

Math 104B, Number Theory, Winter 2003.

Lecture 10. Sums of Squares.

Last Time we introduced quadratic residues and the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } p|a. \end{cases}$$

We also saw

Proposition 9.1.9. (Euler's Criterion). Let p be an odd prime and a an integer such that $(a, p) = 1$; then

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

In particular,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Theorem 14.4.7. Let p be an odd prime. Then

$$p \equiv 1 \pmod{4} \quad \Leftrightarrow \quad \text{there exist } x \text{ and } y \text{ with } p = x^2 + y^2.$$

(We can see that x and y must in fact be relatively prime.)

Proving \Leftarrow is trivial. Indeed if $p = x^2 + y^2$ then reducing modulo 4 the squares are 0 and 1, so p is 0, 1 or 2 modulo 4. Since p is odd we have $p \equiv 1 \pmod{4}$.

Proving the other direction is less trivial. We will start by showing the modified result:

Proposition. Let p be an odd prime. Then

$$p \equiv 1 \pmod{4} \quad \Leftrightarrow \quad \text{there exist } x \text{ and } y \text{ with } (x, y) = 1 \text{ and } p|x^2 + y^2.$$

Proof. We will use the fact that there is a close relationship between whether p divides a sum of two relatively prime squares and whether -1 is a quadratic residue modulo p . Indeed, notice that if $p|x^2 + y^2$ and $(x, y) = 1$ then we must have $(p, y) = 1$, since otherwise we get $p|y$ so $p|x^2$ so $p|x$ and $p|(x, y)$. But

$$(*) \quad p|x^2 + y^2, (p, y) = 1 \quad \Leftrightarrow \quad x^2 \equiv -y^2 \not\equiv 0 \pmod{p} \quad \Leftrightarrow \quad (xy^{-1})^2 \equiv -1 \pmod{p}.$$

Hence if p divides a sum of relatively prime squares, then -1 is a quadratic residue modulo p , which since p is odd implies that $p \equiv 1 \pmod{4}$. Conversely, if $p \equiv 1 \pmod{4}$

then -1 is a quadratic non-residue modulo p so there exists x with $x^2 \equiv -1 \pmod{p}$ which implies $p|x^2 + 1$.

We have now reduced Theorem 14.4.7 to proving the following.

$$\begin{aligned} \text{there exist } x \text{ and } y \text{ with } (x, y) = 1 \text{ and } p|x^2 + y^2 \\ \Rightarrow \qquad \qquad \text{there exist } X \text{ and } Y \text{ with } p = X^2 + Y^2. \end{aligned}$$

To prove this we defined the Gaussian integers $\mathbb{Z}[i]$ following Definitions 14.4.2, 14.4.3, and we proved

Lemma 14.4.4. $(a^2 + b^2)(c^2 + d^2)$ is a sum of two squares.

Proof.

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= (a + ib)\overline{(a + ib)}(c + id)\overline{(c + id)} = (a + ib)(c + id)\overline{(a + ib)(c + id)} \\ &= (ac - bd + i(ad + bc))\overline{(ac - bd + i(ad + bc))} = (ac - bd)^2 + (ad + bc)^2. \end{aligned}$$

and following the proof in the book 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.

We also gave examples.