The Eisenstein Reciprocity Law

Frank Kelly

May 18, 2005

Abstract

Since the dawn of time primitive man wondered about the peculiar relation that power residue symbols had to each other when their arguments were flipped. In this paper we set to rest the souls of so many caveman mathematicians by proving the Eisenstein reciprocity law and observing two interesting corollaries.

We start with a couple of lemmas.

1 A Couple of Useful Lemmas

Lemma 1. *Let $\boldsymbol{K}/\mathbb{Q}$ be a number field and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the $n = [\boldsymbol{K} : \mathbb{Q}]$ isomorphisms of $\boldsymbol{K}$ into $\mathbb{C}$. If α an algebraic number has the property $|\alpha^{\sigma_i}| \leq 1, i = 1, 2, \ldots, n$ then α is a root of unity.*

Proof. α must be a root of

$$f(x) = \prod_{i=1}^{n} (x - \alpha^{\sigma_i}) \in \mathbb{Z}[x].$$

$|\alpha^{\sigma_i}| \leq 1$ implies the coefficient of x^m in $f(x)$ is an integer less than or equal to $\binom{n}{m}$. Therefore only finitely many such f can exist. $|\alpha^{\sigma_i}| \leq 1$ implies that all powers of alpha also have this property, and since this finite set of polynomials has a finite set of roots, we have that two distinct powers of α must be equal. Therefore α is a root of unity. □

Lemma 2. *For a galois extension $\boldsymbol{K}/\mathbb{Q}$ with galois group $\boldsymbol{G}$, we have for and ideal $\boldsymbol{A}$ in the ring of integers $\mathbf{D}$ that*

$$\prod_{\sigma \in \boldsymbol{G}} \sigma(\boldsymbol{A}) = (N(\boldsymbol{A})).$$

Proof. That the norm is multiplicative allows us to simply prove the case where $\mathbf{A}$ is a prime ideal $\mathbf{P}$.

Let the ideals $\mathbf{P} = \mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_g$ be the ideals in $\{\sigma(\mathbf{P}) : \sigma \in \mathbf{G}\}$. Then

$|\mathbf{G}| = g|Stab_{\mathbf{G}}(P)|$ where $Stab_{\mathbf{G}}(P)$ is the set of automorphisms fixing $\mathbf{P}$. By our favorite equation, $efg = n = [\mathbf{K} : \mathbb{Q}] = |\mathbf{G}|$, we must have $|Stab_{\mathbf{G}}(P)| = ef$. By stuff we did in class,

$$\prod_{\sigma \in \mathbf{G}} \sigma(\mathbf{P}) = (\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_g)^{ef} = (p)^f = (p^f),$$

where p is the integer prime such that $P_i \cap \mathbb{Z} = p\mathbb{Z}$. But $N(\mathbf{P}) = |\mathbf{D}_m/\mathbf{P}| = p^f$, so we're done.

Note here that we also used for $\mathbf{P}_i, \mathbf{P}_j$ primes in $\mathbf{D}$ lying over p that there exists $\sigma \in \mathbf{G}$ such that $\sigma(\mathbf{P}_i) = \mathbf{P}_j$. To see this, assume not; by the generalized chinese remainder theorem, there exists some $\alpha \in \mathbf{D}$ such that $\alpha \equiv 0(\mathbf{P}_0), \alpha \equiv 1(\sigma\mathbf{P}_i)$ for the rest of the i and for all $\sigma \in \mathbf{G}$. Then $N(\alpha) = \prod_{\sigma \in \mathbf{G}} \sigma\alpha \in \mathbf{P}_0 \cap \mathbb{Z} = p\mathbb{Z}$, so $N(\alpha) \in \mathbf{P}_i$. Because $\mathbf{P}_i$ is prime, there must be some σ such that $\sigma\alpha \in \mathbf{P}_i$. But then we would have $\alpha \in \sigma^{-1}\mathbf{P}_i$, which contradicts the fact that $\alpha \equiv 1(\sigma^{-1}\mathbf{P}_i)$. □

