Teoria dei numeri
Compito relativo al corso dell'A.A. 04/05 tenuto da P. Corvaja e U.Zannier

Stefano Pascolutti

4 aprile 2005

Compito di Teoria dei Numeri

1. Sia k un intero positivo. Dimostrare che nel piano esiste una circonferenza di raggio intero e centro in $\mathbb{Z}^2$ contenente almeno k punti in $\mathbb{Z}^2$.
   Sia $r(X)$ il numero dei punti in $\mathbb{Z}^2$ che stanno sul disco chiuso di raggio X e centro l'origine.
   Dimostrare che per X che tende a infinito $r(X) = \pi X^2 + s(X)$, dove $|s(X)| = O(X)$.
   Dedurre dalla prima parte dell'esercizio che la funzione $s(X)$ non è limitata.

2. Si consideri la forma quadratica $q(x, y) = 9x^2 - 34xy + 37y^2$.

   (a) verificare che essa è definita positiva;

   (b) determinare due numeri complessi ω_1, ω_2 tali che valga

   $$q(x, y) = |\omega_1 x - \omega_2 y|^2$$

   e $\Im(\omega_2/\omega_1) > 0$;

   (c) posto $u = \omega_2/\omega_1$, determinare una trasformazione $A \in PSL_2(\mathbb{Z})$ tale che $A(u)$ appartenga al dominio fondamentale canonico per l'azione di $PSL_2(\mathbb{Z})$ sul semipiano;

   (d) ridurre la forma quadratica $q(x, y)$.

3. Dimostrare che 7 non è differenza di un cubo e un quadrato.

Soluzione. [dell'esercizio 1] Consideriamo la formula per il conteggio dei punti a coordinate intere su una cerchio di raggio al quadrato n:

$$r_2(n) = 4 \cdot \prod_{p \equiv_4 1 \text{ e } p^h || n} (h+1) \cdot \prod_{p \equiv_4 3 \text{ e } p^k || n} \frac{1+(-1)^k}{2}.$$

Si vede immediatamente che per ogni k si più scegliere un n tale che $r_2(n) = 4k > k$. Basta prendere $n = 5^{k/2}$ se k pari oppure $n = 5^{(n+1)/2}$, se k dispari. Infatti $r_2(5^{k-1}) = 4 \cdot (k-1+1) = 4k$. Altrimenti, si può vedere che esistono infiniti primi della forma $4k+1$ e quindi considerare l'enumerazione p_i dei numeri in quella forma. Sia $\prod_{i=1}^{k} p_i = n$. In questo caso, $r_2(n) = 2^{k+2} > k$. Vediamo una espressione per $r(X)$:

$$r(X) = |\left\{(x,y) \in \mathbb{Z}^2 | x^2 + y^2 \leq X^2\right\}| = 1 + 4 \cdot \sum_{i=0}^{\lfloor X \rfloor} \left\lfloor \sqrt{X^2 - i^2} \right\rfloor.$$

La formula è evidente e non necessita di dimostrazioni. Inoltre tutti i termini coinvolti sono positivi o nulli. Vediamo come è possibile maggiorare la $r(X)$:

$$1 + 4 \cdot \sum_{i=0}^{\lfloor X \rfloor} \left\lfloor \sqrt{X^2 - i^2} \right\rfloor < 1 + 4 \cdot \sum_{i=0}^{\lfloor X \rfloor} \sqrt{X^2 - i^2} < 1 + \int_0^X \sqrt{X^2 - t^2}\, dt.$$

L'integrale è esattamente l'area di $1/4$ del disco. Pertanto:

$$1 + 4 \cdot \sum_{i=0}^{\lfloor X \rfloor} \left\lfloor \sqrt{X^2 - i^2} \right\rfloor < 1 + \pi X^2. \tag{1}$$

Devo dimostrare che $r(X) = \pi X^2 + s(X)$, con $|s(X)| = O(X)$, vale a dire $\frac{|s(X)|}{X}$ è limitata. Ma con lo stesso metodo appena visto, posso ottenere una minorazione per la $r(X)$, della stessa magnetudine (X^2). Pertanto la differenza tra la maggiorazione e la minorazione, che è maggiore dell'errore, è $O(X)$.
Dimostrato questo, è banale verificare che la $s(X)$ non è limitata. Per quanto visto all'inizio, dato $\tilde{k}$ esiste $\tilde{n}$ tale che $r_2(\tilde{n}) > \tilde{k}$. Ma possiamo scrivere la $r(X)$ in termini della funzione $r_2(\cdot)$:

$$r(X) = \sum_{i=0}^{\lfloor X \rfloor} r_2(i).$$

Se prendiamo un raggio $\tilde{X} = \sqrt{\tilde{n}} - \varepsilon$, con $\varepsilon > 0$, $r(\sqrt{\tilde{n}}) - r(\tilde{X}) = r_2(\tilde{n}) = \tilde{k}$ mentre $\pi\tilde{n} - \pi\tilde{X}^2 = \pi(\tilde{n} - \tilde{n} + 2\varepsilon\sqrt{\tilde{n}} - \varepsilon^2) = \pi(2\varepsilon\sqrt{\tilde{n}} - \varepsilon^2)$ può essere piccolo a piacere.

