DWORK'S p-ADIC PROOF OF RATIONALITY OF THE ζ-FUNCTION
NOTES FOR STAGE, FALL 2020

DANIEL KRIZ

Abstract. In 1959, ex-electrical engineer Bernard Dwork shocked the mathematical world by proving the first Weil conjecture on the rationality of the zeta function. Dwork's proof introduced striking new p-adic methods, and defied the expectation that the Weil conjectures could only be solved by developing a suitable Weil cohomology theory (later found to be ℓ-adic etale cohomology). In the first talk we will outline Dwork's proof and begin the initial part of the argument, introducing Dwork's general notion of "splitting functions", the Artin-Hasse exponential and Dwork's lemma.

In the second talk, we will go over the main steps of Dwork's argument in detail. First, we will construct a splitting function for the standard additive character and show it has good convergence properties using Dwork's lemma. Next we will establish the "analytic Lefschetz fixed point formula" by studying the trace of this splitting function acting on p-adic Banach spaces of power series. Finally, we will show this analytic fixed point formula implies the zeta-function is the ratio of two entire functions, and conclude with a general rationality criterion for p-adic power series that implies the zeta-function is rational.

1. Bernard Dwork

First, some brief background on Dwork, following the wonderful memorial article of Katz and Tate [4]. Bernard Dwork showed early talent for mathematics and began pursuing it in college, but was persuaded by his parents to pursue a more practical career, which turned out to be electrical engineering. Dwork served in the United States army during World War II, and was stationed in Korea after the war. According to one story, he accidentally caused a 24-hour blackout in Seoul in the late 40s by "getting his wires crossed".

In the late 40s, Dwork worked as an electrical engineer but started taking night classes on commutative algebra at NYU taught by Emil Artin (who apparently commuted from Princeton to NYC and back several evenings a week to give these classes). He soon became "hooked" and applied for the math Ph.D. program at NYU and Columbia. He was not admitted by NYU, but Columbia accepted him. He found out after he was admitted - and after quitting his day job as an electrical engineer - that Columbia's scholarship only covered tuition[1]. As he had a family by that point, Dwork taught night classes at Brooklyn Polytechnic to make ends meet. He did his thesis under Tate (an instructor at Princeton at that point, who was two years his junior). Dwork got his Ph.D. in 1954, and five years later proved the first Weil conjecture on rationality of the zeta function. Dwork would go on to make many fundamental contributions to p-adic analysis, p-adic geometry and p-adic differential equations, inspiring mathematicians like Katz (his student), Coleman, Koblitz (his grand-student), Robba (his unofficial student) and Ogus among others. It is my (and many others') personal belief that Dwork's striking and bold originality derived from his unique background and development as a mathematician.

[1] As Wei pointed out.

2. Outline of Dwork's proof of the first Weil conjecture

2.1. **The first Weil conjecture.** Throughout, we let $k = \mathbb{F}_q$, where $q = p^s$, and let $k_d = \mathbb{F}_{q^d}$. Let $N_d = \#X(k_d)$. Recall that the *ζ-function* of X/k is

$$\zeta(X/k, T) := \exp\left(\sum_{d=1}^{\infty} N_d T^d/d\right) \in 1 + T\mathbb{Q}[\![T]\!]. \tag{1}$$

One can actually show that

$$\zeta(X/k, T) \in \mathbb{Z}[\![T]\!] \tag{2}$$

as follows. Recall a *closed point* $\mathfrak{p}$ is a $\mathrm{Gal}(\bar{k}/k)$-orbit in $X(\bar{k})$. Let $\deg(\mathfrak{p})$ denote the order of this orbit, and let B_d denote the number of closed points of degree d. Then

$$N_d = \sum_{0<r|d} rB_r,$$

and so

$$\begin{aligned}\zeta(X/k, T) &= \exp\left(\sum_{d=1}^{\infty} N_d T^d/d\right) = \exp\left(\sum_{d=1}^{\infty}\left(\sum_{0<r|d} rB_r\right) T^d/d\right) = \exp\left(\sum_{r=1}^{\infty} B_r \sum_{m=1}^{\infty} (T^r)^m/m\right)\\ &= \exp\left(\sum_{r=1}^{\infty} B_r \log(1-T^r)^{-1}\right) = \prod_{r=1}^{\infty}(1-T^r)^{-B_r} = \prod_{\mathfrak{p}}(1-T^{\deg(\mathfrak{p})})^{-1},\end{aligned}$$

which clearly has integer coefficients.

Theorem 2.1 (Rationality of ζ-function)**.** *Suppose X/k is an algebraic variety. Then there exist polynomials $P(T), Q(T) \in \mathbb{Z}[T]$ such that*

$$\zeta(X/k, T) = \frac{P(T)}{Q(T)}$$

as power series in $\mathbb{Z}[\![T]\!]$. In particular,

$$\zeta(X/k, T) = \frac{\prod_i (1-\alpha_i T)}{\prod_j (1-\beta_j T)}$$

for some $\alpha_i, \beta_j \in \mathbb{C}$.

As an immediate corollary, we get that

$$N_d = \sum_j \beta_j^d - \sum_i \alpha_i^d$$

and so all the N_d are determined by the first finitely many N_d.

2.2. **Weil/Grothendieck's idea.** Of course, letting

$$F = \mathrm{Frob}_q : \bar{k} \to \bar{k}, \qquad x \mapsto x^q,$$

we have $N_d = \#X^{F^d}$. So as with Lefschetz's trace formula in topology, we should try to find some suitable (i.e. "Weil") cohomology theory $H^i(X/\bar{k})$ with an action by F on it, and express $\zeta(X/k, T)$ in terms of it. In particular we would expect

$$\text{"Lefschetz trace/fixed point formula"} \implies \text{rationality of } \zeta(X/k, T),$$

and the factors in the numerator/denominator given by $P_i := \det(1 - TF|_{H^i(X/\bar{k})})$, with fixed parity for i appearing in the numerator (resp. denominator):

$$\zeta(X/k, T) = \frac{\prod_{i \text{ odd}} P_i(T)}{\prod_{i \text{ even}} P_i(T)}. \tag{3}$$

This was the strategy proposed (in greater detail) by Weil and Grothendieck in the late 40s and early 50s. The theory of ℓ-adic étale cohomology ($\ell \neq p$) was developed in the early 60s by Grothendieck's school to play the role of $H^i(X/\bar{k})$.

This was also enough to prove (by 1964) the second and third Weil conjectures, on the functional equation of the ζ-function and the relation to Betti numbers, but was not enough to prove the remaining "Riemann hypothesis". Of course, as we have seen, Deligne's stunning proof of this last conjecture used ideas and methods well outside the scope of étale cohomology. It is an open question to this day whether a purely Grothendieckian proof of the Riemann hypothesis exists.

