Introduction to Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Legendre's Symbol

Quadratic Congruences

- We studied the linear congruence

$$ax \equiv b \pmod{n}.$$

- We now study the **quadratic congruence**

$$x^2 \equiv a \pmod{n}.$$

- This amounts to the study of the general quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{n}.$$

Reduction of the General to the Special Case

- Suppose we would like to solve
$$ax^2+bx+c\equiv 0 \pmod{n}.$$
- Set
  - $d=b^2-4ac$;
  - $y=2ax+b$.

  Then, we get
$$\begin{gathered} n \mid ax^2+bx+c \\ 4an \mid 4a(ax^2+bx+c) \\ 4an \mid 4a^2x^2+4abx+4ac \\ 4an \mid (4a^2x^2+4abx+b^2)-(b^2-4ac) \\ 4an \mid y^2-d. \end{gathered}$$
  Thus, $ax^2+bx+c\equiv 0 \pmod{n}$ reduces to
$$y^2\equiv d \pmod{4an}.$$

Quadratic Residues

- Let n be a natural number and a any integer, such that $(a,n)=1$.
- Then a is called a **quadratic residue** $\pmod{n}$ if the congruence

$$x^2 \equiv a \pmod{n}$$

  is soluble.
- Otherwise, it is called a **quadratic non-residue** $\pmod{n}$.

The Legendre Symbol

- The **Legendre symbol** $\left(\frac{a}{p}\right)$, where p is a prime and $(a, p) = 1$, is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue} \pmod{p} \\ -1, & \text{if } a \text{ is a quadratic non-residue} \pmod{p} \end{cases}$$

- The symbol is customarily extended to the case when p divides a by defining it as 0 in this instance.
- Clearly, if $a \equiv a' \pmod{p}$, we have $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$.

Subsection 2

Euler's Criterion

Necessary Condition for Quadratic Non-Residues

Lemma

Let p be an odd prime and $r = \frac{1}{2}(p-1)$. If a is a quadratic non-residue $\pmod{p}$, then $a^r \not\equiv 1 \pmod{p}$.

- Note that, in any reduced set of residues $\pmod{p}$, there are:
  - r quadratic residues $\pmod{p}$;
  - r quadratic non-residues $\pmod{p}$.

  The numbers $1^2, 2^2, \ldots, r^2$ are mutually incongruent $\pmod{p}$.
  (If $p \mid i^2 - j^2 = (i+j)(i-j)$, then $p \mid i+j$ or $p \mid i-j$.)
  For any integer k, $(p-k)^2 \equiv k^2 \pmod{p}$.
  Thus, the listed numbers are all the quadratic residues $\pmod{p}$.
  Each of the numbers satisfies $x^r \equiv 1 \pmod{p}$.
  By Lagrange's theorem, this congruence has $\leq r$ solutions $\pmod{p}$.
  Hence, if a is a quadratic non-residue $\pmod{p}$, then a is not a solution of the congruence.

Euler's Criterion

Theorem (Euler's Criterion)

If p is an odd prime, then

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

Set $r = \frac{1}{2}(p-1)$.

Note that, if a is a quadratic residue $\pmod{p}$, then for some x in $\mathbb{N}$, we have $x^2 \equiv a \pmod{p}$.

By Fermat's theorem,

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

I.e., $a^r \equiv \pm 1 \pmod{p}$.

The conclusion now follows from the Lemma.

Euler's Criterion in $\mathbb{F}_p$

- Observe that, from Fermat's theorem, every element of $\mathbb{F}_p$ other than 0 is a zero of one of the polynomials
$$x^{\frac{1}{2}(p-1)} \pm 1.$$
- From Lagrange's theorem,
$$x^{\frac{1}{2}(p-1)} - 1$$
has precisely the zeros $1^2, 2^2, \ldots, (\frac{1}{2}(p-1))^2$, which is a complete set of quadratic residues.
- Alternatively, in terms of a primitive root $\pmod{p}$, say g, it is clear that the quadratic residues $\pmod{p}$ are given by $1, g^2, \ldots, g^{2(r-1)}$.

