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:

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

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 $\frac{T}{100} < t < 100T$

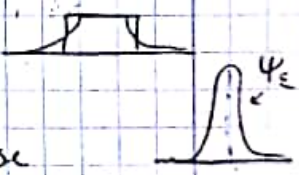
$$P(t) = -\frac{t^{1/2}}{\pi} \sum_{0<|m|<T^{3/4}} \frac{\cos(2\pi t|m| + \pi/4)}{|m|^{3/2}} + O(T^{1/4})$$

$0 \neq m \in \mathbb{Z}^2$

Why this is reasonable (not a proof!):

We look at a smooth counting function,

$$N_\varepsilon(R) = \sum_{n \in \mathbb{Z}^2} \chi_\varepsilon\left(\frac{n}{R}\right), \quad \chi_\varepsilon = \chi * \psi_\varepsilon =$$



$$\chi(y) = \begin{cases} 1 & |y| \le 1 \\ 0 & \text{otherwise} \end{cases}$$

Poisson Summation:

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

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, $\Phi''(x_0) \neq 0$

$$\int A(x) e^{i\lambda\Phi(x)}\,dx \underset{\lambda\to\infty}{\sim} e^{i\frac{\pi}{4}\operatorname{Sgn}\Phi''(x_0)} A(x_0)\sqrt{\frac{2\pi}{|\Phi''(x)|}}\,\frac{e^{i\lambda\Phi(x_0)}}{\sqrt{\lambda}}$$

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

Notations:

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

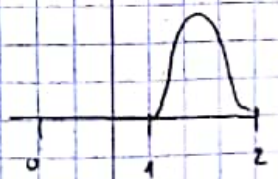
Note, for $t \neq T$ we have,

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

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



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

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

Claim:

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

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

assume $\lim_{t\to 0} S(t) = 0 \Longrightarrow \lim_{T\to\infty} \frac{1}{T}\int_T^{2T} S(t)\,dt = \frac{1}{T}\int_T^{2T} \underbrace{\lim_{t\to\infty} S(t)}_{=0}\,dt = 0$

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

insert the expansion for $\cos(t)$

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

Separating the cos

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

$$\int e^{-2\pi i t(1\mp|m|)} \omega\left(\tfrac{t}{T}\right) \frac{dt}{T} = \int e^{-2\pi i u T(1\mp|m|)} \omega(u)\, du =$$

$$\frac{t}{T} = u.$$

$$= \hat{\omega}\left(T(1 \mp |m|)\right)$$

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

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

Hence,

$$\sum \frac{1}{|m|^{3/2}} \hat{\omega}\, T(1+|m|) << \frac{1}{T^{100}} \sum \underbrace{\frac{1}{|m|^{3/2+100}}}_{\infty} << \frac{1}{T^{100}}.$$

$-\frac{3}{2} + 100 \to 2$

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

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

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

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

$$(*) \quad -\frac{4e^{i\pi/4}}{\pi} = C \neq 0 \quad !!!$$

$$\Longrightarrow \lim_{T\to\infty} A(T) = C \neq 0 \text{ so } S(t) \not\longrightarrow 0 \text{ as } t \to \infty. \text{ i.e } P(R) = \Omega(R^{1/2})$$

Hardy (maybe Littlewood 1920):

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

H. Cramer 1920:

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

Question:

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

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

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 $d=2$)

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

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

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

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

Fact:

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

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

Will show: $P_d(R) = \Omega(R^{d-2})$ (instead of $O(R^{\frac{d-1}{2}+\varepsilon})$)

$d-2 > \frac{d-1}{2} \iff d > 3$ 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.:

$r_4(n) \neq 0 \iff$ Every $n \geq 0$ is a sum of 4 squares.

Note:

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

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

Jacobi: ($d=4$)

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

Fermat: ($d=2$)

If p is prime $\equiv 3 \bmod 4 \implies p = a^2 + b^2$

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

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

We get $R^d = o(R^d)$ $\Downarrow$ in contradiction.

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)

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

$R^2 = n$

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

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

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

$$\Longrightarrow \theta \geq d-2$$

■

Conj for $d=3$:

$$N_3(R) - \omega_3 R^2 = O(R^{1+\varepsilon}) \quad \forall \varepsilon > 0.$$

Thm: (Gauss / Legandere)

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

Thm.:

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

$$n = x_1^2 + x_2^2 + x_3^2 \quad \Longleftrightarrow \quad n \neq 0, 4, 7 \mod 8$$

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

C.L Siegel: (1930)

$n \neq 0, 4, 7 \mod 8$ then $\forall \varepsilon > 0 \ \exists c(\varepsilon) > 0$. $r_3(n) > c(\varepsilon) n^{\frac{1}{2} - \varepsilon}$

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

Ex.

$$r_3(4^a) = 6$$

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

Fact:

$$\forall n \; \forall \varepsilon > 0. \; r_3(n) << n^{\frac{1}{2}+\varepsilon}$$

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

The Gaussian integers:

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

Fact:

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

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

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

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

$\Longrightarrow$ 1) Every ideal is principal

2) irreducible = prime

π is irr. if:
$\pi = \alpha\beta \Rightarrow \alpha$ or β are units
(units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$

$\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha$ or $\pi \mid \beta$

3) Unique factorization into primes.

$\forall \alpha \in \mathbb{Z}[i], \alpha \neq 0, \text{unit} \Rightarrow \alpha = \prod_j \pi_j$, π_j 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 $\left[N(\alpha) = \alpha\bar{\alpha}\right]$ then α is irred. in $\mathbb{Z}[i]$.

Example:

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

Proof:

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

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

$\beta, \gamma \in \mathbb{Z}$

$\Rightarrow N(\gamma) = 1$ or $N(\beta) = 1$. Cont. ↯

γ unit $\Leftrightarrow N(\gamma) = 1$

β unit $\Leftrightarrow N(\beta) = 1$

∎

Observe:

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

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

Thm. (Fermat)

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

[Easy: if $n \equiv 3 \bmod 4 \Rightarrow n \neq a^2+b^2$]

Proof:

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

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

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

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

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

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

(prime in $\mathbb{Z}[i]$)

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

$\pm 1 = pb$, $b \in \mathbb{Z}$. Cont ↯

∎

So:

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

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

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

So $r_2(p) > 0$ if $p \not\equiv 3 \bmod 4$, $r_2(2) = 4$.

Claim:

$r_3(p) = 8$, $p \equiv 1 \bmod 4$

Proof:

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

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

Pf:

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

α irred $\Rightarrow$ prime, $\alpha \mid \gamma$ or $\alpha \mid \delta$

but $N(p) = p^2 = N(\gamma\delta) = N(\gamma)N(\delta) \Rightarrow N(\gamma) = p = N(\delta)$, $N(\alpha) = p$

Thm.:

$$n = \square + \square \iff n = 2^a \prod_{p_j \equiv 1 \bmod 4} p_j^{b_j} \prod_{q_j \equiv 3 \bmod 4} q_j^{2c_j}$$

i.e. if $p \equiv 3 \pmod 4$ $n = p^\gamma m$ $p \nmid m$ then γ is even.

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

Thm.:

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

Conclusion:

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

Next time:

$$d(n) \ll n^\varepsilon \qquad \forall \varepsilon > 0.$$