Introduction to Analytic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Quadratic Residues

Quadratic Residues and Nonresidues

- We will be concerned with quadratic congruences of the form

$$x^2 \equiv n \pmod{p},$$

where p is an odd prime and $n \not\equiv 0 \pmod{p}$.

- Since the modulus is prime we know that such a congruence has at most two solutions.
- Moreover, if x is a solution so is $-x$.
- Hence the number of solutions is either 0 or 2.

Definition

If the congruence has a solution, we say that n is a **quadratic residue mod** p and we write nRp.
If $x^2 \equiv n \pmod{p}$ has no solution we say that n is a **quadratic nonresidue mod** p and we write $n\overline{R}p$.

Basic Problems

- Two basic problems dominate the theory of quadratic residues.
  1. Given a prime p, determine which n are quadratic residues mod p and which are quadratic nonresidues mod p.
  2. Given n, determine those primes p for which n is a quadratic residue mod p and those for which n is a quadratic nonresidue mod p.

Example

- To find the quadratic residues modulo 11 we square the numbers $1, 2, \ldots, 10$ and reduce mod 11.
- We obtain

$$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 9,\ 4^2 \equiv 5,\ 5^2 \equiv 3 \pmod{11}.$$

- It suffices to square only the first half of the numbers since

$$6^2 \equiv (-5)^2 \equiv 3,\ 7^2 \equiv (-4)^2 \equiv 5, \ldots, 10^2 \equiv (-1)^2 \equiv 1 \pmod{11}.$$

- Consequently, the quadratic residues mod 11 are $1, 3, 4, 5, 9$.
- The quadratic nonresidues mod 11 are $2, 6, 7, 8, 10$.

Quadratic Residues Modulo a Prime

Theorem

Let p be an odd prime. Then every reduced residue system mod p contains exactly $\frac{p-1}{2}$ quadratic residues and exactly $\frac{p-1}{2}$ quadratic nonresidues mod p. The quadratic residues belong to the residue classes containing the numbers

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

- First we note that the given numbers are distinct mod p.
  If $x^2 \equiv y^2 \pmod{p}$, with $1 \leq x \leq \frac{p-1}{2}$ and $1 \leq y \leq \frac{p-1}{2}$, then
  $$(x-y)(x+y) \equiv 0 \pmod{p}.$$
  But $1 < x+y < p$. So $x-y \equiv 0 \pmod{p}$. Hence $x=y$.
  Since $(p-k)^2 \equiv k^2 \pmod{p}$, every quadratic residue is congruent mod p to exactly one of the numbers in the list.

Example

- The following brief table of quadratic residues R and nonresidues $\overline{R}$ was obtained with the help of the preceding theorem.

	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$
R	1	1, 4	1, 2, 4	1, 3, 4, 5, 9	1, 3, 4, 9, 10, 12
$\overline{R}$	2	2, 3	3, 5, 6	2, 6, 7, 8, 10	2, 5, 6, 7, 8, 11

Subsection 2

Legendre's Symbol and Its Properties

Legendre's Symbol

Definition

Let p be an odd prime. If $n \not\equiv 0 \pmod{p}$, we define **Legendre's symbol** $(n|p)$ as follows:

$$(n|p) = \begin{cases} +1, & \text{if } nRp \\ -1, & \text{if } n\overline{R}p \end{cases}$$

If $n \equiv 0 \pmod{p}$, we define $(n|p) = 0$.

Example:

- $(1|p) = 1$;
- $(m^2|p) = 1$;
- $(7|11) = -1$;
- $(22|11) = 0$.

- It is clear that $(m|p) = (n|p)$ whenever $m \equiv n \pmod{p}$.
- So $(n|p)$ is a periodic function of n with period p.

Consequence of Little Fermat Theorem

- The Little Fermat Theorem tells us that

$$n^{p-1} \equiv 1 \pmod{p}, \text{ if } p \nmid n.$$

- Note that

$$n^{p-1} - 1 = (n^{\frac{p-1}{2}} - 1)(n^{\frac{p-1}{2}} + 1).$$

- It follows that

$$n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Euler's Criterion

Theorem (Euler's Criterion)

Let p be an odd prime. Then, for all n we have

$$(n|p) \equiv n^{\frac{p-1}{2}} \pmod{p}.$$

- If $n \equiv 0 \pmod{p}$,

$$(n|p) = 0 \equiv n^{\frac{p-1}{2}} \pmod{p}.$$

If $(n|p) = 1$, then there is an x, such that $x^2 \equiv n \pmod{p}$.
Hence, we get

$$n^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 = (n|p) \pmod{p}.$$

Euler's Criterion (Cont'd)

