RECIPROCITY LAWS AND PRIME DECOMPOSITION

HARUZO HIDA

I would like to describe reciprocity laws appeared in the history of number theory in terms of prime decomposition. Hereafter, p and q are always distinct odd primes.

1. Quadratic Reciprocity Law

For an integer n ($p \nmid n$) the Legendre symbol $\left(\frac{n}{p}\right)$ is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv n \mod p \text{ has solution,} \\ -1 & \text{otherwise.} \end{cases}$$

Since $x^2 \equiv n \mod p$ has a solution if and only if $n \in (\mathbb{F}_p^\times)^2$ for $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $n \mapsto \left(\frac{n}{p}\right)$ gives an identification of $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ with $\{\pm 1\}$; in particular, $n \mapsto \left(\frac{n}{p}\right)$ is a character of the finite multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$.

The quadratic reciprocity law guessed by Euler and proven by Gauss is:

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right) \text{ (Legendre, 1785)} \Leftrightarrow \left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \text{ (Euler, 1744)},$$

where $p^* = (-1)^{(p-1)/2}p$. Thus $n \mapsto \left(\frac{p^*}{n}\right)$ is equal to the character: $n \mapsto \left(\frac{n}{p}\right)$.

This character determines how a prime decomposes in $\mathbb{Q}[\sqrt{p^*}]$. We look into the ring $R = \mathbb{Z}[\sqrt{p^*}] = \mathbb{Z}[X]/(X^2 - p^*)$. In R, a prime ideal (q) of $\mathbb{Z}$ could remain prime or become a product of two prime ideals, that is, $(q) = \mathfrak{q}\mathfrak{q}'$ or $(q) = \mathfrak{q}$ for prime ideals $\mathfrak{q}, \mathfrak{q}'$ in R. Note that $R/(q) = \mathbb{F}_q[X]/(X^2 - p^*)$. The polynomial $X^2 - p^*$ is reducible in $\mathbb{F}_q[X]$ if and only if it has solution in $\mathbb{F}_p$:

$$R/(q) \cong \mathbb{F}_q \oplus \mathbb{F}_q \iff \left(\frac{p^*}{q}\right) = 1 \iff (q) = \mathfrak{q}\mathfrak{q}',$$

where $\mathfrak{q}$ is the kernel of the projection of R onto the first factor $\mathbb{F}_q$ in $R/(q) \cong \mathbb{F}_q \oplus \mathbb{F}_q$.

The non-trivial automorphism σ of $\mathbb{Q}[\sqrt{p^*}]$ interchanges the roots of $X^2 - p^*$, it interchanges $\mathfrak{q}$ and $\mathfrak{q}'$; so, $\mathfrak{q}' = \sigma(\mathfrak{q})$. Thus if $\left(\frac{p^*}{q}\right) = 1$, the subgroup of $\mathrm{Gal}(\mathbb{Q}[\sqrt{p^*}]/\mathbb{Q})$ fixing a prime factor of (q) is trivial and is given by the image of $\left(\frac{p^*}{q}\right) = 1$ identifying $\{\pm 1\}$ with $\mathrm{Gal}(\mathbb{Q}[\sqrt{p^*}]/\mathbb{Q})$.

If $(q) = \mathfrak{q}$ remains prime, $[R/(q) : \mathbb{F}_q] = 2$, and $\sigma(\mathfrak{q}) = \mathfrak{q}$. Thus the stabilizer of $\mathfrak{q}$ is the entire Galois group, and $\langle\left(\frac{p^*}{q}\right)\rangle = \{\pm 1\} \cong \mathrm{Gal}(\mathbb{Q}[\sqrt{p^*}]/\mathbb{Q})$ gives the stabilizer. In summary, identifying $\mathrm{Gal}(\mathbb{Q}[\sqrt{p^*}]/\mathbb{Q})$ with $\{\pm 1\}$, the subgroup generated by $\left(\frac{p^*}{q}\right)$ gives the stabilizer of a prime ideal $\mathfrak{q}|q$ in R. The stabilizer is called the decomposition subgroup of q or the *monodromy* group of q. The information of monodromy group of q is equivalent to knowing how the prime (q) splits in R.

Perspective Colloquium Talk at UCLA on February 26, 2001.

2. Cyclotomic Version

Let μ_p be the group of all p–th roots of unity, and consider the extension $\mathbb{Q}[\mu_p]$ generated by p–th roots of unity. Fixing one primitive root of unity, say, $\zeta = \zeta_p = \exp\left(\frac{2\pi\sqrt{-1}}{p}\right)$, μ_p is a cyclic group of order p generated by ζ_p. Each automorphism σ of μ_p takes ζ to another primitive root of unity ζ^m. Since ζ^m is primitive, $p \nmid m$ and hence, we have an identification $\mathrm{Aut}(\mu_p) \cong \mathbb{F}_p^\times$ by $\chi_p : \sigma \mapsto m$. Since $\sigma \in \mathrm{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q})$ induces $\mathrm{Aut}(\mu_p)$ (and $[\mathbb{Q}[\mu_p] : \mathbb{Q}] = |\mathbb{F}_p^\times|$), we see that $\mathrm{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q}) \cong \mathbb{F}_p^\times$ by χ_p. We write $\phi_q \in \mathrm{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q})$ with $\chi_p(\phi_q) = q$; so, $\phi_q(\zeta) = \zeta^q$.

