Il nome dell'algoritmo deriva dalla prima lettera dei cognomi di coloro che lo inventarono nell'Aprile del 1977: Ronald L. **R**ivest, Adi **S**hamir e Leonard M. **A**dleman.

I campi di impiego dell'algoritmo sono diversi e variano passando dall'uso all'interno di programmi fino ad arrivare a costituire l'elemento portante di vere e proprie tecnologie di rete. Fra le varie applicazioni possiamo sicuramente ricordare:

- PGP;
- Secure Socket Layer (SSL)
- Secure Electronic Transactions (SET);

Analisi dell'algoritmo

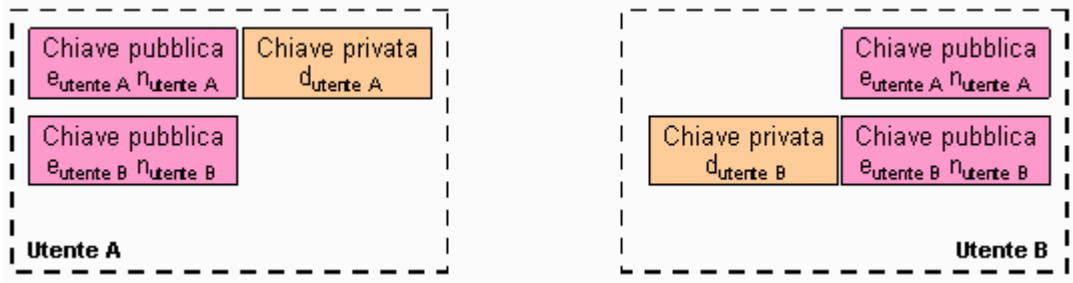
In linea di principio, l'analisi dell'algoritmo potrebbe essere facilmente suddivisa in due parti: la generazione della coppia di chiavi e l'utilizzo delle stesse.

La prima parte, la generazione della coppia di chiavi, viene solitamente effettuata in questo modo:

- vengono scelti due numeri primi p, q molto grandi;
- viene calcolato n=pq, e la funzione di Eulero $\Phi(n) = (p - 1)(q - 1)$ dopo di che i due primi p, q vengono eliminati;
- si sceglie un intero e minore di $\Phi(n)$ e primo con esso;
- utilizzando la versione estesa dell'algoritmo di Euclide viene calcolato l'intero d così da avere $e * d = 1 \bmod \Phi(n)$;
- vengono resi pubblici i valori e,n che costituiscono la chiave pubblica e mantenuto segreto d che, utilizzato con n rappresenta la chiave privata.

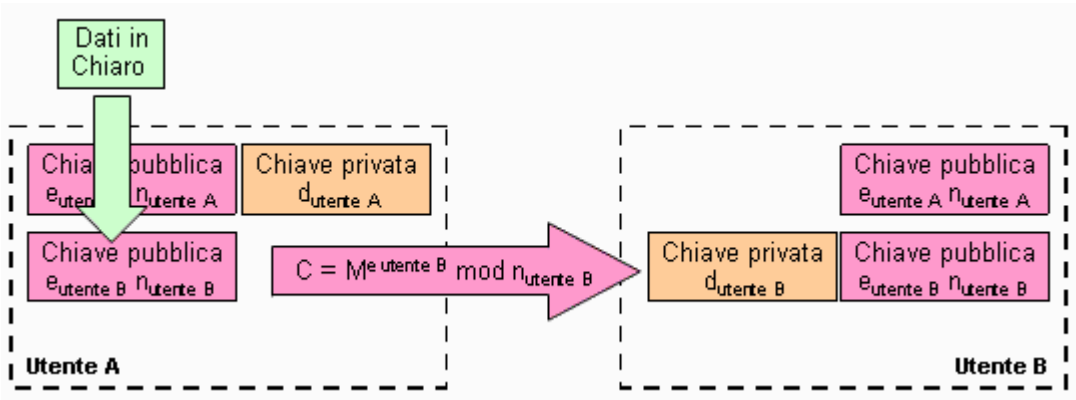
Sicuramente vi starete chiedendo su cosa viene basata l'inviolabilità dell'algoritmo. La risposta è molto semplice e coinvolge l'impiego di diversi principi matematici. (****Vedi l'appendice alla fine del documento***)