2 The Power Residue Symbol

Lemma 3. *Let $\boldsymbol{D}_m$ be the ring of integers of $\mathbb{Q}(\zeta_m)$, $\alpha \in \boldsymbol{D}_m, \alpha \notin \boldsymbol{P}$ a prime ideal of $\boldsymbol{D}_m$. Then there is an integer i, unique modulo m, such that*

$$\alpha^{(NP-1)/m} \equiv \zeta_m^i(\boldsymbol{P}).$$

Proof. $|\mathbf{D}_m/\mathbf{P}| = NP - 1$ so by Euler's theorem $\alpha^{(NP-1)/m} \equiv 1(\mathbf{P})$. Therefore

$$\prod_{i=0}^{m-1} (\alpha^{(NP-1)/m} - \zeta_m^i) \equiv 0(\mathbf{P}).$$

$\mathbf{P}$ is prime, so one of the lefthand factors must be 0, so there must be an $i, 0 \leq i < m$ such that $\alpha^{(NP-1)/m} \equiv \zeta_m^i(\mathbf{P})$. This i is unique modulo m because $\zeta_m^i \neq \zeta_m^j(\mathbf{P})$ when $i \neq j(m)$. □

Definition. *For $\alpha \in \boldsymbol{D}_m, \boldsymbol{P}$ a prime ideal not containing m, define the mth power residue symbol $(\alpha/\boldsymbol{P})_m$ as follows:*

(i) $(\alpha/\boldsymbol{P})_m = 0$ *if* $\alpha \in \boldsymbol{P}$

(ii) If $\alpha \notin \boldsymbol{P}, (\alpha/\boldsymbol{P})_m$ *is the unique mth root of unity such that* $\alpha^{(\boldsymbol{NP}-1)/m} \equiv (\alpha/\boldsymbol{P})_m(\boldsymbol{P})$.

Proposition 1. *(i)* $(\alpha/\boldsymbol{P})_m = 1 \iff x^m \equiv \alpha(\boldsymbol{P})$ *has a solution in* $\boldsymbol{D}_m$.

(ii) $\forall \alpha \in \boldsymbol{D}_m, \alpha^{(NP-1)/m} \equiv (\alpha/\boldsymbol{P})_m(\boldsymbol{P})$.

(iii) $(\alpha\beta/\boldsymbol{P})_m = (\alpha/\boldsymbol{P})_m(\beta/\boldsymbol{P})_m$.

(iv) If $\alpha \equiv \beta(\boldsymbol{P})$ *then* $(\alpha/\boldsymbol{P})_m = (\beta/\boldsymbol{P})_m$.

Proof. The proofs of these statements are similar to those for the analogous statements when $m = 2$ and are therefore omitted here. □

We extend the definition of $(\alpha/\mathbf{P})_m$ in an analogous way for $(\alpha/\beta)_m$ with β relatively prime to m. This is essential to the language of the reciprocity law.

Definition. *For an ideal $\boldsymbol{A} \subset \boldsymbol{D}_m$ relatively prime to m with $\boldsymbol{A} = \boldsymbol{P}_1\boldsymbol{P}_2 \dots \boldsymbol{P}_n$ the decomposition of $\boldsymbol{A}$ into prime ideals. For $\alpha \in \boldsymbol{D}_m$, define $(\alpha/\boldsymbol{A})_m = \prod_i (\alpha/\boldsymbol{P}_i)$. For $\beta \in \boldsymbol{D}_m, \beta$ relatively prime to m let $(\alpha/\beta)_m = (\alpha/(\beta))_m$.*

We know state three important properties of our generalization. Because they are straightforward from the definitions, we do not include proofs here.

Proposition 2. *If $\boldsymbol{A}, \boldsymbol{B}$ are ideals relatively prime to (m), then*

(i) $(\alpha\beta/\boldsymbol{A})_m = (\alpha/\boldsymbol{A})_m(\beta/\boldsymbol{A})_m$.

(ii) $(\alpha/\boldsymbol{AB})_m = (\alpha/\boldsymbol{A})_m(\alpha/\boldsymbol{B})_m$.

(iii) If α is relatively prime to $\boldsymbol{A}$ and $x^m \equiv \alpha(\boldsymbol{A})$ has a solution in $\boldsymbol{D}_m$ then $(\alpha/\boldsymbol{A})_m = 1$.

Below, using the exponential notation for automorphisms, we show the effect of $\sigma \in \mathbf{G} = Gal(\mathbf{K}/\mathbb{Q})$ on our power residue symbol.

