(*July 28, 2010*)

Kummer, Eisenstein, computing Gauss sums as Lagrange resolvents

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

1. Solving cyclic equations by Lagrange resolvents
2. Kummer's approximation of Gauss sums
3. Galois equivariance and prime factorizations
4. Ambiguity by units
5. Evaluating Gauss sums
6. Numerical examples
7. Appendix: Kronecker's theorem, Kummer (-Teichmüller) character, Gauss sums

We re-purpose results of Kummer and Eisenstein to compute Lagrange resolvents for roots of unity. In principle, everything here has been known for 160 years, but perhaps is not as visible as it deserves to be.

Roots of unity are abelian over $\mathbb{Q}$, so are expressible in radicals. Expressions in radicals are obtained via Lagrange resolvents, in this case Gauss sums.

Evaluation of squares of quadratic Gauss sums is well known, due to Gauss, and shows that the quadratic subfield of the field $\mathbb{Q}(\zeta)$ obtained by adjoining a p^{th} root of unity ζ to $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{p\cdot(-1/p)_2})$, for p odd.

In fact, [Eisenstein 1850] evaluated cubes and fourth powers of Gauss sums attached to cubic and quartic characters to prove the corresponding reciprocity laws. One essential point is the p-adic approximation of Gauss sums by [Kummer 1847], generalized in [Stickelberger 1890]. Since the rings of algebraic integers generated by third or fourth roots of unity have class number one and finitely-many units, cubic (and sextic) and quartic subfields of cyclotomic fields are readily expressible in radicals, via Lagrange resolvents.

More generally, when a prime p splits into *principal* ideals in $\mathbb{Z}[\omega]$ with ω an m^{th} root of unity with $m|(p-1)$, Kummer and Eisenstein systematically produce Lagrange resolvents for the unique degree m subfield of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$, with ζ a p^{th} root of unity. [1]

The expressions for resolvents for degree-m subfields of $\mathbb{Q}(\zeta)$ inevitably involve auxiliary m^{th} roots of unity ρ, so are literal expressions in the larger field $\mathbb{Q}(\zeta,\rho)$. However, the resolvents do lie in the degree-m subfield of $\mathbb{Q}(\zeta)$. This is a more general instance of the minor scandal from the Renaissance, that the radical expression for roots of cubics involved complex numbers (cube roots of unity), even when the cubic had three real roots. Further, since the auxiliary roots of unity are of lower degrees, an induction proves that everything in sight is expressible in radicals.

Our expression for the m^{th} power of a Gauss sum of an order m character contains a root of unity which we determine numerically in examples. A more serious ambiguity is the argument of Gauss sums themselves: the quadratic case was a difficult result of Gauss, and the cubic case was only relatively recently treated by [Heath-Brown Patterson 1979].

The accessible example of fifth roots of unity illustrates the result and pertinent ambiguities. Namely, for a fifth root of unity ζ, there are two ways to express ζ. First, rearranging the defining equation to

$$\left(\zeta+\frac{1}{\zeta}\right)^2+\left(\zeta+\frac{1}{\zeta}\right)-1 \;=\; 0$$

[1] Ramification-theoretic arguments suggest a qualitative conclusion of this sort, but fall short. Namely, first, by elementary Kummer theory, a cyclic extension of degree m dividing $p-1$ over a groundfield with m^{th} roots of unity is obtained by adjoining m^{th} roots of an element ξ in the groundfield. Considering ramification, since the only primes ramifying in $\mathbb{Q}(\omega,\zeta_p)$ over $\mathbb{Q}(\omega)$ are primes lying over p, the prime factorization of ξ should not include any primes other than those lying over p. However, there is no indication about avoiding ramification at primes dividing m. Since p splits completely in an extension of $\mathbb{Q}$ by m^{th} roots of unity, there are many inequivalent choices of products of the primes lying over p. Even when the prime factors are determined, there is ambiguity by units.

and solving two successive quadratic equations, fixing a choice of $\sqrt{5}$ and suppressing the sign,

$$\zeta \;=\; \frac{1}{4}\cdot\Big(-1+\sqrt{5}\pm\sqrt{-2\sqrt{5}(1+\sqrt{5})}\Big)$$

On the other hand, 5 splits as $5=(2+i)(2-i)$ in $\mathbb{Z}[i]$, and as an example of computing Lagrange resolvents following Kummer and Eisenstein,

$$\zeta \;=\; \frac{1}{4}\cdot\Big(-1+\sqrt{5}+\sqrt[4]{(2+i)(2-i)^3}+\sqrt[4]{(2+i)^3(2-i)}\Big) \qquad \text{(ambiguous fourth roots of unity)}$$

It is apparently true, though not obvious, that, for suitable choices of roots of unity throughout,

$$\sqrt[4]{(2+i)(2-i)^3}+\sqrt[4]{(2+i)^3(2-i)} \;=\; \sqrt{-2\sqrt{5}(1+\sqrt{5})} \qquad \text{(with suitable roots of unity)}$$

Of course, cyclotomic fields mostly require more than successive solutions of quadratics. Even in exceptional cases, Fermat primes such as $p=17$, determination of the quadratic subfield $\mathbb{Q}(\sqrt{17})$ via the quadratic Gauss sum is easier and more coherent than the naive, direct computation.

For $p=7$, the cubic subfield is expressible by radicals because *every* cubic is solvable by radicals, via Lagrange resolvents. Already in this case the resolvent is more intelligibly and memorably expressed via the cube of the cubic Gauss sum rather than as a special case of general computations. Let ρ be a cube root of unity and ζ_7 a seventh. Observe that $7=(3+\rho)(3+\overline{\rho})=(3+\rho)(2-\rho)$. We will obtain

$$\big(\text{ cubic subfield of } \mathbb{Q}(\rho,\zeta_7) \text{ over } \mathbb{Q}(\rho)\ \big) \;=\; \mathbb{Q}(\rho)\big(\sqrt[3]{-\rho^2\cdot(3+\rho)\cdot(2-\rho)^2}\big)$$

Similarly,

$$\mathbb{Q}(\rho,\zeta_7) \;=\; \mathbb{Q}(\rho)\big(\sqrt[6]{\rho^2\cdot(3+\rho)\cdot(2-\rho)^5}\big)$$

For $p=11$, the quintic subfield's expressibility in radicals is necessarily special, since general quintics are not solvable. Brute-force hand computation of Lagrange resolvents is possible, but unilluminating. Luckily, in the ring $\mathbb{Z}[\omega]$ obtained by adjoining a fifth root of unity $\omega=\omega_5$, 11 splits nicely

$$11 \;=\; (2+\omega)(2+\omega^2)(2+\omega^3)(2+\omega^4)$$

Let ζ_{11} be an eleventh root of unity. We will see that

$$\big(\text{ quintic subfield of } \mathbb{Q}(\omega_5,\zeta_{11}) \text{ over } \mathbb{Q}(\omega_5)\ \big) \;=\; \mathbb{Q}(\omega)\big(\sqrt[5]{-\omega^2\cdot(2+\omega)(2+\omega^2)^3(2+\omega^3)^2(2+\omega^4)^4}\big)$$

Surprisingly large examples are accessible from this viewpoint. For example, letting ζ_{17} be a $17th$ root of unity, and $\omega=\omega_{16}$ a primitive sixteenth, the octic subfield of $\mathbb{Q}(\omega_{16},\zeta_{17})$ is generated over $\mathbb{Q}(\omega_{16})$ by

$$\sqrt[8]{(\omega+2)(\omega^3+2)^3(\omega^5+2)^5(\omega^7+2)^7}$$

The Kummer-Eisenstein approach determines the prime factorization of the m^{th} power of order-m Gauss sums for $m|(p-1)$ and p prime. This was further elaborated in Stickelberger's work decades later. Further, as in Eisenstein's reciprocity laws, when the primes lying over p in $\mathbb{Z}[\omega_m]$ are *principal*, with ω_m a primitive m^{th} root of unity, the ambiguous unit must be a *root of unity*. This renders feasible, by hand computation, numerical examples of cyclotomic Lagrange resolvents otherwise out of reach.

