Reciprocity laws

The law of quadratic reciprocity has fascinated mathematicians for over 200 years. Its applications and analogues play a central part in number theory. This is going to be an elementary introduction to "What is the general reciprocity problem?"

Let \( f = T^n + (n-1) T^{n-1} + \ldots + T + 1 \), \( n \in \mathbb{Z} \) be a monic polynomial. Suppose that \( f \) is irreducible, e.g. \( T^2 + 1, \ T^3 - T - 1 \)

In fact, Selmer proved that \( T^n - T - 1 \) is irreducible for every \( n > 1 \).

Let \( p \) be a prime & \( f_p(x) := \) reducing coeff. of \( f(x) \mod p \). 

\[ \text{Spl}(f) = \{ p \mid f_p(x) \text{ splits into distinct linear factors} \} \]

The general reciprocity problem we shall be considering is: "Given \( f(x) \) as above, describe the factorisation of \( f_p(x) \) as a function of the prime \( p \)."

Ask for less: Give a rule to determine which primes belong to \( \text{Spl}(f) \).

Let us see how "Quadratic reciprocity law" gives "reciprocity laws" above:

**Quadratic**

For a quadratic poly \( f(x) \):

1. \( f_p(x) = l_1(x) \) where \( l_1(x) \) is linear.
2. \( f_p(x) = l_1(x) l_2(x) \) where \( l_1(x), l_2(x) \) are linear.
3. \( f_p(x) \) remains irreducible modulo \( p \).
We consider the polynomial of the form $x^2 - q$ where $q$ is a prime. Then $x^2 - q$ splits completely modulo $p$ if $(\frac{q}{p}) = +1$ and remains irreducible if $(\frac{q}{p}) = -1$.

\[ \because \text{P \in \text{Spl}(f) \iff } (\frac{q}{p}) = +1 \]

Since there are infinitely many primes, to describe $\text{Spl}(f)$ we need infinite amount of work by above method. If somehow $(\frac{q}{p})$ is related to $(\frac{p}{q})$ then we are done since there are only finitely many residue classes modulo $q$.

This is given by,

"Quadratic reciprocity law". (Legendre)

For $p$, an odd prime
1. $(-\frac{1}{p}) = (-1)^{(p-1)/2}$
2. $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$
3. If $q$ is another odd prime, distinct from $p$ then $(\frac{2}{p}) = (-1)^{(p-1)(q-1)/4}(\frac{p}{q})$

Theorem: If $q \equiv 1 (\mod 4)$ then $(\frac{p}{q}) = (\frac{q}{p})$

\[ \begin{align*}
2 & \equiv 3 (\mod 4) \quad \text{then} \quad \left\{ \begin{array}{ll}
(\frac{p}{q}) & = (\frac{p}{q}) \text{ if } p \equiv 1 (\mod 4) \\
(\frac{p}{q}) & = -(\frac{p}{q}) \text{ if } p \equiv 3 (\mod 4)
\end{array} \right. \\
\text{e.g.} \quad q = 17 \quad \text{then} \quad \text{Spl}(x^2 - 17) = \left\{ p \mid (\frac{p}{17}) = +1 \right\}
\end{align*} \]

i.e. $p \equiv 1, 2, 4, 8, 9, 13, 15, 16 (\mod 17)$
Splitting of \( x^2 - q \) is given by congruence condn modulo a no. that is dependent on \( f(x) \).

**Cyclotomic polynomials:**

Suppose \( \zeta \) is a primitive \( n \)-th root of unity. Then the minimal poly of \( \zeta \) can be written as \( \Phi_n(x) \) which is of deg \( \phi(n) \). Also,

\[
x^n - 1 = \prod_{d|n} \Phi_d(x).
\]

E.g., \( \Phi_1(x) = x - 1 \), \( \Phi_p(x) = x + x^{-1} + \ldots + x + 1 \)

**Theorem (cyclotomic reciprocity law)**

The cyclotomic poly \( \Phi_n(x) \) factors into distinct linear factors modulo \( p \iff p \equiv 1 \pmod{n} \).