- If $(n|p) = -1$, consider the polynomial

$$f(x) = x^{\frac{p-1}{2}} - 1.$$

$f(x)$ has degree $\frac{p-1}{2}$.
So the congruence $f(x) \equiv 0 \pmod{p}$ has at most $\frac{p-1}{2}$ solutions.
But the $\frac{p-1}{2}$ quadratic residues mod p are solutions.
So the nonresidues are not.
Hence, if $(n|p) = -1$,

$$n^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}.$$

But $n^{\frac{p-1}{2}} = \pm 1 \pmod{p}$.
So

$$n^{\frac{p-1}{2}} \equiv -1 \equiv (n|p) \pmod{p}.$$

Multiplicativity of Legendre's Symbol

Theorem

Legendre's symbol $(n|p)$ is a completely multiplicative function of n.

- If $p \mid m$ or $p \mid n$, then $p \mid mn$.

  So $(mn|p) = 0$ and either $(m|p) = 0$ or $(n|p) = 0$.

  Therefore, if $p \mid m$ or $p \mid n$, then $(mn|p) = (m|p)(n|p)$.

  If $p \nmid m$ and $p \nmid n$, then $p \nmid mn$.

  Moreover, we have

  $$(mn|p) \equiv (mn)^{\frac{p-1}{2}} = m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv (m|p)(n|p) \pmod{p}.$$

  But each of $(mn|p)$, $(m|p)$ and $(n|p)$ is 1 or -1.

  So the difference $(mn|p) - (m|p)(n|p)$ is either 0, 2, or -2.

  Since this difference is divisible by p, it must be 0.

Quadratic Character

- $(n|p)$ is a completely multiplicative function of n.
- Moreover, it is periodic with period p and vanishes when $p \mid n$.
- It follows that

$$(n|p) = \chi(n),$$

  where χ is one of the Dirichlet characters modulo p.
- The Legendre symbol is called the **quadratic character** mod p.

Subsection 3

Evaluation of $(-1|p)$ and $(2|p)$

Evaluation of $(-1|p)$

Theorem

For every odd prime p, we have

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

- By Euler's Criterion we have $(-1|p) \equiv (-1)^{\frac{p-1}{2}} \pmod p$.

  But each member of this congruence is 1 or -1.

  So the two members are equal.

Evaluation of $(2|p)$

Theorem

For every odd prime p, we have

$$(2|p) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8} \\ -1, & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

- Consider the following $\frac{p-1}{2}$ congruences:

$$\begin{array}{rcll} p-1 & \equiv & 1(-1)^1 & \pmod{p} \\ 2 & \equiv & 2(-1)^2 & \pmod{p} \\ p-3 & \equiv & 3(-1)^3 & \pmod{p} \\ 4 & \equiv & 4(-1)^4 & \pmod{p} \\ & \vdots & & \\ r & \equiv & \frac{p-1}{2}(-1)^{\frac{p-1}{2}} & \pmod{p}, \end{array}$$

where r is either $p - \frac{p-1}{2}$ or $\frac{p-1}{2}$.

Evaluation of $(2|p)$ (Cont'd)

- Multiply these together and note that each integer on the left is even:

$$2 \cdot 4 \cdot 6 \cdots (p-1) = \left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{p-1}{2}} \pmod{p}.$$

This gives us

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Since $(\frac{p-1}{2})! \not\equiv 0 \pmod{p}$, this implies

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

By Euler's Criterion we have $2^{\frac{p-1}{2}} \equiv (2|p) \pmod{p}$.

Since each member is 1 or -1, the two members are equal.

Subsection 4

Gauss' Lemma

Gauss' Lemma

Theorem (Gauss' Lemma)

Assume $n \not\equiv 0 \pmod{p}$ and consider the least positive residues mod p of the following $\frac{p-1}{2}$ multiples of n:

$$n, 2n, 3n, \ldots, \frac{p-1}{2}n.$$

If m denotes the number of these residues which exceed $\frac{p}{2}$, then

$$(n|p) = (-1)^m.$$

Gauss' Lemma (Cont'd)

- The numbers in the list are incongruent mod p.

  Consider their least positive residues.

  Distribute them into two disjoint sets A and B, according as the residues are $< \frac{p}{2}$ or $> \frac{p}{2}$.

  - $A = \{a_1, a_2, \ldots, a_k\}$ where each $a_i \equiv tn \pmod{p}$, for some $t \leq \frac{p-1}{2}$ and $0 < a_i < \frac{p}{2}$;
  - $B = \{b_1, b_2, \ldots, b_m\}$, where each $b_i \equiv sn \pmod{p}$, for some $s \leq \frac{p-1}{2}$ and $\frac{p}{2} < b_i < p$.