Surely none of what is done here would have surprised Kummer, Eisenstein, nor the mature Gauss, circa 1850. It might not have surprised Lagrange in 1770, nor Vandermonde. [2] Indeed, our principal

[2] [O'Connor-Robertson 2001] notes that Kronecker claimed in 1888 that modern algebra began with the first (1771) paper of Vandermonde, and that Cauchy states that Vandermonde had priority over Lagrange for the remarkable idea of permutations of roots.

advantage is the post-Dedekind, post-Noether conception of abstract algebra, which removes conceptual difficulties from the Kummer-Eisenstein computations, but otherwise adds little.

---

1. *Solving cyclic equations by Lagrange resolvents*

We recall [3] how to solve cyclic equations in radicals by Lagrange resolvents.

Let k be a field and K a *cyclic* extension with Galois group G of order n prime to the characteristic. Assume that k contains n^{th} roots of unity. Given $\theta \in K$ and a character $\alpha : G \to k^\times$, the *Lagrange resolvent* is an average in K:

$$R \;=\; R(\alpha,\theta) \;=\; \sum_{g\in G} \alpha(g)\, g(\theta)$$

Thus, by design, for $h \in G$

$$h(R) \;=\; \alpha(h^{-1}) \cdot R$$

Since G is cyclic of order n, necessarily $\alpha^n = 1$, and for $h \in G$,

$$h(R^n) \;=\; \alpha(h^{-1})^n \cdot R^n \;=\; R^n$$

Thus, $R(\alpha,\theta)^n \in k$, since it is Galois-invariant. Indeed, for α of order m, $R(\alpha,\theta)^m \in k$, for the same reason.

Since G is cyclic, the group of characters α is cyclic. Fix a generator χ, and fix a generator g for G. The element θ is expressible in terms of the collection of resolvents $R(\chi^\ell,\theta)$, using the invertibility of the Vandermonde matrix

$$V_\chi \;=\; \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \chi(g^0) & \chi(g^1) & \chi(g^2) & \dots & \chi(g^{n-1}) \\ \chi^2(g^0) & \chi^2(g^1) & \chi^2(g^2) & \dots & \chi^2(g^{n-1}) \\ \vdots & & & & \vdots \\ \chi^{n-1}(g^0) & \chi^{n-1}(g^1) & \chi^{n-1}(g^2) & \dots & \chi^{n-1}(g^{n-1}) \end{pmatrix}$$

Specifically, the Vandermonde matrix V_χ is explicitly invertible:

$$V_\chi \cdot V_{\chi^{-1}}^\top \;=\; n \cdot 1_n$$

Thus, from

$$\begin{pmatrix} R(\chi^0,\theta) \\ R(\chi^1,\theta) \\ R(\chi^2,\theta) \\ \vdots \\ R(\chi^{n-1},\theta) \end{pmatrix} \;=\; V_\chi \cdot \begin{pmatrix} g^0(\theta) \\ g^1(\theta) \\ g^2(\theta) \\ \vdots \\ g^{n-1}(\theta) \end{pmatrix}$$

we have

$$\begin{pmatrix} g^0(\theta) \\ g^1(\theta) \\ g^2(\theta) \\ \vdots \\ g^{n-1}(\theta) \end{pmatrix} \;=\; \frac{1}{n} \cdot V_{\chi^{-1}}^\top \cdot \begin{pmatrix} R(\chi^0,\theta) \\ R(\chi^1,\theta) \\ R(\chi^2,\theta) \\ \vdots \\ R(\chi^{n-1},\theta) \end{pmatrix}$$

[3] Many contemporary treatments of Galois theory neglect Lagrange resolvents, emphasizing other features. The introduction of resolvents in [Lagrange 1770] considerably predates Ruffini, Abel, and Galois.

Then

$$\theta \;=\; g^0(\theta) \;=\; \frac{1}{n}\cdot\big(R(\chi^0,\theta)+R(\chi^1,\theta)+\ldots+R(\chi^{n-1},\theta)\big)$$

Expressing each $R(\chi^\ell,\theta)^n$ in terms of the coefficients of the irreducible for θ over k yields the expression for θ in radicals.

In fact, while θ itself may have no special significance, construction of resolvents *produces* special elements whose roots generate field extensions, including intermediate extensions.

For cyclotomic extensions, *Lagrange resolvents are Gauss sums*: let $\theta = \zeta$ be a p^{th} root of unity, ω a $(p-1)^{th}$ root of unity, $k=\mathbb{Q}(\omega)$, $K=\mathbb{Q}(\zeta,\omega)$, $\psi(a)=\zeta^a$, identify $\mathrm{Gal}(K/k)$ with $(\mathbb{Z}/p)^\times$ by $\sigma_a(\zeta)=\zeta^a$. Then

$$R(\alpha,\zeta) \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \alpha(a)\,\sigma_a(\zeta) \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \alpha(a)\,\psi(a) \;=\; (\text{Gauss sum attached to } \alpha,\psi)$$

Thus, for $m|(p-1)$, for a multiplicative character α of order m, the Gauss sum $\gamma(\alpha)$ is a Lagrange resolvent for a generator for the unique degree m subfield of $\mathbb{Q}(\zeta,\omega)$ over $\mathbb{Q}(\omega)$. Of course, the values of α often generate a smaller field $\mathbb{Q}(\alpha)$ than $\mathbb{Q}(\omega)$, and then

$$0 \;\neq\; \gamma(\alpha)^m \;\in\; \mathbb{Q}(\alpha)$$

When such an m^{th} power can be evaluated in useful terms, generators for subfields are expressible in terms of radicals.

---

2. *Kummer's approximation of Gauss sums*

For a multiplicative character α on $(\mathbb{Z}/p)^\times$ and an additive character ψ on $\mathbb{Z}/p$, the corresponding Gauss sum is

$$\gamma(\alpha) \;=\; \sum_a \alpha(a)\,\psi(a)$$

We recall [Kummer 1847]'s (see [Cohen 2007] p. 155) and [Stickelberger 1890]'s by-now standard $\mathfrak{P}$-adic [4] approximation. A key point is expression of the given character as a power of the *Kummer (-Teichmüller)* [5] *character*. This approximation determines the prime factorization of $\gamma(\alpha)$, as recalled in the following section.

Let p be a prime, $\zeta = \zeta_p$ a p^{th} root of unity in an extension of $\mathbb{Q}$. The prime lying over p in $\mathbb{Z}[\zeta]$ is generated by $\zeta-1$. Specify an additive character ψ on $\mathbb{Z}/p$ by

$$\psi(a) \;=\; \zeta^a \qquad\qquad (\text{for } a\in\mathbb{Z}/p)$$

The choice of ζ and the corresponding character ψ will be fixed throughout, so will be implicit. Let $\omega=\omega_{p-1}$ be a primitive $(p-1)^{th}$ root of unity. Let $\mathfrak{q}$ be one of the primes lying over p in $\mathbb{Z}[\omega]$, noting that p splits completely in $\mathbb{Z}[\omega]$. Let $\mathfrak{P}$ be the prime lying over $\mathfrak{q}$ in $\mathbb{Z}[\zeta,\omega]$: at all primes over p, the extension $\mathbb{Z}[\zeta,\omega]/\mathbb{Z}[\omega]$ is totally ramified. Since p splits completely in $\mathbb{Z}[\omega]$, the inclusion of residue class fields

$$\mathbb{Z}/p \;\longrightarrow\; \mathbb{Z}[\omega]/\mathfrak{q}$$

[4] Of course, the notion of p-adic approximation was not explicit in Kummer's time, nor Stickelberger's but this is the most reasonable description of the result.

