$\zeta(s)$ and prime numbers

$\zeta(s) = \sum_{n\geq 1} n^{-s}$ ($Re(s) > 1 \Rightarrow$ absolute convergence to a holomorphic function,

since $n^{-s} := e^{-s\ln(n)}$ satisfies $|n^{-s}| = n^{-\sigma}$, $\underline{s = \sigma + it}$, and $\sum_{n\geq 1} n^{-\sigma} < C + \int_1^\infty x^{-\sigma} dx < \infty$ $\forall \sigma > 1$)

Euler : values $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, ...

method: $\underbrace{\frac{\sin(z)}{z}}_{1 - \frac{z^2}{3!} + \frac{z^4}{5!} - \cdots} \stackrel{?}{=} \underbrace{\prod_{n\geq 1}\left(1 - \left(\frac{z}{\pi n}\right)^2\right)}_{1 - z^2\frac{\zeta(2)}{\pi^2} + \cdots}$ (same zeroes !)

apply $\frac{d}{dz}\log$, get $\cot g(\pi z) = \frac{1}{z} + \sum_{n\geq 1}\left(\frac{1}{z+n} + \frac{1}{z-n}\right) = \frac{1}{z} - \sum_{n\geq 1} 2\zeta(2n) z^{2n-1}$

$\Rightarrow \boxed{-2\zeta(2n) = \frac{(2\pi i)^{2n} B_{2n}}{(2n)!}}$ (Bernoulli numbers: $\frac{t}{e^t - 1} = \sum_{k\geq 0} B_k \frac{t^k}{k!}$)

Euler product : $\zeta(s) = \prod_{p \text{ prime}} (1 + p^{-s} + p^{-2s} + \cdots) = \prod_p (1 - p^{-s})^{-1}$ $(Re(s) > 1)$

$\Updownarrow$

(unique factorisation in $\mathbb{Z}$)

$\forall x \geq 1$ $\quad C + \ln(x) = C + \int_1^x \frac{dt}{t} \leq \sum_{n\leq x} \frac{1}{n} \leq \prod_{p\leq x} (1 + p^{-1} + p^{-2} + \cdots) = \prod_{p\leq x} (1 - p^{-1})^{-1}$

Take $\ln$ and use $-\ln(1 - T) = \sum_{k\geq 1} T^k/k$ ($|T| < 1$ or $|T| = 1 \neq T$)

$$C_1 + \ln\ln(x) \leq \sum_{p\leq x} -\ln(1 - p^{-1}) = \sum_{p\leq x}\sum_{k\geq 1} p^{-k}/k = \sum_{p\leq x}\frac{1}{p} + \underbrace{\sum_{\substack{p\leq x\\ k\geq 2}} p^{-k}/k}_{\leq \frac{1}{2}\sum_{k,n\geq 2} n^{-k} = \frac{1}{2}\sum_{n\geq 2}\frac{1}{n(n-1)} = \frac{1}{2}} \leq \frac{1}{2} + \sum_{p\leq x}\frac{1}{p}$$

$\Rightarrow \sum_{p\leq x}\frac{1}{p} \geq C_2 + \ln\ln(x)$ (Euler)

Variant: $\underbrace{1 - 2^{-s} + 3^{-s} - 4^{-s} + \cdots}_{\text{converges and is } >0 \text{ if } s=\sigma>0} \underset{Re(s)>1}{\overset{\uparrow}{=}} (1 - 2^{1-s})\zeta(s)$ $\Bigg\} \Rightarrow \lim_{\sigma\to 1+} (\sigma - 1)\zeta(\sigma) = \frac{\sum_{n\geq 1} (-1)^n/n}{\ln(2)} = 1$

$\Rightarrow \lim_{\sigma\to 1+}\left(\ln\zeta(\sigma) - \ln\left(\frac{1}{\sigma - 1}\right)\right) = 0$ $\qquad \boxed{\ln\zeta(\sigma) = \ln\frac{1}{\sigma - 1} + o(1) \text{ for } \sigma \to 1+}$

Landau's notation : (a) $f = O(g)$ as $x \to x_0$: $\exists C > 0$ $|f(x)| \leq C g(x)$ for $x \in$ neighbourhood of x_0

(b) $f = o(g)$ as $x \to x_0$: $\forall \varepsilon > 0$ $\exists$ neighbourhood of x_0 in which $|f(x)| \leq \varepsilon g(x)$

(c) $f \sim g$ — " — : $\lim_{x\to x_0} f(x)/g(x) = 1$

Vinogradov's notation : $f \asymp g$ as $x \to x_0$: $\exists$ $c_1, c_2 > 0$ $\exists$ neighbourhood of x_0 in which $c_1 g(x) \leq f(x) \leq c_2 g(x)$.

In particular : $f = O(1) \Leftrightarrow |f|$ is bounded around x_0

$f = o(1) \Leftrightarrow f \to 0$ as $x \to x_0$

For $\sigma \to 1+$, $\ln \frac{1}{\sigma-1} = \ln \zeta(\sigma) + o(1)$ and

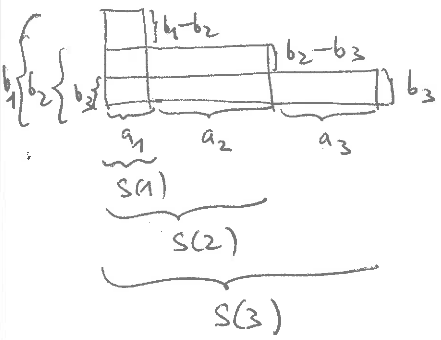
$$\ln \zeta(\sigma) = \sum_p \sum_{k\geq 2} p^{-k\sigma}/k = \sum_p p^{-\sigma} + O(1)$$

$$\Rightarrow \boxed{\sum_{p \text{ prime}} p^{-\sigma} = \ln \frac{1}{\sigma-1} + O(1) \quad \text{as } \sigma \to 1+}$$

<u>General Dirichlet series</u> : $\sum_{n\geq 1} \frac{a_n}{n^s}$ $\quad (a_n \in \mathbb{C})$

<u>Abel's summation</u> : $\displaystyle\sum_{n=M}^{N} a_n b_n = \sum_{n=M}^{N} \underbrace{(a_M + \cdots + a_n)}_{S(n)} (b_n - b_{n+1}) \cancel{+ S(N) b_{N+1}}$ $\quad (b_{N+1} = 0)$

$$= \sum_{n=M}^{N-1} S(n)(b_n - b_{n+1}) + S(N) b_N$$



<u>Variant</u> : $\displaystyle\sum_{n=M}^{N} a_n b_n = S(N) b_N - \sum_{n=M}^{N-1} S(n)(b_{n+1} - b_n)$

If $f : [M, +\infty) \to \mathbb{C}$ is $\mathcal{C}^1$ and $f(n) = b_n$ $\forall n \in [M, +\infty) \cap \mathbb{Z}$, then

$$\forall x \geq M \quad \sum_{M \leq n \leq x} a_n f(n) = S([x]) \underbrace{b_{[x]}}_{f([x])} - \underbrace{\sum_{n=M}^{[x]-1} S(n) \int_n^{n+1} f'(t)\,dt}_{\int_M^{[x]} S(t) f'(t)\,dt} = S(x) f(x) - \int_M^x S(t) f'(t)\,dt$$

$$S(x) := \sum_{M \leq n \leq x} a_n = S([x])$$

<u>Our case</u> : $f(t) = t^{-s}$, $f'(t) = -s t^{-s-1}$ $\Rightarrow \displaystyle\sum_{n=M}^{N} \frac{a_n}{n^s} = \frac{S(N)}{N^s} + s \int_M^N \frac{S([t])}{t^{s+1}}\,dt$

$$S(x) = \sum_{M \leq n \leq x} a_n = S([x])$$

<u>Case (1) : If $\forall \varepsilon > 0$ $\quad a_n = O(n^{\varepsilon})$ as $n \to +\infty$</u> : $\Rightarrow \forall \varepsilon > 0$ $\quad |S(x)| = O(x^{1+\varepsilon})$

$\Rightarrow$ if $\mathrm{Re}(s) > 1$, then $\displaystyle\sum_{n=M}^{\infty} \frac{a_n}{n^s}$ converges to $\displaystyle s \int_M^{\infty} \frac{S(t)}{t^{s+1}}\,dt$ (holomorphic in $\mathrm{Re}(s) > 1$)

<u>(1a)</u> : <u>$M = 1$, $\forall n$ $a_n = 1$</u> : $S(x) = [x] \Rightarrow$ for $\mathrm{Re}(s) > 1$

$$\zeta(s) = s \int_1^{\infty} \frac{[x]}{x^{s+1}}\,dx = s \int_1^{\infty} \frac{x - \{x\}}{x^{s+1}}\,dx = \underbrace{s \int_1^{\infty} \frac{dx}{x^s}}_{\frac{s}{s-1}} - s \int_1^{\infty} \frac{\{x\}}{x^{s+1}}\,dx$$

$$\Rightarrow \text{for } \mathrm{Re}(s) > 1 \qquad \zeta(s) - \frac{1}{s-1} = 1 - s \int_1^{\infty} \frac{\{x\}\,dx}{x^{s+1}}$$

$\Rightarrow$ <u>holomorphic continuation</u> of $\zeta(s) - \frac{1}{s-1}$ to ~~converges to a~~ holomorphic function for $\underline{\mathrm{Re}(s) > 0}$

(1b) $M=1$ and $|S(x)| \le C$ (i.e., $|S(x)| = O(1)$ as $x \to \cancel{+\infty}$):

$$\Rightarrow \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ converges to } \underbrace{s\int_1^{\infty} \frac{S(x)}{x^{s+1}}\,dx}_{\text{holomorphic for } \mathrm{Re}(s)>0} \quad \text{for } \mathrm{Re}(s)>0$$

Primes in arithmetic progressions (Dirichlet)

Ex1:

$p \equiv 1\,[4]$	5	13	17	29	37	41	53	61	73	89	97	101
$p \equiv -1\,[4]$	3	7	11	19	23	31	43	47	59	67	71	79

Ex 2:

$p \equiv 1\,[3]$	7	13	19	31	37	43	61	67	73	79	97	103
$p \equiv -1\,[3]$	2	5	11	17	23	29	41	47	53	59	71	83

Notation: $\pi(x) := \sum_{p \le x} 1$, $\pi(x; a, m) := \sum_{\substack{p \le x \\ p \equiv a[m]}} 1$

(p=prime)

It seems: (a) $\pi(x; \pm 1, 4) \overset{?}{\longrightarrow} +\infty$, $\pi(x; \pm 1, 3) \overset{?}{\longrightarrow} +\infty$ as $x \to +\infty$ (true)

(b) $\pi(x; 1, m) - \pi(x; -1, m) \overset{?}{<} 0$ for $m = 3, 4$ (false)

Dirichlet's Thm: $(a,m)=1 \Rightarrow \sum_{p \equiv a[m]} \frac{1}{p} = +\infty$ $\left(\Rightarrow \pi(x; a, m) \xrightarrow{x\to+\infty} +\infty\right)$

Čebyšev's phenomenon ("prime number races"): it seems that, for $m=3,4$

" $\pi(x; 1, m) < \pi(x; -1, m)$ "more often" than $\pi(x;1,m) > \pi(x;-1,m)$ "

(true under standard conjectures on L-functions)

Littlewood's Thm: $(*)$ $(\pi(x; 1, m) - \pi(x; -1, m))$ changes sign infinitely many ~~values~~ times

(for $m = 3, 4$)

as $x \to +\infty$. (in fact, $\liminf_{x\to+\infty} (*) = -\infty$, $\limsup_{x \to +\infty} (*) = +\infty$)

Relevant L-functions:

$$L_{-4}(s) = 1 - 3^{-s} + 5^{-s} - 7^{-s} + \dots = \sum_{\substack{n \ge 1 \\ (4,n)=1}} \frac{\chi_{-4}(n)}{n^s} = \prod_{p \ne 2} \left(1 - \chi_{-4}(p) p^{-s}\right)^{-1}, \quad \chi_{-4} : (\mathbb{Z}/4\mathbb{Z})^{\times} \to \{\pm 1\}$$

$\chi_{-4}(\pm 1 \pmod 4) = \pm 1$

$$L_{-3}(s) = 1 - 2^{-s} + 4^{-s} - 5^{-s} + \dots = \sum_{\substack{n \ge 1 \\ (3,n)=1}} \frac{\chi_{-3}(n)}{n^s} = \prod_{p \ne 3} \left(1 - \chi_{-3}(p) p^{-s}\right)^{-1}, \quad \chi_{-3} : (\mathbb{Z}/3\mathbb{Z})^{\times} \to \{\pm 1\}$$

$\chi_{-3}(\pm 1 \pmod 3) = \pm 1$

For $m \in \{3, 4\}$, (a) $L_{-m}(s)$ converges and is holomorphic for $\mathrm{Re}(s) > 0$

(b) $L_{-m}(\sigma) > 0$ for $\sigma \in (0, +\infty)$

(c) In particular, $L_{-4}(1)$ $\left(= \frac{\pi}{4}\right) > 0$

and $L_{-3}(1)$ $\left(= \frac{\pi}{3\sqrt{3}}\right) > 0$

For $\mathrm{Re}(s)>1$: $\quad \zeta(s)L_{-m}(s) = (1-q^{-s})^{-1}\prod_{p\equiv 1[m]}(1-p^{-s})^{-2}\prod_{p\equiv -1[m]}(1-p^{-2s})^{-1}$

$m\in\{3,4\}$

$q=3,2$

$\Downarrow$ for $s=\sigma\in(1,+\infty)$

$$\ln\zeta(\sigma)+\ln L_{-m}(\sigma) = 2\sum_{p\equiv 1[m]}\frac{1}{p^\sigma}+\underbrace{\sum_{p\equiv -1[m]}\frac{1}{p^{2\sigma}}}_{O(1)}+O(1)$$

For $\sigma\to 1+$

But $\ln\zeta(\sigma) = \sum_{p\equiv 1[m]}\frac{1}{p^\sigma}+\sum_{p\equiv -1[m]}\frac{1}{p^\sigma}+O(1)$

$= \ln\left(\frac{1}{\sigma-1}\right)+o(1)$

and $\boxed{L_{-m}(1)\neq 0} \Rightarrow \ln L_{-m}(\sigma) = O(1)$ as $\sigma\to 1+$

Conclusion: for $\sigma\to 1+$, $m\in\{3,4\}$, $a=\pm 1$

$$\sum_{p\equiv a[m]}\frac{1}{p^\sigma} = \frac{1}{2}\ln\left(\frac{1}{\sigma-1}\right)+O(1)$$

Dirichlet's Thm – general case

Thm (Dirichlet) If $m\geq 1$ and $(a,m)=1$, then

$$\boxed{\sum_{p\equiv a[m]}\frac{1}{p^\sigma} = \frac{1}{\varphi(m)}\ln\left(\frac{1}{\sigma-1}\right)+O(1)}\quad \text{for } \sigma\to 1+$$

($\Rightarrow$ there are infinitely many primes $p\equiv a\,[m]$).

