UNIVERSITÀ DEGLI STUDI DI TORINO
Dipartimento di Matematica
Welcome Home Workshop
Dicembre 2014

The distribution of lattice points and the Gauss Circle Problem

Riccardo W. Maffucci
King's College London

- Per quali $n \in \mathbb{N}$ possiamo scrivere $n = a^2 + b^2$, per opportuni interi a, b?
- Quante rappresentazioni ammette n come somma di due quadrati?

Un quadrato può essere congruente a 0 o 1 $\pmod 4$, quindi la somma di due quadrati non può mai essere 3 $\pmod 4$. Se $n \equiv 3 \pmod 4$, allora n non è somma di due quadrati.

Se n è somma di due quadrati, allora ogni primo $q \equiv 3 \pmod 4$ che divide n deve dividerlo con un esponente pari.

- Per quali $n \in \mathbb{N}$ possiamo scrivere $n = a^2 + b^2$, per opportuni interi a, b?
- Quante rappresentazioni ammette n come somma di due quadrati?

Un quadrato può essere congruente a 0 o 1 $\pmod 4$, quindi la somma di due quadrati non può mai essere 3 $\pmod 4$. Se $n \equiv 3 \pmod 4$, allora n non è somma di due quadrati.

Se n è somma di due quadrati, allora ogni primo $q \equiv 3 \pmod 4$ che divide n deve dividerlo con un esponente pari.

n è somma di due quadrati se e solo se ogni primo $q \equiv 3 \pmod 4$ che divide n lo divide con un esponente pari.

In $\mathbb{Z}[i]$, la fattorizzazione è unica a meno dell'ordine, elementi invertibili e primi associati.

$$2 = -i(1+i)^2, \quad p = (a+bi)(a-bi) = a^2 + b^2, \quad q \text{ è inerte in } \mathbb{Z}[i].$$

Ogni primo $p \equiv 1 \pmod 4$ è somma di due quadrati (e in modo essenzialmente unico). Naturalmente anche gli interi 2 e q^2 sono somme di due quadrati.

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

$$|(x+iy)|^2 |(s+it)|^2 = |(x+iy)(s+it)|^2.$$

n è somma di due quadrati se e solo se ogni primo $q \equiv 3 \pmod 4$ che divide n lo divide con un esponente pari.

In $\mathbb{Z}[i]$, la fattorizzazione è unica a meno dell'ordine, elementi invertibili e primi associati.

$$2 = -i(1+i)^2, \quad p = (a+bi)(a-bi) = a^2+b^2, \quad q \text{ è inerte in } \mathbb{Z}[i].$$

Ogni primo $p \equiv 1 \pmod 4$ è somma di due quadrati (e in modo essenzialmente unico). Naturalmente anche gli interi 2 e q^2 sono somme di due quadrati.

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

$$|(x+iy)|^2|(s+it)|^2 = |(x+iy)(s+it)|^2.$$

Il numero di rappresentazioni

Sia

$$n = p_1^{\alpha_1} \cdots p_h^{\alpha_h} \cdot q_1^{2\beta_1} \cdots q_l^{2\beta_l} \cdot 2^{\nu}.$$

Sia $r(n)$ il numero di rappresentazioni di n come somma di due quadrati. Allora

$$r(n) = 4 \prod_{i=1}^{h} (\alpha_i + 1).$$

$p_1^{\alpha_1} \cdots p_h^{\alpha_h} \cdot q_1^{\beta_1} \cdots q_l^{\beta_l} \cdot 2^\nu = n = A^2 + B^2 = (A + Bi)(A - Bi)$. Allora

$$\begin{cases} A + Bi = \prod (a + bi)^{\alpha_1} (a - bi)^{\alpha_2} \prod q^{\beta_1} (1 + i)^{\nu_1} (1 - i)^{\nu_2} i^t \\ A - Bi = \prod (a + bi)^{\alpha_2} (a - bi)^{\alpha_1} \prod q^{\beta_2} (1 + i)^{\nu_2} (1 - i)^{\nu_1} i^{-t} \end{cases}$$

dove $t = 0, 1, 2, 3$, $\nu_1 + \nu_2 = \nu$, $\alpha_1 + \alpha_2 = \alpha$, $\beta_1 + \beta_2 = \beta$.

