ESTRATTO

Salvatore Damantino, Emanuele Campeotto

Aritmetica modulare

Teoria e applicazioni

scienza express edizioni

Dimostrazione. Basta osservare che

$$d \mid b+1 \qquad \Longleftrightarrow \qquad b \equiv -1 \pmod{d}$$

(da cui $b^k \equiv 1 \pmod{d}$ per k pari e $b^k \equiv -1 \pmod{d}$ per k dispari) e dunque

$$N = a_m b^m + \cdots + a_1 b + a_0 \equiv (-1)^m a_m + \cdots + a_2 - a_1 + a_0 \pmod{d}.$$

□

Ad esempio, in base 13, un intero è divisibile per 2, 3, 4, 6, 12 se e solo se lo è la somma delle sue cifre ($2, 3, 4, 6, 12$ sono tutti divisori di $13 - 1 = 12$); un intero è divisibile per 7 (o per 2) se e solo se lo è la somma delle sue cifre a segno alterno (7 è un divisore di $13 + 1 = 14$).
Ancora, in base 8, un intero è divisibile per 2 o per 4 se e solo se lo è la sua ultima cifra; un intero è divisibile per $4^2 = (20)_8$ se e solo se lo è il numero costituito dalle sue ultime due cifre.

Esempio 1.3.5. Un intero positivo n è costituito da 501 cifre comprese tra 0 e 6. Letto in base 10 è multiplo di 3, in base 7 è multiplo di 6, in base 16 è multiplo di 15. Quanto può valere al massimo la somma delle cifre di n ?

Soluzione. In base 7, un intero è divisibile per 6 se e solo se lo è la somma delle sue cifre; analogamente per la divisibilità per 3 in base 10 e quella per 15 in base 16. La somma delle cifre di n è pertanto multipla di 3, 6 e 15, quindi del minimo comune multiplo 30. Al massimo può valere $6 \cdot 501 = 3006$. Il valore cercato è quindi il più grande multiplo di 30 minore o uguale di 3006, cioè 3000. □

1.4 Il Piccolo Teorema di Fermat

In questa sezione presentiamo un risultato elementare ma di grande importanza e utilità in teoria dei numeri, vale a dire il **Piccolo Teorema di Fermat**. Pierre de Fermat (1601-1665) è considerato uno dei padri fondatori della moderna Teoria dei numeri. Una delle caratteristiche della sua attività matematica fu quella di non scrivere mai le dimostrazioni dei suoi risultati, limitandosi a semplici annotazioni (celebri sono quelle a margine della copia in suo possesso dell'*Arithmetica* di Diofanto) che diffondeva mediante una fitta corrispondenza con altri cultori della matematica dell'epoca, tra cui M. Mersenne. Egli scoprì il Teorema che porta il

suo nome intorno al 1636, chiaramente senza dimostrarlo[7], e ciò consentì anche di giustificare la cosiddetta *ipotesi cinese* (tra l'altro vera solo in parte) secondo cui un intero p è primo se e solo se $2^p \equiv 2 \pmod{p}$. Circa cento anni più tardi, il matematico svizzero Leonhard Euler $(1707 - 1783)$, famoso anche per la sua abilità nel dimostrare o confutare le congetture di Fermat, riuscì non solo a dare una dimostrazione corretta del risultato congetturato da Fermat ma anche a generalizzarlo al caso di moduli non primi[8].
Del Teorema di Fermat daremo due versioni, la seconda delle quali è quella comunicata dal matematico francese a B. Frenicle de Bessy.
Premettiamo il seguente risultato.

Proposizione 1.4.1. *Per ogni primo p e ogni $x, y \in \mathbb{Z}$ vale la seguente congruenza:*

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

Dimostrazione. Per la formula dello sviluppo del binomio di Newton[9], risulta

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p.$$

Essendo p primo, ogni coefficiente binomiale (intero) è divisibile per p e quindi risulta $\binom{p}{k} \equiv 0 \pmod{p}$ per ogni $k = 1, 2, \ldots, p-1$. Di conseguenza si ha

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

□

Osservazione 1.4.2. Nella proposizione precedente è fondamentale che la potenza del binomio abbia come esponente un numero primo. Infatti, non è sempre vero, ad esempio, che $(x+y)^4 \equiv x^4 + y^4 \pmod{4}$ per ogni $x, y \in \mathbb{Z}$. Per rendersene conto basta prendere $x = 3$ e $y = 5$ e verificare che $(3+5)^4 \not\equiv 3^4 + 5^4 \pmod{4}$.

Proviamo adesso il preannunciato

Proposizione 1.4.3 (Piccolo Teorema di Fermat)**.** *Sia a un intero e p un numero primo. Allora*

$$a^p \equiv a \pmod{p}.$$

[7] Fu Gottfried Wilhelm Leibniz il primo a darne una dimostrazione completa in un manoscritto non datato.

[8] Euler dimostrò anche che la somma dei cubi di due interi non è mai il cubo di un intero, caso particolare di quello che è noto come Ultimo Teorema di Fermat.