The proof relies on analytic properties of Dirichlet's L-functions, which generalise the functions $L_{-3}(s)$ and $L_{-4}(s)$.

Def. Let $m\geq 1$. A Dirichlet character (mod m) is a group homomorphism $\chi:(\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow U(1)=\{z\in\mathbb{C}\mid |z|=1\}$. Its L-function is defined as

$$L(\chi,s) := \sum_{\substack{n\geq 1\\(n,m)=1}}\frac{\chi(n)}{n^s} = \prod_{p\nmid m}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$$

($\mathrm{Im}(\chi)\subset\mu_{\varphi(m)}(\mathbb{C}) \Rightarrow L(\chi,s)$ is holomorphic for $\mathrm{Re}(s)>1$).

Ex 1: the trivial character $\chi_0(a)=1 \quad \forall a\in(\mathbb{Z}/m\mathbb{Z})^\times$

$$L(\chi_0,s) = \sum_{\substack{n\geq 1\\(n,m)=1}} n^{-s} = \prod_{p\nmid m}(1-p^{-s})^{-1} = \zeta(s)\prod_{p\mid m}(1-p^{-s})$$

Ex 2: $m=q\neq 2$ prime, $\chi(a \pmod q) = \left(\frac{a}{q}\right)$ (the Legendre symbol)

For $q=3$, we obtain $L\left(\left(\frac{\cdot}{3}\right),s\right) = L_{-3}(s)$.

Generalities on characters

(1) For any finite abelian group G, the characters of G form an abelian group $\widehat{G} := \{\chi : G \to U(1) \text{ group morphism}\}$ ("the dual abelian group") with product
$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$$

(2)
$$\begin{array}{ccc} \widehat{G_1 \oplus G_2} & = & \widehat{G_1} \oplus \widehat{G_2} \\ \ni & & \ni \\ \chi & \longleftrightarrow & (\chi_1, \chi_2) \end{array}, \qquad \chi((g_1,g_2)) = \chi_1(g_1)\chi_2(g_2)$$

(3) If G is cyclic of order $n \geq 1$ and if $g_1 \in G$ is a fixed generator of G, then
$$\begin{array}{ccc} \widehat{G} & \xrightarrow{\sim} & \mu_n(\mathbb{C}) \\ \chi & \longmapsto & \chi(g_1) \\ (\chi : g_1^a \mapsto \zeta^a) & \longleftarrow & \zeta \end{array}$$
is a group isomorphism

(4) G is (non-canonically) isomorphic to $\widehat{G}$ ($\Rightarrow |\widehat{G}| = |G|$)

(write $G = \oplus$ cyclic gps and apply (2) and (3))

(5) the canonical map
$$\begin{array}{ccc} G & \longrightarrow & \widehat{\widehat{G}} \\ g & \longmapsto & (\chi \mapsto \chi(g)) \end{array}$$
is a group isomorphism

In other words, the rôles of G and $\widehat{G}$ in the pairing
$$\begin{array}{ccc} \widehat{G} \times G & \longrightarrow & U(1) \\ \chi, g & \longmapsto & \chi(g) \end{array}$$
can be interchanged

(6) $\forall \chi \in \widehat{G}$
$$S := \sum_{g \in G} \chi(g) = \begin{cases} |G| & \chi = 1 \\ 0 & \chi \neq 1 \end{cases} \qquad \Big(\Leftarrow \forall h \in G \quad \chi(h) S = \sum_g \chi(\underbrace{hg}_{g'}) = S\Big)$$

(7) $\forall g \in G$
$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & g = e \\ 0 & g \neq e \end{cases} \Leftarrow (5) + (6)$$

$$\Big(\Rightarrow \forall a, b \in G \quad \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(a)^{-1}\chi(b) = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}\Big)$$

Primary decomposition of Dirichlet characters:

If $m = \prod_{p \mid m} p^{r_p}$, then
$$\begin{tikzcd} (\mathbb{Z}/m\mathbb{Z})^\times \arrow[r, "\sim"] \arrow[dr, "\chi"'] & \bigoplus_{p \mid m} (\mathbb{Z}/p^{r_p}\mathbb{Z})^\times \arrow[d, "(\chi_p)_{p \mid m}"] \\ & U(1) \end{tikzcd}$$

Primitive and nonprimitive Dirichlet characters

For the trivial character $\chi_0 \pmod m$ we have $L(\chi_0, s) = \zeta(s) \prod_{p|m} (1-p^{-s})^{-1}$, which is not good, since we want $\zeta(s)$. The point is that χ_0 factors as

$$\begin{tikzcd} (\mathbb{Z}/m\mathbb{Z})^\times \arrow[rr, "pr"] \arrow[dr, "\chi_0"'] & & (\mathbb{Z}/1\cdot\mathbb{Z})^\times \arrow[dl, "\chi_1"] \\ & U(1) & \end{tikzcd}$$

and $L(\chi_1, s) = \zeta(s)$.

<u>Def</u>. A Dirichlet character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow U(1)$ modulo m is <u>primitive</u> if it <u>does not factor</u> as

$$\begin{tikzcd} (\mathbb{Z}/m\mathbb{Z})^\times \arrow[rr, "pr"] \arrow[dr, "\chi"'] & & (\mathbb{Z}/d\mathbb{Z})^\times \arrow[dl, "\chi'"] \\ & U(1) & \end{tikzcd}$$

for any divisor $d|m$, $d \neq m$.

<u>Ex</u>: $m = p$ prime, $\chi \neq \chi_0$ (e.g., $\chi = \left(\frac{\cdot}{p}\right)$ if $p \neq 2$)

<u>Prop</u>. For every $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow U(1)$ there exists a <u>unique</u> <u>primitive character</u> $\chi_{prim} : (\mathbb{Z}/d\mathbb{Z})^\times \longrightarrow U(1)$ (the <u>primitive character</u> associated to χ) such that $d|m$ and

$$\begin{tikzcd} (\mathbb{Z}/m\mathbb{Z})^\times \arrow[rr, "pr"] \arrow[dr, "\chi"'] & & (\mathbb{Z}/d\mathbb{Z})^\times \arrow[dl, "\chi_{prim}"] \\ & U(1) & \end{tikzcd}.$$

The integer $d \geq 1$ is called the <u>conductor of χ</u> (= the conductor of χ_{prim}).

<u>Notation</u>: $d = f_\chi$ or $f(\chi)$ or q_χ or $q(\chi)$ or $c(\chi)$ ...

<u>Ex</u>: $\chi = \chi_0 \iff f_\chi = 1$.

<u>Pf</u>. Write $\chi = \prod_{p|m} \chi_p$; it is enough to prove Prop. for each $\chi_p : (\mathbb{Z}/p^{r_p}\mathbb{Z})^\times \longrightarrow U(1)$ (then $\chi_{prim} = \prod_{p|m} (\chi_p)_{prim}$).

But if $\chi : (\mathbb{Z}/p^r\mathbb{Z})^\times \longrightarrow U(1)$, then there is unique $k \in \{0, \dots, r\}$ such that χ factors through $\chi_{prim} : (\mathbb{Z}/p^k\mathbb{Z})^\times \longrightarrow U(1)$, but not $(\mathbb{Z}/p^{k-1}\mathbb{Z})^\times \to U(1)$:

$$\begin{tikzcd} (\mathbb{Z}/p^r\mathbb{Z})^\times \arrow[r] \arrow[drr, "\chi"'] & (\mathbb{Z}/p^{r-1}\mathbb{Z})^\times \cdots \arrow[r] & (\mathbb{Z}/p^k\mathbb{Z})^\times \arrow[r] \arrow[d, dotted] & \cdots \arrow[r] & (\mathbb{Z}/p\mathbb{Z})^\times \arrow[r] & (\mathbb{Z}/1\cdot\mathbb{Z})^\times \\ & & U(1) & & & \end{tikzcd}$$

<u>Rmk</u>. A Dirichlet character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow U(1)$ is <u>real</u> (i.e., $\forall a \;\; \chi(a) = \overline{\chi(a)}$) $\iff \mathrm{Im}(\chi) \subset U(1) \cap \mathbb{R} = \{\pm 1\} \iff \chi^2 = \chi_0$.

<u>Prop</u>. $\chi \neq \chi_0$ is a <u>primitive real character</u> $\iff$ $\underbrace{\chi = \chi_D}_{\text{Kronecker's symbol}}$ for some $D = D_K$, $[K:\mathbb{Q}] = 2$

<u>Pf</u>. ($\Leftarrow$) Each χ_D is primitive: enough to show for $D = D_q$, but then either $q \neq 2$, $D = q^*$ and $\chi_{q^*} = \left(\frac{\cdot}{q}\right)$, or $q = 2$ and $D \in \{-4, \pm 8\}$; these characters are all primitive.

($\Rightarrow$) By primary decomposition we can assume that $\chi : (\mathbb{Z}/p^r\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ for some prime p ~~and~~, $r \geq 1$ and $\chi^2 = \chi_0 \neq \chi$. If $p \neq 2$, χ factors through $(\mathbb{Z}/p^r\mathbb{Z})^\times / (\mathbb{Z}/p^r\mathbb{Z})^{\times 2} \xrightarrow{\sim} \mathbb{F}_p^\times / \mathbb{F}_p^{\times 2} \implies r = 1$ and $\chi = \left(\frac{\cdot}{p}\right) = \chi_{p^*}$. If $p = 2$, then either $r = 2$ and $\chi = \chi_{-4}$, or $r \geq 3$ and χ factors through $(\mathbb{Z}/2^r\mathbb{Z})^\times / (\mathbb{Z}/2^r\mathbb{Z})^{\times 2} \xrightarrow{\sim} (\mathbb{Z}/8\mathbb{Z})^\times$ but not $(\mathbb{Z}/4\mathbb{Z})^\times \implies \chi = \chi_8$ or χ_{-8}.

Analytic properties of $L(\chi, s)$, $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to U(1)$

(1) $\chi = \chi_0 \Rightarrow$ $\underbrace{L(\chi_0, s)}_{\zeta(s)\prod_{p|m}(1-p^{-s})} - \frac{c}{s-1}$ has holomorphic continuation to $\mathrm{Re}(s) > 0$

$\left(C = \prod_{p|m} (1 - p^{-1}) \neq 0 \right)$

(2) $\chi \neq \chi_0 \Rightarrow$ $L(\chi, s)$ converges to a holomorphic function for $\mathrm{Re}(s) > 0$

(3) $\overline{L(\chi, s)} = L(\overline{\chi}, \overline{s})$

(4) For $\sigma \in (1, +\infty)$, $\ln L(\chi, \sigma) = \sum_{p \nmid m} \sum_{k \geq 1} \frac{1}{k} \left(\frac{\chi(p)}{p^\sigma} \right)^k = \sum_{p \nmid m} \frac{\chi(p)}{p^\sigma} + O(1)$
as $\sigma \to 1+$

---

(5) $\ln L(\chi_0, \sigma) = \ln \left(\frac{1}{\sigma - 1} \right) + O(1)$ as $\sigma \to 1+$

---

(6) Fix $a \in (\mathbb{Z}/m\mathbb{Z})^\times$; then

$$\frac{1}{\varphi(m)} \sum_{\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to U(1)} \chi(a)^{-1} \ln L(\chi, \sigma) = \sum_{p \nmid m} \frac{1}{p^\sigma} \underbrace{\left(\frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} \chi(p) \right)}_{= \begin{cases} 1 & p \equiv a\,[m] \\ 0 & p \not\equiv a\,[m] \end{cases}} + O(1)$$

$$= \sum_{\cancel{p \nmid m}\ p \equiv a\,[m]} \frac{1}{p^\sigma} + O(1).$$

Key Thm: $\boxed{\forall \chi \neq \chi_0 \qquad L(\chi, 1) \neq 0}$

$\Downarrow$

$\forall \chi \neq \chi_0 \quad \ln(\chi, \sigma) = O(1)$ as $\sigma \to 1+$

$\Downarrow$ (5), (6)

$$\underbrace{\sum_{p \equiv a\,[m]} \frac{1}{p^\sigma} = \frac{1}{\varphi(m)} \ln \left(\frac{1}{\sigma - 1} \right) + O(1) \quad \text{as } \sigma \to 1+}_{\text{Dirichlet's Thm}}$$

Pf of Key Thm. (Step 1) ($\Rightarrow$ the "easy case" $\chi \neq \overline{\chi}$): $\forall \sigma \in (1, +\infty)$

$$\frac{1}{\varphi(m)} \sum_\chi \ln L(\chi, \sigma) = \sum_{p \nmid m} \sum_{k \geq 1} \frac{1}{k p^{k\sigma}} \underbrace{\left(\frac{1}{\varphi(m)} \sum_\chi \chi(p^k) \right)}_{= \begin{cases} 1 & p^k \equiv 1\,[m] \\ 0 & p^k \not\equiv 1\,[m] \end{cases}} > 0$$

$\Rightarrow \boxed{\forall \sigma > 1 \qquad \prod_\chi L(\chi, \sigma) > 1}$

$\Rightarrow \boxed{\sum_\chi \mathrm{ord}_{s=1} L(\chi, s) \leq 0}$

But $\quad \mathrm{ord}_{s=1} L(\chi_0, s) = -1$

$\forall \chi \neq \chi_0 \quad \mathrm{ord}_{s=1} L(\chi, s) = \mathrm{ord}_{s=1} L(\overline{\chi}, s) \geq 0$

$\Rightarrow$ there is <u>at most one</u> $\chi \neq \chi_0$ $\quad (\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow U(1))$ for which $\underbrace{\mathrm{ord}_{s=1} L(\chi, s) > 0}_{\Longleftrightarrow\ L(\chi,1)=0}$; such a χ satisfies $\chi = \overline{\chi}$ (and $\mathrm{ord}_{s=1} L(\chi, s) = 1$)

Therefore $L(\chi,1) \neq 0$ if $\chi \neq \overline{\chi}$.