Proposition 3. *If $\boldsymbol{A}$ is relatively prime to m and $\sigma \in \boldsymbol{G}$ then*

$$(\frac{\alpha}{\boldsymbol{A}})_m^\sigma = (\frac{\alpha^\sigma}{\boldsymbol{A}^\sigma})_m.$$

Proof. By the multiplicativity properties in the previous propositions, it suffices to check this for $\mathbf{A} = \mathbf{P}$ a prime ideal. By our definition of the power symbol,

$$\alpha^{(NP-1)/m} = (\frac{\alpha}{\mathbf{P}})_m(\mathbf{P}).$$

Applying σ to both sides,

$$(\alpha^\sigma)^{(NP-1)/m} = (\frac{\alpha}{\mathbf{P}})_m^\sigma(\mathbf{P}^\sigma)$$

since $N(\mathbf{P}^\sigma) = N(\mathbf{P})$. Thus $(\frac{\alpha^\sigma}{\mathbf{A}^\sigma})_m \equiv (\frac{\alpha}{\mathbf{A}})_m^\sigma(\mathbf{P})$, which implies $(\frac{\alpha^\sigma}{\mathbf{A}^\sigma})_m = (\frac{\alpha}{\mathbf{A}})_m^\sigma(\mathbf{P})$. □

3 The Stickelberger Relation

Suppose the prime ideal $\mathbf{P} \subset \mathbf{D}_m \subset \mathbb{Q}(\zeta_m)$ and $m \notin \mathbf{P}$. Also letting $N(\mathbf{P}) = p^k = q$, we have the field $\mathbf{F} = \mathbf{D}_m/\mathbf{P}$ is the field with $p^k = q$ elements. For $\gamma \in \mathbf{D}_m, \bar{\gamma} = t$ the residue class of γ modulo $\mathbf{P}$, define the multiplicative character χ_P and the additive character ψ as follows:

Definition. *(i)* $\chi_P = (\frac{\gamma}{\boldsymbol{P}})_m^{-1} = (\frac{\bar{\gamma}}{\boldsymbol{P}})_m$.

(ii) $\psi(t) = \zeta_p^{tr(t)}$ *where* $tr(t) = t + t^p + t^{p^2} + \ldots + t^{p^{f-1}}$.

Note that χ_P is well-defined and multiplicative by the Proposition 1. Using these, let $g(\mathbf{P}) = \sum_{t \in \mathbf{F}} \chi_p(t)\psi(t)$ and $\Phi(\mathbf{P}) = g(\mathbf{P})^m$. At this point we are now ready to state the Stickelberger relation.

Theorem 4. *(Stickelberger Relation) If* $\boldsymbol{P}$ *is prime in* $\boldsymbol{D}_m$ *and* $m \notin \boldsymbol{P}$ *then*

$$(\Phi(\boldsymbol{P})) = \prod_{\sigma_t} (\sigma_t^{-1}(\boldsymbol{P}))^t$$

where $1 \leq t < m$ *and* $(t, m) = 1$.

While this machinery seems complicated now, the function Φ is essential to manipulations of the power residue symbol.

4 Moving right along...

For an ideal $\mathbf{A} \subset \mathbf{D}_m$ relatively prime to m with prime decomposition $\mathbf{A} = \mathbf{P}_1\mathbf{P}_2 \ldots \mathbf{P}n$, define $\Phi(\mathbf{A}) = \Phi(\mathbf{P}_1)\Phi(\mathbf{P}_2) \ldots \Phi(\mathbf{P}_n)$. There are a few natural consequences of this definition.

Proposition 5. *For* $\boldsymbol{A}, \boldsymbol{B} \subset \boldsymbol{D}_m$ *both prime to* m, $\alpha \in \boldsymbol{D}_m$ *also prime to* m, *and let* $\gamma = \sum_t t\sigma_t^{-1}$. *Using the symbolic power notation* $\alpha^{\sum k\sigma} = \prod_\sigma \sigma(\alpha)^k$ *for* $1 \leq t < m$ *and* $(t, m) = 1$, *we have the following:*

(i) $\Phi(\boldsymbol{AB}) = \Phi(\boldsymbol{A})\Phi(\boldsymbol{B})$

(ii) $|\Phi(\boldsymbol{A})|^2 = (N\boldsymbol{A})^m$

(iii) $(\Phi(\boldsymbol{A})) = \boldsymbol{A}^\gamma$

(iv) $\Phi((\alpha)) = u(\alpha)\alpha^\gamma$ *for* $u(\alpha)$ *a unit in* $\boldsymbol{D}_m$