[9] Per questa formula si veda *Calcolo combinatorio*, Teorema 2.32.

Prima dimostrazione. Supponiamo $a \geq 0$, per cui possiamo procedere per induzione prendendo come variabile di induzione a stessa. Se $a = 0$ il risultato è ovvio. Supponiamo allora vero il risultato per a, cioè

$$a^p \equiv a \pmod{p},$$

e dimostriamolo per $a+1$. Essendo p primo, per la Proposizione 1.4.1 risulta

$$(a+1)^p \equiv a^p + 1^p.$$

Ma $1^p \equiv 1$ e $a^p \equiv a$ per l'ipotesi induttiva. Quindi

$$(a+1)^p \equiv a + 1$$

che è quanto volevamo provare.
Supponiamo ora $a < 0$. Allora $0 \equiv 0^p = (a + (-a))^p \equiv a^p + (-a)^p \pmod{p}$. Dato che è $-a > 0$, per quanto provato al punto precedente è $(-a)^p \equiv -a$, quindi $0 \equiv a^p - a$ cioè $a^p \equiv a \pmod{p}$.
Seconda dimostrazione (combinatorica). Abbiamo a disposizione delle perle di a colori diversi e costruiamo delle collane ognuna fatta di esattamente p perle a partire da stringhe di lunghezza p.
Complessivamente si possono formare a^p differenti stringhe; se da queste scartiamo quelle monocromatiche (cioè costituite da perle dello stesso colore) rimangono esattamente $a^p - a$ stringhe.
Uniamo, adesso, le estremità di ogni stringa per ottenere così le collane. In questo modo, due stringhe che differiscono di una permutazione ciclica delle proprie perle risultano di fatto indistinguibili come collane. Ma d'altra parte ci sono esattamente p permutazioni cicliche di p perle su una stringa. Pertanto il numero di collane distinte non monocromatiche è pari a

$$N = \frac{a^p - a}{p}.$$

Siccome N dev'essere un numero intero, necessariamente $p \mid a^p - a$ cioè $a^p \equiv a \pmod{p}$, da cui la tesi. □

Esempio 1.4.1. Risulta, ad esempio, $25^{41} \equiv 25 \pmod{41}$, essendo 41 un numero primo. Ancora, $36^{2011} \equiv 36 \pmod{2011}$ in quanto 2011 è un numero primo.

Il Piccolo Teorema di Fermat può essere utilizzato come test di **non primalità** di un numero naturale. Infatti, abbiamo visto che se p è primo allora qualunque sia a intero risulta $a^p \equiv a \pmod{p}$. Possiamo pertanto enunciare il seguente

Proposizione 1.4.4 (Test di non primalità)**.** *Se n è un numero naturale ed esiste un intero a verificante la condizione*

$$a^n \not\equiv a \pmod{n},$$

allora n non è primo.

Esempio 1.4.2. Applichiamo il test per verificare che 187 non è un numero primo. Scegliamo $a = 3$. Osserviamo che $3^8 = 6561 \equiv 16 \pmod{187}$, quindi $3^{24} \equiv 16^3 \equiv -18 \pmod{187}$. Ancora, $3^{72} \equiv -35 \pmod{187}$, da cui $3^{144} \equiv 103 \pmod{187}$ e quindi $3^{187} = 3^{144} \cdot 3^{24} \cdot 3^8 \cdot 3^8 \cdot 3^3 \equiv 103 \cdot (-18) \cdot 16 \cdot 16 \cdot 27 \equiv 103 \cdot (-18) \cdot (-7) \equiv 27 \cdot (-18) \equiv 75 \pmod{187}$. Di conseguenza 187 non è primo (d'altronde $187 = 11 \cdot 17$).

Si noti che il test, pur assicurando che il numero non è primo, non permette di trovarne la fattorizzazione. In genere, inoltre, si utilizza un a piccolo, in modo da tenere sotto controllo i calcoli; ad esempio si prova con $a = 2$ oppure $a = 3$.

Osservazione 1.4.5. Osserviamo che, in generale, il Piccolo Teorema di Fermat non è invertibile, nel senso che se n è un intero (≥ 2) tale che $a^n \equiv a \pmod{n}$ per qualche $a \in \mathbb{Z}$, $a \neq 0$, allora n *non* è necessariamente primo. Infatti, siano $n = 341 = 11 \cdot 31$ ed $a = 2$. Mostriamo che $2^{341} \equiv 2 \pmod{341}$ pur non essendo 341 un numero primo. Infatti, come facilmente si verifica, risulta $2^{11} \equiv 2 \pmod{31}$, $2^{31} \equiv 2 \pmod{11}$ e quindi $2^{341} = \left(2^{11}\right)^{31} \equiv 2^{11} \equiv 2 \pmod{31}$ e $2^{341} = \left(2^{31}\right)^{11} \equiv 2^{31} \equiv 2 \pmod{11}$. Ne segue che $2^{341} \equiv 2 \pmod{[11, 31]}$, cioè $2^{341} \equiv 2 \pmod{341}$, mentre 341 non è primo[10].

