Ring of Gaussian Integers

Lecture 32

Q1. Which integers can be written as sum of two squares?

Let $n \in \mathbb{Z}$ want to write $n = A^2 + B^2$. which is equivalent to write n as norm of an elt $A + iB \in \mathbb{Z}[i]$

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

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

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

If $p_i \equiv 1 \pmod 4$ then $p_i = \pi \bar{\pi}$ 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 $p_i = \pi_i \bar{\pi}_i$

what will be $A + iB$ s.t

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

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

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

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

$$A + iB = \pi_1 \bar{\pi}_2 \bar{\pi}_3 \cdots \bar{\pi}_r$$

Example Can 17.29 be written as sum of two squares?

Both 17 & 29 are cong 1 mod 4.

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

$A+iB$ can be the following elts.

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

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

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

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

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

There are 4 units in $\mathbb{Z}[i]$. So there will 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 $p_1 \equiv 3 \pmod 4$ & $p_i \equiv 1 \pmod 4$ for $i = 2, \ldots, r$.

$A+iB = p_1 \pi_2 \pi_3 \cdots \pi_r$.

Propn. Let n be a +ve int and write

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

where $p_1, \ldots, p_r$ are distinct primes congruence to $1 \bmod 4$ and $q_1, \ldots, q_s$ are distinct primes congruence to $3 \bmod 4$. Then n can be written as sum of two squares in $\mathbb{Z}$ i.e $n = A^2 + B^2$ with $A, B \in \mathbb{Z}$ iff each b_i is even and in this case the number of representations of n as a sum of two squares is

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

note that $2 = (1+i)(1-i)$.

Pf: First statement I have already discussed. Assume that all b_i's are even & $p_i = \pi_i \bar{\pi}_i$ for $i = 1, \ldots, r$.

$$A+iB = (1+i)^k \left(\pi_1^{a_{1,1}} \bar{\pi}_1^{a_{1,2}}\right) \cdots$$

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

with non-negative integers $a_{i,1}, a_{i,2}$ satisfying $a_{i,1} + a_{i,2} = a_i$ for $i = 1, \ldots, r$. Since $a_{i,1}$ can have the 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. Since there are 4 units in $\mathbb{Z}[i]$ the statement is proved.

Polynomial rings over UFD

Q1. If R is an UFD then is $R[x]$ is an UFD?

Q2. Let R be an UFD and K be the quotient field of R. Let $f(x) \in R[x]$ be a poly. Would like relate the factorization of $f(x)$ in $R[x]$ and also in $K[x]$.

$p_i'(x) \in K[x]$ $\quad p_1'(x) \cdots p_r'(x) = f(x)$ in $K[x]$

$p_1(x) \cdots p_r(x) = f(x) \in R[x]$

$p_i \in R[x]$

Consider the poly $f_x \in \mathbb{Z}[x]$

Is it irreducible in $\mathbb{Z}[x]$? Is it irreducible over $\mathbb{Q}[x]$?