Proof. (i) is obvious from the definition of $\Phi(\mathbf{A})$. By multiplicativity of the norm, we only need to show (ii) for a prime $\mathbf{P}$. But then we have $|\Phi(\mathbf{A})|^2 = |g(\mathbf{P})^m|^2 = (N(\mathbf{P}))^m$. (iii) is the generalized statement of the Stickleberger Relation. By (iii), we get $(\Phi(\mathbf{A})) = (\alpha)^\gamma = (\alpha^\gamma)$, which means that $\Phi((\alpha))$ and α^γ generate the same ideal and are therefore equal up to a unit multiple. □

But how, praytell, does σ act on $\Phi(\mathbf{A})$?

Proposition 6. *For* $\boldsymbol{A} \subset \boldsymbol{D}_m$ *and* $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, *we have*

$$\Phi(\boldsymbol{A})^\sigma = \Phi(\boldsymbol{A}^\sigma).$$

Proof. Once again we need only prove this for $\mathbf{P}$ a prime ideal by the multiplicativity of everything.

First note that we can write

$$g(\mathbf{P}) = \sum_\alpha (\frac{\alpha}{\mathbf{P}})_m^{-1} \zeta_p^{tr(\bar{\alpha})}$$

summing over coset representatives of $\mathbf{D}_m/\mathbf{P}$.

Consider ρ the automorphism of $\mathbb{Q}(\zeta_m, \zeta_p)/\mathbb{Q}$ that is σ on $\mathbb{Q}(\zeta_m)$ and the identity map on $\mathbb{Q}(\zeta_p)$. Note this ρ exists because $(p, m) = 1$. Using Proposition 3, we get

$$g(\mathbf{P})^\rho = \sum_\alpha (\frac{\alpha^\sigma}{\mathbf{P}^\sigma})_m^{-1} \zeta_p^{tr(\bar{\alpha})},$$

because $tr(\bar{\alpha}) \in \mathbb{Z}/p\mathbb{Z}$ implies that $tr(\bar{\alpha}^\sigma) = tr(\bar{\alpha})$. Since this is the form of $g(\mathbf{P})^\sigma$, we simply raise both sides of this equation to the mth power to get the equation we wanted for prime ideals. □

Proposition 7. *For $\alpha \in \boldsymbol{D}_m, |\alpha^\gamma|^2 = |N(\alpha)|^m$.*

Proof. Let σ_{-1} be the complex conjugation automorphism on $\mathbb{Q}(\zeta_m)$. We have

$$|\alpha^\gamma|^2 = \alpha^\gamma \alpha^{\gamma\sigma_{-1}} = \alpha^{\gamma(1+\sigma_{-1})}.$$

By our definition, $\sigma_{-1}\gamma = \sigma_{-1} \sum t\sigma_t^{-1} = \sum t\sigma_{-t}^{-1}$. The indices are equivalent modulo m, and so $\gamma = \sum (m-t)\sigma_{m-t}^{-1}$. Reordering and using the fact that $t = m - (m-t)$ we get $(1+\sigma_{-1})\gamma = m \sum \sigma_t^{-1}$. Since $N(\alpha) = \alpha^{\sum \sigma_t^{-1}}$, we have the desired equation. □

At this point you're probably asking, "Hold on, what's with all these lemmas, and what about that '$u(\alpha)$' in Proposition 5?" I was just getting to that...

Proposition 8. *For $\alpha \in \boldsymbol{D}_m$ relatively prime to m, $\Phi((\alpha)) = u(\alpha)\alpha^\gamma$ with $u(\alpha) = \pm\zeta_m^i$ for some integer i.*

Proof. The first part merely restates Proposition 5, part (iv).

By Proposition 5, part (ii) we have $|\Phi((\alpha))|^2 = (N\alpha)^m$ and Proposition 7 we have $|\alpha^\gamma|^2 = |N(\alpha)|^m$.

We also know $N((\alpha)) = |N(\alpha)|$, because $(N((\alpha))) = \prod \sigma((\alpha)) = \prod(\sigma\alpha) = (\prod \sigma(\alpha)) = (N(\alpha))$. Therefore the two can differ by at most an integer unit, so their absolute values are equal.

