

Lecture 7:

2/5/2018

Lower bounds for the remainder term $P(R) = N(R) - R^2 \pi$

$$N(R) = \# \{ \mathbb{Z}^2 \cap B(0, R) \}$$

We saw:

$$|P(R)| = O(R^{2/3})$$

Conj:

$$|P(R)| = O(R^{1/2+\epsilon}) \quad \forall \epsilon > 0$$

Prop.:

$\exists c > 0$, There are arbitrary large R 's s.t. $|P(R)| > cR^{1/2}$
(notation: $P(R) = \Omega(R^{1/2})$)

Prop.: (no proof)

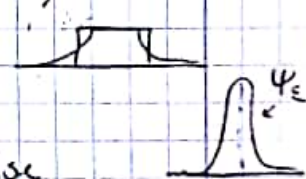
$T \gg 1$, for $\frac{T}{100} < t < 100T$

$$P(t) = - \frac{t^{1/2}}{T} \sum_{\substack{0 \leq |m| < T^{3/4} \\ s \neq m \in \mathbb{Z}^2}} \frac{\cos(2\pi t |m| + \pi/4)}{|m|^{3/2}} + O(T^{-1/4})$$

Why this is reasonable (not a proof!):

We look at a smooth counting function,

$$N_\epsilon(R) = \sum_{n \in \mathbb{Z}^2} \chi_\epsilon\left(\frac{n}{R}\right), \quad \chi_\epsilon = \chi * \psi_\epsilon =$$
$$\chi(y) = \begin{cases} 1 & |y| \leq 1 \\ 0 & \text{otherwise} \end{cases}$$



Poisson Summation:

$$N_\epsilon(R) = \pi R^2 + R^2 \sum_{0 \neq m \in \mathbb{Z}^2} \hat{\psi}(\epsilon R |m|) \hat{\chi}(Rm)$$

We used Van der Corput to bound $\hat{\chi}(y) \ll \frac{1}{|y|^{3/2}}$

In fact, we can derive an asymptotic formula for $\hat{\chi}$.

Stationary phase : (wasn't proved)

If x_0 is the only critical pt. of $\phi(x)$, which is non-degenerate, $\phi''(x_0) \neq 0$

$$\int A(x) e^{i\lambda \phi(x)} dx \sim_{\lambda \rightarrow \infty} e^{i \frac{\pi}{4} \text{Sgn } \phi''(x_0)} A(x_0) \sqrt{\frac{2\pi}{|\phi''(x_0)|}} \frac{e^{i\lambda \phi(x_0)}}{\sqrt{\lambda}}$$

$$\Rightarrow \hat{\chi}(y) \sim * \frac{\cos(2\pi|y| + \pi/4)}{|y|^{3/2}} + O\left(\frac{1}{|y|^{5/2}}\right)$$

↑
Something

Notations:

$$S(t) := \frac{N(t) + \pi t^2}{\sqrt{t}}$$

Note, for $t \ll T$ we have,

$$S(t) = -\frac{1}{\pi} \sum_{0 < |m| < T^{3/4}} \frac{\cos(2\pi |m|t + \pi/4)}{|m|^{3/2}}$$

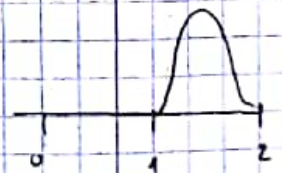
Want:

to contradict the claim $S(t) = o(1)$.

Let $\omega \in C_c^\infty([1, 2])$, $\omega \geq 0$, $\int_{\mathbb{R}} \omega(x) dx = 1$ & compute

$$\int_{-\infty}^{\infty} S(t) e(-t) \omega\left(\frac{t}{T}\right) \frac{dt}{T} =: A(T)$$

$\frac{1}{e(z)} = e^{2\pi i z}$



Claim:

$$\lim_{T \rightarrow \infty} A(T) = c \neq 0, \infty$$

$\Rightarrow S(t)$ cannot go to 0. i.e. $\exists$ arbitrary large t 's s.t. $|S(t)| > c$.

