23/1/2023

References: Diamond-Shurman; Notes on the parity conjecture by Dokchitser

L-functions have all sorts of incarnations, we will focus on two of them:

for $f \in M_k(\Gamma_1(N))$, there is

$$L(f,s) = \sum_{n\geq 1} \frac{a_n}{n^s},$$

where

$$f = \sum_{n\geq 0} a_n q^n \quad \text{(remember that } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)\text{)}$$

for $E/\mathbb{Q}$ with conductor N, there is

$$L(E,s) = \prod_p F_p(p^{-s})^{-1},$$

where

$$\begin{cases} F_p(t) = \det(1 - t\,\mathrm{Frob}_p^{-1} \mid (V_\ell E)^{I_p}) \\ \text{we will see in more detail later} \end{cases}$$

The "modular functions" side of things is easier to study: one shows that it converges on $\mathrm{Re}\, s > k$ ($k > k_2 + 1$ if f is cuspidal), that it satisfies a functional equation (which allows an analytic continuation on the complex plane) (if f is nice), and that it admits an Euler product.

As for $L(E,s)$, it admits an Euler product by design, and we would like to show that it satisfies a functional equation. (still a conj. for E/K general n.f. K (Hasse-Weil conj.)) This can be achieved in a rather roundabout way, by showing that $\exists f \in S_2(\Gamma_0(N))$ ($N = N(E)$) such that $L(f,s) = L(E,s)$: this is one of the many equivalent formulations of modularity.

(think of it like this!) it basically boils down to

$a_p(f) = a_p(E)$ $(= p+1 - \#E(\mathbb{F}_p))$ for primes of good red.

& more complicated stuff for primes of bad red.

L-functions, modular side

In a way, L-functions are modelled after the Riemann zeta function $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$, and more generally $L(f,s)$ is an instance of a Dirichlet series, which associates to a succession $\{a_n\}$ a series $\sum_{n\geq 1} \frac{a_n}{n^s}$.

Prop: If $|a_n| \leq C \cdot n^k$ ($k \in \mathbb{R}$), then $\sum_{n\geq 1} \frac{a_n}{n^s}$ converges uniformly on compact subsets on $\{\mathrm{Re}\, s > k+1\}$ (using that $\sum_{n\geq 1} \frac{1}{n^\kappa}$ converges $\Leftrightarrow \kappa > 1$)

We know that ζ has the Euler product $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$, and also $\sum \frac{a_n}{n^s} = \prod_p \sum_{i=0}^{\infty} a_{p^i} p^{-is}$ for an mult. (i.e. $a_{mn} = a_m a_n$ for $(m,n) = 1$).

Remember that ζ satisfies a functional equation which is better stated using the ξ function: [redacted]

Def: $\Gamma(s) = \int_0^{+\infty} e^{-t} t^s \frac{dt}{t}$ is holomorphic for $\mathrm{Re}\, s > 0$. It is called the gamma function, (integration by parts) and satisfies $\Gamma(s+1) = s\Gamma(s)$, which lets us define Γ meromorphic, with poles for $s = -1, -2, \ldots$

$$\xi(s) = \zeta(s) \cdot \Gamma(s/2) \cdot \pi^{-s/2}$$

Then, ξ is meromorphic (no proof), with poles in $1, 0$ with residues $1, -1$, and satisfies $\xi(s) = \xi(1-s)$.

To prove that, one uses the Mellin transform. ($e^{i\kappa t} \mapsto \kappa^{-s}\Gamma(s)$, $\vartheta(t) - 1 \mapsto 2\xi(2s)$)

Def: For $f:\mathbb{R}_{>0}\to\mathbb{C}$, one defines its Mellin transform as

$$\hat{f}(s)=\int_0^\infty f(t)\,t^s\,\frac{dt}{t},$$

($t=e^{-u}$ shows that it's basically the Fourier transform of $f(e^{-u})$)

whenever the integral converges absolutely. (under the appropriate regularity hypotheses)

One can prove the following inversion formula:

$$f(t)=\int_{c-i\infty}^{c+i\infty}\hat{f}(s)\,t^{-s}\,ds$$

(doesn't depend on c)

Prop: Let $f\in M_k(\Gamma_1(N))$, [redacted] and [redacted] write it as $f=\sum_{n\geq 0}a_n q^n$.