These three facts together show that $|u(\alpha)| = 1$, and Proposition 6 implies that $|u(\alpha)^\sigma| = 1$ as well for each $\sigma \in \mathbf{G}$. Then the Useful Lemma implies that u is a root of unity, and since the only roots of unity in $\mathbb{Q}(\zeta_m)$ are $\pm\zeta_m^i$, it follows that $u(\alpha)$ must be one of those. □

5 Back to the power residue symbol

Proposition 9. *For prime ideals $\boldsymbol{P}, \boldsymbol{P'} \subset \boldsymbol{D}_m$ both prime to m with $(N\boldsymbol{P}, N\boldsymbol{P'}) = 1$, we have*

$$(\frac{\Phi(\boldsymbol{P})}{\boldsymbol{P'}})_m = (\frac{N\boldsymbol{P'}}{\boldsymbol{P}})_m.$$

Proof. Let $N\mathbf{P}' = p'^{k'} = q'$. Since $q' \equiv 1(m)$, we get the following modulo p' by exponentiating:

$$g(\mathbf{P})^{q'} \equiv \sum \chi_P(t)^{q'} \psi(t)^{q'}$$
$$\equiv \sum \chi_P(t)\psi(q't)$$
$$\equiv (\frac{q'}{\mathbf{P}})_m g(\mathbf{P}),$$

the second step arising because $q' = p'^{f'}$. If we separate one factor

$$g(\mathbf{P})^{q'-1} = \Phi(\mathbf{P})^{(q'-1)/m},$$

but the righthand side is equivalent to $(\frac{\Phi(\mathbf{P})}{\mathbf{P}'})_m$ modulo $\mathbf{P}'$. We can substitute back to get

$$(\frac{\Phi(\mathbf{P})}{\mathbf{P}'})_m \equiv (\frac{N\mathbf{P}'}{\mathbf{P}})_m(\mathbf{P}'),$$

and since $m \notin \mathbf{P}'$ we get equality in addition to congruence. □

Note that this generalizes to arbitrary ideals $\mathbf{A}, \mathbf{B} \subset \mathbf{D}_m$ that are prime to m and have $(N\mathbf{A}, N\mathbf{B}) = 1$, because the power residue symbol is multiplicative.

Corollary 10. *Suppose $\boldsymbol{A}, \boldsymbol{B}$ are as above, and also $\boldsymbol{A} = (\alpha)$ for some $\alpha \in \boldsymbol{D}_m$. Then*

$$(\frac{u(\alpha)}{\boldsymbol{B}})_m(\frac{\alpha}{N\boldsymbol{B}})_m = (\frac{N\boldsymbol{B}}{\alpha})_m.$$

Proof. First by Proposition 5, part (iv) we have

$$(\frac{\Phi(\alpha)}{\mathbf{B}})_m = (\frac{u(\alpha)}{\mathbf{B}})_m(\frac{\alpha^\gamma}{\mathbf{B}})_m.$$

By Proposition 3, we know

$$(\frac{\alpha^{t\sigma_t^{-1}}}{\mathbf{B}})_m = (\frac{\alpha^{\sigma_t^{-1}}}{\mathbf{B}})_m^t = (\frac{\alpha^{\sigma_t^{-1}}}{\mathbf{B}})_m^{\sigma_t} = (\frac{\alpha}{\mathbf{B}^{\sigma_t}})_m.$$

Therefore we can take the product over all t to get

$$(\frac{\alpha^\gamma}{\mathbf{B}})_m = \prod_t (\frac{\alpha^{t\sigma_t^{-1}}}{\mathbf{B}})_m = \prod_t (\frac{\alpha}{\mathbf{B}^{\sigma_t}})_m = (\frac{\alpha}{N\mathbf{B}})_m.$$

The multiplicativity of the power symbol and Lemma 2 give us the final equality. □

Now we assume that $m = l$ some odd prime number.

