I NUMERI PRIMI DI GAUSS

Carlo Federico Gauss nel 1828

https://upload.wikimedia.org/wikipedia/commons/3/33/Bendixen_-_Carl_Friedrich_Gau%C3%9F%2C_1828.jpg
By Siegfried Detlev Bendixen (published in "Astronomische Nachrichten" 1828) [Public domain], via Wikimedia Commons

Ci sono altri numeri primi oltre a quelli che conosciamo?

Naturalmente, il concetto di numero primo a prima vista si applica solo agli interi reali. Appena entriamo nel campo dei numeri razionali, sembra che il concetto svanisca, perché una divisione di due numeri interi è sempre possibile, senza dare un resto, che, nel campo dei numeri razionali, non sappiamo neppure cosa sia. Non parliamo poi dei numeri irrazionali, trascendenti o reali, che per quanto riguarda l'esistenza di resti eccetera ne sono ancora più lontani dei numeri razionali.

La storia cambia se passiamo ai numeri complessi. In questo campo il lavoro pionieristico fu fatto da Carlo Federico Gauss, detto talvolta "*princeps mathematicorum*". In suo onore parliamo di "interi Gaussiani " e di "primi Gaussiani".

Qui, sulle sue orme, vedremo:

I) Come si estende il concetto di numero intero dal campo reale a quello complesso.

II) Come si estende il concetto di numero primo dal campo reale al campo complesso e come tale estensione faccia magicamente scomparire metà dei numeri primi dall'asse reale, permettendone la scomposizione in due fattori complessi (e primi nel campo complesso).

III) Come si possa costruire un'aritmetica di numeri interi complessi a cui possiamo trasferire senza troppo sforzo concetti e teoremi validi per i numeri naturali (MCD, lemma di Bézout, etc.)

IV) Come il teorema del'unica scomposizione in fattori primi, sia valido anche per un intero Gaussiano.

V) Infine mostrerò – con parziale dimostrazione – un bel teorema sulla scomposizione di un numero primo della forma 4n+1 nella somma di due quadrati (questa è la base del risultato annunciato in (II).

I) Estensione del concetto di numero intero al campo complesso.

Per quanto riguarda il primo punto, evidentemente i numeri interi complessi saranno numeri che hanno un intero tanto nella parte reale quanto nella parte immaginaria, come 2 +3i, 1-i etc.

In prima battuta, numeri interi Gaussiani sono anche i numeri **naturali**, cioè i numeri interi positivi da 1 in avanti. Possiamo aggiungere lo zero, che serve a molte cose, e non nuoce al ragionamento successivo. Tuttavia, tutte le proprietà dei numeri naturali (in particolare le proprietà di *divisibilità*, che sono un poco lo spartiacque tra l'aritmetica elementarissima e la teoria dei numeri sul serio) si ripetono tal quali scegliendo altre tre unità, e costruendo tre nuovi semiassi di (quasi) numeri naturali.

Sono dunque numeri interi di Gauss per prima cosa tutti i numeri naturali, che chiameremo "ordinari", che sono interi, reali, positivi. Questi numeri occupano il semiasse disegnato in nero in figura e uno si potrebbe aspettare che tra loro i numeri primi reali siano anche numeri primi di Gauss. *Il problema è che questa affermazione non è vera*. Circa metà dei numeri primi "ordinari" non è un numero primo di Gauss. Vedremo perché.

Il primo "nuovo semiasse" – in giallo in figura - è basato sull'unità -1 (sono i nostri vecchi numeri negativi, che si comportano allo stesso modo di quelli positivi, se non facciamo confusione: per esempio, (-8)/(-3) = 2, con resto? Il resto è (-8) – 2(-3) = -8 + 6 = -2. Noto che quando facciamo una divisione, il resto ne risulta automaticamente. *Ma la definizione che ci sarà utile in seguito è quella appena data: Resto = Dividendo meno Prodotto del Quoziente per il Divisore.*
Noto ancora che il resto -2 non è altro che il resto valido per i numeri naturali, moltiplicato per la nuova unità (-1).

Il secondo nuovo semiasse – in rosso in figura - è basato sull'unità +i . Questi sono i numeri "interi" immaginari puri, che si comportano allo stesso modo di quelli reali positivi, anche qui se non facciamo confusione: per esempio, (+8i)/(+3i) = 2, con resto? Il resto è (8i) – 2(3i) = 8i-6i = 2i. Di nuovo, il resto è dato dal resto originario, 2, per la nuova unità (+i).

Il terzo nuovo semiasse – in azzurro in figura - è basato sull'unità -i: per esempio, (-8i)/(-3i) = 2, con resto? Il resto è (-8i) – 2(-3i) = -8i + 6i = -2i

Dunque il nostro piano complesso assume la forma data in Fig.1 , con i suoi 3 nuovi semiassi di numeri (quasi) naturali.

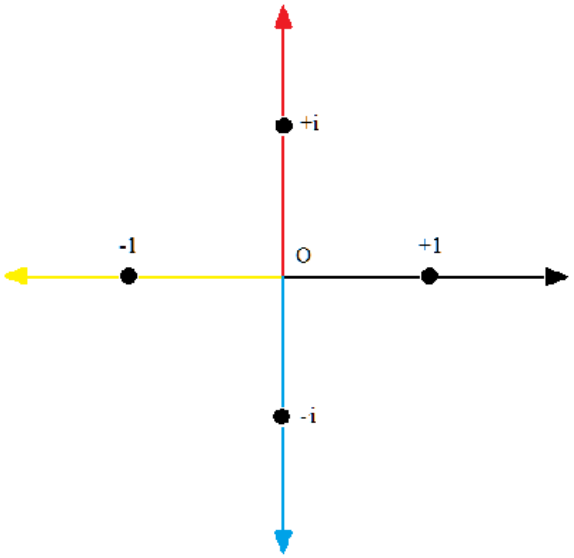

Fig.1

Abbiamo in pratica quattro unità differenti, che non cambiano le proprietà dei numeri naturali generalizzati, e quindi di tutti i numeri del campo complesso. Ogni numero del piano complesso avrà quindi di norma tre ***associati***, moltiplicandolo per una differente unità.

Gli associati di 1+2i sono quindi:
1) moltiplicando il numero per l'unità -1: -1-2i;
2) moltiplicando il numero per l'unità +i: i -2 = -2+i;
3) moltiplicando il numero per l'unità –i: -i+2 = 2-i.

Dato che si tratta di unità, si può continuare a moltiplicare o per la stessa o per altre unità, sempre ritrovando uno dei quattro associati. Per esempio, moltiplicando (-i)(2-i) si ritrova -1-2i etc.

Figura 2 riproduce le posizioni dei quattro associati.

