S.Giuseppe

Da Wilson a Fermat

(pubblicazione web del 04-05-2015)

In queste pagine osserveremo quali sono le caratteristiche dei numeri interi che ci consentono una dimostrazione aritmetica del teorema di Wilson

Rimaneggiando poi queste caratteristiche approderemo a un teorema che ho indicato con la sigla W-F .
La scelta "W-F" vuole indicare che questo teorema è l'anello di congiunzione tra i due più noti teorema della teoria dei numeri, il Teorema di Wilson e il Piccolo teorema di Fermat, rivelandone la loro proprietà comune e facendoli apparire come facce di una stessa medaglia.
Le particolarità dei numeri primi sintetizzate da questi teoremi sono anche quelle su cui si sviluppa una parte dell'algebra modulare.

Teorema di Wilson

Condizione necessaria e sufficiente affinché un numero intero positivo p (p > 1) sia primo è che sia valida l'uguaglianza:

$$(p-1)!+1 = m \cdot p$$

La condizione è necessaria.

Sia p numero primo , dimostriamo che il fattoriale (p-1)! addizionato a 1 è multiplo di p: $(p-1)!+1 = m \cdot p$
Consideriamo l'insieme A di tutti i resti delle divisioni dei numeri interi positivi, che non siano multipli di p, per p.

$$A = \{1 , 2 , 3 , 4 , \ldots , (p-1)\}$$

In modo evidente gli elementi dell'insieme A sono tutti i fattori del fattoriale (p-1)!
Moltiplichiamo ciascun termine dell'insieme A per tutti gli elementi dello stesso A .
- I prodotti del primo termine, cioè 1, per tutti i termini dell'insieme A riproduce lo stesso insieme A .
- I prodotti del secondo termine, cioè 2 , per tutti gli elementi di A forma l'insieme dei primi (p-1) multipli di 2: $M_2=\{2, 4 , \ldots , 2(p-1)\}$
Calcoliamo ora i resti che si ottengono dividendo i multipli di 2 dell'insieme M_2 per il numero primo p.
Si otterrà in questo modo un insieme B_2 formato da p-1 elementi che hanno le seguenti caratteristiche:
1) tra essi non c'è il numero 0, perché nessun elemento di M_2 è multiplo di p ;
2) ciascuno di essi è minore di p ;
3) sono tutti diversi tra loro.

Dimostriamo quest'ultima asserzione.
Siano 2x e 2y due elementi distinti di M_2.
Essendo x e y elementi distinti dell'insieme A , sono entrambi minori di p e maggiori di 0 , sia x > y .
Eseguiamo le divisioni di 2x e 2y per p e supponiamo, per assurdo, che producano lo stesso resto r .
Si avranno così le relazioni: $2x=kp+r$; $2y=hp+r$
Da qui, sottraendo membro a membro, ne consegue che $2(x - y) = p(k - h)$, ma ciò è impossibile.
Infatti, dato che $(x - y) \in A$, ne risulterebbe che il prodotto di due numeri, minori di p e maggiori di 0, è multiplo di p, la qual cosa non si può verificare perché p è numero primo.
In generale, siano c , b, m interi e p primo: $c \cdot b=p \cdot m \Rightarrow c=p \cdot (m/b) \Rightarrow c=p \cdot d$. Se $0< c<p$, questa uguaglianza è impossibile.
Essendo caduti in contradizione, non resta che concludere che gli elementi di B_2 sono tutti distinti tra loro.

Considerando i punti 1) 2) 3) , possiamo affermare che B_2 è formato dagli stessi elementi di A , anche se ordinati in modo diverso.

(***) A questo punto facciamo una scelta tra gli elementi dell'insieme B_2: consideriamo il resto 1.

Di seguito sceglieremo sempre lo stesso resto 1 in tutti gli insiemi contrassegnati con la lettera B.
Diciamo che l'elemento r_j dell'insieme A che determina il resto 1 in B_2 è l'elemento simmetrico di 2 in A.
Segniamo la coppia di elementi simmetrici $(2, r_j)$ dell'insieme A.

