Primi proprio primi

Il concetto di numero primo (naturale) p si estende con una certa semplicità al campo dei numeri complessi. Anche qui è possibile definire dei numeri primi g che non hanno fattori tranne quelli ovvi e cioè l'unità e sé stessi.

Ogni numero primo di questa natura viene detto gaussiano, per ragioni più che comprensibili[1]. Scriveremo quindi

$$g = x + iy$$

Il modulo del numero $|g|$ non può essere un numero composto, pertanto per trovare i primi gaussiani dobbiamo partire dai numeri primi naturali. Ora, a parte 2, i numeri primi sono tutti dispari e quindi divisibili in due classi distinte tra loro: tale suddivisione è della massima importanza

- primo tipo: $g_1 = 4k + 3$;
- secondo tipo: $g_2 = 4k + 1$.

Solo i numeri del secondo tipo sono scomponibili nel prodotto di due soli primi gaussiani, in quanto sono esprimibili come somma di due quadrati in un solo modo:

$$g_2 = a^2 + b^2 = (a + ib)(a - ib)$$

Naturalmente la scomposizione è unica se non si considerano le unità che, nel nostro caso, sono ben quattro ovvero

$$1, -1, i, -i$$

Infatti

$$(a + ib)(a - ib) = (-a - ib)(-a + ib) = (b - ia)(b + ia) = (-b + ia)(-b - ia)$$

supporremo quindi, senza perdere di generalità, che sia

$$0 < a \leq b$$

Il numero primo eccezionale è l'unico pari, ma, dal fatto che $2=1^2+1^2$, abbiamo subito la sua scomposizione in primi gaussiani:

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

[1] K. F. Gauss, *Theoria residuorum biquadraticorum (commentatio secunda)*, art. 33 (1828) in *Commentationes societatis regiae Gottingensis recentiores*, vol. VII (1832). La Commentatio prima era uscita nel 1828.

Il primo successivo del secondo tipo è

$$5 = 1 + 4 = (1 + 2i)(1 - 2i)$$

Tutti gli altri sono dispari; scrivo solo i più piccoli:

$$13 = 4 + 9 = (2 + 3i)(2 - 3i)$$

$$17 = 1 + 16 = (1 + 4i)(1 - 4i)$$

$$29 = 4 + 25 = (2 + 5i)(2 - 5i)$$

Naturalmente in ciascun primo gaussiano la parte reale e quella immaginaria sono prime tra loro.

È possibile rappresentare tutti i primi gaussiani nel piano che porta il nome del Maestro. Se ricordiamo cha a ciascun valore ne sono associati altri 7 ottenuti mediante simmetria di riflessione rispetto ai due assi e rotazione di 90° della figura risultante, abbiamo la seguente figura per tutti i primi naturali inferiore a 1000 (fig. 1).

In essa si distinguono aree prive di numeri primi, se le evidenziamo opportunamente otteniamo la fig. 2.

Osservando attentamente, notiamo che i numeri sono situati lungo rette tutte parallele alla bisettrice del primo e terzo quadrante (i punti appartenete alla stessa retta sono rappresentati col medesimo colore).

Avremo quindi che, avendo a, b parità opposta, è

$$b = a + (2k + 1)$$

che vale per tutti i primi naturali maggiori di 2.

