The maximal ideal factorization of Gauss sums

January 22, 2014

Let's recall the set-up from last time. (By the way, my source for these two lectures has largely been this article: http://www.bprim.org/cyclotomicfieldbook/jacn.pdf)

We start with the following initial data:

- A prime power $q = p^d$. (Let us also assume $p > 2$.)
- A maximal ideal P of $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ lying above p.

This gives us all of the following:

- A finite field $\mathbb{F}_P$ of size q, namely the quotient $\mathbb{F}_P = \mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/P$.
- A generating character $\omega : \mathbb{F}_P^\times \to \{z^{q-1} = 1\}$, defined by $\omega(a) = \zeta$ if ζ is congruent to a (mod P).
- For every $k \in \mathbb{Z}/(q-1)\mathbb{Z}$, a Gauss sum

$$G(\omega^{-k}) = \sum_{a \in \mathbb{F}_P^\times} \omega(a)^{-k} \cdot \zeta_p^{Tr(a)}$$

  in $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1},\zeta_p)}$. Here $Tr(a) = a + a^p + \ldots + a^{p^{d-1}} \in \mathbb{F}_p$.
- The maximal ideal $\widetilde{P} = (P, \pi)$ of $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1},\zeta_p)}$. This lies above P in $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ and $(\pi) = (1 - \zeta_p)$ in $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. The relationship between $\widetilde{P}$ and P is exactly like the relationship between (π) and p.

The main claim is the following:

Theorem 0.1. *Fix the initial data q, P as above, and let $k \in \mathbb{Z}/(q-1)\mathbb{Z}$. Define $s(k)$ to be the sum of the digits of the base-p expansion of the "least positive residue" of k. Then $s(k)$ equals $v_{\widetilde{P}}(G(\omega^{-k}))$, the exponent of $\widetilde{P}$ in the unique maximal ideal factorization of $(G(\omega^{-k}))$.*

"Least positive residue" just means, represent k by an integer in the range $0 \leq x < q - 1$.

It's possible to just dig right in to this theorem, following the same method we used in determining the sign of the quadratic Gauss sum. Namely, we can also consider π-adic expansions in $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1},\zeta_p)}$. To make them well-defined, we just need to choose a set of representatives for the quotient $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1},\zeta_p)}/\pi = \mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/p$; then these will be our possible coefficients for the π-adic expansion. And if we're only

interested in the first $p-1$ digits of the π-adic expansion, then since $(\pi)^{p-1} = p$, there is actually no choice of representatives required, and we can actually think of the coefficients as lying in $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/p$. Furthermore, if in the end all we're interested in is $v_{\widetilde{P}}$ of the element we're π-adically expanding, we can even take the coefficients as lying in $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/P = \mathbb{F}_P$ and not lose the relevant information.

The upshot is that the method of π-adic expansion of an element $x \in \mathcal{O}_{\mathbb{Q}(\zeta_{q-1},\zeta_p)}$ will, in principle, let us determine when $v_{\widetilde{P}}(x)$ is $\geq v$, for any $0 \leq v \leq p-1$: namely, this occurs if and only if the π-adic expansion of x with coefficients in $\mathbb{F}_P$ has all zeros as coefficients up through degree $v-1$. This won't get us all the way to the above theorem, but it'll be a start, and then we can use the multiplicative properties of Gauss sums proved in the previous lecture to go all the way.

Actually, it'll be enough for us just to analyze the first two coefficients of the π-adic expansion. So consider

$$G(\omega^{-k}) = \sum_{a \in \mathbb{F}_P^\times} \omega(a)^{-k} (1-\pi)^{a+a^p+\ldots+a^{p^{d-1}}}.$$

The zeroth coefficient is the sum $\sum_{a \in \mathbb{F}_P^\times} \omega(a)^{-k}$. For $k \neq 0$, this is the sum of the values of a nontrivial character, so it is zero. Now, from now on we'll abbreviate $v(k) = v_{\widetilde{P}}(G(\omega^{-k}))$, so we're trying to show $v(k) = s(k)$. Then we deduce:

- When $k \neq 0$, we have $v(k) \geq 1$. (When $k = 0$, we have $G(\omega^{-k}) = 0$; I'll tend to ignore that case.)

