

TEOREMA ALGEBRICO SUI NUMERI PRIMI

$$\text{Gruppo abeliano } P = \{\pm 6n \pm 1\}$$

=

Con le forme aritmetiche sui numeri primi, si dimostra che questi, i loro prodotti e le loro potenze (tranne, in tutti e tre i casi, per il 2 e il 3), sono della forma generale:

$$P = 6n \pm 1$$

$$P = p \bullet q = (6n \pm 1) (6m \pm 1)$$

$$P = p^k = (6n \pm 1)^k$$

Con questo lavoro dimostreremo che tutti i numeri della forma

$$\pm 6 \bullet n \pm 1$$

con n da 0 a ∞ , e quindi anche $\pm 6 \bullet 0 \pm 1 = \pm 1$ per $n = 0$, sono tutti elementi di un insieme numerico P , che è anche gruppo abeliano (cioè commutativo) munito dell'operatore binario "moltiplicazione" o "prodotto", e di operazione inversa (divisione) limitata però soltanto alla fattorizzazione.

DIMOSTRAZIONE

Qualsiasi prodotto tra due o più elementi p, q, r , ecc. appartenente all'insieme P , e quindi anche qualsiasi k -esima potenza di un qualsiasi elemento di P , è ancora un elemento di P .

$$p = (\pm 6n \pm 1) \in P$$

$$p \bullet q = (\pm 6n \pm 1) (6m \pm 1) \in P$$

$$p^k = (\pm 6n \pm 1) \in P$$

L'operazione "prodotti" è commutativa

$$p \bullet q = q \bullet p = r \in P$$

e anche associativa

$$p \bullet q \bullet r = (p \bullet q) \bullet r = p \bullet (q \bullet r) = s \in P$$

Tale prodotto non è però distributivo, poiché il gruppo non è munito di addizione, essendo privo dell'elemento neutro 0.

L'operazione inversa è però limitata alla sola fattorizzazione di qualsiasi prodotto o potenza di elementi, in fattori primi, e quindi alla condizione

$$\frac{r}{q} = p \text{ solo e solo se } p \bullet q = r \in P$$

solo se p, q ed r sono elementi di P , ed r è cioè divisibile solo per p e q ; questi sono divisibili solo per 1 e per se stessi (fattori impropri), e quindi sono numeri primi.

Anche 1 e -1 sono elementi di P, quando $n = 0$, come si è visto;¹ per cui il gruppo P è fornito dell'elemento neutro 1, con il quale

$$p \bullet 1 = p$$

$$q \bullet 1 = q$$

$$r \bullet 1 = r,$$

$$\text{e } \frac{p}{p} = 1, \frac{q}{q} = 1, \frac{r}{r} = 1 \text{ ecc.}$$

in quanto 1 associa a p, nell'operazione prodotto, lo stesso numero p, come avviene nel gruppo più grande degli interi relativi Z

$$n \bullet 1 = n, \quad \frac{n}{n} = 1$$

Nei termini del teorema delle forme aritmetiche, abbiamo, più dettagliatamente

$$r = p \bullet q = (\pm 6n \pm 1) (\pm 6m \pm 1);$$

da cui

$$p = \frac{r}{q} = \frac{(\pm 6n \pm 1) (\pm 6m \pm 1)}{(\pm 6m \pm 1)} = (\pm 6n \pm 1) = p$$

oppure, viceversa,

$$q = \frac{r}{p} = (\pm 6m \pm 1)$$

da ciò deriva un algoritmo per una fattorizzazione lineare e semplificata

¹ Nota: anche 1 e -1 sono numeri primi secondo la definizione: Sulle "Spalle dei giganti" ci sono i motivi di convenienza per escluderli ed 1 è l'unico elemento neutro per il gruppo P. L'elemento -1 comporterebbe un cambio di segno al numero primo preso di esempio.

$$\frac{r}{6n \pm 1} \text{ con } n \text{ variabile da } 1 \text{ a } \frac{\sqrt{r}}{6} + 1$$

Per esempio $p = 35$, $q = 11$, fanno parte di P , e così il loro prodotto, $r = 35 \cdot 11 = 385$, ma non le divisioni tra di loro

$$\frac{35}{11} = 3,18 \text{ e } \frac{11}{35} = 0,31,$$

che non fanno parte di P poiché non sono della forma $\pm 6n \pm 1$ come tutti gli altri elementi di P , definiti esclusivamente da tale forma dal Teorema n° 1.

Lo sono invece i rapporti

$$\frac{r}{p} = \frac{385}{11} = 35, \text{ ed } \frac{r}{q} = \frac{385}{35} = 11,$$

perché, per definizione, $r \in P$ solo se $r = p \cdot q$ con $r, p \text{ e } q \in P$.

Lo stesso vale per le k -esime potenze di un qualsiasi elemento $p \in P$.

Per esempio

p^k ; $p = 5$; $k = 3$ (k non necessariamente elemento di P , può essere un numero intero positivo qualsiasi).

$$5^3 = 5 \cdot 5 \cdot 5 = 125$$

$125 \in P$ in quanto è della forma $\pm 6n \pm 1$;

infatti

$$\frac{125+1}{6} = \frac{126}{6} = 21 = n$$

L'operazione inversa, in questo caso, oltre alla normale fattorizzazione

$$125 \Big| 5 = 5 \cdot 5 \cdot 5 = 5^3$$

$$\begin{array}{r|l} 25 & 5 \\ 5 & 5 \\ 1 & \end{array}$$

è allo stesso tempo anche l'estrazione della radice k di r , e cioè poiché

$$p^k = r; \quad p = \sqrt[k]{r}.$$

Per p negativo, e quindi $(-p)^k$, k deve essere pari affinché r sia positivo; se k è dispari avremo $-r$, e $\sqrt[k]{-r}$ sarà un numero complesso, non $\in P$ che comporterebbe una addizione $(a + bi)$, e questa non è operazione binaria in P .