2.3. **Summary of Dwork's idea.** Dwork came at this problem from a completely different (p-adic) direction. If one were to summarize Dwork's argument, it would be that he comes up with a suitable "analytic trace" to replace the role of the algebraic trace from Grothendieck's idea. This analytic trace is the trace of a completely continuous "U-operator" acting on a p-adic Banach space of suitable power series. Dwork expresses N_d in terms of formulas involving additive characters of k; he "lifts to characteristic 0", finding nice p-adic power series expressions for these character formulas which live in this Banach space and which can be then studied using the analytic trace of the U-operator.

We note that Dwork's proof can be refined to give the more precise form of the ζ-function given by (3).

For the remainder of the section, we follow the very nice exposition of [4].

2.4. **Character formulas for N_d.** Dwork's first reduction is to reduce to the affine case, using the Principle of Inclusion-Exclusion and the definition (1). Another easy PIE argument reduces us to the hyperplane case, where X/k is given by one equation $f = 0$, $f \in k[X_1, \ldots, X_n]$. Considering hyperplane sections, one can also reduce to X/k given by $f = 0$ where $x_i \neq 0 \forall i$.

Now choose a nontrivial additive character

$$\psi : k \to K^\times,$$

where K is a (suitably large) characteristic 0 field (e.g. $K = \mathbb{C}$, but we will soon take a p-adic field). Additive means $\psi(x + y) = \psi(x)\psi(y)$. For example, for any $\zeta_p \in \mu_p$ we have the character

$$e : \mathbb{F}_p = \mathbb{Z}/p \to \mu_p, \qquad e(a) = \zeta_p^a,$$

and taking ζ_p primitive we can (and will) take

$$\psi = e \circ \mathrm{trace}_{k/\mathbb{F}_p}.$$

Let $\psi_d := \psi \circ \mathrm{trace}_{k_d/k} : k_d \to K^\times$, which is hence a nontrivial additive character valued in μ_p.

Then we have "orthogonality relations"

$$\sum_{y \in k_d} \psi_d(yf(x)) = \begin{cases} 0 & f(x) \neq 0 \\ q^d & f(x) = 0 \end{cases},$$

from which we get

$$\sum_{y \in k_d, x \in (k_d^\times)^n} \psi_d(yf(x)) = q^d N_d \implies \sum_{y \in k_d^\times, x \in (k_d^\times)^n} \psi_d(yf(x)) = q^d N_d - (q^d - 1)^n. \tag{4}$$

2.5. **"Splitting functions", i.e. p-adic analytic lifts of ψ_d.** We now let

$$W := W(\overline{\mathbb{F}}_p) = \breve{\mathbb{Z}}_p^{\mathrm{ur}}, \qquad K_0 = W[1/p] \qquad K = W[\mu_p][1/p].$$

The reason we take this K, is to contain the values of our ψ_d (note that $\psi_d = e \circ \mathrm{trace}_{k_d/\mathbb{F}_p}$ and so has values in μ_p). More importantly, we extend to a field containing K_0 in order to lift elements of $\overline{\mathbb{F}}_p$: Recall that by Hensel's lemma, any $a \in \mathbb{F}_{p^r}$ has a *unique* lift $\tilde{a} \in W$ that is a solution of $x^{p^r} - x$. In particular, if $a \neq 0$, $\tilde{a} \in \mu_{p^r-1}$. This gives us a multiplicative (and NOT additive) map $\overline{\mathbb{F}}_p \to W$, $a \mapsto \tilde{a}$, called the *Teichmüller lift*. For tuples $x = (x_1, \ldots, x_n) \in (\overline{\mathbb{F}}_p)^n$, we will let $\tilde{x} \in W^n$ denote the tuple obtained by applying the Teichmüller lift to each component.

Definition 2.2. A *splitting function* is an element $\theta(T) \in K[\![T]\!]$ which converges on

$$D_r := \{x \in \mathbb{C}_p : |T| < r\}$$

with $r > 1$, and which for all $d \geq 1$ satisfies

$$\psi_d(a) = \prod_{i=0}^{d-1} \theta(\tilde{a}^{q^i}). \tag{5}$$

In other words, $\theta(T)$ gives us a characteristic 0 lift of ψ_d that "splits" into nice factors.

Remark 2.3. The existence of such a $\theta(T)$ is highly non-trivial, and is one of the key steps in Dwork's argument.

Admitting the existence of θ, we can now rewrite (4) as follows. Recall $f = 0$ defines X/k. Let $X = (X_1, \ldots, X_n)$ (hopefully not to be confused with the variety X/k; we will always write "X/k" and not "X" for this variety). By convention, for $w \in (\mathbb{Z}_{\geq 0})^n$ we will write

$$X^w = X_1^{w_1} \cdots X_r^{w_r},$$

and for $a \in \mathbb{Z}_{\geq 0}$ we will let $aX = (aX_1, \ldots, aX_n)$ and $X^a = (X_1^a, \ldots, X_r^a)$. Write $f = f(X) = \sum_w a_w X^w$ where $w = (w_1, \ldots, w_n)$ ranges over $(\mathbb{Z}_{\geq 0})^n$ and let

$$\tilde{f}(X) := \sum_w A_w X^w \in W[X_1, \ldots, X_n], \qquad A_w := \tilde{a}_w.$$

Now let

$$F(Y, X) := \prod_w \theta(A_w Y X^w),$$

so that for any $(y, x) \in k^{n+1}$,

$$\psi(yf(x)) = \psi(y \sum_w a_w x^w) = \prod_w \psi(y a_w x^w) \overset{(5),\, d=1}{=} \prod_w \theta(\tilde{y} A_w \tilde{x}^w) =: F(\widetilde{(y,x)}).$$

Further let

$$F_d(y, X) = \prod_{i=0}^{d-1} F(Y^{q^i}, X^{q^i}),$$

so that for any $(y, x) \in k_d^{n+1}$,

$$\psi_d(yf(x)) = \psi_d(y \sum_w a_w x^w) = \prod_w \psi_d(y a_w x^w) \overset{(5)}{=} \prod_w \prod_{i=0}^{d-1} \theta(\tilde{y}^{q^i} a_w \tilde{x}^{q^i w}) = \prod_{i=0}^{d-1} F(\tilde{y}^{q^i}, \tilde{x}^{q^i}) = F_d(\widetilde{(y,x)}). \tag{6}$$

Now from (4), we have

$$\sum_{y \in k_d^\times, x \in (k_d^\times)^n} F_d(\widetilde{(y,x)}) = q^d N_d - (q^d - 1)^n. \tag{7}$$

2.6. **The U_q-operator and its trace.** We will eventually rewrite the LHS of (7) in terms of an analytic trace, more precisely the trace of a "U_q-operator" acting on a p-adic Banach space of power series. This p-adic Banach space will be (really, a subring of) $B := K[\![X_1, \dots, X_{n+1}]\!]$ (with its supremum norm). Now $w = (w_1, \dots, w_{n+1}) \in (\mathbb{Z}_{\geq 0})^{n+1}$, and $X^w = X_1^{w_1} \cdots X_{n+1}^{w_{n+1}}$.

