(*January 11, 2011*)

Factorization of zeta-functions, reciprocity laws, non-vanishing

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

Dirichlet's 1837 theorem on primes in arithmetic progressions needs a *non-vanishing* result for L-functions, namely, $L(1,\chi) \neq 0$ for Dirichlet characters χ.

Dirichlet proved this in simple cases by showing that these L-functions are factors in *zeta functions* $\zeta_{\mathfrak{o}}(s)$ of rings of integers $\mathfrak{o} = \mathbb{Z}[\omega]$ with ω a root of unity, and using simple properties of the zeta functions $\zeta_{\mathfrak{o}}(s)$. The result is clearest for characters defined modulo a prime q: for ω a primitive q^{th} root of unity,

$$\zeta(s) \times \prod_{\text{non–trivial } \chi \bmod q} L(s,\chi) \;=\; \text{zeta function } \zeta_{\mathfrak{o}}(s) \text{ of } \mathfrak{o} = \mathbb{Z}[\omega] \qquad (\text{with } \omega \text{ a } q^{th} \text{ root of } 1)$$

We know the Laurent expansion of $\zeta(s)$ at 1:

$$\zeta(s) \;=\; \frac{1}{s-1} + (\text{holomorphic at } s = 1)$$

Various methods prove that, for non-trivial χ, $L(s,\chi)$ extends to a *holomorphic* function near $s = 1$. If we *also* know that

$$\zeta_{\mathfrak{o}}(s) \;=\; \frac{\kappa}{s-1} + (\text{holomorphic at } s = 1) \qquad (\text{for non-zero } \kappa \in \mathbb{C})$$

then none of the $L(s,\chi)$ can vanish at $s = 1$.

The factorization of $\zeta_{\mathfrak{o}}(s)$ is the main issue. After giving a definition of this zeta function, we will see that the factorization is equivalent to understanding the behavior of rational primes in the extension ring $\mathbb{Z}[\omega]$ of $\mathbb{Z}$: do they *stay prime*, or do they *factor* as products of primes in $\mathbb{Z}[\omega]$?

A complication is that the rings $\mathbb{Z}[\omega]$ are rarely principal ideal domains. To delay contemplation of this, we treat several examples of factorization where the rings involved *are* principal ideal domains.

A factorization of a zeta function of an extension as a product of Dirichlet L-functions of the base ring is a type of **reciprocity law**. [1]

The secondary issue is the slight analytic continuation [2] of $\zeta_{\mathfrak{o}}(s)$, and certification that it has a non-trivial pole at $s = 1$. In the simplest cases, this is literally a calculus exericise. The general argument is non-trivial,

[1] The first reciprocity law was *quadratic reciprocity*, conjectured by Legendre and Gauss, and proven by Gauss in 1799. In the mid-19th century, Eisenstein proved *cubic* and *quartic* reciprocity. About 1928, Takagi and Artin proved a general reciprocity law, called *classfield theory*, for *abelian* field extensions. In the late 1960's, Langlands formulated conjectures including reciprocity laws for *non-abelian* extensions.

[2] A decisive understanding of the analytic continuation of zeta functions of number fields was not obtained until E. Hecke's work of 1917. Dedekind had systematically defined these zetas around 1870, and established analytic continuation to strips of the form $\text{Re}(s) > 1 - \frac{1}{n}$, where n is the degree of the field extension. The case of cyclotomic fields had been treated decades earlier, motivated by work on Fermat's last theorem, so was available to Dirichlet. About 1950, Iwasawa and Tate (independently) modernized Hecke's treatment, having the effect that the general case is so simple that it looks like a modernized form of Riemann's argument for $\mathbb{Z}$.

requiring appreciation of Dirichlet's *Units Theorem*, and *finiteness of class number*. Rather than give a general argument, we treat several examples.

Systematic treatment of such factorization, and of the analytic continuation, will be taken up later.

---

1. *Gaussian integers* $\mathfrak{o} = \mathbb{Z}[i]$

The ring $\mathfrak{o} = \mathbb{Z}[i]$ of Gaussian integers is the simplest example for many questions.

[1.1] The norm Let $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$ be the non-trivial automorphism

$$\sigma \ : \ a + bi \ \longrightarrow \ a - bi \qquad\qquad (\text{with } a, b \in \mathbb{Q})$$

The automorphism σ stabilizes $\mathfrak{o}$. Let $N : \mathbb{Q}(i) \to \mathbb{Q}$ be the *norm*

$$N(a+bi) \ = \ (a+bi) \cdot (a+bi)^\sigma \ = \ (a+bi)(a-bi) \ = \ a^2 + b^2 \qquad\qquad (\text{with } a, b \in \mathbb{Q})$$

The norm maps $\mathbb{Q}(i) \to \mathbb{Q}$, and $\mathfrak{o} \to \mathbb{Z}$. Since σ is a field automorphism, the norm is *multiplicative*:

$$N(\alpha\beta) \ = \ (\alpha\beta) \cdot (\alpha\beta)^\sigma \ = \ \alpha\alpha^\sigma \cdot \beta\beta^\sigma \ = \ N\alpha \cdot N\beta$$

[1.2] Units $\mathfrak{o}^\times$ For $\alpha\beta = 1$ in $\mathfrak{o}$, taking norms gives $N\alpha \cdot N\beta = 1$. Since the norm maps $\mathfrak{o} \to \mathbb{Z}$, $N\alpha = \pm 1$. Since the norm is of the form $a^2 + b^2$, it must be 1. That is, the norm of a unit in the Gaussian integers is 1.

It is easy to determine all the units: solve $a^2 + b^2 = 1$ for integers a, b. This finds the four units:

$$\mathfrak{o}^\times \ = \ \{1, -1, i, -i\}$$

[1.3] Euclidean-ness We claim that the Gaussian integers $\mathfrak{o}$ form a *Euclidean* ring, in the sense that, given α, β in $\mathfrak{o}$ with $\beta \neq 0$, we can divide α by β with an integer remainder *smaller* than β, when measured by the *norm*. That is, given α, β with $\beta \neq 0$, there is $q \in \mathfrak{o}$ such that

$$N(\alpha - q \cdot \beta) \ < \ N\beta \qquad\qquad (\text{given } \alpha, \beta \neq 0, \text{ for some } q \in \mathfrak{o})$$

To prove this, observe that the inequality is equivalent to the inequality obtained by dividing through by $N\beta$, using the multiplicativity:

$$N(\frac{\alpha}{\beta} - q) \ < \ N(1) \ = \ 1$$

That is, given $\alpha/\beta \in \mathbb{Q}(i)$, there should be $q \in \mathfrak{o}$ such that $N(\gamma - q) < 1$. Indeed, let $\alpha/\gamma = a + bi$ with $a, b \in Q$, and let $a', b' \in \mathbb{Z}$ be the closest integers to a, b, respectively. (If a or b falls exactly half-way between integers, choose either.) Then $|a - a'| \leq \frac{1}{2}$ and $|b - b'| \leq \frac{1}{2}$, and

$$N(\frac{\alpha}{\beta} - q) \ = \ (a-a')^2 + (b-b')^2 \ \leq \ (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 \ = \ \tfrac{1}{4} + \tfrac{1}{4} \ < \ 1$$

This proves the Euclidean-ness. Therefore, the Gaussian integers form a *principal ideal domain*, and a *unique factorization domain*.

[1.4] Behavior of primes in the extension $\mathfrak{o}$ of $\mathbb{Z}$ Prime numbers p in $\mathbb{Z}$, which we'll call *rational primes* to distinguish them from primes in other rings, are not usually prime in larger rings such as $\mathfrak{o}$. For example, the prime 5 factors as a product

$$5 \ = \ (2+i) \cdot (2-i)$$

(Since the norms of $2 \pm i$ are both 5, these are not units.)

There is a surprisingly clear description of what happens:

[1.4.1] Theorem: A rational prime p stays prime in $\mathfrak{o}$ if and only if $p = 3 \bmod 4$. A rational prime $p = 1 \bmod 4$ factors as $p = p_1 p_2$ with distinct primes p_i. The rational prime 2 ramifies: $2 = (1+i)(1-i)$, where $1+i$ and $1-i$ differ by a unit.

[1.4.2] Remark: Primes that *stay* prime are *inert*, and primes that *factor* (with no factor repeating) are said to *split*. A prime that factors and has *repeated factors* is *ramified*.

Proof: The case of the prime 2 is clear. Recall that an ideal I in a commutative ring R is *prime* if and only if R/I is an *integral domain*. Then

$$\mathbb{Z}[i]/\langle p\rangle \;\approx\; \mathbb{Z}[x]/\langle x^2+1, p\rangle \;\approx\; \Big(\mathbb{Z}[x]/\langle p\rangle\Big)/\langle x^2+1\rangle \;\approx\; \mathbb{F}_p[x]/\langle x^2+1\rangle$$

where $\mathbb{F}_p \approx \mathbb{Z}/p$ is the finite field with p elements. This is a quadratic field extension of $\mathbb{F}_p$ if and only if x^2+1 is irreducible in $\mathbb{F}_p$. For odd p, this happens if and only if there is no primitive fourth root of unity in $\mathbb{F}_p$. Since $\mathbb{F}_p^\times$ is cyclic of order $p-1$, there is a primitive fourth root of unity in $\mathbb{F}_p$ if and only if $4|p-1$, for odd p. That is, if $p = 3 \bmod 4$, x^2+1 is irreducible in $\mathbb{F}_p$, and p stays prime in $\mathbb{Z}[i]$.

