RECIPROCITY LAWS

DAN YASAKI

Abstract. Informal notes for a talk at UNCG on reciprocity laws (such as quadratic reciprocity and Shimura-Taniyama). This material is from *Fearless Symmetry* by Ash and Gross [1] and *Galois Representations and Modular Forms* by Ribet [2].

1. Overview

During the last few decades, the field of number theory has been increasingly permeated by the theory of automorphic forms and automorphic representations. This collection of conjectures is often called *Langlands program*, though it involves the work of many mathematicians. Parts of this program can be viewed as vast generalization of the reciprocity laws in number theory, such as quadratic reciprocity and Artin reciprocity.

The term *reciprocity* seems to go back to Legendre. Originally, the term referred to reciprocity between two primes p and q: whether or not p was a square modulo q being determined according to a simple rule depending on whether or not q was a square modulo p. Quadratic reciprocity, proved by Gauss, is commonly the celebrated result at the end of a course in Elementary Number Theory.

The Shimura-Taniyama conjecture, now known as the modularity theorem (semi-stable case due to Wiles in 1995 and finished off by Breuil, Conrad, Diamond, and Taylor in 2001) relates elliptic curves over $\mathbb{Q}$ to weight two modular forms that are eigen with respect to the action of the Hecke algebra.

We will see that both quadratic reciprocity and the modularity theorem can be interpreted as reciprocity laws. To this end, we need the Galois group.

The absolute Galois group G is the automorphism group of the field of algebraic numbers. This is an extremely complicated group... *extremely* complicated. Some say that the goal of modern number theory is to understand G.

Since G is complicated, we turn instead to trying to understand the (linear) representations of G. These are group homomorphisms from G to the automorphism group of a vector space. This is still complicated, so we content ourselves to understanding the trace of such maps evaluated on Frobenius elements. Specifically, let $\rho\colon G \to \mathrm{GL}(V)$ be a Galois representation. We wish to understand the sequence $\chi_\rho(\mathrm{Frob}_p)$, where χ_ρ is the composition of ρ with trace, and p ranges over all but finitely many primes. A reciprocity law is a "black box" which produces these values in some other way.

2. The absolute Galois group

Let $\overline{\mathbb{Q}}$ be the field of algebraic numbers, the algebraic closure of $\mathbb{Q}$.

Some examples and non-examples:

(1) $\sqrt{5}$, $\sqrt[3]{7-\sqrt{5}}$, and i are in $\overline{\mathbb{Q}}$.

Key words and phrases. reciprocity.

(2) π is not in $\overline{\mathbb{Q}}$
(3) While $\overline{\mathbb{Q}}$ contains all numbers that can be obtained from the integers using multiplication, division, addition, subtraction, and nth root, not every algebraic number can be expressed in this way. (Abel's proof of the insolvability of general quintic polynomials.)

Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote the *absolute Galois group of* $\mathbb{Q}$, the group of automorphisms of $\overline{\mathbb{Q}}$. In particular, for all $g \in G$ and $a, b \in \overline{\mathbb{Q}}$, we have

$$g(a+b) = g(a) + g(b) \quad \text{and} \quad g(ab) = g(a)g(b).$$

Note that for $g \in G$,

(1) $g(t) = t$ for all $t \in \mathbb{Q}$,
(2) if α is a root of a $\mathbb{Z}$-polynomial f, then $g(\alpha)$ is also a root of f.

The absolute Galois group is a very natural group to consider, but it is extremely complicated. There are only two elements of $\mathbf{G}$ which we can completely describe—the identity element e and complex conjugation τ.

Note that the Galois group of a $\mathbb{Z}$-polynomial f (or its splitting field F) is related to the absolute Galois group by the restriction morphism

$$r_F \colon G \to \mathrm{Gal}(F/\mathbb{Q}).$$

Namely, since $g \in G$ permutes the roots of f, it acts on F. Moreover, every automorphism of F can be realized in this way.

3. Frobenius

As mentioned above, we only really have a handle on two elements of the absolute Galois group. We want more. To this end, we consider the Frobenius elements.