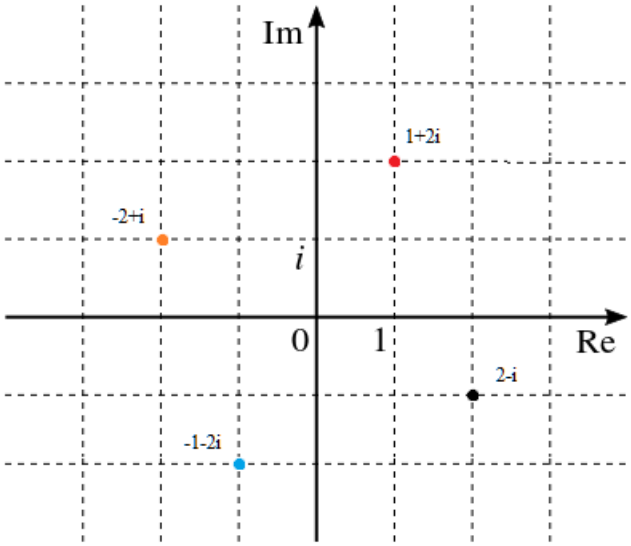

Fig.2

Le quattro operazioni sono intuitive, con qualche complicazione in più, come il solito, per la divisione:

1) Addizione: (a+ib)+(c+id) = (a+c) +i (b+d)

2) Sottrazione: (a+ib)-(c+id) = (a-c) +i(b-d)

3) Moltiplicazione: (a+ib)(c+id) = (ac-bd) +i(bc+ad)

4) Divisione: $\frac{a+ib}{c+id} = \frac{a+ib}{c+id}\frac{c-id}{c-id} = \frac{(ac+bd)+i(bc-ad)}{c^2+d^2} = \frac{(ac+bd)}{c^2+d^2} + i\frac{(bc-ad)}{c^2+d^2}$

L'ultima forma nella divisione permette di esprimere il risultato della divisione come un quoziente più un resto. Ottenere il quoziente e il resto non è immediato come per i numeri naturali: nel nostro caso, tanto per la parte reale quanto per la parte immaginaria *del quoziente* si sceglie **l'intero più vicino** possibile ai valori trovati. Una volta operato questo arrotondamente, il *resto* sarà la differenza fra il dividendo e il quoziente moltiplicato il divisore, come dall'originaria definizione di resto. Essendo tanto il dividendo quanto il prodotto che gli è sottratto due numeri interi (Gaussiani), anche il resto sarà un numero intero.

Un esempio numerico:

Si voglia esprimere nella forma "quoziente più resto" il rapporto $\frac{8+7i}{1+2i}$. (a=8, b =7, c=1, d = 2)

Svolgendo il calcolo regolare, identificando (a=8, b =7, c=1, d = 2), si ottiene:

$$\frac{8+7i}{1+2i} = \frac{22}{5} - i\,\frac{9}{5}$$

Ora si **arrotonda**, cioè si cercano **gli interi più vicini** a 22/5 e 9/5. Essi sono rispettivamente 4 (= 20/5) e 2 (=10/5), per cui l'intero gaussiano più vicino è 4-2i. Questo è il nostro quoziente. Come si è detto, il resto sarà la differenza fra il dividendo e il quoziente moltiplicato il divisore.

Ora si fa la differenza (8 + 7i) – (4-2i)(1+2i) = 8+7i – [(4+4)+i(8-2)] = 8 +7i- (8 +6i) =i

Inaspettatamente (per un matematico ciclista come me) il sistema funziona anche per una divisione come la seguente:

$$(5+6i)/(2+3i) = \frac{28}{13} - \frac{3i}{13}$$

Che, messa nella forma "quoziente, resto" diventa: 2, 1. In effetti 28/13 dà 2 con avanzo di 2/13 mentre 3/13 dà 0, con avanzo di 3/13. Ora (5+6i) -2 *(2+3i) =1, il resto.

Alcuni concetti sono, si suppone, già noti.

1) **Complesso coniugato**. E' il numero che ha la parte reale uguale e la parte immaginaria di segno opposto. Ad esempio 1+ 2i ha come complesso coniugato 1-2i *che (di solito) non è un associato.*

Il lettore stakanovista potrà notare che *i quattro associati divengono due coppie di complessi coniugati se le parti reali sono eguali a quelle immaginarie*. La prova la si può ottenere moltiplicando per le tre unità immaginarie un numero complesso qualsiasi che goda di questa

proprietà, per esempio $a+ia$, ottenendo così due paia di complessi coniugati. Se fa l'esercizio, con 2 + 2 I, trova il simpatico risultato che *a + ia* è il coniugato di *(-i)(a+ia)*, mentre (-a + ia) è il coniugato di (i)(-a+ia).

2) Norma. La norma è il prodotto di un numero complesso per il complesso coniugato *(per alcuni altri autori è la radice quadrata di tale prodotto).* Per uno dei primi prodotti notevoli che si apprendono a scuola, e tenendo conto del fatto che (i) (-i) = +1, la norma è *sempre* la somma di due quadrati. Ed è quindi un (intero) positivo. Esempio: $(a+ib)(a-ib) = a^2 + b^2$.

Come si può vedere facendo la somma di due qualsiasi quadrati, dividendo la somma di due quadrati per 4 non si ha mai resto 3. Quindi, nessuna Norma, divisa per 4, può dare resto 3.

Infatti, la somma di due quadrati di due numeri pari è un multiplo di 4 (divisa per 4 dà resto 0), in quanto

$(2n)^2 + (2m)^2 = 4(n^2 + m^2) + 0$

La somma di due quadrati dispari invece, divisa per 4 dà resto 2:

$(2n+1)^2 + (2m+1)^2 = 4n^2 + 4n + 1 + 4m^2 + 4m + 1 = 4(n^2+n+ m^2 + m) + 2$

E infine la somma di un quadrato di un numero pari più il quadrato di un numero dispari, dà resto 1:

$(2n+1)^2 + (2m)^2 = 4n^2 + 4n + 1 + 4m^2 = 4(n^2+n+ m^2) + 1$

Questo suggerisce un giochetto di società: Domanda. Qual è il resto della divisione per 4 di $3^2 + 2^{10}$? Quanto abbiamo scritto sopra ci assicura che il resto è 1. Con numeri così piccoli, la vittima può essere tentata a fare i conti. Ma il resto della divisione per 4 è uno anche se proponiamo come dividendo $113^{1566} + 8024^{654238}$, cosa che non credo nessun iPhone possa fare.

Dopo tutto io scrivo e tu leggi tutto questo per divertimento. Perché no?

