# IL PICCOLO GIGANTE

# Cioè

# IL PICCOLO TEOREMA DI FERMAT

Pierre Fermat

*https://upload.wikimedia.org/wikipedia/commons/f/f3/Pierre_de_Fermat.jpg*
*See page for author [Public domain], via Wikimedia Commons*

## 1. IL TEOREMA

Il "piccolo teorema di Fermat" (pron FERMÀ) è un semplice teorema che permette quasi incredibili calcoli di un tipo speciale. (Il grande teorema, solo recentemente dimostrato è quello che afferma che non si possono trovare quattro numeri x,y,z,a, che soddisfacciano la relazione $x^a+y^a= z^a$, per a >2).

Pierre Fermat era un avvocato/magistrato Francese del Seicento che fece il seguente ragionamento:

Prendiamo due numeri, un numero primo *p* e un numero *a* che sia primo con *p* (che cioè non è divisibile per *p*). Per andar sul sicuro, noi prendiamo due numeri primi, per esempio 7 e 5, contando sul fatto che due primi in senso assoluto sono sempre anche primi fra loro.
Come noi sappiamo, dividendo un numero per sette abbiamo sei resti possibili, cioè tutti i numeri più piccoli di sette.

Adesso prendiamo 5 e dividiamo per sette, otteniamo resto **5**.

Prendiamo 2 x5 e dividiamo per sette, otteniamo resto **3**.
Prendiamo 3x5 e dividiamo per sette, resto **1**
Prendiamo 4x5 dividiamo per 7, resto **6**
Prendiamo 5x5, dividiamo per sette, resto **4**
Prendiamo 6x5, dividiamo per sette, resto **2**.

In altre parole abbiamo moltiplicato 5 per i sei numeri più piccoli di sette, che sono tutti primi con sette, che è un numero primo e quindi non ha divisori. Il numero 7 non divide 5 (perché 5 è primo) e non divide nessuno dei numeri che moltiplicano 5 (perché tutti più piccoli di 7), per cui nessuno dei prodotti ( 1 x 5, 2 x 5, 3 x 5….) è divisibile per 7. Tutti i prodotti lasciano un resto. Infatti 7 non può dividere per esempio 4 x 5, perché se un numero primo divide il prodotto di due fattori, o divide l'uno o divide l'altro. Questo, chiamato anche Lemma di Euclide, è evidentemente un teorema fondamentale, ma chi lo sa dimostrare? In effetti la dimostrazione è tutt'altro che elementare, pur senza essere riservata a un piccolo numero di eletti. La si può però trovare in questo sito, nella pagina dal titolo "Divisione – Tre variazioni sul tema".

Inoltre, due resti non possono essere eguali.
La dimostrazione è per assurdo: in tal caso, avremmo R7(5 *m*) = R7(5 *n*), e , poiché la differenza dei resti è il resto della differenza, ne seguirebbe R7(5(*m* - *n*))=0, cioè 7 dovrebbe dividere la differenza (*m* - *n*), visto che non divide 5 per ipotesi. Ma (*m* - *n*) è minore di 7, visto che sono minori di 7 sia *m* che *n*, e quindi abbiamo un assurdo, perché tutti i numeri minori di 7 sono primi con 7.

Nel nostro caso abbiamo trovato tutti i sei resti possibili della divisione per sette in un qualche ordine particolare (5,3,1,6,4,2) , ma il loro prodotto è uguale a 1 x 2 x 3 x 4 x 5 x 6.
Abbiamo quindi l'eguaglianza:

$$R7\ (5^6 \times 1x2x3x4x5x6) = 1x2x3x4x5x6.$$

**Ma sappiamo che il resto del prodotto è eguale al prodotto dei resti. Questo, se non lo sappiamo, è facile da dimostrare (si veda la pagina "Congruenze elementari" su questo stesso sito).**
**Quindi, chiamando R7 il resto della divisione per 7 di ambo i membri:**

$R7\ (5^6) \times R7\ (1x2x3x4x5x6) = R7(1x2x3x4x5x6)$
Semplificando: $R7\ (5^6)=1$
O anche

$$R7\ (5^6-1)=0$$

Questo è il nostro gigante.
Generalizzando il nostro risultato, esso ci dice che, dati due numeri primi fra loro *a* e *p*, il resto della divisione per *p* di $a^{(p-1)}$ è 1. O anche: il numero $a^{(p-1)} - 1$ è divisibile per *p*. Non si scappa.

Dato che lo abbiamo dimostrato solo per due numeri specifici, 5 e 7, questa non può essere considerata una dimostrazione. Tuttavia, quel che abbiamo fatto è molto simile ad una dimostrazione, perché può essere ripetuto per qualsiasi coppia di numeri primi. Se siete forti a usare lettere invece di numeri, dopo qualche esercizio potete forse trovare da soli una dimostrazione per due numeri qualsiasi *a* e *p*, di cui non occorre che *a* sia primo, solo che sia primo con *p, che invece è primo*.

La dimostrazione incomincia così: dati *a* e *p*, primi fra loro, si prendono i prodotti di *a* per i numeri primi con *p*, più piccoli di *p*, che sono tutti i *p-1* numeri più piccoli di *p*, dato che quest'ultimo è

primo. Ogni prodotto *a, 2a,3a, …(p-1)a* viene diviso per *p*. Da ciascuna di queste *(p-1)* divisioni viene un resto (nessuno dei due fattori del prodotto è divisibile per p). Ma tutti i *(p-1)* resti sono differenti. Perché?
Supponiamo che dalla divisione per *p* di $m \cdot a$ e di $n \cdot a$ risultino due resti eguali.
Questo vorrebbe dire che *(m-n)a* diviso *p* dà resto zero, infatti R(*ma/p*) = R(*na/p*) e quindi R(*(m - n)a/p*)=0. E quindi, dato che *m-n* è più piccolo di *p*, *p* deve dividere *a*, poiché un numero primo che divide un prodotto di due fattori, o divide l'uno o divide l'altro. Ma *p* ed *a* dovevano essere primi fra loro e quindi l'ipotesi che due resti siano eguali è impossibile.
A questo punto continuate voi.