Then, $|a_n|\leq C\cdot n^{k-1}$ and $L(f,s)$ converges absolutely for $\mathrm{Re}\,s>k$.

If moreover $f\in S_k(\Gamma_1(N))$ is a cusp form, then $|a_n|\leq C\cdot n^{k/2}$ and $L(f,s)$ converges absolutely for $\mathrm{Re}\,s>\frac{k}{2}+1$.

Proof: One can write $M_k(\Gamma_1(N))=S_k(\Gamma_1(N))\oplus E_k(\Gamma_1(N))$, so it's enough to prove the statement for cusp forms and for Eisenstein series.

For a cusp form $f(q)$, by Cauchy's formula we know that

$$a_n=\frac{1}{2\pi i}\int_{|q|=r}f(q)\,q^{-n}\,\frac{dq}{q}=\int_0^1 f(x+iy)\,e^{-2\pi in(x+iy)}\,dx.$$

($\Gamma_1(N)\backslash\mathbb{H}$, one can restrict to a fund. domain, and for $y\to+\infty$ it decreases exponentially)

Pick $y=1/n$, and [redacted] choose $C'>0$ s.t. $y^{k/2}|f(z)|\leq C'\ \forall z\in\mathbb{H}$. Finally,

$$|a_n| = \left|e^{2\pi}\int_0^1 f(x+iy)\,y^{k/2}\cdot y^{-k/2}\cdot e^{-2\pi inx}\,dx\right| \quad (y=1/n)$$
$$\leq e^{2\pi}\int_0^1 C'\cdot n^{k/2}\cdot|e^{-2\pi inx}|\,dx = e^{2\pi}\cdot C'\cdot\int_0^1 dx\cdot n^{k/2}$$

For an Eisenstein series, we would need to study them in more detail, which is outside of our scope. □ (basically, the Fourier coeff. is related to $\sigma_{k-1}(n)$, actually $\leq\sigma_{k-1}(n)$; but $n^{k-1}\sum_{n\mid n}\left(\frac{n}{n}\right)^{k-1}\leq n^{k-1}\sum_{d=1}^{n}\frac{1}{d^{k-1}}=\zeta(k-1)\,n^{k-1}$ ↻ this only works for $k\geq 3$)

Before proving the functional equation and the Euler product of $L(f,s)$, we need a detour:

Hecke operators, reprise

($\Delta=GL_2^+(\mathbb{Q})$)

Remember that we had defined $H(\Gamma,\Delta)=\mathbb{Z}[\Gamma\backslash\Delta/\Gamma]$, with product

$$(\Gamma\alpha\Gamma)*(\Gamma\beta\Gamma)=\sum_{i,j}\Gamma\alpha_i\beta_j\Gamma,$$

where $\Gamma\alpha\Gamma=\coprod\Gamma\alpha_i$, $\Gamma\beta\Gamma=\coprod\Gamma\beta_j$. This [redacted] ring acted on $\mathrm{Jac}(X(\Gamma))$ via the Hecke operators [redacted]. It also admits a natural action on $M_k(\Gamma)$, $S_k(\Gamma)$ given by $f|[\Gamma\alpha\Gamma]_k=\sum f|[\alpha_i]_k$ ($=(\det\alpha_i)^{k/2}\,j(\alpha_i,\tau)^{-k}f(\alpha_i(\tau))$). They are again called Hecke operators (or double coset operators).

[redacted]

When $\Gamma=\Gamma_0(N)$, we can in particular consider $[\Gamma\left(\begin{smallmatrix}0&-1\\N&0\end{smallmatrix}\right)\Gamma]_k$.

Def: The Fricke involution is the operator $w_N f = f[\Gamma\left(\begin{smallmatrix}0 & -1\\ N & 0\end{smallmatrix}\right)\Gamma]_k$.

