LECTURE 9: QUADRATIC RESIDUES AND THE LAW OF QUADRATIC RECIPROCITY

1. Basic properties of quadratic residues

We now investigate residues with special properties of algebraic type.

Definition 1.1. (i) When $(a, m) = 1$ and $x^n \equiv a \pmod{m}$ has a solution, then we say that a is an n**th power residue modulo** m.
(ii) When $(a, m) = 1$, we say that a is a **quadratic residue** modulo m provided that the congruence $x^2 \equiv a \pmod{m}$ is soluble. If the latter congruence is insoluble, then we say that a is a **quadratic non-residue modulo** m.

Theorem 1.2. *Suppose that p is a prime number and $(a, p) = 1$. Then the congruence $x^n \equiv a \pmod{p}$ is soluble if and only if*

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

Proof. Let g be a primitive root modulo p. Then for some natural number r one has $a \equiv g^r \pmod{p}$. If

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

then

$$g^{\frac{r(p-1)}{(n,p-1)}} \equiv 1 \pmod{p}.$$

But since g is primitive, the latter congruence can hold only when

$$(p-1) \left| \frac{r(p-1)}{(n, p-1)} \right. ,$$

whence $(n, p-1) \mid r$. But by the Euclidean Algorithm, there exist integers u and v with $nu + (p-1)v = (n, p-1)$, so on writing $r = k(n, p-1)$, we obtain

$$a \equiv g^{k(n,p-1)} \equiv (g^{ku})^n (g^{p-1})^{kv} \equiv (g^{ku})^n \pmod{p}.$$

Thus a is indeed an nth power residue under these circumstances.

On the other hand, if the congruence $x^n \equiv a \pmod{p}$ is soluble, then

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

on making use of Fermat's Little Theorem. This completes the proof of the theorem. □

Example 1.3. Determine whether or not 3 is a 4th power residue modulo 17.

Observe that on making use of Theorem 1.2, the congruence $x^4 \equiv 3 \pmod{17}$ is soluble if and only if $3^{16/4} \equiv 1 \pmod{17}$, that is, if $81 \equiv 1 \pmod{17}$. Since this congruence is not satisfied, one finds that 3 is not a 4th power residue modulo 17.

Definition 1.4. When p is an odd prime number, define the **Legendre symbol** $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{when } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{when } a \text{ is a quadratic non-residue modulo } p, \\ 0, & \text{when } p \mid a. \end{cases}$$

Theorem 1.5 (Euler's criterion)**.** *When p is an odd prime, one has*

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

Proof. If $a^{(p-1)/2} \equiv 1 \pmod{p}$, then the desired conclusion is an immediate consequence of Theorem 1.2. The conclusion is also immediate when $p \mid a$. It remains to consider the situation in which $a^{(p-1)/2} \not\equiv 1 \pmod{p}$. Let a be an integer with $(a, p) = 1$, write $r = a^{(p-1)/2}$, and note that in view of Fermat's Little Theorem, one has $r^2 = a^{p-1} \equiv 1 \pmod{p}$, whence $r \equiv \pm 1 \pmod{p}$. Then if $r \not\equiv 1 \pmod{p}$, one necessarily has $r \equiv -1 \pmod{p}$. Thus, in the situation in which $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, wherein Theorem 1.2 establishes that a is a quadratic non-residue modulo p, one has $a^{(p-1)/2} \equiv -1 \pmod{p}$, and so the desired conclusion follows once again. This completes the proof of the theorem. □

Theorem 1.6. *Let p be an odd prime number. Then*
(i) for all integers a and b, one has

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right);$$

(ii) whenever $a \equiv b \pmod{p}$, one has

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right);$$

(iii) whenever $(a, p) = 1$, one has

$$\left(\frac{a^2}{p}\right) = 1 \quad \textit{and} \quad \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right);$$

(iv) one has

$$\left(\frac{1}{p}\right) = 1 \quad \textit{and} \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Proof. These conclusions are essentially immediate from Theorem 1.5. For example, the latter theorem shows that

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p},$$

and so the conclusion of part (i) of the theorem follows on noting that since p is odd, one cannot have $1 \equiv -1 \pmod{p}$. Parts (ii) and (iv) are trivial from the last observation, and part (iii) follows from Fermat's Little Theorem. □

Note: The number of solutions of the congruence $x^2 \equiv a \pmod{p}$ is given by $1 + \left(\frac{a}{p}\right)$. For when $(a,p) = 1$ and the congruence is soluble, one has two distinct solutions and $1 + \left(\frac{a}{p}\right) = 1 + 1 = 2$. In the corresponding case in which the congruence is insoluble, one has $1 + \left(\frac{a}{p}\right) = 1 + (-1) = 0$. When $(a,p) > 1$, one the other hand, one has the single solution $x \equiv 0 \pmod{p}$, and then $1 + \left(\frac{a}{p}\right) = 1 + 0 = 1$.

