MATH 361: NUMBER THEORY — NINTH LECTURE

1. Algebraic numbers and algebraic integers

We like numbers such as i and $\omega = \zeta_3 = e^{2\pi i/3}$ and $\varphi = (1+\sqrt{5})/2$ and so on. To think about such numbers in a structured way is to think of them not as *radicals*, but as *roots*.

Definition 1.1. *A complex number α is an* **algebraic number** *if α satisfies some monic polynomial with rational coefficients,*

$$p(\alpha) = 0, \quad p(x) = x^n + c_1 x^{n-1} + \cdots + c_n, \quad c_1, \ldots, c_n \in \mathbb{Q}.$$

Every rational number r is algebraic because it satisfies the polynomial $x - r$, but not every algebraic number is rational, as shown by the examples given just before the definition. For example, $(1+\sqrt{5})/2$ satisfies the polynomial $p(x) = x^2 - x - 1$. Every complex number expressible over $\mathbb{Q}$ in radicals is algebraic, but not conversely.

The algebraic numbers form a field, denoted $\overline{\mathbb{Q}}$. This is shown as follows.

Theorem 1.2. *Let α be a complex number. The following conditions on α are equivalent:*

(1) *α is an algebraic number, i.e., $\alpha \in \overline{\mathbb{Q}}$.*
(2) *The ring $\mathbb{Q}[\alpha]$ is a finite-dimensional vector space over $\mathbb{Q}$.*
(3) *α belongs to a ring R in $\mathbb{C}$ that is a finite-dimensional vector space over $\mathbb{Q}$.*

Proof. (1) $\implies$ (2): Let α satisfy the monic polynomial $p(x) \in \mathbb{Q}[x]$, and let $n = \deg(p)$. For any nonnegative integer m, the division algorithm in $\mathbb{Q}[x]$ gives

$$x^m = q(x)p(x) + r(x), \quad \deg(r) < n \text{ or } r = 0.$$

Thus, because $p(\alpha) = 0$,

$$\alpha^m = r(\alpha) \in \mathbb{Q} \oplus \mathbb{Q}\alpha \oplus \cdots \oplus \mathbb{Q}\alpha^{n-1}.$$

Because $\mathbb{Q}[\alpha]$ is generated over $\mathbb{Q}$ as a vector space by the nonnegative powers of α, this shows that $\mathbb{Q}[\alpha]$ is generated by the finite set $\{1, \alpha, \cdots, \alpha^{n-1}\}$.

(2) $\implies$ (3) is immediate: let $R = \mathbb{Q}[\alpha]$.

(3) $\implies$ (1): Let the ring R have basis $v_1, \ldots, v_n$ as a vector space over $\mathbb{Q}$. Multiplying each generator by α gives a rational linear combination of the generators,

$$\alpha v_i = \sum_{j=1}^{n} c_{ij} v_j, \quad i = 1, \cdots, n.$$

That is, letting $M = [c_{ij}] \in \mathbb{Q}^{n \times n}$,

$$\alpha \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = M \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}.$$

This shows that α is an eigenvalue of M, and so it satisfies the characteristic polynomial of M, a monic polynomial with rational coefficients. $\square$

The implications (1) $\implies$ (2) $\implies$ (3) in the theorem are essentially trivial. The one idea in the theorem is the argument that (3) $\implies$ (1) in consequence of α being an eigenvalue. Here the ring structure and the vector space structure of R interact. For example, if we take $\alpha = \omega = \zeta_3 = e^{2\pi i/3}$ and $R = \mathbb{Q}[\alpha]$ then multiplication by α takes 1 to α and α to $\alpha^2 = -1 - \alpha$, so the matrix in the proof that (3) $\implies$ (1) is $M = \left[\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right]$, whose characteristic polynomial $\det(xI - M) = x^2 + x + 1$ is indeed the characteristic polynomial of α.

Condition (3) in the theorem easily proves

Corollary 1.3. *The algebraic numbers $\overline{\mathbb{Q}}$ form a field.*

Proof. Let α and β be algebraic numbers. Then the rings $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\beta]$ have respective bases

$$\{\alpha^i : 0 \le i < m\} \quad \text{and} \quad \{\beta^j : 0 \le j < n\}$$

as vector spaces over $\mathbb{Q}$. Let

$$R = \mathbb{Q}[\alpha, \beta],$$

spanned as a vector space over $\mathbb{Q}$ by the set

$$\{\alpha^i\beta^j : 0 \le i < m,\ 0 \le j < n\}.$$

Then $\alpha + \beta$ and $\alpha\beta$ belong to R, making them algebraic numbers by condition (3) of the theorem. If $\alpha \ne 0$ then its polynomial $p(x)$ can be taken to have a nonzero constant term c_n after dividing through by its lowest power of x. The relations $\alpha \mid c_n - p(\alpha)$ in $\mathbb{Q}[\alpha]$ and $p(\alpha) = 0$ give $\alpha \mid c_n$ in $\mathbb{Q}[\alpha]$, so that