Una volta generata la coppia di chiavi, vediamo insieme le operazioni effettuabili, immaginando di avere due utenti, l'Utente A e l'Utente B, entrambi con la propria coppia di chiavi, pubblica e privata, più la chiave pubblica della controparte:



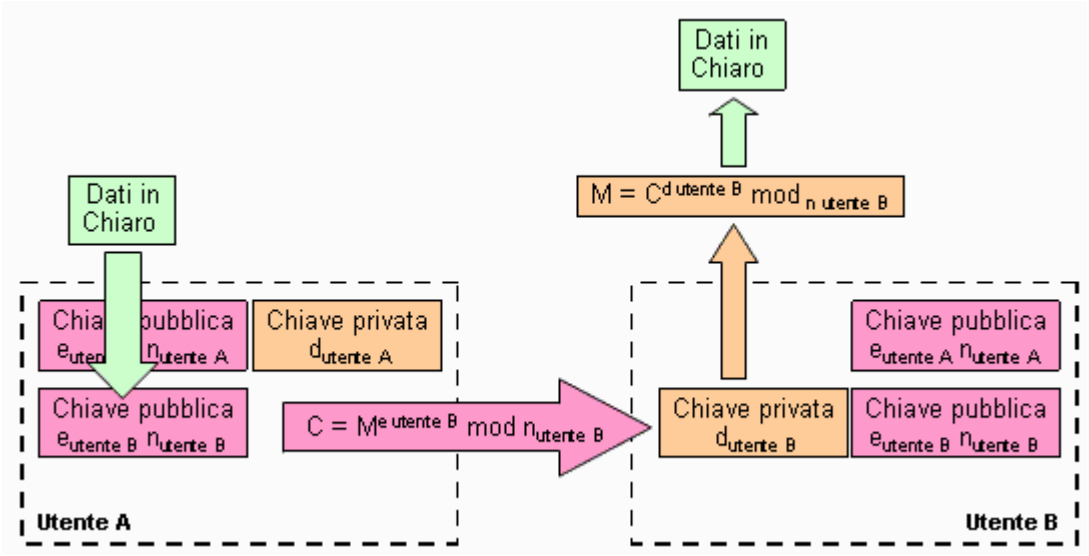
Cifratura

L'Utente A deve inviare del materiale cifrato all'Utente B. Per fare questo utilizzerà la chiave pubblica dell'Utente B effettuando queste operazioni:



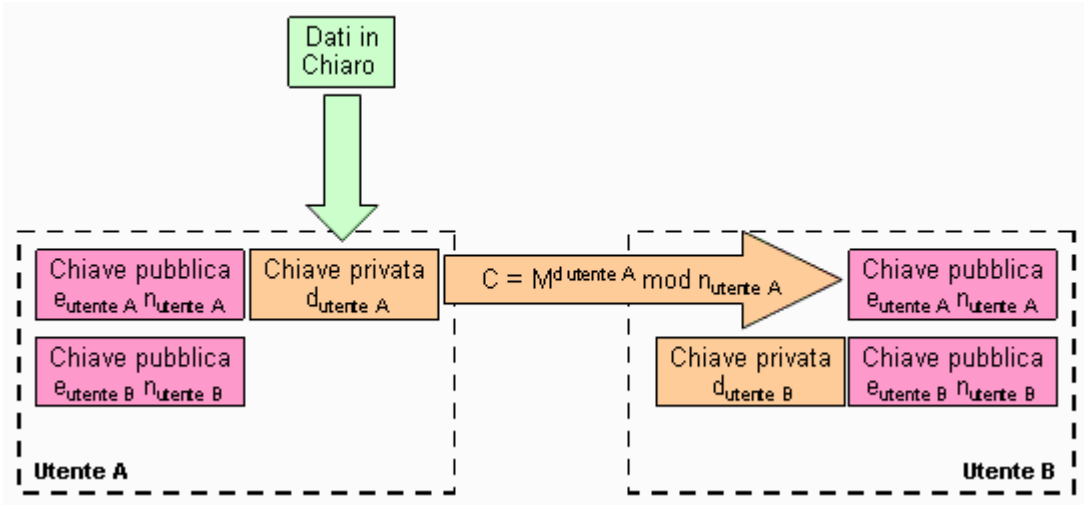
Decifratura

Ricevuto i dati cifrati, l'Utente B utilizzerà la sua chiave privata per eseguire l'operazione opposta di decifratura.



