Home Teorema W-F Teorema V-V Teoria dei numeri mp3

Il teorema che ho indicato con la sigla W-F non esaurisce la sua potenzialità con i teoremi descritti nella relazione "Da Wilson a Fermat" , anzi dimostra la sua centralità ancora di più nel momento in cui lo generalizziamo a tutti i numeri dispari: se ne deduce il famoso teorema di Eulero. E non solo questo. Chi volesse commentare questa relazione, può inviarmi una e-mail all'indirizzo indicato sopra.

pubblicazione web del 10-01-2016

Teorema di Eulero

Se q è un intero positivo dispari e a (0 < a < q) è coprimo con q , necessariamente deve valere l'uguaglianza:

$$a^{\phi(q)} - 1 = mq$$

Il simbolo $\phi(q)$ è la funzione phi di Eulero e rappresenta il numero degli interi **a** (0<a<q) coprimi con q.

Dimostrazione

Sia q intero positivo dispari

Consideriamo l'insieme A di tutti i resti delle divisioni dei numeri interi positivi, che non siano multipli di q, per q:

$$A=\{1, 2, 3, \ldots, (q-1)\}$$

- Se q è numero primo, tutti gli elementi di A sono coprimi con q , per cui $\phi(q)=(q-1)$.
In questo caso "Il piccolo teorema di Fermat" appare come un caso particolare del teorema di Eulero.

- Se q è numero composto, consideriamo il sottoinsieme F degli elementi di A che sono coprimi con q:

$$F=\{c_1 , c_2 , c_3 , \ldots , c_{\phi(q)}\}$$

Si tenga presente che: se $c \in F$, anche $(q-c) \in F$ e tra gli elementi di F ci sono sempre 1 e q-1 .
Moltiplichiamo ciascun termine dell'insieme F per tutti gli elementi dello stesso F .
- I prodotti del primo termine di F , cioè 1, per tutti i termini di F riproducono lo stesso insieme F .
- I prodotti di un qualsiasi altro termine j di F per tutti gli elementi dello stesso F formano l'insieme M_j, costituito da $\phi(q)$ multipli di j :

$$M_j = \{j \cdot c_1 , j \cdot c_2 , j \cdot c_3 , \ldots , j \cdot c_{\phi(q)}\}$$

Calcoliamo ora i resti che si ottengono dividendo ciascun elemento di M_j per q e indichiamo con B_j il loro insieme.
Gli elementi dell'insieme B_j hanno le seguenti caratteristiche:
1) - sono tanti quanti sono quelli di F ;
2) - ciascun di essi è coprimo con q , maggiore di 0 e minore di q ;
3) - sono tutti diversi tra loro.

---

* Dimostriamo che ogni elemento $a \in B_j$ è coprimo con q , cioè: $(a , q) = 1$
Basta osservare che a si ottiene dall'uguaglianza: $j \cdot c = g \cdot q + a$, essendo j e c elementi di F e quindi coprimi con q.
Se a e q non fossero coprimi, indicando con d un loro divisore comune [$(a , q) = d$; $d \neq 1$], si avrebbe l'uguaglianza : $j \cdot c/d = g \cdot q/d + a/d$
Quindi d dovrebbe essere un divisore anche di j o di c o di entrambi, in contradizione con l'ipotesi.
Dobbiamo quindi ammettere che tutti gli elementi di B_j sono coprimi con q.

* Dimostriamo che gli elementi di B_j sono tutti diversi gli uni dagli altri.
Siano $j \cdot x$ e $j \cdot y$ due elementi distinti di M_j .
Essendo x e y elementi distinti dell'insieme F , sono entrambi coprimi con q , minori di q e maggiori di 0 , sia x > y .
Eseguiamo le divisioni di $j \cdot x$ e di $j \cdot y$ per q e supponiamo, per assurdo, che producano lo stesso resto r .
Si avranno così le relazioni : $j \cdot x = hq + r$; $j \cdot y = kq + r$
Da queste, sottraendo membro a membro, ne consegue che $(x - y) \cdot j = (h - k) \cdot q$; ma ciò è impossibile.
Infatti dall'uguaglianza $(x-y) = q(h-k)/j$, essendo q e j coprimi, ne consegue che (h-k) è multiplo di j , per cui si avrebbe: $(x-y)=qm$
Questa uguaglianza è falsa perché: $0 < (x-y) < q$
Essendo caduti in contradizione, non resta che concludere che gli elementi di B_j sono tutti distinti tra loro.