Per qualsiasi p positivo $\in P$, $p^k \in P$ quale che sia k , da 0 a ∞ .

Per $k = 0$, $p^0 = 1 \in P$, poiché $1 = 6 \cdot 0 + 1 = 1$.

Vediamo ora gli aspetti geometrici del gruppo P .

Con le forme aritmetiche, abbiamo visto come tutti i numeri primi, loro prodotti e potenze sono della forma generale (già scoperta da Eulero)

$$6n \pm 1,$$

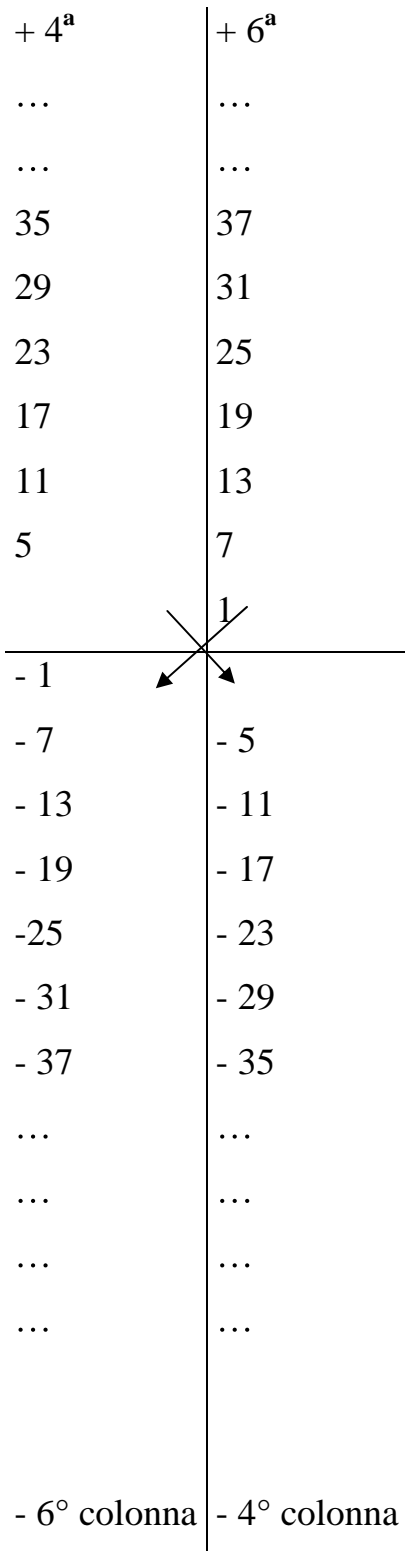
tranne che per il 2 e per il 3, che sono capofila della 1° e della 2° colonna rispettivamente (mentre i capofila della 3° e della 5° colonna sono 4 e 6, composti; e i capofila della 4° e della 6° colonna sono 5 e 7, primi, della forma $6n \pm 1$;

$$5 = 6 \cdot 1 - 1; \quad 7 = 6 \cdot 1 + 1.$$

I numeri della 4° e 6° colonna, quelle che contengono tutti gli elementi del gruppo P, sono positivi; ma se togliamo progressivamente $-6n'$ a partire da uno qualsiasi di essi, quando n' diventa più grande di n , si passa ai numeri negativi, poiché anche $6n'$ è più grande di $6n$; infatti, per $n' > n$, $6n \pm 1 - 6n' = -6m \pm 1$.

A questo punto, superato lo 0, le colonne 4° e 6° si invertono di posto, e anche di segno algebrico. La 6° colonna $(6n + 1)$ positiva, si pone sotto la 4° colonna $(6n - 1)$, ma con segni $+$ e $-$ invertiti. Pertanto le due colonne possono essere ora considerate una sola, della forma $\pm 6n \pm 1$, divisa in due semicolonne, una positiva $(6n + 1)$ ed una negativa $(6n - 1)$, vedi fig. 1.

FIGURA 1



Per es. $13 - 18 = -5$
 $(6 \bullet 2 + 1) - (6 \bullet 3) = -(6 \bullet 1 - 1)$
 $n \qquad m \qquad \downarrow$
 $m - n = 3 - 2 = 1$

$17 - 36 = -19$
 $(6 \bullet 3 - 1) - (6 \bullet 6) = -(6 \bullet 3 + 1)$
 $m \qquad n \qquad \downarrow$
 $m - n = 6 - 3 = 3$

In generale $(6n \pm 1) - 6m = -(6 \bullet m - n \pm 1)$ se $m > n$; e $(6n \pm 1) \pm 6m = \pm (6m \pm n) \pm 1$ in ogni caso, sia $m > n$ che $m < n$

$+17 + 36 = 53$
 $(6n - 1) + (6m) = (6 \bullet 9 - 1) = 54$
 $(6 \bullet 3 - 1) + (6 \bullet 6) = [6(3+9) - 1] = 54$

e così via.