$$\alpha^{-1} = (1/c_n) \cdot (c_n/\alpha) \in \mathbb{Q}[\alpha],$$

making α^{-1} an algebraic number by condition (3) as well. □

The end of the proof just given, showing that the inverse of a nonzero algebraic number α is again algebraic, can be written more formulaically as follows. The relation $p(\alpha) = 0$ is

$$\alpha^n + c_1\alpha^{n-1} + \cdots + c_{n-1}\alpha + c_n = 0, \quad c_n \ne 0,$$

or

$$\alpha(\alpha^{n-1} + c_1\alpha^{n-2} + \cdots + c_{n-1}) = -c_n,$$

and so

$$\alpha^{-1} = -c_n^{-1}(\alpha^{n-1} + c_1\alpha^{n-2} + \cdots + c_{n-1}).$$

If α and β are algebraic numbers satisfying the monic rational polynomials $p(x)$ and $q(x)$ then the proofs of Corollary 1.3 and of (3) $\implies$ (1) in Theorem 1.2 combine to produce the polynomials satisfied by $\alpha + \beta$ and $\alpha\beta$ and $1/\alpha$ if $\alpha \ne 0$. For example, let $\alpha = i$ and $\beta = \sqrt{2}$. Then

$$\mathbb{Q}[i, \sqrt{2}] = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}i\sqrt{2}.$$

Compute that

$$(i + \sqrt{2}) \begin{bmatrix} 1 \\ i \\ \sqrt{2} \\ i\sqrt{2} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 1 \\ 0 & 2 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ i \\ \sqrt{2} \\ i\sqrt{2} \end{bmatrix}.$$

Thus $i + \sqrt{2}$ satisfies the characteristic polynomial of the matrix in the display.

The theory of **resultants** provides a general algorithm to find such polynomials. The idea is that given any field $\mathbf{k}$, and given any two nonzero polynomials $f(T), g(T) \in \mathbf{k}[T]$, their resultant

$$R(f(T), g(T)) \in \mathbf{k}$$

is zero if and only if f and g share a root that is algebraic over $\mathbf{k}$. That is:

> *The condition $R(f(T), g(T)) = 0$ eliminates the variable T from the simultaneous equations $f(T) = 0$, $g(T) = 0$.*

Now, suppose that the algebraic numbers α and β respectively satisfy the polynomials $f(T)$ and $g(U)$ over $\mathbb{Q}$. Then the condition

$$R(f(T), R(g(U), T + U - V)) = 0$$

first eliminates U from the simultaneous conditions $g(U) = 0$, $V = T + U$, leaving a polynomial condition $h(T, V) = 0$, and then it eliminates T from the simultaneous conditions $f(T) = 0$, $h(T, V) = 0$, leaving a polynomial $k(V)$ over $\mathbb{Q}$ having $\alpha + \beta$ as a root. Almost identically, the condition

$$R(f(T), R(g(U), TU - V)) = 0$$

is a polynomial condition $k(V)$ over $\mathbb{Q}$ having $\alpha\beta$ as a root.

One can now consider complex numbers α satisfying monic polynomials with coefficients in $\overline{\mathbb{Q}}$. But in fact $\overline{\mathbb{Q}}$ is **algebraically closed**, meaning that any such α is already in $\overline{\mathbb{Q}}$. The proof again uses condition (3) in Theorem 1.2.

Corollary 1.4. *The field $\overline{\mathbb{Q}}$ of algebraic numbers is algebraically closed.*

Proof. (Sketch.) Consider a monic polynomial whose coefficients are algebraic numbers,

$$x^n + c_1 x^{n-1} + \cdots + c_n, \quad c_i \in \overline{\mathbb{Q}},$$

and let α be one of its roots. Because each ring $\mathbb{Q}[c_i]$ is a finite-dimensional vector space over $\mathbb{Q}$, so is the ring

$$R_o = \mathbb{Q}[c_1, \ldots, c_n].$$

Let

$$R = R_o[\alpha].$$

If $\{v_i : 1 \le i \le m\}$ is a basis for R_o over $\mathbb{Q}$ then

$$\{v_i \alpha^j : 1 \le i \le m,\ 0 \le j < n\}$$

is a spanning set for R as a vector space over $\mathbb{Q}$. (This set is not necessarily a basis because α might satisfy a polynomial of degree lower than n.) Now condition (3) of the theorem shows that $\alpha \in \overline{\mathbb{Q}}$. $\square$

A loose analogy holds here:

> *Just as the finite-cover notion of* **compactness** *clarifies analytic phenomena by translating them into topological terms, so* **finite generation** *clarifies algebraic phenomena by translating them into structural terms.*

The slogan for the proof that the field of algebraic numbers is algebraically closed is *finitely generated over finitely generated is finitely generated*.

