Lecture 8: 9/5/2018

Gaussian Integers

$\mathbb{Z}[i] = \{ m+ni \mid m,n \in \mathbb{Z} \}$ norm $N(\alpha) = \alpha\bar{\alpha} = a^2+b^2$ where $\alpha = a+bi$

units ($\alpha \in \mathbb{Z}[i]$ s.t $\frac{1}{\alpha} \in \mathbb{Z}[i]$) $\pm 1, \pm i = \{ \alpha \mid N(\alpha) = 1 \}$

Euclidian:

$\forall \alpha, \beta \in \mathbb{Z}[i] \ \exists\, Q, R \in \mathbb{Z}[i] \quad \alpha = Q\beta + R, \quad N(R) \lneq N(\beta)$

Consequences:

Euclidian $\Longrightarrow$ PID (Principal ideal domain) $\Longrightarrow$

$\Longrightarrow$ UFD (unique factorization domain)

UFD: $\forall \alpha \in \mathbb{Z}[i]$, ($\alpha \neq 0$, unit) is a product of irreducibles in a unique way.

$\mathbb{C}[X_1, \dots, X_n]$ is a UFD but not a PID.

$\mathbb{Z}[\qquad]$ is a PID but not euclidian.

For $\mathbb{Z}[i]$: "irreducible" = "prime"

Irreducible: $\alpha = \beta\gamma \Longrightarrow \beta$ or γ is unit

Prime: $\alpha \mid \beta\gamma \Longrightarrow \alpha \mid \beta$ or $\alpha \mid \gamma$

Last time we classified irreducibles in $\mathbb{Z}[i]$:

1) Split: $p \equiv 1 \mod 4$, rational prime, then $p = \pi \cdot \bar{\pi} = a^2+b^2$, $\pi = a+bi$, $\pi, \bar{\pi}$ are irred. not associate

2) Inert: $q \equiv 3 \mod 4$ remain irreducible in $\mathbb{Z}[i]$

3) Ramified: $1+i$, $N(1+i) = 2$

Cor.:

p prime $p = \square + \square \iff p \equiv 2$ or $1 \mod 4$

Def.:

$$r_2(n) = \#\{ (a,b) \in \mathbb{Z}^2 \mid n = a^2+b^2 \}$$

If $p \equiv 1 \mod 4$ then $r_2(p) = 8$ & $r_2(2) = 4$.

Which integers n are $n = \square + \square$? What is $r_2(n)$?

<u>Thm:</u>

Write $n = 2^a \prod_{p_i \equiv 1(4)} p_i^{b_i} \prod_{q_j \equiv 3(4)} q_j^{c_j}$. Then $n = \square + \square \iff c_j$ even $\forall j$

& in that case $4d\left(\prod p_j^{b_j}\right) = 4\prod(b_j+1) = r_2(n)$

<u>Example:</u>

$r_2(10) = 4$, $r_2(5) = 4 \cdot 2 = 8$ $r_2(25) = 4(1+2) = 12$, $r_2(9) = 4$

<u>Proof:</u>

$n = a^2+b^2 = (a+bi)(a-bi)$ So we need to calculate

# of factorizations, $n = \nu\bar{\nu}$ $\nu \in \mathbb{Z}[i]$. Write in $\mathbb{Z}[i]$

$\nu = i^\delta (1+i)^a \prod \pi_j^{r_j} \bar{\pi}_j^{\bar{r}_j} \prod_{q_k \equiv 3 \mod 4} q_k^{c_k}$

$\delta \in \{0,1,2,3\}$

<u>Norm:</u>

$n = N(\nu) = N(i)^\delta \cdot 2^a \prod N(\pi_j)^{r_j} N(\bar{\pi}_j)^{\bar{r}_j} \prod N(q_k)^{c_k} =$

$= 2^a \prod p_j^{r_j+\bar{r}_j} \prod q_k^{2c_k}$ so a & q_k, c_k are

determined by n & p_j determined by n, $r_j + \bar{r}_j$ is

determined by $p_k^{r+\bar{r}} \| n$.

Norm will be $n = 2^a \prod p_k^{R_k} \prod q_k^{2c_k}$. $0 \leq r_k \leq R$.

get $R_k + 1$. The four comes from the 4 options for δ.

