Lecture 32

March 30th

Unique factorization of Gaussian integers

$\alpha \in \mathbb{Z}[i]$

$\alpha = u\pi_1 \cdots \pi_r$

u: unit $\qquad \pi_i$ (normalize) Gaussian primes

$\begin{cases} \text{uniqueness} \leftarrow \text{use Gaussian prime divisibility property} \\ \text{existence} \leftarrow \text{use induction on norm} \end{cases}$

Suppose we have factorization up to α $N(\alpha) \leq N$

Let $\alpha \in \mathbb{Z}[i]$ with $N(\alpha) = N+1$

If α is a prime, nothing to prove.

If α is not a prime, $\alpha = \beta \cdot \gamma$. $N(\beta) < N(\alpha) = N+1$

$N(\gamma) < N(\alpha) = N+1$

u units on $\mathbb{Z}[i] \Leftrightarrow$ with $N(u) = N+1$

By induction hypothesis $\beta = \pi_1 \cdots \pi_r$

$\gamma = \pi_1' \cdots \pi_s'$

then $\alpha = \beta \cdot \gamma = \pi_1 \cdots \pi_r \cdot \pi_1' \cdots \pi_s'$

$\pi | \alpha\beta \Rightarrow \pi \ \alpha$ or $\pi | \beta$

$\pi | \alpha_1 \cdots \alpha_r \Rightarrow \pi | \alpha_i$ for some i

$\alpha = u\pi_1 \cdots \pi_r = v\pi_1' \cdots \pi_s'$

$\pi_1 | v\pi_1' \cdots \pi_s' \Rightarrow \pi_1 | \pi_i'$ for some i

By renumbering, let $\pi_i' = \pi_1'$ and divide by π_1'.

$\Rightarrow u\pi_2 \cdots \pi_r = v\pi_2' \cdots \pi_s'$

repeat the process

$R(N)$ = the number the ways to write N. as a sum of two squares

$S(m) = \#\{m = a^2 + b^2 : a \geq b \geq 0\}$

$S(p) = 1$, $p \equiv 1 \bmod 4$

$R(p) = 8$

$$\begin{aligned} 5 &= 2^2 + 1^2 = 1^2 + 2^2 \\ &= (-2)^2 + 1^2 = (-1)^2 + 2^2 \\ &= 2^2 + (-1)^2 = 1^2 + (-2)^2 \\ &= (-2)^2 + (-1)^2 = (-1)^2 + (-2)^2 \end{aligned}$$

$S(p_1 \cdots p_r) = 2^{r-1}$ $\quad p_i \equiv 1 \bmod 4$ distinct

$R(p_1 \cdots p_r) = 8 \cdot 2^{r-1}$

Thm (Legendre) N pos integer

D_1 = the number of positive divisors d of N s.t. $d \equiv 1 \bmod 4$

$D_3 = \cdots \qquad d \equiv 3 \bmod 4$

Then $R(N) = 4(D_1 - D_3)$

$R(p) = 4 \times 2 = 8$, $p \equiv 1 \bmod 4$

$p = 1 \cdot p$

$R(p_1 \cdots p_r) = 4 \times 2^r$ $\quad p_i \equiv 1 \bmod 4$ distinct

divisors of $p_1 \cdots p_r$ $\{1, p_1\}, \{1, p_2\}, \cdots, \{1, p_r\}$

divisors of $p_1 \cdots p_r$ are product of one from each set.

$\#$ of divisors $= \underbrace{2 \times 2 \cdots \times 2}_{r} = 2^r$.

e.g. $45 = 3^2 \times 5 = 3^2(2^2+1^2) = 6^2+3^2$

$D_1 = \{1, 5, 9, 45\}$

$D_3 = \{3, 15\}$

$R(45) = 4(4-2) = 8$

e.g. $N = 28949649300$

$= 2^2(5^2 \cdot 13^3)(3^2 \cdot 11^4)$

$5, 13 \equiv 1 \mod 4$

$3, 11 \equiv 3 \mod 4$

$2 = -i(1+i)$, $5 = (2+i)(2-i)$

$13 = (2+3i)(2-3i)$

$\Rightarrow N = -(i+1)^4(2+i)^2(2-i)^2(2+3i)^3(2-3i)^3 \cdot 3^2 \cdot 11^4$

prime factorization of N

Suppose $N = A^2+B^2 = (A+Bi)(A-Bi)$

By unique factorization

$A+Bi$ is a product of some of the primes dividing N ..

$A-Bi$ also divide N

So is $(a+bi)^e \mid A+Bi$

$(a-bi)^e \mid A-Bi$

$\Rightarrow A+Bi$ should be of the form

$A+Bi = \text{unit}\ (1+i)^2(2+i)^n(2-i)^{2-n}(2+3i)^m(2-3i)^{3-m} \cdot 3 \cdot 11^2$

$n = 0, 1, 2$, $m = 0, 1, 2, 3$

$A-Bi = \text{unit}\ (1+i)^2(2-i)^n(2+i)^{2-n}(2-3i)^m(2+3i)^{3-m} 3 \cdot 11^2$

$1-i = \underbrace{-i}_{\text{unit}}(1+i)$

There are 4 choices of unit $\pm 1, \pm i$

$R(N) = 4 \times 3 \times 4 = 48.$

$N = 2^t \cdot \underbrace{p_1^{e_1} \cdots p_r^{e_r}}_{p_i \equiv 1 \bmod 4} \cdot \underbrace{q_1^{f_1} \cdots q_s^{f_s}}_{q_j \equiv 3 \bmod 4}$

$2 = -i(1+i)^2$

$p_j = (a_j + b_j i)(a_j - b_j i)$

$\Rightarrow N = (-i)^t(1+i)^{2t} \cdot (a_1+b_1 i)^{e_1}(a_1-b_1 i)^{e_1} \cdots (a_r+b_r i)^{e_r}(a_r-b_r i)^{e_r} \cdot q_1^{f_1} \cdots q_s^{f_s}$

If f_j is odd for some j. N cannot be written as a sum of two squares

$\Rightarrow f_1, \dots, f_s$ all even.

$N = A^2+B^2 = (A+Bi)(A-Bi)$

$A+Bi = u(1+i)^t(a_1+b_1 i)^{x_1}(a_1-b_1 i)^{e_1-x_1} \cdots (a_r+b_r i)^{x_r}(a_r-b_r i)^{e_r-x_r} \cdot q_1^{f_1/2} \cdots q_s^{f_s/2}$

u unit $0 \le x_1 \le e_1$

$$R(N) = \begin{cases} 4(e_1+1)\cdots(e_r+1) & \text{if } f_1 \cdots f_s \text{ are all even} \\ 0 & \text{if one of } f_i \text{ is odd} \end{cases}$$

Claim: $$D_1 - D_3 = \begin{cases} (e_1+1)\cdots(e_r+1) & \text{if } f_1 \cdots f_s \text{ all even} \\ 0 & \text{o.w.} \end{cases}$$

Proof: Induction on s.

$s = 0$, $N = 2^t p_1^{e_1} \cdots p_r^{e_r}$, $D_3 = 0$

$D_1 = \#\{\text{odd divisors of } p_1^{e_1} \cdots p_r^{e_r}\} = (e_1+1)\cdots(e_r+1)$

Divisors of $p_1^{e_1} \cdots p_r^{e_r}$ are $p_1^{x_1} \cdots p_r^{x_r}$, $0 \le x_1 \le e_1, \dots, 0 \le x_r \le e_r$