LECTURE 7. THE LANG-WEIL ESTIMATE AND THE ZETA FUNCTION OF AN ARITHMETIC SCHEME

Our main goal in this lecture is to introduce the zeta function of an arithmetic scheme. In order to compute the abscissa of convergence of this function, we will use the Lang-Weil estimate. The proof of this estimate will make use of the Chow variety, which we review in the first section.

1. The Chow variety

We review in this section some basic facts concerning the Chow variety. For proofs and further properties, see [Kol, Chapter I].

Suppose first that K is an algebraically closed field, and $V \subseteq \mathbf{P} = \mathbf{P}^n_K$ is a closed subvariety of dimension r and degree d. Let $\mathbf{P}^* \simeq \mathbf{P}^n_K$ denote the dual projective space parametrizing the hyperplanes in $\mathbf{P}$. Consider the following incidence variety:

$$\Lambda := \{x, H_1, \ldots, H_{r+1}) \in V \times (\mathbf{P}^*)^{r+1} \mid x \in H_i \, \text{for all} \, i\}.$$

Let $f\colon \Lambda \to V$ and $g\colon \Lambda \to (\mathbf{P}^*)^{r+1}$ denote the morphisms induced by projections. It is clear that every $f^{-1}(x)$ is isomorphic to $(\mathbf{P}^{n-1}_K)^{r+1}$. Therefore Λ is irreducible, of dimension $r + (n-1)(r+1)$. On the other hand, since we can find $(H_1, \ldots, H_{r+1}) \in (\mathbf{P}^*)^{r+1}$ such that $V \cap H_1 \ldots \cap H_{r+1}$ is a nonempty finite set, it follows that g is generically finite onto its image W. Therefore W is an irreducible subvariety of $(\mathbf{P}^*)^{r+1}$ of codimension equal to $(r+1)n-(r+(r+1)(n-1)) = 1$, hence a divisor. One can show that $\mathcal{O}(W) = \mathcal{O}(d, d, \ldots, d)$. The *Caylay form* of V is an equation defining W. This is given by a polynomial R_V in $(r+1)$ sets of $(n+1)$ variables (unique up to a nonzero scalar), homogeneous of degree d in each set of variables. Note that W determines V: $x \in \mathbf{P}$ lies in V if and only if W contains all $(H_1, \ldots, H_{r+1}) \in (\mathbf{P}^*)^{r+1}$ such that $x \in H_i$ for all i. We thus have an injective map from the set of irreducible subvarieties of $\mathbf{P}$ of dimension r and degree d to $|\mathcal{O}(1, \ldots, 1)|$. The image $\mathrm{Chow}^{\circ}_K(n, d, r)$ is a quasiprojective variety, whose closure is the Chow variety $\mathrm{Chow}_K(n, d, r)$. In particular, the complement $\mathrm{Chow}_K(n, d, r) \smallsetminus \mathrm{Chow}^{\circ}_K(n, d, r)$ is a closed subset of $|\mathcal{O}(1, \ldots, 1)|$.

In fact, $\mathrm{Chow}_K(n, d, r)$ parametrizes effective r-cycles of degree d in $\mathbf{P}^n$, as follows. Consider an effective r-cycle $Z = \sum_i m_i V_i$ of degree d (that is, $\sum_i m_i \deg(V_i) = d$). Note that $R_Z := \prod_i R_{V_i}^{m_i}$ defines a divisor in $|\mathcal{O}(d, \ldots, d)|$. One can show that this gives a bijection between the set of cycles as above and $\mathrm{Chow}_K(n, d, r)$.

If k is an arbitrary field, let K be an algebraic closure of k. Every subscheme $Y \hookrightarrow \mathbf{P}^n_k$ of pure dimension r and degree d determines an r-cycle $[Y \times_k K]$ of degree d, hence a point $\Phi(Y) \in \mathrm{Chow}_K(n, d, r)$. Note that $\Phi(Y) \in \mathrm{Chow}^{\circ}_K(n, d, r)$ if and only if Y is generically reduced and geometrically irreducible (recall that Y is geometrically irreducible if $Y \times_k K$ is irreducible).

We will need two facts about Chow varieties. The first is that if $X \subseteq \mathbf{P}^n_K$ is an irreducible variety and $H \subset \mathbf{P}^n_K$ is a hyperplane that does not contain X, then $R_{[X\cap H]}(u_1,\ldots,u_r) = R_X(u_1,\ldots,u_r,h)$, where h is an equation of H (in the special case when $X \cap H$ is integral, this is an immediate consequence of the above definitions).

The second fact that we need is that one can do the above construction over $\operatorname{Spec}\mathbf{Z}$. More precisely, we have schemes $\mathrm{Chow}^{\circ}_{\mathbf{Z}}(n,d,r) \subset \mathrm{Chow}_{\mathbf{Z}}(n,d,r)$ such that for every algebraically closed field K, after taking the product with $\operatorname{Spec} K$ we obtain $\mathrm{Chow}^{\circ}_K(n,d,r) \subset \mathrm{Chow}_K(n,d,r)$. The upshot is that we can find e such that the subvariety

$$\mathrm{Chow}_K(n,d,r) \smallsetminus \mathrm{Chow}^{\circ}_K(n,d,r) \subset \mathbf{P}(\Gamma((\mathbf{P}^n_K)^* \times \ldots \times (\mathbf{P}^n_K)^*, \mathcal{O}(d,\ldots,d))^*)$$

is defined (set-theoretically) by finitely many equations of degree e with coefficients in the prime field of K (the key point is that e is independent of the field K).

2. The Lang-Weil estimate

In this section we work with a geometrically irreducible variety X defined over a finite field k. We show that if we assume that X is embedded in a projective space of fixed dimension, then we have universal estimates for $|X(k')|$, where k'/k is finite, in terms of $\dim(X)$, $\deg(X)$, and $|k'|$. More precisely, we show the following

Theorem 2.1. ([LaWe]) *Given nonnegative integers n, d, and r, with $d > 0$, there is a positive constant $A(n,d,r)$ such that for every finite field $k = \mathbf{F}_q$, and every geometrically irreducible subvariety $X \subseteq \mathbf{P}^n_k$ of dimension r and degree d, we have*

$$|\#X(k) - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + A(n,d,r)q^{r-1}. \tag{1}$$

The proof we give follows [LaWe], arguing by induction on r. The case of curves is a consequence of the Riemann hypothesis part of the Weil conjectures, that we have proved in Lecture 4. For the induction argument, we will need two lemmas. The first one gives a weaker bound than the assertion in the theorem.

Lemma 2.2. *Given n, d, and r as in Theorem 2.1, there is a positive constant $A_1(n,d,r)$ such that for every finite field $k = \mathbf{F}_q$, and every irreducible subvariety $X \subseteq \mathbf{P}^n_k$ of dimension r and degree $\leq d$, we have*

$$\#X(k) \leq A_1(n,d,r)q^r. \tag{2}$$

Proof. We argue by induction on n. If $n = 0$, then $X = \operatorname{Spec} k$, hence $r = 0$ and $d = 1$, and we may take $A_1(0,1,0) = 1$.

Suppose now that we have $A_1(n',d,r)$ for $n' \leq n$ that satisfy the condition in the lemma. Let $X \subseteq \mathbf{P}^{n+1}_k$ be an irreducible subvariety of dimension r and degree d. For every $\lambda \in k$, let $H_\lambda \subset \mathbf{P}^{n+1}_k$ be the hyperplane defined by $(x_1 - \lambda x_0 = 0)$, and let H_∞ be the hyerplane $(x_0 = 0)$. If X is degenerate, then it lies in some $\mathbf{P}^n_k$, and we get (2) if $A_1(n+1,d,r) \geq A_1(n,d,r)$. On the other hand, if X is nondegenerate, then each

$X_\lambda := (X \cap H_\lambda)_{\mathrm{red}}$ is a subvariety of $\mathbf{P}^n_k$ of degree $\leq d$, and of pure dimension $(r-1)$. In particular, if its irreducible components are $X^1_\lambda, \ldots, X^{m_\lambda}_\lambda$, then $m_\lambda \leq d$. Therefore

$$|X(k)| \leq \sum_{\lambda \in k \cup \{\infty\}} |X_\lambda(k)| \leq dA_1(n,d,r)(q+1)q^r \leq 2dA_1(n,d,r)q^{r+1}.$$

Therefore it is enough to take $A_1(n+1,d,r) = 2dA_1(n,d,r)$. □

Remark 2.3. Suppose that X is as in Lemma 2.2, but instead of being irreducible, we only assume that it has pure dimension r. In this case the number of irreducible components of X is bounded above by d. Therefore we deduce from the lemma that $\#X(k) \leq dA_1(n,d,r)q^r$.

If X is allowed to have components of smaller dimension, then the number of such components is not controlled by the degree. However, we still get

Corollary 2.4. *If X is an r-dimensional variety over $\mathbf{F}_q$, then there is $c_X > 0$ such that $\#X(\mathbf{F}_{q^e}) \leq c_X q^{re}$ for every $e \geq 1$.*

Proof. Arguing by induction on r, we see that it is enough to show that if $U \subseteq X$ is a dense affine open subset, then we have a similar bound for $\#U(\mathbf{F}_{q^e})$ (this follows since $\dim(X \smallsetminus U) < r$). It is of course enough to give such a bound for the closure $\overline{U}$ of U in some projective space. This in turn follows by applying Lemma 2.2 to each irreducible component of $\overline{U}$. □

Recall that we denote by $(\mathbf{P}^n_k)^*$ the dual projective space of $\mathbf{P}^n_k$. Note that a k-rational point of $(\mathbf{P}^n_k)^*$ corresponds to a k-hyperplane in $\mathbf{P}^n_k$, that is, to a hyperplane given by an equation $\sum_{i=0}^n a_i x_i = 0$, with all $a_i \in k$.

Lemma 2.5. *Given n, d, and r as in Theorem 2.1, with $r \geq 2$, there is a positive constant $A_2(n,d,r)$ such that for every nondegenerate geometrically irreducible subvariety $X \subseteq \mathbf{P}^n_k$ of dimension r and degree d, the number of k-hyperplanes H in $\mathbf{P}^n_k$ such that $H \cap X$ is either not geometrically irreducible, or not generically reduced, is $\leq A_2(n,d,r)q^{n-1}$.*

Proof. We make use of the definitions and notation introduced in §1. Let $K = \overline{k}$, and consider $V = \mathrm{Chow}_K(n-1,d,r-1) \smallsetminus \mathrm{Chow}^\circ_K(n-1,d,r-1)$. As we have mentioned, $V = W \times_k K$ for a closed subvariety $W \hookrightarrow \mathbf{P}^N_k$ that is the set-theoretic intersection of finitely many hypersurfaces Z_j of degree e (where N and e only depend on n, d, and r).