La Norma di un numero intero gaussiano α, che chiameremo N(α) gode della proprietà moltiplicativa, cioè "la norma del prodotto è il prodotto delle norme":

Infatti:

$N(a+ib)\ N(c+id) = (a^2 + b^2)(c^2 + d^2) = a^2 c^2 + a^2d^2 + b^2c^2 + b^2d^2$

Mentre

$N[(a+ib)(c+id)] = N[(ac-bd)+i(bc+ad)] = a^2 c^2 + b^2d^2 - 2acbd + b^2c^2 + a^2d^2 + 2bcad = a^2 c^2 + a^2d^2 + b^2c^2 + b^2d^2 = N(a+ib)\ N(c+id).$

Ma da questa formula abbiamo anche:

$N(a+ib) * N(c+id) = N[(ac-bd)+i(bc+ad)]$

Da cui , calcolando le tre Norme dei tre numeri complessi che appaiono nella relazione, segue la celebrata formula che il prodotto delle somme di due quadrati è la somma di due quadrati, cioè

$$(a^2 + b^2)(c^2 + d^2) = (ac-bd)^2 + (bc+ad)^2$$

(identità di **Brahmagupta-Fibonacci).**

Ne segue anche un'altra proprietà: chiamiamo (a+ib)(c+id) = (f + ig). Ma questo comporta che se (a + ib) divide (f + ig), N(a+ib) è un divisore di N(f+ig). Qui, a pensarci bene, è una chiave per ritrovare i numeri primi Gaussiani, perché la Norma di un numero primo gaussiano è un numero primo, in quanto dovrebbe essere data dal prodotto delle Norme dei suoi divisori. D'altronde, se la norma di un numero intero Gaussiano non ha divisori, non ha divisori neppure l'intero gaussiano, che quindi è primo.

La Norma delle quattro unità , come si verifica subito, è 1 (ce lo si poteva aspettare), inoltre, dato che i quattro associati risultano dal prodotto di uno di essi per tre altre unità, per la proprietà moltiplicativa delle Norme, i quattro associati hanno tutti Norma eguale, cioè sono situati su un cerchio centrato sull'origine, il cui raggio è la radice quadrata della Norma di uno dei quattro numeri. Le quattro unità, come è facile accertarsi, sono gli unici interi gaussiani che hanno Norma 1 (infatti un numero intero Gaussiano ha norma a^2+b^2 che deve essere eguale a 1, il che accade solo se uno di due interi a,b vale 1 e l'altro vale 0)

3) Qui vediamo profilarsi un interessante problema: **i numeri interi** (o anche non interi) **Gaussiani non formano un corpo ordinato**, cioè non possono essere messi in fila come i numeri naturali ordinari, in successione crescente. Ovviamente, la *Norma ci dà un'indicazione*, in quanto se un numero u + iv ha Norma maggiore di un numero x + iy, possiamo senz'altro dire che "u+iv è maggiore di x+iy" essendo più lontano dall'origine del piano dei numeri complessi. Ma tutti gli interi di eguale Norma, che si trovano su un cerchio il cui raggio è la radice quadrata della Norma che abbiamo scelto, hanno eguali diritti, e – che io sappia - non si è ancora trovata una convenzione utile che permetta di stabilire che essi possono essere ordinati in qualche modo universalmente utile.

II) Estensione del concetto di numero primo al campo complesso.

Riassumendo, il concetto di numero primo a questo punto si è già infiltrato nel nostro ragionamento. Grazie alla nostra estensione del concetto di divisione, abbiamo il concetto di **divisori** di un numero dividendo, che, come per l'aritmetica elementare, sono gli interi che dividono "esattamente" il dividendo senza lasciare resto.

Si estendono allora altrettanto facilmente i numeri primi, che sono i numeri che non hanno altri divisori che se stessi e...le quattro unità +1, -1, i, -i.

I **primi** sul piano complesso (una volta trovati) sono disordinatissimi, ma se guardiamo meglio, vediamo comparire certe simmetrie, basate sull'esistenza dei numeri associati.

Già una prima immagine dei numeri primi Gaussiani nei dintorni dell'origine (Fig.3) mostra queste simmetrie dissimmetriche :

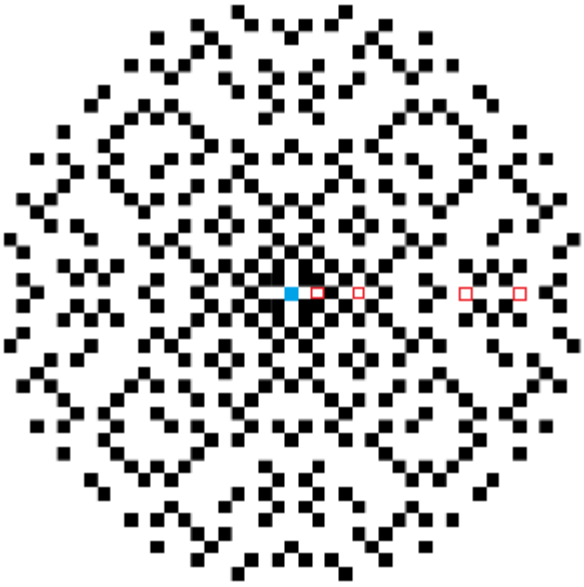

Fig.3

La figura è degna di nota. In blu è segnata l'origine. **Con quadrati rossi vuoti sono notati sull'asse dei numeri naturali certi numeri primi ordinari che, considerati come interi gaussiani, non sono più numeri primi.** Qui sono segnati 2, 5, 13, 17. Perché non sono più numeri primi?
La figura è basata su
https://upload.wikimedia.org/wikipedia/commons/8/85/Gaussian_primes.png

L'immagine sottostante (Fig.4), che proviene da Wikipedia ("Gaussian Primes") rappresenta i numeri primi sul piano complesso su un'area molto più estesa, e sembra disordinata, ma se la guardate bene presenta certe strane regolarità … irregolari. A cercare queste regolarità irregolari c'è quasi da impazzire.