$|A + Bi| = |A - Bi|$ da cui $\beta_1 = \beta_2$ per ogni β, che è quindi pari.
4 scelte per t, $\nu + 1$ scelte per ν_1, ν_2 e $\alpha + 1$ scelte per α_1, α_2.
Tuttavia, una diversa scelta di ν_1 moltiplica $A + Bi$ per una potenza di $\frac{1+i}{1-i} = i$, di cui abbiamo già tenuto conto con la scelta di t.
Ogni scelta di un α_j cambia la rappresentazione $n = A^2 + B^2$ in maniera non banale; le quattro scelte possibili di t corrispondono a cambiare di segno A o B.

Sia χ il carattere di Dirichlet non principale (mod 4):

$$\chi(d) = \sin\left(\frac{\pi}{2}d\right) = \begin{cases} 1 & \text{se } d \equiv 1 \mod 4 \\ -1 & \text{se } d \equiv 3 \mod 4 \\ 0 & \text{se } 2 \mid d. \end{cases}$$

χ è una funzione moltiplicativa.

$$r(n) = 4\prod_{i=1}^{h}(\alpha_i + 1) = 4\sum_{d|n}\chi(d) = 4(d_1(n) - d_3(n)).$$

$r(n)/4$ è una funzione moltiplicativa.

$$r(n) = 4\prod_{i=1}^{h}(\alpha_i + 1) = 4\sum_{d|n}\chi(d) = 4(d_1(n) - d_3(n)).$$

$$p_1^{\alpha_1}\cdots p_h^{\alpha_h}\cdot q_1^{\beta_1}\cdots q_l^1 \longleftrightarrow p_1^{\alpha_1}\cdots p_h^{\alpha_h}\cdot q_1^{\beta_1}\cdots q_l^2,$$
$$p_1^{\alpha_1}\cdots p_h^{\alpha_h}\cdot q_1^{\beta_1}\cdots q_l^3 \longleftrightarrow p_1^{\alpha_1}\cdots p_h^{\alpha_h}\cdot q_1^{\beta_1}\cdots q_l^4,$$

$$\sum_{d|n}\chi(d) = |\{d \mid n : d = p_1^{\gamma_1}\cdots p_h^{\gamma_h}\}|.$$