Multiplicative Property of the Legendre Symbol

Corollary

For all integers a, b, not divisible by p,

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

- Noting that all values are ± 1, we have $\pmod{p}$:

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

The Status of -1

Corollary

-1 is a quadratic residue of all primes $\equiv 1 \pmod 4$ and a quadratic non-residue of all primes $\equiv 3 \pmod 4$.

- We have
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}.$$
From this, the conclusion follows.
- Recall that when $p \equiv 1 \pmod 4$, the solutions of $x^2 \equiv -1 \pmod p$ are given by $x = \pm(\frac{p-1}{2}!)$.

Subsection 3

Gauss' Lemma

Numerically Least Residues

- Let n be a natural number and let a be any integer.
- The **numerically least residue** of $a \pmod{n}$ is the integer a' for which
$$a \equiv a' \pmod{n} \quad \text{and} \quad -\frac{1}{2}n < a' \leq \frac{1}{2}n.$$

Gauss' Lemma

Theorem (Gauss' Lemma)

Let p be an odd prime and a an integer, such that $(a,p)=1$. Let a_j be the numerically least residue of $aj \pmod{p}$, for $j=1,2,\ldots$. If ℓ is the number of $j \le \frac{1}{2}(p-1)$, for which $a_j<0$, then $\left(\frac{a}{p}\right)=(-1)^{\ell}$.

- Observe that $|a_j|$, with $1 \le j \le r$, where $r=\frac{1}{2}(p-1)$, are simply the numbers $1,2,\ldots,r$ in some order:
  - $1 \le |a_j| \le r$;
  - If $a_j=-a_k$, with $k \le r$, then $a(j+k) \equiv 0 \pmod{p}$, with $0<j+k<p$, which is impossible;
  - If $a_j=a_k$, then $a_j \equiv a_k \pmod{p}$, whence $j=k$.

  Hence, we have $a_1 \cdots a_r=(-1)^{\ell} r!$.

  But $a_j \equiv aj \pmod{p}$, and, so, $a_1 \cdots a_r \equiv a^r r! \pmod{p}$.

  Thus, $a^r \equiv (-1)^{\ell} \pmod{p}$.

  The result now follows from Euler's Criterion.

2 as a Quadratic Residue

Corollary

For p an odd prime,

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

i.e., 2 is

- a quadratic residue of all primes $\equiv \pm 1 \pmod 8$;
- a quadratic non-residue of all primes $\equiv \pm 3 \pmod 8$.

- Note that, when $a = 2$, we have

$$a_j = \begin{cases} 2j, & \text{if } 1 \leq j \leq [\frac{1}{4}p] \\ 2j - p, & \text{if } [\frac{1}{4}p] < j \leq \frac{1}{2}(p-1) \end{cases}$$

  Hence, in this case, $\ell = \frac{1}{2}(p-1) - [\frac{1}{4}p]$.
  Now check that $\ell \equiv \frac{1}{8}(p^2-1) \pmod 2$.

Subsection 4

Law of Quadratic Reciprocity

The Euler-Gauss Law of Quadratic Reciprocity

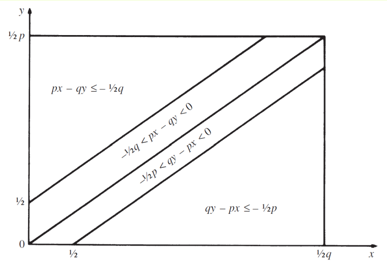
Theorem (Euler-Gauss Law of Quadratic Reciprocity)

If p, q are distinct odd primes, then

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

- By Gauss' lemma, $\left(\frac{p}{q}\right) = (-1)^{\ell}$, where ℓ is the number of lattice points (pairs of integers) (x, y) satisfying $0 < x < \frac{1}{2}q$ and $-\frac{1}{2}q < px - qy < 0$.

  These give $y < \frac{px}{q} + \frac{1}{2} < \frac{1}{2}(p+1)$. Hence, since y is an integer, we see that ℓ is the number of lattice points in the rectangle R, defined by $0 < x < \frac{1}{2}q$, $0 < y < \frac{1}{2}p$, satisfying $-\frac{1}{2}q < px - qy < 0$.