Osservazione 1.4.6. L'esempio precedente porta a considerare numeri del tipo $2^n - 2$, di notevole interesse storico, e a chiedersi quando vale la seguente proposizione:

$$\text{un intero } n \text{ è primo} \qquad \Longleftrightarrow \qquad n \mid (2^n - 2).$$

Tale proposizione risulta essere valida per $n \leq 340$ ma l'esempio precedente mostra che, in generale, essa non è valida. Ciò ha portato a definire i cosiddetti *numeri pseudoprimi*, cioè interi n non primi tali che $n \mid (2^n - 2)$.
Da notare che, se n è dispari, allora:

$$n \text{ è pseudoprimo} \qquad \Longleftrightarrow \qquad 2^{n-1} \equiv 1 \pmod{n}[11].$$

[10] L'esempio è dovuto al matematico francese Pierre Frédéric Sarrus e risale al 1819.

[11] basta osservare che $n \mid (2^n - 2)$ equivale a $2^n \equiv 2 \pmod{n}$, che semplificata, da $2^{n-1} \equiv 1 \pmod{n}$.

I numeri pseudoprimi minori di 1000 sono $341, 561$ e 645.[12]

Aggiungendo un'ulteriore ipotesi al risultato contenuto nella Proposizione 1.4.3, si ottiene la formulazione originaria del Piccolo Teorema di Fermat, della quale presentiamo due dimostrazioni.

Proposizione 1.4.7 (Piccolo Teorema di Fermat, versione originaria)**.** *Se p è un numero primo e $a \in \mathbb{Z}$ è tale che $(a, p) = 1$, allora*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Prima dimostrazione. Essendo a e p coprimi, è possibile semplificare la congruenza $a^p \equiv a \pmod{p}$ per a ottenendo così $a^{p-1} \equiv 1 \pmod{p}$.
Seconda dimostrazione[13]. Consideriamo gli insiemi $S_1 = \{0, 1, 2, 3, \ldots, p-1\}$ e $S_2 = \{0, a, 2a, 3a, \ldots, (p-1)a\}$. Poiché p non divide a, per la Proposizione 1.1.5, S_1 e S_2 rappresentano due sistemi completi di residui modulo p; pertanto ogni elemento di S_2 è congruo modulo p ad uno ed un solo elemento di S_1 ed elementi distinti di S_2 sono congrui modulo p ad elementi distinti di S_1. Di conseguenza si ha

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

cioè

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}.$$

Essendo $(p-1)!$ non divisibile per p, è possibile semplificare la precedente congruenza per $(p-1)!$, ottenendo così

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Risulta, ad esempio, $25^{40} \equiv 1 \pmod{41}$, essendo 41 un numero primo e $(25, 41) = 1$. Ancora, $36^{2010} \equiv 1 \pmod{2011}$ in quanto 2011 è un numero primo e $(36, 2011) = 1$.

[12] La nozione di numero pseudoprimo è legata a quella di un tipo più raro di numeri, i cosiddetti *numeri di Carmichael* cioè interi n non primi tali che $a^{n-1} \equiv 1 \pmod{n}$ per ogni intero a coprimo con n. Si dimostra facilmente che un intero non primo n è di Carmichael se e solo se $n \mid (a^n - a)$ per ogni intero a. Ne segue che ogni numero di Carmichael è pseudoprimo. Il viceversa, in generale, è falso, in quanto, ad esempio, 341 non è di Carmichael. Infatti si vede che $31 \nmid (11^{341} - 11)$ e quindi $341 \nmid (11^{341} - 11)$. Il più piccolo numero di Carmichael è 561, il successivo 1105.

[13] La dimostrazione è dovuta al matematico e astronomo scozzese James Ivory e risale al 1806. Per le sue ricerche in campo astronomico, fu la prima persona a essere insignita (nel 1826) della Medaglia Royal, per un importante risultato in campo astronomico.

Esempio 1.4.3. Determinare il resto della divisione per 43 del numero

$$2^{2019} + 5^{2019} + 7^{2019} + 9^{2019}.$$

Soluzione. Osservato che $2, 5, 7, 9$ sono coprimi con 43, per il Piccolo Teorema di Fermat risulta $2^{42} \equiv 5^{42} \equiv 7^{42} \equiv 9^{42} \equiv 1 \pmod{43}$ e quindi, essendo $2019 = 42 \cdot 48 + 3$, si ha

$$2^{2019}+5^{2019}+7^{2019}+9^{2019} = \left(2^{42}\right)^{48} \cdot 2^3 + \left(5^{42}\right)^{48} \cdot 5^3 + \left(7^{42}\right)^{48} \cdot 7^3 + \left(9^{42}\right)^{48} \cdot 9^3 \equiv$$
$$8 + 125 + 49 \cdot 7 + 81 \cdot 9 \equiv 133 + 6 \cdot 7 + (-5) \cdot 9 \equiv 4 - 1 - 2 \equiv 1 \pmod{43}.$$

Il resto della divisione di $2^{2019} + 5^{2019} + 7^{2019} + 9^{2019}$ per 43 è, pertanto, 1. □

Esempio 1.4.4. Dimostrare che per ogni $n \in \mathbb{N}$ il numero

$$7n^{21} + 6n^{31} + 34n^3 + 8n$$

è divisibile per 5.

