Advanced – TdN 2

Titolo nota 04/09/2014

Richiami sugli interi di Gauss.

$$\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \qquad i^2 = -1$$

Negli interi di Gauss c'è una proprietà di fattorizzazione unica:
ogni elemento si scrive in "modo unico" come prodotto di fattori primi.
"unico": in realtà si possono cambiare:
- l'ordine dei fattori
- il fatto che ogni fattore può essere moltiplicato (o diviso) per un elemento invertibile

Elementi invertibili: In $\mathbb{Z}$: ± 1
In $\mathbb{Z}[i]$: $\pm 1, \pm i$.

Per determinare quali sono gli elementi primi in $\mathbb{Z}[i]$, basta fattorizzare in $\mathbb{Z}[i]$ gli usuali numeri primi.
Esempio: $70 = 2 \cdot 5 \cdot 7$ in $\mathbb{Z}$.
$70 = (1+i)(1-i)(2+i)(2-i)7$ in $\mathbb{Z}[i]$.

Idea: bisogna vedere se i numeri primi di $\mathbb{Z}$ rimangono primi (cioè non si fattorizzano ulteriormente in $\mathbb{Z}[i]$) oppure si fattorizzano ulteriormente.

Sia p un numero primo di $\mathbb{Z}$
Come si può eventualmente fattorizzare in $\mathbb{Z}[i]$?
$p = (a+bi)(c+di)$
Ci si riconduce (fondamentale!) ad un'uguaglianza fra interi.

$$p^2 = (a^2+b^2)(c^2+d^2)$$

Nota:
$$p^2 = \begin{cases} 1 \cdot p^2 \\ p \cdot p \\ p^2 \cdot 1 \end{cases}$$

Se $a^2+b^2=1$ oppure $c^2+d^2=1$, si ha
$a+bi$ oppure $c+id = \pm 1, \pm i$ (elemento invertibile)
$\rightarrow$ non c'è "vera" fattorizzazione.

L'unico caso serio è vedere se si può fare
$a^2+b^2 = c^2+d^2 = p$.
$p=2, \quad 2 = p = 1^2+1^2$
$p \equiv 3 \pmod 4$ impossibile
$p \equiv 1 \pmod 4$ non solo è possibile, ma si può sempre fare.

(Hint: $p \equiv 1 \pmod 4$ implica che -1 è un residuo quadratico modulo p. Quindi si può risolvere $x^2+1 \equiv 0 \pmod p$ $\quad x^2+1 = kp$ con $k < p$ $(k < p)$. $\quad (p^2/4+1 < p^2)$.
Da questo si deduce che è possibile risolvere $x^2+y^2 = kp$ e a sua volta $x^2+y^2 = p$).
(2° hint: Se $p \equiv 1 \pmod 4$ rimanesse primo in $\mathbb{Z}[i]$, questo vorrebbe dire che, ragionando modulo p, in $\mathbb{Z}[i]$ (modulo p) non ci sarebbero divisori di zero e quindi ogni polinomio di grado d avrebbe $\leq d$ radici.

Ora x^2+1 ha radici $\pm i$ e $\pm a$ dove $a^2 \equiv -1 \pmod p$ $\to$ 4 radici per un polinomio di grado 2 $\to$ assurdo).

Altri primi $\equiv 1 \bmod 4$

$13 = 3^2+2^2$, $17 = 4^2+1^2$, $29 = 5^2+2^2$, ...

Conclusione: se prendo $n \in \mathbb{N}$ e lo fattorizzo in maniera usuale (in $\mathbb{Z}$):

$$n = 2^a p_1^{b_1} \cdots p_r^{b_r} q_1^{c_1} \cdots q_s^{c_s}$$

dove $p_i \equiv 1 \pmod 4$ e $q_j \equiv 3 \pmod 4$

qual è la fattorizzazione di n in $\mathbb{Z}[i]$?

E': $$n = (1+i)^a (1-i)^a (x_1+iy_1)^{b_1} (x_1-iy_1)^{b_1} \cdots (x_r+iy_r)^{b_r} (x_r-iy_r)^{b_r} q_1^{c_1} \cdots q_s^{c_s}.$$

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

quindi $(1-i)^a = (-i)^a (1+i)^a$

$2^a = (-i)^a (1+i)^{2a}$.