The Euler-Gauss Law of Quadratic Reciprocity (Cont'd)

- We showed ℓ is the number of lattice points in the rectangle R, defined by $0 < x < \frac{1}{2}q$, $0 < y < \frac{1}{2}p$, satisfying $-\frac{1}{2}q < px - qy < 0$.

  Similarly, $\left(\frac{q}{p}\right) = (-1)^m$, where m is the number of lattice points in R, satisfying $-\frac{1}{2}p < qy - px < 0$.

  Claim: $\frac{1}{4}(p-1)(q-1) - (\ell + m)$ is even.

  But $\frac{1}{4}(p-1)(q-1)$ is just the number of lattice points in R, and, thus, the latter expression is the number of lattice points in R, satisfying either $px - qy \leq -\frac{1}{2}q$ or $qy - px \leq -\frac{1}{2}p$. The regions R' and R'' in R defined by these inequalities are disjoint and they contain the same number of lattice points: The substitution $x = \frac{1}{2}(q+1) - x'$, $y = \frac{1}{2}(p+1) - y'$ furnishes a one-one correspondence between them.

  The theorem follows.

Applications of Quadratic Reciprocity

- Since $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}$,
  - if p, q are not both congruent to 3 (mod 4), then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$;
  - in the exceptional case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.
- The law of quadratic reciprocity is useful in the calculation of Legendre symbols.

  Example:

  $$\left(\frac{15}{71}\right) = \left(\frac{3}{71}\right)\left(\frac{5}{71}\right) = -\left(\frac{71}{3}\right)\left(\frac{71}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = -(-1)\cdot 1 = 1.$$

  Example: Further, for instance, we obtain

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

  whence -3 is a quadratic residue of all primes $\equiv 1 \pmod 6$ and a quadratic non-residue of all primes $\equiv -1 \pmod 6$.

Another Example

- We evaluate

$$\left(\frac{-5}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)=(-1)^{\frac{1}{2}(p-1)}(-1)^{\frac{1}{4}(5-1)(p-1)}\left(\frac{p}{5}\right)=(-1)^{\frac{1}{2}(p-1)}\left(\frac{p}{5}\right).$$

Note that

$$\left(\frac{p}{5}\right)=\begin{cases} 1, & \text{if } p\equiv \pm 1 \pmod 5 \\ -1, & \text{if } p\equiv \pm 2 \pmod 5 \end{cases}$$

Thus, -5 is a:
  - quadratic residue of all primes $\equiv 1,3,7,9 \pmod{20}$;
  - a quadratic non-residue of primes $\equiv -1,-3,-7,-9 \pmod{20}$.

Subsection 5

Jacobi's Symbol

Jacobi's Symbol

- This is a generalization of the Legendre symbol.
- Let n be a positive odd integer and suppose that $n = p_1 p_2 \cdots p_k$ as a product of primes, not necessarily distinct.
- For any integer a, with $(a, n) = 1$, the **Jacobi symbol** is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right),$$

  where the factors on the right are Legendre symbols.
- When $n = 1$, the Jacobi symbol is defined as 1.
- When $(a, n) > 1$, it is defined as 0.
- Clearly, if $a \equiv a' \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{a'}{n}\right)$.

Jacobi's Symbol and Quadratic Residues

- $\left(\frac{a}{n}\right) = 1$ does not imply that a is a quadratic residue $\pmod{n}$.
  Indeed a is a quadratic residue $\pmod{n}$ if and only if a is a quadratic residue $\pmod{p}$, for each prime divisor p of n.
- But $\left(\frac{a}{n}\right) = -1$ does imply that a is a quadratic non-residue $\pmod{n}$.
  Example: Note that
  $$\left(\frac{6}{35}\right) = \left(\frac{6}{5}\right)\left(\frac{6}{7}\right) = \left(\frac{1}{5}\right)\left(\frac{-1}{7}\right) = -1.$$
  Therefore, 6 is a quadratic non-residue $\pmod{35}$.