Soluzione. Applichiamo il Piccolo Teorema di Fermat per calcolare le potenze modulo 5.
Se n è divisibile per 5 il risultato è banalmente vero. Supponiamo allora che n non sia divisibile per 5, cioè che $(n, 5) = 1$. Per il Piccolo Teorema di Fermat risulta $n^4 \equiv 1 \pmod{5}$ e quindi

$$n^{21} = (n^4)^5 \cdot n \equiv n \pmod{5}, \qquad n^{31} = (n^4)^7 \cdot n^3 \equiv n^3 \pmod{5}.$$

Di conseguenza

$$7n^{21} + 6n^{31} + 34n^3 + 8n \equiv 2n + n^3 + 4n^3 + 3n \equiv 5n + 5n^3 \equiv 0 \pmod{5}$$

e quindi $7n^{21} + 6n^{31} + 34n^3 + 8n$ è divisibile per 5 qualunque sia $n \in \mathbb{N}$.
Da notare che la dimostrazione poteva anche essere effettuata per induzione[14] su n (esercizio per il lettore). □

Esempio 1.4.5. Dimostrare che se p è un numero primo diverso da 2, 3 e 5 allora p divide il numero $u_p = 111\ldots1$ costituito da $p - 1$ cifre uguali a 1.

Soluzione. Osservato che $(p, 10) = 1$, per il Piccolo Teorema di Fermat si ha $10^{p-1} \equiv 1 \pmod{p}$, per cui p divide $10^{p-1} - 1$. Ma $10^{p-1} - 1 = 9 \cdot u_p$, sicché p divide $9 \cdot u_p$; ma p non divide 9 (ed è primo), pertanto p divide u_p. □

[14] Per il Principio di Induzione si veda *Teoria dei numeri*, Paragrafo 1.1.

1.5 La funzione di Eulero e il teorema di Eulero

Il Piccolo Teorema di Fermat permette di calcolare potenze modulari nel caso in cui il modulo sia un numero primo e fornisce una importante relazione che è possibile applicare in svariate tipologie di problemi.
Nel 1760, il matematico svizzero Leonhard Euler generalizzò il teorema di Fermat al caso di moduli composti. Tale generalizzazione restituisce, ovviamente, il risultato ottenuto da Fermat quando il modulo è primo.
Per far questo, Eulero fece uso di una particolare funzione, da lui stesso ideata e che di seguito definiamo.

Definizione 1.5.1. Sia $n \geq 1$ intero. Si definisce **funzione di Eulero** di n e si indica con $\varphi(n)$ la funzione che rappresenta il numero di interi positivi minori o uguali ad n e relativamente primi con n (cioè tutti gli interi positivi a tali che $a \leq n$ e $(a, n) = 1$)[15].

Ad esempio, $\varphi(20) = 8$ perché i numeri minori o uguali a 20 e relativamente primi con 20 sono $1, 3, 7, 9, 11, 13, 17, 19$.
Nella tabella seguente riportiamo i valori della funzione $\varphi(n)$ per alcuni valori di n.

n	1	2	3	4	6	8	9	10	12	13	15
$\varphi(n)$	1	1	2	2	2	4	6	4	4	12	8

Le proposizioni che seguono permettono di calcolare la funzione di Eulero *per ogni intero n del quale si conosca la fattorizzazione.*

Proposizione 1.5.2. *φ è una funzione* moltiplicativa*, cioè*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \qquad \forall a, b \in \mathbb{N}^+ \ \textit{tali che} \ (a, b) = 1.$$

Dimostrazione. Se almeno uno degli interi a e b è 1, essendo $\varphi(1) = 1$ si ha immediatamente la tesi.
Siano allora $a, b > 1$. Come sappiamo, il numero $\varphi(ab)$ è uguale al numero complessivo di termini della tabella seguente

1,	2,	3,	...,	r,	...,	a-1,	a
a+1,	a+2,	a+3,	...,	a+r,	...,	2a-1,	2a
2a+1,	2a+2,	2a+3,	...,	2a+r,	...,	3a-1,	3a
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
(b-1)a+1,	(b-1)a+2,	(b-1)a+3,	...,	(b-1)a+r,	...,	ab-1,	ab

