Dwork's proof of the rationality of the zeta function

Galop seminar, Oxford – 6 February 2019

Tiago J. Fonseca*

Contents

Introduction **2**

1) Weil conjectures **4**

2) Back to the future: cohomological proof of W1 **5**

3) Dwork's method **7**

3.1) The Borel–Dwork theorem 7

3.2) Meromorphy of ζ_X 9

*Notes digitized with the help of artificial intelligence from the speaker's handwritten notes, without careful revision.

Introduction

These are the notes of a talk given at the Galop seminar in Oxford on 6 February 2019. Its aim was to explain the key ideas of Dwork's original proof (1960) of the first of the Weil conjectures: the zeta function of any variety over a finite field is a rational function. The notes follow the structure of the talk:

1) the Weil conjectures;

2) "back to the future": the cohomological proof of rationality, which came later but is the one usually presented today;

3) Dwork's method, which combines a rationality criterion *à la* Borel with the p-adic meromorphy of the zeta function, obtained by writing it in terms of Fredholm determinants of certain "nuclear" operators on p-adic Banach spaces.

Some arguments that were only sketched in the talk are expanded here, using a typed draft that the author had started at the time.

References. Dwork's original paper is

[1] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.

A very readable account, which we largely follow in Section 3, is Serre's Bourbaki talk

[2] J.-P. Serre, *Rationalité des fonctions ζ des variétés algébriques (d'après Bernard Dwork)*, Séminaire Bourbaki, exp. 198 (1959/60).

The rationality criterion goes back to

[3] É. Borel, *Sur une application d'un théorème de M. Hadamard*, Bull. Sci. Math. (2) **18** (1894), 22–25.

Other references:

[4] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

[5] P. Deligne, *La conjecture de Weil. I*, Publ. Math. IHÉS **43** (1974), 273–307.

[6] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Graduate Texts in Mathematics 58, Springer, New York, 1984, Chapter V.

[7] A. Chambert-Loir, *Théorèmes d'algébricité en géométrie diophantienne (d'après J.-B. Bost, Y. André, D. & G. Chudnovsky)*, Séminaire Bourbaki, exp. 886 (2000/01), Astérisque **282** (2002).

[8] J.-P. Serre, *Endomorphismes complètement continus des espaces de Banach p-adiques*, Publ. Math. IHÉS **12** (1962), 69–85.

Koblitz's book [6] contains a complete and elementary exposition of Dwork's proof.

Throughout, p is a prime number. For simplicity we work only over the prime field $\mathbb{F}_p$. By a *variety over* $\mathbb{F}_p$ we mean a separated scheme of finite type over $\mathbb{F}_p$.

1) Weil conjectures

Definition 1.1 (Zeta function)**.** For a variety X over $\mathbb{F}_p$, we set

$$\zeta_X(T) = \exp\Big(\sum_{n\geqslant 1} \#X(\mathbb{F}_{p^n})\,\frac{T^n}{n}\Big) \in \mathbb{Q}[[T]].$$

Equivalently, $\zeta_X(T)$ is the unique element of $\mathbb{Q}[[T]]$ such that $\zeta_X(0) = 1$ and

$$T\frac{d}{dT}\log\zeta_X(T) = \sum_{n\geqslant 1} \#X(\mathbb{F}_{p^n})\,T^n,$$

that is, the logarithmic derivative of ζ_X is the generating series of the numbers of points of X.

Example 1.2 (Affine and projective spaces)**.** Since $\#\mathbb{A}^d(\mathbb{F}_{p^n}) = p^{dn}$,

$$T\frac{d}{dT}\log\zeta_{\mathbb{A}^d}(T) = \sum_{n\geqslant 1} p^{dn}T^n = \frac{p^dT}{1-p^dT} = T\frac{d}{dT}\log\frac{1}{1-p^dT},$$

so that

$$\zeta_{\mathbb{A}^d}(T) = \frac{1}{1-p^dT}.$$

Using the decomposition $\mathbb{P}^d = \mathbb{A}^0 \sqcup \mathbb{A}^1 \sqcup \cdots \sqcup \mathbb{A}^d$ (and the fact that point counts are additive), we get

$$\zeta_{\mathbb{P}^d}(T) = \frac{1}{(1-T)(1-pT)\cdots(1-p^dT)}.$$

In 1949, Weil conjectured the following [4]. Let X be a smooth projective variety over $\mathbb{F}_p$ of dimension d.

