HIGHER RANK ZETA FUNCTIONS AND RIEMANN HYPOTHESIS FOR ELLIPTIC CURVES

LIN WENG AND DON ZAGIER

ABSTRACT. In [8], a non-abelian zeta function was defined for any smooth curve X over a finite field $\mathbb{F}_q$ and any integer $n \geq 1$ by

$$\zeta_{X/\mathbb{F}_q,n}(s) \;=\; \sum_{[V]} \frac{|H^0(X,V)\smallsetminus\{0\}|}{|\mathrm{Aut}(V)|}\, q^{-\deg(V)s} \qquad (\Re(s)>1)\,,$$

where the sum is over isomorphism classes of $\mathbb{F}_q$-rational semi-stable vector bundles V of rank n on X with degree divisible by n. This function, which agrees with the usual Artin zeta function of $X/\mathbb{F}_q$ if $n=1$, is a rational function of q^{-s} with denominator $(1-q^{-ns})(1-q^{n-ns})$ and conjecturally satisfies the Riemann hypothesis. In this paper we study the case of genus 1 curves in detail. We show that in that case the Dirichlet series

$$\mathfrak{Z}_{X/\mathbb{F}_q}(s) \;=\; \sum_{[V]} \frac{1}{|\mathrm{Aut}(V)|}\, q^{-\mathrm{rank}(V)s} \qquad (\Re(s)>0)\,,$$

where the sum is now over isomorphism classes of $\mathbb{F}_q$-rational semi-stable vector bundles V of degree 0 on X, is equal to $\prod_{k=1}^{\infty}\zeta_{X/\mathbb{F}_q}(s+k)$, and use this fact to deduce the validity of the Riemann hypothesis for $\zeta_{X,n}(s)$ for all n.

INTRODUCTION

Let X be a smooth projective curve of genus g over a finite field $\mathbb{F}_q$. For all integers $n \geq 0$ and d we define the α and β invariants of $X/\mathbb{F}_q$ by

$$\alpha_{X,n}(d) \;=\; \sum_{[V]} \frac{q^{h^0(X,V)}-1}{|\mathrm{Aut}(V)|}\,, \qquad \beta_{X,n}(d) \;=\; \sum_{[V]} \frac{1}{|\mathrm{Aut}(V)|}\,. \tag{1}$$

Here the sums are over isomorphism classes of $\mathbb{F}_q$-rational semi-stable vector bundles V of rank n and degree d on X, and $\mathrm{Aut}(V)$ and $h^0(X,V)$ denote the automorphism group of V and the dimension of its space of global sections.

The beta invariants were studied by Harder-Narasimhan in their work on moduli spaces of vector bundles [5]. In fact, when $(d,n)=1$, all semi-stable bundles of rank n and degree d become stable, hence have only trivial automorphisms. Consequently, $\beta_{X,n}(d) = \frac{1}{q-1}\cdot|\mathcal{M}_{X,n}(d)(\mathbb{F}_q)|$ counts the number of $\mathbb{F}_q$-rational points of the corresponding moduli space $\mathcal{M}_{X,n}(d)$.

In [8] a "non-abelian rank n zeta function" of $X/\mathbb{F}_q$ was defined by

$$\zeta_{X,n}(s) \;=\; \zeta_{X/\mathbb{F}_q,n}(s) \;=\; \sum_{d\equiv 0 \pmod n} \alpha_{X,n}(d)\, t^d \;=\; \sum_{m=0}^{\infty} \alpha_{X,n}(mn)\, T^m\,, \tag{2}$$

where $t = q^{-s}$, $T = t^n = Q^{-s}$ with $Q = q^n$, and the following properties were shown, using Riemann-Roch, duality and vanishing for semi-stable bundles:

Theorem. *Define $\zeta_{X,n}(s)$ for all $n \geq 1$ by (2). Then*

(i) *The function $\zeta_{X,1}(s)$ equals $\zeta_X(s)$, the Artin zeta function of $X/\mathbb{F}_q$.*
(ii) *There exists a degree $2g$ polynomial $P_{X,r}(T) \in \mathbb{Q}[T]$ such that*

$$\zeta_{X,n}(s) \;=\; \frac{P_{X,n}(T)}{(1-T)(1-QT)}\,. \tag{3}$$

(iii) *The function $\zeta_{X,n}$ satisfies the functional equation*

$$\zeta_{X,n}(1-s) \;=\; Q^{(g-1)(2s-1)} \cdot \zeta_{X,n}(s)\,. \tag{4}$$

The following conjecture was also proposed in [8].

Conjecture (Riemann Hypothesis). *If $\zeta_{X,n}(s) = 0$, then $\Re(s) = \frac{1}{2}$.*

In this paper, we study the case of elliptic curves $X = E$, i.e., $g = 1$. Here $\alpha_{E,n}(d) = (q^d - 1)\beta_{E,n}(d)$ for $d > 0$ (because $h^0(V) - h^1(V) = d$ by the Riemann-Roch theorem and $h^1(V)$ vanishes) and $\beta_{E,n}(mn) = \beta_{E,n}(0)$ for all m (because tensoring with a line bundle of degree 1 gives an isomorphism between the sets of rank n semi-stable vector bundles of degree d and degree $d+n$ for any $d \in \mathbb{Z}$), so the zeta function (2) reduces simply to

$$\zeta_{E,n}(s) \;=\; \alpha_{E,n}(0) \,+\, \beta_{E,n}(0)\,\frac{(Q-1)T}{(1-T)(1-QT)}\,. \tag{5}$$

We will give explicit formulas and generating functions for $\alpha_{E,n}(0)$ and $\beta_{E,n}(0)$ and prove the Riemann Hypothesis for $\zeta_{E,n}(s)$. The main result of the paper, Theorem 5, gives a rather elegant formula for the generating function $\sum \beta_{E,n}(0) q^{-ns}$ as a product of translates of the zeta function of E.

1. Statement of main results

From now on E will denote an elliptic curve over $\mathbb{F}_q$. By an "Atiyah bundle" over E we mean any direct sum of the vector bundles I_1, I_2, ... over E defined by Atiyah in [1]: $I_1 = \mathcal{O}_E$ is the trivial line bundle and I_k for $k \geq 2$ the unique (up to isomorphism) non-trivial extension of I_{k-1} by I_1. For $n \geq 1$ let $\alpha^{\mathrm{At}}_{E,n}(0)$ and $\beta^{\mathrm{At}}_{E,n}(0)$ be the numbers defined as in (1), but with the summations now ranging only over Atiyah bundles. We will show:

Theorem 1. *For $n \geq 1$ we have*

$$\alpha^{\mathrm{At}}_{E,n}(0) \;=\; \sum_{\mathbf{m}} \left(q^{m_1+m_2+\cdots} \,-\, 1\right) \frac{\varepsilon(m_1)\,\varepsilon(m_2)\cdots}{q^{N(m_1,m_2,\dots)}}\,, \tag{6}$$

$$\beta^{\mathrm{At}}_{E,n}(0) \;=\; \sum_{\mathbf{m}} \frac{\varepsilon(m_1)\,\varepsilon(m_2)\cdots}{q^{N(m_1,m_2,\dots)}}\,, \tag{7}$$

where the sum is over all partitions $n = m_1 + 2m_2 + 3m_3 + \cdots$ of n and

$$\varepsilon(m) \;=\; \frac{q^{m^2}}{|\mathrm{GL}_m(\mathbb{F}_q)|} \;=\; \frac{q^{m(m+1)/2}}{(q^m-1)(q^{m-1}-1)\cdots(q-1)}\,, \tag{8}$$

$$N(m_1, m_2, \dots) \;=\; \sum_{k,\,\ell \geq 1} m_k\, m_\ell\, \min(k,\ell)\,. \tag{9}$$

From this we will deduce the following simple formulas for $\alpha^{\mathrm{At}}_{E,n}(0)$ and $\beta^{\mathrm{At}}_{E,n}(0)$ ("special counting miracle") by a direct combinatorial argument:

Theorem 2. *For $n \geq 0$ we have*

$$\alpha^{\mathrm{At}}_{E,n+1}(0) \;=\; \beta^{\mathrm{At}}_{E,n}(0) \;=\; q^{-n}\varepsilon(n)\,. \tag{10}$$

This in turn will be used together with considerations of algebraic structures of semi-stable bundles of degree 0 to obtain the following intrinsic relation between α and β invariants ("general counting miracle"):

Theorem 3. *For all $n \geq 0$ we have*

$$\alpha_{E,n+1}(0) \;=\; \beta_{E,n}(0)\,. \tag{11}$$

We mention that Theorem 3 has been generalized to curves of arbitrary genus by Sugahara [6].

