

Math 104B, Number Theory, Winter 2003.

Lecture 11. Sums of Squares.

Theorem. Let p be a prime.

there exist x and y with $(x, y) = 1$ and $p|x^2 + y^2$
 \Rightarrow there exist X and Y with $p = X^2 + Y^2$.

Proof. Let

$$S_0 = \{ \text{primes } p : \text{there exist } x \text{ and } y \text{ with } (x, y) = 1 \text{ and } p|x^2 + y^2 \}$$

and let

$$S = \{ \text{primes } p : \text{there exist } X \text{ and } Y \text{ with } p = X^2 + Y^2 \}.$$

We aim to show that $S_0 \subset S$. Let's index the elements of S_0 as $p_1 < p_2 < p_3 < \dots$. We will show by induction that $p_j \in S$ for every j . First note that $p_1 = 2$ since $2|1^2 + 1^2$. But $2 = 1^1 + 1^2$ so $2 \in S$. Now suppose that $p_1, \dots, p_{j-1} \in S$. We just need to show $p_j \in S$ and then by induction we are done.

Now $p_j|x^2 + y^2$ with $(x, y) = 1$. We claim that we can replace x and y with numbers of absolute value less than $p_j/2$. Indeed, write

$$x = p_j q + r, \quad y = p_j q' + r'$$

where $|r|, |r'| < p_j/2$. Then

$$p_j|x^2 + y^2 = (p_j q + r)^2 + (p_j q' + r')^2 = p_j^2 q^2 + 2p_j q r + r^2 + p_j^2 q'^2 + 2p_j q' r' + r'^2,$$

so $p_j|r^2 + r'^2$. Now $p_j \nmid r$ and $p_j \nmid r'$. Hence $p_j \nmid (r, r')$. But since

$$p_j \mid (r, r')^2 \left(\left(\frac{r}{(r, r')} \right)^2 + \left(\frac{r'}{(r, r')} \right)^2 \right)$$

we get

$$p_j \mid \left(\frac{r}{(r, r')} \right)^2 + \left(\frac{r'}{(r, r')} \right)^2.$$

Replacing x by $r/(r, r')$ and y by $r'/(r, r')$ we get that $p_j|x^2 + y^2$ with $(x, y) = 1$ and $|x|, |y| < p_j/2$. We see that $x^2 + y^2 < p_j^2/2$ so

$$\frac{x^2 + y^2}{p_j} < \frac{p_j}{2}.$$

Hence we can make the prime factorization

$$\frac{x^2 + y^2}{p_j} = q_1 \cdots q_s$$

where each prime q_j is less than p . But by the inductive hypothesis, each of the primes q_j is a sum of two squares, and last time we showed

Lemma 14.4.6. If a prime $q = a^2 + b^2$ divides $n = x^2 + y^2$ then n/q is a sum of two squares.

Hence applying this in our case we get

$$\begin{aligned} & \frac{x^2 + y^2}{q_1} && \text{is a sum of two squares} \\ \Rightarrow & \frac{x^2 + y^2}{q_1 q_2} && \text{is a sum of two squares} \\ \Rightarrow & \frac{x^2 + y^2}{q_1 q_2 q_3} && \text{is a sum of two squares} \\ \Rightarrow & \dots\dots\dots && \\ \Rightarrow & p_j = \frac{x^2 + y^2}{q_1 q_2 \cdots q_s} && \text{is a sum of two squares} \end{aligned}$$

This completes the proof.

We did an example of how to write a number as a sum of two squares using this method, and then we went through the last question on the practice midterm.