Con tale capovolgimento della 4° e delle 6° colonna del Teorema n° 1, e loro inversione dopo aver oltrepassato lo zero, abbiamo ottenuto i due nuovi elementi

$+1$ e -1 ; che sono risultato della fattorizzazione impropria $\frac{p}{p} = 1$, $\frac{-p}{p} = -1$; ma

sono anche e soprattutto della forma $\pm 6 \bullet 0 \pm 1 = \pm 1$, e quindi, come tali, da considerare elementi di P, che quindi contiene tutti i numeri della forma:

$$\pm 6n \pm 1$$

e quindi $+1$ e -1 compresi, oltre che tutti i primi, prodotti tra primi e potenze k di primi con k qualsiasi intero positivo, e $-k$ negativo solo se pari, poiché

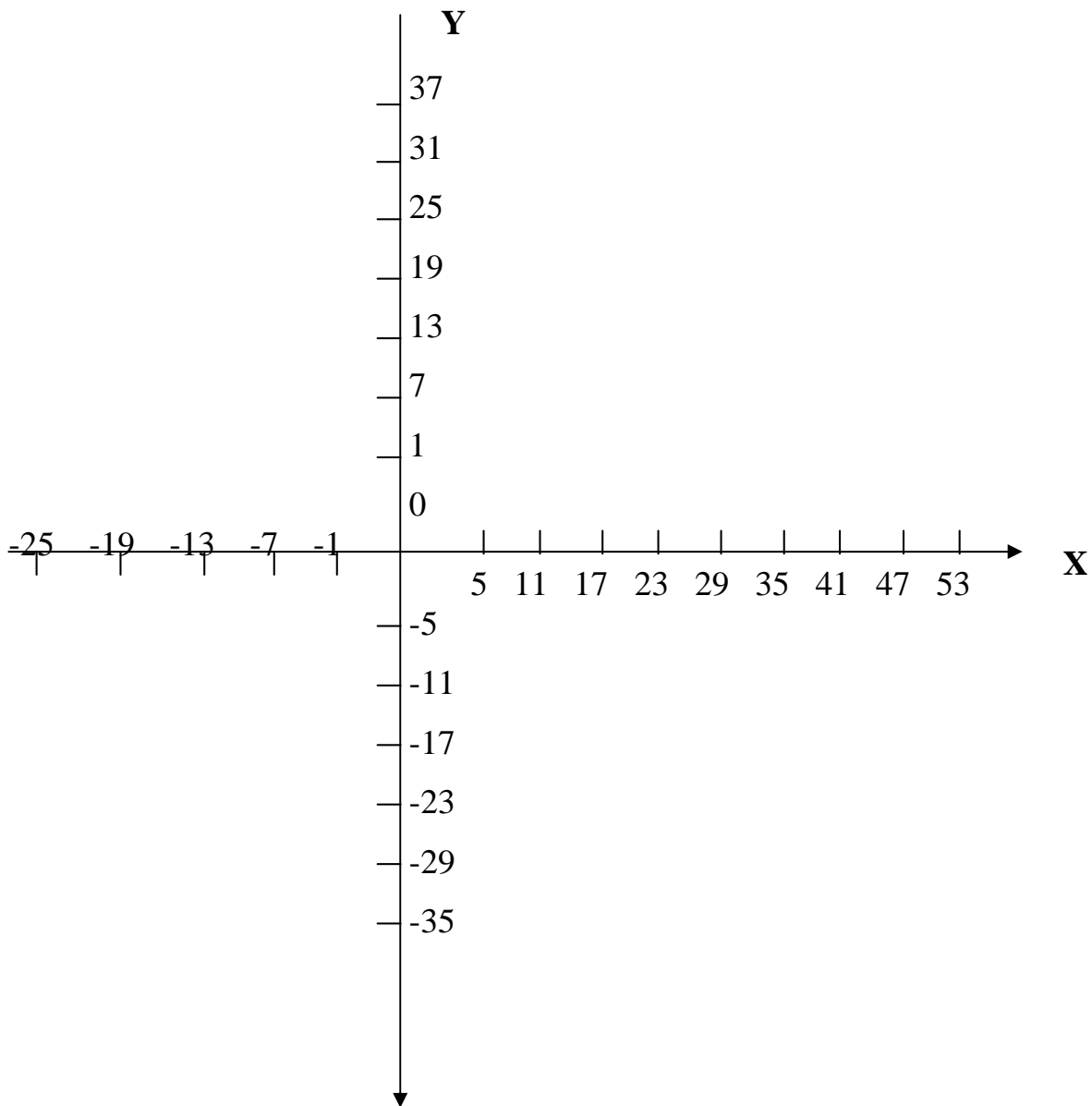
Avremo, indipendentemente dai segni algebrici, tutti i prodotti e potenze della forma $p \bullet q = r \in P$. (r appartiene a P)

E' ovvio che tutti i numeri primi, come valore assoluto, e cioè indipendentemente dai segni $+$ e $-$, sulla prima riga e sulla prima colonna, quale prodotto di sè stessi per 1 (tranne sempre il 2 e il 3, non $\in P$), e i loro quadrati sulla diagonale che divide in due parti simmetriche la tavola di moltiplicazione. Tutti i prodotti r , invece, stanno sulle altre righe e colonne diverse dalle prime, e precisamente all'incrocio di quelle che iniziano con i loro fattori p e q . La fattorizzazione, così, significa trovare i due fattori primi di r all'inizio della p -ma riga e della q -esima colonna, all'incrocio delle quali ci sta r . Per es. $r = 221 = 17 \bullet 13$, si trova all'incrocio tra la 17° riga e dalla 13° colonna.

