

Quadratic number fields, with $\mathbb{Q}(\sqrt{-3})$ worked out in detail

Claude Opus 5.5

at the behest of Michael O. Rubinstein

Abstract

Working notes. Section 1 summarizes the arithmetic of quadratic fields: rings of integers, units, ideals and class groups, the splitting of rational primes, and the factorization $\zeta_K(s) = \zeta(s)L(s, \chi_D)$. Section 2 works out $K = \mathbb{Q}(\sqrt{-3})$ and its ring of integers $\mathbb{Z}[\omega]$ (the Eisenstein integers) in full, with complete elementary proofs. It describes the ideals of $\mathbb{Z}[\omega]$ as lattices, with figures, and it covers primary elements in the convention $\alpha \equiv 1 \pmod{3}$ used by the OpenAI papers on the quasi-Riemann hypothesis. Section 3 treats the quadratic, cubic and sextic residue symbols on $\mathbb{Z}[\omega]$, cubic reciprocity, and cubic Gauss and Jacobi sums, with the signs in that convention. Section 4 treats additive characters, Gauss sums and Poisson summation over $\mathbb{Z}[\omega]$, and Section 5 the cubic theta function of Kubota and Patterson, both as they are used in the 11/12 argument. Section 6 has tables of how the rational primes below 100 factor, of the primary elements of norm at most 100, and of cubic and sextic residue symbols. Every numerical entry was generated by a computer program, which also checked numerically, over a range of cases, the identities stated here for $\mathbb{Z}[\omega]$.

$\mathbb{Q}(\sqrt{-3})$ at a glance	
Field	$K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega), \quad \omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$
Integers	$\mathcal{O}_K = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}, \quad \omega^2 + \omega + 1 = 0$
Discriminant	$D = -3$
Norm, trace	$N(a + b\omega) = a^2 - ab + b^2, \quad \text{Tr}(a + b\omega) = 2a - b$
Units	$\pm 1, \pm\omega, \pm\omega^2$ (the sixth roots of unity, $w = 6$)
Class number	$h = 1$ ($\mathbb{Z}[\omega]$ is Euclidean)
Ramified prime	$3 = -\omega^2\lambda^2, \quad \lambda = 1 - \omega, \quad N\lambda = 3$
Splitting	$p \equiv 1 \pmod{3}$: $p = \pi\bar{\pi}$ splits; $p \equiv 2 \pmod{3}$: p stays prime
Primary	$\alpha \equiv 1 \pmod{3}$, i.e. $a \equiv 1, b \equiv 0 \pmod{3}$
Zeta function	$\zeta_K(s) = \zeta(s)L(s, \chi_{-3}), \quad \chi_{-3}(n) = \left(\frac{n}{3}\right)$

Contents

1	Quadratic fields in general	2
1.1	Fields, norm and trace	2
1.2	The ring of integers	3
1.3	Units	3

1.4	Ideals and the class group	3
1.5	How rational primes factor	4
1.6	The Dedekind zeta function and the class number formula	4
2	The field $\mathbb{Q}(\sqrt{-3})$ and the Eisenstein integers	5
2.1	The ring $\mathbb{Z}[\omega]$	5
2.2	Geometry	5
2.3	Units	6
2.4	Division with remainder	6
2.5	The prime λ and residues modulo 3	7
2.6	Primes of $\mathbb{Z}[\omega]$ and the factorization of rational primes	7
2.7	Primary elements	8
2.8	Ideals of $\mathbb{Z}[\omega]$ as lattices	9
2.9	Counting, and the zeta function of K	11
2.10	Characters on $\mathbb{Z}[\omega]$	12
3	Residue symbols on $\mathbb{Z}[\omega]$	13
3.1	Definitions	13
3.2	Units and rational integers	14
3.3	Cubic reciprocity	14
3.4	Cubic Gauss and Jacobi sums	15
3.5	The sextic symbol in examples	16
4	Poisson summation over $\mathbb{Z}[\omega]$	16
4.1	Additive characters and duality	17
4.2	Gauss sums	18
4.3	The Poisson summation formula for $\mathbb{Z}[\omega]$	19
4.4	Poisson summation with a character	20
4.5	How the 11/12 paper uses Poisson summation	20
5	The cubic theta function of Kubota and Patterson	21
5.1	Hyperbolic three-space	22
5.2	The Kubota character	22
5.3	The theorem of Kubota and Patterson	23
5.4	The cubic Gauss sums and the theta coefficients	24
5.5	How the 11/12 paper uses the theta function	25
6	Tables	28

1 Quadratic fields in general

1.1 Fields, norm and trace

Every quadratic field is $K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ for a unique squarefree integer $d \neq 0, 1$. It is *imaginary* if $d < 0$ and *real* if $d > 0$. The nontrivial automorphism is $\sigma(\sqrt{d}) = -\sqrt{d}$ (complex conjugation when $d < 0$), and for $x \in K$

$$\mathrm{Tr}x = x + \sigma x, \quad \mathrm{N}x = x \sigma x; \quad \mathrm{Tr}(a + b\sqrt{d}) = 2a, \quad \mathrm{N}(a + b\sqrt{d}) = a^2 - db^2. \quad (1.1)$$

The norm is multiplicative. Each $x \in K \setminus \mathbb{Q}$ is a root of $X^2 - (\mathrm{Tr}x)X + \mathrm{N}x$.

1.2 The ring of integers

The ring of integers $\mathcal{O}_K$ is the set of $x \in K$ that are roots of a monic polynomial in $\mathbb{Z}[X]$. For $x \notin \mathbb{Q}$ this means that $\text{Tr}x$ and $\text{N}x$ are integers.

Theorem 1. $\mathcal{O}_K = \mathbb{Z}[\theta] = \{m + n\theta : m, n \in \mathbb{Z}\}$, where

$$\theta = \sqrt{d} \quad \text{if } d \equiv 2, 3 \pmod{4}, \quad \theta = \frac{1 + \sqrt{d}}{2} \quad \text{if } d \equiv 1 \pmod{4}. \quad (1.2)$$

Proof. Let $x = a + b\sqrt{d}$ have $A = 2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$. Then $A^2 - d(2b)^2 \in 4\mathbb{Z}$, so $d(2b)^2 \in \mathbb{Z}$. Since d is squarefree, $B = 2b \in \mathbb{Z}$: if $2b = u/v$ in lowest terms, then $v^2 \mid d$, so $v = 1$. Moreover $A^2 \equiv dB^2 \pmod{4}$, and squares are 0 or 1 modulo 4. If $d \equiv 2, 3 \pmod{4}$, then B odd would make $dB^2 \equiv 2, 3$, which is impossible. So B is even, then A is even, and $x \in \mathbb{Z}[\sqrt{d}]$. If $d \equiv 1 \pmod{4}$, the condition is exactly $A \equiv B \pmod{2}$, i.e. $x = \frac{A-B}{2} + B \frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Conversely $\sqrt{d}$ is integral, and when $d \equiv 1 \pmod{4}$ so is $\theta = \frac{1+\sqrt{d}}{2}$, a root of $X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X]$. $\square$

The *discriminant* is $D = D_K = (\theta - \sigma\theta)^2$, that is,

$$D = d \quad (d \equiv 1 \pmod{4}), \quad D = 4d \quad (d \equiv 2, 3 \pmod{4}). \quad (1.3)$$

Uniformly, $\mathcal{O}_K = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$. For imaginary K , $\mathcal{O}_K$ is a lattice in $\mathbb{C}$ with covolume (the area of a fundamental parallelogram) $\sqrt{|D|}/2$.

1.3 Units

If $d < 0$ then $\text{N}x = |x|^2$, and the units are the elements of norm 1. There are only finitely many. The unit group is $\{\pm 1\}$ except for $d = -1$ ($\pm 1, \pm i$; $w = 4$) and $d = -3$ (the sixth roots of unity; $w = 6$). We write $w = w_K$ for the number of units.

If $d > 0$, Dirichlet's unit theorem gives $\mathcal{O}_K^\times = \{\pm \varepsilon^n : n \in \mathbb{Z}\}$ for a *fundamental unit* $\varepsilon > 1$, with $\text{N}\varepsilon = \pm 1$. Examples: $\varepsilon = 1 + \sqrt{2}$ (norm -1), $2 + \sqrt{3}$ (norm $+1$), and $\frac{1+\sqrt{5}}{2}$ (norm -1).

1.4 Ideals and the class group

$\mathcal{O}_K$ is a Dedekind domain: every nonzero ideal factors uniquely as a product of prime ideals. Each nonzero prime ideal $\mathfrak{p}$ contains exactly one rational prime p . The *norm* $\text{N}\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}|$ is multiplicative, $\text{N}(x\mathcal{O}_K) = |\text{N}x|$, and $\text{N}\mathfrak{p}$ is p or p^2 . The ideal classes (nonzero fractional ideals modulo principal ones) form a finite group, the class group, whose order is the class number $h = h_K$. We have

$$\mathcal{O}_K \text{ is a PID} \iff \mathcal{O}_K \text{ is a UFD} \iff h_K = 1. \quad (1.4)$$

For example, in $\mathbb{Z}[\sqrt{-5}]$ (where $h = 2$), $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two factorizations into irreducibles that are not associates. As ideals both become

$$(6) = \mathfrak{p}_2^2 \mathfrak{p}_3 \mathfrak{p}_3', \quad \mathfrak{p}_2 = (2, 1 + \sqrt{-5}), \quad \mathfrak{p}_3 = (3, 1 + \sqrt{-5}), \quad \mathfrak{p}_3' = (3, 1 - \sqrt{-5}), \quad (1.5)$$

with $(2) = \mathfrak{p}_2^2$, $(3) = \mathfrak{p}_3 \mathfrak{p}_3'$ and $(1 \pm \sqrt{-5}) = \mathfrak{p}_2 \mathfrak{p}_3$ or $\mathfrak{p}_2 \mathfrak{p}_3'$. The imaginary quadratic fields with $h = 1$ are exactly those with

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163 \quad (1.6)$$

(Heegner, Baker, Stark; see [1]).

1.5 How rational primes factor

For a fundamental discriminant D , the *Kronecker symbol* $\chi_D(n) = \left(\frac{D}{n}\right)$ is defined as follows:

- at odd primes p it is the Legendre symbol $\left(\frac{D}{p}\right)$;
- at $p = 2$ it is 0 if D is even, 1 if $D \equiv 1 \pmod{8}$, and -1 if $D \equiv 5 \pmod{8}$;
- it is extended completely multiplicatively.

It is a primitive real Dirichlet character modulo $|D|$, with $\chi_D(-1) = \text{sign } D$.

Theorem 2. *Let p be a prime. Then*

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}\bar{\mathfrak{p}}, & \mathfrak{p} \neq \bar{\mathfrak{p}}, & N\mathfrak{p} = p & \text{(split) if } \chi_D(p) = 1, \\ p\mathcal{O}_K & \text{prime, } & N = p^2 & \text{(inert) if } \chi_D(p) = -1, \\ \mathfrak{p}^2, & N\mathfrak{p} = p & & \text{(ramified) if } \chi_D(p) = 0, \text{ i.e. } p \mid D. \end{cases} \quad (1.7)$$

Sketch. Let f be the minimal polynomial of θ in Theorem 1; its discriminant is D . Then $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[X]/(\bar{f})$ (Dedekind–Kummer). If $\bar{f}$ has two distinct roots $r \neq s$ in $\mathbb{F}_p$, then p splits, with $\mathfrak{p} = (p, \theta - r)$ and $\bar{\mathfrak{p}} = (p, \theta - s)$. If $\bar{f}$ is irreducible, p is inert. If $\bar{f} = (X - r)^2$, then p ramifies, with $\mathfrak{p} = (p, \theta - r)$. For odd p these three cases occur exactly when D is a nonzero square, a nonsquare, or zero modulo p . For $p = 2$ and $d \equiv 1 \pmod{4}$, $\bar{f} = X^2 + X + \frac{1-d}{4}$ splits if $d \equiv 1 \pmod{8}$ and is irreducible if $d \equiv 5 \pmod{8}$. For $p = 2$ and $d \equiv 2, 3 \pmod{4}$, $\bar{f} = X^2 - d$ is X^2 or $(X - 1)^2$ modulo 2, so 2 ramifies, in agreement with $2 \mid D$. $\square$

Since χ_D is periodic modulo $|D|$, *whether p splits depends only on p modulo $|D|$* . This is one form of quadratic reciprocity.

d	D	$\mathcal{O}_K$	units	h	ramified	p splits iff
-1	-4	$\mathbb{Z}[i]$	$\pm 1, \pm i$	1	2	$p \equiv 1 \pmod{4}$
-2	-8	$\mathbb{Z}[\sqrt{-2}]$	± 1	1	2	$p \equiv 1, 3 \pmod{8}$
-3	-3	$\mathbb{Z}[\omega]$	$\pm 1, \pm\omega, \pm\omega^2$	1	3	$p \equiv 1 \pmod{3}$
-5	-20	$\mathbb{Z}[\sqrt{-5}]$	± 1	2	2, 5	$p \equiv 1, 3, 7, 9 \pmod{20}$
-7	-7	$\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$	± 1	1	7	$p \equiv 1, 2, 4 \pmod{7}$
-23	-23	$\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$	± 1	3	23	p a nonzero square mod 23
2	8	$\mathbb{Z}[\sqrt{2}]$	$\pm(1 + \sqrt{2})^n$	1	2	$p \equiv \pm 1 \pmod{8}$
3	12	$\mathbb{Z}[\sqrt{3}]$	$\pm(2 + \sqrt{3})^n$	1	2, 3	$p \equiv \pm 1 \pmod{12}$
5	5	$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$	$\pm\left(\frac{1+\sqrt{5}}{2}\right)^n$	1	5	$p \equiv \pm 1 \pmod{5}$

1.6 The Dedekind zeta function and the class number formula

For $\Re s > 1$ put $\zeta_K(s) = \sum_{\mathfrak{a} \neq 0} N\mathfrak{a}^{-s} = \prod_p (1 - N\mathfrak{p}^{-s})^{-1}$.

Theorem 3. $\zeta_K(s) = \zeta(s)L(s, \chi_D)$. *Equivalently, the number of ideals of norm n is $\sum_{m \mid n} \chi_D(m)$.*

Proof. Compare Euler factors at each p using Theorem 2. Split: $(1 - p^{-s})^{-2}$. Inert: $(1 - p^{-2s})^{-1} = (1 - p^{-s})^{-1}(1 + p^{-s})^{-1}$. Ramified: $(1 - p^{-s})^{-1}$. In each case this is $(1 - p^{-s})^{-1}(1 - \chi_D(p)p^{-s})^{-1}$. $\square$

Thus ζ_K has a simple pole at $s = 1$ with residue $L(1, \chi_D)$, and Dirichlet's class number formula [3, Ch. 6] reads

$$L(1, \chi_D) = \frac{2\pi h}{w\sqrt{|D|}} \quad (D < 0), \quad L(1, \chi_D) = \frac{2h \log \varepsilon}{\sqrt{D}} \quad (D > 0). \quad (1.8)$$

For $D < 0$ there is also the finite formula $h = -\frac{w}{2|D|} \sum_{a=1}^{|D|} a \chi_D(a)$; for $D = -20$ it gives $-\frac{2}{40}((1 + 3 + 7 + 9) - (11 + 13 + 17 + 19)) = 2$.

Binary quadratic forms. For $D < 0$, ideal classes correspond to $\mathrm{SL}_2(\mathbb{Z})$ -classes of primitive positive definite forms $ax^2 + bxy + cy^2$ with $b^2 - 4ac = D$. The class of $\mathcal{O}_K$ corresponds to the principal form $x^2 + xy + \frac{1-D}{4}y^2$ or $x^2 - \frac{D}{4}y^2$. When $h = 1$ the principal form represents each $n \geq 1$ exactly $w \sum_{m|n} \chi_D(m)$ times (counting all $(x, y) \in \mathbb{Z}^2$). Each element of norm n gives a representation, and there are w generators for each ideal.

2 The field $\mathbb{Q}(\sqrt{-3})$ and the Eisenstein integers

2.1 The ring $\mathbb{Z}[\omega]$

Here $d = -3 \equiv 1 \pmod{4}$, so $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and $D = -3$. Put

$$\omega = \frac{-1 + \sqrt{-3}}{2} = e^{2\pi i/3}. \quad (2.1)$$

Since $\frac{1+\sqrt{-3}}{2} = 1 + \omega$, we have $\mathcal{O}_K = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, the *Eisenstein integers*. The field is $K = \mathbb{Q}(\omega)$, the third cyclotomic field. The basic identities are

$$\omega^2 + \omega + 1 = 0, \quad \omega^3 = 1, \quad \bar{\omega} = \omega^2 = -1 - \omega, \quad \sqrt{-3} = 1 + 2\omega = \omega - \omega^2, \quad 1 + \omega = -\omega^2 = e^{\pi i/3}. \quad (2.2)$$

For $\alpha = a + b\omega$ and $\beta = c + d\omega$:

$$\begin{aligned} \alpha\beta &= (ac - bd) + (ad + bc - bd)\omega, & \bar{\alpha} &= (a - b) - b\omega, \\ N\alpha &= \alpha\bar{\alpha} = a^2 - ab + b^2, & \mathrm{Tr}\alpha &= \alpha + \bar{\alpha} = 2a - b, \\ 4N\alpha &= (2a - b)^2 + 3b^2, & \alpha &= (a - \frac{b}{2}) + \frac{b}{2}\sqrt{-3}. \end{aligned} \quad (2.3)$$

The last identity gives $N\alpha = x^2 + 3y^2$ with $x = a - \frac{b}{2}$ and $y = \frac{b}{2}$. Also $\omega(a + b\omega) = -b + (a - b)\omega$, which is rotation by 120° . Finally $\beta \mid \alpha$ if and only if both coordinates of $\alpha\bar{\beta}$ are divisible by $N\beta$, since $\alpha/\beta = \alpha\bar{\beta}/N\beta$.

