CYCLOTOMIC-INTERMEDIATE FIELDS VIA GAUSS SUMS

Let p be an odd prime, and let m divide $p-1$. Let $\zeta = e^{2\pi i/p}$ and let $\omega = e^{2\pi i/m}$. The field extension

$$\mathbb{Q}(\omega) \subset \mathbb{Q}(\omega, \zeta)$$

is Galois with cyclic Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$. The unique field between $\mathbb{Q}(\omega)$ and $\mathbb{Q}(\omega, \zeta)$ having degree m over $\mathbb{Q}(\omega)$ takes the form

$$\mathbb{Q}(\omega, \tau)$$

where τ is a Gauss sum, to be described below. Furthermore, under some conditions we can compute τ^m as an element α of $\mathbb{Q}(\omega)$, thus expressing the degree-m intermediate field extension as a radical extension,

$$\mathbb{Q}(\omega, \tau) = \mathbb{Q}\big(\omega, \sqrt[m]{\alpha}\big).$$

After laying out the theory, the writeup gives several examples, all computable by hand. Everything here is drawn very closely from a vignette by Paul Garrett,

`http://www.math.umn.edu/~garrett/m/v/kummer_eis.pdf`

1. Simplest Case: the Quadratic Gauss Sum

Let p be an odd prime. The pth cyclotomic field,

$$K = \mathbb{Q}(\zeta), \quad \zeta = e^{2\pi i/p},$$

is Galois over $\mathbb{Q}$ with cyclic Galois group $G \approx (\mathbb{Z}/p\mathbb{Z})^\times$. The associated quadratic Gauss sum is (letting $(\cdot/p)$ be the Legendre symbol)

$$\tau = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} (a/p)\zeta_p^a \in K.$$

A standard calculation, reviewed in the appendix, shows that $\tau^2 = (-1/p)p$. Thus the unique quadratic field between $\mathbb{Q}$ and K is $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{(-1/p)p})$.

2. Gauss Sums as Lagrange Resolvents

Retain the odd prime p and the field $K = \mathbb{Q}(\zeta)$ from above, and introduce the auxiliary field

$$F = \mathbb{Q}(\omega), \quad \omega = e^{2\pi i/(p-1)}$$

and the composite field

$$L = FK = \mathbb{Q}(\omega, \zeta).$$

Rather than the Legendre symbol, consider now a not-necessarily quadratic character modulo p,

$$\chi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow F^\times.$$

The associated Gauss sum is

$$\tau(\chi) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(a)\zeta^a \in L.$$

This section shows that the Gauss sum is a special case of a general symmetrizing device that has built-in equivariance and equation-solving properties. These properties are often shown directly for Gauss sums in particular, but the direct demonstrations mix together general ideas and specific details confusingly.

Working quite generally now, let L/F be a Galois field extension with cyclic Galois group G. (If the characteristic is nonzero then assume that the order of G is coprime to it.) Consider two data, an element of the larger field and a character of the Galois group into the multiplicative group of the smaller one,

$$\theta \in L, \qquad \chi : G \longrightarrow F^\times.$$

The Lagrange resolvent associated to θ and χ is the χ-weighted average over the Galois orbit of θ,

$$R = R(\theta, \chi) = \sum_{g \in G} \chi(g) g(\theta) \in L.$$

Since R is a weighted average and since the character-outputs are fixed by the Galois group, the equivariance property of the Lagrange resolvent is immediate: for any $g \in G$,

$$g(R) = g(\sum_{\tilde{g}} \chi(\tilde{g})\tilde{g}(\theta)) = \sum_{\tilde{g}} \chi(\tilde{g})(g\tilde{g})(\theta) = \chi(g^{-1}) \sum_{\tilde{g}} \chi(g\tilde{g})(g\tilde{g})(\theta) = \chi(g^{-1})R.$$

Consequently, letting $d = |\mathrm{Gal}(L/F)|$,

$$g(R^d) = (g(R))^d = (\chi(g^{-1})R)^d = R^d \quad \text{since } \chi^d = 1,$$

showing that R^d lies in the smaller field F. Indeed, letting m denote the order of χ, this argument shows that $R(\theta, \chi)^m \in F$. However, the matter of finding a method to express $R(\theta, \chi)^m$ as an element of F is context-specific.

As for the equation-solving properties of the Lagrange resolvent, begin by noting that the group of characters χ of the finite cyclic Galois group G is again finite cyclic of the same order. Assume now that F is large enough to contain the range of all such characters. Fix generators g of the Galois group and χ of the character group. The expression of each Lagrange resolvent as a linear combination of the Galois orbit of θ encodes as an equality of column vectors in L^d (with $d = |G|$ as before),

$$\begin{bmatrix} R(\theta, \chi^0) \\ R(\theta, \chi^1) \\ \vdots \\ R(\theta, \chi^{d-1}) \end{bmatrix} = V_\chi \begin{bmatrix} g^0(\theta) \\ g^1(\theta) \\ \vdots \\ g^{d-1}(\theta) \end{bmatrix},$$

where the matrix relating the vectors is the Vandermonde matrix,

$$V_\chi = \begin{bmatrix} \chi^0(g^0) & \chi^0(g^1) & \cdots & \chi^0(g^{d-1}) \\ \chi^1(g^0) & \chi^1(g^1) & \cdots & \chi^1(g^{d-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \chi^{d-1}(g^0) & \chi^{d-1}(g^1) & \cdots & \chi^{d-1}(g^{d-1}). \end{bmatrix} \in F^{d \times d}.$$

The top row and the left column of V_χ are all 1's. As a very small case of Fourier analysis, orthogonality shows (see the appendix) that the inverse of the Vandermonde matrix is essentially the transpose of another one,

$$V_{\chi^{-1}}^{\mathrm{T}} V_\chi = d\, I_d.$$

Thus we can invert the equality of column vectors in L^d to solve for θ and its conjugates in terms of the resolvents,

$$\begin{bmatrix} g^0(\theta) \\ g^1(\theta) \\ \vdots \\ g^{d-1}(\theta) \end{bmatrix} = \tfrac{1}{d} V_{\chi^{-1}}^{\mathrm{T}} \begin{bmatrix} R(\theta,\chi^0) \\ R(\theta,\chi^1) \\ \vdots \\ R(\theta,\chi^{d-1}) \end{bmatrix}.$$

Especially, equate the top entries to see that θ itself is the average of its resolvents,

$$\theta = \tfrac{1}{d} \sum_{i=0}^{d-1} R(\theta,\chi^i).$$

Since each resolvent is a dth root over F, this expresses θ in radicals.

