



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



Families of curves with Galois action and their L -functions



Cornelius Greither

*Institut für Theoretische Informatik und Mathematik, Universität der Bundeswehr,
München, 85577 Neubiberg, Germany*

ARTICLE INFO

Article history:

Received 26 February 2014
Received in revised form 24
February 2015
Accepted 24 February 2015
Available online 4 April 2015
Communicated by Gebhard Böckle

MSC:

11M38
11G20
11G25
11G45
14F30

Keywords:

Picard 1-motives
Class groups
Galois coverings
Equivariant L -functions
Galois module structure
Fitting ideals

ABSTRACT

We generalise results of Chris Hall on the L -function of curves E over characteristic p function fields K , by using equivariant L -functions and cohomologically trivial modules. In fact, K will be the rational function field over a fixed finite field most of the time. The curves which we can treat are superelliptic curves which come as Galois covers of prime degree of the projective line over K . We are thus able to determine the degree of the L -function (which is a polynomial in our situation), and sometimes we get upper bounds on the analytic rank.

© 2015 Elsevier Inc. All rights reserved.

E-mail address: cornelius.greither@unibw.de.

<http://dx.doi.org/10.1016/j.jnt.2015.02.015>

0022-314X/© 2015 Elsevier Inc. All rights reserved.

0. Introduction

In the paper [Ha], Chris Hall looked at the Hasse–Weil L -function $L(T, E/K)$ of certain elliptic curves over the function field K of a curve C over a fixed finite field \mathbb{F}_q , assuming that the j -invariant of E is not constant. In other words, he considered a nontrivial family of curves indexed with the points of C , where almost all fibres are elliptic curves, and a finite number of fibres may be singular. For the computation of the L -function it is practical to fix a Weierstraß model $\mathcal{E} \rightarrow C$. The special case $C = \mathbb{P}^1$ is of central importance in Hall’s paper, and we shall essentially restrict ourselves to this situation.

One of the main results of Hall concerns a family of elliptic curves over C (with finitely many singular fibres) given by a simple Legendre equation. Cleverly using the presence of 2-torsion points in the fibres, he proved a congruence modulo 2 for the L -function, which is in fact a polynomial. This gives the degree of $L(T, E/K)$ at once, some information about the analytic rank of E/K , and in some cases actually a verification of the rank part of the Birch–Swinnerton-Dyer conjecture.

Hall’s arguments are basically very explicit. It is our goal here to demonstrate that these results are underpinned by Galois theory and cohomology, and that they can be generalised to superelliptic curves that are cyclic covers of the projective line \mathbb{P}_K^1 , if one is willing to accept some technical hypotheses. In this approach cohomologically trivial modules play a big role. Our philosophy can be summarised in two statements. (1) Equivariant L -functions that are constructed using cohomologically trivial modules have better integrality properties over the group ring than L -functions which are constructed via the characters of the group and then assembled. (2) Integrality of an object over the group ring translates into congruences between the images of that object under the characters of the group. (We are not claiming that either of these statements is at all new.) This underpinning by module-theoretic concepts is one main difference with respect to Hall’s paper. The other major difference is the fact that for more general curves there is no fast and simple analog of the minimal Weierstraß model of an elliptic curve, so new technicalities arise; we will say a little more on this near the end of the introduction.

Our main general result may be stated as follows, omitting a few details now. We consider a superelliptic curve E/K over $K = \mathbb{F}_q(t)$ which is not constant (that is, not induced from a curve over \mathbb{F}_q) and comes as a cyclic cover of the projective line \mathbb{P}_K^1 , with $K = \mathbb{F}_q(t)$ the function field of the projective line over \mathbb{F}_q . This projective line with coordinate t is written C , so $K = \mathbb{F}_q(C) = \mathbb{F}_q(t)$. We continue to denote the curve over K by E , even though it need not be an elliptic curve; its genus g_E will usually be greater than 1. The curve E is given by an affine equation

$$y^r = (x - f_1(t)) \cdots (x - f_d(t)),$$

where r is a fixed natural number dividing $q - 1$ and greater than 1, and the $f_i(t)$ are pairwise distinct polynomials in $\mathbb{F}_q[t]$. Then E is a cyclic Galois cover of \mathbb{P}_K^1 of degree r ; the Galois group will be denoted G throughout.