Solo i numeri primi si trovano sulla prima riga e sulla prima colonna, quelle che cominciano con 1, poiché $\frac{p}{p} = 1$; $\frac{p}{1} = p$ sono le loro uniche fattorizzazioni possibili, cioè quelle improprie, per se stessi e per 1.

Vediamo ora l'aspetto geometrico cartesiano vero e proprio, ponendo la serie di elementi dalla forma $\pm 6n \pm 1$ sui due assi cartesiani x e y , fig. 3.

FIGURA 3

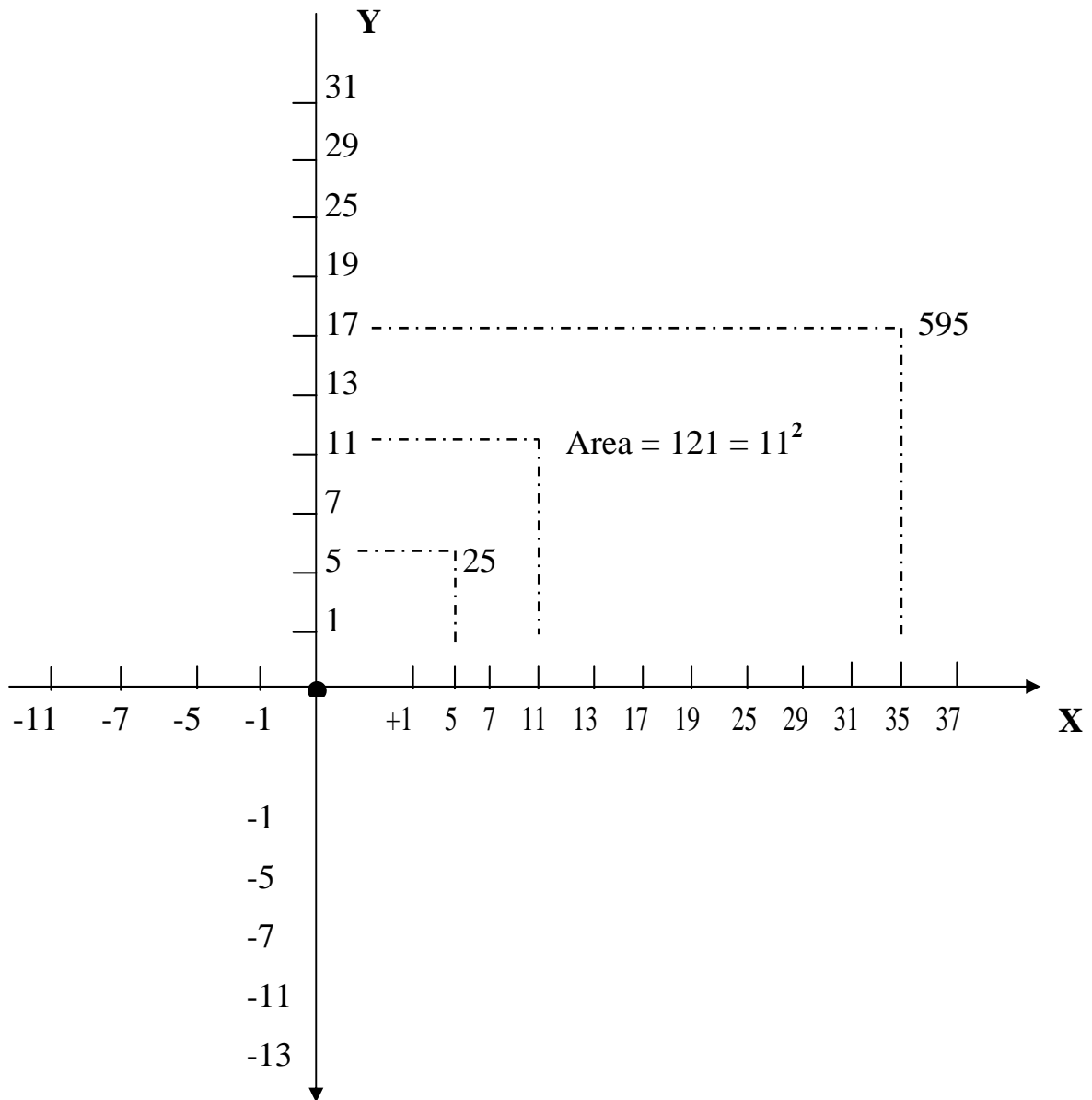


0 = punto di inversione del segno algebrico, vedi fig. 1.