To see that the Lagrange resolvent subsumes Gauss sums, specialize the environment back to $F = \mathbb{Q}(\omega)$ (with $\omega = e^{2\pi i/(p-1)}$) and $L = FK$ where $K = \mathbb{Q}(\zeta)$ (with $\zeta = e^{2\pi i/p}$). Then $\mathrm{Gal}(L/F) \approx (\mathbb{Z}/p\mathbb{Z})^\times$, the automorphisms being

$$g_a : \zeta \longmapsto \zeta^a, \quad a \in (\mathbb{Z}/p\mathbb{Z})^\times.$$

Also specializing the top-field element θ to ζ, the Lagrange resolvent is indeed the Gauss sum if we view any character $\chi : G \longrightarrow F^\times$ as a character of $(\mathbb{Z}/p\mathbb{Z})^\times$ as well

$$R(\zeta,\chi) = \sum_{g\in G} \chi(g) g(\zeta) = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi(a)\zeta^a = \tau(\chi).$$

3. The Kummer Character

The group of characters of $(\mathbb{Z}/p\mathbb{Z})^\times$ is generated by a particularly useful character, the Kummer character (usually called the Teichmüller character). The field $F = \mathbb{Q}(\omega)$ where $\omega = e^{2\pi i/(p-1)}$ is Galois over $\mathbb{Q}$ with cyclic Galois group isomorphic to $(\mathbb{Z}/(p-1)\mathbb{Z})^\times$, the automorphisms being

$$\sigma_b : \omega \longmapsto \omega^b, \quad b \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times.$$

Since $p = 1 \pmod{p-1}$ the rational prime p splits completely in F, which is to say that as an ideal in the integer ring of F it takes the form

$$p\mathbb{Z}[\omega] = \prod_b \sigma_b \mathfrak{q} \qquad (e = f = 1,\ g = \phi(p-1)).$$

The inertia degree f is 1, and so the residue field injection $\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}[\omega]/\mathfrak{q}$ is an isomorphism, and so it restricts to an isomorphism of multiplicative groups,

$$(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}[\omega]/\mathfrak{q})^\times, \qquad a + p\mathbb{Z} \longmapsto a + \mathfrak{q}.$$

Also, the natural ring surjection $\mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathfrak{q}$ restricts to a multiplicative group homomorphism

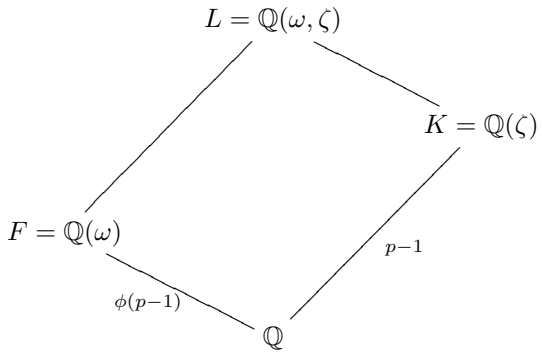
$$\mathbb{Z}[\omega]^\times \longrightarrow (\mathbb{Z}[\omega]/\mathfrak{q})^\times.$$

The group on right side is cyclic of order $p-1$, making us suspect that the homomorphism takes the cyclic subgroup $\langle\omega\rangle$ of $\mathbb{Z}[\omega]^\times$ isomorphically to it. Indeed this is the case, as shown in the appendix. The Kummer character is the first isomorphism just discussed followed by the inverse of the second, having the characterization

$$\chi_{\mathfrak{q}} : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \langle\omega\rangle, \qquad \chi_{\mathfrak{q}}(a + p\mathbb{Z}) = a \pmod{\mathfrak{q}}.$$

4. The Approximation Problem

Again let p be an odd prime, let $\zeta = e^{2\pi i/p}$, and let $\omega = e^{2\pi i/(p-1)}$. In the configuration of fields



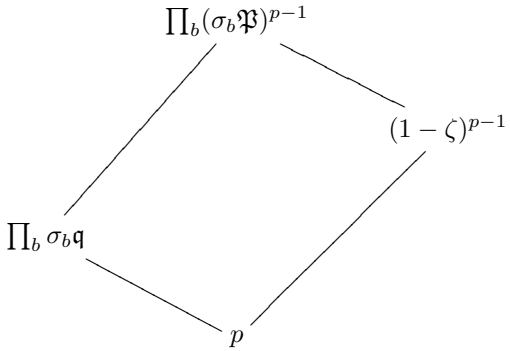
where as described above,

$$\mathrm{Gal}(L/F) \approx \mathrm{Gal}(K/\mathbb{Q}) \approx (\mathbb{Z}/p\mathbb{Z})^\times \quad \text{has elements} \quad g_a : \zeta \longmapsto \zeta^a$$

and

$$\mathrm{Gal}(L/K) \approx \mathrm{Gal}(F/\mathbb{Q}) \approx (\mathbb{Z}/(p-1)\mathbb{Z})^\times \quad \text{has elements} \quad \sigma_b : \omega \longmapsto \omega^b,$$

we have the factorizations



For any character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}[\omega]^\times$, the Gauss sum identity $\tau(\chi)\tau(\chi^{-1}) = \chi(-1)p$ shows that the only possible primes dividing $\tau(\chi)$ in L are $\mathfrak{P}$ and its Galois conjugates. Thus to factor Gauss sums $\tau(\chi)$ in L at the level of ideals we want a formula for the quantity

$$\mathrm{ord}_{\sigma_b \mathfrak{P}}(\tau(\chi_{\mathfrak{q}}^{-n})), \quad b \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times,\ 1 \le n \le p-2.$$

Furthermore, letting m denote the order $(p-1)/\gcd(n, p-1)$ of $\chi_{\mathfrak{q}}^{-n}$, we know that $\tau(\chi_{\mathfrak{q}}^{-n})^m$ lies in the field

$$F_o = \mathbb{Q}(\omega_m), \quad \omega_m = e^{2\pi i/m}.$$

The factorization of p in the integer ring of F_o is

$$p\mathbb{Z}[\omega_m] = \prod_{\beta \in (\mathbb{Z}/m\mathbb{Z})^\times} \sigma_\beta \mathfrak{p} \qquad (e = f = 1,\ g = \phi(m)),$$

where $\sigma_\beta : \omega_m \mapsto \omega_m^\beta$ is the restriction of $\sigma_b : \omega_{p-1} \mapsto \omega_{p-1}^b$ for the $\phi(p-1)/\phi(m)$ values of b in $(\mathbb{Z}/(p-1)\mathbb{Z})^\times$ such that $b = \beta \pmod m$. To factor the Gauss sum power $\tau(\chi_\mathfrak{q}^{-n})^m$ in F_o at the level of ideals, we also want a formula for the quantity

$$\mathrm{ord}_{\sigma_\beta \mathfrak{p}}(\tau(\chi_\mathfrak{q}^{-n})^m), \quad \beta \in (\mathbb{Z}/m\mathbb{Z})^\times,\ 1 \le n \le p-2.$$

We will obtain both desired formulas in the next section.