<u>(Step 2)</u> (the difficult case) If $\chi \neq \chi_0$ and $\chi = \overline{\chi}$ ($\Leftrightarrow \chi^2 = \chi_0$), then $L(\chi, 1) \neq 0$.

<u>Pf</u> (due to de la Vallée Poussin): assume $L(\chi, 1) = 0$

$\Rightarrow \mathrm{ord}_{s=1} L(\chi, s) = 1 \Rightarrow F(s) := \dfrac{L(\chi, s) L(\chi_0, s)}{L(\chi_0, 2s)}$ <u>is holomorphic for $\mathrm{Re}(s) > \frac{1}{2}$</u>

and $\lim\limits_{\sigma \to \frac{1}{2}+} F(\sigma) = 0$ (since $L(\chi_0, 2\sigma) \longrightarrow +\infty$).

For <u>$\mathrm{Re}(s) > 1$</u>,
$$F(s) = \prod_{p \nmid m} \left\{ \begin{array}{ll} (1-p^{-2s})/(1-p^{-s})^2 & \chi(p) = 1 \\ (1-p^{-2s})/(1+p^{-s})(1-p^{-s}) & \chi(p) = -1 \end{array} \right\} =$$
$$= \prod_{\chi(p)=1} \left(\frac{1+p^{-s}}{1-p^{-s}} \right) = \sum_{n \geq 1} a_n n^{-s}, \quad \underline{a_1 = 1, \ \forall n \ a_n \geq 0}$$

$F(s)$ holomorphic for $\mathrm{Re}(s) > \frac{1}{2} \Rightarrow$
$$F(s) = \sum_{m \geq 0} \frac{1}{m!} F^{(m)}(2) \, (s-2)^m \qquad \text{if } |s-2| < \frac{3}{2}$$

But $\quad F^{(m)}(2) = (-1)^m \sum\limits_{n \geq 1} a_n (\ln(n))^m n^{-2} = (-1)^m b_m, \qquad b_m \geq 0$

$$\Rightarrow \quad F(s) = \sum_{m \geq 0} \frac{1}{m!} b_m (2-s)^m \qquad \text{if } |s-2| < \frac{3}{2}$$

For <u>$s = \sigma \in (\frac{1}{2}, 2)$</u>, $\quad b_m (2-\sigma)^m \geq 0 \Rightarrow$ <u>$F(\sigma) \geq F(2) \geq 1$</u>

contradiction with $\lim\limits_{\sigma \to \frac{1}{2}+} F(\sigma) = 0$. Therefore $L(\chi, 1) \neq 0$.

<u>Dirichlet's proof of the difficult case</u>: his original article contained a complete proof only for $m = q$ $(\neq 2)$ prime, using an explicit formula for $L(\chi, 1) = L((\frac{\cdot}{q}), 1)$. The general case follows from Dirichlet's class number formula – proved by him a few years later – which gives a somewhat less explicit, but manifestly non-zero, value of $L(\chi, 1)$ $(\chi = \overline{\chi})$. The formula relies on the QRL, though.

Zeta-functions and L-functions of number fields

Recall: the Riemann zeta-function $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1-\frac{1}{p^s}\right)^{-1}$

the Dedekind zeta-function $\zeta_K(s) := \sum_{\substack{I \subset \mathcal{O}_K \\ \text{ideal} \neq (0)}} \frac{1}{N(I)^s} = \prod_{P \in \mathrm{Max}(\mathcal{O}_K)} \left(1-\frac{1}{N(P)^s}\right)^{-1}$

($[K:\mathbb{Q}]<\infty$, s = formal variable)

Partial Dedekind zeta-function: fix an ideal class $\mathcal{C} \in Cl_K = \mathrm{Pic}(\mathcal{O}_K)$

$$\boxed{\zeta_{K,\mathcal{C}}(s) := \sum_{\substack{(0) \neq I \subset \mathcal{O}_K \\ [I] = \mathcal{C}}} \frac{1}{N(I)^s}}$$

($[I]$ = the ideal class of I)

Prop. For any $J \in I(\mathcal{O}_K)$ with $[J] = \mathcal{C}^{-1}$ the map

$$\begin{array}{ccc} (J \smallsetminus \{0\})/\mathcal{O}_K^\times & \longrightarrow & \{ (0) \neq I \subset \mathcal{O}_K \mid [I] = \mathcal{C} \} \\ \alpha \mathcal{O}_K^\times & \longmapsto & I = (\alpha) J^{-1} \end{array}$$

is a bijection.

Pf: $\alpha \in J \smallsetminus \{0\} \Longrightarrow (\alpha) \subset J \Longrightarrow I := \underbrace{(\alpha) J^{-1}}_{\text{depends only on } \alpha\mathcal{O}_K^\times} \subset J J^{-1} = \mathcal{O}_K$, $[I] = [(\alpha)J^{-1}] = [J]^{-1} = \mathcal{C}$

conversely, if $(0) \neq I \subset \mathcal{O}_K$ is an ideal and $[I] = \mathcal{C}$, then $[IJ] = \mathcal{C}\mathcal{C}^{-1} = 1$, hence $IJ = (\alpha)$, $0 \neq \alpha \in IJ \subset J$; and $I = (\alpha)J^{-1}$.

Cor. $$\boxed{\zeta_{K,\mathcal{C}}(s) = N(J)^s \sum_{\alpha \in (J \smallsetminus \{0\})/\mathcal{O}_K^\times} \frac{1}{|N_{K/\mathbb{Q}}(\alpha)|^s} \qquad [J] = \mathcal{C}^{-1}}$$

Pf: $N((\alpha)J^{-1}) = |N_{K/\mathbb{Q}}(\alpha)| / N(J)$.

Ex 1. If $\mathcal{O}_K$ is factorial ($\Longleftrightarrow Cl_K = \{1\}$), then $$\boxed{\zeta_K(s) = \sum_{\alpha \in (\mathcal{O}_K \smallsetminus \{0\})/\mathcal{O}_K^\times} \frac{1}{|N_{K/\mathbb{Q}}(\alpha)|^s}}$$

Ex (1a): $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot i$, $N_{K/\mathbb{Q}}(x+yi) = x^2+y^2$, $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$

$$\boxed{\zeta_{\mathbb{Q}(i)}(s) = \frac{1}{4} \sum_{x,y \in \mathbb{Z}}{}' \frac{1}{(x^2+y^2)^s}}$$

($\sum'$ = one omits $\binom{x}{y} = \binom{0}{0}$)

(1b): $K = \mathbb{Q}(i\sqrt{3})$, $\mathcal{O}_K = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\rho$, $\rho = e^{2\pi i/3}$, $N_{K/\mathbb{Q}}(x+y\rho) = x^2 - xy + y^2$, $\mathcal{O}_K^\times = \{\pm 1, \pm\rho, \pm\rho^2\}$

$$\boxed{\zeta_{\mathbb{Q}(i\sqrt{3})}(s) = \frac{1}{6} \sum_{x,y \in \mathbb{Z}}{}' \frac{1}{(x^2-xy+y^2)^s}}$$

(1c): $K = \mathbb{Q}(\sqrt{2})$, $\mathcal{O}_K = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\sqrt{2}$, $N_{K/\mathbb{Q}}(x+y\sqrt{2}) = x^2 - 2y^2$, $\mathcal{O}_K^\times = \pm \underbrace{(1+\sqrt{2})}_{\varepsilon}{}^{\mathbb{Z}}$

$$\boxed{\zeta_{\mathbb{Q}(\sqrt{2})}(s) = \frac{1}{2} \sum_{x+y\sqrt{2} \in (\mathbb{Z}[\sqrt{2}] \smallsetminus \{0\})/\varepsilon^{\mathbb{Z}}} \frac{1}{|x^2-2y^2|^s}}$$

Convergence of $\zeta_K(s)$

$\forall$ prime p: $\quad p\mathcal{O}_K = (p) = \prod_{P|p} P^{e_P}$, $N(P) = p^{f_P}$, $\sum_{P|p} e_P f_P = [K:\mathbb{Q}]$

$\Rightarrow \quad \forall \sigma > 0 \qquad \prod_{P|p} \underbrace{(1-N(P)^{-\sigma})^{-1}}_{\sum_{k\geq 0} N(P)^{-k\sigma}} \leq \left(\sum_{k\geq 0} p^{-k\sigma}\right)^{[K:\mathbb{Q}]} = (1-p^{-\sigma})^{-[K:\mathbb{Q}]}$

$\Rightarrow \quad \forall \sigma > 1 \qquad \zeta_K(\sigma) \leq \zeta(\sigma)^{[K:\mathbb{Q}]}$

$\Rightarrow \quad \zeta_K(s)$ converges (absolutely) for $\mathrm{Re}(s) > 1$ to a holomorphic function

---

Back to $K = \mathbb{Q}(\sqrt{2})$: we want a nice set of representatives for

$$(\mathcal{O}_K \setminus \{0\})/\mathcal{O}_K^\times = (\mathbb{Z}[\sqrt{2}] \setminus \{0\}) / \pm\varepsilon^{\mathbb{Z}}, \qquad \varepsilon = 1+\sqrt{2}$$

We construct geometrically such a set of representatives for $(\mathbb{Z}[\sqrt{2}]\setminus\{0\})/\varepsilon^{\mathbb{Z}}$.

Recall: $K = \mathbb{Q}(\sqrt{2}) \xhookrightarrow{\sigma} K_{\mathbb{R}} = \mathbb{R}\times\mathbb{R} \xrightarrow{N} \mathbb{R}$, $\quad N(x_1,x_2) = x_1x_2$

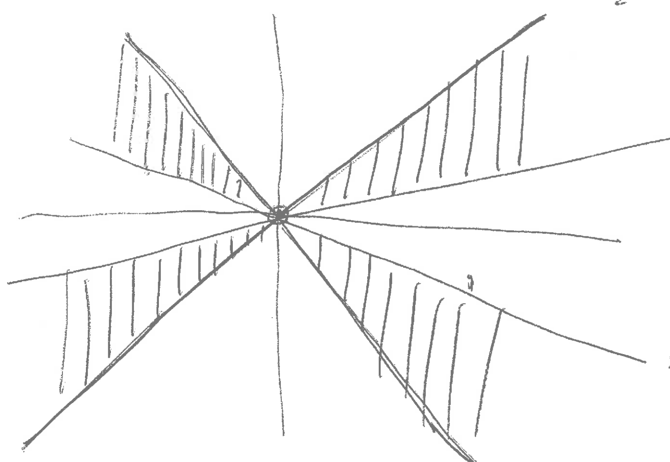
$\alpha = a+b\sqrt{2} \longmapsto (\underbrace{a+b\sqrt{2}}_{\alpha}, \underbrace{a-b\sqrt{2}}_{\alpha'})$

$\sigma(\mathcal{O}_K) = \mathbb{Z}\cdot(1,1) \oplus \mathbb{Z}\cdot(\sqrt{2},-\sqrt{2})$, $\qquad \sigma(\varepsilon) = (\varepsilon,\varepsilon') = (\varepsilon, -\varepsilon^{-1}) = (1+\sqrt{2}, 1-\sqrt{2})$

Nice fundamental domain for $\sigma(\varepsilon)^{\mathbb{Z}} \subset \mathbb{R}^\times \times \mathbb{R}^\times$:

$$X := \{(x_1,x_2) \in \mathbb{R}^\times \times \mathbb{R}^\times \mid 1 \leq |x_1/x_2| < |\varepsilon|^2\}$$

$$\mathbb{R}^\times \times \mathbb{R}^\times = \coprod_{u\in\varepsilon^{\mathbb{Z}}} u\cdot X$$



(this works for arbitrary real quadratic fields ($\mathcal{O}_K^\times = \pm\varepsilon^{\mathbb{Z}}$, $|\varepsilon| > 1$).)

therefore $\quad \zeta_K(s) = \frac{1}{2} \sum_{(x_1,x_2)\in\sigma(\mathcal{O}_K)\cap X} \frac{1}{|x_1x_2|^s}$.

