Honors 1: Undergraduate Math Lab*

Peter Sarnak†, Steven Miller‡, Alex Barnett§

September 11^{th}, 2002

Courant Institute of Mathematical Sciences
New York University
New York, NY

Abstract

We give Eisenstein's proof of Quadratic Reciprocity, and then introduce the Graph Theory problems. Lecture by Steven Miller and Peter Sarnak; notes by Steven Miller.

1 Eisenstein's Proof of Quadratic Reciprocity

1.1 Preliminaries

Theorem 1.1 (Quadratic Reciprocity) *Let p and q be distinct odd primes. Then*

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

As p and q are distinct, odd primes, both $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ are ± 1. The difficulty is figuring out which signs are correct, and how the two signs are related.

We use Euler's Criterion, proved in a previous lecture:

---

*Homepage: `http://www.math.nyu.edu/~millerj/`
†E-mail: `sarnak@math.princeton.edu`
‡E-mail: `millerj@cims.nyu.edu` or `sjmiller@math.princeton.edu`
§E-mail: `barnett@nmr.mgh.harvard.edu`

Lemma 1.2 (Euler's Criterion)

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

The idea behind Eisenstein's proof is as follows: $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$ is -1 to a power. Further, we only need to determine the power mod 2. Eisenstein shows many expressions are equivalent, mod 2, to this power. Eventually, we arrive at an expression which is trivial to calculate (mod 2).

1.2 First Stage

Consider all even multiples of q by an $a \leq p-1$: $\{2q, 4q, 6q, \ldots, (p-1)q\}$. Denote a generic multiple by aq. Recall $[x]$ is the greatest integer less than or equal to x. By integer division,

$$aq = \left[\frac{aq}{p}\right]p + r_a,\ 0 \leq r_a < p-1. \tag{3}$$

Thus, r_a is the least non-negative number equivalent to qa mod p.

The numbers $(-1)^{r_a} r_a$ are equivalent to even numbers in $\{0, \ldots, p-1\}$. If r_a is even this is clear; if r_a is odd, then $(-1)^{r_a} r_a \equiv p - r_a$ mod p, and as p and r_a are odd, this is even.

Lemma 1.3 *If* $(-1)^{r_a} r_a \equiv (-1)^{r_b} r_b$*, then* $a = b$*.*

Proof: We quickly get $\pm r_a \equiv r_b$ mod p. If the plus sign holds, then $r_a \equiv r_b$ mod p implies $qa \equiv qb$ mod p. As q is invertible mod p, we get $a \equiv b$ mod p, which yields $a = b$ (as a and b are even integers between 0 and $p-1$).

If the minus sign holds, then $r_a + r_b \equiv 0$ mod p, or $qa + qb \equiv 0$ mod p. Multiplying by q^{-1} mod p now gives $a + b \equiv 0$ mod p. As a and b are even integers between 0 and $p-1$, $0 < a + b \leq 2(p-1)$. The only integer strictly between 0 and $2p$ which is equivalent to 0 mod p is p; however, p is odd and $a + b$ is even. Thus, the minus sign cannot hold, and the elements are all distinct. $\square$.

Lemma 1.4

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{a\, even} r_a}. \tag{4}$$

Proof: For each even a, $qa \equiv r_a \bmod p$. Thus, mod p:

$$\begin{aligned}\prod_{a \text{ even}} qa &\equiv \prod_{a \text{ even}} r_a \\ q^{\frac{p-1}{2}} \prod_{a \text{ even}} a &\equiv \prod_{a \text{ even}} r_a \\ \left(\frac{q}{p}\right) \prod_{a \text{ even}} a &\equiv \prod_{a \text{ even}} r_a, \end{aligned} \tag{5}$$

where the above follows from the fact that we have $\frac{p-1}{2}$ choices for an even a (to get $q^{\frac{p-1}{2}}$ and Euler's Criterion (to replace $q^{\frac{p-1}{2}}$ with $\left(\frac{q}{p}\right)$).

As a ranges over all even number from 0 to $p-1$, so too do the numbers $(-1)^{r_a} r_a \bmod p$. Thus, mod p,

$$\begin{aligned}\prod_{a \text{ even}} a &\equiv \prod_{a \text{ even}} (-1)^{r_a} r_a \\ \prod_{a \text{ even}} a &= (-1)^{\sum_{a \text{ even}} r_a} \prod_{a \text{ even}} r_a. \end{aligned} \tag{6}$$

Combining gives

$$\left(\frac{q}{p}\right)(-1)^{\sum_{a \text{ even}} r_a} \prod_{a \text{ even}} r_a \equiv \prod_{a \text{ even}} r_a. \tag{7}$$

As each r_a is invertible mod p, so is the product. Thus,

$$\left(\frac{q}{p}\right)(-1)^{\sum_{a \text{ even}} r_a} \equiv 1 \bmod p. \tag{8}$$

As $\left(\frac{q}{p}\right)$ is its own inverse, the Lemma now follows by multiplying both sides by $\left(\frac{q}{p}\right)$. $\Box$.