Il Problema del Cerchio di Gauss

Definiamo

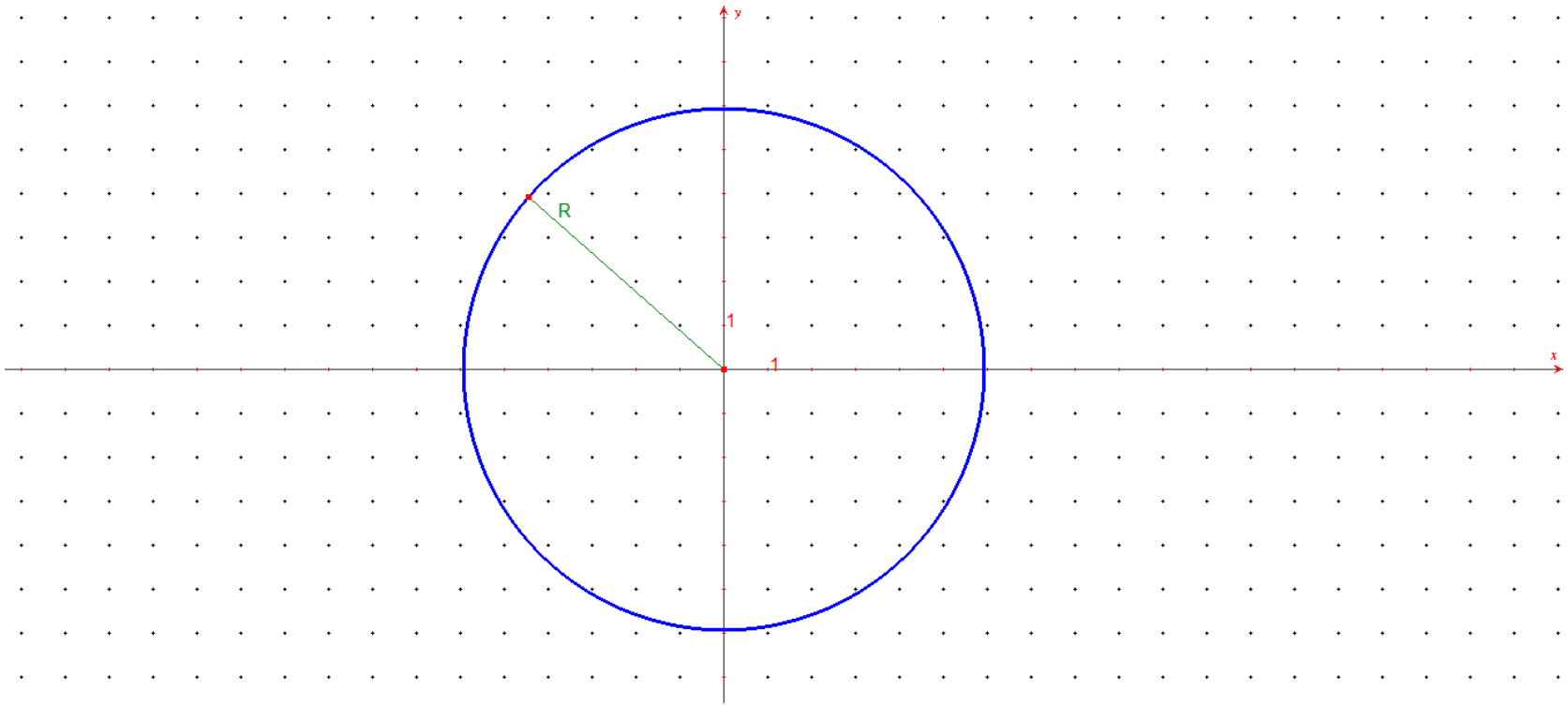
$$D = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq R^2\}$$

Contiamo il numero di punti reticolari (lattice points) all'interno di D:

$$N(R) = |\{D \cap \mathbb{Z}^2\}|$$

Al tendere del raggio all'infinito, ci chiediamo quale sia l'andamento asintotico di N.

Il Problema del Cerchio di Gauss



Risultato di Gauss

$$|N(R) - \pi R^2| \leq 2\sqrt{2}\pi R + 2\pi$$

$$f(x) = O(g(x)) \qquad \text{per} \quad x \to \infty$$

se esiste una costante $M > 0$ tale che $|f(x)| \leq M|g(x)| \qquad \forall x > x_0$.

Usando la notazione O grande: $N(R) = \pi R^2 + O(R)$.

$$N(R) = \pi R^2 + E(R), \qquad E(R) = O(R)$$

Una stima più precisa del resto $E(R)$:

Risultato di Van der Corput e Sierpinski

$$E(R) = O(R^{\frac{2}{3}})$$

Hardy provò che $E(R) \neq o(R^{\frac{1}{2}} \log^{\frac{1}{4}} R)$, e congetturò che $E(R) = O(R^{\frac{1}{2}+\epsilon})$ $\forall \epsilon > 0$.

La stima attuale è dovuta a Huxley (2003): $E(R) = O(R^{\alpha+\epsilon})$, dove $\alpha = \frac{131}{208} \approx 0.63$.

$$N(R) = \pi R^2 + E(R), \qquad E(R) = O(R)$$

Una stima più precisa del resto $E(R)$:

Risultato di Van der Corput e Sierpinski

$$E(R) = O(R^{\frac{2}{3}})$$

Hardy provò che $E(R) \neq o(R^{\frac{1}{2}} \log^{\frac{1}{4}} R)$, e congetturò che $E(R) = O(R^{\frac{1}{2}+\epsilon})$ $\forall \epsilon > 0$.