- Passiamo poi ai prodotti del terzo termine , cioè 3, per tutti i termini dell'insieme A (Se dovesse essere $r_j = 3$, passiamo al 4° termine)
Procedendo con il 3 allo stesso modo con cui abbiamo operato con il 2 otteniamo l'insieme B_3 , anch'esso coincidente con l'insieme A, e da qui ricaviamo la coppia di elementi simmetrici $(3, r_h)$ di A , essendo r_h l'elemento di A che determina il resto 1 in B_3.
- Continuiamo in questo modo con i successivi elementi di A , fino ad esaurirli tutti.
Certamente, con questo procedimento, per ciascun elemento di A si troverà un altro elemento di A ad esso simmetrico, ma occorre rispondere a due domande.

1*) - E' possibile che due elementi distinti di A abbiano lo stesso elemento simmetrico?
Supponiamo che ciò sia possibile, cioè che due elementi distinti di A, siano essi a e b (a>b), abbiano lo stesso simmetrico r_q .
In questa ipotesi, si avrà: $a \cdot r_q = p \cdot g+1$; $b \cdot r_q = p \cdot f+1$ e, sottraendo membro a membro: $(a-b) \cdot r_q = (g-f) \cdot p$
Ma, come abbiamo già dimostrato prima, questa uguaglianza è falsa, perché r_q e (a-b) sono elementi di A e p è primo.
Quindi ogni elemento di A ha un suo simmetrico specifico, diverso da quello associato a ciascuno degli altri elementi di A.

2*) - E' possibile che qualche elemento di A abbia come simmetrico sé stesso?
Sia b un qualsiasi elemento di A e supponiamo che abbia sé stesso come elemento simmetrico: $b^2 = tp+1$
Da qui ne segue che $b^2 - 1 = tp$, cioè: $(b-1)(b+1) = tp$
Quindi, se questo numero intero b esiste, è tale che il prodotto del suo precedente per il suo successivo è multiplo di p.
Andiamo ad esaminare l'insieme A alla ricerca di questo elemento.
* Se $1 < b < (p-1)$; il precedente di b e il successivo di b sono due elementi distinti di A e il loro prodotto non può essere multiplo di p, che è numero primo. Quindi, in questo caso, nessuno elemento $b \in A$ ha i requisiti cercati. $[0 < (b-1) < (p-2) ; 2 < (b+1) < p]$
* Se b=1, il successivo di 1 è il 2 e il precedente è 0, per cui effettivamente questo elemento ha i requisiti cercati: $(1-1)(1+1) = 0p$
* Se b=(p-1) il precedente è (p-2) e il successivo è p, per cui anche questo elemento ha i requisiti cercati: $(p-2)p = mp$

Conclusioni.
Ciò che caratterizza i numeri primi, diversamente da quelli composti, è che tutti i fattori del fattoriale (p-1)! , esclusi 1 e (p-1) , si possono associare in coppie simmetriche, e ciascuna coppia è formata da elementi distinti.
Associando tutte le coppie simmetriche, costituite da elementi distinti del fattoriale (p-1)! , il prodotto $1 \cdot (p-1) = (p-1)$ rimane isolato:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = 1 \cdot (2 \cdot r_j) \cdot (3 \cdot r_h) \cdot (4 \cdot rk) \cdot \ldots \cdot (p-1)$$

Il prodotto degli elementi simmetrici di ciascuna coppia, è un numero della forma $g \cdot p+1$, essendo $g \geq 0$ intero. Nei fatti abbiamo determinato ciascuna coppia di elementi simmetrici con numeri che hanno questa forma.
Inoltre, il prodotto di due o più numeri della forma $gp+1$ è ancora un numero della stessa forma, per cui:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = 1 \cdot (2 \cdot r_j) \cdot (3 \cdot r_h) \cdot (4 \cdot rk) \cdot \ldots \cdot (p-1) = 1 \cdot (fp+1) \cdot (p-1) = fp^2 - fp+p -1 = (fp-f+1)p - 1$$

e da questa, indicando con m il numero intero positivo fp-f+1 , ricaviamo la formula dell'enunciato: $(p-1)! +1 = mp$

(Se p non è primo accade che . . . tutti gli elementi di A , non coprimi con p , non hanno un loro elemento simmetrico).