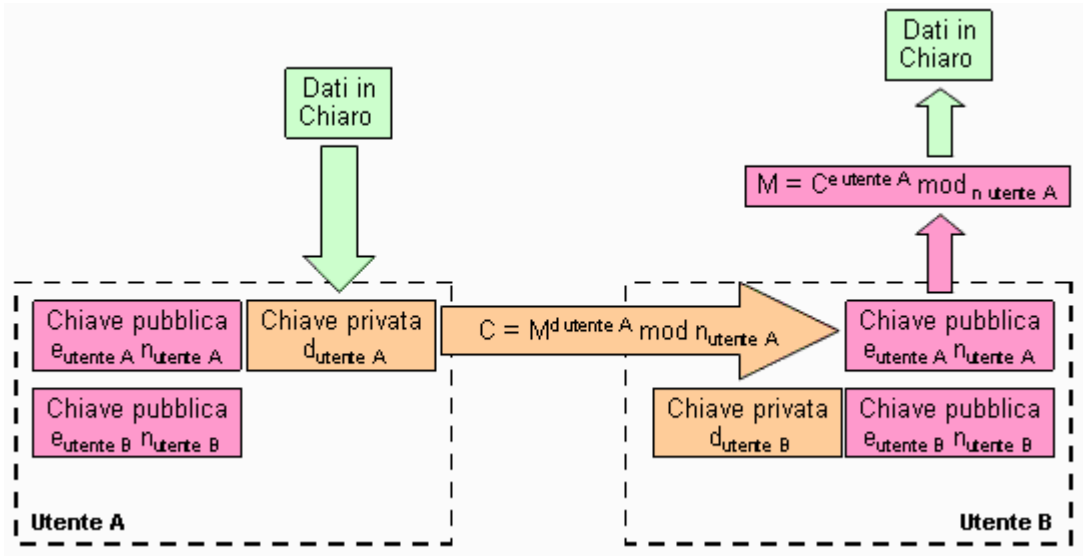
Firma

L'operazione di firma prevede l'utilizzo della chiave privata dell'Utente A sui dati, come riportato di seguito:



Verifica

Per verificare i dati ricevuti, l'Utente B utilizzerà la chiave pubblica dell'utente A:



Velocità dell'algoritmo

Si stima che il rapporto tra la velocità di un cifrario simmetrico e quella di un cifrario asimmetrico sia indicativamente un millesimo nelle realizzazioni hardware e un centesimo in quelle software. A titolo puramente indicativo, ecco quanto riportato sulla rivista Byte Italia del Maggio 1998. La tabella si riferisce ai tempi in secondi necessari all'elaborazione di un messaggio di un singolo carattere su un sistema Pentium 133.

Operazione	512 bit	768 bit	1024 bit
Cifratura	0,03	0,05	0,08
Decifratura	0,16	0,48	0,93
Firma	0,16	0,52	0,97
Verifica	0,02	0,07	0,08

APPENDICE MATEMATICA

Il matematico Pierre de Fermat scoprì che se come modulo veniva utilizzato un numero primo, l'elevamento a potenza di un numero utilizzando come potenza il numero primo scelto meno 1, equivaleva ad 1.

In altre parole, avendo un numero primo **p** ed un numero positivo **m**, inferiore di **p** si avrà:

$$m^{(p-1)} \bmod p = 1$$

Verifichiamolo insieme utilizzando un esempio. A quanto equivale 7^{10} mod 11?

