SUMS OF TWO SQUARES VIA L-FUNCTIONS

Consider a quadratic number field and its ring of algebraic integers,

$$\mathbb{F} = \mathbb{Q}(i), \qquad D = \mathbb{Z}[i].$$

Thus D now denotes the ring of *Gaussian integers* rather than the ring of Eisenstein integers. The two rings are very similar in their structures. Specifically,

- D is a Euclidean ring with norm function

  $$N : D \longrightarrow \mathbb{N}, \qquad Nz = z\overline{z}, \quad N(a+bi) = a^2 + b^2.$$

  (This shows why the algebraic structure of D should help us to study sums of two squares.) Consequently, D is a PID and thus a UFD.
- The unit group of D is cyclic of order 4,

  $$D^* = \{\pm 1, \pm i\} = \langle i \rangle = \langle -i \rangle.$$

- Rational primes decompose in D as follows:
  - $p \equiv 1 \pmod 4 \implies p$ splits: $p = \pi\overline{\pi}$, $N\pi = p$, $D/\pi D \cong \mathbb{Z}/p\mathbb{Z}$.
  - $p \equiv 3 \pmod 4 \implies p$ is inert: p is prime in D, $Np = p^2$, $D/pD \cong (\mathbb{Z}/p\mathbb{Z})^2$.
  - 2 ramifies: $2 = -i(1+i)^2$, $N(1+i) = 2$, $D/(1+i)D \cong \mathbb{Z}/2\mathbb{Z}$.

The *quadratic character modulo 4* is the homomorphism

$$\chi : (\mathbb{Z}/4\mathbb{Z})^* \longrightarrow \{\pm 1\} \subset \mathbb{C}^*, \qquad \begin{cases} \chi(1+4\mathbb{Z}) = 1, \\ \chi(3+4\mathbb{Z}) = -1. \end{cases}$$

The character extends to the multiplicative function

$$\chi : \mathbb{Z} \longrightarrow \{0, \pm 1\}, \qquad \chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 3 \bmod 4, \\ 0 & \text{if } n \equiv 0 \bmod 2. \end{cases}$$

The *Euler–Riemann zeta function* is

$$\zeta(s) = \sum_{n \in \mathbb{Z}^+} n^{-s} = \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1}.$$

The sum and the product are formally equal by the Fundamental Theorem of Arithmetic. Both sides converge absolutely for all $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > 1$, but we don't need this fact. The *quadratic L-function* associated to χ is

$$L(\chi, s) = \sum_{n \in \mathbb{Z}^+} \chi(n) n^{-s} = \prod_{p \in \mathcal{P}} (1 - \chi(p) p^{-s})^{-1}.$$

Equality between the sum and the product is no harder to prove than before because χ is multiplicative. The *zeta function of the number field* $\mathbb{F} = \mathbb{Q}(i)$ is

$$\zeta_{\mathbb{F}}(s) = \sum_{\nu \in (D - \{0\})/\sim} N\nu^{-s} = \prod_{\pi \in \mathcal{P}_D/\sim} (1 - N\pi^{-s})^{-1}.$$

Here the equivalence relation on D is $x \sim y$ if $y = ux$ for some $u \in D^*$, i.e., two elements are similar if they are associate. Again, equality between the sum and the product is proved in the same way.

Let $r(n,2)$ be the *representation number* of n as the sum of two squares,

$$\begin{aligned} r(n,2) &= \#\{a+bi \in D : N(a+bi) = n\} \\ &= \#\{(a,b) \in \mathbb{Z}^2 : a^2+b^2 = n\}. \end{aligned}$$

The additive expression for $\zeta_{\mathbb{F}}(s)$ regroups as a generating function for these representation numbers,

$$\zeta_{\mathbb{F}}(s) = \frac{1}{4} \sum_{n \in \mathbb{Z}^+} \sum_{\nu : N\nu = n} n^{-s} = \frac{1}{4} \sum_{n \in \mathbb{Z}^+} r(n,2) n^{-s}.$$

On the other hand, the arithmetic of D and then the definition of the function χ show that the multiplicative form of $\zeta_{\mathbb{F}}(s)$ is

$$\begin{aligned} \zeta_{\mathbb{F}}(s) &= (1-2^{-s})^{-1} \prod_{p \equiv 1(4)} (1-p^{-s})^{-2} \prod_{p \equiv 3(4)} (1-p^{-2s})^{-1} \\ &= \zeta(s) \prod_{p \equiv 1(4)} (1-p^{-s})^{-1} \prod_{p \equiv 3(4)} (1+p^{-s})^{-1} \\ &= \zeta(s) L(\chi, s). \end{aligned}$$

And the additive form of this last product is

$$\zeta(s) L(\chi, s) = \sum_{n_1 \in \mathbb{Z}^+} n_1^{-s} \sum_{n_2 \in \mathbb{Z}^+} \chi(n_2) n_2^{-s} = \sum_{n \in \mathbb{Z}^+} \left[\sum_{d \mid n} \chi(d) \right] n^{-s}.$$

Equate the coefficients of the two additive forms of $\zeta_{\mathbb{F}}(s)$ to obtain an expression for the representation number,

$$r(n,2) = 4 \sum_{d \mid n} \chi(d).$$