The ring of integers $\mathbb{Z}$ in the rational number field $\mathbb{Q}$ has a natural analogue in the field of algebraic numbers $\overline{\mathbb{Q}}$. To begin discussing this situation, note that any algebraic number satisfies a *unique* monic polynomial of lowest degree, because subtracting two distinct monic polynomials of the same degree gives a nonzero polynomial of lower degree, which can be rescaled to be monic. The unique monic polynomial of least degree satisfied by an algebra number α is called the **minimal polynomial** of α.

Definition 1.5. *An algebraic number α is an* **algebraic integer** *if its minimal polynomial has integer coefficients.*

The set of algebraic integers is denoted $\overline{\mathbb{Z}}$. Immediately from the definition, the algebraic integers in the rational number field $\mathbb{Q}$ are the usual integers $\mathbb{Z}$, now called the **rational integers**. Also in consequence of the definition, a small exercise shows that every algebraic number takes the form of an algebraic integer divided by a rational integer. Note, however, that the algebraic numbers

$$\omega = \frac{-1+i\sqrt{3}}{2} \quad \text{and} \quad \varphi = \frac{1+\sqrt{5}}{2}$$

are algebraic integers despite "having denominators"—indeed, they satisfy the polynomials x^2+x+1 and x^2-x-1 respectively. Similarly to Theorem 1.2 and its corollaries,

Theorem 1.6. *Let α be a complex number. The following conditions on α are equivalent:*

1. *α is an algebraic integer, i.e., $\alpha \in \overline{\mathbb{Z}}$,*
2. *The ring $\mathbb{Z}[\alpha]$ is finitely generated as an Abelian group,*
3. *α belongs to a ring R in $\mathbb{C}$ that is finitely generated as an Abelian group.*

Corollary 1.7. *The algebraic integers $\overline{\mathbb{Z}}$ form a ring.*

Corollary 1.8. *The algebraic integers form an* ***integrally closed*** *ring, meaning that every monic polynomial with coefficients in $\overline{\mathbb{Z}}$ factors down to linear terms over $\overline{\mathbb{Z}}$, i.e., its roots lie in $\overline{\mathbb{Z}}$.*

A vector space over $\mathbb{Q}$ is a $\mathbb{Q}$-module, and an Abelian group is a $\mathbb{Z}$-module; so conditions (3) in Theorems 1.2 and 1.6 can be made uniform, and conformal with parts (1) and (2) of their theorems, by phrasing them as, "α belongs to a ring R in $\mathbb{C}$ that is finitely generated as a $\mathbb{Q}$-module," and "... as a $\mathbb{Z}$-module."

2. Quadratic Reciprocity Revisited

We work in the ring $\overline{\mathbb{Z}}$ of algebraic integers, remembering at the end that an algebraic integer congruence between two rational integers is in fact a rational integer congruence. (Proof: If

$$a, b \in \mathbb{Z} \quad \text{and} \quad a = b \bmod n\overline{\mathbb{Z}},$$

then

$$\frac{b-a}{n} \in \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z},$$

so that

$$a = b \bmod n\mathbb{Z},$$

as desired.)

Let p be an odd prime. To evaluate the Legendre symbol $(2/p)$, introduce not the square root of unity but the eighth root of unity,

$$\zeta = \zeta_8 = e^{2\pi i/8} \in \overline{\mathbb{Z}}.$$

Because $\zeta^4 = -1$, also $\zeta^2 + \zeta^{-2} = 0$, and thus $(\zeta + \zeta^{-1})^2 = 2$. (This equality is also clear from the fact that $\zeta^{\pm 1} = (1 \pm i)/\sqrt{2}$, but the given derivaton uses only the fact that ζ is a primitive eighth root of unity, not its description as a complex number.) Further, a small calculation shows that working modulo $p\overline{\mathbb{Z}}$,

$$\begin{aligned}(\zeta + \zeta^{-1})^p &= \begin{cases} \zeta + \zeta^{-1} & \text{if } p = \pm 1 \bmod 8, \\ -(\zeta + \zeta^{-1}) & \text{if } p = \pm 3 \bmod 8. \end{cases} \\ &= (\zeta + \zeta^{-1})(-1)^{(p^2-1)/8}.\end{aligned}$$

Let

$$\tau = \zeta + \zeta^{-1},$$

and compute τ^{p+1} in two different ways. First, using Euler's law at the last step,

$$\tau^{p+1} = \tau^2(\tau^2)^{(p-1)/2} = 2 \cdot 2^{(p-1)/2} \overset{p\overline{\mathbb{Z}}}{\equiv} 2\left(\frac{2}{p}\right).$$