Per verificare il "piccolo" teorema avete bisogno di calcolatori potenti o programmi speciali, altrimenti non andate lontano, perché il resto di una divisione dipende criticamente dall'ultima cifra del dividendo e i calcolatori di rado prendono più di venti cifre.
Prendiamo un numero relativamente piccolo, per esempio 10, ed uno più grande, 113. Noi sappiamo che il resto della divisione di $10^{112}$ per 113 è uno. Ora, $10^{112}$ ha 122 cifre. Non è mica uno scherzo!

Il lettore attento può chiedersi: perché i numeri devono essere primi fra loro?
Per esempio nella coppia 3 e 6, 3 è primo come deve essere, ma 3 e 6 non sono primi fra loro. E' ancora vero che $6^2$ diviso 3 dà resto 1? No. Che cosa è successo?
Vediamo i resti di 6x1, 6x2, diviso 3: sono 0,0. Non sono 1,2 (= p-1) come era per 7. Quindi alla fine non possiamo semplificare i due prodotti 0,0 e 1,2.
In realtà la comparsa dello zero è quello che ci dice che il teorema non viene del tutto invalidato. In matematica non si può dividere per zero. Punto.

Una volta, in Giappone, chiesi ad un anziano professore: secondo Lei, quanti Giapponesi possono dimostrare sui due piedi il piccolo teorema di Fermat? Lui mi rispose: forse mille (uno su centoventimila Giapponesi). Io credo che fossero molti di più. Ma mi piacerebbe contribuire ad aumentare il numero di persone che ha almeno un'idea di questo notevolissimo teorema.

## 2. IL PICCOLO GIGANTE RIVISITATO.

Vediamo se possiamo estendere il concetto del "piccolo teorema" di Fermat.
Siccome sappiamo che, dati p e a primi,

$$a^{p-1} = 1, \text{ modulo } p$$

si potrebbe *congetturare* che p-1 non sia altro che la $\Phi(p)$ per il numero primo p e che la formula generale per il piccolo Teorema di Fermat sia precisamente

$$a^{\Phi(n)} = 1, \text{ modulo } n,$$

valida anche se n non è primo, purché a ed n siano primi fra loro. Naturalmente la $\Phi(n)$ è la funzione di Eulero di cui ho in
http://dainoequinoziale.it/scienze/matematica/2016/10/06/eulerphi.html.

Verifichiamo con qualche numero, ciò che in teoria dei numeri non funziona (quasi) mai, nel senso che illude (quasi) sempre.

| a | n | $\Phi$ (n) | $a^{\Phi(n)}$ | Resto della divisione di |
|---|---|---|---|---|

| | | | | $a^{\Phi(n)} - 1$ per n |
|---|---|---|---|---|
| 2 | 9 | 6 | 64 | 63/9 = 7, resto 0 |
| 3 | 4 | 2 | 9 | 8/4 = 2, resto 0 |
| 11 | 12 | 4 | 14641 | 14640/12 = 1220, resto 0 |
| 13 | 18 | 6 | 4826809 | 4826808/18 = 268156, resto 0 |

Questo però è uno dei pochi casi in cui da una'osservazione "sperimentale" tiriamo fuori una congettura corretta.

Che però non è impossibile da dimostrare.

Supponiamo dunque che *n* non sia un numero primo, ma valga 12. Tuttavia *a* e *n* devono restare primi fra loro, come abbiamo visto, per evitare che compaiano degli zeri nel prodotto. Come *a* scegliamo 5.
La Φ (12) vale 4, e infatti i numeri primi con 12 sono quattro, cioè **1, 5, 7, 11.**
Moltiplichiamo 5 per i quattro numeri primi con 12, e troviamo 5,25,35,55.
I resti della divisione per 12 di ciascuno di questi quattro numeri sono **5,1,11, 7**. Di nuovo, i resti sono i numeri primi con 12, mescolati tra loro. Di nuovo possiamo procedere come per la nostra (quasi) dimostrazione del piccolo teorema di Fermat.
Possiamo cioè fare i prodotti e di nuovo possiamo semplificare, trovando che $5^4$-1, cioè $5^{\Phi(12)}$ -1, è divisibile per 12, cioè che 624 è divisibile per 12 (ed infatti dà 52 con resto zero). Che due resti non possano coincidere lo abbiamo fatto vedere in precedenza.

Dividendo un multiplo qualunque di 5 per 12 si possono trovare dei resti diversi da questi quattro, cioè non primi con 12. Per esempio 5 × 4 diviso 12 dà resto 8.
E' chiaro quindi che il colpo di genio nella dimostrazione di questo teorema sta nel rendersi conto che moltiplicando un numero *a* che sia primo con *n* per i numeri primi con *n* (e più piccoli di *n*) dà dei numeri che, divisi per *n*, producono dei resti che sono numeri più piccoli di *n* e primi con *n*.

