importanti e fondamentali due proprietà che adesso andremo ad enunciare:

1. una data uguaglianza modulare resta tale anche se si moltiplicano entrambi i membri per la stessa costante:  $F \cdot X(\text{mod } m) = F \cdot R(\text{mod } m)$ . Infatti, applicando la proprietà sul resto di un prodotto si ottiene:

$$F \cdot X(\text{mod } m) = F(\text{mod } m) \cdot R(\text{mod } m) = F(\text{mod } m) \cdot R = F \cdot R(\text{mod } m).$$

2. una data uguaglianza modulare resta tale anche se si aggiunge ad entrambi i membri una stessa costante:  $(F + X)(\text{mod } m) = (F + R)(\text{mod } m)$ . Infatti, applicando la proprietà sul resto di un somma si ottiene:

$$(F + X)(\text{mod } m) = F(\text{mod } m) + R(\text{mod } m) = F(\text{mod } m) + R = (F + R)(\text{mod } m).$$

Allora, per quanto detto finora, sono giustificati i seguenti passaggi sulla generica funzione modulare:  $C = E_k \cdot P(\text{mod } m)$ :

$$D_k \cdot C(\text{mod } m) = D_k \cdot E_k \cdot P(\text{mod } m) = P \cdot (D_k \cdot E_k(\text{mod } m)).$$

**ARITMETICA MODULARE**

Pertanto, basta cercare un  $D_K$  in modo che  $D_K \cdot E_K \pmod{m} = 1$ ; in questo modo si ottiene la funzione inversa:  $P = D_K \cdot C \pmod{m}$ .

Non bisogna mai dimenticare che  $D_K$  esiste solo se  $E_K$  e  $m$  sono primi tra loro.

Vediamo di trovare l'inversa delle funzioni modulari viste in precedenza.

La prima è  $C = 11 \cdot P \pmod{7}$ . Per poterla invertire è sufficiente trovare un  $D_K$  che deve essere un numero naturale tale che  $11 \cdot D_K \pmod{7} = 1$ .

Per  $D_K = 0, 1, 3, 4, 5, 6$  l'uguaglianza non è verificata; mentre per  $D_K = 2$  si verifica l'uguaglianza.

Pertanto, la funzione modulare inversa diventa:  $P = 2 \cdot C \pmod{7}$ .

La seconda è  $C = 6 \cdot P \pmod{7}$ . Sviluppando nello stesso modo dobbiamo trovare un  $D_K$  che soddisfi tale equazione:  $6 \cdot D_K \pmod{7} = 1$ .

Per  $D_K = 0, 1, 2, 3, 4, 5$  l'uguaglianza non è verificata; mentre per  $D_K = 6$  si verifica l'uguaglianza.

Pertanto, la funzione modulare inversa diventa:  $P = 6 \cdot C \pmod{7}$ .

Da notare che in questo caso le due chiavi  $E_K$  e  $D_K$  sono uguali tra loro e pari a 6. La cosa si poteva intuire guardando la tabella e notando l'inversione dei valori di  $C$  e  $P$ .

La terza è  $C = 11 \cdot P \pmod{9}$ . Dobbiamo trovare un  $D_K$  che soddisfi tale equazione:  $11 \cdot D_K \pmod{9} = 1$ .

Per  $D_K = 0, 1, 2, 3, 4, 6, 7, 8$  l'uguaglianza non è verificata; mentre per  $D_K = 5$  si verifica l'uguaglianza.

Per questi semplici casi la determinazione del valore di  $D_K$  è stata intuitiva ed immediata. Non è sempre così. Supponete di avere una funzione modulare in cui  $m$  è formato da un numero elevato di cifre. La determinazione del valore di  $D_K$  non è più così intuitiva e semplice. Fortunatamente, esiste un algoritmo che permette di calcolare tale valore ( $D_K$ ) in tempi di elaborazione

**ARITMETICA MODULARE**

ragionevoli. L'importante è ricordare che  $D_K$  deve essere un numero naturale e deve sottostare alla condizione  $D_K \cdot E_K \pmod{m} = 1$ .