When $p = 1 \bmod 4$, because $\mathbb{F}_p$ contains primitive fourth roots of unity, there are $\alpha, \beta \in \mathbb{F}_p$ such that $x^2+1 = (x-\alpha)(x-\beta)$ in $\mathbb{F}_p[x]$. The derivative of x^2+1 is $2x$, and 2 is invertible mod p, so $\gcd(x^2+1, 2x) = 1$ in $\mathbb{F}_p[x]$. Thus, $\alpha \neq \beta$. Thus, by Sun-Ze's theorem

$$\mathbb{Z}[i]/\langle p\rangle \;\approx\; \frac{\mathbb{F}_p[x]}{\langle x^2+1\rangle} \;\approx\; \frac{\mathbb{F}_p[x]}{\langle x-\alpha\rangle} \times \frac{\mathbb{F}_p[x]}{\langle x-\beta\rangle} \;\approx\; \mathbb{F}_p \times \mathbb{F}_p$$

since taking the quotient of $\mathbb{F}_p[x]$ by the ideal generated by $x-\gamma$ simply maps x to γ. These quotients of $\mathbb{F}_p[x]$ by the linear polynomials $x-\alpha$ and $x-\beta$ are obviously fields.

We claim that in the latter situation, the ideal $p \cdot \mathbb{Z}[i]$ is of the form $p_1 p_2 \cdot \mathbb{Z}[i]$ for *distinct* (non-associate)[3] prime elements p_i of $\mathbb{Z}[i]$. More generally, we have

[1.4.3] Lemma: For a principal ideal domain R, an ideal I, suppose there is an isomorphism

$$\varphi \;:\; R \longrightarrow R/I \;\approx\; D_1 \times D_2$$

to a product of integral domains D_i (with $0 \neq 1$ in each). Then the ideal $\ker\varphi$ is generated by a product $p_1 p_2$ of two distinct (non-associate) prime elements p_i.

Proof: (of Lemma) Note that, in a *principal* ideal domain, every non-zero prime ideal is *maximal*. Let φ_i be the further composition of φ with the projection to D_i. Then the kernel $\ker\varphi_i$ of $\varphi_i : R \to D_i$ is a prime ideal containing I, and

$$\ker\varphi \;=\; \ker\varphi_1 \cap \ker\varphi_2$$

Necessarily $\ker\varphi_1 \neq \ker\varphi_2$, or else $I = \ker\varphi_1 = \ker\varphi_2$ would already be prime, and R/I would be an integral domain, not a product. Let $\ker\varphi_i = p_i \cdot R$ for non-associate prime elements p_1, p_2 of R. Then

$$I \;=\; p_1 R \cap p_2 R \;=\; \{r \in R \;:\; r = a_1 p_1 = a_2 p_2 \text{ for some } a_1, a_2 \in R\}$$

[3] The obvious sense of *distinct* prime elements α, β in a principal ideal domain should be that neither divides the other. Equivalently, they generate distinct ideals. Thus, neither is a *unit* multiple of the other. The property of not differeing by units is sometimes termed being *non-associate*.

Since p_1 and p_2 are distinct primes, $p_2|a_1$ and $p_1|a_2$. Thus, $I = p_1p_2 \cdot R$, proving the lemma. ///

The lemma yields the assertion of the theorem. ///

[1.4.4] Remark: Description of behaviors in an extension, in terms of behavior in the ground ring, is a *reciprocity law.*

[1.5] A quadratic symbol as Dirichlet character: conductor The *quadratic symbol* that tells whether or not -1 is a square mod p is

$$\left(\frac{-1}{p}\right)_2 = \left\{ \begin{array}{ll} 0 & (p=2) \\ +1 & (\text{when } -1 \text{ is a square mod } p) \\ -1 & (\text{when } -1 \text{ is not a square mod } p) \end{array} \right\} \qquad (\text{for primes } p)$$

The previous discussion shows that this quadratic symbol is determined by p mod 4. That is, the *conductor* of this symbol is 4. That is, this quadratic symbol is a *Dirichlet character*

$$\left(\frac{-1}{p}\right)_2 = \left\{ \begin{array}{ll} 0 & (p=2) \\ +1 & (\text{when } p = 1 \bmod 4) \\ -1 & (\text{when } p = 3 \bmod 4) \end{array} \right.$$

[1.6] Definition of $\zeta_{\mathfrak{o}}(s)$ The zeta function of $\mathfrak{o} = \mathbb{Z}[i]$ is a sum over non-zero elements of $\mathfrak{o}$ modulo units:

$$\zeta_{\mathfrak{o}}(s) = \sum_{0 \neq \alpha \in \mathfrak{o} \bmod \mathfrak{o}^\times} \frac{1}{|N\alpha|^s}$$

Since $|\mathfrak{o}^\times| = 4$, this is also

$$\zeta_{\mathfrak{o}}(s) = \frac{1}{4} \sum_{0 \neq \alpha \in \mathfrak{o}} \frac{1}{(N\alpha)^s} = \frac{1}{4} \sum_{m,n \in \mathbb{Z} \text{ not both } 0} \frac{1}{(m^2+n^2)^s}$$

Easy estimates prove that this converges nicely for $\mathrm{Re}\,(s) > 1$. Just as in Euclid's proof of Euler factorization of $\zeta_{\mathbb{Z}}(s)$, the unique factorization in $\mathfrak{o} = \mathbb{Z}[i]$ gives

$$\zeta_{\mathfrak{o}}(s) = \prod_{\text{primes } \pi \bmod \mathfrak{o}^\times} \frac{1}{1 - \frac{1}{|N\pi|^s}} \qquad (\text{for } \mathrm{Re}\,(s) > 1)$$

[1.7] Factoring $\zeta_{\mathfrak{o}}(s)$ We will see that identifying the quadratic symbol for -1 as a Dirichlet character χ yields a factorization of the zeta function $\zeta_{\mathfrak{o}}(s)$

$$\zeta_{\mathfrak{o}}(s) = \zeta_{\mathbb{Z}}(s) \cdot L(s, \chi)$$

To this end, group the Euler factors according to the rational primes the Gaussian prime divides:

$$\zeta_{\mathfrak{o}}(s) = \prod_{\text{rational } p} \prod_{\pi | p} \frac{1}{1 - \frac{1}{|N\pi|^s}}$$

The prime $p = 2$ is *ramified*: $\pi = 1 + i$ is the unique prime dividing 2, and $2 = (1+i)^2/i$. Then

$$\prod_{\pi|2} \frac{1}{1 - \frac{1}{|N\pi|^s}} \;=\; \frac{1}{1 - \frac{1}{|N(1+i)|^s}} \;=\; \frac{1}{1 - \frac{1}{2^s}}$$

$$= \frac{1}{1 - \frac{1}{2^s}} \cdot 1 \quad = \quad 2^{th} \text{ Euler factor of } \zeta_{\mathbb{Z}}(s) \;\times\; 2^{th} \text{ Euler factor of } L(s,\chi)$$

since $\chi(2) = 0$.

Primes $p = 3 \bmod 4$ stay prime in $\mathfrak{o}$, and $\chi(p) = -1$, so

$$\prod_{\pi|p} \frac{1}{1 - \frac{1}{|N\pi|^s}} \;=\; \frac{1}{1 - \frac{1}{|Np|^s}} \;=\; \frac{1}{1 - \frac{1}{p^{2s}}} \;=\; \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 + \frac{1}{p^s}}$$

$$= \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 - \frac{\chi(p)}{p^s}} \quad = \quad p^{th} \text{ Euler factor of } \zeta_{\mathbb{Z}}(s) \;\times\; p^{th} \text{ Euler factor of } L(s,\chi)$$

Primes $p = 1 \bmod 4$ factor as $p = p_1 p_2$, and $\chi(p) = +1$. Note that $p^2 = Np = Np_1 \cdot Np_2$, so since the p_i are not units, $Np_i = p$. Then

$$\prod_{\pi|p} \frac{1}{1 - \frac{1}{|N\pi|^s}} \;=\; \frac{1}{1 - \frac{1}{|Np_1|^s}} \times \frac{1}{1 - \frac{1}{|Np_2|^s}} \;=\; \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 - \frac{1}{p^s}}$$

$$= \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 - \frac{\chi(p)}{p^s}} \quad = \quad p^{th} \text{ Euler factor of } \zeta_{\mathbb{Z}}(s) \;\times\; p^{th} \text{ Euler factor of } L(s,\chi)$$

Putting this all together, for each rational prime p, the product of the π^{th} Euler factors of $\zeta_{\mathfrak{o}}(s)$ for primes π dividing p is exactly the product of the p^{th} Euler factors of $\zeta_{\mathbb{Z}}(s)$ and $L(s,\chi)$. Thus,

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta_{\mathbb{Z}}(s) \cdot L(s,\chi)$$

[1.8] The first pole of $\zeta_{\mathfrak{o}}(s)$

Using the expression

$$\zeta_{\mathfrak{o}}(s) \;=\; \frac{1}{4} \sum_{m,n \in \mathbb{Z} \text{ not both } 0} \frac{1}{(m^2+n^2)^s}$$

the behavior at the first pole can be explicated: we claim that

$$\zeta_{\mathfrak{o}}(s) \;=\; \frac{\pi/4}{s-1} + (\text{holomorphic near } s = 1)$$

The main part is correctly suggested by the heuristic comparison to the corresponding integral:

$$\frac{1}{4} \sum_{m,n \in \mathbb{Z} \text{ not both } 0} \frac{1}{(m^2+n^2)^s} \;\sim\; \frac{1}{4} \int_{x^2+y^2 \geq 1} \frac{dx\,dy}{(x^2+y^2)^s} \;=\; \frac{2\pi}{4} \int_1^\infty \frac{r\,dr}{r^{2s}}$$

$$= \frac{2\pi}{4} \Big[\frac{-1}{(2s-2)\, r^{2s-2}} \Big]_1^\infty \;=\; \frac{\pi/4}{s-1}$$

This more-than-one-dimensional comparison of a sum and an integral requires a little more than the *integral test* in one dimension. One reasonable approach is by *summation-by-parts*, together with a basic *lattice-point counting*.

