Riv. Mat. Univ. Parma (4) 11 (1985), 317-323

NATALIA BALDISSERRI (*)

Sulle coppie di residui consecutivi negli interi di Gauss (**)

1 – J. H. Jordan ha studiato in [**5**]$_2$ alcuni problemi riguardanti coppie di residui di potenze (in particolare quadratici) consecutivi, nell'anello degli interi di Gauss $Z[i]$, modulo un numero primo π dell'anello ($\neq 1+i$). Egli chiama consecutivi due numeri α, β interi di Gauss quando $|\alpha - \beta| = 1$; una coppia di residui consecutivi è pertanto del tipo $(\varrho,\ \varrho+1)$ oppure $(\varrho,\ \varrho+i)$. Ha studiato inoltre ([**3**]$_{1,2}$, [**6**]) sistemi completi o ridotti di resti, secondo un dato modulo, che indicheremo SCR o SRR rispettivamente, in $Z[i]$ e la distribuzione dei resti quadratici modulo un numero primo q di $Z[i]$ che sia primo anche in Z (e quindi della forma $q = 4k+3$). I problemi studiati da Jordan in [**5**]$_2$ sono gli analoghi di problemi ampiamente studiati nel caso dell'anello Z degli interi razionali ([**2**], [**5**]$_1$, [**7**]) per coppie o sequenze di residui consecutivi (1). In questa nota determiniamo il numero di coppie di resti quadratici $\varrho \neq 0$, modulo un primo $\pi \in Z[i]$ ($\pi \neq 1+i$) contenuti in certi SRR modulo π. È opportuno a questo proposito fare alcune osservazioni: nel caso dell'anello degli interi razionali Z, il numero $N(p)$ delle coppie di residui quadratici, modulo un numero primo p dispari, contenuti nel sistema che diremo *naturale* $\{1, 2, \ldots, p-1\}$ è da tempo noto [**4**], [**9**] e vale: $N(p) = (p-5)/4$ se $p = 4k+1$, $N(p) = (p-3)/4$ se $p = 4k+3$. È ovvio che se invece del sistema naturale si considera un diverso SRR il numero delle coppie di resti consecutivi potrà non essere più uguale ad $N(p)$ ed in effetti può anche ridursi

(*) Indirizzo: Dipartimento di Matematica, P.za di Porta S. Donato 5, 40127 Bologna, Italy.

(**) Ricevuto: 9-XII-1983.

(1) G. Pellegrino in [**8**] ha studiato questioni analoghe per terne di residui quadratici consecutivi in un campo finito $F(q)$ con $q = p^n$ dispari. Ma egli chiama consecutivi soltanto elementi della forma $(z, z+1)$, dove 1 è l'elemento unità di $F(q)$.

a zero. Si noterà, ad esempio, che nel SRR $\{-(p-1)/2, \ldots, -1, 1, \ldots, (p-1)/2\}$ il numero delle coppie è ancora $N(p)$ se $p = 4k+3$, mentre se $p = 4k+1$ può ridursi a $N(p)-1$, secondo che la coppia $(2k, 2k+1)$ sia o non sia una coppia di resti. È probabile che il numero delle coppie di resti consecutivi appartenenti a un SRR risulti massimo [2] nel caso del SRR naturale $\{1, \ldots, p-1\}$. Ciò premesso risulta dunque chiaro che anche nel caso di $Z[i]$ di cui ci occupiamo il numero delle coppie $(\varrho, \varrho+1)$, $(\varrho, \varrho+i)$ di residui quadratici consecutivi modulo un primo $\pi \neq (1+i)$ va riferito ad un SRR modulo π. Qui prenderemo in considerazione i SRR seguenti (che verranno definiti con precisione in **2, 3**).

