Lecture 2

Recall the square-free part of an integer. We can write $n = a^2 b$ where $a \in \mathbb{N}$ and $b \in \mathbb{N}$ is square free.

Theorem: Let $n \in \mathbb{N}$ s.t. $\exists\, x, y \in \mathbb{Z}$ $n = x^2 + y^2 \iff$ The sq. free part b of n has no prime factors $\equiv 3 \bmod 4$.

Pf "$\Leftarrow$" b has no prime factors that is $\equiv 3 \bmod 4$. So all prime factors of b are $\equiv 1, 2 \bmod 4$. $\Rightarrow$ $b = 2 p_1 p_2 \ldots p_k$ where $p_i \equiv 1 \bmod 4$.

Each p_i can be written as sum of two squares: say $p_i = r_i^2 + s_i^2$

But product of two sum of squares is again a sum of square.

$$(r_1^2+s_1^2)(r_2^2+s_2^2)$$

$$= r_1^2 r_2^2 + s_1^2 r_2^2 + r_1^2 s_2^2 + s_1^2 s_2^2$$

$$= r_1^2 r_2^2 + s_1^2 s_2^2 + 2 r_1 r_2 s_1 s_2$$
$$+ r_1^2 s_2^2 + r_2^2 s_1^2 - 2 r_1 r_2 s_1 s_2$$

$$= (r_1 r_2 + s_1 s_2)^2 + (r_1 s_2 - r_2 s_1)^2$$

"$\Rightarrow$" Let $n = r^2 + s^2$. We need to show that no prime p with $p \equiv 3 \bmod 4$ divides b. Equivalently, we may show if $p \mid n$ & $p \equiv 3 \bmod 4$ then p must divide a. But $a^2 \mid n \Rightarrow$ the maximal power p^N dividing n must have an even exponent.

We need to show that if $p \equiv 3 \mod 4$ & $p \mid n$ then p divides n even number of times.

We prove this by induction on n.

Base case : $n = 1$ obvious.

Inductive hypothesis : Holds for all $m \in \mathbb{N}$ with $m < n$.

Inductive step : $p \mid n = r^2 + s^2$

claim : $p \mid r$ & $p \mid s$.

Let $p \nmid r \Rightarrow GCD(r, p) = 1$

$\Rightarrow \exists t \in \mathbb{N}$ s.t. $rt \equiv 1 \mod p$

$$r^2 + s^2 \equiv 0 \mod p$$

$\Rightarrow t^2 r^2 + t^2 s^2 \equiv 0 \mod p$

$\Rightarrow t^2 s^2 \equiv -1 \mod p$

$\Rightarrow \left(\frac{-1}{p}\right) = 1$ $\lightning$ as $p \equiv 3 \mod 4$

$\Rightarrow p \mid r \Rightarrow p \mid s$

Hence, we can find r', s' s.t. $r = pr'$ & $s = ps'$.

But $n = r^2 + s^2 = p^2(r'^2 + s'^2) \Rightarrow p^2 \mid n$

$\Rightarrow \quad n/p^2 =: n' = r'^2 + s'^2$

But $n' < n$.

Inductive hypothesis $\Rightarrow$ the assertion is true for n'. Thus it is true for $n = p^2 n'$. $\square$

<u>Theorem</u> (<u>Legendre</u> & <u>Gauss</u>)

Every positive integer can be written as sum of 3 squares except the ones of the form $4^r(8z+1)$ $r, z \in \mathbb{Z}_{\geq 0}$.

<u>Theorem (Lagrange)</u>

Every positive integers can be written as sum of 4 squares.

[Proofs are non-examinable].

Exercise 1: Write 13 as sum of two squares.

Exercise 2: Write 65 as sum of two squares

Sol^n: We saw previously that $13 = 2^2 + 3^2$ and $5 = 2^2 + 1^2$.

Thus $65 = 13 \times 5$

$$= (2^2 + 3^2) \times (2^2 + 1^2)$$

$$= (2 \times 2 + 3 \times 1)^2 + (2 \times 1 - 3 \times 2)^2$$

$$= 7^2 + 4^2$$

Also, $= (2 \times 2 - 3 \times 1)^2 + (2 \times 1 + 3 \times 2)^2$

$$= 1^2 + 8^2.$$

Exercise 3: Write 340 as sum of 2 squares in two different ways.