Therefore, it is sufficient to determine $\sum_{a \text{ even}} r_a \bmod 2$.

We make one last simplification. By integer division, we have

$$\begin{aligned}\sum_{a \text{ even}} qa &= \sum_{a \text{ even}} \left(\left[\frac{qa}{p}\right]p + r_a\right) \\ &= \sum_{a \text{ even}} \left[\frac{qa}{p}\right]p + \sum_{a \text{ even}} r_a. \end{aligned} \tag{9}$$

As we are summing over even a, the Left Hand Side above is even. Thus, the Right Hand Side is even, so

$$\begin{aligned} \sum_{a \text{ even}} \left[\frac{qa}{p}\right] p &\equiv \sum_{a \text{ even}} r_a \bmod 2 \\ p \sum_{a \text{ even}} \left[\frac{qa}{p}\right] &\equiv \sum_{a \text{ even}} r_a \bmod 2 \\ \sum_{a \text{ even}} \left[\frac{qa}{p}\right] &\equiv \sum_{a \text{ even}} r_a \bmod 2, \end{aligned} \tag{10}$$

where the last line follows from the fact that p is odd, so mod 2, dropping the factor of p from the Left Hand Side doesn't change the parity.

We have shown

Lemma 1.5 *It is sufficient to calculate* $\sum_{a \ even} \left[\frac{qa}{p}\right]$

1.3 Second Stage

Consider the rectangle with vertices at $A = (0,0)$, $B = (p,0)$, $C = (p,q)$ and $D = (0,q)$. The upward slopping vertical is given by the equation $y = \frac{q}{p}x$. As p and q are distinct odd primes, there are no pairs of integers (x,y) on the line AC.

We now interpret $\sum_{a \text{ even}} \left[\frac{qa}{p}\right]$. Consider the vertical line with x coordinate a. Then $\left[\frac{qa}{p}\right]$ gives the number of pairs (x,y) with x-coordinate equal to a and y-coordinate an integer at most $\left[\frac{qa}{p}\right]$. Thus, $\sum_{a \text{ even}} \left[\frac{qa}{p}\right]$ is the number of integer pairs (in the rectangle $ABCD$) with even x-coordinate that are below the line AC.

We add some additional points: $E = (\frac{p}{2}, 0)$, $F = (\frac{p}{2}, \frac{q}{2})$, $G = (0, \frac{q}{2})$ and $H = (\frac{p}{2}, q)$. We prove

Lemma 1.6 *The number of integer pairs under the line AC (inside the rectangle) with even x-coordinate is congruent mod 2 to the number of integer pairs under the line AF.*

Let $a > \frac{p}{2}$ be an even integer. The integer pairs on the line $x = a$ are $(a,0)$, $(a,1), \dots, (a,q)$. There are $q+1$ pairs. As q is odd, there are an even number of integer pairs on the line $x = a$. As there are no integer pairs on the line AC, for a fixed $a > \frac{p}{2}$, mod 2 there are the same number of integer pairs *above* AC as there are *below* AC.

Further, the number of integer pairs *above* AC is equivalent mod 2 to the number of integer pairs below AF on the line $x = p - a$. To see this, consider the map which takes (x, y) to $(p - x, q - y)$. As $a > \frac{p}{2}$ and is even, $p - a < \frac{p}{2}$ and is odd. Further, every odd $a < \frac{p}{2}$ is hit (given $a_{odd} < \frac{p}{2}$, start with the even number $p - a_{odd} > \frac{p}{2}$).

Let $\#FCH_{even}$ be the number of integer pairs (x, y) in triangle FCH with x even.

Let $\#EBCH$ be the number of integer pairs in the rectangle $EBCH$; $\#EBCH \equiv 0 \bmod 2$ (we've shown each vertical line has an even number of pairs).

Let $\#AFE_{even}$ be the number of integer pairs (x, y) in the triangle AFE with x even, and let $\#AFE$ be the number of integer pairs in the triangle AFE.

We need to calculate $\sum_{a \text{ even}} \left[\frac{qa}{p}\right]$ mod 2:

$$\begin{aligned}
\sum_{a \text{ even}} \left[\frac{qa}{p}\right] &= \#AFE_{even} + \#EBCH - \#FCH \\
&\equiv \#AFE_{even} + \#EBCH + \#FCH \\
&= \#AFE_{even} + \#FCH + \#EBCH \\
&= \#AFE + \#EBCH \\
&= \#AFE. \qquad (11)
\end{aligned}$$

Therefore, $\mu = \sum_{a \text{ even}} \left[\frac{qa}{p}\right] \equiv \#AFE \bmod 2$, and we have

$$\left(\frac{q}{p}\right) = (-1)^{\mu}. \qquad (12)$$

Reversing the rolls of p and q, we see that

$$\left(\frac{p}{q}\right) = (-1)^{\nu}, \qquad (13)$$

where $\nu \equiv \#AFG \bmod 2$, with $\#AFG$ equal to the number of integer pairs in the triangle AFG.