Lemma 4. *For $\boldsymbol{A} \subset \boldsymbol{D}_l$ prime to l, we have $\Phi(\boldsymbol{A}) \equiv \pm 1(l)$.*

Proof. If we can show that for a prime $\mathbf{P} \subset \mathbf{D}_l, \Phi(\mathbf{P}) \equiv -1(l)$, we'll get the result by multiplicativity. First from the definitions, we get

$$\Phi(\mathbf{P}) = g(\mathbf{P})^l \equiv \sum_t \chi_P(t)^l \psi(t)^l(l).$$

In the character sum the $\chi_P(t)^l$ values vanish because $\mathbf{P}$ is prime to l, and $\psi(t)^l = \psi(tl)$. Since ψ is a nontrivial additive character, $\psi(0) = 1$ and the $\sum_t \psi(t) = 0$, so we now have

$$\sum_t \chi_P(t)^l \psi(t)^l \equiv \sum_{t \neq 0} \psi(lt) \equiv -1(l).$$

□

6 The PROOF!

Definition. *$\alpha \in \boldsymbol{D}$ is **primary** if α is prime to l and $\alpha \equiv n(1-\zeta_l)^2$ for some $n \in \mathbb{Z}$.*

Lemma 5. *If $\alpha \in \boldsymbol{D}$ is primary, then $u(\alpha) = \pm 1$.*

Proof. $(1-\zeta_l)$ is stable under $\sigma \in \mathbf{G}$ because $(1-\zeta_l)$ is the unique prime above l. Then $(1-\zeta_l)^\gamma \subset (1-\zeta_l)$. $\Phi(\alpha) = u(\alpha)\alpha^\gamma$, so by Lemma 4 we have $u(\alpha)\alpha^\gamma \equiv \pm 1(l)$. By definition $\alpha \equiv n(1-\zeta_l)^2$, so

$$\alpha^\gamma = n^\gamma = n^{1+2+\ldots+(l-1)}(1-\zeta_l)^2.$$

By ol' fashioned QR, we know $n^{(l-1)/2} \equiv \pm 1(l)$, which implies

$$\alpha^\gamma \equiv (\pm 1)^l \equiv \pm 1(1-\zeta_l)^2,$$

which means that $u(\alpha) \equiv \pm 1(1-\zeta_l)^2$. Proposition 8 implies $u(\alpha) = \pm\zeta_l^i$ for some i, so if we can show $l \mid i$, we'll be done.

$\zeta_l^i \equiv \pm 1(1-\zeta_l)^2$, and $\zeta_l = 1-(1-\zeta)$, so

$$1 - i(1-\zeta_l) \equiv \pm 1(1-\zeta_l)^2.$$

If it were congruent to -1, then we would get $(1-\zeta_l) \mid 2$, which is impossible since l is odd. So it must be congruent to one, and after subtracting one from both sides we get $(1-\zeta_l) \mid i$, which means $l \mid i$. □

Proposition 11. *For $\alpha \in \boldsymbol{D}_l$ primary, $\boldsymbol{B}$ an ideal prime to l with $N\boldsymbol{B}$ prime to α, we have*

$$(\frac{\alpha}{N\boldsymbol{B}})_l = (\frac{N\boldsymbol{B}}{\alpha})_l.$$

Proof. By Corollary 10, all we need is that $(u(\alpha)/\mathbf{B}) = 1$. α primary implies $u(\alpha) = \pm 1$ by Lemma 5, and since l is odd $(\pm 1)^l = \pm 1$, so $(u(\alpha)/\mathbf{B})$ must in fact be 1. □

Theorem 12. *(Eisenstein Reciprocity) Let l be an odd prime, $a \in \mathbb{Z}$ prime to l, and $\alpha \in \boldsymbol{D}_l$ primary. Also let α and a be relatively prime. Then*

$$(\frac{\alpha}{a})_l = (\frac{a}{\alpha})_l.$$

Proof. For a prime $p \in \mathbb{Z}, p \neq l$ with p prime to $\alpha \in \mathbf{D}_l$, let $\mathbf{P} \subset \mathbf{D}_l$ lie over p. Thus $N\mathbf{P} = p^f$. In Proposition 11, we substitute $\mathbf{P}$ for $\mathbf{B}$, and we get

$$(\frac{\alpha}{p})_l^f = (\frac{p}{\alpha})_l^f.$$

Because $f \mid (l-1) = [\mathbb{Q}(\zeta_l) : \mathbb{Q}]$, we know $(f, l) = 1$. So

$$(\frac{\alpha}{p})_l = (\frac{p}{\alpha})_l.$$

And that's right! By *multiplicativity* we get

$$(\frac{\alpha}{a})_l = (\frac{a}{\alpha})_l.$$

□

7 Applications

The reciprocitly law immediately gives us an interesting test for whether integers are l^{th} powers.