[15] Eulero denotò con $\pi(n)$ il numero di interi positivi minori di n e coprimi con n. La notazione in uso, cioè $\varphi(n)$, è quella che Gauss utilizzò nella sua opera *Disquisitiones Arithmeticae.*

che sono relativamente primi con ab, cioè gli interi che sono relativamente primi sia con a che con b.
Sia quindi r un intero positivo $\leq a$ e consideriamo l'$r-$esima colonna della tabella precedente. Se $(a, r) = 1$, allora tutti i numeri di tale colonna sono relativamente primi con a; se, invece, $(a, r) > 1$, nessuno dei numeri di tale colonna è relativamente primo con a. Ora, il numero di interi positivi $r < a$ tali che $(a, r) = 1$ è ovviamente $\varphi(a)$ e quindi, per quanto detto prima, $\varphi(a)$ rappresenta anche il numero di colonne della tabella i cui elementi sono tutti relativamente primi con a. In ciascuna di tali colonne, per la Proposizione 1.1.5, il numero di elementi relativamente primi con b è pari a $\varphi(b)$.
Abbiamo così provato che in ognuna delle $\varphi(a)$ colonne, in cui i termini sono tutti relativamente primi con a, ci sono $\varphi(b)$ elementi relativamente primi anche con b. Di conseguenza, il numero totale di elementi della tabella relativamente primi con ab, cioè $\varphi(ab)$, è pari a $\varphi(a) \cdot \varphi(b)$. □

Esempio 1.5.1. Calcoliamo la funzione di Eulero degli interi 52 e 120.
Per la proposizione precedente, si ha $\varphi(52) = \varphi(4 \cdot 13) = \varphi(4) \cdot \varphi(13) = 2 \cdot 12 = 24$ e $\varphi(120) = \varphi(8 \cdot 15) = \varphi(8) \cdot \varphi(15) = 4 \cdot 8 = 32$.

La funzione di Eulero non è, tuttavia, completamente moltiplicativa, cioè non è sempre vero che

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \forall a, b \in \mathbb{Z}^+.$$

(basta osservare ad esempio che $8 = \varphi(16) = \varphi(8 \cdot 2) \neq \varphi(8) \cdot \varphi(2) = 4 \cdot 1 = 4$).

Conseguenza immediata della moltiplicatività della funzione di Eulero è, allora, la seguente proposizione.

Proposizione 1.5.3. *Sia $n = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}$ la fattorizzazione di n, con i p_i $(i = 1, \ldots, s)$ primi distinti. Allora risulta*

$$\varphi(n) = \varphi\left(p_1^{h_1}\right) \varphi\left(p_2^{h_2}\right) \cdots \varphi\left(p_s^{h_s}\right).$$

Ad esempio, dato il numero $2016 = 2^5 \cdot 3^2 \cdot 7$, risulta $\varphi(2016) = \varphi\left(2^5\right) \cdot \varphi\left(3^2\right) \cdot \varphi(7)$. Con il precedente risultato a disposizione siamo ridotti semplicemente a dover calcolare il valore di φ sulle potenze di un primo, ossia $\varphi\left(p^h\right)$.

Proposizione 1.5.4. *Se p è un numero primo, allora per ogni $h \geq 1$ intero risulta*

$$\varphi\left(p^h\right) = p^h - p^{h-1}.$$

Dimostrazione. Osserviamo che non sono primi con p^h solo i multipli di p ed essi sono del tipo

$$p \cdot i, \qquad \text{con } 1 \leq i \leq p^{h-1}.$$

Essendo questi ultimi in numero di p^{h-1}, il numero di interi positivi minori di p^h e coprimi con p^h è dato dai rimanenti $p^h - p^{h-1}$ interi. □

Esempio 1.5.2. Usando la Proposizione 1.5.4 troviamo che $\varphi(5^3) = 5^3 - 5^2 = 100$, $\varphi(3^4) = 3^4 - 3^3 = 54$ e $\varphi(2^{10}) = 2^{10} - 2^9 = 512$.

Osservazione 1.5.5. Osserviamo che per un primo p, risulta $\varphi(p) = p - 1$. Ad esempio, $\varphi(11) = 11 - 1 = 10$. D'altronde tutti gli interi positivi minori di p (che sono in numero di $p - 1$) sono primi con p.

Combinando le Proposizioni 1.5.3 e 1.5.4 siamo a questo punto in grado di calcolare $\varphi(n)$ per ogni $n \in \mathbb{Z}^+$ del quale si conosca la fattorizzazione. Infatti, se $n = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}$ si ha

$$\boxed{\varphi(n) = \left(p_1^{h_1} - p_1^{h_1-1}\right)\left(p_2^{h_2} - p_2^{h_2-1}\right)\left(p_3^{h_3} - p_3^{h_3-1}\right)\cdots\left(p_s^{h_s} - p_s^{h_s-1}\right)}$$

o, equivalentemente, raccogliendo a fattor comune la potenza massima all'interno di ogni parentesi,

$$\varphi(n) = p_1^{h_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{h_2}\left(1 - \frac{1}{p_2}\right) \cdot p_3^{h_3}\left(1 - \frac{1}{p_3}\right)\cdots p_s^{h_s}\left(1 - \frac{1}{p_s}\right)$$

da cui

$$\boxed{\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\cdots\left(1 - \frac{1}{p_s}\right)}.$$