$2 = |\underbrace{(\mathcal{O}_K^\times)_{\mathrm{tors}}}_{\{\pm 1\}}|$

A ~~the~~ fundamental domain for $(\mathcal{O}_K^\times)/(\mathcal{O}_K^\times)_{\mathrm{tors}}$ in general

$$\begin{tikzcd}
K\setminus\{0\} \arrow[r, hook, "\sigma"] & K_{\mathbb{R}}^\times \arrow[r, "\sim"] & (\mathbb{R}^\times)^{r_1}\times(\mathbb{C}^\times)^{r_2} \arrow[r, "\ell'"] & \mathbb{R}^{r_1+r_2} \arrow[r, "\Sigma"] & \mathbb{R} \\
 & & (y,z) \arrow[r, mapsto] & ((\log|y_j|),(\log|z_k|^2)) & \\
\mathcal{O}_K^\times \arrow[uu, hook] \arrow[rrr, "\ell"] & & & H=\mathrm{Ker}(\Sigma) \arrow[uu, hook, bend left] &
\end{tikzcd}$$

$$N(y,z)=\prod_1^{r_1}|y_j|\prod_1^{r_2}|z_k|^2$$

Fix $\varepsilon_1,\dots,\varepsilon_{r_1+r_2-1}\in\mathcal{O}_K^\times$ such that

$$\mathcal{O}_K^\times=\underbrace{(\mathcal{O}_K^\times)_{\mathrm{tors}}}_{\text{cyclic of order } w=w_K}\times\varepsilon_1^{\mathbb{Z}}\cdots\varepsilon_{r_1+r_2-1}^{\mathbb{Z}}$$

and let $(\mathcal{O}_K^\times)_{\mathrm{free}}:=\varepsilon_1^{\mathbb{Z}}\cdots\varepsilon_{r_1+r_2-1}^{\mathbb{Z}}\subset\mathcal{O}_K^\times$ (depends on our choice of the ε_j's)

<u>Dirichlet:</u> $\ell:(\mathcal{O}_K^\times)_{\mathrm{free}}\hookrightarrow H$, $\ell((\mathcal{O}_K^\times)_{\mathrm{free}})$ is a <u>lattice in H</u>

<u>Fundamental domains:</u> (a) of $\ell((\mathcal{O}_K^\times)_{\mathrm{free}})$ in H:

$$F=\left\{\sum_{j=1}^{r_1+r_2-1}t_j\,\ell(\varepsilon_j)\;\middle|\;0\le t_j<1\right\}\subset H$$

(b) of $(\mathcal{O}_K^\times)_{\mathrm{free}}$ in $K_{\mathbb{R}}^\times$:

$$X=\mathbb{R}_{>0}\cdot\ell'^{-1}(F)\subset K_{\mathbb{R}}^\times$$

<u>Ex:</u> (1) <u>$K=\mathbb{Q}(\sqrt{d}),\ d<0$</u> : $r_1=0,\ r_2=1,\ (\mathcal{O}_K^\times)_{\mathrm{free}}=\{1\}$, $H=F=\{0\}$

$K_{\mathbb{R}}^\times=\mathbb{C}^\times$, $\ell'^{-1}(F)=U(1)=\{z\in\mathbb{C}^\times;\ |z|=1\}$, $X=\mathbb{C}^\times$

(2) <u>$K=\mathbb{Q}(\sqrt{d}),\ d>0$</u> : (as for $d=2$ above) $(\mathcal{O}_K^\times)_{\mathrm{free}}=\varepsilon^{\mathbb{Z}}$, ~~$\varepsilon>1$~~

$$\begin{tikzcd}
(x_1,x_2)\in K_{\mathbb{R}}^\times=\mathbb{R}^\times\times\mathbb{R}^\times \arrow[d, "\ell'"] \\
(\log|x_1|,\log|x_2|)\in\mathbb{R}\times\mathbb{R}
\end{tikzcd}$$

$H=\{(a,-a)\mid a\in\mathbb{R}\}\subset\mathbb{R}\times\mathbb{R}$

$$F=\{(t,-t)\mid 0\le t<\log|\varepsilon|\}$$

$$X=\{(x_1,x_2)\in\mathbb{R}^\times\times\mathbb{R}^\times\mid 1\le|x_1/x_2|<|\varepsilon|^2\}$$

<u>Measures</u> : $\mu=2^{r_2}\mu_{\mathrm{Lebesgue}}$ on $K_{\mathbb{R}}=\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$

$$\mu_{\mathrm{Lebesgue}}\text{ on }\Big(\mathbb{R}^{r_1+r_2}=\mathbb{R}\cdot(\underbrace{\tfrac1n,\dots,\tfrac1n}_{r_1},\underbrace{\tfrac2n,\dots,\tfrac2n}_{r_2})\oplus H\Big)$$

$$=\mu_{\mathrm{Lebesgue}}\text{ on }\mathbb{R}\cdot\mu_H$$

$$\Rightarrow\quad \mu_H\big(H/\ell((\mathcal{O}_K^\times)_{\mathrm{free}})\big)=R_K=\left|\det\begin{pmatrix}\frac1n & \cdots & \frac2n\\ \log|\sigma_1(\varepsilon_1)| & & \log|\sigma_{r_1+r_2}(\varepsilon_1)|^2\\ \vdots & & \vdots\\ \log|\sigma_1(\varepsilon_{r_1+r_2-1})| & \cdots & \log|\sigma_{r_1+r_2}(\varepsilon_{r_1+r_2-1})|^2\end{pmatrix}\right|$$

<u>the regulator of K</u>

<u>Ex</u>: $K=\mathbb{Q}(\sqrt{d}),\ d>0,\ (\mathcal{O}_K^\times)_{\mathrm{free}}=\varepsilon^{\mathbb{Z}}$:

$$R_K=\left|\det\begin{pmatrix}\frac12 & \frac12\\ \log|\varepsilon| & \log|\varepsilon'|\end{pmatrix}\right|=\big|\log|\varepsilon|\big|\quad(=\log(\varepsilon)\text{ if }\varepsilon>1)$$

Ex. 2. $\underline{K=\mathbb{Q}(i\sqrt{5})}$, $\mathcal{O}_K=\mathbb{Z}\cdot 1+\mathbb{Z}\cdot i\sqrt{5}$, $\mathcal{O}_K^\times=\{\pm 1\}$, $\underline{h_K=2}$

$Cl_K=\{\underbrace{[(1)]}_{\mathcal{O}_K},\ [J]=[J]^{-1}\}$, $J=2\mathbb{Z}+(1+i\sqrt{5})\mathbb{Z}$, $J^2=(2)$, $N(J)=2$

$\alpha=x+y\,i\sqrt{5}\in\mathcal{O}_K \Longrightarrow N_{K/\mathbb{Q}}(\alpha)=\underline{x^2+5y^2=Q_1(x,y)}$

$\alpha=2x+(1+i\sqrt{5})y\in J \Longrightarrow \dfrac{N_{K/\mathbb{Q}}(\alpha)}{N(J)}=\dfrac{(2x+y)^2+5y^2}{2}=\underline{2x^2+2xy+3y^2=Q_2(x,y)}$

$$\left.\begin{aligned}\zeta_{\mathbb{Q}(i\sqrt{5}),[(1)]}(s)&=\frac{1}{2}\sum_{x,y\in\mathbb{Z}}{}'\frac{1}{(x^2+5y^2)^s}\\ \zeta_{\mathbb{Q}(i\sqrt{5}),[J]}(s)&=\frac{1}{2}\sum_{x,y\in\mathbb{Z}}{}'\frac{1}{(2x^2+2xy+3y^2)^s}\end{aligned}\right\}\Longrightarrow \boxed{\zeta_{\mathbb{Q}(i\sqrt{5})}(s)=\frac{1}{2}\sum_{x,y\in\mathbb{Z}}{}'\left(\frac{1}{Q_1(x,y)^s}+\frac{1}{Q_2(x,y)^s}\right)}$$

Factorisation of $\zeta_K(s)$ for $[K:\mathbb{Q}]=2$

Ex 1. $K=\mathbb{Q}(i)$ $\quad(\pi=u+iv,\ u^2+v^2=p)$

$$(p)=\begin{cases}P^2=(1+i)^2 & p=2,\ N(P)=p=2\\ P_1P_2=(\pi)(\bar\pi) & p\equiv 1\,[4],\quad N(P_j)=p\\ P=(p) & p\equiv -1\,[4],\quad N(P)=p^2\end{cases}$$

$$\Longrightarrow \zeta_{\mathbb{Q}(i)}(s)=\left(1-\frac{1}{2^s}\right)^{-1}\prod_{p\equiv 1[4]}\left(1-\frac{1}{p^s}\right)^{-2}\prod_{p\equiv -1[4]}\left(1-\frac{1}{p^{2s}}\right)^{-1}$$

$$=\zeta(s)\underbrace{\prod_{p\equiv 1[4]}\left(1-\frac{1}{p^s}\right)^{-1}\prod_{p\equiv -1[4]}\left(1+\frac{1}{p^s}\right)^{-1}}_{1-\frac{1}{3^s}+\frac{1}{5^s}-\frac{1}{7^s}+\cdots}$$

Ex 2. $K=\mathbb{Q}(i\sqrt{3})$ $\quad(\pi=u+v\rho,\ u^2-uv+v^2=p)$

$$(p)=\begin{cases}P^2=(\rho-\rho^2)^2 & p=3,\ N(P)=p=3\\ P_1P_2=(\pi)(\bar\pi) & p\equiv 1\,[3],\quad N(P_j)=p\\ P=(p) & p\equiv -1\,[3],\quad N(P)=p^2\end{cases}$$

$$\Longrightarrow \zeta_{\mathbb{Q}(i\sqrt{3})}(s)=\left(1-\frac{1}{3^s}\right)^{-1}\prod_{p\equiv 1[3]}\left(1-\frac{1}{p^s}\right)^{-2}\prod_{p\equiv -1[3]}\left(1-\frac{1}{p^{2s}}\right)^{-1}$$

$$=\zeta(s)\underbrace{\prod_{p\equiv 1[3]}\left(1-\frac{1}{p^s}\right)\prod_{p\equiv -1[3]}\left(1+\frac{1}{p^s}\right)}_{1-\frac{1}{2^s}+\frac{1}{4^s}-\frac{1}{5^s}+\frac{1}{7^s}-\frac{1}{8^s}+\cdots}$$

In general: $[K:\mathbb{Q}]=2 \Longleftrightarrow \exists!\, d\in\mathbb{Z}\setminus\{0,1\}$ square-free $K=\mathbb{Q}(\sqrt{d})$

$$D:=D_K=\begin{cases}d & d\equiv 1\,[4]\\ 4d & d\equiv 2,3\,[4]\end{cases}$$

$\forall\, p\neq 2$ (or if $p=2\mid D$)

$$(p)=\begin{cases}P^2 & p\mid d,\quad N(P)=p\\ P_1P_2 & \left(\frac{d}{p}\right)=1,\quad N(P_j)=p\\ P & \left(\frac{d}{p}\right)=-1,\quad N(P)=p^2\end{cases}$$

If $d\equiv 1\,[4]$:

$$(2)=\begin{cases}P_1P_2 & d\equiv 1\,[8],\quad N(P_j)=p\\ (P) & d\equiv 5\,[8],\quad N(P)=p^2\end{cases}$$

$$\Rightarrow \zeta_{\mathbb{Q}(\sqrt{d})}(s) = \zeta(s) \underbrace{\left(\prod_{p \nmid 2d} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p^s}\right)\right)}_{\sum_{\substack{n \geq 1 \\ (n,2d)=1}} \left(\frac{d}{n}\right)\frac{1}{n^s}} \cdot \begin{cases} 1 & d \equiv 2,3\,[4] \\ \left(1 - \frac{1}{2^s}\right)^{-1} & d \equiv 1\,[8] \\ \left(1 + \frac{1}{2^s}\right)^{-1} & d \equiv 5\,[8] \end{cases}$$

$\left(\frac{d}{n}\right)$ = the Jacobi symbol

Ex: $d = -5$, $D = -20$: $\zeta_{\mathbb{Q}(i\sqrt{5})}(s) = \zeta(s) \underbrace{\prod_{p \neq 2,5} \left(1 - \left(\frac{-5}{p}\right)\frac{1}{p^s}\right)^{-1}}_{\sum_{\substack{n \geq 1 \\ (n,20)=1}} \left(\frac{-5}{n}\right)\frac{1}{n^s} = \sum_{\substack{n\geq 1 \\ (n,20)=1}} (-1)^{\frac{n-1}{2}}\left(\frac{n}{5}\right)\frac{1}{n^s}}$

QRL: if $n \geq 1$, $(n,20)=1$ $\Downarrow$

$$\left(\frac{-5}{n}\right) = \left(\frac{-1}{n}\right)\cdot\left(\frac{5}{n}\right) = \underbrace{(-1)^{\frac{n-1}{2}}}_{\substack{\text{depends on} \\ n \,(\mathrm{mod}\, 4)}} \cdot \underbrace{\left(\frac{n}{5}\right)}_{\substack{\text{depends on} \\ n\,(\mathrm{mod}\,5)}}$$