L'aspetto geometrico ora diventa visibile nel piano: tutti i prodotti della tavola di moltiplicazione sono rappresentati come aree, dall'incrocio dei punti del piano x , y , in tutti e quattro i quadranti, a seconda dei segni algebrici $-$ e $+$. Tutti i primi, invece, giacciono sugli assi e nelle rette $\pm 1, x$; $\pm 1, y$; parallele a x e a y . Mettendo

però tutti i possibili numeri $6n \pm 1$ su ognuno degli assi, il piano diventa più reale e preciso, fig. 4, e quindi più studiabile geometricamente, in relazione ai numeri primi

FIGURA 4



In tale piano, i primi giacciono soltanto sugli assi, i prodotti tra primi diversi sono aree di rettangoli o quadrati, anche se il composto come numero è effettivamente

su un asse e non nel piano.² Nel piano ci sono le aree. In questo piano, tutti i primi in P giacciono sugli assi, quindi a distanza 0 da essi (con qualche relazione con gli zeri della funzione zeta di Riemann?).³

A questo punto disponiamo di un gruppo abeliano P munito di prodotto, di un unico elemento neutro 1 e un'operazione inversa (divisione) limitata alla sola fattorizzazione. Gruppo che dispone di proprietà commutativa e associativa ma non distributiva; poiché ricordiamo che il gruppo non è munito di operazione "addizione". Per quanto riguarda quest'ultima, infatti, qualsiasi elemento di P differisce da un altro di un numero della forma $6m$, che non appartiene a P , come abbiamo già visto dopo la fig. 1, sulla inversione di segno della 4° e della 6° colonna.

Poiché ad ogni numero primo e ad ogni composto è associato, dalla forma generale $\pm 6n \pm 1$, un numero intero n qualsiasi, il gruppo P è isomorfo (= stessa forma) ed

² E' sufficiente un solo asse reale per avere sopra tutti i numeri interi, razionali e reali. E' stato il problema di Cantor e di tanti altri. E' difficile uscire da una retta reale. Per un composto di 2 numeri avremmo bisogno di due rette reali e i punti, numeri primi o composti, stanno sempre su una retta (ad esempio $21=3*7$ ha sia il 3 che il 7 su entrambe le rette x e y : solo che ci piace vedere l'area come misura di una base su ascissa x e di una altezza su ordinata y). Ovviamente per composti a n primi si esce dalla geometria a 2 dimensioni (piano) o 3 dimensioni (volume) per arrivare agli ipercubi. Una cosa su cui riflettere: i primi e i composti ci confinano solo nella geometria euclidea? In realtà no.

³ Per la teoria attuale su Riemann gli zeri non banali o stanno sull'asse $\text{Re}(s)=1/2$ o sono una coppia simmetrica rispetto a $1/2$ ovvero possono essere a ventaglio in una zona (teorema della regione libera di zeri non banali). Inoltre sono infiniti (vedi Teorema di Weierstrass)

equipotente (ha lo stesso numero di elementi, e cioè infiniti) al gruppo degli interi relativi Z , e quindi ne possiede le stesse capacità algebriche e geometriche.

Infine P isomorfo a Z può essere anche considerato un piano/insieme di numeri complessi particolari, poiché $-1 = +i^2$ e $+1 = i^4$, ogni elemento di P si potrebbe scrivere anche con la forma dei numeri complessi $a + bi$, ma con $a = 6n$, e $bi = i^2$ o i^4

$$i^4 \bullet 6n + i^2 = 6n - 1$$

$$i^4 \bullet 6n + i^4 = 6n + 1$$

$$i^2 \bullet 6n + i^2 = -6n - 1$$

$$i^2 \bullet 6n + i^4 = -6n - 1$$

da cui la forma generale $\pm 6n \pm 1 = P$, e quindi tutte le quattro possibilità ricadono in P e quindi in Z se si considera il solo elemento n . Il piano complesso vero e proprio è stato già ipotizzato per i numeri primi, in relazione anche all'ipotesi di Riemann.

Il aottogruppo $P = \pm 6n \pm i^2$, $P = \pm 6n \pm i^4$, con i quattro valori possibili di cui sopra, e cioè i possibili elementi $\pm 6n \pm 1$ del gruppo P , potrebbe essere, in futuro, di aiuto nella dimostrazione della suddetta ipotesi?⁴. oltre che per questa considerazione sui complessi, anche per la giacenza di tutti i primi sugli assi, forse collegata all'ipotesi che tutti gli zeri della funzione zeta giacciono su una linea

⁴ L'autore è oltremodo ottimista. Con tale osservazione si mostra un legame degli interi e dei reali al campo complesso che era noto. L'utilizzo semplice solo di numeri complessi rappresentativi di zeri non è così immediata e sicuramente il valore di uno zero non banale ha sia parte reale che parte complessa valori reali e non interi.

critica. Poiché gli assi sono una retta e anche la linea critica è una retta, i primi giacciono sugli assi e i relativi zeri giacciono sulla retta critica, un collegamento diretto dovrà pure esserci; sono due affermazioni equivalenti, molto simili, e dimostrarne una equivale a dimostrare l'altra.⁵

Gli strumenti matematici usati finora nei vari tentativi di dimostrazione (funzioni zeta estese, matrici casuali, numeri complessi, operatori hamiltoniani, analisi di Fourier, ecc.), potrebbero essere utili in futuro a scoprire la connessione sospettata tra le due affermazioni.

Ad essi potrebbero essere aggiunti ora anche il teorema delle forme aritmetiche $6n \pm 1$ e il conseguente nostro gruppo abeliano P descritto in questo lavoro.

GRUPPO ERATOSTENE

⁵ Anche qui bisognerebbe ammettere che Eulero ha mostrato un legame tra primi e zeta; ma per gli zeri della zeta alcuni sono sull'asse reale negativo (a valori pari negativi $-2k$ con $k=1,2,3,4\dots$) detti zeri banali e altri sulla retta critica. In poche parole ce ne sono due di rette. Qua possono nascere altre domande ... Ancora oggi non è chiaramente dimostrato un legame come dice l'autore in termini di rette. Tra l'altro l'addensamento degli zeri avviene all'infinito e i primi si diradano all'infinito.