By construction, if $X \cap H$ is not geometrically irreducible or not generically reduced, then $\Phi(X \cap H) \in V$. Consider the morphism $(\mathbf{P}^n_K)^* \to \mathbf{P}^N_K$ defined over k that takes H to $R_X(\cdot, \ldots, \cdot, h)$, where h is an equation of H. Note that there is j such that $Z_j \times_k K$ does not contain the image of $(\mathbf{P}^n_K)^*$: indeed, since X is geometrically irreducible and $r \geq 2$, we know by Bertini's theorem that there is a hyperplane in $\mathbf{P}^n_K$ whose intersection with $X \times_k K$ is integral. The pull-back of this hypersurface $Z_j \times_k K$ to $(\mathbf{P}^n_K)^*$ is a hypersurface of degree e' defined over k, where e' only depends on n, d, and r. It follows from Lemma 2.2 (see also Remark 2.3) that if we take $A_2(n,d,r) = e'A_1(n,e',n-1)$, this satisfies the requirement in the lemma. □

We can now give the proof of the main result of this section.

Proof of Theorem 2.1. For every variety X, we denote by X_K the variety $X \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, K$, where K is a fixed algebraic closure of k, and for a morphism $\pi \colon Y \to X$, we denote by π_K the corresponding morphism $Y_K \to X_K$. It will be convenient to think of $X(k)$ as the points of X_K fixed under the suitable Frobenius morphism. We will use the fact that $\gamma_n := |\mathbf{P}^n(\mathbf{F}_q)| = \frac{q^{n+1}-1}{q-1}$ (see Lecture 2).

The proof is by induction on r. The case $r = 0$ is trivial, since in this case $|X(k)| = 1 = q^r$. Suppose that $r = 1$, and let $\pi \colon Y \to X$ be the normalization of X. The curve Y is nonsingular, projective, and geometrically connected (for the last assertion, note that we have a dense open subset U of Y such that U_K is irreducible). Therefore we may apply to Y the results in Lecture 4, and in particular the estimate for the number of rational points on Y given by the analogue of the Riemann hypothesis (see Lemma 3.3 and Theorem 3.1 in Lecture 4). We deduce that if g is the genus of Y, then

$$|\#Y(\mathbf{F}_q) - (q+1)| \leq 2gq^{1/2}. \tag{3}$$

Note that

$$|\#X(\mathbf{F}_q) - q| \leq |\#Y(\mathbf{F}_q) - (q+1)| + 1 + \sum_{x \in (X_K)_{\mathrm{sing}}} \deg(\pi_K^{-1}(x)). \tag{4}$$

In order to estimate the sum in (4), as well as the genus of Y, let us consider a general projection of X_K to $\mathbf{P}^2_K$, which gives a birational morphism $\varphi \colon X_K \to C$, where C is an ireducible plane curve of degree d. Let $\psi = \varphi \circ \pi_K$. Note that if $x \in C$ is a smooth point, then ψ is an isomorphism around x, hence $\varphi^{-1}(x)$ is contained in the smooth locus of X_K. Therefore

$$\sum_{x \in (X_K)_{\mathrm{sing}}} \deg(\pi_K^{-1}(x)) \leq \sum_{x \in C_{\mathrm{sing}}} \deg(\psi^{-1}(x)). \tag{5}$$

For every $x \in C_{\mathrm{sing}}$ we have $\deg(\psi^{-1}(x)) \leq d$: if L is a hyperplane in $\mathbf{P}^2_K$ passing through x and not containing C, then $\deg(\psi^{-1}(x)) \leq \deg(\psi^{-1}(C \cap H)) = d$.

The arithmetic genus of C is $h^1(C, \mathcal{O}_C) = \frac{(d-1)(d-2)}{2}$. We have a short exact sequence of sheaves

$$0 \to \mathcal{O}_C \to \psi_*(\mathcal{O}_{Y_K}) \to \oplus_{x \in C_{\mathrm{sing}}} \widetilde{\mathcal{O}_{C,x}}/\mathcal{O}_{C,x} \to 0,$$

where $\widetilde{\mathcal{O}_{C,x}}$ is the integral closure of $\mathcal{O}_{C,x}$. If $\delta_x = \mathrm{length}(\widetilde{\mathcal{O}_{C,x}}/\mathcal{O}_{C,x})$, then we get from the long exact sequence in cohomology that $g = p_a(C) - \sum_{x \in C_{\mathrm{sing}}} \delta_x$. This gives $g \leq p_a(C) = \frac{(d-1)(d-2)}{2}$. We also obtain $\sum_{x \in C_{\mathrm{sing}}} \delta_x \leq \frac{(d-1)(d-2)}{2}$. Since $\delta_x \geq 1$ for every singular point $x \in C$, we deduce that $\#C_{\mathrm{sing}} \leq \frac{(d-1)(d-2)}{2}$. We deduce using (3), (4) and (5) that

$$|\#X(\mathbf{F}_q) - q| \leq (d-1)(d-2)q^{1/2} + \frac{d(d-1)(d-2)}{2} + 1,$$

hence we are done in the case $r = 1$ by taking $A(n, d, 1) = \frac{d(d-1)(d-2)}{2} + 1$.

Suppose now that we can find $A(n, d, r)$ as in the theorem for $r \geq 1$, and let us find $A(n, d, r+1)$. Arguing also by induction on n, we may assume that we can find

$A(n-1,d,r+1)$ as required (note that the cases $n=0$ and $n=1$ are clear). Let X be a geometrically irreducible subvariety of $\mathbf{P}^n_k$, of degree d and dimension $(r+1)$. If X is degenerate, then X lies in some $\mathbf{P}^{n-1}_k$, in which case we get the bound in the theorem if we take $A(n,d,r+1) \geq A(n-1,d,r+1)$. Assume henceforth that X is nondegenerate.

In order to avoid messy computations, we introduce the following notation: given two real numbers a and b, we write $a \leq b + o(q^r)$ if there is an inequality $a \leq b + C \cdot q^r$, where C is a positive constant that is only allowed to depend on n, d, and r. Note that we have $a \leq b + o(q^r)$ if and only if $\gamma_{n-1}a \leq \gamma_{n-1}b + o(q^{r+n-1})$.

Let $W \subseteq X \times (\mathbf{P}^n_k)^*$ be the subvariety consisting of the pairs (x,H) such that $x \in H$. The projections onto the two components give the maps $W \to X$ and $W \to (\mathbf{P}^n_k)^*$. The key idea is to compute in two ways $\#W(\mathbf{F}_q)$, using these two morphisms. Note that for every $x \in X(\mathbf{F}_q)$, the number of $\mathbf{F}_q$-hyperplanes containing x is $\#\mathbf{P}^{n-1}(\mathbf{F}_q) = \gamma_{n-1}$. Therefore

$$|W(\mathbf{F}_q)| = \gamma_{n-1} \cdot |X(\mathbf{F}_q)|. \tag{6}$$

On the other hand, using the morphism $W \to (\mathbf{P}^n_k)^*$, we see that

$$|W(\mathbf{F}_q)| = \sum_{H \in (\mathbf{P}^n)^*(k)} |(X \cap H)(\mathbf{F}_q)|. \tag{7}$$

We break the sum in (7) into two sums, in the first one S_1 collecting all H such that $H \cap X$ is either not geometrically irreducible, or not generically reduced, and in the second one S_2, collecting the remaining terms. Note that for every H that contributes to S_1, the subvariety $(H \cap X)_{\mathrm{red}} \subseteq H \simeq \mathbf{P}^{n-1}_k$ has degree $\leq d$, and pure dimension r. In particular, the number of irreducible components of $(H \cap X)_{\mathrm{red}}$ is $\leq d$, and each has degree $\leq d$. It follows from Lemma 2.2 that $|(X \cap H)(\mathbf{F}_q)| \leq o(q^r)$. On the other hand, we can use Lemma 2.5 to bound the number of such hyperplanes by $A_2(n,d,r+1)q^{n-1}$, hence $S_1 \leq o(q^{r+n-1})$, and therefore

$$\frac{1}{\gamma_{n-1}} S_1 \leq o(q^r). \tag{8}$$

Note, in particular, that this sum can be absorbed in the error term.

On the other hand, if $H \cap X$ is geometrically irreducible and generically reduced, then $(H \cap X)_{\mathrm{red}}$ is a variety of dimension r and degree d, and we can estimate the number of points in $(X \cap H)(\mathbf{F}_q)$ by induction: we have

$$|\#(X \cap H)(\mathbf{F}_q) - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + o(q^{r-1}). \tag{9}$$

Let δ be the number of hyperplanes that contribute to S_2. Note that

$$\left| \frac{1}{\gamma_{n-1}} S_2 - q^{r+1} \right| \leq \left| \frac{1}{\gamma_{n-1}} (S_2 - \delta q^r) \right| + \left| \frac{\delta q^r}{\gamma_{n-1}} - q^{r+1} \right|. \tag{10}$$

By Lemma 2.5 we have $|\delta - \gamma_n| \leq o(q^{n-1})$. This implies $\frac{\delta}{\gamma_{n-1}} \leq o(q)$ and

$$\left| \frac{\delta q^r}{\gamma_{n-1}} - q^{r+1} \right| \leq \frac{|\delta - \gamma_n| \cdot q^r}{\gamma_{n-1}} + \left| \frac{\gamma_n q^r}{\gamma_{n-1}} - q^{r+1} \right| \leq o(q^r).$$

On the other hand, it follows from (9) that

$$\left|\frac{1}{\gamma_{n-1}}(S_2-\delta q^r)|\right| \leq (d-1)(d-2)q^{r+\frac{1}{2}}+o(q^r), \tag{11}$$

hence

$$\left|\frac{1}{\gamma_{n-1}}S_2-q^{r+1}\right| \leq (d-1)(d-2)q^{r+\frac{1}{2}}+o(q^r).$$

By combining this with (8), we get the existence of $A(n,d,r+1)$, which completes the proof of the theorem. ☐

3. Estimating the number of points on arbitrary varieties

We explain in this section how to estimate the number of k-rational points on X when X is not assumed to be geometrically irreducible. In this section, however, the constant in the estimate will be allowed to depend on X.