<u>Corollary:</u>

$r_2(n) \leq 4\, d(n)$. Average of $r_2(n)$ vs. $d(n)$.

$$\frac{1}{N} \sum_{n \leq N} d(n) \sim \log N + C + o(1).$$

So on average $d(n)$ is $\sim \log(n)$.

Scanned by CamScanner

Naive answer:

On average $r_2(n)$ is $\pi = 3.14\ldots$

$$\frac{1}{N}\sum_{n\le N} r_2(n) = \frac{1}{N}\sum_{n\le N} \#\{(x,y)\in\mathbb{Z}^2 \mid x^2+y^2=n\} =$$

$$= \frac{1}{N}\#\{(x,y)\in\mathbb{Z}^2 \mid x^2+y^2\le N\} \sim \frac{\pi N}{N} = \pi$$

However, only 0% of integers are $\square+\square$!!

Among primes the number of $\#\{p\le N \text{ prime} \mid p=\square+\square\} =$

$$= 1 + \#\{p\le N \mid p\equiv 1 \bmod 4\} = 1 + \frac{N}{2\log N} + \text{smaller}$$

Dirichlet:

$\gcd(a,q)=1$, $\quad \dfrac{\#\{p\le N \text{ prime} \mid p\equiv a\ (q)\}}{\#\{p\le N \mid p \text{ prime}\}} \sim \dfrac{1}{\phi(q)}$

Ex.:

look at $n = p_1 p_2$

- q^2 — $p_1=p_2=q$ — 0%
- $p_1, p_2 \equiv 1 \bmod 4$ ← the only good cases
- $p_1\equiv 1\ (4)$, $p_2\equiv 3\ (4)$, vice versa
- $p_1\equiv 3\ (4)$ & $p_2\equiv 3\ (4)$

Hence $\left(\frac{1}{2}\right)^2$ prob. that $n=\square+\square$.

There are $\log\log(N)$ primes typically so in prob

$$\frac{1}{2^{\log\log(N)}} = \frac{1}{\log N}, \quad N=\square+\square$$ & this goes to 0

as $N\to\infty$.

Thm: (E. Landau 1909)

$$\#\{n\le N \mid n=\square+\square\} \underset{N\to\infty}{\sim} K\frac{N}{\sqrt{\log N}}$$

$$K = 0.764\ldots = \frac{\pi}{4}\prod_{p\equiv 1(4)}\left(1-\frac{1}{p^2}\right)^{\frac{1}{2}} = \frac{1}{\sqrt{2}}\prod_{q\equiv 3(4)}\left(1-\frac{1}{q^2}\right)^{-1/2}$$

Compare Prime Number Theorem

$$\pi(n) = \#\{p\le N \mid p \text{ prime}\}, \quad \pi(N) \underset{N\to\infty}{\sim} Li(N) = \int_2^N \frac{1}{\log t}\,dt.$$

Pat 1940's:

$$\theta(N) = \sum_{p \le N} \log p \sim N, \text{ because } \int_2^N \frac{1}{\log t}\,dt = \frac{N}{\log N} + \frac{N}{(\log N)^2} + \cdots$$

Average growth of $r_2(n)$:

$$\frac{1}{\#\{n \le N \mid n = \square + \square\}} \underbrace{\sum_{\substack{n \le N \\ n = \square + \square}} r_2(n)}_{\sim \pi N} \sim \frac{\pi N}{K \cdot \frac{N}{\sqrt{\log N}}} = \frac{\pi}{K}\sqrt{\log N}$$

"On average" $r_2(n)$ is const $\cdot \sqrt{\log N}$.
(on average $d(n)$ is $\log N$).

Worse Case:

$n = p_1^{k_1} \cdots p_L^{k_L}$ then $d(n) = \prod_{j=1}^{L} (k_j + 1)$

Ex.:

$n_k = 2 \cdot 3 \cdots p_k$ product of first k primes, then $d(n_k) = 2^k$.

