Recall: in last class, we studied which primes can be written as of sums of two squares, i.e.

$$p = a^2 + b^2.$$

Answer: A prime can be written as a sum of two squares if and only if $p=2$ or $p \equiv 1 \pmod 4$.

In today's class, we study:

Which integers can be written as sums of two squares?

Definition: Let n be an integer. n is <u>squarefree</u> if the prime decomposition of n is of the form

$$n = p_1 p_2 \cdots p_r$$

with p_i <u>distinct</u>.

Example: $12 = 2 \cdot 2 \cdot 3$ not squarefree

$15 = 3 \cdot 5$ squarefree.

Observation: for any integer n, n can be written in the form

$$n = n_1 n_2^2$$

where n_1 is a squarefree integer

and n_2 is an integer.

Remark: $\gcd(n_1, n_2)$ might be greater than 1.

Example: $24 = 2 \cdot 2 \cdot 2 \cdot 3$

$$= 2 \cdot 3 \cdot 2^2 = 6 \cdot 2^2$$

$n_1 = 6$ squarefree

$n_2^2 = 2^2$.

Question: how to write an integer n is this form?

Answer: By prime decomposition, we can write:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$$

with $\alpha_1, \cdots \alpha_r$ odd and $\beta_1, \cdots \beta_s$ even.

(We just need to rearrange the prime powers.)

Then $n_1 = p_1 p_2 \cdots p_r$

$$n_2 = p_1^{\frac{\alpha_1 - 1}{2}} p_2^{\frac{\alpha_2 - 1}{2}} \cdots p_r^{\frac{\alpha_r - 1}{2}} q_1^{\frac{\beta_1}{2}} \cdots q_s^{\frac{\beta_s}{2}}$$

We can check: $n = n_1 \cdot n_2^2$.

Sometimes, we call n_1 the <u>square free part</u> of n.

Theorem: Let n be an integer. We write $n = n_1 n_2^2$ with $n_1 = p_1 \cdots p_r$ being squarefree.

Then n can be written as sums of two squares if and only if each p_i is 2 or $\equiv 1 \pmod 4$.

Example: (1) $n = 15 \Rightarrow n_1 = 15 = 3 \cdot 5$

$3 \not\equiv 1 \pmod 4$

$\Rightarrow$ 15 can <u>not</u> be written as sums of two squares.

(2) $n = 45 = 5 \cdot 3^2 \Rightarrow n_1 = 5$

$5 \equiv 1 \pmod 4$

$\Rightarrow$ 45 can be written as sums of two squares

$45 = 6^2 + 3^2$.

To prove the theorem, we have two parts:

Let n be an integer and $n = n_1 n_2^2 = p_1 \cdots p_r n_2^2$

(1) If $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$,

then each prime of $p_1, \cdots p_r$ is

either 2 or congruent to 1 (mod 4).

(2) If each prime $p_1, \dots p_r$ is either 2 or $\equiv 1 \pmod 4$,

then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Observation: By the construction of $n = n_1 n_2^2$

$p \mid n_1 \Rightarrow ord_p(n)$ is an odd number.

· Therefore, (1) is saying that: let $n = a^2+b^2$ with $a, b \in \mathbb{Z}$.

if $ord_p(n)$ is odd, then $p \not\equiv 3 \pmod 4$

To prove (1), it suffices to prove this new statement.

Proof of (1) Proof by contradiction:

Let n be an integer such that

(i) $n = a^2 + b^2$ with $a, b \in \mathbb{Z}$

(ii) we can find a prime p such that

$ord_p(n)$ is odd and $p \equiv 3 \pmod 4$.

Since $ord_p(n)$ is odd, $p \mid n$. Then

(i) $\Rightarrow$ $a^2 + b^2 \equiv 0 \pmod p$

If $\gcd(a, p) = 1$, then

$b^2 \equiv -a^2 \pmod p$ and $-a^2$ is a QR

This implies $\left(\frac{-a^2}{p}\right) = \left(\frac{-1}{p}\right) = 1$

This is impossible since $p \equiv 3 \pmod 4$

Therefore $p \mid a$ and $p \mid b$

Then $n = a^2 + b^2 = p^2 \left\{ \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 \right\} \Rightarrow p^2 \mid n$.

We then look at $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2$

If $p \nmid \frac{n}{p^2}$, then $\mathrm{ord}_p(n) = 2$ A contradiction.

If $p \mid \frac{n}{p^2}$, we run the argument again

and we get $\frac{n}{p^4} = \left(\frac{a}{p^2}\right)^2 + \left(\frac{b}{p^2}\right)^2$ with $p^2 \mid a$, $p^2 \mid b$

We can always continuous this process

and finally we show $\mathrm{ord}_p(n)$ is even. A contradiction!

$\square$.

Proof of part (2): We prove (2) in the following steps:

<u>Step I</u>: Let p_1, p_2 be two primes being 2 or $1 \pmod 4$

Then $p_1 p_2 = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Recall: for $x, y, z, w \in \mathbb{R}$

$$(x^2+y^2)(z^2+w^2) = (xz+yw)^2 + (xw-yz)^2$$

By the choice of p_1, p_2 $\quad p_1 = a_1^2 + b_1^2$

$p_2 = a_2^2 + b_2^2$

Then $p_1 p_2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2)$

$$= (a_1 a_2 + b_1 b_2)^2 + (a_1 b_2 - a_2 b_1)^2$$

Step II: Let $n = p_1 \cdots p_r$ be squarefree and each p_i is 2 or $1 \pmod 4$ Then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$

Proof by induction on $\underline{r}$.

Step III: Let $n = n_1 n_2^2 = p_1 \cdots p_r \cdot n_2^2$ with $p_1, \cdots p_r$ are 2 or $1 \pmod 4$ Then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

By step II, $n_1 = a_1^2 + b_1^2$ for some $a_1, b_1 \in \mathbb{Z}$.

$$n = (a_1^2 + b_1^2) \cdot n_2^2$$

$$= (a_1 n_2)^2 + (b_1 n_2)^2$$

∎.