Now let's set $k = 1$. Then the first coefficient of the π-adic expansion is

$$-\sum_{a \in \mathbb{F}_P^\times} \omega(a)^{-1} \cdot (a + a^p + \ldots + a^{p^{d-1}}).$$

But by definition, $\omega(a)^{-1} = a^{-1} = a^{q-2} \pmod{P}$, so we can rewrite this is

$$-\sum_{a \in \mathbb{F}_P^\times} \left(a^{q-1} + a^{p+q-2} + \ldots + a^{p^{d-1}+q-2}\right).$$

Recall our lemma from the analysis of the sign of the Gauss sum, about the sum of the values of a polynomial over a finite field. It says that only the cofficients of index divisble by $(q-1)$ contribute, and those contribute with a $-$ sign. Since $p^{d-1} + q - 2 < 2(q-1)$, the only monomial in the above sum with index divisible by $(q-1)$ is the first one, a^{q-1}. Thus the above sum evaluates to 1, so that's the coefficient of π in the π-adic expansion of $G(\omega^{-1})$. Thus, since $1 \neq 0$, we get:

- We have $v(1) = 1$.

Actually, just these two facts ($v(k) \geq 1$ for $k \neq 0$, $v(1) = 1$) are enough of a seed to get us all the way. We just need the following three lemmas.

Lemma 0.2. *Let $k, k' \in \mathbb{Z}/(q-1)\mathbb{Z}$ with $k + k' \neq 0$. Then $v(k) + v(k') \leq v(k+k')$, and the same with "$\leq$" replaced by "congruent modulo $p-1$".*

Proof. Recall that in this case,

$$G(\omega^{-k}) \cdot G(\omega^{-k'}) = G(\omega^{-(k+k')}) \cdot J,$$

where the only pertinent fact about J is that it lies in $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ (no ζ_p's). If we apply $v_{\widetilde{P}}$ to this expression, since $v_{\widetilde{P}}$ is multiplicative it suffices to see that $v_{\widetilde{P}}(J)$ is ≥ 0 and divisible by $p-1$. Of course, it's ≥ 0 by definition, since J is an algebraic integer. As for divisibility by $p-1$, since $\widetilde{P}$ lies above P and $\widetilde{P}^{p-1} = P$ (just like $(\pi)^{p-1} = (p)$), we have $v_{\widetilde{P}}(J) = (p-1)v_P(J)$, which proves the claim. □

Lemma 0.3. *Let $k, k' \in \mathbb{Z}/(q-1)\mathbb{Z}$, and assume on the other hand that $k + k' = 0$. Then*

$$v(k) + v(k') = d \cdot (p-1).$$

Proof. Recall that $G(\omega^{-k}) \cdot G(\omega^{-k'}) = \pm q$ in this case. Thus it suffices to see that $v_{\widetilde{P}}(q) = d \cdot (p-1)$. This follows from $(q) = (p^d) = (\pi)^{d \cdot (p-1)}$, and the fact that π is the product of all the $\widetilde{P}$'s as P varies over all choices of maximal ideal above p; hence for any particular choice $v_{\widetilde{P}}(\pi) = 1$. □

Lemma 0.4. *For $k \in \mathbb{Z}/(q-1)\mathbb{Z}$, we have $v(pk) = v(k)$.*

Proof. $G(\omega^{-kp}) = G(\omega^{-k})$. □

Now we can prove the theorem. First we claim that $v(k) = k$ for $0 \leq k < p$. Indeed, by the first lemma we have $v(k) \leq k \cdot v(1)$, and the difference is divisible by $p-1$. But we calculated $v(1) = 1$. So $v(k)$ is $\leq k$ and congruent to k (mod $p-1$). Given how small k is and the fact we know $v(k) > 0$ for $k > 0$, the only possibility is $v(k) = k$, as claimed.