$\Rightarrow \left(\frac{-5}{n}\right)$ depends only on $n \pmod{20}$

and $\left(\frac{-5}{mn}\right) = \left(\frac{-5}{m}\right)\left(\frac{-5}{n}\right)$

(above, $m, n \geq 1$ and $(m,20) = (n,20) = 1$)

General formula – Kronecker's symbol

Prop. let $d \in \mathbb{Z} \setminus \{0,1\}$ be square-free, $D := \begin{cases} d, & d \equiv 1\,[4] \\ 4d, & d \equiv 2,3\,[4] \end{cases}$. (1) there exists a unique map $\chi_D : (\mathbb{Z}/|D|\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ such that $\forall\, n \geq 1$ such that $(n, 2d) = 1$ $\left(\frac{d}{n}\right) = \chi_D(n \,(\mathrm{mod}\, |D|))$

(2) $\chi_D(ab) = \chi_D(a)\chi_D(b)$ (i.e., χ_D is a group homomorphism)

Pf: enough to show: $\left(\frac{d}{n}\right)$ depends only on $n \pmod{|D|}$ (for $n \geq 1$ such that $(n,2d)=1$). Write

$D = \prod_{\substack{q \mid D \\ q \text{ prime}}} D_q$, where (a) $|D_q|$ = a power of q $\forall q \mid D$

(b) $D_q \equiv 1\ [4]$ if $q \neq 2$

(ex: $-20 = (-4)\cdot 5$). This determines the D_q's uniquely:

- $q \mid D$, $q \neq 2 \Rightarrow D_q = q^* := (-1)^{\frac{q-1}{2}} q = \begin{cases} q, & q \equiv 1\,[4] \\ -q, & q \equiv -1\,[4] \end{cases}$
- $q \mid D$, $q = 2 \Rightarrow D_2 \in \{-4, \pm 8\}$ (since $\prod_{2 \neq q \mid D} D_q \equiv 1\ [4]$).

If $n \geq 1$ and $(n,2d)=1$, then

$\left(\frac{d}{n}\right) = \left(\frac{D}{n}\right) = \prod_{q \mid D} \left(\frac{D_q}{n}\right)$ and

- $q \mid D$, $q \neq 2 \Rightarrow \left(\frac{D_q}{n}\right) = \left(\frac{q^*}{n}\right) = \left(\frac{n}{q}\right)$ (Legendre's symbol) depends only on $n \pmod q = n \pmod{|D_q|}$
- $q \mid D$, $q = 2 \Rightarrow$ if $D_q = -4 \Rightarrow \left(\frac{-4}{n}\right) = (-1)^{\frac{n-1}{2}}$ depends only on $n \pmod 4$

  if $D_q = 8 \Rightarrow \left(\frac{8}{n}\right) = \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ — " — $n \pmod 8$

  if $D_q = -8 \Rightarrow \left(\frac{-8}{n}\right) = (-1)^{\frac{n-1}{2}}\cdot(-1)^{\frac{n^2-1}{8}}$ — " — .

We now forget the quadratic reciprocity law and instead <u>define</u> χ_D using the formulas in the proof of the above Prop.

<u>Def.</u> let $d \in \mathbb{Z} \setminus \{0,1\}$ be square-free, let $D := \begin{cases} d, & d \equiv 1 [4] \\ 4d, & d \equiv 2,3 [4] \end{cases}$.

Factor $D = \prod_{\substack{q \mid D \\ \text{prime}}} D_q$, $\quad D_q = q^* = (-1)^{\frac{q-1}{2}} q$ if $q \neq 2$, $\quad D_2 \in \{-4, \pm 8\}$ (if $2 \mid D$) and define

$$\chi_{D_q} : (\mathbb{Z}/|D_q|\mathbb{Z})^\times \longrightarrow \{\pm 1\}, \qquad \chi_D : (\mathbb{Z}/|D|\mathbb{Z})^\times \longrightarrow \{\pm 1\}$$ as follows:

$$\chi_D = \prod_{q \mid D} \chi_{D_q}, \qquad \chi_{q^*}(\cdot) := \left(\frac{\cdot}{q}\right) \quad \text{(the Legendre symbol)},$$

$$\chi_{-4}(a \,(\mathrm{mod}\ 4)) := \begin{cases} 1 & a \equiv 1 [4] \\ -1 & a \equiv -1 [4] \end{cases} = (-1)^{\frac{a-1}{2}}$$

$$\chi_8(a \,(\mathrm{mod}\ 8)) := \begin{cases} 1 & a \equiv \pm 1 [8] \\ -1 & a \equiv \pm 5 [8] \end{cases} = (-1)^{\frac{a^2-1}{8}}$$

$$(\chi_{-8} := \chi_{-4}\chi_8)(a \,(\mathrm{mod}\ 8)) := \begin{cases} 1 & a \equiv 1, 3 [8] \\ -1 & a \equiv 5, 7 [8] \end{cases}$$

The group morphism χ_D is called the <u>Kronecker symbol</u>.

<u>Prop.</u> (0) If $n \geq 1$ and $(n, 2d) = 1$, then $\chi_D(n \,(\mathrm{mod}\ |D|)) = \left(\frac{d}{n}\right)$.

(1) $\chi_D(-1) = \mathrm{sgn}(D)$

(2) If $2 \nmid D$ ($\iff d \equiv 1 [4]$), then $\chi_D(2) = \begin{cases} 1 & d \equiv 1 [8] \\ -1 & d \equiv 5 [8] \end{cases}$.

<u>Pf.</u> (1) $q \neq 2 \implies \chi_{D_q}(-1) = \left(\frac{-1}{q}\right) = \mathrm{sgn}(D_q)$

$q = 2$: $\chi_{-4}(-1) = \chi_{-8}(-1) = -1$, $\chi_8(-1) = 1 \implies \chi_{D_q}(-1) = \mathrm{sgn}(D_q)$

(2) $2 \nmid D \implies d = D = \prod_{q \mid D} q^* \equiv 1 [4]$, $\chi_D(2) = \prod_{q \mid D} \left(\frac{2}{q}\right) = \begin{cases} 1 & |d| \equiv \pm 1 [8] \iff d \equiv 1 [8] \\ -1 & |d| \equiv \pm 5 [8] \underset{d \equiv 1 [4]}{\iff} d \equiv 5 [8] \end{cases}$

$|d| = \prod_{q \mid D} q$

<u>Cor.</u> $\forall$ prime p, $K = \mathbb{Q}(\sqrt{d})$, $D = D_K$:

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}^2 & p \mid D \\ \mathfrak{p}_1 \mathfrak{p}_2 & p \nmid D,\ \chi_D(p) = 1 \\ \mathfrak{p} & p \nmid D,\ \chi_D(p) = -1 \end{cases}$$

$$\implies \zeta_{\mathbb{Q}(\sqrt{d})}(s) = \zeta(s) \underbrace{\prod_{p \nmid D} \left(1 - \frac{\chi_D(p)}{p^s}\right)^{-1}}_{\displaystyle \sum_{\substack{n \geq 1 \\ (n,D)=1}} \frac{\chi_D(n \,(\mathrm{mod}\ |D|))}{n^s} =: L(\chi_D, s)}$$

this formula (for all d) is equivalent to the QRL.

Rmk: factorisation in $K=\mathbb{Q}(i\sqrt{5})$ and ideal classes:

$Cl_K=\{1,[J]\}$, $\quad J=(2,1+i\sqrt{5})$

$(2)=J^2$, $(5)=(i\sqrt{5})^2$, $\quad (i\sqrt{5})\sim 1$, $J\nsim 1$

$p\neq 2,5$: $\left(\frac{-5}{p}\right)=-1 \Longrightarrow (p)=P$, $\quad N(P)=p^2$, $P\sim 1$

$\left(\frac{-5}{p}\right)=1$: $\left(\frac{-5}{p}\right)=\underbrace{\left(\frac{-1}{p}\right)}_{\chi_{-4}(p)}\underbrace{\left(\frac{5}{p}\right)}_{\left(\frac{p}{5}\right)}=\chi_{-4}(p)\,\chi_5(p)$, $\quad p=P\overline{P}$, $P\neq\overline{P}$, $N(P)=N(\overline{P})=p$

if $P\sim 1 \Longrightarrow P=(x+i\sqrt{5}\,y) \Longrightarrow p=N(P)=x^2+5y^2\equiv x^2\,[5]\equiv\pm1\,[5]$

$(x,y\in\mathbb{Z})$ $\quad\Longrightarrow \chi_5(p)=\chi_{-4}(p)=1$

if $P\nsim 1 \Longrightarrow PJ=(x+i\sqrt{5}y) \Longrightarrow 2p=N(PJ)=x^2+5y^2\equiv\pm1\,[5]$

$\longrightarrow \chi_5(p)=\chi_{-4}(p)=-1$.

this implies:

$$\zeta_{\mathbb{Q}(i\sqrt{5}),[(1)]}(s)-\zeta_{\mathbb{Q}(i\sqrt{5}),[J]}(s)=\frac{1}{2}\sum_{x,y\in\mathbb{Z}}{}'\frac{1}{(x^2+5y^2)^s}-\frac{1}{2}\sum_{x,y\in\mathbb{Z}}{}'\frac{1}{(2x^2+2xy+3y^2)^s}=$$

$$=\prod_{p\neq 2}\left(1-\frac{\chi_{-4}(p)}{p^s}\right)^{-1}\prod_{p\neq 5}\left(1-\frac{\chi_5(p)}{p^s}\right)^{-1}=\left(\sum_{\substack{n\geq 1\\(2,n)=1}}(-1)^{\frac{n-1}{2}}\frac{1}{n^s}\right)\left(\sum_{\substack{n\geq 1\\(5,n)=1}}\left(\frac{n}{5}\right)\frac{1}{n^s}\right)$$

Abel summation (again)

Prop 1. Assume that $a_n \in \mathbb{C}$ $(n \geq 1)$ and that $S(x) := \sum_{1 \leq n \leq x} a_n = S[x]$ satisfies $\lim_{x \to +\infty} S(x)/x = A \in \mathbb{C}$. Then $L(s) := \sum_{n \geq 1} a_n n^{-s}$ is absolutely convergent for $\mathrm{Re}(s) > 1$ to a holomorphic function and
$$\lim_{\sigma \to 1+} (\sigma - 1) L(\sigma) = A.$$

Pf. Recall that $\sum_{n=1}^{N} a_n n^{-s} = S(N) N^{-s} + s \int_1^N \frac{S(x)}{x^{s+1}} dx$. By assumption, $|S(x)| = O(x)$ for $x \to +\infty$ $\Rightarrow$ for $\mathrm{Re}(s) > 1$ $L(s) = \sum_{n \geq 1} a_n n^{-s}$ converges (absolutely) to $s \int_1^\infty \frac{S(x)}{x^{s+1}} dx$. Write $S(x) = x(A + \varepsilon(x))$, $\lim_{x \to +\infty} \varepsilon(x) = 0$.

$$\forall \sigma > 1 \quad L(\sigma) = \sigma \int_1^\infty \frac{A + \varepsilon(x)}{x^\sigma} dx = \frac{A\sigma}{\sigma - 1} + \sigma \int_1^\infty \frac{\varepsilon(x)}{x^\sigma} dx \Rightarrow \boxed{(\sigma-1) L(\sigma) - A\sigma = \sigma(\sigma-1) \int_1^\infty \frac{\varepsilon(x)}{x^\sigma} dx}$$

Fix $\delta > 0$; $\exists\, x(\delta) \geq 0$ $\forall x \geq x(\delta)$ $|\varepsilon(x)| \leq \delta$. Then $\forall \sigma > 1$

$$\left| \int_1^{x(\delta)} \frac{\varepsilon(x)}{x^\sigma} dx \right| \leq C \int_1^{x(\delta)} \frac{dx}{x} = C \ln(x(\delta)) \quad \text{(for some } C > 0 \text{ depending on } \{a_n\})$$

$$\left| \int_{x(\delta)}^\infty \frac{\varepsilon(x)}{x^\sigma} dx \right| \leq \delta \int_{x(\delta)}^\infty \frac{dx}{x^\sigma} = \frac{\delta}{\sigma - 1} x(\delta)^{1-\sigma}$$

$$\Rightarrow \quad |(\sigma-1) L(\sigma) - A\sigma| \leq C\sigma(\sigma-1) \ln(x(\delta)) + \sigma\delta\, x(\delta)^{1-\sigma}$$

$$\Rightarrow \forall \delta > 0 \quad \limsup_{\sigma \to 1+} |(\sigma-1) L(\sigma) - A\sigma| \leq \delta \Longrightarrow \lim_{\sigma \to 1+} (\sigma-1) L(\sigma) = A.$$

Prop. 2. Assume that $0 < \lambda_1 \leq \lambda_2 \leq \lambda_3 \leq \cdots$, $\lim_{k \to +\infty} \lambda_k = +\infty$, and that $A(t) := |\{k \geq 1;\ \lambda_k \leq t\}|$ $(t \geq 0)$ satisfies $\lim_{t \to +\infty} A(t)/t = A \in \mathbb{R}$. Then $Z(s) := \sum_{k \geq 1} \lambda_k^{-s}$ converges (absolutely) to a holomorphic function for $\mathrm{Re}(s) > 1$, and $\lim_{\sigma \to 1+} (\sigma-1) Z(\sigma) = A$.