L'algoritmo segue questo ragionamento: se si indica con  $Q$  il risultato e non il resto dell'operazione di divisione tra  $(D_K \cdot E_K)$  e  $m$ , dovendo essere  $(D_K \cdot E_K) = m \cdot Q + 1$ , è possibile implementare un'iterazione con  $Q$  che diventa 1, 2, 3, etc. L'algoritmo si arresta quando il

risultato della divisione  $\frac{m \cdot Q + 1}{E_K} = D_K$  è un numero naturale, il primo che si incontra.

Sviluppando tale algoritmo per gli esempi precedenti si vede che nel primo caso si ottiene il valore naturale dopo 3 iterazioni ( $Q = 3$ ); nel secondo dopo 5 iterazioni ( $Q = 5$ ) e nell'ultimo caso dopo 6 iterazioni ( $Q = 6$ ).

Vediamo quante iterazioni ci sono in un caso con  $m$  molto grande:  $C = 11 \cdot P \pmod{10800}$ .

Per prima cosa notiamo che 11 e 10800 sono primi tra loro e, poi, applichiamo l'algoritmo precedente che si ferma dopo appena 6 iterazioni.  $D_K$  vale facendo i conti 5891.

**Funzioni modulari esponenziali ed inverse**

Prima di vedere la struttura di una funzione modulare esponenziale invertibile, è necessario definire la funzione di Eulero<sup>3</sup> o indicatore di Eulero - Gauss:  $\phi(m)$  e vederne le principali proprietà.

La funzione di Eulero di un numero naturale  $m$  è definita come il numero degli interi positivi compresi fra 1 (incluso) e  $m - 1$ , che non hanno fattori in comune con  $m$ , ossia primi con  $m$ .

Vediamo qualche esempio:

<sup>3</sup> Leonard Euler (Eulero). Matematico, nato a Basilea nel 1707 e morto a Pietroburgo nel 1783. Allievo di Giovanni Bernoulli, fu indirizzato allo studio delle matematiche. Infatti, apportò contributi profondi e geniali in quasi tutti i rami della matematica che furono raccolti in una ventina di trattati ed in varie centinaia di memorie pubblicate per lo più dalle Accademie di Pietroburgo e di Berlino: questioni di scienza nautica e di astronomia, analisi e geometria analitica, geometria differenziale, calcolo integrale e differenziale, meccanica razionale, fisica, **teoria dei numeri**, geometria elementare e metafisica.

Notiamo il teorema di Fermat - Eulero: se  $a$  è primo con  $m$ , allora  $a^{\phi(m)} \pmod{m} = 1$ .

**ARITMETICA MODULARE**

- $\phi(9) = 6$  (ovvero 1, 2, 4, 5, 7, 8);
- $\phi(12) = 4$  (ovvero 1, 5, 7, 11);
- $\phi(18) = 6$  (ovvero 1, 5, 7, 11, 13, 17);
- $\phi(11) = 10$  (ovvero  $m - 1$ , perché 11 è un numero primo).

Vediamo, adesso, la proprietà più importante. Se  $m$  è pari al prodotto di due numeri primi<sup>4</sup>, diciamo  $h$  e  $g$ , è:  $\phi(m) = \phi(h \cdot g) = (h - 1) \cdot (g - 1)$ .

La stessa proprietà vale anche se  $m$  è pari al prodotto di più di due numeri primi. Vediamo qualche esempio:

- $\phi(6) = \phi(2 \cdot 3) = (2 - 1) \cdot (3 - 1) = 1 \cdot 2 = 2$  (ovvero i numeri 1 e 5);
- $\phi(10) = \phi(2 \cdot 5) = (2 - 1) \cdot (5 - 1) = 1 \cdot 4 = 4$  (ovvero i numeri 1, 3, 7, 9);
- $\phi(30) = \phi(2 \cdot 3 \cdot 5) = (2 - 1) \cdot (3 - 1) \cdot (5 - 1) = 1 \cdot 2 \cdot 4 = 8$  (ovvero i numeri 1, 7, 11, 13, 17, 19, 23, 29).