W1. (Rationality) $\zeta_X(T) \in \mathbb{Q}(T)$, i.e., ζ_X is the Taylor expansion at 0 of a rational function.

W2. (Functional equation) If $\chi = \chi(X)$ denotes the Euler–Poincaré characteristic of X (the self-intersection $\Delta\cdot\Delta$ of the diagonal in $X\times X$), then

$$\zeta_X\Big(\frac{1}{p^dT}\Big) = \pm\, p^{\frac{d\chi}{2}}\, T^\chi\, \zeta_X(T).$$

W3. (Riemann hypothesis) We can write

$$\zeta_X(T) = \frac{P_1(T)P_3(T)\cdots P_{2d-1}(T)}{P_0(T)P_2(T)\cdots P_{2d}(T)},$$

with $P_0(T) = 1 - T$, $P_{2d}(T) = 1 - p^d T$ and, for $1 \leqslant i \leqslant 2d-1$,

$$P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}T) \in \mathbb{Z}[T],$$

where the α_{ij} are algebraic integers with $|\alpha_{ij}| = p^{i/2}$ (for every complex embedding).

Moreover, if X lifts to a smooth projective variety in characteristic 0, then b_i is the i-th Betti number of the lift.

Remark. These have been theorems since 1973: rationality by Dwork (1960) [1], the functional equation and the cohomological interpretation by Grothendieck and his school (étale cohomology), and the Riemann hypothesis by Deligne [5].

Example 1.3 (Elliptic curves)**.** If E is an elliptic curve over $\mathbb{F}_p$, then

$$\zeta_E(T) = \frac{P_1(T)}{(1-T)(1-pT)},$$

where $P_1(T) = (1 - \alpha T)(1 - \overline{\alpha}T) = 1 - aT + pT^2 \in \mathbb{Z}[T]$. Comparing coefficients, $\#E(\mathbb{F}_p) = 1 + p - a$, and more generally $\#E(\mathbb{F}_{p^n}) = 1 + p^n - \alpha^n - \overline{\alpha}^n$, so that all the numbers $\#E(\mathbb{F}_{p^n})$ depend only on a. The Riemann hypothesis is Hasse's bound $|a| \leqslant 2\sqrt{p}$. The curve E is *supersingular* if $a \equiv 0 \pmod{p}$; for instance, $y^2 = x^3 + b$ with $b \in \mathbb{F}_p^\times$ is supersingular when $p \equiv 2 \pmod{3}$.

The aim of this talk is to explain the key ideas in the original proof of the following theorem.

Theorem 1.4 (Dwork, 1960)**.** *For every variety X over $\mathbb{F}_p$, we have $\zeta_X(T) \in \mathbb{Q}(T)$.*

In particular, this implies **W1**. Observe that X in Theorem 1.4 is more general than in the Weil conjectures: it may be affine or singular.

2) Back to the future: cohomological proof of W1

The "modern" proof of rationality goes as follows. Let H be a *Weil cohomology theory* for smooth projective varieties over $\mathbb{F}_p$, with coefficients in a

field K of characteristic 0; for example, ℓ-adic cohomology ($\ell \neq p$, $K = \mathbb{Q}_\ell$) or crystalline (rigid) cohomology ($K = \mathbb{Q}_p$). The key properties that we need are:

(1) each $H^i(X)$ is a finite-dimensional K-vector space, and $H^i(X) = 0$ unless $0 \leqslant i \leqslant 2d$;

(2) (Lefschetz fixed point formula) if $f\colon X \to X$ is an endomorphism whose set of fixed points $X^f = \{x \in X(\overline{\mathbb{F}}_p) : f(x) = x\}$ is finite, and these fixed points are *isolated* (of multiplicity one), then

$$\#X^f \ (= \Gamma_f \cdot \Delta) = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}\bigl(f^* \mid H^i(X)\bigr).$$

Rationality then follows from a simple lemma in linear algebra.

