Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 336 (2003) 289–292

Number Theory/Algebraic Geometry

On the irreducibility of the two variable zeta-function for curves over finite fields

Sur l'irréductibilité de la fonction zêta d'une courbe définie sur un corps fini

Niko Naumann

Institut für Mathematik, Einsteinstrasse 62, 48149 Münster, Germany

Received 16 October 2002; accepted 14 January 2003

Presented by Christophe Soulé

Abstract

R. Pellikaan (Arithmetic, Geometry and Coding Theory, Vol. 4, Walter de Gruyter, Berlin, 1996, pp. 175–184) introduced a two variable zeta-function $Z(t,u)$ for a curve over a finite field $\mathbb{F}_q$ which, for $u=q$, specializes to the usual zeta-function and he proved rationality: $Z(t,u)=(1-t)^{-1}(1-ut)^{-1}P(t,u)$ with $P(t,u)\in\mathbb{Z}[t,u]$. We prove that $P(t,u)$ is absolutely irreducible. This is motivated by a question of J. Lagarias and E. Rains about an analogous two variable zeta-function for number fields. ***To cite this article: N. Naumann, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

Résumé

R. Pellikaan (Arithmetic, Geometry and Coding Theory, Vol. 4, Walter de Gruyter, Berlin, 1996, pp. 175–184) a introduit une fonction zêta $Z(t,u)$ en deux variables pour une courbe définie sur un corps fini $\mathbb{F}_q$. Pour $u=q$ on obtient la fonction zêta habituelle et Pellikaan démontre que $Z(t,u)$ est une fonction rationelle : $Z(t,u)=(1-t)^{-1}(1-ut)^{-1}P(t,u)$ où $P(t,u)\in\mathbb{Z}[t,u]$. Nous démontrons que $P(t,u)$ est absolument irréductible. Nous avons été motivés par une question de J. Lagarias et E. Rains concernant une fonction zêta en deux variables analogue pour des corps de nombres. ***Pour citer cet article : N. Naumann, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

1. Introduction

Let X be a proper, smooth, geometrically connected curve of genus g over the finite field $\mathbb{F}_q$. The zeta-function of $X/\mathbb{F}_q$ can be written as a power series

E-mail address: naumannn@uni-muenster.de (N. Naumann).

1631-073X/03/$ – see front matter
doi:10.1016/S1631-073X(03)00039-6

$$Z(t) = \sum_D \frac{q^{h^0(D)} - 1}{q - 1} t^{\deg(D)}.$$

Here the sum is over $\mathbb{F}_q$-rational divisor classes of X and $h^0(D) := \dim_{\mathbb{F}_q} H^0(X, \mathcal{O}(D))$.

Writing b_{nk} for the number of divisor classes of degree n and with $h^0(D) = k$ this becomes

$$Z(t) = \sum_{n \geqslant 0} \sum_{k \geqslant 1} b_{nk} \frac{q^k - 1}{q - 1} t^n.$$

In [6] R. Pellikaan observed that the classical proof of rationality and the functional equation for $Z(t)$ go through when q is treated as a variable in this expression. He thus introduced the following power series in [6], Definition 3.1:

$$Z(t, u) := \sum_{n \geqslant 0} \sum_{k \geqslant 1} b_{nk} \frac{u^k - 1}{u - 1} t^n.$$

This is called the two variable zeta-function of the curve. We will denote by h the class-number of $X/\mathbb{F}_q$, i.e., $h = |\operatorname{Pic}^0(X)|$. Then Pellikaan proved:

Theorem 1.1. *We have*: $Z(t, u) = (1 - t)^{-1}(1 - ut)^{-1} P(t, u)$ *with* $P \in \mathbb{Z}[t, u]$. *Furthermore*:

(1) $\deg_t P = 2g$, $\deg_u P = g$.
(2) *In the expansion* $P(t, u) = \sum_{i=0}^{2g} P_i(u) t^i$ *one has* $P_0(u) = 1$, $\deg_u P_i(u) \leqslant i/2 + 1$ *and* $P_{2g-i}(u) = u^{g-i} P_i(u)$ *for* $0 \leqslant i \leqslant 2g$.
(3) $P(1, u) = h$.

Here $\deg_u$ and $\deg_t$ denote the degree of a polynomial in the indicated variable. The above results are all taken from [6], Proposition 3.5, and we copied only those needed later on. Note that the statement $\deg_u P_i(u) \leqslant i/2$ in [loc. cit.] is a misprint. Indeed, we will see below that one always has $\deg_u P_1(u) = 1$ (unless $g = 0$). As expected we have $P(t, u) = 1$ in case $g = 0$.