I punti 1) , 2) , 3) ci assicurano che l'insieme B_j è formato dagli stessi elementi di F , anche se ordinati in modo diverso.
Consideriamo tra gli elementi dell'insieme B_j il resto **a** , essendo **a** uno qualunque dei suoi elementi, e lo denominiamo base.
Diciamo che l'elemento c dell'insieme F che ha determinato il resto **a** in B_j è l'elemento **a**-simmetrico di j in F .
- Procedendo come abbiamo operato con j , per ogni elemento di F si troverà un altro elemento di F ad esso simmetrico rispetto ad **a**.
Pertanto, scelta la base **a** , siamo certi che un qualsiasi elemento j di F ha nello stesso F un suo **a**-simmetrico c :

$$j \cdot c \equiv \mathbf{a} \pmod{q} \; ; \; 0 < \mathbf{a} < q \; ; \; (a , q)=1$$

Ma è possibile che due elementi distinti di F abbiano lo stesso elemento **a**-simmetrico?
Supponiamo che ciò sia possibile, cioè che due elementi distinti di F , siano essi t ed f $(t > f)$, abbiano lo stesso **a**-simmetrico g .
Con questa ipotesi si avrà: $t \cdot g = q \cdot k + \mathbf{a}$; $f \cdot g = q \cdot h + \mathbf{a}$ e , sottraendo membro a membro: $(t-f) \cdot g = q \cdot (k-h)$, cioè $t-f=q \cdot (k-h)/g$
Considerando che (t-f) e (k-h) sono interi e che g e q sono coprimi, necessariamente (k-h) deve essere multiplo di g , per cui: $t-f=q \cdot m$
Ma questa uguaglianza è falsa, perché $0 < (t-f) < q$.
Quindi ogni elemento di F ha un suo **a**-simmetrico specifico, diverso da quello associato a ciascuno degli altri elementi dello stesso F .

Da quanto abbiamo asserito finora si deduce che l'insieme F , costituito dai soli elementi di A coprimi con q , così come lo abbiamo istituito, rispetto all'operazione di moltiplicazione, forma quello che in algebra viene chiamato "gruppo abeliano" .
Ciò vuol dire che: se si assume la base **a**=1 , 1 rappresenta l'elemento neutro di F: $j \cdot 1 = 1 \cdot j = j$, qualunque sia l'elemento j di F ; il prodotto di due elementi qualsiasi di F è ancora un elemento di F ; vale la proprietà commutativa: $a \cdot b = b \cdot a$; vale la proprietà associativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; ogni elemento j di F ha un suo simmetrico j^- in F : $j \cdot j^- = j^- \cdot j = 1$.

Ci chiediamo ora quale possa essere il prodotto di tutti gli elementi di F .

A tal fine, indichiamo l'insieme F col termine " Insieme ϕ " e il prodotto di tutti i suoi elementi col simbolo $\phi!$

$$\phi! = 1 \cdot c_2 \cdot c_3 \cdot \ldots \cdot c_{\phi(q)}$$

Per eseguire questo calcolo è necessario stabilire se qualche elemento dell'insieme ϕ abbia come **a**-simmetrico sé stesso.
Sia d un elemento di ϕ e supponiamo che: $d^2 = t \cdot q + \mathbf{a}$
Se **a** è un quadrato perfetto, cioè è tale che $\mathbf{a}=c^2$, ne segue che: $d^2 - c^2 = t \cdot q$, quindi: $(d-c)(d+c) = t \cdot q$
Essendo q composto, quest'ultima uguaglianza potrebbe essere vera, per cui è possibile che qualche elemento $d \in \phi$ abbia i requisiti richiesti.
Se **a** non è un quadrato perfetto la ricerca degli elementi d, in coppia con sé stessi, sicuramente è più complessa.
In questa relazione non andiamo in fondo alla questione: per i nostri scopi bastano le seguenti considerazioni.
a*) - Gli elementi di ϕ sono in numero pari.
Ciò si deduce dalla formula di $\phi(q)$ e dall'ipotesi che q sia dispari:

$$\phi(q) = q(1-1/d1)(1-1/d2) \ldots (1-1/dn) \quad \text{(Le lettere d indicano i fattori primi di q)}$$