The above observation provides a means of analysing the solubility of quadratic equations. For if $(a,p) = 1$ and $p > 2$, then the congruence $ax^2+bx+c \equiv 0 \pmod{p}$ is soluble if and only if $(2ax+b)^2 \equiv b^2 - 4ac \pmod{p}$ is soluble, that is, if and only if either $b^2 - 4ac \equiv 0 \pmod{p}$, or else

$$\left(\frac{b^2 - 4ac}{p}\right) = 1.$$

The number of solutions of the congruence is therefore precisely

$$1 + \left(\frac{b^2 - 4ac}{p}\right).$$

It is clear from the multiplicative property of $\left(\frac{\cdot}{p}\right)$ that it suffices now to compute $\left(\frac{q}{p}\right)$ for odd prime numbers q and $\left(\frac{2}{p}\right)$ in order to calculate $\left(\frac{a}{p}\right)$ in general.

2. The law of quadratic reciprocity

We now come to one of the most beautiful results of our course — the Law of Quadratic Reciprocity, which Gauss called the "aureum theorema" ("golden theorem"). Euler was the first to make conjectures equivalent to Quadratic Reciprocity, but he was unable to prove it. Legendre also worked on this problem very seriously and developed many valuable ideas, in particular, he also introduced the Legendre symbol. Finally, Gauss gave a complete proof of the Law of Quadratic Reciprocity in 1797, when he was 19. Now there are over 200 different proofs of this fundamental result.

Theorem 2.1 (Law of Quadratic Reciprocity; Gauss)**.** *Let p and q be distinct odd prime numbers. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Rewriting the expression on the right hand side of the last equation in the shape

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)},$$

we see that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless p and q are **both** congruent to 3 modulo 4.

We a give the proof of quadratic reciprocity which is due to Eisenstein. It is based on the following way to compute the Legendre symbol:

Lemma 2.2 (Eisenstein)**.** *For an odd prime p and $(a,p)=1$,*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}\lfloor 2ka/p\rfloor}.$$

Proof. Let $E = \{2,4,\dots,p-1\}$. For every $x \in E$, we write

$$xa = \lfloor xa/p\rfloor p + r_x, \quad 0 \leqslant r_x < p.$$

We observe that each of the numbers $(-1)^{r_x} r_x$ is congruent to an element of E. This is clear when r_x is even, and when r_x is odd, $(-1)^{r_x} r_x \equiv p - r_x \pmod p$ where $p - r_x \in E$. We also claim that if $(-1)^{r_x} r_x \equiv (-1)^{r_y} r_y \pmod p$, then $x = y$. Indeed, if $r_x \equiv r_y \pmod p$, then $xa \equiv ya \pmod p$, and it follows that $x \equiv y \pmod p$. If $r_x \equiv -r_y \pmod p$, then $xa \equiv -ya \pmod p$, and $x \equiv -y \pmod p$, and $p|(x+y)$, but $x+y \leqslant 2(p-1)$, so that this is impossible. Hence, we conclude that

$$\{(-1)^{r_x} r_x \pmod p : x \in E\} = E,$$

and

$$\prod_{x\in E} x \equiv \prod_{x\in E} (-1)^{r_x} r_x \equiv (-1)^{\sum_{x\in E} r_x} \prod_{x\in E} r_x \pmod p.$$

On the other hand,

$$\prod_{x\in E} r_x \equiv \prod_{x\in E} xa \equiv a^{(p-1)/2} \prod_{x\in E} x \pmod p.$$

Since $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$, we deduce that

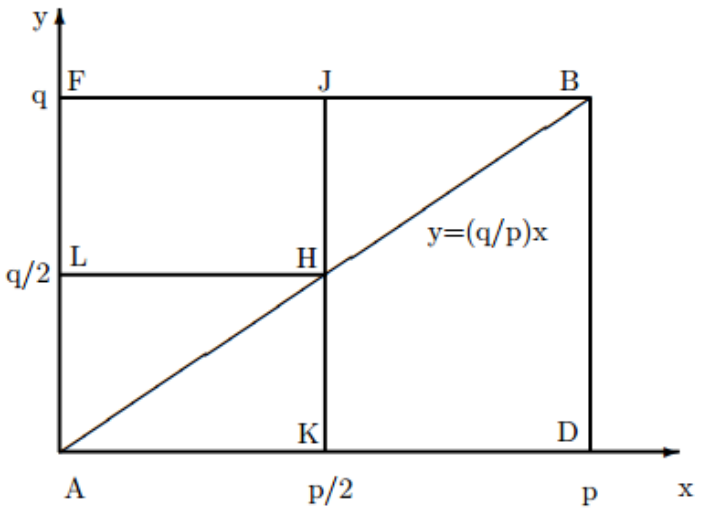
$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x\in E} r_x}.$$

Finally, we observe that $r_x \equiv \lfloor xa/p\rfloor \pmod 2$. This implies the lemma. □

Proof of Quadratic Reciprocity. We shall use the formulas for $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ provided by the Einsenstein Lemma. The main idea of the proof is that the sums

$$\sum_{k=1}^{(p-1)/2} \lfloor 2kq/p\rfloor \quad \text{and} \quad \sum_{k=1}^{(q-1)/2} \lfloor 2kp/q\rfloor$$

can be interpreted geometrically.