Definition 2.4. Define an operator

$$U_q : B \to B, \qquad U_q\left(\sum_w B_w X^w\right) := \sum_w B_{qw} X^w.$$

Remark 2.5. I chose this notation to point out the analogy with Atkin's U-operator in the theory of (p-adic) modular forms as we saw in last semester's topic for STAGE, see [3].

Now fix $F = \sum_w C_w X^w$, and consider the linear operator given by multiplication

$$F : B \to B, \qquad F(G) = FG.$$

Pretend this makes sense (we actually need to be careful about p-adic convergence, i.e. to make this a "completely continuous operator", which entails requiring F to have good convergence properties, but we will worry about that later). By composition, we get an operator

$$U_q \circ F : B \to B.$$

This operator has a matrix, using the monomials X^w as a basis. So the entries are indexed by pairs $(v, w) \in (\mathbb{Z}_{\geq 0})^{2(n+1)}$, and we get a trace

$$\operatorname{trace}(U_q \circ F) = \operatorname{trace}\left(U_q \circ \sum_w C_w X^w\right) = \sum_w C_w \operatorname{trace}(U_q \circ X^w). \tag{8}$$

To further evaluate, we need to compute the diagonal entries of $U_q \circ X^w$ and sum them up. So consider a "basis element" X^v, and note that

$$(U_q \circ X^w)(X^v) = U_q(X^{w+v}) = \begin{cases} 0 & w \neq qv' - v \text{ for all } v' \in (\mathbb{Z}_{\geq 0})^{n+1} \\ X^{v'} & w = qv' - v \text{ for some } v' \in (\mathbb{Z}_{\geq 0})^{n+1} \end{cases}.$$

Hence, the (v, v) diagonal entry of $U_q \circ X^w$ is 1 if $w = (q-1)v$, and 0 otherwise. Hence from (8) we get

$$\operatorname{trace}(U_q \circ F) = \sum_w C_{(q-1)w}. \tag{9}$$

We can further massage this. Namely, note that, assuming rearranging sums works out (again we need to assume good convergence properties on F to make this rigorous)

$$(q-1)^{n+1} \operatorname{trace}(U_q \circ F) = \sum_w C_{(q-1)w} = \sum_{a \in (\mu_{q-1})^{n+1}} F(a) = \sum_{y \in k^\times, x \in (k^\times)^n} F(\widetilde{(y, x)}). \tag{10}$$

Here the first equality follows from the orthogonality relation

$$\sum_{a \in (\mu_{q-1})^{n+1}} a^v = \begin{cases} (q-1)^{n+1} & v = (q-1)w \text{ for some } w \in (\mathbb{Z}_{\geq 0})^{n+1} \\ 0 & \text{else} \end{cases},$$

and the last equality follows by uniqueness of the Teichmüller lift (which gives an explicit isomorphism $(k^\times)^{n+1} \cong \mu_{q-1}^{n+1}, a \mapsto \tilde{a}$).

In particular, the well-definedness of the steps of the previous paragraph depend on F having "good convergence properties", but it turns out that our previous choice

$$F(Y, X) = \prod_w \theta(A_w Y X^w)$$

has good convergence properties (coming from the condition that $\theta(T)$ converges on an open disc strictly containing the closed unit disc), and so the above arguments work. Now from (8), (10) and (7), we get

$$(q-1)^{n+1}\,\mathrm{trace}(U_q \circ F) = qN_1 - (q-1)^n.$$

Note that we didn't use any properties of q above other than it was a p-power, and so replacing "q" with "q^d", we get

$$(q^d-1)^{n+1}\,\mathrm{trace}(U_{q^d} \circ F_d) = q^d N_d - (q^d-1)^n.$$

It is easily checked that as linear operators $B \to B$,

$$(U_q \circ F)^d = U_{q^d} \circ F_d,$$

and so the above equation gives:

Corollary 2.6 ("Key Identities", or "The analytic Lefschetz fixed point formula")**.** *For all $d \geq 1$,*

$$(q^d-1)^{n+1}\,\mathrm{trace}((U_q \circ F)^d) = q^d N_d - (q^d-1)^n. \tag{11}$$

2.7. **An identity involving $\zeta(X/k,T)$.** It may seem like we have lost the plot, but now we will finally start to see $\zeta(X/k,T)$. Because F has good convergence properties, $U_q \circ F$ is a completely continuous endomorphism of a p-adic Banach space, and hence its Fredholm characteristic series

$$\Delta(T) := \det(1 - TU_q \circ F)$$

is a p-adic entire function of T, and is also given by[2]

$$\Delta(T) = \exp\left(-\sum_{d=1}^{\infty} \mathrm{trace}((U_q \circ F)^d)T^d/d\right).$$

This is starting to look familiar. Piugging the key identities (11) into $\Delta(T)$, we get an identity (exercise!)

$$\prod_{i=0}^{n+1} \Delta(q^i T)^{(-1)^{n-i}\binom{n+1}{i}} = \zeta(X/k,qT) \prod_{i=0}^{n} (1-q^iT)^{(-1)^{n-i}\binom{n}{i}}. \tag{12}$$

We thus see that $\zeta(X/k,T)$ is a ratio of two p-adically entire functions. But we're still not done.

2.8. **Rationality of $\zeta(X/k,T)$.** The final step involves gathering the following properties of $\zeta(X/k,T)$:

(1) $\zeta(X/k,T) \in \mathbb{Z}[\![T]\!]$ (from (2)),
(2) $\zeta(X/k,T)$ has a nonzero *archimedean* radius of convergence (using (1) and the trivial bound $N_d \leq (\#k_d^\times)^n = (q^d-1)^n$),
(3) $\zeta(X/k,T)$ is the ratio of two p-adic entire functions (from (12)).

Now generalizing a theorem of Borel, Dwork shows that these properties imply the rationality of $\zeta(X/k,T)$ (Theorem 2.1).