Lemma 2.1. *Let V be a finite-dimensional vector space over a field K of characteristic 0, and let $\varphi \in \operatorname{End}(V)$. Then*

$$\det(1 - \varphi T) = \exp\Bigl(-\sum_{n \geqslant 1} \operatorname{Tr}(\varphi^n) \frac{T^n}{n}\Bigr).$$

Proof. Extending scalars, we may assume that K is algebraically closed, so that $\det(1-\varphi T) = \prod_i (1 - \alpha_i T)$, where the α_i are the eigenvalues of φ (with multiplicity); then the α_i^n are the eigenvalues of φ^n. Hence

$$\begin{aligned} T\frac{d}{dT} \log\det(1 - \varphi T) &= \sum_i T \frac{d}{dT} \log(1 - \alpha_i T) \\ &= -\sum_i \sum_{n \geqslant 1} \alpha_i^n T^n = -\sum_{n \geqslant 1} \operatorname{Tr}(\varphi^n) T^n. \end{aligned}$$ □

Let $f\colon X \to X$ be the Frobenius endomorphism of X ("$x \mapsto x^p$"). Then $X^{f^n} = X(\mathbb{F}_{p^n})$, and all fixed points are isolated. Combining the fixed point formula with Lemma 2.1:

$$\begin{aligned} \zeta_X(T) &= \exp\Bigl(\sum_{n \geqslant 1} \#X(\mathbb{F}_{p^n}) \frac{T^n}{n}\Bigr) = \exp\Bigl(\sum_{n \geqslant 1} \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}\bigl(f^{n*} \mid H^i(X)\bigr) \frac{T^n}{n}\Bigr) \\ &= \prod_{i=0}^{2d} \exp\Bigl(\sum_{n \geqslant 1} \operatorname{Tr}\bigl(f^{n*} \mid H^i(X)\bigr) \frac{T^n}{n}\Bigr)^{(-1)^i} \\ &= \frac{\prod_{i \text{ odd}} \det\bigl(1 - f^*T \mid H^i(X)\bigr)}{\prod_{i \text{ even}} \det\bigl(1 - f^*T \mid H^i(X)\bigr)}. \end{aligned}$$

Remark 2.2. This shows that $\zeta_X(T) \in K(T)$. Since also $\zeta_X(T) \in \mathbb{Q}[[T]]$, we get $\zeta_X(T) \in \mathbb{Q}[[T]] \cap K(T) = \mathbb{Q}(T)$: indeed, by the criterion of Lemma 3.3 below, being rational is a condition on the vanishing of certain determinants in the coefficients, which does not depend on the field.

Remark 2.3. The more general statement of Theorem 1.4 (for arbitrary varieties) can also be obtained in this way, by working with cohomology *with compact supports*, both in the ℓ-adic and in the rigid (p-adic) setting.

Why bother? If the cohomological approach can nowadays be made completely rigorous, why give this talk?

(1) Dwork's proof is beautiful and very original. You'll see.

(2) Dwork's method is better suited for computations: it leads to algorithms for computing zeta functions (cf. the work of Lauder and Wan).

(3) Dwork's work motivated the whole field of p-adic cohomology. It also prompted Serre to write a paper on the Fredholm theory of compact operators on p-adic Banach spaces [8], which is used, e.g., in the theory of overconvergent modular forms.

3) Dwork's method

Dwork's proof has two ingredients:

$$\begin{cases} \text{a rationality criterion } (\grave{a}\ la \text{ Borel}); \\ \text{the } p\text{-adic meromorphy of } \zeta_X. \end{cases}$$

3.1) The Borel–Dwork theorem

The starting point is the following observation: $\zeta_X(T)$ actually has *integral* coefficients.