(1) Se $\pi = q(=4k+3)$, la norma vale $N(\pi) = q^2$ e un SCR ha q^2 elementi. Considereremo i due sistemi ([**3**]$_2$, [**6**]) formati rispettivamente dai numeri interi $\alpha \in Z[i]$ non nulli $(\alpha = x+iy)$ con $|x| \leqslant (q-1)/2$, $|y| \leqslant (q-1)/2$ oppure con $0 \leqslant x \leqslant q-1$, $0 \leqslant y \leqslant q-1$; quest'ultimo sistema è analogo al sistema naturale in Z ricordato sopra.

(2) Se $\pi = a+ib$, $N(\pi) = p = 4k+1$, considereremo quattro tipi di SRR, tre dei quali considerati da Jordan in [**6**]:

(a) il SRR $\{1, 2, \ldots, p-1\}$ che notoriamente è SRR sia modulo p in Z, che modulo π in $Z[i]$; ma in quest'ultimo caso non verrà considerato come sistema naturale;

(b) il sistema chiamato *Utah* in [**6**] che indicheremo con SRRU;

(c) il sistema indicato in [**3**]$_1$, che soddisfa una proprietà di minimo e che indicheremo con SRRM;

(d) un sistema che qui introduciamo, che chiameremo *naturale* e che indicheremo con SRRN.

Calcoleremo il numero di coppie di residui quadratici, modulo π primo di $Z[i]$, consecutivi $(\varrho, \varrho+1)$, $(\varrho, \varrho+i)$ appartenenti ad alcuni dei SRR indicati. Per i tipi (1) e (b) del caso (2) otterremo delle formule esplicite nelle quali figura il simbolo di Legendre usuale (relativo a Z); per gli altri tipi daremo soltanto esempi numerici al fine di illustrare quanto segue: è chiaro che nel caso $\pi = a+ib$ per il sistema $\{1, \ldots, p-1\}$ il numero è $(p-5)/4$ (come per $p = N(\pi) \in Z$ in Z) ma per gli altri SRR il numero è sempre più grande se $p > 5$, tuttavia il numero massimo non si ha sempre per un SRR di tipo determinato.

---

[2] Questa affermazione andrebbe dimostrata, ma qui non ce ne occuperemo.

Naturalmente il procedimento qui seguito si può usare anche per determinare le coppie consecutive di non residui, o le coppie consecutive residuo-non residuo o non residuo-residuo.

Nel seguito indicheremo sempre con N il numero delle coppie di resti quadratici consecutivi contenuti in un certo SRR e con $[\alpha/\pi]$ il simbolo di Legendre in $Z[i]$.

2 - Sia $\pi = q = 4k+3$, primo di Z e quindi di $Z[i]$. Il numero degli elementi di un SCR è $N(q) = q^2$ e i SCR mod π che prenderemo in esame sono

(a) $\{x+yi;\ |x|,\ |y| \leqslant (q-1)/2\}$, (b) $\{x+yi;\ 0 \leqslant x \leqslant q-1,\ 0 \leqslant y \leqslant q-1\}$.

Si dimostra che *il numero N delle coppie di residui consecutivi* mod $q = 4k+3$ (*primo di Z*) *in* $Z[i]$ *relativamente a un* SRR *di tipo* (a) *è dato da*

$$N = \frac{(q-1)^2}{2} - 3 + \left(\frac{k+1}{q}\right), \tag{1}$$

relativamente a un SRR *di tipo* (b) *è dato da*

$$N = \frac{(q-1)^2}{2}. \tag{2}$$

Sappiamo [**3**]$_2$ che $[z/q] = [iz/q]$ e che $[(a+ib)/q] = [(b+ai)/q]$, quindi, sia per determinare (1) che per determinare (2), basta contare il numero delle coppie di residui del tipo $(z, z+1)$, visto che questo risulta uguale al numero delle coppie del tipo $(z, z+i)$. Notiamo poi che

$$\{[z/q]+1\}\{[(z+1)/q]+1\} = \begin{cases} 4 & \text{se } z,\ z+1 \text{ sono entrambi residui} \\ 0 & \text{se } z,\ z+1 \text{ non sono entrambi residui} \\ 2 & \text{se } z = 0 \quad \text{oppure } z = -1. \end{cases}$$