L'importanza e l'utilizzo pratico di tale funzione sta sempre nell'ambito della crittografia a chiave pubblica; infatti, è molto semplice determinarla anche quando  $m$  è pari al prodotto di due numeri primi molto grandi.

<sup>4</sup> Come detto, i numeri primi sono gli interi (escluso 1) che sono divisibili solo per se stessi e per l'unità. Esistono infiniti numeri primi (Euclide), ma non conosciamo né una formula di generazione, né una che ne dia infiniti.

I grandi numeri primi noti sono tutti della forma  $M_m = 2^m - 1$ , con  $m$  numero primo, ma non tutti i numeri calcolati in questo modo (numeri di Mersenne) sono, purtroppo, primi. Es.  $m = 4 \Rightarrow M_4 = 15$  non primo.

Il numero di cifre relativo ai numeri primi conosciuti è cresciuto enormemente durante i secoli. Basti pensare che nel 1461 è stato scoperto il numero primo  $2^{13} - 1 = 8191$ .

Nel 1961 il numero di cifre del numero primo trovato era pari a 1281; mentre nel 1998 si è giunti alla determinazione di un numero primo con 909526 cifre.

E' noto che in tempi brevi si riesce a scoprire se un numero è primo o composto, ma i tempi per trovare i fattori crescono fortemente al crescere del numero secondo la seguente tabella:

Cifre di $m$	Tempo per $m$ primo	Tempo per fattori
50	15 secondi	4 ore
75	22 secondi	104 giorni
100	40 secondi	74 anni
200	10 minuti	$4 \cdot 10^9$ anni (età della terra)
500	3 giorni	$4 \cdot 10^{25}$ anni
1000	1 settimana.....	

**ARITMETICA MODULARE**

La struttura di una funzione modulare esponenziale è la seguente:

$$C = P^{E_K} \pmod{m},$$

dove le variabili e le costanti numeriche hanno lo stesso significato di prima.

Anche adesso è necessario calcolare la funzione modulare esponenziale inversa, pertanto, sia  $C$  sia  $P$  sono dei resti e sono dei numeri naturali compresi tra 0 ed  $(m - 1)$ .

Adesso, però, la funzione  $C = P^{E_K} \pmod{m}$  è invertibile se e solo se  $E_K$  e  $\phi(m)$  sono primi tra loro, ossia non hanno alcun fattore in comune.

Oltre alle proprietà della somma e del prodotto su una data uguaglianza modulare, vale anche quella dell'elevazione; ovvero "una data uguaglianza modulare rimane tale se si elevano entrambi i membri ad una stessa quantità":  $X^{D_K} \pmod{m} = R^{D_K} \pmod{m}$ .

La dimostrazione è molto semplice, infatti:

$$X^{D_K} \pmod{m} = (X \cdot X \cdots)(\pmod{m}) = X(\pmod{m}) \cdot X(\pmod{m}) \cdots = R \cdot R \cdots = R^{D_K} \pmod{m}.$$

Per riuscire ad invertire la nostra funzione modulare esponenziale, si deve fare riferimento ad un teorema della Teoria dei numeri così espresso:

$$C = P^{E_K} \pmod{m} = P^{E_K \pmod{\phi(m)}} \pmod{m}.$$

E', quindi, vero che:  $C^{D_K} \pmod{m} = (P^{E_K \pmod{\phi(m)}} \pmod{m})^{D_K} = P^{D_K \cdot E_K \pmod{\phi(m)}} \pmod{m}$ .

Come prima, è sufficiente cercare un  $D_K$  tale che  $D_K \cdot E_K \pmod{\phi(m)} = 1$ , perché, in tal modo, la funzione modulare esponenziale inversa vale:

$$P = C^{D_K} \pmod{m}.$$

E', sempre, importante ricordare che  $D_K$  esiste solo se  $E_K$  e  $\phi(m)$  sono primi tra loro.