  Note that $m + k = \frac{p-1}{2}$, since A and B are disjoint.

  The number m of elements in B is pertinent in this theorem.

  Form a new set C of m elements by subtracting each b_i from p,

  $$C = \{c_1, c_2, \ldots, c_m\}, \quad c_i = p - b_i.$$

  Now $0 < c_i < \frac{p}{2}$.

  So the elements of C lie in the same interval as the elements of A.

Gauss' Lemma (Cont'd)

Claim: The sets A and C are disjoint.

Assume that $c_i = a_j$, for some pair i and j.

Then $p - b_j = a_j$.

Thus, $a_j + b_i \equiv 0 \pmod{p}$.

Therefore, for some s and t, with $1 < t < \frac{p}{2}$, $1 < s < \frac{p}{2}$,

$$tn + sn = (t+s)n \equiv 0 \pmod{p}.$$

But this is impossible since $p \nmid n$ and $0 < s + t < p$.

Now $A \cup C$ contains $m + k = \frac{p-1}{2}$ integers in the interval $[1, \frac{p-1}{2}]$.

Hence,

$$A \cup C = \{a_1, a_2, \ldots, a_k, c_1, c_2, \ldots, c_m\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

Gauss' Lemma (Conclusion)

- Form the product of all the elements in $A \cup C$ to obtain

$$a_1 a_2 \cdots a_k c_1 c_2 \cdots c_m = \left(\frac{p-1}{2}\right)!.$$

Since $c_i = p - b_i$, this gives us

$$\begin{aligned} (\tfrac{p-1}{2})! &= a_1 a_2 \cdots a_k (p-b_1)(p-b_2)\cdots(p-b_m) \\ &\equiv (-1)^m a_1 a_2 \cdots a_k b_1 b_2 \cdots b_m \pmod{p} \\ &\equiv (-1)^m n(2n)(3n)\cdots(\tfrac{p-1}{2}n) \pmod{p} \\ &\equiv (-1)^m n^{\frac{p-1}{2}} (\tfrac{p-1}{2})! \pmod{p}. \end{aligned}$$

Canceling the factorial we obtain $n^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p}$.
Euler's Criterion shows that $(-1)^m \equiv (n|p) \pmod{p}$.
Hence, $(-1)^m = (n|p)$.

Determining the Parity of m

Theorem

Let m be the number defined in Gauss' Lemma. Then

$$m \equiv \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right] + (n-1)\frac{p^2-1}{8} \pmod{2}.$$

In particular, if n is odd, we have

$$m \equiv \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right] \pmod{2}.$$

Determining the Parity of m

- Recall that m is the number of least positive residues of the numbers $n, 2n, 3n, \ldots, \frac{p-1}{2}n$ which exceed $\frac{p}{2}$.

  Take a typical number, say tn, divide it by p and examine the size of the remainder.

  We have
  $$\frac{tn}{p} = \left[\frac{tn}{p}\right] + \left\{\frac{tn}{p}\right\}, \quad 0 < \left\{\frac{tn}{p}\right\} < 1.$$
  So
  $$tn = p\left[\frac{tn}{p}\right] + p\left\{\frac{tn}{p}\right\} = p\left[\frac{tn}{p}\right] + r_t,$$
  say, where $0 < r_t < p$.

  So $r_t = tn - p[\frac{tn}{p}]$ is the least positive residue of tn modulo p.

Determining the Parity of m (Cont'd)

- Referring again to A and B in the proof of Gauss' Lemma:
  - $\{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\} = \{a_1, a_2, \ldots, a_k, b_1, \ldots, b_m\}$;
  - $\{1, 2, \ldots, \frac{p-1}{2}\} = \{a_1, a_2, \ldots, a_k, c_1, \ldots, c_m\}$, where $c_i = p - b_i$.

  Now we compute the sums of the elements in these sets to obtain the two equations

$$\begin{aligned}\sum_{t=1}^{\frac{p-1}{2}} r_t &= \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j;\\ \sum_{t=1}^{\frac{p-1}{2}} t &= \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} c_j = \sum_{i=1}^{k} a_i + mp - \sum_{j=1}^{m} b_j.\end{aligned}$$

  In the first equation we replace r_t by its definition to obtain

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j = n \sum_{t=1}^{\frac{p-1}{2}} t - p \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right].$$

Determining the Parity of m (Cont'd)