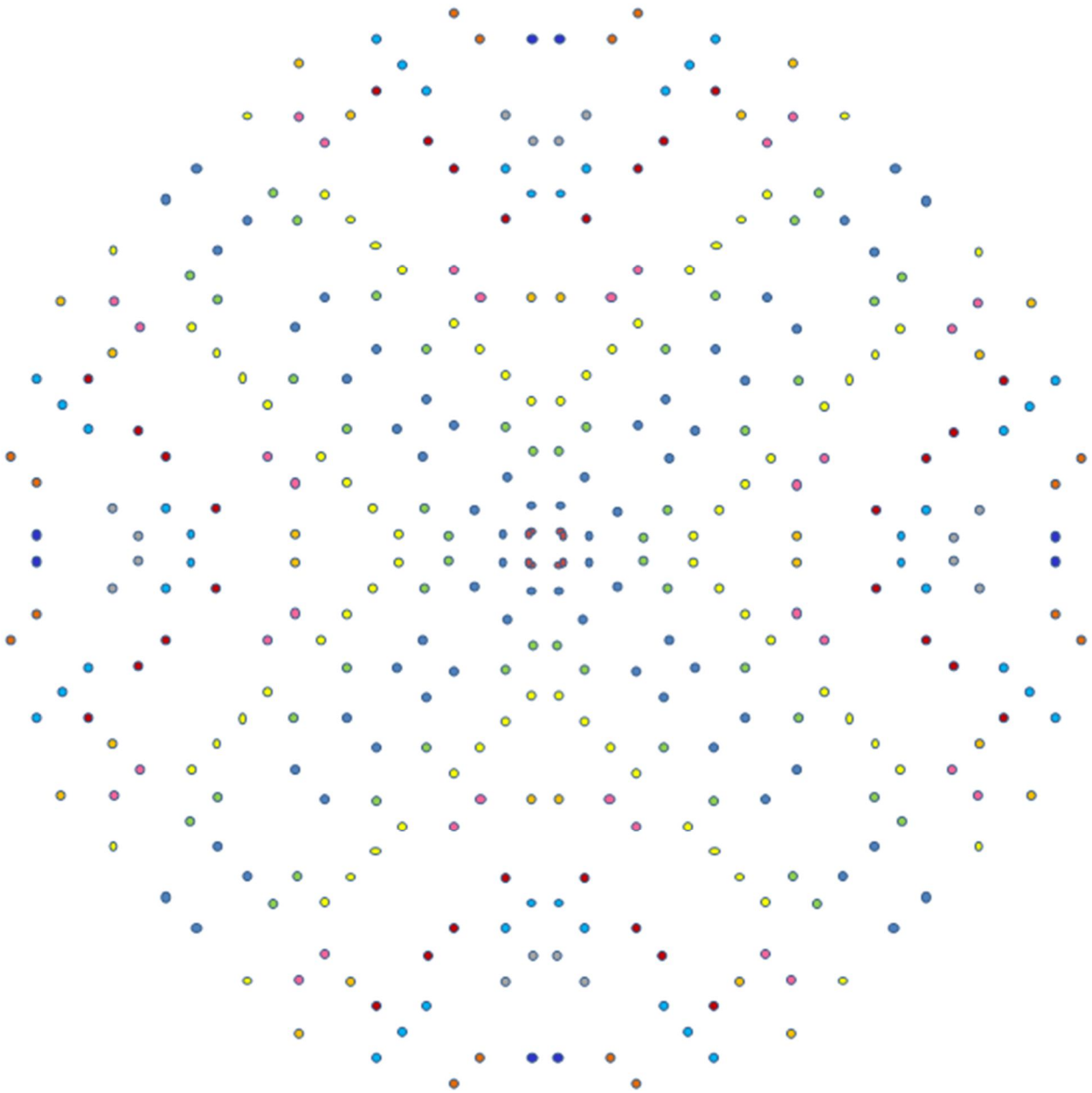


Fig. 1: La rosa dei primi gaussiani e dei loro correlati