Esempio 1.5.3. Si ha $\varphi(72) = \varphi\left(2^3 \cdot 3^2\right) = \varphi\left(2^3\right) \cdot \varphi\left(3^2\right) = \left(2^3 - 2^2\right) \cdot \left(3^2 - 3\right) = 4 \cdot 6 = 24$.
Ancora, se $n = 2016$, risulta $\varphi(2016) = \varphi\left(2^5 \cdot 3^2 \cdot 7\right) = \varphi\left(2^5\right) \cdot \varphi\left(3^2\right) \cdot \varphi(7) = \left(2^5 - 2^4\right) \cdot \left(3^2 - 3\right) \cdot (7 - 1) = 16 \cdot 6 \cdot 6 = 576$.
Equivalentemente si ha

$$\varphi(72) = 72 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 72 \cdot \frac{1}{2} \cdot \frac{2}{3} = 24$$

e

$$\varphi(2016) = 2016 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 72 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 576.$$

Presentiamo, adesso, una dimostrazione alternativa della formula chiusa per il calcolo della funzione di Eulero, che fa uso del *Principio di inclusione-esclusione*[16] Detta $n = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}$ la fattorizzazione di n, definiamo gli insiemi

$$A_i = \{ \text{ interi maggiori o uguali a 1 e minori o uguali a } n \text{ divisibili per } p_i \}$$

per $i = 1, 2, \ldots, s$. Il numero degli interi maggiori o uguali a 1 e minori o uguali a n che **non** sono primi con n è dato dunque da $|A_1 \cup A_2 \cup \ldots \cup A_n|$, calcolabile utilizzando il principio di inclusione-esclusione. Osservato quindi che

$$\begin{aligned}
&|A_i| = \frac{n}{p_i} \quad \text{per } i = 1, 2, \ldots, s \\
&|A_i \cap A_j| = \frac{n}{p_i p_j} \quad \text{per } i, j = 1, 2, \ldots s,\ i \neq j \text{[17]} \\
&|A_i \cap A_j \cap A_k| = \frac{1}{p_i p_j p_k} \quad \text{per } i, j, k = 1, 2, \ldots, s,\ i \neq j \neq k \\
&\quad \vdots \\
&|A_1 \cap A_2 \cap \cdots \cap A_s| = \frac{n}{p_1 p_2 \cdots p_s}
\end{aligned}$$

per il Principio di inclusione-esclusione si ha

$$|A_1 \cup A_2 \cup \cdots \cup A_s| = \sum_{i=1}^{s} \frac{n}{p_i} - \sum_{1 \leq i < j \leq s} \frac{n}{p_i p_j} + \sum_{1 \leq i < j < k \leq s} \frac{n}{p_i p_j p_k} - \cdots + (-1)^{s+1} \frac{n}{p_1 p_2 \cdots p_s} = -n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) + n.$$

Gli interi positivi e minori di n coprimi con n sono quindi in numero pari a

$$n - \left(-n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) + n \right) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right).$$

Esempio 1.5.4. Consideriamo $n \geq 5$ punti distinti, disposti su una circonferenza alla stessa distanza uno dall'altro (sono i vertici di un poligono regolare). Ci

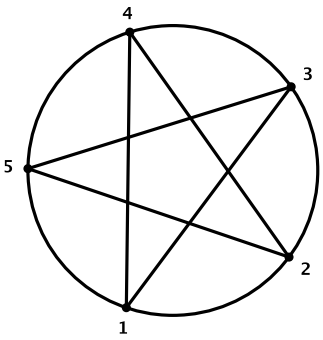
[16] Il Principio di inclusione-esclusione è il nucleo portante di molti problemi di calcolo combinatorio e probabilità. Esso così si può enunciare: dati n insiemi di cardinalità finita $A_1, A_2, A_3, \ldots, A_n$, il numero degli elementi dell'insieme unione $A_1 \cup A_2 \cup \cdots \cup A_n$ è dato da

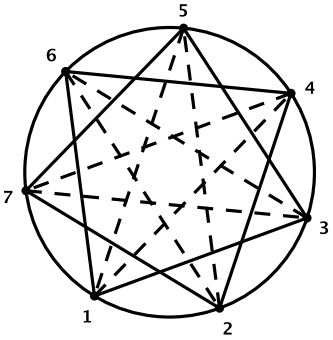
$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

(avendo indicato con $|X|$ il numero di elementi dell'insieme finito X).

[17] Gli interi appartenenti all'intersezione di due insiemi sono quelli divisibili contemporaneamente per p_i e p_j e quindi per $p_i p_j$.

chiediamo in quanti modi diversi (a meno del senso orario o antiorario di percorrenza) è possibile congiungere gli n punti a formare una **stella**, toccando ogni punto una sola volta e ritornando al punto di partenza in maniera non banale (cioè senza formare un poligono). Nella figura sottostante sono visualizzati i casi $n = 5$ (una sola configurazione possibile) e $n = 7$ (due configurazioni possibili)





ottenute, la prima secondo la sequenza $1-3-5-2-4-1$ e le seconde due secondo le sequenze $1-3-5-7-2-4-6-1$ e $1-4-7-3-6-2-5-1$.
Osserviamo pertanto che le condizioni da seguire nel costruire una stella come fatto negli esempi precedenti sono:

❶ la distanza k tra due vertici successivi della stella deve essere costante e diversa da 1 ed $n-1$ (in caso contrario avremmo un poligono);

❷ saltando da un vertice all'altro a distanza di k bisogna tornare al punto di partenza toccando tutti i punti una sola volta e questo accade se e solo se $(k, n) = 1$;

❸ è indifferente se ci muoviamo in senso orario o in senso antiorario.