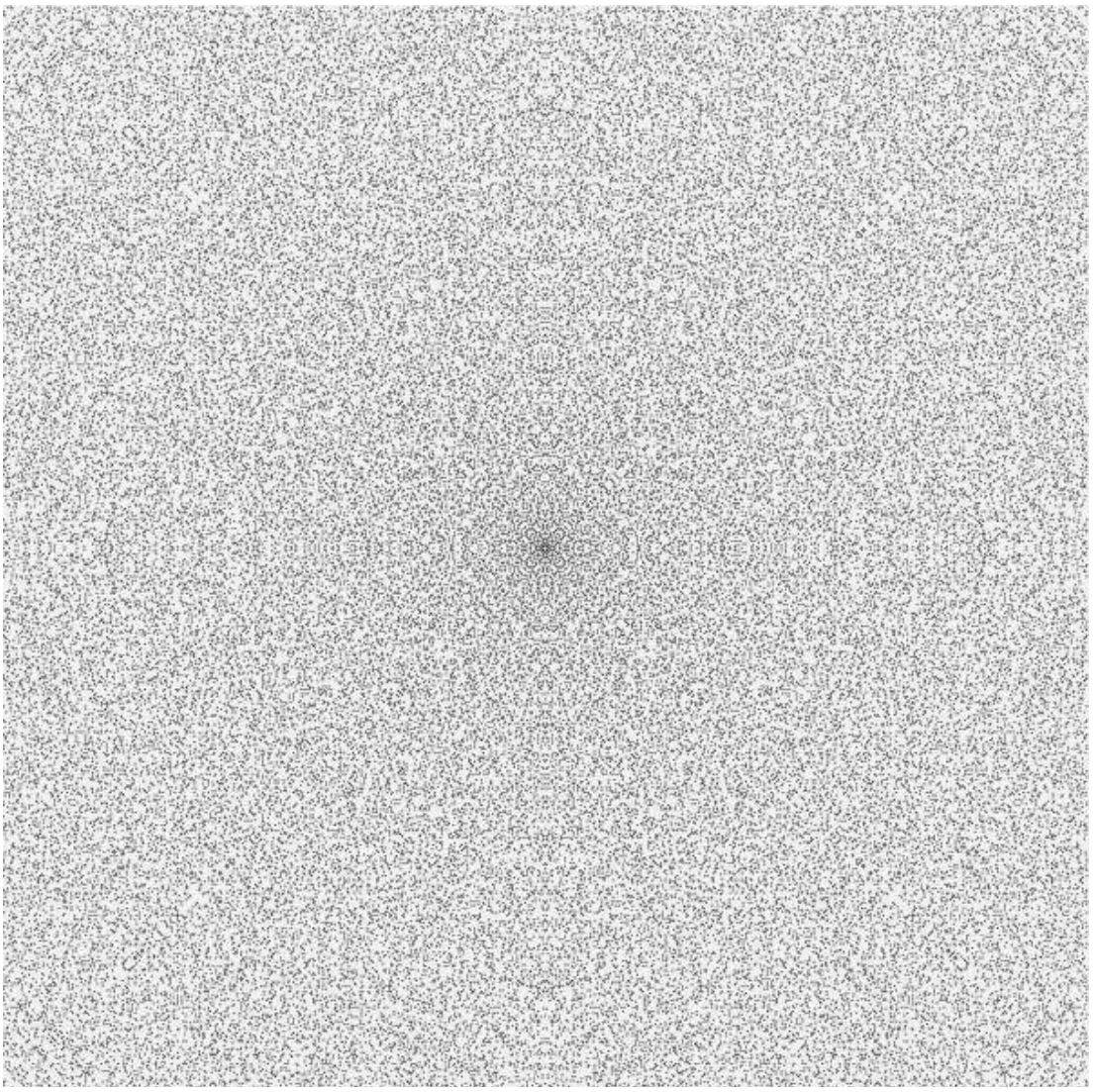

Fig.4

https://commons.wikimedia.org/wiki/File%3AGauss-primes-768x768.png
https://upload.wikimedia.org/wikipedia/commons/c/c8/Gauss-primes-768x768.png
By Truejackster (Own work) [Public domain], via Wikimedia Commons

Ma come si trovano i numeri primi Gaussiani??

Un primo numero primo Gaussiano: $p_1 = 1+ i$

Supponiamo che il numero primo p Gaussiano abbia norma $a^2 + b^2$ pari. In tal caso deve essere $a^2 + b^2=2$, perché la Norma di un numero primo gaussiano è un numero primo naturale (in quanto è un numero naturale reale, che non deve avere divisori), e l'unico numero primo naturale *pari* è 2. Ne segue che, a meno di un'unità, p = 1+i.
Dimostrazione: perché la somma dei quadrati $a^2 + b^2$ sia pari, a e b devono essere entrambi pari (nel qual caso il numero primo ancora incognito p è divisibile per 2 = (1+i)(1-i) che è divisibile per 1+i), o entrambi dispari. Se sono entrambi dispari, p+(1+i) è divisibile per 2, in quanto diventa (a+1)+i (b+1), e tanto a+1 quanto b+1 sono ora pari. Quindi il numero è divisibile per 2=(1+i)(1- i).

In entrambi i casi p è divisibile per 1+i. Ma poiché p è primo, può solo essere p = u (1+ i) dove u è una delle quattro unità. (Incidentalmente , -i(1+i)= (1-i), cioè i due fattori differiscono per una unità e sono associati: ciò vale solo per 1+i perché la parte reale e la parte immaginaria hanno valore 1. E, moltiplicate per qualsiasi unità, o cambiano segno o si riproducono l'una nell'altra)

I numeri primi sono dunque i seguenti:

1) 1+i (e associati), unico numero primo Gaussiano di norma 2:
2) Sono primi gaussiani i **numeri reali primi della forma 4n+3** (la cui norma è il loro quadrato)
3) Sono primi gaussiani numeri interi gaussiani la cui **norma** è un numero *primo* reale.
4) In quanto ai numeri interi Gaussiani della forma 4n +1, questa è sempre scomponibile nella somma di due quadrati: u^2+v^2 (dimostrazione conclusiva di questo saggio) , e quindi nel prodotto (u+iv)(u-iv). Ciascuno di essi è un numero primo Gaussiano, perché, come da (3), la norma di entrambi è lo stesso numero primo.

Possiamo così elencare in ordine di Norma crescente o eguale i numeri primi Gaussiani di norma inferiore a 20.

1 + i (1-i è un suo associato, e non conta), 2+i , 2- i, 3, 3+2i, 3-2i, 4+i, 4-i.
Si noti che 5,7,11 etc hanno norma (il loro quadrato) maggiore di 20.
Nella figura 5 sottostante si mostra come gli otto numeri primi indicati, mediante i loro associati, riempiano completamente il piano di numeri primi Gaussiani. Il lettore patologicamente volonteroso è in grado di identificare quali sono i primi originari, e quali gli associati (che peraltro hanno lo stesso colore):

Fig.5

Intanto ri-notiamo la scomparsa dall'asse reale di tutti i numeri primi della forma 4n + 1 (qui si tratta solo di 5. Come abbiamo visto, 2 scompare per altro motivo)

I numeri primi reali (a parte 2) sono tutti dispari. Questo vuol dire che sono tutti della forma p = 2n + 1. Però i numeri dispari a loro volta sono classificabili in due classi, quelli della forma 4n+1 e quelli della forma 4n +3 (che può anche esser scritta 4n-1).

Chiaramente 1,5,13,17,29 etc. sono della forma 4n+1, mentre 3, 7,19,31 sono della forma 4n-1 o 4n+3. E' un utile esercizio identificare gli n che dovremmo introdurre in ogni numero primo.

Ora, la somma dei quadrati di due numeri interi non può essere un numero primo nel campo complesso, perché uno qualsiasi di questi "falsi" numeri primi è scomponibile nel prodotto di due numeri complessi coniugati. Infatti noi sappiamo che

$(a + i\,b)(a - i\,b) = a^2 + b^2$, ed un numero è primo proprio perché non ha fattori interi (reali o complessi). Qui invece li ha.

Per esempio: 5 = (1+i2)(1-i2) e 29 = (5+2i)(5-2i).