5. Kummer's Approximation

The first step toward the desired formulas is to work with the inverse of the basic Kummer character and with the particular prime $\mathfrak{P}$ that lies over the chosen prime $\mathfrak{q}$ that lies over p, not yet worrying about Galois conjugation. Compute as follows, using the notation "$\stackrel{\mathfrak{a}}{=}$" to denote congruence modulo an ideal $\mathfrak{a}$,

$$\begin{aligned}
\tau(\chi_\mathfrak{q}^{-1}) &= \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi_\mathfrak{q}^{-1}(a)(1+\zeta-1)^a \\
&\stackrel{\mathfrak{P}^2}{=} \sum_a \chi_\mathfrak{q}^{-1}(a)(1+a(\zeta-1)) \quad \text{since } \mathrm{ord}_\mathfrak{P}(\zeta-1)=1 \\
&= (\zeta-1)\sum_a \chi_\mathfrak{q}^{-1}(a)a.
\end{aligned}$$

That is, again since $\mathrm{ord}_\mathfrak{P}(\zeta-1)=1$,

$$\frac{\tau(\chi_\mathfrak{q}^{-1})}{\zeta-1} = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi_\mathfrak{q}^{-1}(a)a \pmod{\mathfrak{P}}.$$

But furthermore, by the defining property of the Kummer character,

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi_\mathfrak{q}^{-1}(a)a \stackrel{\mathfrak{q}}{=} \sum_a a^{-1}a = p-1 \stackrel{p}{=} -1.$$

Thus altogether, since $\mathfrak{P} \mid \mathfrak{q} \mid p$,

$$\frac{\tau(\chi_\mathfrak{q}^{-1})}{\zeta-1} = -1 \pmod{\mathfrak{P}}.$$

Next we work with positive powers of the inverse of the Kummer character. For $2 \le n \le p-2$ (keeping n small enough to avoid the first trivial positive power of $\chi_\mathfrak{q}^{-1}$), assume by induction that

$$\frac{\tau(\chi_\mathfrak{q}^{-(n-1)})}{(\zeta-1)^{n-1}} = \frac{-1}{(n-1)!} \pmod{\mathfrak{P}},$$

and recall the relation of Gauss sums and a Jacobi sum (see the appendix if necessary)

$$\tau(\chi_\mathfrak{q}^{-n}) = \frac{\tau(\chi_\mathfrak{q}^{-1})\tau(\chi_\mathfrak{q}^{-(n-1)})}{J(\chi_\mathfrak{q}^{-1}, \chi_\mathfrak{q}^{-(n-1)})}.$$

To analyze the Jacobi sum, compute that

$$\begin{aligned}
J(\chi_\mathfrak{q}^{-1}, \chi_\mathfrak{q}^{-(n-1)}) &= \sum_a \chi_\mathfrak{q}^{-1}(a)\chi_\mathfrak{q}^{-(n-1)}(1-a) \stackrel{\mathfrak{q}}{=} \sum_a a^{-1}(1-a)^{p-1-(n-1)} \\
&= \sum_a a^{-1} \sum_{j=0}^{p-n} \binom{p-n}{j}(-1)^j a^j = \sum_{j=0}^{p-n} \binom{p-n}{j}(-1)^j \sum_a a^{j-1}.
\end{aligned}$$

Since we may sum over all nonzero a modulo p, the inner sum vanishes unless $j = 1$. Thus the Jacobi sum satisfies

$$J(\chi_{\mathfrak{q}}^{-1}, \chi_{\mathfrak{q}}^{-(n-1)}) \stackrel{\mathfrak{q}}{=} (p-n)(-1)(p-1) \stackrel{p}{=} -n.$$

Altogether then,

$$\frac{\tau(\chi_{\mathfrak{q}}^{-n})}{(\zeta-1)^n} = \frac{\tau(\chi_{\mathfrak{q}}^{-1})}{\zeta-1} \cdot \frac{\tau(\chi_{\mathfrak{q}}^{-(n-1)})}{(\zeta-1)^{n-1}} \cdot \frac{1}{J(\chi_{\mathfrak{q}}^{-1}, \chi_{\mathfrak{q}}^{-(n-1)})} \stackrel{\mathfrak{P}}{=} (-1) \cdot \frac{-1}{(n-1)!} \cdot \frac{1}{(-n)},$$

which is to say,

$$\frac{\tau(\chi_{\mathfrak{q}}^{-n})}{(\zeta-1)^n} = \frac{-1}{n!} \pmod{\mathfrak{P}}, \quad 1 \le n \le p-2.$$

Since $\mathrm{ord}_{\mathfrak{P}}(\zeta - 1) = 1$, the resulting valuation formula is

$$\mathrm{ord}_{\mathfrak{P}}(\tau(\chi_{\mathfrak{q}}^{-n})) = n, \quad 1 \le n \le p-2.$$

Since $\mathfrak{q}$ is any prime of F over p and then $\mathfrak{P}$ is the prime of L over $\mathfrak{q}$, we may conjugate both of them freely by the Galois group with no effect on the formula,

$$\mathrm{ord}_{\sigma_b\mathfrak{P}}(\tau(\chi_{\sigma_b\mathfrak{q}}^{-n})) = n, \quad b \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times,\ 1 \le n \le p-2.$$