Note $\log(n_k) = \sum_{\substack{p \le p_k \\ \text{prime}}} \log(p) \sim p_k \sim k \log k$

$k \sim \frac{n_k}{\log n_k}$

$$d(n_k) \le 2^k \sim 2^{\log(n_k)/\log(\log(n_k))} = n^{\frac{2}{\log\log n}} \ll n^{\varepsilon} \ \forall \varepsilon >$$

Thm.:

$d(n) \ll n^{\varepsilon}$ $\forall \varepsilon > 0$. ($\forall \varepsilon > 0 \ \exists c > 0$ s.t $d(n) < c \cdot n^{\varepsilon}$)

Prop.:

Let $f(n)$ be a "multiplicative function" s.t $f(p^k) \xrightarrow[p^k \to \infty]{} 0$
$\forall$ prime powers, then $f(n) \xrightarrow[n \to \infty]{} 0$

Def.:

$f : \mathbb{N} \to \mathbb{C}$ is multiplicative if $f(1) = 1$ &
$f(mn) = f(m) f(n)$ if $\gcd(m,n) = 1$.

Application:

$f(n) = \frac{d(n)}{n^\delta}$, $d(n)$ is multiplicative $\Rightarrow f(n)$ is multiplicative.

$$f(p^k) = \frac{d(p^k)}{p^{k\delta}} = \frac{k+1}{p^{k\delta}} \xrightarrow[p^k\to\infty]{} 0 \Rightarrow \frac{d(n)}{n^\delta} \xrightarrow[n\to\infty]{} 0$$

$\forall \delta > 0$ & we proved the theorem from the Prop.

∎

Prop proof:

Want: Fix $\varepsilon > 0$ $\exists N_\varepsilon$ s.t $|f(n)| < \varepsilon$ $\forall n > N_\varepsilon$.

$\exists Q = Q_\varepsilon$ s.t $|f(p^k)| < \varepsilon$ $\forall p^k > Q$

Divide prime powers into 3 sets:

$Q_1 = \{p^k \le Q \mid |f(p^k)| \le 1\}$

$Q_2 = \{p^k \le Q \mid |f(p^k)| > 1\} \subseteq S = \{p^k \mid |f(p^k)| > 1\}$ finite set

$Q_3 = \{p^k \mid p^k > Q\}$

$A = \prod_{p^k \in S} |f(p^k)|$

$\forall n \gg 1$ write $n = n_1 \cdot n_2 \cdot n_3$, n_j = product of powers of primes in Q_j s.t n_1, n_2, n_3 co prime.

$$f(n) = f(n_1) f(n_2) f(n_3)$$

$$|f(n_1)| = \prod_{\substack{p^k \mid n \\ p^k \in Q_1}} |f(p^k)| \le 1$$

$$|f(n_2)| = \prod_{\substack{p^k \mid n \\ p^k \in Q_2}} |f(p^k)| \le \prod_{p^k \in S} |f(p^k)| = A \leftarrow \text{const}$$

$f(n_3)$: If $n \gg 1$, then $n_3 \ne 1$.

$$|f(n_3)| = \prod_{\substack{p^k \mid n \\ p^k > Q}} |f(p^k)| \le \prod \varepsilon \le \varepsilon \quad \text{So}$$

$|f(n)| \le 1 \cdot A \cdot \varepsilon = A\varepsilon$ so if $n \gg 1$ then

$$|f(n)| < A\varepsilon \Longleftrightarrow f(n) \longrightarrow 0.$$

So $d(n) = O(n^\varepsilon)$, $r_2(n) = O(n^\varepsilon)$ $\forall \varepsilon > 0$.

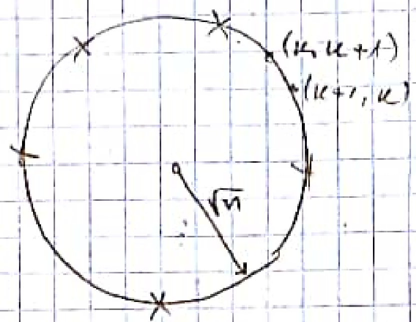
$\boxtimes$

Lattice Points on short arcs:

Take $n = \square + \square$ look at lattice points (a,b) on circle of radius $\sqrt{n}$.

Average dist between two neighbours $= \frac{2\pi\sqrt{n}}{r_2(n)} \gg n^{\frac{1}{2}-\varepsilon}$

But can have close lattice points.