Vale allora, contando successivamente le coppie situate su ogni retta parallela all'asse reale ed escludendo lo zero

$$\begin{aligned} 2N = {} & \sum_{z \in SCR(q)} \{[\tfrac{z}{q}]+1\}\{[\tfrac{z+1}{q}]+1\} - \{[-\tfrac{1}{q}]+1\}\{[\tfrac{0}{q}]+1\} \\ & - \{[\tfrac{0}{q}]+1\}\{[\tfrac{1}{q}]+1\} - \{[\tfrac{(q-1)/2}{q}]+1\}\{[\tfrac{(q+1)/2}{q}]+1\} \\ & - 2\sum_{h=1}^{(q-1/2)} \{[\tfrac{(q-1)/2+hi}{q}]+1\}\{[\tfrac{(q+1)/2+hi}{q}]+1\}. \end{aligned}$$

A questo punto teniamo presente che $[r/q] = 1$ se $r \in Z([\mathbf{3}]_2)$ e che si ha

$$(3) \qquad \sum_{z \in SCR(q)} \{[\frac{z}{q}] + 1\} \{[\frac{z+1}{q}] + 1\} = \sum_{z \in SCR(q)} \{[\frac{z(z+1)}{q}] + 1\};$$

(3) rappresenta il numero dei punti propri della conica irriducibile $\omega^2 = z(z+1)$ in $F(q^2)$ (3) e quindi vale $q^2 - 1$ [**10**].

Inoltre poichè $[\mathbf{3}]_2$

$$[\frac{a+ib}{q}] = (\frac{a^2+b^2}{q}) \quad \text{e} \quad ([\mathbf{4}],\ [\mathbf{9}]) \sum_{h \in SCR} (\frac{h^2+k+1}{q}) = -1\,,$$

si ottiene facilmente

$$\sum_{h=1}^{(q-1)/2} \{[\frac{(q-1)/2 + hi}{q}] + 1\} \{[\frac{(q+1)/2 + hi}{q}] + 1\} = q - 2 - (\frac{k+1}{q})\,,$$

e quindi la (1). Esempi: per $q = 3$, $q = 7$, $q = 19$ si ottiene rispettivamente $N = 0$, $N = 16$, $N = 160$.

Per ottenere la (2), si considera che in questo caso vale

$$2N = \sum_{z \in SCR} \{[\frac{z}{q}] + 1\} \{[\frac{z+1}{q}] + 1\} - \{[\frac{0}{q}] + 1\} \cdot \{[\frac{1}{q}] + 1\} - \sum_{h=0}^{q-1} \{[\frac{q-1+hi}{q}] + 1\} \{[\frac{q+hi}{q}] + 1\}\,.$$

Con semplici passaggi, tenendo presente che per $h \neq 0$ $[hi/q] = 1$ $[\mathbf{3}]_2$ e che $\sum_{h=1}^{q-1} (h^2+1)/q = -2$ [**4**], [**9**], si ricava la (2).

Esempi: per $q = 3, 7, 19$ si ottiene rispettivamente $N = 2$, $N = 18$, $N = 162$.

3 - Sia $\pi = a + ib$, $N(\pi) = p = 4k + 1$ primo di Z e non è restrittivo supporre a, b positivi a dispari, b pari. Il numero degli elementi di un SCR mod π

---

(3) Infatti per tutti i valori di z che danno una rappresentazione di $F(q^2)$ (come sono quelli di (a)), quelli che rendono il prodotto $z(z+1)$ quadrato ($\neq 0$) danno due punti della conica, quelli che lo rendono non quadrato non danno alcun punto, quelli tali che $z(z+1) = 0$ danno un punto. D'altra parte le tre classi di valori di z si hanno rispettivamente per $[z(z+1)/q] = 1, -1, 0$.

