

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 $(1 + \sqrt{5})/2$ 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,*

$$p(\alpha) = 0, \quad p(x) = x^n + c_1x^{n-1} + \cdots + c_n, \quad c_1, \dots, c_n \in \mathbf{Q}.$$

Every rational number r is algebraic since it satisfies the polynomial $x - r$, but not every algebraic number is rational, cf. the examples given just before the definition. E.g., $(1 + \sqrt{5})/2$ satisfies the polynomial $p(x) = x^2 - x - 1$. Every complex number expressible over \mathbf{Q} in radicals is algebraic, but not conversely.

The algebraic numbers form a field, denoted $\overline{\mathbf{Q}}$. 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., $\alpha \in \overline{\mathbf{Q}}$,
- (2) The ring $\mathbf{Q}[\alpha]$ is a finite-dimensional vector space over \mathbf{Q} ,
- (3) α belongs to a ring R in \mathbf{C} that is a finite-dimensional vector space over \mathbf{Q} .

Proof. (1) \implies (2): Let α satisfy the polynomial

$$x^n + c_1x^{n-1} + \cdots + c_n, \quad c_1, \dots, c_n \in \mathbf{Q}.$$

Then

$$\alpha^n = - \sum_{i=0}^{n-1} c_{n-i} \alpha^i,$$

so the complex vector space generated by the powers $\{1, \alpha, \dots, \alpha^{n-1}\}$ also contains α^n . And similarly,

$$\alpha^{n+1} = - \sum_{i=0}^{n-1} c_{n-i} \alpha^{i+1},$$

showing that α^{n+1} is in the space, and so on by induction for all higher powers of α .

(2) \implies (3) is immediate.

(3) \implies (1): Let the ring R have basis g_1, \dots, g_n as a vector space over \mathbf{Q} . Then multiplying each g_i by α gives a rational linear combination of the generators,

$$\alpha g_i = \sum_{j=1}^n c_{ij} g_j, \quad i = 1, \dots, n.$$

Letting g denote the column vector with entries g_i , this means that

$$\alpha g = M g, \quad M = [c_{ij}] \in \mathbf{Q}^{n \times n}.$$

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

Condition (3) in the theorem easily proves

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

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

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

as vector spaces over \mathbf{Q} . Let

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

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

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

Then $\alpha + \beta$ and $\alpha\beta$ belong to R , making them algebraic numbers by condition (3) of the theorem. If $\alpha \neq 0$ 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 relation $p(\alpha) = 0$ gives $\alpha \mid p(\alpha) - c_n = -c_n$, or

$$\alpha^{-1} = \frac{p(\alpha) - c_n}{-c_n \alpha} \in \mathbf{Q}[\alpha],$$

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

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 $\alpha \neq 0$. For example, let $\alpha = i$ and $\beta = \sqrt{2}$. Then

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

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 \mathbf{Q} . Then the condition

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

first eliminates U from the simultaneous conditions $g(U) = 0, T = U + V$, 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 \mathbf{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 \mathbf{Q} having $\alpha\beta$ as a root.

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

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

Proof. (Sketch.) Consider a monic polynomial

$$x^n + c_1x^{n-1} + \cdots + c_n, \quad c_i \in \overline{\mathbf{Q}},$$

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

$$R_o = \mathbf{Q}[c_1, \dots, c_n].$$

Let

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

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

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

is a spanning set for R as a vector space over \mathbf{Q} . (This set is not necessarily a basis since α might satisfy a polynomial of lower degree.) Now condition (3) of the theorem shows that $\alpha \in \overline{\mathbf{Q}}$. \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 *finite-generated over finitely-generated is finitely-generated*.

The ring of integers \mathbf{Z} in the rational number field \mathbf{Q} has a natural analogue in the field of algebraic numbers $\overline{\mathbf{Q}}$.

Definition 1.5. *A complex number α is an **algebraic integer** if α satisfies some monic polynomial with integer coefficients.*

The set of algebraic integers is denoted $\overline{\mathbf{Z}}$. Immediately from the definition, the algebraic integers in the rational number field \mathbf{Q} are the usual integers \mathbf{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

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

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., $\alpha \in \overline{\mathbf{Z}}$,
- (2) The ring $\mathbf{Z}[\alpha]$ is finitely generated as an Abelian group,
- (3) α belongs to a ring R in \mathbf{C} that is finitely generated as an Abelian group.