And second, quoting the small calculation,

$$\tau^{p+1} = \tau \cdot \tau^p \overset{p\overline{\mathbb{Z}}}{\equiv} \tau^2(-1)^{(p^2-1)/8} = 2(-1)^{(p^2-1)/8}.$$

Thus we have a congruence in $\overline{\mathbb{Z}}$,

$$2\left(\frac{2}{p}\right) = 2(-1)^{(p^2-1)/8} \bmod p\overline{\mathbb{Z}},$$

but because both quantities are rational integers we may view the congruence as being set in $\mathbb{Z}$. Because p is odd, we may cancel the 2's,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \bmod p\mathbb{Z},$$

and again because p is odd and because the integers on each side of the congruence are ± 1, the integers must be equal,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

The proof of the main quadratic reciprocity law is similar. Let p and q be distinct odd primes. (In this argument, p and q will play roles respectively analogous to those played by 2 and p a moment ago.) Introduce the pth root of unity,

$$\zeta = \zeta_p = e^{2\pi i/p}.$$

The finite geometric sum formula gives

$$\sum_{a=1}^{p-1} \zeta^{at} = \begin{cases} p-1 & \text{if } t = 0 \bmod p, \\ \quad -1 & \text{if } t \neq 0 \bmod p. \end{cases}$$

Define the **Gauss sum**

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

(Yes, the Gauss sum seems to come out of nowhere. In fact it is a very easy case of a *Lagrange resolvent*.) Compute that the Gauss sum lets us express p in terms of pth roots of unity,

$$\begin{aligned}
\tau^2 &= \sum_{s,t} \left(\frac{s}{p}\right)\left(\frac{t}{p}\right) \zeta^{s+t} = \sum_{s,u} \left(\frac{s}{p}\right)\left(\frac{su}{p}\right) \zeta^{s(1+u)} = \sum_{u} \left(\frac{u}{p}\right) \sum_{s} \zeta^{s(1+u)} \\
&= -\sum_{u \neq -1} \left(\frac{u}{p}\right) + \left(\frac{-1}{p}\right)(p-1) = -\sum_{u} \left(\frac{u}{p}\right) + \left(\frac{-1}{p}\right) p \\
&= p^*, \quad \text{where } p^* \text{ denotes whichever of } \pm p \text{ is } 1 \bmod 4.
\end{aligned}$$

Now similarly to above, we compute τ^{q+1} in two ways. First, by Euler's Law,

$$\tau^{q+1} = \tau^2 (\tau^2)^{(q-1)/2} = p^* (p^*)^{(q-1)/2} \overset{q\overline{\mathbb{Z}}}{\equiv} p^* \left(\frac{p^*}{q}\right).$$

And second, noting for the second equality to follow that $(t/p)^q = (tq^2/p) = (tq/p)(q/p)$ with (q/p) independent of t,

$$\tau^{q+1} = \tau \cdot \tau^q \overset{q\overline{\mathbb{Z}}}{\equiv} \tau \sum_{t} \left(\frac{t}{p}\right)^q \zeta^{qt} = \tau \sum_{t} \left(\frac{qt}{p}\right) \zeta^{qt} \cdot \left(\frac{q}{p}\right) = \tau^2 \left(\frac{q}{p}\right) = p^* \left(\frac{q}{p}\right).$$

Thus we have a congruence in $\overline{\mathbb{Z}}$,

$$p^* \left(\frac{p^*}{q}\right) = p^* \left(\frac{q}{p}\right) \mod q\overline{\mathbb{Z}},$$

but because both quantities are rational integers we may view the congruence as being set in $\mathbb{Z}$. Because p and q are distinct, we may cancel the p^*'s,

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right) \mod q\mathbb{Z},$$

and because q is odd and because the integers on each side of the congruence are ± 1, the integers must be equal,

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

3. Sketch of a Modern Proof of Quadratic Reciprocity

Let p be an odd prime, let $\zeta = e^{2\pi i/p}$, and consider the cyclotomic number field

$$K = \mathbb{Q}(\zeta).$$

Its Galois group

$$G = \mathrm{Gal}(K/\mathbb{Q})$$

is naturally isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, the automorphism that takes ζ to ζ^m mapping to the residue class $m \bmod p$ for $m \in \{1, \dots, p-1\}$.