Now take a general $0 \leq k < q-1$. Write the base p expansion of k as $c_0 + c_1 p + \ldots + c_d p^{d-1}$ with $0 \leq c_i < p$. Then by the first and third lemmas,

$$v(k) \leq v(c_0) + v(c_1 p) + \ldots + v(c_d p^{d-1}) = v(c_0) + v(c_1) + \ldots + v(c_d).$$

But then by what we just said this is $c_0 + c_1 + \ldots c_d = s(k)$. So we have $v(k) \leq s(k)$, whereas what we want is $v(k) = s(k)$. But, letting $k' = q - 1 - k$ (so $k + k' = 0$ in $\mathbb{Z}/(q-1)\mathbb{Z}$), we also have $v(k') \leq s(k')$. Thus

$$v(k) + v(k') \leq s(k) + s(k').$$

But both of these numbers are equal to $d(p-1)$, the first by the second lemma and the second by an elementary observation about base p expansions. Thus we deduce that all the $\leq$'s must have actually been $=$'s, as we wanted. (This last argument is akin to us having known a priori that v_π of the quadratic Gauss sum is $\frac{p-1}{2}$, because the square of the quadratic Gauss sum is $\pm p$.)

So we've calculated $v_{\widetilde{P}} G(\omega^{-k})$: it's this funny number $s(k)$. Then next question to ask is, what about the full maximal ideal factorization of $G(\omega^{-k})$? So, what are the exponents of the other maximal ideals? We know that all the maximal ideals above p are of the form $\widetilde{P'}$ for some choice of maximal ideal P' of $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ lying above p, with $P' \neq P$ potentially. Now the idea is the following: for any such P' we can find a Galois element $\sigma \in Gal(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$ which sends P to P'. Then because it's easy to act by Galois on Gauss sums, we'll be able to understand $v_{\widetilde{P'}}$ of a Gauss sum in terms of $v_{\widetilde{P}}$ of a different Gauss sum. Thus we can get the full maximal ideal factorization just from the above theorem, by considering the Galois action.

To put this into action, let's first prove the claim that for every P', there is a σ with $\sigma P = P'$. Let's further add that σ is not unique, but any two choices of σ differ by a power of $p \in (\mathbb{Z}/(q-1)\mathbb{Z})^\times = Gal(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$.

The first step is to see that σP does lie above p for every σ. That's just because to lie above p is to contain p, and that latter condition is obviously invariant under Galois.

Now we need to see that every P' is equal to some σP. Suppose not; then P' is a maximal ideal distinct from all of the finitely many maximal ideals σP. It follows (though we haven't justified this) that there is some $x \in P'$ which lies in none of the σP's. But then, consider the norm $N(x) \in \mathbb{Z}$. This is the product of all the σx as σ ranges over the Galois group; in particular it is a multiple of x, so it lies in P'. Thus it lies in $P' \cap \mathbb{Z} = p\mathbb{Z}$. So it is a multiple of p, and hence it lies in P, since p does. Thus the product of all the Galois conjugates of x lies in P. Since P is maximal, it follows that one of these Galois conjugates must lie in P, say $\sigma x \in P$. But then $x \in \sigma^{-1}P$, a contradiction.

That justifies the first claim, that $P' = \sigma P$ for some σ. For the second claim, it's equivalent to say that the stabilizer of Galois acting on P is the set of powers of $p \in (\mathbb{Z}/(q-1)\mathbb{Z})^\times = Gal(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$. But note, the collection of such powers of p has size d; but by the orbit-stabilizer theorem, since there are exactly $\varphi(q-1)/d$ possible P''s, this is also the size of our stabilizer of Galois acting on P. Thus it suffices to just see that every stabilizing σ, i.e. $\sigma P = P$, is a power of p; the reverse will be automatic.