La condizione è sufficiente

Dato il numero naturale p , sia $(p-1)! + 1 = mp$. Dimostriamo che p è numero primo.
Supponiamo, per assurdo, che p sia composto e indichiamo con d un suo divisore primo $(1 < d < p)$, per cui: $d \mid mp$
Poiché d è sicuramente un fattore del fattoriale (p-1)! , si avrà anche: $d \mid (p-1)!$
Da qui, data l'uguaglianza $(p-1)! +1 = mp$, ne seguirebbe che $d \mid 1$, il che è palesemente assurdo. Quindi p non può che essere primo.

Le proprietà dei numeri primi che ci hanno consentito la dimostrazione aritmetica del teorema di Wilson ci conducono a quest'altro teorema, da cui trarremo poi la dimostrazione del Piccolo teorema di Fermat. Ma, come vedremo in una prossima relazione, questo stesso teorema, generalizzato a tutti i numeri dispari, ci farà dedurre anche il Teorema di Eulero. Cosicché questi tre famosi teoremi della "Teoria dei Numeri" appariranno legati da un unico filo conduttore.

Teorema W-F

Se un intero positivo p (p >1) è primo , necessariamente deve essere vera una delle due uguaglianze:

$$a^{(p-1)/2} \pm 1 = mp \quad \text{per ogni valore di a , tale che } 0 < a < p$$

Approdiamo a questo teorema apportando delle modifiche al teorema di Wilson.
Sia p primo.
Rifacciamo il discorso fatto precedentemente con il teorema di Wilson, ma al punto (***) , facciamo una scelta diversa.
Questa volta scegliamo un qualsiasi elemento $\mathbf{a} \in B$ che sia diverso da 1 : $1 < \mathbf{a} < p$; denominiamo **a** col termine **base**.
Procedendo allo stesso modo di quando abbiamo scelto **a**=1, deduciamo facilmente che ad un qualsiasi elemento $j \in A$ è possibile associare un altro elemento $k \in A$, tale che il loro prodotto sia congruo ad **a**, secondo il modulo p: $j \bullet k \equiv \mathbf{a} \pmod p$; $j \bullet k = mp + \mathbf{a}$ $(1 < \mathbf{a} < p)$
Ciò implica che è possibile associare in coppie "**a**-simmetriche" tutti i fattori del fattoriale (p-1)!
Adesso però è diversa da quella precedente la risposta alla domanda:

2*) *E' possibile che qualche elemento di A abbia come "**a**-simmetrico" sé stesso ?*

La risposta è positiva in alcuni casi e negativa in altri, dipende dalla scelta di **a** .
Come vedremo di seguito, questo evento si verifica per il 50% dei valori di A , mentre per il restante 50% nessun elemento di A ha come "**a**-simmetrico" sé stesso.