To find the valuation of $\chi_{\mathfrak{q}}^{-n}$ at a conjugate of $\mathfrak{P}$, recall the automorphism

$$\sigma_b : \omega \longmapsto \omega^b,$$

viewed as an element of $\mathrm{Gal}(F/\mathbb{Q})$ or of $\mathrm{Gal}(L/K)$. Since $\chi_{\mathfrak{q}}$ maps each element a of $(\mathbb{Z}/p\mathbb{Z})^\times$ to a power of ω, we have

$$\sigma_b \chi_{\mathfrak{q}}^{-n} = \chi_{\mathfrak{q}}^{-nb}.$$

Also, applying σ_b to the characterizing condition $\chi_{\mathfrak{q}}(a) = a \pmod{\mathfrak{q}}$ gives

$$\sigma_b \chi_{\mathfrak{q}}^{-n} = \chi_{\sigma_b\mathfrak{q}}^{-n}.$$

The two displayed equalities combine to give $\chi_{\mathfrak{q}}^{-nb} = \chi_{\sigma_b\mathfrak{q}}^{-n}$, and now raising both sides to the power $b^{-1} \pmod{p-1}$ gives

$$\chi_{\mathfrak{q}}^{-n} = \chi_{\sigma_b\mathfrak{q}}^{-nb^{-1}}, \quad 1 \le n \le p-2,\ b \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times.$$

Thus, for such n and b, the previous display and then the last display of the previous paragraph but with nb^{-1} in place of n give

$$\mathrm{ord}_{\sigma_b\mathfrak{P}}\big(\tau(\chi_{\mathfrak{q}}^{-n})\big) = nb^{-1} \in \{1, \cdots, p-2\}.$$

This is the first of the two desired formulas from the previous section.

Finally we move down from L to F to find valuation formulas for the relevant powers of the Gauss sums. Since $\tau(\chi_{\mathfrak{q}}^{-n})^{p-1} \in F$ and since $\mathfrak{q}\mathbb{Z}[\omega, \zeta] = \mathfrak{P}^{p-1}$, also for the same such n and b,

$$\mathrm{ord}_{\sigma_b\mathfrak{q}}\big(\tau(\chi_{\mathfrak{q}}^{-n})^{p-1}\big) = nb^{-1} \in \{1, \cdots, p-2\}.$$

Let m denote the order of $\chi_{\mathfrak{q}}^{-n}$. Specifically,

$$m = \frac{p-1}{\gcd(n, p-1)}.$$

Recall the notation $F_o = \mathbb{Q}(\omega_m)$ where $\omega_m = e^{2\pi i/m}$, and recall the factorization

$$p\mathbb{Z}[\omega_m] = \prod_{\beta \in (\mathbb{Z}/m\mathbb{Z})^\times} \sigma_\beta \mathfrak{p},$$

where $\sigma_\beta : \omega_m \mapsto \omega_m^\beta$ is the restriction of $\sigma_b : \omega \mapsto \omega^b$ for any of the $\phi(p-1)/\phi(m)$ values $b \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$ such that $b = \beta \pmod m$. The factorization of any $\sigma_\beta \mathfrak{p}$ in the integer ring of the top field L is

$$\sigma_\beta \mathfrak{p}\mathbb{Z}[\omega,\zeta] = \prod_{b=\beta \ (m)} (\sigma_b \mathfrak{P})^{p-1} \quad (e = p-1,\ f = 1,\ g = \phi(p-1)/\phi(m)).$$

Since the ramification index is $p-1$ and since $\mathrm{ord}_{\sigma_b\mathfrak{P}}(\tau(\chi_\mathfrak{q}^{-n})) \in \{1, \cdots, p-2\}$, the quantity

$$\mathrm{ord}_{\sigma_\beta\mathfrak{p}}(\tau(\chi_\mathfrak{q}^{-n})^m) = \frac{m}{p-1}\,\mathrm{ord}_{\sigma_b\mathfrak{P}}(\tau(\chi_\mathfrak{q}^{-n}))$$

lies in $\{1, \cdots, m-1\}$. Furthermore, since $\mathrm{ord}_{\sigma_b\mathfrak{P}}(\tau(\chi_\mathfrak{q}^{-n})) = nb^{-1}$ (taking b^{-1} modulo $p-1$), we have

$$\mathrm{ord}_{\sigma_\beta\mathfrak{p}}(\tau(\chi_\mathfrak{q}^{-n})^m) = \frac{m}{p-1}\,n\beta^{-1} \quad (\text{taking } \beta^{-1} \text{ modulo } m).$$

Since $m = (p-1)/\gcd(n, p-1)$, the formula is

$$\mathrm{ord}_{\sigma_\beta\mathfrak{p}}(\tau(\chi_\mathfrak{q}^{-n})^m) = n_o\,\beta^{-1} \in \{1, \cdots, m-1\} \quad \text{where } n_o = \frac{n}{\gcd(n, p-1)}.$$

This is the second of the two desired formulas from the previous section.

6. The Principal Case

Retain all the notation from above. Assume now that the divisors of p in $\mathbb{Z}[\omega_m]$ are principal, and let π be a generator of $\mathfrak{p}$. Since the extension $\mathbb{Q}(\omega_m)/\mathbb{Q}$ has trivial inertia and since the embeddings of $\mathbb{Q}(\omega_m)$ occur in complex conjugate pairs (assuming $m > 2$), $\mathrm{N}_{\mathbb{Q}(\omega_m)/\mathbb{Q}}\pi = p$. The factorization of the mth power of the Gauss sum in $\mathbb{Z}[\omega_m]$ becomes

$$\boxed{\tau(\chi_\mathfrak{q}^{-n})^m = u \cdot \prod_{\beta \in (\mathbb{Z}/m\mathbb{Z})^\times} \sigma_\beta \pi^{n_o\beta^{-1}}, \quad \text{where } u \in \mathbb{Z}[\omega_m]^\times}.$$

Here the unit u depends on n. We now show that in fact u is not only a unit but in fact a root of unity.