Remark 2.7. As Bjorn pointed out, the easier statement that a p-adically *entire* function $A(T) = \sum a_n T^n$ that also lies in $\mathbb{Z}[T]$ and has nonzero archimedean radius of convergence is clearly proven using the idèlic product formula $\prod_{p,\infty} |x|_p = 1$: Since $A(T)$ converges for $|T|_\infty = R > 0$, we have that $a_n R^n \to 0$ as $n \to \infty$, and hence $|a_n|_\infty < 1/R^n$ for all $n \gg 0$. Because $A(T)$ p-adically converges on $|T| = 1/R$, we have $a_n(1/R)^N \to 0$ as $n \to \infty$ and hence $|a_n| < 1/R^n$ for

[2]As Bjorn pointed out, this can be proven by reducing to the finite-dimensional case as follows. Since F has "good convergence properties", this means that its coefficients p-adically go to zero, and moreover our choice of F has p-adically integral coefficients (otherwise, simply renormalize F to have integral coefficients). Hence F is a polynomial modulo p^n for every $n \geq 0$, and we can prove the identity in $(\mathcal{O}_K/p^n)[\![T]\!]$ for every n using finite-dimensional linear algebra, which by p-adic completeness implies the identity in $\mathcal{O}_K[\![T]\!]$.

all $n \gg 0$. Now by the idèlic product formula, for all $n \gg 0$ either $a_n = 0$ or, since $a_n \in \mathbb{Z}$, $1 = \prod_{\ell \leq \infty} |a_n|_\ell \leq |a_n||a_n|_\infty < (1/R)^n R^n = 1$, a contradiction. Hence $a_n = 0$ for all $n \gg 0$. The theorem of Borel can be proven using a strengthening of this method, replacing the estimates on the coefficients a_n with the determinants $N_{s,m}$ considered in Lemma 3.12 below.

Remark 2.8. As Wei pointed out, the above theorem of Borel can be strengthened by weakening the hypotheses on radii of convergence as follows. Suppose $\zeta(X/k, T) = A(T)/B(T)$. For a rational prime $\ell \leq \infty$, let $0 \leq R_\ell \leq \infty$ denote the minimum of the ℓ-adic radii of convergence of $A(T), B(T) \in \mathbb{Z}[\![T]\!]$. Then Borel's theorem requires $R_p = \infty$ and $R_\infty > 0$, but the same argument of Section 3.5 works if we instead assume

$$\prod_{\ell \leq \infty} R_\ell > 1.$$

Wei also points out that Bost used a similar lemma in his work on the p-curvature conjecture [1] in order to show that certain solutions of p-adic differential equations (coming from p-curvature) are rational functions. In loc. cit., Bost shows that $R_\infty = \infty$ and thus the above inequality is *a fortiori* satisfied. It seems that in most practical applications of Borel's rationality lemma (or the argument of Section 3.5), one first shows that $R_\ell = \infty$ for some $\ell \leq \infty$ for the power series in consideration.

3. Dwork's Proof in Detail

Since this is STAGE, we need to be more precise and go over the steps in detail. In this section, we follow Koblitz's book [5, p. 92-95, Chapter V.2].

3.1. **Constructing splitting functions.** Let $\psi : k \to K^\times$ and $\psi_d : k_d \to K^\times$ be the previously fixed additive characters, where $K = W(\overline{\mathbb{F}}_p)[1/p, \mu_p]$. Recall that $\zeta_p \in \mu_p$ was a fixed primitive p^{th} root of unity. Let $\lambda = \zeta_p - 1$. Then $\mathrm{ord}_p(\lambda) = \frac{1}{p-1}$. Recall that $k = \mathbb{F}_q = \mathbb{F}_{p^s}$, $k_d = \mathbb{F}_{q^d} = \mathbb{F}_{p^{sd}}$. We now write

$$\psi_d(a) = (1+\lambda)^{\tilde{a} + \tilde{a}^p + \ldots + \tilde{a}^{p^{sd-1}}}.$$

We want to find a splitting function of ψ_d, i.e. a power series $\Theta(T), \theta(T) \in K[\![T]\!]$ with good convergence properties such that

$$\psi_d(a) = \prod_{i=0}^{sd-1} \Theta(\tilde{a}^{p^i}) = \prod_{i=0}^{d-1} \theta(\tilde{a}^{q^i}),$$

so why not try

$$\Theta(T) = (1+\lambda)^T := \sum_{i=0}^{\infty} \binom{T}{i} \lambda^i ?$$

The problem is that $\tilde{a} \notin \mathbb{Z}_p$, and so the $\binom{\tilde{a}}{i}$ have p-denominators and the above expression does not converge at $T = \tilde{a}$. So we need to be more clever and pull something out of a hat.

Definition 3.1. Let

$$F(X,Y) = (1+Y)^X (1+Y^p)^{\frac{X^p - X}{p}} (1+Y^{p^2})^{\frac{X^{p^2} - X^p}{p^2}} \cdots (1+Y^{p^n})^{\frac{X^{p^n} - X^{p^{n-1}}}{p^n}} \cdots \in 1 + (X,Y)\mathbb{Q}_p[\![X,Y]\!]$$

where we use interpret each factor as representing the expansion obtained by formally applying the binomial theorem, and where the inclusion follows expanding the above product out, there are only finitely many "$X^m Y^n$ terms" for each pair (m,n).

The goal of this subsection is to show that, in fact

$$F(X,Y) \in 1 + (X,Y)\mathbb{Z}_p[\![X,Y]\!]$$

(which should be surprising). To do this, we need a general and very useful lemma due to Dwork and commonly referred to as "Dwork's lemma" (though he attributes an earlier form of it to Dieudonné, see [2, Lemma 1]). We formulate in slightly greater generality, but the argument is still the same (and there might be further generalizations).

Lemma 3.2 (Dwork's lemma)**.** *Let R be an integral domain that is a $\mathbb{Z}_p$-algebra, and let $\phi : R \to R$ be a "mod p lift of p-power Frobenius", that is a ring endomorphism such that*

$$\phi \otimes 1 : R \otimes_{\mathbb{Z}_p} \mathbb{Z}/p \to R \otimes_{\mathbb{Z}_p} \mathbb{Z}/p$$

is $x \mapsto x^p$. Let $R_0 = R[1/p]$ so that ϕ extends to $R_0 \to R_0$ by $\mathbb{Z}_p$-linearity, and given $G(T) = \sum_n a_n T^n \in R_0[\![T]\!]$, we let $G^\phi = \sum_n \phi(a_n)T^n$. Then if

$$F(T) \in 1 + TR_0[\![T]\!],$$

we have the following criterion for integrality:

$$F(T) \in 1 + TR[\![T]\!] \iff \frac{F^\phi(T^p)}{F(T)^p} \in 1 + pTR[\![T]\!].$$

In other words, the series F is integral if and only if it "commutes with the p-power map modulo p". In our applications, we will consider the cases $R = \mathbb{Z}_p$ and $R = \mathbb{Z}_p[\![X]\!]$.