Considerando che p è numero primo, per dimostrare il teorema w- **F** , esaminiamo di nuovo le due questioni **1*)** e **2*)** , affrontate precedentemente con il teorema di Wilson, avendo scelto in quella occasione il valore **a=1**.
1*) - E' possibile che due elementi distinti di A abbiano il medesimo elemento **a**-simmetrico?
Supponiamo che ciò sia possibile: due elementi distinti b e c di A abbiano lo stesso **a**-simmetrico r_q.
In questa ipotesi, sia b>c , si avrà: $b \bullet r_q = p \bullet m + \mathbf{a}$; $c \bullet r_q = p \bullet g + \mathbf{a}$ e , sottraendo membro a membro: $(b-c) \bullet r_q = p \bullet (m-g)$
Da qui, poiché $(b-c) \in A$, e anche $r_q \in A$, ne seguirebbe che il prodotto di due elementi di A , minori quindi di p e diversi da 0, è un multiplo di p, il che è assurdo, perché p è primo.
Quindi ogni elemento di A ha un suo **a**-simmetrico, diverso da quello associato a ciascuno degli altri elementi di A.
2*) - E' possibile che qualche elemento di A abbia come **a**-simmetrico sé stesso?
Supponendo possibile un tale evento, sia b un qualsiasi elemento di A tale che: $b^2 = mp + \mathbf{a}$ $(m \geq 0)$; $b^2 - \mathbf{a} = mp$
Quando la base <u>a è un quadrato perfetto</u> ($\mathbf{a} = d^2$; $d \in A$) , si avrà: $b^2 - d^2 = (b-d)(b+d) = mp$.
Essendo p primo , quest'ultima uguaglianza può essere vera solo se si verificano o una , o entrambe le uguaglianze: $b-d=0$; $b+d=p$
Come vedremo, in effetti entrambe le uguaglianze si verificano sempre, rispettivamente con $b=d$ e $b=p-d$, nella stessa base **a**.
Andiamo alla ricerca di tutti gli elementi di A che hanno come **a**-simmetrici sé stessi, anche nel caso in cui **a** non è un quadrato perfetto.
Sia D il sottoinsieme di A costituito dai suoi primi (p-1)/2 elementi: $D = \{1 , 2 , 3 , \ldots , (p-1)/2\}$
e sia E il sottoinsieme di A costituito dai rimanenti elementi: $E = \{(p-1) , (p-2) , (p-3) , \ldots , (p-(p-1)/2)\}$
Calcoliamo i quadrati di ciascun elemento di D e di ciascun elemento di E. Successivamente calcoliamo i residui di ciascun quadrato rispetto al modulo p e denominiamo ciascuno di essi con il termine "residuo quadratico" .
Sono residui quadratici evidenti quei termini di A che sono quadrati perfetti, gli altri residui quadratici di A risultano invece dal calcolo.

* Dimostriamo che 2 qualsiasi elementi distinti di D producono residui quadratici differenti.
Supponiamo per assurdo che b e c (b > c) , appartenenti a D , producono lo stesso residuo quadratico r : $b^2 = gp + r$; $c^2 = fp + r$
da qui, sottraendo membro a membro, si ha: $b^2 - c^2 = mp$ e quindi: $(b-c)(b+c) = mp$
ma questa uguaglianza è impossibile, perché (b-c) e (b+c) sono due elementi di A e p è primo. [Certamente: $b-c \neq 0$; $b+c < p$]

* Dimostriamo che gli elementi di E producono gli stessi residui quadratici prodotti dagli elementi di D.
Infatti se (p-s) è un elemento di E , si avrà: $(p-s)^2 = p^2 - 2ps + s^2 = p(p-2s) + s^2$, per cui vale la congruenza: $(p-s)^2 \equiv s^2 \pmod p$
Osservando che s è un elemento di D, la tesi è dimostrata.

Da quanto abbiamo appena dimostrato, ne segue che il 50% degli elementi di A sono residui quadratici di p e il restante 50% sono invece non-residui quadratici di p.
Possiamo allora suddividere gli elementi di A in due sottoinsiemi equipotenti e disgiunti: il sottoinsieme R dei residui quadratici di p e il sottoinsieme NR dei non-residui quadratici di p.
Fatta questa distinzione, possiamo scegliere la base **a** in due modi differenti.

- Scegliamo come base **a** un non-residuo quadratico.