Pf. $\forall n \in \mathbb{N}_+$ $\quad a_{n+1} := A(n+1) - A(n) = |\{k \geq 1;\ \underbrace{n < \lambda_k \leq n+1}_{\Longrightarrow \forall \sigma > 0 \ (n+1)^{-\sigma} < \lambda_k^{-\sigma} < n^{-\sigma}}\}|$

$$\underset{\forall \sigma > 1}{\Rightarrow} \sum_{n \geq 1} \frac{a_{n+1}}{(n+1)^\sigma} \leq Z(\sigma) - \sum_{\lambda_k \leq 1} \lambda_k^{-\sigma} \leq \sum_{n \geq 1} \frac{a_{n+1}}{n^\sigma}. \text{ Apply Prop. 1.}$$

Dirichlet's geometric thm

Given: $V = \mathbb{R}$- vector space of $\dim_{\mathbb{R}}(V) = d \geq 1$

$L \subset V$ lattice

$X = \mathbb{R}_{>0} X \subset V$

$f : V \longrightarrow \mathbb{R}_{\geq 0}$ such that $\left\{ \begin{array}{l} f(x) = 0 \iff x = 0 \\ \forall t \in \mathbb{R} \quad f(tx) = |t|^d f(x) \end{array} \right\}$

$\boxed{\text{Fix a Lebesgue measure } \mu \text{ on } V.}$

Ex: $V = K_{\mathbb{R}}$, $L = \sigma(J)$, X as above, $f(x) = |N_{K_{\mathbb{R}}/\mathbb{R}}(x)| / N(J)$

Thm. Assume that $\{f \leq 1\} \cap X$ is bounded and "reasonable". Then

(1) $\forall\, t > 0 \quad A(t) := |\{f \leq t\} \cap X \cap L| < \infty$ and

(2) $A := \lim\limits_{t \to +\infty} A(t)/t$ exists and is equal to $\dfrac{\mu(\{f \leq 1\} \cap X)}{\mu(V/L)}$.

(3) $Z(s) := \sum\limits_{0 \neq x \in X \cap L} f(x)^{-s}$ converges (absolutely) for $\mathrm{Re}(s) > 1$ to a holomorphic function

(4) $\lim\limits_{\sigma \to 1+} (\sigma - 1) Z(\sigma) = A = \dfrac{\mu(\{f \leq 1\} \cap X)}{\mu(V/L)}$.

Ex 1. $V = \mathbb{R}$, $L = \mathbb{Z}$, $X = \mathbb{R}_{>0}$, $f(x) = |x|$, $L \cap X = \mathbb{N}_+$, $Z(s) = \zeta(s)$, $A(t) = [t]$, $A = 1$.

Ex 2. $V = \mathbb{R}^2$, $L = \mathbb{Z}^2$, $X = V$, $f(x_1, x_2) = a x_1^2 + b x_1 x_2 + c x_2^2$, $a, b, c \in \mathbb{R}$, $4ac - b^2 > 0$

$$Z(s) = \sum_{x, y \in \mathbb{Z}}{}' (ax^2 + bxy + cy^2)^{-s}, \qquad A = \frac{2\pi}{\sqrt{4ac - b^2}}$$

Ex 3. $K = \mathbb{Q}(\sqrt{d})$, $d < 0$: $\forall\, \mathfrak{C} \in \mathrm{Cl}_K$ $\quad \zeta_{K,\mathfrak{C}}(s) = \dfrac{1}{w_K} Z(s)$, where $Z(s)$ is as in Ex 2, with $a, b, c \in \mathbb{Z}$ and $\underline{\underline{b^2 - 4ac = D_K}}$

$$\overset{\text{Thm}}{\Longrightarrow} \lim_{\sigma \to 1+} (\sigma - 1) \zeta_{K,\mathfrak{C}}(\sigma) = \frac{2\pi}{w_K |D_K|^{1/2}} \Longrightarrow \lim_{\sigma \to 1+} (\sigma - 1) \zeta_K(\sigma) = \frac{2\pi h_K}{w_K |D_K|^{1/2}}$$

$(w_K = |\mathcal{O}_K^\times|)$

Ex 4. $V = K_{\mathbb{R}}$, K any number field, $L = \sigma(J)$, X as above, $\mathfrak{C} = [J]^{-1}$, $f(x) = |N_{K_{\mathbb{R}}/\mathbb{R}}(x)| / N(J) \Longrightarrow w_K Z(s) = \zeta_{K,\mathfrak{C}}(s)$.

We are going to compute

$$\frac{\mu(\{f \leq 1\} \cap X)}{\mu(V/L)} = \frac{2^{r_1} (2\pi)^{r_2} R_K}{|D_K|^{1/2}}$$

$$\Longrightarrow \lim_{\sigma \to 1+} (\sigma - 1) \zeta_{K,\mathfrak{C}}(\sigma) = \frac{2^{r_1} (2\pi)^{r_2} R_K}{w_K |D_K|^{1/2}}$$

$$\boxed{\lim_{\sigma \to 1+} (\sigma - 1) \zeta_K(\sigma) = \frac{2^{r_1} (2\pi)^{r_2} R_K h_K}{w_K |D_K|^{1/2}} \qquad \text{Dedekind's class number formula}}$$

Pf of thm: (1) $\{f\le t\}\cap X = t^{1/d}(\{f\le 1\}\cap X)$ is bounded $\Rightarrow |A(t)|<\infty$

(2) $\{f\le 1\}\cap X$ is "reasonable" $\Rightarrow$ $$\frac{\mu(\{f\le 1\}\cap X)}{\mu(V/L)} = \lim_{t\to+\infty}\frac{|\{f\le 1\}\cap X\cap t^{-1/d}L|}{t^{d}}$$

But multiplication by $t^{1/d}$ defines a bijection between $\{f\le 1\}\cap X\cap t^{-1/d}L$ and $\{f\le t\}\cap X\cap L$.

(3), (4) Apply Prop. 2 to $\{\lambda_k\}=\{f(x)\mid x\in X\cap L\setminus\{0\}\}$ (with multiplicities

---

Ex 3'. $K=\mathbb{Q}(\sqrt d)$, $d>0$, X as above, $V=\underbrace{K_{\mathbb R}}_{\mathbb R\times\mathbb R}$, $L=\sigma(J)$, $\mathcal{C}=[J]^{-1}$

$f(x_1,x_2)=|x_1x_2|/N(J)$, $\mu=\mu_{\text{Lebesgue}}$ on $\mathbb R\times\mathbb R$

$\mu(V/L)=|D_K|^{1/2}N(J)$

$$\frac{\mu(\{f\le 1\}\cap X)}{N(J)} = \mu(\{|x_1x_2|\le 1\}\cap \underbrace{X}_{\{1\le |x_1/x_2|\le|\varepsilon|^2\}}) \qquad |x_j|=e^{y_j}$$

$$= 4\cdot\int_{\substack{y_1,y_2\in\mathbb R\\ y_1+y_2\le 0\\ 0\le y_1-y_2\le 2\log|\varepsilon|}} e^{y_1+y_2}\,dy_1\,dy_2 \qquad \begin{matrix} y_1+y_2=u\\ y_1-y_2=v\end{matrix}$$

$$= 4\int_{\substack{u\le 0\\ 0\le v\le 2\log|\varepsilon|}} e^{u}\,\frac{du\,dv}{2} = 2\cdot\left(\int_{-\infty}^{0} e^{u}\,du\right)\left(\int_0^{2\log|\varepsilon|} dv\right) = 4\log|\varepsilon|$$

$\Rightarrow A=\dfrac{4\log|\varepsilon|}{|D_K|^{1/2}}$. As $Z(s)=\dfrac{\ }{w_K}\zeta_{K,\mathcal C}(s) = 2\zeta_{K,\mathcal C}(s)$, we get

$$\lim_{\sigma\to 1+}(\sigma-1)\zeta_{K,\mathcal C}(\sigma)=\frac{2\log(\varepsilon)}{|D_K|^{1/2}},\qquad \lim_{\sigma\to 1+}(\sigma-1)\zeta_K(\sigma)=\frac{2h_K\log(\varepsilon)}{|D_K|^{1/2}}$$

$\mathcal{O}_K^\times=\pm\varepsilon^{\mathbb Z}$, $\varepsilon>1$

Back to Ex 3. $V=K_{\mathbb R}=\mathbb C=X$, $L=\sigma(J)$, $\mathcal C=[J]^{-1}$

$f(z)=|z|^2/N(J)$, $\mu=2\mu_{\text{Lebesgue}}$ on $\mathbb C$

$\mu(V/L)=|D_K|^{1/2}N(J)$

$\mu(\{f\le 1\}\cap X)=\mu\{z\in\mathbb C\mid |z|^2\le N(J)\}=2\pi N(J)$

$\Rightarrow A=\dfrac{2\pi}{|D_K|^{1/2}}$ $\qquad Z(s)=w_K\,\zeta_{K,\mathcal C}(s)$

$$\Rightarrow \lim_{\sigma\to 1+}(\sigma-1)\zeta_{K,\mathcal C}(\sigma)=\frac{2\pi}{w_K|D_K|^{1/2}},\qquad \lim_{\sigma\to 1+}(\sigma-1)\zeta_K(\sigma)=\frac{2\pi h_K}{w_K|D_K|^{1/2}}$$

$$\left(w_K=\begin{cases} 6 & K=\mathbb Q(i\sqrt3)\\ 4 & K=\mathbb Q(i)\\ 2 & \text{otherwise}\end{cases}\right)$$

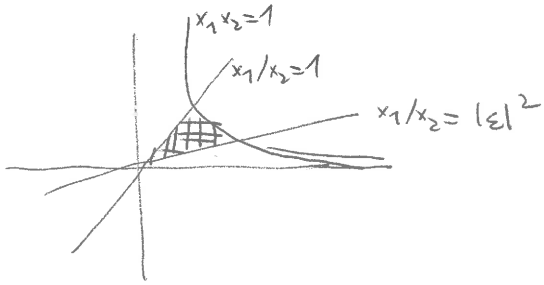
$\mathrm{Ker}(\ell') = \{\pm 1\}^{r_1} \times U(1)^{r_2}$ has measure $2^{r_1}(2\pi)^{r_2}$

<u>Goal</u>: compute $\underline{\mu(X \cap \{|N| \le 1\}) = ?}$

<u>Ex</u>: $K = \mathbb{Q}(\sqrt{d})$ (a) <u>$d<0$</u>: $2 \cdot \mu_{\text{Lebesgue}}\{z \in \mathbb{C} \mid |z|^2 \le 1\} = 2\pi$

(b) <u>$d>0$</u>:

$$4 \cdot \mu_{\text{Lebesgue}}\left\{(x_1,x_2) \in \mathbb{R}^2 \,\middle|\, \begin{array}{l} x_1,x_2>0,\ x_1x_2 \le 1 \\ 1 \le x_1/x_2 \le |\varepsilon|^2 \end{array}\right\} =$$



$= 4 \cdot \log|\varepsilon|$ $\qquad |\varepsilon|>1$

$(\mathcal{O}_K^\times = \pm\varepsilon^{\mathbb{Z}})$

<u>In general</u>: $x = (y,z) \in X \cap \{|N| \le \lambda\}$

$$\Downarrow$$

$$\ell'(x) = t\left(\tfrac{1}{n},\dots,\tfrac{1}{n},\tfrac{2}{n},\dots,\tfrac{2}{n}\right) + h, \qquad h \in F, \quad t \in \mathbb{R}_{\le \log(\lambda)}$$

$$\Rightarrow \mu(X \cap \{|N| \le \lambda\}) = 2^{r_1}(2\pi)^{r_2} \underbrace{\mu_H(F)}_{R_K} \cdot \underbrace{\int_{-\infty}^{\log(\lambda)} e^t\,dt}_{1} = 2^{r_1}(2\pi)^{r_2} R_K \cdot \lambda$$

$$\mu(K_{\mathbb{R}}/\sigma(J)) = |D_K|^{1/2}(\mathcal{O}_K : J) = |D_K|^{1/2} N(J)$$

$$\Rightarrow \boxed{\frac{\mu(X \cap \{|N| \le \lambda\})}{\mu(K_{\mathbb{R}}/\sigma(J))} = \frac{2^{r_1}(2\pi)^{r_2} R_K \cdot \lambda}{|D_K|^{1/2} N(J)}} \qquad (\lambda > 0)$$

For $\lambda = N(J)$,
$$\frac{\mu\left(X \cap \left\{\frac{|N|}{N(J)} \le 1\right\}\right)}{\mu(K_{\mathbb{R}}/\sigma(J))} = \frac{2^{r_1}(2\pi)^{r_2} R_K}{|D_K|^{1/2}}$$

Dirichlet's geometric thm for $V = K_{\mathbb{R}}$, $L = \sigma(J)$, X as above, $f(x) = |N_{K_{\mathbb{R}}/\mathbb{R}}(x)|/N(J)$: $Z(s) = w_K \zeta_{K,\mathfrak{C}}(s)$ $\qquad \mathfrak{C} = [J]^{-1}$

$$\Downarrow$$

$$\lim_{\sigma \to 1+} (\sigma - 1)\zeta_{K,\mathfrak{C}}(\sigma) = \frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K |D_K|^{1/2}}$$

$$\Downarrow$$

$$\lim_{\sigma \to 1+} (\sigma - 1)\zeta_K(\sigma) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K |D_K|^{1/2}}$$

Cyclotomic fields $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$ $\qquad \zeta_n = e^{2\pi i/n}$

Note: $2 \nmid m \Rightarrow \mu_{2m} = \pm \mu_m \Rightarrow \mathbb{Q}(\mu_{2m}) = \mathbb{Q}(\mu_m)$.
$(\Leftrightarrow$ for $n \equiv 2 [4]$, $\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{n/2}))$.