Lemma 3.1. *For every variety X over $\mathbb{F}_p$,*

$$\zeta_X(T) = \prod_x \frac{1}{1 - T^{\deg(x)}} \in \mathbb{Z}[[T]],$$

where x runs through the closed points of X (i.e., the orbits of Frobenius on $X(\overline{\mathbb{F}}_p)$), and $\deg(x) = \min\{n \geqslant 1 : x \in X(\mathbb{F}_{p^n})\}$ is the size of the orbit.

Proof. Taking logarithmic derivatives,

$$T\frac{d}{dT}\log\prod_x \frac{1}{1 - T^{\deg(x)}} = \sum_x \sum_{e \geqslant 1} \deg(x)\, T^{\deg(x)e}$$

$$= \sum_{n \geqslant 1} \Big(\sum_{d \mid n} d \cdot \#\{x : \deg(x) = d\} \Big) T^n,$$

and the coefficient of T^n is $\#X(\mathbb{F}_{p^n})$, since a point of $X(\overline{\mathbb{F}}_p)$ is defined over $\mathbb{F}_{p^n}$ if and only if the degree d of its orbit divides n, and each orbit of degree d has d points. □

Example 3.2 (Warm-up)**.** Let $f(T) = \sum_n a_n T^n \in \mathbb{Z}[[T]]$. If f has (complex) radius of convergence $R > 1$, then $f \in \mathbb{Z}[T]$. Indeed, by the Cauchy estimates, for any $1 < r < R$ there is $C > 0$ with $|a_n| \leqslant C/r^n$; hence $|a_n| < 1$, i.e. $a_n = 0$, for $n \gg 0$.

Borel's theorem replaces "holomorphic" by "meromorphic". It is based on the Cauchy estimates and on the following classical lemma.

Lemma 3.3 (Kronecker)**.** *Let k be a field and $F = \sum_{n\geqslant 0} a_n T^n \in k[[T]]$. Then $F \in k(T)$ if and only if there exists $m \geqslant 0$ such that the* Hankel determinants

$$h_{n,m} = \det \begin{pmatrix} a_n & a_{n+1} & \cdots & a_{n+m} \\ a_{n+1} & a_{n+2} & \cdots & a_{n+m+1} \\ \vdots & \vdots & & \vdots \\ a_{n+m} & a_{n+m+1} & \cdots & a_{n+2m} \end{pmatrix}$$

vanish for all $n \gg 0$.

Proof. See, e.g., Bourbaki, *Algèbre*, Chapter IV, §5, Exercise 3, or [6], Chapter V. (One direction is easy: if $F = P/Q$ with $Q = 1+b_1T+\cdots+b_dT^d$, then the coefficients satisfy the linear recurrence $a_{n+d}+b_1a_{n+d-1}+\cdots+b_da_n = 0$ for $n \gg 0$, so the columns of the Hankel matrix with $m = d$ are linearly dependent.) □

Theorem 3.4 (Borel, 1894)**.** *Let $f(T) = \sum_n a_n T^n \in \mathbb{Z}[[T]]$. If f is the Taylor expansion at the origin of a meromorphic function on a disc $D(0,R) \subseteq \mathbb{C}$ with $R > 1$, then $f \in \mathbb{Q}(T)$.*

Proof. Let $1 < r < R$. Since f has finitely many poles in $\overline{D}(0,r)$, there is a polynomial $P(T) = 1 + b_1T + \cdots + b_dT^d \in \mathbb{C}[T]$ such that

$$g(T) = P(T)f(T) = c_0 + c_1T + c_2T^2 + \cdots$$

is holomorphic on a neighbourhood of $\overline{D}(0,r)$. For $j \geqslant d$ we have $c_j = a_j + b_1a_{j-1} + \cdots + b_da_{j-d}$. Hence, in the Hankel matrix defining $h_{n,m}$ ($m \geqslant d$), adding to each column $j \geqslant d$ (starting from the last one) the linear combination with coefficients $b_1, \ldots, b_d$ of the d preceding columns, we obtain

$$h_{n,m} = \det \begin{pmatrix} a_n & \cdots & a_{n+d-1} & c_{n+d} & \cdots & c_{n+m} \\ a_{n+1} & \cdots & a_{n+d} & c_{n+d+1} & \cdots & c_{n+m+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n+m} & \cdots & a_{n+m+d-1} & c_{n+m+d} & \cdots & c_{n+2m} \end{pmatrix}.$$