By an abuse of notation we also write $w_N = \left(\begin{smallmatrix}0 & -1\\ N & 0\end{smallmatrix}\right)$. Note that w_N normalises $\Gamma_0(N)$

$\left(w_N\left(\begin{smallmatrix}a & b\\ Nc & d\end{smallmatrix}\right)w_N^{-1} = \left(\begin{smallmatrix}d & -c\\ Nb & a\end{smallmatrix}\right)\right)$ so $w_N f = f[w_N]_k = N^{k/2}\frac{1}{(Nz)^k} f(-\frac{1}{Nz})$

actually, like $(-1)^k$id

Also, $w_N^2 = (-N\ -N)$ acts trivially, so $w_N^2 = (-1)^k$id as an operator.

For the sake of clarity, let us fix the notation:

$\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \longmapsto d$

- $\langle d\rangle$: we have $1 \to \Gamma_1(N) \to \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times \to 1$, define $\langle d\rangle f$ to be $f[\Gamma_1(N)\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\Gamma_1(N)]_k$.
  It gives an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $M_k(\Gamma_1(N))$. They of course commute, and give the eigenspace decomposition
  $$M_k(\Gamma_1(N)) = \bigoplus_\chi M_k(\Gamma_1(N),\chi), \quad \text{where } M_k(\Gamma_1(N),\chi) = \{f \in M_k(\Gamma_1(N)) \mid \langle d\rangle f = \chi(d) f \ \forall d \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$
  χ let p be a prime,
- T_p: again $\Gamma = \Gamma_1(N)$, define $T_p f$ to be $f[\Gamma_1(N)\left(\begin{smallmatrix}1 & \\ & p\end{smallmatrix}\right)\Gamma_1(N)]_k$; $p^{k/2-1}$ (anamalisation)
  one computes the formula
  $$a_n(T_p f) = a_{np}(f) + 1_N(p)\, p^{k-1} a_{n/p}(\langle p\rangle f)$$
  $=0$ if $p \nmid n$; $1_N(p) = \begin{cases} 1 & p \nmid N \\ 0 & p \mid N \end{cases}$; (*) ; simpler when $f \in M_k(\Gamma_1(N),\chi)$
  in general: $a_n(T_n f) = \sum_{d(m,n)} d^{k-1} a_{mn/d^2}(f)\, 1_N(d)$
  (enough to show for $f \in M_k(\Gamma_1(N),\chi)$)
  One also finds that T_p, T_q commute for $p \neq q$, and also that $\langle d\rangle$ and T_p commute,
- $\langle n\rangle$: define $\langle n\rangle = 0$ whenever $(N,n) \neq 1$: the $\langle n\rangle$ are completely multiplicative
- T_n: define inductively $T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}$, and extend multiplicatively to define T_n
  This is made so that the "Euler product"
  $$\sum_{n=1}^\infty \frac{T_n}{n^s} = \prod_p \frac{1}{1 - T_p p^{-s} + \langle p\rangle p^{k-1-2s}}$$
  holds.

(Hecke)

Recall that an eigenform is a simultaneous eigenform for all T_n and $\langle n\rangle$. It is normalised when $a_1(f) = 1$.

Rmk: For $(N,n)=1$ the operators in $S_k(\Gamma_1(N))$ commute and are normal for a certain inner product, called the Petersson product. This means that $S_k(\Gamma_1(N))$ can be simultaneously diagonalised. Such an eigenform is then automatically an eigenform for the remaining T_n.

$\langle f,g\rangle_k = \int_{\Gamma\backslash\mathcal{H}} f\bar{g}\, y^k \frac{dx\,dy}{y^2} \Big/ \int_{\Gamma\backslash\mathcal{H}} y^k \frac{dx\,dy}{y^2}$

if it's new, $f \in (\ )^{new}$, $T_n f - a_n(f) f \in (\ )^{new}$ but its a_1 is 0 so $\langle T_n f - a_n(f) f, f\rangle = 0$ (see below)

(Main lemma)

Rmk: When $a_1(f) = 0$, then in some sense we can obtain f from smaller levels $M|N$: we call it an oldform. When f doesn't come from smaller levels, we call it a newform.

we haven't defined precisely what those mean! Basically, when $M \cdot d = N$, then $f \in S_k(\Gamma_1(M)) \subseteq S_k(\Gamma_1(N))$, and we can also do $f \cdot [d]_k$. The space they generate as $d|N$ varies is $(\ )^{old}$, and we set $(\ )^{new} = (\ )^{old\perp}$

Now fix $f \in S_k(\Gamma_1(N))$ a normalised eigenform. What does this entail?

