Lecture 11 Friday Feb 12

Next goal:

Given integer $n \geq 1$

Write n as sum of two squares:

$$n = a^2 + b^2 \qquad a, b \in \mathbb{Z}$$

How many sols for a, b ?

Define

$$Sol(n) = \left\{ (a,b) \mid a,b \in \mathbb{Z},\ n = a^2+b^2 \right\}$$

$$\#(n) = |Sol(n)|$$

Find $\#(n)$

Examples

n	a	b	$\#(n)$
9	0 ± 3	± 3 0	4
14	name		0
18	± 3	± 3	4
20	± 4 ± 2	± 2 ± 4	8
25	± 4 ± 3 ± 5 0	± 3 ± 4 0 ± 5	12
65	± 7 ± 4 ± 8 ± 1	± 4 ± 7 ± 1 ± 8	16

LEM 18 For an integer $n \geq 1$,

(i) $\exists$ bijection

$$\begin{aligned} Sol(n) &\longrightarrow Sol(2n) \qquad * \\ (a,b) &\longrightarrow (a-b,\ a+b) \end{aligned}$$

(ii) the inverse bijection is

$$\begin{aligned} Sol(2n) &\longrightarrow Sol(n) \qquad ** \\ (A,B) &\longrightarrow \left(\frac{A+B}{2},\ \frac{B-A}{2}\right) \end{aligned}$$

(iii) $\#(n) = \#(2n)$

pf (i), (ii) check * is function:

$a^2+b^2=n$

$(a-b)^2 + (a+b)^2 = a^2 - 2ab + b^2 + a^2 + 2ab + b^2 = 2n$ ✓

check ** is function:

Fn $A^2+B^2 = 2n$ (even)

$A \pm B$ even

A, B same parity

$\frac{A+B}{2}, \frac{B-A}{2} \in \mathbb{Z}$

$$\left(\frac{A+B}{2}\right)^2 + \left(\frac{B-A}{2}\right)^2 = n \quad ✓$$

One checks *, ** are inverses.

(iii) Since bijection exists

□

Notation

For an integer $n \geq 1$

Define

$$\text{Div}(n) = \text{number of positive integer divisors of } n$$

$$= \left| \{ d \in \mathbb{Z} \mid d \geq 1, \quad d \mid n \text{ in } \mathbb{Z} \} \right|$$

Ex $n = 6$

divisors of 6: 1, 2, 3, 6

$$\text{Div}(6) = 4$$

Fact $n \geq 1$ factor n over $\mathbb{Z}$:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

$p_1, p_2, \ldots, p_s$ mutually distinct primes (pos)

Fact an integer $d \geq 1$,

$d \mid n$ iff

$$d = p_1^{f_1} p_2^{f_2} \cdots p_s^{f_s}$$

$$0 \leq f_i \leq e_i \qquad (1 \leq i \leq s)$$

$$\text{Div}(n) = (e_1+1)(e_2+1) \cdots (e_s+1)$$

For an integer $n \geq 1$

Find $\#(n)$

Factor

$$n = E P Q$$

For integers E, P, Q such that

each prime factor of E is 2

" " P is $\equiv 3 \pmod 4$

" " Q is $\equiv 1 \pmod 4$

Thm 19 With above notation,

$$\#(n) = \begin{cases} 0 & \text{if } P \text{ is not a square in } \mathbb{Z} \\ 4\,\mathrm{Div}(Q) & \text{if } P \text{ is a square in } \mathbb{Z} \end{cases}$$

Examples

n	E	P	Q	P a square?	Div(Φ)	n
9	1	3^2	1	Y	1	4
14	2	7	1	N	1	0
18	2	3^2	1	Y	1	4
20	2^2	1	5	Y	2	8
25	1	1	5^2	Y	3	12
65	1	1	5·13	Y	4	16

Pf of thm 19

By Lem 18 WLOG n is odd, so $E = 1$:

$$n = P Q$$

Factor P, Q over $\mathbb{Z}$:

$$P = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

mutually dist pos prime integers $p_1, p_2, \ldots, p_s$ all $\equiv 3 \pmod 4$

pos integers $e_1, e_2, \ldots, e_s$

$$Q = q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t}$$

mutually dist pos prime integers $q_1, q_2, \ldots, q_t$ all $\equiv 1 \pmod 4$

pos integers $f_1, f_2, \ldots, f_t$

Factor P, Q over $\mathbb{Z}[i]$:

Fix $1 \le j \le s$

p_j is prime in $\mathbb{Z}[i]$ (by LEM 15)

Fix $1 \le j \le t$ $\exists$ integers $a_j, b_j > 0$ s.t. (by LEM 14)

$$q_j = a_j^2 + b_j^2$$

So in $\mathbb{Z}[i]$,

$$q_j = (a_j + ib_j)(a_j - ib_j)$$

$\uparrow$ $\nearrow$ (by LEM 16)

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

Note

$a_j + ib_j$, $a_j - ib_j$ not associates

since q_j is odd

In $\mathbb{Z}[i]$, prime factorization of n is

$$n = \prod_{j=1}^{s} p_j^{e_j} \times \prod_{j=1}^{t} (a_j + ib_j)^{f_j} (a_j - ib_j)^{f_j}$$

mutually non assoc primes in $\mathbb{Z}[i]$

Obs

$\#(n) =$ number of factorizations

$n = x \bar{x}$ $\quad x \in \mathbb{Z}[i]$

Given a solution x,

$x \mid n$ in $\mathbb{Z}[i]$

So

$$x = u \prod_{j=1}^{s} p_j^{E_j} \times \prod_{j=1}^{t} (a_j + ib_j)^{F_j} (a_j - ib_j)^{F_j'}$$

where

u is unit in $\mathbb{Z}[i]$,

$0 \le E_j \le e_j$ $\quad 1 \le j \le s$

$0 \le F_j, F_j' \le f_j$ $\quad 1 \le j \le t$

Observe

$$\bar{x} = \underset{\| \; u^{-1}}{\bar{u}} \prod_{j=1}^{s} p_j^{E_j} \times \prod_{j=1}^{t} (a_j - i b_j)^{F_j} (a_j + i b_j)^{F_j'}$$

Since $n = x\bar{x}$, require

$$2E_j = e_j \qquad 1 \le j \le s$$

$$F_j + F_j' = f_j \qquad 1 \le j \le t$$

No sol'n x unless

e_j is even $\quad 1 \le j \le s$

ie p is a square in $\mathbb{Z}$

For such p, the solutions x correspond to the sequences

$$u, F_1, F_2, \ldots, F_t$$

where

u is a unit in $\mathbb{Z}[i]$ (4 choices)

$$0 \le F_j \le f_j \qquad 1 \le j \le t$$

($f_j + 1$ choices)

So

$$\#(n) = 4 \prod_{j=1}^{t} (f_j + 1)$$

$$= 4 \, \mathrm{Div}(\varphi)$$

□