Vediamo, adesso, due esempi sulla determinazione della  $D_K$ :

**ARITMETICA MODULARE**

1. Si scelgono due numeri primi tra loro:  $h = 13$  e  $g = 17$ ;  $m$  sarà pari al loro prodotto:  $m = 221$ . La funzione di Eulero  $\phi(m) = \phi(221) = (h-1) \cdot (g-1) = 12 \cdot 16 = 192$ . Decomponiamo tale numero:  $192 = 2^6 \cdot 3 = 3 \cdot 64$ .

$E_K$  deve, a sua volta, essere primo rispetto a  $\phi(m)$ , ossia i fattori di cui è composto  $E_K$  non devono essere presenti in  $\phi(m)$ . Una possibile scelta è  $E_K = 5 \cdot 7 = 35$ . La funzione da invertire è  $C = P^{35} \pmod{221}$ .

Deve verificarsi che  $D_K \cdot 35 \pmod{192} = 1$ ; si utilizza lo stesso algoritmo visto precedentemente con  $\phi(m)$  al posto di  $m$ . L'algoritmo si arresta quando il risultato della

divisione:  $\frac{\phi(m) \cdot Q + 1}{E_K} = \frac{192 \cdot Q + 1}{35} = D_K$  è un numero naturale, come nel caso

precedente il primo che arriva. Dopo appena 2 iterazioni ( $Q = 2$ ) si ottiene  $D_K = 11$ . Pertanto, la cercata funzione modulare esponenziale inversa è  $P = C^{11} \pmod{221}$ .

2. Sia  $m = h \cdot g = 23 \cdot 31 = 713$ ;  $\phi(713) = 660$ ; decomponiamo  $660 = 3 \cdot 2^2 \cdot 5 \cdot 11$ .

Scelgo  $E_K = 7 \cdot 13 = 91$ , primo con  $\phi(m)$ . La funzione modulare esponenziale da invertire risulta  $C = P^{91} \pmod{713}$ .

Ragionando come per il primo esempio si giungerà al valore di  $D_K = 631$  dopo 87 iterazioni ( $Q = 87$ ).

Pertanto, la cercata funzione modulare esponenziale inversa è  $P = C^{631} \pmod{713}$ .

Potrebbe sembrare che aumentando i valori di  $m$  e  $E_K$ , si aumenti sensibilmente il numero di iterazioni. Niente di più falso. Infatti, con  $m = 47 \cdot 61 = 2867$ ,  $\phi(m) = 46 \cdot 60 = 2760$ , e scegliendo  $E_K = 7 \cdot 13 \cdot 13 = 1183$ , si ottiene la funzione da invertire:  $C = P^{1183} \pmod{2867}$ . Ebbene, il valore di  $D_K = 7$  si ottiene con lo stesso algoritmo dopo appena 3 iterazioni ( $Q = 3$ ).

La funzione inversa è  $P = C^7 \pmod{2867}$ .

**ARITMETICA MODULARE**

E' possibile determinare  $D_K$  con una seconda funzione di Eulero, semplice solo per numeri non elevati. Si deve determinare la funzione di Eulero della funzione di Eulero  $\phi(\phi(m))$ . La

$$D_K = E_K^{\phi(\phi(m))-1} \pmod{\phi(m)}.$$

Nel primo caso si ottiene  $\phi(\phi(m)) = \phi(192) = 192 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 64$ . Il valore di  $D_K$

corrispondente si determina in questo modo:  $D_K = 35^{63} \pmod{192} = 11$ .

Stesso procedimento per gli altri casi.

**Test di Fermat**

Si è sicuramente notato l'importanza ed il grande utilizzo dei numeri primi nell'aritmetica modulare e, poi, nella crittografia. Vediamo, pertanto, la definizione di numero primo e come si può determinare di un numero la primalità.