Seguendo quanto scoperto da Fermat, dovrebbe essere uguale ad 1. Proviamolo:

$7^{10} = 282475249$

$282475249 / 11 = 25679568$ con resto di 1

quindi 7^{10} mod 11 = 1

Non è tutto, un altro matematico, Eulero, scoprì che una relazione simile esiste utilizzando come modulo il prodotto di due numeri primi. In pratica, dato **n = p * q** con **p** e **q** primi, ed **m** primo relativo con **n**, si avrà:

$$m^{(p-1)(q-1)} \bmod n = 1$$

Naturalmente sostituendo a **(p - 1)(q - 1)** la funzione di Eulero **Φ(n)** si otterrebbe sempre una relazione simile:

$$m^{\Phi(n)} \bmod n = 1$$

Esempio:

Avendo **p = 11** e **q = 5**, **n** sarà uguale a **p * q = 11 * 5 = 55** e quindi Φ(n) sarà uguale a **(p - 1)(q - 1) = (11 - 1)(5 - 1) = 10 * 4 = 40**.

Come abbiamo detto in precedenza affinchè la relazione sia verificata occorrerà che **m** sia primo relativo con **n**. Nel nostro caso, essendo **n = 55**, basterà avere **m = 38** per ottenere quanto scoperto da Eulero:

$$38^{40} \bmod 55 = 1$$

Verifichiamolo:

Forse utilizzando una qualsiasi calcolatrice ci potrebbero essere dei problemi ma, basandoci su una delle proprietà delle potenze, la cosa risulterà più semplice, infatti, 38^{40} può essere scritto come:

$38^{10} * 38^{10} * 38^{10} * 38^{10} = 38^{(10 + 10 + 10 + 10)} = 38^{40}$

e quindi, visto che $38^{10} = 6278211847988224$, dividendolo per 55 si avrà:

$6278211847988224 / 55 = 114149306327058$ con resto 34

ed allora ne segue che:

$38^{40} \bmod 55 = (38^{10} * 38^{10} * 38^{10} * 38^{10}) \bmod 55$

e visto che $38^{10} \bmod 55 = 34$, sostituendo con il valore ottenuto:

$$= (34 * 34 * 34 * 34) \bmod 55$$

$$= 1336336 \bmod 55 \quad (1336336 / 55 = 24297 \text{ resto } 1)$$

$$= 1 \bmod 55$$

Verificata la relazione, torniamo alla forma generica e proviamo a moltiplicare entrambi i lati dell'equazione per **m** così da avere:

$$m^{(p-1)(q-1)} * m \bmod n = 1 * m$$

e siccome potremmo scrivere **m** come $\mathbf{m^1}$ otterremo:

$$m^{[(p-1)(q-1)]+1} \bmod n = m$$

quindi, una funzione ed un esponente che ci permettono di ottenere in un qualche modo, il valore di partenza, conoscendo quello di arrivo.

Come viene sfruttato tutto questo nell'algoritmo RSA? Trovando un numero **e** minore di **Φ(n)** e primo con esso, ed un numero **d**, tale che:

$$e * d = [(p - 1) * (q - 1)] + 1$$

oppure utilizzando l'aritmetica in modulo e sostituendo a **(p - 1) * (q - 1)** la funzione di Eulero:

$$e * d = 1 \bmod \Phi(n)$$

in questo modo, utilizzando il principio appena esposto, si avrà per il valore **m**, questa equazione:

$$m^e \bmod n = c$$

Quale sarà il valore di **c**? Naturalmente variabile, in base ai valori utilizzati e di regola a noi sconosciuto, ma questo non è un problema, anzi, ben si presta a rappresentare il nostro dato originario nella forma cifrata.

Cosa avviene se proviamo ad effettuare l'operazione opposta? La risposta è semplice, otterremo nuovamente il nostro valore di partenza:

$$c^d \bmod n = m$$

Perche? Per il risultato avuto in precedenza, sappiamo che a **c** possiamo sostituire $\mathbf{m^e \bmod n}$, quindi:

$$(m^e)^d \bmod n$$

che equivale a:

$$m^{e*d} \bmod n$$

ma a cosa era uguale **e * d**? Per definizione a **(p - 1) * (q - 1) + 1**, allora sostituiamo ed otteniamo:

$$m^{[(p-1)(q-1)]+1} \bmod n$$

che come abbiamo già visto in precedenza è uguale al nostro valore di partenza:

$$m^{[(p-1)(q-1)]+1} \bmod n = m$$

Matematica di base

Elevamento a potenza

Dati un numero reale **a** ed un numero intero **n** positivo, si dice potenza n-esima di **a** il prodotto di **n** fattori uguali ad **a**.