Again we ask how a prime (q) decomposes in the ring $R = \mathbb{Z}[\mu_p]$. Pick a prime ideal $\mathfrak{q}|q$ in R, we find that $R/\mathfrak{q}$ is a finite extension of $\mathbb{F}_q$; so, it is of the form $\mathbb{F}_{q^f}$ for $f = \dim_{\mathbb{F}_q} R/\mathfrak{q}$. Thus $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ is a cyclic group of order f generated by a canonical generator F taking $x \in \mathbb{F}_{q^f}$ to $x^q \in \mathbb{F}_{q^f}$; thus, the automorphism F of $\mathbb{F}_{q^f}$ is induced by ϕ_q; in other words,

- *The monodromy group of $\mathfrak{q}|q$ is given by $\langle\phi_q\rangle \cong \langle q\rangle \subset \mathbb{F}_p^\times$,*
- *q is of order f in $\mathbb{F}_p^\times \iff (q) = \mathfrak{q}\sigma(\mathfrak{q})\cdots\sigma^d(\mathfrak{q})$ in R for $d = [\mathbb{Q}[\mu_p] : \mathbb{Q}]/f$,*

where σ is the generator of $\mathrm{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q})/\langle\phi_q\rangle$.

Thus one feature of the reciprocity law is the determination of the monodromy group of a given prime q in a given Galois extension $K/\mathbb{Q}$.

3. Geometric Interpretation

To further generalize the law, we need to ponder a philosophical reason why we have such an arithmetic way of describing the monodromy group. One feature of the cyclotomic version is the existence of a canonical generator ϕ_q of the monodromy group, and another is the appearance of the exponential function: $\mathbf{e}(z) = \exp(2\pi\sqrt{-1}z)$ because of the fundamental identity:

$$\mathbf{e}\left(\frac{1}{p}\right)^{\phi_q} = \phi_q(\zeta) = \zeta^q = \mathbf{e}\left(\frac{q}{p}\right).$$

So, roughly, the complex analytic function $\mathbf{e} : \mathbb{C} \to \mathbb{C}^\times$ contains all information of the reciprocity law, and $\mathbf{e}\left(\frac{1}{p}\right)$ gives a canonical generator ζ of the field $\mathbb{Q}[\mu_p]$ and behaves nicely under its Galois automorphism.

The function $\mathbf{e}$ gives rise to the following exact sequence:

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{C} \xrightarrow{\mathbf{e}} \mathbb{C}^\times \to 1,$$

and thus we evaluated the function $\mathbf{e}$ at the fraction $\frac{1}{p} \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$.

Hilbert asked in his twelfth problem (of his famous Paris ICM lecture in 1900), for a given Galois extension (actually an abelian extension in his original setting),
Is there any complex analytic function which describes fully the reciprocity law of the extension?

4. Kronecker's Reciprocity Law

In the language of Poincaré, the fundamental group of $\mathbb{C}^\times$ is given by $\mathbb{Z}$, and the universal covering of $\mathbb{C}^\times$ is given by $\mathbb{C} \xrightarrow{\mathbf{e}} \mathbb{C}^\times$. We can create such a situation starting with an imaginary quadratic field $\mathbb{Q}[\sqrt{-D}]$ with discriminant $-D < 0$ in place of $\mathbb{Q}$. Thus for any given ideal $\mathfrak{a} \subset R$ (for the integer ring $R \subset K$), we can think of the following exact sequence:

$$0 \longrightarrow \mathfrak{a} \longrightarrow \mathbb{C} \longrightarrow E(\mathbb{C}) \longrightarrow 0.$$

For the moment $E(\mathbb{C})$ is just a quotient space $\mathbb{C}/\mathfrak{a}$, which is a Riemann surface of genus 1. Actually, for any $\mathbb{R}$–base (w_1, w_2) of $\mathbb{C}$, we can think of $E_L(\mathbb{C}) = \mathbb{C}/L$ for $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$ replacing $\mathfrak{a}$ by L.