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

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

2. QUADRATIC RECIPROCITY REVISITED

We work in the ring $\overline{\mathbf{Z}}$ 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

$$a, b \in \mathbf{Z} \quad \text{and} \quad a = b \pmod{p\overline{\mathbf{Z}}},$$

then

$$\frac{b-a}{p} \in \mathbf{Q} \cap \overline{\mathbf{Z}} = \mathbf{Z},$$

so that

$$a = b \pmod{p\mathbf{Z}},$$

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,

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

Since $\zeta^4 = -1$, consequently $\zeta^2 + \zeta^{-2} = 0$, and thus $(\zeta + \zeta^{-1})^2 = 2$. Also, a small calculation shows that working modulo $p\overline{\mathbf{Z}}$,

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

Let

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

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

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

And second, quoting the small calculation,

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

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

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

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

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

and again since p is odd and since 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 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 p th root of unity,

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

The finite geometric sum formula gives

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

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 *Fourier transform*.) Compute that

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

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

$$\tau^{q+1} = \tau^2 (\tau^2)^{(q-1)/2} = p^* (p^*)^{(q-1)/2} \stackrel{q\bar{\mathbf{Z}}}{\equiv} p^* \left(\frac{p^*}{q}\right).$$

And second,

$$\tau^{q+1} = \tau \cdot \tau^q \stackrel{q\bar{\mathbf{Z}}}{\equiv} \tau \sum_t \left(\frac{t}{p}\right)^q \zeta^{qt} = \tau \left(\frac{q}{p}\right) \sum_t \left(\frac{qt}{p}\right)^q \zeta^{qt} = \tau^2 \left(\frac{q}{p}\right) = p^* \left(\frac{q}{p}\right).$$

Thus we have a congruence in $\bar{\mathbf{Z}}$,

$$p^* \left(\frac{p^*}{q}\right) = p^* \left(\frac{q}{p}\right) \pmod{q\bar{\mathbf{Z}}},$$

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

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

and since q is odd and since 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

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

Its Galois group

$$G = \text{Gal}(K/\mathbf{Q})$$

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

Since 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. A short calculation shows that p^* is a square in K (forgetting that we already know that p^* is the square of the Gauss sum τ):

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

and so substituting $X = 1$ gives

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

But $\zeta = (\zeta^{(p+1)/2})^2$ is a square, and so the calculation has indeed shown that p^* is a square in K as desired. Consequently, the unique quadratic subfield of K is

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

Its Galois group

$$Q = \text{Gal}(F/\mathbf{Q})$$

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,

$$\begin{array}{ccc} G & \longrightarrow & (\mathbf{Z}/p\mathbf{Z})^\times \\ \downarrow & & \downarrow \\ Q & \longrightarrow & \{\pm 1\}. \end{array}$$

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

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

whose action on the integers of K is characterized by the condition

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

The Frobenius automorphism has no choice but to be

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

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

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

characterized by the condition

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

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

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

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

$$\begin{array}{ccc} \text{Frob}_{q,K} & \longmapsto & q \pmod{p} \\ \downarrow & & \downarrow \\ \text{Frob}_{q,F} & \longmapsto & (p^*/q). \end{array}$$

The right vertical arrow shows that:

As a function of q , (p^/q) depends only on $q \pmod{p}$.*

This is quadratic reciprocity. (A variant of the punchline is that the map down the right side is $q \pmod{p} \mapsto (q/p)$, 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

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

We now show, following Ireland and Rosen, that in both cases the sign is “+”. The proof establishes first that a certain product equals \sqrt{p} if $p \equiv 1 \pmod{4}$ and equals $i\sqrt{p}$ if $p \equiv 3 \pmod{4}$, and then it establishes that the 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,

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

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

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

It follows that

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

The j th 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 $1/2 < j < p/4 + 1/2$, and similarly the sine is negative for $p/4 + 1/2 < j < (p+1)/2$. If $p \equiv 1 \pmod{4}$ then the sine is positive for $j = 1, \dots, (p-1)/4$, 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 $p \equiv 3 \pmod{4}$ then the sine is positive for $j = 1, \dots, (p+1)/4$, 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,

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

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

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

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

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

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

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

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 $x \in \mathbf{R}$, 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

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

We show again, using Fourier analysis, that in both cases the sign is “+”.