Because the Galois group is cyclic of even order, the cyclotomic field K has a unique quadratic subfield. To describe this field, let $p^* = (-1)^{(p-1)/2} p$; thus p^* is whichever of $\pm p$ equals 1 mod 4. We know that p^* is a square in K, the square of the Gauss sum τ. Consequently, the unique quadratic subfield of K is

$$F = \mathbb{Q}(\sqrt{p^*}).$$

Its Galois group

$$Q = \mathrm{Gal}(F/\mathbb{Q})$$

is naturally isomorphic to $\{\pm 1\}$, the nontrivial automorphism that takes $\sqrt{p^*}$ to $-\sqrt{p^*}$ mapping to -1. Summarizing so far, we have a commutative diagram in which the horizontal arrows are isomorphisms, so that the left vertical arrow (restriction of automorphisms) gives rise to the right vertical arrow,

$$\begin{tikzcd} G \arrow[r] \arrow[d] & (\mathbb{Z}/p\mathbb{Z})^\times \arrow[d] \\ Q \arrow[r] & \{\pm 1\}. \end{tikzcd}$$

Any odd prime $q \neq p$ is unramified in K, and so it has a unique Frobenius automorphism,

$$\mathrm{Frob}_{q,K} \in G,$$

whose action on the integers of K, written in exponential notation, is characterized by the condition

$$x^{\mathrm{Frob}_{q,K}} = x^q \bmod q\mathcal{O}_K, \quad x \in \mathcal{O}_K.$$

The Frobenius automorphism has no choice but to be

$$\mathrm{Frob}_{q,K} : \zeta \longmapsto \zeta^q.$$

The odd prime $q \neq p$ is also unramified in F, so that again it has a unique Frobenius automorphism, this time denoted

$$\mathrm{Frob}_{q,F} \in Q,$$

characterized by the condition

$$x^{\mathrm{Frob}_{q,F}} = x^q \bmod q\mathcal{O}_F, \quad x \in \mathcal{O}_F,$$

and (because $(p^*)^{(q-1)/2} = (p^*/q) \bmod q$, where (p^*/q) is the Legendre symbol) working out to

$$\mathrm{Frob}_{q,F} : \sqrt{p^*} \longmapsto (p^*/q)\sqrt{p^*}.$$

Finally, $\mathrm{Frob}_{q,F}$ is the restriction of $\mathrm{Frob}_{q,K}$ to F. So, in the commutative diagram we have

$$\begin{tikzcd} \mathrm{Frob}_{q,K} \arrow[r, mapsto] \arrow[d, mapsto] & q \bmod p \arrow[d, mapsto] \\ \mathrm{Frob}_{q,F} \arrow[r, mapsto] & (p^*/q). \end{tikzcd}$$

The right vertical arrow shows that:

As a function of q, (p^*/q) depends only on q mod p.

This is quadratic reciprocity. A less conceptual but more concrete variant of the punchline is that the map down the right side is $q \bmod p \longmapsto (q/p)$, and so the commutative diagram shows that $(p^*/q) = (q/p)$.

4. The Sign of the Quadratic Gauss Sum

Let p be an odd prime and let $p^* = (-1)^{(p-1)/2}p$; thus p^* is whichever of $\pm p$ equals 1 mod 4. Let $\zeta = e^{2\pi i/p}$ and let τ denote the quadratic Gauss sum modulo p,

$$\tau = \sum_{t=1}^{p-1} (t/p)\zeta^t.$$

We know that $\tau^2 = p^*$, so that

$$\tau = \begin{cases} \pm\sqrt{p} & \text{if } p = 1 \pmod 4, \\ \pm i\sqrt{p} & \text{if } p = 3 \pmod 4. \end{cases}$$

Ireland and Rosen narrate Gauss's original demonstration that in both cases the sign is "+", and their exposition is rewritten here. However, the sign is readily found by a Poisson summation argument, to be given in the next section, so the reader should feel free to skip to there absent the desire to see a more elementary argument.

The proof first establishes that a certain product equals $\sqrt{p}$ if $p = 1$ mod 4 and equals $i\sqrt{p}$ if $p = 3$ mod 4, and then it establishes that this product also equals the Gauss sum.

It is elementary that

$$\sum_{j=0}^{p-1} X^j = \prod_{j=1}^{p-1}(X - \zeta^j) = \prod_{j=1}^{(p-1)/2} (X - \zeta^j)(X - \zeta^{-j}).$$

But the product as written is overspecific in that the exponents of ζ need only to vary through any set of nonzero residue classes modulo p. The residue system that will help us here is the length-$(p-1)$ arithmetic progression of $2 \pmod 4$ numbers symmetrized about 0,

$$\pm(4\cdot 1 - 2),\ \pm(4\cdot 2 - 2),\ \pm(4\cdot 3 - 2),\ \cdots,\ \pm(4\cdot \tfrac{p-1}{2} - 2).$$

Thus

$$\sum_{j=0}^{p-1} X^j = \prod_{j=1}^{(p-1)/2} (X - \zeta^{4j-2})(X - \zeta^{-(4j-2)}).$$