The above results, whose proofs are given in §2, show that the higher rank zeta functions for elliptic curves are completely determined by their beta invariants. To understand the latter, we first use results of Harder-Narasimhan [5], Desale-Ramanan [4] and Zagier [9] to get an explicit formula for $\beta_{E,n}(0)$ in terms of special values of the Artin zeta function of $E/\mathbb{F}_q$:

Theorem 4. *For $n \geq 1$ we have*

$$\beta_{E,n}(0) \;=\; \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{n_1+\cdots+n_k=n \\ n_1,\ldots,n_k>0}} \frac{v_{E,n_1}\cdots v_{E,n_k}}{(q^{n_1+n_2}-1)\cdots(q^{n_{k-1}+n_k}-1)}\,, \tag{12}$$

where the numbers $v_{E,n}$ $(n>0)$ are defined by

$$v_{E,n} \;=\; \zeta^*_E(1)\zeta_E(2)\cdots\zeta_E(n)\,, \qquad \zeta^*_E(1) \;=\; \lim_{s\to 1}(1-q^{1-s})\,\zeta_E(s)\,. \tag{13}$$

In §3, we will use (12) and a fairly complicated combinatorial calculation to establish the following simple formula for the generating Dirichlet series of the invariants $\beta_{E,n}(0)$:

Theorem 5. *Define a Dirichlet series $\mathfrak{Z}_E(s) = \mathfrak{Z}_{E/\mathbb{F}_q}(s)$ for $\Re(s) > 0$ by*

$$\mathfrak{Z}_{E/\mathbb{F}_q}(s) \;=\; \sum_{n=0}^{\infty} \beta_{E,n}(0)\, q^{-ns} \;=\; \sum_{[V]} \frac{1}{|\mathrm{Aut}(V)|}\, q^{-\mathrm{rank}(V)\,s}\,, \tag{14}$$

where the second sum is over isomorphism classes of $\mathbb{F}_q$-rational semi-stable vector bundles V of degree 0 on E. Then

$$\mathfrak{Z}_{E/\mathbb{F}_q}(s) \;=\; \prod_{k=1}^{\infty} \zeta_{E/\mathbb{F}_q}(s+k)\,. \tag{15}$$

This formula will then be used in §4 to prove the following estimate:

Proposition 6. *For $n \geq 2$ we have the inequalities*

$$1 \;<\; \frac{\beta_{E,n}(0)}{\beta_{E,n-1}(0)} \;<\; \frac{q^{n/2}+1}{q^{n/2}\,-\,1}\,. \tag{16}$$

(In fact, we prove a stronger estimate; see (51).) Combining these bounds with equations (5) and (11), we will deduce:

Theorem 7. *The Riemann Hypothesis is true for elliptic curves.*

2. Calculation of the α and β invariants of elliptic curves

In this section we will give explicit formulas for $\alpha_{E,n}(mn)$ and $\beta_{E,n}(mn)$ for an elliptic curve $E/\mathbb{F}_q$. By what was already explained in the introduction, it suffices to do this for $m = 0$. We will prove Theorems 1–4 as stated in §1.

2.1. **Automorphisms of Atiyah bundles.** Let V be an Atiyah bundle of rank n over E as defined in §1. Then V can be uniquely written in the form

$$V \;\cong\; \bigoplus_{k\geq 1} I_k^{\oplus m_k} \tag{17}$$

for integers $m_k \geq 0$ with $\sum_{k\geq 1} k m_k = n$, so Theorem 1 follows from:

Proposition 8. *For V/E as in* (17)*, we have $h^0(V) = \sum_{k\geq 1} m_k$ and*

$$|\mathrm{Aut}(V)| \;=\; q^{N(m_1,m_2,\dots)} \prod_{k\geq 1} q^{-m_k^2} \,|\mathrm{GL}_{m_k}(\mathbb{F}_q)|\,, \tag{18}$$

where $N(m_1, m_2, \dots)$ is defined as in equation (9)*.*

Proof. By Theorem 8 of [1], for any integers k, $\ell \geq 1$ we have

$$I_k \otimes I_\ell \;\cong \bigoplus_{\substack{|k-\ell|\,<\,m\,<\,k+\ell \\ m\equiv k+\ell-1 \pmod 2}} I_m$$

and consequently, since I_k is self-dual,

$$\dim \mathrm{Hom}(I_k, I_\ell) \;=\; h^0(I_k^\vee \otimes I_\ell) \;=\; h^0(I_k \otimes I_\ell) \;=\; \min(k,\ell)\,. \tag{19}$$

This can be seen explicitly as follows. The bundle I_k has a realization given locally away from $0 \in E$ by k-tuples of regular functions and near 0 by k-tuples $(f_1, \dots, f_k)$ where f_1 and each $zf_i - f_{i-1}$ $(2 \leq i \leq k)$ is regular, where z is a local parameter at 0. (In other words, f_i is allowed to have a pole of order $i-1$ at 0 and, for instance, the residue of f_2 equals the value of f_1 at 0.) The space $\mathrm{Hom}(I_k, I_\ell)$ is then spanned by the maps

$$(f_1, \dots, f_k) \;\mapsto\; (\underbrace{0, \dots, 0}_{\ell-s}, f_1, \dots, f_s) \qquad (\,1 \leq s \leq \min(k,\ell)\,)\,.$$

As a special case of (19) we have $h^0(I_k) = 1$ for all k, making the first statement of Proposition 8 obvious. We prove the second in several steps.

1. In the special case $V = I_k$, we have

$$|\mathrm{Aut}(I_k)| \;=\; q^{k-1}(q-1)\,.$$

Indeed, from the above description, any endomorphism of I_k has the form

$$\varphi \;=\; \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ 0 & a_1 & \cdots & a_{k-2} & a_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_1 & a_2 \\ 0 & 0 & \cdots & 0 & a_1 \end{pmatrix} \tag{20}$$

for some $a_i \in \mathbb{F}_q$, and φ is an isomorphism if and only if $a_1 \neq 0$.

2. More generally, for any positive integers k and m we have

$$|\mathrm{Aut}(I_k^{\oplus m})| \;=\; q^{(k-1)m^2}\,|\mathrm{GL}_m(\mathbb{F}_q)|\,, \tag{21}$$

because the automorphisms of $I_k^{\oplus m}$ have the same form as (20), but with each a_i now being an $m \times m$ matrix over $\mathbb{F}_q$ and with a_1 invertible.

3. Finally, if V is a general Atiyah bundle as in (17), then

$$|\mathrm{Aut}(V)| \;=\; \prod_{k\neq\ell} |\mathrm{Hom}(I_k, I_\ell)|^{m_k m_\ell} \cdot \prod_k |\mathrm{Aut}(I_k^{\oplus m_k})|\,,$$

and equation (18) then follows from (19) and (21). □

2.2. **Proof of Theorem 2.** Introduce the three generating functions

$$\mathcal{A}(x) = \sum_{n=1}^{\infty} \alpha^{\mathrm{At}}_{E,n}(0)\, x^{n-1}\,, \quad \mathcal{B}(x) = \sum_{n=0}^{\infty} \beta^{\mathrm{At}}_{E,n}(0)\, x^n\,, \quad \mathcal{C}(x) = \sum_{n=0}^{\infty} q^{-n}\,\varepsilon(n)\, x^n\,,$$

where the notations are as in Theorem 2. We must show that they coincide.

There is a bijection between terminating sequences $(m_1, m_2, \dots)$ of non-negative integers and monotone decreasing terminating sequences $(p_1, p_2, \dots)$ of non-negative integers, given by setting $p_k = \sum_{\ell\geq k} m_\ell$, $m_k = p_k - p_{k+1}$. Under this correspondence, we have

$$\begin{aligned} N(m_1, m_2, \dots) \;&=\; \sum_{k=1}^{\infty} k\, m_k\, (m_k + 2m_{k+1} + 2m_{k+2} + \cdots) \\ &=\; \sum_{k=1}^{\infty} k\,(p_k - p_{k+1})(p_k + p_{k+1}) \;=\; \sum_{k=1}^{\infty} p_k^2\,. \end{aligned}$$

Hence Theorem 1 shows that $\mathcal{A}(x)$ and $\mathcal{B}(x)$ can be given as

$$\mathcal{A}(x) \;=\; \frac{1}{x}\sum_{p=1}^{\infty} (q^p - 1)\,\mathcal{B}_p(x)\,, \qquad \mathcal{B}(x) \;=\; \sum_{p=0}^{\infty} \mathcal{B}_p(x)\,, \tag{22}$$

with $\mathcal{B}_p(x) \in \mathbb{Q}(q)[[x]]$ defined by

$$\mathcal{B}_p(x) \;=\; \sum_{p=p_1\geq p_2\geq \ldots \geq 0} \prod_{k=1}^{\infty} \Big(\varepsilon(p_k - p_{k+1})\, q^{-p_k^2}\, x^{p_k} \Big)$$

or, equivalently (set $h = p_2$ on the right-hand side), by the recursive formulas

$$\mathcal{B}_0(x) \;=\; 1\,, \qquad q^{p^2}\, x^{-p}\, \mathcal{B}_p(x) \;=\; \sum_{h=0}^{p} \varepsilon(p-h)\, \mathcal{B}_h(x)\,. \tag{23}$$