Proof of Lemma 3.2. . The " $\Longrightarrow$ " direction follows simply because if $F(T) \in R[\![T]\!]$, then

$$F^\phi(T^p) \equiv F(T)^p \pmod{p}.$$

The " $\Longleftarrow$ " direction is trickier. Write $F(T) = \sum_{n=0}^\infty a_n T^n$. Then we have by assumption

$$\sum_{n=0}^\infty \phi(a_n)T^{pn} = \left(\sum_{n=0}^\infty a_n T^n\right)^p \left(1 + pT\sum_{n=0}^\infty b_n T^n\right)$$

where $b_n \in R$. We now proceed by induction on n to show $a_n \in R$. Since $a_0 = 1$, we have the base case. Now assume that $a_i \in R$ for $0 \le i < n$. Then reducing the above equality modulo (p, T^{n+1}), we get

$$\sum_{i=0}^{n-1} \phi(a_i)T^{pi} \equiv \left(\sum_{i=0}^{n} a_i T^i\right)^p \pmod{pR[\![T]\!] + T^{n+1}R_0[\![T]\!]}.$$

By induction hypothesis, the RHS is congruent to

$$\sum_{i=0}^{n-1} a_i^p T^{pi} + pa_n T^n \equiv \sum_{i=0}^{n-1} \phi(a_i)T^{pi} + pa_n T^n \pmod{pR[\![T]\!] + T^{n+1}R_0[\![T]\!]},$$

and hence clearing both sides we get

$$pa_n \equiv 0 \pmod{pR},$$

which implies $a_n \in R$. We have finished the induction. □

Now we start applying Dwork's lemma to our power series. We start with a warm-up.

Remark 3.3 (Warm-up application of Dwork's lemma)**.** Even though the assigned reading covers the Artin-Hasse exponential, and the abstract mentions it, we will not need the Artin-Hasse exponential explicitly in our discussion. We mention it here briefly anyways. Recall the exponential is defined as a power series

$$\exp(X) = 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \dots.$$

This has infinite archimedean radius of convergence (and so is an entire function on $\mathbb{C}$), but only converges p-adically on $|X| < p^{-1/(p-1)}$ due to the p-divisibilities appearing in $n!$. For certain purposes, it is useful to have a notion of exponential that has a larger raius of convergence (e.g. $|X| < 1$). The *Artin-Hasse exponential* is defined as the series

$$E_p(X) = \exp\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \dots\right) \in 1 + X\mathbb{Q}[\![X]\!].$$

In fact one has

$$E_p(X) \in 1 + X\mathbb{Z}_p[\![X]\!]$$

For this, note that

$$\frac{E_p(X^p)}{E_p(X)^p} = \exp\left(\left(X^p + \frac{X^{p^2}}{p} + \frac{X^{p^3}}{p^2} + \dots\right) - p\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \dots\right)\right) = \exp(-pX) \in 1 + p\mathbb{Z}_p[\![X]\!],$$

and so the " $\Longleftarrow$ " direction of Dwork's lemma with $R = \mathbb{Z}_p$, $\phi = \mathrm{id}$ implies the desired integrality. As a consequence, the radius of convergence of $E_p(X)$ is at least $|X| < 1$ (and this can be shown to be the exact radius of convergence).

Now we state our main application of Dwork's lemma.

Corollary 3.4. *We have*

$$F(X, Y) \in 1 + (X, Y)\mathbb{Z}_p[\![X, Y]\!].$$

Proof. First, note that $1 + Y \in 1 + Y\mathbb{Z}_p[\![Y]\!]$. Applying the " $\Longrightarrow$ " direction of Lemma 3.2 with $R = \mathbb{Z}_p$ and $\phi = \mathrm{id}$, we see that

$$\frac{1 + Y^p}{(1 + Y)^p} = 1 + pYG(Y), \qquad G(Y) \in \mathbb{Z}_p[\![Y]\!].$$

Hence

$$\frac{F(X^p, Y^p)}{F(X, Y)^p} = \frac{(1 + Y^p)^X}{(1 + Y)^{pX}} = \left(\frac{1 + Y^p}{(1 + Y)^p}\right)^X = (1 + pYG(Y))^X = \sum_{n=0}^{\infty} \binom{X}{n} p^n (YG(Y))^n \in 1 + p(X, Y)\mathbb{Z}_p[\![X, Y]\!],$$

where

$$\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!} \in \frac{1}{n!}\mathbb{Z}[X],$$

and the inclusion of the previous identity follows because $\binom{X}{n} p^n \in \mathbb{Z}_p[X]$. Hence, applying the " $\Longleftarrow$ " direction of Lemma 3.2 with $R = \mathbb{Z}_p[\![X]\!]$, $\phi(f(X)) = f(X^p)$, we see that $F(X, Y) \in 1 + (X, Y)\mathbb{Z}_p[\![X, Y]\!]$ as claimed. □

Using Corollary 3.4, write

$$F(X, Y) = \sum_{n=0}^{\infty} \left(X^n \sum_{m=n}^{\infty} a_{m,n} Y^m\right), \qquad a_{m,n} \in \mathbb{Z}_p.$$

Now we can finally define our splitting function.

Definition 3.5 (Definition of our splitting function)**.** Let $\lambda = \zeta_p - 1$ as above, and recall $k = \mathbb{F}_{p^s}$. Let

$$\Theta(T) := F(T, \lambda) = \sum_{n=0}^{\infty} a_n T^n, \qquad \theta(T) := \prod_{i=0}^{s-1} \Theta(T^{p^i})$$

where $a_n = \sum_{m=n}^{\infty} a_{m,n} \lambda^m$. Then $\mathrm{ord}_p(a_n) \geq n/(p-1)$ since $\lambda^n | a_n$. By completeness of $\mathbb{Q}_p(\zeta_p)$ (it is a finite extension of $\mathbb{Q}_p$) we have $a_n \in \mathbb{Q}_p(\zeta_p)$, and so

$$\Theta(T), \theta(T) \in \mathbb{Z}_p[\zeta_p][\![T]\!] \subset \mathcal{O}_K[\![T]\!].$$

Since $\mathrm{ord}_p(a_n) \geq n/(p-1)$, $\Theta(T)$ converges for $|T| < p^{1/(p-1)}$, and $p^{1/(p-1)} > 1$, and the same with $\theta(T)$.

We just need to check the final "splitting property" for θ with respect to ψ_d. Given $a \in k_d$, let $t = \tilde{a}$, so that $|t| < p^{1/(p-1)}$ and $\Theta(t)$ converges. In particular, $t^{p^{sd}} = t$. We have

$$(1+Y)^{t+t^p+\ldots+t^{p^{sd-1}}} = F(t, Y) F(t^p, Y) \cdots F(t^{p^{sd-1}}, Y).$$

To see this, expand the RHS out to get

$$(1+Y)^{t+t^p+\ldots+t^{p^{sd-1}}} (1+Y^p)^{(t^{p^{sd}}-t)/p} (1+Y^{p^2})^{(t^{p^{sd+1}}-t^p)/p^2} (1+Y^{p^2})^{(t^{p^{sd+2}}-t^{p^2})/p^3} \cdots,$$

and since $t^{p^{sd}} = t$ we get the desired identity. In all, for all $d \geq 1$, recalling that $q = p^s$,

$$\psi_d(a) = \prod_{i=0}^{sd-1} \Theta(\tilde{a}^{p^i}) = \prod_{i=0}^{d-1} \theta(\tilde{a}^{q^i}),$$

and hence $\theta(T)$ is a splitting function.