Da tali condizioni ricaviamo immediatamente che il numero di stelle distinte a $n \geq 5$ punte è dato da

$$\frac{\varphi(n) - 2}{2}.$$

Infatti, per il punto ❷, è possibile disegnare al massimo $\varphi(n)$ stelle, numero degli interi positivi minori di n e coprimi con n; da tale numero, per il punto ❶, dobbiamo togliere due configurazioni. Infine, per il punto ❸, è necessario dividere tutto per 2 altrimenti ogni configurazione verrebbe contata due volte.
Da quanto appena detto, segue che non è possibile formare stelle a 6 punte; esistono, invece, 2 stelle a nove punte e 3 stelle a sedici punte. □

Di fondamentale importanza è il seguente risultato che generalizza il Piccolo Teorema di Fermat al caso di moduli arbitrari. Ne proponiamo due dimostrazioni, una che ricalca l'idea della dimostrazione del Piccolo Teorema di Fermat (Proposizione 1.4.7), l'altra basata sul Principio di Induzione.

Proposizione 1.5.6 (Teorema di Eulero)**.** *Se a ed n sono due interi positivi tali che $(a, n) = 1$, allora*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Prima dimostrazione. Sia $a_1, a_2, \ldots, a_{\varphi(n)}$ un sistema ridotto di residui modulo n, cioè $\varphi(n)$ interi a due a due non congrui modulo n e coprimi con n. Consideriamo l'insieme

$$S = \left\{aa_1, aa_2, aa_3, \ldots, aa_{\varphi(n)}\right\}$$

e dimostriamo che i suoi elementi costituiscono un sistema ridotto di residui modulo n. A tal fine occorre dimostrare che gli interi sono a due a due non congrui modulo n e coprimi con n.
Supponiamo per assurdo che $aa_i \equiv aa_j \pmod{n}$ per qualche $i \neq j$. Essendo $(a, n) = 1$, è possibile semplificare la congruenza per a e ottenere $a_i \equiv a_j \pmod{n}$. Ciò contraddice il fatto che a_i e a_j sono elementi di un sistema ridotto di residui e quindi $a_i \not\equiv a_j \pmod{n}$. Ne segue che tutti gli elementi di S sono a due a due non congrui.
Inoltre, dato che $(a_i, n) = 1$, per ogni $i = 1, 2, 3, \ldots, \varphi(n)$, e $(a, n) = 1$, tutti gli elementi di S sono coprimi con n.
S è, quindi, un sistema ridotto di residui modulo n. Conseguentemente gli elementi di S sono congrui, in qualche ordine, agli interi $a_1, a_2, \ldots, a_{\varphi(n)}$. Possiamo così scrivere

$$(aa_1)(aa_2)\cdots(aa_{\varphi(n)}) \equiv a_1 a_2 \cdots a_{\varphi(n)} \pmod{n},$$

e dividere ambo i membri per ciascuno degli interi $a_1, a_2, \ldots, a_{\varphi(n)}$ per ottenere

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

cioè la tesi.
Seconda dimostrazione. Procederemo per gradi: proveremo innanzitutto che se p è un primo che non divide a, allora

$$a^{\varphi\left(p^k\right)} \equiv 1 \pmod{p^k} \qquad \forall k \in \mathbb{Z}^+.$$

Procediamo per induzione su k. Per $k = 1$ risulta

$$a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p}$$

che altro non è che il Piccolo Teorema di Fermat, già dimostrato. Supponiamo che $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$ sia vera per k e dimostriamola per $k+1$. Essa si può scrivere come

$$a^{\varphi(p^k)} = 1 + hp^k$$

per qualche $h \in \mathbb{Z}$. Si noti anche che

$$\varphi\left(p^{k+1}\right) = p^{k+1} - p^k = p\left(p^k - p^{k-1}\right) = p \cdot \varphi\left(p^k\right).$$

Quindi, applicando la formula dello sviluppo del binomio di Newton,

$$a^{\varphi(p^{k+1})} = a^{p\cdot\varphi(p^k)} = \left(1 + hp^k\right)^p = 1 + \binom{p}{1} hp^k + \binom{p}{2} \underbrace{\left(hp^k\right)^2}_{\equiv 0 \pmod{p^{k+1}}} + \cdots$$

$$\cdots + \binom{p}{p-1} \underbrace{\left(hp^k\right)^{p-1}}_{\equiv 0 \pmod{p^{k+1}}} + \underbrace{\left(hp^k\right)^p}_{\equiv 0 \pmod{p^{k+1}}} \equiv 1 + \binom{p}{1} hp^k \equiv 1 \pmod{p^{k+1}}$$

perché $\binom{p}{1} hp^k$ è un multiplo di p^{k+1}. Abbiamo così dimostrato che $a^{\varphi(p^{k+1})} \equiv 1 \pmod{p^{k+1}}$ e quindi, per il Principio di induzione, $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$ per ogni $k \geq 1$ intero.
Dimostriamo ora il caso generale. Sia $(a, n) = 1$, e sia