Fattorizzazione anti RSA

Nel piano P dei numeri $\pm 6n \pm 1$, ogni composto $p \cdot q$ vuol dire

$$(1) \quad r = p \cdot q = (6n \pm 1)(6m \pm 1)$$

che, sviluppato, diventa

$$(2) \quad 36 \cdot m \cdot n \pm 6m \pm 6n \pm 1 = r = p \cdot q,$$

e che, nel caso di un quadrato $p = q$ e $m = n$,

diventa

$$(3) \quad 36m \pm 12m \pm 1.$$

La (2) si potrebbe utilizzare come metodo di fattorizzazione, enormemente semplificata (e quindi utile in crittografia) tramite un algoritmo dicotomico sulle ramificazioni possibili della (2), una volta trovato un numero base

$b \simeq \frac{r}{36}$, e i suoi fattori m ed n ; se questo numero b è decimale, si fattorizzano i

due interi immediatamente inferiori e superiori al numero decimale.

Algoritmo che si potrebbe usare anche come test di primalità se non vengono trovati fattori primi, il che significa che r è primo.

Per esempio $r = p \cdot q = 187 = 11 \cdot 17$

$b \simeq \frac{r}{36} = \frac{187}{36} = 5,19$

5 intero inferiore a "b"

6 intero superiore a "b"

Si fattorizzano i due interi contigui a b;

e cioè $5 = 5 = \text{primo}$

$$6 = \underline{2} \cdot \underline{3} = m \cdot n$$

Algoritmo applicato ai singoli primi, con i fattori trovati 2 e 3

a) $6 \cdot m \pm 1 = \underline{6 \cdot 2 \pm 1} = \begin{matrix} \swarrow \boxed{11} \\ \searrow 13 \end{matrix}$

poiché $\frac{187}{11} = 17 = 19$

b) $6n \pm 1 = \underline{6 \cdot 3 \pm 1} = \begin{matrix} \swarrow \boxed{17} \\ \searrow 19 \end{matrix} = q$

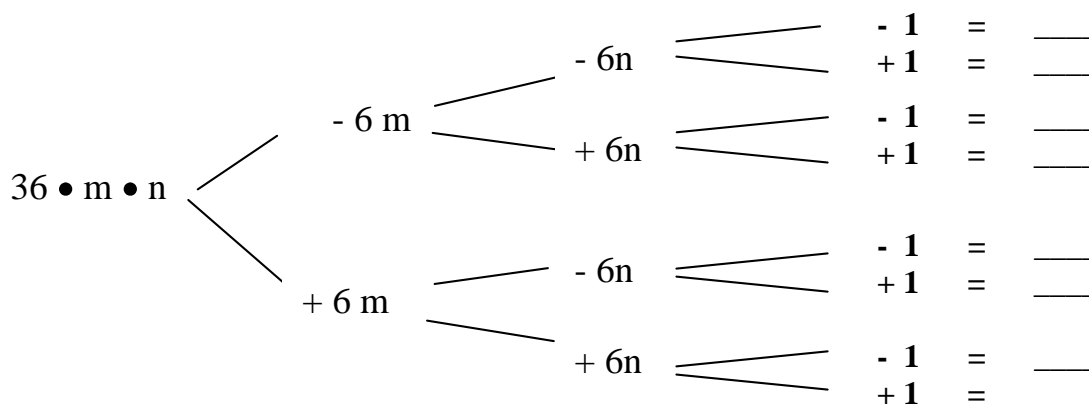
poiché $\frac{187}{17} = 11 = p.$

I percorsi esatti, tra i due possibili in entrambi i casi (fattori 2 e 3) sono quelli tratteggiati, che portano subito ai numeri primi p e q, senza la fattorizzazione classica (divisione di r per tutti i primi fino a trovare il più piccolo tra p e q).

Si possono anche costruire le possibili ramificazioni della (2) per giungere a

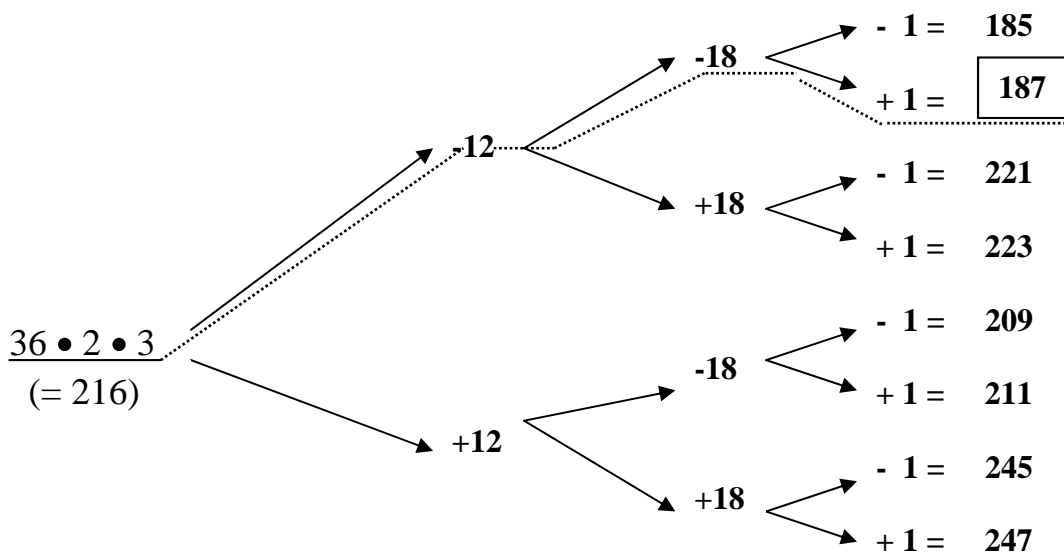
r = 187: _____

Ramificazioni teoriche



Alla fine di una delle 8 ramificazioni possibili, ci sarà r

Esempi per r = 187 = 11 • 17



Percorso esatto = il percorso tratteggiato.