b*) - Se $c \in \phi$, anche $(q-c) \in \phi$
Infatti, posto q-c=e , se supponiamo che ci sia un divisore t di e di q [$(q , e)=t$ $(t \neq 1)$] , dovremmo ammettere che t divida anche c, in contraddizione con l'ipotesi che q e c siano coprimi. Di conseguenza q-c non può che essere coprimo con q , quindi appartiene a ϕ .
c*) - Se esiste c tale che $c^2 = \mathbf{a}$, anche q-c dà origine allo stesso residuo quadratico. Infatti: $(q-c)^2 = q^2 - 2qc + c^2 \equiv c^2 \pmod{q}$.
Da qui deduciamo che, se dovessero esserci elementi di ϕ che hanno sé stessi come **a**-simmetrici, questi sono in numero pari.
d*) - Il prodotto: $c \cdot (q-c) \equiv -c^2 \pmod{q}$ ci dice che $c \cdot (q-c) \equiv -\mathbf{a}$, essendo $a \in \phi$ la base in cui c ha come **a**-simmetrico sé stesso.
In particolare, se $\mathbf{a}=1$, ne segue che $c \cdot (q-c) \equiv -1 \pmod{q}$

Fatte queste considerazioni, distinguiamo due situazioni differenti, relative alla base scelta.
1) - In ϕ non ci sono elementi in coppia con sé stessi.
In questo caso, certamente, possiamo associare tutti gli elementi di ϕ in coppie **a**-simmetriche:

$$\phi! = (c_1 \cdot c_j) \cdot (c_2 \cdot c_t) \cdot \ldots \cdot (c_{\phi(q)} \cdot c_h)$$

2) - In ϕ ci sono elementi in coppia con sé stessi.
In quest'altro caso possiamo associare gli elementi di ϕ , alcuni in coppie **a**-simmetriche , e gli altri, quelli che hanno sé stessi come **a**-simmetrici, in coppie della forma (c ; q-c) :

$$\phi! = (c_1 \cdot c_j) \cdot (c_2 \cdot c_t) \cdot \ldots \cdot [c_h \cdot (q - c_h)] \cdot \ldots \cdot [c_k \cdot (q - c_k)]$$

In entrambi i casi, se scegliamo la base **a**=1, sarà facile calcolare il valore del fi fattoriale, esso è dato dalle congruenze:

$$\phi! \equiv \pm 1 \pmod{q} \text{ , qualunque sia il numero dispari q}$$

Sarà +1 se le coppie (c ; q-c) sono in numero pari, valore 0 compreso, e -1 se invece sono dispari.

Dopo avere stabilito il valore di $\phi!$, rifacciamo il calcolo considerando una qualsiasi altra base **a** di ϕ $(a \neq 1)$.
Con ciascuna di queste basi si avranno le seguenti congruenze:

$$\phi! \equiv \pm a^{\phi(q)/2} \equiv \pm 1 \pmod{q} \text{ , } a \in \phi$$

Elevando al quadrato i membri di queste congruenze si ottiene il teorema di Eulero:

$$a^{\phi(q)} \equiv 1 \pmod{q} \text{ , } a \in \phi$$

Approfondendo lo studio dell'insieme ϕ è possibile dedurre in modo più specifico i valori di $\phi!$ e di $a^{\phi(q)/2}$
Il teorema che ho indicato con la sigla "V-V" mostra in modo più completo le caratteristiche dell'insieme ϕ , facendo apparire i tre più famosi teoremi della "Teoria dei numeri" (Teorema di Wilson, Piccolo teorema di Fermat, Teorema di Eulero-Fermat, come casi particolari di questo teorema più generale.
Qui di seguito ne do l'enumnciato

Teorema V-V

Sia q un qualsiasi numero intero dispari.

- Se q è composto da due o più fattori primi, oppure da potenze di due o più fattori primi:

$$\phi! \equiv 1 \pmod{q}$$
$$\phi! \equiv a^{\phi(q)/2} \equiv 1 \pmod{q} \text{ , } a \in \phi$$

- Se q è primo, oppure la potenza di un solo primo:

$$\phi! \equiv -1 \pmod{q}$$
$$\phi! \equiv a^{\phi(q)/2} \equiv -1 \pmod{q} \text{ , } a \in \phi \quad \text{non residuo quadratico}$$
$$\phi! \equiv -a^{\phi(q)/2} \text{ ; } a^{\phi(q)/2} \equiv 1 \pmod{q} \text{ , } a \in \phi \quad \text{residuo quadratico}$$

Per la dimostrazione cliccare su Teorema V-V