Ring of Gaussian integers

Lecture 25

Pf of (3) $\Rightarrow$ (1): $\mathbb{Z}[i] \cong \dfrac{\mathbb{Z}[x]}{(x^2+1)}$.

Let a be an elt s.t $a^2 \equiv -1 \pmod{p}$

$$\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}[x]/(x^2+1)}{(p, x^2+1)/(x^2+1)}$$

$$\cong \frac{\mathbb{Z}[x]}{(p, x^2+1)}$$

$$\frac{R/I}{J/I} \cong R/J$$

$$\cong \frac{\mathbb{Z}[x]/(p)}{(p, x^2+1)/(p)}.$$

$(p)\mathbb{Z}[x] = (p)$.

$$\cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2+\bar{1})}$$

$$\left[\frac{\mathbb{Z}[x]}{(p)} \cong \mathbb{Z}/p\mathbb{Z}[x]\right]$$

$$\cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x+a)(x-a)}.$$

Since a is a solution of $x^2 \equiv -1 \pmod{p}$

$\Rightarrow a$ is a root of the eqn $x^2 + 1 \equiv 0 \pmod{p}$.

Thus p is not irreducible.

Let π be an irreducible factor of p i.e $p = \pi\delta$ where δ is an non unit elt.

$\therefore N(p) = N(\pi)\,N(\delta) = p^2$

$\Rightarrow N(\pi) = p \quad [\because N(\delta) \neq 1]$

$\therefore \pi\overline{\pi} = p.$

Cor. [Fermat's two square Thm]

Let p be a prime int. Then p is a sum of two squares iff $p = 2$ or $p \equiv 1 \pmod{4}$

Cor. The irreducible elts of $\mathbb{Z}[i]$ are

(1) $(1+i)$ and its associates which has norm 2.

(2) prime integers p s.t $p \equiv 3 \pmod 4$.

(3) $a+ib$, $a-ib$ the distinct irreducible factors of $p = a^2+b^2$
$= (a+ib)(a-ib)$
for the prime with $p \equiv 1 \pmod 4$.

Q. Which integers can be written as sum of two squares?

Let $n \in \mathbb{N}$ want to write $n = A^2 + B^2$.

which is equivalent to write

n as norm of an elt $A+iB \in \mathbb{Z}[i]$.

i.e. $n = N(A+iB) = A^2 + B^2$.

Let $n = p_1 p_2 \cdots p_r$.

If $p_i \equiv 3 \pmod 4$ then p_i is irreducible elt. $N(p_i) = p_i^2$

If $p_i \equiv 1 \pmod 4$ then $p_i = \pi\overline{\pi}$

where π is an irreducible elt.

$N(\pi) = p_i$.

case 1. Let $n = p_1 p_2 \cdots p_r$ s.t all $p_i \equiv 1 \pmod 4$ i.e $p_i = \pi_i \overline{\pi_i}$ for some irreducible elt π_i s.t $N(\pi_i) = p_i$, where $\pi_i = a+ib$

what will be $A+iB$ s.t

$$N(A+iB) = n \ ?$$

$$A+iB = \pi_1 \pi_2 \cdots \pi_r.$$

$$N(A+iB) = N(\pi_1) N(\pi_2) \cdots N(\pi_r)$$

$$= p_1 p_2 \cdots p_r = n.$$

$$\boxed{(A+iB) = \overline{\pi_1}\ \overline{\pi_2} \cdots \overline{\pi_r}}$$

Example. Can $n = 17 \times 29$ be written as sum of two squares?

Note both 17 & 29 are cong 1 mod 4.

$17 = (4+i)(4-i)$, $29 = (5+2i)(5-2i)$

$A + iB$ can be the following Nos

$(4+i)(5+2i) = 18 + 13i$

$(4+i)(5-2i) = 22 - 3i$

$(4-i)(5+2i) = 22 + 3i$

$(4-i)(5-2i) = 18 - 13i$

$N((A+iB)u) = N(A+iB)$.

There are 4 units in $\mathbb{Z}[i]$. So there will be total 16 possibilities for $A+iB$ s.t $N(A+iB) = n$

Case 2. Let $n = p_1^2 p_2 \cdots p_r$

s.t $p_1 \equiv 3 \pmod 4$ & $p_i \equiv 1 \pmod 4$

$\hookrightarrow N(p_1) = p_1^2$ for $i = 2, \ldots, r$.

$$A + iB = p_1 \alpha_2 \alpha_3 \cdots \alpha_r$$

Propn Let n be a $+$ve int and

$$n = 2^k p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$$

where $p_1, \ldots, p_r$ are distinct primes cong to 1 mod 4 and $q_1, \ldots, q_s$ are distinct primes cong to 3 mod 4. Then n can be written as sum of two squares in $\mathbb{Z}$ iff each b_i is even and in this case the number of

representation of n as a sum of two squares is

$$4(a_1+1)(a_2+1)\cdots(a_r+1).$$

Pf: Assume all b_i's are even

$\times$ $p_i = \pi_i \overline{\pi_i}$ for $i = 1, \ldots, r$.

$$A+iB = (1+i)^k \left(\pi_1^{a_{1,1}} \overline{\pi_1}^{a_{1,2}}\right)\cdots$$

$$\cdots \left(\pi_r^{a_{r,1}} \overline{\pi_r}^{a_{r,2}}\right) q_1^{b_1/2} \cdots q_s^{b_s/2}.$$

with non-negative int a_{i1}, a_{i2} satisfies $a_{i1} + a_{i2} = a_i$ for $i = 1, \ldots, r$. Since $a_{i,1}$ can have values $0, 1, \ldots, a_i$ there are total $(a_1+1)(a_2+1)\cdots(a_r+1)$

distinct elts $(A+iB)$ in $\mathbb{Z}[i]$.
with norm n.