Nel caso di un quadrato, m = n.

Per esempio r = p • q = 169 = 13 • 13 = 13²

$$\frac{169}{36} \simeq 4,6 \begin{cases} 4 = \underline{2} \cdot 2 = m \cdot \\ 5 = \text{primo} \end{cases}$$

in tal caso si applica la (3)

$$\underline{36 \cdot 2 \cdot 2 + 12 \cdot 2 \pm 1} \begin{cases} \boxed{169} \\ 167 \end{cases}$$

Con la ricerca del numero primo, abbiamo

$$\underline{6 \cdot 2 \pm 1} \begin{cases} 11 \\ \boxed{13} \end{cases}$$

13 è il numero cercato, poiché $\frac{169}{13} = 13 = p = q$.

Quando i fattori di $b \simeq \frac{r}{36}$ sono più di due, bisogna provarli anche a gruppi, di due o di tre, oltre che singolarmente, con il loro prodotto o la loro somma.

Per esempio $37 \cdot 37 = 1369$

$$b \simeq \frac{1369}{36} = 38,02 \begin{cases} 39 = 13 \cdot \underline{3} \\ 38 = 2 \cdot 19 \end{cases}$$

$$6 \cdot \underline{2} \cdot \underline{3} = \underline{6 \cdot 6 \pm 1} \begin{cases} \boxed{35} \\ \boxed{37} \end{cases}$$

pur essendo 1369 il quadrato di 37, m ed n a volte non sono uguali, come in questo caso.

Un caso più complesso è $131 \bullet 131 = 17161$

$$b \simeq \frac{17161}{36} = 476,6$$

\swarrow
 \searrow

$476 = \underline{2}^2 \bullet 7 \bullet 17$
 $477 = \underline{3}^2 \bullet 53$

$$6 \bullet (17 + 3 + 2) \pm 1$$

\swarrow
 \searrow

131

133

$$6 \bullet 22 - 1 = 131$$

In questo caso m è $22 = 17 + 3 + 2$, con questi ultimi presi una sola volta.

Per cui, a volte, la ricerca di $m \bullet n$ è un po' laboriosa, soprattutto quando i fattori interi di b interi sono tanti;

Ma, per numeri r molto grandi, ne varrebbe la pena, rispetto alla fattorizzazione tradizionale, che comporterebbe una serie di calcoli molto più lunghi.

Sui numeri complessi

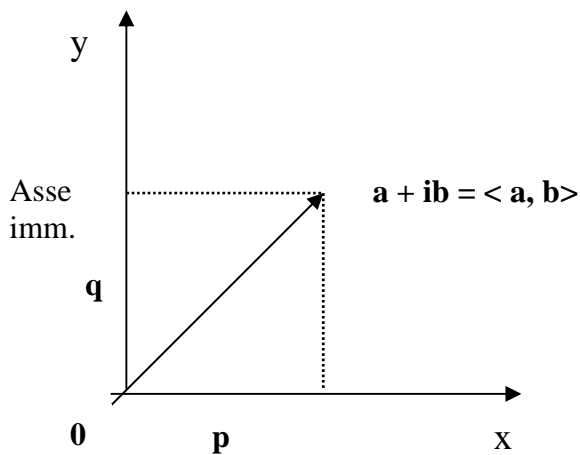
Volendo considerare i numeri primi p e q come numeri complessi con parte immaginaria nulla, essi si potrebbero scrivere come segue:

$$p = p + 0i$$

$$q = q + 0i$$

e il loro prodotto $p \cdot q = (p + 0i)(q + 0i)$; secondo la regola classica $(a + bi)(c + id) = ac - bd + i(bc + ad)$ avremo: $pq - 00 + i0q - i0p = p \cdot q - 0 + 0 - 0 = p \cdot q$ che ricade nell'asse x di P , con parte immaginaria nulla ($0i$).

Un numero complesso può essere raffigurato, com'è noto, come un punto su un piano cartesiano, chiamato piano di Argand-Gauss.

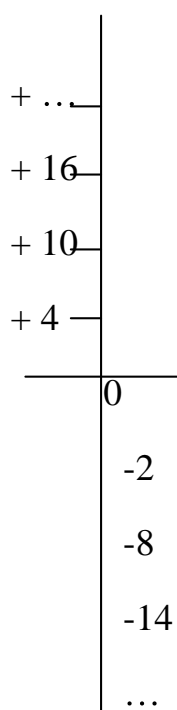


Inversione delle altre colonne numeriche del Teorema n° 1

creazione di due nuovi gruppi per 2° e 5° colonna che si autoinvertono.