2.2 Geometry

In $\mathbb{C} = \mathbb{R}^2$, $\mathbb{Z}[\omega]$ is the hexagonal (triangular) lattice spanned by 1 and ω (Figure 1). A fundamental parallelogram has area $\Im\omega = \sqrt{3}/2 = \sqrt{|D|}/2$. Every lattice point has six nearest neighbours at distance 1; around 0 they are the six units. Counting lattice points in a disc gives

$$\#\{\alpha \in \mathbb{Z}[\omega] : N\alpha \leq X\} = \frac{\pi X}{\sqrt{3}/2} + O(\sqrt{X}) = \frac{2\pi}{\sqrt{3}}X + O(\sqrt{X}). \quad (2.4)$$

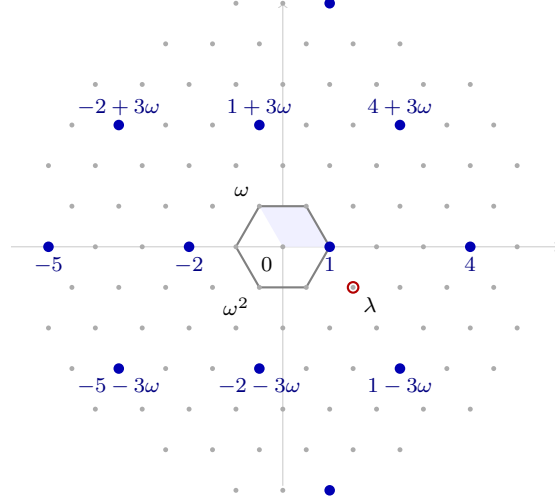


Figure 1: The Eisenstein integers $a + b\omega$, plotted at $(a - \frac{b}{2}, \frac{\sqrt{3}}{2}b)$. The six units form the grey hexagon, the shaded parallelogram is a fundamental domain, and $\lambda = 1 - \omega$ is circled. The large dots are the *primary* elements, those $\equiv 1 \pmod{3}$. They form the translated sublattice $1 + 3\mathbb{Z}[\omega]$ (one point in nine), and each nonzero ideal prime to 3 has exactly one of them as a generator.

2.3 Units

Proposition 4. $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\} = \langle \zeta \rangle$, where $\zeta = 1 + \omega = -\omega^2 = e^{\pi i/3}$. This is cyclic of order 6.

Proof. $N(a + b\omega) = 1$ means $(2a - b)^2 + 3b^2 = 4$, so $|b| \leq 1$. If $b = 0$ then $a = \pm 1$; if $b = 1$ then $a \in \{0, 1\}$, giving $\omega, 1 + \omega$; if $b = -1$ then $a \in \{0, -1\}$, giving $-\omega, -1 - \omega$. $\square$

2.4 Division with remainder

Proposition 5. For $\alpha, \beta \in \mathbb{Z}[\omega]$ with $\beta \neq 0$ there are $q, r \in \mathbb{Z}[\omega]$ with $\alpha = q\beta + r$ and $Nr \leq \frac{3}{4}N\beta$. Hence $\mathbb{Z}[\omega]$ is Euclidean, so it is a PID and a UFD, and $h = 1$.

Proof. Write $\alpha/\beta = s + t\omega$ with $s, t \in \mathbb{Q}$, and choose $m, n \in \mathbb{Z}$ with $|s - m|, |t - n| \leq \frac{1}{2}$. Put $q = m + n\omega$. With $u = s - m$ and $v = t - n$, $N(\alpha/\beta - q) = u^2 - uv + v^2 \leq u^2 + |u||v| + v^2 \leq \frac{3}{4}$. So $r = \alpha - q\beta$ has $Nr \leq \frac{3}{4}N\beta$. $\square$

(The hexagonal geometry gives the sharp constant $\frac{1}{3}$: every point of $\mathbb{C}$ lies within $1/\sqrt{3}$ of the lattice.)

Example 6 (Finding a prime of norm 61). Since $13^2 + 13 + 1 = 183 = 3 \cdot 61$, $r = 13$ is a root of $x^2 + x + 1$ modulo 61, and $\gcd(61, 13 - \omega)$ is a prime above 61. We have $\frac{61}{13 - \omega} = \frac{61(13 - \bar{\omega})}{183} = \frac{14 + \omega}{3}$, which rounds to $q = 5$. The Euclidean algorithm runs

$$61 = 5(13 - \omega) + (-4 + 5\omega), \quad 13 - \omega = (-2 - \omega)(-4 + 5\omega) + 0. \quad (2.5)$$

So $\gcd(61, 13 - \omega) = -4 + 5\omega$, of norm $16 + 20 + 25 = 61$. Its primary associate (§2.7) is $\omega(-4 + 5\omega) = -5 - 9\omega$, and $61 = (-5 - 9\omega)(4 + 9\omega)$. (The cofactor $-2 - \omega = \omega^2\lambda$ has norm 3.)

2.5 The prime λ and residues modulo 3

Put $\lambda = 1 - \omega$, so $N\lambda = 3$. Then

$$\lambda^2 = -3\omega, \quad 3 = -\omega^2\lambda^2, \quad \bar{\lambda} = 1 - \omega^2 = -\omega^2\lambda, \quad \sqrt{-3} = \omega\lambda, \quad (2.6)$$

so $(3) = (\lambda)^2$: the prime 3 ramifies. Since $\omega \equiv 1 \pmod{\lambda}$, we have $a + b\omega \equiv a + b \pmod{\lambda}$. Hence

$$\mathbb{Z}[\omega]/\lambda \cong \mathbb{F}_3 = \{0, 1, -1\}, \quad \lambda \mid a + b\omega \iff 3 \mid a + b. \quad (2.7)$$

The ring $\mathbb{Z}[\omega]/3 = \mathbb{Z}[\omega]/\lambda^2$ has 9 elements $a + b\omega$ (a, b modulo 3). Its unit group has 6 elements, represented exactly by the six units (see Proposition 11). Also $N(a + b\omega) = (a + b)^2 - 3ab \equiv (a + b)^2 \pmod{3}$, so every α prime to 3 has $N\alpha \equiv 1 \pmod{3}$. For later use, $\mathbb{Z}[\omega]/2 \cong \mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$.

2.6 Primes of $\mathbb{Z}[\omega]$ and the factorization of rational primes

Theorem 7. *Up to units, the primes of $\mathbb{Z}[\omega]$ are the following.*

1. $\lambda = 1 - \omega$, with $N\lambda = 3$ and $3 = -\omega^2\lambda^2$ (3 ramifies).
2. For each prime $p \equiv 1 \pmod{3}$, two conjugate primes $\pi, \bar{\pi}$ that are not associates, with $p = \pi\bar{\pi}$ and $N\pi = N\bar{\pi} = p$ (p splits).
3. For each prime $p \equiv 2 \pmod{3}$, the prime p itself, with $Np = p^2$ (p is inert).

So p splits, is inert, or ramifies according as $\chi_{-3}(p) = \left(\frac{p}{3}\right)$ is 1, -1 or 0. This agrees with Theorem 2, since $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$ by quadratic reciprocity.

Proof. Let π be a prime of $\mathbb{Z}[\omega]$. Since $\pi \mid \pi\bar{\pi} = N\pi \in \mathbb{Z}$, π divides a rational prime p , and only one: if $\pi \mid p$ and $\pi \mid q \neq p$ then $\pi \mid 1$. Then $N\pi \mid Np = p^2$. If $N\pi = p^2$, then p/π is a unit and $\pi \sim p$. If $N\pi = p$, then $p = \pi\bar{\pi}$. It remains to decide, for each p , whether an element of norm p exists. (An element of prime norm is irreducible, hence prime, since $\mathbb{Z}[\omega]$ is a UFD.)

$p = 3$: λ has norm 3.

$p \equiv 2 \pmod{3}$: $4N(a + b\omega) = (2a - b)^2 + 3b^2 \equiv (2a - b)^2 \pmod{3}$, while $4p \equiv 2 \pmod{3}$ is not a square modulo 3. So no element has norm p , and p is prime in $\mathbb{Z}[\omega]$.

$p \equiv 1 \pmod{3}$: $\mathbb{F}_p^\times$ is cyclic of order divisible by 3, so some $r \in \mathbb{Z}$ has $r^2 + r + 1 \equiv 0 \pmod{p}$. Then $p \mid (r - \omega)(r - \bar{\omega}) = r^2 + r + 1$, but p divides neither factor (their ω -coordinates are ∓ 1). So p is not prime, and $p = \pi\bar{\pi}$ with $N\pi = p$. The prime π divides one factor, say $r - \omega$, and then $\bar{\pi} \mid r - \bar{\omega}$. If $\bar{\pi}$ were an associate of π , then π would divide both factors and hence their difference $\omega - \bar{\omega} = \sqrt{-3}$, so $p \mid N\sqrt{-3} = 3$, which is false. $\square$

Corollary 8 (Fermat, Euler, Gauss). *Let $p \neq 3$ be prime.*

1. $p = a^2 - ab + b^2$ for some $a, b \in \mathbb{Z} \iff p = x^2 + 3y^2$ for some $x, y \in \mathbb{Z} \iff p \equiv 1 \pmod{3}$.
2. If $p \equiv 1 \pmod{3}$, then $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod{3}$, and L is unique while M is unique up to sign. If $\pi = a + b\omega$ is either primary prime above p (§2.7), then $L = -\text{Tr}\pi = b - 2a$ and $M = \pm b/3$.

Proof. (1) An element of norm p exists iff $p \equiv 1 \pmod{3}$. Among $\alpha, \omega\alpha, \omega^2\alpha$ the ω -coordinates are $b, a - b$ and $-a$. Since p is odd, a and b are not both even, and then one of these three is even. Using that associate, $p = (a - \frac{b}{2})^2 + 3(\frac{b}{2})^2$. (2) For primary $\pi = a + b\omega$ we have $3 \mid b$, and $4p = (2a - b)^2 + 3b^2$. Conversely, if $4p = L^2 + 27M^2$, then $L \equiv M \pmod{2}$, and $\frac{L+3M\sqrt{-3}}{2} = \frac{L+3M}{2} + 3M\omega$ is an element of norm p whose ω -coordinate is divisible by 3. It is therefore $\pm$ a primary prime above p , and L is determined up to sign. Since $a \equiv 1$ and $b \equiv 0 \pmod{3}$, $-\text{Tr}\pi = b - 2a \equiv 1 \pmod{3}$, which fixes the sign. $\square$

Residue fields. If $p \equiv 1 \pmod{3}$ and $\pi = a + b\omega$ has norm p , then $\mathbb{Z}[\omega]/\pi \cong \mathbb{F}_p$, and the isomorphism sends $\omega \mapsto r \equiv -ab^{-1} \pmod{p}$. (Here $p \nmid b$: otherwise $p \mid a$, and then $p^2 \mid N\pi$.) The value r is a root of $x^2 + x + 1$, and $\bar{\pi}$ corresponds to the other root r^2 . If $p \equiv 2 \pmod{3}$, then $\mathbb{Z}[\omega]/p \cong \mathbb{F}_{p^2}$.

Galois view. $K = \mathbb{Q}(\zeta_3)$, and for $p \neq 3$ the Frobenius at p is $\zeta_3 \mapsto \zeta_3^p$. It is trivial exactly when $p \equiv 1 \pmod{3}$, the case in which p splits.

2.7 Primary elements

Definition 9. $\alpha \in \mathbb{Z}[\omega]$ is *primary* if $\alpha \equiv 1 \pmod{3}$. In coordinates, $a + b\omega$ is primary $\iff a \equiv 1$ and $b \equiv 0 \pmod{3}$.

Remark 10 (Conventions). This is the convention of the OpenAI quasi-Riemann hypothesis papers [11] (and of our guides to them). Ireland and Rosen [8, Ch. 9] instead call a prime primary if it is $\equiv 2 \pmod{3}$, which is -1 times ours. Some authors use $\equiv \pm 1 \pmod{3}$ (“semi-primary”; each ideal prime to 3 has two such generators). Cubic residue symbols do not see the difference, since $-1 = (-1)^3$ is a cube. The Gauss and Jacobi sums of §3.4, and the integer $L \equiv 1 \pmod{3}$ in $4p = L^2 + 27M^2$, are unchanged. Their expressions in terms of the chosen generator have different signs: with $\pi' = -\pi$, $J = -\pi = \pi'$, $g^3 = -p\pi = p\pi'$, and $L = -\text{Tr}\pi = \text{Tr}\pi'$.

Proposition 11. 1. Every α prime to 3 has exactly one primary associate. Hence every nonzero ideal prime to 3 has exactly one primary generator.

2. Products and conjugates of primary elements are primary. A rational integer n is primary iff $n \equiv 1 \pmod{3}$; for instance $-2, 4, -5, 7, \dots$. In particular, for $p \equiv 2 \pmod{3}$ the primary generator of (p) is $-p$.

3. Every primary element is uniquely a product of primary primes, with no unit factor. In particular, if $p \equiv 1 \pmod{3}$, then $p = \pi\bar{\pi}$ exactly, with $\pi, \bar{\pi}$ primary.

Proof. (1) Distinct units are incongruent modulo 3: if $u \neq u'$, then $0 < N(u - u') \leq 4 < 9 = N3$. So the six units represent the six classes of $(\mathbb{Z}[\omega]/3)^\times$. If α is prime to 3, it is invertible modulo 3, and exactly one unit u satisfies $u \equiv \alpha^{-1}$, i.e. $u\alpha \equiv 1 \pmod{3}$. (2) $\bar{3} = 3$ and $\bar{1} = 1$. (3) Write $\alpha = u \prod \pi_i$ with primary primes π_i , using unique factorization and (1); no π_i is λ because α is prime to 3. The product $\prod \pi_i$ is primary, so $u \equiv 1 \pmod{3}$, and $u = 1$ by (1). For the last claim note that $p \equiv 1 \pmod{3}$ is itself primary. $\square$

So primary elements correspond one-to-one to the nonzero ideals prime to 3, and

$$\sum_{\alpha \text{ primary}} N\alpha^{-s} = (1 - 3^{-s}) \zeta_K(s). \quad (2.8)$$

The primary primes of norm below 50 are

$$\begin{aligned} -2 \ (4), \quad 1 + 3\omega, \quad -2 - 3\omega \ (7), \quad 4 + 3\omega, \quad 1 - 3\omega \ (13), \quad -2 + 3\omega, \quad -5 - 3\omega \ (19), \quad -5 \ (25), \\ 1 + 6\omega, \quad -5 - 6\omega \ (31), \quad 7 + 3\omega, \quad 4 - 3\omega \ (37), \quad 7 + 6\omega, \quad 1 - 6\omega \ (43), \end{aligned} \quad (2.9)$$

with norms in parentheses. Table 2 lists all primary elements of norm at most 100.

2.8 Ideals of $\mathbb{Z}[\omega]$ as lattices

Since $\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega$, an additive subgroup $I \subseteq \mathbb{Z}[\omega]$ is an ideal as soon as $\omega I \subseteq I$. Multiplication by ω is the rotation through 120° , and $I = -I$. So *the nonzero ideals of $\mathbb{Z}[\omega]$ are the nonzero subgroups of $\mathbb{Z}[\omega]$ that are mapped to themselves by the rotation through 60°* , which is multiplication by the unit $1 + \omega = e^{\pi i/3}$. Such a subgroup contains $N\alpha$ and $N\alpha\omega$ for each of its elements $\alpha \neq 0$, so it is a sublattice of finite index.

Every ideal is principal (Proposition 5):

$$I = (\alpha) = \alpha\mathbb{Z}[\omega] = \mathbb{Z}\alpha + \mathbb{Z}\omega\alpha. \quad (2.10)$$

As a map of $\mathbb{C}$, multiplication by α is the rotation through $\arg \alpha$ followed by the dilation by $|\alpha| = \sqrt{N\alpha}$. So (α) is a rotated and enlarged copy of the hexagonal lattice $\mathbb{Z}[\omega]$. This has three consequences.

- *Generators.* The generators of (α) are its six elements $u\alpha$, u a unit. They are the nonzero elements of (α) nearest to 0, and they are the vertices of a regular hexagon of radius $\sqrt{N\alpha}$, just as the units are for $\mathbb{Z}[\omega]$. If (α) is prime to 3, exactly one of them is primary (Proposition 11).
- *Norm, index and area.* The parallelogram spanned by α and $\omega\alpha$ is a fundamental domain of (α) . Its area is $N\alpha \cdot \frac{\sqrt{3}}{2}$, which is $N\alpha$ times the area of a fundamental domain of $\mathbb{Z}[\omega]$. The index of a sublattice is the ratio of these areas, so

$$N\alpha = [\mathbb{Z}[\omega] : (\alpha)] = |\mathbb{Z}[\omega]/(\alpha)|. \quad (2.11)$$

The points of $\mathbb{Z}[\omega]$ in the half-open parallelogram $\{s\alpha + t\omega\alpha : 0 \leq s, t < 1\}$ form a complete set of residues modulo α .

- *Operations.* For ideals $I = (\alpha)$ and $J = (\beta)$,

$$I + J = (\gcd(\alpha, \beta)), \quad I \cap J = (\text{lcm}(\alpha, \beta)), \quad IJ = (\alpha\beta), \quad N(IJ) = NI \cdot NJ. \quad (2.12)$$

Here IJ is the set of finite sums of products xy with $x \in I$ and $y \in J$; if $I = (\alpha_1, \alpha_2)$ and $J = (\beta_1, \beta_2)$, it is generated by the four products $\alpha_i\beta_j$. Also $I \supseteq J$ if and only if $I \mid J$: *to contain is to divide*. If $I + J = \mathbb{Z}[\omega]$, i.e. I and J are coprime, then $IJ = I \cap J$, and the Chinese remainder theorem gives $\mathbb{Z}[\omega]/IJ \cong \mathbb{Z}[\omega]/I \times \mathbb{Z}[\omega]/J$. Without coprimality the product can be smaller than the intersection; for example $(\lambda)(\lambda) = (3)$ but $(\lambda) \cap (\lambda) = (\lambda)$.