The lattice-point counting is reasonably intuitive, as follows. The *lattice* in question is $\mathbb{Z}^2$, sitting in $\mathbb{C} \approx \mathbb{R}^2$. The *principle* is that the number of these lattice points inside a disc centered at $(0,0)$ should be the area of the disc, up to a smaller-order error term. More precisely, we claim that [4]

$$\text{card}\big\{(m,n) \ : \ \sqrt{m^2+n^2} < r\big\} \ = \ \pi r^2 + O(r)$$

To prove this, we consider unit squares centered at every lattice point. These overlap only on their boundaries, which have area 0, and fill up the plane. Then, when a lattice-point lies *inside* the disk of radius r, the unit square centered on it certainly lies inside the disk of radius $r + \frac{1}{\sqrt{2}}$, since the radius of a unit square is $1/\sqrt{2}$. When a lattice point lies *outside* the disk of radius r, the unit square centered on it certainly lies *outside* the disk of radius $r - \frac{1}{\sqrt{2}}$. We have two comparisons:

$$\pi\big(r - \frac{1}{\sqrt{2}}\big)^2 \ \leq \ \text{card}\big\{(m,n) \ : \ \sqrt{m^2+n^2} < r\big\} \ \leq \ \pi\big(r + \frac{1}{\sqrt{2}}\big)^2$$

This gives the asserted asymptotic-with-error-term. Let

$$\nu(T) \ = \ \text{card}\{(m,n) \ : \ m^2+n^2 \leq T\}$$

We have shown that $\nu(T) = \pi T + O(\sqrt{T})$. Noting that m^2+n^2 assumes only integer values,

$$\sum_{m,n} \frac{1}{(m^2+n^2)^s} \ = \ \frac{\nu(1)}{1^s} + \sum_{\ell \geq 2} \frac{\nu(\ell) - \nu(\ell-1)}{\ell^s}$$

Summation-by-parts is

$$\frac{\nu(1)}{1^s} + \frac{\nu(2)-\nu(1)}{2^s} + \frac{\nu(3)-\nu(2)}{3^s} + \frac{\nu(4)-\nu(3)}{4^s} + \dots$$

$$= \ \nu(1)\big(\frac{1}{1^s} - \frac{1}{2^s}\big) + \nu(2)\big(\frac{1}{2^s} - \frac{1}{3^s}\big) + \nu(3)\big(\frac{1}{3^s} - \frac{1}{4^s}\big) + \dots$$

Using the first-order estimate

$$\frac{1}{\ell^s} - \frac{1}{(\ell+1)^s} \ = \ \frac{1}{s\,\ell^{s+1}} + O(\frac{1}{\ell^{s+2}})$$

we have

$$\sum_{\ell \geq 1} \nu(\ell)\big(\frac{1}{\ell^s} - \frac{1}{(\ell+1)^s}\big) \ = \ \sum_{\ell \geq 1} \big(\pi\ell + O(\sqrt{\ell})\big) \cdot \big(\frac{1}{s\,\ell^{s+1}} + O(\frac{1}{\ell^{s+2}})\big)$$

$$= \ \frac{\pi}{s} \sum_{\ell \geq 1} \frac{1}{\ell^s} + O\Big(\sum_{\ell} \frac{1}{\ell^{s+\frac{1}{2}}}\Big) \ = \ \frac{\pi}{s}\zeta(s) + O(\zeta(s+\tfrac{1}{2})) \ = \ \frac{\pi}{s}\frac{1}{s-1} + O(1) \qquad (\text{as } s \to 1^+)$$

Since $s = 1 + (s-1)$, this can be written as

$$\sum_{m,n} \frac{1}{(m^2+n^2)^s} \ = \ \frac{\pi}{s-1} + O(1) \qquad (\text{as } s \to 1^+)$$

[4] As usual, the Landau big-Oh notation $O(r)$ means a function bounded by $C \cdot r$. In the present context, it is implied that $r \to +\infty$.

Dividing by 4 to account for the units,

$$\zeta_{\mathfrak{o}}(s) \;=\; \frac{\pi/4}{s-1} + O(1) \qquad\qquad (\text{as } s \to 1^+)$$

[1.9] Non-vanishing of $L(1,\chi)$ Earlier, summation by parts showed that $L(s,\chi)$ is *finite* up to $\mathrm{Re}\,(s) \geq \frac{1}{2}$. Thus, the factorization and evaluation of residues at $s = 1$ give

$$\frac{\pi/4}{s-1} + O(1) \;=\; \zeta_{\mathfrak{o}}(s) \;=\; \zeta_{\mathbb{Z}}(s) \cdot L(s,\chi) \;=\; \Big(\frac{1}{s-1} + O(1)\Big) \cdot \Big(L(1,\chi) + O(s-1)\Big)$$

From this,

$$L(1,\chi) \;=\; \frac{\pi}{4}$$

[1.9.1] Remark: There are only two Dirichlet characters mod 4, the trivial one and

$$\chi(p) \;=\; \Big(\frac{-1}{p}\Big)_2$$

treated above. The non-vanishing $L(1,\chi) = \pi/4$ completely legitimizes the Dirichlet's argument for primes in arithmetic progressions modulo 4.

---

2. *Eisenstein integers* $\mathfrak{o} = \mathbb{Z}[\omega]$

We repeat the discussion for the Eisenstein integers $\mathfrak{o} = \mathbb{Z}[\omega]$, where ω is a primitive cube root of 1:

$$\omega \;=\; \frac{-1+\sqrt{-3}}{2}$$

[2.1] The norm Let $\sigma : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ be the non-trivial automorphism

$$\sigma \;:\; a + b\omega \;\longrightarrow\; a + b\overline{\omega} \;=\; a + b\omega^2 \qquad\qquad (\text{with } a, b \in \mathbb{Q})$$

The automorphism σ stabilizes $\mathfrak{o}$. Let $N : \mathbb{Q}(\omega) \to \mathbb{Q}$ be the *norm*

$$N(a+b\omega) \;=\; (a+b\omega)\cdot(a+b\omega)^\sigma \;=\; (a+b\omega)(a+b\overline{\omega}) \;=\; a^2 + ab + b^2 \qquad\qquad (\text{with } a, b \in \mathbb{Q})$$

The norm maps $\mathbb{Q}(\omega) \to \mathbb{Q}$, and $\mathfrak{o} \to \mathbb{Z}$. Since σ is a field automorphism, the norm is *multiplicative*:

$$N(\alpha\beta) \;=\; (\alpha\beta)\cdot(\alpha\beta)^\sigma \;=\; \alpha\alpha^\sigma \cdot \beta\beta^\sigma \;=\; N\alpha \cdot N\beta$$

[2.2] Units $\mathfrak{o}^\times$ For $\alpha\beta = 1$ in $\mathfrak{o}$, taking norms gives $N\alpha \cdot N\beta = 1$. Since the norm maps $\mathfrak{o} \to \mathbb{Z}$, $N\alpha = \pm 1$. Since the norm is of the form $a^2 + ab + b^2 = (a + \frac{1}{2}b)^2 + \frac{3}{4}b^2$, it must be 1. That is, the norm of a unit in the Eisenstein integers is 1.

It is easy to determine all the units: solve $a^2 + ab + b^2 = 1$ for integers a, b. This finds the six units:

$$\mathfrak{o}^\times \;=\; \{1,\, -1,\, \omega,\, \omega^2,\, -\omega,\, -\omega^2\}$$

[2.3] Euclidean-ness We claim that the Eisenstein integers $\mathfrak{o}$ form a *Euclidean* ring. That is, given α, β with $\beta \neq 0$, there is $q \in \mathfrak{o}$ such that

$$N(\alpha - q \cdot \beta) \ < \ N\beta \qquad\qquad (\text{given } \alpha, \beta \neq 0, \text{ for some } q \in \mathfrak{o})$$

To prove this, observe that the inequality is equivalent to the inequality obtained by dividing through by $N\beta$, using the multiplicativity:

$$N(\frac{\alpha}{\beta} - q) \ < \ N(1) \ = \ 1$$

That is, given $\alpha/\beta \in \mathbb{Q}(\omega)$, there should be $q \in \mathfrak{o}$ such that $N(\gamma - q) < 1$. Indeed, let $\alpha/\gamma = a + b\omega$ with $a, b \in Q$, and let $a', b' \in \mathbb{Z}$ be the closest integers to a, b, respectively. (If a or b falls exactly half-way between integers, choose either.) Then $|a - a'| \leq \frac{1}{2}$ and $|b - b'| \leq \frac{1}{2}$, and

$$N(\frac{\alpha}{\beta} - q) \ = \ (a-a')^2 + (a-a')(b-b') + (b-b')^2 \ \leq \ (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 \ = \ \tfrac{3}{4} \ < \ 1$$

This proves the Euclidean-ness. Therefore, the Eisenstein integers form a *principal ideal domain*, and a *unique factorization domain*.

[2.4] Behavior of primes in the extension $\mathfrak{o}$ of $\mathbb{Z}$ The description is very clear:

[2.4.1] Theorem: A rational prime p stays prime in $\mathfrak{o}$ if and only if $p = 2 \bmod 3$. A rational prime $p = 1 \bmod 3$ factors as $p = p_1 p_2$ with distinct primes p_i. The rational prime 3 ramifies: $3 = -\sqrt{-3} \cdot \sqrt{-3}$.