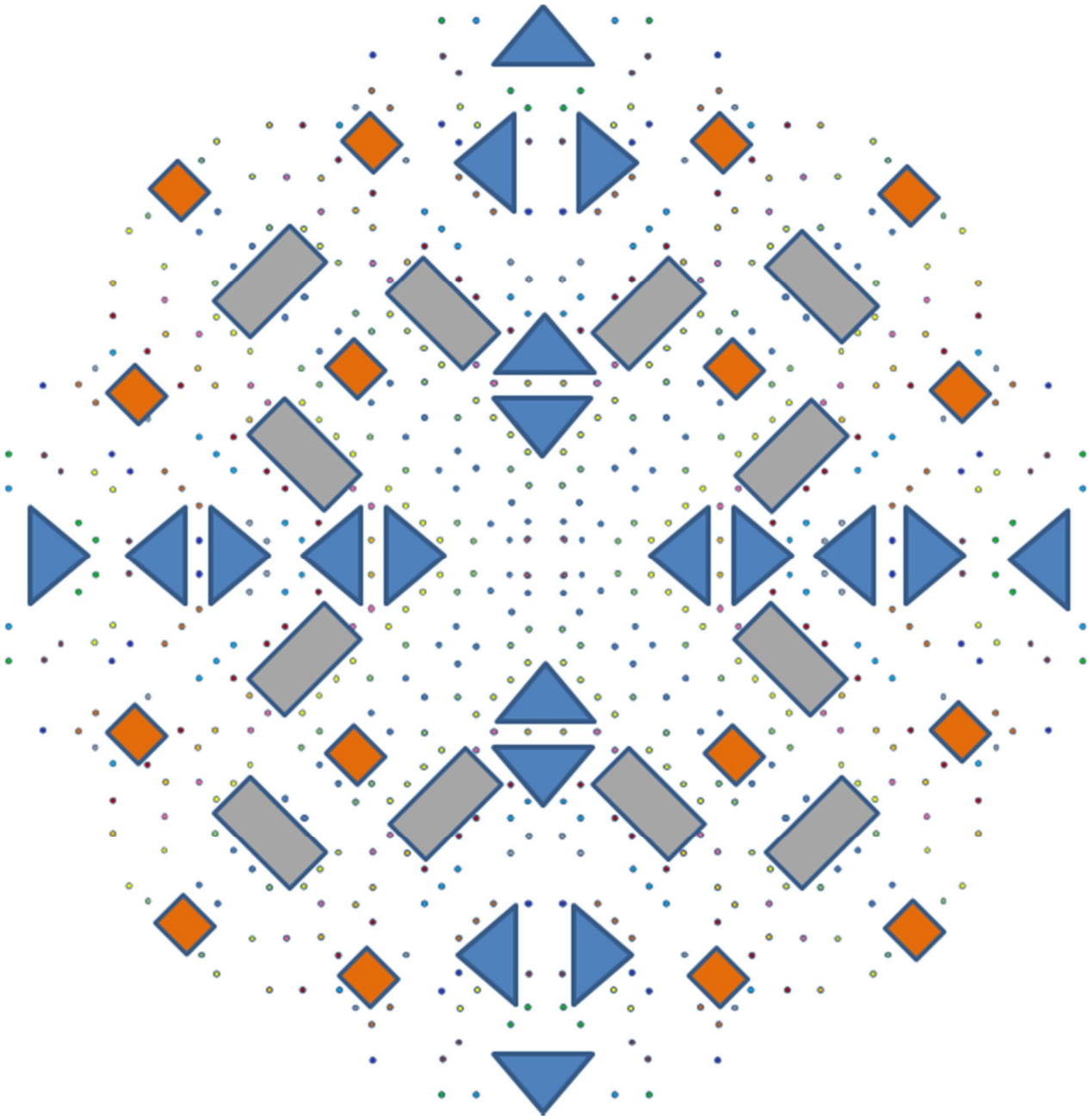
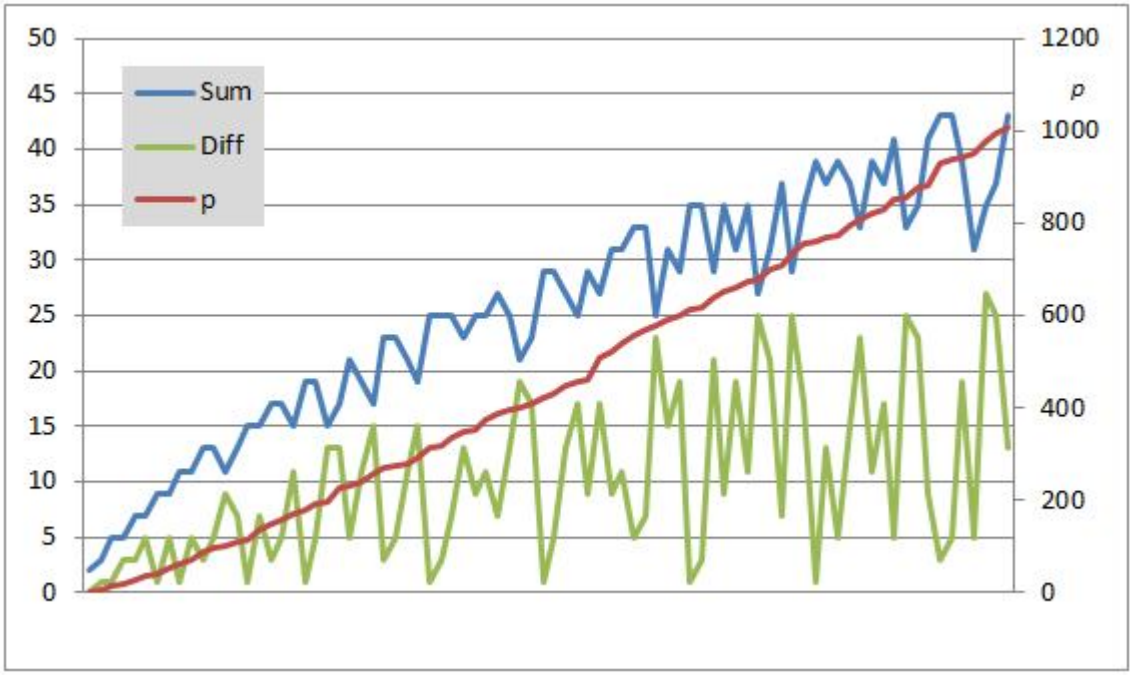