- The second equation is

$$mp + \sum_{i=1}^{k} a_i - \sum_{j=1}^{m} b_j = \sum_{y=1}^{\frac{p-1}{2}} t.$$

Adding these, we get

$$\begin{aligned} mp + 2\textstyle\sum_{i=1}^{k} a_i &= (n+1)\textstyle\sum_{t=1}^{\frac{p-1}{2}} t - p\textstyle\sum_{t=1}^{\frac{p-1}{2}} [\frac{tn}{p}] \\ &= (n+1)\frac{p^2-1}{8} - p\textstyle\sum_{t=1}^{\frac{p-1}{2}} [\frac{tn}{p}]. \end{aligned}$$

Note that $n+1 \equiv n-1 \pmod 2$ and $p \equiv 1 \pmod 2$. So reducing the preceding modulo 2,

$$m \equiv (n-1)\frac{p^2-1}{8} + \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tn}{p}\right] \pmod 2.$$

Subsection 5

The Quadratic Reciprocity Law

The Quadratic Reciprocity Law

- The quadratic reciprocity law states that if p and q are distinct odd primes, then:
  - $(p|q) = -(q|p)$, if $p \equiv q \equiv 3 \pmod 4$;
  - $(p|q) = (q|p)$, in all other cases.

Theorem (Quadratic Reciprocity Law)

If p and q are distinct odd primes, then

$$(p|q)(q|p) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

- By Gauss' Lemma and the preceding theorem, we have

$$(q|p) = (-1)^m,$$

where

$$m \equiv \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tq}{p}\right] \pmod 2.$$

The Quadratic Reciprocity Law (Cont'd)

- Similarly,

$$(p|q) = (-1)^n,$$

where

$$n \equiv \sum_{s=1}^{\frac{q-1}{2}} \left[\frac{sp}{q}\right] \pmod 2.$$

Hence

$$(p|q)(q|p) = (-1)^{m+n}.$$

So the conclusion follows at once from the identity

$$\sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tq}{p}\right] + \sum_{s=1}^{\frac{q-1}{2}} \left[\frac{sp}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}.$$

The Quadratic Reciprocity Law (Cont'd)

- Consider the function

$$f(x,y) = qx - py.$$

If x and y are nonzero integers, then $f(x,y)$ is a nonzero integer.
Let:
  - x range over the values $1, 2, \ldots, \frac{p-1}{2}$;
  - y range over the values $1, 2, \ldots, \frac{q-1}{2}$

Then $f(x,y)$ takes $\frac{p-1}{2}\frac{q-1}{2}$ values.

No two of these $\frac{p-1}{2}\frac{q-1}{2}$ values are equal.

We have

$$f(x,y) - f(x',y') = f(x-x', y-y') \neq 0.$$

We count the number of values of $f(x,y)$ which are positive and the number which are negative.

The Quadratic Reciprocity Law (Identity)

- For fixed x, we have $f(x,y) > 0$ if and only if $y < \frac{qx}{p}$, or $y \leq [\frac{qx}{p}]$. Hence, the total number of positive values is

$$\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right].$$

Similarly, the number of negative values is

$$\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right].$$

But the number of positive and negative values together is $\frac{p-1}{2}\frac{p-1}{2}$. So this proves the identity.

Subsection 6

Applications of the Reciprocity Law

Example

- Determine whether 219 is a quadratic residue or nonresidue mod 383.

  Our goal is to evaluate the Legendre symbol $(219|383)$.

  For this, we use:
  - The multiplicative property;
  - The Reciprocity Law;
  - Periodicity;
  - The special values $(-1|p)$ and $(2|p)$ calculated earlier.

  Since $219 = 3 \cdot 73$, by the multiplicative property,

  $$(219|383) = (3|383)(73|383).$$

  By the reciprocity law and periodicity, we have

  $$\begin{array}{rcl}(3|383) & = & (383|3)(-1)^{\frac{(383-1)(3-1)}{4}} \\ & = & -(-1|3) \\ & = & -(-1)^{\frac{3-1}{2}} = 1.\end{array}$$

Example (Cont'd)

- By the reciprocity law and periodicity, we also have

$$\begin{aligned} (73|383) &= (383|73)(-1)^{\frac{(383-1)(73-1)}{4}} \\ &= (18|73) \\ &= (2|73)(9|73) \\ &= (-1)^{\frac{(73)^2-1}{8}} \\ &= 1. \end{aligned}$$

Hence $(219|383) = (3|383)(73|383) = 1 \cdot 1 = 1$.

So 219 is a quadratic residue mod 383.

Example

- Determine those odd primes p for which 3 is a quadratic residue and those for which it is a nonresidue.

  Again, by the reciprocity law we have

$$(3|p) = (p|3)(-1)^{\frac{(p-1)(3-1)}{4}} = (-1)^{\frac{p-1}{2}}(p|3).$$

  - To determine $(p|3)$ we need to know the value of p mod 3.
  - To determine $(-1)^{\frac{p-1}{2}}$ we need to know the value of $\frac{p-1}{2}$ mod 2, or the value of p mod 4.