Proof: The case of the prime 3 is clear. Recall that an ideal I in a commutative ring R is *prime* if and only if R/I is an *integral domain*. Then

$$\mathbb{Z}[\omega]/\langle p\rangle \ \approx \ \mathbb{Z}[x]/\langle x^2 + x + 1, p\rangle \ \approx \ \Big(\mathbb{Z}[x]/\langle p\rangle\Big)/\langle x^2 + x + 1\rangle \ \approx \ \mathbb{F}_p[x]/\langle x^2 + x + 1\rangle$$

where $\mathbb{F}_p \approx \mathbb{Z}/p$ is the finite field with p elements. This is a quadratic field extension of $\mathbb{F}_p$ if and only if $x^2 + x + 1$ is irreducible in $\mathbb{F}_p$. For odd p, this happens if and only if there is no primitive third root of unity in $\mathbb{F}_p$. Since $\mathbb{F}_p^\times$ is cyclic of order $p - 1$, there is a primitive third root of unity in $\mathbb{F}_p$ if and only if $3|p - 1$, for odd p. That is, if $p = 2 \bmod 3$, $x^2 + x + 1$ is irreducible in $\mathbb{F}_p$, and p stays prime in $\mathbb{Z}[\omega]$.

When $p = 1 \bmod 3$, because $\mathbb{F}_p$ contains primitive third roots of unity, there are $\alpha, \beta \in \mathbb{F}_p$ such that $x^2 + x + 1 = (x - \alpha)(x - \beta)$ in $\mathbb{F}_p[x]$. The derivative of $x^2 + x + 1$ is $2x + 1$, so $\gcd(x^2 + x + 1, 2x + 1) = 1$ in $\mathbb{F}_p[x]$. Thus, $\alpha \neq \beta$. Thus, by Sun-Ze's theorem

$$\mathbb{Z}[\omega]/\langle p\rangle \ \approx \ \frac{\mathbb{F}_p[x]}{\langle x^2 + x + 1\rangle} \ \approx \ \frac{\mathbb{F}_p[x]}{\langle x - \alpha\rangle} \times \frac{\mathbb{F}_p[x]}{\langle x - \beta\rangle} \ \approx \ \mathbb{F}_p \times \mathbb{F}_p$$

since taking the quotient of $\mathbb{F}_p[x]$ by the ideal generated by $x - \gamma$ simply maps x to γ. These quotients of $\mathbb{F}_p[x]$ by the linear polynomials $x - \alpha$ and $x - \beta$ are obviously fields.

By the general lemma proven in the discussion of the Gaussian integers, in the latter situation, the ideal $p \cdot \mathbb{Z}[\omega]$ is of the form $p_1 p_2 \cdot \mathbb{Z}[\omega]$ for *distinct* (non-associate) prime elements p_i of $\mathbb{Z}[\omega]$. This finishes the theorem. ///

[2.5] A quadratic symbol as Dirichlet character: conductor The field extension at hand is $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. The *quadratic symbol* that tells whether or not -3 is a square mod p is

$$\Big(\frac{-3}{p}\Big)_2 \ = \ \left\{ \begin{array}{ll} 0 & (p = 3) \\ +1 & (\text{when } -3 \text{ is a square mod } p) \\ -1 & (\text{when } -3 \text{ is not a square mod } p) \end{array} \right\} \qquad (\text{for primes } p)$$

Since ω and $\sqrt{-3}$ are expressible in terms of each other, the previous discussion shows that this quadratic symbol is determined by p mod 3. That is, the *conductor* of this symbol is 3. That is, this quadratic symbol is a *Dirichlet character*

$$\left(\frac{-3}{p}\right)_2 \;=\; \begin{cases} 0 & (p=3) \\ +1 & (\text{when } p=1 \bmod 3) \\ -1 & (\text{when } p=2 \bmod 3) \end{cases}$$

[2.6] Definition of $\zeta_{\mathfrak{o}}(s)$ The zeta function of $\mathfrak{o} = \mathbb{Z}[\omega]$ is a sum over non-zero elements of $\mathfrak{o}$ modulo units:

$$\zeta_{\mathfrak{o}}(s) \;=\; \sum_{0\neq\alpha\in\mathfrak{o} \bmod \mathfrak{o}^\times} \frac{1}{|N\alpha|^s}$$

Since $|\mathfrak{o}^\times| = 6$, this is also

$$\zeta_{\mathfrak{o}}(s) \;=\; \frac{1}{6}\sum_{0\neq\alpha\in\mathfrak{o}} \frac{1}{(N\alpha)^s} \;=\; \frac{1}{6}\sum_{m,n\in\mathbb{Z} \text{ not both } 0} \frac{1}{(m^2++mn+n^2)^s}$$

Easy estimates prove that this converges nicely for $\mathrm{Re}(s) > 1$. Unique factorization in $\mathfrak{o} = \mathbb{Z}[\omega]$ gives

$$\zeta_{\mathfrak{o}}(s) \;=\; \prod_{\text{primes } \pi \bmod \mathfrak{o}^\times} \frac{1}{1-\dfrac{1}{|N\pi|^s}} \qquad\qquad (\text{for } \mathrm{Re}(s)>1)$$

[2.7] Factoring $\zeta_{\mathfrak{o}}(s)$ Identifying the quadratic symbol for -3 as a Dirichlet character χ yields a factorization of the zeta function $\zeta_{\mathfrak{o}}(s)$

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta_{\mathbb{Z}}(s)\cdot L(s,\chi)$$

To this end, group the Euler factors according to the rational primes the Eisenstein prime divides:

$$\zeta_{\mathfrak{o}}(s) \;=\; \prod_{\text{rational } p}\ \prod_{\pi|p} \frac{1}{1-\dfrac{1}{|N\pi|^s}}$$

The prime $p = 3$ is *ramified*. Then

$$\prod_{\pi|3} \frac{1}{1-\dfrac{1}{|N\pi|^s}} \;=\; \frac{1}{1-\dfrac{1}{|N(\sqrt{-3})|^s}} \;=\; \frac{1}{1-\dfrac{1}{3^s}}$$

$$=\; \frac{1}{1-\dfrac{1}{3^s}}\cdot 1 \;=\; 3^{th} \text{ Euler factor of } \zeta_{\mathbb{Z}}(s) \;\times\; 3^{th} \text{ Euler factor of } L(s,\chi)$$

since $\chi(3) = 0$.

Primes $p = 2 \bmod 3$ stay prime in $\mathfrak{o}$, and $\chi(p) = -1$, so

$$\prod_{\pi|p} \frac{1}{1-\dfrac{1}{|N\pi|^s}} \;=\; \frac{1}{1-\dfrac{1}{|Np|^s}} \;=\; \frac{1}{1-\dfrac{1}{p^{2s}}} \;=\; \frac{1}{1-\dfrac{1}{p^s}}\times\frac{1}{1+\dfrac{1}{p^s}}$$

$$= \frac{1}{1-\frac{1}{p^s}} \times \frac{1}{1-\frac{\chi(p)}{p^s}} \quad = \quad p^{th} \text{ Euler factor of } \zeta_{\mathbb{Z}}(s) \ \times \ p^{th} \text{ Euler factor of } L(s,\chi)$$

Primes $p = 1 \bmod 3$ factor as $p = p_1 p_2$, and $\chi(p) = +1$. Note that $p^2 = Np = Np_1 \cdot Np_2$, so since the p_i are not units, $Np_i = p$. Then

$$\prod_{\pi|p} \frac{1}{1-\frac{1}{|N\pi|^s}} = \frac{1}{1-\frac{1}{|Np_1|^s}} \times \frac{1}{1-\frac{1}{|Np_2|^s}} = \frac{1}{1-\frac{1}{p^s}} \times \frac{1}{1-\frac{1}{p^s}}$$

$$= \frac{1}{1-\frac{1}{p^s}} \times \frac{1}{1-\frac{\chi(p)}{p^s}} \quad = \quad p^{th} \text{ Euler factor of } \zeta_{\mathbb{Z}}(s) \ \times \ p^{th} \text{ Euler factor of } L(s,\chi)$$

Putting this all together, for each rational prime p, the product of the π^{th} Euler factors of $\zeta_{\mathfrak{o}}(s)$ for primes π dividing p is exactly the product of the p^{th} Euler factors of $\zeta_{\mathbb{Z}}(s)$ and $L(s,\chi)$. Thus,

$$\zeta_{\mathfrak{o}}(s) \ = \ \zeta_{\mathbb{Z}}(s) \cdot L(s,\chi)$$

[2.8] The first pole of $\zeta_{\mathfrak{o}}(s)$

Using the expression

$$\zeta_{\mathfrak{o}}(s) \ = \ \frac{1}{6} \sum_{m,n \in \mathbb{Z} \text{ not both } 0} \frac{1}{(m^2+mn+n^2)^s}$$

the behavior at the first pole can be explicated: we claim that

$$\zeta_{\mathfrak{o}}(s) \ = \ \frac{\pi}{3\sqrt{3}(s-1)} + (\text{holomorphic near } s=1)$$

We use *summation-by-parts*, and *lattice-point counting*.