**Cioè questi resti fanno necessariamente parte del club dei Φ (*n*) numeri che rappresentano la totalità dei numeri più piccoli di *n* e primi con *n*.**
Per convincervene potete provare a mettere 7 o 35 (che sono primi con 12) al posto di 5 e trovare i resti delle divisioni di 7, 35, 49, 77 per 12 o di 35, 175, 245, 385 per 12. Non uscirete mai dal club (1,5,7,11) dato in qualche ordine.
Ma perché?
Se *a m* (dove m è primo con n) diviso n non desse come resto un numero primo con n, vorrebbe dire che potremmo scrivere che tanto il resto R quanto n sono multipli di uno stesso divisore q, cioè R = *r q* e n = *s q*. Quindi:

$$a\,m = kn + R = k\,n + r\,q, \text{ in cui } n = s\,q.$$
$$a\,m = (k\,s + r)\,q = A\,q.$$

Se possiamo scrivere questa espressione, ciò significa che *q* è un divisore di *a m* . Ma *q* non può essere un divisore di *m*, il quale è primo con *n*, cioè non ha divisori comuni con *n*. Quindi *q* deve avere divisori comuni con *a*. Ma poiché abbiamo assunto che *q* divida anche *n*, ne risulterebbe l'assurdo che *a* ed *n* non sono primi fra loro, come invece li avevamo scelti fin dall'inizio. Quindi non si può avere un resto di *a m* (con m primo con n) che non sia primo con *n*.

Supponiamo ora che i numeri primi con n siano $p_1, p_2, p_{3\ldots}p_s$ , dove s è Φ (*n*), il numero dei numeri primi con n ed inferiori ad n.
Abbiamo che $R_n$ (a $p_1$ a $p_2$ ...a $p_s$) = $R_n$ ($a^s$ $p_1$ $p_2$ $p_{3\ldots}p_s$) = $p_1$ $p_2$ $p_{3\ldots}p_s$ da cui, ricordando che s = Φ (*n*), la formula magica

$$a^{\Phi(n)} = 1 \; mod \; n.$$

Ovviamente la dimostrazione vale anche per il caso precedente (ricorderete che fino in fondo al caso generale non c'eravamo arrivati) , in cui n è primo e Φ (*n*)= n-1

Nel nostro esempio abbiamo l'equazione: R12( 5x25x35x55)==R12($5^4$ (1 x 5 x 7 x 11)) = R12(1 x 5 x 7 x 11) = (1 x 5 x 7 x 11)) e, semplificando:

R12 ($5^4$-1)=0, che dimostra il teorema.

E se ci fossimo dimenticati uno dei quattro primi? Per esempio 7, tenendo solo 1,5,11? Avremmo trovato che 5 x 11/12 dà resto 7, cioè ci propone un altro membro del club (che faremo bene ad accettare).

Una prima conseguenza è che se un numero n è il prodotto di due numeri primi n = pq, allora:

$a^{(p-1)(q-1)}$ = 1 modulo pq.

perché sappiamo che *Φ(pq) = (p-1)(q-1).* E dalla formula generale per la Φ si ottiene la forma esplicita del teorema per qualsiasi numero si voglia.

## 3. CIFRARE E DECIFRARE SERIAMENTE

Qualcuno avrà sentito parlare di modi di cifrare e decifrare in cui entrano i numeri primi. I numeri primi entrano in questo gioco perché sono degli esseri straordinari, e credo che i metodi in cui entrano i numeri primi siano oggi quelli più usati per costruire dei sistemi di cifra seri.

Esistono altri sistemi di cifratura, ma sono, per quanto ne so, basati sul fatto che i due corrispondenti hanno la stessa chiave, sia essa una tabella di sostituzione, più o meno complessa, un disco ruotante, una parola o frase chiave, una "griglia", un dizionario col numero di codice segreto (Vedi Appendice).
Tutti questi sistemi ricadono nel seguente schema. Giorgio e Giacomo si sono provveduti di chiavi identiche. Giacomo scrive il suo messaggio, lo chiude in una scatola con un lucchetto, chiude il lucchetto (queste due operazioni corrispondono alla cifratura), manda la scatola (che magari si autodistrugge se si tenta di aprirla con la chiave sbagliata). Giorgio riceve la scatola, apre il lucchetto con la chiave in suo possesso (questa operazione corrisponde alla decifrazione), legge il messaggio.
Il problema è che due persone hanno due chiavi identiche. Quindi il sistema è doppiamente vulnerabile.

Si incominciò quindi a studiare la possibilità di creare una situazione alquanto diversa.
Giorgio ha un lucchetto con la sua chiave, che Giacomo non ha e non ha mai visto; Giacomo ha un lucchetto con la sua chiave, che Giorgio non ha mai visto. Se Giorgio vuol ricevere un messaggio da Giacomo gli manda anzitutto la sua scatola con il suo lucchetto aperto. Giacomo ci mette il suo messaggio e chiude il lucchetto. Notate che per chiudere il lucchetto non c'è bisogno della chiave. Poi Giacomo manda a Giorgio la scatola col lucchetto chiuso, che Giorgio aprirà con la chiave che lui solo ha. Semplice. Un'eventuale spia dovrebbe avere la chiave in possesso di Giacomo per capire i messaggi di Giorgio e la chiave di Giorgio per capire i messaggi di Giacomo. Nel caso precedente, invece, bastava una delle due chiavi, perché erano identiche.

A questo punto arrivano i numeri primi.

Come abbiamo detto, scomporre un numero in fattori primi (ed eventualmente scoprire che è primo) non è uno scherzo. Il tempo di analisi, usando i sistemi più rozzi, viene semplicemente moltiplicato per tre ad ogni cifra che aggiungiamo (ricordate che in linea di principio dobbiamo analizzare tutti i numeri primi fino alla radice quadrata del numero, e tre è circa la radice quadrata di dieci: moltiplicando un numero per dieci, la sua radice quadrata si moltiplica grosso modo per tre. Per esempio la radice di 4 è 2, quella di 40 è poco più di 6, quella di 400 è 20. Non sembra molto, ma a poco a poco pesa. Nel 2005 il numero più grande, non primo, completamente fattorizzato era di 200 cifre.