E con questo, come vedremo, ci siamo persi circa metà dei numeri impostori che se ne stavano tranquilli sull'asse reale fingendosi primi e sapendo bene di non esserlo (non dimostrerò che si tratta di metà, anche se è ragionevole congetturarlo)

Quanti sono e come sono riconoscibili questi impostori? C'è una regola semplice per capire se un numero primo è primo oppure no, anche senza provare a scomporlo nella somma di due quadrati, lavoro lungo e sgradevole?

Ora, abbiamo già visto che la **somma dei quadrati di due numeri interi non può mai essere della forma 4n-1 (o 4n + 3, che è lo stesso).**

Se quindi dividiamo per 4 un candidato numero primo e troviamo un resto 3 (o -1), andiamo sul sicuro: il numero non può essere la somma di due quadrati, e quindi può essere un numero primo nel campo complesso, *purché lo sia nel campo reale.*

Esiste però, come già annunciato, il bel teorema inverso dalla più lunga dimostrazione, che darò a conclusione di questo saggio ed è valido solo per i numeri primi, secondo il quale **TUTTI i numeri PRIMI (sull'asse reale) della forma 4n+1 sono scomponibili in due quadrati e quindi nel campo complesso non sono primi).** Provare per credere: 5 = 1+4; 13 = 9+4; 17 = 16+1, 29 = 25 + 4 etc.

1 = 0 x 4 +1 andrebbe bene se 1 fosse un numero primo, ma per convenzione non lo è: è il primo numero , ma non è un numero primo, perché ammetterlo - oltre ad altre conseguenze discutibili - manderebbe in pezzi un teorema fondamentale dell'aritmetica, quello dell'*unica* scomposizione di un numero in fattori primi. Infatti, per esempio 6 potrebbe essere scomposto come 2 x3, 1 x 2 x 3, 1 x 1 x 2 x 3 eccetera.

Dunque, se prendiamo un numero primo reale, a parte il solito 2, e lo dividiamo per 4, non abbiamo che da esaminare il resto: se il resto è 1, non può essere un numero primo nel campo complesso.

E con questo, metà dei numeri primi sull'asse reale (quelli della forma 4n+1) non sono più primi nel campo complesso (che siano metà, è, a questo punto, solo una congettura).

Questa osservazione ha una conseguenza. Come sappiamo, nella successione dei numeri primi reali esistono (pare) infinite coppie sempre più rade di numeri primi la cui differenza è 2 (come 5 e7, 11 e 13, 17 e 19, 29 e 31 etc.), e quindi sono necessariamente della forma 4n+1 e 4n-1. Ebbene, queste coppie perdono uno dei partner se considerate come coppie di numeri primi Gaussiani, e quindi i numero primi restano soli, sempre più soli, e – in media - sempre più lontani gli uni dagli altri. Questa accresciuta solitudine nel campo reale, però, è controbilanciata nel campo complesso dallo gioiosa vicinanza di uno sciame di numeri primi, che almeno si toccano in un vertice. Guardando la figura 3 non si vede in realtà alcun numero primo Gaussiano isolato: ce ne sono sempre almeno due che si toccano in un vertice, come se si tenessero per mano. Magari andando lontano dall'origine ci saranno pure dei primi Gaussiani isolati, ma va a sapere.

III. Aritmetica con i numeri interi Gaussiani.

Come vedremo, abbiamo creato un sistema di numeri che si comportano in grandissima parte come gli interi a noi noti, mutatis mutandis, e le dimostrazioni che ci interessano e che useremo per dimostrare ulteriori teoremi possono essere ripetute parola per parola.

III.1 il Massimo Comun Divisore.

Un primo esempio è dato dal calcolo del MCD. Mentre il metodo della fattorizzazione, come dimostrerò in Appendice II , è possibile, esso è assai laborioso, ben s'intende per numeri grandi. Invece, come nel caso dei numeri naturali, l'algoritmo Euclideo è applicabile, funziona, ed è efficiente.

La base di questa applicabilità è che possiamo eseguire una divisione (dividendo diviso divisore) che ci dà un quoziente ed un resto. E poi si continua usando la coppia (divisore, resto), che ci darà un secondo quoziente con un secondo resto e così via. Ciò che è importante è che il resto sia ogni volta "più piccolo" del divisore. E per noi lo è, se per più piccolo intendiamo che la Norma del resto è in ogni divisione inferiore alla Norma del divisore (Essendo partiti con la divisione del numero di Norma maggiore per quello di Norma minore nella coppia di cui vogliamo il MCD).

Se si giungerà a un resto zero, avremo trovato un MCD. Se si giungerà ad una delle nostre quattro unità, avremo trovato che i due numeri di partenza sono primi fra loro. Questo ancora non ci dà un numero primo.

Facciamo dunque un semplice esempio. Si voglia il MCD di -4416+ i 1040 e 780- i 1882:

Operazione	Dividendo X	Divisore Y	Quoziente, q	Resto R=X-qY
1	-4416+ i 1040	780- i 1882	-1- 2i	128+ i 718
2	780- i 1882	128+ i 718	-2-2i	-400-i 190
3	128+ i 718	-400-i 190	-1-i	-82+ i 128
4	-400-i 190	-82+ i 128	3i	-16+ i 56
5	-82+ i 128	-16+ i 56	2+ i	6 + i 32
6	-16+ i 56	6 + i 32	2 + i	4- i 14
7	6 + i 32	**4- i 14**	-2 + i	0

Il MCD è dunque 4 – i 14, che, incidentalmente, non è un numero primo Gaussiano, essendo quanto meno divisibile per 2.

Se noi avessimo battezzato i due numeri complessi di cui volevamo il MCD rispettivamente α e β, e in simile modo tutti gli altri numeri complessi che compaiono nell'algoritmo euclideo, l'algoritmo sarebbe indistinguibile da quello dato per i numeri reali, ad esempio in http://dainoequinoziale.it/scienze/matematica/2017/10/30/vardiv.html.

Possiamo per esempio percorrere a ritroso l'agoritmo e, per evitare di perdere tempo su un soggetto semplice (l'unico lettore, se è sopravvissuto, potrà continuare l'esercizio), supporre che i numeri di cui vogliamo il MCD siano quelli della linea 4, cioè -400-i 190 e -82 + i 128.Come si sarà notato, per l'Algoritmo Euclideo è indifferente cercare il MCD di una qualunque delle coppie che compaiono in seconda e terza colonna della nostra tavola.
Dunque:
4- i 14 = (-16+i 56)- (2+i)(6+32 i)
Ma -16+i56= -400-i 190 – 3i (-82+i128) e (6+32i) =(-82+i 128) – (2+i)(-16 + i 56)
Quindi
4-i 14 = (-400 – i 190) – 3i(-82+ i128) - (2+i)((-82 + i 128) – (2+i)(-16+i56))
4+i14 =(-400 – i 190) – 3i(-82+ i128) - (2+i)((-82 + i 128) – (2+i)(-400-i 190 – 3i (-82+i128)))=

Eseguendo le operazioni senza perderci la testa (un primo aiuto è, una volta trovato uno dei due numeri di partenza, non lasciarlo sfuggire coinvolgendolo in calcoli, e un secondo aiuto è dare ai due numeri rossi i nomi x e y, e cercarne i coefficienti complessi), possiamo calcolare i coefficienti dei numeri originali: otteniamo:

(4+i 4) (-400 – i 190) + (10- i 13)(-82+ i 128) = 4-i 14 (Cdd)

Cioè abbiamo mostrato – non dimostrato - (come dovevamo aspettarci) che il MCD di due numeri è una loro "combinazione lineare".