The lattice-point counting is reasonably intuitive, as follows. The *lattice* in question is $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}\omega$, sitting in $\mathbb{C}$. Every point in $\mathbb{C}$ is uniquely expressible as $a + b\omega$ for $a, b \in \mathbb{R}$. Thus, by subtracting $a + b\omega \in \mathfrak{o}$ from a given point in $z \in \mathbb{C}$, we can arrange that $z - (a + b\omega)$ lies inside the rhombus

$$R \ = \ \{a + b\omega \ : \ -\tfrac{1}{2} \le a \le \tfrac{1}{2}, \ -\tfrac{1}{2} \le b \le \tfrac{1}{2}\}$$

The idea of the counting principle is that the number of points of $\mathfrak{o}$ inside a disc centered at $(0,0)$ should be the area of the disc divided by the area of R, up to a smaller-order error term. More precisely, we claim that

$$\text{card}\big\{(m,n) \ : \ \sqrt{m^2+mn+n^2} < r\big\} \quad = \quad \frac{2\pi r^2}{\sqrt{3}} + O(r)$$

To prove this, we consider copies of R centered at every lattice point. These overlap only on their boundaries, which have area 0, and fill up the plane. Then, when a lattice-point lies *inside* the disk of radius r, the copy of R centered on it certainly lies inside the disk of radius $r + \frac{\sqrt{3}}{2}$, since the radius of R is $\sqrt{3}/2$. When a lattice point lies *outside* the disk of radius r, the copy of R centered on it certainly lies *outside* the disk of radius $r - \frac{\sqrt{3}}{2}$. Note that

$$|a + b\omega|^2 \ = \ N(a + b\omega) \ = \ a^2 + ab + b^2$$

Since the area of R is $\sqrt{3}$,

$$\pi\big(r - \frac{\sqrt{3}}{2}\big)^2 \ \le \ \sqrt{3} \cdot \text{card}\big\{(m,n) : \sqrt{m^2+mn+n^2} < r\big\} \ \le \ \pi\big(r + \frac{\sqrt{3}}{2}\big)^2$$

This gives the asserted asymptotic-with-error-term. Let

$$\nu(T) \;=\; \mathrm{card}\,\{(m,n)\;:\; m^2+mn+n^2 \le T\}$$

We have shown that $\nu(T) = \frac{2\pi}{\sqrt{3}}T + O(\sqrt{T})$. Noting that m^2+mn+n^2 assumes only integer values,

$$\sum_{m,n} \frac{1}{(m^2+mn+n^2)^s} \;=\; \frac{\nu(1)}{1^{2s}} + \sum_{\ell\ge 2} \frac{\nu(\ell)-\nu(\ell-1)}{\ell^{2s}}$$

Summation-by-parts and the first-order estimate

$$\frac{1}{\ell^s} - \frac{1}{(\ell+1)^s} \;=\; \frac{1}{s\,\ell^{s+1}} + O(\frac{1}{\ell^{s+2}})$$

give

$$\sum_{\ell\ge 1} \nu(\ell)\big(\frac{1}{\ell^s} - \frac{1}{(\ell+1)^s}\big) \;=\; \sum_{\ell\ge 1} \big(\frac{2\pi}{\sqrt{3}}\ell + O(\sqrt{\ell})\big)\cdot\big(\frac{1}{s\,\ell^{s+1}} + O(\frac{1}{\ell^{s+2}})\big)$$

$$= \;\frac{2\pi}{s\sqrt{3}}\sum_{\ell\ge 1}\frac{1}{\ell^s} + O\Big(\sum_{\ell}\frac{1}{\ell^{s+\frac{1}{2}}}\Big) \;=\; \frac{2\pi}{s\sqrt{3}}\zeta(s) + O(\zeta(s+\tfrac{1}{2})) \;=\; \frac{2\pi}{s\sqrt{3}(s-1)} + O(1) \qquad (\text{as } s\to 1^+)$$

Since $s = 1+(s-1)$, this can be written as

$$\sum_{m,n} \frac{1}{(m^2+mn+n^2)^s} \;=\; \frac{2\pi}{\sqrt{3}(s-1)} + O(1) \qquad (\text{as } s\to 1^+)$$

Dividing by 6 to account for the units,

$$\zeta_{\mathfrak{o}}(s) \;=\; \frac{\pi}{3\sqrt{3}(s-1)} + O(1) \qquad (\text{as } s\to 1^+)$$

[2.9] Non-vanishing of $L(1,\chi)$ Earlier, another summation by parts showed that $L(s,\chi)$ is *finite* up to $\mathrm{Re}(s) \ge \frac{1}{2}$. Thus, the factorization and evaluation of residues at $s=1$ give

$$\frac{\pi}{3\sqrt{3}(s-1)} + O(1) \;=\; \zeta_{\mathfrak{o}}(s) \;=\; \zeta_{\mathbb{Z}}(s)\cdot L(s,\chi) \;=\; \Big(\frac{1}{s-1}+O(1)\Big)\cdot\Big(L(1,\chi)+O(s-1)\Big)$$

From this,

$$L(1,\chi) \;=\; \frac{\pi}{3\sqrt{3}}$$

[2.9.1] Remark: There are only two Dirichlet characters mod 3, the trivial one and

$$\chi(p) \;=\; \Big(\frac{-3}{p}\Big)_2$$

just treated. The non-vanishing $L(1,\chi) = \pi/3\sqrt{3}$ completely legitimizes the Dirichlet's argument for primes in arithmetic progressions modulo 3.

3. *Integers* $\mathbb{Z}[\sqrt{2}]$

The integers $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ present a new feature, namely, that the group of units $\mathfrak{o}^\times$ is *infinite*. Related to this is the feature that the *norm*

$$N(a + b\sqrt{2}) \;=\; a^2 - 2b^2$$

is no longer a positive-definite [5] quadratic function for $a, b \in \mathbb{R}$.

[3.1] The norm and real imbeddings Let $\rho : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ be the non-trivial automorphism

$$\rho \;:\; a + b\sqrt{2} \;\longrightarrow\; a - b\sqrt{2} \qquad \text{(with } a, b \in \mathbb{Q}\text{)}$$

The automorphism ρ stabilizes $\mathfrak{o}$. Let $N : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}$ be the *norm*

$$N(a + b\sqrt{2}) \;=\; (a + b\sqrt{2}) \cdot (a + b\sqrt{2})^\rho \;=\; (a + b\sqrt{2})(a - b\sqrt{2}) \;=\; a^2 - 2b^2 \qquad \text{(with } a, b \in \mathbb{Q}\text{)}$$

The norm maps $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}$, and $\mathfrak{o} \to \mathbb{Z}$. Since ρ is a field automorphism, the norm is *multiplicative*.

In contrast to the Gaussian integers, where $|a + bi| = |a - bi|$, the sizes of the real numbers $a + b\sqrt{2}$ and $a - b\sqrt{2}$ (with $\sqrt{2}$ the usual positive square root) can be wildly different. Further, in the abstract field $\mathbb{Q}[x]/\langle x^2 - 2\rangle$, there is no way to distinguish a *positive* square root. What we can say is that there are two *real imbeddings* (of fields)

$$\sigma, \tau \;:\; \mathbb{Q}[x]/\langle x^2 - 2\rangle \;\longrightarrow\; \mathbb{R}$$

and that σ, τ differ by ρ, in the sense that

$$\tau \;=\; \sigma \circ \rho$$

[3.2] Units $\mathfrak{o}^\times$ For $\alpha\beta = 1$ in $\mathfrak{o}$, taking norms gives $N\alpha \cdot N\beta = 1$. Since the norm maps $\mathfrak{o} \to \mathbb{Z}$, $N\alpha = \pm 1$. Conversely, when $N\alpha = \pm 1$, then $\alpha \cdot \alpha^\sigma = \pm 1$, so $\alpha \in \mathfrak{o}^\times$. Unlike the Gaussian integers and Eisenstein integers, there are infinitely-many solutions to the equation [6]

$$a^2 - 2b^2 \;=\; \pm 1$$

For example, $N(1 + \sqrt{2}) = -1$, and *powers* of $\eta = 1 + \sqrt{2}$ are *distinct*: for a moment let $\sqrt{2}$ be the *positive real* square root of 2. Then $1 + \sqrt{2} > 1$, so positive integer powers of $1 + \sqrt{2}$ go to $+\infty$. Thus, when $\eta^m = \eta^n$ with $m \le n$, $\eta^{n-m} = 1$, implying $m = n$. [7]

[3.3] Euclidean-ness We claim that the Eisenstein integers $\mathfrak{o}$ form a *Euclidean* ring. That is, given α, β with $\beta \neq 0$, there is $q \in \mathfrak{o}$ such that

$$|N(\alpha - q \cdot \beta)| \;<\; |N\beta| \qquad \text{(given } \alpha, \beta \neq 0\text{, for some } q \in \mathfrak{o}\text{)}$$

Note that now we must takd the abolute value of the norm, since the norm can assume negative values. The inequality is equivalent to the inequality obtained by dividing through by $|N\beta|$, using the multiplicativity:

$$|N(\frac{\alpha}{\beta} - q)| \;<\; |N(1)| \;=\; 1$$

[5] A function $Q(x, y) = Ax^2 + Bxy + Cy^2$, called a *binary quadratic form*, is *positive-definite* if $Q(x, y) = 0$ for *real* x, y implies $x = y = 0$. This is easily detected in terms of the sign of the discriminant $B^2 - 4AC$: the quadratic form is positive-definite if and only if the discriminant is *negative*.

[6] This equation is an instance of the mis-named *Pell's equation*, studied by Fermat.

[7] In fact, η and ± 1 generate the whole units group $\mathfrak{o}^\times$, but we don't need this fact just yet.

That is, given $\alpha/\beta \in \mathbb{Q}(\sqrt{2})$, there should be $q \in \mathfrak{o}$ such that $|N(\gamma - q)| < 1$. Indeed, let $\alpha/\gamma = a + b\sqrt{2}$ with $a, b \in Q$, and let $a', b' \in \mathbb{Z}$ be the closest integers to a, b, respectively. (If a or b falls exactly half-way between integers, choose either.) Then $|a - a'| \leq \frac{1}{2}$ and $|b - b'| \leq \frac{1}{2}$, and

$$N(\frac{\alpha}{\beta} - q) \;=\; |(a-a')^2 - 2(b-b')^2| \;\leq\; (\tfrac{1}{2})^2 + 2 \cdot (\tfrac{1}{2})^2 \;=\; \tfrac{3}{4} \;<\; 1$$

This proves the Euclidean-ness. Therefore, the integers $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ form a *principal ideal domain*, and a *unique factorization domain*.

[3.4] Behavior of primes in the extension $\mathfrak{o}$ of $\mathbb{Z}$

The description is simple:

[3.4.1] Theorem: The rational prime 2 is *ramified*: $2 = \sqrt{2} \cdot \sqrt{2}$ A rational prime p is *inert* in $\mathfrak{o}$ if and only if $p = 3$ or 5 modulo 8. A rational prime $p = 1$ or 7 modulo 8 *splits* as $p = p_1 p_2$ with distinct primes p_i.