The next proposition lists all ideals explicitly in coordinates.

Proposition 12 (Ideals in coordinates). *1. Let $m \geq 1$, and let $r \in \mathbb{Z}$ satisfy $r^2 + r + 1 \equiv 0 \pmod{m}$. Then $x + y\omega \mapsto x + ry \pmod{m}$ is a ring homomorphism from $\mathbb{Z}[\omega]$ onto $\mathbb{Z}/m\mathbb{Z}$, and its kernel*

$$I_{m,r} = \{x + y\omega : x + ry \equiv 0 \pmod{m}\} = \mathbb{Z}m + \mathbb{Z}(\omega - r) \quad (2.13)$$

is an ideal of norm m . It depends only on r modulo m .

2. *Every nonzero ideal equals $cI_{m,r}$ for exactly one integer $c \geq 1$, one $m \geq 1$ and one r modulo m with $r^2 + r + 1 \equiv 0 \pmod{m}$. Here c is the gcd of the coordinates of the elements of the ideal, and the norm of the ideal is c^2m .*
3. *Hence, if $\varrho(m)$ is the number of r modulo m with $r^2 + r + 1 \equiv 0 \pmod{m}$, the number of ideals of norm n is $\sum_{c^2 \mid n} \varrho(n/c^2)$.*

Proof. (1) The map is additive and sends 1 to 1, so it is onto, and its kernel has index m . By (2.3), $(x + y\omega)(x' + y'\omega) = (xx' - yy') + (xy' + x'y - yy')\omega$, and

$$(x + ry)(x' + ry') - (xx' - yy' + r(xy' + x'y - yy')) = yy'(r^2 + r + 1) \equiv 0 \pmod{m}, \quad (2.14)$$

so the map is multiplicative and its kernel is an ideal. Both m and $\omega - r$ lie in the kernel. Conversely, if $x + ry \equiv 0 \pmod{m}$, then $x + y\omega = y(\omega - r) + (x + ry) \in \mathbb{Z}(\omega - r) + \mathbb{Z}m$.

(2) Let $I \neq 0$, let c be the gcd of the coordinates of its elements, and put $J = c^{-1}I$. This is an ideal, and the coordinates of its elements have gcd 1. The ω -coordinates of the elements of J form a subgroup $d\mathbb{Z}$ of $\mathbb{Z}$. If $x + y\omega \in J$, then $\omega(x + y\omega) = -y + (x - y)\omega \in J$, so $d \mid y$ and $d \mid x - y$, hence $d \mid x$. Thus d divides every coordinate, and $d = 1$. So J contains an element $\omega - r$ with $r \in \mathbb{Z}$. Also $J \cap \mathbb{Z} = m\mathbb{Z}$ for some $m \geq 1$. If $x + y\omega \in J$, then $x + ry = (x + y\omega) - y(\omega - r) \in J \cap \mathbb{Z}$, so $J = \mathbb{Z}m + \mathbb{Z}(\omega - r) = I_{m,r}$. Finally $\omega(\omega - r) = -(1 + r)(\omega - r) - (r^2 + r + 1)$ lies in J , so $r^2 + r + 1 \in J \cap \mathbb{Z} = m\mathbb{Z}$. The data are unique: c is determined by I , m by $J \cap \mathbb{Z} = m\mathbb{Z}$, and r modulo m because $\omega - r$ and $\omega - r'$ in J imply $r' - r \in J \cap \mathbb{Z}$. The norm is $[\mathbb{Z}[\omega] : c\mathbb{Z}[\omega]] [c\mathbb{Z}[\omega] : cJ] = c^2m$.

(3) This follows from (2). $\square$

By the Chinese remainder theorem ϱ is multiplicative. Also $\varrho(3) = 1$ (the root is $r = 1$) and $\varrho(9) = 0$, so $\varrho(3^k) = 0$ for $k \geq 2$. For a prime $p \neq 3$, $x^2 + x + 1$ has a root modulo p if and only if $p \equiv 1 \pmod{3}$ (proof of Theorem 7), and then it has two. Since $(2r + 1)^2 = 4(r^2 + r + 1) - 3$, the derivative $2r + 1$ of $x^2 + x + 1$ at a root is prime to p , so by Hensel's lemma $\varrho(p^k) = 1 + \chi_{-3}(p)$ for all $k \geq 1$. With these values, part (3) agrees with (2.19); we also checked this for every $n \leq 3000$.

Prime ideals in coordinates. The prime ideals of Theorem 7 are as follows.

- $(\lambda) = I_{3,1} = \{x + y\omega : 3 \mid x + y\}$, the kernel of the reduction $\mathbb{Z}[\omega] \rightarrow \mathbb{F}_3$, $\omega \mapsto 1$ (§2.6).
- If $p \equiv 1 \pmod{3}$, let r and $r' = -1 - r$ be the two roots of $x^2 + x + 1$ modulo p . The two primes above p are $\mathfrak{p} = I_{p,r}$ and $\bar{\mathfrak{p}} = I_{p,r'}$, the kernels of the two homomorphisms $\mathbb{Z}[\omega] \rightarrow \mathbb{F}_p$ that send ω to r and to r' . Complex conjugation exchanges them, since $\bar{x} + y\omega = (x - y) - y\omega$ and $(x - y) + r(-y) = x + r'y$. A generator is $\gcd(p, \omega - r)$, which the Euclidean algorithm finds; in Example 6, $I_{61,13} = (-5 - 9\omega)$.
- If $p \equiv 2 \pmod{3}$, then $(p) = pI_{1,0} = p\mathbb{Z}[\omega]$, a copy of $\mathbb{Z}[\omega]$ scaled by p .

For $p = 7$ the roots of $x^2 + x + 1$ are 2 and 4, and

$$\mathfrak{p} = I_{7,2} = (7, \omega - 2) = (1 + 3\omega), \quad \bar{\mathfrak{p}} = I_{7,4} = (7, \omega - 4) = (-2 - 3\omega), \quad (2.15)$$

since $1 + 2 \cdot 3 = 7$ and $-2 + 4 \cdot (-3) = -14$. The six generators of $\mathfrak{p}$ are $\pm\pi$, $\pm\omega\pi$ and $\pm\omega^2\pi$, where $\pi = 1 + 3\omega$, $\omega\pi = -3 - 2\omega$ and $\omega^2\pi = 2 - \omega$. In particular $\omega - 2 = -\omega^2\pi = (1 + \omega)\pi$ is a generator, so $\mathfrak{p} = (\omega - 2)$. Figure 2 shows $\mathfrak{p}$, and Figure 3 shows (λ) and (2) .

Example 13 (Products). With the two-element generators of (2.15), $\mathfrak{p}\bar{\mathfrak{p}}$ is generated by the four products of generators:

$$\mathfrak{p}\bar{\mathfrak{p}} = (49, 7(\omega - 4), 7(\omega - 2), (\omega - 2)(\omega - 4)) = (49, 7\omega - 28, 7\omega - 14, 7 - 7\omega) = (7). \quad (2.16)$$

Indeed, every generator is a multiple of 7, and $7 = 49 - 3((7\omega - 14) - (7\omega - 28))$ lies in the ideal. As $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are coprime, $\mathfrak{p}\bar{\mathfrak{p}} = \mathfrak{p} \cap \bar{\mathfrak{p}}$: the ideal (7) consists of the points common to the two lattices

(Figure 4, left). The Chinese remainder theorem gives $\mathbb{Z}[\omega]/(7) \cong \mathbb{F}_7 \times \mathbb{F}_7$, $x + y\omega \mapsto (x + 2y, x + 4y)$. In the same way

$$\mathfrak{p}^2 = (49, 7(\omega - 2), (\omega - 2)^2) = (3 - 5\omega) = (\pi^2) = (-8 - 3\omega) = I_{49,30}, \quad (2.17)$$

because $(\omega - 2)^2 = 3 - 5\omega = \omega\pi^2$ already generates $\mathfrak{p}^2$. Here 30 is the root of $r^2 + r + 1 \equiv 0 \pmod{49}$ with $r \equiv 2 \pmod{7}$, and $-8 + 30 \cdot (-3) = -98$. The ideal $\mathfrak{p}^2$ has index 7 in $\mathfrak{p}$ (Figure 4, right). So $\mathfrak{p} \cdot \mathfrak{p}$ is strictly smaller than $\mathfrak{p} \cap \mathfrak{p} = \mathfrak{p}$, unlike the coprime product $\mathfrak{p}\bar{\mathfrak{p}} = \mathfrak{p} \cap \bar{\mathfrak{p}}$. The three ideals of norm 49 are $\mathfrak{p}^2 = I_{49,30}$, $\bar{\mathfrak{p}}^2 = I_{49,18}$ and $\mathfrak{p}\bar{\mathfrak{p}} = 7I_{1,0}$, in agreement with $\varrho(49) + \varrho(1) = 3 = \sum_{d|49} \chi_{-3}(d)$. Likewise $(\lambda)\mathfrak{p} = (\lambda) \cap \mathfrak{p} = (\lambda\pi)$ has norm 21, and $(\lambda)^2 = (3)$ has index 3 in (λ) (Figure 3).

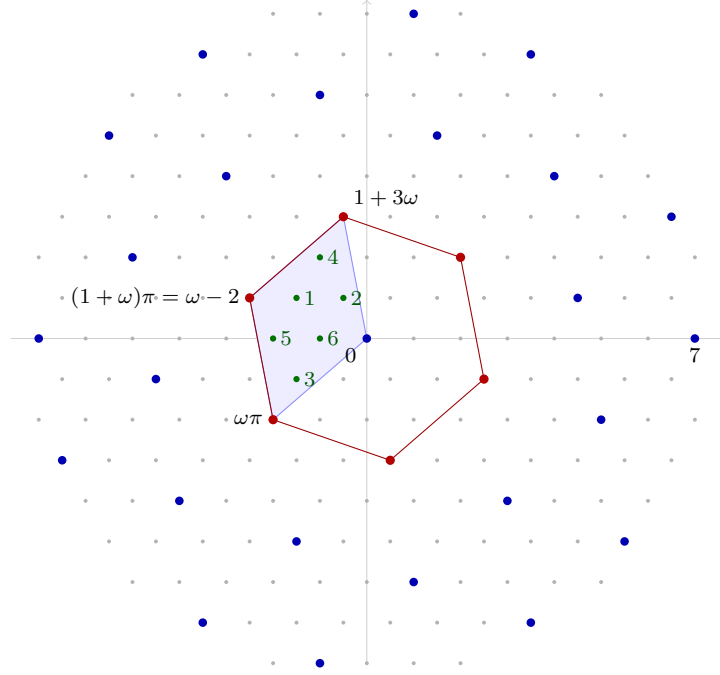


Figure 2: The prime ideal $\mathfrak{p} = (1 + 3\omega) = (7, \omega - 2) = I_{7,2}$ of norm 7. Small grey dots are the elements of $\mathbb{Z}[\omega]$, and large dots are the elements of $\mathfrak{p}$, the $x + y\omega$ with $x + 2y \equiv 0 \pmod{7}$. The six generators $\pm\pi, \pm\omega\pi, \pm\omega^2\pi$ (red), with $\pi = 1 + 3\omega$ the primary one, are the elements of $\mathfrak{p}$ nearest 0, and they form a regular hexagon. Another generator is $\omega - 2 = (1 + \omega)\pi$. The shaded parallelogram, spanned by π and $\omega\pi$, is a fundamental domain of $\mathfrak{p}$, with 7 times the area of that of $\mathbb{Z}[\omega]$. The 7 points of $\mathbb{Z}[\omega]$ in it (half-open: 0 and the green points) are labelled by their residues $x + 2y \pmod{7}$, that is, by their images under $\mathbb{Z}[\omega]/\mathfrak{p} \cong \mathbb{F}_7$, $\omega \mapsto 2$. The integer $7 = \pi\bar{\pi}$ lies in $\mathfrak{p}$ but does not generate it.

2.9 Counting, and the zeta function of K

By Theorem 3 and $w = 6$, for every $n \geq 1$:

$$\#\{(a, b) \in \mathbb{Z}^2 : a^2 - ab + b^2 = n\} = \#\{\alpha : N\alpha = n\} = 6 \sum_{m|n} \chi_{-3}(m), \quad (2.18)$$

$$\#\{\text{ideals of norm } n\} = \sum_{m|n} \chi_{-3}(m), \quad (2.19)$$



Figure 3: Left: the ramified prime $(\lambda) = I_{3,1} = \{x + y\omega : 3 \mid x + y\}$ of norm 3. Its six generators $\pm\lambda, \pm\omega\lambda, \pm\omega^2\lambda$ (red) form a hexagon turned by 30° relative to the units, and the parallelogram spanned by λ and $\omega\lambda$ contains one point of each class of $\mathbb{Z}[\omega]/\lambda \cong \mathbb{F}_3$ (0 and the green points), labelled by $x + y \bmod 3$. Black rings mark $(\lambda)^2 = (3)$, of index 3 in (λ) . Right: the inert prime $(2) = 2\mathbb{Z}[\omega]$ of norm 4, a copy of $\mathbb{Z}[\omega]$ scaled by 2. The parallelogram spanned by 2 and 2ω contains the residues 0, $1, \omega, 1 + \omega$, which represent $\mathbb{Z}[\omega]/2 \cong \mathbb{F}_4$ (note $1 + \omega = -\omega^2 \equiv \omega^2$).

$$\#\{\alpha \text{ primary} : N\alpha = n\} = \sum_{m|n} \chi_{-3}(m) \quad \text{if } 3 \nmid n, \quad 0 \quad \text{if } 3 \mid n. \quad (2.20)$$

For example, $n = 91 = 7 \cdot 13$ has 4 ideals, and the four primary elements of norm 91 are the products of one primary prime above 7 with one above 13:

$$\begin{aligned} (1 + 3\omega)(4 + 3\omega) &= -5 + 6\omega, & (1 + 3\omega)(1 - 3\omega) &= 10 + 9\omega, \\ (-2 - 3\omega)(4 + 3\omega) &= 1 - 9\omega, & (-2 - 3\omega)(1 - 3\omega) &= -11 - 6\omega. \end{aligned} \quad (2.21)$$

The Dedekind zeta function is

$$\zeta_K(s) = \frac{1}{6} \sum_{\alpha \neq 0} N\alpha^{-s} = \zeta(s)L(s, \chi_{-3}) = \frac{1}{1-3^{-s}} \prod_{p \equiv 1(3)} \frac{1}{(1-p^{-s})^2} \prod_{p \equiv 2(3)} \frac{1}{1-p^{-2s}}, \quad (2.22)$$

with $L(s, \chi_{-3}) = 1 - 2^{-s} + 4^{-s} - 5^{-s} + 7^{-s} - 8^{-s} + \dots$ (the terms with $3 \mid n$ vanish). The class number formula with $w = 6$ and $|D| = 3$ reads

$$L(1, \chi_{-3}) = \frac{2\pi h}{6\sqrt{3}} = \frac{\pi}{3\sqrt{3}} = 0.6045997\dots, \quad h = 1, \quad (2.23)$$

and the finite formula gives $h = -\frac{6}{6}(1 \cdot 1 + 2 \cdot (-1)) = 1$. As a check, the number of ideals of norm $\leq X$ is $\frac{1}{6} \cdot \frac{2\pi}{\sqrt{3}}X + O(\sqrt{X}) = \frac{\pi}{3\sqrt{3}}X + O(\sqrt{X})$, in agreement with the residue $L(1, \chi_{-3})$. The reciprocal is $1/\zeta_K(s) = \sum_{m \geq 1} c(m)m^{-s}$ with $c(m) = \sum_{de=m} \mu(d)\mu(e)\chi_{-3}(e)$, the coefficients used in the guide to the 11/12 argument.

2.10 Characters on $\mathbb{Z}[\omega]$

Two kinds of characters on (ideals of) $\mathbb{Z}[\omega]$ appear in the quasi-Riemann hypothesis papers.