First, Frob_∞ is complex conjugation τ. For the others, fix a prime p. Here the situation is more delicate. First, we define a set $\mathcal{F}(p)$, a union of conjugacy classes of elements in the absolute Galois group G. Let Frob_p refer to any element of $\mathcal{F}(p)$.

Because there is choice involved, we must be careful when we talk about Frob_p and only discuss characteristics that do not depend on the choice. What sort of things can we describe? Let $\rho \colon G \to \mathrm{GL}_n(R)$ be a Galois representation. Let $\chi_\rho \colon G \to R$ be the trace

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g)).$$

Then outside of a finite set of bad primes $S = S_\rho$, $\chi_\rho(\mathrm{Frob}_p)$ is well-defined.

Here is a working definition of Frob_p. Namely, we describe $\mathrm{Frob}_p(\alpha)$ when p is unramified with respect to α.

First, note that the action of Frob_p on $\overline{\mathbb{Q}}$ is determined by its action of $\overline{\mathbb{Z}}$. Suppose $\alpha \in \overline{\mathbb{Z}}$. Then α satisfies a monic polynomial f. The $\mathrm{Frob}_p(\alpha)$ is a root of f. Furthermore, the norm $\mathrm{N}(\mathrm{Frob}_p(\alpha) - \alpha^p)$ is divisible by p. If there is only one root β of f such that $\mathrm{N}(\beta - \alpha^p)$ is divisible by p, then $\mathrm{Frob}_p(\alpha)$ is β. It is possible that β is equal to α itself. When there is more than one β, the definition is a bit more subtle.

Example 3.1. Let's compute $\mathrm{Frob}_p(i)$. First, 2 is ramified with respect to i, so 2 is a bad prime. Thus we do not compute $\mathrm{Frob}_2(i)$. It turns out that 2 is the only ramified prime with respect to i. Note that i satisfies $x^2 + 1 = 0$, so for $p > 2$, $\mathrm{Frob}_p(i)$ is either i or $-i$. We compute

$$\mathrm{N}(i - i^3) = \mathrm{N}(2i) = 4 \quad \text{and} \quad \mathrm{N}(-i - i^3) = \mathrm{N}(0) = 0.$$

It follows that $\mathrm{Frob}_3(i) = -i$. A similar computation shows $\mathrm{Frob}_5(i) = i$. More generally, for an odd prime p, we have

$$\mathrm{Frob}_p(i) = \begin{cases} i & \text{if } p \equiv 1 \bmod 4, \\ -i & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Since the various Frobenius elements are elements of the absolute Galois group, they act on other algebraic numbers as well. Let's compute $\mathrm{Frob}_p(\sqrt{2})$. As above, 2 is a bad prime. Since $\sqrt{2}$ satisfies $x^2 - 2 = 0$, we have $\mathrm{Frob}_p(\sqrt{2})$ is $\sqrt{2}$ or $-\sqrt{2}$. We compute

$$\mathrm{N}(\sqrt{2} - (\sqrt{2})^3) = \mathrm{N}(-\sqrt{2}) = -2 \quad \text{and} \quad \mathrm{N}(-\sqrt{2} - (\sqrt{2})^3) = \mathrm{N}(-3\sqrt{2}) = -18.$$

It follows that $\mathrm{Frob}_3(\sqrt{2}) = -\sqrt{2}$. A similar computations shows that $\mathrm{Frob}_5(\sqrt{2}) = -\sqrt{2}$, $\mathrm{Frob}_7(\sqrt{2}) = \sqrt{2}$. More generally,

$$\mathrm{Frob}_p(\sqrt{2}) = \begin{cases} \sqrt{2} & \text{if } p \equiv 1 \text{ or } 7 \bmod 8, \\ -\sqrt{2} & \text{if } p \equiv 3 \text{ or } 5 \bmod 8. \end{cases}$$

4. Galois representation attached to the variety $x^2 - W$

Fix a non-zero square-free integer W. Let E be the variety defined by $x^2 - W$. The complex points of this variety $E(\mathbb{C})$ consists of two points, which we denote $\sqrt{W}$ and $-\sqrt{W}$. Note that these points live in $\overline{\mathbb{Q}}$. In particular, the absolute Galois group G acts by permuting these roots so that for $\sigma \in G$, we have $\sigma(\sqrt{W}) = \pm\sqrt{W}$. This gives rise to a map $\rho_W \colon G \to \{\pm 1\}$ defined by

$$\sigma(\sqrt{W}) = \rho_W(\sigma)\sqrt{W}.$$

Note that ρ_W is a representation $G \to \mathrm{GL}_1(\mathbb{C})$.