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}.$$

Per quanto provato, per ogni i risulta

$$a^{\varphi\left(p_i^{k_i}\right)} \equiv 1 \pmod{p_i^{k_i}}, \qquad i = 1, 2, \ldots, s. \qquad (*)$$

Essendo la funzione φ moltiplicativa, risulta che $\varphi\left(p_i^{k_i}\right)$ divide $\varphi(n)$ per ogni $i = 1, 2, \ldots s$, per cui, elevando entrambi i membri di $(*)$ alla potenza $\dfrac{\varphi(n)}{\varphi\left(p_i^{k_i}\right)}$ si ottiene

$$a^{\varphi(n)} \equiv 1^{\frac{\varphi(n)}{\varphi\left(p_i^{k_i}\right)}} \equiv 1 \pmod{p_i^{k_i}}$$

per ogni $i = 1, 2, \ldots, s$. Ma allora, osservando che $\left[p_1^{k_1}, p_2^{k_2}, \ldots, p_s^{k_s}\right] = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$, si ha

$$a^{\varphi(n)} \equiv 1 \pmod{p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}}$$

e quindi

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

□

Esempio 1.5.5. Posto $n = 21$ e $a = 10$, essendo $(10, 21) = 1$ e $\varphi(21) = \varphi(3 \cdot 7) = \varphi(3) \cdot \varphi(7) = 2 \cdot 6 = 12$, per il teorema di Eulero risulta $10^{\varphi(21)} \equiv 1 \pmod{21}$, cioè $10^{12} \equiv 1 \pmod{21}$.

Vediamo come è possibile risolvere problemi di aritmetica modulare applicando il Teorema di Eulero.

Esempio 1.5.6. Determinare le ultime due cifre della rappresentazione decimale dei numeri 9^{201} e 3^{950}.

Soluzione. Osserviamo che $\varphi(100) = \varphi\left(5^2 \cdot 2^2\right) = \left(5^2 - 5\right)\left(2^2 - 2\right) = 40$ e quindi $9^{\varphi(100)} = 9^{40} \equiv 1 \pmod{100}$. Ne segue che $9^{201} = (9^{40})^5 \cdot 9 \equiv 9 \pmod{100}$ e quindi il resto della divisione di 9^{201} per 100 è pari a 9, cioè le ultime due cifre di 9^{201} sono 0 e 9.
D'altra parte, sempre per il Teorema di Eulero, $3^{40} = 3^{\varphi(100)} \equiv 1 \pmod{100}$, quindi $3^{950} = 3^{40 \cdot 23} \cdot 3^{30} = (3^{40})^{23} \cdot (3^5)^6 \equiv 1 \cdot 43^6 \equiv 49^3 \equiv 49 \pmod{100}$. Ne segue che le ultime due cifre del numero 3^{950} sono 4 e 9. □

Esempio 1.5.7. Se un intero positivo n è prodotto di due primi distinti, la conoscenza di $\varphi(n)$ equivale a saper fattorizzare n. Infatti, se $n = p \cdot q$, risulta $\varphi(n) = (p-1)(q-1)$, e quindi risolvendo il sistema

$$\begin{cases} pq = n \\ (p-1)(q-1) = \varphi(n) \end{cases}$$

è possibile determinare p e q e quindi la fattorizzazione di n.
Ad esempio, se $n = 2279$ e $\varphi(2279) = 2184$, sapendo che $n = p \cdot q$ e risolvendo il sistema

$$\begin{cases} pq = 2279 \\ (p-1)(q-1) = 2184 \end{cases}$$

si trova $p = 43$ e $q = 53$, cioè $2279 = 43 \cdot 53$. □

Esempio 1.5.8. Determinare le ultime tre cifre del numero 13^{9999}.

Soluzione. Determinare le ultime tre cifre di 13^{9999} equivale a trovare il resto della divisione del numero per 1000. Detto x tale resto, si ha $13^{9999} \equiv x \pmod{1000}$ e quindi $13x \equiv 13^{10000} \pmod{1000}$; essendo 13 e 1000 primi tra loro, per il Teorema di Eulero $13^{\varphi(1000)} \equiv 1 \pmod{1000}$. Ma $\varphi(1000) = \varphi\left(2^3 \cdot 5^3\right) = 400$, quindi $13^{400} \equiv 1 \pmod{1000}$. Da ciò segue che $13^{10000} \equiv \left(13^{400}\right)^{25} \equiv 1 \pmod{1000}$. Allora basta determinare x tale che $13x \equiv 1 \pmod{1000}$. A tale scopo osserviamo