We claim that the solution of this recursion is given by

$$\mathcal{B}_p(x) \;=\; \prod_{j=1}^{p} \frac{qx}{(q^j - 1)(q^j - x)} \qquad (p \geq 0)\,. \tag{24}$$

To prove this, we denote the right-hand side of (24) by $B_p(x)$ and show that $B_p(x)$ satisfies the same recursion (23) as $\mathcal{B}_p(x)$, i.e., that we have

$$\widehat{B}(x,t) \;=\; \Big(\sum_{n=0}^{\infty} \varepsilon(n)\, t^n \Big)\, B(x,t) \;=\; \mathcal{C}(qt)\, B(x,t)\,, \tag{25}$$

where $B(x,t)$ and $\widehat{B}(x,t)$ are the *two* generating series defined by

$$B(x,t) \;=\; \sum_{p=0}^{\infty} B_p(x)\, t^p\,, \qquad \widehat{B}(x,t) \;=\; \sum_{p=0}^{\infty} q^{p^2} x^{-p}\, B_p(x)\, t^p\,.$$

But this is now fairly easy. The definition of $B_p(x)$ gives the formulas

$$(1-x)\, B_p(qx) \;=\; (q^p - x)\, B_p(x)\,, \quad (1-x)(q^p-1)\, B_p(qx) \;=\; qx\, B_{p-1}(x)\,,$$

which translate into the four generating series identities

$$\begin{aligned} (1-x)\, B(qx,t) \;&=\; B(x,qt) \;-\; xB(x,t)\,, \\ (1-x)\big(B(qx,qt) \;-\; B(qx,t)\big) \;&=\; qxt\, B(x,t)\,, \end{aligned} \tag{26}$$

and

$$\begin{aligned} (1-x)\, \widehat{B}(qx,qt) \;&=\; \widehat{B}(x,qt) \;-\; x\, \widehat{B}(x,t)\,, \\ (1-x)\big(\widehat{B}(qx,qt) \;-\; \widehat{B}(qx,t)\big) \;&=\; qt\, \widehat{B}(x,qt)\,. \end{aligned} \tag{27}$$

Now using the identity $\mathcal{C}(t) = (1-t)\mathcal{C}(qt)$, which follows from

$$\mathcal{C}(qt) - \mathcal{C}(t) \;=\; \sum_{n\geq 1} \frac{q^{n(n-1)/2}\, t^n}{(q-1)\cdots(q^{n-1}-1)} \;=\; t\,\mathcal{C}(qt)\,,$$

we find from (26) that $\mathcal{C}(qt)B(x,t)$ satisfies the same two recursions (27) as $\widehat{B}(x,t)$, and hence that these two power series are equal. This proves (25) and hence also (24) and lets us rewrite (22) as

$$\mathcal{A}(x) \;=\; \frac{1}{x}\,\big(B(x,q) \;-\; B(x,1)\big)\,, \qquad \mathcal{B}(x) \;=\; B(x,1)\,.$$

Substituting $t = q^{-1}$ into the sum of the two equations (26) now gives $(1-x)\mathcal{B}(qx) = \mathcal{B}(x)$ and hence $\mathcal{B}(x) = \mathcal{C}(x)$, and then substituting $t = 1$ into the first of equations (26) gives $\mathcal{A}(x) = \mathcal{B}(x)$. This completes the proof.

2.3. **Proof of Theorem 3.** Let V be a semi-stable vector bundle of rank n and degree 0 over $E/\mathbb{F}_q$. By the classification of indecomposable bundles on elliptic curves defined over algebraic closed fields given by Atiyah [1], we know that there are no stable bundles of rank ≥ 2 and degree 0 over $\overline{E} := E \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$. Consequently, over $\overline{E}$, the graded bundle $G(V)$ associated to a Jordan-Hölder filtration of V decomposes as

$$G(V) = L_1 \oplus L_2 \oplus \cdots \oplus L_n$$

for some line bundles L_i of degree 0 on $\overline{E}$. (For basics of Jordan-Hölder filtrations and their associated graded bundles for semi-stable bundles, see e.g. [7].) Since L_i need not be defined over $\mathbb{F}_q$, usually it is a bit complicated to classify V over E. (This classification problem depends on the arithmetic of the curve E, and specifically, on the number of $\mathbb{F}_q$-rational torsion points of order $\leq n$ on E.) Instead of doing this, we first note that in order to get a non-trivial contribution to α invariants, we must have $h^0(V) \neq 0$. Guided by this, we regroup the bundles appearing in the summation defining the α-invariant in the following way. Assume (after renumbering) that $L_j \cong \mathcal{O}_E$ for $1 \leq j \leq i$ and $L_j \ncong \mathcal{O}_E$ for $i < j \leq n$. Since there are non non-trivial

extensions of $\mathcal{O}_E$ by L_j for $L_j \ncong \mathcal{O}_E$, we can uniquely decompose V as $U \oplus W$ where U and W are $\mathbb{F}_q$-rational semi-stable bundles of degree 0 over E with

$$G(U) \;\cong\; \mathcal{O}_E^{\oplus i}\,, \qquad G(W) \;\cong\; L_{i+1} \oplus \cdots \oplus L_n\,, \quad L_j \ncong \mathcal{O}_E\,.$$

Then $h^0(E,V) = h^0(E,U)$ and $\mathrm{Aut}(V) \cong \mathrm{Aut}(U) \times \mathrm{Aut}(W)$ (because there are no non-trivial homomorphisms among $\mathcal{O}_E$ and L_j), and U and W range independently over bundles with the properties listed above. Hence

$$\alpha_{E,n}(0) \;=\; \sum_{i=1}^{n} \alpha^*_{E,i}\, \beta^*_{E,n-i}\,,$$

where $\alpha^*_{E,i}$ and $\beta^*_{E,k}$ are the modified α and β invariants defined by

$$\alpha^*_{E,i} \;=\; \sum_{\substack{U \text{ semi-stable} \\ G(U) \cong \mathcal{O}_E^{\oplus i}}} \frac{q^{h^0(E,U)} - 1}{|\mathrm{Aut}(U)|}, \qquad \beta^*_{E,k} \;=\; \sum_{\substack{W \text{ semi-stable} \\ G(W) \cong L_1 \oplus \cdots \oplus L_k \\ \deg(L_j)=0,\; L_j \ncong \mathcal{O}_E}} \frac{1}{|\mathrm{Aut}(W)|}\,.$$

But, by using Atiyah's classification of indecomposable bundles on elliptic curves defined over algebraic closed fields again, we know that the bundles U in the sum defining $\alpha^*_{E,i}$ are precisely the Atiyah bundles $U = \bigoplus_k I_k^{\oplus m_k}$ with $\sum k m_k = i$. Hence $\alpha^*_{E,i} = \alpha^{\mathrm{At}}_{E,i}(0)$. By the same argument, of course, we have $\beta_{E,n}(0) = \sum_{i=0}^{n} \beta^{\mathrm{At}}_{E,i}(0) \beta^*_{E,n-i}$. (Note that this time the summation starts at $i = 0$, whereas for $\alpha_{E,n}(0)$ we started at $i = 1$ because $\alpha^*_{E,0} = 0$.) Theorem 3 now follows immediately from Theorem 2.

2.4. **Proof of Theorem 4.** In this subsection, in which X is again a curve of arbitrary genus $g \geq 1$, we combine results of [5], [4] and [9] to give a closed formula for $\beta_{X,n}(0)$ for all $n \geq 1$.

The invariant $\beta_{X,n}(d)$ is periodic in d of period n by the same argument as given for $g = 1$ in the introduction. We renormalize slightly by setting

$$\widehat{\beta}_{X,n}(d) \;=\; q^{-(g-1)\,n(n-1)/2}\, \beta_{X,n}(d)\,, \qquad \widehat{\zeta}_X(s) \;=\; q^{(g-1)s}\, \zeta_X(s)\,, \tag{28}$$

(notice that these agree with $\beta_{X,n}(d)$ and $\zeta_X(s)$ in the case when $g = 1$), because this gives a simpler functional equation $\widehat{\zeta}_X(1-s) = \widehat{\zeta}_X(s)$ and will also lead to a formula in Theorem 9 that has no explicit dependence on g. We also define

$$\widehat{v}_{X,n} \;=\; \widehat{\zeta}^*_X(1) \widehat{\zeta}_X(2) \cdots \widehat{\zeta}_X(n)\,, \qquad \widehat{\zeta}^*_X(1) \;=\; \lim_{s \to 1} (1 - q^{1-s})\, \widehat{\zeta}_X(s) \tag{29}$$

instead of (13). Then the work of Harder-Narasimhan and Desale-Ramanan implies the following relation, involving an infinite summation:

Theorem. *For $n \geq 1$ and any $d \in \mathbb{Z}$ we have*

$$\sum_{k \geq 1} \sum_{\substack{n_1 + \cdots + n_k = n \\ n_1, \ldots, n_k > 0}} \Bigg(\sum_{\substack{\frac{d_1}{n_1} > \cdots > \frac{d_k}{n_k} \\ d_1 + \cdots + d_k = d}} \frac{\prod_{j=1}^{k} \widehat{\beta}_{X,n_j}(d_j)}{q^{\sum_{i<j}(d_i n_j - d_j n_i)}} \Bigg) \;=\; \widehat{v}_{X,n}\,. \tag{30}$$

This theorem is stated at page 236 of [4] (lines −9 to −4), except that there the authors use β and ζ instead of $\widehat{\beta}$ and $\widehat{\zeta}$ and write the equation in the slightly different form $\widehat{\beta}_{X,n}(d) = \widehat{v}_{X,n} -$ (sum over terms with $k \geq 2$ in (30))

to make it clear that this equation gives a recursive determination of all $\widehat{\beta}_{X,n}(d)$. This recursion relation was inverted in [9]. We state the result here in detail since in that paper only a corollary (namely, the application to the calculation of the Betti numbers of the moduli space $\mathcal{M}_{X,n}(d)$) was written out explicitly. The following theorem, however, is an immediate consequence of equation (30) and Theorem 2 of [9]. Note that here the sum is finite!