Un numero è primo quando è divisibile solo per se stesso e per 1; altrimenti, se possiede altri divisori si dice che il numero è composto.

Una caratteristica fondamentale dei numeri primi è che essi, escluso il 2, sono tutti dispari. Non è però vero che tutti i numeri dispari sono primi (il 9 per esempio).

Controllare la primalità di un numero significa classificare il numero in questione tra i numeri primi o tra i numeri composti. In effetti non è facile affermare se un numero è primo soprattutto se composto da molte cifre.

Esiste un algoritmo che permette di controllare la "quasi" primalità di un numero con un elevato numero di cifre, e che si basa sul cosiddetto "piccolo teorema di Fermat<sup>5</sup>".

---

<sup>5</sup> Pierre de Fermat. Matematico, nato a Beaumont de Lomagne nel 1601 e morto a Castres nel 1665. Fu consigliere del Parlamento di Tolosa ed ebbe relazioni con R. Descartes (Cartesio). Sembra che abbia avuto l'idea della geometria analitica indipendentemente da questo ultimo e che abbia osservato come dall'equazione di una curva se ne possano dedurre tutte le proprietà. Trattò questioni di massimo e di minimo (metodi generali ed applicazioni all'ottica geometrica). Fondò con Pascal la teoria della probabilità, si occupò della **teoria dei numeri** e dello studio di alcune curve. Non pubblicò quasi nulla dei suoi scritti che, infatti, furono pubblicati postumi. Tra i principali enunciati di Fermat:

**ARITMETICA MODULARE**

Vediamo il teorema per alcuni numeri primi: 2, 3 e 5:

- Sia  $m = 2$ , necessariamente  $a = 1$ . Pertanto,  $a^m \pmod{m} = a = 1^2 \pmod{2} = 1$ . Verificato.
- Sia  $m = 3$ ,  $a$  vale 1 e 2. Per  $a = 1$  si ha:  $a^m \pmod{m} = a = 1^3 \pmod{3} = 1$ . Verificato.  
Per  $a = 2$  si ha  $a^m \pmod{m} = a = 2^3 \pmod{3} = 2$ . Verificato.
- Sia  $m = 5$ ,  $a$  vale 1, 2, 3 e 4. Per  $a = 1$  si ha  $1^5 \pmod{5} = 1$ . Verificato.  
Per  $a = 2$ ,  $2^5 \pmod{5} = 2$ . Per  $a = 3$ ,  $3^5 \pmod{5} = 3$ . Per  $a = 4$   $4^5 \pmod{5} = 4$ . Verificato  
in tutti i casi.

Se non si verifica per almeno un valore di  $a$ , vuol dire che il numero  $m$  non è primo ma è un numero composto. Per esempio, con  $m = 4$ , si ottiene che  $a = 1, 2$  e  $3$ .

Per  $a = 1 \Rightarrow 1^4 \pmod{4} = 1$ , verificato.

Per  $a = 2 \Rightarrow 2^4 \pmod{4} = 0$ , non verificato.

Per  $a = 3 \Rightarrow 3^4 \pmod{4} = 1$ , non verificato. Pertanto, il numero quattro non è un numero primo ma è un numero composto.

Purtroppo, non è possibile affermare che  $m$  è un numero primo anche se per ogni  $a$  appartenente all'intervallo aperto  $(0, m)$  sia verificata  $a^m \pmod{m} = a$ . Esistono infatti, numeri composti dal prodotto di numeri primi che soddisfano il teorema ma che non sono primi. In questo caso si parla di numeri di Carmichael, cioè numeri composti che si comportano come numeri primi per tutte le