1. *Characters through the norm.* If χ is a Dirichlet character, then $\eta(\mathfrak{a}) = \chi(N\mathfrak{a})$ is a finite-order Hecke character, and

$$L(s, \eta) = \sum_{\mathfrak{a} \neq 0} \frac{\chi(N\mathfrak{a})}{N\mathfrak{a}^s} = L(s, \chi) L(s, \chi\chi_{-3}). \quad (2.24)$$

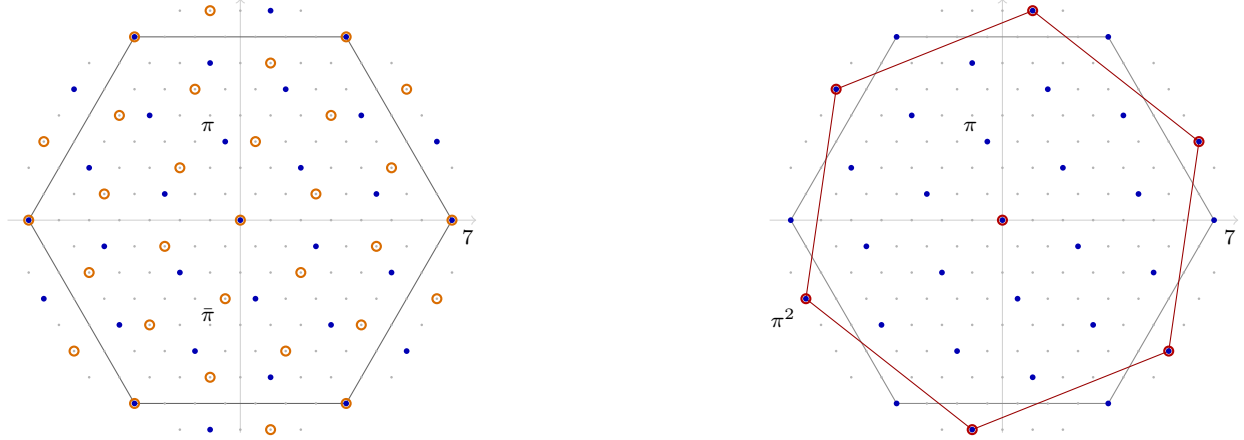


Figure 4: Products of ideals, with $\pi = 1 + 3\omega$. Left: $\mathfrak{p} = (\pi)$ (blue dots) and $\bar{\mathfrak{p}} = (\bar{\pi})$ (orange rings). The points in both form $\mathfrak{p} \cap \bar{\mathfrak{p}} = \mathfrak{p}\bar{\mathfrak{p}} = (7)$, whose generators $\pm 7, \pm 7\omega, \pm 7\omega^2$ lie on the grey hexagon. Right: $\mathfrak{p}$ (blue dots) and $\mathfrak{p}^2 = (\pi^2)$ (red rings), $\pi^2 = -8 - 3\omega$, of index 7 in $\mathfrak{p}$. Both $\mathfrak{p}\bar{\mathfrak{p}}$ and $\mathfrak{p}^2$ have norm 49, so their generators lie on the circle of radius 7, but the hexagon of $\mathfrak{p}^2$ (red) is turned relative to that of (7) (grey).

To check this, compare Euler factors. Split: $(1 - \chi(p)p^{-s})^{-2}$. Inert: $(1 - \chi(p)^2 p^{-2s})^{-1} = (1 - \chi(p)p^{-s})^{-1}(1 + \chi(p)p^{-s})^{-1}$. Ramified: $(1 - \chi(3)3^{-s})^{-1}$. For $\chi = 1$ this recovers $\zeta_K = \zeta \cdot L(\cdot, \chi_{-3})$.

2. *Residue-symbol characters.* For fixed $u \in \mathbb{Z}[\omega]$, the map $n \mapsto (u/n)_6$ on primary n prime to $6u$ (§3) is a finite-order Hecke character, and in general it is not of the previous kind.

3 Residue symbols on $\mathbb{Z}[\omega]$

3.1 Definitions

Let π be a prime of $\mathbb{Z}[\omega]$ with $\pi \nmid 6$, i.e. not associate to λ or to 2. Then $N\pi \equiv 1 \pmod{6}$: either $N\pi = p \equiv 1 \pmod{6}$, or $N\pi = p^2$ with $p \equiv 5 \pmod{6}$. The six units are distinct modulo π , since their differences have norm 1, 3 or 4. As $(\mathbb{Z}[\omega]/\pi)^\times$ is cyclic of order $N\pi - 1$, we may define, for $\alpha \in \mathbb{Z}[\omega]$,

$$\left(\frac{\alpha}{\pi}\right)_6 = \begin{cases} 0, & \pi \mid \alpha, \\ \text{the sixth root of unity} \equiv \alpha^{(N\pi-1)/6} \pmod{\pi}, & \pi \nmid \alpha, \end{cases} \quad (3.1)$$

and

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_6^2, \quad \left(\frac{\alpha}{\pi}\right)_2 = \left(\frac{\alpha}{\pi}\right)_6^3. \quad (3.2)$$

The cubic symbol $(\alpha/\pi)_3 \equiv \alpha^{(N\pi-1)/3}$ makes sense for every $\pi \nmid 3$, including $\pi = 2$, where $(\alpha/2)_3 \equiv \alpha \pmod{2}$. For $n = \prod \pi_i^{e_i}$ prime to 6 (to 3 for $k = 3$) put $(\alpha/n)_k = \prod (\alpha/\pi_i)_{k_i}^{e_i}$. In the papers' notation $\chi_n(u) = (u/n)_6$, so χ_n^2 and χ_n^3 are the cubic and quadratic symbols. The symbols satisfy the following.

- $(\alpha/n)_k$ depends only on α modulo n and on the ideal (n) , and it is multiplicative in both α and n .
- *Euler's criterion:* for prime π and $\pi \nmid \alpha$, $(\alpha/\pi)_k = 1$ iff α is a k -th power modulo π .

- *Conjugation:* $\overline{(\alpha/\pi)_k} = (\bar{\alpha}/\bar{\pi})_k$.

3.2 Units and rational integers

Throughout this subsection $\pi \nmid 6$ is a prime of $\mathbb{Z}[\omega]$, and p is the rational prime below it, that is, the prime number with $\pi \mid p$ (Theorem 7). Then $p \geq 5$, and either $p \equiv 1 \pmod{3}$ and $N\pi = p$, or $p \equiv 2 \pmod{3}$, π is an associate of p , and $N\pi = p^2$.

For a unit u , the power $u^{(N\pi-1)/6}$ is itself a sixth root of unity, so $(u/\pi)_6 = u^{(N\pi-1)/6}$ exactly. Since $u^6 = 1$, this depends only on $(N\pi - 1)/6$ modulo 6, that is, on $N\pi$ modulo 36. In particular

$$\left(\frac{\omega}{\pi}\right)_6 = \omega^{(N\pi-1)/6}, \quad \left(\frac{\omega}{\pi}\right)_3 = \omega^{(N\pi-1)/3}, \quad \left(\frac{-1}{\pi}\right)_6 = (-1)^{(N\pi-1)/6}, \quad \left(\frac{-1}{\pi}\right)_3 = 1, \quad (3.3)$$

and $(-1/\pi)_6 = -1$ exactly when $N\pi \equiv 7 \pmod{12}$.

Now let $k \in \mathbb{Z}$ with $p \nmid k$. The symbol $(k/\pi)_6$ is computed in the residue field $\mathbb{Z}[\omega]/\pi$, and k lies in its prime field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. A congruence between rational integers modulo p holds in $\mathbb{Z}[\omega]$ as well, and then also modulo π , since $\pi \mid p$. So Fermat's little theorem gives

$$k^{p-1} \equiv 1 \pmod{p} \text{ in } \mathbb{Z}, \quad \text{hence} \quad k^{p-1} \equiv 1 \pmod{\pi} \text{ in } \mathbb{Z}[\omega]. \quad (3.4)$$

- If $p \equiv 2 \pmod{3}$, then p is inert and $N\pi = p^2$. Also $p \equiv 5 \pmod{6}$, since p is odd, so $\frac{p+1}{6}$ is an integer. By (3.4),

$$k^{(N\pi-1)/6} = k^{(p-1)\frac{p+1}{6}} = (k^{p-1})^{(p+1)/6} \equiv 1 \pmod{\pi}, \quad (3.5)$$

so $(k/\pi)_6 = 1$. In terms of the residue field $\mathbb{Z}[\omega]/\pi \cong \mathbb{F}_{p^2}$: the subgroup $\mathbb{F}_p^\times$ of $\mathbb{F}_{p^2}^\times$ has order $p-1$, which divides $(p^2-1)/6$, so every element of $\mathbb{F}_p^\times$ is a sixth power in $\mathbb{F}_{p^2}$.

- If $p \equiv 1 \pmod{3}$, then $p = \pi\bar{\pi}$ up to a unit, and $\mathbb{Z}[\omega]/\pi \cong \mathbb{F}_p$, with $k \mapsto k \pmod{p}$. So $(k/\pi)_6$ is the sixth root of unity congruent to $k^{(p-1)/6}$ modulo π , and in general it is not 1. Cubing it, and using Euler's criterion in $\mathbb{F}_p$, gives $(k/\pi)_2 \equiv k^{(p-1)/2} \equiv \left(\frac{k}{p}\right) \pmod{\pi}$. Both sides are ± 1 , and $1 \not\equiv -1 \pmod{\pi}$, so

$$\left(\frac{k}{\pi}\right)_2 = \left(\frac{k}{p}\right) \quad (\text{the Legendre symbol}). \quad (3.6)$$

In the same way $(k/\pi)_3 = 1$ iff $k^{(p-1)/3} \equiv 1 \pmod{p}$, i.e. iff k is a cube modulo p . By the conjugation rule, and since $\bar{k} = k$, we have $(k/\bar{\pi})_6 = \overline{(k/\pi)_6}$, so

$$\left(\frac{k}{p}\right)_6 = \left(\frac{k}{\pi}\right)_6 \left(\frac{k}{\bar{\pi}}\right)_6 = \left|\left(\frac{k}{\pi}\right)_6\right|^2 = 1. \quad (3.7)$$

Hence $(k/m)_6 = 1$ whenever $k, m \in \mathbb{Z}$ are coprime and m is prime to 6, because each rational prime dividing m contributes 1: *rational integers do not see each other through the sextic symbol*. A single prime π above a split p does see them, as Tables 4 and 6 show.

3.3 Cubic reciprocity

Theorem 14 (Cubic reciprocity; [8], Ch. 9). *If π, ρ are primary primes with $N\pi \neq N\rho$, then $(\pi/\rho)_3 = (\rho/\pi)_3$. Moreover, if $\pi = a + b\omega$ is a primary prime with $a = 3m + 1$ and $b = 3n$, then*

$$\left(\frac{\omega}{\pi}\right)_3 = \omega^{-m-n}, \quad \left(\frac{\lambda}{\pi}\right)_3 = \omega^m, \quad \left(\frac{3}{\pi}\right)_3 = \omega^n. \quad (3.8)$$

In Ireland and Rosen's convention $\pi' = -\pi = (3m' - 1) + 3n'\omega$, with $m' = -m$ and $n' = -n$, the supplements become $\omega^{m'+n'}$, $\omega^{2m'}$ and $\omega^{2n'}$. The prime -2 (of norm 4) is allowed.

The conjugate case. Let $\pi = a + b\omega$ be a primary prime of norm $p \equiv 1 \pmod{3}$, with $a = 3m + 1$ and $b = 3n$. We show that $(\pi/\bar{\pi})_3 = 1$, so the law $(\pi/\bar{\pi})_3 = (\bar{\pi}/\pi)_3 = (\pi/\bar{\pi})_3$ holds here too.

- Modulo $\bar{\pi}$ we have $\pi \equiv \pi - \bar{\pi} = b\sqrt{-3} = 3n\omega\lambda$.
- The primary prime $\bar{\pi} = (a - b) - b\omega$ has parameters $(m - n, -n)$. By the supplements, $(3\omega\lambda/\bar{\pi})_3 = \omega^{-n} \omega^{-m+2n} \omega^{m-n} = 1$, so $(\pi/\bar{\pi})_3 = (n/\bar{\pi})_3$.
- Here $0 < |n| < p$, and $(-1/\bar{\pi})_3 = 1$. If $3 \mid n$, then each factor 3 of n contributes $(3/\bar{\pi})_3 = \omega^{-n} = 1$.
- Let $q \neq 3$ be a prime dividing n , and let ρ be a primary prime above q . Then $N\rho \neq p$. By the law for different norms, $(\rho/\bar{\pi})_3 = (\bar{\pi}/\rho)_3 = (a/\rho)_3$, because $\bar{\pi} \equiv a \pmod{q}$. Multiplying over the primary primes above q (whose product is $\pm q$) gives $(q/\bar{\pi})_3 = (a/q)_3 = 1$ by §3.2, since $a, q \in \mathbb{Z}$ are coprime. (For $q = 2$, $(a/2)_3 \equiv a \equiv 1 \pmod{2}$ directly.)

Consequently $(\alpha/\beta)_3 = (\beta/\alpha)_3$ for all coprime primary α, β . We also checked by computer the law for all pairs of primary primes of norm ≤ 400 (including conjugate pairs and the inert primes $-2, -5, -11, -17$), and the three supplements for every primary prime of norm ≤ 400 . Table 3 shows the symbols for small primes; its symmetry is cubic reciprocity.

3.4 Cubic Gauss and Jacobi sums

Let π be a primary prime with $N\pi = p \equiv 1 \pmod{3}$. Then $\rho_\pi(t) = \chi_\pi(t)^2 = (t/\pi)_3$, for $t \in \mathbb{Z}$, is a cubic Dirichlet character modulo p ; χ_π continues to denote the sextic character. Put

$$g(\pi) = \sum_{t=1}^{p-1} \rho_\pi(t) e^{2\pi it/p}, \quad J(\pi) = \sum_{t \bmod p} \rho_\pi(t) \rho_\pi(1-t). \quad (3.9)$$

Theorem 15 ([8, Ch. 8–9], in our sign convention). $|g(\pi)|^2 = p$, $g(\pi)^3 = -p\pi$, and $J(\pi) = -\pi$.

In Ireland–Rosen's convention these read $g^3 = p\pi'$ and $J = \pi'$, with $\pi' = -\pi$. Consequences:

- (Gauss) The number of solutions of $x^3 + y^3 = 1$ in $\mathbb{F}_p^2$ is $p - 2 + L$, where $L = 2\Re J(\pi) = -\text{Tr}\pi$ is the L of Corollary 8 ($L \equiv 1 \pmod{3}$).
- (Gauss) 2 is a cube modulo p iff L and M are even iff $p = x^2 + 27y^2$ [1, §4].

We checked all three identities of Theorem 15 and both consequences numerically for every $p < 400$, $p \equiv 1 \pmod{3}$. Cubic Gauss sums over $\mathbb{Z}[\omega]$ (sums modulo c over all of $\mathbb{Z}[\omega]$, with an additive character of $\mathbb{Z}[\omega]$) are, up to normalization, the Fourier coefficients of Kubota's cubic theta function. Heath-Brown and Patterson [7] used this theta function to show that the arguments of the Gauss sums $g(\pi)$ at primes are equidistributed. Patterson's conjecture on the bias in sums of cubic Gauss sums was proved by Dunn and Radziwiłł [4], assuming the Generalized Riemann Hypothesis. These sums are the source of the cubic Gauss sums in the quasi-Riemann hypothesis papers.

3.5 The sextic symbol in examples

Tables 4–7 illustrate the properties of $(\alpha/\pi)_6$ established above.

- *A character of order 6.* For a prime $\pi \nmid 6$, the map $x \mapsto (x/\pi)_6$ is a homomorphism from the cyclic group $(\mathbb{Z}[\omega]/\pi)^\times$, of order $N\pi - 1$, onto the six sixth roots of unity. Its kernel is the group of sixth powers, of index 6, and its square and cube are the cubic and quadratic symbols. Table 4 shows it for the primes of norm 7 and 13. If $N\pi = 7$, then $(N\pi - 1)/6 = 1$, so $(x/\pi)_6$ is simply the unit congruent to x modulo π . The map is then an isomorphism $\mathbb{F}_7^\times \rightarrow \{\pm 1, \pm\omega, \pm\omega^2\}$, and the order of $(x/\pi)_6$ is the order of x modulo 7. For instance $\omega \equiv 2 \pmod{1+3\omega}$, so $(\frac{2}{1+3\omega})_6 = \omega$. If $N\pi = 13$, each value is taken twice, and the kernel is $\{\pm 1\}$, the sixth powers modulo 13.
- *An inert prime.* Table 5 shows $(\alpha/5)_6$ on all of $\mathbb{Z}[\omega]/5 \cong \mathbb{F}_{25}$. Each value is taken $24/6 = 4$ times. The nonzero rational integers (the row $b = 0$) all give 1, as (3.5) predicts. Since $\bar{5} = 5$, conjugating α conjugates the symbol. By (3.3), multiplying α by ω multiplies the symbol by $(\omega/5)_6 = \omega^{24/6} = \omega$.
- *Units and rational integers.* Table 6 gives $(x/\pi)_6$ for $x = -1, \omega, 1 + \omega, \lambda, 2, 3, 5, 7$ and every primary prime $\pi \nmid 6$ of norm at most 121. Several of the facts above are visible in it.
 - In the columns of units, each entry depends only on $N\pi$ modulo 36; compare the rows of norm 7, 43 and 79.
 - In the columns of rational integers, the rows of π and $\bar{\pi}$ (adjacent rows of equal norm) are complex conjugates, and the inert rows -5 and -11 are 1 (apart from $(5/-5)_6 = 0$).
 - For a split prime, $N\pi = p$, the cube of a rational entry is the Legendre symbol (3.6). For example, $(\frac{3}{1+3\omega})_6 = -\omega^2$, whose cube is $-1 = (\frac{3}{7})$.
 - For a split prime, $N\pi = p$, the entry for 2 is ± 1 exactly when 2 is a cube modulo p , that is, when $p = x^2 + 27y^2$ (§3.4): $p = 31, 43, 109$ in this table. The inert rows also have entry 1 for 2, by (3.5), but the representation criterion does not apply to them.
 - Since $3 = -\omega^2\lambda^2$ and $-\omega^2 = 1 + \omega$, the column of 3 is the column of $1 + \omega$ times the square of the column of λ .
- *Reciprocity.* Table 7 gives $(\pi/\rho)_6$ for primary primes. It is not symmetric. Its square is the table of cubic symbols, which is symmetric by cubic reciprocity, so $(\pi/\rho)_6 = \pm(\rho/\pi)_6$. The sign is $(\pi/\rho)_2(\rho/\pi)_2$, the factor in the quadratic reciprocity law of K . It depends only on the classes of π and ρ modulo 4, and it is 1 when π or ρ is congruent to 1, ω or ω^2 modulo 4. Both facts follow from Hilbert’s reciprocity law: since K has no real places, the sign equals the quadratic Hilbert symbol (π, ρ) at the prime 2, which is unramified in K . We checked both facts for all pairs of primary primes prime to 6 of norm below 1000. For 30 of the 78 unordered pairs of classes in $(\mathbb{Z}[\omega]/4)^\times$ the sign is -1 . For example, $(\frac{4+3\omega}{1+3\omega})_6 = -\omega^2$ but $(\frac{1+3\omega}{4+3\omega})_6 = \omega^2$.