Let $r_0 > 0$ be the radius of convergence of f (we may assume $r_0 \leqslant 1$). By the Cauchy estimates, for any $r_0' < r_0$ there is $C > 0$ such that $|a_k| \leqslant C/r_0'^k$ and $|c_k| \leqslant C/r^k$ for all k. Expanding the determinant, we get

$$|h_{n,m}| \leqslant C' \frac{1}{r_0'^{dn}\, r^{(m-d+1)n}},$$

with C' independent of n. If m is large enough so that $r_0'^d r^{m-d+1} > 1$, then $|h_{n,m}| \to 0$ as $n \to \infty$. Since $h_{n,m} \in \mathbb{Z}$, this forces $h_{n,m} = 0$ for $n \gg 0$, and we conclude by Lemma 3.3. □

Now consider the field $\mathbb{C}_p$, the completion of an algebraic closure of $\mathbb{Q}_p$, with its absolute value $|\cdot|_p$ normalized by $|p|_p = 1/p$. For $R > 0$, let $D_p(0, R) = \{t \in \mathbb{C}_p : |t|_p < R\}$. The radius of convergence of $F = \sum_n a_n T^n \in \mathbb{C}_p[[T]]$ is given by the usual formula $1/R = \limsup_n |a_n|_p^{1/n}$, and the Cauchy estimates hold in the form: if F converges on $D_p(0, R)$, then for every $r < R$ we have $|a_n|_p r^n \to 0$.

Definition 3.5. We say that $F \in \mathbb{C}_p[[T]]$ is *meromorphic* on $D_p(0, R)$ if it is a quotient of two power series converging on $D_p(0, R)$. The (*p-adic*) *radius of meromorphy* of F is the supremum of such R. We say that F is meromorphic on $\mathbb{C}_p$ if its radius of meromorphy is $+\infty$.

Theorem 3.6 (Borel–Dwork)**.** *Let $F \in \mathbb{Z}[[T]]$, and denote by R_∞ (resp. R_p) its complex (resp. p-adic) radius of meromorphy. If $R_\infty, R_p > 0$ and*

$$R_\infty R_p > 1,$$

then $F \in \mathbb{Q}(T)$.

Idea of proof. One repeats the proof of Borel's theorem both in the complex and in the p-adic setting, using the p-adic Cauchy estimates and the fact that $|a_n|_p \leqslant 1$. This gives two upper bounds for the Hankel determinants $h_{n,m}$: an archimedean one and a p-adic one, whose product tends to 0 as $n \to \infty$ if m is large enough, thanks to $R_\infty R_p > 1$. One concludes by remarking that *a non-zero integer cannot be simultaneously small for $|\cdot|_\infty$ and $|\cdot|_p$*: if $h \in \mathbb{Z} \setminus \{0\}$, then $|h|_\infty |h|_p \geqslant 1$. See [1], §4, or [2], Proposition 2. □

Remark. This is the prototype of many "algebraicity criteria" in diophantine geometry; see Chambert-Loir's Bourbaki talk [7].

3.2) Meromorphy of ζ_X

Objective. Prove that ζ_X is meromorphic on $\mathbb{C}_p$ (i.e. $R_p = +\infty$), by writing it as an alternating product of Fredholm determinants of certain nuclear operators on p-adic Banach spaces.