Proof: The case of the prime 2 is clear. Since an ideal I in a commutative ring R is *prime* if and only if R/I is an *integral domain*, compute

$$\mathbb{Z}[\sqrt{2}]/\langle p\rangle \;\approx\; \mathbb{Z}[x]/\langle x^2 - 2, p\rangle \;\approx\; \Big(\mathbb{Z}[x]/\langle p\rangle\Big)/\langle x^2 - 2\rangle \;\approx\; \mathbb{F}_p[x]/\langle x^2 - 2\rangle$$

where $\mathbb{F}_p \approx \mathbb{Z}/p$ is the finite field with p elements. This is a quadratic field extension of $\mathbb{F}_p$ if and only if $x^2 - 2$ is irreducible in $\mathbb{F}_p$.

In previous examples, the polynomial in question was *cyclotomic*, so the cyclic-ness of $(\mathbb{Z}/p)^\times$ gives an easy answer to questions about whether the polynomial factored, or not. We need to interpret 2 in terms of roots of unity. Another necessary ingredient, also using cyclic-ness of $(\mathbb{Z}/p)^\times$, is *Euler's criterion*:

[3.4.2] Theorem: For prime p, define the quadratic symbol

$$\Big(\frac{a}{p}\Big)_2 \;=\; \begin{cases} 0 & (\text{when } p|a) \\ \\ 1 & (\text{when } a \text{ is a square mod } p) \\ \\ -1 & (\text{when } a \text{ is a non-square mod } p) \end{cases}$$

Then

$$\Big(\frac{a}{p}\Big)_2 \;=\; a^{\frac{p-1}{2}} \bmod p$$

Proof: When $a = b^2 \bmod p$,

$$a^{\frac{p-1}{2}} = b^{p-1} \bmod p \;=\; \begin{cases} 0 & (\text{when } p|a) \\ \\ 1 & (\text{otherwise}) \end{cases}$$

That was the easy half. On the other hand, when a is a *non-square* mod p, we must invoke the cyclic-ness of $(\mathbb{Z}/p)^\times$: let γ be a generator. Then $a = \gamma^{2\ell+1} \bmod p$ for some integer ℓ, and

$$a^{\frac{p-1}{2}} = \gamma^{(p-1)\ell + \frac{p-1}{2}} \;=\; \gamma^{\frac{p-1}{2}} \bmod p$$

Since γ is of order $p - 1$, that power of it cannot be $1 \bmod p$. But its square is $1 \bmod p$, so it must be $-1 \bmod p$. This proves Euler's criterion. ///

To describe 2 in terms of roots of unity, recall that in the discussion of the Gaussian integers, we noticed that

$$2 \;=\; -i \cdot (1+i)^2$$

Thus, using the latter expression and Euler's criterion,

$$\left(\frac{2}{p}\right)_2 \;=\; 2^{\frac{p-1}{2}} \bmod p \;=\; \big(-i(1+i)^2\big)^{\frac{p-1}{2}} \bmod p \;=\; (-i)^{\frac{p-1}{2}} \cdot (1+i)^{p-1} \bmod p$$

Note that *this computation is taking place in a quotient of a larger ring*, namely the quotient $\mathbb{Z}[i]/\langle p\rangle$ of the Gaussian integers $\mathbb{Z}[i]$. Since p is odd, there is a $2^{-1} \bmod p$, and we can rewrite the previous as

$$(-i)^{\frac{p-1}{2}} \cdot (1+i)^{p-1} \;=\; (-i)^{\frac{p-1}{2}} \cdot \frac{(1+i)^p}{(1+i)} \;=\; \frac{1-i}{2}\,(-i)^{\frac{p-1}{2}} \cdot (1+i)^p$$

By unique factorization in $\mathbb{Z}$, the inner binomial coefficients $p!/j!(p-j)!$ (with $0 < j < p$) are divisible by p, since the denominators have no factor of p. Thus, the binomial expansion of $(1+i)^p$ is just $1+i^p \bmod p$, and the previous is

$$\frac{1-i}{2}\,(-i)^{\frac{p-1}{2}} \cdot (1+i^p) \bmod p \;=\; \begin{cases} \frac{1-i}{2}\,(-i)^{\frac{p-1}{2}} \cdot (1+i) \;=\; (-1)^{\frac{p-1}{4}} & (\text{for } p = 1 \bmod 4) \\ \frac{1-i}{2}\,(-i)^{\frac{p-1}{2}} \cdot (1-i) \;=\; (-i)^{\frac{p-1}{2}+1} & (\text{for } p = 3 \bmod 4) \end{cases}$$

$$= \begin{cases} (-1)^{\frac{p-1}{4}} & (\text{for } p = 1 \bmod 4) \\ (-1)^{\frac{p+1}{4}} & (\text{for } p = 3 \bmod 4) \end{cases} = \begin{cases} 1 & (\text{for } p = 1 \bmod 8) \\ -1 & (\text{for } p = 5 \bmod 8) \\ -1 & (\text{for } p = 3 \bmod 8) \\ 1 & (\text{for } p = 7 \bmod 8) \end{cases}$$

For $(2/p)_2 = -1$, p stays prime in $\mathbb{Z}[\sqrt{2}$, and for $(2/p)_2 = +1$, the general lemma proven in the discussion of the Gaussian integers shows that the ideal $p \cdot \mathbb{Z}[\sqrt{2}]$ is of the form $p_1 p_2 \cdot \mathbb{Z}[\sqrt{2}]$ for *distinct* (non-associate) prime elements p_i of $\mathbb{Z}[\sqrt{2}]$. This finishes the theorem. ///

[3.4.3] Remark: Thus, the quadratic symbol $(2/p)_2$ is a *Dirichlet character* with conductor 8.

[3.5] Definition of $\zeta_{\mathfrak{o}}(s)$ The zeta function of $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ is a sum over non-zero elements of $\mathfrak{o}$ modulo units:

$$\zeta_{\mathfrak{o}}(s) \;=\; \sum_{0 \neq \alpha \in \mathfrak{o} \bmod \mathfrak{o}^\times} \frac{1}{|N\alpha|^s}$$

Since $\mathfrak{o}^\times$ is *infinite*, this zeta function is *not* a constant multiple of a sum over a lattice, in contrast to the Gaussian and Eisenstein examples above.

It is not as trivial now to see that this converges nicely for $\mathrm{Re}(s) > 1$. But, granting convergence, unique factorization in $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ gives the Euler factorization

$$\zeta_{\mathfrak{o}}(s) \;=\; \prod_{\text{primes } \pi \bmod \mathfrak{o}^\times} \frac{1}{1 - \frac{1}{|N\pi|^s}} \qquad\qquad (\text{for } \mathrm{Re}(s) > 1)$$

[3.6] Factoring $\zeta_{\mathfrak{o}}(s)$ Identifying the quadratic symbol for 2 as a Dirichlet character χ yields a factorization of the zeta function $\zeta_{\mathfrak{o}}(s)$

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta_{\mathbb{Z}}(s) \cdot L(s, \chi)$$

To this end, group the Euler factors according to the rational primes the Eisenstein prime divides:

$$\zeta_{\mathfrak{o}}(s) \;=\; \prod_{\text{rational } p} \prod_{\pi | p} \frac{1}{1 - \frac{1}{|N\pi|^s}}$$

The prime $p = 2$ is *ramified*. Then

$$\prod_{\pi|2} \frac{1}{1 - \frac{1}{|N\pi|^s}} \;=\; \frac{1}{1 - \frac{1}{|N(\sqrt{2})|^s}} \;=\; \frac{1}{1 - \frac{1}{2^s}}$$

$$=\; \frac{1}{1 - \frac{1}{2^s}} \cdot 1 \quad = \quad 2^{th} \text{ Euler factor of } \zeta_{\mathbb{Z}}(s) \;\times\; 2^{th} \text{ Euler factor of } L(s, \chi)$$

since $\chi(2) = 0$.

Primes $p = \pm 3 \bmod 8$ stay prime in $\mathfrak{o}$, and $\chi(p) = -1$, so for such primes

$$\prod_{\pi|p} \frac{1}{1 - \frac{1}{|N\pi|^s}} \;=\; \frac{1}{1 - \frac{1}{|Np|^s}} \;=\; \frac{1}{1 - \frac{1}{p^{2s}}} \;=\; \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 + \frac{1}{p^s}}$$

$$=\; \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 - \frac{\chi(p)}{p^s}} \quad = \quad p^{th} \text{ Euler factor of } \zeta_{\mathbb{Z}}(s) \;\times\; p^{th} \text{ Euler factor of } L(s, \chi)$$

Primes $p = \pm 1 \bmod 8$ factor as $p = p_1 p_2$, and $\chi(p) = +1$. Note that $p^2 = Np = Np_1 \cdot Np_2$, so since the p_i are not units, $Np_i = p$. Then

$$\prod_{\pi|p} \frac{1}{1 - \frac{1}{|N\pi|^s}} \;=\; \frac{1}{1 - \frac{1}{|Np_1|^s}} \times \frac{1}{1 - \frac{1}{|Np_2|^s}} \;=\; \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 - \frac{1}{p^s}}$$

$$=\; \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 - \frac{\chi(p)}{p^s}} \quad = \quad p^{th} \text{ Euler factor of } \zeta_{\mathbb{Z}}(s) \;\times\; p^{th} \text{ Euler factor of } L(s, \chi)$$

Putting this all together, for each rational prime p, the product of the π^{th} Euler factors of $\zeta_{\mathfrak{o}}(s)$ for primes π dividing p is exactly the product of the p^{th} Euler factors of $\zeta_{\mathbb{Z}}(s)$ and $L(s, \chi)$. Thus,

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta_{\mathbb{Z}}(s) \cdot L(s, \chi)$$

[3.7] The first pole of $\zeta_{\mathfrak{o}}(s)$ Because the quadratic form $a^2 - 2b^2$ is *not* positive-definite, it is no longer a trivial calculus exercise to determine the residue κ of the first pole of $\zeta_{\mathfrak{o}}(s)$, at $s = 1$, to see that it is non-zero. This is related to the plenitude of units $\mathfrak{o}^\times$. As in the general case, these two complications are mutually compensating, as follows. First, we have to get a grip on the units.

