

WHENCE GAUSS SUMS?

Typically in a first number theory course the quadratic Gauss sum,

$$\tau = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \zeta_p^t,$$

is pulled out of thin air, and its properties established by elementary calculations that appear to work for no discernible reason. A person might wonder just what is going on and how anybody might conceive of such a thing.

In fact the quadratic Gauss sum is a particular case of a *Lagrange resolvent*. The idea is as follows.

- Let K/k be an extension of fields; that is, K is a superfield of k .
- The automorphisms of K that fix k pointwise form a group G . Assume that the subfield of K that is fixed pointwise by every automorphism in G is exactly k , not a larger field. (That is, we assume that K/k is *Galois*.)
- Suppose that for some positive integer n we want to find an element r of the larger field K that is an n th root over the smaller field k .

The trick is to symmetrize. Suppose that we can find a k^\times -valued character of order n on the automorphism group,

$$\chi : G \longrightarrow k^\times, \quad \chi^n = 1.$$

Take any element x of the larger field K . Its Lagrange resolvent is again an element of K ,

$$r = r(x) = \sum_{\sigma \in G} \chi(\sigma) \sigma(x).$$

The Lagrange resolvent is symmetrized in the sense that for any automorphism $\sigma_o \in G$,

$$\begin{aligned} \sigma_o(r) &= \sigma_o \left(\sum_{\sigma \in G} \chi(\sigma) \sigma(x) \right) \\ &= \sum_{\sigma \in G} \chi(\sigma) (\sigma_o \sigma)(x) \\ &= \bar{\chi}(\sigma_o) \sum_{\sigma \in G} \chi(\sigma_o \sigma) (\sigma_o \sigma)(x) \\ &= \bar{\chi}(\sigma_o) r. \end{aligned}$$

Consequently, for any automorphism $\sigma_o \in G$,

$$\sigma_o(r^n) = (\sigma_o(r))^n = (\bar{\chi}(\sigma_o) r)^n = r^n.$$

Thus $r^n \in k$ according to the second bullet above.

As a special case, let $k = \mathbf{Q}$ and let $K = \mathbf{Q}(\zeta_p)$. In this case, the automorphism group $G \cong (\mathbf{Z}/p\mathbf{Z})^\times$ admits a unique character of order 2, the quadratic character (\cdot/p) . Choose $x = \zeta_p$ to recover the definition of the quadratic Gauss sum τ . We see now that τ is concocted so that its square is rational.