Let us first introduce some notation. Suppose that $k=\mathbf{F}_q$ is a finite field, and $X\hookrightarrow \mathbf{P}^n_k$ is an irreducible closed subvariety of degree d and dimension r. We denote by $\Gamma=\{W_1,\ldots,W_m\}$ the set of irreducible components of $X_{\overline{k}}=X\times_k\overline{k}$. It follows from Proposition 2.4 in the Appendix that $G=G(\overline{k}/k)$ acts transitively on Γ. Let $G'\subseteq G$ be the stabilizer of any of the elements of Γ with respect to this action. Note that $G'=G(\overline{k}/\mathbf{F}_{q^\ell})$, where $\mathbf{F}_{q^\ell}$ is the smallest extension of $\mathbf{F}_q$ over which one (hence all) of the W_i is defined (see Proposition 2.6 in the Appendix, and its proof). Since G/G' has ℓ elements, it follows that $\ell=m$.

Proposition 3.1. *Let n,d,r be nonnegative integers, with $d>0$. Given any $k=\mathbf{F}_q$ and X as above, there are positive constants c_X and c'_X such that if m is as above, then for every $e\geq 1$ we have*

$$|\#X(\mathbf{F}_{q^e})-mq^{er}|\leq\frac{(d-m)(d-2m)}{m}q^{e(r-\frac{1}{2})}+c_Xq^{e(r-1)}\ \textit{if}\ m|e,\ \textit{and}$$

$$\#X(\mathbf{F}_{q^e})\leq c'_Xq^{e(r-1)},\ \textit{if}\ m\not|e.$$

Furthermore, if X is smooth over $\mathbf{F}_q$, then we may take $c'_X=0$ and c_X only to depend on n, d, and r (but not on X or on k).

Proof. For every $e\geq 1$, let $X_e:=X\times_{\mathbf{F}_q}\mathbf{F}_{q^e}$. If $m|e$, then X_e has m irreducible components $V_1,\ldots,V_m$, and each of them is geometrically irreducible. Furthermore, we have $\dim(V_i)=r$ and $\deg(V_i)=\frac{d}{m}$ for every i. Note that each $V_i\cap V_j$ is the extension to $\mathbf{F}_{q^e}$ of the corresponding intersection of irreducible components defined over $\mathbf{F}_{q^m}$, and has dimension $<r$ when $i\neq j$. Moreover, if X is smooth, then $V_i\cap V_j=\emptyset$ for $i\neq j$. Since

$$|\#X(\mathbf{F}_{q^e})-mq^{er}|\leq\sum_{i=1}^m|\#V_i(\mathbf{F}_{q^e})-q^{er}|+\sum_{i<j}\#(V_i\cap V_j)(\mathbf{F}_{q^e}),$$

we deduce the first estimate in the proposition from Theorem 2.1 and Corollary 2.4. Moreover, when X is smooth, it is enough to take $c_X=d\cdot\max_{1\leq d'\leq d}A(n,d',r)$, where we use the notation in Theorem 2.1.

Suppose now that m does not divide e. Recall that if $F = \mathrm{Frob}_{X,q} \times \mathrm{Id}$, then $X(\mathbf{F}_{q^e})$ can be identified with the fixed points of F^e on $X_{\overline{k}}$. By assumption, none of $W_1, \ldots, W_m$ is fixed by $G(\overline{k}/\mathbf{F}_{q^e}) \subseteq G$. Note also that an irreducible subset $Z \subset X_{\overline{k}}$ is fixed by $G(\overline{k}/\mathbf{F}_{q^e})$ if and only if $F^e(Z) \subseteq Z$ (see the proof of Proposition 2.6 in the Appendix). It follows that if $u \in W_i$ is fixed by F^e, then $u \in \bigcap_j F^{ej}(W_i)$, which is a proper closed subvariety of W_i, defined over $\mathbf{F}_{q^e}$ (empty when X is smooth). Since its dimension is $\leq r-1$, we conclude by Remark 2.3 that we can find c'_X as required (note that the varieties $\bigcap_j F^{ej}(W_i)$ only depend on the congruence class of e mod ℓ, hence we only get finitely many such varieties). This completes the proof of the proposition. □

It is now straightforward to estimate the number of $\mathbf{F}_{q^e}$-rational points on an arbitrary variety X over $\mathbf{F}_q$. Let $X_1, \ldots, X_\ell$ be the irreducible components of X of maximal dimension r, and let m_i be the number of irreducible components of $X_i \times_k \overline{k}$.

Proposition 3.2. *For every X as above, there are positive constants α_X, α'_X such that for every $e \geq 1$, if we put $a_e = \sum_{m_i|e} m_i$, then*

$$|\#X(\mathbf{F}_{q^e}) - a_e q^{er}| \leq \alpha_X q^{e(r-\frac{1}{2})} \text{ if } a_e > 0, \text{ and}$$

$$\#X(\mathbf{F}_{q^e}) \leq \alpha'_X q^{e(r-1)}, \text{ otherwise.}$$

Proof. Let $U_i \subseteq X_i$ be affine open subsets that do not intersect the other irreducible components of X, and let $U = \bigcup_{i=1}^{\ell} U_i$. Since $\dim(X \smallsetminus U) < r$, it follows from Corollary 2.4 that it is enough to prove the assertion in the proposition for U. If $\overline{U_i}$ is the closure of U_i in some projective space, and $\overline{U} = \bigsqcup_{i=1}^{\ell} \overline{U_i}$, it follows as before that it is enough to prove the estimate for $\overline{U}$. This follows by applying Proposition 3.1 to each of the $\overline{U_i}$. □

4. Review of Dirichlet series

In this section we collect some basic facts about Dirichlet series. In the first part we follow [Se, Chapter VI, §2]. A *Dirichlet series* is a series of functions of the form

$$\sum_{n\geq 1} \frac{a_n}{n^s}, \tag{12}$$

where $a_n \in \mathbf{C}$, and s varies over $\mathbf{C}$. The following proposition is the basic result that controls the convergence of Dirichlet series.

Proposition 4.1. *If the series $\sum_{n\geq 1} \frac{a_n}{n^s}$ converges for $s = s_0$, then it converges uniformly in every domain of the form:* $\mathrm{Re}(s - s_0) \geq 0$, $\mathrm{Arg}(s - s_0) \leq \alpha$, *where* $0 < \alpha < \pi/2$.

Proof. Let us write $s - s_0 = z = x + yi$, with $x, y \in \mathbf{R}$. It is enough to show that the sequence of functions $\left(\sum_{n=1}^{m} \frac{a_n}{n^s}\right)_m$ is uniformly Cauchy in any domain with $x \geq 0$, and $|z| \leq Mx$. Suppose that $\varepsilon > 0$ is given. By hypothesis, we can find m such that $|A_p| \leq \varepsilon$ for every p, where $A_p = \sum_{n=m+1}^{m+p} \frac{a_n}{n^{s_0}}$.

We may of course assume that $x > 0$, and we write

$$\sum_{n=m+1}^{m+p} \frac{a_n}{n^s} = \sum_{n=m+1}^{m+p} \frac{a_n}{n^{s_0}} \cdot \frac{1}{n^z} = \frac{A_p}{(m+p)^z} + \sum_{\ell=1}^{p-1} A_\ell \left(\frac{1}{(m+\ell)^z} - \frac{1}{(m+\ell+1)^z} \right) \tag{13}$$

We now bound

$$\left| \frac{1}{(m+\ell)^z} - \frac{1}{(m+\ell+1)^z} \right| = \left| z \cdot \int_{\log(m+\ell)}^{\log(m+\ell+1)} e^{-tz} dt \right| \leq |z| \cdot \int_{\log(m+\ell)}^{\log(m+\ell+1)} e^{-tx} dt$$
$$= \frac{|z|}{x} \left(\frac{1}{(m+\ell)^x} - \frac{1}{(m+\ell+1)^x} \right).$$

Using this bound and the condition on $|A_\ell|$, we conclude that that

$$\left| \sum_{n=m+1}^{m+p} \frac{a_n}{n^s} \right| \leq \frac{\varepsilon}{(m+p)^x} + \varepsilon \frac{|z|}{x} \cdot \sum_{\ell=1}^{p-1} \left(\frac{1}{(m+\ell)^x} - \frac{1}{(m+\ell+1)^x} \right) \leq \varepsilon(1+M).$$

This completes the proof of the proposition. □

The *abscissa of convergence* of the series $\sum_{n\geq 1} \frac{a_n}{n^s}$ is

$$\rho = \inf\{\mathrm{Re}(s) \mid \sum_{n\geq 1} \frac{a_n}{n^s} \text{ is convergent at } s\}.$$

It follows from Proposition 4.1 that $\sum_{n\geq 1} \frac{a_n}{n^s}$ converges uniformly on every compact subset contained in $\{s \mid \mathrm{Re}(s) > \rho\}$ (this is called the half-plane of convergence of the series). In particular, it defines a holomorphic function on this half-plane. It follows from definition that the series is divergent at every s with $\mathrm{Re}(s) < \rho$. Note that $\rho = \infty$ if and only if the series diverges everywhere, and $\rho = -\infty$ if and only if the series is everywhere convergent.

Example 4.2. Suppose that $\alpha \in \mathbf{R}$ is such that the sequence $|a_n|/n^\alpha$ is bounded above. In this case the abscissa of convergence ρ of $\sum_{n\geq 1} \frac{a_n}{n^s}$ satisfies $\rho \leq 1 + \alpha$. Furthermore, suppose that $a_n \in \mathbf{R}_{\geq 0}$ and $\liminf_{n\to\infty} \frac{a_n}{n^\alpha} > 0$; in this case $\rho = \alpha + 1$. Both assertions follow from the fact that for $p \in \mathbf{R}$, the series $\sum_{n\geq 1} \frac{1}{n^p}$ is convergent if and only if $p > 1$.

Example 4.3. If we consider the Dirichlet series $\sum_{n\geq 1} \frac{1}{n^s}$ defining the Riemann zeta function $\zeta(s)$, then the abscissa of convergence is $\rho = 1$.