Multiplicativity of Jacobi's Symbol

- The Jacobi symbol is multiplicative, i.e.,
$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right),$$
for all integers a, b relatively prime to n.
- Further, if m, n are odd and $(a, mn) = 1$ then
$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

The Jacobi's Symbol for -1,2 and Reciprocity

- We have
$$\left(\frac{-1}{n}\right)=(-1)^{\frac{1}{2}(n-1)}, \qquad \left(\frac{2}{n}\right)=(-1)^{\frac{1}{8}(n^2-1)}.$$
- The analogue of the law of quadratic reciprocity holds, namely if m, n are odd and $(m, n)=1$, then
$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{1}{4}(m-1)(n-1)}.$$
- For the proofs, note that
$$\begin{aligned} \tfrac{1}{2}(n_1 n_2-1)-\tfrac{1}{2}(n_1-1)-\tfrac{1}{2}(n_2-1) &= \tfrac{1}{2}(n_1 n_2-n_1-n_2+1) \\ &= \tfrac{1}{2}(n_1-1)(n_2-1) \\ &\equiv 0 \pmod{2}. \end{aligned}$$

  Thus,
$$\frac{1}{2}(n-1) \equiv \frac{1}{2}(n_1-1)+\frac{1}{2}(n_2-1) \pmod{2}.$$
  A similar congruence holds for $\frac{1}{8}(n^2-1)$.

Applications of Jacobi's Symbol

- Jacobi symbols can be used to facilitate the calculation of Legendre symbols.

  Example:

$$\begin{aligned}
\left(\frac{335}{2999}\right) &= (-1)^{\frac{1}{4}(335-1)(2999-1)}\left(\frac{2999}{335}\right) = (-1)^{250333}\left(\frac{2999}{335}\right) \\
&= -\left(\frac{2999}{335}\right) = -\left(\frac{9\cdot 335-16}{335}\right) = -\left(\frac{-16}{335}\right) = -\left(\frac{-1}{335}\right)\left(\frac{2}{335}\right)^4 \\
&= -(-1)^{\frac{1}{2}(335-1)}(-1)^{4\cdot\frac{1}{8}(335^2-1)} = -(-1)^{167}(-1)^{56112} = 1.
\end{aligned}$$

  Since 2999 is a prime, 335 is a quadratic residue $\pmod{2999}$.

Applications of Jacobi's Symbol (Cont'd)

- Example:

$$\begin{aligned}\left(\frac{21}{275}\right) &= (-1)^{\frac{1}{4}(21-1)(275-1)}\left(\frac{275}{21}\right) = (-1)^{1370}\left(\frac{21\cdot 13+2}{21}\right) \\ &= \left(\frac{2}{21}\right) = (-1)^{\frac{1}{8}(21^2-1)} = (-1)^{55} = -1.\end{aligned}$$

If $\left(\frac{a}{n}\right) = -1$, then $\left(\frac{a}{p}\right) = -1$, for some prime factor p of n.

Moreover, $x^2 \equiv a \pmod{n}$ implies $x^2 \equiv a \pmod{p}$.

So a is a quadratic non-residue of n.

We conclude that 21 is a quadratic non-residue of 275.

Applications of Jacobi's Symbol (Cont'd)

- The converse is not true.

  Example:

$$\begin{aligned}\left(\tfrac{3}{275}\right) &= (-1)^{\frac{1}{4}(3-1)(275-1)}\left(\tfrac{275}{3}\right)\\ &= (-1)^{137}\left(\tfrac{2}{3}\right) = (-1)(-1)^{\frac{1}{8}(3^2-1)} = 1.\end{aligned}$$

  But we cannot conclude that 3 is a quadratic residue of 275.

  Indeed

$$\left(\frac{3}{5}\right) = (-1)^{\frac{1}{4}(3-1)(5-1)}\left(\frac{5}{3}\right) = (-1)^2\left(\frac{2}{3}\right) = -1.$$

  So 3 is a quadratic non-residue of 275.