Theorem 9. *For $n \geq 1$ and any $d \in \mathbb{Z}$ we have*

$$\widehat{\beta}_{X,n}(d) \;=\; \sum_{k\geq 1}(-1)^{k-1} \sum_{\substack{n_1+\cdots+n_k=n \\ n_1,\ldots,n_k>0}} \prod_{j=1}^{k} \widehat{v}_{X,n_j} \cdot \prod_{j=1}^{k-1} \frac{q^{(n_j+n_{j+1})\,\{d(n_1+\cdots+n_j)/n\}}}{q^{(n_j+n_{j+1})}\,-\,1}\;,$$

where $\{t\}$ for $t \in \mathbb{R}$ denotes the fractional part of t.

Theorem 4 is just the special case $d = 0$ and $X = E$, since $\widehat{\beta}_{E,n} = \beta_{E,n}$.

3. The generating series of the beta invariants

3.1. **Explicit formulas.** We keep all notations as in the Introduction and §1. Recall that the Artin zeta function of E and its renormalized special value at $s = 1$ as defined by (13) are given by

$$\zeta_{E/\mathbb{F}_q}(s) \;=\; \frac{1\,-\,aq^{-s}\,+\,q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}\;, \qquad \zeta^*_{E/\mathbb{F}_q}(1) \;=\; \frac{|E(\mathbb{F}_q)|}{q-1}\;,$$

where $a \in \mathbb{Z}$ is defined by $|E(\mathbb{F}_q)| = q - a + 1$ and satisfies $|a| \leq 2\sqrt{q}$. For convenience, from now on we write simply β_n instead of $\beta_{E,n}(0)$. Note that β_n depends only on q and a and belongs to $\mathbb{Q}(q)[a]$.

The closed formula for β_n given in Theorem 4 has $\mathrm{O}(2^n)$ terms. In this subsection we will give several alternative expressions, including closed formulas with $p(n) = \mathrm{O}(e^{c\sqrt{n}})$ terms and with $\mathrm{O}(n^3)$ terms, the generating series formula (15), and a recursion permitting the calculation of $\beta_1, \ldots, \beta_n$ in $\mathrm{O}(n)$ steps. The proofs of these relations will be given in the rest of the section.

We begin by calculating the first few values of β_n from (12). Here we notice that there is considerable cancellation and that we always have

$$\beta_n \;\in\; \frac{1}{(q^n-1)\cdots(q-1)}\,\mathbb{Z}[a,q]\;, \tag{31}$$

even though the least common denominator of the denominators of the terms in (12) is much greater, e.g., the first few values of β_n are given by

$$\begin{aligned}
\beta_0 &= 1\,, \qquad \beta_1 = v_1 = \frac{q-a+1}{q-1}\,,\\
\beta_2 &= v_2 - \frac{v_1^2}{q^2-1} = \frac{(q^3-aq+1)(q-a+1)}{(q^2-1)(q-1)^2} - \frac{(q-a+1)^2}{(q^2-1)(q-1)^2}\\
&= \frac{(q-a+1)(q^2+q-a)}{(q^2-1)(q-1)}\,,\\
\beta_3 &= v_3 - 2\,\frac{v_1v_2}{q^3-1} + \frac{v_1^3}{(q^2-1)^2}\\
&= \frac{(q-a+1)(q^5+q^4-(a-2)q^3-(2a-1)q^2-(a+1)q+a^2)}{(q^3-1)(q^2-1)(q-1)}\,.
\end{aligned}$$

Some more experimentation shows that in fact much more is true, namely

$$\begin{aligned}
\beta_1 &= w_1\,, \quad \beta_2 = \frac{w_1^2 + w_2}{2}\,, \quad \beta_3 = \frac{w_1^3 + 3w_1w_2 + 2w_3}{6}\,,\\
\beta_4 &= \frac{w_1^4 + 6w_1^2w_2 + 8w_1w_3 + 3w_2^2 + 6w_4}{24}\,, \quad \dots\,,
\end{aligned}$$

where the numbers $w_m = w_{m,E} = w_m(a,q)$ $(m \ge 1)$ are defined by

$$w_m = \zeta^*_{E/\mathbb{F}_{q^m}}(1) = \frac{(\alpha^m-1)(\overline{\alpha}^m-1)}{q^m-1} \qquad (\alpha+\overline{\alpha}=a,\ \alpha\overline{\alpha}=q)\,. \tag{32}$$

These special cases suggest that the following theorem should hold:

Theorem 10. *The numbers $\beta_n = \beta_{E,n}(0)$ are given by*

$$\beta_n = \sum_{\substack{n_1,n_2,\dots\ge 0,\\ n_1+2n_2+\dots=n}} \frac{w_1^{n_1}w_2^{n_2}\cdots}{1^{n_1}2^{n_2}\cdots\, n_1!\,n_2!\,\cdots} \qquad (n \ge 0), \tag{33}$$

where the numbers $w_m = w_{E,m}$ $(m \ge 1)$ are defined by eq. (32)*.*

Equation (33) is the promised formula expressing β_n as a sum of $p(n) = \mathrm{O}(e^{\pi\sqrt{2n/3}})$ rather than $\mathrm{O}(2^n)$ terms.

To proceed further, we introduce the generating funtion

$$\mathbb{B}(x) = \mathbb{B}_{E/\mathbb{F}_q}(x) = \mathbb{B}(x;a,q) = \sum_{n=0}^{\infty} \beta_n\, x^n\,. \tag{34}$$

Then formula (33) is equivalent to the formula

$$\mathbb{B}(x) = \exp\biggl(\sum_{m=1}^{\infty} w_m\,\frac{x^m}{m}\biggr)\,,$$

and substituting for w_m from (32) we find

$$\begin{aligned}
\frac{\mathbb{B}(qx)}{\mathbb{B}(x)} &= \exp\biggl(\sum_{m=1}^{\infty}(q^m-1)\,w_m\,\frac{x^m}{m}\biggr) = \exp\biggl(\sum_{m=1}^{\infty}\frac{q^m-\alpha^m-\overline{\alpha}^m+1}{m}\,x^m\biggr)\\
&= \frac{(1-\alpha x)(1-\overline{\alpha}x)}{(1-qx)(1-x)} = \frac{1-ax+qx^2}{(1-x)(1-qx)}\,.
\end{aligned} \tag{35}$$

This in turn can be rewritten in three different ways, each of which is equivalent to Theorem 10. The first is obtained by replacing x by x/q^k in (35) and taking the product over all $k \geq 1$ to get the following multiplicative formua for the generating function $\mathbb{B}(x;a,q)$:

Theorem 11. *The generating function $\mathbb{B}(x;a,q)$ defined in* (34) *has the product expansion*

$$\mathbb{B}(x;a,q) \;=\; \prod_{k=1}^{\infty} \frac{1 \,-\, aq^{-k}x \,+\, q^{1-2k}x^2}{(1 \,-\, q^{-k}x)(1 \,-\, q^{1-k}x)} \,. \tag{36}$$

Theorem 11 is clearly equivalent to Theorem 5 of §1, by setting $x = q^{-s}$.

For the second, we recall the "q-Pochhammer symbol" $(x;q)_n$, defined for $x,\, q \in \mathbb{C}$ as $\prod_{m=0}^{n-1}(1-q^m x)$. This also makes sense for $n = \infty$ if $|q| < 1$. Since our q has absolute value greater rather than less than 1, we replace it by its inverse. Then the calculation in (35) is just a version of the "quantum dilogarithm identity"

$$\sum_{m=1}^{\infty} \frac{x^m}{m\,(q^m-1)} \;=\; \sum_{m,\,r\geq 1} \frac{q^{-rm}x^m}{m} \;=\; \log \frac{1}{(q^{-1}x;\,q^{-1})_\infty} \qquad (\,|q|>1\,)$$

(we refer to [10], pp. 28–31, for a review of the quantum dilogarithm), and equation (36) says simply

$$\mathbb{B}(x;a,q) \;=\; \frac{(q^{-1}\alpha x;\,q^{-1})_\infty\,(q^{-1}\overline{\alpha}x;\,q^{-1})_\infty}{(q^{-1}x;\,q^{-1})_\infty\,(x;\,q^{-1})_\infty} \,. \tag{37}$$

Together with the standard power series expansions of $(x;q)_\infty$ and $1/(x;q)_\infty$ as given in the survey paper just quoted, this implies the following result, which is the above-mentioned closed formula for β_n with $\mathrm{O}(n^3)$ terms.