Proposition 4.4. *Suppose that $f(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ and $g(s) = \sum_{n\geq 1} \frac{b_n}{n^s}$ are both convergent for every s with $\mathrm{Re}(s) > \alpha$. If $f(s) = g(s)$ for every such s, then $a_n = b_n$ for every $n \geq 1$.*

Proof. By considering $h = \sum_{n\geq 1} \frac{a_n - b_n}{n^s}$, we see that it is enough to prove the assertion when all b_n are zero. In this case, we prove by induction on n that $a_n = 0$. Suppose that $a_1 = \ldots = a_{n-1} = 0$, and that $f(s) = 0$ for all s with $\mathrm{Re}(s) > \alpha$. It follows from Proposition 4.1 that the series of functions $\sum_{m\geq n} \frac{a_m n^s}{m^s}$ is uniformly convergent (to 0, by our assumption) for $s \in \mathbf{R}$, with $s > \rho$. For every $m > n$ we have $\lim_{s\to\infty} \frac{a_m n^s}{m^s} = 0$, hence $a_n = \lim_{s\to\infty} \sum_{m\geq n} \frac{a_m n^s}{m^s} = 0$. This completes the induction step.

□

As we have seen in Example 4.2, if $|a_m| \leq Cm^\alpha$ for all m, then the abscissa of convergence of the Dirichlet series $\sum_{n\geq 1} \frac{a_n}{n^s}$ is $\leq 1+\alpha$. The following proposition improves this upper bound when $\alpha \geq 0$ and when we have the similar bound for all sums $a_1+\ldots+a_m$.

Proposition 4.5. *If $\alpha \in \mathbf{R}_{\geq 0}$ is such that $|\sum_{n=1}^m a_n| \leq Cm^\alpha$ for all m, then the Dirichlet series $\sum_{n\geq 1} \frac{a_n}{n^s}$ is convergent in the half-plane $\{s \mid \mathrm{Re}(s) > \alpha\}$.*

Proof. We follow a similar argument to that used in the proof of Proposition 4.1. Note that we have $|\sum_{n=m+1}^{m+\ell} a_n| \leq C((m+\ell)^\alpha + m^\alpha) \leq 2C(m+\ell)^\alpha$ for all m and ℓ. Consider $s \in \mathbf{C}$ with $\mathrm{Re}(s) > \alpha$, and let us write $s = x+yi$, with $x, y \in \mathbf{R}$. If we put $A_p = \sum_{n=m+1}^{m+p} a_n$ for all p, then we have

$$\left|\sum_{n=m+1}^{m+p} \frac{a_n}{n^s}\right| = \left|\frac{A_p}{(m+p)^s} + \sum_{\ell=1}^{p-1} A_\ell \left(\frac{1}{(m+\ell)^s} - \frac{1}{(m+\ell+1)^s}\right)\right|$$

$$\leq \frac{|A_p|}{(m+p)^x} + \sum_{\ell=1}^{p-1} |A_\ell s| \cdot \left|\int_{\log(m+\ell)}^{\log(m+\ell+1)} e^{-ts} dt\right| \leq \frac{2C}{(m+p)^{x-\alpha}} + \sum_{\ell=1}^{p-1} |s| \int_{\log(m+\ell)}^{\log(m+\ell+1)} |A_\ell| e^{-tx} dt.$$

Since $|A_\ell| \leq 2C(m+\ell)^\alpha$, it follows that $|A_\ell| \leq 2Ce^{\alpha t}$ for $t \geq \log(m+\ell)$. Therefore

$$\sum_{\ell=1}^{p-1} \int_{\log(m+\ell)}^{\log(m+\ell+1)} |A_\ell| e^{-tx} dt \leq 2C \cdot \sum_{\ell=1}^{p-1} \int_{\log(m+\ell)}^{\log(m+\ell+1)} e^{t(\alpha-x)} dt = 2C \cdot \int_{\log(m+1)}^{\log(m+p)} e^{t(\alpha-x)} dt$$

$$= \frac{2C}{x-\alpha}\left(\frac{1}{(m+1)^{x-\alpha}} - \frac{1}{(m+p)^{x-\alpha}}\right).$$

We thus conclude that

$$\left|\sum_{n=m+1}^{m+p} \frac{a_n}{n^s}\right| \leq \frac{2C}{(m+p)^{x-\alpha}} + \frac{2C|s|}{x-\alpha}\left(\frac{1}{(m+1)^{x-\alpha}} - \frac{1}{(m+p)^{x-\alpha}}\right),$$

and for fixed s this can be made arbitrarily small by taking m large enough. This shows that $\sum_{n\geq 1} \frac{a_n}{n^s}$ is convergent. $\square$

Proposition 4.6. *The Riemann zeta function has a meromorphic continuation to the half-space $\{s \mid \mathrm{Re}(s) > 0\}$, with a unique pole at $s = 1$, which is simple, and with residue 1.*

Proof. The trick is to consider the following auxiliary Dirichlet series

$$\zeta_r(s) = \sum_{n\geq 1} \frac{a_{n,r}}{n^s} = \sum_{r \nmid m} \frac{1}{m^s} - \sum_{r|m} \frac{r-1}{m^s},$$

for every $r \geq 2$. It is clear that $\sum_{n=1}^m a_{n,r} \in \{0, 1, \ldots, r-1\}$, hence Proposition 4.5 applies to give that $\zeta_r(s)$ is a holomorphic function on $\{s \mid \mathrm{Re}(s) > 0\}$. It is clear that for $\mathrm{Re}(s) > 1$ we have $\zeta_r(s) + r^{1-s}\zeta(s) = \zeta(s)$, hence

$$\zeta(s) = \frac{\zeta_r(s)}{1 - r^{1-s}}.$$

This shows that ζ has a meromorphic continuation to the half-plane $\{s \mid \mathrm{Re}(s) > 0\}$. Furthermore, every pole in this region is simple, and it is of the form $1 + \frac{2m\pi i}{\log(r)}$, for some $m \in \mathbf{Z}$. By considering $r = 2$ and $r = 3$, we see that in fact, the only possible pole of ζ in this region is at $s = 1$.

Note that the residue at 1 is $\frac{\zeta_2(1)}{\log(2)}$. Recall that we have $\log(1+x) = \sum_{n\geq 1}(-1)^{n-1}\frac{x^n}{n}$ for $|x| < 1$. The series is convergent at $x = 1$, hence by Abel's theorem the sum for $x = 1$ is equal to $\lim_{x\in\mathbf{R},x\to 1}\log(x) = \log(2)$. Therefore $\log(2) = \sum_{n\geq 1}\frac{(-1)^{n-1}}{n} = \zeta_2(1)$, and we see that the residue of ζ at $s = 1$ is 1. $\square$

In fact, ζ can be meromorphically extended to $\mathbf{C}$, and the only pole is $s = 1$. Furthermore, after multiplication by a suitable factor involving the Γ-function, ζ satisfies a functional equation. We refer to [Lang, Chapter XIII] for the statement of the functional equation, for proofs and generalizations.

In the case of Dirichlet series with nonnegative coefficients, the sum has a singularity at the real point on the boundary of the half-plane of convergence. More precisely, we have the following.

Proposition 4.7. *Consider a Dirichlet series $\sum_{n\geq 1}\frac{a_n}{n^s}$, with $a_n \in \mathbf{R}_{\geq 0}$ for all n. If the abscissa of convergence ρ is finite, then the sum $f(s)$ of this series can not be analytically extended to a holomorphic function in the neighborhood of $s = \rho$.*

Proof. Let us denote $f(s) = \sum_{n\geq 1}\frac{a_n}{n^s}$ for $\mathrm{Re}(s) > \rho$, and suppose that f has an analytic continuation to a neighborhood of ρ. In this case there is $\varepsilon > 0$ such that f is holomorphic inside the disc $\{s \mid |s - (\rho+1)| < 1 + 2\varepsilon\}$. Therefore in the interior of this disc we have the Taylor expansion

$$f(s) = \sum_{i\geq 0}\frac{f^{(i)}(\rho+1)}{i!}(s-\rho-1)^i. \tag{14}$$

On the other hand, since the series converges uniformly in the half-space $\{s \mid \mathrm{Re}(s) > \rho\}$, we can differentiate term-by-term in this region to get

$$f^{(i)}(s) = \sum_{n\geq 1}\frac{a_n}{n^s}(-\log n)^i. \tag{15}$$

By taking $s = \rho + 1$, we get

$$f^{(i)}(\rho+1) = \sum_{n\geq 1}\frac{a_n}{n^{\rho+1}}(-\log n)^i. \tag{16}$$

Computing $f(\rho - \varepsilon)$ via (14), and using also (16), we deduce that

$$f(\rho-\varepsilon) = \sum_{i\geq 0}\frac{f^{(i)}(\rho+1)}{i!}(-1-\varepsilon)^i = \sum_{i\geq 0}\sum_{n\geq 1}\frac{a_n}{n^{\rho+1}}\frac{((1+\varepsilon)\log n)^i}{i!}.$$

Since this is a convergent double series with nonnegative terms, we may change the order of summation, and deduce that

$$\sum_{n\geq 1}\frac{a_n}{n^{\rho+1}}\sum_{i\geq 0}\frac{((1+\varepsilon)\log n)^i}{i!}=\sum_{n\geq 1}\frac{a_n}{n^{\rho-\varepsilon}}$$

is convergent. Hence our Dirichlet series is convergent for $s=\rho-\varepsilon$, a contradiction. $\square$

Suppose now that $\sum_{n\geq 1}\frac{a_n}{n^s}$ is an arbitrary Dirichlet series. The *abscissa of absolute convergence* ρ^+ of this series is the abscissa of convergence of $\sum_{n\geq 1}\frac{|a_n|}{n^s}$. It is clear that if ρ is the abscissa of convergence of the given Dirichlet series, then $\rho\leq\rho^+$. One can show that $\rho^+\leq\rho+1$, hence in particular $\rho<\infty$ if and only if $\rho^+<\infty$. We will not use this result, so we simply refer to [MoVa, Theorem 1.4] for a proof.

We now want to show that in the half-plane of absolute convergence, under suitable multiplicative properties, we can decompose the sum of the Dirichlet series as an Euler product. Before doing this, let us recall a basic lemma concerning infinite products. Recall that if $(a_n)_{n\geq 1}$ is a sequence of complex numbers, then the product $\prod_{n\geq 1}(1+a_n)$ is *absolutely convergent* if the series $\sum_{n\geq 1}a_n$ is absolutely convergent.

Lemma 4.8. *If the product $\prod_{n\geq 1}(1+a_n)$ is absolutely convergent, then it is convergent. Furthermore, the product is independent of the order of the factors, and it is zero if and only if one of the factors is zero.*

It is clear that if $(a_i)_{i\in I}$ is any set of complex numbers indexed by a countable set, then it makes sense to say that the product $\prod_{i\in I}(1+a_i)$ is absolutely convergent. The lemma implies that in this case the product $\prod_{i\in I}(1+a_i)$ is well-defined.