assume $\lim_{t \rightarrow \infty} S(t) = 0 \Rightarrow \lim_{T \rightarrow \infty} \frac{1}{T} \int_+^{2T} S(t) dt = \frac{1}{T} \lim_{T \rightarrow \infty} \int_T^{2T} S(t) dt = 0$

$$A(T) = \sum_{0 < |m| < T^{3/4}} \frac{1}{|m|^{3/2}} \int_{\mathbb{R}} \cos(2\pi |m|t + \frac{\pi}{4}) e^{-2\pi i t} \omega\left(\frac{t}{T}\right) \frac{dt}{T}$$

insert the expansion for $S(t)$

$$= \frac{e^{2\pi i |m|T} + e^{-2\pi i |m|T}}{2}$$

Separating the cos

$$= \frac{1}{2} \sum_{0 < |m| < T^{3/4}} \frac{1}{|m|^{3/2}} e^{\pm \frac{\pi}{4}} \int_{\mathbb{R}} e^{-2\pi i t(1 \pm |m|)} \omega\left(\frac{t}{T}\right) \frac{dt}{T}$$

$$\int_{\mathbb{R}} e^{-2\pi i t(1 \pm |m|)} \omega\left(\frac{t}{T}\right) \frac{dt}{T} = \int_{\frac{t}{T} = u} e^{-2\pi i u T(1 \pm |m|)} \omega(u) du =$$

$$= \hat{\omega}(T(1 \pm |m|))$$

$$\Rightarrow A(T) = \sum_{0 < |m| < T^{3/4}} \frac{1}{|m|^{3/2}} \left(e^{i\frac{\pi}{4}} \hat{\omega}(T(1 - |m|)) + e^{-i\frac{\pi}{4}} \hat{\omega}(T(1 + |m|)) \right)$$

Recall: $\hat{\omega}(y) \ll \frac{1}{|y|^{100}}$, so $\hat{\omega}(T(1 + |m|)) \ll \frac{1}{T^{100} |m|^{100}}$

Hence,

$$\sum_{|m| \geq 1} \frac{1}{|m|^{3/2}} \hat{\omega}(T(1 + |m|)) \ll \frac{1}{T^{100}} \sum_{|m| \geq 1} \frac{1}{|m|^{3/2 + 100}} \ll \frac{1}{T^{100}}$$

$\frac{3}{2} + 100 > 2$

So this part contributes $o(1)$ to $A(T)$.

Likewise if $1 - |m| \neq 0 \Rightarrow T(1 - |m|) > \frac{T|m|}{\sqrt{2}}$ so

you also get a negligible contribution to $A(T)$.

So we're left with $|m| = 1$, i.e. $m = \pm(1, 0), \pm(0, 1)$

These contribute:

$$= \frac{1}{\pi} \sum_{m = \pm(1, 0), \pm(0, 1)} \frac{1}{|m|^{3/2}} e^{i\frac{\pi}{4}} \hat{\omega}(0) = -\frac{4e^{i\pi/4}}{\pi} \hat{\omega}(0) \quad \textcircled{=}$$

$$\hat{\omega}(0) = \int_{\mathbb{R}} \omega(x) dx = 1$$

$$\textcircled{=} = -\frac{4e^{i\pi/4}}{\pi} = C \neq 0$$

$$\Rightarrow \lim_{T \rightarrow \infty} A(T) = C \neq 0 \text{ so } S(t) \not\rightarrow 0 \text{ i.e. } P(R) \sim R^{1/2}$$

Hardy (maybe Littlewood 1920):

$$P(R) = \Omega(R^{1/2} (\log(R))^{1/4})$$

H. Cramér 1920:

$$\lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T S(t)^2 dt = c > 0$$

Question:

Is $S(t)$ "random" (i.e. Gaussian). i.e. is there a limiting distribution:

$$\exists \lim_{T \rightarrow \infty} \frac{1}{T} \text{meas} (0 < t < T \mid \alpha < S(t) < \beta) = \int_{\alpha}^{\beta} p(x) dx$$

e.g. Gaussian $p(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$

A. Wintner 1940:

$\exists$ limiting distribution, $F(t)$

1990's: $F(t) \neq$ Gaussian, K.M. Tsang: $\frac{1}{T} \int_0^T S(t)^2 dt \neq 0$

Conj:

In 3-dim. the limiting dist. is indeed Gaussian.