Theorem 12. *The numbers $\beta_n = \beta_{E,n}(0)$ are given by the sum*

$$\beta_n(E/\mathbb{F}_q) \;=\; \sum_{\substack{n_1,\,n_2,\,n_3,\,n_4\geq 0\\ n_1+n_2+n_3+n_4=n}} \frac{(-1)^{n_1+n_2}\,q^{\binom{n_1+1}{2}+\binom{n_2}{2}}\,\alpha^{n_3}\,\overline{\alpha}^{n_4}}{(q;q)_{n_1}\,(q;q)_{n_2}\,(q;q)_{n_3}\,(q;q)_{n_4}} \qquad (n \geq 0)\,,$$

where α and $\overline{\alpha}$ are defined as in eq. (32).

Finally, multiplying both sides of (35) by their common denominator and comparing coefficients of x^n, we obtain:

Theorem 13. *The numbers β_n satisfy, and are uniquely determined by, the recursion relation*

$$(q^n-1)\,\beta_n \;=\; (q^n + q^{n-1} - a)\,\beta_{n-1} \;-\; (q^{n-1}-q)\,\beta_{n-2} \tag{38}$$

together with the initial conditions $\beta_0 = 1$ and $\beta_{-1} = 0$.

Theorem 13 gives the simplest algorithm for computing β_n of all the formulas we have given, since, as already mentioned, it calculates each β_n in time $\mathrm{O}(1)$ from its predecessors and hence requires time only $\mathrm{O}(n)$ to calculate all the numbers $\beta_1, \ldots, \beta_n$. We also remark that equation (38) immediately implies the assertion (31) by induction on n.

3.2. **Proof of Theorem 5: First part.** In the previous subsection we formulated four theorems, found experimentally, each of which was equivalent to the others and to Theorem 5. Of these, the simplest by far is the recursion relation (38). Unfortunately, we were not able to find a direct proof that the numbers defined by (12) satisfy this recursion, and the proof of Theorem 5 that we give will be indirect and fairly complicated.

There are two main ideas. The first is to replace the "closed formula" (12) for β_n by a recursive formula (thus in some sense undoing the calculation in [9] that led to that formula, which began with the recursion (30) and then inverted it). To do this, we break up the sum (12) into n pieces according to the value of the last n_i, i.e., we decompose β_n as

$$\beta_0 \;=\; b_0^{(0)}\,, \qquad \beta_n \;=\; \sum_{m=1}^{n} \beta_n^{(m)} \qquad (n \ge 1)\,, \tag{39}$$

where $\beta_n^{(m)} = \beta_n^{(m)}(E/\mathbb{F}_q) = \beta_n^{(m)}(a,q)$ is the partial sum defined by

$$\beta_n^{(m)} \;=\; \sum_{k=1}^{\infty} \sum_{\substack{n_1,\dots,n_{k-1}\ge 1,\ n_k=m \\ n_1+\cdots+n_k=n}} \frac{(-1)^{k-1}\, v_{n_1}\cdots v_{n_k}}{(q^{n_1+n_2}-1)\cdots(q^{n_{k-1}+n_k}-1)} \quad (n \ge m \ge 1)\,.$$

Denoting the last-but-one variable n_{k-1} in this sum by p whenever k is at least 2, we find

$$\beta_n^{(m)} \;=\; v_m \cdot \begin{cases} 1 & \text{if } m = n, \\ -\displaystyle\sum_{p=1}^{n-m} \frac{\beta_{n-m}^{(p)}}{q^{m+p}-1} & \text{if } 1 \le m \le n-1, \end{cases}$$

which defines all the numbers $\beta_n^{(m)}$ (and hence also all the numbers β_n) by recursion. Multiplying this formula by x^n and summing over all $n \ge 0$, we find that the generating functions

$$\mathbb{B}^{(m)}(x) \;=\; \mathbb{B}^{(m)}_{E/\mathbb{F}_q}(x) \;=\; \mathbb{B}^{(m)}(x;a,q) \;=\; \sum_{n=0}^{\infty} \beta_n^{(m)}\, x^n \tag{40}$$

of the $\beta_n^{(m)}$ (observe that the sum here actually starts at $n = m$, so that $\mathbb{B}^{(m)}(x) = \mathrm{O}(x^m)$, and also that $\mathbb{B}^{(0)}(x) \equiv 1$) satisfy the identity

$$\mathbb{B}^{(m)}(x) \;=\; v_m\, x^m \left(1 \,-\, \sum_{p=1}^{\infty} \frac{\mathbb{B}^{(p)}(x)}{q^{m+p}-1}\right) \qquad (m \ge 1)\,. \tag{41}$$

A natural strategy of proof would therefore be to guess a closed formula for the individual series $\mathbb{B}^{(m)}(x)$ that satisfies the same recursion and that gives (36) when summed over $m \ge 0$. Unfortunately, we were not able to do this here, so that we have to argue indirectly. The second idea is therefore to prove the identity for special values of the parameter a. Since the desired formula (36) is equivalent to the recursion (38), which is an identity among polynomials in a and therefore is true if it can be verified for infinitely many values of the argument a for each n, it is enough to prove the identity (36) only for the special values

$$a \;=\; a_k \;:=\; q^{k+1} \,+\, q^{-k} \qquad (k \in \mathbb{Z},\ \ k \ge 0)\,. \tag{42}$$

We denote by $\beta_{n,k}$ and $\beta_{n,k}^{(m)}$ the specializations of β_n and $\beta_n^{(m)}$ to this value of a, and by $\mathbb{B}_k(x)$ and $\mathbb{B}_k^{(m)}(x)$ the corresponding generating series. Then (41) specializes to the identity

$$\mathbb{B}_k^{(m)}(x) \;=\; v_{m,k}\, x^m \left(1 \,-\, \sum_{p=1}^{\infty} \frac{\mathbb{B}_k^{(p)}(x)}{q^{m+p}-1}\right) \qquad (m \ge 1,\; k \ge 0)\,, \tag{43}$$

where $v_{m,k}$ denotes the specialization of $v_m = v_m(a,q)$ to $a = a_k$, so that if we can guess some other collection of numbers $\widetilde{\beta}_{n,k}^{(m)}$ whose generating functions satisfy the same identity, then we automatically have $\beta_{n,k}^{(m)} = \widetilde{\beta}_{n,k}^{(m)}$. The reason for looking at the special value (42) is that equation (36) for this value of a says that the generating function $\mathbb{B}_k(x)$ $(k \ge 0)$ is given by

$$\mathbb{B}_k(x) \;=\; \prod_{r=1}^{\infty} \frac{\big(1-q^{-k-r}x\big)\big(1-q^{k+1-r}x\big)}{\big(1-q^{-r}x\big)\big(1-q^{1-r}x\big)} \;=\; \prod_{j=1}^{k} \frac{1\,-\,q^j x}{1\,-\,q^{-j}x} \tag{44}$$

(in particular, it is a rational function of x), and also that the numbers $v_{m,k}$ are given by

$$v_{m,k} \;=\; \begin{cases} (-1)^{m-1}\, q^{\binom{m}{2}-km}\, \dfrac{(q)_{k+m}}{(q)_m\,(q)_{m-1}\,(q)_{k-m}} & \text{if } 1 \le m \le k, \\[2ex] 0 & \text{if } m > k, \end{cases} \tag{45}$$

as one checks easily. (Here and for the rest of the section we use the notation $(x)_n$ for the q-Pochhammer symbol $(1-x)(1-qx)\cdots(1-q^{n-1}x)$, with $(x)_0 = 1$.) After a considerable amount of computer experimentation, we found that the generating function $\mathbb{B}_k^{(m)}(x)$ is given by the following closed formula.