Proof. The hypothesis implies in particular that $\lim_{n\to\infty}a_n=0$. Therefore there is n_0 such that $|a_n|<1$ for all $n\geq n_0$. For all statements in the lemma we may ignore finitely many of the factors, hence we may assume that $n_0=1$. Since

$$\log\left(\prod_{i=1}^{n}(1+a_i)\right)=\sum_{i=1}^{n}\log(1+a_i),$$

the first two assertions in the lemma follow if we show that the series $\sum_{i\geq 1}|\log(1+a_i)|$ is convergent. For every u with $|u|<1$, we have

$$|\log(1+u)|=\left|\sum_{n\geq 1}(-1)^{n-1}\frac{u^n}{n}\right|\leq\sum_{n\geq 1}\frac{|u|^n}{n}=-\log(1-|u|)=\log(1+w)\leq w,$$

where $1+w=(1-|u|)^{-1}$. Note that $w=\frac{|u|}{1-|u|}\leq\frac{1}{2}|u|$ if $|u|\leq\frac{1}{2}$, hence $|\log(1+u)|\leq\frac{1}{2}|u|$ when $|u|\leq\frac{1}{2}$. Since $|a_i|\leq\frac{1}{2}$ for $i\gg 0$, the hypothesis that $\sum_{i\geq 1}|a_i|$ is convergent implies that $\sum_{i\geq 1}|\log(1+a_i)|$ is convergent.

For the last assertion in the lemma, note that if $\sum_{n\geq 1}\log(1+a_n)=u$, then the product $\prod_{n\geq 1}(1+a_n)$ is equal to $\exp(u)$, hence it is nonzero. $\square$

Remark 4.9. Note that the infinite product $\prod_{n\geq 1}(1+|a_n|)$ is convergent if and only if it is absolutely convergent. Indeed, the "if" part follows from the above lemma, while the "only if" part is a consequence of the fact that for every n

$$\sum_{i=1}^{n}|a_i| \leq \prod_{i=1}^{n}(1+|a_i|) \leq \prod_{i=1}^{\infty}(1+|a_i|).$$

This implies that the infinite product $\prod_{n\geq 1}(1+a_n)$ is absolutely convergent if and only if the product $\prod_{n\geq 1}(1+|a_n|)$ is convergent, which is the case if and only if the series with nonnegative terms $\sum_{n\geq 0}\log(1+|a_n|)$ is convergent.

Exercise 4.10. Consider $(a_{m,n})_{m,n\geq 1}$, with $a_{m,n}\in \mathbf{C}$. Show that if each infinite product $\prod_{n\geq 1} a_{m,n}$ is absolutely convergent and $b_m = \prod_{n\geq 1} a_{m,n}$, then the following are equivalent

i) The product $\prod_{m\geq 1} b_m$ is absolutely convergent.
ii) The product $\prod_{m,n\geq 1} a_{m,n}$ is absolutely convergent.

Furthermore, show that in this case $\prod_{m,n\geq 1} a_{m,n} = \prod_{m\geq 1} b_m$.

We say that a sequence $(a_n)_{n\geq 1}$ is *multiplicative* if $a_{mn} = a_m a_n$ whenever m and n are relatively prime. In this case we have $a_1\cdot a_m = a_m$ for every m. In particular, we either have $a_m = 0$ for all m, or $a_1 = 1$. In order to avoid trivial cases, we always assume that $a_1 = 1$.

Proposition 4.11. *Let $(a_n)_{n\geq 1}$ be a multiplicative sequence, and consider the Dirichlet series $f = \sum_{n\geq 1}\frac{a_n}{n^s}$. If the abscissa of absolute convergence ρ^+ is not $+\infty$, then for every s with $\mathrm{Re}(s) > \rho^+$ the following product over all positive prime integers*

$$\prod_{p}\left(\sum_{m\geq 0}\frac{a_{p^m}}{p^{ms}}\right) \tag{17}$$

is absolutely convergent, and it is equal to $f(s)$. Furthermore, if we assume that all $a_n\geq 0$ and we know that the product (17) is convergent for every $s_0\in\mathbf{R}$ with $s_0 > \alpha$, then $\rho = \rho^+ \leq \alpha$.

Proof. Let $s\in\mathbf{C}$ be such that $\mathrm{Re}(s) > \rho^+$. By assumption, the series $\sum_{n\geq 1}\frac{a_n}{n^s}$ is absolutely convergent. In particular, we see that $\sum_p\sum_{m\geq 1}\frac{|a_{p^m}|}{p^{ms}}$ is absolutely convergent, hence the product (17) is absolutely convergent.

Let $f_p(s)$ be the factor in (17) corresponding to the prime p. If $p_1,\ldots,p_r$ are the first r prime integers, then the series

$$S_r := \sum_{n=p_1^{j_1}\cdots p_r^{j_r}}\frac{a_n}{n^s}$$

is absolutely convergent, where n varies over the positive integers whose prime factors are among $p_1,\ldots,p_r$. The sum of this series is equal to $\prod_{i=1}^{r} f_{p_i}(s)$. By assumption, S_r converges to $f(s)$, hence we get the assertion in the proposition.

Suppose now that all $a_m \geq 0$, and that $\prod_p \left(\sum_{m\geq 0} \frac{a_{p^m}}{p^{ms_0}}\right)$ is convergent whenever $s_0 \in \mathbf{R}$ with $s_0 > \alpha$. Let us fix such s_0. With the above notation, we see that S_r is finite, and $S_r \leq \prod_p \left(\sum_{m\geq 0} \frac{a_{p^m}}{p^{ms_0}}\right)$. Therefore the sequence $(S_r)_{r\geq 1}$ is convergent, and its limit is clearly equal to $\sum_{n\geq 1} \frac{a_n}{n^{s_0}}$. This implies that $\rho = \rho^+ \leq \alpha$. □

Corollary 4.12. *Under the assumptions in the above proposition, suppose that the sequence $(a_n)_{n\geq 1}$ is* strongly multiplicative, *in the sense that $a_{mn} = a_m a_n$ for all positive integers m and n, and $a_0 = 1$. In this case we have the decomposition*

$$\sum_{n\geq 1} \frac{a_n}{n^s} = \prod_p \frac{1}{1 - a_p p^{-s}}$$

for every $s \in \mathbf{C}$ with $\mathrm{Re}(s) > \rho^+$.

Proof. The assertion follows from the formula in Proposition 4.11, noting that for every prime p we have

$$\sum_{m\geq 0} \frac{a_{p^m}}{p^{ms}} = \sum_{m\geq 0} \frac{a_p^m}{p^{ms}} = \frac{1}{1 - a_p p^{-s}}.$$

□

Example 4.13. In the case of the Riemann zeta function we have $\rho^+ = \rho = 1$, and we get the product decomposition

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

for every $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. Note also that since the product is absolutely convergent, it follows from Lemma 4.8 that $\zeta(s) \neq 0$ for every s with $\mathrm{Re}(s) > 0$.

Let us recall the notion of product of Dirichlet series. Given ℓ Dirichlet series $f_i = \sum_{n\geq 1} \frac{a_{n,i}}{n^s}$ for $1 \leq i \leq \ell$, let us consider the *product* of the f_i defined by $g = \sum_{n\geq 1} \frac{b_n}{n^s}$, where $b_n = \sum_{d_1\cdots d_\ell = n} a_{d_1,1} \cdots a_{d_\ell,\ell}$, the sum being over all tuples of positive integers $(d_1, \ldots, d_\ell)$ such that $d_1 \cdots d_\ell = n$.

Proposition 4.14. *With the above notation, the following hold:*

i) *We have the following relation between the abscissas of absolute convergence*
$$\rho^+(g) \leq \max_i \rho^+(f_i),$$
and for every $s \in \mathbf{C}$ with $\mathrm{Re}(s) > \max_i \rho^+(f_i)$, we have $g(s) = \prod_{i=1}^{\ell} f_i(s)$.

ii) *If each sequence $(a_{n,i})_{n\geq 1}$ is multiplicative, and if we consider the Euler product decompositions $f_i = \prod_p f_i^{(p)}$, then the sequence $(b_n)_{n\geq 1}$is multiplicative, and the Euler product decomposition of g is given by $g = \prod_p g^{(p)}$, where $g^{(p)} = \prod_{i=1}^{\ell} f_i^{(p)}$.*

iii) *If $h = \sum_{n\geq 1} \frac{c_n}{n^s}$ is a Dirichlet series such that $h(s) = \prod_{i=1}^{\ell} f_i(s)$ for $\mathrm{Re}(s) \gg 0$, then $b_n = c_n$ for every n. In particular, we have $\rho^+(h) \leq \max_i \rho^+(f_i)$.*

Proof. All the assertions are straightforward to prove, so we leave them as an exercise. We only note that iii) is a consequence of i) and of Proposition 4.4. $\square$

In what follows we make some considerations that will be useful in the next section, when dealing with zeta functions of arithmetic schemes. Suppose that f is a formal power series $f = \sum_{m\geq 0} a_m t^m \in \mathbf{C}[\![t]\!]$. Given a prime p, we may associate to f the Dirichlet series $\widetilde{f} = \sum_{m\geq 0} \frac{a_m}{p^{ms}}$. If $r(f)$ is the radius of convergence of f, then $\widetilde{f}(s)$ is absolutely convergent for $\mathrm{Re}(s) > -\frac{\log(r(f))}{\log p}$, and it is divergent for $\mathrm{Re}(s) < -\frac{\log(r(f))}{\log p}$. Therefore $\rho(\widetilde{f}) = \rho^+(\widetilde{f}) = -\frac{\log(r(f))}{\log p}$.

If $f(0) = 0$, then we may consider $g = \exp(f)$. It is clear that $r(g) \geq r(f)$, and it follows from the above formulas that $\rho(\widetilde{g}) \leq \rho(\widetilde{f})$.

Suppose now that for every prime p we have a formal power series $f_p = \sum_{m\geq 1} a_m^{(p)} t^m$ with $a_m \in \mathbf{R}_{\geq 0}$ for all m, and consider as above the corresponding Dirichlet series $\widetilde{f}_p = f_p(1/p^s) = \sum_{m\geq 0} \frac{a_m^{(p)}}{p^{ms}}$. Let $g_p = \exp(f_p)$, and $\widetilde{g}_p = g_p(1/p^s)$.