- the condition on the $\langle d\rangle$ tells us that $f \in S_k(\Gamma_1(N),\chi)$, where $\chi(d)$ is the $\langle d\rangle$-eigenvalue
- the condition on the T_n tells us, by (*), that
  $$a_1(T_n f) = a_n(f),$$
  so the T_n-eigenvalue is $a_n(f)$. In particular, each eigenspace has dimension at most one!

Remember how the T_n were defined! For a normalised eigenform f, one must have

$$a_1(f)=1,$$
$$a_{mn}(f)=a_m(f)\cdot a_n(f) \quad \text{for } (m,n)=1,$$
$$a_{p^r}(f)=a_p(f)\,a_{p^{r-1}}(f)-\chi(p)p^{k-1}a_{p^{r-2}}(f).$$

Back to L-functions.

Prop: Let $f\in S_k(\Gamma_1(N),\chi)$ be a normalised eigenform. Then $L(f,s)$ has an Euler product (by construction of the T_n!)

$$L(f,s)=\prod_p \frac{1}{1-a_p p^{-s}+\chi(p)p^{k-1-2s}}$$

In a way, all of this is concocted so that the local factors in $L(f,s)$ and $L(E,s)$ correspond: one sees for example that $((V_\ell E)^\vee)^{I_p}$ is 2-dim $\Leftrightarrow p\nmid N$, in which case one has already shown that $\det(\mathrm{id}-t\,\mathrm{Frob}_p^{-1})=1-a_p t+pt^2$, so we would like to have $k=2$, $\chi=1_N$. (which is exactly like saying $f\in S_k(\Gamma_1(N),1_N)=S_k(\Gamma_0(N))$)

Let's now prove the functional equation that f satisfies. Let $f\in S_k(\Gamma_1(N))$ be a cusp form of weight k (we don't assume it to be an eigenform anymore). (we actually need k even)

We can compute its Mellin transform to be

$$\int_0^\infty f(it)t^s\frac{dt}{t}\overset{(1)}{=}(2\pi)^{-s}\Gamma(s)L(f,s)$$

(1): same reasoning as in $\mathcal{E}(-1)\to\mathcal{E}(2s)$

As we did with ξ, we consider $\Lambda(f,s)=N^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s)$, which will satisfy our functional equation.

Now, consider again w_N. It is an involution, so it decomposes ($(-1)^k=1$) and is self-adjoint for the Petersson product

$$S_k(\Gamma_1(N))=S_k(\Gamma_1(N))^+\oplus S_k(\Gamma_1(N))^-$$

Theorem: Suppose $f\in S_k(\Gamma_1(N))^\pm$. Then $\Lambda(f,s)$ satisfies

$$\Lambda(s)=\pm i^k\cdot\Lambda(k-s).$$

Consequently, $L(f,s)$ has an analytic continuation to the full complex plane

Proof: (dt/t is scaling invariant, we did a change of var.)

$$\Lambda(s)\overset{(1)}{=}N^{s/2}\int_0^\infty f(it)t^s\frac{dt}{t}=\int_0^\infty f\left(i\tfrac{t}{\sqrt{N}}\right)t^s\frac{dt}{t}=$$
$$=\int_1^\infty f\left(\tfrac{it}{\sqrt{N}}\right)t^s\frac{dt}{t}+\int_0^1 i^k(w_N f)\left(\tfrac{i}{\sqrt{N}t}\right)t^{s-k}\frac{dt}{t}\overset{\text{change of var.}}{=}\int_1^\infty\left(f\left(\tfrac{it}{\sqrt{N}}\right)t^s+i^k\underbrace{(w_N f)}_{=\pm f}\left(\tfrac{it}{\sqrt{N}}\right)t^{k-s}\right)\frac{dt}{t}=$$
$$=\int_1^\infty f\left(\tfrac{it}{\sqrt{N}}\right)\left(t^s\pm i^k t^{k-s}\right)\frac{dt}{t}=$$
$$\overset{i^{2k}=1}{=}\pm i^k\Lambda(k-s).$$

□

Now, if $f\in S_k(\Gamma_0(N))$ newform is given, then it is automatically an eigenform for w_N. (enough to consider these; $=\mathrm{id}$)

$[w_N,T_n]=0$ for $(n,N)=1$, use the mult. one theorem

L-functions, geometric side

In a way, the L function for f was a way to neatly package all of the a_p, for $p \nmid N$, in such a way as to have a Euler product. The information on the a_p for $p \mid N$ is messier, but in the case of a newform (this will be our case), we don't need to worry too much about it.