La stima attuale è dovuta a Huxley (2003): $E(R) = O(R^{\alpha+\epsilon})$, dove $\alpha = \frac{131}{208} \approx 0.63$.

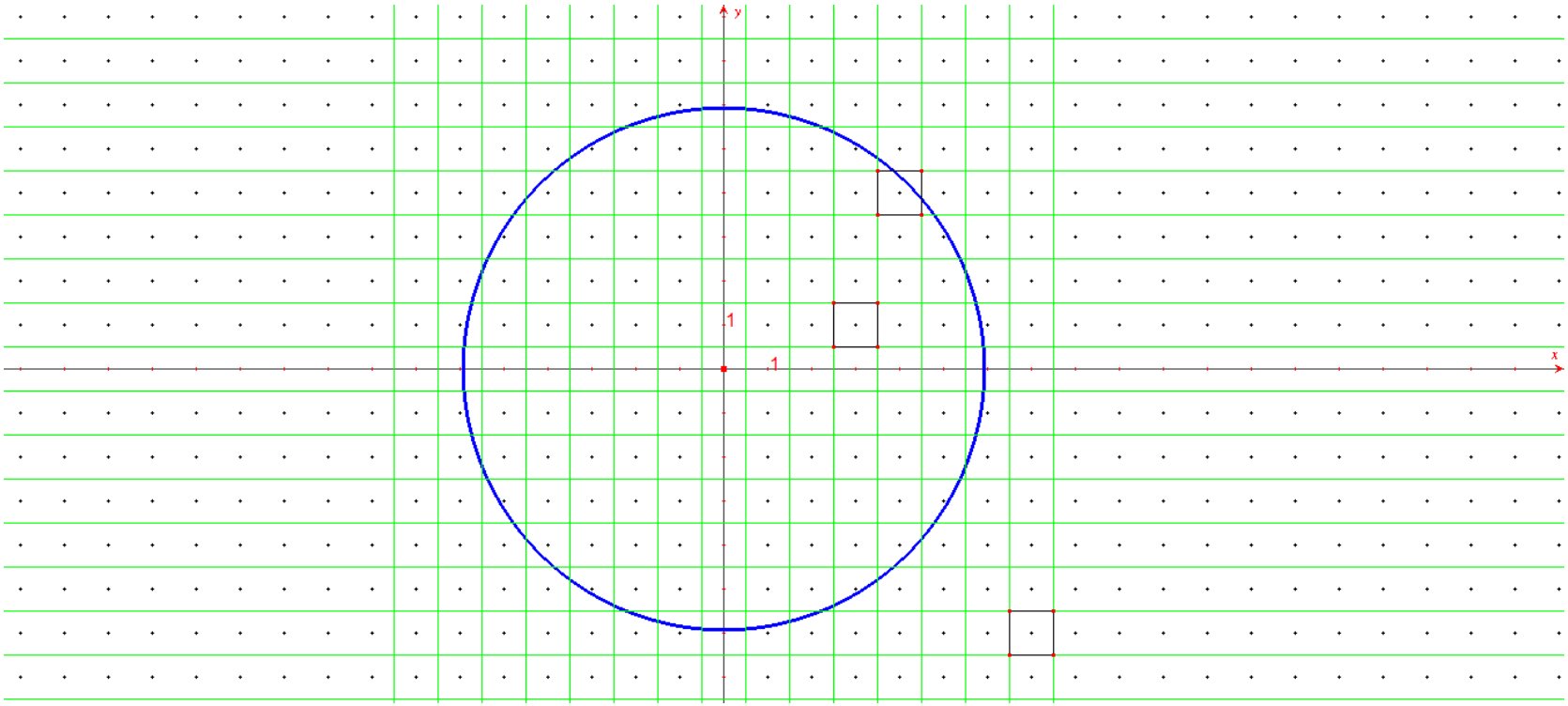
Dimostrazione del risultato di Gauss

Sia S l'insieme dei quadrati di lato 1 nel piano cartesiano, centrati nei punti a coordinate intere:

$$s_{m,n} = \left\{ (x,y) \in \mathbb{R}^2 : m - \frac{1}{2} \leq x \leq m + \frac{1}{2},\ n - \frac{1}{2} \leq y \leq n + \frac{1}{2} \right\}$$

$$S = \{ S_{m,n} : m, n \in \mathbb{Z} \}$$

Dimostrazione del risultato di Gauss



Dimostrazione del risultato di Gauss

Sia $m(R)$ il numero di quadrati completamente contenuti nel disco di raggio R:

$$m(R) = |\{s \in S : s \subset D\}|$$

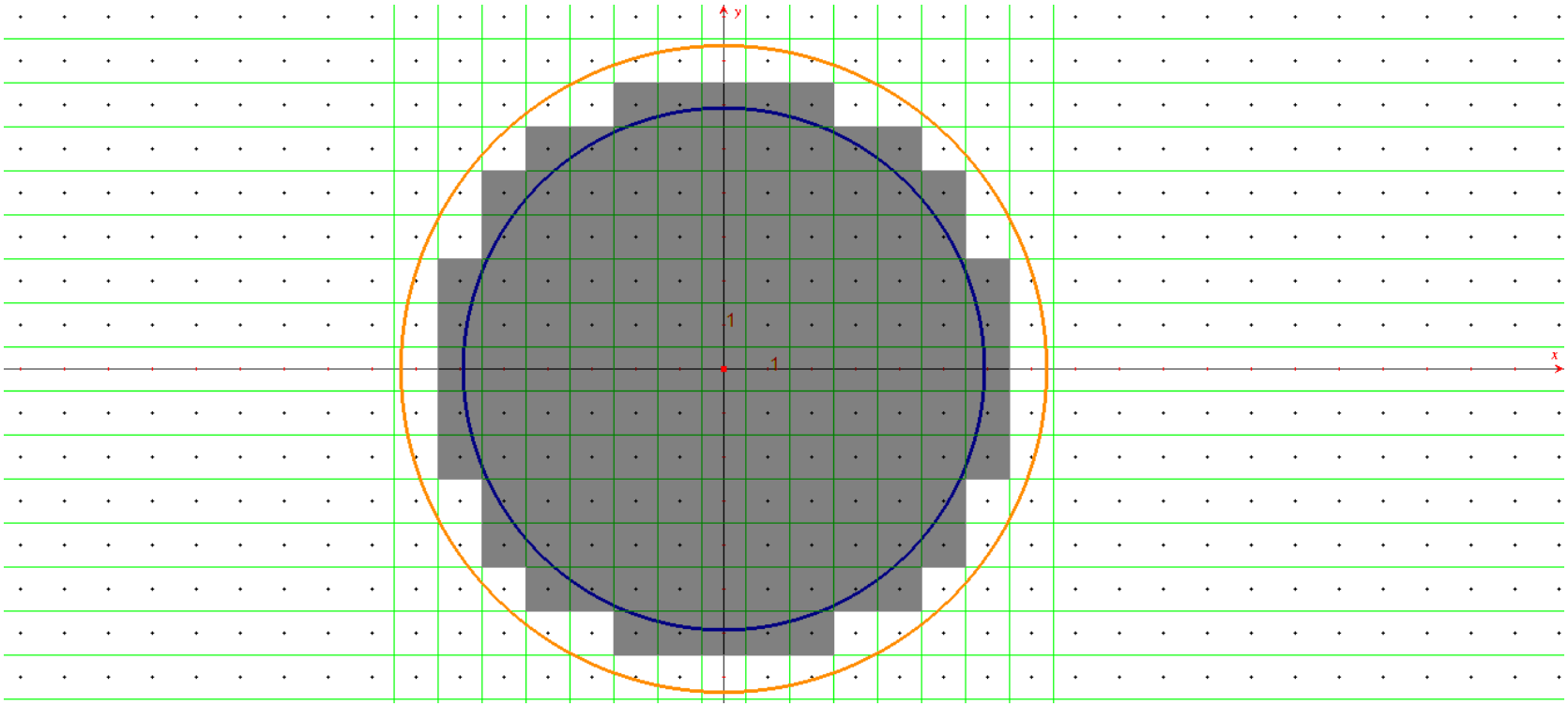
e sia $M(R)$ il numero di quadrati contenuti o interamente o in parte nel disco di raggio R:

$$M(R) = |\{s \in S : s \cap D \neq \emptyset\}|.$$

$N(R)$ è almeno grande quanto il numero di quadrati completamente contenuti in D, e non può superare il numero di quadrati che hanno intersezione non vuota con D:

$$m(R) \leq N(R) \leq M(R).$$

Stima dall'alto



Dimostrazione del risultato di Gauss

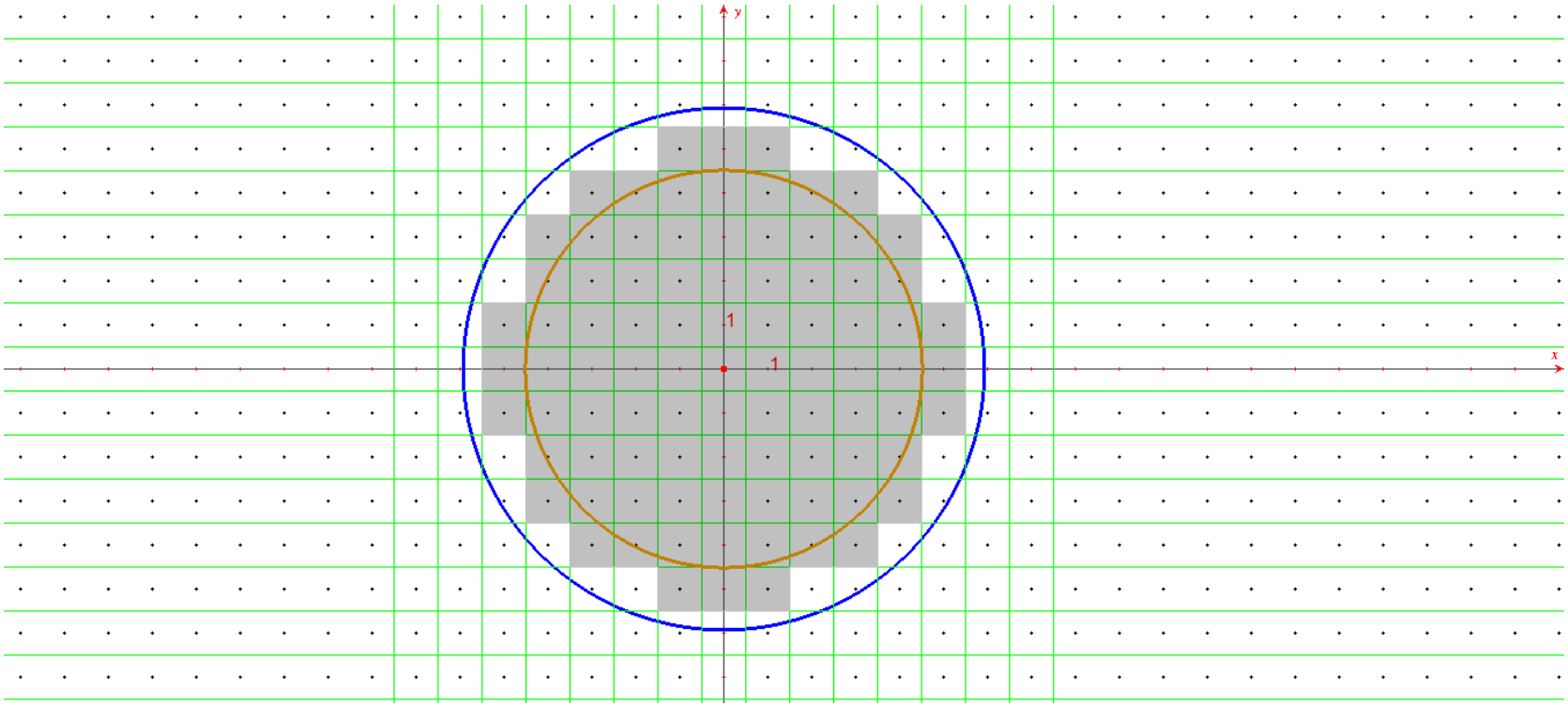
Dato che le diagonali dei quadrati misurano $\sqrt{2}$, $m(R)$ è almeno grande quanto l'area del disco di raggio $R - \sqrt{2}$. Allo stesso modo, $M(R)$ non può superare l'area del disco di raggio $R + \sqrt{2}$:

$$\pi(R - \sqrt{2})^2 \leq m(R) \leq N(R) \leq M(R) \leq \pi(R + \sqrt{2})^2$$

$$|N(R) - \pi R^2| \leq 2\sqrt{2}\pi R + 2\pi = O(R).$$

$$\sum_{n=1}^{X} r(n) = \pi X + O(\sqrt{X})$$

Stima dal basso



La dimostrazione del risultato di Van der Corput e Sierpinski utilizza la sommazione di Poisson e il principio di fase stazionaria.
La sommazione di Poisson può essere descritta come una relazione tra la trasformata di Fourier e la serie di Fourier.
Data $f : \mathbb{R}^n \longrightarrow \mathbb{R}$, consideriamo

$$\widehat{f(\xi)} = \int_{\mathbb{R}^n} f(x) \exp(-i\xi \cdot x) dx$$

come definizione di trasformata di Fourier.

Sommazione di Poisson

Sia $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ continua, $f(x) = O(\frac{1}{x^{n+\epsilon}})$ e $\widehat{f(\xi)} = O(\frac{1}{\xi^{n+\epsilon}})$. Allora

$$\sum_{j \in \mathbb{Z}^n} f(j) = \sum_{k \in \mathbb{Z}^n} \widehat{f(2\pi k)}$$

se entrambe le serie sono assolutamente convergenti.

Principio di fase stazionaria

Dati $a, b, \tau \in \mathbb{R}$ e funzioni $f, \phi : \mathbb{C} \longrightarrow \mathbb{C}$, desideriamo stimare l'integrale

$$\int_a^b \exp(i\tau f(\theta))\phi(\theta)d\theta$$

per $\tau \to \infty$ (fase f e ampiezza ϕ sono olomorfe).

$$\left| \int_a^b \exp(i\tau f(\theta))\phi(\theta)d\theta \right| \leq \int_a^b |\phi(\theta)|d\theta = O(1)$$

Se tutti i punti stazionari di f sono non degeneri,

$$\int_a^b \exp(-i\tau f(\theta))\phi(\theta)d\theta = O\left(\frac{1}{\sqrt{\tau}}\right).$$

$E(R) = O(R^{\frac{2}{3}})$ Van der Corput e Sierpinski

Definiamo una funzione con cui stimare $N(R)$:

$$N_\epsilon(R) = \sum_{\nu \in \mathbb{Z}^2} (\chi_R * \rho_\epsilon)(\nu)$$

dove χ_R è la funzione indicatrice del disco di raggio R (vale 1 se $\nu \in D$ e vale 0 altrimenti); ρ_ϵ è una funzione di smoothing (liscia e con supporto compatto). Approssimando $N(R)$ con $N_\epsilon(R)$ si commette un errore $O(R\epsilon)$, mentre $N_\epsilon(R) = \pi R^2 + O(\frac{R}{\epsilon})^{\frac{1}{2}}$.

$$N(R) = \pi R^2 + O(R\epsilon) + O\left(\frac{R}{\epsilon}\right)^{\frac{1}{2}} = \pi R^2 + O(R^{\frac{2}{3}}).$$

Grazie per l'attenzione.