Invece è relativamente facile moltiplicare tra loro numeri primi, anche di cento cifre. Per la cronaca, il numero primo più grande che si conosca oggi (2010) ha circa 12 milioni di cifre, ma il fatto che è primo non viene scoperto attraverso la fattorizzazione. Si usano test molto ingegnosi che rivelano direttamente se il numero è primo o no, ma qui non li vedremo. In ogni caso in genere QBasic ed altri programmi gratuiti in rete arrivano solo a 20-40 cifre esatte.

Nel nostro esempio useremo numeri primi piccoli.
Incominciamo col dire che i due che vogliono scriversi, Giorgio e Giacomo, hanno entrambi una tavola in cui i messaggi sono tutti numeri di poche cifre. Se il messaggio riguarda che cosa farà Giacomo domenica, i messaggi possono essere
1 = vado colla mia famiglia; 2= vado in piscina; 3= non so; 4 = sto a casa; 5 = vado alla partita; 6 = museo; eccetera.

Ma ancora, il messaggio è qui di una cifra solo per non fare calcoli troppo lunghi.

Giorgio vuole mandare la scatola col lucchetto aperto a Giacomo.
Per costruire il lucchetto aperto, gli occorre un numero N che sia il prodotto di due numeri primi. In linea di principio si scelgono due numeri primi enormi. Noi ci accontentiamo di 3 e 5, che proprio enormi non sono. Il prodotto è N = 15. Anche se non è consigliato farlo, lo possiamo gridare sui tetti (soprattutto se non è 15 ma ha duecento cifre, perché allora scomporlo in fattori primi sarà duro). Adesso calcoliamo $\Phi(15)$. Anche se i due numeri primi fossero assai grandi, noi sapremmo (he he) che $\Phi(3x5)= (p-1)(q-1) = 2 \times 4= 8$.
Questo 8 lo conosciamo solo noi, perché solo noi sappiamo fattorizzare N.

Ora ci occorre un numero che sia più piccolo di $\Phi = 8$ e primo con 8. Noi scegliamo 3 (che chiameremo in generale E). Il "lucchetto aperto" è costituito da due numeri (N, E), nel nostro caso (15,3), di cui "nessuno" sa se 15 sia primo e quali siano i suoi fattori e quindi nessuno sa quale sia la $\Phi$. Tutti possono però conoscere 15. In particolare lo conosce Giacomo (che però neanche lui conosce i fattori). Inoltre, di numeri primi con 3 ne esistono diversi, e di qui non possiamo risalire alla $\Phi$.
Inutile aggiungere che se invece di (15,3) mandassimo a Giacomo il numero 135, da cui lui potrebbe immediatamente ricavare 15 e 3, i problemi degli eventuali curiosi aumenterebbero.

Ora Giacomo ha il lucchetto aperto, non ha che mettere il messaggio nella scatola e chiudere.
Questa operazione è quello che si chiama "cifrare il messaggio".
Supponiamo che Giacomo voglia mandare il messaggio M=3 ("non so").
Il messaggio cifrato, C, è il resto della divisione di $M^E$ per 15 (che è il nostro N). I matematici scriverebbero con bella notazione $C = 3^3 \mod 15$.
$3^3$ vale 27 ed il resto della divisione per 15 è 12. Questo 12 è dunque il messaggio cifrato C.

Giorgio riceve il “lucchetto chiuso” o messaggio cifrato C, ovvero 12.

Ora a Giorgio occorre la chiave.
Per fabbricare la chiave gli occorre un numero D tale che (ED -1) sia divisibile per Φ , cioè 8, ricordando che E=3. Per tentativi troviamo 3 (cioè verifichiamo se 3-1, 3 x 2 -1, 3 x 3-1, etc. siano divisibili per 8). Ma già 9-1 è divisibile per 8.
Questo secondo numero 3, D, lo sappiamo solo noi (o lo sa solo Giorgio), perché per trovarlo abbiamo usato la Φ = 8, che solo noi conosciamo.

Per aprire il lucchetto, Giorgio deve soltanto calcolare il resto della divisione di $C^D$ per 15, cioè esegue $12^3$ mod 15, e trova che 1728/15 dà resto 3, che era appunto il messaggio M originale. Valeva certamente la pena fare tutti questi conti per scoprire che Giacomo non sa cosa farà domenica!

Noto intanto che D=11 va ancora bene, perché 3x11-1 =32 è divisibile per 8. Andrebbe bene per decifrare il messaggio cifrato C=12? Cioè, $12^{11}$/15, dà resto 3? Ma certo. Il problema è che numeri anche così piccoli ($12^{11}$ = 743 008 370 688) già sfuggono a QBasic, nel senso che ci darebbe dei risultati approssimati. Google ce la fa appena.

Che cosa dovrebbe fare uno che volesse decifrare il messaggio 12 senza conoscere D? Lui conosce 3 e 15. Semplice, deve trovare un numero M tale che $M^3$ - 12 sia divisibile per 15. Anche qui, si provano ordinatamente diversi M e si vede se il loro cubo meno 12 è divisibile per 15. Ora:
M=1, 1-12 non è divisibile per 15
M=2, 8-12 non è divisibile per 15
M=3, 27 -12 =15, è divisibile per 15.
Quindi M=3. E adesso anche il curioso, se ha in mano sua la tabella delle corrispondenza numeri-messaggi, sa che Giacomo non sa cosa fare domenica. Sempre utile a sapersi.
Il curioso può anche usare un’altra via, cioè trovarsi la D da solo, se riesce a scoprire con lunghi calcoli che 15 = 3 x 5, Φ =8, e D deve essere tale che 3D-1 sia divisibile per 8.