Facts: (1) $\forall n \geq 1$ the cyclotomic polynomial $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$

(if $n = p^r$, $r \geq 1$, p prime, then $\Phi_{p^r}(1+X) = \dfrac{(1+X)^{p^r}-1}{(1+X)^{p^{r-1}}-1}$ is p-Eisenstein)

$\Rightarrow \Phi_n(X)$ is the minimal polynomial of ζ_n over $\mathbb{Q} \Rightarrow [\mathbb{Q}(\mu_n):\mathbb{Q}] = \varphi(n)$.

(2) If $n = \prod_j p_j^{r_j}$, then $\mu_n = \mathbb{C}^\times[n] = \bigoplus_j \mathbb{C}^\times[p_j^{r_j}] = \bigoplus_j \mu_{p_j^{r_j}}$

$\Rightarrow \mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{p_1^{r_1}}, \dots, \mu_{p_k^{r_k}})$

(3) $p \nmid n \Rightarrow (X^n - 1, nX^{n-1}) = (1)$ in $\mathbb{F}_p[X]$ (since $n \in \mathbb{F}_p^\times$)

$\Rightarrow p \nmid \operatorname{disc}(X^n-1) \Rightarrow p \nmid \operatorname{disc}(\Phi_n) \Rightarrow p$ is unramified in $\mathbb{Q}(\mu_n)/\mathbb{Q}$

(4) p_j is totally ramified in $\mathbb{Q}(\mu_{p_j^{r_j}})/\mathbb{Q} \Rightarrow$ it is ramified in $\mathbb{Q}(\mu_n)/\mathbb{Q}$

(if $p_j^{r_j} > 2$ and $n = \prod_{j=1}^{k} p_j^{r_j}$)

(5) $\mathcal{O}_{\mathbb{Q}(\mu_n)} = \mathbb{Z}[\zeta_n]$ (true if $n = p^r$, by (1) and (3); in general one can write $\mathbb{Q} \subset \mathbb{Q}(\mu_{p_1^{r_1}}) \subset \mathbb{Q}(\mu_{p_1^{r_1}}, \mu_{p_2^{r_2}}) \subset \cdots \subset \mathbb{Q}(\mu_n)$ and use a relative version of this argument for each layer of this tower)

(6) If $p \nmid n$ and if $f = \min\{m \geq 1 \mid p^m \equiv 1 [n]\}$, then

$$p\,\mathcal{O}_{\mathbb{Q}(\mu_n)} = P_1 \cdots P_g, \qquad fg = \varphi(n), \qquad N(P_i) = p^f$$

($p \nmid \operatorname{disc}(X^n - 1) \Rightarrow \mu_n \subset \mathcal{O}_{\mathbb{Q}(\mu_n)}^\times \to \underbrace{(\mathcal{O}_{\mathbb{Q}(\mu_n)}/P_i)}_{k(P_i)}{}^\times$ is injective

$\Rightarrow n \mid \underbrace{|k(P_i)^\times|}_{N(P_i)-1 = p^{f_{P_i}}-1} \Rightarrow f \mid f_{P_i}$)

(7) If $p \nmid n$, then
$$\prod_{\substack{\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to U(1) \\ p \,(\mathrm{mod}\, n) \text{ has order} = f}} (1 - \chi(p)T) = \prod_{\zeta^f = 1} (1 - \zeta T)^{\varphi(n)/f} = (1 - T^f)^{\varphi(n)/f}$$

$$\Rightarrow \prod_\chi (1 - \chi(p)p^{-s})^{-1} = \prod_{P \mid p} (1 - N(P)^{-s})^{-1}$$

$$\Rightarrow \zeta_{\mathbb{Q}(\mu_n)}(s) = \Big(\prod_{\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to U(1)} L(\chi, s)\Big) \cdot \prod_{P \mid n} (1 - N(P)^{-s})^{-1}$$

Fact: $$\zeta_{\mathbb{Q}(\mu_n)}(s) = \prod_{\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to U(1)} L(\chi_{\mathrm{prim}}, s)$$

Properties of $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$ $\quad (\zeta_n = e^{2\pi i/n})$

1. If $n \equiv 2\,[4]$, then $\mu_n = \pm \mu_{n/2} \Rightarrow \mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{n/2})$
2. $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n)$ $\quad (\Leftrightarrow \Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$)
3. $\mathcal{O}_{\mathbb{Q}(\mu_n)} = \mathbb{Z}[\zeta_n]$
4. If $n = \prod_{p|n} p^{r_p}$, then $\mathbb{Q}(\mu_n) = \mathbb{Q}(\{\zeta_{p^{r_p}}\}_{p|n})$
5. p is totally ramified in $\mathbb{Q}(\mu_{p^r})/\mathbb{Q}$
6. If $n \not\equiv 2\,[4]$, then p is ramified in $\mathbb{Q}(\mu_n)/\mathbb{Q} \Leftrightarrow p|n$
7. $p \nmid n \Rightarrow$ $\quad p\mathcal{O}_{\mathbb{Q}(\mu_n)} = P_1 \cdots P_g$, $\quad N(P_j) = p^f$, $\quad fg = \varphi(n)$

   $f = \min\{d \geq 1 \mid p^d \equiv 1\,[n]\}$
8. $$\zeta_{\mathbb{Q}(\mu_n)}(s) = \prod_{\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to U(1)} L(\chi_{prim}, s) \qquad \left(= \prod_{\chi \in \widehat{G}} L(\chi_{prim}, s) \right)$$

Subfields of $\mathbb{Q}(\mu_n)$: $\quad G := Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$

$$\left(\begin{matrix} & g & \longleftrightarrow & a \pmod n \\ \forall \zeta \in \mu_n & g(\zeta) = \zeta^a & & \end{matrix} \right)$$

$$\begin{matrix} K = \mathbb{Q}(\mu_n)^H & & \\ \updownarrow & \updownarrow & \\ H & \{\text{subgroups } H \subset G\} \\ \| & & \\ Gal(\mathbb{Q}(\mu_n)/K) & & \end{matrix}$$

$$\zeta_K(s) = \prod_{\substack{\chi \in \widehat{G} \\ \chi(H) = 1}} L(\chi_{prim}, s)$$

$$= \prod_{\chi \in \widehat{Gal(K/\mathbb{Q})}} L(\chi_{prim}, s)$$

But $\chi \in \widehat{G}$, $\chi(H) = 1$

$\Updownarrow$

$\chi \in \widehat{G/H}$, and

$G/H = Gal(K/\mathbb{Q})$

<u>Note</u> : $$\zeta_{\mathbb{Q}(\mu_n)}(s) \overset{*}{=} \left(\prod_{\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to U(1)} L(\chi, s) \right) \prod_{P|n} (1 - N(P)^{-s})^{-1}$$ (easier version of (8))

together with $\lim_{\sigma \to 1^+} (\sigma - 1)\zeta_{\mathbb{Q}(\mu_n)}(\sigma) \in \mathbb{R} \setminus \{0\}$ (class number formula)

$\Downarrow$

$\forall \chi \neq \chi_0 \quad L(\chi, 1) \neq 0$

Dirichlet's class number formula

If $[K:\mathbb{Q}]=2$, $K=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{Z}\setminus\{0,1\}$ square-free,

$$D:=D_K=\begin{cases} d & d\equiv 1\,[4] \\ 4d & d\equiv 2,3\,[4] \end{cases} \qquad \zeta_K(s)=\zeta(s)\,L(\chi_D,s)$$

$$\Rightarrow \quad L(\chi_D,1)=\lim_{\sigma\to 1+}(\sigma-1)\zeta_K(\sigma)=\begin{cases} \dfrac{2\pi h_K}{w_K|D_K|^{1/2}} & D<0 \\[2ex] \dfrac{2h_K\log(\varepsilon_K)}{D_K^{1/2}} & D>0 \quad \left(\mathcal{O}_K^\times=\pm\varepsilon^{\mathbb{Z}},\ \varepsilon>1\right) \end{cases}$$

$(\Rightarrow \underline{\underline{L(\chi_D,1)\neq 0}})$

Cyclotomic fields

Let $K=\mathbb{Q}(\mu_n)$, $n>2$, $K^+:=\mathbb{R}\cap K=\mathbb{Q}(\zeta_n+\zeta_n^{-1})$

$$\underbrace{\mathbb{Q}\ \text{———}\ K^+\overset{H}{\text{———}}K}_{G}$$

$$G=\mathrm{Gal}(K/\mathbb{Q})\xrightarrow{\sim}(\mathbb{Z}/n\mathbb{Z})^\times$$
$$\cup \qquad\qquad\qquad \cup$$
$$H=\mathrm{Gal}(K/K^+)\xrightarrow{\sim}\{\pm 1\}$$

$$\zeta_K(s)=\prod_{\chi\in\widehat{(\mathbb{Z}/n\mathbb{Z})^\times}}L(\chi_{prim},s), \quad \zeta_{K^+}(s)=\prod_{\chi(-1)=1}L(\chi_{prim},s)$$

$$\zeta_K(s)/\zeta_{K^+}(s)=\prod_{\chi(-1)=-1}L(\chi_{prim},s)$$

Weaker statement: $$\zeta_K(s)=\left(\prod_{\chi:(\mathbb{Z}/n\mathbb{Z})^\times\to U(1)}L(\chi,s)\right)\prod_{P|n}(1-N(P)^{-s})^{-1}$$

$$\Rightarrow \underbrace{\lim_{\sigma\to 1+}(\sigma-1)\zeta_K(\sigma)}_{>0}=\left(\prod_{\chi\neq\chi_0}L(\chi,1)\right)\prod_{P|n}(1-N(P)^{-1})^{-1}$$

$$\Rightarrow \forall\chi\neq\chi_0 \qquad L(\chi,1)\neq 0.$$

Cyclotomic (p-)units

$\forall n\geq 1$ $$(X^n-1)/(X-1)=\prod_{0\neq a\in\mathbb{Z}/n\mathbb{Z}}(X-\zeta_n^a)\overset{X=1}{\Longrightarrow}\underbrace{\prod_{0\neq a\in\mathbb{Z}/n\mathbb{Z}}(1-\zeta_n^a)=n}$$

Möbius $$\Rightarrow \prod_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}(1-\zeta_n^a)=\begin{cases} p & n=p^r,\ p \text{ prime},\ r\geq 1 \\ 1 & \text{otherwise} \end{cases}$$

$\Rightarrow$ if $n\neq p^r$, then $\forall a\in(\mathbb{Z}/n\mathbb{Z})^\times$ $\quad 1-\zeta_n\in\mathbb{Z}[\zeta_n]^\times$

If $p\nmid ab$, then $1-\zeta_{p^r}^a\in\mathbb{Z}[\zeta_{p^r},\tfrac{1}{p}]^\times$, $\quad \dfrac{1-\zeta_{p^r}^a}{1-\zeta_{p^r}^b}\in\mathbb{Z}[\zeta_{p^r}]^\times$

$$\Rightarrow \boxed{(p)=(1-\zeta_{p^r})^{\varphi(p^r)}}$$

Quadratic Gauss sums and quadratic reciprocity law

Notation: $G(a,b) := \sum\limits_{x \in \mathbb{Z}/b\mathbb{Z}} \zeta_b^{ax^2} \qquad (a \in \mathbb{Z} \setminus \{0\},\ b \in \mathbb{N}_+,\ \zeta_b = e^{2\pi i/b})$

Properties: (1) $b = p \neq 2$ prime, $p \nmid a$:

$$G(a,p) = \sum_{x \in \mathbb{F}_p} \zeta_p^{ax^2} = \sum_{y \in \mathbb{F}_p} \left(1 + \left(\frac{ay}{p}\right)\right) \zeta_p^{ay} = \sum_{y \in \mathbb{F}_p} \left(\frac{y}{p}\right) \zeta_p^{ay} = \sum_{y \in \mathbb{F}_p^\times} \left(\frac{y}{p}\right) \zeta_p^{ay} = \left(\frac{a}{p}\right) \sum_{y \in \mathbb{F}_p^\times} \left(\frac{y}{p}\right) \zeta_p^{y}$$

$$= \left(\frac{a}{p}\right) G(1,p)$$

(2) $(b_1, b_2) = 1 \implies G(a, b_1 b_2) = G(ab_1, b_2)\, G(ab_2, b_1)$

Pf: chinese remainder thm: $\exists\, u_1, u_2 \in \mathbb{Z}$ $\quad 1 = u_2 b_1 + u_1 b_2 \Rightarrow \underline{(u_j, b_j) = 1}$

$$\mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/b_2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/b_1 b_2 \mathbb{Z}$$

$$(x_1, x_2) \longmapsto u_1 b_2 x_1 + u_2 b_1 x_2 = x$$

$x^2 \equiv (u_1 b_2 x_1)^2 + (u_2 b_1 x_2)^2\ [b_1 b_2]$ implies that

$$G(a, b_1 b_2) = \sum_{\substack{x_j \in \mathbb{Z}/b_j\mathbb{Z} \\ j = 1,2}} \zeta_{b_1 b_2}^{a((u_1 b_2 x_1)^2 + (u_2 b_1 x_2)^2)} = \left(\sum_{x_1 \in \mathbb{Z}/b_1\mathbb{Z}} \zeta_{b_1}^{a u_1^2 b_2 x_1^2}\right)\left(\sum_{x_2 \in \mathbb{Z}/b_2\mathbb{Z}} \zeta_{b_2}^{a u_2^2 b_1 x_2^2}\right)$$

$$= \underbrace{G(a u_1^2 b_2, b_1)}_{G(ab_2, b_1)}\ \underbrace{G(a u_2^2 b_1, b_2)}_{G(ab_1, b_2)}$$