High dimensions (so far only for $d=2$)

$$N_d(R) = \# \{ \mathbb{Z}^d \cap B(0, R) \}$$

$$N_d(R) \sim \underset{d}{\text{Vol}} (B(0, R)) = \underbrace{\omega_d}_{= \text{Vol}_d(B(0, 1))} R^d$$

$$N_d(R) - \omega_d R^d = O(R^{d-1})$$

$$P_d(R) := N_d(R) - \omega_d R^d$$

Fact:

In dimension $d \geq 4$, the question is trivial.

In particular, it is not true that there is square-root cancellation.

Will show: $P_d(R) = \sqrt{2}(R^{d-2})$ (instead of $O(R^{\frac{d-1}{2}+\epsilon})$)
 $d-2 > \frac{d-1}{2} \iff d > 3$ i.e. $\underline{d \geq 4}$

Def.:

$$r_d(n) = \# \left\{ x \in \mathbb{Z}^d \mid x_1^2 + x_2^2 + \dots + x_d^2 = n \right\} =$$

= # of reps of $n \geq 0$ as a sum of d squares.

Lagrange's 4 squares thm.:

$$r_d(n) \neq 0 \iff \text{Every } n \geq 0 \text{ is a sum of } d \text{ squares.}$$

Notes:

$$N_d(R) = \sum_{n \leq R^2} r_d(n)$$

$$\# \left\{ x \in \mathbb{Z}^d \mid |x|^2 \leq R^2 \right\} = \sum_{n \leq R^2} \# \left\{ x \in \mathbb{Z}^d \mid |x|^2 = n \right\}$$

Jacobi: ($d=4$)

p prime number. $r_4(p) = 8(p+1)$

Fermat: ($d=2$)

If p is prime $\not\equiv 3 \pmod{4} \implies p = a^2 + b^2$

We can even compute:

$r_2(p) = 8$, $p \equiv 1 \pmod{4}$, $r_2(2) = 4$, $r_2(p') = 0$, $p' \equiv 3 \pmod{4}$
 e.g. $5 = (\pm 2)^2 + (\pm 1)^2 = (\pm 1)^2 + (\pm 2)^2$

Trivial lemma:

$\exists$ arbitrary large n 's s.t. $r_d(n) > n^{\frac{d-2}{2}}$

Proof:

$$\sum_{n \leq R^2} r_d(n) = \# \left\{ x \in \mathbb{Z}^d \mid |x| \leq R \right\} = N_d(R) \sim \omega_d R^d$$

So if $r_d(n) = o(n^{\frac{d-2}{2}})$ then,

$$R^d \ll N_d(R) = \sum_{n \leq R^2} r_d(n) = \sum_{n \leq R^2} o(n^{\frac{d-2}{2}}) = o\left(\sum_{n \leq R^2} n^{\frac{d}{2}-1}\right)$$

We get $R^d = o(R^d)$ in contradiction. $\ll (R^2)^{\frac{d}{2}} = R^d$

Much more is known:

$d \geq 5$: There are constants $0 < c_d < C_d$ s.t.

$$c_d n^{\frac{d-2}{2}} < r_d(n) < C_d n^{\frac{d-2}{2}}$$

Using the "Circle method".

Prop:

$$P_d(R) = \Omega(R^{d-2})$$

Proof:

Assume, $P_d(R) = O(R^\theta)$ we want $\theta \geq d-2$.