è $N(\pi) = p$ e i SCR mod π che prenderemo in esame sono:

(c) $\{0, 1, 2, \ldots, p-1\}$ che chiameremo SCR *razionale* e indicheremo con SCRR.

(d) L'insieme $A \cup B$, dove

$$A = \{x + yi;\ x, y \in Z,\ 0 \leqslant x \leqslant a-1,\ 0 \leqslant y \leqslant a-1\}\ ,$$

$$B = \{x + yi;\ x, y \in Z,\ a \leqslant x \leqslant a+b-1,\ 0 \leqslant y \leqslant b-1\}\ .$$

In [**6**] tale SCR viene indicato con nome di *Utah* e lo indicheremo con SCRU.

(e) L'insieme C degli interi di Gauss interni al quadrato di vertici $(\pm 1 \pm i)(\pi/2)$. Tale sistema di resti soddisfa la proprietà seguente: dato D, anch'esso SCR mod π, si ha $\sum_{\alpha \in C} |\alpha| \leqslant \sum_{\beta \in D} |\beta|$; tale SCR lo chiameremo *minimo* e lo indicheremo con SCRM.

(f) L'insieme degli interi di Gauss interni al quadrato di vertici $0, \pi$, $(1-i)\pi$, $-i\pi$. Tale SCR lo chiameremo *naturale* e lo indicheremo con SCRN.

Per (c), (d), (e) vedi [**3**]$_1$, [**6**] e non ci sono difficoltà per stabilire (f).

Naturalmente per SCRR si ha $N = (p-5)/4$, come per $p \in Z$.

Ponendo $\{(x/p) + 1\}\{(y/p) + 1\} = f(x, y)$, si dimostra che *il numero N delle coppie di residui consecutivi* mod $\pi = a + ib (N(\pi) = a^2 + b^2 = p = 4k+1$ *primo in Z) in $Z[i]$ relativamente al* SRRU *è dato da*

$$(4)\qquad 4N = 2p - 5 - (-1)^{p-1/4} - \sum_{h=0}^{b-1} f(ab - b^2 - a + hb,\ ab - b^2 + hb)$$

$$- \sum_{h=b}^{a-1} f(hb - a - b^2,\ hb - b^2) - \sum_{l=0}^{a-1} f(al - ab - b,\ l + b) - \sum_{l=0}^{a+b-1} f(al + b^2 - b,\ l - a)$$

nel caso $a > b$, e da

$$(5)\qquad 4N = 2p - 5 - (-1)^{p-1/4} - \sum_{h=0}^{b-1} f(ab - b^2 - a + hb,\ ab - b^2 + hb)$$

$$- \sum_{l=0}^{a-1} f(al + ab - b,\ l + b) - \sum_{l=a}^{a+b-1} f(al + b^2 - b,\ l - a)$$

nel caso $a < b$.

Le dimostrazioni ricalcano quelle precedenti, tenendo presente che, essendo a

dispari, $[(r+is)/\pi] = [(ar+bs)/p]$ [1] e in particolare

$$[\frac{i}{\pi}] = (\frac{b}{p}) = i^{2k} = (-1)^k = (-1)^{p-1/4}, \qquad [\frac{1}{\pi}] = (\frac{a}{p}) = 1 .$$

Da (4) segue subito che per il SRRU si ha

$$\frac{2p-5-(-1)^{p-1/4}}{4} - (2a+b) < N < \frac{2p-5-(-1)^{p-1/4}}{4},$$

e, poichè $p = a^2 + b^2$, ne discende che è sempre (per $p > 5$) valida la $N > (p-5)/4$ ossia che il SRRU contiene più coppie di residui che il sistema SRRR.

Analogamente si può procedere partendo da (5).