Dévissage. We may assume that

$$X = V(f) \cap \mathbb{G}_{\mathrm{m}}^d \subseteq \mathbb{A}^d$$

for some $f \in \mathbb{F}_p[X_1, \dots, X_d]$. This follows from the formula

$$\zeta_{U \cup V} = \frac{\zeta_U \, \zeta_V}{\zeta_{U \cap V}}$$

(for $U, V \subseteq X$ open, or more generally constructible), together with some combinatorics: one first reduces to the case where X is affine, then to the case where X is an affine hypersurface, and finally to the case where X is a hypersurface in a torus (using the decomposition of $\mathbb{A}^d$ into the tori $\mathbb{G}_{\mathrm{m}}^S$, $S \subseteq \{1, \dots, d\}$).

Remark 3.7. If $X \subseteq \mathbb{A}^d$, then $\#X(\mathbb{F}_{p^n}) \leqslant p^{dn}$, so ζ_X is dominated coefficientwise (as is clear from Lemma 3.1) by $\zeta_{\mathbb{A}^d} = 1/(1 - p^d T)$. Hence the complex radius of convergence, and a fortiori R_∞, is $\geqslant p^{-d} > 0$. By the Borel–Dwork theorem, it suffices to prove that $R_p = +\infty$.

For $a \in \mathbb{F}_{p^n}$, denote by $\widehat{a} \in \mathbb{C}_p$ its *Teichmüller lift*: $\widehat{0} = 0$ and, if $a \neq 0$, $\widehat{a}$ is the unique $(p^n - 1)$-th root of unity in $\mathbb{C}_p$ reducing to a. Thus $\widehat{a}^{p^n} = \widehat{a}$, and $a \mapsto \widehat{a}$ is multiplicative.

Lemma 3.8 (Dwork's splitting function)**.** *Let $\pi \in \mathbb{C}_p$ with $\pi^{p-1} = -p$, and let*

$$\Theta(T) = \exp\bigl(\pi(T - T^p)\bigr) \in \mathbb{C}_p[[T]].$$

Then:

(1) Θ is "overconvergent", i.e., it converges on $D_p(0, 1+\varepsilon)$ for some $\varepsilon > 0$ (in fact, its radius of convergence is $p^{(p-1)/p^2}$);

(2) for every $n \geqslant 1$, the map

$$\Theta_n \colon \mathbb{F}_{p^n} \to \mathbb{C}_p^\times, \qquad a \longmapsto \Theta(\widehat{a})\,\Theta(\widehat{a}^{\,p}) \cdots \Theta(\widehat{a}^{\,p^{n-1}})$$

is a non-trivial additive character of $\mathbb{F}_{p^n}$. More precisely, $\Theta(1)$ is a primitive p-th root of unity and $\Theta_n(a) = \Theta(1)^{\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(a)}$.

About the proof. Plain p-adic analysis; see [6], Chapter IV, or [2], §3 (where a variant of Θ is constructed from $(1+Y)^t$). Note that one cannot simply argue that the product in (2) "telescopes" to $\exp\bigl(\pi(\widehat{a} - \widehat{a}^{\,p^n})\bigr) = \exp(0) = 1$: the series $\exp(\pi T)$ only converges for $|T|_p < 1$, and the whole point is that Θ converges a little beyond the unit disc. In other words, if $\psi \colon \mathbb{F}_p \to \mathbb{C}_p^\times$ is the additive character $x \mapsto \Theta(1)^x$, then $\Theta_n = \psi \circ \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}$. □

Orthogonality relations. For $u \in \mathbb{F}_{p^n}$,

$$1 + \sum_{x_0 \in \mathbb{F}_{p^n}^\times} \Theta_n(x_0 u) = \sum_{x_0 \in \mathbb{F}_{p^n}} \Theta_n(x_0 u) = \begin{cases} 0, & u \neq 0, \\ p^n, & u = 0. \end{cases}$$