Substitute $X = 1$ to get

$$\begin{aligned} p &= \prod_{j=1}^{(p-1)/2} (1 - \zeta^{4j-2})(1 - \zeta^{-(4j-2)}) \\ &= \prod_{j=1}^{(p-1)/2} (\zeta^{-(2j-1)} - \zeta^{2j-1})(\zeta^{2j-1} - \zeta^{-(2j-1)}), \end{aligned}$$

and so multiplying by $(-1)^{(p-1)/2}$ gives

$$p^* = \prod_{j=1}^{(p-1)/2} (\zeta^{2j-1} - \zeta^{-(2j-1)})^2.$$

It follows that

$$\prod_{j=1}^{(p-1)/2}(\zeta^{2j-1}-\zeta^{-(2j-1)}) = \begin{cases} \pm\sqrt{p} & \text{if } p=1 \pmod 4, \\ \pm i\sqrt{p} & \text{if } p=3 \pmod 4. \end{cases}$$

The jth multiplicand is

$$\zeta^{2j-1}-\zeta^{-(2j-1)} = 2i\sin(2\pi(2j-1)/p),$$

and the sine is positive for $0 < 2(2j-1)/p < 1$, or $1/2 < j < p/4+1/2$, or $1 \le j < p/4+1/2$; and similarly the sine is negative for $p/4+1/2 < j \le (p-1)/2$. If $p = 1 \pmod 4$ then the sine is positive for $j = 1, \cdots, (p-1)/4$, and so

$$\begin{aligned}\prod_{j=1}^{(p-1)/2}(\zeta^{2j-1}-\zeta^{-(2j-1)}) &= (\text{positive number}) \times i^{(p-1)/2}(-1)^{(p-1)/2-(p-1)/4} \\ &= (\text{positive number}) \times (-1)^{(p-1)/4}(-1)^{(p-1)/4},\end{aligned}$$

a positive number. If $p = 3 \pmod 4$ then the sine is positive for $j = 1, \cdots, (p+1)/4$, and so

$$\begin{aligned}\prod_{j=1}^{(p-1)/2}(\zeta^{2j-1}-\zeta^{-(2j-1)}) &= (\text{positive number}) \times i^{(p-1)/2}(-1)^{(p-1)/2-(p+1)/4} \\ &= (\text{positive number}) \times i(-1)^{(p-3)/4}(-1)^{(p-3)/4},\end{aligned}$$

a positive multiple of i. Thus both "$\pm$" signs are positive,

$$\prod_{j=1}^{(p-1)/2}(\zeta^{2j-1}-\zeta^{-(2j-1)}) = \begin{cases} \sqrt{p} & \text{if } p=1 \pmod 4, \\ i\sqrt{p} & \text{if } p=3 \pmod 4. \end{cases}$$

To complete the argument, we need to show that the Gauss sum τ equals the product $\prod_{j=1}^{(p-1)/2}(\zeta^{2j-1}-\zeta^{-(2j-1)})$ rather than its negative.

Let

$$\tau = \varepsilon \prod_{j=1}^{(p-1)/2}(\zeta^{2j-1}-\zeta^{-(2j-1)}),$$

where we know that $\varepsilon = \pm 1$ and we want to show that $\varepsilon = 1$. Consider the polynomial

$$f(X) = \sum_{t=1}^{p-1}(t/p)X^t - \varepsilon \prod_{j=1}^{(p-1)/2}(X^{2j-1}-X^{p-(2j-1)}).$$

Then $f(1) = 0$ and $f(\zeta) = 0$. So $f(X)$ is divisible by $X^p - 1$,

$$\sum_{t=1}^{p-1}(t/p)X^t - \varepsilon \prod_{j=1}^{(p-1)/2}(X^{2j-1}-X^{p-(2j-1)}) = (X^p-1)g(X).$$

Replace X by e^z to get

$$\sum_{t=1}^{p-1}(t/p)e^{tz} - \varepsilon \prod_{j=1}^{(p-1)/2}(e^{(2j-1)z}-e^{(p-(2j-1))z}) = (e^{pz}-1)g(e^z). \tag{1}$$

On the left side of (1), each multiplicand has constant term 0, so that the lowest exponent of z in the product is $(p-1)/2$, and each multiplicand has linear term $(4j-p-2)z$. Thus the overall coefficient of $z^{(p-1)/2}$ on the left side of (1) is

$$\frac{\sum_{t=1}^{p-1}(t/p)t^{(p-1)/2}}{((p-1)/2)!} - \varepsilon \prod_{j=1}^{(p-1)/2}(4j-p-2).$$

On the right side of (1), each coefficient of the power series expansion

$$e^{pz}-1=\sum_{n=1}^{\infty}\frac{p^n}{n!}z^n$$

has more powers of p in its numerator than in its denominator. Thus the coefficient of $z^{(p-1)/2}$ on the left side of (1) is 0 modulo p, and so after clearing a denominator we have

$$\sum_{t=1}^{p-1}(t/p)t^{(p-1)/2} \overset{p}{\equiv} \varepsilon((p-1)/2)!\prod_{j=1}^{(p-1)/2}(4j-2).$$