[5] The character nowadays named after Teichmüller was used by Kummer 80 years earlier.

is an *isomorphism*. This isomorphism identifies the images of the $(p-1)^{th}$ roots of unity in the quotient $\mathbb{Z}[\omega]/\mathfrak{q}$ with the cyclic group $(\mathbb{Z}/p)^\times$. For a choice of $\mathfrak{q}$ lying over p, the corresponding *Kummer (-Teichmüller) character*[6]

$$\chi \;=\; \chi_{\mathfrak{q}} \;:\; (\mathbb{Z}/p)^\times \;\longrightarrow\; \mathbb{Z}[\omega]^\times$$

is defined by

$$\chi(a) \;=\; \chi_{\mathfrak{q}}(a) \;=\; a \bmod \mathfrak{q} \qquad\qquad (\text{for } a \in (\mathbb{Z}/p)^\times, \text{ fixed } \mathfrak{q} \text{ in } \mathbb{Z}[\omega] \text{ over } p)$$

Since $(\mathbb{Z}/p)^\times$ is cyclic, every character is a power of the Kummer (-Teichmüller) character. In any case, all Gauss sums $\gamma(\chi^{-n})$ lie in $\mathbb{Z}[\omega,\zeta]$. We prove Kummer's estimate

$$\frac{\gamma(\chi_{\mathfrak{q}}^{-n})}{(\zeta-1)^n} \;=\; \frac{-1}{n!} \bmod \mathfrak{P} \qquad\qquad (\text{with } \mathfrak{P} \text{ over } \mathfrak{q})$$

The first and clearest example of Kummer's approximation is that of the Gauss sum attached to the inverse of the Kummer (-Teichmüller) character χ itself,

$$\gamma(\chi^{-1}) \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \psi(a)\,\chi^{-1}(a)$$

First, recalling that $(\zeta-1)\mathbb{Z}[\zeta]$ lies under $\mathfrak{P}$,

$$\sum_{a\in(\mathbb{Z}/p)^\times} \chi^{-1}(a)\,\psi(a) \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \chi^{-1}(a)\,(1+\zeta-1)^a$$

$$=\; \sum_{a\in(\mathbb{Z}/p)^\times} \chi^{-1}(a)\,(1+a(\zeta-1)) \bmod \mathfrak{P}^2 \;=\; (\zeta-1) \sum_{a\in(\mathbb{Z}/p)^\times} a\,\chi^{-1}(a)$$

since $\sum_a \chi^{-1}(a) = 0$. Thus,

$$\frac{\gamma(\chi^{-1})}{\zeta-1} \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} a\,\chi^{-1}(a) \bmod \mathfrak{P} \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} a\,a^{-1} \bmod \mathfrak{P} \;=\; p-1 \bmod \mathfrak{P} \;=\; -1 \bmod \mathfrak{P}$$

That is, we conclude that

$$\frac{\gamma(\chi^{-1})}{\zeta-1} \;=\; -1 \bmod \mathfrak{P}$$

The general case is obtained from this by induction, as follows. Start from the elementary relation among Gauss sums and Jacobi sums:

$$\gamma(\alpha)\,\gamma(\beta) \;=\; \gamma(\alpha\beta)\cdot \sum_{b\neq 0,1} \alpha(b)\,\beta(1-b) \qquad\qquad (\text{for } \alpha\beta \neq 1)$$

Expressing α,β in terms of the Kummer (-Teichmüller) character, $\alpha = \chi^{-m}$ and $\beta = \chi^{-n}$, the Jacobi sum $\sum \alpha(b)\,\beta(1-b)$ can be evaluated modulo $\mathfrak{P}$, producing a result resembling a beta function, as follows. With equalities modulo $\mathfrak{q}$,

$$\sum_{b\neq 0,1} \chi^{-m}(b)\,\chi^{-n}(1-b) \;=\; \sum_{b\neq 0,1} b^{-m}\,(1-b)^{-n} \;=\; \sum_{b\neq 0} b^{-m}\,(1-b)^{-n} \qquad\qquad (\text{all equalities mod } \mathfrak{q})$$

[6] See the appendix for proof of *existence* of this character. Some sources normalize $\chi(a) = a^{-1} \bmod \mathfrak{q}$. The choice of a or a^{-1} is inessential, but obviously affects details.

Note that the sum over b now *does* include 1. Continuing, modulo $\mathfrak{q}$, this is

$$= \sum_{b\neq 0} b^{-m}\,(1-b)^{(p-1)-n} \;=\; \sum_{j=0}^{p-1-n} \sum_{b\neq 0} b^{-m} \binom{p-1-n}{j} (-1)^j\, b^j \qquad \text{(all equalities mod } \mathfrak{q})$$

$$= \sum_{j=0}^{p-1-n} \binom{p-1-n}{j} (-1)^j \sum_{b\neq 0} b^{j-m} \qquad (\text{mod } \mathfrak{q})$$

The inner sum over b is 0 unless $j-m=0$, in which case it is $p-1$, since $b\to b^{j-m}$ is a character mod p. Thus, modulo $\mathfrak{q}$,

$$\sum_b \chi^{-m}(b)\,\chi^{-n}(1-b) \;=\; \binom{p-1-n}{m}(-1)^m(p-1) \;=\; \binom{p-1-n}{m}(-1)^{m+1} \bmod \mathfrak{q}$$

Thus, for $m=1$ and replacing n by $n-1$, the Jacobi sum can be approximated $\mathfrak{q}$-adically by

$$\sum_b \chi^{-1}(b)\,\chi^{-(n-1)}(1-b) \;=\; \binom{p-1-(n-1)}{1} \bmod \mathfrak{q} \;=\; p-1-(n-1) \;=\; -n \bmod \mathfrak{q}$$

Going back to the elementary relation relating Gauss sums and Jacobi sums, we have

$$\gamma(\chi^{-1})\cdot\gamma(\chi^{-(n-1)}) \;=\; -n\cdot\gamma(\chi^{-n}) \bmod \mathfrak{P}$$

or

$$\gamma(\chi^{-n}) \;=\; \frac{\gamma(\chi^{-1})\cdot\gamma(\chi^{-(n-1)})}{-n} \bmod \mathfrak{P}$$

Thus, induction gives Kummer's result

$$\frac{\gamma(\chi^{-n})}{(\zeta-1)^n} \;=\; \frac{\gamma(\chi^{-1})}{\zeta-1}\cdot\frac{\gamma(\chi^{-(n-1)})}{(\zeta-1)^{n-1}}\cdot\frac{1}{\sum_b \chi^{-1}(b)\,\chi^{-(n-1)}(1-b)} \;=\; (-1)\cdot\frac{-1}{(n-1)!}\cdot\frac{1}{-n} \;=\; \frac{-1}{n!} \bmod \mathfrak{P}$$

---

3. *Galois equivariance and prime factorizations*

Galois equivariance of Kummer's estimate is straightforward, and determines the prime ideal factorization of Gauss sums.