In questo caso nessun elemento b di A è tale che $b^2 \equiv \mathbf{a} \pmod p$, per cui nessun elemento b di A ha come **a**-simmetrico sé stesso.
Quindi, se p è primo e <u>a è non-residuo</u> quadratico, i fattori del fattoriale (p-1)! si possono associare tutti in coppie **a**-simmetriche e ogni coppia è formata da due fattori distinti di (p-1)!

$$(p-1)! = 1 \bullet 2 \bullet 3 \bullet \ldots \bullet (p-1) = (1 \bullet a) \bullet (2 \bullet r2) \bullet (3 \bullet r3) \bullet \ldots \bullet ((p-1) \bullet (p-a))$$

a è sempre in coppia con 1 e (p-1) con (p-a)

Passiamo alle congruenze , ricordando il teorema di Wilson , cioè che $(p-1)! \equiv -1 \pmod p$

$$(p-1)! \equiv a \bullet a \bullet a \bullet \ldots \bullet a \equiv a^{(p-1)/2} \equiv -1 \pmod p$$

(*+) $$a^{(p-1)/2} + 1 = mp \quad (1 < a < p \text{ non-residuo})$$

- Scegliamo come base **a** un residuo quadratico.

Se p è primo e <u>a è residuo</u> quadratico, ci sono solo due elementi di A che hanno come **a**-simmetrici sé stessi.
Ciò perché il residuo quadratico **a** si ottiene da un solo elemento g di D e da un solo elemento (p-g) di E : $g^2 \equiv (p-g)^2 \equiv \mathbf{a} \pmod p$
Ma, **attenzione!** , non rientra nella scelta del residuo quadratico il valore **a**=1 che dà origine al teorema di Wilson.
Pur essendo 1 sempre residuo quadratico, qualunque sia il numero primo p , tuttavia, il risultato che si ottiene con questo valore è diverso da quello ottenuto con un qualsiasi altro residuo quadratico.
Quando $\mathbf{a} \neq 1$ è residuo , associando in coppie **a**-simmetriche i fattori di (p-1)! restano isolati soltanto i due fattori g e (p-g).

$$(p-1)! = 1 \bullet 2 \bullet 3 \bullet \ldots \bullet (p-1) = (1 \bullet a) \bullet (2 \bullet r2) \bullet (3 \bullet r3) \bullet \ldots \bullet [(p-1) \bullet (p-a)] \bullet [g \bullet (p-g)]$$

Dal teorema di Wilson sappiamo che $(p-1)! \equiv -1 \pmod p$, mentre $g \bullet (p-g) \equiv -g^2 \equiv -\mathbf{a} \pmod p$.
Pertanto sono valide queste congruenze:

$$(p-1)! \equiv a \bullet a \bullet a \bullet \ldots \bullet a \bullet (-a) \equiv -1 \pmod p \text{ , cioè: } (p-1)! \equiv -a^{(p-1)/2} \equiv -1 \pmod p \text{ Quindi:}$$

(*-) $$a^{(p-1)/2} - 1 = mp \quad (1 < a < p \text{ residuo})$$

Accomunando le due formule **(*+)** e **(*-)** , si avrà l'enunciato del teorema W-F .

Una applicazione delle due formule **(*+)** e **(*-)** *è nota come "Criterio di Eulero".*
Esse, utilizzate con un principio inverso a quello descritto sopra, consentono di stabilire quali sono i residui quadratici relativi a un dato numero primo p.
Sia: p primo e a coprimo con p,

- *se* $a^{(p-1)/2} \equiv 1 \pmod p$ ne segue che a è residuo quadratico
- *se* $a^{(p-1)/2} \equiv -1 \pmod p$ ne segue che a è non-residuo quadratico

Perché la condizione del teorema W-F è solo necessaria e non sufficiente ?