\( \therefore \operatorname{Sel}(f) \) is given by congruence condn depending upon \( f \).

**Abelian polynomials**

A nice description of \( \operatorname{Sel}(f) \) is not always possible. But, one can characterise for which polynomials congruence condn gives the result.

- Let \( K_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \) where \( \alpha_i \in \mathbb{C} \) are roots of \( f \).
- We call it a root field (= splitting field of \( f \)).
- \( f \) is abelian if \( \operatorname{Gal}(K_f/\mathbb{Q}) \) is abelian.

**Abelian polynomial theorem:** The set \( \operatorname{Sel}(f) \) can be described by congruences w.r.t. a modulus depending only on \( f \iff f(x) \) is an abelian polynomial.
Proof of this theorem involves almost all of class field theory over $\mathbb{Q}$.

Let me get to more useful statement by giving a sketch of how to prove the sufficiency part.

\[ \begin{array}{cccc}
K & \mathbb{Q}_K & \mathfrak{p}_K = \mathfrak{p}_1, \ldots, \mathfrak{p}_r & \mathbb{Q}_K / \mathfrak{p}_i \\
\mathbb{Q} & \mathbb{Z} & \mathfrak{p} & \mathbb{Z} / \mathfrak{p} \\
\end{array} \]

residue field extension, cyclic, generated by $\mathfrak{p}$; the Frobenius

$\phi(a) = a^p \equiv a + \mathfrak{p}_i / \mathfrak{p}_i$.

- Except for finitely many primes called (ramified primes) the $\mathfrak{p}_i$'s appearing in $\mathbb{Q}_K$ are all distinct.

- If $K \nmid \mathfrak{p}$ is a Galois extension and $\mathfrak{p}$ is a prime that is not ramified then for each $\mathfrak{p}_i$ there is a unique $\sigma \in G$ such that $\sigma$ reduces to the Frobenius modulo $\mathfrak{p}_i$. We denote it by $\mathfrak{F}_{\mathfrak{p}_i}$. The Artin symbol corresponding to $\mathfrak{p}$ is given by $\mathfrak{F}_{\mathfrak{p}_i}(a) = a^p \equiv a + \mathfrak{p}_i / \mathfrak{p}_i$.

We know that all $\mathfrak{F}_{\mathfrak{p}_i}$'s corresponding to a single $\mathfrak{p}$ are conjugates.

- If $\text{Gal}(K / \mathbb{Q})$ is abelian then the conjugate class is represented by a unique member, called the Artin symbol $\mathfrak{F}_p$, $\mathfrak{F}_p \in G$.
let $\mathbb{Z} \times \mathbb{Z}$ be the free abelian gp generated by the primes. Then, Artin symbol gives a homomorphism $\sigma: \Gamma' \rightarrow G$ by extending $\sigma_{\mathfrak{p}} x \cdot y = \sigma_{\mathfrak{p}} y \cdot \sigma_{\mathfrak{p}} x$ for $x, y = \mathfrak{p}^{-1}$. $\sigma$ is called the Artin map.

Ray group: $\Gamma a = \{ x \in \mathbb{Z}^+ | c = d (\bmod a) \}$ where $a = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_s$, where $\mathfrak{p}_i$'s are ramified primes and $\mathfrak{p}_s > 1$.

Artin reciprocity law: let $K \prec \mathbb{Q}$ be a finite Galois abelian extn with the Galois group $G$. Let $\Gamma'$ be the subgroup of $\mathbb{Q}^\times$ as above. Then the Artin map $\sigma: \Gamma' \rightarrow G$ is surjective whose kernel contains the ray group $\Gamma a$, where $a$ is an appropriate product of the ramified primes.

Artin reciprocity together with the following lemma will prove: If $f(x)$ is an abelian poly., then $\text{Sp}(f)$ can be described by congruence conditions.

Lemma: Suppose $f(x)$ is an abelian poly. with root field $K$, Galois gp $G$ & Artin map $\sigma: \Gamma' \rightarrow G$.

Then except for finitely many exceptional primes $f(x)$ splits modulo $p \iff \sigma p$ is trivial.