  Hence we consider p mod 12.

  There are only four cases to consider, $p \equiv 1, 5, 7$ or $11 \pmod{12}$.

  The other cases are excluded, since p is odd.

Example (The Four Cases)

- **Case 1**: $p \equiv 1 \pmod{12}$.

  We have $p \equiv 1 \pmod 3$.

  So $(p|3) = (1|3) = 1$.

  Also $p \equiv 1 \pmod 4$.

  So $\frac{p-1}{2}$ is even.

  Hence $(3|p) = (-1)^{\frac{p-1}{2}}(p|3) = 1$.
- **Case 2**: $p \equiv 5 \pmod{12}$.

  In this case $p \equiv 2 \pmod 3$.

  So $(p|3) = (2|3) = (-1)^{\frac{3^2-1}{8}} = -1$.

  Again, $\frac{p-1}{2}$ is even, since $p \equiv 1 \pmod 4$.

  So $(3|p) = (-1)^{\frac{p-1}{2}}(p|3) = -1$.

Example (The Four Cases Cont'd)

- **Case 3**: $p \equiv 7 \pmod{12}$.

  In this case $p \equiv 1 \pmod{3}$.

  So $(p|3) = (1|3) = 1$.

  Also $\frac{p-1}{2}$ is odd, since $p \equiv 3 \pmod{4}$.

  Hence $(3|p) = (-1)^{\frac{p-1}{2}}(p|3) = -1$.

  Case 4: $p \equiv 11 \pmod{12}$.

  In this case $p \equiv 2 \pmod{3}$.

  So $(p|3) = (2|3) = -1$.

  Again $\frac{p-1}{2}$ is odd, since $p \equiv 3 \pmod{4}$.

  Hence $(3|p) = (-1)^{\frac{p-1}{2}}(p|3) = 1$.
- Summarizing, $3Rp$ if $p \equiv \pm 1 \pmod{12}$ and $3\overline{R}p$ if $p \equiv \pm 5 \pmod{12}$.

Subsection 7

The Jacobi Symbol

The Jacobi Symbol

Definition

Let P be a positive odd integer with prime factorization

$$P = \prod_{i=1}^{r} p_i^{a_i}.$$

The **Jacobi symbol** $(n|P)$ is defined, for all integers n, by the equation

$$(n|P) = \prod_{i=1}^{r} (n|p_i)^{a_i},$$

where $(n|p_i)$ is the Legendre symbol.
We also define $(n|1) = 1$.

Comments

- The possible values of $(n|P)$ are $1, -1$ or 0.
- Moreover, $(n|P) = 0$ if and only if $(n, P) > 1$.
- Suppose the congruence $x^2 \equiv n \pmod{P}$ has a solution.

  Then $(n|p_i) = 1$, for each prime p_i.

  Hence, $(n|P) = 1$.
- However, the converse is not true.

  $(n|P)$ can be 1 if an even number of factors -1 appears in the defining product.

Properties of the Jacobi Symbol

Theorem

If P and Q are odd positive integers, we have:

(a) $(m|P)(n|P) = (mn|P)$;

(b) $(n|P)(n|Q) = (n|PQ)$;

(c) $(m|P) = (n|P)$, whenever $m \equiv n \pmod{P}$;

(d) $(a^2n|P) = (n|P)$, whenever $(a, P) = 1$.

- The listed properties of the Jacobi symbol can be deduced from properties of the Legendre symbol.

Evaluation of $(-1|P)$ and $(2|P)$

Theorem

If P is an odd positive integer we have

$$(-1|P) = (-1)^{\frac{P-1}{2}} \quad \text{and} \quad (2|P) = (-1)^{\frac{P^2-1}{8}}.$$

- Write $P = p_1 p_2 \cdots p_m$, where the p_i's are not necessarily distinct.

  This can also be written as

$$P = \prod_{i=1}^{m}(1 + p_i - 1) = 1 + \sum_{i=1}^{m}(p_i - 1) + \sum_{i \neq j}(p_i - 1)(p_j - 1) + \cdots .$$

  Now each factor $p_i - 1$ is even.

  So each sum after the first is divisible by 4.