4 Poisson summation over $\mathbb{Z}[\omega]$

A key step of the 11/12 argument for ζ [13] applies Poisson summation over the lattice $\mathbb{Z}[\omega]$ to a mean square of sums of sextic characters. This section collects what that step uses:

- additive characters of $\mathbb{Z}[\omega]$ and their duality (§4.1);
- Gauss sums and the identities between them (§4.2);

- the Poisson summation formula for $\mathbb{Z}[\omega]$ (§4.3), and its version twisted by a character (§4.4).

Section 4.5 shows how these combine in the paper. We use the papers' normalizations. In this section and the next we write

$$\sqrt{-3} = 1 + 2\omega = \omega - \omega^2 = \omega\lambda, \quad (4.1)$$

where $\lambda = 1 - \omega$ as before. The papers denote $\sqrt{-3}$ by λ ; since the two differ by the unit ω , statements about ideals are unaffected. Throughout, $\mu(n)$ is the Möbius function of the ideal (n) : it is $(-1)^k$ if (n) is a product of k distinct prime ideals, and 0 if (n) is not squarefree.

4.1 Additive characters and duality

For $z \in \mathbb{C}$ put

$$\check{e}(z) = \exp(2\pi i(z + \bar{z})) = e^{2\pi i \operatorname{Tr} z}, \quad e(z) = \check{e}\left(\frac{z}{\sqrt{-3}}\right) = \exp\left(\frac{4\pi i \operatorname{Im} z}{\sqrt{3}}\right). \quad (4.2)$$

Both are characters of the additive group of $\mathbb{C}$. Dunn and Radziwiłł [4], and the theta function in Section 5, use $\check{e}$; the 11/12 paper uses e . The reason for e is the following.

Proposition 16 (Self-duality). *For $z, w \in \mathbb{C}$ put $B(z, w) = 2 \operatorname{Im}(zw)/\sqrt{3} = \operatorname{Tr}(zw/\sqrt{-3})$, so that $e(zw) = e^{2\pi i B(z, w)}$. Then B is real bilinear and symmetric, and on the basis $1, \omega$ its Gram matrix is*

$$\begin{pmatrix} B(1, 1) & B(1, \omega) \\ B(\omega, 1) & B(\omega, \omega) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}, \quad (4.3)$$

of determinant -1 . Consequently, for $y \in \mathbb{C}$, $e(xy) = 1$ for all $x \in \mathbb{Z}[\omega]$ if and only if $y \in \mathbb{Z}[\omega]$. Equivalently, the trace dual $\{y \in K : \operatorname{Tr}(xy) \in \mathbb{Z} \text{ for all } x \in \mathbb{Z}[\omega]\}$ is $\frac{1}{\sqrt{-3}}\mathbb{Z}[\omega]$.

Proof. $B(1, 1) = 0$, $B(1, \omega) = 2 \operatorname{Im} \omega/\sqrt{3} = 1$ and $B(\omega, \omega) = 2 \operatorname{Im} \omega^2/\sqrt{3} = -1$. For $y = s + t\omega$ with $s, t \in \mathbb{R}$ this gives $B(1, y) = t$ and $B(\omega, y) = s - t$, which are both integers if and only if $s, t \in \mathbb{Z}$. For the trace dual, note that $\operatorname{Tr}(xy) = B(x, \sqrt{-3}y)$. $\square$

Hence, for $m \neq 0$, the Nm functions $x \mapsto e(hx/m)$, $h \bmod m$, are well defined on $\mathbb{Z}[\omega]/m$ and pairwise distinct, so they are all the characters of the additive group $\mathbb{Z}[\omega]/m$. In particular

$$\sum_{x \bmod m} e\left(\frac{hx}{m}\right) = \begin{cases} Nm, & m \mid h, \\ 0, & m \nmid h, \end{cases} \quad (4.4)$$

and every $f : \mathbb{Z}[\omega]/m \rightarrow \mathbb{C}$ has the finite Fourier expansion

$$f(x) = \sum_{h \bmod m} \hat{f}(h) e\left(\frac{hx}{m}\right), \quad \hat{f}(h) = \frac{1}{Nm} \sum_{x \bmod m} f(x) e\left(-\frac{hx}{m}\right). \quad (4.5)$$

With $\check{e}$ in place of e , the dual lattice of $\mathbb{Z}[\omega]$ is $\frac{1}{\sqrt{-3}}\mathbb{Z}[\omega]$. For a function with a different translation lattice, that lattice must also be taken into account. For example, the theta function in Section 5 is invariant under translations by $3\mathbb{Z}[\omega]$, whose trace dual is $(3\sqrt{-3})^{-1}\mathbb{Z}[\omega] = (\sqrt{-3})^{-3}\mathbb{Z}[\omega]$. This explains the allowed frequency lattice in (5.6); further automorphy forces many of its coefficients to vanish. The support in $(\sqrt{-3})^{-4}\mathbb{Z}[\omega]$ at the other two cusps comes from their translation laws and multipliers, as recorded in Theorem 23, rather than from trace duality for $\mathbb{Z}[\omega]$ alone. For a split primary prime $\pi = a + b\omega$ of norm p and $t \in \mathbb{Z}$,

$$e\left(\frac{t}{\pi}\right) = \exp\left(-\frac{2\pi i bt}{p}\right), \quad \check{e}\left(\frac{t}{\pi}\right) = \exp\left(\frac{2\pi i t \operatorname{Tr} \pi}{p}\right), \quad (4.6)$$

since $t/\pi = t\bar{\pi}/p$ and $\operatorname{Im} \bar{\pi} = -\frac{\sqrt{3}}{2}b$.

4.2 Gauss sums

Let $m \neq 0$, and let ψ be a character of $(\mathbb{Z}[\omega]/m)^\times$, extended by zero to all of $\mathbb{Z}[\omega]$. It is *primitive* if for every proper divisor m' of m (proper: m/m' is not a unit), ψ is nontrivial on the subgroup of classes $c \equiv 1 \pmod{m'}$. Its normalized Gauss sum is

$$\gamma(\psi) = \frac{1}{\sqrt{Nm}} \sum_{x \bmod m} \psi(x) e\left(\frac{x}{m}\right). \quad (4.7)$$

Lemma 17. *If ψ is primitive modulo m , then for every $h \in \mathbb{Z}[\omega]$*

$$\sum_{x \bmod m} \psi(x) e\left(\frac{hx}{m}\right) = \overline{\psi(h)} \sqrt{Nm} \gamma(\psi), \quad \text{and} \quad |\gamma(\psi)| = 1. \quad (4.8)$$

Proof. If $(h, m) = 1$, substitute $x \mapsto h^{-1}x$. Otherwise let $\delta = \gcd(h, m)$ and $m' = m/\delta$, a proper divisor. By primitivity there is $c \equiv 1 \pmod{m'}$, prime to m , with $\psi(c) \neq 1$. Replacing x by cx does not change $e(hx/m)$, because $h(c-1)x/m = (h/\delta)((c-1)/m')x \in \mathbb{Z}[\omega]$. So the sum S satisfies $S = \psi(c)S$, hence $S = 0 = \overline{\psi(h)}$. For the modulus, sum $|S|^2$ over $h \bmod m$. By (4.4) the result is $Nm \sum_x |\psi(x)|^2 = Nm \varphi(m)$, where $\varphi(m) = |(\mathbb{Z}[\omega]/m)^\times|$, while the first part gives $Nm |\gamma(\psi)|^2 \varphi(m)$. $\square$

For squarefree primary n prime to 6 and $j \in \mathbb{Z}$, the character $\chi_n^j = \prod_{p|n} \chi_p^j$ is primitive modulo n when $6 \nmid j$. Put

$$\gamma_j(n) = \frac{1}{\sqrt{Nn}} \sum_{x \bmod n} \chi_n(x)^j e\left(\frac{x}{n}\right), \quad \alpha(n) = \frac{n}{|n|}, \quad G(n) = \overline{\chi_n(4)} \gamma_3(n), \quad (4.9)$$

All powers of a character are taken on the unit group and then extended by zero. Thus $\chi_n^{-1} = \overline{\chi_n}$ and $\chi_n^0(x) = \mathbf{1}_{(x,n)=1}$. Here γ_2 is a *cubic* Gauss sum, since $\chi_n^2 = (\cdot/n)_3$, and γ_3 is a quadratic one.

Proposition 18 (Gauss-sum identities [13, Lemma 4.1]). *For squarefree primary n prime to 6,*

$$\gamma_1(n) \gamma_{-1}(n) = \chi_n(-1), \quad (4.10)$$

$$\gamma_2(n)^3 = \mu(n) \alpha(n), \quad (4.11)$$

$$\gamma_1(n) \gamma_2(n) = \mu(n) \alpha(n) G(n), \quad (4.12)$$

$$\mu(n) \gamma_{-1}(n) = \chi_n(-1) G(n)^{-1} \overline{\alpha(n)} \gamma_2(n). \quad (4.13)$$

Proof. Reduction to primes. If a, b are coprime, write $x = bx_1 + ax_2$ with $x_1 \bmod a$ and $x_2 \bmod b$. Then $e(x/ab) = e(x_1/a)e(x_2/b)$, $\chi_a(x) = \chi_a(bx_1)$ and $\chi_b(x) = \chi_b(ax_2)$, so

$$\gamma_j(ab) = (\chi_a(b) \chi_b(a))^j \gamma_j(a) \gamma_j(b). \quad (4.14)$$

The factor $\chi_a(b) \chi_b(a)$ is a sixth root of unity. In (4.10) it occurs to the powers 1 and -1 , in (4.11) to the power 6, and in (4.12) to the power 3 on both sides, because $G(ab) = (\chi_a(b) \chi_b(a))^3 G(a) G(b)$. Since μ, α and $\chi_n(-1)$ are multiplicative, it suffices to prove (4.10)–(4.12) for a prime $n = \pi$. Then (4.13) follows: $\mu \gamma_{-1} = \mu \chi_n(-1) \gamma_2 / (\gamma_1 \gamma_2) = \chi_n(-1) \gamma_2 / (\alpha G)$ by (4.10) and (4.12).

Primes. Let $q = N\pi$, $\chi = \chi_\pi$, and $\tau(\chi^j) = \sqrt{q} \gamma_j(\pi)$.

- By $x \mapsto -x$, $\overline{\tau(\chi)} = \chi(-1) \tau(\bar{\chi})$, so $\tau(\chi) \tau(\bar{\chi}) = \chi(-1) |\tau(\chi)|^2 = \chi(-1) q$ by Lemma 17. This is (4.10).

- Substituting $x = \sqrt{-3}y$ in γ_2 and using $e(z) = \check{e}(z/\sqrt{-3})$ gives

$$\gamma_2(\pi) = \left(\frac{\sqrt{-3}}{\pi}\right)_3 \frac{g(\pi)}{|\pi|}, \quad g(c) = \sum_{y \bmod c} \left(\frac{y}{c}\right)_3 \check{e}\left(\frac{y}{c}\right), \quad (4.15)$$

where $g(c)$ is the cubic Gauss sum of Dunn and Radziwiłł. For primary c , Hasse's formula [4, §2] gives $g(c)^3 = \mu(c)c^2\bar{c}$. So $\gamma_2(\pi)^3 = -\pi^2\bar{\pi}/q^{3/2} = -\alpha(\pi)$, which is (4.11). For a split prime this is Theorem 15. By (4.6), $g(\pi) = \sum_t (t/\pi)_3 e^{2\pi i t \text{Tr} \pi/p} = (\text{Tr} \pi/\pi)_3 g(\pi)_{\S 3.4}$, where the subscript means the Gauss sum of §3.4. Moreover $\text{Tr} \pi \equiv \bar{\pi} \pmod{\pi}$ and $(\bar{\pi}/\pi)_3 = 1$ (§3.3), so the two Gauss sums agree.

- The Hasse–Davenport product formula [2], applied with the quadratic character χ^3 , gives

$$\tau(\chi)\tau(\chi^4) = \overline{\chi(4)} \tau(\chi^2)\tau(\chi^3). \quad (4.16)$$

Also $\tau(\chi^4)\tau(\chi^2) = \chi^2(-1)q = q$ by the first item, since $\chi^4 = \chi^{-2}$. Hence $\gamma_1 = \overline{\chi(4)}\gamma_2^2\gamma_3$. Multiplying by γ_2 and using (4.11) gives $\gamma_1\gamma_2 = -\alpha(\pi)\overline{\chi(4)}\gamma_3 = \mu(\pi)\alpha(\pi)G(\pi)$. $\square$

Identity (4.13) is the arithmetic heart of the first step of the 11/12 argument. Cancellation in the Möbius coefficients is difficult to exploit directly. Multiplying $\mu(n)$ by the sextic Gauss sum $\gamma_{-1}(n)$ produced by Poisson summation gives the cubic Gauss coefficient $\alpha(n)\gamma_2(n)$, up to the factor $\chi_n(-1)G(n)^{-1}$ of modulus 1. That factor depends only on the class of n modulo a fixed modulus [13, Lemma 4.1]. We checked (4.10)–(4.13) numerically for all 193 squarefree primary n prime to 6 with $Nn \leq 700$, and (4.16) for all primes of norm ≤ 700 .

4.3 The Poisson summation formula for $\mathbb{Z}[\omega]$

Theorem 19. *For every Schwartz function f on $\mathbb{C} = \mathbb{R}^2$,*

$$\sum_{x \in \mathbb{Z}[\omega]} f(x) = \frac{2}{\sqrt{3}} \sum_{y \in \mathbb{Z}[\omega]} \hat{f}(y), \quad \hat{f}(y) = \int_{\mathbb{C}} f(z) e(-zy) d^2z, \quad (4.17)$$

where d^2z is Lebesgue measure on $\mathbb{R}^2$.

Proof. For a lattice $L \subset \mathbb{R}^2$, Poisson summation reads

$$\sum_{x \in L} f(x) = \frac{1}{\text{covol}(L)} \sum_{\xi \in L^*} \int_{\mathbb{R}^2} f(z) e^{-2\pi i \xi(z)} d^2z, \quad (4.18)$$

where L^* is the lattice of real linear functionals ξ that are integral on L . It follows from the case $L = \mathbb{Z}^2$ by a linear change of variables. Every real linear functional on $\mathbb{C}$ is $z \mapsto B(z, y)$ for a unique $y \in \mathbb{C}$, and by Proposition 16 it is integral on $\mathbb{Z}[\omega]$ exactly when $y \in \mathbb{Z}[\omega]$. Finally $\text{covol}(\mathbb{Z}[\omega]) = \sqrt{3}/2$. $\square$

If $f(z) = \Phi(|z|^2)$ is radial, then so is $\hat{f}$, because $e(-(e^{i\vartheta}z)y) = e(-z(e^{i\vartheta}y))$. Following the papers, we include the factor $2/\sqrt{3}$ and write

$$\hat{\Phi}(|y|^2) = \frac{2}{\sqrt{3}} \int_{\mathbb{C}} \Phi(|z|^2) e(-zy) d^2z. \quad (4.19)$$

The substitution $w = t + mz$ and a dilation give, for $H > 0$, $t \in \mathbb{C}$ and $m \neq 0$,

$$\frac{2}{\sqrt{3}} \int_{\mathbb{C}} \Phi\left(\frac{|t + mz|^2}{H}\right) e(-zy) d^2z = \frac{H}{Nm} e\left(\frac{ty}{m}\right) \hat{\Phi}\left(\frac{HNy}{Nm}\right). \quad (4.20)$$

Example 20 (Gaussian weights). For $\Phi(t) = e^{-at}$ ($a > 0$), $\widehat{\Phi}(t) = \frac{2\pi}{\sqrt{3}a} e^{-4\pi^2 t/(3a)}$, and (4.17) becomes the transformation formula of the theta series of the hexagonal lattice:

$$\sum_{x \in \mathbb{Z}[\omega]} e^{-aNx} = \frac{2\pi}{\sqrt{3}a} \sum_{y \in \mathbb{Z}[\omega]} e^{-4\pi^2 Ny/(3a)}. \quad (4.21)$$

It is symmetric under $a \mapsto 4\pi^2/(3a)$, with fixed point $a = 2\pi/\sqrt{3}$. We checked (4.21) numerically for $a = 0.3, 1, 2.5$.

In the paper Φ is a fixed radial Schwartz weight with $\Phi \geq 0$, $\Phi \geq 1$ on $[0, 1]$, and $\widehat{\Phi}$ real and compactly supported. One can take a positive multiple of a dilate of $|\beta|^2$, where β is the inverse transform of a smooth radial bump β .

4.4 Poisson summation with a character

Lemma 21 ([13, Lemma 4.2]). *Let $H > 0$, let Φ be a radial Schwartz weight, let ψ be a primitive character modulo m (extended by zero), and let r be squarefree and primary. Then*

$$\sum_{k \in \mathbb{Z}[\omega]} \psi(k) \mathbf{1}_{(k,r)=1} \Phi\left(\frac{Nk}{H}\right) = \frac{H\gamma(\psi)}{\sqrt{Nm}} \sum_{d|r} \frac{\mu(d)\psi(d)}{Nd} \sum_{h \in \mathbb{Z}[\omega]} \overline{\psi(h)} \widehat{\Phi}\left(\frac{HNh}{NdNm}\right), \quad (4.22)$$

where d runs over the primary divisors of r . If ψ is nonprincipal, the frequency $h = 0$ does not contribute, since $\psi(0) = 0$. If $m = 1$, it contributes $H\widehat{\Phi}(0) \prod_{p|r} (1 - Np^{-1})$.