We want something similar for E, packaging all the information on the $a_p(E) = p+1-|\tilde{E}(\mathbb{F}_p)|$ when $p \nmid N$, and something messier for $p \mid N$, where $N = N(E)$ is the conductor of E.

Remember how we defined $\tilde{E}$ by $\tilde{F}(x,y)=0 \bmod p$, when p was a prime of good reduction. One can do this construction even when $\tilde{E}$ is not an elliptic curve, in which case there will be a singular point: we distinguish the case where it is a node, where we call p a prime of multiplicative reduction, and the case where it is a cusp, where we call p a prime of additive reduction.

Rem: p has mult. red. $\Leftrightarrow \tilde{E}^{sm} \simeq \mathbb{G}_m$ over $\bar{\mathbb{F}}_p$
p has add. red. $\Leftrightarrow \tilde{E}^{sm} \simeq \mathbb{G}_a$ over $\bar{\mathbb{F}}_p$

Moreover, if E has mult. red. over p, we call it split multiplicative reduction if $\tilde{E}^{sm} \simeq \mathbb{G}_m$ over $\mathbb{F}_p$, and nonsplit multiplicative reduction otherwise. As it happens, they are in any case isomorphic over $\mathbb{F}_{p^2}$.

Why does $L(E,s)$ involve such a complicated formula involving the Tate module? First of all,

Def: $E/\mathbb{Q}$ e.c., ℓ a prime. The ℓ-adic Tate module of E is given by

$$T_\ell E = \varprojlim E[\ell^n], \leftarrow \text{free } \mathbb{Z}_\ell\text{-mod of rank 2}$$

$$V_\ell E = T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

$T_\ell E$ has a natural structure of $\mathbb{Z}_\ell[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$-module, meaning that $V_\ell E$ is a representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, called the ℓ-adic representation associated to $E/\mathbb{Q}$.

Now if $p \neq \ell$, we can consider the absolute inertia group $I_p = \ker(D_p \to \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p))$, then a lifting of the Frobenius element of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ is unique up to conjugation by I_p, let Frob_p be a representative.

If p is a prime of good reduction, we find that $T_\ell\tilde{E} \hookrightarrow (T_\ell E)^{I_p}$ (reduced map; always true) must be an isomorphism, so the rank of $(T_\ell E)^{I_p}$ is 2 (I_p acts trivially), and Frob_p acts like in $T_\ell\tilde{E}$, with char. pol. $t^2 - a_p(E)t + p$. (ind. of ℓ!)

A converse holds as well, and much more:

Theorem (Néron-Ogg-Shafarevich criterion): $E/\mathbb{Q}$, $p \neq \ell$. Then

i) E has good red. at $p \iff T_\ell E$ unramified

ii) E has good or mult. red. at $p \iff \mathrm{rk}((T_\ell E)^{I_p}) \geq 1$.

At this point, the definition of $L(E,s)$ will make more sense.

Def: $E/\mathbb{Q}$ e.c. For each p prime, choose $\ell \neq p$, and define

$$F_p(t) = \det(\mathrm{id} - \mathrm{Frob}_p^{-1} t \mid (V_\ell E^\vee)^{I_p}),$$

$$L(E/\mathbb{Q}, s) = \prod_p F_p(p^{-s})^{-1}$$

It follows immediately from our previous criterion that $F_p(t)$ has degree $2 \iff E$ has good red at $p \iff p \nmid N$, in which case $F_p(p^{-s}) = 1 - a_p(E)p^{-s} + p^{1-2s}$. It follows that $L(E,s)$ looks like $\prod \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$ except for a finite number of exceptions, in which case $F_p(t)$ will have degree 1 or 0.

