MAT 401 - Quadratic Reciprocity and Lucas Polynomials

Evan Kim, Stony Brook University

December 2, 2021

Contents

1 Introduction

In number theory, quadratic reciprocity is a reciprocity law that gives conditions for the solvability of quadratic equations mod prime numbers. The reciprocity relationship can be compactly expressed with Legendre symbols, which is calculated using Euler's criterion.

One of Gauss's proofs for the law of quadratic reciprocity uses Gauss sums and complex integration to show the reciprocity relation analytically. Gauss sums are also useful in algebraic number theory because they generate an extension of the cyclotomic (abelian) field $\mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p^{th} root of unity and p is prime.

An alternative proof for quadratic reciprocity is given here and is based on the resultant of the Lucas polynomial, the fundamental theorem of symmetric polynomials, and properties of monic polynomials. Lucas polynomials are used in computational geometry, where the Gauss-Lucas theorem gives a geometric relation between the roots of a polynomial p and its derivatives.

2 Euler's Criterion

Definition 2.0.1 (Euler's Criterion)**.** Euler's criterion determines whether an integer is a quadratic residue.

Let p be an odd prime and a be coprime to p. Then

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \mod p \text{ if there is an integer } x \text{ such that } a \equiv x^2 \\ -1 \mod p \text{ otherwise} \end{cases}$$

Euler's criterion can be expressed using the Legendre symbol as

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

3 Fundamental Theorem of Symmetric Polynomials

Definition 3.0.1 (Symmetric Polynomial)**.** A polynomial $f \in \mathbb{Z}[x_1, \ldots, x_k]$, a finite field of order k, is **symmetric** if

$$f(x_{i_1}, \ldots, x_{i_k}) = f(x_1, \ldots, x_k)$$

for every permutation of variables $[x_{i_1}, \ldots, x_{i_k}]$.

Definition 3.0.2 (Elementary Symmetric Polynomials)**.** Define the **elementary symmetric polynomials** $\sigma_1, \ldots, \sigma_n \in \mathbb{Z}[x]$ as

$$\begin{aligned} \sigma_1 &= x_1 + \cdots + x_n \\ &\vdots \\ \sigma_r &= \sum_{i_i < i_2 < \cdots < i_r} x_{i_1} x_{i_2} \ldots x_{i_r} \\ &\vdots \\ \sigma_n &= x_1 x_2 \ldots x_n \end{aligned}$$

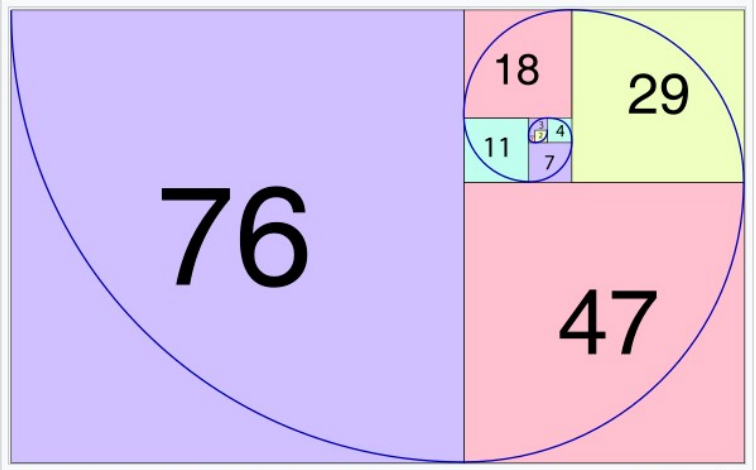
Example - when $n = 4$ the elementary symmetric polynomials are

$$\sigma_1(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4$$
$$\sigma_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_3 + x_2x_4 + x_3x_4$$
$$\sigma_3(x_1, x_2, x_3, x_4) = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$
$$\sigma_4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4$$

Theorem 3.1 (The Fundamental Theorem of Symmetric Polynomials)**.**

Every symmetric polynomial in $\mathbb{Z}[x]$ has a unique representation as n elementary symmetric polynomials. With Viète's formulas from number theory, it can be shown that the coefficients of symmetric polynomials can be given in terms of its roots.

4 Lucas Polynomials



The Lucas spiral, made with quarter-arcs, is a good approximation of the golden spiral when its terms are large. However, when its terms become very small, the arc's radius decreases rapidly from 3 to 1 then increases from 1 to 2.

Figure 1: Source: Wikipedia

Lucas polynomials are a family of Fibonacci polynomials and can be formed via the recursive sequence

$$L_n(x) = \begin{cases} 2, & n = 0 \\ x, & n = 1 \\ xL_{n-1}(x) + L_{n-2}(x), & n \geq 2 \end{cases}$$

The first few are

$$L_1(x) = x$$
$$L_2(x) = x^2 + 2$$
$$L_3(x) = x^3 + 3x$$
$$L_4(x) = x^4 + 4x^2 + 2$$
$$L_5(x) = x^5 + 5x^3 + 5x$$

Lucas polynomials are symmetric, monomial, and have the divisibility property that $L_n(x)$ divides $L_m(x)$ if and only if m is an odd multiple of n. For prime p, $L_p(x)/x = H_p$ is an irreducible polynomial.

5 Resultant of Lucas Polynomials

Definition 5.0.1 (Resultant)**.** Given two monic polynomials $f, g \in \mathbb{Z}[x]$, the **resultant** is defined as $Res(f, g) = \alpha - \beta$ where α, β are roots of f, g respectively. The first observation is that f, g have common factors if and only if $Res(f, g) = 0$. The second observation is that $Res(f, g) = (-1)^{mn} Res(g, f)$.

Given a monic polynomial $f \in \mathbb{Z}[x]$, there exists a polynomial $H \in \mathbb{Z}[x]$ such that $Res(f, g) = H$ for every polynomial $g \in \mathbb{Z}[x]$ where β is a root of g. It follows that for monic polynomials $f, g, h \in \mathbb{Z}[x]$, if $g \equiv h \mod d$ then $Res(f, g) \equiv Res(f, h) \mod d$.

6 Quadratic Reciprocity Proof

Theorem 6.1 (The Law of Quadratic Reciprocity)**.**

The quadratic reciprocity law states that if p, q are distinct odd primes, then

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

The key properties from Lucas polynomials to prove quadratic reciprocity are the following:

- For every prime p, $L_p(x) \equiv x^p \mod p$. Equivalently $H_p \equiv x^{p-1/2} \mod p$ where H_p are the even terms.
- For distinct odd primes p, q, $Res(H_p, H_q) = \pm 1$.

Let p, q be distinct odd primes. Then we have $Res(H_p, H_q) \equiv Res(x^{(p-q)/2}, H_q) = (-1)^{pq} H_q(0)^{(p-1)/2} \mod p$. Since $H_q(0) = q$ and $q^{(p-1)/2} \equiv \left(\frac{q}{p}\right)$ by Euler's criterion, we have $Res(H_p, H_q) \equiv \left(\frac{q}{p}\right) \mod p$. By symmetry we have $Res(H_q, H_p) = \frac{p}{q}$ and we get

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

7 References

Reference 7.1. Reciprocity via Lucas Polynomials - `https://mattbaker.blog/2020/06/02/quadratic-reciprocity-via-lucas-polynomials/`

Reference 7.2. Ideals, Varieties, and Algorithms by David A. Cox, John Little, Donal O'Shea