Continue to take ω a $(p-1)^{th}$ root of unity, ζ a p^{th} root of unity, $\mathfrak{q}$ a prime lying over p in $\mathbb{Z}[\omega]$, $\mathfrak{P}$ the unique prime over $\mathfrak{q}$ in $\mathbb{Z}[\omega,\zeta]$, and $\chi=\chi_{\mathfrak{q}}=\chi_{\mathfrak{P}}$ the corresponding Kummer (-Teichmüller) character. Rewrite Kummer's result as

$$\frac{\gamma(\chi_{\mathfrak{P}}^{-n})}{(\zeta-1)^n} \;+\; \frac{1}{n!} \;\in\; \mathfrak{P}$$

A Galois automorphism of $\mathbb{Q}(\omega,\zeta)$ over $\mathbb{Q}(\zeta)$ does not change ζ and does not change the character $\psi(a)=\zeta^a$, so the effect of σ on a Gauss sum $\gamma(\alpha)$ is only via α, namely,

$$\sigma\big(\gamma(\alpha)\big) \;=\; \sigma\big(\sum_a \alpha(a)\,\psi(a)\big) \;=\; \sum_a \sigma\big(\alpha(a)\big)\,\psi(a)\big) \;=\; \gamma(\sigma\alpha)$$

This gives the obvious Galois equivariance

$$\frac{\gamma(\sigma\chi_{\mathfrak{P}}^{-n})}{(\zeta-1)^n} \;+\; \frac{1}{n!} \;\in\; \sigma\mathfrak{P}$$

The definition of the Kummer (-Teichmüller) characters attached to primes $\mathfrak{q}$ or $\mathfrak{P}$ over p also has an obvious Galois equivariance: applying σ to the relation $\chi_{\mathfrak{P}}(a) - a \in \mathfrak{P}$ gives

$$\sigma\chi_{\mathfrak{P}}(a) - a \ \in \ \sigma\mathfrak{P} \qquad\qquad (\text{for } a \in (\mathbb{Z}/p)^\times)$$

For $b \in (\mathbb{Z}/(p-1))^\times$, let σ_b be the automorphism

$$\sigma_b\omega \ = \ \omega^b \qquad \sigma_b\zeta \ = \ \zeta \qquad\qquad (\text{for } b \in (\mathbb{Z}/(p-1))^\times)$$

Then

$$\chi_{\mathfrak{P}}^b(a) - a \ = \ \sigma_b\chi_{\mathfrak{P}}(a) - a \ \in \ \sigma_b\mathfrak{P} \qquad\qquad (\text{for } a \in (\mathbb{Z}/p)^\times,\ b \in (\mathbb{Z}/(p-1))^\times)$$

That is,

$$\chi_{\sigma_b\mathfrak{P}} \ = \ \chi_{\mathfrak{P}}^b \qquad\qquad (\text{for } b \in (\mathbb{Z}/(p-1))^\times)$$

Since $\zeta - 1$ splits completely in $\mathbb{Z}[\omega, \zeta]$ over $\mathbb{Z}[\zeta]$,

$$\mathrm{ord}_{\sigma_b\mathfrak{P}}(\zeta - 1) \ = \ 1 \qquad\qquad (\text{for all } b \text{ prime to } p-1)$$

Thus, from Kummer's estimate,

$$\mathrm{ord}_{\mathfrak{P}}\,\gamma(\chi_{\sigma_b\mathfrak{P}}^{-1}) \ = \ \mathrm{ord}_{\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-b}) \ = \ b \qquad\qquad (\text{for } b \in (\mathbb{Z}/(p-1))^\times)$$

Likewise,

$$\mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-1}) \ = \ b^{-1} \mod p-1$$

For arbitrary n, the same argument gives

$$\mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n}) \ = \ b^{-1}n \mod p-1 \qquad\qquad (\text{with } b^{-1}n \text{ in the range } 0, 1, 2, \ldots, p-2)$$

The elementary property $\gamma(\chi^{-n}) \cdot \gamma(\chi^n) = \chi^n(-1) \cdot p$ shows that no primes other than those lying above p divide these Gauss sums, so we have the prime ideal factorization in $\mathbb{Z}[\omega_{p-1}, \zeta_p]$.

Its Galois equivariance shows that the $(p-1)^{th}$ power of $\gamma(\chi_{\mathfrak{P}}^{-1})$ lies in $\mathbb{Z}[\omega]$. The prime $\mathfrak{P}$ is totally ramified over the prime $\mathfrak{q}$ under it in $\mathbb{Z}[\omega]$, of degree $p-1$, so

$$\mathrm{ord}_{\sigma_b\mathfrak{q}}\,\gamma(\chi_{\mathfrak{P}}^{-n})^{p-1} \ = \ \frac{1}{p-1} \cdot \mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n})^{p-1}$$

$$= \ \mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n}) \ = \ b^{-1}n \mod p-1 \qquad\qquad (b^{-1}n \text{ in the range } 0, 1, 2, \ldots, p-2)$$

Generally, let the order of the character χ^{-n} be

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

The Gauss sum $\gamma(\chi^{-n})$ lies in the subfield $\mathbb{Q}(\omega_m, \zeta_p)$ of $\mathbb{Q}(\omega_{p-1}, \zeta_p)$, and its m^{th} power $\gamma(\chi^{-n})^m$ lies in $\mathbb{Z}[\omega_m]$. The prime ideal factorization of $\gamma(\chi^{-n})^m$ in $\mathbb{Z}[\omega_m]$ is completely determined, as follows. Let $\mathfrak{p}$ be the prime under $\mathfrak{P}$ in $\mathbb{Z}[\omega_m]$. The ramification degree of $\mathfrak{P}$ over $\mathfrak{p}$ is $p-1$. Then

$$\mathrm{ord}_{\sigma_b\mathfrak{p}}\,\gamma(\chi_{\mathfrak{P}}^{-n})^m \ = \ \frac{1}{p-1} \cdot \mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n})^m \ = \ \frac{1}{p-1} \cdot m \cdot \mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n})$$

$$= \ \frac{1}{p-1} \cdot m \cdot \big(b^{-1}n \bmod p-1\big) \ = \ \frac{1}{p-1} \cdot m \cdot \gcd(n, p-1) \cdot \Big(\frac{b^{-1}n}{\gcd(n, p-1)} \bmod m\Big)$$

$$= \ \frac{b^{-1}n}{\gcd(n, p-1)} \bmod m \qquad\qquad (\text{for } b \in (\mathbb{Z}/(p-1))^\times,\ b^{-1}n/\gcd(n, p-1) \text{ in the range } 0, 1, \ldots, m-1\ )$$

4. *Ambiguity by units*

To complete the evaluation of m^{th} powers of Gauss sums of order m characters, we must assume that the ideals in $\mathbb{Z}[\omega_m]$ over p are *principal*. Under this hypothesis, the Gauss sum can be determined up to a *root of unity*, rather than up to a more general unit.

Let $\omega = \omega_m$ and $\zeta = \zeta_p$. Let $\chi_{\mathfrak{P}}^{-n}$ be of order $m = (p-1)/\gcd(n, p-1)$, and put

$$\ell \;=\; \frac{n}{\gcd(n, p-1)}$$

Let q_o generate $\mathfrak{p}$, the ideal lying under $\mathfrak{P}$ in $\mathbb{Z}[\omega]$, where $\mathfrak{P}$ defines the Kummer (-Teichmüller) character. Identify $(\mathbb{Z}/m)^\times$ with the Galois group of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, which we know acts transitively on primes over p in $\mathbb{Z}[\omega]$. Let τ_b be the Galois automorphism

$$\tau_b(\omega) \;=\; \omega^b \qquad\qquad (\text{for } b \in (\mathbb{Z}/m)^\times)$$

The prime ideal factorization of $\gamma(\chi^{-n})^m$ gives

$$\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \eta \cdot \prod_{b \in (\mathbb{Z}/m)^\times} (\tau_b q_o)^{b^{-1}\ell \bmod m} \qquad\qquad (\text{exponents in the range } 0, 1, 2, \ldots, m-1)$$

with a unit η in $\mathbb{Z}[\omega]$. We will show that η is a *root of unity*, by applying Kronecker's theorem (see appendix) that an algebraic integer with absolute value 1 at every archimedean place is a root of unity.