Applying this to $u = f(x_1, \dots, x_d)$, with $x = (x_1, \dots, x_d) \in (\mathbb{F}_{p^n}^\times)^d$, and summing over x, we get

$$p^n \, \#X(\mathbb{F}_{p^n}) = (p^n - 1)^d + \underbrace{\sum_{(x_0,\dots,x_d) \in (\mathbb{F}_{p^n}^\times)^{d+1}} \Theta_n\big(x_0 f(x_1, \dots, x_d)\big)}_{S_n \text{ (exponential sum)}}.$$

Since $\sum_n (p^n - 1)^d T^n/n = \sum_n \#\mathbb{G}_{\mathrm{m}}^d(\mathbb{F}_{p^n}) T^n/n$, this gives

$$\zeta_X(pT) = \zeta_{\mathbb{G}_{\mathrm{m}}^d}(T)\, L(T), \qquad L(T) = \exp\Big(\sum_{n \geqslant 1} S_n \frac{T^n}{n}\Big),$$

where $\zeta_{\mathbb{G}_{\mathrm{m}}^d}(T) = \prod_{j=0}^d (1 - p^j T)^{(-1)^{d-j+1}\binom{d}{j}} \in \mathbb{Q}(T)$.

Claim. $L(T)$ is meromorphic on $\mathbb{C}_p$.

Write

$$X_0\, f(X_1, \dots, X_d) = \sum_I a_I X^I, \qquad a_I \in \mathbb{F}_p,$$

where $I = (i_0, \dots, i_d)$ runs through a finite set of multi-indices and $X^I = X_0^{i_0} \cdots X_d^{i_d}$. Since Θ_n is a character and Teichmüller lifts are multiplicative,

$$\begin{aligned} S_n &= \sum_x \Theta_n\Big(\sum_I a_I x^I\Big) = \sum_x \prod_I \Theta_n(a_I x^I) = \sum_x \prod_I \prod_{j=0}^{n-1} \Theta((\widehat{a}_I \widehat{x}^I)^{p^j}) \\ &= \sum_{y \in \mu_{p^n-1}(\mathbb{C}_p)^{d+1}} G(y)\, G(y^p) \cdots G(y^{p^{n-1}}), \end{aligned}$$

where x runs through $(\mathbb{F}_{p^n}^\times)^{d+1}$, $y = \widehat{x}$, and

$$G(X) = \prod_I \Theta(\widehat{a}_I X^I) \in \mathbb{C}_p[[X_0, \dots, X_d]].$$

Here we used that $\widehat{a}_I \in \mu_{p-1} \cup \{0\} \subseteq \mathbb{Z}_p$, so that $\widehat{a}_I^p = \widehat{a}_I$.

Lemma 3.9 (Dwork's trace formula)**.** *Let*

- $\Psi \colon \mathbb{C}_p[[X_0, \dots, X_d]] \to \mathbb{C}_p[[X_0, \dots, X_d]]$ *be the operator* $\sum_J c_J X^J \mapsto \sum_J c_{pJ} X^J$*;*

- $G = \sum_I g_I X^I \in \mathbb{C}_p[[X_0, \dots, X_d]]$ *be such that* $|g_I|_p \leqslant p^{-\varepsilon|I|}$ *for some* $\varepsilon > 0$, *where* $|I| = i_0 + \cdots + i_d$ *(cf. "weak completions" in Monsky–Washnitzer cohomology);*
- $\alpha = \Psi \circ L_G$, *where* L_G *denotes multiplication by* G.

Then, for every $n \geqslant 1$, *the trace of* α^n *(the trace of an infinite matrix, in the basis of monomials* X^J*) converges, and*

$$(p^n - 1)^{d+1} \operatorname{Tr}(\alpha^n) = \sum_{y \in \mu_{p^n-1}^{d+1}} G(y)\, G(y^p) \cdots G(y^{p^{n-1}}).$$

