Quadratic Reciprocity

Presented by Nabila Razeq

- “For those who consider the theory of numbers ‘the Queen of Mathematics,’ this (Quadratic Reciprocity Law) is one of the jewels in her crown.”
    - David Burton
- “The gem of higher arithmetic”
    - Gauss

The History

- Fermat- first mathematician to study reciprocity questions
- Euler- Euler's Criterion
- Legendre- the Legendre Symbol
- Gauss- first mathematician to find a complete proof of the law.
- Cauchy, Jacobi, Dirichlet, Eisenstein, Kronecker, and Dedekind

Euler's Criterion

- Let p be an odd prime and gcd (a, p) = 1. Then, a is a quadratic residue of p if and only if

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

Example using Euler's criterion

- Let p = 13.
- Which one of the congruences $x^2 \equiv a(\text{mod}\,13)$ is solvable when *a* runs through the set {1, 2, ..., 12}.
- Modulo 13,

$$1^2 \equiv 12^2 \equiv 1,$$

$$2^2 \equiv 11^2 \equiv 4,$$

$$3^2 \equiv 10^2 \equiv 9,$$

$$4^2 \equiv 9^2 \equiv 3,$$

$$5^2 \equiv 8^2 \equiv 12,$$

$$6^2 \equiv 7^2 \equiv 10$$

- Therefore, 1,3, 4, 9, 10, 12 are quadratic residues of 13.

The Legendre symbol

- Definition: let p be an odd prime and gcd(a, p)=1. The Legendre symbol

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

Example using the Legendre symbol

- Let $p = 13$.
- The quadratic residues:

$$\left(\frac{1}{13}\right)=\left(\frac{3}{13}\right)=\left(\frac{4}{13}\right)=\left(\frac{9}{13}\right)=\left(\frac{10}{13}\right)=\left(\frac{12}{13}\right)=1$$

- The quadratic nonresidues:

$$\left(\frac{2}{13}\right)=\left(\frac{5}{13}\right)=\left(\frac{6}{13}\right)=\left(\frac{7}{13}\right)=\left(\frac{8}{13}\right)=\left(\frac{11}{13}\right)=-1$$

Quadratic Reciprocity Law

- Let p and q be distinct odd primes, then

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

Proof of Quadratic Reciprocity

- Gauss' Lemma
- Eisenstein

Application of Quadratic reciprocity

- The Chinese remainder theorem
  - If gcd $(a, b) = 1$, then each $n = 0, 1, 2, \ldots, ab-1$ has a distinct pair of remainders on division by a and b.

Example using the Chinese remainder theorem

- Let $a = 3$ and $b = 5$
- Each $n = 0, 1, \ldots, 14$ has a distinct pair of remainders
- Question: find the integer that leaves remainder 2 on division by 3 and remainder 3 on division by 5.
- Answer: $8 \equiv (2, 3)$ (mod3, mod 5)

Summary of Results

- Euler's criterion
- The Legendre symbol
- The Law of Quadratic Reciprocity
- Chinese remainder theorem

References

- Burton, David M.. Elementary Number Theory. Boston: Allyn and Bacon, INC., 1976.

- Lemmermeyer, Franz. Reciprocity Laws: from Euler to Eisenstien. Berlin Hiedelberg New York: Springer-Verlag, 2000.

- Stillwell, John. Elements of Number Theory. New York: Springer-Verlag, 2003.