To combine the relation $\tau\overline{\tau} = p$ (see the appendix if necessary) with our expression for τ^m, note that since σ_{-1} acts as complex conjugation we have (substituting β for $-\beta$ to get the second equality)

$$\overline{\tau^m} = \overline{u} \cdot \prod_\beta \sigma_{-\beta}\pi^{n_o\beta^{-1}} = \overline{u} \cdot \prod_\beta \sigma_\beta \pi^{m - n_o\beta^{-1}}.$$

Thus

$$p^m = \tau^m\overline{\tau^m} = u\overline{u} \cdot \prod_\beta \sigma_\beta\pi^m = u\overline{u} \cdot \mathrm{N}_{\mathbb{Q}(\omega_m)/\mathbb{Q}}\pi^m = u\overline{u} \cdot p^m.$$

And so $u\overline{u} = 1$. It follows that for any $\beta \in (\mathbb{Z}/m\mathbb{Z})^\times$,

$$\sigma_\beta u \cdot \overline{\sigma_\beta u} = \sigma_\beta u \cdot \sigma_{-1}\sigma_\beta u = \sigma_\beta u \cdot \sigma_\beta\sigma_{-1}u = \sigma_\beta(u\overline{u}) = \sigma_\beta 1 = 1.$$

By a little theorem of Kronecker (see the appendix), u is thus a root of unity as claimed.

7. Determining the Root of Unity

Continuing to assume that the factors of p in $\mathbb{Z}[\omega_m]$ are principal, we now show that in the formula

$$\tau(\chi_{\mathfrak{q}}^{-n})^m = u \cdot \prod_{\beta \in (\mathbb{Z}/m\mathbb{Z})^\times} \sigma_\beta \pi^{n_o \beta^{-1}}$$

the root of unity $u \in \mathbb{Z}[\omega_m]^\times$ can be determined by a congruence.

Begin with the factorization of the pth cyclotomic polynomial,

$$\prod_{i=1}^{p-1}(X - \zeta^i) = \sum_{j=0}^{p-1} X^j.$$

Substitute 1 for X to get

$$\prod_{i=1}^{p-1}(1 - \zeta^i) = p.$$

Each multiplicand $1 - \zeta^i$ is $(1-\zeta)\sum_{j=0}^{i-1}\zeta^j$, and so

$$(1-\zeta)^{p-1}\prod_{i=1}^{p-1}\sum_{j=0}^{i-1}\zeta^j = p.$$

Since $(1-\zeta)^{p-1}$ and p generate the same ideal of $\mathbb{Z}[\zeta]$, their quotient is a unit,

$$\frac{p}{(1-\zeta)^{p-1}} = \prod_{i=1}^{p-1}\sum_{j=0}^{i-1}\zeta^j \in \mathbb{Z}[\zeta]^\times.$$

On the right side, work modulo the ideal generated by $1-\zeta$ by substituting 1 for ζ,

$$\frac{p}{(1-\zeta)^{p-1}} \overset{1-\zeta}{=} (p-1)! \overset{p}{=} -1.$$

Thus, since $\mathfrak{P} \mid 1-\zeta \mid p$, the previous display gives a congruence modulo $\mathfrak{P}$, and multiplying through by the denominator gives

$$(1-\zeta)^{p-1} = -p \pmod{\mathfrak{P}^p}.$$

Now we can characterize the unit u. From Kummer's estimate,

$$\frac{\tau(\chi_{\mathfrak{q}}^{-n})}{(\zeta-1)^n} = \frac{-1}{n!} \pmod{\mathfrak{P}},$$

it follows that

$$\frac{\tau(\chi_{\mathfrak{q}}^{-n})^m}{(\zeta-1)^{mn}} = \left(\frac{-1}{n!}\right)^m \pmod{\mathfrak{P}}.$$

We know that $m = (p-1)/\gcd(n, p-1)$ and we have defined $n_o = n/\gcd(n, p-1)$, so the exponent of the left side denominator is $nm = (p-1)n_o$, and now

$$\frac{\tau(\chi_{\mathfrak{q}}^{-n})^m}{(\zeta-1)^{(p-1)n_o}} = \left(\frac{-1}{n!}\right)^m \pmod{\mathfrak{P}}.$$

or, by the work of the previous paragraph,

$$\tau(\chi_{\mathfrak{q}}^{-n})^m = \left(\frac{-1}{n!}\right)^m (\zeta-1)^{(p-1)n_o} \pmod{\mathfrak{P}^p} = \left(\frac{-1}{n!}\right)^m (-p)^{n_o} \pmod{\mathfrak{P}^p},$$

and finally divide back through by $(-p)^{n_o}$ to get

$$\frac{\tau(\chi_{\mathfrak{q}}^{-n})^m}{(-p)^{n_o}} = \left(\frac{-1}{n!}\right)^m \pmod{\mathfrak{P}}.$$

Since all the quantities in the previous display are set in $F = \mathbb{Q}(\omega_m)$, and since $\mathfrak{P} \cap \mathbb{Z}[\omega_m] = \mathfrak{p} = \pi\mathbb{Z}[\omega_m]$, in fact we have

$$\frac{\tau(\chi_{\mathfrak{q}}^{-n})^m}{(-p)^{n_o}} = \left(\frac{-1}{n!}\right)^m \pmod{\pi}.$$

Substitute the formula for the mth power of the Gauss sum,

$$\boxed{\frac{u\prod_{\beta\in(\mathbb{Z}/m\mathbb{Z})^\times}\sigma_\beta\pi^{n_o\beta^{-1}}}{(-p)^{n_o}} = \left(\frac{-1}{n!}\right)^m \pmod{\pi}, \qquad \begin{cases} m = \frac{p-1}{(n,p-1)} \\ n_o = \frac{n}{(n,p-1)} \end{cases}}.$$

This congruence suffices to determine the unit u. In the particular case when $n \mid p-1$, so that $m = (p-1)/n$ and $n_o = 1$, we have, recalling that $\mathrm{N}_{\mathbb{Q}(\omega_m)/\mathbb{Q}}\pi = p$,

$$\boxed{-u\prod_{\beta\in(\mathbb{Z}/\frac{p-1}{n}\mathbb{Z})^\times}\sigma_\beta\pi^{\beta^{-1}-1} = \left(\frac{-1}{n!}\right)^{(p-1)/n} \pmod{\pi} \qquad \text{if } n \mid p-1}.$$

8. Numerical Examples

The calculations here use the boxed formula for $\tau(\chi_{\mathfrak{q}}^{-n})^m$ and the boxed formulas for the congruence that determines the unit u. Usually we have $n \mid p-1$ so that the second formula for the congruence applies.