Weierstrass studied analysis and geometry of $E(\mathbb{C})$ and created the following function well defined over $E(\mathbb{C})$:

$$x(u) = \mathcal{P}(u) = \frac{1}{u^2} + \sum_{\ell \in L - \{0\}} \left(\frac{1}{(u-\ell)^2} - \frac{1}{\ell^2} \right) \quad \text{(an average over } L\text{)}.$$

This function converges absolutely over $\mathbb{C} - L$ and gives a meromorphic function on $E(\mathbb{C})$. The Taylor expansion of $\mathcal{P}$ and its derivative can be easily computed, and we have

$$x(u) = \mathcal{P}(u) = \frac{1}{u^2} + \frac{g_2}{20}u^2 + \frac{g_3}{28}u^4 + \cdots, \;\; y(u) = \mathcal{P}'(u) = -\frac{2}{u^3} + \sum_{n \geq 1} a_n u^n,$$

where $g_2 = g_2(L) = 60 \sum_{\ell \neq 0} \ell^{-4}$ and $g_3 = g_3(L) = 140 \sum_{\ell \neq 0} \ell^{-6}$. The constant g_2 and g_3 are actually a complex analytic function of $w = (w_1, w_2)$.

Canceling the pole and the constant term, we consider $\varphi = y^2 - 4x^3 + g_2 x + g_3$ which is holomorphic everywhere on a compact Riemann surface $E(\mathbb{C})$; so, it has to be constant. The function φ has to be 0, because φ has no constant term. Thus $u \mapsto \mathbf{E}(u) = (u^3 x(u), u^3 y(u), u^3) \in \mathbf{P}^2$ embeds the Riemann surface into the projective space of dimension 2, whose image is an algebraic curve (called an *elliptic curve*) defined by the homogeneous equation: $Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$ ($x = X/Z$ and $y = Y/Z$). We write $\Delta = g_3^2 - 27 g_2^3$ for the discriminant of $4x^3 - g_2 x - g_3$.

If we pick $\lambda \in \mathbb{C}^\times$, we have an isomorphism of Riemann surface: $u \mapsto \lambda u$ of $E_L(\mathbb{C}) \cong E_{\lambda L}(\mathbb{C})$. By definition, $g_i(\lambda L) = \lambda^{-2i} g_i(L)$ and $\Delta(\lambda L) = \lambda^{-12}\Delta(L)$. The following facts are known from general theory of algebraic curves:

- If $\phi : E_L \to E_{L'}$ is a holomorphic (group) homomorphism with $\phi(0) = 0$, then there exists $\lambda \in \mathbb{C}^\times$ such that $L' \supset \lambda L$ and $\phi(u) = (\lambda u \mod L')$;
- Write any morphism $\phi : E_L \to E_{L'}$ as $\phi(u) = (\phi_x(u), \phi_y(u), 1)$ using the coordinates of the projective space $\mathbf{P}^2$. Then ϕ_x and ϕ_y are rational functions of x_L and y_L, that is, $\phi_x = \frac{A(x,y,g_2,g_3)}{B(x,y,g_2,g_3)}$ and $\phi_y = \frac{\alpha(x,y,g_2,g_3)}{\beta(x,y,g_2,g_3)}$ for polynomials A, B, α, β with coefficients in $\mathbb{Q}$ independent of L;
- Every genus 1 Riemann surface can be obtained as E_L for some L.
- Let $j(w) = j(L) = \frac{g_2^3}{\Delta}$. Then $E_L \cong E_{L'} \iff j(L) = j(L')$.

The function j is an example of *modular functions* and g_2 and g_3 are examples of *modular forms*. What Kronecker found is

Theorem (Kronecker-Weber). *Let H/K be the Hilbert class field of K. Then for each prime ideal $\mathfrak{p}$ of R, write $\phi_\mathfrak{p}$ for the canonical generator of the monodromy group of* $\mathrm{Gal}(H/K)$. *Then $H = K[j(\mathfrak{a})]$ for any ideal $0 \neq \mathfrak{a} \subset R$ and $j(\mathfrak{a})^{\phi_\mathfrak{p}} = j(\mathfrak{p}^{-1}\mathfrak{a})$. In particular,* $\mathrm{Gal}(H/K)$ *is isomorphic to the ideal class group of K.*

We do not prove this, instead we explain why $j(\mathfrak{a})$ is an algebraic number. If $\mathrm{End}(E_L)$ contains the integer ring R of an imaginary quadratic field K, then $RL \subset L$; so, $L \subset \Omega K$ for $0 \neq \Omega \in L$. Thus we may assume that L is an ideal $\mathfrak{a}$ of K. Since the isomorphism class of $E_\mathfrak{a}$ only depends on $\mathfrak{a}$ up to scalar multiplication, there are only countably many isomorphism classes of E_L with $\mathrm{End}(E_L) \supset R$. Regard $E_\mathfrak{a}$ as a curve defined by the equation: $y^2 = 4x^3 - g_2 x - g_3$, and consider its conjugate $E_\mathfrak{a}^\sigma$ defined by $y^2 = 4x^3 - \sigma(g_2)x - \sigma(g_3)$ for any field automorphism σ of $\mathbb{C}$. Then $\mathrm{End}(E_\mathfrak{a}^\sigma)$ contains R because all endomorphisms