We note that Theorem 1.1(2) means that the familiar functional equation holds true:

$$Z(t, u) = u^{g-1} t^{2g-2} Z\left(\frac{1}{tu}, u\right).$$

In [3] van der Geer and R. Schoof used analogies from Arakelov-theory to define a two variable zeta-function for number fields along the above lines. As the number field case will serve only as a motivation in this note we refer to the original sources [3] and [5] for definitions and to [1] for a comparison between them. Suffice it to say that in [5], Section 8, we find an entire function $\xi_{\mathbb{Q}}(w, s)$ of two complex variables which for $w = 1$ equals Riemann's ξ-function. In particular, the zeroes of $\xi_{\mathbb{Q}}(1, s)$ are precisely the non-trivial zeros of the Riemann zeta-function. One is thus led to study the zero-locus of $\xi_{\mathbb{Q}}(w, s)$. Lagarias and Rains [5] ask whether it might be the closure of a single irreducible complex-analytic variety of multiplicity one. The corresponding question in the geometric case seems to be whether the zero-locus of $P(t, u)$ is irreducible. This is indeed the case:

Theorem 1.2. *In the above situation,* $P(t, u)$ *is irreducible in* $\mathbb{C}(u)[t]$.

Note that the usual L-series of $X/\mathbb{F}_q$ $L(t) = P(t, q) \in \mathbb{Z}[t]$ may well be reducible. For example, if X is an elliptic curve the fundamental result of Tate [7] shows that L is reducible over $\mathbb{Q}$ if and only if X is supersingular and all of its endomorphisms are defined over $\mathbb{F}_q$.

As an illustration of Theorem 1.2 we discuss the cases $g = 1$ and $g = 2$:

For $g = 1$ setting $N := |X(\mathbb{F}_q)|$ we have $P(t,u) = 1+(N-1-u)t+ut^2$, cf. [6], Example 3.4. This polynomial is reducible in $\mathbb{C}(u)[t]$ if and only if $N = 0$ in which case we have $P(t,u) = (1-t)(1-ut)$. But it is well known that a curve of genus one over a finite field always has a rational point, i.e., $N \neq 0$.

In case $g = 2$ let the usual zeta-function of X be $Z(t) = (1-t)^{-1}(1-qt)^{-1}L(t)$ with $L(t) = 1+at+bt^2+qat^3+q^2t^4$ for certain $a, b \in \mathbb{Z}$. As X is hyperelliptic, Proposition 4.3. of [6] can be used to compute

$$P(t,u) = 1+\big((a+q)-u\big)t+\big(\big(q(q-1)+aq+b\big)-(a+q-1)u\big)t^2+\big((a+q)-u\big)ut^3+u^2t^4.$$

This will not be used in the sequel and we omit the proof.

In order not to lead intuition astray we point out that in general $Z(t,u)$ is not determined by $Z(t)$, see [6], Example 4.4.

After a lengthy computation with discriminants one sees that a neccessary condition for this $P(t,u)$ to be reducible is $b+a(q+1)+(q^2+1) = 0$. However, this expression equals $L(1) = h \neq 0$!

The fact that $h \neq 0$ enters in the general proof of Theorem 1.2 precisely through the condition $\beta \neq 0$ of Lemma 2.1 below. Note, however, that condition (2) of this lemma cannot be dropped. So one needs one more result on $P(t,u)$, contained in Proposition 2.2, which follows from Clifford's theorem.

2. Proof

We will use the following criterion for irreducibility:

Lemma 2.1. *Let k be a field, $F \in k[u,t]$ and assume*:

(1) *F is monic in t;*
(2) *the leading coefficient of F as a polynomial in u is irreducible in $k[t]$;*
(3) *there are $\alpha, \beta \in k$, $\beta \neq 0$ with $F(u,\alpha) = \beta$.*

Then F is irreducible in $k(u)[t]$.

This lemma will be applied to $F = \widetilde{P}(t,u) := t^{2g}P(t^{-1},u) \in \mathbb{C}[u,t]$. Note that the irreducibility of $\widetilde{P}$ in $\mathbb{C}(u)[t]$ will imply the irreducibility of P because $P(0,u) = P_0(u) = 1 \neq 0$ by Theorem 1.1. The advantage of $\widetilde{P}$ is that it is monic in t and so satisfies condition (1) of Lemma 2.1. Also (3) is satisfied (with $\alpha = 1$, $\beta = h$) according to Theorem 1.1(3).

Proof of Lemma 2.1. Assume to the contrary that $F = fg$ in $k(u)[t]$ with f and g of positive degree and monic. One knows, cf., for example, [2], Proposition 4.11, that the coefficient of f and g are integral over $k[u]$ and as $k[u]$ is integrally closed we have $f, g \in k[u,t]$. So we can consider the decomposition $F = fg$ as polynomials in u and infer from (2) that the leading coefficient of f as a polynomial in u lies in $k[t]^* = k^*$ (upon exchanging f and g if neccessary). In particular $n := \deg_u f(u,t) = \deg_u f(u,\alpha)$. Substituting (3) gives $\beta = f(u,\alpha)g(u,\alpha)$ in $k[u]$. As $\beta \neq 0$ we get $n = 0$, i.e., f is constant in u hence $f \in k^*$, contradiction. □

We are left with verifying condition (2) of Lemma 2.1 for the given $\widetilde{P}$, i.e., the leading coefficient of $\widetilde{P}$ as a polynomial in u is irreducible in $k[t]$. We will in fact determine this coefficient:

Proposition 2.2. *For $g \geqslant 1$: $\widetilde{P}(t,u) = (1-t)u^g + \mathrm{O}(u^{g-1})$.*