Working modulo p, and quoting Euler's Law and then Fermat's Little Theorem, the left side is

$$\sum_{t=1}^{p-1}(t/p)t^{(p-1)/2}=\sum_{t=1}^{p-1}t^{(p-1)/2}t^{(p-1)/2}=\sum_{t=1}^{p-1}t^{p-1}=\sum_{t=1}^{p-1}1=-1,$$

and the right side is

$$\begin{aligned}\varepsilon((p-1)/2)!\prod_{j=1}^{(p-1)/2}(4j-2) &= \varepsilon((p-1)/2)!2^{(p-1)/2}\prod_{j=1}^{(p-1)/2}(2j-1)\\ &= \varepsilon(2\cdot 4\cdots(p-1))(1\cdot 3\cdots(p-2))\\ &= \varepsilon(p-1)!\\ &= -\varepsilon \quad \text{by Wilson's Theorem.}\end{aligned}$$

So $\varepsilon=1$ and the argument is complete.

5. The Sign of the Quadratic Gauss Sum by Fourier Analysis

Let p be an odd prime and let $p^*=(-1)^{(p-1)/2}p$; thus p^* is whichever of $\pm p$ equals 1 mod 4. Let $e_p(x)=e^{2\pi ix/p}$ for $x\in\mathbb{R}$, and let τ denote the quadratic Gauss sum modulo p,

$$\tau=\sum_{t=1}^{p-1}(t/p)e_p(t).$$

We know that $\tau^2=p^*$, so that

$$\tau=\begin{cases}\pm\sqrt{p} & \text{if } p=1 \pmod 4,\\ \pm i\sqrt{p} & \text{if } p=3 \pmod 4.\end{cases}$$

We show again, using Fourier analysis this time, that in both cases the sign is "+".

Begin with the observations that (letting R stand for *residue* and N for *non-residue*)

$$\tau=\sum_{\mathrm{R}}e_p(\mathrm{R})-\sum_{\mathrm{N}}e_p(\mathrm{N}),$$

while by the finite geometric sum formula

$$0 = 1 + \sum_{\mathrm{R}} e_p(\mathrm{R}) + \sum_{\mathrm{N}} e_p(\mathrm{N}),$$

so that adding the previous two displays shows that the Gauss sum is

$$\tau = 1 + 2\sum_{\mathrm{R}} e_p(\mathrm{R}) = \sum_{n=0}^{p-1} e^{2\pi i n^2/p} = \sum_{n=0}^{p-1} e^{2\pi i p(n/p)^2}.$$

We will evaluate the more general sum associated to any positive integer N,

$$S_N = \sum_{n=0}^{N-1} e^{2\pi i N(n/N)^2}, \quad N \in \mathbb{Z}_{>0}.$$

The result, encompassing the sign of the Gauss sum, will be that

$$S_N = \sqrt{N}\cdot \begin{cases} 1+i & \text{if } N = 0 \bmod 4 \\ 1 & \text{if } N = 1 \bmod 4 \\ 0 & \text{if } N = 2 \bmod 4 \\ i & \text{if } N = 3 \bmod 4. \end{cases}$$

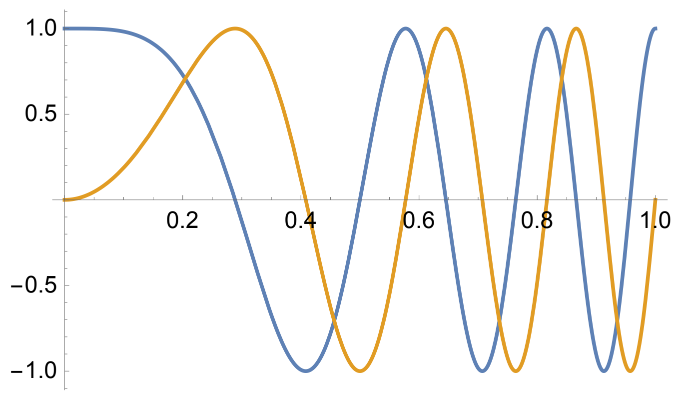

FIGURE 1. Real and imaginary parts of $f(x) = e^{2\pi i N x^2}$ for $N = 3$

The summands of S_N are values of the function

$$f : [0,1] \longrightarrow \mathbb{C}, \qquad f(x) = e^{2\pi i N x^2}$$

(see Figure 1). As will be explained below, the Fourier series of f converges pointwise to f even at 0 because $f(1) = f(0)$ and f is differentiable from the right at 0 and from the left at 1. Thus

$$\begin{aligned} S_N = \sum_{n=0}^{N-1} f(n/N) &= \sum_{n=0}^{N-1}\sum_{k\in\mathbb{Z}} \int_0^1 f(x)e^{2\pi i k x}\,\mathrm{d}x \cdot e^{-2\pi i k n/N} \\ &= \sum_{k\in\mathbb{Z}} \int_0^1 f(x)e^{2\pi i k x}\,\mathrm{d}x \cdot \sum_{n=0}^{N-1} e^{-2\pi i k n/N}. \end{aligned}$$