[3.8] Units $\mathbb{Z}[\sqrt{2}]^\times$ Let $\sqrt{2}f$ be an *abstract* square root of 2, for example, the image of x in the quotient $\mathbb{Q}[x]/\langle x^2 - 2\rangle$. Specifically, we do *not* want to precipitously identify $\sqrt{2}$ with a *real number*. Indeed, there are two imbeddings σ_1, σ_2 of k into $\mathbb{R}$, namely

$$\sigma_1(a + b\alpha) \;=\; a + b \cdot 1.4142135\ldots \qquad\qquad \sigma_2(a + b\alpha) \;=\; a - b \cdot 1.4142135\ldots$$

where we recognize that decimal as the positive real square root of 2. Imbed $k = \mathbb{Q}(\sqrt{2})$ and its integers $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ into $\mathbb{R}^2$ by

$$\sigma = \sigma_1 \oplus \sigma_2 \;:\; a + b\alpha \;\longrightarrow\; (a + b\sqrt{2}) \oplus (a - b\sqrt{2}) \;\in\; \mathbb{R}^2$$

This imbeds $\mathbb{Z}$ on the diagonal in $\mathbb{R}^2$. Integer multiples $\mathbb{Z} \cdot \sqrt{2}$ are on the anti-diagonal.

Under this imbedding, the units $\mathfrak{o}^\times$ are on the two hyperbolas $xy = \pm 1$. We can find the unit $\eta = 1 + \sqrt{2}$ by trial-and error. Optimistically, we hope to prove that *all* units in $\mathfrak{o}$ are of the form $\pm\eta^\ell$ for $\ell \in \mathbb{Z}$.

To prove that there are no other units, observe that the image $\sigma(\mathfrak{o}^\times)$ of the units sits inside the intersection of the *lattice*

$$\sigma(\mathfrak{o}) \;=\; \mathbb{Z} \cdot (1,1) + \mathbb{Z} \cdot (1.414\ldots, -1.414\ldots)$$

with the *closed subset* $\{(x,y) : xy = \pm 1\}$. Things can be simplified by noting that multiplication by $\sigma(-1) = (-1,-1)$ sends the third quadrant $\{x < 0, y < 0\}$ to the first quadrant $\{x > 0, y > 0\}$, and multiplication by $\sigma(\pm\eta)$ sends the second and fourth quadrants $\{x < 0, y > 0\}$ and $\{x > 0, y < 0\}$ to the first. Thus, noting that $\sigma(\eta^2)$ is in the first quadrant, to prove that η and ± 1 generate all the units, it suffices to show that all units with image under σ in the first quadrant are powers of

$$\varepsilon \;=\; \eta^2 \;=\; (1+\sqrt{2})^2 \;=\; 3 + 2\sqrt{2}$$

For units α with $\sigma(\alpha)$ in the first quadrant, the log map

$$\alpha \;\longrightarrow\; \log \sigma_1(\alpha)$$

is a homeomorphism from the branch $\{xy = 1 : x > 0, y > 0\}$ of the hyperbola to the real line. Since the units are a (topologically closed) [8] *discrete* multiplicative subgroup of the hyperbola, the image under the log map is a *discrete* additive subgroup of the real line.

Since $3 + 2\sqrt{2} \neq 1$, this discrete subgroup of $\mathbb{R}$ is not just $\{0\}$.

The crucial claim, topological in nature, is that a non-trivial (topologically closed) discrete subgroup Γ of $\mathbb{R}$ is of the form $\Gamma = \mathbb{Z} \cdot \gamma$ for some $\gamma \neq 0$. To see this, first note that discreteness asserts that there is a neighborhood N of $\{0\}$ such that $N \cap \Gamma = \{0\}$. Since Γ is non-trivial, and is closed under additive inverses, it contains both positive and negative elements. By the completeness of the real numbers, the positive elements of Γ have an *infimum* γ. By the discreteness, this infimum γ is strictly positive. For any other element δ of Γ, since γ is an $\mathbb{R}$ basis for $\mathbb{R}$, there is $t \in \mathbb{R}$ such that $\delta = t \cdot \gamma$. Let $t = \ell + r$ with $\ell \in \mathbb{Z}$ and $0 \leq r < 1$. If $r \neq 0$, then $\delta - \ell\gamma \in \Gamma$ is a strictly smaller positive element of Γ than γ, contradiction. Therefore, $\delta = \ell \cdot \gamma$, and $\Gamma = \mathbb{Z} \cdot \gamma$.

Can $3 + 2\sqrt{2}$ fail to generate the first-quadrant subgroup of $\sigma(\mathfrak{o}^\times)$? Is there a *smaller* positive integer $0 < a < 3$ and another integer $b \neq 0$ such that $a^2 - 2b^2 = 1$? The only interesting possibility is $a = 2$, and $2^2 - 2b^2 = 1$ has no integer solutions. Therefore,

$$\mathbb{Z}[\sqrt{2}]^\times \;=\; \{\pm 1\} \cdot \{\eta^\ell \;:\; \ell \in \mathbb{Z}\}$$

[3.9] Representatives for $\mathfrak{o}/\mathfrak{o}^\times$ Earlier, for explicit computations, we took advantage of the *finiteness* of the units groups of rings of integers, to correctly assess the blow-up of the corresponding zeta function at its first pole. There, the obvious trick was to sum over all non-zero elements of $\mathfrak{o}$ and divide by the number of units. With infinitely-many units, as in the present example, this device is insufficient.

[8] In general, *discrete* subgroups of topological spaces need not be closed: $\{\frac{1}{n} : 1 \leq n \in \mathbb{Z}\}$ is discrete but not closed in $\mathbb{R}$. However, discrete *subgroups* Γ of topological *groups* G are always closed, seen as follows. Let N be a neighborhood of $e \in G$ such that $N \cap \Gamma = \{e\}$. By *continuity* of the group operation, let $U \subset N$ be a small-enough neighborhood of e such that $U^{-1} \cdot U \subset N$. For a limit point g_o of Γ, for $\gamma, \gamma' \in g_o \cdot U$, $\gamma^{-1} \cdot \gamma \in U^{-1}U \cap \Gamma = \{e\}$. That is, $\gamma = \gamma'$. But that means that $g_o \cdot U$ contains a unique element γ of Γ. Since G is presumed *Hausdorff*, for g_o to be in the closure of Γ requires that $g_o = \gamma \in \Gamma$. This proves that discrete subgroups Γ are *closed*.

Given any non-zero $\alpha \in \mathfrak{o}$, we can adjust its image $\sigma(\alpha)$ by multiplying by $\sigma(\theta)$ for any $\theta \in \mathfrak{o}^\times$, without changing the norm $|N\alpha|$, since

$$|N(\theta\alpha)| \;=\; |N\alpha| \cdot |N\theta| \;=\; |N\alpha| \cdot |\pm 1| \;=\; |N\alpha|$$

Knowing what we do about the units, from above, we can move $\sigma(\alpha)$ into the first quadrant $\{x > 0, y > 0\}$. Note that replacing α by $\varepsilon \cdot \alpha$ has the effect

$$\log \frac{\sigma_1(\varepsilon \cdot \alpha)}{\sigma_2(\varepsilon \cdot \alpha)} \;=\; 2 \log \sigma_1(\varepsilon) \;+\; \log \frac{\sigma_1(\alpha)}{\sigma_2(\alpha)} \qquad\qquad (\text{since } \sigma_1(\varepsilon) \cdot \sigma_2(\varepsilon) = 1)$$

Then we can adjust by powers of $\varepsilon = \eta^2$ to obtain a unique image in

$$0 \;\le\; \log \frac{\sigma_1(\alpha)}{\sigma_2(\alpha)} \;<\; 2 \log \sigma_1(\varepsilon)$$

Converting back to the multiplicative presentation, we have shown that every (non-zero) coset in $\mathfrak{o}/\mathfrak{o}^\times$ has a unique representative inside the set

$$X \;=\; \{(x, y) \in \mathbb{R} \;:\; x > 0,\; y > 0,\; 1 \le x/y < \sigma_1(\varepsilon)^2\}$$

There is still more work to be done to estimate the zeta function sufficiently.

[3.10] Lattice points in expanding domains

One sufficient approach to estimating the zeta function of $\mathbb{Z}[\sqrt{2}]$ combines partial summation with estimates of lattice points in expanding domains. With the set X as above, let

$$X_t \;=\; \{(x, y) \in X \;:\; xy \le t^2\}$$

Let F be the *fundamental parallelogram*[9] for the lattice $\sigma(\mathfrak{o})$ in $\mathbb{R}^2$:

$$F \;=\; \{t_1 \cdot (1, 1) + t_2 \cdot (1.414\ldots, -1.414\ldots) \;:\; -\tfrac{1}{2} \le t_1 < \tfrac{1}{2},\; -\tfrac{1}{2} \le t_2 < \tfrac{1}{2}\}$$

The salient property is that, given $v \in \mathbb{R}^2$, there are unique $\lambda \in \sigma(\mathfrak{o})$ and $v_o \in F$ such that $v = v_o + \lambda$. We claim that[10]

$$\text{card}\big(X_t \cap \sigma(\mathfrak{o})\big) \;=\; \frac{\text{area } X_t}{\text{area } F} + O(\sqrt{t}) \;=\; \frac{\text{area } X_1}{\text{area } F} \cdot t^2 \;+\; O(t) \qquad\qquad (\text{as } t \to +\infty)$$