Proof. Write $\mathbf{1}_{(k,r)=1} = \sum_{d|(k,r)} \mu(d)$ and $k = d\ell$, so the left side is $\sum_{d|r} \mu(d)\psi(d) \sum_{\ell} \psi(\ell)\Phi(N\ell/H')$ with $H' = H/Nd$. Split $\ell = t + mz$ by residue classes $t \bmod m$ ($z \in \mathbb{Z}[\omega]$), apply (4.17) to $z \mapsto \Phi(N(t + mz)/H')$ and use (4.20):

$$\sum_{\ell} \psi(\ell)\Phi\left(\frac{N\ell}{H'}\right) = \frac{H'}{Nm} \sum_{y \in \mathbb{Z}[\omega]} \left(\sum_{t \bmod m} \psi(t) e\left(\frac{ty}{m}\right) \right) \widehat{\Phi}\left(\frac{H'Ny}{Nm}\right). \quad (4.23)$$

By Lemma 17 the inner sum is $\overline{\psi(y)}\sqrt{Nm}\gamma(\psi)$. □

The lemma exchanges a sum of length about H for one of length about $NdNm/H$, and it attaches the Gauss sum $\gamma(\psi)$. We checked (4.22) numerically, with the Gaussian of Example 20 as Φ , for $\psi = \overline{\chi_{1+3\omega}}\chi_{4+3\omega}$, $r = -2 + 3\omega$ and $H = 40, 300$; the two sides agree to 10^{-14} .

4.5 How the 11/12 paper uses Poisson summation

Let $W \in C_c^\infty((0, \infty); \mathbb{C})$ be fixed and nonzero. For $u \in \mathbb{Z}[\omega]$ consider the sums

$$A_u(D) = \sum_n \mu(n)\chi_n(u)W\left(\frac{Nn}{D}\right), \quad (4.24)$$

over squarefree primary n prime to 6. The paper needs a bound for their mean square over the rows u , with a row range $H = D^{1+\theta}$ slightly longer than the column range D . Smoothing the rows and expanding the square gives

$$\sum_u \Phi\left(\frac{Nu}{H}\right) |A_u(D)|^2 = \sum_{n_1, n_2} \mu(n_1)\mu(n_2) \overline{W\left(\frac{Nn_1}{D}\right)} W\left(\frac{Nn_2}{D}\right) \sum_u \Phi\left(\frac{Nu}{H}\right) \overline{\chi_{n_1}(u)} \chi_{n_2}(u). \quad (4.25)$$

Write $g = \gcd(n_1, n_2)$ and $n_i = gz_i$. Then $\overline{\chi_{n_1}(u)}\chi_{n_2}(u) = \mathbf{1}_{(u,g)=1}\psi(u)$ with $\psi = \overline{\chi_{z_1}}\chi_{z_2}$. This character is primitive modulo $z_1 z_2$, since its component at each prime is $\chi_p^{\pm 1} \neq 1$. Lemma 21, with $r = g$ and $m = z_1 z_2$, transforms the inner sum over u . Three things happen.

1. *The diagonal.* The zero frequency occurs only when $z_1 = z_2 = 1$, that is, $n_1 = n_2$. These terms contribute about $H \sum_n |W(Nn/D)|^2 \asymp HD$.
2. *Shorter sums.* Since $\hat{\Phi}$ is compactly supported, the frequencies satisfy

$$Nh \ll \frac{NdN(z_1z_2)}{H} \ll \frac{D^2}{HNg}, \quad (4.26)$$

because $d \mid g$ and $Nz_i \asymp D/Ng$. With $H = D^{1+\vartheta}$, the new row range is at most about $D^{1-\vartheta}$, shorter than the column range D .

3. *New coefficients.* By the computation behind (4.14), and since $\overline{\chi_{z_1}(z_2)}\chi_{z_2}(z_1) = R(z_1, z_2) = \pm 1$ by sextic reciprocity [13, (4.1)],

$$\gamma(\overline{\chi_{z_1}}\chi_{z_2}) = R(z_1, z_2) \gamma_{-1}(z_1)\gamma_1(z_2). \quad (4.27)$$

By (4.13), and by (4.12) in the form $\mu\gamma_1 = G\overline{\alpha}\gamma_2$,

$$\mu(z_1)\mu(z_2) \gamma(\overline{\chi_{z_1}}\chi_{z_2}) = R(z_1, z_2) \chi_{z_1}(-1) \frac{G(z_2)}{G(z_1)} a(z_1) \overline{a(z_2)}, \quad a(n) = \overline{\alpha(n)}\gamma_2(n). \quad (4.28)$$

The factor in front of $a(z_1)\overline{a(z_2)}$ in (4.28) has modulus 1 and depends only on the classes of z_1, z_2 modulo a fixed modulus. One may take modulus 72 and the group $\mathcal{G} = \{x \in (\mathbb{Z}[\omega]/72\mathbb{Z}[\omega])^\times : x \equiv 1 \pmod{3}\}$; [13, §4.1] works with an unspecified fixed ray class group. Expanding the factor in characters of $\mathcal{G} \times \mathcal{G}$ splits it into products $\xi(z_1)\overline{\xi'(z_2)}$. After separating the remaining weights, this produces mixed products of sums with coefficients $a(n)\xi(n)$ and $a(n)\overline{\xi'(n)}$; the two characters need not agree. Cauchy–Schwarz reduces their estimation to mean squares of the schematic form

$$\sum_{0 < Nh \ll D^2/H} \left| \sum_n a(n)\xi(n)\chi_n(h) W\left(\frac{Nn}{D}\right) \right|^2, \quad (4.29)$$

with the shorter frequency range $Nh \ll D^2/H$. In the paper, removing the coprimality conditions adds a further twist $\chi_n(f)^4$, and the column range is divided into ranges $Nn \asymp X$ [13, §4]. By §5.4, $\gamma_2(n)$ is proportional to a Fourier coefficient of the conjugate cubic theta function, with a factor depending only on $n \pmod{9}$. The additional angular factor $\overline{\alpha(n)}$ in $a(n)$ is supplied by differentiation and a Mellin transform (§5.5). The next step uses the automorphy of the theta function.

5 The cubic theta function of Kubota and Patterson

The coefficients $a(n) = \overline{\alpha(n)}\gamma_2(n)$ of (4.28) are related to the Fourier coefficients of Kubota’s cubic theta function, an automorphic function on hyperbolic three-space. Passing from those Fourier coefficients to $a(n)$ requires a congruence twist, complex conjugation, and the angular factor $\overline{\alpha(n)}$. This section states the properties of θ that the 11/12 argument imports. Section 5.4 identifies the coefficients precisely, and Section 5.5 explains how differentiation and a Mellin transform supply the angular factor. We continue to write $\sqrt{-3} = 1 + 2\omega$.

5.1 Hyperbolic three-space

Let $\mathbb{H}^3 = \mathbb{C} \times \mathbb{R}_{>0}$, with points $w = (z, v)$. Viewing w as the quaternion $z + vj$, the group $\mathrm{SL}_2(\mathbb{C})$ acts by $\gamma w = (aw + b)(cw + d)^{-1}$. In coordinates,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z, v) = \left(\frac{(az + b)\overline{(cz + d)} + a\bar{c}v^2}{|cz + d|^2 + |c|^2v^2}, \frac{v}{|cz + d|^2 + |c|^2v^2} \right). \quad (5.1)$$

This is the analogue of the action of $\mathrm{SL}_2(\mathbb{R})$ on the upper half-plane, where $\mathrm{Im}(\gamma\tau) = \mathrm{Im}\tau/|c\tau + d|^2$. The metric $(|dz|^2 + dv^2)/v^2$ is invariant, and its Laplacian is

$$\Delta = v^2 \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial v^2} \right) - v \frac{\partial}{\partial v} \quad (z = x + iy). \quad (5.2)$$

The matrix $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ acts by $z \mapsto z + b$. So a function invariant under translations by a lattice of b 's has a Fourier expansion in z , in the characters $\check{e}(\mu z)$. The building blocks are eigenfunctions of Δ : for every s ,

$$\Delta v^s = s(s-2)v^s, \quad \Delta[vK_{s-1}(4\pi|\mu|v)\check{e}(\mu z)] = s(s-2)vK_{s-1}(4\pi|\mu|v)\check{e}(\mu z), \quad (5.3)$$

where K_ν is the K -Bessel function, which decays exponentially at ∞ . The theta function has $s = 2/3$, which gives the term $v^{2/3}$ and the Bessel function $K_{-1/3} = K_{1/3}$. We checked (5.3) for $s = 2/3$ numerically.

5.2 The Kubota character

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z}[\omega])$, let $\Gamma(3) = \{\gamma \in \Gamma : \gamma \equiv I \pmod{3}\}$ (the papers write $\Gamma_1(3)$), and let $\Gamma_2 = \mathrm{SL}_2(\mathbb{Z})\Gamma(3) = \{\gamma_0\gamma_1 : \gamma_0 \in \mathrm{SL}_2(\mathbb{Z}), \gamma_1 \in \Gamma(3)\}$. This is a subgroup of Γ , because $\Gamma(3)$, the kernel of reduction modulo 3, is normal in Γ .

- *Entries.* Γ_2 consists of the matrices in Γ whose entries are congruent to rational integers modulo 3. That is, $\Gamma_2 = \mathrm{SL}_2(\mathbb{Z} + 3\mathbb{Z}[\omega])$, where $\mathbb{Z} + 3\mathbb{Z}[\omega] = \mathbb{Z}[3\omega]$ is the order of conductor 3 in $\mathbb{Z}[\omega]$. Indeed, if the entries of γ are rational modulo 3, then γ modulo 3 lies in $\mathrm{SL}_2(\mathbb{Z}/3)$. Since reduction $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/3)$ is onto, there is $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma_0 \equiv \gamma \pmod{3}$, and then $\gamma_0^{-1}\gamma \in \Gamma(3)$. The other inclusion is clear.
- *Index.* Γ_2 has index 27 in Γ [4, §5.1]. Since $\Gamma_2 \supset \Gamma(3)$, the index equals the index of the image of Γ_2 in $\mathrm{SL}_2(\mathbb{Z}[\omega]/3)$, and that image is $\mathrm{SL}_2(\mathbb{F}_3)$, of order 24. Reduction $\Gamma \rightarrow \mathrm{SL}_2(\mathbb{Z}[\omega]/3)$ is onto: $\mathbb{Z}[\omega]/3 = \mathbb{Z}[\omega]/\lambda^2$ is a local ring by (2.6), so $\mathrm{SL}_2(\mathbb{Z}[\omega]/3)$ is generated by elementary matrices, and these lift to Γ . Reduction modulo λ maps $\mathrm{SL}_2(\mathbb{Z}[\omega]/\lambda^2)$ onto $\mathrm{SL}_2(\mathbb{F}_3)$. Its kernel consists of the matrices $I + \lambda X$ with $X \in M_2(\mathbb{F}_3)$ and $\mathrm{tr} X = 0$, because $\det(I + \lambda X) \equiv 1 + \lambda \mathrm{tr} X \pmod{\lambda^2}$; there are 27 of them. So $|\mathrm{SL}_2(\mathbb{Z}[\omega]/3)| = 24 \cdot 27 = 648$, and the index is $648/24 = 27$.

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(3)$ the entries a, d are primary and $3 \mid b, c$. The *Kubota character* is

$$\kappa(\gamma) = \begin{cases} \left(\frac{c}{a}\right)_3, & c \neq 0, \\ 1, & c = 0. \end{cases} \quad (5.4)$$

Theorem 22 (Kubota [9, 10]; Patterson [12]). κ is a homomorphism $\Gamma(3) \rightarrow \{1, \omega, \omega^2\}$. It extends to a homomorphism on Γ_2 that is trivial on $\mathrm{SL}_2(\mathbb{Z})$.

Concretely, $\kappa(\gamma_0\gamma_1) = \kappa(\gamma_1)$ for $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$ and $\gamma_1 \in \Gamma(3)$.

The proof rests on cubic reciprocity (Theorem 14). It is the cubic analogue of the multiplier system of the classical theta function $\sum_n e^{\pi i n^2 \tau}$, which involves the quadratic symbol (c/d) . Two remarks.

- On $\Gamma(3)$, also $\kappa(\gamma) = (b/d)_3$ [4, §5.1].
- κ is trivial on the unipotent matrices $\begin{pmatrix} 1 & 3x \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 3y & 1 \end{pmatrix}$, but it is not trivial on $\Gamma(3)$. So these matrices do not generate $\Gamma(3)$.

We checked $\kappa(\gamma\gamma') = \kappa(\gamma)\kappa(\gamma')$, and $(c/a)_3 = (b/d)_3$, numerically. The check used 400 random pairs in $\Gamma(3)$, whose entries and products have norms up to about 10^9 ; in 276 of the pairs, $\kappa(\gamma\gamma') \neq 1$. We also enumerated $\mathrm{SL}_2(\mathbb{Z}[\omega]/3)$. The reductions of the elementary matrices $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$, $x \in \{1, \omega\}$, generate all 648 of its elements, and the reductions of $\mathrm{SL}_2(\mathbb{Z})$ form a subgroup of order 24, so $[\Gamma : \Gamma_2] = 27$.

5.3 The theorem of Kubota and Patterson

Kubota [10] constructed θ as the residue of an Eisenstein series for $\Gamma(3)$ twisted by κ . Patterson [12, Theorem 8.1 and Table III] computed its Fourier expansions. The coefficients involve the cubic Gauss sums

$$g(r, c) = \sum_{x \bmod c} \left(\frac{x}{c}\right)_3 \check{e}\left(\frac{rx}{c}\right), \quad g(c) = g(1, c), \quad (5.5)$$

for primary squarefree c (which may be even) and $r \in \mathbb{Z}[\omega]$. The following is the form in which the 11/12 argument imports these facts, in the normalization of Dunn and Radziwiłł [4, §5.1 and Appendix]. In it, c, d denote primary elements with c squarefree, and ν is an integer.

Theorem 23 (Kubota, Patterson). *There is a smooth function θ on $\mathbb{H}^3$ with the following properties.*

(T1) $\theta(\gamma w) = \theta(w)$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and $\theta(\gamma w) = \kappa(\gamma)\theta(w)$ for $\gamma \in \Gamma(3)$.

(T2) At the cusp ∞ ,

$$\theta(z, v) = \frac{3^{5/2}}{2} v^{2/3} + \sum_{0 \neq \mu \in (\sqrt{-3})^{-3}\mathbb{Z}[\omega]} \tau(\mu) v K_{1/3}(4\pi|\mu|v) \check{e}(\mu z), \quad (5.6)$$

where $\tau(\mu) = 0$ unless μ has one of the following forms, in which case

$$\tau(\mu) = \begin{cases} \overline{g(-3, c)} |d/c| 3^{\nu/2+2}, & \mu = \pm(\sqrt{-3})^{3\nu-4} cd^3, \nu \geq 1, \\ e^{-2\pi i/9} \overline{g(-3\omega, c)} |d/c| 3^{\nu/2+2}, & \mu = \pm\omega(\sqrt{-3})^{3\nu-4} cd^3, \nu \geq 1, \\ e^{2\pi i/9} \overline{g(-3\omega^2, c)} |d/c| 3^{\nu/2+2}, & \mu = \pm\omega^2(\sqrt{-3})^{3\nu-4} cd^3, \nu \geq 1, \\ \overline{g(1, c)} |d/c| 3^{\nu/2+5/2}, & \mu = \pm(\sqrt{-3})^{3\nu-3} cd^3, \nu \geq 0. \end{cases} \quad (5.7)$$

(T3) At the cusps $\gamma_+\infty$ and $\gamma_-\infty$, where $\gamma_+ = \begin{pmatrix} 1 & 0 \\ \omega & 1 \end{pmatrix}$ and $\gamma_- = \begin{pmatrix} 1 & 0 \\ \omega^2 & 1 \end{pmatrix}$,

$$\theta(\gamma_{\pm} w) = \sum_{0 \neq \mu \in (\sqrt{-3})^{-4}\mathbb{Z}[\omega]} t_{\pm}(\mu) v K_{1/3}(4\pi|\mu|v) \check{e}(\mu z), \quad (5.8)$$

with no constant term, where $t_+(\mu) = \omega \tau_2(\omega\mu)\check{e}(\mu)$ and $t_-(\mu) = \omega^2 \tau_1(\omega^2\mu)\check{e}(\mu)$. Here τ_1, τ_2 vanish except at the following points:

$$\tau_1(\mu) = \begin{cases} 9\omega \overline{g(-3, c)} |d/c|, & \mu = (\sqrt{-3})^{-4} cd^3, \\ 9e^{-2\pi i/9} \omega^2 \overline{g(-3\omega, c)} |d/c|, & \mu = \omega(\sqrt{-3})^{-4} cd^3, \\ 9e^{2\pi i/9} \overline{g(-3\omega^2, c)} |d/c|, & \mu = \omega^2(\sqrt{-3})^{-4} cd^3, \end{cases} \quad (5.9)$$

$$\tau_2(\mu) = \begin{cases} 9\omega^2 \overline{g(-3, c)} |d/c|, & \mu = -(\sqrt{-3})^{-4} cd^3, \\ 9e^{-2\pi i/9} \overline{g(-3\omega, c)} |d/c|, & \mu = -\omega(\sqrt{-3})^{-4} cd^3, \\ 9\omega e^{2\pi i/9} \overline{g(-3\omega^2, c)} |d/c|, & \mu = -\omega^2(\sqrt{-3})^{-4} cd^3. \end{cases} \quad (5.10)$$

In [4], $\gamma_{\pm}$ are γ_{10} and γ_{19} , two of the 27 coset representatives of $\Gamma_2 \backslash \Gamma$ [12, Table II]. The transformation in §5.5 needs only the three expansions of θ , $\theta \circ \gamma_+$ and $\theta \circ \gamma_-$ [13, App. A.2]. Three features of Theorem 23 matter.