La difficoltà nasce dal fatto che appena i numeri sono un po’ grandi, i calcoli che il curioso deve fare diventano proibitivi. Il metodo si chiama “Algoritmo RSA”, dai nomi dei tre inventori, Rivest, Shamir, Adleman. Se andate su Wikipedia.com (inglese) e cercate “RSA algorithm” (e sapete l’inglese) trovate un esempio svolto, in cui N = 61 x 53=3233, Φ = 60 x 52 = 3120, E = 17. Anche per Giorgio, trovare D non è banale. Dobbiamo ora risolvere l’equazione
17×D-1 = k×3120. Ora la soluzione è D = 2753.
Il modo più semplice di ottenere D è moltiplicare 3120 per k= 1,2,3,4,5…, aggiungere 1 ogni volta, e vedere se il risultato è divisibile per 17, e qual è questo risultato. Incomincia ad essere un bel lavoro, a farlo a mano, ma è ancora facile da fare con un normale PC. Ci sono anche altri metodi più rapidi.

Nell’esempio di Wikipedia, M = 123, C, il messaggio cifrato, è…il resto della divisione di $123^{17}$ per 3233. I numeri, anche se così piccoli, sono ormai fuori della portata dei normali programmi. Neanche Google ce la fa più e deve dare un risultato approssimato, che non serve più a nulla. Comunque con un buon programma si trova che C= 855. Giorgio adesso deve trovare il resto della divisione per 3233 di $855^{2753}$ ….. Auguri!

Abbiamo dunque due problemi:
1) capire perché il metodo funziona;

2) vedere come calcolare $A^B \bmod C$ rapidamente. Appena si va in numeri primi di due cifre, si incomincia ad uscire dalle possibilità dei programmi meno sofisticati. Un programma come Mathematica (ma non è precisamente gratuito) fa conti del genere in quattro e quattr'otto.

Per quel che riguarda (1), se ci ricordiamo il piccolo teorema di Fermat esteso a numeri non primi, notiamo che $A^{\Phi(N)} = 1 \bmod N$. Cioè il resto della divisione di $A^{\Phi(N)}$ per N dà 1, se A è primo con N. Nel nostro caso A ha solo due fattori primi, p, q.
Chiamando $\mathbf{C = M^E \bmod N}$ (ovvero il resto di $M^E$ diviso N) il messaggio cifrato, l'operazione richiesta per decifrare C non è altro che

$$\mathbf{C^D \bmod N} = M^{\underline{ED}} \bmod N = M^{\underline{(1+k\Phi)}} \bmod N = M\, M^{k\Phi} \bmod N = \mathbf{M\,(M^{\Phi})^k \bmod N,}$$

indicando con Φ la Φ(N).
Ma, come abbiamo indicato, $M^{\Phi}/N$ dà resto 1, ovvero $M^{\Phi} = 1 \bmod N$ e la sua potenza $(M^{\Phi})^k \bmod N$ sarà evidentemente ancora 1.

Da cui:

$$\mathbf{C^D \bmod N = M.}$$

Francamente, però, io credo che i metodi di cifratura basati sulla scomposizione in fattori primi si basino troppo sul fatto che il "curioso" non sia in grado di effettuare una scomposizione in fattori primi di numeri enormi. Ma che ne sappiamo? Magari lui si è comprato l'ultimo prototipo di calcolatore, di cui noi manco conosciamo l'esistenza, che può scomporre numeri di questo tipo, e allora siamo fritti. Quindi penso che il futuro della cifratura non sia in questa direzione.

Restava da dire come si potrebbe fare a trovare il resto dell'elevazione a potenza di due numeri abbastanza grandi da spaventarci.
Per esempio, si voglia trovare il resto della divisione di $13^{112}$ per 113.
Ora, $13^{112}$ è un numerino niente male, 124 cifre:
5776376046244110391962960638671780840283856460004148387811278264418486799668036454334543741320404101515448754373815708983648 1.
Dovremmo dividerlo per 113 e trovare il resto. Questo sarebbe il metodo di forza bruta, che però riesce, a parte il fatto che trovare il numerino niente male richiede o molta pazienza o un programma niente male.

Ma si può far di meglio della forza bruta.

Se noi conosciamo le successive potenze di due (1, 2, 4, 8, 16, 32, 64, 128 etc.) intanto possiamo sempre scrivere qualsiasi numero (in questo caso l'esponente 112) come somma di queste potenze. Questo equivale a scriverlo in base due.
Se non sappiamo queste cose, vediamo che in 112 certo ci sta un 64; ci resta 48. Da 48 possiamo togliere 32, ci resta 16. 16 è uno dei numeri della nostra tabellina di potenze di 2. Quindi possiamo scrivere 112=64+32+16. E quindi $\mathbf{13^{112}=13^{64}13^{32}13^{16}}$.

Alternativamente possiamo usare il nostro arsenale di conoscenze sul calcolo con basi diverse da 10, in questo caso 2, scriviamo l'esponente 112 in base 2. Sappiamo come fare.

Dividendo 112 per 2 si trova 56, resto 0
Dividendo 56 per 2 si trova 28, resto 0

Dividendo 28 per 2 si trova 14, resto 0
Dividendo 14 per 2 si trova 7, resto 0
Dividendo 7 per 2 si trova 3, resto 1
Dividendo 3 per 2 si trova 1 resto 1
Dividendo 1 per 2 si trova 0, resto 1.

L'esponente in base binaria, elencando i resti a partire dall'ultimo trovato, è **1110000**, che (e questo era lo scopo dell'esercizio) possiamo scrivere come $2^4+2^5+2^6 = 16 + 32 + 64 = 112$.
$13^{112} = 13^{64+32+16}$ è quindi il prodotto di tre fattori che hanno tutti 13 come base, e come esponenti potenze di 2 cioè $\mathbf{13^{64}13^{32}13^{16}}$. Una scomposizione del genere è sempre possibile, perché un numero qualsiasi può sempre essere scritto in base 2 (o altra base a piacere).