Sketch. One checks that $L_G \circ \Psi = \Psi \circ L_{G(X^p)}$, hence $\alpha^n = \Psi^n \circ L_{G(X)G(X^p)\cdots G(X^{p^{n-1}})}$; this reduces the claim to $n = 1$ (replacing p by p^n). For $n = 1$, the matrix of α in the basis of monomials is $(g_{pv-u})_{u,v}$, so $\operatorname{Tr}(\alpha) = \sum_u g_{(p-1)u}$, which converges by the hypothesis on G. On the other hand, $\sum_{y \in \mu_{p-1}^{d+1}} y^v$ equals $(p-1)^{d+1}$ if $p-1$ divides all the entries of v, and 0 otherwise. Hence $\sum_y G(y) = (p-1)^{d+1} \sum_u g_{(p-1)u}$. See [2], Proposition 4. □

Since Θ is overconvergent, the series G above satisfies the hypothesis of the lemma. Therefore

$$S_n = (p^n - 1)^{d+1} \operatorname{Tr}(\alpha^n) = \sum_{j=0}^{d+1} \binom{d+1}{j} (-1)^{d+1-j} (p^j)^n \operatorname{Tr}(\alpha^n),$$

so that

$$L(T) = \prod_{j=0}^{d+1} \exp\Big(\sum_{n \geqslant 1} \operatorname{Tr}(\alpha^n) \frac{(p^j T)^n}{n} \Big)^{(-1)^{d+1-j}\binom{d+1}{j}}.$$

Lemma 3.10 (Fredholm determinant)**.** *With* α *as in Lemma 3.9:*

(1) the Fredholm determinant

$$\Delta(T) = \det(1 - \alpha T) = \sum_{n \geqslant 0} \gamma_n T^n,$$

$$\gamma_n = (-1)^n \sum_{i_1 < \cdots < i_n} \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\, \alpha_{i_1 i_{\sigma(1)}} \cdots \alpha_{i_n i_{\sigma(n)}},$$

is well defined (here (α_{ij}) *is the matrix of* α *in the basis of monomials, indexed by* $\mathbb{N}^{d+1}$ *in some order); for instance,* $\gamma_0 = 1$, $\gamma_1 = -\operatorname{Tr}(\alpha) = -\sum_i \alpha_{ii}$ *and* $\gamma_2 = \sum_{i<j} (\alpha_{ii}\alpha_{jj} - \alpha_{ij}\alpha_{ji})$*;*

(2) as in Lemma 2.1,

$$\Delta(T) = \exp\Big(- \sum_{n \geqslant 1} \operatorname{Tr}(\alpha^n) \frac{T^n}{n} \Big);$$

(3) $\Delta(T)$ *converges on all of* $\mathbb{C}_p$*, i.e., it is an* entire *function.*

About the proof. Item (2) is proved by truncating α to finite matrices and passing to the limit; item (3) follows from the estimate $\mathrm{ord}_p(\gamma_n)/n \to +\infty$, which comes from the hypothesis on the coefficients of G. See [2], Proposition 5, and, for the general theory of such "completely continuous" operators, [8]. □

Putting everything together, we obtain

$$L(T) = \prod_{j=0}^{d+1} \Delta(p^j T)^{(-1)^{d-j}\binom{d+1}{j}},$$

hence

$$\zeta_X(pT) = \prod_{j=0}^{d} (1 - p^j T)^{(-1)^{d-j+1}\binom{d}{j}} \prod_{j=0}^{d+1} \Delta(p^j T)^{(-1)^{d-j}\binom{d+1}{j}}.$$

Since Δ is entire, this shows that ζ_X is meromorphic on $\mathbb{C}_p$, i.e. $R_p = +\infty$. By the Borel–Dwork theorem, $\zeta_X(T) \in \mathbb{Q}(T)$, which concludes the proof of Theorem 1.4. □

Remark 3.11 (Cohomology?). With hindsight, one can interpret Dwork's construction cohomologically:

- Dwork works at the "cochain level" of (a p-adic cohomology of) $\mathbb{A}^d \setminus X$, or rather of the complement of the hypersurface $x_0 f(x) = 0$ in the torus;
- the operator α plays the role of (the inverse of) a "lift of Frobenius".

This point of view was developed by Dwork himself in his later work, and led to Monsky–Washnitzer and rigid cohomology.