Si noti che, nel caso $a = 1$, $\pi = 1 + 2gi$, $p = 1 + 4g^2$, il SCRN coincide con SCRU; infatti in tal caso l'insieme A si riduce allo zero e l'insieme B al quadrato di vertici 1, $2g$, $2g + (2g-1)i$, $1 + (2g-1)i$. Questo risulta interno al quadrato di vertici $0, \pi, (1-i)\pi, -i\pi$ e gli insiemi degli interi di Gauss contenuti in entrambi i quadrati vengono a coincidere. La (4) si riduce a

$$4N = 2p - 5 - (-1)^{g^2} - \sum_{h=0}^{2g-1} \{(\frac{2g}{p})(\frac{h-1}{p}) + 1\} \{(\frac{2g}{p})(\frac{h+1-2g}{p}) + 1\}$$

$$- \sum_{l=1}^{2g} \{(\frac{1-2g-1}{p}) + 1\} \{(\frac{l-1}{p}) + 1\} .$$

4 – Abbiamo applicate le formule trovate ad alcuni casi numerici e per questi abbiamo calcolato anche direttamente il numero dalle coppie di residui consecutivi contenuti nei SRR dei tipi M, N. I risultati sono esposti nella seguente tabella.

p	SRRR	SRRU	SRRM	SRRN
5	0	0	0	0
13	2	2	2	4
17	3	4	4	4
29	6	9	10	8
37	8	16	12	16
41	9	13	12	12
53	12	22	21	20
61	14	24	24	24
73	17	26	32	24

Come si vede per il SRRR N ha il valore minimo, ma il valore massimo di N non corrisponde sempre allo stesso SRR.

Bibliografia

[1] L. BIANCHI, *Lezioni sulla teoria dei numeri algebrici*, Spoerri Enrico, Pisa 1923.

[2] R. L. GRAHAM, *On quadruples of consecutive K-th power residues*, Proc. Am. Math. Soc. **15** (1964), 196-197.

[3] N. R. HARDMAN and J. H. JORDAN: $[\cdot]_1$ *A minimum problem connected with complete residue system in the Gaussian integers*, Amer. Math. Monthly, 74, **5** (1967), 559-561; $[\cdot]_2$ *The distribution of quadratic residues in fields of order* p^2, Math. Mag. **42** (1969), 12-17.

[4] H. HASSE, *Vorlesungen über Zahlentheorie*, Springer-Verlag, Berlin-Göttingen-Heidelberg 1954.

[5] J. H. JORDAN: $[\cdot]_1$ *Pairs of consecutive power residues or non-residues*, Can. J. Math. **16** (1964), 310-314; $[\cdot]_2$ *Consecutive residues or non-residues in the Gaussian integers*, Journal Number Theory **1** (1969), 477-485.

[6] J. H. JORDAN and C. J. POTRATZ, *Complete residue systems in the Gaussian integers*, Math. Mag. **38** (1965), 1-12.

[7] D. M. LEHMER, E. LEHMER and W. H. MILLS, *Pairs of consecutive power residues*, Can. J. Math. **15** (1963), 172-177.

[8] G. PELLEGRINO, *Sui campi di Galois, di ordine dispari, che ammettono terne di elementi quadrati (non quadrati) consecutivi*, Boll. Un. Mat. Ital. (5) **17** B (1980), 1482-1495.

[9] A. R. RAJWADE, *Cyclotomy-A survey article*, Math. Student, 48, **1** (1980), 70-111.

[10] B. SEGRE, *Istituzioni di Geometria Superiore* (II), Istituto Matematico Guido Castelnuovo, Roma 1965.

Summary

In the Gaussian integers, we calculate the number of pairs of consecutive residues, as regards to various complete residue systems mod π, $\pi = q = 4k + 3$ *prime in Z, or* $\pi = a + ib$, $a^2 + b^2 = p = 4k + 1$, *prime in Z.*

* * *