<u>Se p non è primo</u>, i fattori di (p-1)! non si possono raggruppare in coppie **a**-simmetriche, per cui: $(p-1)! \not\equiv \pm a^{(p-1)/2}$ $(1 < a < p)$
Dobbiamo ricordarci che in questo caso vale la congruenza $(p-1)! \equiv 0 \pmod p$, perché $(p-1)! = mp$
Ciò che inficia la condizione sufficiente del teorema W-F è il valore delle congruenze, modulo p, delle potenze $\pm a^{(p-1)/2}$; queste potrebbe valere +1 o -1 , nonostante che non rappresentino il fattoriale (p-1)! .
In effetti le prove pratiche e alcuni teoremi confermano che questa possibilità è reale e finora l'unico modo per stabilire la primalità di un intero p, con una condizione che sia anche sufficiente, oltre che necessaria, rimane quello di calcolare l'intero fattoriale (p-1)! .

Piccolo Teorema di Fermat

Se p è un numero primo e la base a è un intero coprimo con p, necessariamente deve valere l'uguaglianza:

$$a^{p-1} - 1 = mp$$

Dimostrazione.

Il "Piccolo teorema di Fermat" si può dedurre dal "Teorema W-F " in modo molto semplice, basta seguire alcuni passaggi.

$$a^{(p-1)/2} \pm 1 = mp \Rightarrow a^{(p-1)/2} = mp \pm 1 \Rightarrow (a^{(p-1)/2})^2 = (mp \pm 1)^2 \Rightarrow a^{(p-1)} = m^2p^2 \pm 2mp+1 \Rightarrow a^{(p-1)} - 1 = (mp \pm 2)mp$$

Dato che m rappresenta un generico numero intero, da quest'ultima uguaglianza ne segue la tesi.

Purtroppo questo teorema offre una condizione necessaria, ma non sufficiente.

Infatti, come ha dimostrato il matematico palermitano Michele Cipolla (1880-1947), l'uguaglianza $a^{(p-1)} -1= mp$ è valida anche per infiniti numeri composti, detti pseudoprimi nella base a.

Il motivo per cui questa uguaglianza si verifica, oltre che per tutti i numeri primi, anche per alcuni numeri composti, sarà il tema di un'altra relazione.

Il grande Pierre De Fermat (1601-1665) è famoso anche per avere dichiarato di non aveva carta a sufficienza per dimostrare alcuni dei suoi teoremi.

Anche nel caso di questo teorema, designato col termine "piccolo", Fermat ne ha comunicato l'enunciato senza la dimostrazione.

Ne diede una dimostrazione lo svizzero Eulero nel 1736, a distanza di circa un secolo.

Più travagliata, con risvolti romanzeschi, è la storia di un altro teorema, noto come "L'ultimo teorema di Fermat", che ha impegnato per diversi secoli i ricercatori intenzionati a trovarne una dimostrazione. Infine è riuscito nell'impresa l'inglese Andrew Wiles nel 1993.

Qual è la dimostrazione del "piccolo teorema di Fermat" a cui è pervenuto il matematico francese e in che modo sia arrivato ad esso non ci è dato sapere. E' possibile che egli abbia dedotto il tutto dalle proprietà descritte in quello che ho denominato "Teorema W-F" .

Sta di fatto che i due teoremi hanno le stesse problematiche nelle applicazioni: ci offrono una condizione necessaria, ma non sufficiente.

Cosicché, quando la condizione necessaria di questi teoremi non si verifica, si è certi che il numero p in esame è composto; quando invece la condizione necessaria è verificata non si è certi che p sia primo.

Per questo motivo, il test di primalità basato sul teorema di Fermat viene ripetuto, cambiando diverse volte la base **a**, fino ad avere un'alta probabilità che p sia primo.

Un altro indizio che Pierre De Fermat sia approdato al suo teorema tramite le proprietà del " teorema W-F " si ha nel momento in cui generalizziamo questo a tutti i numeri dispari, cioè nel momento in cui passiamo a un altro famoso teorema, dimostrato da Eulero e noto come "teorema di Eulero-Fermat"

Infatti lo studio che ci impegna a determinare le proprietà sintetizzate da quest'altro teorema ci fa approdare inevitabilmente al noto "metodo di fattorizzazione di Fermat".

Chi volesse saperne di più, può continuare con le mie relazione: " Teorema di Eulero " ; " L'insieme ϕ "