Proposition 14. *For $k \ge 0$ and $m \ge 1$ the generating function $\mathbb{B}_k^{(m)}(x) = \mathbb{B}^{(m)}(x; a_k, q)$ is a rational function of x, equal to 0 if $m > k$ and otherwise given by*

$$\mathbb{B}_k^{(m)}(x) \;=\; (-1)^{m-1}\, \frac{(q)_{m+k}}{(q)_k (q)_{m-1}}\, \frac{x^m\, Y_k^{(m)}(x)}{D_k(x)}\,, \tag{46}$$

where $D_k(x) \in \mathbb{Z}[q,x]$ is defined by the product expansion

$$D_k(x) \;=\; \prod_{j=1}^{k} \big(q^j - x\big)$$

and where $Y_k^{(m)}(x) \in \mathbb{Z}[q,x]$ is the polynomial of degree $k-m$ defined by

$$\begin{aligned} Y_k^{(m)}(x) \;&=\; \sum_{r=0}^{k-m} q^{\binom{r+1}{2}+\binom{k-m-r+1}{2}} \begin{bmatrix} k \\ r \end{bmatrix} \begin{bmatrix} k \\ k-m-r \end{bmatrix} x^r \\ &=\; \text{Coefficient of } T^{k-m} \text{ in } \prod_{j=1}^{k} \big(1+q^jT\big)\big(1+q^jTx\big)\,. \end{aligned} \tag{47}$$

The symbol $\begin{bmatrix} k \\ r \end{bmatrix}$ used in (47) is the q-binomial coefficient $\dfrac{(q)_k}{(q)_r(q)_{k-r}}$, which occurs in the following two well-known q-versions of the binomial theorem

$$\sum_{r=0}^{k} (-1)^r q^{\binom{r}{2}} \begin{bmatrix} k \\ r \end{bmatrix} x^r \;=\; (x)_k\,, \qquad \sum_{r=0}^{\infty} \begin{bmatrix} k+r-1 \\ r \end{bmatrix} x^r \;=\; \frac{1}{(x)_k}\,, \tag{48}$$

where k denotes an integer ≥ 0. The equality of the two expressions in (47) follows from the first of these formulas.

The proof of Proposition 14 will be given in the next subsection. Here we show that it implies our main identity (36). For this, as we have already explained, it suffices to show that the sum over $m \geq 1$ of the rational functions (46) coincides with the right-hand side of (44). Combining (46) with the second of equations (47) and the second of equations (48), we find

$$\begin{aligned} \frac{1}{x}\,\frac{D_k(x)}{1-q^{k+1}} \sum_{m=1}^{\infty} \mathbb{B}_k^{(m)}(x) \;&=\; \sum_{m=1}^{k} (-x)^{m-1} \begin{bmatrix} k+m \\ k+1 \end{bmatrix} Y_k^{(m)}(x) \\ &=\; \text{Coefficient of } T^{k-1} \text{ in } \frac{\prod_{j=1}^{k}\bigl(1+q^jT\bigr)}{\bigl(1+xT\bigr)\bigl(1+q^{k+1}xT\bigr)}\,. \end{aligned}$$

But by comparing poles and residues (partial fractions decomposition), we see that

$$\begin{aligned} &\frac{\prod_{j=1}^{k}\bigl(1+q^jT\bigr)}{\bigl(1+xT\bigr)\bigl(1+q^{k+1}xT\bigr)} \\ &\;=\; \frac{\prod_{j=1}^{k}\bigl(1-q^jx^{-1}\bigr)}{\bigl(1-q^{k+1}\bigr)\bigl(1+xT\bigr)} \;+\; \frac{\prod_{j=1}^{k}\bigl(1-q^{j-k-1}x^{-1}\bigr)}{\bigl(1-q^{-k-1}\bigr)\bigl(1+q^{k+1}xT\bigr)} \;+\; P_{k-2}(T)\,, \end{aligned}$$

where $P_{k-2}(T)$ is a polynomial of degree $\leq k-2$ in T. It follows that

$$\begin{aligned} \sum_{m=1}^{\infty} \mathbb{B}_k^{(m)}(x) \;&=\; \frac{(-x)^k}{D_k(x)} \Biggl(-\prod_{j=1}^{k}(1-q^jx^{-1}) \;+\; q^{k(k+1)} \prod_{j=1}^{k}(1-q^{j-k-1}x^{-1}) \Biggr) \\ &=\; -1 \;+\; \prod_{j=1}^{k} \frac{1-q^jx}{1-q^{-j}x} \;=\; -1 \;+\; \mathbb{B}_k(x)\,, \end{aligned}$$

where the final equality is equation (44). Since $\mathbb{B}_k^{(0)}(x) = 1$, this completes the proof that the sum of the functions $\mathbb{B}^{(m)}(x)$ defined recursively by (41) coincides with the right-hand side of equation (36) and hence, by what has already been said, completes the proof of Theorem 11.

3.3. **Completion of the proof.** It remains to prove Proposition 14. For this purpose we reverse the order of the logic, taking equation (46) (with $Y_k^{(m)}(x)$ defined as 0 if $m > k$) as the *definition* of the power series $\mathbb{B}_k^{(m)}(x)$ for all $m \geq 1$ and $k \geq 0$ and then proving that these power series satisfy the identity (43). Inserting equations (44), (46) and (47) into (43), we see after

multiplying both sides by a common factor that the identity to be proved is

$$q^{km-\binom{m}{2}}\,Y_k^{(m)}(x) \;=\; \begin{bmatrix} k \\ m \end{bmatrix} D_k(x) + \frac{(q)_{k+1}}{(q)_m (q)_{k-m}} \sum_{p=1}^{k} \begin{bmatrix} k+p \\ k+1 \end{bmatrix} Y_k^{(p)}(x)\, \frac{(-x)^p}{q^{m+p}-1}\,. \tag{49}$$

But a simpler version of the same partial fraction argument as the one used above shows that $D_k(x)$ is the coefficient of T^k in $(1+xT)^{-1}\prod_{j=1}^{k}(1+q^jT)$, and one also sees without difficulty that $Y_k^{(m)}(x)$ equals $(q^{k+1}x)^{-m}$ times the coefficient of T^{k+m} in the same product $\prod_{j=1}^{k}(1-q^jT)(1-q^jTx)$ as the one used in the orginal definition (47), so that the left-hand side of (49) can be written, using the first equation in (48), as

$$\begin{aligned} q^{km-\binom{m}{2}}\,Y_k^{(m)}(x) \;&= \text{Coefficient of } T^k \text{ in} \\ &\qquad \prod_{j=1}^{k}\bigl(1+q^jT\bigr)\cdot \sum_{s=0}^{k-m} q^{\binom{s+1}{2}+ms} \begin{bmatrix} k \\ m+s \end{bmatrix} (xT)^s\,. \end{aligned}$$

The identity (49) then follows immediately from the lemma below by replacing x by xT, multiplying both sides by $\prod_{j=1}^{k}(1+q^jT)$, and comparing the coefficients of T^k on both sides.

Lemma 15. *For fixed $k \ge 0$ and $m \ge 1$, define two power series $\mathcal{F}_1(x)$ and $\mathcal{F}_2(x)$ by*

$$\begin{aligned} \mathcal{F}_1(x) \;&=\; (-qx)_k \sum_{p=1}^{\infty} \begin{bmatrix} k+p \\ k+1 \end{bmatrix} \frac{(-x)^p}{q^{m+p}-1}\,, \\ \mathcal{F}_2(x) \;&=\; \begin{bmatrix} k \\ m \end{bmatrix} (1+x)^{-1} \;-\; \sum_{s=0}^{k-m} q^{\binom{s+1}{2}+ms} \begin{bmatrix} k \\ m+s \end{bmatrix} x^s\,. \end{aligned}$$

Then

$$\mathcal{F}_2(x) \;=\; -\,\frac{(q)_{k+1}}{(q)_m (q)_{k-m}}\mathcal{F}_1(x)\,. \tag{50}$$

Proof. The power series $\mathcal{F}_1$ and $\mathcal{F}_2$ satisfy the functional equations

$$\begin{aligned} &(1+qx)\,q^m\mathcal{F}_1(qx) \;-\; (1+q^{k+1}x)\,\mathcal{F}_1(x) \\ &\quad=\; (-qx)_{k+1} \sum_{p=1}^{\infty} \begin{bmatrix} k+p \\ p-1 \end{bmatrix} (-x)^p \;=\; \frac{-x}{1+x} \end{aligned}$$

(here we have used the second of equations (48)) and

$$\begin{aligned}
&(1+qx)\,q^m\mathcal{F}_2(qx) \;-\; (1+q^{k+1}x)\,\mathcal{F}_2(x)\\
&\quad=\; \begin{bmatrix} k \\ m \end{bmatrix}\Big(q^m - \frac{1+q^{k+1}x}{1+x}\Big)\\
&\qquad\quad -\sum_{s=0}^{k-m} q^{\binom{s+1}{2}+ms}\begin{bmatrix} k \\ m+s \end{bmatrix}\Big\{\big(q^{m+s}-1\big)-\big(q^{k-m-s}-1\big)q^{s+1+m}x\Big\}\,x^s\\
&\quad=\; \begin{bmatrix} k \\ m \end{bmatrix}\Big(\big(1-q^{k+1}\big)\,\frac{x}{1+x} \;-\; \big(1-q^m\big)\Big)\\
&\qquad\quad +\;\big(1-q^k\big)\sum_{s=0}^{k+m}\begin{bmatrix} k-1 \\ m+s-1 \end{bmatrix} q^{\binom{s+1}{2}+ms}x^s\\
&\qquad\quad -\;\big(1-q^k\big)\sum_{s=0}^{k+m-1}\begin{bmatrix} k-1 \\ m+s \end{bmatrix} q^{\binom{s+2}{2}+m(s+1)}x^{s+1}\\
&\quad=\; \frac{(q)_{k+1}}{(q)_m(q)_{k-m}}\,\frac{x}{1+x} \qquad\qquad \text{(telescoping series)}\,.
\end{aligned}$$

Together these imply (50), since it is easily seen that a power series $\mathcal{F}(x)$ satisfyng $(1+qx)q^m\mathcal{F}(qx) = (1+q^{k+1}x)\mathcal{F}(x)$ for some integers $k \geq 0$ and $m \geq 1$ must vanish identically.