Observe that τ_{-1} acts as *complex conjugation* in the sense that, for every complex imbedding of $\mathbb{Q}(\omega)$, the automorphism τ_{-1} is the restriction of complex conjugation to the image. Since p splits completely in $\mathbb{Z}[\omega]$ over $\mathbb{Z}$,

$$\prod_b \tau_b q_o \;=\; \pm p$$

Since $\mathbb{Q}(\omega)$ has only complex archimedean places, none real, the factors $\tau_b q_o$ occur in complex conjugate pairs. This eliminates the ambiguity of sign:

$$\prod_b \tau_b q_o \;=\; p$$

Compute

$$\tau_{-1}\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \tau_{-1}\eta \cdot \prod_b \tau_{-1}\big((\tau_b q_o)^{b^{-1}\ell \bmod m}\big) \;=\; \prod_b (\tau_{-b} q_o)^{b^{-1}\ell \bmod m}$$

$$= \prod_b (\tau_b q_o)^{m - b^{-1}\ell \bmod m} \qquad\qquad (\text{exponents in the range } 0, 1, \ldots, m-1)$$

by replacing b^{-1} by $m - b^{-1}$ in the product. Thus,

$$\prod_b (\tau_b q_o)^{b^{-1}\ell \bmod m} \cdot \prod_b \tau_{-1}\big((\tau_b q_o)^{b^{-1}\ell \bmod m}\big) \;=\; \prod_b (\tau_b q_o)^m \;=\; p^m$$

On the other hand, it is elementary that the product of a Gauss sum and its complex conjugate is p, so also

$$\gamma(\chi_{\mathfrak{P}}^{-n})^m \cdot \tau_{-1}\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; p^m$$

Thus, $\eta \cdot \tau_{-1}\eta = 1$. Thus, for *any* complex imbedding $j : \mathbb{Q}(\omega) \to \mathbb{C}$, we have $|j(\eta)| = 1$. Invoking Kronecker's theorem, η is a root of unity. ///

In summary, for $\chi_{\mathfrak{P}}^{-n}$ of order m, with $\ell = n/\gcd(n, p-1)$, when the prime ideals over p in $\mathbb{Z}[\omega_m]$ are *principal*, with generators $\tau_b q_o$, there is a *root of unity* η such that

$$\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \eta \cdot \prod_{b \in (\mathbb{Z}/m)^\times} (\tau_b q_o)^{b^{-1}\ell \bmod m} \qquad\qquad (\text{exponents in the range } 0, 1, 2, \ldots, m-1)$$

5. *Evaluating Gauss sums*

We combine Kummer's estimate, the prime factorization, and the fact that the ambiguous unit η is a root of unity, to set up subsequent numerical computations. Specifically, we obtain a congruence that completely determines η.

As above, let $\chi_{\mathfrak{P}}^{-n}$ be of order $m = (p-1)/\gcd(n, p-1)$, put $\ell = n/\gcd(n, p-1)$, and suppose that the primes lying over p in $\mathbb{Z}[\omega]$ are *principal*. We just saw that

$$\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \eta \cdot \prod_{b \in (\mathbb{Z}/m)^\times} (\tau_b q_o)^{b^{-1}\ell \bmod m} \qquad \text{(exponents in the range } 0, 1, 2, \dots, m-1)$$

On the other hand, from Kummer's estimate,

$$\Big(\frac{\gamma(\chi_{\mathfrak{P}}^{-n})}{(\zeta-1)^n}\Big)^m \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod \mathfrak{P}$$

or

$$\frac{\gamma(\chi_{\mathfrak{P}}^{-n})^m}{(\zeta-1)^{\ell\cdot(p-1)}} \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod \mathfrak{P}$$

Combining these,

$$\frac{\eta \cdot \prod_{b \in (\mathbb{Z}/m)^\times} (\tau_b q_o)^{b^{-1}\ell \bmod m}}{(\zeta-1)^{\ell\cdot(p-1)}} \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod \mathfrak{P}$$

This will determine η completely. The relation admits simplification, as follows. From

$$0 \;=\; \zeta^{p-1} + \ldots + \zeta + 1 \;=\; \big((\zeta-1)+1\big)^{p-1} + \ldots + \big((\zeta-1)+1\big) + 1 \;=\; (\zeta-1)^{p-1} + \ldots + p$$

we have

$$(\zeta-1)(\zeta^2-1)\ldots(\zeta^{p-1}-1) \;=\; p$$

Since $\zeta = 1 \bmod \zeta - 1$,

$$\frac{p}{(\zeta-1)^{p-1}} \;=\; \frac{(\zeta-1)(\zeta^2-1)\ldots(\zeta^{p-1}-1)}{(\zeta-1)^{p-1}}$$

$$=\; 1 \cdot (\zeta+1)\cdot(\zeta^2+\zeta+1)\ldots(\zeta^{p-2}+\ldots+1) \;=\; (p-1)! \bmod \mathfrak{P} \;=\; -1 \bmod \mathfrak{P}$$

Thus, the relation determining η becomes

$$\frac{\eta \cdot \prod_{b \in (\mathbb{Z}/m)^\times} (\tau_b q_o)^{b^{-1}\ell \bmod m}}{(-p)^\ell} \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod \mathfrak{P}$$

Since now everything is in $\mathbb{Z}[\omega]$, this is

$$\frac{\eta \cdot \prod_{b \in (\mathbb{Z}/m)^\times} (\tau_b q_o)^{b^{-1}\ell \bmod m}}{(-p)^\ell} \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod q_o$$

For simplicity, consider the case $n|(p-1)$, so $m = \frac{p-1}{n}$ and $\ell = 1$:

$$\frac{\eta \cdot \prod_{b \in (\mathbb{Z}/m)^\times} (\tau_b q_o)^{b^{-1} \bmod \frac{p-1}{n}}}{-p} \;=\; \Big(\frac{-1}{(\frac{p-1}{m})!}\Big)^m \bmod q_o$$

Since p is the product of the elements $\tau_b q_o$, in this case the left-hand side simplifies a little, to

$$-\eta \cdot \prod_{b\in(\mathbb{Z}/m)^\times} (\tau_b q_o)^{b^{-1} \bmod \frac{p-1}{n}-1} \;=\; \Big(\frac{-1}{(\frac{p-1}{m})!}\Big)^m \bmod q_o$$

with $b^{-1} \bmod \frac{p-1}{n}$ in the range $1, \dots, \frac{p-1}{n} - 1$. The fact that $\mathbb{Z}[\omega]$ modulo q_o has m^{th} roots of unity *almost* assures that η is completely determined by this congruence. However, for m *odd*, $\mathbb{Z}[\omega]$ also contains the $2m^{th}$ roots of unity. Luckily, p is odd, so $\mathbb{Z}[\omega]$ mod q_o *also* has $2m^{th}$ roots of unity. That is, the map from roots of unity in $\mathbb{Z}[\omega]$ to $\mathbb{Z}[\omega]$ modulo q_o is *injective*, so η is completely determined by this congruence, as claimed.

That is, since η is a root of unity, rather than a more general unit in $\mathbb{Z}[\omega]$, Kummer's estimate is sufficient to determine η completely.

---

6. *Numerical examples*

We illustrate the above discussion with several examples of primes p and Gauss sums attached to characters $\chi_{\mathfrak{P}}^{-n}$ of order m, with $n = \frac{p-1}{m}$. Naturally, we take advantage of coincidences to arrange less laborious examples.