3.2. **Traces of operators on p-adic Banach spaces of power series.** We now carry out the "analytic trace" part of Dwork's proof. For most of this section, K can be any complete subfield of $\mathbb{C}_p$, but later we will take $K = W[\mu_p][1/p]$ in order to work with our $\theta(T)$.

Let $B = K[\![X_1, \ldots, X_n]\!]$. Then B is an infinite-dimensional vector space with basis given by monomials X^w with $w = (w_1, \ldots, w_n)$ (recall that $X^w := X_1^{w_1} \cdots X_n^{w_n}$). Let $U_q : B \to B$ be defined as earlier

$$U_q(\sum_w B_w X^w) = \sum_w B_{qw} X^w.$$

Now fix $F = \sum_w C_w X^w$, and consider the linear operator $F : B \to B$ given by multiplication $G \mapsto FG$. Then we get a composition

$$\Psi_{q,F} := U_q \circ F : B \to B.$$

We want to consider the trace of $U_q \circ F$, i.e. the "sum of the diagonal terms of the (infinite) matrix of $U_q \circ F$", but the obvious definition does not converge unless we restrict to some subring of element with "good convergence properties"; this is our p-adic Banach space. Define a height function $|\cdot| : \mathbb{Z}_{\geq 0}^n \to \mathbb{Z}_{\geq 0}$ by $|(w_1, \ldots, w_n)| = \sum_{i=1}^n w_i$.

Definition 3.6. Define the set of *overconvergent power series*

$$B_0 := \left\{ G = \sum_w g_w X^w \in R : \exists M > 0, \mathrm{ord}_p(g_w) \geq M|w| \ \forall w \in \mathbb{Z}_{\geq 0}^n \right\}. \tag{13}$$

One can check that B_0 is closed under multiplication.

Remark 3.7. As Bjorn pointed out, the terminology "overconvergent" comes from the fact that the power series in B_0 converge on some polydisc of radius strictly greater than 1, which is easily checked from the definition.

Now write the matrix $A = (a_{v,w})$ of $\Psi_{q,F} : B \to B$. For $F \in B_0$, we have a successful definition of $\mathrm{trace}(\Psi_{q,F}) : B \to K$ and its iterates as

$$\mathrm{trace}(\Psi_{q,F}) := \sum_w a_{ww} \in K.$$

Proposition 3.8. *Let $F \in B_0$. The above definition of $\mathrm{trace}(\Psi^s_{q,F})$ converges for $s \in \mathbb{Z}_{\geq 1}$, and*

$$(q^s - 1)^n \,\mathrm{trace}(\Psi^s_{q,F}) = \sum_{x \in (\mu_{q^s-1})^n} F(x)F(x^q)\cdots F(x^{q^{s-1}}).$$

Proof. For $s = 1$, we have by (9) that

$$\mathrm{trace}(\Psi_{q,F}) = \sum_w C_{(q-1)w}$$

which converges since $F \in B_0$. Now the identity follows from (10). For larger s, we note that as linear operators,

$$\Psi^s_{q,F} = \Psi_{q^s,F_s}$$

where

$$F_s(x) = \prod_{i=0}^{s-1} F(x^{q^i})$$

(this is the same definition as in (6)). Now the identity follows from the argument of the $s = 1$ case by replacing F with F_s and q with q^s.

See [5, Chapter V.3, Lemma 3] for a slightly different argument. □

Now let $A = (a_{vw})_{v,w \in \mathbb{Z}^n_{\geq 0}}$ denote the matrix of $\Psi_{q,F}$.

Proposition 3.9. *Let $F \in B_0$. The Fredholm characteristic series*

$$\Delta(T) := \det(1 - TA) \in K[\![T]\!]$$

is well-defined and has an infinite radius of convergence (i.e. is "entire").

Proof. Again a computation, see [5, Chapter V.3, pp. 120-121] for details. □

Finally, we end with an important identity which will be used later to relate the Fredholm characteristic series to $\zeta(X/k, T)$.

Proposition 3.10. *Let $F \in B_0$. Then we have*

$$\Delta(T) = \exp\left(-\sum_{d=1}^{\infty} \mathrm{trace}(A^d)T^d/d\right).$$

Proof. This is again a "suped up" version of the argument for finite matrices, see [5, Chapter V.3, pp. 121-122] for details. We recall the argument when A is a finite matrix. Recall that trace is known to be conjugate-invariant. Base-changing from K to $\mathbb{C}_p$ (which is algebraically closed), we may find a change of basis to make A upper-triangular (e.g. using Jordan normal form). So without loss of generality, suppose A is upper-triangular. Then the characteristic series is a finite product

$$\det(1 - TA) = \prod(1 - a_{ii}T)$$

and $\mathrm{trace}(A^d) = \sum a^d_{ii}$. Hence

$$\exp\left(-\sum_{d=1}^{\infty}\sum a^d_{ii}T^d/d\right) = \prod \exp\left(-\sum_{d=1}^{\infty}(a_{ii}T)^d/d\right) = \prod \exp\left(\log(1 - a_{ii}T)\right) = \prod(1 - a_{ii}T),$$

which gives the identity. □

3.3. **The ζ-function is meromorphic.** Recall that by our previous reductions, we may assume without loss of generality that X/k is given by

$$f(X_1, \ldots, X_n) = 0, X_i \neq 0 \ \forall 1 \leq i \leq n. \tag{14}$$

Recall that we wrote $f = \sum_w a_w X^w \in k[X_1, \ldots, X_n]$ and let $A_w = \tilde{a}_w$. For shorthand, we continue to write $X = (X_1, \ldots, X_n)$, X^w as before. Now we take

$$F(X_0, X_1, \ldots, X_n) = \prod_w \theta(A_w X_0 X^w).$$

Note that this is a *finite* product (since f is a polynomial).

Proposition 3.11. *We have $F \in B_0$ (where we replace "$X_0, \ldots, X_n$" with "$X_0, \ldots, X_{n+1}$" in (13)).*

Proof. We recall that $\theta(T)$ converges on $|T| < p^{1/(p-1)}$, and hence each $\theta(A_w X_0^{q^i} X^{q^i w})$ belongs to B_0 with $M = 1/q^i(p-1)$. Thus the finite product F also belongs to B_0. □

With the above prerequisites, the argument of Section 2.6 goes through and we obtain our "analytic Lefschetz fixed point formula" for all $d \geq 1$ (see (11), which we just restate here for easy reference)

$$(q^d - 1)^{n+1} \operatorname{trace}(\Psi_{q,F}^d) = q^d N_d - (q^d - 1)^n.$$

Now we expand out the binomials on both sides to get

$$N_d = \sum_{i=0}^{n} (-1)^n \binom{n}{i} q^{d(n-i-1)} + \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} q^{d(n-i)} \operatorname{trace}(\Psi_{q,F}^d).$$