In the general mantra, we wish to understand $\chi_{\rho_W}(\mathrm{Frob}_p)$ for good primes p. By relating the cycle type of $\rho_W(\mathrm{Frob}_p)$ to how the polynomial $x^2 - W$ factors, we get the following result.

Theorem 4.1. *W, p as above. Then*

$$\chi_{\rho_W}(\mathrm{Frob}_p) = \rho_W(\mathrm{Frob}_p) = \left(\frac{W}{p}\right),$$

where $\left(\frac{W}{p}\right)$ is the Legendre symbol *defined by*

$$\left(\frac{W}{p}\right) = \#E(\mathbb{F}_p) - 1.$$

Note that on one hand, we are done. Our goal was to produce a "black box" attached to the Galois representation which produces the sequence of traces of Frobenius elements. Specifically, for the Galois representation attached to the variety E defined by $x^2 - W$, the "black box" is a normalized point count of $E(\mathbb{F}_p)$.

5. Reciprocity

In this section, we produce another "black box" to compute $\chi_{\rho_W}(\text{Frob}_p)$, where ρ_W is the Galois representation defined above. This is a reciprocity law which can be used to prove the traditional statement of quadratic reciprocity.

Theorem 5.1 (Quadratic Reciprocity)**.** *Let p and q be odd primes. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4, \\ -1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \bmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \bmod 8. \end{cases}$$

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

Let N be an integer greater than 1. Let $\mathcal{F}_N$ denote the set of functions from $(\mathbb{Z}/N\mathbb{Z})^\times$ to $\mathbb{C}^\times$. A *simultaneous eigenfunction* in $\mathcal{F}_N$ is a function $f \in \mathcal{F}_N$ such that for each $p \nmid N$, there is a complex number a_p with

$$f(p^{-1}x) = a_p f(x) \quad \text{for all } x \in (\mathbb{Z}/N\mathbb{Z})^\times.$$

Theorem 5.2 (Weak Reciprocity)**.** *Given a square-free integer W, there exists a positive integer N and a simultaneous eigenfunction $f \in \mathcal{F}_N$ with eigenvalues $a_2, a_3, \ldots$ such that*

$$\chi_{\rho_W}(\text{Frob}_p) = a_p$$

for every prime $p \nmid N$.

Theorem 5.3 (Strong Reciprocity)**.** *$N = 4|W|$ works in the Theorem above.*

Let's see what these results give us. For an eigenfunction f (normalized so that $f(1) = 1$), and an odd prime p, taking $x = p$, we see that

$$f(1) = 1 = a_p f(p).$$

More generally, taking $x = py$, we get

$$f(y) = a_p f(py)$$

so that

$$f(p)f(y) = f(py).$$

Applying this result to all prime divisors of x, we see that f defines a group homomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Furthermore, for $p \nmid W$, we have $a_p = \left(\frac{W}{p}\right) \in \{\pm 1\}$. This allows us to see precisely what this eigenfunction is. Namely,

$$f(p) = \frac{1}{a_p} = a_p = \left(\frac{W}{p}\right).$$

Note that f is a function on $(\mathbb{Z}/N\mathbb{Z})^\times$. Now Strong Reciprocity says that we can take $N = 4|W|$. This implies that $\left(\frac{W}{p}\right)$ only depends on $p \bmod 4|W|$. This explains the first two equations in the traditional statement of Quadratic Reciprocity.