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

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

while by the finite geometric sum formula

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

so that in fact the Gauss sum is

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

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

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

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

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

Define

$$f : \mathbf{R} \longrightarrow \mathbf{C}, \quad f(x) = e^{2\pi i x^2/N}.$$

For any integer n , let

$$f_n = f \text{ restricted to } [n, n+1) \text{ and then extended periodically to } \mathbf{R}.$$

Note that f_n is smooth except for its jump-discontinuities at \mathbf{Z} . Thus by Fourier analysis, the average of $f(n)$ and $f(n+1)$ is the Fourier series of f_n evaluated at zero,

$$\frac{1}{2}(f(n) + f(n+1)) = \sum_{k \in \mathbf{Z}} \int_0^1 f_n(x) e^{2\pi i k x} dx = \sum_{k \in \mathbf{Z}} \int_n^{n+1} f(x) e^{2\pi i k x} dx.$$

Note that the sum to be evaluated meshes tidily with the previous display,

$$\begin{aligned}
 S_N &= \sum_{n=0}^{N-1} \frac{1}{2}(f(n) + f(n+1)) \\
 &= \sum_{n=0}^{N-1} \sum_{k \in \mathbf{Z}} \int_n^{n+1} f(x) e^{2\pi i k x} dx \\
 &= \sum_{k \in \mathbf{Z}} \sum_{n=0}^{N-1} \int_n^{n+1} f(x) e^{2\pi i k x} dx \\
 &= \sum_{k \in \mathbf{Z}} \int_0^N f(x) e^{2\pi i k x} dx.
 \end{aligned}$$

To analyze the k th integral, complete the square in the exponent,

$$\begin{aligned}
 \int_0^N f(x) e^{2\pi i k x} dx &= \int_0^N e^{2\pi i(x^2/N + kx)} dx \\
 &= N \int_0^1 e^{2\pi i N(x^2 + kx)} dx \\
 &= N e^{-2\pi i N k^2/4} \int_0^1 e^{2\pi i N(x^2 + kx + k^2/4)} dx \\
 &= N e^{-2\pi i N k^2/4} \int_0^1 e^{2\pi i N(x+k/2)^2} dx.
 \end{aligned}$$

But $e^{-2\pi i N k^2/4} = (e^{\pi i/2})^{-N k^2}$, and k^2 is 0 mod 4 for k even and is 1 mod 4 for k odd, so that the calculation has shown that the k th integral is

$$\int_0^N f(x) e^{2\pi i k x} dx = \begin{cases} N \int_{k/2}^{k/2+1} e^{2\pi i N x^2} dx & \text{if } k = 0 \text{ mod } 2, \\ N i^{-N} \int_{k/2}^{k/2+1} e^{2\pi i N x^2} dx & \text{if } k = 1 \text{ mod } 2. \end{cases}$$

Thus the sum of the integrals works out to a constant multiple of a normalized integral,

$$\begin{aligned}
 S_N &= \sum_{k \in \mathbf{Z}} \int_0^N f(x) e^{2\pi i k x} dx \\
 &= N(1 + i^{-N}) \sum_{k \in \mathbf{Z}} \int_{k/2}^{k/2+1} e^{2\pi i N x^2} dx \\
 &= N(1 + i^{-N}) \int_{\mathbf{R}} e^{2\pi i N x^2} dx \\
 &= \sqrt{N}(1 + i^{-N}) \int_{\mathbf{R}} e^{2\pi i x^2} dx.
 \end{aligned}$$

In the relation

$$S_N = \sqrt{N}(1 + i^{-N}) \int_{\mathbf{R}} e^{2\pi i x^2} dx,$$

the integral converges robustly because a change of variable shows that the tail of the rapidly-increasing oscillation is the tail of a dampened uniform oscillation.

Specifically, for $0 \leq L \leq M$,

$$\int_L^M e^{2\pi i x^2} dx = \frac{1}{2} \int_{L^2}^{M^2} x^{-1/2} e^{2\pi i x} dx,$$

and asymptotically the right side integral is L^{-1} . (This can be seen via integration by parts or by thinking about the dampened cosine and sine.) The integral is also visibly independent of N , so we may evaluate it by setting $N = 1$. The result is

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

The casewise formula for S_N follows immediately.