are rational functions of (x,y,g_2,g_3); so, applying σ to their coefficients, we get an endomorphism $\phi^\sigma \in \mathrm{End}(E_\mathfrak{a}^\sigma)$ from $\phi \in \mathrm{End}(E_\mathfrak{a})$. The morphism $\phi \mapsto \phi^\sigma$ is an isomorphism of rings. Thus $E_\mathfrak{a}^\sigma = E_\mathfrak{b}$ for an ideal $\mathfrak{b}$ in K and $j(\mathfrak{a})^\sigma = j(\mathfrak{b})$; so, $j(\mathfrak{a})$ has only countably many conjugates. This implies that they are finitely many, because if $x \in \mathbb{C}$ is transcendental over $\mathbb{Q}$, one can embed $\mathbb{Q}(x)$ into $\mathbb{C}$ by continuously many different ways ($\mathbb{C}$ has continuously many transcendental numbers). Thus the number of conjugates of $j(\mathfrak{a})$ is finite. Since $j(\lambda\mathfrak{a}) = j(\mathfrak{a})$, the fractional ideals of K modulo scalar multiplication are finitely many: finiteness of the class group, and

$$\mathrm{Gal}(H/K) \cong \frac{\text{fractional ideals of } K}{\text{principal ideals}} = \text{the class group of } K.$$

This is the explicit class field theory for the imaginary quadratic field K. This type of result is generalized by Shimura-Taniyama and Weil to totally imaginary quadratic extensions (CM fields) of a totally real field, using a quotient $\mathbb{C}^d/L$ for a lattice L of higher rank (Theory of abelian varieties with complex multiplication).

5. Reciprocity Law For Elliptic Curves

We can slightly generalize the above construction. Let

$$E_L[p] = \{u \in E_L(\mathbb{C}) \mid pu = 0\} = \frac{1}{p}L/L \cong \mathbb{F}_p^2.$$

Note that $\mathbf{E}(0) = (0,-2,0) \in \mathbf{P}^2(\mathbb{Q})$. Thus the point 0 of E_L does not move after applying $\sigma \in \mathrm{Aut}(\mathbb{C})$. Then since $\sigma \in \mathrm{Aut}(\mathbb{C})$ brings $p : E_L \to E_L$ to $p : E_L^\sigma \to E_L^\sigma$ because they are rational functions of (x,y,g_2,g_3); so, if E_L is defined over a number field $M = \mathbb{Q}[g_2(L), g_3(L)]$, $\sigma \in \mathrm{Aut}(\mathbb{C}/M)$ induces a linear automorphism of $E_L[p]$. Taking a base $W = (\frac{w_1}{p}, \frac{w_2}{p})$ of $E_L[p]$, we find $\sigma(W) = W\rho(\sigma)$ for a 2×2 matrix $\rho(\sigma) \in GL_2(\mathbb{F}_p)$, and so, we can identify $\mathrm{Gal}(M(E[p])/M)$ with a subgroup $\mathrm{Im}(\rho)$ of $GL_2(\mathbb{F}_p)$. Here $M(E[p])$ is the field generated by $x(\frac{w_i}{p})$ and $y(\frac{w_i}{p})$ $(i = 1,2)$ over M. Thus we have, identifying $E[p]$ with the column vector space $\mathbb{F}_p^2$ by ${}^t(a,b) \mapsto W{}^t(a,b) \in E[p]$, we have

$$x(\rho(\sigma)v)^\sigma = x(v)^\sigma \text{ and } y(\rho(\sigma)v)^\sigma = y(v)^\sigma.$$

This reciprocity law is still half baked, because we have not made explicit the form of $\rho(\phi_\mathfrak{q})$ for the canonical generator $\phi_\mathfrak{q}$ of the monodromy group of a prime $\mathfrak{q}$ of M. This can be done when L is a fractional ideal of an imaginary quadratic field, and the refined version is an example of Shimura's reciprocity laws (although this one is basically due to Kronecker). When L is not in an imaginary quadratic field, $\mathrm{Im}(\rho)$ is almost always full (by a result of Serre), and we can make explicit $\mathrm{Tr}(\rho(\phi_\mathfrak{q}))$ and $\det(\rho(\phi_\mathfrak{q}))$. However this information is still short of determining the splitting of a prime $\mathfrak{q}$ in $M(E[p])$, and the analysis of the Galois representation $\rho : \mathrm{Gal}(M(E[p])/M) \hookrightarrow GL_2(\mathbb{F}_p)$ is still a central subject today.

From what I said, it is clear that *the study of modular functions and modular forms is natural and crutial in algebraic number theory,* although they are rather analytic and geometric objects.