Proof. We already know $\deg_u \widetilde{P} = g$. Also the assertion is clear for $g = 1$ from the formula for $P(t,u)$ recalled in the introduction. We assume $g \geqslant 2$. Looking at

$$\widetilde{P}(t,u) = t^{2g} + P_1(u)t^{2g-1} + \cdots + P_g(u)t^g + uP_{g-1}(u)t^{g-1} + \cdots + u^g t^0$$

and using the bound $\deg_u P_i(u) \leqslant i/2+1$ we see that u^g can only occur in the last three terms: $u^{g-2}P_2(u)t^2 + u^{g-1}P_1(u)t + u^g$. So the proof is completed by the following result on P_1 and P_2. □

Proposition 2.3. *For $g \geqslant 1$:*

(1) $\deg_u P_1(u) = 1$ *and the leading coefficient is* -1.
(2) $\deg_u P_2(u) \leqslant 1$.

Proof. This is again clear for $g = 1$. We assume $g \geqslant 2$ and write $P_i(u) = \sum_k \alpha_{ik} u^k$, $\alpha_{ik} \in \mathbb{Z}$. As we already know $\deg_u P_1(u) \leqslant 1$ and $\deg_u P_2(u) \leqslant 2$ we need to show $\alpha_{11} = -1$ and $\alpha_{22} = 0$. Recalling the notation b_{nk} from the introduction we have the following

Claim. $b_{12} = \alpha_{00} + \alpha_{11}$ *and* $b_{23} = \alpha_{00} + \alpha_{11} + \alpha_{22}$.

Granting this we observe that Clifford's thorem, cf. [4], IV, Theorem 5.4, gives $b_{12} = b_{23} = 0$. Recalling also $\alpha_{00} = 1$, because $P_0(u) = 1$, and substituting gives indeed $\alpha_{11} = -1$ and $\alpha_{22} = 0$. □

To prove the above claim we write the rational expression for $Z(t, u)$ in Theorem 1.1 in terms of coefficients:

$$Z(t,u) = \sum_{n\geqslant 0}\sum_{k\geqslant 1} b_{nk}\frac{u^k-1}{u-1}t^n = \left(\sum_{i\geqslant 0} t^i\right)\left(\sum_{j\geqslant 0}(ut)^j\right)\left(\sum_{l\geqslant 0}\sum_{k\geqslant 0}\alpha_{lk}u^k t^l\right).$$

This gives

Lemma 2.4.

(1) *for* $\nu,\alpha \geqslant 0$: $\sum_{k\geqslant \alpha+1} b_{\nu k} = \sum_{\mu,i\geqslant 0,\mu+i\leqslant \nu} \alpha_{i,\alpha-\mu}$,
(2) *for* $\nu \geqslant 0$, $\mu \geqslant 1$: $b_{\nu\mu} = \sum_{i=0}^{\nu}(\alpha_{i,\mu-\nu-1+i} - \alpha_{i\mu})$.

We omit the details of this straightforward computation except to say that for (1) one uses $(u^k - 1)/(u - 1) = 1 + \cdots + u^{k-1}$ and (2) follows from (1) by a telescope-summation. In the formulation of the lemma it is understood that $\alpha_{nk} = 0$ whenever $k < 0$. We get from (2):

$$b_{23} = \alpha_{00} - \alpha_{03} + \alpha_{11} - \alpha_{13} + \alpha_{22} - \alpha_{23} \quad \text{and} \quad b_{12} = \alpha_{00} - \alpha_{02} + \alpha_{11} - \alpha_{12}.$$

However, we know $\alpha_{02} = \alpha_{03} = \alpha_{12} = \alpha_{13} = \alpha_{23} = 0$ because $\deg_u P_i(u) \leqslant i/2 + 1$.

This concludes the proof of the claim, hence of Theorem 1.2.

Acknowledgements

I would like to thank C. Deninger for posing the above problem and for useful discussions on the topic and J. Lagarias for suggesting improvements of a first draft of this Note.

References

[1] C. Deninger, Two-variable zeta functions and regularized products, Preprint, 2002.
[2] D. Eisenbud, Commutative Algebra with a View Towards Algebraic Geometry, in: Graduate Texts in Math., Vol. 150, Springer, New York, 1995.
[3] G. van der Geer, R. Schoof, Effectivity of Arakelov divisors and the theta divisor of a number field, Selecta Math. (N.S.) 6 (4) (2000) 377–398.
[4] R. Hartshorne, Algebraic Geometry, in: Graduate Texts in Math., Vol. 52, Springer, New York, 1977.
[5] J. Lagarias, E. Rains, On a two-variable zeta function for number fields, arXiv:math.NT/0104176, v5, 7 July 2002.
[6] R. Pellikaan, On special divisors and the two variable zeta function of algebraic curves over finite fields, in: Arithmetic, Geometry and Coding Theory, Vol. 4, Luminy, 1993, W. de Gruyter, Berlin, 1996, pp. 175–184.
[7] J. Tate, Endomorphisms of Abelian varieties over finite fields, Invent. Math. 2 (1966) 143–144.