Continuing the pre/review of the simple (!?) case...

So far, we have sketched the connection between *prime numbers*, and *zeros of the zeta function*, given by Riemann's formula

$$\sum_{p^m<X} \log p \;=\; X \;-\; (b+1) \;-\; \lim_{T\to\infty} \sum_{|\mathrm{Im}\,(\rho)|<T} \frac{X^\rho}{\rho} \;+\; \sum_{n\geq 1} \frac{X^{-2n}}{2n}$$

A different example (though connected to zeta functions and L-functions at a deeper level!) is Gauss' *Quadratic Reciprocity*:

$$\left(\frac{q}{p}\right)_2 \cdot \left(\frac{p}{q}\right)_2 \;=\; (-1)^{\frac{(p-1)(q-1)}{4}}$$

We'll reprise the latter, and then look at *factorization* of Dedekind zeta-functions into Dirichlet L-functions.

Reprise of end of the Quadratic Reciprocity discussion: from the Cancellation Lemma, $g(\chi)^2 = q \cdot (-1)^{q-1}$, and then

Using $g(\chi)^2 = \chi(-1)q$ and plugging into Euler's criterion: computing mod p in $\mathbb{Z}[e^{2\pi i/q}]$, noting that apparently q and $g(\chi)$ are invertible there (!),

$$\binom{q}{p}_2 = q^{\frac{p-1}{2}} = \left((-1)^{\frac{q-1}{2}} \cdot g(\chi)^2\right)^{\frac{p-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}} \cdot \frac{g(\chi)^p}{g(\chi)}$$

Again using $\binom{p}{j} = 0 \bmod p$ for $0 < j < p$,

$$g(\chi)^p = \sum_{b \bmod q} \chi(b)^p \cdot \psi(p \cdot b) = \sum_{b \bmod q} \chi(b) \cdot \psi(p \cdot b)$$

$$= \sum_{b \bmod q} \chi(bp^{-1}) \cdot \psi(b) = \binom{p}{q}_2 \cdot g(\chi) \bmod p$$

Thus, in $\mathbb{Z}[e^{2\pi i/q}]$ mod p,

$$\binom{q}{p}_2 = (-1)^{\frac{(p-1)(q-1)}{4}} \cdot \frac{g(\chi)^p}{g(\chi)}$$

$$= (-1)^{\frac{(p-1)(q-1)}{4}} \cdot \frac{\binom{p}{q}_2 \cdot g(\chi)}{g(\chi)} = (-1)^{\frac{(p-1)(q-1)}{4}} \cdot \binom{p}{q}_2$$

Since these values are ± 1, their equality in $\mathbb{Z}[e^{2\pi i/q}]$ mod p for $p > 2$ gives their equality as numbers in $\{\pm 1\}$. ///

Factorization of Dedekind zeta functions As noted earlier, Dirichlet's 1837 theorem on primes in arithmetic progressions $a + \ell N$ needs a *non-vanishing* result for L-functions, namely, $L(1, \chi) \neq 0$ for Dirichlet characters χ mod N.

Dirichlet proved this in simple cases by showing that these L-functions are factors in *Dedekind zeta functions* $\zeta_{\mathfrak{o}}(s)$ of rings of integers $\mathfrak{o} = \mathbb{Z}[\omega]$ with ω an N^{th} root of unity, and using simple properties of the zeta functions $\zeta_{\mathfrak{o}}(s)$.