Vediamo ora secome nel caso dei numeri reali, una combinazione lineare di numeri primi possadare risultato 1. Scegliamo ad esempio (dalla figura 5, tanto per stare sul sicuro) 2+i e 4 –i. Noi cerchiamo due numeri complessi x e y tali che

$$x(4-i)- y(2+i) = u$$

Dove u è una delle 4 unità che rionosciamo.
E' allora sufficiente dividere il numero a Norma maggiore (4-i) per quello a Norma minore (2+i), e si trova come quoziente 1 – i e resto 1, che vuol dire, ricordando la definizione di resto :
D = q d+r , dove D è il dividendo, d il divisore e r il resto:
(4- i)= (1-i)(2+i) + 1, cioè:

(4 – i) – (1-i) (2+i) = 1 (Cdd)

Questo risultato e il precedente hanno applicazioni straordinarie: si pensi ad un gruppo di conigli immaginari che hanno 4-i zampe ciascuno e oche non meno immaginarie che hanno 2+i zampe ciascuna, per un totale di 23 zampe! Se il lettore seguirà l'algoritmo indicato in
http://dainoequinoziale.it/scienze/matematica/2017/10/30/vardiv.html
troverà l'ambita soluzione generale, che particolarizzerà assegnando un numero immaginario, spero, di teste.

Tocca ora all'importante teorema fondamentale dell'aritmetica, quello dell'unica fattorizzazione dei numeri interi in fattor primi

IV.2 Scomposizione di un numero intero Gaussiano in fattori primi. Unica scomposizione.

Sarà facile provare l'unica fattorizzazione e la maggior parte dei vari teoremi simili a quelli che valgono per i numeri naturali reali. Resta però almeno un problema non del tutto banale: Come si fa a scomporre un intero Gaussiano in fattori Primi Gaussiani?

IV.1. Scomposizione di un intero Gaussiano in fattori primi Gaussiani

Nel caso di un numero reale da scomporre in fattori primi reali noi essenzialmente dividiamo il nostro numero originale progressivamente per una serie di fattori primi incominciando dai più piccoli. Questi li conosciamo a memoria. Quando poi troviamo un numero N che non è divisibile per nessuno di quelli, allora dobbiamo vedere se N sia primo o no. E questo lo si fa a tentativi, provando con i vari interi p, inferiori alla *radice quadrata* di N. Questo per la nota ragione che se un numero maggiore della radice quadrata di N divide N, inevitabilmente il risultato della divisione è inferiore alla radice quadrata di N, perché solo la radice quadrata di N presenta due fattori eguali e il prodotto di due fattori entrambi superiori alla radice quadrata di N produce sempre un numero superiore ad N. (Si veda ad esempio :
http://dainoequinoziale.it/scienze/matematica/2017/03/23/radici.html)
Grande o piccolo che sia N, questo è il metodo "ingenuo" di scomposizione, funziona , ed è immediatamente comprensibile.

Se vogliamoscomporre un intero Gaussiano z, procedendo per analogia, potremmo pensare di calcolarci la Norma dell' intero z , che chiameremo z, e poi costruirci o ricercare una tavola di numeri primi Gaussiani di Norma inferiore a quella di z, che chiameremo N(z), e poi provare con tutti se qualcuno di essi divide senza resto il numero originale z. Ma c'è un modo più semplice di procedere, anche se prende il suo tempo.

Esso è basato sul fatto che la Norma N è moltiplicativa, cioè, dati due interi gaussiani α e β abbiamo che $N(\alpha\beta) = N(\alpha)N(\beta)$, e poi, con le regole apprese a suo tempo, dalle Norme risaliamo ai fattori primi.

Quindi
1) Il primo passo è calcolare la Norma del numero. Dato che la Norma del numero è data dal prodotto delle Norme dei fattori, il secondo passo è:

2) Scomporre la Norma di z nei suoi fattori primi. Otterremmo:
$N(z)= N(\alpha)N(\beta)N(\gamma)...N(\omega)$

Ogni Norma contiene uno o due possibili fattori primi Gaussiani di z.
a) Se vale 2, essa è data da (1+1), Norma di (1-i) e di (1+i), ma (1-i), come già notato, non è altro che (1+i) (-i), cioè è lo stesso fattore.
b) se essa è un numero reale primo della forma p =4n+3, p è un fattore primo di z.
c) se essa è della forma N(p)=4n+1, allora p può essere scomposto in due quadrati: $p = a^2+b^2 = (a+ib)(a-ib)$, che a sua volta offre due possibilità, (a+ ib) e (a –ib). Anche qui bisognerà vedere quale delle due possibilità divide esattamente Z, e quindi ne è fattore primo.

Facciamo un esempio: vogliamo scomporre in fattori primi Gaussiani il numero Z = 279+105i .

La Norma è 88866. La scomposizione in fattori primi dà:
88866= 2 x 3 x 3 x 4937.

1) Dunque il primo fattore ci offre una sola possibilità, 1+i.
Questo può essere verificato eseguendo la divisione (279+105 i)/(1+i), che produce 192+87 I, un intero Gaussiano, e quindi abbiamo trovato il primo fattore.

2) il secondo e il terzo fattore valgono 3, chiaramente della forma 4n + 3 (per n =0), per cui abbiamo due volte il fattore primo 3. Ma ciò è dovuto al fatto che si tratta di una norma di un numero reale, che è il quadrato del medesimo. Nel numero z, invece, 3 entra una volta sola.

3) Il caso 4937 è un po' più complicato. Dividendo per 4 otteniamo resto 1. 4937 è quindi dato dalla somma di due quadrati.
Questo numero apre due *excursus*: i) quali sono i due quadrati (e come trovarli); se la decomposizione sia unica (e la risposta è che per un numero primo, come 4937, lo è).

Per numeri primi piccoli, la decomposizione la si trova facilmente o a occhio o con pochi calcoli.

Ma se il numero incomincia d essere grande, come il 4937 che abbiamo trovato, abbiamo diverse possibilità di crescente complicazione, che però tutte – per quanto ne so - richiedono un algoritmo che è bene lasciar fare ad un calcolatore. Ora è mia intenzione utilizzare l'algoritmo concettualmente più semplice possibile, lasciando ai professionisti di calcolo numerico il compito di trovare un algoritmo migliore (il che è già stato fatto, e più volte): lo scopo in questo breve saggio è solo quello di mostrare gli elementi del funzionamento dei numeri interi e primi Gaussiani.