- The coefficients are conjugate cubic Gauss sums. The main family is $\mu = (\sqrt{-3})^{-3} cd^3$, the last line of (5.7) with $\nu = 0$ and sign $+$, where $\tau(\mu) = 3^{5/2} |d| \overline{g(c)} / |c|$.
- The coefficients are supported on indices cd^3 with cube factors d^3 , which enter with weight $|d|$. So the theta function sees the sums over squarefree n in (4.29) only together with their “cube completions”. Removing the added cubes is a separate step of the argument (the descent).
- τ is even, and among these three expansions only the one at ∞ has a constant term.

5.4 The cubic Gauss sums and the theta coefficients

The Gauss sums (5.5) satisfy the following identities [4, §2], [13]. Here c, c_1, c_2 are primary and squarefree, $\tilde{g}(c) = g(c)/|c|$, and $(\cdot/\cdot)_3$ is extended to even primary denominators as in §3.

$$g(r, c) = \left(\frac{r}{c}\right)_3 g(c) \quad ((r, c) = 1), \quad (5.11)$$

$$\tilde{g}(c_1 c_2) = \left(\frac{c_1}{c_2}\right)_3 \tilde{g}(c_1) \tilde{g}(c_2) \quad ((c_1, c_2) = 1), \quad (5.12)$$

$$g(c)^3 = \mu(c) c^2 \bar{c}, \quad g(-2) = 2, \quad |\tilde{g}(c)| = 1, \quad (5.13)$$

$$\gamma_2(n) = \left(\frac{\sqrt{-3}}{n}\right)_3 \tilde{g}(n) \quad ((n, 6) = 1). \quad (5.14)$$

The first follows from $x \mapsto r^{-1}x$. The second follows from the Chinese remainder theorem as in (4.14), together with cubic reciprocity $(c_2/c_1)_3 = (c_1/c_2)_3$. The last is (4.15). We checked (5.11)–(5.14) numerically. In particular we checked $g(c)^3 = \mu(c) c^2 \bar{c}$ for all 159 primary c with $1 < Nc \leq 400$, squarefree or not.

The 11/12 argument works with the conjugate $\bar{\theta}$, whose Fourier coefficients are $d_0(\ell) = \overline{\tau(-\ell)} = \overline{\tau(\ell)}$, and similarly $d_{\pm}(\ell) = \overline{t_{\pm}(-\ell)}$ at the other two cusps. Theorem 23 and (5.13) give the following [13, §2 and Lemma 6.4].

Corollary 24. 1. For $\sigma \in \{0, +, -\}$, $d_{\sigma}(\ell) = 0$ unless $\ell = u(\sqrt{-3})^m nb^3$ with u a unit, $m \geq -4$, and n, b primary with n squarefree. This representation is unique, and

$$|d_{\sigma}(u(\sqrt{-3})^m nb^3)| \leq 27 \cdot 3^{m/6} |b|. \quad (5.15)$$

2. For squarefree primary n and primary b , $d_0((\sqrt{-3})^{-3}nb^3) = 3^{5/2}|b|\tilde{g}(n)$, and these are the only indices $\ell \in (\sqrt{-3})^{-3}\mathbb{Z}[\omega]$ with $(\sqrt{-3})^3\ell$ primary and $d_0(\ell) \neq 0$. If $(n, 6) = 1$, then

$$d_0((\sqrt{-3})^{-3}nb^3) = 3^{5/2}|b| \overline{\left(\frac{\sqrt{-3}}{n}\right)}_3 \gamma_2(n). \quad (5.16)$$

So, apart from the factor $\overline{(\sqrt{-3}/n)}_3$, which depends only on $n \bmod 9$ by the supplementary law (Theorem 14), the coefficient of $\bar{\theta}$ at the index $(\sqrt{-3})^{-3}n$ is $3^{5/2}\gamma_2(n)$. Removing the congruence factor and the constant $3^{5/2}$, then multiplying by $\alpha(n)$, gives $a(n)$ from (4.28). The angular factor depends on the argument of n , not just its residue class; differentiation followed by the Mellin transform below supplies it.

5.5 How the 11/12 paper uses the theta function

The argument applies Theorem 23 to twisted sums of the coefficients $a(n)$, completed by cubes:

$$T(X; \Psi) = \sum_n^* \sum_b \frac{\overline{\alpha(n)}\gamma_2(n)\Psi(n)\overline{\alpha(b)}^3\Psi(b)^3}{\sqrt{Nn}Nb} V\left(\frac{NnNb^3}{X}\right). \quad (5.17)$$

The star restricts n to squarefree primary elements prime to 6; b runs over all primary elements, including 1, and need not be squarefree. With $\mathcal{G}$ as in §4.5, write $\Psi(x) = \xi_0(x) \prod_{p \in \mathcal{P}} \chi_p(x)^{j_p}$, where ξ_0 is a character of $\mathcal{G}$, $\mathcal{P}$ is a finite set of primary primes prime to 6, and $0 \leq j_p \leq 5$. Extend ξ_0 by zero outside primary elements prime to 6, and every $\chi_p^{j_p}$ by zero on multiples of p , including when $j_p = 0$. Thus Ψ is completely multiplicative on primary elements and $\Psi(b) = 0$ if $(b, 6) \neq 1$. Finally $V \in C_c^\infty((0, \infty))$ [13, §6.2]. The steps [13, §6.2, App. A.2], which follow Dunn and Radziwiłł [4, §5], are as follows.

1. *Twisted theta series.* Retain only the modes with $x = (\sqrt{-3})^3\ell$ primary and prime to 6, and multiply their coefficients by $(\sqrt{-3}/x)_3\Psi(x)$. At $\ell = (\sqrt{-3})^{-3}nb^3$, $(\sqrt{-3}/nb^3)_3 = (\sqrt{-3}/n)_3$, so this cancels the conjugate symbol in (5.16). The resulting series Θ_Ψ has coefficients $3^{5/2}|b|\gamma_2(n)\Psi(n)\Psi(b)^3$ at these modes and zero elsewhere, including at the constant mode.
2. *Translates.* The twist is periodic, so its finite Fourier expansion (4.5) writes Θ_Ψ as a finite combination of translates $\theta(z + a/c, v)$ by rational points a/c . The denominator c is divisible by every prime p with $j_p \neq 0$.
3. *Automorphy at the cusp a/c .* Write the translate in lowest terms, with $(a, c) = 1$ and $c \neq 0$. Normalize (a, c) by a common unit so that $a \equiv 1 \pmod{3}$ if $\lambda \mid c$, and $c \equiv 1 \pmod{3}$ otherwise. If $\lambda \mid c$, choose δ with $a\delta \equiv 1 \pmod{3c}$; if $\lambda \nmid c$, choose $a\delta \equiv 1 \pmod{c}$ and $\delta \equiv 0 \pmod{3}$. These choices are possible by coprimality and the Chinese remainder theorem. Put $b' = (a\delta - 1)/c$ and $g = \begin{pmatrix} a & b' \\ c & \delta \end{pmatrix}$. Then $g \in \Gamma$, and the following choices give $g_1 = gH^{-1} \in \Gamma(3)$:

$$H = \begin{cases} I, & \lambda^2 \mid c, \\ \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}, & u \in \{\sqrt{-3}, -\sqrt{-3}\}, u \equiv c \pmod{3}, \lambda \mid c, \lambda^2 \nmid c, \\ \begin{pmatrix} u & -1 \\ 1 & 0 \end{pmatrix}, & u \equiv a \pmod{3}, \lambda \nmid c. \end{cases} \quad (5.18)$$

In the last case take u from a fixed set of representatives of $\mathbb{Z}[\omega]/3\mathbb{Z}[\omega]$. By (T1), $\theta(Hw) = \theta(\gamma_\sigma w)$: here $\sigma = 0$ in the first case; $\sigma = -, +$ for $u = \sqrt{-3}, -\sqrt{-3}$, respectively, in the second;

and $\sigma = 0, -, +$ according as $u \equiv 0, \omega, -\omega \pmod{\mathbb{Z} + 3\mathbb{Z}[\omega]}$ in the third. These identifications follow by multiplying γ_σ on the left by matrices in $\mathrm{SL}_2(\mathbb{Z})$ and by translations or lower unipotents with parameter in $3\mathbb{Z}[\omega]$, on which κ is trivial. Consequently, $\theta(gw) = \kappa(g_1)\theta(\gamma_\sigma w)$, where $\gamma_0 = I$.

To track the multiplier uniformly as the twist varies, the paper refines these choices by fixed congruences at the primes above 2 and 3 [13, App. A.2]. With those choices, cubic reciprocity gives $\kappa(g_1) = \kappa_0 \prod_{p|c, p \nmid 6} \chi_p(a)^2$, where κ_0 depends only on fixed congruence data; the primes $p \nmid 6$ occur to the first power in the reduced denominator c . Finally, (5.1) gives

$$g^{-1}\left(\frac{a}{c} + z, v\right) = \left(-\frac{\delta}{c} - \frac{\bar{z}}{c^2(v^2 + |z|^2)}, \frac{v}{\mathrm{N}c(v^2 + |z|^2)}\right). \quad (5.19)$$

At $z = 0$ this is $(-\delta/c, 1/(\mathrm{N}c v))$: small v becomes large v .

4. *Mellin transform.* Write $\partial_{\bar{z}} = \frac{1}{2}(\partial_x + i\partial_y)$ and $\partial_z = \frac{1}{2}(\partial_x - i\partial_y)$. Differentiation kills the constant term $v^{2/3}$ and gives $\partial_{\bar{z}}\check{e}(\ell z) = 2\pi i \bar{\ell}\check{e}(\ell z)$. Put $F_\sigma(z', v') = \overline{\theta(\gamma_\sigma(z', v'))}$. At $z = 0$, the coordinates (z', v') in (5.19) satisfy $\partial_{\bar{z}}z' = -(cv)^{-2}$ and $\partial_{\bar{z}}\bar{z}' = \partial_{\bar{z}}v' = 0$. The chain rule therefore gives

$$\partial_{\bar{z}}\overline{\theta(a/c + z, v)}\Big|_{z=0} = -\frac{\overline{\kappa(g_1)}}{c^2v^2}(\partial_{z'}F_\sigma)\left(-\frac{\delta}{c}, \frac{1}{\mathrm{N}cv}\right). \quad (5.20)$$

On the reflected side the derivative is $\partial_{z'}$, so a Fourier mode acquires $2\pi i \ell$ instead of $2\pi i \bar{\ell}$. This explains the factor $\alpha(\ell)$ in (5.22). Now take $\int_0^\infty \partial_{\bar{z}}\Theta_\Psi(z, v)|_{z=0} v^{2s-1} dv$. The single-mode integral is

$$\int_0^\infty v^{2s} K_{1/3}(4\pi|\ell|v) dv = 2^{2s-1} \Gamma(s + \tfrac{1}{3}) \Gamma(s + \tfrac{2}{3}) (4\pi|\ell|)^{-2s-1} \quad (\mathrm{Re} s > -\tfrac{1}{3}). \quad (5.21)$$

Thus each mode ℓ contributes a multiple of $\overline{\alpha(\ell)} \mathrm{N}\ell^{-s}$, and termwise integration is justified initially for $\Re s > 1$. Since $\alpha((\sqrt{-3})^{-3}) = i$, this is where the factor $\overline{\alpha(n)} \overline{\alpha(b)}^3$ in (5.17) comes from. The result is the Dirichlet series of T times $\Gamma(s + \frac{1}{3})\Gamma(s + \frac{2}{3})$.

5. *Functional equation.* In (5.20), the substitution $v' = 1/(\mathrm{N}cv)$ changes $v^{-2}v^{2s-1} dv$ into $(\mathrm{N}c)^{2-2s}(v')^{2(1-s)-1} dv'$ after reversing the limits. Thus the Mellin transform at s equals a finite combination of the corresponding transforms at $1-s$ of the expansions at the three cusps, with additive twists $\check{e}(-\delta\ell/c)$. After differentiation, the cusp expansions give exponential decay at both ends of the height integral, so its Mellin transform is entire. Together with the vertical bounds established in the source paper, this permits the contour shift; no zero-free region for ζ is used. Inverting the Mellin transform gives [13, Proposition 6.2]

$$T(X; \Psi) = \sum C \sum_{0 \neq \ell \in (\sqrt{-3})^{-4}\mathbb{Z}[\omega]} \frac{d_\sigma(\ell)\alpha(\ell)}{\sqrt{\mathrm{N}\ell}} \psi((\sqrt{-3})^4\ell) \prod_p B_{p,j_p}((\sqrt{-3})^4\ell) V^\sharp\left(\frac{\mathrm{N}\ell X}{\mathrm{N}c^2}\right). \quad (5.22)$$

Here the outer sum is finite, $|C| \ll 1$, ψ is an additive character from a fixed finite set, the product runs over the primes $p \nmid 6$ dividing c , and

$$V^\sharp(x) = \frac{1}{2\pi i} \int_{(0)} \widehat{V}(-t) \frac{\Gamma(\frac{7}{6} + t)\Gamma(\frac{5}{6} + t)}{\Gamma(\frac{7}{6} - t)\Gamma(\frac{5}{6} - t)} \left(\frac{(2\pi)^4 x}{27}\right)^{-t} dt, \quad \widehat{V}(s) = \int_0^\infty V(x) x^s \frac{dx}{x}, \quad (5.23)$$

decays rapidly for large x . A sum of length X becomes one of length about $\mathrm{N}c^2/X$.

6. *The local factors.* At a prime $p \mid c$ with twist χ_p^j , three ingredients combine:

- the finite Fourier coefficient of χ_p^j at frequency h , which is proportional to $\chi_p(h)^{-j}$ by Lemma 17;
- the Kubota factor, which enters through $\bar{\theta}$ as $\overline{\chi_p(a)^2} = \chi_p(a)^{-2}$, where $a \equiv \sigma h \pmod{p}$ for a fixed σ ;
- the reflected phase $e(\epsilon h^{-1}x/p)$, since $\delta \equiv a^{-1} \pmod{p}$.

Summing over $h \neq 0$, and substituting $y = h^{-1}$, gives a Gauss sum:

$$\sum_{y \neq 0} \chi_p(y)^{j+2} e\left(\frac{\epsilon y x}{p}\right) = \overline{\chi_p(\epsilon x)}^{j+2} \sqrt{Np} \gamma_{j+2}(p) \quad (j \neq 4). \quad (5.24)$$

Including the finite Fourier coefficient, the local factors are

$$B_{p,j}(x) = \begin{cases} \chi_p(x)^{-j-2}, & j \notin \{0, 4\}, \\ (Np)^{-1/2} \chi_p(x)^{-2}, & j = 0 \text{ (active)}, \\ (Np)^{-1/2} (-1 + Np \mathbf{1}_{p|x}), & j = 4. \end{cases} \quad (5.25)$$

The omitted factors have absolute value one, are independent of x , and are included in C in (5.22). For $j = 1$ the factor is $\chi_p(x)^{-3} = \chi_p(x)^3 = (x/p)_2$: *the sextic twist becomes quadratic*. For $j = 4$ the sum is instead a Ramanujan sum. For $j = 0$ there are two branches, because

$$\mathbf{1}_{p \nmid x} = 1 - \frac{1}{Np} - \frac{1}{Np} \sum_{h \neq 0 \pmod{p}} e\left(\frac{hx}{p}\right). \quad (5.26)$$

The nonzero frequencies give the active factor in (5.25). The zero frequency leaves p out of c and contributes the scalar $1 - (Np)^{-1}$ (the inactive branch). Both branches occur in the outer sum of (5.22). Their number is bounded by a divisor function of the twist modulus, and their scalars have absolute value at most one; see [13, §6.2, App. A.2]. We checked the local transform for all j and all primes of norm ≤ 200 .

For squarefree rows k prime to the auxiliary twist moduli, the factors with $j = 1$ give the quadratic character $(x/k)_2$. Repeated prime factors in the rows and the other local factors are handled separately in the source paper. Heath-Brown's quadratic large sieve [6], in the number-field form of Goldmakher and Louvel [5], is applied with squarefree rows and squarefree columns. It bounds the completed mean square; removing the added cubes still requires the descent.