Osservazione 2 Come mai x_k+iy_k sono primi?

Perché $|x_k+iy_k|^2 = p$ e, se si potessero scrivere come prodotto di due cose, una dovrebbe avere "norma" (= quadrato del valore assoluto) $=1$ e l'altro norma p.

Quello di norma 1 è invertibile $\to$ fattorizzazione "fasulla".

Osservazione In $\mathbb{Z}[i]$ "sì ca" che c'è fattorizzazione unica. Non è ovvio: per esempio in $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$

$(1 + i\sqrt{5})(1 - i\sqrt{5}) = 1 + 5 = 6 = 2 \cdot 3$

e queste sono due fattorizzazioni diverse dello stesso numero.

Esempio facile sull'importanza della fattorizzazione in $\mathbb{Z}[i]$: terne pitagoriche.

Terne "primitive" $a^2 + b^2 = c^2$ con $(a, b, c) = 1$.

$$a^2 + b^2 = c^2 \iff (a+bi)(a-bi) = c^2.$$

M.C.D. fra $a+bi$ e $a-bi$?

- divide $2a$, divide $2b$ $\Rightarrow$ divide 2
- è dispari $\Rightarrow$ MCD $= 1$.

Ne segue che

$a + bi = (u + iv)^2 = u^2 - v^2 + 2iuv$ $\qquad a = u^2 - v^2$

$a - bi = (u - iv)^2 = u^2 - v^2 - 2iuv$ $\qquad b = 2uv$.

Problema proposto a IMO 2004 (N7).

Enunciato: p primo dispari, n intero positivo. Otto punti distinti a coordinate intere stanno su una circonferenza di diametro p^n.

Dimostrare che tre di questi punti formano un triangolo tale che i quadrati delle lunghezze dei suoi lati sono interi divisibili per p^{n+1}.

Soluzione. Sia O il centro della circonferenza

$O = \left(\frac{a}{c}, \frac{b}{c}\right)$ (numeri razionali)

e posso supporre $(a, b, c) = 1$

Es $\left(\frac{3}{5}, \frac{7}{4}\right) \to \left(\frac{12}{20}, \frac{35}{20}\right)$

Stabiliamo quale potenza di p divide (eventualmente) c:

$$c = p^\gamma c_1 \quad \text{con} \quad p \nmid c_1. \leftarrow$$

Sia P un punto a coordinate intere sulla circonferenza. Avremo $\vec{OP} = \left(\frac{x}{c}, \frac{y}{c}\right)$ con

$$a + x \equiv b + y \equiv 0 \pmod{c}$$

e

$$\frac{x^2 + y^2}{c^2} = \frac{p^{2n}}{4} \qquad (1)$$

Riscrivendo, otteniamo

$$4(x^2 + y^2) = p^{2n} c^2 = p^{2n+2\gamma} c_1^2. \qquad (\otimes)$$

1° caso $p \equiv 3 \pmod 4$. Sia x che y sono divisibili per $p^{n+\gamma}$. Ne segue che il quadrato della distanza fra due qualsiasi di questi punti è divisibile per $p^{2n} \geq p^{n+1}$. FINE.

2° caso $p \equiv 1 \pmod 4$. Allora

$$p = (r+si)(r-si) \text{ in } \mathbb{Z}[i].$$

In $(\otimes)$ a destra c'è $p^{2n+2\gamma} = (r+si)^{2n+2\gamma}(r-si)^{2n+2\gamma}$

a sinistra c'è $(x+iy)(x-iy)$

Ottengo: $x+iy = (r+si)^k (r-si)^{2n+2\gamma-k}$. Altre cose prime con p

2a) $\gamma > 0$ (cioè $p \mid c$).

Osserviamo che $(x, y, c) = 1$.

Ci sono solo 2 possibilità: $k = 0$, $k = 2n + 2\gamma$.

Se prendo 5 di questi punti, 3 hanno lo stesso k. Quindi, WLOG, 3 sono divisibili per $(r+si)^{2n+2\gamma}$ → quindi la loro differenza → quindi il quadrato del valore assoluto della loro differenza è divisibile per $p^{2n+2\gamma} \geq p^{n+1}$.