8.1. **$\mathbf{p = 5}$.** This case can is small enough to take care of first by hand. Let $\zeta = e^{2\pi i/5}$. Then from $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$,

$$(\zeta + \zeta^{-1})^2 + (\zeta + \zeta^{-1}) - 1 = 0.$$

Also,

$$\zeta^2 - \zeta(\zeta + \zeta^{-1}) + 1 = 0,$$

and hence we can obtain ζ from $\mathbb{Q}$ by solving two successive quadratics. Specifically,

$$\zeta_5 = \frac{1}{4}\cdot\left(-1 + \sqrt{5} + i\sqrt{2\sqrt{5}(1+\sqrt{5})}\right).$$

To apply our general methods when $p = 5$, note first that the auxiliary field is $F = \mathbb{Q}(i)$, in which we have the factorization

$$5 = (2+i)(2-i).$$

Let $\pi = 2 + i$, with Galois conjugate $\sigma_3\pi = 2 - i$. The Kummer character χ_π has order 4. Choose $n = 1$, so that $m = (5-1)/\gcd(1, 5-1) = 4$. Thus we have

$$\tau(\chi_\pi^{-1})^4 = u(2+i)(2-i)^3 = u\cdot 5(2-i)^2 = u\cdot 5(3-4i),$$

where the root of unity $u \in \{\pm 1, \pm i\}$, is characterized by the condition

$$-u(2-i)^2 = 1 \pmod{2+i}.$$

On the left side, substitute $-2i$ for $2 - i$ to get $4u = 1 \pmod{2+i}$. Since $4 = -1 \pmod 5$ and $2 + i \mid 5$, we get $u = -1$ and so the Gauss sum power is

$$\tau(\chi_\pi^{-1})^4 = -5(3-4i).$$

In sum, this calculation has shown that

$$\mathbb{Q}(i,\zeta_5) = \mathbb{Q}\big(i,\, \sqrt[4]{-5(3-4i)}\big).$$

Similar calculations show that $\tau(\chi_\pi^{-3})^4 = -5(3+4i)^2$, so that, since χ_π^{-3} is the inverse of χ_π^{-1}, and since $\chi_\pi^{-1}(-1) = -1$, the general identity $\tau(\chi)\tau(\chi^{-1}) = \chi(-1)p$ gives in this case a relation between two fourth roots,

$$\tau(\chi_\pi^{-3}) = \sqrt[4]{-5(3+4i)}, \quad \tau(\chi_\pi^{-1})\tau(\chi_\pi^{-3}) = -5.$$

And since χ_π^{-2} is the quadratic character, its Gauss sum is $\tau(\chi_\pi^{-2}) = \sqrt{5}$, and finally the trivial character has Gauss sum -1. Since ζ_5 is the average of its resolvents,

$$\zeta_5 = \frac{1}{4}\left(-1+\sqrt{5}+\sqrt[4]{-5(3-4i)}+\sqrt[4]{-5(3+4i)}\right).$$

Comparing against the earlier expression for ζ_5 gives an identity among radicals, assuming that suitable roots of unity are chosen throughout,

$$\sqrt{-2\sqrt{5}(1+\sqrt{5})} = \sqrt[4]{-5(3-4i)}+\sqrt[4]{-5(3+4i)}.$$

8.2. $\mathbf{p=7}$. The Kummer character $\chi_{\mathfrak{q}}$ has order 6. Let $n=2$, so that $m=3$. Then $7 = (2-\omega_3)(3+\omega_3)$. Thus we take $\pi = 2-\omega_3$, so that $\sigma_2\pi = 2-\omega_3^2 = 3+\omega_3$. The Gauss sum power is

$$\tau(\chi_{\mathfrak{q}}^{-2})^3 = u(2-\omega_3)(3+\omega_3)^2 = u\cdot 7(3+\omega_3).$$

where the root of unity $u \in \{\pm 1, \pm\omega_3, \pm\omega_3^2\}$ satisfies the congruence

$$-u(3+\omega_3) = (-1/2!)^3 \pmod{2-\omega_3}.$$

The congruence is $u(3+\omega_3) = 1 \pmod{2-\omega_3}$, giving $5u = 1 \pmod{2-\omega_3}$ and hence $u = 3 = 1+\omega_3 = -\omega_3^2 \pmod{2-\omega_3}$. That is, $u = -\omega_3^2$, determining the Gauss sum power, and so the cubic extension of $\mathbb{Q}(\omega_3)$ in $\mathbb{Q}(\omega_3,\zeta_7)$ is

$$\mathbb{Q}\big(\omega_3,\, \sqrt[3]{-\omega_3^2 7(3+\omega_3)}\big).$$

Continuing with $p=7$, choose instead $n=1$ so that $m=6$. The auxiliary field remains unchanged since $\omega_6 = -\omega_3^2$. Still $7 = (2-\omega_3)(3+\omega_3)$, but now $3+\omega_3 = \sigma_5(2-\omega_3)$ and the calculation is

$$\tau(\chi_{\mathfrak{q}}^{-1})^6 = u(2-\omega_3)(3+\omega_3)^5 = u\cdot 7(3+\omega_3)^4$$

where

$$-u(3+\omega_3)^4 = (-1/1!)^6 \pmod{2-\omega_3}.$$

The congruence gives $-u\cdot(-2)^4 = 1 \pmod{2-\omega_3}$, so that again $5u = 1 \pmod{2-\omega_3}$ and $u = -\omega_3^2$. Consequently,

$$\mathbb{Q}(\omega_3,\zeta_7) = \mathbb{Q}\big(\omega_3,\, \sqrt[6]{-\omega_3^2\cdot 7(3+\omega_3)^4}\big).$$

8.3. $\mathbf{p = 11.}$ The full auxiliary field is $F = \mathbb{Q}(\omega_{10})$ and the Kummer character $\chi_{\mathfrak{q}}$ has order 10. Choose $n = 2$, so that $m = 5$ and the smaller auxiliary field is $F_o = \mathbb{Q}(\omega_5)$. Flukishly,

$$11 = \frac{-33}{-3} = \frac{(-2)^5 - 1}{-2 - 1} = \sum_{i=0}^{4} X^i|_{X=-2} = \prod_{j=1}^{4}(X - \omega_5^j)|_{X=-2} = \prod_{j=1}^{4}(2 + \omega_5^j).$$

So by the usual formulas,

$$\tau(\chi_{\mathfrak{q}}^{-2})^5 = u(2 + \omega_5)(2 + \omega_5^2)^3(2 + \omega_5^3)^2(2 + \omega_5^4)^4$$

where the root of unity $u \in \mathbb{Z}[\omega_5]^\times$ satisfies

$$-u(2 + \omega_5^2)^2(2 + \omega_5^3)(2 + \omega_5^4)^3 = -1/2^5 \pmod{2 + \omega_5}.$$