Theorem 13. *Let $a \in \mathbb{Z}$ with $l \nmid a$ for l an odd prime. If $x^l \equiv a(p)$ has a solution for all but finitely many primes p, then $a = b^l, b \in \mathbb{Z}$.*

Proof. We begin by restating the problem. If $a \neq b^l$ then there are infinitely many p such that $x^l \equiv a(p)$ has no solution.

Assume $a \in \mathbb{Z}, a \neq b^l$. Let $a\mathbf{D}_l = \mathbf{P}_1^{e_1}\mathbf{P}_1^{e_1} \dots \mathbf{P}_n^{e_n}$. We want to show $l \nmid a_i$ for some at least one i. Let $p_i\mathbb{Z} = \mathbf{P}_i \cap \mathbb{Z}$. $l \nmid a$ implies $l \neq p_i$, which means p_i is unramified in $\mathbf{D}_l$. Thus $ord_{p_i} a = ord_{\mathbf{P}_i} a = a_i$. If $l \mid a_i$ for all i then a would necessarily by an l^{th} power, so we can assume without loss of generality l does not divide one of them, say a_n.

Let $\{\mathbf{Q}_1, \mathbf{Q}_2, \dots, \mathbf{Q}_k\}$ be a set of primes such that $\mathbf{Q}_i \neq \mathbf{P}_j$ for all i, j and also $\mathbf{Q}_i \neq (1 - \zeta_l)$. Using the chinese remainder theorem and the fact that these primes are all distinct, we know there exists $\delta \in \mathbb{D}_l$ such that $\delta \equiv 1(\mathbf{Q}_i)$ for $i = 1, 2, \dots, k, \delta \equiv 1(l), \delta \equiv 1(\mathbf{P}_j)$ for $j = 1, 2, \dots, n-1$, and $\delta \equiv \alpha(\mathbf{P}_n)$ where the element α is such that $(\alpha/\mathbf{P}_n)_l = \zeta_l$.

$\delta \equiv 1(l)$ implies δ is primary, so by our construction we get

$$(\frac{a}{\delta})_l = (\frac{\delta}{a})_l = \prod (\frac{\delta}{\mathbf{P}_i})_l^{a_i} = \zeta_l^{a_n} \neq 1.$$

But considering the prime decomposition $(\delta) = \mathbf{R}_1\mathbf{R}_2 \dots \mathbf{R}_m$, we get

$$(\frac{a}{\delta})_l = \prod_j (\frac{a}{\mathbf{R}_j})_l.$$

So we immediatel get that for some $j, (a/\mathbf{R}_j)_l \neq 1$. By construction of δ we get that that particular $\mathbf{R}_j \notin \{\mathbf{Q}_1, \mathbf{Q}_2, \ldots, \mathbf{Q}_k\} \cup \{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_n\} \cup \{(1-\zeta_l)\}$.

Since this set of primes was arbitrary, we have therefore shown that there are infinitely many such $\mathbf{R}$'s such that the power symbol does not equal one, and hence $x^l \equiv a(\mathbf{R})$ is not solvable. Let the above $\mathbf{R}_j = \mathbf{Q}, \mathbf{Q} \cap \mathbb{Z} = q\mathbb{Z}$, then we necessarily get infinitely many integer primes q such that $x^l \equiv a(q)$ is not solvable because only finitely many primes of $\mathbf{D}_l$ lie over q. □

We also consider a 1912 theorem of Furtwangler that utilizes Eisenstein reciprocity to make progress on Fermat's Last Theorem.

Theorem 14. *(Furtwangler)For x, y, z non-zero, pairwise relatively prime integers such that $x^l + y^l + z^l = 0$ and $l \nmid yz$, we have for all prime factors p of y that $p^{l-1} \equiv 1(l^2)$.*

First we have a lemma to prove.