Proposition 4.15. *With the above notation, suppose that the $C > 0$ and $\alpha \in \mathbf{R}$, and $p_0 \in \mathbf{Z}_{>0}$ are such that*

$$a_m^{(p)} \leq \begin{cases} Cp^{m\alpha}, & \text{if} p \geq p_0, m \geq 1; \\ Cp^{m(\alpha+1)}, & \text{if} p < p_0, m \geq 1. \end{cases}$$

In this case $\prod_p \widetilde{g}_p(s)$ is the Euler product decomposition of a Dirichlet series with non-negative coefficients, which is absolutely convergent in the half-plane $\{s \mid \mathrm{Re}(s) > \alpha + 1\}$.

Proof. Let us write $g_p = \sum_{m\geq 0} b_m^{(p)} t^m$, so that $\widetilde{g}_p(s) = \sum_{m\geq 0} \frac{b_m^{(p)}}{p^{ms}}$. Note that $b_0^{(p)} = 1$, and since $a_m^{(p)} \geq 0$ for all m and p, we have $b_m^{(p)} \geq 0$ for all m and p. For a positive integer n having the prime decomposition $n = p_1^{m_1} \cdots p_r^{m_r}$, we put $b_n = b_{m_1}^{(p_1)} \cdots b_{m_r}^{(p_r)}$. Let us consider the Dirichlet series $g(s) = \sum_{n\geq 1} \frac{b_n}{n^s}$.

It is enough to show that the product $\prod_p \widetilde{g}_p(s)$ is convergent for every $s \in \mathbf{R}$ with $s > \alpha + 1$. Indeed, we can then apply Proposition 4.11 to deduce that this is the Euler product decomposition of $g(s)$, whose abscissa of convergence is $\leq \alpha + 1$.

Let us fix $s \in \mathbf{R}$ with $s > \alpha + 1$. Using the definition of the $\widetilde{g}_p$, we see that it is enough to show that $\sum_p \widetilde{f}_p(s)$ is convergent. Note that this is a series with nonnegative terms, and by assumption we have

$$\sum_{p<p_0} \sum_{m\geq 1} \frac{a_m^{(p)}}{p^{ms}} \leq C \cdot \sum_{p<p_0} \sum_{m\geq 1} p^{m(\alpha-s+1)} = C \cdot \sum_{p<p_0} \frac{1}{p^{s-\alpha-1} - 1} < \infty, \text{ and}$$

$$\sum_{p\geq p_0} \sum_{m\geq 1} \frac{a_m^{(p)}}{p^{ms}} \leq C \cdot \sum_{p\geq p_0} \sum_{m\geq 1} p^{m(\alpha-s)} = C \cdot \sum_{p\geq p_0} \frac{1}{p^{s-\alpha} - 1} \leq 2C \cdot \sum_{p\geq p_0} \frac{1}{p^{s-\alpha}} < \infty.$$

Since the above series are convergent, this completes the proof. $\square$

5. The zeta function of an arithmetic scheme

In this section we consider arithmetic schemes, that is, schemes of finite type over $\mathbf{Z}$. For every such scheme X, we denote by X_p the fiber of X over the point $p\mathbf{Z}$ in $\operatorname{Spec}\mathbf{Z}$. This is a scheme of finite type over $\mathbf{F}_p$. The following lemma describes the set X_{cl} of closed points of an arithmetic scheme X.

Lemma 5.1. *If X is a scheme of finite type over $\mathbf{Z}$, and $x \in X$ is a point, then x is a closed point if and only if its residue field $k(x)$ is a finite field. In this case, the image of x in* $\operatorname{Spec}\mathbf{Z}$ *is a closed point.*

Proof. Let $\pi\colon X \to \operatorname{Spec}\mathbf{Z}$ denote the canonical morphism. If $k(x)$ is a finite field, then $k(\pi(x))$ is finite too, being a subfield of $k(x)$, hence $\pi(x)$ is a closed point $p\mathbf{Z}$. In this case we know that x is a closed point in the fiber X_p, hence it is closed in X.

Conversely, suppose that x is closed in X. If $U = \operatorname{Spec} A$ is an affine open neighborhood of x, then x is closed in U, hence it corresponds to a maximal ideal $\mathfrak{m} \subset A$. If $\pi(x)$ is a closed point, then we are done: since x is a closed point on a scheme of finite type over $\mathbf{F}_p$, the residue field $k(x)$ is finite. Suppose that $\pi(x)$ is the generic point of $\operatorname{Spec}\mathbf{Z}$. The field $K = A/\mathfrak{m}$ is a finitely generated $\mathbf{Z}$-algebra. In particular, it is a finitely generated $\mathbf{Q}$-algebra, hence it is finite over $\mathbf{Q}$ by Nullstellensatz. If B is the integral closure of $\mathbf{Z}$ in K, then B is a Dedekind domain with field of fractions K. Since K is a finitely generated $\mathbf{Z}$-algebra, it is also finitely generated over B, hence it is equal to $B[1/b]$ for some nonzero $b \in B$. However, b is only contained in finitely many prime ideals, while B has infinitely many such ideals. Therefore $B[1/b]$ can not be a field. This contradiction shows that $\pi(x)$ is a closed point. $\square$

Let X be an arithmetic scheme. For every closed point $x \in X$, we put $N(x) = |k(x)|$. Note that given any M, there are only finitely many closed points $x \in X$ with $N(x) \leq M$. Indeed, this condition bounds the characteristic of $k(x)$, and we have seen in Lecture 2 that on every X_p there are only finitely many closed points with $\deg(k(x)/\mathbf{F}_p)$ bounded.

A 0-cycle on X is an element of the free abelian group on the set of closed points of X. We say that a 0-cycle $\alpha = \sum_{i=1}^{\ell} m_i x_i$ is *effective* if all m_i are non-negative. In this case, we put $N(\alpha) := \prod_i N(x_i)^{m_i}$. Note that if α is an effective cycle on X_p, then $N(\alpha) = p^{\deg(\alpha)}$.

The zeta function L_X of X is defined by $L_X(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$, where a_n is the number of effective 0-cycles α on X with $N(\alpha) = n$ (with the convention $a_1 = 1$). Note that the sequence $(a_n)_{n \geq 1}$ is multiplicative: this is an easy consequence of the fact that for every closed point $x \in X$, $N(x)$ is a prime power, hence $N(x)$ divides a product mn, with m and n relatively prime if and only if it divides precisely one of m and n. Therefore we have an Euler product decomposition of L_X as $L_X(s) = \prod_p L_{X,p}(s)$, where

$$L_{X,p}(s) = \sum_{n \geq 0} \frac{b_n^{(p)}}{p^{ns}},$$

where $b_n^{(p)}$ is the number of effective 0-cycles on X_p of degree n. It follows from Remark 3.4 in Lecture 2 that $L_{X,p}(s) = Z(X_p, p^{-s}) = L_{X_p}(s)$ (for a possibly non-reduced scheme W of finite type over $\mathbf{F}_p$, we put $Z(W,t) = Z(W_{\mathrm{red}}, t)$).

Up to this point, the above Euler product only holds at a formal level, since we have not proved yet that the above Dirichlet series converges in a nonempty half-plane. Our main goal in this section is to prove this fact, to compute the abscissa of convergence, and to show that the zeta function has a meromorphic continuation to a half-space containing the half-plane of convergence. Note that the above Dirichlet series has nonnegative coefficients, so in this case the abscissa of absolute convergence is equal to the abscissa of convergence.

As a warm-up, we start with the case of a scheme that lies over a closed point in $\operatorname{Spec}\mathbf{Z}$. Suppose that Y is a scheme of finite type over $\mathbf{F}_p$. Recall that in this case we have $L_Y(s) = Z(Y, p^{-s})$. The following is the main result in this setting.

Theorem 5.2. *If Y is a scheme of finite type over $\mathbf{F}_p$, then the Dirichlet series with nonnegative coefficients $L_Y(s)$ is convergent for $\mathrm{Re}(s) > r := \dim(Y)$, and it has no zeros in this half-plane. Furthermore, if the r-dimensional irreducible components of Y are $Y_1, \ldots, Y_\ell$, and each $Y_j \times_{\mathbf{F}_p} \overline{\mathbf{F}_p}$ has m_j irreducible components, then*

$$L_Y(s) = \widetilde{L}(s) \cdot \prod_{j=1}^{\ell} \frac{1}{1 - p^{m_j(r-s)}},$$

where $\widetilde{L}$ is the sum of a Dirichlet series with abscissa of absolute convergence $\leq r - \frac{1}{2}$. In particular, the abscissa of convergence of L_Y is r, and L_Y admits a meromorphic continuation to the half-plane $\{s \mid \mathrm{Re}(s) > r - \frac{1}{2}\}$, such that the set of poles is given by

$$\left\{ r + \frac{2\pi i m}{m_j \log(p)} \mid m \in \mathbf{Z}, 1 \leq j \leq \ell \right\}.$$

Proof. Let $f = \sum_{e \geq 1} \frac{N_e}{e} t^e$, where $N_e = |Y(\mathbf{F}_{p^e})|$, and $g = \exp(f)$, so that $L_Y(s) = g(p^{-s})$. We thus are in the setting discussed at the end of §4. It follows from Corollary 2.4 that there is a constant $\alpha_Y > 0$ such that $N_e \leq \alpha_Y p^{er}$ for every $e \geq 1$. This implies $N_e^{1/e} \leq \alpha_Y^{1/e} p^r$, so that the radius of convergence R of f is $\geq p^{-r}$, and we thus obtain

$$\rho(L_Y) = \rho^+(L_Y) = -\frac{\log(R)}{\log p} \leq r.$$

Note also that if $\mathrm{Re}(s) > r$, then $L_Y(s) = \exp(f(p^{-s}))$, hence it is nonzero. This proves the first assertion in the theorem.