2b) $\gamma = 0$ (cioè $p \nmid c$).

$$x + iy = (r+si)^k (r-si)^{2n-k} \cdot \text{altre cose}$$

Consideriamo dapprima i punti in cui si può avere $k = n$. Questo vuol dire

$$x + iy = p^n \cdot \text{altre cose}$$

$p^n \mid x$ $p^n \mid y$, $x = p^n x_1$, $y = p^n y_1$.

L'equazione (*) diventa

$$4 p^{2n} (x_1^2 + y_1^2) = p^{2n} c_1^2$$

$$4 (x_1^2 + y_1^2) = c_1^2$$

Questo dice che necessariamente

$$-\frac{c_1}{2} \leq x_1, y_1 \leq \frac{c_1}{2}.$$

Però la classe resto di x_1, y_1 modulo c_1 è fissata. Quindi c'è al più una soluzione, a meno che una delle classi sia $\frac{c_1}{2}$ $(= -\frac{c_1}{2})$ e l'altra sia zero.

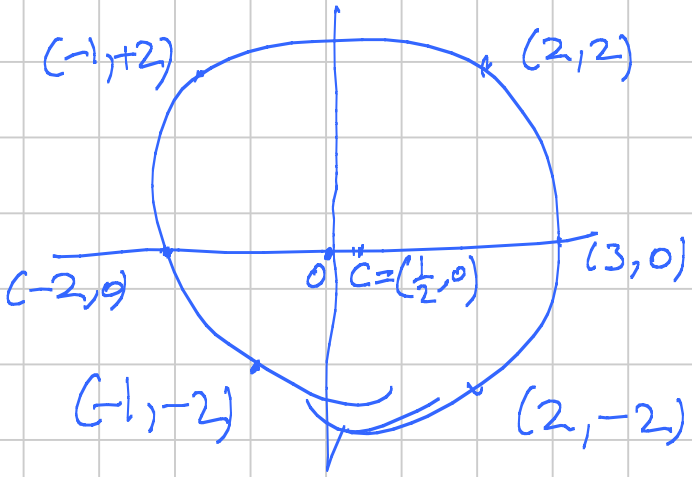
→ Il n° di punti con $k = n$ è ≤ 2.

Quindi, se prendo 7 punti, ce ne sono almeno 5 con $k \neq n$ e quindi almeno 3 con $k > n$

(per simmetria), cioè $k \geq n+1$, cioè
$x+iy$ divisibile per $(r+si)^{n+1}$
Le differenze fra questi punti sono divisibili per $(r+si)^{n+1}$ → i quadrati dei loro valori assoluti sono divisibili per p^{n+1}.

Esempio (Meno di 7 punti non basta).

Circonferenza di centro $\left(\frac{1}{2}, 0\right)$ e diametro 5 (raggio $5/2$).



CONTROLLARE CHE NON VA.

Esempio (IMO 6 – 1988)

Siano a, b interi positivi tali che
$$ab+1 \mid a^2+b^2$$
Allora $\dfrac{a^2+b^2}{ab+1} = \square$.

Sol. $\boxed{a^2+b^2 = k(ab+1)}$ $k \in \mathbb{Z}$ $k>0$.
L'equazione $\boxed{x^2 - kbx + b^2 - k = 0}$
ha come sol. $x=a$
Questa ha anche un'altra sol intera, $x=a'$, tale che
$$a+a' = kb \qquad aa' = b^2-k$$
Si può passare (tenendo fisso k) da una

coppia di soluzioni (a, b) a una coppia $(a', b) = (kb - a, b)$.

Può essere $a = b$? Avremmo $2a^2 = k(a^2+1)$

$\Rightarrow k=1 \quad a=1 \quad 1 = \square$.

Per simmetria, supponiamo $a > b$.

Notiamo che anche a' deve essere ≥ 0.

$$aa' = b^2 - k \Rightarrow a' < b$$

Passo da (a, b) ad (a', b)

$a > b$ $\quad$ $a' < b$

Posso scambiare i ruoli fra a e b

$(a, b) \to (a', b) \to (a', b') \to (a'', b') \to (a'', b'')$

$a > b \quad a' < b \quad a' > b'$

IMPORTANTE: TUTTI QUESTI PASSAGGI LASCIANO FISSO k

SCENDO FINO alla soluzione 0. $\to k = \square$.