Dividendo per due 4937, uno dei due addendi (sia esso x^2) deve essere inferiore al risultato della divisione per due. Nel nostro caso , il massimo valore possibile per x è la radice quadrata della metà di, diciamo per far cifra tonda, 5000, cioè circa 50. Quindi tentiamo con i quadrati dei numeri x da 1 a 50, e vediamo se 4937- $x^2 = y^2$, altro quadrato perfetto.Se tale è il risultato, abbiamo trovato i due quadrati, e i due numeri interi Gaussiani $x \pm iy$ candidati ad essere un divisore primo del nostro z, come dovremo verificare. Come sapremo dal teorema che dimostreremo per ultimo, il secondo quadrato deve esistere.

Il programma minimale in SmallBasic è:

```
For I = 1 To 50
  q1 = I*I
  q2 = 4937-I*I
  root = Math.SquareRoot(q2)
  rroot = Math.Round(root)
  If rroot = root Then
Goto result
  EndIf
EndFor
result:
TextWindow.WriteLine("Primo = "+ I + ";  second: "+ root)
```

E il risultato, ottenuto in questo caso in una frazione di secondo, è: 4937 = $29^2 + 64^2$, cioè i due numeri con i quali dobbiamo provare a vedere se si tratta di divisori esatti del nostro intero gaussiano, sono 29+64 i e 29-64 i.
La prima divisione (279+105 i)/(29+64 i) produce un intero, 3-3i

Viceversa, la divisione (279+105 i)/(29-64 i) produce 1371/4937+(i 20901)/4937, non intero. Abbiamo quindi la decomposizione:

$$\mathbf{z = 279+105\ i \ = \ (1+i),\ 3,\ (29+64\ i)}$$

IV.2. Teorema fndamentale dell'aritmetica: unica fattorizzazione di un intero, reale o gaussiano che sia.

Per questo vediamo le tracce della dimostrazione data in
http://dainoequinoziale.it/scienze/matematica/2017/10/30/vardiv.html
Là dicevamo:
Supponiamo che un numero N sia decomponibile in due modi in fattori primi:

$$N = p_1p_2p_{3...}\ p_r \ = q_1q_2q_3...q_s$$

Siccome p_1 divide N, applicando il risultato precedente, vediamo che deve dividere uno dei fattori q_i, che però è primo e non ha divisori. Quindi, se p_1 divide $q_{i,}$ i due numeri p_1 e q_i sono eguali e possono essere semplificati. Si rifà lo stesso ragionamento con p_2 e si semplifica un altro q. Si continua in questo modo fino a che il prodotto delle p si riduce a 1, e a destra non possono restare q, perché sono tutte superiori a 1. Dunque, magari con i fattori in diverso ordine, le due scomposizioni sono identiche.

Nulla va cambiato in questa dimostrazione. Soltanto, i fattori primi vanno reintepretati come fattori primi Gaussiani, e il teorema è dimostrato.

V. GRAN FINALE.

TUTTI i numeri PRIMI (sull'asse reale) della forma 4n+1 sono scomponibili in due quadrati (nel campo complesso, e quindi in questo campo non sono primi). Dimostrazione di Lagrange (1773).

Molti studiosi alle prime armi di questo campo lamentano che una leggibile dimostrazione di questo cruciale teorema è per lo più assente dai vari testi che si occupano di numeri primi Gaussiani. Fedele ai miei programmi, la propongo nella forma di Lagrange.

La dimostrazione di Lagrange non è brevissima, ma si basa su teoremi relativamente antichi e noti. Le successive dimostrazioni (e ce ne sono diverse) sono sempre più brevi in sè, ma fanno riferimento a conoscenze sempre meno immediate, per cui occorre dimostrare altri teoremi meno noti, non necessariamene banali. Chi è in possesso di queste cognizioni, ovviamente, è avvantaggiato. Chi non lo è, deve studiare molto più a lungo prima di arrivare alla dimostrazione conclusiva, che magari è data in una riga.

Confesso che non darò una dimostrazione completa, ma solo una, spero, soddisfacente semi-dimostrazione:

I. Il punto di partenza è il **teorema di Wilson**.

Abbiamo visto in questo sito una presentazione elementare delle congruenze. Qui ampliamo il vocabolario per dire le stesse cose: diciamo che

$$a \equiv r \ (mod\ n)$$

in cui il triplo tratto nel segno di eguale si legge "è congruente", per dire che (a-b) è divisibile per n, ovvero $a - r = kn$, in cui r è il resto della divisione di a per kn. Come abbiamo detto altrove, l'universo dei numeri interi, in base n, viene così diviso in n "classi di resti" eguali. Queste hanno il nome di "classi di residui di interi modulo n". Ora, bisogna farci qualche attenzione. Usiamo la notazione $[0]_n$ per indicare la classe dei residui 0 della divisione per n, cioè la classe degli infiniti numeri che divisi per n danno resto zero.

La cosa è banale per i numeri naturali: si divide e si calcola il resto.

Per esempio, nella divisione per 4, abbiamo 4 classi di residui:

$[0]_4$ = {0,4,8,12,16 etc.}

$[1]_4$ = {1,5,9,13,17 etc..

$[2]_4$ = {2, 6,10,14,18 etc.}

$[3]_4$ = {3, 7,11,15,19 etc.}

I numeri fra parentesi quadre possono ricevere il nome di "rappresentanti della classe di residui".

Ma intanto notiamo che queste classi di residui si possono estendere ai numeri negativi. Ora, questo non è banale. O meglio, un modo banale esiste ed è quello di procedere verso sinistra sottraendo

progressivamente 4 al primo numero di una successione. Ma quanti sono capaci al primo colpo di dire che -3 è nella classe $[1]_4$? Ad ogni modo la cosa è semplice se si ricorda che -3-x deve essere eguale a 4k. Il primo k possibile è - 1. E per -5 ? Di nuovo, -5- x = 4k. Ne viene che $[3]_4$ è il numero x cercato, con k = -2.

Le nostre tavole si allungano infinitamente a sinistra:

$[0]_4$ = {...-12,-8 -4,0,4,8,12,16 etc.}

$[1]_4$ = {...-11, -7, -3,+1,5,9,13,17 etc..}

$[2]_4$ = {...-14,-10,-6, - 2, 2, 6,10,14,18 etc.}

$[3]_4$ = {...-13,-9,-5,-1, -3, 7,11,15,19 etc.}

Per aumentare il numero di notazioni, introduciamo ora
I/(4), l'insieme delle classi modulo n, che per 4 è { $[0]_4$, $[1]_4$, $[2]_4$, $[3]_4$ } caso particolare di I/(n) , { $[0]_n$, $[1]_n$, $[2]_n$,... $[3]_{n-1}$ }

Un'aritmetica modulare (per addizione emoltiplicazione) può essere creata, tenendo i resti delle operazioni modulo n.
Per esempio, modulo 4, 5 +3 dà 0, 5 -3 dà 2, 5 x 3 dà 3.
Si può introdurre un inverso moltiplicativo, ma questo non è sempre possibile. Questo avviene quando un dato numero moltiplicato l'inverso 1* diviso il modulo, dà resto 1. Per esempio, modulo 7, 2 x 4 dà resto 1, come 4x 2 dà resto 1, per cui i due sono inversi l'uno dell'altro – beninteso modulo 7. Questo vuol dire che 2 x4 –k 7 = 1. E noi sappiamo che questo risultato (se si ricordano le oche e i conigli) è sempre possibile solo se 4 e 7 hanno MCD =1 ovvero sono primi fra loro. Per esempio 3 a- k 15 =1 non è possibile perché 3 e 15 non sono primi fra loro. Ma il fatto che due numeri sano inversi vuol dire che il loro prodotto diviso per p dà resto 1.