Take $n = R^2$ s.t. $r_d(n) > n^{\frac{d-2}{2}}$ (by the trivial lemma)

$$r_d(n) \stackrel{\uparrow}{\leq} N_d\left(R + \frac{1}{R^2}\right) - N_d\left(R - \frac{1}{R^2}\right) =$$

$$= \omega_d \left(R + \frac{1}{R^2}\right)^d + P_d\left(R + \frac{1}{R^2}\right) - \omega_d \left(R - \frac{1}{R^2}\right)^d - P_d\left(R - \frac{1}{R^2}\right) =$$

Taylor expansion: $= O(R^{d-3}) + O(R^\theta)$

$$\Rightarrow R^{d-2} = n^{\frac{d-2}{2}} < r_d(n) < R^{d-3} + R^\theta$$

$$\Rightarrow \theta \geq d-2$$

□

Conj for $d=3$:

$$N_3(R) - \omega_3 R^2 = O(R^{2+\epsilon}) \quad \forall \epsilon > 0.$$

Thm. (Gauss / Legendre)

$$r_3(n) > 0 \iff n \neq 4^a(8b+7)$$

Thm.:

n has a primitive rep. as a sum of 3 squares.

$$n = x_1^2 + x_2^2 + x_3^2$$

$$\gcd(x_1, x_2, x_3) = 1$$

$$\iff n \not\equiv 0, 4, 7 \pmod{8}$$

C.L. Siegel: (1930)

$n \not\equiv 0, 4, 7 \pmod{8}$ then $\forall \epsilon > 0 \exists c(\epsilon) > 0. r_3(n) > c(\epsilon) n^{\frac{1}{2} - \epsilon}$

$$\frac{1}{2} = \frac{d-2}{2}$$

Ex.

$$\sqrt[3]{4^9} = 6$$

Hint: $4^a = (\pm 2)^a + 0^a + 0^a$

Fact:

$$\forall n \forall \epsilon > 0, \sqrt[3]{n} < n^{\frac{1}{2} + \epsilon}$$

New Topic: lattice pts. in short arcs on a circle

The Gaussian integers:

$$\mathbb{Z}[i] = \{ m + ni \mid m, n \in \mathbb{Z} \} \text{ is a ring}$$

Fact:

$\mathbb{Z}[i]$ is a Euclidean domain w.r.t the norm: $N(\alpha) = \alpha \bar{\alpha}$

i.e. $\forall \alpha, \beta \in \mathbb{Z}[i] \exists Q, R \in \mathbb{Z}[i] \text{ s.t.}$

a) $\alpha = Q\beta + R$

b) $N(R) < N(\beta)$

$\Rightarrow$ 1) Every ideal is principal

2) irreducible = prime

π is irr. if:

$$\pi = \alpha\beta \Rightarrow \alpha \text{ or } \beta \text{ are units}$$

(units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$)

$$\pi \mid \alpha\beta \Rightarrow \begin{matrix} \pi \mid \alpha \\ \text{or} \\ \pi \mid \beta \end{matrix}$$

3) Unique factorization into primes.

$$\forall \alpha \in \mathbb{Z}[i], \alpha \neq 0, \text{unit} \Rightarrow \alpha = \prod_i \pi_i, \pi_i \text{ primes}$$

& rep. is "unique".

Classification of Primes/irred. in $\mathbb{Z}[i]$:

Lemma:

If $\alpha \in \mathbb{Z}[i]$ s.t. $N(\alpha) = p \in \mathbb{Z}$ is a prime [$N(\alpha) = \alpha \bar{\alpha}$]
then α is irred. in $\mathbb{Z}[i]$.

Example:
 $\alpha = 2+i \Rightarrow N(\alpha) = 5$

Proof:

Otherwise $\alpha = \beta \gamma$ & $N(\alpha) = \text{prime}$ & γ, β not units.

$$\Rightarrow p = N(\alpha) = N(\beta \gamma) = N(\beta) N(\gamma) \Rightarrow$$

$$\begin{matrix} \uparrow & \uparrow \\ \mathbb{Z} & \mathbb{Z} \end{matrix}$$

$$\Rightarrow N(\gamma) = 1 \quad \text{or} \quad N(\beta) = 1 \quad \text{Cont.} \quad \nexists$$

$$\begin{matrix} \uparrow & \uparrow \\ \gamma \text{ unit} & \beta \text{ unit} \end{matrix}$$