Cor. $p \neq q$ primes $\neq 2 \implies \boxed{G(1, pq) = G(p,q)\,G(q,p) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) G(1,q)\,G(1,p)}$

$$\boxed{\text{Thm. } \forall b \geq 1 \qquad G(1,b) = \sum_{x \in \mathbb{Z}/b\mathbb{Z}} \zeta_b^{x^2} = b^{1/2}\, \frac{1 + i^{-b}}{1 + i^{-1}}}$$

Cor. $p \neq q$ primes $\neq 2 \implies \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \dfrac{G(1,pq)}{G(1,p)\,G(1,q)} = \dfrac{(1 + i^{-pq})(1 + i^{-1})}{(1 + i^{-p})(1 + i^{-q})} =$

$$= \begin{cases} -1 & p \equiv q \equiv -1\ [4] \\ 1 & \text{otherwise} \end{cases}$$

Pf of Thm (Dirichlet) (1) Assume that $F \in \mathcal{C}^1(\mathbb{R}, \mathbb{C})$. Restrict F to $[0,1]$ and make it periodic: let $f: \mathbb{R}/\mathbb{Z} \longrightarrow \mathbb{C}$

$$f(x) = \begin{cases} F(x), & x \notin \mathbb{Z} \\ \dfrac{F(0) + F(1)}{2}, & x \in \mathbb{Z} \end{cases} ; \text{ then}$$

$$f \in \mathcal{C}^1(\mathbb{R}/\mathbb{Z} \setminus \{0\}),\ \underbrace{\lim_{x \to 0+} f(x)}_{f(0+) = F(0)} \neq \underbrace{\lim_{x \to 1-} f(x)}_{f(1-) = F(1)},\ \lim_{x \to 0+} f'(x),\ \lim_{x \to 1-} f'(x) \text{ exist}$$

Dirichlet $\implies \forall x \in \mathbb{R}/\mathbb{Z}$

$$\lim_{n \to +\infty} \sum_{|m| \leq n} \left(\int_0^1 f(t)\, e^{2\pi i m t}\, dt\right) e^{-2\pi i m x} = \frac{f(x+) + f(x-)}{2}$$

$\overset{x=0}{\Longrightarrow} \quad \lim_{n\to+\infty} \sum_{|m|\le n} \left(\int_0^1 F(t) e^{2\pi i m t} dt \right) = \frac{F(0)+F(1)}{2}$

Apply this to $F(x+k)$ $(k\in\mathbb{Z})$: we obtain, for $M, N \in \mathbb{Z}$, $M<N$:

$$\underbrace{\sum_{k=M}^{N}{}' F(k)}_{\frac{1}{2}F(M)+F(M+1)+\cdots+F(N-1)+\frac{1}{2}F(N)} = \lim_{n\to+\infty} \sum_{|m|\le n} \int_M^N F(x) e^{2\pi i m x} dx$$

Our case: $\boxed{F(x) = e^{2\pi i x^2/b}}$

$$G(1,b) = \sum_{k=0}^{b}{}' F(k) = \lim_{n\to+\infty} \sum_{|m|\le n} \int_0^b e^{2\pi i x^2/b + 2\pi i m x} dx \overset{x=by}{=}$$

$$= b\cdot \lim_{n\to+\infty} \sum_{|m|\le n} \int_0^1 e^{2\pi i b \underbrace{(y^2+my)}_{(y+\frac{m}{2})^2-(\frac{m}{2})^2}} dy =$$

$$= b\cdot \lim_{n\to+\infty} \sum_{|m|\le n} \underbrace{e^{-\pi i b m^2/2}}_{\begin{cases} 1, & 2\mid m \\ i^{-b}, & 2\nmid m \end{cases}} \int_{\frac{m}{2}}^{\frac{m}{2}+1} e^{2\pi i b y^2} dy$$

$$= b(1+i^{-b}) \underbrace{\int_{\mathbb{R}} e^{2\pi i b y^2} dy}_{\lim_{T\to+\infty}\left(\int_{-T}^{T} e^{2\pi i b y^2} dy\right)} \overset{by^2=z^2}{=} b^{1/2}(1+i^{-b}) \underbrace{\int_{\mathbb{R}} e^{2\pi i z^2} dz}_{\substack{I \\ \text{(Fresnel's integral)}}}$$

For $b=1$: $1 = G(1,1) = (1+i^{-1})\, I \Longrightarrow G(1,b) = b^{1/2} \dfrac{1+i^{-b}}{1+i^{-1}}$.

Note: If $b\ge 1$ squarefree, $2\nmid b$ $\Rightarrow$ $b = \prod_{p\mid b} p$ distinct primes $p\ne 2$

$$\Rightarrow \quad G(1,b) = \prod_{p\mid b} \underbrace{G\left(\tfrac{b}{p}, p\right)}_{\left(\frac{b/p}{p}\right) G(1,p)}$$

Gauss sums attached to Dirichlet characters

Def. For $\chi : (\mathbb{Z}/M\mathbb{Z})^\times \longrightarrow U(1)$ and $b \in \mathbb{Z}$, let

$$G_a(\chi) := \sum_{x \in (\mathbb{Z}/M\mathbb{Z})^\times} \chi(x)\, \zeta_M^{ax} \quad , \quad G(\chi) := G_1(\chi)$$

Properties: (2) If $M = M_1 M_2$, $(M_1, M_2) = 1$, then $\chi = \chi_1 \chi_2$, $\chi_j : (\mathbb{Z}/M_j\mathbb{Z})^\times \to U(1)$ and

$$\underline{G_a(\chi) = \chi_1(M/M_1)\, \chi_2(M/M_2)\, G_a(\chi_1)\, G_a(\chi_2)}$$

Pf: $1 = u_2 M_1 + u_1 M_2$, $\quad \frac{1}{M} = \frac{u_1}{M_1} + \frac{u_2}{M_2}$, $\quad \zeta_M = \zeta_{M_1}^{u_1} \zeta_{M_2}^{u_2}$, $\quad u_j \frac{M}{M_j} \equiv 1\,[M_j]$

$$G_a(\chi) = \sum_{\substack{x_j \in (\mathbb{Z}/M_j\mathbb{Z})^\times \\ j=1,2}} \chi_1(x_1)\chi_2(x_2)\, \zeta_{M_1}^{a x_1 u_1} \zeta_{M_2}^{a x_2 u_2} = \underbrace{G_{au_1}(\chi_1)}_{\chi_1\left(\frac{M}{M_1}\right) G_a(\chi_1)} G_{au_2}(\chi_2)$$

$$\Downarrow$$

$$\chi_j(u_j)^{-1} = \chi_j\left(\frac{M}{M_j}\right)$$

---

(1) If $(u, M) = 1$, then $\underbrace{G_{au}(\chi)}_{} = \chi(u)^{-1} G_a(\chi) = \overline{\chi(u)}\, G_a(\chi)$

$$\sum_x \chi(x)\, \zeta_M^{aux} \underset{ux = y}{=} \sum_y \chi(u^{-1}y)\, \zeta_M^{ay} = \chi(u)^{-1} G_a(\chi)$$

---

(3) Cor: If $b \geq 1$ square-free, $2 \nmid b$, $b = \prod_{p \mid b} p$

$$\chi = \left(\frac{\cdot}{b}\right) = \prod_{p \mid b} \left(\frac{\cdot}{p}\right) : (\mathbb{Z}/b\mathbb{Z})^\times \longrightarrow \{\pm 1\} \qquad \text{Jacobi symbol}$$

$$\Longrightarrow G\left(\left(\frac{\cdot}{b}\right)\right) = \prod_{p \mid b} \underbrace{\left(\frac{b/p}{p}\right) G\left(\left(\frac{\cdot}{p}\right)\right)}_{QG(b/p,\, p)} = G(1, b)$$

~~(4) $\chi = \chi_{prim} \Longrightarrow |G(\chi)|^2 = M$ Pf: define $\chi(x) = 0$ if $(x, M) > 1$, then~~

~~Pf: $\overline{G(\chi)} = \sum_x \overline{\chi(x)}\, \zeta_M^{-x} = \chi(-1) \sum_x \overline{\chi(x)}\, \zeta_M^{x} = \chi(-1)\, G(\overline{\chi})$~~

~~Define $\chi(x) = 0$ if $(x, M) \neq 1$~~

~~$G(\chi)\overline{G(\chi)} = \sum_{x, y \in (\mathbb{Z}/M\mathbb{Z})^\times} \chi(xy^{-1})\, \zeta_M^{x-y} \underset{x = yz}{=} \sum_{y, z \in (\mathbb{Z}/M\mathbb{Z})^\times} \chi(z)\, \zeta_M^{y(z-1)}$~~

~~$= \sum_{z \in (\mathbb{Z}/M\mathbb{Z})^\times} \chi(z) \sum_{y \in (\mathbb{Z}/M\mathbb{Z})^\times} \left(\zeta_M^{z-1}\right)^y$~~

(4) $\chi = \chi_{prim}$ $\Longrightarrow$ ~~$\forall u \in \mathbb{Z}$~~ $G_{au}(\chi) = \overline{\chi(u)}\, G_a(\chi)$

~~Pf. ok if $(u, M) = 1$. Assume $d := (u, M) > 1$. Then~~ $\chi(u) = 0$

~~$\varphi(M)\, |G(\chi)|^2 = \sum_{y \in \mathbb{Z}/M\mathbb{Z}} |\chi(y)\, G(\chi)|^2 = \sum_{y \in \mathbb{Z}/M\mathbb{Z}}$~~

$\chi = \chi_{prim} \Longrightarrow \exists\, b \equiv 1\,[M/d]$, $(b, M) = 1$, $\chi(b) \neq 1 \Longrightarrow db \equiv d\,[M] \Longrightarrow ub \equiv u\,[M]$

Thm. Let $[K:\mathbb{Q}]=2$, $K=\mathbb{Q}(\sqrt{d})$, $D=D_K$. Then

$$W_D := \frac{G(\chi_D)}{|G(\chi_D)|} = \frac{G(\chi_D)}{|D|^{1/2}} \text{ is equal to } \begin{cases} 1 & D>0 \\ i & D<0. \end{cases}$$

Pf. (1) $D \in \{-4, \pm 8\}$: explicit calculation

(2) $D = D_q = q^*$, $q \neq 2$ prime: $\chi_D = \left(\frac{\cdot}{q}\right)$, $G(\chi_D) = G(1,q) = q^{1/2}\frac{1+i^{-q}}{1+i^{-1}}$

$$\Rightarrow W_D = \begin{cases} 1 & q \equiv 1[4] (\Leftrightarrow D>0) \\ i & q \equiv 3[4] (\Leftrightarrow D<0). \end{cases}$$

(3) $2 \nmid D$: $D \equiv 1[4]$, $D = \prod_{q|D} D_q$, $D_q = q^*$, $\chi_D = \prod_{q|D}\left(\frac{\cdot}{q}\right) = \left(\frac{\cdot}{|D|}\right)$

$|D| \equiv \mathrm{sgn}(D)\ [4]$

$$\Rightarrow G(\chi_D) = G(1,|D|) \Rightarrow W_D = \frac{1+i^{-|D|}}{1+i^{-1}} = \frac{1+i^{-\mathrm{sgn}(D)}}{1+i^{-1}} = \begin{cases} 1 & D>0 \\ i & D<0. \end{cases}$$

(4) $2 \mid D$: $D = D_2 D'$, $D' \equiv 1[4]$ as in (3), $D_2 \in \{-4, \pm 8\}$

$$W_D = \chi_{D_2}(D')\, \chi_{D'}(D_2)\, W_{D_2} W_{D'}$$

$D_2 = -4$: $W_D = 1 \cdot \mathrm{sgn}(D') \cdot i \cdot W_{D'} = \begin{cases} 1 & D'<0 \\ i & D'>0 \end{cases}$

$D_2 = 8$: $\chi_{D_2}(D') = \left.\begin{cases} 1 & D' \equiv 1[8] \\ -1 & D' \equiv 5[8] \end{cases}\right\} = \chi_{D'}(2) (= \chi_{D'}(D_2))$

$$\Rightarrow W_D = W_{D'}$$

$D_2 = -8$: $W_D = \underbrace{\chi_{D'}(2)\ \chi_{D'}(D_2)}_{\mathrm{sgn}(D')}\, i\, W_{D'} = \begin{cases} 1 & D'<0 \\ i & D'>0. \end{cases}$

---

(4) If $\chi = \chi_{prim}$, then $G_a(\chi) = \begin{cases} 0 & (a,M) \neq 1 \\ \overline{\chi(a)}\, G(\chi) & (a,M) = 1 \end{cases}$

and $|G(\chi)|^2 = M$.

Note: $\chi = \chi_D : (\mathbb{Z}/|D|\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ is primitive

$$\Rightarrow |D| = G(\chi)\underbrace{\overline{G(\chi)}}_{\chi(-1)\, G(\overline{\chi})} = \underbrace{\chi_D(-1)}_{\mathrm{sgn}(D)}\, G(\chi)^2 \Rightarrow \boxed{G(\chi_D)^2 = D}$$