The congruence determining the unit gives

$$u(2 + 2^2)^2(2 - 2^3)(2 + 2^4)^3 = -1 \pmod{2 + \omega_5},$$

so that $3 \cdot 5 \cdot 7^3 u = -1 \pmod{2 + \omega_5}$, and integer modular arithmetic shows that $u = 4 = \omega_5^2 \pmod{2 + \omega_5}$. Thus the quintic extension of $\mathbb{Q}(\omega_5)$ in $\mathbb{Q}(\omega_5, \zeta_{11})$ is

$$\mathbb{Q}\big(\omega_5, \sqrt[5]{\omega_5^2 \cdot 11(2 + \omega_5^2)^2(2 + \omega_5^3)(2 + \omega_5^4)^3}\big).$$

8.4. $\mathbf{p = 13.}$ The full auxiliary field is $F = \mathbb{Q}(\omega_{12})$ and the Kummer character $\chi_{\mathfrak{q}}$ has order 12. Choose $n = 3$, so that $m = 4$ and the smaller auxiliary field is $F_o = \mathbb{Q}(i)$. Similarly to above,

$$13 = (3 + 2i)(3 - 2i),$$

so that we take $\pi = 3 + 2i$ and $\sigma_3\pi = 3 - 2i$. Now

$$(\tau(\chi_{\mathfrak{q}}^{-3}))^4 = u(3 + 2i)(3 - 2i)^3 \quad \text{where} \quad -u(3 - 2i)^2 = 1/6^4 \pmod{3 + 2i}.$$

The condition determining u is $-u(-4i)^2 = 2^4 \pmod{3+2i}$, so that $u = 1$. In sum, the quartic extension of $\mathbb{Q}(i)$ in $\mathbb{Q}(i, \zeta_{13})$ is

$$\mathbb{Q}\big(i, \sqrt[4]{13(5 - 12i)}\big).$$

8.5. $\mathbf{p = 17.}$ The full auxiliary field is $F = \mathbb{Q}(\omega_{16})$ and the Kummer character $\chi_{\mathfrak{q}}$ has order 16. Choose $n = 4$, so that $m = 4$ and the smaller auxiliary field is $F_o = \mathbb{Q}(i)$. This time,

$$17 = (4 + i)(4 - i),$$

so that we take $\pi = 4 + i$ and $\sigma_3\pi = 4 - i$. Now

$$(\tau(\chi_{\mathfrak{q}}^{-4}))^4 = u(4 + i)(4 - i)^3 \quad \text{where} \quad -u(4 - i)^2 = 1/24^4 \pmod{4 + i}.$$

The condition determining u is $4u = 13 \pmod{4 + i}$, so that $u = -1$. In sum, the quartic extension of $\mathbb{Q}(i)$ in $\mathbb{Q}(i, \zeta_{17})$ is

$$\mathbb{Q}\big(i, \sqrt[4]{-17(15 - 8i)}\big).$$

Still working with $p = 17$, if instead we take $n = 2$ then $m = 8$. Now we have

$$\begin{aligned} 17 = (4 + i)(4 - i) &= (2 - \omega_8^{-1})(2 + \omega_8^{-1}))(2 - \omega_8)(2 + \omega_8) \\ &= (2 + \omega_8)(2 + \omega_8^3)(2 + \omega_8^5)(2 + \omega_8^7). \end{aligned}$$

The usual formulas become

$$\tau(\chi_{\mathfrak{q}}^{-2})^8 = u(2 + \omega)(2 + \omega_8^3)^3(2 + \omega_8^5)^5(2 + \omega_8^7)^7$$

where

$$-u(2+\omega_8^3)^2(2+\omega_8^5)^4(2+\omega_8^7)^6 = 1/2^6 \pmod{2+\omega_8}.$$

The congruence is

$$-u(2-8)^2(2-32)^4(2-128)^6 = 1 \pmod{2+\omega_8}.$$

From here, routine calculations show that $u = -1$. Thus the unique octic extension of $\mathbb{Q}(\omega_8)$ in $\mathbb{Q}(\omega_8, \zeta_{17})$ is

$$\mathbb{Q}\big(\omega_8, \sqrt[8]{-17(2+\omega_8^3)^2(2+\omega_8^5)^4(2+\omega_8^7)^6}\big).$$

8.6. **Mersenne Primes and Fermat Primes.** Suppose that $p = 2^r - 1$ is a Mersenne prime, so that r is prime as well. Note that $r \mid p-1$, trivially if $r = 2$ and by Fermat's Little Theorem otherwise. Consider the cyclotomic factorization

$$\Phi_r(X) = \sum_{i=0}^{r-1} X^i = \prod_{j=1}^{r-1}(X - \omega_r^j),$$

and substitute 2 for X to get

$$p = \prod_{j=1}^{r-1}(2 - \omega_r^j).$$

Thus p factors into principal ideals in the auxiliary field $F = \mathbb{Q}(\omega_r)$.

Suppose that $p = 2^{2^r}+1$ is a Fermat prime. Consider the cyclotomic factorization

$$\Phi_{2^{r+1}}(X) = X^{2^r} + 1 = \prod_{\substack{j=1 \\ \text{odd}}}^{2^{r+1}-1} (X - \omega_{2^{r+1}}^j),$$

and substitute 2 for X to get

$$p = \prod_{\substack{j=1 \\ \text{odd}}}^{2^{r+1}-1} (2 - \omega_{2^{r+1}}^j).$$

Thus p factors into principal ideals in the auxiliary field $F = \mathbb{Q}(\omega_{2^{r+1}})$.