Hence

(15)

$$\begin{aligned}
\zeta(X/k, T) &:= \exp\left(\sum_{d=1}^{\infty} N_d T^d/d\right) \\
&= \prod_{i=0}^{n} \left(\exp\left(q^{d(n-i-1)} T^d/d\right)\right)^{(-1)^i \binom{n}{i}} \cdot \prod_{i=0}^{n+1} \left(\exp\left(\sum_{d=1}^{\infty} q^{d(n-i)} \operatorname{trace}(\Psi_{q,F}^d) T^d/d\right)\right)^{(-1)^i \binom{n+1}{i}} \\
&= \prod_{i=0}^{n} (1 - q^{n-i-1}T)^{(-1)^{i+1}\binom{n}{i}} \cdot \prod_{i=0}^{n+1} \Delta(q^{n-i}T)^{(-1)^{i+1}\binom{n+1}{i}}.
\end{aligned}$$

3.4. **A general rationality criterion ("The Hillary Step").** [3] We begin with a general criterion for rationality for p-adic meromorphic functions. We copy the proof verbatim from [5, Chapter V.5, Lemma 5]. This is a quite technical step that we need to complete before reaching the summit (next section).

[3] Right before the summit of Mt. Everest, there is a sheer cliff face of about 40ft which requires several technical maneuvers to navigate.

Lemma 3.12. *Suppose* $F(T) = \sum_{i=0}^{\infty} a_i T^i \in K[\![T]\!]$ *where* K *is any field. For* $m, s \geq 0$*, let* $A_{s,m} = (a_{s+i+j})_{0 \leq i,j \leq m}$*, i.e.* $A_{s,m}$ *is the matrix*

$$\begin{pmatrix} a_s & a_{s+1} & a_{s+2} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & a_{s+3} & \cdots & a_{s+m+1} \\ a_{s+2} & a_{s+3} & a_{s+4} & \cdots & a_{s+m+2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m} \end{pmatrix},$$

and let $N_{s,m} := \det(A_{s,m})$*. Then* $F(T)$ *is rational (i.e. is a quotient* $F(T) = P(T)/Q(T)$*,* $P(T), Q(T) \in K[T]$*) if and only if there exist integers* $m \geq 0$ *and* S *such that* $N_{s,m} = 0$ *whenever* $s \geq S$*.*

Proof. " $\Longrightarrow$ ": Supposing $F(T) = P(T)/Q(T)$ where $P(T), Q(T) \in K[T]$, let $P(T) = \sum_{i=0}^{m} b_i T^i$ and $Q(T) = \sum_{i=0}^{n} c_i T^i$. Then from $P(T) = F(T)Q(T)$, we get for $i > \max(m, n)$,

$$\sum_{j=0}^{n} a_{i-n+j} c_{n-j} = 0.$$

Let $S = \max(m-n+1, 1)$ and let $m = n$. If $s \geq S$, we write the above equation for $s+n \leq i \leq s+2n$ to obtain

$$\begin{aligned} a_s c_n + a_{s+1} c_{n-1} + \cdots + a_{s+n} c_0 &= 0 \\ a_{s+1} c_n + a_{s+2} c_{n-1} + \cdots + a_{s+n+1} c_0 &= 0 \\ &\vdots \\ a_{s+n} c_n + a_{s+n+1} c_{n-1} + \cdots + a_{s+2n} c_0 &= 0. \end{aligned}$$

Hence $N_{s,m} = 0$ if $s \geq S$.

" $\Longleftarrow$ ": Let m be minimal with the property that there exists S such that $N_{s,m} = 0$ for all $s \geq S$. We claim that, in fact:

Claim 3.13. $N_{s,m-1} \neq 0$ for *all* $s \geq S$.

Proof of Claim 3.13. Suppose otherwise, i.e. there exist $s \geq S$ such that $N_{s,m-1} = 0$. Then some linear combination of the first m rows $r_0, r_1, \ldots, r_{m-1}$ of $A_{s,m}$ vanish in all except possibly the last column. Let r_{i_0} be the first row having nonzero coefficient in this linear combination so that there is some linear combination

$$a_1 r_{i_0+1} + a_2 r_{i_0+2} + \cdots a_{m-i_0-1} r_{m-1}$$

equal to r_{i_0} except possibly in the last coordinate. Now replace r_{i_0} by $r_{i_0} - (a_1 r_{i_0+1} + \cdots a_{m-i_0-1} r_{m-1})$ and consider two cases:

(1) $i_0 > 0$, so that our matrix (with r_{i_0} replaced as above) is

$$\begin{pmatrix} a_s & a_{s+1} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & \cdots & a_{s+m+1} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots 0 & \beta \\ \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m} \end{pmatrix},$$

and hence the minor formed by deleting the first row and last column has determinant $N_{s+1,m-1} = 0$.

(2) $i_0 = 0$, and so our replaced matrix is

$$\begin{pmatrix} 0 & 0 & \cdots 0 & \beta \\ a_{s+1} & a_{s+2} & \cdots & a_{s+m+1} \\ \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m} \end{pmatrix},$$

and hence $N_{s+1,m-1}$ is the determinant of the minor formed by deleting the first row and last column, and of the minor formed by deleting the last row and first column. Then either the determinant of the former minor is 0 (in which case $N_{s+1,m-1} = 0$), or else since the determinant of the entire matrix is $N_{s,m} = 0$, we must have $\beta = 0$, which implies the determinant of the latter minor is 0 and hence $N_{s+1,m-1} = 0$ again.

Hence $N_{s+1,m-1} = 0$ in any case, and by induction on s (note that in the above argument we showed $N_{s,m-1} = 0 \implies N_{s+1,m-1} = 0$) one can show $N_{s',m-1} = 0$ for all $s' \geq s$. This contradicts the minimality of m. □

By the Claim, for any $s \geq S$ we have $N_{s,m} = 0$ and $N_{s,m-1} \neq 0$. Thus there is a linear combination of the rows of $A_{s,m}$ which vanishes *and* such that the coefficient of the last row in this linear combination is nonzero. Thus, any solution

$$\begin{pmatrix} a_S & a_{S+1} & a_{S+2} & \cdots & a_{s+m} \\ a_{S+1} & a_{S+2} & a_{S+3} & \cdots & a_{S+m+1} \\ a_{S+2} & a_{S+3} & a_{S+4} & \cdots & a_{S+m+2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{S+m-1} & a_{S+m} & a_{S+m+1} & \cdots & a_{s+2m-1} \end{pmatrix} \begin{pmatrix} u_m \\ u_{m-1} \\ u_{m-2} \\ \vdots \\ u_0 \end{pmatrix} = 0,$$

is also a solution to

$$a_{S+m}u_m + a_{S+m+1}u_{m-1} + \cdots + a_{S+2m}u_0 = \begin{pmatrix} a_{S+m} & a_{S+m+1} & a_{S+m+2} & \cdots & a_{S+2m} \end{pmatrix} \begin{pmatrix} u_m \\ u_{m-1} \\ u_{m-2} \\ \vdots \\ u_0 \end{pmatrix} = 0.$$

Thus, by induction on s, we get that it is a solution to

$$a_s u_m + a_{s+1}u_{m-1} + \cdots + a_{s+m}u_0 = 0$$

for *every* $s \geq S$. In particular, we see that

$$\left(\sum_{i=0}^{m} u_i X^i\right) \cdot \left(\sum_{i=0}^{\infty} a_i X^i\right)$$

is a polynomial of degree $< S + m$, which gives the rationality. □

3.5. **The final step: the ζ-function is rational ("The Summit").** With Lemma 3.12 in hand, we are ready to push to the summit. Throughout, we will let $|\cdot|$ denote the p-adic absolute value, and let $|\cdot|_\infty$ denote the usual archimedean absolute value.