Fig. 2: Le zone più estese prive di primi gaussiani sono colorate

Dopo averne apprezzato l'elevato grado di simmetria e quindi di godibilità anche grafica, si possono condurre alcune analisi sul comportamento dei primi gaussiani, limitandone lo studio al primo quadrante.

Dato un qualsiasi primo gaussiano $a + ib$ si possono studiare i due numeri

$$s = a + b, \quad d = b - a$$

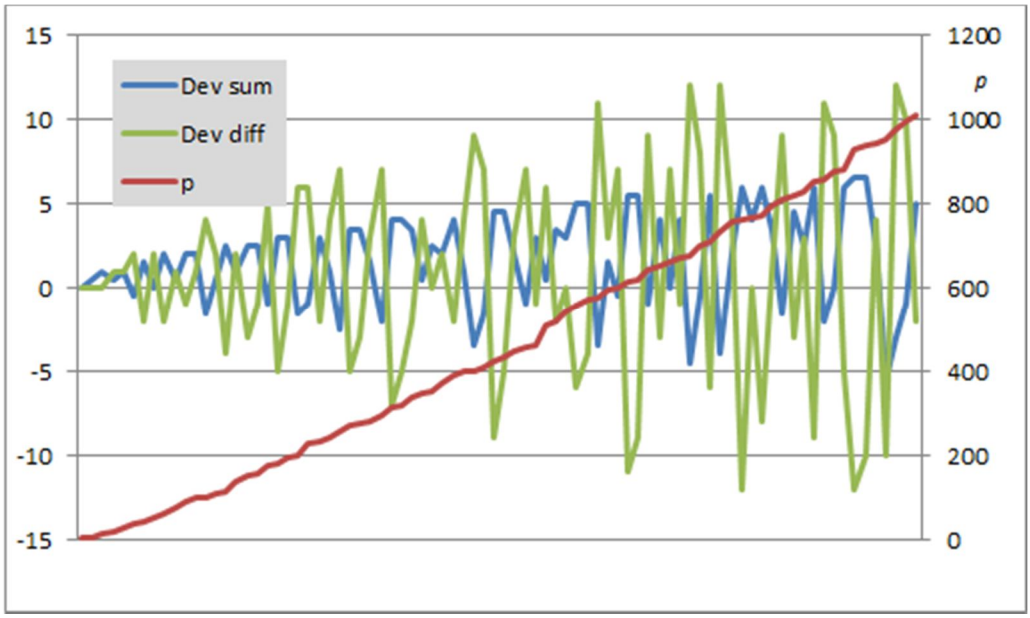


Andamento della somma e della differenza tra parte immaginaria e parte reale

Per ciascun primo abbiamo i seguenti limiti per i due suddetti valori:

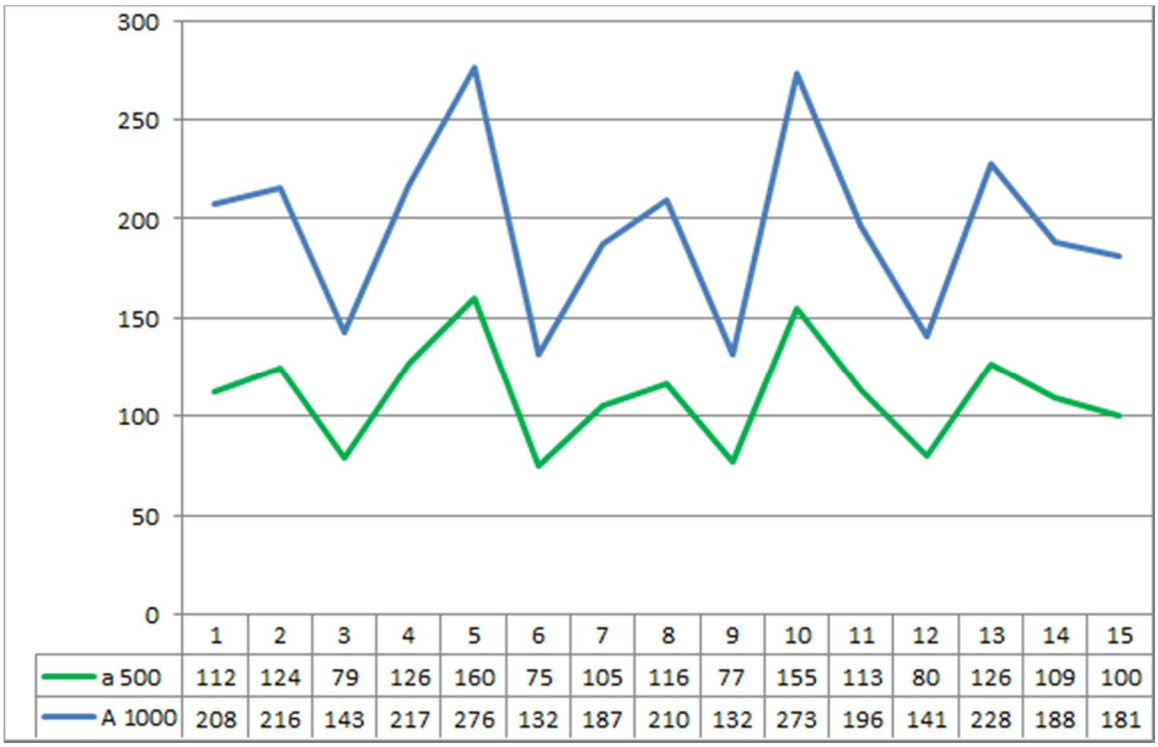
$$1 + [\sqrt{n}] \leq s \leq 2[\sqrt{n}]$$

$$1 \leq d \leq [\sqrt{n}] - 1$$



Scostamento di somma e differenza rispetto al valore medio

Se contiamo quanti primi gaussiani hanno la forma $n + it$ per i primi 15 valori della componente reale e per i primi 500 e i primi 1000 di quella immaginaria otteniamo il seguente andamento



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a 500	112	124	79	126	160	75	105	116	77	155	113	80	126	109	100
A 1000	208	216	143	217	276	132	187	210	132	273	196	141	228	188	181

Al raddoppiare del valore della componente immaginaria la quantità di primi gaussiano cresce approssimativamente di un fattore $1{,}8 \cong \sqrt{\pi}$, che è abbastanza costante per tutti i valori di n.

