

Math 104B, Number Theory, Winter 2003.

Lecture 12. Quadratic Reciprocity.

We just have a final Theorem to prove on sums of squares:

Theorem. Let $n = 2^{a_0} p_1^{a_1} \dots p_j^{a_j} q_1^{b_1} \dots q_k^{b_k}$ be the prime factorization of n , where p_1, \dots, p_j are distinct primes congruent to 1 modulo 4 and q_1, \dots, q_k are distinct primes congruent to 3 modulo 4. Then n is a sum of two squares if and only if all the q_j s are even.

Proof. First assume that n has the factorization given where the q_j s are even. Note that $2 = 1^2 + 1^2$ is a sum of two squares and

$$q_\ell^{b_\ell} = (q_\ell^{b_\ell/2})^2 + 0^2$$

is a sum of two squares. We already showed that any prime congruent to 1 modulo 4 is a sum of two squares. Hence n is a product of numbers all of which are sums of two squares, but such a number must be a sum of two squares because we showed that the product of $a^2 + b^2$ and $c^2 + d^2$ is also a sum of two squares, so by induction the same is true for any finite product of numbers each of which is a sum of two squares.

Conversely, suppose that $n = x^2 + y^2$. Then

$$n = (x, y)^2 \left(\left(\frac{x}{(x, y)} \right)^2 + \left(\frac{y}{(x, y)} \right)^2 \right).$$

If (x, y) has prime factorization $r_1^{c_1} \dots r_\ell^{c_\ell}$ where r_1, \dots, r_ℓ are distinct primes then $(x, y)^2$ has prime factorization $r_1^{2c_1} \dots r_\ell^{2c_\ell}$. However, we already showed that since $x/(x, y)$ and $y/(x, y)$ are relatively prime, any odd prime divisor of

$$\left(\frac{x}{(x, y)} \right)^2 + \left(\frac{y}{(x, y)} \right)^2$$

is congruent to 1 modulo 4. Hence we have the prime factorization

$$\left(\frac{x}{(x, y)} \right)^2 + \left(\frac{y}{(x, y)} \right)^2 = 2^{d_0} p_1^{d_1} \dots p_m^{d_m}$$

where p_1, \dots, p_m are distinct primes congruent to 1 modulo 4, and

$$n = 2^{d_0} p_1^{d_1} \dots p_m^{d_m} r_1^{2c_1} \dots r_\ell^{2c_\ell}.$$

All the prime factors of n which are congruent to 3 modulo 4 are among r_1, \dots, r_ℓ and are raised to an even power.

We now turn our attention back to quadratic residues.

Theorem 17.1.2. If p is an odd prime then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv 1, 7, \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8}. \end{cases}$$

Quadratic Reciprocity Theorem. If p and q are odd primes then

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

We will start by proving a Lemma called Gauss's Lemma. Recall

Fermat's Theorem. If p is prime and $p \nmid a = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. The elements $0, a, 2a, 3a, \dots, (p-1)a$ form a complete residue system modulo p . Indeed, these are all distinct modulo p since $ja \equiv ka \pmod{p} \Rightarrow j \equiv k \pmod{p}$ but $0, 1, 2, 3, \dots, (p-1)$ are all distinct modulo p . Since there are p of these elements, they form a complete residue system modulo p . Hence modulo p , the set

$$\{a, 2a, 3a, \dots, (p-1)a\}$$

is equal to the set

$$\{1, 2, 3, \dots, (p-1)a\}$$

and

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

and dividing both sides by $1 \cdot 2 \cdot 3 \cdots (p-1)$ we get

$$a^{p-1} \equiv 1 \pmod{p}.$$

To understand the Legendre symbol, let's consider instead the elements

$$S = \{a, 2a, 3a, \dots, \frac{p-1}{2}a\}.$$

Take the representatives of these elements in the absolute least residue system to get the set S' .

17.2.2. Gauss's Lemma. Let p be an odd prime and suppose $p \nmid a$. Let n be the number of negative terms in S' . Then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Examples. Let's check this for $\left(\frac{2}{11}\right)$ and $\left(\frac{3}{11}\right)$. Note that the quadratic residues modulo 11 are 1, 4, 9, 5, 3.

On the other hand using Gauss's Lemma, when $a = 2$,

$$S = \{2, 4, 6, 8, 10\}, \quad S' = \{2, 4, -5, -3, -1\}.$$

$n = 3$ and so by Gauss's Lemma $\left(\frac{2}{11}\right) = (-1)^3 = -1$.

For $a = 3$,

$$S = \{3, 6, 9, 12, 15\}, \quad S' = \{3, -5, -2, 1, 4\}.$$

and $n = 2$ and so by Gauss's Lemma $\left(\frac{3}{11}\right) = (-1)^2 = 1$.

Proof of Gauss's Lemma. Let s_i be the remainder of ai in the absolute least residue system modulo p , so $S' = \{s_1, \dots, s_{(p-1)/2}\}$. We first claim that the elements $|s_1|, \dots, |s_{(p-1)/2}|$ are just the elements $1, 2, \dots, (p-1)/2$ in some order. Indeed, with $1 \leq i, j \leq (p-1)/2$,

$$s_i = s_j \Rightarrow ai \equiv aj \pmod{p} \Rightarrow i \equiv j \pmod{p} \Rightarrow i = j,$$

and

$$s_i = -s_j \Rightarrow ai \equiv -aj \pmod{p} \Rightarrow i \equiv -j \pmod{p} \Rightarrow p|i + j,$$

which is impossible since $2 \leq i + j \leq p - 1$. Hence we see that $|s_1|, \dots, |s_{(p-1)/2}|$ are all distinct numbers between 1 and $(p-1)/2$, and since there are $(p-1)/2$ of them, they are $1, 2, \dots, (p-1)/2$ in some order. Hence

$$\begin{aligned} a^{(p-1)/2} 1 \cdot 2 \cdots \frac{p-1}{2} &\equiv a \cdot (2a) \cdots \frac{(p-1)a}{2} \\ &\equiv s_1 \cdot s_2 \cdots s_{(p-1)/2} \equiv (-1)^n 1 \cdot 2 \cdots \frac{p-1}{2}, \pmod{p} \end{aligned}$$

and cancelling $1 \cdot 2 \cdots \frac{p-1}{2}$ from both sides we get

$$a^{(p-1)/2} \equiv (-1)^n \pmod{p},$$

but by Euler's criterion we then get

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

and since both sides are ± 1 and p is odd, we get $\left(\frac{a}{p}\right) = (-1)^n$.

Now we are going to look at the set S directly and determine which elements are congruent to negative elements in the absolute least residue system. Let's take the example of $p = 11$ and see which elements are congruent to positive elements and which are congruent to negative elements in the absolute least residue system.

		⋮	
$-\frac{11}{2} < m < 0 :$	$-5, -4, -3, -2, -1$		-
$0 < m < \frac{11}{2} :$	$1, 2, 3, 4, 5$		+
$\frac{11}{2} < m < 11 :$	$6, 7, 8, 9, 10$		-
$11 < m < \frac{3 \cdot 11}{2} :$	$12, 13, 14, 15, 16$		+
		⋮	

We see that m is negative in the absolute least residue system modulo p if and only if there exists an odd j with

$$\frac{jp}{2} < m < \frac{(j+1)p}{2}.$$