Quindi:

$$a^n = a*a*a \ldots *a \text{ (n volte)}$$

Esempio:

$$2^7 = 2*2*2*2*2*2*2 = 128$$

Il numero reale **a** si dice base mentre il numero intero **n** si dice esponente della potenza $\mathbf{a^n}$.

Proprietà delle potenze

Il prodotto di due (o più) potenze di uguale base è una potenza che ha per base la stessa base e per esponente la somma degli esponenti:

$$a^n * a^m = a^{(n+m)}$$

Esempio:

$2^3 * 2^4 = 2^{(3+4)} = 2^7$ Prova: $2^3 = 2*2*2 = 8$

$2^4 = 2*2*2*2 = 16 * 8 = 128$

$2^7 = 2*2*2*2*2*2*2 = 128$

La potenza di una potenza è ancora una potenza che ha come base la stessa base e come esponente il prodotto degli esponenti:

$$(a^n)^m = a^{(n*m)}$$

Esempio:

Normalmente si ha:

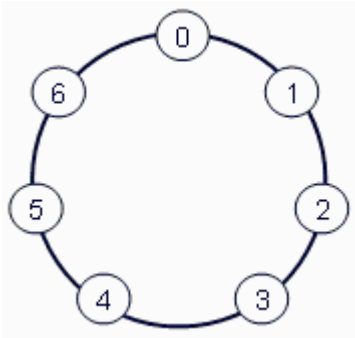
$$(2^3)^4 = (8)^4 = 4096$$

applicando la proprietà:

$$(2^3)^4 = 2^{(3*4)} = 2^{12} = 4096$$

Aritmetica in modulo

L'aritmetica dei moduli prende in considerazione un gruppo limitato di numeri disposti ad anello, un po' come le ore sul quadrante dell'orologio.



Questo quadrante per esempio corrisponde al modulo 7, scritto (mod 7), e comprende solo 7 numeri, da 0 a 6.

Per calcolare 2 + 3 si partirà da 2 e ci si sposterà di 3 numeri, ottenendo 5. Per calcolare 2 + 6 si partirà da 2 e ci si sposterà di 6 numeri. In questo modo, attraversando l'intero anello, si otterrà come risultato 1.

In pratica:

```
2 + 3 = 5 mod 7

2 + 6 = 1 mod 7
```

In generale, per effettuare delle operazioni in modulo, bisognerà procedere in questo modo:

- Effettuare il calcolo secondo l'aritmetica normale;
- Dividere il risultato per il modulo (x);
- Il resto ottenuto corrisponderà al risultato (mod x).

Esempio:

Calcolare 11 * 99 mod 13.

Effettuiamo il calcolo secondo l'aritmetica normale ed otteniamo:

```
11 * 99 = 1089;
```

Dividiamo il risultato per il modulo:

```
1089 / 13 = 83 con un resto di 10 (visto che 13 * 83 = 1079);
```

Il risultato finale è quindi:

```
11 * 99 = 10 mod 13
```

Questo processo viene anche chiamato riduzione in modulo. In pratica, sottraendo il modulo (e tutti i multipli del modulo) un numero viene "ridotto" in un numero più piccolo. Nell'esempio precedente, quando il numero 1089 viene "ridotto" a 10 si potrebbe dire che "1089 viene ridotto modulo 13".

Inversi in modulo

Due numeri sono inversi in modulo l'uno dell'altro se il loro prodotto è uguale ad 1.

Esempio:

Utilizziamo i numeri 7, 343 ed il modulo 2400:

$$7 * 343 = 2401;$$

$$7 * 343 = 1 \bmod 2400$$

Numeri primi e test di Fermat

Un numero maggiore di 1 si dice primo se è divisibile solo per se stesso e per l'unità altrimenti si dirà composto.

L'insieme dei numeri primi è infinito e non se ne conosce né una formula di generazione né una che ne dia infiniti. Esistono però diversi metodi per trovare numeri primi, fra questi, possiamo utilizzare il seguente:

1. Scegliere un numero casuale;
2. Assicurarsi che sia dispari, aggiungendo eventualmente 1. Questo perchè tutti i numeri pari sono divisibili per 2;
3. Dividere il numero per i principali numeri primi conosciuti (3, 5, 7, 11, ...). Se il numero non è divisibile continuare con il punto 4, altrimenti saltare al punto 5;
4. Ripetere per quattro volte il test di Fermat, utilizzando ogni volta un primo diverso (2, 3, 5, 7). Se il test viene superato, considerare il numero primo, altrimenti passare al punto 5;
5. Aggiungere due al numero e tornare al passo 3.