Appendix

A Basic Gauss Sum Calculation. Let $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}[\omega]^\times$ be a character, where $\omega = e^{2\pi i/(p-1)}$. The associated Gauss sum is

$$\tau(\chi) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(a)\zeta^a \in \mathbb{Q}(\omega, \zeta).$$

Let χ^{-1} be the inverse of χ. Then (taking all sums over $(\mathbb{Z}/p\mathbb{Z})^\times$)

$$\begin{aligned}
\tau(\chi)\tau(\chi^{-1}) &= \sum_{a,b} \chi(ab^{-1})\zeta^{a+b} = \sum_{a,c} \chi(c^{-1})\zeta^{a(1+c)} \quad \text{letting } b = ac \\
&= \sum_c \chi(c^{-1}) \sum_a \zeta^{a(1+c)} = \chi(-1)(p-1) - \sum_{c \neq -1} \chi(c^{-1}) \\
&= \chi(-1)p.
\end{aligned}$$

The result $\tau((\cdot/p))^2 = (-1/p)p$ is a special case. Also, since

$$\overline{\tau(\chi)} = \sum_a \chi^{-1}(a)\zeta^{-a} = \chi(-1)\sum_a \chi^{-1}(a)\zeta^a = \chi(-1)\tau(\chi^{-1}),$$

the calculation has shown that $\tau(\chi)\overline{\tau(\chi)} = p$.

Orthogonality. For any nontrivial character χ of a finite group G, there is some group element g_o such that $\chi(g_o) \neq 1$. Thus

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(g_o g) = \chi(g_o)\sum_{g\in G} \chi(g).$$

Since $\chi(g_0) \neq 1$, the sum vanishes. If instead χ is trivial then the sum is $|G|$. Similarly, for any nonidentity element g of G, there some character χ_o of G such that $\chi_o(g) \neq 1$. Thus, letting G^* denote the group of characters of G,

$$\sum_{\chi\in G^*} \chi(g) = \sum_{\chi\in G^*} (\chi_o\chi)(g) = \chi_o(g)\sum_{\chi\in G^*} \chi(g).$$

Since $\chi_o(g) \neq 1$, the sum vanishes. If instead g is the identity element then the sum is $|G^*| = |G|$.

Recall that a generator g of the order-d cyclic group and a generator χ of the dual group of characters determine a d-by-d Vandermonde matrix,

$$V_\chi = [\chi^i(g^j)]_{i,j\in\{0,\cdots,d-1\}}.$$

The (i,j)th entry of the product $V_{\chi^{-1}}^{\mathrm{T}} V_\chi$ is

$$\sum_{k=0}^{d-1} \chi^{j-i}(g^k).$$

The first part of the previous paragraph shows that the sum is 0 if $i \neq j$ and is d if $i = j$, which is to say that $V_{\chi^{-1}}^{\mathrm{T}} V_\chi = d\, I_d$. The second part of the previous paragraph shows that also $V_\chi V_{\chi^{-1}}^{\mathrm{T}} = d\, I_d$, but in any case this is a standard fact from linear algebra due to the finiteness. In infinite dimension, a one-sided inverse need not be a two-sided inverse.

The Kummer Character. Using the established notation, we show that for each $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$ there exists a unique $x \in \mathbb{Z}[\omega]^\times$ such that $x = a \pmod{\mathfrak{q}}$, and in fact x is a power of ω. Consider a polynomial and its derivative,

$$f(X) = X^{p-1} - 1, \qquad f'(X) = (p-1)X^{p-2}.$$

Let $x_1 = a + \mathfrak{q} \in \mathbb{Z}[\omega]/\mathfrak{q}$. Then $x_1 = a \pmod{\mathfrak{q}}$ and

$$f(x_1) = 0 \pmod{\mathfrak{q}}, \qquad f'(x_1) \neq 0 \pmod{\mathfrak{q}}.$$

Hensel's Lemma provides a unique lift $x \in \mathbb{Z}[\omega]_{\mathfrak{q}}$ of x_1 such that $f(x) = 0$, i.e., $x^{p-1} = 1$. In the integral domain $\mathbb{Z}[\omega]_{\mathfrak{q}}$, the $p-1$ distinct powers of ω (including $\omega^0 = 1$) provide a full contingent of roots of f. Thus x is a power of ω, lying in $\mathbb{Z}[\omega]^\times$ with no need for the localization at $\mathfrak{q}$.

Gauss Sums and Jacobi Sums. If $\chi, \widetilde{\chi} : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}[\omega]^\times$ are characters and all of χ, $\widetilde{\chi}$, and $\chi\widetilde{\chi}$ are nontrivial, then (summing here over all of $\mathbb{Z}/p\mathbb{Z}$ with the understanding that the nontrivial characters χ and $\widetilde{\chi}$ vanish at 0)

$$\begin{aligned}\tau(\chi)\tau(\widetilde{\chi}) &= \sum_{a,b} \chi(a)\widetilde{\chi}(b)\zeta^{a+b} = \sum_{a,b} \chi(a)\widetilde{\chi}(b-a)\zeta^{b} \quad \text{replacing } b \text{ by } b-a \\ &= \sum_{b\neq 0}\sum_{a} \chi(a)\widetilde{\chi}(b-a)\zeta^{b} + \sum_{a} \chi(a)\widetilde{\chi}(-a).\end{aligned}$$

The second sum is $\widetilde{\chi}(-1)\sum_a (\chi\widetilde{\chi})(a)$, which vanishes since $\chi\widetilde{\chi}$ nontrivial. In the first sum, replace a by ab to get

$$\begin{aligned}\tau(\chi)\tau(\widetilde{\chi}) &= \sum_{b\neq 0}\sum_{a} \chi(ab)\widetilde{\chi}((1-a)b)\zeta^{b} = \sum_{b\neq 0} (\chi\widetilde{\chi})(b)\zeta^{b} \sum_{a} \chi(a)\widetilde{\chi}(1-a) \\ &= \tau(\chi\widetilde{\chi})J(\chi,\widetilde{\chi}) \quad \text{where } J(\chi,\widetilde{\chi}) = \sum_{a} \chi(a)\widetilde{\chi}(1-a) \text{ is the Jacobi sum.}\end{aligned}$$

In the Jacobi sum we may exclude $a = 0$ and/or $a = 1$ as desired.

Kronecker's Root of Unity Theorem. Let u be an algebraic integer such that every embedding σ of its number field in $\mathbb{C}$ (including real embeddings if there are any) takes u to a number σu of absolute value 1. Then u is a root of unity.

The proof is that since all positive powers u^k lie in $\mathbb{Q}(u)$, the degrees of their minimal polynomials are bounded by the degree of the minimal polynomial of u, and the rational integer coefficients of their minimal polynomials are uniformly bounded because of the degree-bound and the fact that all embedded images $\sigma(u^k)$ have absolute value 1. Thus two powers u^k and u^ℓ have the same minimal polynomial.