Evaluation of $(-1|P)$ and $(2|P)$ (Cont'd)

- Hence,

$$P \equiv 1 + \sum_{i=1}^{m} (p_i - 1) \pmod 4.$$

Equivalently,

$$\frac{1}{2}(P-1) \equiv \sum_{i=1}^{m} \frac{1}{2}(p_i - 1) \pmod 2.$$

Therefore,

$$(-1|P) = \prod_{i=1}^{m} (-1|p_i) = \prod_{i=1}^{m} (-1)^{\frac{p_i-1}{2}} = (-1)^{\frac{P-1}{2}}.$$

Evaluation of $(-1|P)$ and $(2|P)$ (Cont'd)

- To prove the second equation, we write

$$P^2 = \prod_{i=1}^{m}(1+p_i^2-1) = 1+\sum_{i=1}^{m}(p_i^2-1)+\sum_{i\neq j}(p_i^2-1)(p_j^2-1)+\cdots.$$

Since p_i is odd, we have $p_i^2-1\equiv 0 \pmod 8$.
So $P^2\equiv 1+\sum_{i=1}^{m}(p_i^2-1) \pmod{64}$.
Hence,

$$\frac{1}{8}(P^2-1)=\sum_{i=1}^{m}\frac{1}{8}(p_i^2-1) \pmod 8.$$

This also holds mod 2, whence

$$(2|P)=\prod_{i=1}^{m}(2|p_i)=\prod_{i=1}^{m}(-1)^{\frac{p_i^2-1}{8}}=(-1)^{\frac{P^2-1}{8}}.$$

Reciprocity Law for Jacobi Symbols

Theorem (Reciprocity Law for Jacobi Symbols)

If P and Q are positive odd integers with $(P,Q)=1$, then

$$(P|Q)(Q|P)=(-1)^{\frac{(P-1)(Q-1)}{4}}.$$

- Write $P=p_1\cdots p_m$ and $Q=q_1\cdots q_n$, with p_i, q_i primes. Then

$$(P|Q)(Q|P)=\prod_{i=1}^{m}\prod_{j=1}^{n}(p_i|q_j)(q_j|p_i)=(-1)^r, \text{ say.}$$

Reciprocity Law for Jacobi Symbols (Cont'd)

- By the quadratic reciprocity law,

$$r = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{1}{2}(p_i - 1)\frac{1}{2}(q_j - 1) = \sum_{i=1}^{m} \frac{1}{2}(p_i - 1) \sum_{j=1}^{n} \frac{1}{2}(q_j - 1).$$

In the proof of the preceding theorem, we showed that

$$\sum_{i=1}^{m} \frac{1}{2}(p_i - 1) \equiv \frac{1}{2}(P - 1) \pmod{2}.$$

Similarly, we get

$$\sum_{j=1}^{n} \frac{1}{2}(q_j - 1) \equiv \frac{1}{2}(Q - 1) \pmod{2}.$$

Therefore,

$$r \equiv \frac{P-1}{2}\frac{Q-1}{2} \pmod{2}.$$

Example

- We determine whether 888 is a quadratic residue or nonresidue of the prime 1999.

  We have

  $$(888|1999) = (4|1999)(2|1999)(111|1999) = (111|1999).$$

  We calculate $(111|1999)$ using Legendre symbols.

  Write

  $$(111|1999) = (3|1999)(37|1999).$$

  Apply the quadratic reciprocity law to each factor on the right.

  The calculation is simpler with Jacobi symbols,

  $$(111|1999) = -(1999|111) = -(1|111) = -1.$$

  Therefore, 888 is a quadratic nonresidue of 1999.

Example

- We determine whether -104 is a quadratic residue or nonresidue of the prime 997.

  Since $104 = 2 \cdot 4 \cdot 13$, we have

$$\begin{aligned}(-104|997) &= (-1|997)(2|997)(13|997) \\ &= -(13|997) \\ &= -(997|13) \\ &= -(9|13) \\ &= -1.\end{aligned}$$

  Therefore -104 is a quadratic nonresidue of 997.

Subsection 8

Applications to Diophantine Equations

A Diophantine Equation

Theorem

The Diophantine equation

$$y^2 = x^3 + k$$

has no solutions if k has the form

$$k = (4n-1)^3 - 4m^2,$$

where m, n are integers, such that no prime $p \equiv -1 \pmod{4}$ divides m.

- We assume a solution x, y exists.
  We obtain a contradiction by considering the equation modulo 4.
  Note that $k \equiv -1 \pmod{4}$.
  So we have
  $$y^2 \equiv x^3 - 1 \pmod{4}.$$

A Diophantine Equation (Cont'd)

- Now $y^2 \equiv 0$ or $1 \pmod 4$, for every y.
  So
  $$y^2 \equiv x^3 - 1 \pmod 4$$
  cannot be satisfied if x is even or if $x \equiv -1 \pmod 4$.
  Therefore, we must have $x \equiv 1 \pmod 4$.
  Let $a = 4n - 1$ so that $k = a^3 - 4m^2$.
  Write $y^2 = x^3 + k$ in the form
  $$y^2 + 4m^2 = x^3 + a^3 = (x + a)(x^2 - ax + a^2).$$
  But $x \equiv 1 \pmod 4$ and $a \equiv -1 \pmod 4$.
  So we have
  $$x^2 - ax + a^2 \equiv 1 - a + a^2 \equiv -1 \pmod 4.$$
  Hence, $x^2 - ax + a^2$ is odd.
  By the last equation, not all its prime factors can be $\equiv 1 \pmod 4$.