[6.1] $p = 5$ and order $m = 4$ The tiniest case is $p = 5$ and order $m = 4$. The prime $p = 5$ has factors $q_o = 2 + i$ and $\tau_3 q_o = 2 - i$ in $\mathbb{Z}[i]$. We have

$$\gamma(\chi_{\mathfrak{P}}^{-1})^4 \;=\; \eta \cdot (2+i) \cdot (2-i)^3$$

and the congruence for the unit η is

$$-(2-i)^2 \cdot \eta \;=\; \big(\frac{-1}{(\frac{5-1}{4})!}\big)^4 \bmod (2+i)$$

or simply

$$-(2-i)^2 \cdot \eta \;=\; 1 \bmod (2+i)$$

Since $2 - i = (2 + i) - 2i$, we have $-(-2i)^2\eta = 1 \bmod (2 + i)$, or $\eta = 1 \bmod (2 + i)$, so $\eta = 1$. That is,

$$\gamma(\chi_{\mathfrak{P}}^{-1})^4 \;=\; (2+i) \cdot (2-i)^3$$

and $\mathbb{Q}(\zeta_5, \omega)$ is generated by a fourth root of $(2 + i) \cdot (2 - i)^3$ over $\mathbb{Q}(\omega)$. Thus,

$$\mathbb{Q}(\zeta_5, i) \;=\; \mathbb{Q}(i)\big(\sqrt[4]{(2+i)\cdot(2-i)^3}\big)$$

[6.2] $p = 13$ and order $m = 4$ Take $q_o = 3 + 2i$ and $\tau_3 q_o = 3 - 2i$. We have

$$\gamma(\chi_{\mathfrak{P}}^{-1})^4 \;=\; \eta \cdot (3+2i) \cdot (3-2i)^3$$

The congruence for the unit η is

$$-(3-2i)^2 \cdot \eta \;=\; \big(\frac{-1}{(\frac{13-1}{4})!}\big)^4 \bmod (3+2i)$$

or simply

$$-(3-2i)^2 \cdot \eta \;=\; \frac{1}{6^4} \bmod (3+2i)$$

Since $3-2i = (3+2i) - 4i$ and $2\cdot 6 = -1 \bmod 13$, this is

$$16\cdot\eta \;=\; (-2)^4 \bmod (3+2i)$$

from which $\eta = 1$. Thus,

$$\gamma(\chi_{\mathfrak{P}}^{-3})^4 \;=\; q_o\cdot(\tau_3 q_o)^3\cdot\eta \;=\; (3+2i)\cdot(3-2i)^3$$

and the quartic subfield $\mathbb{Q}(\zeta_{13},\omega)$ over $\mathbb{Q}(\omega)$ is generated by a fourth root of $(3+2i)\cdot(3-2i)^3$. Thus, the quartic subfield of $\mathbb{Q}(\zeta_{13},i)$ over $\mathbb{Q}(i)$ is

$$\Big(\text{quartic subfield of } \mathbb{Q}(\zeta_{13},i) \text{ over } \mathbb{Q}(i)\Big) \;=\; \mathbb{Q}(i)\big(\sqrt[4]{(3+2i)\cdot(3-2i)^3}\big)$$

[6.3] $p = 17$ and order $m = 4$ Take $q_o = 4+i$ and $\tau_3 q_o = 4-i$. We have

$$\gamma(\chi_{\mathfrak{P}}^{-1})^4 \;=\; \eta\cdot(4+i)\cdot(4-i)^3$$

and the congruence for the unit η is

$$-(4-i)^2\cdot\eta \;=\; \big(\frac{-1}{(\frac{17-1}{4})!}\big)^4 \bmod (4+i)$$

or

$$-(4-i)^2\cdot\eta \;=\; \frac{1}{7^4} \bmod (4+i)$$

Since $4-i = (4+i) - 2i$ and $5\cdot 7 = 1 \bmod 17$, this is

$$4\cdot\eta \;=\; 5^4 \bmod (4+i)$$

Since $-4\cdot 4 = 1 \bmod 17$,

$$\eta \;=\; -4\cdot 8^2 \;=\; -(2\cdot 8)^2 \;=\; -(-1)^2 \;=\; -1 \bmod 4+i$$

Thus,

$$\gamma(\alpha)^4 \;=\; \eta\cdot(4+i)(4-i)^3 \;=\; -(4+i)(4-i)^3$$

Therefore, the quartic subfield of and $\mathbb{Q}(\zeta_{17},\omega)$ over $\mathbb{Q}(\omega)$ is generated by a fourth root of $-(4+i)\cdot(4-i)^3$, and

$$\Big(\text{quartic subfield of } \mathbb{Q}(\zeta_{17},i) \text{ over } \mathbb{Q}(i)\Big) \;=\; \mathbb{Q}(i)\big(\sqrt[4]{-(4+i)\cdot(4-i)^3}\big)$$

[6.4] $p = 7$ and order $m = 3$ Let ρ be a cube root of unity, with Galois conjugate $\overline{\rho}$. Note that $\overline{\rho} = -1-\rho$, and

$$(a+b\rho)(a+b\overline{\rho}) \;=\; a^2 - ab + b^2$$

For $p = 7$, take $q_o = 2-\rho$ and $\tau_{-1}q_o = 2-\overline{\rho} = 3+\rho$.

$$\gamma(\chi_{\mathfrak{P}}^{-2})^3 \;=\; \eta\cdot(2-\rho)\cdot(3+\rho)^2$$

The congruence for the unit η is

$$-(3+\rho)\cdot\eta \;=\; \big(\frac{-1}{(\frac{7-1}{3})!}\big)^3 \bmod (2-\rho)$$

which becomes $(3+\rho)\cdot\eta = 1 \bmod (2-\rho)$. Since

$$3+\rho \;=\; 3+\rho+2(2-\rho) \;=\; -\rho \bmod 2-\rho$$

the congruence for η is

$$-\rho\cdot\eta \;=\; 1 \bmod (2-\rho)$$

so $\eta = -\rho^2$. That is,

$$\gamma(\chi_{\mathfrak{P}}^{-2})^3 \;=\; \eta\cdot(2-\rho)\cdot(3+\rho)^2 \;=\; -\rho^2\cdot(2-\rho)\cdot(3+\rho)^2$$

and the cubic subfield of $\mathbb{Q}(\zeta_7,\rho)$ over $\mathbb{Q}(\omega)$ is generated by a cube root of $-\rho^2\cdot(2-\rho)\cdot(3+\rho)^2$:

$$\big(\text{cubic subfield of } \mathbb{Q}(\rho,\zeta_7) \text{ over } \mathbb{Q}(\rho)\big) \;=\; \mathbb{Q}(\rho)\big(\sqrt[3]{-\rho^2\cdot(2-\rho)\cdot(3+\rho)^2}\big)$$

[6.5] $p = 7$ and order $m = 6$ Use $q_o = 2-\rho$ and $\tau_{-1}q_o = 2-\overline{\rho} = 3+\rho$. We have

$$\gamma(\chi_{\mathfrak{P}}^{-1})^6 \;=\; \eta\cdot(2-\rho)\cdot(3+\rho)^5$$

and η satisfies

$$-(3+\rho)^4\cdot\eta \;=\; \big(\frac{-1}{(\frac{7-1}{6})!}\big)^6 \bmod (2-\rho)$$

Using $\rho = 2 \bmod 2-\rho$ and $5 = -2 \bmod 7$, this is

$$-(-2)^4\cdot\eta \;=\; 1 \bmod (2-\rho)$$

or

$$2\cdot\eta \;=\; -1 \bmod (2-\rho)$$

Thus,

$$\eta \;=\; -4 \;=\; -\rho^2 \bmod 2-\rho$$

and

$$\gamma(\chi_{\mathfrak{P}}^{-1})^6 \;=\; -\rho^2\cdot(2-\rho)\cdot(3+\rho)^5$$

Thus,

$$\mathbb{Q}(\rho,\zeta_7) \;=\; \mathbb{Q}(\rho)\big(\sqrt[6]{\rho^2\cdot(2-\rho)\cdot(3+\rho)^5}\big)$$