Tutto questo è basato sulle radici dell'equazione fondamentale

$$x^4 = 1$$

L'equazione binomia di terzo grado

$$x^3 = 1$$

ha radici

$$1, \quad \omega = \frac{-1 + i\sqrt{3}}{2}, \qquad \omega^2 = \frac{-1 - i\sqrt{3}}{2}$$

il cui prodotto vale chiaramente 1. Alla stregua di quanto visto, è lecito chiedersi se tali valori possano generare i numeri primi estesi in tal senso, il cui prodotto corrisponda ad un numero primo naturale.

Cerchiamo quindi dei numeri tali che

$$(a + k\omega)(b + m\omega^2) = p$$

Affinché il prodotto sia un numero reale è necessaria la condizione

$$am = bk \quad \text{cioè } \frac{a}{b} = \frac{k}{m}$$

con il che abbiamo senz'altro la soluzione corrispondente a $k = m = 1$

$$\left(\frac{\sqrt{4p-3}+1}{2} + \omega\right)\left(\frac{\sqrt{4p-3}+1}{2} + \omega^2\right) = p$$

Affinché la parte reale rappresenti un intero il radicando, che è un numero dispari, deve essere un quadrato:

$$4p - 3 = (2u + 1)^2$$

ed infine

$$p = u^2 + u + 1 \quad [1]$$

Quindi nell'estensione $(1,\ \omega,\ \omega^2)$ i primi naturali della forma [1] ammettono seguente la scomposizione in fattori primi:

$$p = (u + 1 + \omega)(u + 1 + \omega^2)$$

Tra i primi 10000 valori di u ve ne sono 1410 che soddisfano la condizione; ecco i primi

$$3 = (1 + \omega)(1 + \omega^2)$$

$$7 = (2 + \omega)(2 + \omega^2)$$

$$13 = (3 + \omega)(3 + \omega^2)$$

p è indifferentemente congruo a 1 o a 3 (mod 4).

Possiamo non considerare l'equazione

$$x^2 - \sqrt{5}x + 1 = 0$$

le cui radici sono la sezione aurea φ e il suo inverso Φ.

Allora cerchiamo di risolvere il problema

$$(r + k\varphi)(s + m\Phi) = p$$

Per essa deve valere la condizione

$$ks + mr = 0$$

Imponendo ora che sia $k = -m = 1$ deve valere l'ulteriore condizione che

$$4p + 5 = (2u + 1)^2$$

ed infine

$$p = u^2 + u - 1 \quad [2]$$

Quindi nell'estensione $(1, \varphi, \Phi)$ i primi naturali della forma [2] ammettono seguente la scomposizione in fattori primi:

$$p = (u + 1 + \varphi)(u + 1 - \Phi)$$

Tra i primi 10000 valori di u ve ne sono 2187 che soddisfano la condizione; i primi essendo

$$5 = (3 + \varphi)(3 - \Phi)$$

$$11 = (4 + \varphi)(4 - \Phi)$$

$$19 = (5 + \varphi)(5 - \Phi)$$

Anche qui p è indifferentemente congruo a 1 o a 3 (mod 4).

Va notato che il caso precedente della cubica e questo fibonacciano rappresentano due primi differenti di due unità: abbiamo quindi solo primi gemelli.

Quanto detto vale in genere per l'equazione

$$x^2 - \alpha x + 1 = 0$$

le cui radici chiamiamo r_1 e r_2.

Allora cerchiamo di risolvere il problema

$$(r + kr_1)(s + mr_2) = p$$

La condizione di realtà vuole che sia

$$ks = mr$$

Imponendo ora che sia $k = m = 1$ otteniamo

$$p = u^2 + \alpha u + 1 \quad [3]$$

che è valida se α è un intero.

In tale specifico caso quindi nell'estensione $(1,\ r_1, r_2)$ i primi naturali della forma [3] ammettono seguente la scomposizione in fattori primi:

$$p = (u + r_1)(u + r_2)$$

Se α è un numero razionale $\frac{t}{v}$, allora occorre imporre la condizione che sia $u = kv$. Se invece α è un numero algebrico occorre che il radicando sia un quadrato perfetto, come visto.