(Dal fondo: ho una soluzione $x=0$

$(a, 0)$ $\quad$ $a^2 + b^2 = k(ab+1)$

$\downarrow$ $\quad$ $a^2 + 0 = k \quad k = a^2$

(a, b) $\quad$ b è sol. dell'equazione:

($x^2 - kbx + b^2 - k = 0$ diventa):

$$x^2 - a^2 \cdot a \cdot x + a^2 - a^2 = 0$$

$$x = 0, \; x = a^3$$

$(a, 0) \to (a, a^3) \to (y, a^3)$

$$x^2 - a^2 \cdot a^3 x + a^6 - a^2 = 0$$

$$x = \frac{a^5 \pm \sqrt{a^{10} - 4a^6 + 4a^2}}{2} = \frac{a^5 \pm a(a^4 - 2)}{2} =$$

$$a^5 - a, \; a$$

$\therefore$

Sono passato alla coppia $(a^5 - a, a^3)$

Esempio 2 IMO 2007. Problema 5.

a, b interi positivi tali che

$$4ab - 1 \mid (4a^2 - 1)^2.$$

Allora $a = b$.

Sol. Supponiamo che esista una sol. con $a \neq b$ (p.es. $a < b$). Poniamo

$$k = \frac{(4a^2-1)^2}{4ab-1}$$

Si vede che $k \equiv -1 \pmod{4a}$, cioè

k è del tipo $4ab' - 1$

$$4ab' - 1 \mid (4a^2-1)^2$$

(a,b) sol. $\Rightarrow (a,b')$ sol.

Naturalmente $a < b \Rightarrow a > b'$ e viceversa

Altra osservazione: considero una congruenza modulo $4ab-1$. $\left(-1 \equiv -4ab \cdot 1 \equiv 16a^2b^2\right)$

$$(4b^2-1)^2 \equiv (4b^2 - 16a^2b^2)^2 = 16b^4(4a^2-1)^2$$

Quindi $4ab-1 \mid (4a^2-1)^2 \mid (4b^2-1)^2$

C'è una simmetria, e le coppie (a,b) sono tali che

$4ab-1$ divide sia $(4a^2-1)^2$ che $(4b^2-1)^2$.

LA SIMMETRIA mi consente di fare come prima una discesa concatenata fino ad arrivare ad una sol minimale $(a = 1)$

$$4ab - 1 = 4b - 1 \mid 4a^2 - 1 = 3 \quad \text{cioè } b = 1$$

e quindi $a=b$ assurdo.

Esempio 3 PREIMO 8 (2007).

Equazione diofantea

$$a^m b^n = (a+b)^2 + 1$$

dove a, b, m, n sono interi positivi.

Sol. 1 (tradizionale) Si ha facilmente

$$a \mid b^2+1 \qquad b \mid a^2+1$$ (*)

Se $a=b$, allora $a=b=1$.

Supponiamo $a<b$.

- caso $a=1$ $\quad b \mid 2 \Rightarrow b=2$ NON VA BENE. $(2^n = 3^2+1 = 10)$.

- caso $a \geq 2$ $\quad a^m b^n = (a+b)^2+1 < 4b^2 \leq a^2 b^2 < ab^3 \leq a^m b^3$ (#)

$$\rightarrow \quad n < 3,$$

⊛ sottocaso $n=2$ $\quad a^m b^2 < 4b^2 \quad a^m < 4$

$m=1 \quad a=2 \quad \rightarrow b=5$

$m=1 \quad a=3 \quad \rightarrow 3b^2 = (3+b)^2+1$ NO sol

⊗ sottocaso $n=1$ Sostituendo in # ho $a^m b < 4b^2 \quad a^m < 4b$

e poi uso $b \mid a^2+1$.

(i) $b = a^2+1$

da $a \mid b^2+1$ si ha $a \mid a^4+4a^2+2 \quad a=2$

$b=5$ MA NON FUNZIONA.