Now, $\mu + \nu = \#AFE + \#AFG$, which is the number of integer pairs in the rectangle $AEFG$. There are $\frac{p-1}{2}$ choices for x and $\frac{q-1}{2}$ choices for y, giving $\frac{p-1}{2}\frac{q-1}{2}$ pairs of integers in the rectangle $AEFG$.

Thus,

$$\begin{aligned} \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) &= (-1)^{\mu+\nu} \\ &= (-1)^{\#AFE+\#AFG} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}, \end{aligned} \tag{14}$$

which completes the proof of Quadratic Reciprocity. □.

2 Central Limit Theorem

$X_1, X_2, X_3, \ldots$ an infinite sequence of random variables such that the X_j are independent identically distributed random variables (abbreviated i.i.d.r.v.) with $E[X_j] = \bar{X}_j = 0$ (can always renormalize by shifting) and variance $E[X_j^2] = 1$. Let $S_N = \sum_{j=1}^{N} X_j$.

Theorem 2.1 *Fix $-\infty < a \leq b < \infty$. Then as $N \to \infty$,*

$$Prob\Big(\frac{S_N}{\sqrt{N}} \in [a,b]\Big) \to \frac{1}{\sqrt{2\pi}} \int_a^b e^{-\frac{t^2}{2}} dt. \tag{15}$$

The probability function is called the Gaussian or the Normal distribution. This is the universal curve of probability. Note how robust the Central Limit Theorem is: it doesn't depend on fine properties of the X_j.

3 Possible Problems

3.1 Combinatorics and Probability

Combinatorics is the number of ways of doing something. A **graph** is a set of **vertices** (V) and **edges** (E) between them. Thus, edges are unordered pairs of vertices.

Four Color Theorem (proved by an exhaustive search by the computer). Say you have a graph in the plane (thus, if you draw the vertices and edges in the plane, no two edges cross). Call such a graph a **planar graph**. Can you color the vertices such that if two vertices are joined by an edge, they have different colors? Sure, by using $|V|$ colors! What is the least number of colors needed?

Theorem 3.1 (Four Coloring Theorem) *You can color the vertices of a planar graph using at most four colors such that no two joined vertices have the same color.*

A **k-regular graph** is a graph such that there are k-edges out of each vertex. A 2-regular graph has no freedom: you get a closed cycle.

Consider 3-regular graphs. To each graph associate the **adjacency matrix** A. (First to study may be Kirchhoff). Say $G = (V, E)$ has $|V| = n$ vertices. For now, assume there are no **multiple edges** (ie, between any two vertices is at most one edge, and there are no edges connecting a vertex to itself). A is an $n \times n$ matrix, rows and columns indexed by the vertices, and $A_{ij} = 1$ if there is an edge from v_i to v_j and 0 otherwise.

Thus, the adjacency matrix is a matrix with 0s and 1s, and is symmetric.

Problem: What is the second largest eigenvalue of A? How does it vary? What do we expect?

In Linear Algebra, we learn we can diagonalize a real symmetric matrix. The eigenvalues are real, and satisfy $p_A(\lambda) = \det(\lambda I - A)$, the characteristic polynomial. This is a polynomial in λ of degree n with integer coefficients. Thus, the eigenvalues are algebraic numbers. The leading coefficient is λ^n, the constant term is $\det(A)$.

Thus, $p_A(\lambda) = \lambda^n + \cdots + \det(A)$, and by the Fundamental Theorem of Algebra, there are n complex roots. If the leading coefficient of the defining polynomial is 1, we say the roots are **algebraic integers**. These roots are the eigenvalues of A.

Why must the eigenvalues be real? Want $Av = \lambda v$, v a non-zero vector.

Fact: if $v = (1, 1, \ldots, 1)^T$, v is an eigenvector of A with eigenvalue k. Why? As each vertex is connected to k distinct vertices, each row has exactly k entries that are 1 and $n - k$ entries that are 0. Thus, k is an eigenvalue, denote by λ_0.

Problem 1 *Show, for such adjacency matrices A, that all eigenvalues satisfy $-k \leq \lambda \leq k$.*

Consider connected graphs G. How big is $\lambda_1(G)$ for the random 3-regular graph?

Theorem 3.2 (Kirchhoff's Theorem) *Let $det^*(kI - A)$ be the product of the non-zero eigenvalues of A. Then $det^*(kI - A)$ equals the number of vertices times the number of spanning trees.*

A tree is a connected graph with no cycles. A **spanning tree** is a connected sub-graph containing all the vertices. Sometimes called complexity of the graph.