Adesso siamo pronti a partire. Il resto di 13 elevato a 1, cioè $2^0$ è 13.
Eleviamo al quadrato. Ora $13^2 = 169$ e il resto della divisione per 113 è 56.
Il resto di $13^4$ è il quadrato del resto precedente, 56 x 56 =3136 che, diviso ancora per 113, dà come resto 85.
Il resto di $13^8$ è il quadrato del resto precedente, 85 x 85 = 7225, che, diviso ancora per 113, dà come resto 106.
Il resto di $\mathbf{13^{16}}$ è il quadrato del resto precedente, 106 x 106 =11236. Il nuovo resto è **49**. Questo ce lo teniamo da parte perché è uno dei tre fattori di $13^{112}$.
Il resto di $\mathbf{13^{32}}$ viene da 49 x 49 =2401, il cui resto della divisione per 113 è **28**. Teniamo anche questo.
Infine il resto di $\mathbf{10^{64}}$ viene da 28 x 28= 784, con nuovo resto **106**. E ci teniamo anche questo.

Il prodotto dei resti è il resto del prodotto **49 x 28 x 106** diviso 113.
Credeteci o no, il resto è 1, come avremmo dovuto sapere, visto che 13 e 113 sono primi (e primi fra loro). Naturalmente, abbiamo potuto svolgere questo esercizio solo perché questo numero, lungo e in cui le cifre si susseguono senza ordine apparente, può esser scritto come $13^{112}$.

Dunque per trovare il resto di $A^B$ mod C :
1) scomporre l'esponente B in potenze di due (o per semplice sottrazioni successive o scrivendolo in forma binaria, il che ci permette di sapere quali potenze di 2 intervengono nell'esponente). Scomponendo l'esponente in una somma di potenze di 2 noi scomponiamo al tempo stesso la potenza $A^B$ in un prodotto di potenze della stessa base i cui esponenti sono tutti potenze di 2.
2) calcolare i resti della divisione per C delle successive potenze A, $A^2$, $A^4$, $A^{16}$ etc. e tutte le altre
3) calcolare il resto del *prodotto* dei fattori che entrano in $A^B$.

Con questi pochi, ma intelligenti calcoli, tutti fattibili a mano o con una piccola calcolatrice, avete trovato il resto della divisione di
5776376046244110391962960638671780840283856460004148387811278264418486799668036454334543741320404101515448754373815708983648 1
per 113.

Di che riempire di conti un foglio lungo più di un metro, se scrivete piccolo. Io dico che se avete capito il procedimento e lo potete ripetere con altri giganti del genere, potete essere fieri di voi stessi, un po' come i cavalieri erranti che domavano giganti o dragoni che sputavano fuoco.

Se non vi è passata la paura dei numeri questa volta….

## 4. QUALCHE ALTRA APPLICAZIONE

Per me, l'applicazione più avvincente al mio modesto livello, è il fatto che, grazie al "piccolo teorema di Fermat", si possono trovare dei numeri e delle situazioni affascinanti.

Ad esempio, si scelga come base 10 e p un numero primo con 10.

Il piccolo teorema afferma che $10^{p-1}-1$ è divisibile per p. Sembra una cosa da ridere, ma questo ci dice che, ad esempio, $10^{112}-1$ è divisibile per 113. Questo è già un bel risultato. Ma il fatto è che $10^{112-1}$ può essere scritto quasi senza pensare. Infatti, che razza di numero è $10^{112}-1$??
Ci vuole un istante a scoprire che è un numero costituito da 112 cifre eguali, tutti 9. Bisogna solo aver la pazienza di scrivere 112 cifre 9. Per esempio, $10^6-1$ deve essere divisibile per 7. Ora, $10^6-1$ = 999999. Sembra incredibile, ma questo numero è divisibile per 7, come si verifica subito.

Questo è dunque un bel risultato. Potete scommettere con un amico che gli scrivete subito un numero costituito da soli 9 divisibile per qualsiasi numero primo.
Ma se volessimo un numero composto da soli 1 o soli 2 o soli 3 divisibile per un dato numero primo, per esempio 7?
Basta notare che 999999= 9 x 111111. Ora per quel solito lemma di Euclide. Ora, o 7 divide 9 o divide 111111. Poiché non divide 9, devedividere 111111. Provare per credere. Ma allora siamo a cavallo (motto di famiglia). Infatti tutti i numeri 2 x 111111, 3 x 111111 eccetera presenteranno la stessa proprietà: 7 divide 111111, e quindi dividerà tutti i prodotti di 1, 2, 3, 4, 5, 6, 7, 8, 9 per tale numero, cioè dividerà 222222, 333333, 444444 eccetera. Tutti i numeri primi funzionano così. Per i numeri non primi , per esempio 21, sappiamo che $\Phi(21) = 12$. Dovremmo avere che $10^{12}-1$ (un numero costituito da 12 cifre 9 ) è divisibile per 21. Si provi e si vedrà che funziona.

Il problema è con i numeri che contengono i due fattori primi di 10, cioè 2 e 5. Con questi il metodo non funziona, perché, se si ricorda, la base (per noi 10) e il numero a cui va elevata, devono essere primi fra loro. Quindi i numeri su cui possiamo fare le nostre dimostrazioni son subito assai grandi: 9, 21, 27, 33.