6 Tables

p	$\chi_{-3}(p)$	type	factorization in $\mathbb{Z}[\omega]$	$p = a^2 - ab + b^2$	$p = x^2 + 3y^2$	$4p = L^2 + 27M^2$
2	-1	inert	$2 = -1 \cdot (-2)$	—	—	—
3	0	ramified	$3 = -\omega^2 \lambda^2$	$1^2 - 1 \cdot 2 + 2^2$	$0^2 + 3 \cdot 1^2$	—
5	-1	inert	$5 = -1 \cdot (-5)$	—	—	—
7	1	split	$7 = (1 + 3\omega)(-2 - 3\omega)$	$3^2 - 3 \cdot 1 + 1^2$	$2^2 + 3 \cdot 1^2$	$1^2 + 27 \cdot 1^2$
11	-1	inert	$11 = -1 \cdot (-11)$	—	—	—
13	1	split	$13 = (4 + 3\omega)(1 - 3\omega)$	$4^2 - 4 \cdot 1 + 1^2$	$1^2 + 3 \cdot 2^2$	$(-5)^2 + 27 \cdot 1^2$
17	-1	inert	$17 = -1 \cdot (-17)$	—	—	—
19	1	split	$19 = (-2 + 3\omega)(-5 - 3\omega)$	$5^2 - 5 \cdot 2 + 2^2$	$4^2 + 3 \cdot 1^2$	$7^2 + 27 \cdot 1^2$
23	-1	inert	$23 = -1 \cdot (-23)$	—	—	—
29	-1	inert	$29 = -1 \cdot (-29)$	—	—	—
31	1	split	$31 = (1 + 6\omega)(-5 - 6\omega)$	$6^2 - 6 \cdot 1 + 1^2$	$2^2 + 3 \cdot 3^2$	$4^2 + 27 \cdot 2^2$
37	1	split	$37 = (7 + 3\omega)(4 - 3\omega)$	$7^2 - 7 \cdot 3 + 3^2$	$5^2 + 3 \cdot 2^2$	$(-11)^2 + 27 \cdot 1^2$
41	-1	inert	$41 = -1 \cdot (-41)$	—	—	—
43	1	split	$43 = (7 + 6\omega)(1 - 6\omega)$	$7^2 - 7 \cdot 1 + 1^2$	$4^2 + 3 \cdot 3^2$	$(-8)^2 + 27 \cdot 2^2$
47	-1	inert	$47 = -1 \cdot (-47)$	—	—	—
53	-1	inert	$53 = -1 \cdot (-53)$	—	—	—
59	-1	inert	$59 = -1 \cdot (-59)$	—	—	—
61	1	split	$61 = (4 + 9\omega)(-5 - 9\omega)$	$9^2 - 9 \cdot 4 + 4^2$	$7^2 + 3 \cdot 2^2$	$1^2 + 27 \cdot 3^2$
67	1	split	$67 = (7 + 9\omega)(-2 - 9\omega)$	$9^2 - 9 \cdot 2 + 2^2$	$8^2 + 3 \cdot 1^2$	$(-5)^2 + 27 \cdot 3^2$
71	-1	inert	$71 = -1 \cdot (-71)$	—	—	—
73	1	split	$73 = (1 + 9\omega)(-8 - 9\omega)$	$9^2 - 9 \cdot 1 + 1^2$	$5^2 + 3 \cdot 4^2$	$7^2 + 27 \cdot 3^2$
79	1	split	$79 = (10 + 3\omega)(7 - 3\omega)$	$10^2 - 10 \cdot 3 + 3^2$	$2^2 + 3 \cdot 5^2$	$(-17)^2 + 27 \cdot 1^2$
83	-1	inert	$83 = -1 \cdot (-83)$	—	—	—
89	-1	inert	$89 = -1 \cdot (-89)$	—	—	—
97	1	split	$97 = (-8 + 3\omega)(-11 - 3\omega)$	$11^2 - 11 \cdot 3 + 3^2$	$7^2 + 3 \cdot 4^2$	$19^2 + 27 \cdot 1^2$

Table 1: How the rational primes $p < 100$ factor in $\mathbb{Z}[\omega]$; the type is given by $\chi_{-3}(p)$, which is 1 for split, -1 for inert and 0 for ramified. Split primes are written as $p = \pi\bar{\pi}$ with both factors primary; for these there is no unit (Proposition 11). For inert p , the primary generator of (p) is $-p$. In the last column $L \equiv 1 \pmod{3}$ and $L = -\text{Tr}\pi$ (Corollary 8).

α	$N\alpha$	factorization	α	$N\alpha$	factorization
1	1	unit	$-2 + 6\omega$	52	$(-2) \cdot (1 - 3\omega)$
-2	4	prime	$-8 - 6\omega$	52	$(-2) \cdot (4 + 3\omega)$
$1 + 3\omega$	7	prime	$4 + 9\omega$	61	prime
$-2 - 3\omega$	7	prime	$-5 - 9\omega$	61	prime
$4 + 3\omega$	13	prime	-8	64	$(-2)^3$
$1 - 3\omega$	13	prime	$7 + 9\omega$	67	prime
4	16	$(-2)^2$	$-2 - 9\omega$	67	prime
$-2 + 3\omega$	19	prime	$1 + 9\omega$	73	prime
$-5 - 3\omega$	19	prime	$-8 - 9\omega$	73	prime
-5	25	prime	$10 + 6\omega$	76	$(-2) \cdot (-5 - 3\omega)$
$4 + 6\omega$	28	$(-2) \cdot (-2 - 3\omega)$	$4 - 6\omega$	76	$(-2) \cdot (-2 + 3\omega)$
$-2 - 6\omega$	28	$(-2) \cdot (1 + 3\omega)$	$10 + 3\omega$	79	prime
$1 + 6\omega$	31	prime	$7 - 3\omega$	79	prime
$-5 - 6\omega$	31	prime	$10 + 9\omega$	91	$(1 + 3\omega) \cdot (1 - 3\omega)$
$7 + 3\omega$	37	prime	$-5 + 6\omega$	91	$(1 + 3\omega) \cdot (4 + 3\omega)$
$4 - 3\omega$	37	prime	$-11 - 6\omega$	91	$(-2 - 3\omega) \cdot (1 - 3\omega)$
$7 + 6\omega$	43	prime	$1 - 9\omega$	91	$(-2 - 3\omega) \cdot (4 + 3\omega)$
$1 - 6\omega$	43	prime	$-8 + 3\omega$	97	prime
$-5 + 3\omega$	49	$(-2 - 3\omega)^2$	$-11 - 3\omega$	97	prime
7	49	$(1 + 3\omega) \cdot (-2 - 3\omega)$	10	100	$(-2) \cdot (-5)$
$-8 - 3\omega$	49	$(1 + 3\omega)^2$			

Table 2: All primary elements $\alpha = a + b\omega$ ($a \equiv 1, b \equiv 0 \pmod{3}$) with $N\alpha \leq 100$, ordered by norm. There are 41 of them, one for each ideal of norm ≤ 100 prime to 3. Each factors into primary primes with no unit (Proposition 11). No norm is divisible by 3, and the number of entries of norm n is $\sum_{m|n} \chi_{-3}(m)$.

	-2	$1 + 3\omega$	$-2 - 3\omega$	$4 + 3\omega$	$1 - 3\omega$	$-2 + 3\omega$	$-5 - 3\omega$	-5	$1 + 6\omega$	$-5 - 6\omega$
-2	$\cdot$	ω^2	ω	ω	ω^2	ω	ω^2	1	1	1
$1 + 3\omega$	ω^2	$\cdot$	1	ω	ω^2	ω	ω	ω^2	1	ω
$-2 - 3\omega$	ω	1	$\cdot$	ω	ω^2	ω^2	ω^2	ω	ω^2	1
$4 + 3\omega$	ω	ω	ω	$\cdot$	1	ω^2	1	1	ω^2	ω
$1 - 3\omega$	ω^2	ω^2	ω^2	1	$\cdot$	1	ω	1	ω^2	ω
$-2 + 3\omega$	ω	ω	ω^2	ω^2	1	$\cdot$	1	ω	ω	ω^2
$-5 - 3\omega$	ω^2	ω	ω^2	1	ω	1	$\cdot$	ω^2	ω	ω^2
-5	1	ω^2	ω	1	1	ω	ω^2	$\cdot$	ω	ω^2
$1 + 6\omega$	1	1	ω^2	ω^2	ω^2	ω	ω	ω	$\cdot$	1
$-5 - 6\omega$	1	ω	1	ω	ω	ω^2	ω^2	ω^2	1	$\cdot$

Table 3: The cubic residue symbol $(\pi/\rho)_3$ for primary primes of norm ≤ 31 , with π indexing the row and ρ the column. The table is symmetric (cubic reciprocity, Theorem 14); in particular $(\pi/\bar{\pi})_3 = 1$ for each conjugate pair.

$p = 7, \pi = 1 + 3\omega, \bar{\pi} = -2 - 3\omega$						
x	1	2	3	4	5	6
order of $x \bmod 7$	1	3	6	3	6	2
$(x/\pi)_6$	1	ω	$-\omega^2$	ω^2	$-\omega$	-1
$(x/\bar{\pi})_6$	1	ω^2	$-\omega$	ω	$-\omega^2$	-1
$(x/\pi)_3$	1	ω^2	ω	ω	ω^2	1
$(x/\pi)_2$	1	1	-1	1	-1	-1
$(\frac{x}{7})$	1	1	-1	1	-1	-1

$p = 13, \pi = 4 + 3\omega, \bar{\pi} = 1 - 3\omega$												
x	1	2	3	4	5	6	7	8	9	10	11	12
order of $x \bmod 13$	1	12	3	6	4	12	12	4	3	6	12	2
$(x/\pi)_6$	1	$-\omega^2$	ω^2	ω	-1	$-\omega$	$-\omega$	-1	ω	ω^2	$-\omega^2$	1
$(x/\bar{\pi})_6$	1	$-\omega$	ω	ω^2	-1	$-\omega^2$	$-\omega^2$	-1	ω^2	ω	$-\omega$	1
$(x/\pi)_3$	1	ω	ω	ω^2	1	ω^2	ω^2	1	ω^2	ω	ω	1
$(x/\pi)_2$	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1
$(\frac{x}{13})$	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1

Table 4: The sextic symbol modulo the primary primes above 7 and 13, on the rational representatives $x = 1, \dots, p-1$ of $(\mathbb{Z}[\omega]/\pi)^\times \cong \mathbb{F}_p^\times$. The cubic and quadratic symbols are the square and cube of the sextic one, and the quadratic symbol is the Legendre symbol (3.6). Modulo 13 the cubes are $\pm 1, \pm 5$, which are exactly the x with $(x/\pi)_3 = 1$. In each column $(x/\bar{\pi})_6$ is the complex conjugate of $(x/\pi)_6$ (§3.2).

$b \backslash a$	0	1	2	3	4
0	.	1	1	1	1
1	ω	ω^2	$-\omega$	-1	$-\omega^2$
2	ω	-1	ω^2	$-\omega^2$	$-\omega$
3	ω	$-\omega$	$-\omega^2$	ω^2	-1
4	ω	$-\omega^2$	-1	$-\omega$	ω^2

Table 5: The sextic symbol $(\alpha/5)_6$ for $\alpha = a + b\omega$, $0 \leq a, b \leq 4$, a complete set of residues modulo the inert prime 5 (primary generator -5 , norm 25). In the row $b = 0$ (rational integers), the nonzero residues have symbol 1; the origin has symbol 0, displayed as a dot. Each sixth root of unity occurs 4 times. Moving from α to $\omega\alpha$ multiplies the entry by ω , and $(\bar{\alpha}/5)_6 = \overline{(\alpha/5)_6}$.

π	$N\pi$	$N\pi \bmod 36$	-1	ω	$1+\omega$	λ	2	3	5	7
$1+3\omega$	7	7	-1	ω	$-\omega^2$	-1	ω	$-\omega^2$	$-\omega$	.
$-2-3\omega$	7	7	-1	ω	$-\omega^2$	ω	ω^2	$-\omega$	$-\omega^2$	.
$4+3\omega$	13	13	1	ω^2	ω	$-\omega^2$	$-\omega^2$	ω^2	-1	$-\omega$
$1-3\omega$	13	13	1	ω^2	ω	-1	$-\omega$	ω	-1	$-\omega^2$
$-2+3\omega$	19	19	-1	1	-1	$-\omega$	$-\omega^2$	$-\omega^2$	ω^2	1
$-5-3\omega$	19	19	-1	1	-1	ω^2	$-\omega$	$-\omega$	ω	1
-5	25	25	1	ω	ω^2	$-\omega^2$	1	1	.	1
$1+6\omega$	31	31	-1	ω^2	$-\omega$	-1	1	$-\omega$	ω^2	ω
$-5-6\omega$	31	31	-1	ω^2	$-\omega$	ω^2	1	$-\omega^2$	ω	ω^2
$7+3\omega$	37	1	1	1	1	ω	$-\omega$	ω^2	$-\omega^2$	ω^2
$4-3\omega$	37	1	1	1	1	ω^2	$-\omega^2$	ω	$-\omega$	ω
$7+6\omega$	43	7	-1	ω	$-\omega^2$	ω	-1	$-\omega$	$-\omega$	$-\omega^2$
$1-6\omega$	43	7	-1	ω	$-\omega^2$	-1	-1	$-\omega^2$	$-\omega^2$	$-\omega$
$4+9\omega$	61	25	1	ω	ω^2	ω^2	$-\omega^2$	1	ω^2	$-\omega^2$
$-5-9\omega$	61	25	1	ω	ω^2	ω^2	$-\omega$	1	ω	$-\omega$
$7+9\omega$	67	31	-1	ω^2	$-\omega$	ω	$-\omega$	-1	-1	$-\omega^2$
$-2-9\omega$	67	31	-1	ω^2	$-\omega$	$-\omega$	$-\omega^2$	-1	-1	$-\omega$
$1+9\omega$	73	1	1	1	1	-1	ω	1	$-\omega^2$	-1
$-8-9\omega$	73	1	1	1	1	-1	ω^2	1	$-\omega$	-1
$10+3\omega$	79	7	-1	ω	$-\omega^2$	-1	ω^2	$-\omega^2$	ω	$-\omega$
$7-3\omega$	79	7	-1	ω	$-\omega^2$	ω	ω	$-\omega$	ω^2	$-\omega^2$
$-8+3\omega$	97	25	1	ω	ω^2	-1	ω^2	ω^2	$-\omega^2$	$-\omega^2$
$-11-3\omega$	97	25	1	ω	ω^2	$-\omega$	ω	ω	$-\omega$	$-\omega$
$-2+9\omega$	103	31	-1	ω^2	$-\omega$	ω	ω^2	-1	$-\omega$	ω
$-11-9\omega$	103	31	-1	ω^2	$-\omega$	$-\omega$	ω	-1	$-\omega^2$	ω^2
$7+12\omega$	109	1	1	1	1	$-\omega$	-1	ω^2	ω^2	ω^2
$-5-12\omega$	109	1	1	1	1	$-\omega^2$	-1	ω	ω	ω
-11	121	13	1	ω^2	ω	ω	1	1	1	1

Table 6: The sextic symbol $(x/\pi)_6$ for the primary primes $\pi \nmid 6$ of norm ≤ 121 (rows) and $x = -1, \omega, 1+\omega, \lambda, 2, 3, 5, 7$ (columns), where $\lambda = 1 - \omega$ and $1 + \omega = -\omega^2$ generates the units. A dot means $\pi \mid x$. The unit columns depend only on $N\pi$ modulo 36 (3.3). In the rational columns conjugate primes give conjugate values, and the inert primes $-5, -11$ give 1 (§3.2).

	$1 + 3\omega$	$-2 - 3\omega$	$4 + 3\omega$	$1 - 3\omega$	$-2 + 3\omega$	$-5 - 3\omega$	-5	$1 + 6\omega$	$-5 - 6\omega$
$1 + 3\omega$	$\cdot$	-1	ω^2	$-\omega$	$-\omega^2$	$-\omega^2$	$-\omega$	1	ω^2
$-2 - 3\omega$	-1	$\cdot$	$-\omega^2$	ω	$-\omega$	$-\omega$	$-\omega^2$	ω	1
$4 + 3\omega$	$-\omega^2$	ω^2	$\cdot$	-1	ω	-1	-1	ω	$-\omega^2$
$1 - 3\omega$	ω	$-\omega$	-1	$\cdot$	-1	ω^2	-1	$-\omega$	ω^2
$-2 + 3\omega$	ω^2	$-\omega$	$-\omega$	1	$\cdot$	-1	ω^2	$-\omega^2$	$-\omega$
$-5 - 3\omega$	$-\omega^2$	ω	1	$-\omega^2$	-1	$\cdot$	ω	$-\omega^2$	$-\omega$
-5	ω	ω^2	-1	-1	$-\omega^2$	$-\omega$	$\cdot$	$-\omega^2$	$-\omega$
$1 + 6\omega$	-1	ω	$-\omega$	ω	ω^2	$-\omega^2$	ω^2	$\cdot$	-1
$-5 - 6\omega$	ω^2	-1	ω^2	$-\omega^2$	$-\omega$	ω	ω	-1	$\cdot$

Table 7: The sextic residue symbol $(\pi/\rho)_6$ for the primary primes $\pi, \rho \nmid 6$ of norm ≤ 31 , with π indexing the row and ρ the column. The squares of the entries form the symmetric table of cubic symbols (Table 3, without -2), so the entries in positions (π, ρ) and (ρ, π) agree up to sign. The sign is the quadratic reciprocity factor $(\pi/\rho)_2(\rho/\pi)_2$ (§3.5).

References

- [1] D. A. Cox, *Primes of the Form $x^2 + ny^2$* , 2nd ed., Wiley, 2013.
- [2] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151–182.
- [3] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Graduate Texts in Mathematics 74, Springer, 2000.
- [4] A. Dunn and M. Radziwiłł, *Bias in cubic Gauss sums: Patterson’s conjecture*, Ann. of Math. (2) **200** (2024), 967–1057.
- [5] L. Goldmakher and B. Louvel, *A quadratic large sieve inequality over number fields*, Math. Proc. Cambridge Philos. Soc. **154** (2013), 193–212.
- [6] D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), 235–275.
- [7] D. R. Heath-Brown and S. J. Patterson, *The distribution of Kummer sums at prime arguments*, J. Reine Angew. Math. **310** (1979), 111–130.
- [8] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics 84, Springer, 1990.
- [9] T. Kubota, *Ein arithmetischer Satz über eine Matrizengruppe*, J. Reine Angew. Math. **222** (1966), 55–57.
- [10] T. Kubota, *On Automorphic Functions and the Reciprocity Law in a Number Field*, Lectures in Mathematics, Department of Mathematics, Kyoto University, No. 2, Kinokuniya, Tokyo, 1969.
- [11] OpenAI, papers on the quasi-Riemann hypothesis (September 30 and October 5, 2026), github.com/openai/math.
- [12] S. J. Patterson, *A cubic analogue of the theta series*, J. Reine Angew. Math. **296** (1977), 125–161.
- [13] OpenAI, *The Quasi-Riemann Hypothesis*, manuscript dated October 5, 2026, [manuscript and source on GitHub](#). Section and equation numbers refer to its PDF.