We may think about $\lfloor 2kq/p \rfloor$ as the number of points (x, y) with $x = 2k$ and y equal to positive integer at most $\lfloor 2kq/p \rfloor$. Then the sum $\sum_{k=1}^{(p-1)/2} \lfloor 2kq/p \rfloor$ is equal to the number of integral points with even x-coordinate contained in the interior of triangle ABD. Note that there are no integral points on the line AB (why?). We note that the number of integral points contained in the interior of rectangle $AFBD$ and lying on a fixed integral vertical line is equal to $q - 1$, thus, even. This implies that the number of integral points in $KHBD$ with even x-coordinate is equal modulo 2 to the number of integral points in HJB with even x-coordinate. We also observe that the transformation $(x, y) \to (p-x, q-y)$ send the integral points with even x-coordinates contained in HJB to the integral points with odd x-coordinates contained in AHK. Finally, we conclude that he number of integral points with even x-coordinate contained in the interior of triangle ABD is congruent modulo 2 to the sum of the integral points with odd x-coordinates contained in AHK plus the integral points with even x-coordinates contained in AHK, namely, it is precisely the number of integral points contained in AHK. We obtain that

$$\sum_{k=1}^{(p-1)/2} \lfloor 2kq/p \rfloor \equiv v_1 \pmod 2,$$

where v_1 is the number of integral points contained in AHK. The same argument gives that

$$\sum_{k=1}^{(q-1)/2} \lfloor 2kp/q \rfloor \equiv v_2 \pmod 2,$$

where v_2 is the number of integral points contained in ALH. In view of Eisenstein's Lemma,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{v_1+v_2},$$

but $v_1 + v_2$ is precisely the number of integral points in $ALHK$. Hence,

$$v_1 + v_2 = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

This completes the proof. □

Theorem 2.3. *For any odd prime p,*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Proof. We use that

$$\sum_{k=1}^{(p-1)/2} \lfloor 4k/p \rfloor = |\{k \in \mathbb{N} : \, p/4 < k < p/2\}| = \lfloor p/2 \rfloor - \lfloor p/4 \rfloor.$$

When $p = 8m \pm 1$, then

$$\sum_{k=1}^{(p-1)/2} \lfloor 4k/p \rfloor = \lfloor 4m \pm 1/2 \rfloor - \lfloor 2m \pm 1/4 \rfloor \equiv 0 \equiv (p^2-1)/8 \pmod 2.$$

When $p = 8m \pm 3$, then

$$\sum_{k=1}^{(p-1)/2} \lfloor 4k/p \rfloor = \lfloor 4m \pm 3/2 \rfloor - \lfloor 2m \pm 3/4 \rfloor \equiv 2m \pm 1 \equiv 1 \equiv (p^2-1)/8 \pmod 2.$$

□

Example 2.4. Determine the value of $\left(\dfrac{-3}{p}\right)$.

By Quadratic Reciprocity we have

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(3-1)(p-1)/4} = (-1)^{(p-1)/2},$$

and by Euler's criterion, on the other hand,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Thus we see that

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)/2}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

But

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\dfrac{1}{3}\right) = 1, & \text{when } p \equiv 1 \pmod 3, \\ \left(\dfrac{2}{3}\right) = -1, & \text{when } p \equiv 2 \pmod 3. \end{cases}$$

Thus we deduce that

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

One can use this evaluation to show that the only possible prime divisors of $x^2 + 3$, for integral values of x, are 3 and primes p with $p \equiv 1 \pmod 3$. From here, an argument similar to that due to Euclid shows that there are infinitely many primes congruent to 1 modulo 3.

Example 2.5. Determine the value of $\left(\frac{21}{71}\right)$.

Applying the multiplicative property of the Legendre symbol, followed by quadratic reciprocity, one finds that

$$\begin{aligned}\left(\frac{21}{71}\right) &= \left(\frac{3}{71}\right)\left(\frac{7}{71}\right) = (-1)^{(71-1)(3-1)/4+(71-1)(7-1)/4}\left(\frac{71}{3}\right)\left(\frac{71}{7}\right) \\ &= \left(\frac{71}{3}\right)\left(\frac{71}{7}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{7}\right) = \left(\frac{2}{3}\right) = -1.\end{aligned}$$

So $\left(\frac{21}{71}\right) = -1$, and hence 21 is not a quadratic residue modulo 71.