(ii) $b \leq \dfrac{a^2+1}{2} \qquad a^m < 2(a^2+1)$

Si verifica facilmente che $\begin{cases} a=2 \quad m \leq 3 \\ \text{oppure} \\ m \leq 2 \end{cases}$

Esaminando i casi si ottiene

- $a=2 \to b \le 5/2$ NON FUNZIONA
- $m=1$ $\quad ab = (a+b)^2+1$ NON FUNZIONA
- $m=2$ $\quad$ do $\quad a^2 < 4b$ e $b \mid a^2+1$

si ricava che $\quad a^2+1 = b, 2b, 3b, 4b$

$a^2+1 = b$ già fatto

$a^2+1 \not\equiv 0 \pmod 3$ $\quad a^2+1 \not\equiv 0 \pmod 4$

resta il caso $\quad a^2+1 = 2b$

$a \mid b^2+1 \Rightarrow 4a \mid 4b^2+4 = a^4+2a^2+5$

$a=5 \to b=13$ è OK

Sol. 2

LEMMA $\quad x^2+y^2+1 = kxy$ ha soluzioni in interi positivi se e solo se $k=3$.

DIM. LEMMA $\quad$ Se $k \neq 3$ non ci possono essere soluzioni con $x=y$. Infatti questo darebbe

$$1 = (k-2)x^2 .$$

Supponiamo che esista una soluzione (a,b) con $a>b$. Quindi a è soluzione dell'equazione

$$x^2 - kbx + b^2 + 1 = 0 .$$

L'altra soluzione, a', soddisfa $a' < b$

(se fosse $a' \ge b$ avrei $aa' \ge (b+1)b = b^2+b > b^2+1$ a meno che $b=1$).

In ogni caso posso concatenare le coppie di soluzioni ed arrivare a una (minimale) con $b=1$, che corrisponde all'equazione

$$x^2 - kx + 2 = 0 .$$

che può avere solo (come soluzioni intere pos.) $x=1, x=2$

$x=1 \to k=3 \qquad x=2 \to k=3.$

—— ∘ ——

Applichiamo il lemma al nostro problema

Trasformiamo l'equazione originale in

$$a^m b^n = a^2+b^2+2ab+1$$

$$ab(a^{m-1}b^{n-1}-2) = a^2+b^2+1$$

$$\downarrow$$

$$k$$

Basta considerare solo il caso $k=3$

$$a^{m-1}b^{n-1} = 5$$

$a^{m-1}=5$	$b^{n-1}=1$	$a=5$	$m=2$	$b=2,13$	$n=1$
$a^{m-1}=1$	$b^{n-1}=5$	$b=5$	$n=2$	$a=2,13$	$m=1$

———

Applicazione di Chevalley-Warning.

(IMO Shortlist N8, 2003)

Sia p un primo e A un insieme di interi positivi tale che:

(i) L'insieme dei divisori primi degli elementi di A contiene esattamente $p-1$ elementi

(ii) Per ogni $B \subseteq A$, $B \neq \emptyset$ il prodotto $\prod_{b \in B} b$ non è una potenza p-esima.

Quanti elementi al massimo può avere A?

———

Se considero $B_i = \{p_i, p_i^{p+1}, p_i^{2p+1}, \dots, p_i^{(p-2)p+1}\}$

$|B_i| = p-1$ $\quad A = \cup B_i$ ha $(p-1)^2$ elementi

e questo funziona $\quad \boxed{r=p-1}$

Congettura: la risposta è $r^2 = (p-1)^2$.

Supponiamo che $|A| \geq r^2+1$

$$A = \{t_1, t_2, \dots, t_{r^2+1}\}.$$

$$t_i = p_1^{a_{i1}} \cdots p_r^{a_{ir}}$$

Scegliere B in modo che il prodotto dei suoi elementi venga una potenza p-esima è come scegliere $y_i \in \{0,1\}$ in modo tale che

$$\begin{cases} \sum a_{i1} y_i \equiv 0 \pmod p \\ \vdots \\ \sum a_{ir} y_i \equiv 0 \pmod p \end{cases}$$

Trucco: $y_i = x_i^{p-1} = x_i^r$, il sistema diventa

$$\begin{cases} F_1 = \sum a_{i1} x_i^r \equiv 0 \pmod p \\ \vdots \\ F_r = \sum a_{ir} x_i^r \equiv 0 \pmod p \end{cases}$$

Cerco una sol. non banale del sistema.
In realtà, basta cercare una soluzione non banale della singola equazione

$$F = F_1^r + F_2^r + \dots + F_r^r \equiv 0 \pmod p$$

L'equazione ha grado r^2 e r^2+1 variabili.
Chevalley-Warning $\Rightarrow$ ha sol. non banale