In cosa consiste il test di Fermat riportato al punto 4?

Il test si basa su una scoperta di Fermat, secondo cui avendo un numero primo **p**, ed un numero **m**, inferiore a **p**, si ha:

$$m^{(p - 1)} \bmod p = 1$$

da cui **m** sarà uguale a:

$$m * m^{(p - 1)} \bmod p = m * 1$$
$$m^{(p - 1) + 1} \bmod p = m$$
$$m^{p} \bmod p = m$$

questo naturalmente partendo dal presupposto che **p** sia primo. E se non lo fosse? Il risultato non dovrebbe, a parte alcuni casi, corrispondere ad **m**.

Nella pratica, vedremo dopo perchè, si preferisce utilizzare per **m** un numero primo. Esempio:

$$7^{13} \bmod 13 = 7$$

$7^{15} \bmod 15 = 13$

Ma cosa accade se il numero da testare è uguale a 6 ed **m** è uguale a 3?

$3^{6} \bmod 6 = 3$

Dal risultato ottenuto si potrebbe arrivare erroneamente alla conclusione che 6 è un numero primo. Il problema risiede nel fatto che, come abbiamo detto in precedenza, quando **p** non è un numero primo il risultato potrebbe essere qualsiasi numero inferiore a **p** stesso. E' per questo motivo che in questo caso abbiamo ottenuto 3, che è in effetti inferiore al modulo utilizzato, cioè 6.

Per evitare questo, ed essere relativamente sicuri del risultato, è conveniente effettuare più volte il test utilizzando per **m** diversi numeri primi. Infatti già per **m = 5**, si ha:

$5^{6} \bmod 6 = 1$

Che conferma quanto già noto. 6 non è un numero primo. Ma quante volte conviene fare il test per essere proprio sicuri? Diverse fonti danno come numero minimo di volte almeno quattro, utilizzando i numeri primi 2, 3, 5, 7.

Passiamo adesso ad un esempio che prenda in esame tutto il procedimento:

1. Iniziamo scegliendo un numero a caso, 288;
2. E' pari, bisognerà quindi renderlo dispari aggiungendo 1, otteniamo 289;
3. Proviamo a dividerlo per alcuni primi conosciuti, (3, 5, 7, 11). Scopriamo che il numero scelto non è divisibile, quindi passiamo al primo passaggio del test di Fermat;
4. Cominciamo prendendo **m = 2**
   $2^{289} \bmod 289 = (2^{100} * 2^{100} * 2^{89}) \bmod 289 = (135 * 135 * 121) \bmod 289 = 2205225 \bmod 289 = 155$
   Apparentemente 289 non è primo, riproviamo con **m = 3**
   $3^{289} \bmod 289 = 224$
   Proviamo con **m = 5**
   $5^{289} \bmod 289 = 158$
   Proviamo con **m = 7**
   $7^{289} \bmod 289 = 75$
   Il test è fallito per quattro volte. Saltiamo al passo successivo.
5. Aggiungiamo 2 al numero scelto: 289 + 2 = 291. E torniamo ad applicare quanto fatto al passo 3;
6. Dividiamo il numero per la lista di primi noti scelta in precedenza e ci accorgiamo che 291 / 3 = 97. Non va bene;
7. Aggiungiamo 2: 291 + 2 = 293;
8. 293 non è divisibile per la lista di primi noti utilizzata come campione. Bene, passiamo al test di Fermat.
9. Naturalmente iniziamo con **m = 2**
   $2^{293} \bmod 293 = 2$, siamo sulla buona strada, continuiamo
   $3^{293} \bmod 293 = 3$
   $5^{293} \bmod 293 = 5$
   $7^{293} \bmod 293 = 7$
10. I diversi passaggi sono stati superati, ne segue che 293 è da considerarsi primo.