This completes the proof of the lemma, the proposition and hence also of Theorem 5.

4. The Riemann Hypothesis

4.1. **Proof of Proposition 6.** We can use the recursion relation (38) to give an easy inductive proof of the inequality (16), which, as we will see in a moment, implies the Riemann hypothesis for our zeta functions. Indeed, (16) holds for $n = 2$ since

$$\frac{\beta_2}{\beta_1} \;=\; \frac{q^2+q-a}{q^2-1} \;=\; 1 \,+\, \frac{N}{q^2-1}\,,$$

where $N = q - a + 1 = |E(\mathbb{F}_q)|$ satisfies $0 < N < 2q+2$, and if $n \geq 3$ and we assume by induction on n that (16) holds for $n-1$, then (38) gives

$$\frac{\beta_n}{\beta_{n-1}} \;>\; \frac{q^n+q^{n-1}-a\;-\;(q^{n-1}-q)}{q^n-1} \;=\; 1\,+\,\frac{N}{q^n-1} \;>\; 1$$

and

$$\begin{aligned}
&(q^n-1)\left(\frac{q^{n/2}+1}{q^{n/2}-1} \;-\; \frac{\beta_n}{\beta_{n-1}}\right)\\
&\quad=\; \big(q^{n/2}+1\big)^2 \;-\; \big(q^n+q^{n-1}-a\big) \;+\; \big(q^{n-1}-q\big)\,\frac{\beta_{n-2}}{\beta_{n-1}}\\
&\quad>\; 2q^{n/2}+1-q^{n-1}-(q+1)+\big(q^{n-1}-q\big)\,\frac{q^{(n-1)/2}-1}{q^{(n-1)/2}+1}\\
&\quad=\; \frac{2(q^{n-1}-q^{n/2})(q^{1/2}-1)}{q^{(n-1)/2}+1} \;>\; 0
\end{aligned}$$

(where we have again used only $|a| < q+1$, and not the stronger estimate $|a| \le 2\sqrt{q}$ given by the usual Riemann hypothesis of $E/\mathbb{F}_q$), completing the proof of (16) by induction.

In fact the estimates (16) are quite wasteful, and by a more careful analysis one finds that

$$\frac{\beta_n}{\beta_{n-1}} \;=\; 1 \,+\, \frac{(n-1)(q-a+1) \,-\, c(q)}{q^n} \,+\, \mathrm{O}\Big(\frac{n^2}{q^{2n-2}}\Big) \tag{51}$$

uniformly as $q^n \to \infty$, where $c(q) = 2+3(a-2)/q + \cdots$ is independent of n. (Recall that $a = \mathrm{O}(\sqrt{q})$.) We also remark that the bounds (16) together with the initial value $\beta_0 = 1$ give upper and lower estimates for each β_n. In particular, we have the uniform estimate

$$\beta_n \;=\; 1 \,+\, \mathrm{O}\big(1/\sqrt{q}\big)\,, \tag{52}$$

where the implicit constant is universal and can be taken, e.g., to be 3.

4.2. **Proof of the Riemann Hypothesis.** By equations (5) and (11), the polynomial $P_{E,n}(T)$ appearing in (3) is given by

$$\frac{1}{\alpha_{E,n}(0)}\,P_{E,n}(T) \;=\; 1 - \Big((Q+1) - (Q-1)\frac{\beta_{E,n}(0)}{\beta_{E,n-1}(0)}\Big)T + QT^2\,, \tag{53}$$

and by the inequalities (16) the coefficient of T in the second factor lies between -2 and $2\sqrt{Q}$. Theorem 7 follows immediately.

Notice that this argument gives much more than just the Riemann hypothesis, for which we would only need that the coefficient of T is between $-2\sqrt{Q}$ and $2\sqrt{Q}$. In fact, inserting (51) into (53), we see that the reciprocal roots of $P_{E,n}(T)$, divided by $q^{n/2}$, are not uniformly distributed on the unit circle, but are actually very near to i and $-i$ for n large. In a related direction, we mention that, since each $\beta_{E,n}(a)$ is completely determined by n, q and a, the usual Sato-Tate distribution property for the roots of the local zeta functions of the reductions $\bar{E}/\mathbb{F}_p$ at varying primes p of an elliptic curve E defined over $\mathbb{Q}$ implies a corresponding explicit Sato-Tate distribution for the roots of the higher zeta-functions $\zeta_{\bar{E}/\mathbb{F}_p,\,n}$ as p varies with n fixed, and also, after a suitable renormalization, as $n \to \infty$.

5. Complements

The most important consequence of Theorem 5, of course, is the Riemann hypothesis for the higher rank zeta functions $\zeta_{E,n}(s)$, but the theorem has several other corollaries that seem to be of independent interest. We end the paper by listing some of these.

The first statement concerns the analytic continuation and functional equation of the Dirichlet series $\mathfrak{Z}_{E/\mathbb{F}_q}(s)$ defined by equation (14).

Corollary 16. *The function $\mathfrak{Z}_{E/\mathbb{F}_q}(s)$ continues meromorphically to the entire complex plane and satisfies the functional equation*

$$\mathfrak{Z}_E(s-1) \;=\; \zeta_E(s)\,\mathfrak{Z}_E(s)\,. \tag{54}$$

Proof. The meromorphic continuation is obvious from equation (15), since $\zeta_E(s)$ is meromorphic and tends rapidly to 1 as $\Re(s) \to +\infty$. The functional equation (54) then follows tautologically from equation (15). □

Corollary 17. *The meromorphic function defined by*

$$\mathfrak{Z}^{\pm}_{E/\mathbb{F}_q}(s) \;=\; \mathfrak{Z}_{E/\mathbb{F}_q}(s)\,\mathfrak{Z}_{E/\mathbb{F}_q}(-s) \tag{55}$$

is invariant under $s \mapsto s+1$.

Proof. This follows from (54) and the functional equation of $\zeta_{E/\mathbb{F}_q}(s)$:

$$\frac{\mathfrak{Z}^{\pm}_{E/\mathbb{F}_q}(s-1)}{\mathfrak{Z}^{\pm}_{E/\mathbb{F}_q}(s)} \;=\; \frac{\mathfrak{Z}_{E/\mathbb{F}_q}(s-1)}{\mathfrak{Z}_{E/\mathbb{F}_q}(s)}\,\frac{\mathfrak{Z}_{E/\mathbb{F}_q}(1-s)}{\mathfrak{Z}_{E/\mathbb{F}_q}(-s)} \;=\; \frac{\zeta_{E/\mathbb{F}_q}(s)}{\zeta_{E/\mathbb{F}_q}(1-s)} \;=\; 1\,.$$

Alternatively, we could apply the functional equation of $\zeta_{E/\mathbb{F}_q}(s)$ to each factor of the infinite product defining $\mathfrak{Z}_{E/\mathbb{F}_q}(-s)$ to write $\mathfrak{Z}^{\pm}_{E/\mathbb{F}_q}(s)$ as the absolutely convergent doubly infinite product $\prod_{n\in\mathbb{Z}} \zeta_{E/\mathbb{F}_q}(s+n)$, from which the periodicity is obvious. □

There is a curious relation between Corollary 17 and the theory of elliptic curves over $\mathbb{C}$. Denote by $\theta(x;q^{-1})$ the Jacobi theta function

$$\theta(x;\,q^{-1}) \;=\; \sum_{n\in\mathbb{Z}+\frac{1}{2}} (-1)^{[n]}\,q^{-n^2/2}\,x^n \qquad (q,\,x\in\mathbb{C}^*,\;\; |q|>1)\,.$$

It has the well-known elliptic transformation property

$$\theta(qx;\,q^{-1}) \;=\; -\,q^{1/2}\,x\,\theta(x;\,q^{-1}) \tag{56}$$

saying that the function $\theta(e^{2\pi i z};e^{2\pi i\tau})$ is doubly periodic, up to simple non-vanishing factors, with respect to translation of $z\in\mathbb{C}$ by the lattice $\mathbb{Z}\tau+\mathbb{Z}$. The Jacobi triple product formula is the formula

$$\theta(x;q^{-1}) \;=\; q^{-1/8}x^{1/2}\,(q^{-1};\,q^{-1})_\infty\,(q^{-1}x;\,q^{-1})_\infty\,(x^{-1};\,q^{-1})_\infty$$

expressing $\theta(x;q^{-1})$ as a product of three infinite q-Pochhammer symbols. Combining this with equation (37), we find that the symmetrized zeta function (55) is related to the Jacobi theta function by

$$\mathfrak{Z}^{\pm}_{E/\mathbb{F}_q}(s) \;=\; \frac{1}{\alpha}\,\frac{\theta(\alpha q^{-s};\,q^{-1})\,\theta(\alpha q^{s};\,q^{-1})}{\theta(q^{-s};\,q^{-1})\,\theta(q^{s};\,q^{-1})}\,, \tag{57}$$

so that the periodicity statement of Corollary 17 can also be seen as a consequence of the elliptic transformation property (56) of $\theta(x;q^{-1})$. This gives some kind of connection between the zeta function of an elliptic curve E over $\mathbb{F}_q$ and the theory of elliptic functions for the elliptic curve $\mathbb{C}^*/q^{\mathbb{Z}}$ over $\mathbb{C}$.