[6.6] $p = 17$ and order $m = 8$ Since $\omega = \omega_8$ satisfies $\omega^4+1 = 0$,

$$0 \;=\; \big((\omega+2)-2\big)^4+1 \;=\; (\omega+2)^4+\ldots+(2^4+1)$$

and, since the constant term $17 = 2^4+1$ is the norm of $q_o = \omega+2$,

$$17 \;=\; (\omega+2)(\omega^3+2)(\omega^5+2)(\omega^7+2)$$

The eighth power of the octic Gauss sum is

$$\gamma(\chi_{\mathfrak{P}}^{-2})^8 \;=\; \eta\cdot(\omega+2)\,(\omega^3+2)^3\,(\omega^5+2)^5\,(\omega^7+2)^7$$

and the congruence for η is

$$-\eta\,(\omega^3+2)^2\,(\omega^5+2)^4\,(\omega^7+2)^6 \;=\; \big(\frac{-1}{(\frac{17-1}{8})!}\big)^8 \bmod (\omega+2)$$

This is

$$-\eta\,((-2)^3+2)^2\,((-2)^5+2)^4\,((-2)^7+2)^6 \;=\; \frac{1}{2^8} \bmod (\omega+2)$$

Using $2^4 = -1 \bmod 17$,

$$-\eta \cdot 2 \cdot 4^4 \cdot 10^6 \;=\; 1 \bmod (\omega+2)$$

or

$$-\eta \cdot 2^{15} \cdot 5^6 \;=\; 1 \bmod (\omega+2)$$

which gives $\eta \cdot 2^3 \cdot 8^3 \;=\; 1 \bmod (\omega+2)$ and then $\eta \;=\; -1 \bmod (\omega+2)$. Thus $\eta = -1$, and

$$(\text{octic subfield of } \mathbb{Q}(\omega_8, \zeta_{17}) \text{ over } \mathbb{Q}(\omega_8))\mathbb{Q}(\omega_8)\big(\sqrt[8]{-(\omega+2)\,(\omega^3+2)^3\,(\omega^5+2)^5\,(\omega^7+2)^7}\big)$$

[6.7] $p = 11$ and order $m = 5$ Since $\omega = \omega_5$ satisfies $\omega^4 + \omega^3 + \ldots + \omega + 1 = 0$,

$$0 \;=\; \big((\omega+2)-2\big)^4 + \big((\omega+2)-2\big)^3 + \ldots + \big((\omega+2)-2\big) + 1 \;=\; (\omega+2)^4 + \ldots + 11$$

The constant term $11 = (2^5+1)/(2+1)$ is the norm of $q_o = \omega + 2$, so

$$11 \;=\; (\omega+2)(\omega^2+2)(\omega^3+2)(\omega^4+2)$$

The fifth power of the quintic Gauss sum is

$$\gamma(\chi_{\mathfrak{P}}^{-2})^5 \;=\; \eta \cdot (\omega+2)\,(\omega^2+2)^3\,(\omega^3+2)^2\,(\omega^4+2)^4$$

and the congruence for η is

$$-\eta\,(\omega^2+2)^2\,(\omega^3+2)\,(\omega^4+2)^3 \;=\; \big(\frac{-1}{(\frac{11-1}{5})!}\big)^5 \bmod (\omega+2)$$

Using $\omega = -2 \bmod \omega + 2$, this is

$$\eta\,((-2)^2+2)^2\,((-2)^3+2)\,((-2)^4+2)^3 \;=\; \frac{1}{2^5} \bmod (\omega+2)$$

or

$$\eta \cdot 6^2 \cdot (5) \cdot (7)^3 \;=\; -1 \bmod (\omega+2)$$

which simplifies to $\eta \cdot 3 \cdot 5 \cdot 2 \;=\; -1 \bmod (\omega+2)$ and then $3\eta = 1 \bmod (\omega+2)$, so $\eta = 4 \bmod (\omega+2)$. Since $\omega = -2 \bmod (\omega+2)$, this gives $\eta = \omega^2$. Thus,

$$\gamma(\chi_{\mathfrak{P}}^{-2})^5 \;=\; \omega^2 \cdot (\omega+2)\,(\omega^2+2)^3\,(\omega^3+2)^2\,(\omega^4+2)^4$$

and the quintic subfield of $\mathbb{Q}(\omega_5, \zeta_{11})$ is generated over $\mathbb{Q}(\omega_5)$ by the fifth root of this.

[6.8] $p = 43$ and order $m = 7$ With $p = 43$, from $(2^7+1)/(2+1) = 43$, with $\omega = \omega_7$, the prime splits into principal factors in $\mathbb{Z}[\omega_7]$:

$$43 \;=\; (\omega+2)(\omega^2+2)(\omega^3+2)(\omega^4+2)(\omega^5+2)(\omega^6+2)$$

The seventh power of the septic Gauss sum is

$$\gamma(\chi_{\mathfrak{P}}^{-6})^7 \;=\; \eta \cdot (\omega+2)(\omega^2+2)^4(\omega^3+2)^5(\omega^4+2)^2(\omega^5+2)^3(\omega^6+2)^6$$

and the congruence for η is

$$\eta\,(\omega^2+2)^3(\omega^3+2)^4(\omega^4+2)(\omega^5+2)^2(\omega^6+2)^5 \;=\; \big(\frac{-1}{(\frac{43-1}{7})!}\big)^7 \bmod (\omega+2)$$

Using $\omega = -2 \bmod \omega + 2$, and $(-2)^7 = 1 \bmod 43$, the indicated computation is easily feasible by hand, but not interesting enough to carry out in detail here.

[6.9] Mersenne primes For $p = 2^r - 1$ prime, p splits into principal primes in $\mathbb{Z}[\omega_r]$, so the degree r subfield of $\mathbb{Q}(\omega_r, \zeta_p)$ is expressible in radicals. The identity for factorization into principal ideals is

$$0 \;=\; \big((\omega-2)+2\big)^{r-1} + \ldots + \big((\omega-2)+2\big) + 1 \;=\; (\omega-2)^{r-1} + \ldots + (2^{r-1} + 2^{r-2} + \ldots + 2 + 1)$$

$$= \; (\omega-2)^{r-1} + \ldots + (2^r - 1)$$

[6.10] Fermat primes The discussion for $p = 17$ and order $m = 8$ applies to any Fermat prime $p = 2^{2^r} + 1$ and the corresponding order 2^{r+1} Gauss sum's $(2^{r+1})^{th}$ power. Namely, with $\omega = \omega_{2^{r+1}}$, the identity

$$0 \;=\; \big((\omega+2)-2\big)^{2^r} + 1 \;=\; (\omega+2)^{2^r-1} + \ldots + (2^{2^r} + 1)$$

demonstrates that $2^{2^r} + 1$ splits into principal primes in $\mathbb{Z}[\omega_{2^{r+1}}]$.