Non solo la 4° e la 6° colonna si invertono l'una nell'altra come segno algebrico e come valori assoluti dei numeri (da $6n + 1$ a $6n - 1$ e viceversa), creando il gruppo P munito di prodotto ed elemento neutro 1; ma anche la 1° colonna si inverte con la 3° (e viceversa) ma, a differenza con la 4° e la 6°, non costituiscono gruppo ne per la moltiplicazione ne per l'addizione, poiché, nel punto di inversione, non comprendono ne il numero 1 ne il numero 0, necessari come elementi neutri in qualsiasi gruppo (tali che $a - 1 = a$; $a + 0 = a$).

GRAFICO



Da +4, sottraendo 6, abbiamo -2, quindi ne l'1 né lo 0 fanno parte della serie numerica che comprende la 1° e la 3° colonna

Così pure la 2° colonna che però rimane invariata se si inverte (autoinvertita), a parte il segno algebrico dei loro numeri, e non contiene i numeri 1 e 0, poiché

$$+4 - 6 = -2, \text{ e } -2 + 6 = +4$$

(per la regola che ogni elemento differisce dal successivo di 6, e di $6n$ da qualsiasi altro).

2° colonna	+ 27		+ 24
	+ 21		+ 18
	+ 15		+ 12
	+ 9		+ 6
	+ 3		0
	- 3		- 6
	- 9		- 12
	- 15		- 18
	- 21		- 24
	- 27		...

Mentre la 5° colonna (di forma $6 \cdot n$), anche questa auto invertente, contiene l'elemento 0, e quindi costituisce gruppo rispetto all'addizione.

Anche questo gruppo è commutativo:

$$6n + 6m = 6m + 6n$$

associativo:

$$6m + 6n + 6r = (6m + 6n) + 6r = 6m + (6n + 6r)$$

ma non distributivo perché il gruppo non è munito del prodotto come operazione binaria, nè dell'elemento 1 come suo elemento neutro, sebbene il prodotto tra due elementi qualsiasi faccia parte del gruppo.

Riepilogando:

- a) La 1° e 3° colonna si invertono tra loro, ma non costituiscono gruppo;
- b) La 2° colonna si auto inverte ma non costituisce gruppo;
- c) La 5° colonna si auto inverte e costituisce gruppo rispetto all'addizione, perché contiene il numero 0, elemento neutro rispetto a questa operazione;
- d) La 4° e 6° colonna si invertono l'una nell'altra e costituiscono gruppo (il gruppo P di questo lavoro) rispetto alla moltiplicazione perché contengono l'elemento neutro 1, e contiene tutti i numeri primi, i prodotti tra loro e le loro k-esima potenze, tranne che, in tutti i casi, per il 2 e per il 3; e come operazione inversa, solo la fattorizzazione dei suoi composti in primi.

Tutti i numeri di tutte le colonne, uniti insieme, infine, costituiscono l'insieme di tutti i numeri interi relativi, Z che costituisce gruppo abeliano rispetto alla addizione e alla moltiplicazione, contenendo anche i rispettivi numeri neutri 0 e 1, e con operazione inversa la normale divisione aritmetica (compresa la fattorizzazione di tutti i composti nei loro fattori primi), ora compresi anche il 2 e il 3, i due soli numeri primi anomali perché non sono della forma generale $6n \pm 1$.

NOTA FINALE

Le 6 colonne del teorema delle forme aritmetiche, oltre che in forma compatta, che ricordiamo

	1°	2°	3°	4°	5°	6°
1	<u>2</u>	<u>3</u>	4	<u>5</u>	6	<u>7</u>
	8	9	10	<u>11</u>	12	<u>13</u>
	14	15	16	<u>17</u>	18	<u>19</u>
	20	21	22	<u>23</u>	24	25

(solo il numero 1 è fuori da queste 6 colonne), e che possiedono le proprietà algebriche descritte, si possono scrivere in modo diverso, più diradato a scala, e cioè in modo tale che alla fine possono essere incastrate l'una nell'altra, e formare tutta la serie dei numeri naturali, disposti in una sola colonna verticale.

<u>1°</u>	<u>2°</u>	<u>3°</u>	<u>4°</u>	<u>5°</u>	<u>6°</u>
1					
2					
	3				
		4			
			5		
				6	
					7
8					

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

che contratte in senso verticale danno le 6° colonne del teorema delle forme aritmetiche, mentre contratte in senso orizzontale, danno la serie completa dei numeri interi N ,

1

2

3

4
5
6
7
8
9
10
11
12
13
...

sui quali si sono costruiti tutti i gruppi algebrici noti, e anche tutti i calcoli possibili e immaginabili; e naturalmente anche tutti i teoremi e i calcoli sui numeri primi (crivello di Eratostene, fattorizzazione, ecc.); mentre, con il teorema delle forme aritmetiche e i conseguenti, il crivello di Eratostene viene limitato solo alla 4° e alla 6° colonna, (essendo tutte le altre colonne fatte tutte di numeri composti, eccetto il 2 e il 3, primi anomali), e la fattorizzazione viene semplificata dall'algorithm:

$(p = \frac{r}{6n \pm 1}$ con n variabile da 1 a $\frac{\sqrt{r}}{6} + 1$), e considerato come la sola possibile

operazione inversa ma limitata ai soli composti per il gruppo P.

(Nel gruppo N l'operazione inversa completa è la normale divisione, che è possibile per tutti i numeri; mentre la fattorizzazione riguarda solo di numeri primi;

dopo e tranne il 2 e il 3, tutti gli altri numeri primi $\in P$, come pure, ricordiamo, tutti i loro prodotti e potenze).

GRUPPO ERATOSTENE

Caltanissetta, Giugno 2009

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.