In the next statement, our result for elliptic curves over finite fields is used to motivate the definition of a new zeta function for elliptic curves defined over $\mathbb{Q}$, and to prove a factorization result for this function.

Corollary 18. *Let E be an elliptic curve over $\mathbb{Q}$, and define $\{b_m(E/\mathbb{Q})\}_{m\in\mathbb{N}}$ as the multiplicative function with $b_{p^n}(E/\mathbb{Q}) = \beta_n(E/\mathbb{F}_p)$. Then the Dirichlet series $\mathfrak{Z}_{E/\mathbb{Q}}(s)$ defined for $s \in \mathbb{C}$ with $\Re(s) > 1$ by*

$$\mathfrak{Z}_{E/\mathbb{Q}}(s) \;=\; \sum_{m=1}^{\infty} \frac{b_m(E/\mathbb{Q})}{m^s} \;=\; \prod_{p \text{ prime}} \mathfrak{Z}_{E/\mathbb{F}_p}(s)$$

continues meromorphically to all s and has the product expansion

$$\mathfrak{Z}_{E/\mathbb{Q}}(s) \;=\; \prod_{k=1}^{\infty} \zeta_{E/\mathbb{Q}}(s+k)\;.$$

We do not know whether these higher global zeta functions have other interesting properties.

The final corollary of Theorem 5 that we will give concerns the limiting values of the invariants we have been studying. To explain it properly, we must first recall the geometric meaning of the numbers $v_{E,n}$ occurring in Theorem 4. In (13) these numbers were simply defined as the products of the values of $\zeta_{E/\mathbb{F}_q}(s)$ at $s = 1, \dots, n$ (with the value at the pole $s = 1$ being replaced by a suitable limit), because this was all that was necessary for our purposes. But that formula is actually a theorem, due to Desale and Ramanan in the paper [4] already quoted, rather than a definition. In fact, $v_{E,n}$ is $v_{E,n}(0)$, where $v_{X,n}(d)$ is defined, for all curves $X/\mathbb{F}_q$ and for all integers $n > 0$ and d, by

$$v_{X,n}(d) \;=\; \sum_{\text{all } [V]} \frac{1}{|\mathrm{Aut}(V)|}\;,$$

i.e., by the same summation as $\beta_{X,n}(d)$ in (1), but with the summation now ranging over all isomorphism classes of $\mathbb{F}_q$-rational vector bundles of rank n and degree d rather than just the semi-stable ones. Using the fact that the Tamagawa number of $\mathrm{SL}(n)$ equals 1, one shows (Proposition 1 of [4], summed over all $|\mathrm{Pic}^0(X)(\mathbb{F}_q)| = (q-1)\widehat{\zeta}_X^*(1)$ possible values of the determinant) that $v_{X,n}(d) = q^{(g-1)\,n(n-1)/2}\,\widehat{v}_{X,n}$ (independent of d!) with $\widehat{v}_{X,n}$ defined as in (29), i.e., $v_{X,n}(d)$ is related to $\widehat{v}_{X,n}$ in the same way as $\beta_{X,n}(d)$ and $\widehat{\beta}_{X,n}(d)$ are related in (28). Note that this formula includes as a special case the formula $v_{E/\mathbb{F}_q}(n,0) = v_{E,n}$ mentioned above. Also, since semi-stable bundles form a subset of all bundles, it is clear from the geometric definition that $\beta_{X,n}(d) \le v_{X,n}(d)$ and $\widehat{\beta}_{X,n}(d) \le \widehat{v}_{X,n}$ for all n, with equality if $n = 1$.[1] (This is also visible in the Harder-Narasimhan-Desale-Ramanan recursion (30), in which the $k = 1$ term on the left equals $\widehat{\beta}_{X,n}(d)$.) Therefore the following result can be interpreted as saying that, at least in the case of elliptic curves, "almost all bundles of large rank are semi-stable."

Corollary 19. *The limiting values $\beta_{E,\infty} := \lim_n \beta_{E,n}$ and $v_{E,\infty} := \lim_n v_{E,n}$ of the sequences $\{\beta_{E,n}(0)\}$ and $\{v_{E,n}\}$ exist and coincide, with the value*

$$\beta_{E,\infty} \;=\; v_{E,\infty} \;=\; \zeta_E^*(1)\,\zeta_E(2)\,\zeta_E(3)\,\cdots\,. \tag{58}$$

[1] From (13) and Proposition 6 we also have the inequalities $v_{E,1} < v_{E,2} < \cdots$ and $\beta_{E,1} < \beta_{E,2} < \cdots$, for which there does not seem to be an obvious geometric explanation.

Of course the uniform bound for the numbers β_n that we gave in (52) also holds for the limiting value β_∞.

Just for fun, we mention that the analogue of the product appearing on the right-hand side of (58) when the function field $\mathbb{F}_q(E)$ is replaced by the number field $\mathbb{Q}$ is the number $\prod_{n=2}^{\infty}\zeta(n) \;=\; 2.2948565916733\cdots$, which has a well-known interpretation as the average number of abelian groups of given order. It would be interesting to know whether the product occurring in (58), or its global analogue

$$\mathrm{Res}_{s=0}\big(\mathfrak{Z}_{E/\mathbb{Q}}(s)\big) \;=\; \mathrm{Res}_{s=1}\big(\zeta_{E/\mathbb{Q}}(s)\big)\cdot\prod_{m=2}^{\infty}\zeta_{E/\mathbb{Q}}(m)\,,$$

has any similar geometrical or arithmetical interpretation. In particular, as was suggested to us by Christopher Deninger, one can ask whether there is any connection with the famous Cohen-Lenstra class number heuristics. (Compare equation (15) with Theorem 3.2 (ii) of [2], or Corollary 17 with Theorem 7.1 of [3].)

6. Acknowledgments

The first author would like to thank the JSPS, which partially supported this work. The authors would also like to thank the Max Planck Institute for Mathematics and Kyushu University for providing excellent research environments.

References

[1] M.F. Atiyah, Vector bundles over an elliptic curve. Proc. London Math Soc (3) **7** (1957), 414–452.

[2] H. Cohen and H.W. Lenstra, Jr., Heuristics on class groups. In *Number Theory, New York, 1982*, Lecture Notes in Math. **1052**, Springer, Berlin (1984) 26–36.

[3] H. Cohen and H.W. Lenstra, Jr., Heuristics on class groups of number fields. In *Number Theory Noordwijkerhout 1983*, Lecture Notes in Math. **1068**, Springer, Berlin (1984) 33–62.

[4] U.V. Desale and S. Ramanan, Poincaré polynomials of the variety of stable bundles. Math. Annalen **26** (1975), 233–244.

[5] G. Harder and M.S. Narasimhan, On the cohomology groups of moduli spaces of vector bundles on curves. Math. Annalen **212** (1975), 215-248.

[6] K. Sugahara, A relation for bundle counting. In preparation.

[7] L. Weng, Non-abelian zeta function for function fields. Amer. J. Math. **127** (2005), 973–1017.

[8] L. Weng, Zeta functions for curves over finite fields. Preprint, arXiv:1202.3183.

[9] D. Zagier, Elementary aspects of the Verlinde formula and the Harder-Narasimhan-Atiyah-Bott formula. Israel Mathematical Conference Proceedings **9** (1996), 445–462.

[10] D. Zagier, The dilogarithm function. In *Frontiers in Number Theory, Physics and Geometry II*, P. Cartier, B. Julia, P. Moussa, P. Vanhove (eds.), Springer-Verlag, Berlin-Heidelberg-New York (2006), 3–65.

Graduate School of Mathematics, Kyushu University, Fukuoka, Japan
E-Mail: weng@math.kyushu-u.ac.jp

Max-Planck Institute für Mathematik, Bonn, Germany
and Collège de France, Paris, France
E-Mail: dbz@mpim-bonn.mpg.de