Il più piccolo è 9, la cui $\Phi(9) = 6$. Ma non c'è bisogno di andare così lontano, già 9 è divisibile per 9. In altre parole, non è detto che $a^{p-1}-1$ o $a^{\Phi(p)}-1$ siano i numeri più piccoli divisibili per p.
Talvolta basta elevare *a* ad un divisore della $\Phi(p)$, e sottrarre 1 per avere un multiplo esatto di p.
Un caso evidente è quello di 11, per cui non occorre ricorrere a 9 999 999 999: basta 99, divisibile appunto per 11. M quali numeri richiedono la $\Phi$ completa nella sua gloria, e quali si accontentano di un divisore? Mistero.

Ad ogni modo, sapere di primo acchito che 555 555 555 555 è divisibile per 13 è già una bella soddisfazione. O no?

# Appendice

# DECIFRAZIONE “INGENUA”

Un gioco che viene fatto sovente è quello di decifrare un messaggio nascosto.
La prima idea che viene in mente è quella di sostituire alle lettere dell'alfabeto altri simboli, o le stesse lettere dell'alfabeto in ordine diverso, in modo – ovviamente - che ogni lettera corrisponda ad una ed una sola lettera.

Ad esempio, ricevete il messaggio italiano cifrato

⊗∞●☺☻ ▲’∞☼♠♣ ◙♣◊☺☻♥◊ ◊ ♣▲ ⊗∞◙♣☺∞●☻

Come si fa a decifrarlo?
Sia ben chiaro che la scienza della criptografia (o dello scrivere messaggi nascosti) ha fatto enormi progressi, e nessuno si sognerebbe più di usare un sistema così semplice. Ma come gioco di società va ancora bene, e ci dà anche qualche insegnamento in più.

*Quanto più lungo è il messaggio, in teoria tanto più facile è decifrare il messaggio cifrato con cifrature ingenue di questo tipo,* perché esistono tavole di frequenze delle varie lettere, che ci dicono, per esempio, che in Italiano le lettere più frequenti sono, nell’ordine, E A I O N L R T S C D P etc. Se abbiamo un testo cifrato (lungo) in italiano e mettiamo in ordine di frequenza le lettere che lo compongono, dovremmo arrivare alla decifrazione con pochi tentativi, perché la lettera più frequente dovrebbe essere una E, la seconda in ordine di frequenza una A, la terza una I e via dicendo.
Devo dire che un po’ di pazienza e più di un tentativo sono necessari. Magari ci vuole anche un computer (e un programma, magari in Qbasic, per contare le lettere).

| Frequenza standard (Wikipedia) in Italiano | Dante Alighieri: “La Divina Commedia”. Canto I. | De Amicis – “Cuore” Il primo giorno di scuola. | Salgari. “Le due Tigri”, capo I, circa 5800 lettere |
|---|---|---|---|
| E | E | A | A |
| A | A | E | E |
| I | I | I | I |
| O | O | O | O |
| N | R | R | N |
| L | L | N | L |
| R | T | L | R |

Pur con un brano che conti diverse migliaia di lettere, una perfetta aderenza non la si ha. Salgari è decisamente il migliore, e lo scambio tra A e E potrebbe esser corretto subito. Ma, se avessimo cifrato un brano di De Amicis ed avessimo identificato il simbolo più frequente con la E, il quinto con la N, avremmo avuto qualche problema in più.

Nel nostro brano, abbiamo le seguenti ripetizioni, e adattandole alle frequenze otterremmo:

∞ ∞ ∞ ∞ E A
♣♣♣♣ A E
◊◊◊ I O N
☺ ☺ ☺ O N I
☻ ☻ ☻ N I O
▲▲ L R T
⊗⊗ R L T
●● T L R
☼ S C D
♠ C D S
♥ D S C

Ma il brano è troppo breve. Troppi simboli compaiono con la stessa frequenza. Scegliere l'ordine di frequenza non è facile.

Ci potrebbero allora aiutare le osservazioni
1) che le parole italiane polisillabiche tendono a terminare per vocale, quindi ♣ ◊ ☻ sarebbero vocali;
2) che prima di un apostrofe ci sta solo un C, D, L, M, N, S, T, V; mentre dopo l'apostrofe ci può essere solo una vocale;
3) che una lettera isolata può essere solo A, E, I , O;
4) il penultimo gruppo di due lettere, visto che la prima lettera è una vocale, può essere solo AD, AI, AL, ED, IL, IN, IO, OD,OH,

Eccetera. Ma, ripeto, il brano è troppo breve e in questo caso il lavoro che resta da fare è molto. In fine di sezione darò il testo originale, in caso qualcuno ci sia voluto provare.

Però, è chiaro che il testo è vulnerabile alla decifrazione quanto più è lungo.
Furono quindi escogitati sistemi assai più sicuri.

Nel Cinquecento si incominciò a pensare che il sistema in cui ad ogni lettera dell'alfabeto si sostituisce sempre la stessa lettera o simbolo fosse poco sicuro, proprio per la ragione indicata, che con metodi statistici si arriva presto alla decifrazione. Per cui si pensò ad inserire simboli che indicavano che era stata cambiata la cifratura. Nella forma più semplice possiamo supporre che vengano cifrati i ventun simboli dell'alfabeto Italiano in quelli dell'alfabeto inglese, che ha in più J K W X Y. I due che si scrivono possono avere per esempio cinque diverse tabelle di cifratura, ciascuna identificata con una delle lettere assenti in Italiano. Si può concordare che si incominci a cifrare con una tabella. Poi, quando piace al cifratore, questi inserisce uno di questi simboli assenti in italiano (cifrato o no a seconda della convenzione) il quale non fa parte del messaggio originale ma indica di passare ad una nuova tabella.
Leon Battista Alberti (1404-1472) pensò ad uno strumento meccanico per avere a disposizione molte tabelle di cifratura. Si tratta dei "dischi cifranti". Su Wikipedia si può trovare un esempio di disco cifrante di Leon Battista Alberti, con semplici istruzioni per l'uso. Non so se Alberti (che, incidentalmente, era un genio) avesse notizia della possibilità di decifrazione con il metodo statistico, che certamente era stata già escogitata da studiosi arabi prima dei suoi tempi. Certo il suo sistema rende impossibile usare questo metodo di decifrazione indesiderata.