A Diophantine Equation (Cont'd)

- Therefore some prime $p \equiv -1 \pmod 4$ divides $x^2 - ax + a^2$.

  The equation

  $$y^2 + 4m^2 = (x + a)(x^2 - ax + a^2)$$

  shows that this also divides $y^2 + 4m^2$.

  In other words,

  $$y^2 \equiv -4m^2 \pmod p,$$

  for some $p \equiv -1 \pmod 4$.

  But $p \nmid m$ by hypothesis.

  So $(-4m^2|p) = (-1|p) = -1$.

  This contradicts $y^2 \equiv -4m^2 \pmod p$.

Subsection 9

Gauss Sums and the Quadratic Reciprocity Law

Gauss Sums Modulo a Prime

- We give another proof of the Quadratic Reciprocity Law.
- We use the Gauss sums

$$G(n,\chi)=\sum_{r \mod p}\chi(r)e^{2\pi inr/p},$$

where $\chi(r)=(r|p)$ is the quadratic character mod p.
- Since the modulus is prime, χ is a primitive character.
- So we have the Separability Property

$$G(n,\chi)=(n|p)G(1,\chi),\text{ for every } n.$$

- Also, by a previous theorem,

$$|G(1,\chi)|^2=p.$$

The Value of $G(1,\chi)^2$

Theorem

If p is an odd prime and $\chi(r)=(r|p)$, we have

$$G(1,\chi)^2=(-1|p)p.$$

- We have

$$G(1,\chi)^2=\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}(r|p)(s|p)e^{2\pi i(r+s)/p}.$$

For each pair r,s, there is unique t mod p, such that $s\equiv tr \pmod{p}$. Moreover, $(r|p)(s|p)=(r|p)(tr|p)=(r^2|p)(t|p)=(t|p)$. Hence,

$$\begin{aligned} G(1,\chi)^2 &= \textstyle\sum_{t=1}^{p-1}\sum_{r=1}^{p-1}(t|p)e^{2\pi ir(1+t)/p} \\ &= \textstyle\sum_{t=1}^{p-1}(t|p)\sum_{r=1}^{p-1}e^{2\pi ir(1+t)/p}. \end{aligned}$$

The Value of $G(1,\chi)^2$

- The last sum on r is a geometric sum given by

$$\sum_{r=1}^{p-1} e^{2\pi i r(1+t)/p} = \begin{cases} -1, & \text{if } p \nmid (1+t), \\ p-1, & \text{if } p \mid (1+t). \end{cases}$$

Therefore,

$$\begin{aligned} G(1,\chi)^2 &= -\textstyle\sum_{t=1}^{p-2}(t|p) + (p-1)(p-1|p) \\ &= -\textstyle\sum_{t=1}^{p-2}(t|p) + p(p-1|p) - (p-1|p) \\ &= -\textstyle\sum_{t=1}^{p-1}(t|p) + p(-1|p) \\ &= (-1|p)p. \end{aligned}$$

Equivalent Form of Quadratic Reciprocity

Theorem

Let p and q be distinct odd primes and let χ be the quadratic character mod p. Then the quadratic reciprocity law

$$(q|p) = (-1)^{\frac{(p-1)(q-1)}{4}}(p|q)$$

is equivalent to the congruence

$$G(1,\chi)^{q-1} \equiv (q|p) \pmod{q}.$$

- From $G(1,\chi)^2 = (-1|p)p$, we have

$$G(1,\chi)^{q-1} = (-1|p)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}}.$$

Equivalent Form of Quadratic Reciprocity

- By Euler's Criterion,

$$p^{\frac{q-1}{2}} \equiv (p|q) \pmod{q}.$$

So we get

$$G(1,\chi)^{q-1} = (-1)^{\frac{(p-1)(q-1)}{4}}(p|q) \pmod{q}.$$

Suppose the second congruence holds.

Then we obtain

$$(q|p) \equiv (-1)^{\frac{(p-1)(q-1)}{4}}(p|q) \pmod{q}.$$

This implies the first equation since both members are ± 1.

Conversely, suppose the first equation holds.