---

7. *Appendix: background*

- Kronecker's theorem
- Existence of Kummer (-Teichmüller) character
- Basic properties of Gauss sums

[7.1] A little theorem of Kronecker *An algebraic integer all whose complex imbeddings have absolute value* 1 *is a root of unity.*

To prove this, let α be an algebraic integer such that $|\sigma(\alpha)| = 1$ for all complex (or real) imbeddings $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$. Then the same property is true of all powers of α, and these powers are of degree over $\mathbb{Q}$ no more than that of α. Thus, the monic irreducibles of the powers of α over $\mathbb{Q}$ are of uniformly bounded degree and have uniformly bounded coefficients. The coefficients are in $\mathbb{Z}$, since α is an algebraic integer. There are only finitely-many polynomials of bounded degree with bounded integer coefficients. Thus, $\alpha^i = \alpha^j$ for some $i \neq j$. ///

[7.2] Existence of Kummer (-Teichmüller) character As above, let p be a prime, and ω a primitive $(p-1)^{th}$ root of unity. Fix a prime $\mathfrak{q}$ lying over p in $\mathbb{Z}[\omega]$. The complete splitting of p in $\mathbb{Z}[\omega]$ implies that the residue class field extension is trivial, so the inclusion

$$j \;:\; \mathbb{Z}/p \;\longrightarrow\; \mathbb{Z}[\omega]/\mathfrak{q}$$

is an *isomorphism*. The units in $\mathbb{Z}[\omega]$ certainly map to units in $\mathbb{Z}[\omega]/\mathfrak{q}$. It would be perverse if the $(p-1)^{th}$ roots of unity in $\mathbb{Z}[\omega]$ did not surject to the units in $\mathbb{Z}[\omega]/\mathfrak{q}$, but this requires proof. Thus, we can use Hensel's lemma to specify a $\mathbb{Z}[\omega]_{\mathfrak{q}}^{\times}$-valued character on $(\mathbb{Z}/p)^{\times}$, beginning with

$$\chi_{\mathfrak{q}}(a) \;=\; j(a) \bmod \mathfrak{q}$$

To solve the equation $x^{p-1} - 1 = 0$ in $\mathbb{Z}[\omega]_{\mathfrak{q}}$, let $x_1 = a$. Since the derivative $(p-1)a^{p-2}$ is a $\mathfrak{q}$-adic unit, Hensel's lemma produces $x \in \mathbb{Z}[\omega]_{\mathfrak{q}}$ such that $x^{p-1} - 1 = 0$ and $x = a \bmod \mathfrak{q}$, as desired. Of course, the $(p-1)^{th}$ roots of unity are in $\mathbb{Z}[\omega]$, without completing, but this discussion does prove that the $(p-1)]th$ roots of unity *surject* to the units in $(\mathbb{Z}/p)^{\times} \approx (\mathbb{Z}[\omega]/\mathfrak{q})^{\times}$.

This proves existence of the Kummer (-Teichmüller) character.

[7.3] Elementary property of Gauss sums

For a multiplicative character α and additive character ψ on $\mathbb{Z}/p$, the product $\gamma(\alpha)\cdot\gamma(\alpha^{-1})$ of Gauss sums is simply $p\cdot\alpha((-1)$, by a straightforward computation, as follows:

$$\gamma(\alpha)\cdot\gamma(\alpha^{-1}) \;=\; \big(\sum_a \alpha(a)\,\psi(a)\big)\cdot\big(\sum_b \alpha^{-1}(b)\,\psi(b)\big) \;=\; \sum_{a,b}\alpha(a)\,\alpha^{-1}(b)\,\psi(a+b)$$

Replace b by ab:

$$\gamma(\alpha)\cdot\gamma(\alpha^{-1}) \;=\; \sum_{a,b}\alpha^{-1}(b)\,\psi(a(1+b))$$

For fixed b, the sum over a is -1 unless $1+b=0$, in which case it is $p-1$. Thus,

$$\gamma(\alpha)\cdot\gamma(\alpha^{-1}) \;=\; -\sum_{b\neq -1}\alpha^{-1}(b)+\alpha^{-1}(-1)\cdot(p-1) \;=\; \alpha^{-1}(-1)+\alpha^{-1}(-1)\cdot(p-1) \;=\; \alpha(-1)\cdot p$$

since $\alpha(-1)=\alpha^{-1}(-1)$. That is,

$$\gamma(\alpha)\cdot\gamma(\alpha^{-1}) \;=\; \alpha(-1)\cdot p$$

On the other hand, for two multiplicative characters α,β with $\alpha\beta\neq 1$, an analogous computation has a different outcome, involving a Jacobi sum:

$$\gamma(\alpha)\cdot\gamma(\beta) \;=\; \sum_a \alpha(a)\,\psi(a)\cdot\sum_b\beta(b)\,\psi(b) \;=\; \sum_{a,b}\alpha(a)\,\beta(b)\,\psi(a+b)$$

$$=\sum_{a\neq 0}\sum_b \alpha(a-b)\,\beta(b)\,\psi(a)+\sum_b\alpha(-b)\,\beta(b) \;=\; \sum_{a\neq 0}\sum_b\alpha(a-b)\,\beta(b)\,\psi(a)+\alpha(-1)\sum_b\alpha(b)\,\beta(b)$$

For $\alpha\beta\neq 1$, the last sum vanishes. In the first sum, replace b by ab:

$$\gamma(\alpha)\cdot\gamma(\beta) \;=\; \sum_{a\neq 0}\sum_{b\neq 0,1}\alpha(a(1-b))\,\beta(ab)\,\psi(a)$$

$$=\sum_{a\neq 0}\sum_{b\neq 0,1}\alpha(a)\beta(a)\,\psi(a)\sum_b\alpha(1-b))\,\beta(b) \;=\; \gamma(\alpha\beta)\cdot\sum_{b\neq 0,1}\alpha(1-b))\,\beta(b)$$

That is,

$$\gamma(\alpha)\cdot\gamma(\beta) \;=\; \gamma(\alpha\beta)\cdot\sum_{b\neq 0,1}\alpha(1-b))\,\beta(b) \qquad\qquad (\text{with } \alpha\beta\neq 1)$$

The latter sum is a *Jacobi sum*.

[Cohen 2007] H. Cohen, *Number Theory: Volume I, Tools and Diophantine Equations*, ... *Volume II, Analytic and Modern Tools*, Springer-Verlag, 2007.

[Dedekind 1871] R. Dedekind, *Über die Theorie der ganzen algebraischen Zahlen. X*, supplement to P.G.L. Dirichlet's *Vorlesungen über Zahlentheorie*, 2nd ed., Vieweg, Braunschweig, 1871. Fourth edition 1894.

[Eisenstein 1850] G. Eisenstein, *Über en einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze*, J. reine angew. Math. **39** (1850), 351-364; *Mathematische Werke, II*, 623-636, Chelsea, New York, 1975.

[Heath-Brown Patterson 1979] D.R. Heath-Brown, S.J. Patterson, *The distribution of Kummer sums at prime arguments*, J. reine und Angew. Math. **310** (1979), 111-130.

[Hilbert 1897] D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresber. Deutsch. Math. Verein. **4** (1897), 175-546.

[Koch 1997] H. Koch, *Number Theory: Algebraic Numbers and Functions*, AMS, 2000; translation by D. Kramer of *Zahlentheorie: Algebraische Zahlen und Funktionen*, F. Vieweg, Braunschweig/Wiesbaden, 1997.

[Kummer 1847] E. Kummer, *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihtre Primfactoren*, J. reine angew. Math. **35** 91847), 327-367. *Collected Papers, I*, 211-251.

[Lagrange 1870] J. L. Lagrange, *Réflexions sur la résolution algébrique des équations*, 1770.

[Lang 1970] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, 1970.

[Lang 1978,80] S. Lang, *Cyclotomic Fields, I,II*, Springer-Verlag, 1978, 1980.

[O'Connor-Robertson 2001] J.J. O'Connor and E.F. Robertson, *Alexandre-Théophile Vandermonde*, http://www-history.mcs.st-and.ac.uk/Biographies/Vandermonde.html

[Stickelberger 1890] L. Stickelberger, *Über einer Verallgemeinerung der Kreistheilung*, Math. Ann. **37** (1890), 321-367.

[Washington 1982], L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.

[Vandermonde 1771] A.-T. Vandermonde, *Memoire sur la resolution des équations*, Acad. Sci. Paris, 1771.