- 
1. Piccolo teorema di Fermat: è un caso particolare del teorema di Eulero. Se  $m$  è un numero primo ed  $a$  non è un suo multiplo, si ha  $a^m \pmod{m} = a$ , per tutti i valori naturali di  $a$  appartenenti all'intervallo aperto  $(0, m)$ . Questo teorema fu enunciato nel 1679; mentre la prima dimostrazione è dovuta ad Eulero nel 1736, che ne diede una formulazione generale (vedi nota 3).
  2. Grande teorema di Fermat: se  $n$  è un numero naturale maggiore di 2, non esistono valori interi  $x, y, z$  tali che  $x^n + y^n = z^n$ . Del teorema non si conosce tuttora una dimostrazione generale. E' stato dimostrato per  $n = 4$  da Fermat; per  $n = 3$  da Eulero, per  $n = 5$  da Legendre, per  $n = 14$  da Lejeune-Dirichlet, per  $n = 7$  da Lamè, per  $n < 100$  da Kummel e per  $n < 7000$  da Dickson.
  3. Principio di Fermat in ottica: un raggio luminoso che vada da un punto A ad un punto B segue il cammino al quale corrisponde il minimo tempo; il principio vale anche se il mezzo è costituito da più zone, separatamente omogenee. Come conseguenza vi sono le leggi di rifrazione.
  4. Spirale di fermat: spirale di equazione polare  $\rho = a \cdot \phi^n$ , con  $n$  intero positivo ed  $a$  costante reale.

**ARITMETICA MODULARE**

basi, ossia per tutti i valori di  $a$  validi per il teorema. Per esempio, il numero composto  $1729 = 7 \cdot 13 \cdot 19$ .

Esistono anche alcuni numeri composti, chiamati pseudoprimi, che si comportano come se fossero primi solo per un numero limitato di basi, cioè di valori possibili per  $a$ .

Per esempio, il numero  $341 = 11 \cdot 31$  verifica il teorema con 120 basi su 340 totali.

Un altro esempio è il numero composto 91, dato dal prodotto di 7 e 13. In questo caso 91 è uno pseudoprimo in 48 basi su 90.

Un ultimo caso è il numero composto 15, dato dal prodotto di 3 e di 5. Risulta pseudoprimo in 8 basi su 14.

Fortunatamente, se confrontati con i numeri primi, i numeri di Carmichael, numeri pseudoprimi in ogni base, sono molto rari; non è così per i numeri pseudoprimi per alcune basi, come visto nei tre esempi precedenti.

Vediamo, adesso, le probabilità che un numero non venga riconosciuto come numero composto dal test di Fermat.

Scegliamo a caso una base del numero 15; la probabilità che venga considerato un numero primo

è pari al rapporto tra le basi (8) per le quali è primo e le totalità delle basi (14):  $\frac{8}{14} = 0,57$ .

Se riproviamo, nuovamente, avremo un diverso rapporto:  $\frac{7}{13} = 0,54$ ; andando avanti, le probabilità che si ottengono decrescono.

La domanda che dobbiamo porci, a questo punto, è del tipo: se il numero 15 non viene riconosciuto come numero composto per  $n$  volte consecutive, che probabilità ha di superare il test di Fermat per la  $(n + 1)$ -esima volta?

Siccome le basi sono considerate indipendenti, basta fare il prodotto tra le  $n$  probabilità a partire dalla più alta. Nel caso in esempio, la risposta è  $0,57 \cdot 0,54 \cdot 0,5 \cdot 0,45 = 0,07$ .

***ARITMETICA MODULARE***

In conclusione, escludendo i numeri di Carmichael, risulta che i numeri pseudoprimi per alcune basi, sono  $t_{a,m}$ , per un numero di basi  $a$ , che, al più, è circa la metà di quelli compresi nell'intervallo aperto  $(0,m)$ .

Se, quindi, il controllo della primalità è su un numero molto grande, scegliendo a caso 100 basi differenti, la probabilità che un numero pseudoprimo non venga riconosciuto come numero composto, nemmeno al 101-esimo test, è circa minore o uguale di:

$$P = \left( \frac{1}{2^{100}} \right) = \frac{1}{1024^{10}} \text{ circa uguale a } \frac{1}{10^{30}}.$$

Pertanto, un numero che non viene riconosciuto come numero composto dopo 100 test di Fermat è quasi certamente un numero primo.