Possiamo trionfalmente dire che "l'aritmetica modulo n è un anello commutativo con un elemento unità" Se poi il modulo n è un numero primo, allora l'aritmetica modulo n è un "campo".

Ma ora entra in scena Wilson, che fece un'interessante scoperta (forse si illudeva che con essa la ricerca dei numeri primi sarebbe stata facilitata, ma se ci riflettete un momento vedete che a prima vista fu invece enormemente complicata, per colpa di quel malefico fattoriale che troveremo).

(Teorema di Wilson) Se p è primo, allora

$$(p-1)! \equiv -1 \ (mod\ p)$$

L'inverso esiste perché p è primo e qualsiasi numero più piccolo di p è comunque primo con p.
Perché l'inverso esista deve essere:

$$A\ A^{-1} - k\ p = 1$$

E il numero A^{-1} cercato proviene al fatto che A e p sono primi fra loro (questo deriva dalla considerazione del MCD di due numeri primi fra loro e si è visto col nome di lemma di Bézout in http://dainoequinoziale.it/scienze/matematica/2017/10/30/vardiv.html)
Abbiamo p-1 numeri, numero pari che possiamo dividere in coppie di inversi, il cui prodotto, diviso per p dà resto 1. Tuttavia ci sono due numeri eccezionali che sono 1 e p-1, che moltiplicati l'un per l'altro sono congruenti a -1 ($p-1 \equiv -1 \ (mod\ p)$)

Non ce ne possono essere altri, perché i prodotti di tutte le altre cpppie sono congruenti a 1 . In conclusione, tutte le coppie divise per p danno resto 1 (perché p è primo) ad eccezione della coppia 1 e p-1 il cui prodotto dà resto -1- Da cui,

$$(p-1)! \equiv -1 \ (mod\ p)$$

Abbiamo ora il **"Lemma di Lagrange":**
Un numero primo della forma p = 4n+1 divide m^2+1 essendo m un numero naturale.

Dimostrazione: Supponiamo di applicare il teorema di Wilson al numero primo p= 4n+1, per il quale p-1= 4n.
Abbiamo:

$$-1 \equiv 1 \text{ x } 2 \text{ x } 3 \text{ x } 4 \ldots \text{ x } 4n \ (mod\ p) \equiv$$
$$(1 \text{ x } 2 \text{ x } 3 \ldots \text{x } 2n)(\text{x } (2n+1)\text{x } (2n+2)\text{x } (2n+3) \ldots \text{x } (4n)) \ (mod\ p)$$

Ma abbiamo che

$$2n+1 \equiv -2n \ (mod\ p)$$

$$2n+2 \equiv -2n+1 = -(2n-1) \ (mod\ p)$$

Se questo sembra strano, si ricordi che 2n+1 è il resto della divisione di 2n +1 per p, 2n è il resto della divisione di 2n per p. La somma dei resti è 0, perché 2n+1 +2n = 4n+1 , che diviso per p = 4n+1 dà 0, da cui il risultato che un termine è il negativo dell'altro. E ciò vale per tutte le altre coppie di resti.

Abbiamo quindi, mettendo insieme

$$-1 \equiv (1\ x\ 2\ x\ 3 \ldots x\ 2n)^2 \ (mod\ p)$$

Prendendo m = 2n!, abbiamo l'importante risultato:

$$m^2 = -1 \ (\text{mod p})$$

Cioè che p divide $m^2 + 1$.

Giungiamo così finalmente al **teorema di Fermat "dei due quadrati":** Se p = 4n+1 , è primo in **Z** (campo dei numeri naturali) , allora

$$p = a^2 + b^2 \quad \text{per qualche a, b in } \mathbf{Z}.$$

Dimostrazione: dato p, si supponga che esso divida m^2+1, come vuole il Lemma di Lagrange. Ma

$$m^2 + 1 = (m + i)(m - i)$$

Quindi, anche se p divide m^2+1, non divide nessuno dei due fattori, perché la divisione non produce un intero gaussiano. Infatti, se p non è un'unità, la parte immaginaria del quoziente è 1/p, che non è intera.

Quindi p non è un primo Gaussiano, perché se p fosse un numero primo di cui si sa che divide il prodotto αβ, esso dovrebbe dividere o α o β.

Non essendo primo, è dato dal prodotto di almeno due fattori:

$$p = (a + bi)\ z$$

I due fattori sono quindi interi gaussiani con norma minore della norma di p, che è p^2, essendo p reale. Il complesso coniugato di p (che è reale) è eguale a

$$p = (a - bi)\overline{z}$$

e la Norma di p è

$$p^2 = (a^2 + b^2)\, z\overline{z}$$

In cui le due norme sono entrambe maggiori di 1.
Ma (come si è dimostrato) anche nel campo degli interi Gaussiani vale il teorema dell'unica fattorizzazione di un intero, per cui $p^2 = p \times p$, e $p = a^2 + b^2$. (Cdd)

Naturalmente, non ogni numero dispari non primo della forma 4n+1 è scomponibile nella somma di due quadrati, come si vede subito, per esempio usando il primo di essi, che è 9. E similmente non solo i numeri primi della forma 4n+1 sono scomponibili nella somma di due quadrati: 85 è della forma 4n +1, è dato dalla somma $9^2 + 2^2$, ma non è primo.

Conclusione

Così termina la nostra escursione in una regione della matematica di cui molti non sospettano neppure l'esistenza. Penso anche che questa regione non abbia alcun contatto diretto col mondo reale: ma è un difetto? Un mio amico mi diceva: ho altre cose da fare che studiare i numeri primi di Gauss. Ne chiesi l'elenco. Mentre me le diceva si rendeva pian piano conto che questo mondo dei numeri primi Gaussiani ingigantiva, mentre le sue occupazioni inderogabli rimpicciolivano, pur senza perdere la loro urgenza. Questo è purtroppo il nostro destino: vivere circondati da un mondo di cose interessanti, che farebbero lavorare il cervello, e non avere il tempo per farlo. Un vero supplizio di Tantalo. L'unica soluzione è non pensarci, non volerci pensare.