Then we get the second congruence.

Value of $G(1,\chi)^{q-1}$

Theorem

If p and q are distinct odd primes and if χ is the quadratic character mod p, we have

$$G(1,\chi)^{q-1} = (q|p) \sum_{r_1 \bmod p} \cdots \sum_{\substack{r_q \bmod p \\ r_1+\cdots+r_q \equiv q \pmod p}} (r_1 \cdots r_q|p).$$

- The Gauss sum $G(n,\chi)$ is a periodic function of n with period p.

  The same is true of $G(n,\chi)^q$.

  So we have a finite Fourier expansion

  $$G(n,\chi)^q = \sum_{m \bmod p} a_q(m) e^{2\pi imn/p},$$

  where $a_q(m) = \frac{1}{p}\sum_{n \bmod p} G(n,\chi)^q e^{-2\pi imn/p}$.

Value of $G(1,\chi)^{q-1}$ (Cont'd)

- From the definition of $G(n,\chi)$ we have

$$\begin{aligned} G(n,\chi)^q &= \textstyle\sum_{r_1 \mod p}(r_1|p)e^{2\pi i n r_1/p}\cdots\sum_{r_q \mod p}(r_q|p)e^{2\pi i n r_q/p} \\ &= \textstyle\sum_{r_1 \mod p}\cdots\sum_{r_q \mod p}(r_1\cdots r_q|p)e^{2\pi i n(r_1+\cdots+r_q)/p}. \end{aligned}$$

Now we get

$$a_q(m) = \frac{1}{p}\sum_{r_1 \mod p}\cdots\sum_{r_q \mod p}(r_1\cdots r_q|p)\sum_{n \mod p}e^{2\pi i n(r_1+\cdots+r_q-m)/p}.$$

The sum on n is a geometric sum which vanishes unless $r_1+\cdots+r_q\equiv m \pmod p$, in which case the sum is equal to p. Hence,

$$a_q(m) = \sum_{r_1 \mod p}\cdots\sum_{\substack{r_q \mod p \\ r_1+\cdots+r_q\equiv q \pmod p}}(r_1\cdots r_q|p).$$

Value of $G(1,\chi)^{q-1}$ (Conclusion)

- Next, we obtain an alternate expression for $a_q(m)$.
  We use the following properties:
  - The separability of $G(n,\chi)$;
  - The relation $(n|p)^q = (n|p)$, for odd q;
  - The equation
  $$G(1,\chi)G(-1,\chi) = G(1,\chi)\overline{G(1,\chi)} = |G(1,\chi)|^2 = p.$$

  We find
  $$\begin{array}{rcl} a_q(m) & = & \frac{1}{p}G(1,\chi)^q \sum_{n \mod p}(n|p)e^{-2\pi imn/p} \\ & = & \frac{1}{p}G(1,\chi)^q G(-m,\chi) \\ & = & \frac{1}{p}G(1,\chi)^q (m|p)G(-1,\chi) \\ & = & (m|p)G(1,\chi)^{q-1}. \end{array}$$

  Taking $m = q$ and using the previously obtained expression for $a_q(m)$ we obtain the conclusion.

Proof of the Quadratic Reciprocity Law

- Now we take into account the two preceding theorems.
- They show that to deduce the Quadratic Reciprocity Law, it suffices to show that

$$\sum_{r_1 \bmod p} \cdots \sum_{r_q \bmod p} (r_1 \cdots r_q | p) \equiv 1 \pmod{q},$$

  where the summation indices $r_1, \ldots, r_q$ are subject to the restriction $r_1 + \cdots + r_q \equiv q \pmod{p}$.
  - Suppose all the indices $r_1, \ldots, r_q$ are congruent to each other mod p. Then their sum is congruent to qr_j, for each $j = 1, 2, \ldots, q$.
    So $r_1 + \cdots + r_q \equiv q \pmod{p}$ holds if, and only if, $qr_j \equiv q \pmod{p}$.
    I.e., if, and only if $r_j \equiv 1 \pmod{p}$, for each j.
    In this case the corresponding summand in the sum is $(1|p) = 1$.

Proof of the Quadratic Reciprocity Law (Cont'd)

- For all other choices of indices satisfying $r_1 + \cdots + r_q \equiv q \pmod{p}$, there must be at least two incongruent indices among $r_1, \ldots, r_q$. So, every cyclic permutation of $r_1, \ldots, r_q$ gives a new solution of this congruence which contributes the same summand, $(r_1 \cdots r_q | p)$. Therefore each such summand appears q times and contributes 0 modulo q to the sum.

Hence, the only contribution to the sum which is nonzero modulo q is $(1|p) = 1$.