To describe Dedekind zetas, for an ideal $\mathfrak{a}$ of suitable $\mathfrak{o}$, let the *ideal norm* be $N\mathfrak{a} = \mathrm{card}\,(\mathfrak{o}/\mathfrak{a})$. Then

$$\zeta_{\mathfrak{o}}(s) \;=\; \sum_{\mathfrak{a}\neq 0} \frac{1}{(N\mathfrak{a})^s}$$

In suitable $\mathfrak{o}$, every non-zero ideal factors uniquely into *prime ideals* (not necessarily prime *numbers*) (one says these are *Dedekind domains*), so the zeta function has an Euler product

$$\zeta_{\mathfrak{o}}(s) \;=\; \sum_{\mathfrak{a}\neq 0} \frac{1}{(N\mathfrak{a})^s} \;=\; \prod_{\mathfrak{p}\text{ prime}} \frac{1}{1 - N\mathfrak{p}^{-s}} \qquad\qquad (\text{for } \mathrm{Re}\,(s) > 1)$$

For $\mathfrak{o} = \mathbb{Z}[\omega]$, 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 $\mathbb{Z}[\omega]$?

Letting ω be a primitive q^{th} root of unity for q prime, and Φ_q the q^{th} cyclotomic polynomial,

$$\mathbb{Z}[\omega]/p \approx \big(\mathbb{Z}[x]/\Phi_q\big)/p \approx \big(\mathbb{Z}[x]/p\big)/\Phi_q$$

$$\approx \mathbb{F}_p[x]/\Phi_q \approx \mathbb{F}_p[x]/\varphi_1 \oplus \ldots \oplus \mathbb{F}_p[x]/\varphi_m$$

where φ_i are irreducible factors of Φ_q in $\mathbb{F}_p[x]$.

On the other hand, assuming the Dedekind-domain property, and that $p = \mathfrak{P}_1 \ldots \mathfrak{P}_n$ with distinct $\mathfrak{P}_i$, then by Sun-Ze's theorem

$$\mathbb{Z}[\omega]/p \approx \mathbb{Z}[\omega]/\mathfrak{P}_1 \oplus \ldots \oplus \mathbb{Z}[\omega]/\mathfrak{P}_n$$

Thus,

$$\mathbb{F}_p[x]/\varphi_1 \oplus \ldots \oplus \mathbb{F}_p[x]/\varphi_m \approx \mathbb{Z}[\omega]/\mathfrak{P}_1 \oplus \ldots \oplus \mathbb{Z}[\omega]/\mathfrak{P}_n$$

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**. 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.

Since the rings $\mathbb{Z}[\omega]$ are rarely principal ideal domains, examples where the rings involved *are* principal ideal domains are best to have at first.

The easiest proofs of PID-ness are by Euclidean-ness.

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

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*

$$N(a+bi) \;=\; (a+bi)\cdot(a+bi)^\sigma \;=\; (a+bi)(a-bi) \;=\; a^2+b^2$$

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*:

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

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, finding the four units

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

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

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

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 $\gamma = \alpha/\beta \in \mathbb{Q}(i)$, there should be $q \in \mathfrak{o}$ such that $N(\gamma - q) < 1$. Indeed, let $\gamma = a + bi$ with $a, b \in \mathbb{Q}$, 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

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

This proves the Euclidean-ness, and PID-ness, and UFD-ness.

Behavior of primes in the extension $\mathbb{Z}[i]$ of $\mathbb{Z}$ Prime numbers p in $\mathbb{Z}$, which we'll call *rational primes* to distinguish them, do not usually *stay prime* in larger rings. For example, the prime 5 factors:

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

The norms of $2 \pm i$ are both 5, so these are not units.

Expanding on the two-squares theorem:

Theorem: A rational prime p stays prime in $\mathbb{Z}[i]$ 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*, in the sense that $2 = (1+i)(1-i)$ and $1+i$ and $1-i$ differ by a unit.

Terminology: Primes that *stay* prime are *inert*, and primes that *factor* (with no factor repeating) are *split*. A prime that factors and has *repeated factors* is *ramified*.

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

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

$$\approx\; \mathbb{F}_p[x]/\langle x^2+1\rangle$$

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 $4|p-1$. 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 $p = 1 \bmod 4$, $\mathbb{F}_p$ contains primitive fourth roots of unity, so there are $\alpha, \beta \in \mathbb{F}_p$ such that $x^2+1 = (x-\alpha)(x-\beta)$. 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

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

[continued]