But, when $\sigma P = P$ we see that σ induces an automorphism of the quotient $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/P = \mathbb{F}_P$. But every automorphism of a finite field is a power of the Frobenius, which sends $\zeta_{q-1} \mapsto \zeta_{q-1}^p$. So we see that σ can only send ζ_{q-1} to a p^{th} power of ζ_{q-1} (recall from last lecture that all the $(q-1)^{st}$ roots of unity are distinct modulo P). This proves the claim.

To recap, we can uniquely describe all the maximal ideals of $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ lying above p as σP, where σ runs over a set of coset representatives for $p^{\mathbb{Z}}$ in $(\mathbb{Z}/(q-1)\mathbb{Z})^\times = Gal(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$, and P is our fixed choice.

Now, given any $\sigma \in Gal(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$, we can lift it to a $\widetilde{\sigma} \in Gal(\mathbb{Q}(\zeta_{q-1}, \zeta_p)/\mathbb{Q})$ by letting it act by the identity on ζ_p. (Recall that $\mathbb{Q}(\zeta_{q-1}, \zeta_p) = \mathbb{Q}(\zeta_{(q-1)p})$, so we understand this Galois group and can easily the claim that there exists such a $\widetilde{\sigma}$; it follows from the fact that $q-1$ and p are relatively prime.) Then by acting by $\widetilde{\sigma}$ on maximal ideal factorizations, we see that

$$v_{\widetilde{\sigma^{-1}P}}(G(\omega^{-k})) = v_P(\widetilde{\sigma} G(\omega^{-k})).$$

But clearly if σ corresponds to $a \in (\mathbb{Z}/(q-1)\mathbb{Z})^\times$, then $\widetilde{\sigma} G(\omega^{-k}) = G(\omega^{-ka})$. The upshot is the following:

Theorem 0.5. *Let our initial data q, P be as above. Then for $k \in \mathbb{Z}/(q-1)\mathbb{Z}$, the unique maximal ideal factorization of $G(\omega^{-k})$ in $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1}, \zeta_p)}$ is*

$$(G(\omega^{-k})) = \prod_{a \in (\mathbb{Z}/(q-1)\mathbb{Z})^\times / p^{\mathbb{Z}}} \widetilde{(\sigma_a^{-1} P)}^{s(ka)},$$

where we write $a \leftrightarrow \sigma_a$ for the isomorphism $(\mathbb{Z}/(q-1)\mathbb{Z})^\times = Gal(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$.

Now that's all well and good, but we were really interested in prime cyclotomic fields. So let ℓ be a prime different from p. We can choose d to be the order of p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$; then with the choice $q = p^d$ we have

$$\mathbb{Q}(\zeta_\ell) \subset \mathbb{Q}(\zeta_{q-1}).$$

If we choose the character $\chi = \omega^{-\frac{q-1}{\ell}}$, then χ takes values in the ℓ^{th} roots of unity, so that $G(\chi) \in \mathbb{Q}(\zeta_\ell, \zeta_p)$. Thus for $k = \frac{q-1}{\ell}$ the above factorization is actually taking place in $\mathcal{O}_{\mathbb{Q}(\zeta_\ell,\zeta_p)}$, and the result is the following:

Theorem 0.6. *Let $\ell \neq p$ be distinct odd primes, and let P be a maximal ideal lying above p in $\mathcal{O}_{\mathbb{Q}(\zeta_\ell)}$. Then for $\chi = \omega^{-\frac{q-1}{\ell}}$, we have the following factorization of ideals in $\mathcal{O}_{\mathbb{Q}(\zeta_\ell,\zeta_p)}$:*

$$(G(\chi)) = \prod_{a \in (\mathbb{Z}/\ell\mathbb{Z})^\times/p^{\mathbb{Z}}} (\widetilde{\sigma_a^{-1}P})^{s(\frac{q-1}{\ell}a)},$$

where again $\widetilde{P}$ denotes the unique maximal ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_\ell,\zeta_p)}$ lying above P.