Examples:

The distance between $(k+1, k)$ & $(k, k+1)$ is $\sqrt{2} = O(1)$

$n = 2k^2 + 2k + 1 = (k+1)^2 + k^2$

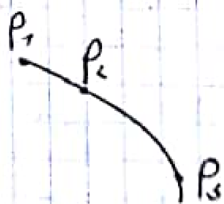
Question: Can one put 3 close lattice points?

Answer: No!

V. Jarnik (1926):

An arc of length $8R^{1/3}$ on the circle $x^2+y^2=R^2$ cannot contain 3 lattice points.

Pf 1:



Take 3 lattice points, & we will show

$$|P_1 - P_2||P_2 - P_3||P_1 - P_3| > c \cdot R$$

$\Longrightarrow (\max |P_i - P_j|)^3 \geq \text{product} > cR \Longrightarrow$

$\Longrightarrow \max |P_i - P_j| \gg R^{1/3}$

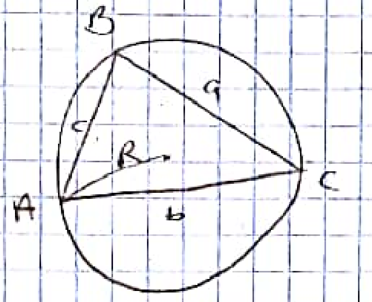
So enough to show $|P_1 - P_2||P_2 - P_3||P_1 - P_3| > cR$.

3 Points on the circle cannot be co-linear so span a triangle with positive area.

A lattice triangle has area $\geq \frac{1}{2}$.

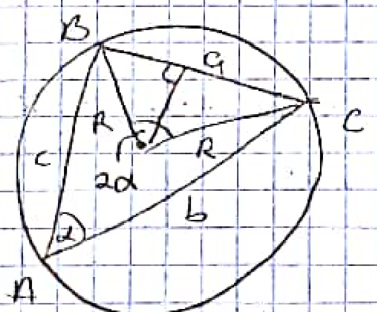
<u>pf:</u>

Herons formula for area of a triangle with sides a, b, c inscribed in a circle of radius R.



$4A \cdot R = a \cdot b \cdot c \Longrightarrow 4 \cdot A \cdot R \geq 4 \cdot \frac{1}{2} \cdot R = 2R$, on the other hand, it is $abc = |P_1 - P_2||P_2 - P_3||P_1 - P_3|$

<u>Proof of Heron's formula:</u>



$Area = \frac{1}{2} b \cdot c \sin\alpha$ & $\sin\alpha = \frac{a}{2R}$ so $A = \frac{1}{4}\frac{bca}{R}$

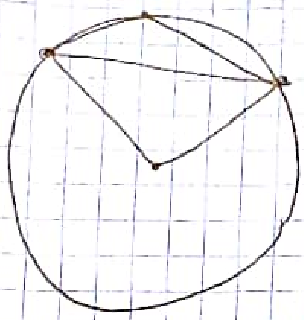
$\Longrightarrow 4AR = abc$.

<u>Second proof:</u>

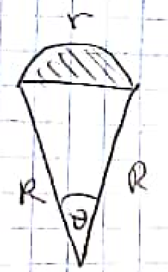
Give an upper bound for A in terms of

$\frac{\text{diamater}}{\text{arclength}} = \frac{r}{R}$ $\quad A \ll r^3/R$ & $A \geq \frac{1}{2}$

that finishes the proof



A = area of cap



The area of is $\frac{rR}{2}$ & of is
$\frac{1}{2}R^2\sin\theta \approx \frac{1}{2}R^2\left(\theta - \frac{\theta^3}{6}\right)$ so is:

$\frac{1}{2}R^2\frac{\theta^3}{6} = \frac{1}{12}R^2\left(\frac{r^3}{R^3}\right) = \frac{1}{12}\frac{r^3}{R}$ as we wanted.

Because then $A \ll r^3/R$.

Exercise:
In dimension 3 show that all latice points in a cap of diamater $\ll R^{1/4}$ on sphere are co-planer.

Example:
3 lattice points in arc of length $\asymp R^{1/3}$

$R_n = 16n^6 + 4n^4 + 4n^2 + 1$

$(4n^3+1, 2n^2, 2n), (4n^3, 2n^2, 1), 4n^3-1, 2n^2, 2n)$

lie in arc of length $\sim 16R^{1/3}$