Fact: ① if E has split mult. red. at p (ord$_p$) then $F_p(t) = 1 - t$,
② if E has nonsplit mult. red. at p, then $F_p(t) = 1 + t$,
③ if E has add. red. at p, then $F_p(t) = 1$

One of the equivalent formulations of E being modular is that there is a newform $f \in S_2(\Gamma_0(N))$ such that $L(E,s) = L(f,s)$, which is equivalent to $a_p(f) = a_p(E)$ $\forall p$. (given $\varphi: X_0(N) \to E$ min par., then $f dz = \varphi^*(\omega)$) This in turn implies that E satisfies a functional equation

$$\Lambda(E,s) = -\varepsilon_f \Lambda(E, 2-s),$$

where we have called $w_N f = \varepsilon_f f$.

Fricke involution and Heegner points

Remember that $Y_0(N)$ parametrises pairs (E, C), $C \cong \mathbb{Z}/N\mathbb{Z}$. We defined $x_n \in Y_0(N)$ like this: (we start from $\mathcal{O} = \mathcal{O}_n$, n squarefree, $(N,n)=1$) choose $\mathfrak{n} = \mathfrak{n}_n$ s.t. $\mathcal{O}/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$, then $x_n = (\frac{\mathbb{C}}{\mathcal{O}}, \frac{\mathfrak{n}^{-1}}{\mathcal{O}})$. (remember that $Cl(\mathcal{O}) \cong \mathrm{Ell}(\mathcal{O})$, $\mathfrak{a} \mapsto \mathbb{C}/\mathfrak{a}$)

More generally, we can consider $(\frac{\mathbb{C}}{\mathfrak{a}}, \frac{\mathfrak{n}^{-1}}{\mathfrak{a}})$, which then depends on the choice of $\mathfrak{a} \in Cl(\mathcal{O})$, $\mathfrak{n} \mid N$. We use the notation $(\mathcal{O}, \mathfrak{n}, \mathfrak{a})$ to refer to this point. ($\forall p \mid N$ splits in $\mathcal{O}_K$)

By Heegner's condition, when $\mathcal{O} = \mathcal{O}_1 = \mathcal{O}_K$, then choosing $\mathfrak{n}_1$ amounts to

picking a prime $\not| p \ \forall \ p | N$.

Now, by the bijection $Y_0(N) = \mathcal{H}/\Gamma_0(N) \rightleftharpoons \{(E,C)\}/\sim$ we know that we can choose $\{\omega_1, \omega_2\} = \alpha$ oriented basis s.t. $\frac{\alpha n^{-1}}{\alpha} = \{\frac{\omega_2}{N}\}$, which means that $\{\omega_1, \frac{\omega_2}{N}\} = \alpha n^{-1}$.

We also know that $w_N \frac{\mathbb{C}}{\{\omega_1, \omega_2\}} = \frac{\mathbb{C}}{\{-\omega_2, N\omega_1\}}$, but now observe that $\frac{\mathbb{C}}{\{-\omega_2, N\omega_1\}} = \frac{\mathbb{C}}{\{N\omega_1, \omega_2\}}$, which is homothetical to $\frac{\mathbb{C}}{\{\omega_1, \frac{\omega_2}{N}\}} = \frac{\mathbb{C}}{\alpha n^{-1}}$.

Likewise one finds that $\frac{\mathbb{C}}{\{-\omega_2, \omega_1\}}$ is the same e.c. as $\frac{\mathbb{C}}{\alpha}$.

Putting everything together, we find that

$$w_N(\mathcal{O}, n, \alpha) = (\mathcal{O}, \bar{n}, \alpha n^{-1}),$$

indeed we've seen that $w_N \frac{\mathbb{C}}{\alpha} = \frac{\mathbb{C}}{\alpha n^{-1}}$, and the N-cyclic group is described by

$$\frac{\mathbb{C}/\alpha n^{-1}}{\mathbb{C}/\alpha} \cong \frac{\alpha}{\alpha n^{-1}} \cong \frac{\alpha n^{-1}(n^{-1})}{\alpha n^{-1}},$$

after observing that $n^{-1} = n^{-1}$ in $Cl(\mathcal{O})$.