The inner sum is N if $k \in N\mathbb{Z}$ and 0 otherwise, so now

$$S_N = N \sum_{k \in \mathbb{Z}} \int_0^1 f(x) e^{2\pi i N k x} \,\mathrm{d}x = N \sum_{k \in \mathbb{Z}} \int_0^1 e^{2\pi i N (x^2 + kx)} \,\mathrm{d}x.$$

To analyze the kth summand, complete the square in the exponent, and then note that $e^{-2\pi i/4} = i^{-1}$ and that k^2 is 0 mod 4 for k even and is 1 mod 4 for k odd,

$$\begin{aligned} \int_0^1 e^{2\pi i N(x^2+kx)} \,\mathrm{d}x &= e^{-2\pi i N k^2/4} \int_0^1 e^{2\pi i N (x+k/2)^2} \,\mathrm{d}x \\ &= i^{-Nk^2} \int_{k/2}^{k/2+1} e^{2\pi i N x^2} \,\mathrm{d}x \\ &= \left\{ \begin{matrix} 1 & \text{if } k \text{ is even} \\ i^{-N} & \text{if } k \text{ is odd} \end{matrix} \right\} \int_{k/2}^{k/2+1} e^{2\pi i N x^2} \,\mathrm{d}x. \end{aligned}$$

As k varies through the even integers, the last integral in the previous display runs over $\mathbb{R}$, and similarly for the odd integers. Thus summing over the last expression in the previous display gives

$$S_N = N(1 + i^{-N}) \int_{\mathbb{R}} e^{2\pi i N x^2} \,\mathrm{d}x = \sqrt{N}(1 + i^{-N}) \int_{\mathbb{R}} e^{2\pi i x^2} \,\mathrm{d}x.$$

Note that the last integral $I = \int_{\mathbb{R}} e^{2\pi i x^2} \,\mathrm{d}x$ in the previous display is independent of N. In a moment we will show that I converges, perhaps surprisingly because its integrand does not go to 0 as x goes to $\pm\infty$. Granting the convergence, the formula $S_N = \sqrt{N}(1 + i^{-N})I$ for $N = 1$ is $1 = (1 - i)I$, giving $I = (1 + i)/2$. Thus the general value of S_N is

$$S_N = \sqrt{N}\, \frac{(1 + i^{-N})(1 + i)}{2}.$$

The casewise formula for S_N follows immediately.

The integral $I = \int_{\mathbb{R}} e^{2\pi i x^2} \,\mathrm{d}x$ converges because its integrand oscillates ever faster with unit amplitude as $|x|$ grows, making its value stabilize. To establish the convergence analytically, make a change of variable and then integrate by parts: for $0 < L \leq M$,

$$\begin{aligned} \int_L^M e^{2\pi i x^2} \,\mathrm{d}x &= \frac{1}{2} \int_{L^2}^{M^2} u^{-1/2} e^{2\pi i u} \,\mathrm{d}u \quad \text{where } u = x^2 \\ &= \frac{1}{4\pi i} \left(u^{-1/2} e^{2\pi i u} \Big|_{L^2}^{M^2} + \frac{1}{2} \int_{L^2}^{M^2} u^{-3/2} e^{2\pi i u} \,\mathrm{d}u \right), \end{aligned}$$

which is asymptotically of order L^{-1}.

Finally, to show the pointwise convergence of the Fourier series of f to f at 0, replace f by $f - f(0)$ and compute the Mth partial sum of the Fourier series at 0,

$$\begin{aligned} \sum_{k=-M}^{M} \int_0^1 f(x) e^{2\pi i k x} \,\mathrm{d}x &= \int_0^1 f(x) \sum_{k=-M}^{M} e^{2\pi i k x} \,\mathrm{d}x \\ &= \int_0^1 \frac{f(x)}{e^{2\pi i x} - 1} (e^{2\pi i (M+1) x} - e^{-2\pi i M x}) \,\mathrm{d}x. \end{aligned}$$

In the integrand, the term

$$\frac{f(x)}{e^{2\pi ix}-1}=\frac{f(x)}{x}\cdot\frac{x}{e^{2\pi ix}-1}$$

extends continuously at $x = 0$ to the right derivative $f'(0)$ times the reciprocal derivative $1/(2\pi i)$ of $e^{2\pi ix}$ at 0, and similarly it extends continuously at $x = 1$. Thus the integral goes to 0 as M grows, by the Riemann–Lebesgue Lemma.