$\therefore \text{Sp}(f)$ contains all primes $p$ such that $p \equiv 1 (\bmod a)$ with almost finitely many exceptions.
General polynomial

If $f(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$ which is not abelian, then the best statement one can make is about the relative size of $\text{Spl}(f)$.

Let $\Pi = \text{set of all primes}$ and $T \subseteq \Pi$, $x \in \mathbb{R}$ s.t. $x \geq 1$.

Let $\delta(T, x) = \frac{\# \{ P \in T \mid P < x^{\frac{1}{2}} \}}{\# \{ P \in \Pi \mid P < x^{\frac{1}{2}} \}}$

Then: If $\lim_{x \to \infty} \delta(T, x) = \delta(T)$ then $T$ has density $\delta(T)$.

Dirichlet's theorem: If $\mu = 1$

Suppose $m$ is a positive integer and $a$ is any integer prime to $m$ then the set of all primes congruent to $a \pmod{m}$ has density equal to $\frac{1}{\phi(m)}$.

Weak Takhtajan-Thomas theorem: If $f(x)$ irreducible polynomial in $\mathbb{Z}[x]$ with root field $K_f$ and suppose that $[K_f : \mathbb{Q}] = n$. Then $\text{Spl}(f)$ has density $= \frac{1}{n}$.

Check: This implies Dirichlet's theorem when $f = \Phi_m$. 
- Let $N_p(f)$ = no. of roots of $f$ in $F_p$.

The fundamental insight of Langlands was that there is a "formule" for $N_p(f)$ for every poly. $f$ abelian or not.

Example (Serre): $f = T^3 - T - 1$, $\text{Gal}(K^{1,\alpha}) = S_3$, $f$ is not abelian.

Then $N_p(f) = 1 + ap$ where $a_n$'s are coefficients of the formal power series

$$q \prod_{k=1}^{\infty} \left(1 - q^{-k}\right) \left(1 - q^{-2k^2}\right) = q - q^2 - q^3 + 2q^6 + 2q^8 - \cdots$$

It follows that $a_p \in \{-1, 0, 2\}$

We thus have a formula for $N_p(T^3 - T - 1)$ which constitutes a "reciprocity law for $T^3 - T - 1$".

2. There are reciprocity laws even for $f \in \mathbb{Z}[s, t]$ such as

$f = s^2 + s + t^3 + t^2$.

Fact: $N_p(f) = p - ap$ where $a_n$'s are coeff. of the formal power series

$$q \prod_{k=1}^{\infty} \left(1 - q^{-k}\right)^2 \left(1 - q^{-2k^2}\right)^2 = 0, 1 + a_1q + \sum_{n \geq 2} C_n q^n$$

By exploring properties of these $a_p$'s, Langlands, Wiles, and others (Diamond, Taylor,
(Conrad, ...) have proved the equalities of Artin L-functions & Hecke L-functions for elliptic curves. This equality encapsulates the "reciprocity law". They proved that are valid

"Similar formulae for $N_p(t)$, such equality of $L$-functions are valid for each of the infinitely many $f \in \mathbb{Z}[s,t]$ which defines an elliptic curve; there by settling a conjecture of Shimura, Taniyama I was.

Among all instances of Langlands' program at its most basic level, reciprocity law is a search for patterns in the sequence $N_p(f)$ for fixed but arbitrary $t$.

Langlands predicted that there is a "reciprocity law" for $f$ as soon as he can give an embedding $\mathfrak{f} : \text{Gal}(K^{1/\alpha}) \to \text{GL}_d(\mathbb{C})$

$d = 1$ is a class field theory

Essentially the only known cases are $d = 2$ & $\mathfrak{f}(G_f)$ is solvable (Langlands + Tunnell) $d = 2$ & $\mathfrak{f}(\mathfrak{c})$ is not of the from $(\sigma, 0)$ for any $\alpha \in \mathbb{C}^*$ where $\mathfrak{c} \in G_f$ sending $\alpha \mapsto e^{-i\theta} (\text{Khare + Wintenberger + Kisin})$