How does this give the last statement? Suppose $p \equiv q \bmod 4$. Then let $W = (p-q)/4$ so that $p = 4W + q$. Then we compute

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

Now we consider the other case. First note that for any W, $f(p) = 1$ for any prime p dividing $4W - 1$. It follows that

$$f(4W-1) = f(-1) = 1.$$

Suppose $p + q \equiv 0 \bmod 4$. Let $W = (p+q)/4$ so that $q = 4W - p$. We compute

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

Then

$$\left(\frac{W}{p}\right) = \left(\frac{4W}{p}\right) = \left(\frac{p+q}{p}\right) = \left(\frac{q}{p}\right)$$
$$= \left(\frac{W}{q}\right) = \left(\frac{4W}{q}\right) = \left(\frac{p+q}{q}\right) = \left(\frac{p}{q}\right)$$

as desired.

6. Galois representation attached to elliptic curves

Let E be an elliptic curve over $\mathbb{Q}$ with integer coefficients

$$y^2 = x^3 + Ax + B,$$

where A and B are integers such that the discriminant $-16(4A^3 + 27B^2) \neq 0$. We view E as a variety. For a field R, the points $E'(R) = E(R) \cup \{\mathcal{O}\}$ form a group.

Let n be a positive integer. An element $P \in E(\mathbb{C})$ is an *n-torsion* point if

$$\overbrace{P + P + \cdots + P}^{n \text{ times}} = \mathcal{O}.$$

The n-torsion points of E are denoted $E[n]$.

Theorem 6.1. *Let E be an elliptic curve, and let n be a positive integer. All of the n-torsion points of E have coordinates in $\overline{\mathbb{Q}}$, and the number of elements in $E(\overline{\mathbb{Q}})$ that are n-torsion is n^2.*

This theorem implies that G acts on $E[n]$. Note that $E'(\mathbb{C})$ is the complex torus $\mathbb{C}/L$, where L is the lattice of periods associated to the cubic equation. Then $E[n]$ may be modeled as $\frac{1}{n}L/L$. Thus $E[n]$ is a free module of rank 2 over $\mathbb{Z}/n\mathbb{Z}$.

For $\sigma \in G$ and $P, Q \in E[n]$, we have

$$\sigma(P+Q) = \sigma(P) + \sigma(Q).$$

It follows that we have a continuous homomorphism

$$\rho_{E,n} \colon G \to \mathrm{Aut}(E[n]).$$

By choosing a basis for $E[n]$, we identify $\mathrm{Aut}(E[n])$ with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

The kernel of $\rho_{E,n}$ defines a finite Galois extension $K/\mathbb{Q}$ which is the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the various points in $E[n]$. The Galois group $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$ is the image of $\rho_{E,n}$.

It is natural to ask for a description of G_n. When E has complex multiplication over $\mathbb{C}$, then G_n is much smaller than $\mathrm{GL}_n(\mathbb{Z}/n\mathbb{Z})$. Recall that E has complex multiplication when there is a complex number $\alpha \notin \mathbb{Z}$ such that $\alpha L \subseteq L$. In the more common case where E does not have complex multiplication, Serre shows that the index of G_n in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is bounded as a function of n. It follows that $G_p = \mathrm{GL}_2(\mathbb{F}_p)$ for all but finitely many primes p.

The number field K_n depends on E and n. The discriminant of K_n is divisible only by those primes which divide n or the conductor of E. In other words, if $p \nmid n$ is a prime which does not divide the discriminant of E, then $K_n/\mathbb{Q}$ is unramified at p. In this case, Frob_p defines a conjugacy class in G_n. In particular, $\chi_{\rho_{E,n}}(\mathrm{Frob}_p)$ is well-defined for these primes.

Theorem 6.2. *E, n, p, as above. Then*

$$\chi_{\rho_{E,n}}(\mathrm{Frob}_p) \equiv b_p \bmod n,$$

where $b_p = p + 1 - \#E'(\mathbb{F}_p)$.