Observe:

$$\text{If } p = a^2 + b^2 \iff p = N(\alpha), \alpha = a + bi$$

Example: $3 \neq a^2 + b^2$

Thm. (Fermat)

$$\text{If } p \equiv 1 \pmod{4}, p \text{ prime} \Rightarrow p = a^2 + b^2$$

$$[\text{Easy: if } n \equiv 3 \pmod{4} \Rightarrow n \neq a^2 + b^2]$$

Proof:

$$\text{Assume by cont. that } p \neq a^2 + b^2 \iff p \neq N(\alpha) \iff p \text{ irred.}$$

$$\iff p \text{ is prime in } \mathbb{Z}[i].$$

$$\text{Fermat: If } p \equiv 1 \pmod{4} \Rightarrow \left(\frac{-1}{p}\right) = +1 \iff -1 = x^2 \pmod{p}$$

$$\Rightarrow \exists x \in \mathbb{Z} \text{ s.t. } p \mid x^2 + 1 \Rightarrow x^2 + 1 = p \cdot n \Rightarrow$$

$$\Rightarrow (x-i)(x+i) = pn$$

$$\text{So in } \mathbb{Z}[i], p \mid (x+i)(x-i) \Rightarrow p \mid x+i \text{ or } p \mid x-i$$

$\uparrow$
 prime in $\mathbb{Z}[i]$

$$\Rightarrow (x \pm i) = p \cdot (a + bi) \text{ Compare imaginary part,}$$

$$\pm 1 = pb, b \in \mathbb{Z} \quad \text{Cont.} \quad \nexists$$

$\square$

So:

If $p \equiv 1 \pmod{4}$ (split) $\Rightarrow p = a^2 + b^2$ & $a+bi = \pi$ is prime in $\mathbb{Z}[i]$

If $p \equiv 3 \pmod{4}$ (Inert) $\Rightarrow p \neq a^2 + b^2 \Rightarrow p$ is irred in $\mathbb{Z}[i]$

If $p = 2$ (Ramified), $-i(1+i)^2 = 2$, $1+i$ is prime.

So $r_2(p) > 0$ if $p \neq 3 \pmod{4}$, $r_2(2) = 1$.

Claim:

$$r_3(p) = 8, \quad p \equiv 1 \pmod{4}$$

Proof:

$p \equiv 1 \pmod{4}$, $p = N(\alpha)$, α is irred.

$p = \delta \cdot \bar{\delta}$, $\delta, \bar{\delta}$ not units $\Rightarrow$ either $\delta = \begin{pmatrix} \pm 1 \\ \pm i \end{pmatrix} \alpha$ or $\delta = \begin{pmatrix} \pm 1 \\ \pm i \end{pmatrix} \bar{\alpha}$

Pf:

$$\alpha \cdot \bar{\alpha} = N(\alpha) = p = \delta \bar{\delta}$$

α irred $\Rightarrow$ prime, $\alpha \mid \delta$ or $\alpha \mid \bar{\delta}$

but $N(p) = p^2 = N(\delta \bar{\delta}) = N(\delta) N(\bar{\delta}) \Rightarrow N(\delta) = p = N(\bar{\delta})$, $N(\alpha) = p$

Thm.:

$$n = \square + \square \iff n = 2^a \prod_{p_i \equiv 1 \pmod{4}} p_i^{b_i} \prod_{q_j \equiv 3 \pmod{4}} q_j^{2c_j}$$

i.e. if $p \equiv 3 \pmod{4}$ $n = p^\delta m$ $p \nmid m$ then δ is even.

e.g. $9 = \square + \square = 3^2 + 0$.

Thm.:

$$\text{If } n = 2^a \prod_{p_i \equiv 1 \pmod{4}} p_i^{b_i} \prod_{q_j \equiv 3 \pmod{4}} q_j^{2c_j} \Rightarrow r_2(n) = 4 \underbrace{\prod_j (b_j + 1)}_{\text{number of divisors}} = d\left(\prod p_i^{b_i}\right)$$

Conclusion:

$$r_2(n) \leq 4 d(n)$$

Next time:

$$d(n) \ll n^\epsilon \quad \forall \epsilon > 0$$