Now, it's convenient to adopt the following notation: since the Galois action on ideals respects the multiplication of ideals, we can promote the action by Gal to an action by the monoid ring $\mathbb{N}[Gal]$. For this we use exponential notation, so so for $x \in \mathbb{N}[Gal]$ and I an ideal we have another ideal I^x. Then we can rewrite the conclusion of the above theorem as

$$(G(\chi)) = \widetilde{P}^{\sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^\times/p^{\mathbb{Z}}} s(\frac{q-1}{\ell}a)\widetilde{\sigma_a^{-1}}}.$$

By some elementary manipulations, the sum in the exponent can be simplified, giving the following:

$$(G(\chi)) = \widetilde{P}^{(p-1)\sum_{a=1}^{\ell-1} \frac{a}{\ell}\cdot\widetilde{\sigma_a^{-1}}}.$$

But actually, this last expression is deceptive: the exponent doesn't have $\mathbb{N}$-coefficients, even with the multiplication by $(p-1)$. But when you project from $(\mathbb{Z}/\ell\mathbb{Z})^\times$ to $(\mathbb{Z}/\ell\mathbb{Z})^\times/p^{\mathbb{Z}}$, i.e. collect together the coefficients of σ_a^{-1} with $\sigma_{p^i a}^{-1}$ for all i, then it does magically have $\mathbb{N}$-coefficients. So it's good enough for acting on $\widetilde{P}$, since $\widetilde{\sigma_{p^i}}$ fixes $\widetilde{P}$, as we saw above.

There's even more subtlety in the above expression. Recall that $\widetilde{P}^{p-1} = P$ lies in $\mathcal{O}_{\mathbb{Q}(\zeta_\ell)}$. So the above expression is suggesting that the Gauss sum $G(\chi)$ "wants to" live actually in $\mathbb{Q}(\zeta_\ell)$, not just $\mathbb{Q}(\zeta_\ell, \zeta_p)$, and that its maximal ideal factorization "wants to be" the simple

$$\text{“}(G(\chi)) = P^{\sum_{a=1}^{\ell-1} \frac{a}{\ell}\sigma_a^{-1}}.\text{”}$$

The amazing thing to notice here is that the exponent doesn't depend on p! So if the above were true, the exponent would give a universal expression which converts any maximal ideal (and hence any ideal) into a principal ideal. (It doesn't apply to the maximal ideal above ℓ, but that one's already principal.) But the above can't actually be true, because on the one hand we know that $G(\chi)$ has a bunch of ζ_p's in it (and they don't cancel, they really don't), and on the other hand the sum $\sum_{a=1}^{\ell-1} \frac{a}{\ell}\sigma_a^{-1}$ doesn't have $\mathbb{N}$-coefficients, so the expression on the right makes no sense. But Stickelberger figured out that both of these obstructions match up. He expressed this in the following theorem, which we'll show next time:

Theorem 0.7. *Suppose $x \in \mathbb{N}[(\mathbb{Z}/\ell\mathbb{Z})^\times]$ has the property that $x \cdot \sum_{a=1}^{\ell-1} \frac{a}{\ell}\sigma_a^{-1}$ also lies in $\mathbb{N}[(\mathbb{Z}/\ell\mathbb{Z})^\times]$. Then $G(\chi)^x$ lies in $\mathcal{O}_{\mathbb{Q}(\zeta_\ell)}$, and*

$$(G(\chi)^x) = P^{x\cdot\sum_{a=1}^{\ell-1} \frac{a}{\ell}\sigma_a^{-1}}.$$

The simplest x to take is just the number ℓ. There we can already see that $G(\chi)^\ell$ lies in $\mathbb{Q}(\zeta_\ell)$ as a consequence of the multiplicativity properties we established for Gauss sums. But the most interesting x to take is maybe $\sigma_{-k} + k$, with k ranging from 2 to $\ell - 1$.