Note that this means $\rho_{E,n}$ encapsulates information about b_p for all primes of good reduction which are prime to n. This is a striking result since $\rho_{E,n}$ depends on n, and b_p does not depend on n. For fixed E, the representations $\rho_{E,n}$ form a compatible family of Galois representations because they have the "same" traces on Frobenius elements. This is a general fact about étale cohomology.

Notice that b_p is determined by looking at how often $x^3 + Ax + B$ is a square modulo p. This has the same feel as looking at quadratic residues. In other words, the number of times $x^3 + Ax + B$ is a square modulo p is related to the n-torsion in $E'(\mathbb{C})$.

7. The Shimura-Taniyama conjecture

Suppose $f \in S_2(N)$ is a weight 2 cusp form of level N. Then

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \quad \text{where } q = e^{2\pi i z}.$$

Further suppose f is a normalized ($a_1 = 1$) eigenform for the action of the Hecke algebra. Then the coefficients a_n are algebraic integers. Furthermore, the Fourier coefficients of f coincide with its Hecke eigenvalues

$$f|T_n = a_n f \quad \text{for all } n \geq 1.$$

Let K_f be the field generated by the Fourier coefficients of f. Then Shimura associates to f an abelian variety A_f over $\mathbb{Q}$ whose dimension on the degree $[K_f, \mathbb{Q}]$. If f has integer coefficients, then $K_f = \mathbb{Q}$ and so A_f is 1-dimensional. This means that A_f is an elliptic curve E_f. According to a theorem of Eichler and Shimura, the eigenvalues a_p are reflected in the arithmetic of E_f in the following way. If $p \nmid N$, then E_f has good reduction at p. For such a p, we have that a_p coincides with

$$b_p = p + 1 - \#E'_f(\mathbb{F}_p).$$

In other words, $a_p = b_p$ for $p \nmid N$.

The Shimura-Taniyama conjecture asserts there is an analogous relationship for all elliptic curves. Namely, every elliptic curve E over $\mathbb{Q}$ is *modular* in the sense that E is isogenous to an elliptic curve E_f for some $f \in S_2(N)$. In other words, the Shimura-Taniyama conjecture asserts the surjectivity of the construction $f \mapsto A_f$, viewed as a map from eigenforms with integral coefficients to isogeny classes of elliptic curves over $\mathbb{Q}$ of conductor N is surjective.

8. Galois representation attached to modular forms

Suppose $f \in S_2(N)$ is a normalized eigenform. Let E_f denote the associated elliptic curve. Then we have the construction described in Section 6 for producing a family of Galois representations $\rho_{E_f,n}$. These representations are related to f by congruences.

Theorem 8.1. *f, N as above. Then*

$$\chi_{\rho_{E_f,n}}(\mathrm{Frob}_p) \equiv a_p \bmod n$$

for all $p \nmid nN$.

We are most interested in the case where n is a prime number ℓ.

It is tempting to write $\rho_{f,\ell}$. We cannot quite do that, however, since E_f is determined up to isogeny. If one replaces E_f by an isogenous curve, the representations may change. To fix this, we introduce *semisimplifications* of the $\rho_{E_f,\ell}$. This can really be viewed as a fine tuning procedure which, for a fixed elliptic curve E, only affects a small number of representations. Specifically, Mazur shows that $\rho_{E,\ell}$ is irreducible for all ℓ not in $\{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$. The semisimplification of an irreducible representation ρ is ρ itself. Otherwise ρ is "upper-triangular", and extension of a 1-dimensional representation α by another β. Then the semisimplification is the direct sum $\alpha \oplus \beta$.

References

[1] A. Ash and R. Gross, *Fearless symmetry*, Princeton University Press, Princeton, NJ, 2006, Exposing the hidden patterns of numbers, With a foreword by Barry Mazur.

[2] K. A. Ribet, *Galois representations and modular forms*, Bull. Amer. Math. Soc. (N.S.) **32** (1995), no. 4, 375–402.

Dan Yasaki, Department of Mathematics and Statistics, The University of North Carolina at Greensboro, Greensboro, NC 27412, USA

E-mail address: d_yasaki@uncg.edu

URL: http://www.uncg.edu/~d_yasaki/