Scomposizione di un numero in fattori primi

La scomposizione di un numero in fattori primi si basa su questi due teoremi:

- Ogni numero naturale, diverso da 1, può essere scomposto nel prodotto di fattori primi in uno ed un solo modo a meno dell'ordine dei fattori.
- Un numero naturale **n** composto è uguale al prodotto di fattori primi, cioè ammette come divisori almeno un altro numero naturale diverso da 1 e da **n**.

Esempio:

Scomposizione in fattori primi del numero 48.

```
48 | 2          48 = 2^4 * 3
24 | 2
12 | 2
 6 | 2
 3 | 3
 1 | 1
```

Massimo comun divisore (M.C.D.)

Per calcolare il M.C.D. di due o più numeri si può seguire il procedimento indicato nel seguente esempio:

Siano 360, 5940 e 300 i tre numeri dei quali vogliamo calcolare il M.C.D.
Scomponiamoli in fattori primi:

```
360 | 2    5940 | 2    300 | 2       360 = 2^3 * 3^2 * 5
180 | 2    2970 | 2    150 | 2      5940 = 2^2 * 3^3 * 5 * 11
 90 | 2    1485 | 3     75 | 3       300 = 2^2 * 3 * 5^2
 45 | 3     495 | 3     25 | 5
 15 | 3     165 | 3      5 | 5
  5 | 5      55 | 5      1 | 1
  1 | 1      11 | 11
              1 | 1
```

Ricordando il criterio generale di divisibilità per cui, ogni divisore di un numero può contenere solo fattori che figurano nella sua scomposizione con esponenti uguali o inferiori a quelli con i quali essi figurano in tale scomposizione, risulta:

M.C.D. (360, 5940, 300) = $2^2 * 3 * 5 = 60$

Algoritmo di Euclide

E' possibile determinare il Massimo Comun Divisore (M.C.D.) di due numeri naturali utilizzando l'algoritmo euclideo.

In pratica, dividendo due numeri naturali **a** e **b,** naturalmente con **a > b**, si ottiene come risultato un quoziente **q**, ed un eventuale resto, **r**:

$$a / b = q + r$$

Se **r** sarà uguale a 0, **b** sarà un divisore di **a** e perciò si avrà che:

M.C.D. (a, b) = b

Se **r** è diverso da 0, ogni divisore di **a** e di **b** sarà anche divisore di **r** poiché:

```
r = a - b * q
```

quindi sarà

```
M.C.D. (a, b) = M.C.D. (b, r);
```

Il vantaggio di questa uguaglianza sta nel fatto che la ricerca del M.C.D. si sposta da **a**, **b** verso **b**, **r**, che sono numeri rispettivamente minori di **a** e **b**.

Dividiamo ora **b** per **r**; siano **q1** e **r1** rispettivamente quoziente e resto:

```
b = (r * q1) + r1
```

Se **r1** = 0, **r** è un divisore di **b**, perciò:

```
M.C.D. (b, r) = r.
```

Se **r1** è diverso da 0 dividiamo **r** per **r1** e, indicando con **q2** ed **r2** rispettivamente quoziente e resto, sarà:

```
r = (r1 * q2) + r2
```

Se **r2** è uguale a 0, **r1** è un divisore di **r** e quindi di **b** e di **a**, possiamo allora scrivere:

```
M.C.D. (r, r1) = M.C.D. (b, r) = M.C.D. (a, b) = r1
```

Se **r2** è diverso da 0 si continua fino a quando si perviene ad un resto necessariamente nullo.

In pratica, utilizzando l'algoritmo, il M.C.D. di due numeri naturali corrisponderà all'ultimo resto non nullo.

Esempio 1:

Calcolare il M.C.D. tra 18 e 6.

```
18 / 6 = 3     r = 0
```

Quindi M.C.D. (18, 6) = 6

Esempio 2:

Calcolare il M.C.D. tra 1290 e 465.

```
1290 / 465 = 2     r = 360
 465 / 360 = 1     r = 105
 360 / 105 = 3     r = 45
 105 / 45  = 2     r = 15     <- Ultimo resto non nullo
  45 / 15  = 3     r = 0
```

Si ha perciò: M.C.D. (1280, 465) = 15

Versione estesa dell'algoritmo di Euclide

Dati due numeri naturali **a > b**, la versione estesa dell'algoritmo di Euclide ci permette di calcolare, non solo il M.C.D. ma anche due interi **x** ed **y** per cui:

M.C.D.(a, b) = ax + by

Per giungere a questo sarà necessario costruire una tabella in cui, la parte sinistra sarà data dalla successione delle divisioni con i relativi resti mentre la parte destra consisterà in due colonne che ci permetteranno di calcolare **x** ed **y**.