The second assertion is the deeper one, and for this we will make use the Lang-Weil estimate. Let $f_1 = \sum_{i=1}^{\ell} \sum_{m_i | e} \frac{m_i p^{er}}{e} t^e$ and $f_2 = f - f_1$. Note that

$$f_1 = \sum_{i=1}^{\ell} \sum_{j \geq 1} \frac{p^{j m_i r} t^{j m_i}}{j} = -\sum_{i=1}^{\ell} \log(1 - p^{m_i r} t^{m_i}),$$

hence $\exp(f_1)=\prod_{i=1}^{\ell}\frac{1}{1-p^{rm_i}t^{m_i}}$. On the other hand, if we write $f_2=\sum_{m\geq 1}\frac{b_m}{m}t^m$, it follows from Proposition 3.2 that there is a constant $C>0$ such that $|b_m|\leq Cp^{(r-\frac{1}{2})m}$ for all m. Arguing as above, we see that the radius of convergence of f_2 is $\geq p^{-r+\frac{1}{2}}$. Therefore the abscissa of convergence of $\widetilde{L}(s)=\exp(f_2)(p^{-s})$ is $\leq r-\frac{1}{2}$, and we have

$$L_Y(s)=\exp(f_1)(p^{-s})\cdot\exp(f_2)(p^{-s})=\widetilde{L}(s)\cdot\prod_{i=1}^{\ell}\frac{1}{1-p^{m_i(r-s)}}.$$

Note also that if $\mathrm{Re}(s)>r-\frac{1}{2}$, then $\widetilde{L}(s)=\exp(f_2(p^{-s}))\neq 0$. The last assertions in the theorem are now easy consequences. □

Exercise 5.3. Let $(m_i)_{i\in I}$ be positive integers, where I is a countable set, such that for every M there are only finitely many i with $m_i\leq M$. Show that if the power series $f(t)=\prod_{i\in I}(1-t^{m_i})^{-1}\in\mathbf{Z}[\![t]\!]$ has radius of convergence R, then for every $u\in\mathbf{C}$ with $|u|<\min\{1,R\}$ the product $\prod_{i\in I}(1-u^{m_i})^{-1}$ is absolutely convergent and $f(u)=\prod_{i\in I}(1-u^{m_i})^{-1}$.

Exercise 5.4. Show that if Y is a scheme of finite type over $\mathbf{F}_p$, then for every $s\in\mathbf{C}$ with $\mathrm{Re}(s)>\dim(Y)$ the product $\prod_{x\in Y_{\rm cl}}(1-N(x)^{-s})^{-1}$ is absolutely convergent, and $L_Y(s)=\prod_{x\in X_{\rm cl}}(1-N(x)^{-s})^{-1}$.

The case of an arithmetic scheme X whose irreducible components dominate $\mathrm{Spec}\,\mathbf{Z}$ is more involved. We begin by giving an upper-bound for the abscissa of convergence of an arbitrary arithmetic scheme. This will be a consequence of the following complement to Corollary 2.4.

Proposition 5.5. *For every arithmetic scheme X of dimension r, there is a constant $c_X>0$ and p_0 such that for every prime $p\geq p_0$ and every $e\geq 1$, we have*

$$\#X(\mathbf{F}_{p^m})\leq\begin{cases} c_Xp^{m(r-1)}, & if p\geq p_0, m\geq 1;\\ c_Xp^{mr}, & if p<p_0, m\geq 1.\end{cases}$$

Proof. It is enough to show that there is c_X and p_0 such that $\#X(\mathbf{F}_{p^m})\leq c_Xp^{m(r-1)}$ for all $p\geq p_0$ and $m\geq 1$. Indeed, applying Proposition 3.2 to each X_p with $p<p_0$, we see that after possibly enlarging c_X we have $\#X(\mathbf{F}_{p^m})\leq p^{mr}$ for all $p<p_0$ and $m\geq 1$.

We first prove this assertion in the case when X is irreducible, and it is smooth and projective over $\mathrm{Spec}\,\mathbf{Z}[1/N]$ for some positive integer N. Consider an embedding $X\hookrightarrow\mathbf{P}^n_{\mathbf{Z}[1/N]}$, and let d denote the degree of the fibers. In particular, for every prime p that does not divide N, $X_p\hookrightarrow\mathbf{P}^n_{\mathbf{F}_p}$ is a smooth closed subvariety of dimension $r-1$ and degree d. In particular, $X_p\times_{\mathbf{F}_p}\overline{\mathbf{F}_p}$ has $\leq d$ irreducible components. Applying Proposition 3.1 to each connected component of X, we see that there is a positive constant c_X such that $\#X(\mathbf{F}_{p^e})\leq c_Xp^{(r-1)e}$ for every p that does not divide N, and every $e\geq 1$.

We now consider the general case, that we prove by induction on r. If $r=0$, then X_p is empty for $p\gg 0$, and the assertion to prove is trivial. Suppose that $r\geq 1$. Note first that we may assume that X is irreducible: if $X_1, \ldots, X_\ell$ are the irreducible components of X, and if we can find c_{X_i} for every i, then it is enough to take $c_X = \sum_{i=1}^{\ell} c_{X_i}$.

Suppose from now on that X is irreducible, and after replacing X by X_{red} we may also assume that X is reduced. If X does not dominate $\operatorname{Spec}\mathbf{Z}$, then X_p is empty for $p \gg 0$, hence the assertion to prove is trivial. We henceforth assume that X dominates $\operatorname{Spec}\mathbf{Z}$.

Note that if X is birational to Y, for an integral scheme Y of finite type over $\operatorname{Spec}\mathbf{Z}$, and if we can find c_Y as required, then we can also find c_X. Indeed, if V is an open subset of X isomorphic to an open subset of Y, then we can find $c_{X \smallsetminus V}$ by induction, and it is enough to take $c_X = \max\{c_Y, c_{X\smallsetminus V}\}$.

In particular, we may assume that X is projective over $\operatorname{Spec}\mathbf{Z}$. We apply Hironaka's theorem on resolution of singularities to find a projective birational morphism $\varphi_{\mathbf{Q}} \colon \widetilde{X}_{\mathbf{Q}} \to X \times_{\mathbf{Z}} \mathbf{Q}$, with $\widetilde{X}_{\mathbf{Q}}$ nonsingular, hence smooth over $\mathbf{Q}$. We can find a positive integer N such that $\varphi_{\mathbf{Q}}$ is obtained by base-change from a projective birational morphism $\varphi \colon \widetilde{X} \to X \times_{\mathbf{Z}} \mathbf{Z}[1/N]$, such that $\widetilde{X}$ is smooth and projective over $\operatorname{Spec}\mathbf{Z}[1/N]$. We have already seen that the assertion in the proposition holds for $\widetilde{X}$, and since X is birational to $\widetilde{X}$, it follows that we can find c_X as required. This completes the proof of the proposition. $\square$

Corollary 5.6. *If X is an arithmetic scheme of dimension r, then the Dirichlet series with nonnegative coefficients L_X is convergent in $\{s \mid \mathrm{Re}(s) > r\}$, and it has no zeros in this region.*

Proof. Let $f_p = \sum_{e\geq 1} \frac{N_e(p)}{e} t^e$, where $N_e(p) = \#X(\mathbf{F}_{p^e})$. It follows from Proposition 5.5 that there is a constant $c_X > 0$ and p_0 such that the series f_p satisfy the conditions in Proposition 4.15, with $\alpha = r-1$. Since $\prod_p \exp(f_p(p^{-s}))$ is the Euler product corresponding to L_X, we deduce that $L_X(s)$ is (absolutely) convergent for $\mathrm{Re}(s) > r$. Furthermore, each of the factors of the Euler product is nonzero, hence $L_X(s)$ is nonzero in this half-plane. $\square$

Remark 5.7. It follows from Corollary 5.6 and Proposition 4.11 that if X is an arithmetic scheme of dimension r, then $L_X(s) = \prod_p L_{X_p}(s)$ whenever $\mathrm{Re}(s) > r$. Furthermore, it follows from Exercise 5.4 that for every prime p, we have $L_{X_p}(s) = \prod_{x \in (X_p)_{\mathrm{cl}}} \left(1 - N(x)^{-s}\right)^{-1}$, and the product is absolutely convergent. We conclude using Exercise 4.10 that

$$L_X(s) = \prod_{x \in X_{\mathrm{cl}}} \left(1 - N(x)^{-s}\right)^{-1},$$

and the product is absolutely convergent.

Example 5.8. Let K be a number field and $\mathcal{O}_K$ the ring of integers of K (that is, the ring of elements of K that are integral over $\mathbf{Z}$). The zeta function of K (also called the Dedekind zeta function of K) is $\zeta_K := L_{\operatorname{Spec}\mathcal{O}_K}$. Corollary 5.6 implies that ζ_K is (absolutely) convergent in the half-plane $\{s \mid \mathrm{Re}(s) > 1\}$. We deduce from the previous remark that we have a product description in this region

$$\zeta_K(s) = \prod_{P \in \operatorname{Spec}(\mathcal{O}_K)} \left(1 - \frac{1}{N(P)^s}\right)^{-1}.$$

The description of ζ_K as a Dirichlet series can also be written as

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s},$$

where the sum is over all proper nonzero ideals $\mathfrak{a}$ of $\mathcal{O}_K$, and where $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ (by the unique factorization of an ideal in $\mathcal{O}_K$ as a product of prime ideals, we can identify nonzero ideals in $\mathcal{O}_K$ with effective cycles on $\operatorname{Spec} \mathcal{O}_K$, such that the two definitions of $N(\mathfrak{a})$ are compatible). Of course, if $K = \mathbf{Q}$, then ζ_K is the Riemann zeta function.

Example 5.9. Recall that by Corollary 3.8 in Lecture 2 we have

$$Z(\mathbf{P}^n_{\mathbf{F}_p}, t) = \frac{1}{(1-t)(1-pt)\cdots(1-p^n t)}.$$

Therefore the zeta function of $\mathbf{P}^n_{\mathbf{Z}}$ is given by

$$L_{\mathbf{P}^n_{\mathbf{Z}}}(s) = \prod_p Z(\mathbf{P}^n_{\mathbf{F}_p}, p^{-s}) = \prod_{i=0}^{n} \prod_p \frac{1}{(1-p^{i-s})} = \prod_{i=0}^{n} \zeta(s-i).$$

Remark 5.10. If X is an arithmetic scheme, Y is a closed subscheme of X, and $U = X \smallsetminus Y$, then $L_X(s) = L_Y(s) L_U(s)$ for all $s > \dim(X)$. Indeed, this is a consequence of the Euler product description of the zeta function, and of the fact that $Z(X_p, t) = Z(Y_p, t) \cdot Z(U_p, t)$ for all primes p. In particular, we see that L_X is the product of L_Y and L_U in the sense of Proposition 4.14, and therefore $\rho(L_X) \leq \max\{\rho(L_Y), \rho(L_U)\}$.

Our last result in this section describes, in particular, the abscissa of convergence of zeta functions of arithmetic schemes.