Per finire con le sostituzioni lettera per lettera, con una o più tabelle, indico un altro sistema, dovuto a Vigenère, non migliore di quello di Alberti. Occorre essenzialmente che i due che vogliono corrispondere tra loro abbiano in mente o una parola o una frase. Per esempio, si voglia cifrare la frase “domenica piove”. Vi si scrive sotto la frase concordata MILANINTER, lettera per lettera, quante volte basta.

D O M E N I C A P I O V E
M i l a n i n t e r m i l

Poi bisogna codificare il messaggio. Se sotto alla D di domenica troviamo la M di Milan, ciò vuol dire che dobbiamo usare per la codificazione della D un alfabeto in cui la M corrisponde alla A, e quindi la D alla terza lettera dopo la M, quarta contando la M, cioè P. Vigenère, per aiutare il cifratore, costruì la tabella qui di seguito (che è facilissima a farsi da soli).

La lettera da cifrare è data nella prima riga. L’alfabeto da usare è quello dato nella riga che incomincia con la lettera della “chiave” milaninter che sta sotto la lettera del messaggio da cifrare. Quindi la prima lettera del messaggio cifrato è P e la seconda è W

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V **W** X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O **P** Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

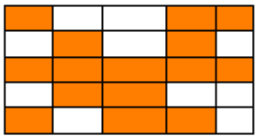
Per decifrare si compie il cammino inverso, sempre scrivendo sotto al messaggio cifrato la frase MILANINTER ripetuta quanto basta e andando a cercare a quale lettera della prima riga corrisponde la lettera da decifrare nella riga che incomincia con la lettera sottostante della frase chiave.

Altro sistema è la **griglia.**
In questo caso i due che vogliono corrispondere segretamente hanno entrambi una maschera o griglia da porre sul messaggio.

Giorgio manda a Giacomo il messaggio (non è detto che debba essere in un quadrato, che insospettisce). In questo caso, abbiamo un quadrato e Giacomo sa che deve mettere le varie lettere in quadrato.

| | | | | |
|---|---|---|---|---|
| E | V | A | R | I |
| D | E | O | F | A |
| F | I | N | T | A |
| L | A | N | C | I |
| A | N | O | M | E |

Poi mette su questo quadrato la sua brava griglia, che tiene in un cassetto.



e il messaggio risulta chiaro, "Vado al cine".

| | | | | |
|---|---|---|---|---|
| | V | A | | |
| D | | O | | A |
| | | | | |
| L | | | C | I |
| | N | | | E |

Evidentemente non c'è nessuna ragione di inviare il messaggio sotto forma di griglia quadrata invece che lineare. In realtà ci sono piuttosto molte ragioni per non disporre il messaggio in una griglia quadrata. Basta sapere, ad esempio, che la griglia è 5 x 5 e le 25 lettere possono essere inviate in messaggio lineare. Poi chi le riceve le mette in una griglia 5 x 5 e applica la sua maschera. In fin dei conti l'obiettivo è solo quello di selezionare in qualche modo le lettere interessanti del messaggio. A rigore si può pensare che i due soci usino come griglia la frase chiave, che solo loro conoscono essendosi messi d'accordo una volta per tutte, "Nel mezzo del cammin di nostra vita". Si può allora scrivere questa frase sotto il messaggio cifrato avendo pure concordato che - per esempio - solo le lettere sopra alle vocali contano. In questo caso la griglia manco esiste concretamente. Il messaggio potrebbe essere allora:
*"evita, ladro, i vari loschi piani e va'"*, in cui si ignorano spazi, segni di interpunzione, apostrofi.

e v i t a l a d r o i v a r i l o s c h i p i a n i e v a
N E L M E Z Z O D E L C A M M I N D I N O S T R A V I T A

Sopra alle vocali della frase chiave troviamo il messaggio : *"vado al cine"*.

In molte istituzioni che volevano evitare lo spionaggio, fino a che non fu introdotta la crittografia a

macchina od elettronica, vigeva un altro sistema di cifratura che si poteva fare a mano.
Le due parti avevano una specie di dizionario segreto, in cui ad ogni parola corrispondeva un gruppo, per esempio di cinque cifre.
Per esempio a “Ministero” corrispondeva il gruppo “54321”. Poi, ogni mese o anche più frequentemente, i due corrispondenti si comunicavano un numero segreto di cinque cifre, ad esempio 87861. Nel cifrare a mano il messaggio si doveva sommare a tutti i gruppi di cinque cifre il numero segreto 87861, **ma senza eseguire riporti**, cifra per cifra. Se vogliamo era una somma “modulo 10”. Quindi “Ministero” diventava 54321 + 87861 = 31182. Il mese dopo, magari, il numero segreto era 98687, e “Ministero” diventava 54321 + 98687 = 42908. Per decifrare non si aveva che sottrarre al messaggio cifrato lo stesso numero 98687 o 87861, cifra per cifra, aggiungendo dieci al minuendo se necessario. Eventuali curiosi dovevano avere una copia del dizionario ed una copia dei numeri segreti che venivano regolarmente sostituiti, per leggere i messaggi cifrati.

SOLUZIONE:

Il messaggio
⊗∞●☺☻ ▲’∞☼♠♣ ◙♣◊☺☻♥◊ ◊ ♣▲ ⊗∞◙♣☺∞●☻
è il primo verso della Gerusalemme Liberata: “*Canto l’armi pietose e il Capitano*”.