Let r be the *radius* of F. On one hand, for every $\lambda \in \sigma(\mathfrak{o}) \cap X_t$, while the translate $\lambda + F$ may not fit entirely inside X_t, every point of it is within distance r of X_t. On the other hand, for $\lambda \notin \sigma(\mathfrak{o}) \cap X_t$, the translate $\lambda + F$ may meet X_t, but all points of it are within distance r of the boundary ∂X_t of X_t. Thus, letting

$$B_t \;=\; \{z \in \mathbb{R}^2 \;:\; z \text{ is within distance } r \text{ of } X_t\}$$

[9] The notion of *fundamental parallelogram* for a lattice Λ in a Euclidean space V plays a large role in traditional discussions. Since there are infinitely-many different choices of $\mathbb{Z}$-basis for a given lattice, there is tremendous ambiguity in this notion. One can prove that various constructs are independent of choices, but this is mostly wasted effort. The better notion is simply that of the *quotient* V/Λ. Rather than asking about measuring a fundamental domain for Λ, one should prove that there is a unique group-invariant measure on V/Λ such that the natural identity holds: for $f \in C_c^o(V)$,

$$\int_V f(v)\, dv \;=\; \int_{V/\Lambda} \Big(\sum_{\lambda \in \Lambda} f(\lambda + w) \Big)\, dw$$

[10] This estimate on lattice points inside expanding regions is intuitive, but *does* need hypotheses on the boundary and shape of X_1. Thus, the argument cannot be completely trivial.

we have

$$\text{area}\, X_t - \text{area}\, B_t \;\le\; (\text{number of } \lambda \in \sigma(\mathfrak{o}) \cap X_t) \cdot \text{area}\, F \;\le\; \text{area}\, X_t + \text{area}\, B_t$$

Thus, we are interested in estimating the area of B_t. It is at this point that we use the fact that B_t is the union of a *finite* collection of *smooth* curves.

That is, given a smooth, finite curve C in $\mathbb{R}^2$, show that the area of the set of points within distance r of the dilate tC is $O(t)$, an order of magnitude smaller than the area of X_t, which is $O(t^2)$. Use the non-trivial calculus fact that we can assume C is *parametrized by arc length*. Given t, take $1 + \frac{t}{r}\,\text{length}\, C$ points c_i equidistributed on tC, of distance at most r apart. Given a point p on tC, there is at least one c_i within distance r. The disk of radius r centered at p is contained in the disk of radius $2r$ at c_i. Thus, every point within distance r of tC is inside one of the $1 + \frac{t}{r}\,\text{length}\, C$ disks of radius $2r$. Thus,

$$\text{area}\,\{z \in \mathbb{R}^2 : z \text{ within distance } r \text{ of } tC\} \;=\; (1 + \frac{t}{r}\,\text{length}\, C) \cdot \pi(2r)^2 \;=\; O(t) \qquad\qquad (\text{depending on } C)$$

We conclude that the area of B_t is $O(t)$, so

$$(\text{number of } \lambda \in \sigma(\mathfrak{o}) \cap X_t) \cdot \text{area}\, F \;=\; \text{area}\, X_t + O(t) \;=\; t^2 \cdot \text{area}\, X_1 + O(t)$$

Dividing through by $\text{area}\, F$, we have counted lattice points:

$$(\text{number of } \lambda \in \sigma(\mathfrak{o}) \cap X_t) \;=\; t^2 \cdot \frac{\text{area}\, X_1}{\text{area}\, F} + O(t)$$

The area of the rectangle F is obviously $\sqrt{2}$, but some computation is needed to find $\text{area}\, X_1$. The first-quadrant region X_1 is bounded by curves $y = x$, $y = x/\varepsilon^2$, and $xy = 1$. Letting $\varepsilon = 3 + 2\sqrt{2}$, this area is

$$\text{area}\, X_1 \;=\; \int_0^1 x(1 - \frac{1}{\varepsilon^2})\, dx + \int_1^\varepsilon (\frac{1}{x} - \frac{x}{\varepsilon^2})\, dx$$

$$=\; \tfrac{1}{2}(1 - \frac{1}{\varepsilon^2}) + \log\varepsilon - \tfrac{1}{2}(\varepsilon^2 - 1)\frac{1}{\varepsilon^2} \;=\; \log\varepsilon \;=\; \log(3 + 2\sqrt{2})$$

In summary,

$$(\text{number of } \lambda \in \sigma(\mathfrak{o}) \cap X_t) \;=\; t^2 \cdot \frac{\log(3 + 2\sqrt{2})}{\sqrt{2}} + O(t)$$

[3.11] Partial summation and the residue of $\zeta_{\mathfrak{o}}(s)$ Having the asymptotics of lattice points in X_t, with a power-saving error term, partial summation will yield the analytical properties on a right half-plane including $s = 1$. Let

$$\nu(t) \;=\; (\text{number of } \lambda \in \sigma(\mathfrak{o}) \cap X_t)$$

The zeta function of $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ is

$$\zeta_{\mathfrak{o}}(s) \;=\; \sum_{n=1}^{\infty} \frac{\nu(\sqrt{n}) - \nu(\sqrt{n-1})}{n^s}$$

Summation-by-parts is

$$\frac{\nu(1)}{1^s} + \frac{\nu(\sqrt{2}) - \nu(1)}{2^s} + \frac{\nu(\sqrt{3}) - \nu(\sqrt{2})}{3^s} + \frac{\nu(\sqrt{4}) - \nu(\sqrt{3})}{4^s} + \dots$$

$$=\; \nu(1)\big(\frac{1}{1^s} - \frac{1}{2^s}\big) + \nu(\sqrt{2})\big(\frac{1}{2^s} - \frac{1}{3^s}\big) + \nu(\sqrt{3})\big(\frac{1}{3^s} - \frac{1}{4^s}\big) + \dots$$

Using the first-order estimate

$$\frac{1}{n^s} - \frac{1}{(n+1)^s} \;=\; \frac{1}{s\,n^{s+1}} + O(\frac{1}{n^{s+2}})$$

we have

$$\sum_{n\geq 1} \nu(\sqrt{n})\big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\big) \;=\; \sum_{n\geq 1} \big(\frac{n\cdot\log(3+2\sqrt{2})}{\sqrt{2}} + O(\sqrt{n})\big)\cdot\big(\frac{1}{s\,n^{s+1}} + O(\frac{1}{n^{s+2}})\big)$$

$$= \;\frac{\log(3+2\sqrt{2})}{\sqrt{2}} \sum_{n\geq 1} \frac{1}{sn^s} + O\Big(\sum_n \frac{1}{n^{s+\frac{1}{2}}}\Big) \qquad\qquad (\text{as } s\to 1^+)$$

Since

$$\sum_{n\geq 1} \frac{1}{n^s} \;=\; \frac{1}{s-1} + O(1) \qquad\qquad (\text{as } s\to 1+)$$

and $s = 1 + (s-1)$, this becomes

$$\zeta_{\mathfrak{o}}(s) \;=\; \frac{\log(3+2\sqrt{2})}{\sqrt{2}(s-1)} + O(1) \qquad\qquad (\text{as } s\to 1^+)$$

[3.12] Value of $L(1,\chi)$ Let $\kappa = \frac{1}{\sqrt{2}}\log(3+2\sqrt{2})$. From the factorization of $\zeta_{\mathfrak{o}}(s)$, and knowing that its first pole is at $s=1$, is simple, and has residue κ,

$$\frac{\kappa}{s-1} + O(1) \;=\; \zeta_{\mathfrak{o}}(s) \;=\; \zeta_{\mathbb{Z}}(s)\cdot L(s,\chi) \;=\; \Big(\frac{1}{s-1} + O(1)\Big)\cdot\Big(L(1,\chi) + O(s-1)\Big)$$

Therefore,

$$L(1,\chi) \;=\; \kappa \;=\; \frac{\log(3+2\sqrt{2})}{\sqrt{2}} \;\neq\; 0$$

In particular,

$$L(1,\chi) \;\neq\; 0$$

[3.12.1] Remark: There are four Dirichlet characters mod 8: the trivial one, and

$$\chi_2(p) = \Big(\frac{2}{p}\Big)_2 \qquad \chi_{-1}(p) = \Big(\frac{-1}{p}\Big)_2 \qquad \chi_{-2}(p) = \Big(\frac{-2}{p}\Big)_2$$

We know that χ_{-1} is defined modulo 4, so is not primitive mod 8, and we have already shown that $L(1,\chi_{-1}) \neq 0$. If the case of $\sqrt{-2}$ were treated, then we would have non-vanishing for all characters mod 8, and would have completed Dirichlet's argument for primes mod 8.

4. *Appendix: Euclidean-ness*

In many simple, useful situations, a commutative ring R can be proven to be a *principal ideal domain*, and, thus, a *unique factorization domain*, by verifying the *Euclidean property*: there is a multiplicative As usual, a function N is *multiplicative* when $N(ab) = N(a) \cdot N(b)$. positive-integer-valued function $N : R \to \mathbb{Z}$ such that, given $\alpha \in R$ and $0 \neq \beta \in R$, there is $q \in R$ such that

$$N\big(\alpha - q \cdot \beta\big) \quad < \quad N(\beta)$$

In words, the Euclidean property is that division-with-remainder can produce remainders smaller than the divisor.

The proof that Euclidean-ness of R implies that R is a principal ideal domain is the natural one. Namely, given a non-zero ideal I in R, let $r \in I$ be such that $N(r) > 0$ is minimum among non-zero values of N on I. Note that the strict inequality in the description of the Euclidean property implies that $N(\beta) > 0$ for $\beta \neq 0$. Since N is positive-integer-valued, this minimum does occur. Then, for any element $x \in I$, invoke the Euclidean property to find q such that

$$N(x - q \cdot r) \quad < \quad N(r)$$

Since $x - qr \in I$, the minimality of $N(r)$ implies that $N(x - qr) = 0$, and that $x - qr = 0$. That is, $x = qr$, and x is a multiple of r. That is, $I = R \cdot r$, so the ideal is principal. ///