In pratica, le operazioni da svolgere saranno le seguenti:

1. Nelle due colonne a destra iniziamo riportando i valori:

```
1 0
0 1
```

2. Inseriamo nella colonna a sinistra (riga inferiore) il risultato della divisione di **a** per **b**, nella forma a = **q**uoziente(b) + **r**esto (con **r** compreso tra e **0** e **b**);

3. Se **r** è uguale a 0, saltiamo al passo 5, altrimenti se la riga è superiore ad 1, in ognuna delle due colonne a destra, aggiungiamo un nuovo valore, calcolato nel modo seguente:

$$x = q_{(riga - 1)}\ x_{(riga - 1)} + x_{(riga - 2)}$$

$$y = q_{(riga - 1)}\ y_{(riga - 1)} + y_{(riga - 2)}$$

4. Sostituiamo **b** ad **a** ed **r** a **b** e torniamo al passo 2.

5. Avendo ottenuto **r = 0**, il M.C.D. sarà uguale all'ultimo resto non nullo, in pratica il valore di **b** nell'ultima divisione, mentre, supponendo che **x'** ed **y'** siano gli ultimi due valori delle colonne a destra, potremmo avere:

M.C.D.(a, b) = ax' - by' così che x = x', y = -y'

oppure

M.C.D.(a, b) = by' - ax' e quindi x = -x', y = y'

Facciamo un esempio, prendendo i due valori già visti in precedenza per l'Algoritmo di Euclide, e cioè 1290 e 465:

riga	a	q	b	r	x	y
0					1	0
1	1290	= 2	x 465	+ 360	0	1
2	465	= 1	x 360	+ 105	1	2
3	360	= 3	x 105	+ 45	1	3
4	105	= 2	x 45	+ 15	4	11
5	45	= 3	x 15	+ 0	9	25

e quindi avremo:

15 = -9(1290) + 25(465)

Primi relativi

Due o più numeri si diranno primi relativi o primi tra loro se, scomposti in fattori primi, non avranno divisori comuni all'infuori dell'unità.

Esempio:

Verificare se i numeri 15 e 28 sono primi tra di loro.

```
15 | 3          28 | 2          M.C.D. (15, 28) = 1
 5 | 5          14 | 2
 1 | 1           7 | 7
                 1 | 1
```

Funzione di Eulero

Per un intero **n** > 1 si definisce la funzione di Eulero **Φ(n)** come il numero di interi minori di **n** e relativamente primi con esso ed in particolare **Φ(n) = n - 1** se **n** è primo.

Un procedimento di calcolo, per **n > 1** non primo, è il seguente:

$$\Phi(n) = n * (1 - 1/p_l) * ... * (1 - 1/p_k)$$

dove p_l, ..., p_k sono i fattori primi di **n** presi senza molteplicità.

Esempio:

Per questo esempio useremo il numero 12.

Scomponiamolo in fattori primi:

```
12 | 3
 6 | 3
 2 | 2
 1 | 1
```

Dopo di che passiamo a vedere come appare la funzione:

$$\Phi(12) = 12 * (1 - 1/3) * (1 - 1/2) = 12 * 2/3 * 1/2 = 4$$

Sarà facile dimostrare che i 4 numeri interi primi relativi con 12 sono: 1, 5, 7 e 11.

Se **n** è il prodotto di due numeri primi, **n = p * q**, si ottiene:

$$\Phi(n) = n * (1-1/p) * (1 - 1/q)= (p-1) * (q-1)$$

Esempio:

Utilizzando il numero 6, dato dal prodotto dei due numeri primi 3 e 2:

$$\Phi(6)=6(1-1/3)(1-1/2)=(3-1)(2-1)=2$$

I due numeri primi relativi con 6 sono naturalmente 1 e 5.