Lemma 6. *If $i \neq j, 0 \leq i, j < l$, then $x + \zeta^i y$ and $x + \zeta^j y$ are relatively prime in $\boldsymbol{D}_l$. Note here $\zeta = \zeta_l$.*

Proof. Suppose for an ideal $\mathbf{A} \subset \mathbf{D}_l$ and $x + \zeta^i y, x + \zeta^j y \in \mathbf{A}$. This implies $(\zeta^j - \zeta^i)x, (\zeta^i - \zeta^j)y \in \mathbf{A}$ also. $(x, y) = 1$ implies $(\zeta^j - \zeta^i) \in \mathbf{A}$, which implies $\lambda = 1 - \zeta \in \mathbf{A}$. (λ) is maximal, so either $(\lambda) = \mathbf{A}$ or $\mathbf{A} = \mathbf{D}_l$. If the former were true, the consider the factorization we get from the our supposition:

$$(x + y)(x + \zeta y) \ldots (x + \zeta^{l-1} y) = (-z)^l.$$

(λ) maximal then implies $(-z) \in (\lambda)$ and consequently that $z \in (\lambda)$, and thus $l \mid z$, which contradicts our assumption. Therefore $\mathbf{A} = \mathbf{D}_l$, so $x + \zeta^i y, x + \zeta^j y$ generate the unit ideal. □

We also get this nice corollary.

Corollary 15. *The ideals generated by $(x + \zeta^i y)$ are perfect l^{th} powers.*

Now back to our proof.

Proof. We actually make two claims: first that for an element $\alpha = (x+y)^{l-2}(x+\zeta y)$ we have α is a perfect l^{th} power. This is merely by Corollary 15. The second claim is that $\alpha \equiv 1 - u\lambda(\lambda^2$ with $u = (x + y)^{l-2} y$. To see this notice $(x+\zeta y) = x+y-y\lambda$, and so $\alpha = (x+y)^{l-1} - \lambda u$. We know $x^l + y^l + z^l \equiv x+y+z(l)$. If $l \mid (x + y)$ we would get $l \mid z$, which is a contradiction. So $l \nmid (x + y)$ and $(x + y)^{l-1} \equiv 1(l)$, which implies our second claim.
Now consider $\zeta^{-u}\alpha = (1 - \lambda)^{-u}\alpha \equiv (1 + u\lambda)(1 - u\lambda) \equiv 1(\lambda^2)$. This is our condition for $\zeta^{-u}\alpha$ to be primary. Then by Eisenstein reciprocity we get

$$(\frac{p}{\zeta^{-u}\alpha})_l = (\frac{\zeta^{-u}\alpha}{p})_l = (\frac{\zeta}{p})_l^{-u}(\frac{\alpha}{p})_l. \tag{1}$$

We already claimed and proved $(\alpha) = (\zeta^{-u}\alpha)$ is an l^{th} power, so we get that the left hand side of (1) is equal to 1. Furthermore, $p \mid y, \alpha \equiv (x+y)^{l-1}(p)$, so

$$(\frac{\alpha}{p})_l = (\frac{(x+y)^{l-1}}{p})_l = (\frac{p}{(x+y)^{l-1}})_l = 1,$$

becaue we know that the ideal generated by $(x+y)$ must be an l^{th} power.

Now we also get from (1) that $(\zeta/p)_l^u = 1$ because otherwise the left hand side of that equation would be -1. All that remains is to compute $(\zeta/p)_l$.

Let $p\mathbf{D}_l = \mathbf{P}_1\mathbf{P}_2 \dots \mathbf{P}_k$, and since $N\mathbf{P}_i = p^f$ and also since $p \neq l, e = 1$, we have that $gf = l - 1$. Then we have

$$(\frac{\zeta}{p})_l = \prod_i (\frac{\zeta}{\mathbf{P}_i})_l = \prod_i \zeta^{(p^f-1)/l} = \zeta^{k[(p^f-1)/l]}.$$

Since $(\zeta/p)_l^u = 1$, we get

$$uk\frac{p^f - 1}{l} \equiv 0(l).$$

$g \mid l - 1$ implies $l \nmid g$. $u = (x+y)^{l-2}y$ implies $l \nmid u$. So then we necessarily have

$$\frac{p^f - 1}{l} \equiv 0(l), p^f \equiv 1(l^2).$$

The fact that $f \mid l - 1$ then gives us our desired result. □

8 Conclusion

Like many great number theory achievements, what are important than this result or its consequences are the steps needed to reach the final proof. It combined a great deal of familiarity with the structure of cyclotomic field extensions along with the arithmetic of Jacobi sums, bringing together many aspects from the algebra we have studied up to this point.

9 Acknowledgments

These proofs followed those from the fourteenth chapter of Ireland and Rosen's *A Classical Introduction to Modern Number Theory.*