Theorem 5.11. *If X is an arithmetic scheme of dimension r, then the following hold:*

i) *The abscissa of convergence of L_X is $\rho = r$.*
ii) *L_X admits a meromorphic continuation to the half-plane $\{s \mid \operatorname{Re}(s) > r - \varepsilon\}$, for some $\varepsilon > 0$, and $s = r$ is a pole.*
iii) *If X is irreducible and dominates* $\operatorname{Spec} \mathbf{Z}$*, then the only pole of L_X in the half-plane $\{s \mid \operatorname{Re}(s) > r - \varepsilon\}$, with ε as in ii), is at $s = r$, and this occurs with order one.*

In fact, as we will explain below, one can show that one can take $\varepsilon = \frac{1}{2}$ in the theorem. The key ingredient that we will need, in addition to the Lang-Weil estimate, is given by the special case of the ring of integers in a number field. This is the content of the following proposition.

Proposition 5.12. *If K is a number field with* $\deg(K/\mathbf{Q}) = \ell$*, then ζ_K admits a meromorphic continuation to the half-plane $\{s \mid \operatorname{Re}(s) > 1 - \frac{1}{\ell}\}$. In this region the only pole is $s = 1$, and this occurs with order one. In particular, the abscissa of convergence of ζ_K is $\rho = 1$.*

Proof. We will use the following result from algebraic number theory: there is a positive number α_K such that if $i(m)$ denotes the number of proper nonzero ideals I in $\mathcal{O}_K$ with

$N(I) \leq m$, then

$$\frac{i(m) - \alpha_K m}{m^{1-\frac{1}{\ell}}}$$

is bounded see [Mar, Theorem 39]. This implies that if we write $\zeta_K - \alpha_K\zeta(s)$ as a Dirichlet series $\sum_{m\geq 1}\frac{b_m}{m^s}$, then there is a positive constant C such that $|b_1+\ldots+b_m| \leq Cm^{1-\frac{1}{\ell}}$ for all m. Proposition 4.5 implies that $\zeta_K - \alpha_K\zeta$ is analytic in the half-plane $\{s \mid \mathrm{Re}(s) > 1-\frac{1}{\ell}\}$. On the other hand, by Proposition 4.6 we know that ζ is meromorphic in the half-plane $\{s \mid \mathrm{Re}(s) > 0\}$, with a unique (simple) pole at $s = 1$. This gives the assertions in the proposition concerning ζ_K. $\square$

One can show that, in fact, ζ_K admits a meromorphic continuation to $\mathbf{C}$, such that the only pole is at $s = 1$. However, the proof is quite involved, so we refer to [Lang, Chapter XIII] for this result.

Proof of Theorem 5.11. Note first that if U is an open subset of X such that $\dim(W) < \dim(X)$, where $W = X \smallsetminus U$, then the theorem holds for X if and only if it holds for U. Indeed, $L_X(s) = L_W(s)L_U(s)$ by Remark 5.10. Since $\dim(W) \leq r-1$, the function L_W is analytic in $\{s \mid \mathrm{Re}(s) > r-1\}$ by Corollary 5.6, and it has no zeros in this half-plane. Therefore the assertions in the theorem hold for X if and only if they hold for U. This implies, in particular, that if X and Y are birational integral schemes, then the theorem holds for X if and only if it holds for Y.

Given any X, let us consider an affine open subset U of X with $\dim(X \smallsetminus U) < r$, such that U is isomorphic to the disjoint union of some U_i, with each U_i irreducible of dimension r. Since $L(U, s) = \prod_i L_{U_i}(s)$, it is clear that if each U_i satisfies properties i) and ii), then so does U, and therefore so does X. This shows that we may assume that X is affine and irreducible, and after replacing X by X_{red}, we may assume that X is integral.

If X does not dominate $\mathrm{Spec}\,\mathbf{Z}$, then $X = X_p$ for some p. In this case, Theorem 5.2 shows that properties i) and ii) are satisfied with $\varepsilon = \frac{1}{2}$. Hence from now on we may assume that X dominates $\mathrm{Spec}\,\mathbf{Z}$. Arguing as in the proof of Proposition 5.5, we find an integral scheme Y that is smooth and projective over some $\mathrm{Spec}\,\mathbf{Z}[1/N]$, connected, and that is birational to X. As we have seen, it is enough to show that Y satisfies the assertions in the theorem.

Let $\pi\colon Y \to \mathrm{Spec}\,\mathbf{Z}[1/N]$ be the structure morphism. After possibly replacing N by a multiple, we may assume that $\pi_*(\mathcal{O}_Y)$ is free (say, of rank m) and $\pi_*(\mathcal{O}_{Y_p}) \simeq \pi_*(\mathcal{O}_Y) \otimes \mathbf{Z}/p\mathbf{Z}$ for all primes p that do not divide N. Therefore $A = \Gamma(Y, \mathcal{O}_Y)$ is an integral domain, free of rank m over $\mathbf{Z}[1/N]$. If $K = A \otimes_{\mathbf{Z}} \mathbf{Q}$, then K is a domain that is a finite extension of $\mathbf{Q}$, hence it is a number field, equal to the fraction field of A. If $\mathcal{O}_K$ is the ring of integers in K, then we have an inclusion $A \subseteq \mathcal{O}_K[1/N]$. After possibly replacing N by a multiple, we may assume that $A = \mathcal{O}_K[1/N]$ and that $O_K[1/N]$ is smooth over $\mathbf{Z}[1/N]$.

Suppose that p is a prime that does not divide N, and let us consider its prime decomposition in $\mathcal{O}_K$:

$$pO_K = P_1 \cdot \ldots \cdot P_\ell,$$

and let $m_i = [\mathcal{O}_K/P_i : \mathbf{F}_p]$. Note that the fiber Y_p is a smooth, $(r-1)$-dimensional projective variety, with ℓ irreducible components $Y_p^{(1)}, \ldots, Y_p^{(\ell)}$, with $Y_p^{(i)} \times_{\operatorname{Spec} \mathbf{F}_p} \operatorname{Spec} \overline{\mathbf{F}_p}$ having m_i irreducible components.

For every prime p that does not divide N, let $f_p = \sum_{e \geq 1} \frac{|X(\mathbf{F}_{p^e})|}{e} t^e$ and

$$f_p^{(1)} = \sum_{e \geq 1} \frac{|\operatorname{Spec} \mathcal{O}_K(\mathbf{F}_{p^e})|}{e} t^e = \sum_{i=1}^{\ell} \sum_{m_i | e} \frac{m_i}{e} t^e.$$

If we write $f_p^{(2)}(t) = f_p(t) - f_p^{(1)}(p^{r-1}t) = \sum_{e \geq 1} \frac{b_e^{(p)}}{e} t^e$, then we apply Proposition 3.1 to every connected component of Y_p to deduce that we have a positive constant C such that $|b_e^{(p)}| \leq C p^{(r-\frac{1}{2})e}$ for all e and all primes p that do not divide N. We deduce from Proposition 4.15 that $\prod_{p \nmid N} \exp(f_p^{(2)})(p^{-s})$ is the Euler product of a Dirichlet series $\widetilde{L_Y}$ that is absolutely convergent in the half-plane $\{s \mid \operatorname{Re}(s) > r - \frac{1}{2}\}$, and which has no zeros in this region. On the other hand, if we put $Y' = \operatorname{Spec} \mathcal{O}_K[1/N]$, then $L_Y(s) = L_{Y'}(s-r+1)\widetilde{L_Y}(s)$. Note that $\zeta_K(s) = L_{Y'}(s) \prod_j \left(1 - \frac{1}{N(P_j)^s}\right)^{-1}$, where the P_j are the (finitely many) prime ideals of $\mathcal{O}_K$ that lie over primes in $\mathbf{Z}$ dividing N. It follows from Proposition 5.12 that $L_{Y'}(s)$ is a meromorphic function in the half-plane $\{s \mid \operatorname{Re}(s) > 1 - \frac{1}{d}\}$, where $d = \deg(K/\mathbf{Q})$, and its only pole in this region is at $s = 1$, and this has order one. We deduce that properties i), ii), and iii) are satisfied by L_Y, where we may take $\varepsilon = 1/d$. This completes the proof of the theorem. □

Remark 5.13. If one assumes the fact that ζ_K has a meromorphic continuation to the half-plane $\{s \mid \operatorname{Re}(s) > \frac{1}{2}\}$, we see that the argument in the proof of Theorem 5.11 shows that for every arithmetic scheme of dimension r, the zeta function L_X can be extended as a meromorphic function to $\{s \mid \operatorname{Re}(s) > r - \frac{1}{2}\}$.

Remark 5.14. If X is any arithmetic scheme of dimension r, then the order of $s = r$ as a pole of L_X is equal to the number of r-dimensional irreducible components of X. Indeed, if $X_1, \ldots, X_\ell$ are the r-dimensional irreducible components of X, then the order of $s = r$ as a pole of L_X is the sum of the corresponding orders of $s = r$ as a pole of each L_{X_j}. These orders in turn can be computed using Theorem 5.2 (for those X_j that lie in a fiber over $\operatorname{Spec} \mathbf{Z}$) and Theorem 5.11 (for those X_j that dominate $\operatorname{Spec} \mathbf{Z}$).

It is conjectured that for *every* arithmetic scheme X, the zeta function L_X admits a meromorphic continuation to $\mathbf{C}$. This seems, however, to be completely out of reach at the moment. One important case is when $X \times_{\mathbf{Z}} \mathbf{Q}$ is an elliptic curve, in which case the assertion is known to follow from the famous Taniyama-Shimura conjecture, proved in [Wil], [TW], and [BCDT].

References

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over Q: wild 3-adic exercises, J. Amer. Math. Soc. 14 (2001), 843–939. 21

[Kol] J. Kollár, *Rational curves on algebraic varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, 32, Springer-Verlag, Berlin, 1996. 1

[Lang] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994. 10, 20

[LaWe] S. Lang and A. Weil, Number of points of varieties in finite fields, Amer. J. Math. **76** (1954), 819–827. 2

[Mar] D. A. Marcus, *Number fields*, Universitext, Springer Verlag, New York-Heidelberg, 1977. 20

[MoVa] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, 97, Cambridge University Press, Cambridge, 2007. 11

[Se] J.-P Serre, *A course in arithmetic*, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York-Heidelberg, 1973. 7

[TW] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. of Math. (2) **141** (1995), 553–572. 21

[Wil] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) **141** (1995), 443–551. 21