For brevity, let $Z(T) = \zeta(X/k, T)$. From (15) we have $Z(T) = A(T)/B(T)$ where $A(T)$ and $B(T)$ are p-adic entire functions. We now invoke the Weierstrass Preparation Theorem ([5, Chapter IV.4, Theorem 14]) for $R > 0$ to write $B(T) = P(T)/G(T)$ where $G(T) \in 1 + T\mathcal{O}_K[\![T]\!]$ converges on $|T| < R$ and $P(T) \in \mathcal{O}_K[T]$, i.e. is a polynomial. We take $R = q^{2n}$ for simplicity (recall

$X/k \subset \mathbb{A}^n_k$). In fact since we may take $B(T) \in 1 + T\mathcal{O}_K[\![T]\!]$, we can take $P(T) \in 1 + T\mathcal{O}_K[T]$. Letting $F(T) = A(T)G(T)$, which converges on $|T| < R$, we get

$$F(T) = P(T)Z(T).$$

Write $Z(T) = \sum_{i=0}^{\infty} a_i T^i \in 1 + T\mathbb{Z}[\![T]\!]$. Hence we can write $F(T) = \sum_{i=0}^{\infty} b_i T^i \in 1 + T\mathcal{O}_K[\![T]\!]$ and $P(T) \in \sum_{i=0}^{\infty} c_i T^i \in 1 + T\mathcal{O}_K[T]$. We have the following trivial archimedean bound for the a_i.

Lemma 3.14. $|a_i|_\infty \leq q^{ni}$.

Proof. We know that $N_d \leq (\#k_d)^n = q^{nd}$ trivially (in fact, by our reduction (14) we have $\leq (q^d - 1)^n$, but we will not need this). Since all the N_d are positive, the coefficients of $\zeta(X/k, T)$ are less than or equal to the coefficients of the series obtained by replacing N_d with q^{nd}. But now

$$\exp\left(\sum_{i=0}^{\infty} q^{nd} T^d/d\right) = \exp(-\log(1 - q^n T)) = 1/(1 - q^n T) = \sum_{i=0}^{\infty} q^{ni} T^i.$$

□

Moreover, since $F(T)$ converges for $|T| < R$, we have (by the p-adic Cauchy criterion) that for $i \gg 0$,

$$|b_i| \leq R^{-i} = q^{-2ni}.$$

Now choose and fix $m > 2e$. Let $A_{s,m} = (a_{s+i+j})_{0 \leq i,j, \leq m}$, and $N_{s,m} = \det(A_{s,m})$ as before. We claim that for our m, we have $N_{s,m} = 0$ for all $s \gg 0$. Then by Lemma 3.12, this gives the desired rationality of $Z(T)$.

By equating the coefficients in the identity $F(T) = P(T)Z(T)$, we see that

$$b_{j+e} = a_{j+e} + c_1 a_{j+e-1} + c_2 a_{j+e-2} + \cdots + c_e a_j.$$

In $A_{s,m}$ add to each $(j + e)$th column, starting from the rightmost and moving left until the eth column, the linear combination of the previous e columns with coefficient c_k for the $(j + e - k)$th column. From this we obtain a matrix $B_{s,m}$ whose first e columns are the same as those of $A_{s,m}$ and in the remaining columns, the a's are replaced by the corresponding b's. Clearly $\det(B_{s,m}) = \det(A_{s,m}) = N_{s,m}$. We will examine $B_{s,m}$ in order to estimate $|N_{s,m}|$.

Because $a_i \in \mathbb{Z}$, $|a_i| \leq 1$. Hence, by the nonarchimedean supertriangle inequality, $|N_{s,m}| \leq (\max_{j \geq s+e} |b_j|)^{m+1-e} < R^{-s(m+1-e)}$ for $s \gg 0$. Since $R = q^{2n}$ and $m > 2e$, we get

$$|N_{s,m}| < q^{-ns(m+2)}.$$

On the other hand, using $A_{s,m}$ to compute $N_{s,m}$ and the archimedean triangle inequality, we see that

$$|N_{s,m}|_\infty \leq (m+1)! q^{n(s+2m)(m+1)} = (m+1)! q^{2nm(m+1)} q^{ns(m+1)}.$$

Now multiplying the bounds we get for all $s \gg 0$

$$|N_{s,m}| \cdot |N_{s,m}|_\infty < q^{-ns(m+2)} \cdot (m+1)! q^{2nm(m+1)} q^{ns(m+1)} = \frac{(m+1)! q^{2nm(m+1)}}{q^{ns}} < 1.$$

For a (not necessarily finite) prime ℓ, briefly let $|\cdot|_\ell$ denote the standard absolute value on $\mathbb{Q}_\ell$. Then since $N_{s,m} \in \mathbb{Z}$, we have $|N_{s,m}|_\ell \leq 1$ for all finite primes ℓ. By the idèlic product formula, for all $s \gg 0$ either $N_{s,m} = 0$ or

$$1 = \prod_{\ell \leq \infty} |N_{s,m}|_\ell \leq |N_{s,m}| \cdot |N_{s,m}|_\infty < 1,$$

a contradiction, and hence $N_{s,m} = 0$ for all $s \gg 0$. We are done.

References

[1] J.-B. Bost, *Algebraic leaves of algebraic foliations over number fields*, Publications Mathématiques de l'IHÉS, Tome 93 (2001) , pp. 161-221.

[2] B. Dwork, *Norm residue Symbol in local number Fields*. Abh. Math. Sem. Univ. Hamburg 22 1958 180-90.

[3] N. Katz, *p-adic properties of modular schemes and modular forms*: pp. 69-190 in "Modular Functions of One Variable III", Springer Lecture Notes in Mathematics 350 (1973).

[4] N. Katz, J. Tate, *Bernard Dwork (1923-1998)*, Notices of the AMS, volume 46 no. 3, 1998.

[5] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta functions*, Graduate Texts in Mathematics book series (GTM, volume 58).