□

Soluzione. [dell'esercizio 2] Proviamo che $q(x,y)$ è definita positiva. È sufficiente mostrare che è definita positiva la matrice associata:

$$q(x,y) = \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} 81 & -153 \\ -153 & 333 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} \cdot M \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

Per mostrare che $q(x,y)$ è definita positiva, è sufficiente mostrare che $M_{1,1} > 0$ e $\det M > 0$. Ma $M_{1,1} = 81 > 0$ e $\det M = 9 \cdot 37 - 17 \cdot 17 = 44 > 0$. Quindi $q(x,y)$ è definita positiva.
Cerchiamo $\omega_1, \omega_2 \in \mathbb{R}[i]$. Quindi $\omega_1 = a + ib, \omega_2 = c + id$, con $a,b,c,d \in \mathbb{R}$. Vogliamo che i due numeri soddisfino la seguente:

$$q(x,y) = |\omega_1 x - \omega_2 y|^2 = (\omega_1 x - \omega_2 y)(\overline{\omega_1} x - \overline{\omega_2} y), \tag{2}$$

che è equivalente alla seguente:

$$(\omega_1 x - \omega_2 y)(\overline{\omega_1} x - \overline{\omega_2} y) = (x - \frac{\omega_2}{\omega_1} y)(x - \frac{\overline{\omega_2}}{\overline{\omega_1}} y).$$

Quindi, detto $u = \omega_2/\omega_1$, u è radice del polinomio deomogeneizzato in y: $81x^2 - 306xy + 333$. Le radici sono date dalla solita formula e sono le seguenti: $x_{1/2} = \left(\frac{17 \pm \sqrt{17^2 - 4 \cdot 9 \cdot 37}}{9}\right) = \frac{17 \pm \sqrt{-44}}{9} = \frac{17 \pm 2i\sqrt{11}}{9}$. voglio che $\Im(u) > 0$, pertanto prenderò $u = \frac{17 + 2i\sqrt{11}}{9}$.

Ora voglio spostare u, tramite una matrice in $PSL_2(\mathbb{Z})$, nel dominio fondamentale $\mathcal{D}$. Vediamo che è sufficiente prendere la trasformazione

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix},$$

la quale manda u in $\mathcal{D}$. $A = S \circ T^{-1} \circ T^{-1}$. Sotto questa trasformazione, $u \mapsto A(u) = \frac{1 + 2i\sqrt{11}}{5}$ e $|\Re(A(u))| = 1/5 < 1/2$ e $|A(u)| = 45/25 = 9/5 > 1$. Quindi $A(u) \in \mathcal{D}$. Detto questo, cerchiamo la forma quadratica che otteniamo tramite questa trasformazione: cerchiamo, quindi, una $\tilde{q}(x,y)$ tale che $q(x,y) = \tilde{q}(A(x,y))$. Ma allora $\tilde{q} = q \circ A^{-1}$. $A^{-1}(x,y) = (2x - y, x)$ e quindi $\tilde{q}(x,y) = 5x^2 - 2xy + 9y^2$. I minimi corrispondenti sono $\tilde{q}(1,0) = 1$, $\tilde{q}(0,1) = \frac{9}{5}$, $\tilde{q}(-1,1) = \frac{12}{5}$.

□

Soluzione. [dell'esercizio 3] Vogliamo dimostrare che non esistono $x, y \in \mathbb{Z}$ tali che valga

$$x^3 + 7 = y^2 \tag{3}$$

Osserviamo innanzitutto che x deve essere dispari. Se fosse pari, y sarebbe dispari e quindi $y^2 \equiv_4 1$. D'altra parte, avendo supposto x pari, x è della

forma $x = 2n$. Quindi $x^8 = 8n^3 \equiv_4 0$. Pertanto, riducendo la (3) modulo 4, otteniamo $7 \equiv_4 1$, Assurdo. Quindi x è dispari. Aggiungiamo 1 a entrambi i membri della (3):

$$x^3 + 8 = y^2 + 1$$

Il primo membro di fattorizza: $x^3 + 8 = (x + 2)(x^2 - 2x + 4)$. Ponendo $x = 2n+1$, abbiamo $x^3+8 = (2n+3)(4n^2+4n+1-4n-2+4) = (2n+3)(4n^2+3)$. Ma il termine $4n^2+3$ o è primo o ha almeno un fattore primo del tipo $4k+3$. Pertanto $4k+3|x^3+8$ e quindi $4k+3|x^2+1$. Ma allora $4k+3$ si scriverebbe come somma di quadrati. Assurdo. Quindi 7 non è differenza di un cubo e un quadrato.

□