The main technical hypothesis we need to make concerns an integral model \mathcal{E} of this curve; we have to assume that it has only rational singularities. The discussion of criteria for rational singularities occupies Section 2. For reasons of simplicity we assume r prime in later sections (even though this might be unnecessary if one is willing to accept more complicated statements), and we then actually write ℓ for r , since we will deal with cohomology, and it is customary to speak of ℓ -adic (not r -adic) cohomology. Then at the end of Section 4 we obtain a congruence for the Hasse–Weil L -function of the curve:

$$L(T, E/K) \equiv (1 - T)^{2-2d+\kappa} \text{ modulo } \ell,$$

where κ is an explicit natural number counting the nodes in the ramification divisor of $\mathcal{E} \rightarrow \mathbb{P}_C^1$. For instance if we look at Hall’s Legendre curve $y^2 = x(x-1)(x-t)$, the ramification divisor of $E \rightarrow \mathbb{P}_C^1$ is the union of four sections $(x, y) : \mathbb{P}_C^1 \rightarrow E$ of $E \rightarrow \mathbb{P}_C^1$ given by $x = 0, 1, t, \infty$ and $y = 0$. In this ramification locus there are two simple nodes at $t = 0$ and $t = 1$: the $x = 0$ (resp. $x = 1$) section meets the $x = t$ section. Moreover the three sections $x = 1, t, \infty$ meet over $t = \infty$. (The last statement is not entirely obvious; one finds that the $x = 1$ section meets the $x = \infty$ section when one puts $s = 1/t$ and transforms the equation at $s = 0$ into standard Weierstraß form, see the details in Subsection 1.1.) Here we obtain $\kappa = 4$ and $L(T, E/K) \equiv 1$. Since the L -function is a polynomial and its leading coefficient is known (and not zero mod ℓ), this implies, as already obtained by Hall, that the L -function is 1 itself. In the above congruence one needs the assumption that all nodes in the ramification divisor are \mathbb{F}_q -rational, but one also gets interesting congruences (actually more useful ones in order to majorise the analytic rank) without this assumption. In particular, we exhibit in Section 5 a class of superelliptic curves E/K with arbitrary prime degree ℓ of the covering, such that the analytic rank is bounded above by $2(\ell - 1)g_E$.

Our starting point is the construction of certain cohomologically trivial $\mathbb{Z}_\ell[G]$ -modules attached to smooth curves over finite fields, see [GP]. The characteristic polynomial of Frobenius on these modules is close to the L -function of the curve and has better integrality properties. We generalise this construction to singular curves over finite fields in Section 3, and then to the relative situation in Section 4: here we have to work with an integral model $\mathcal{E} \rightarrow C$, which is a family of curves over the base C (which is \mathbb{P}^1), with smooth generic fibre and finitely many singular fibres. Before, we discuss our choice of integral model \mathcal{E} and in particular its singularities in detail (Section 2). We need all singularities to be rational, in order to have the “correct” geometrical interpretation of the local factors of the L -function at places $v \in C$ with singular fibre \mathcal{E}_v . The conditions ensuring this are rather explicit and easy to manage, but establishing them does take some space. In a final section we deduce consequences concerning the degree of the L -function and the analytic rank, and we discuss several examples in detail. We remark

that it would appear more natural to work with “the” minimal regular proper model of E over C . (In writing “the” we assume C has positive genus.) But we need to keep things very explicit, and so we pay the price of working with a possibly non-regular model \mathcal{E} . Via our verification of rationality of singularities, a regular model is lurking in the background, but we do not want to look at it too closely.

It should be noted that our approach gives upper bounds on the analytic rank of the Jacobian $J_{E/K}$, likely to be finer than the bound simply given by the degree of the L -function, and hence by Tate’s work (one inequality in the rank part of B–SD, cf. [U1] Proposition 6.2.4 (1)) it also gives upper bounds on the Mordell–Weil rank. In [U1] and earlier papers, Ulmer gives *lower* bounds on the analytic rank of J_E in certain towers. His methods also use Galois theory, with a distinct slant towards representation theory. It would be interesting to explore the relations between these approaches.

1. Zeta functions and L -functions

1.1. Zeta functions of varieties

For a general variety X over \mathbb{F}_q , let $x \in X$ always denote a *closed* point, and $d(x)$ the degree of its residue field over \mathbb{F}_q . The zeta function $Z(T, X)$ is defined as $\prod_{x \in X} (1 - T^{d(x)})^{-1}$. For X an \mathbb{F}_q -rational point, the affine line, or the projective line over \mathbb{F}_q , the zeta function is $1/(1 - T)$, $1/(1 - qT)$, and $1/((1 - T)(1 - qT))$ respectively. There is a well-known alternative definition using the number of \mathbb{F}_{q^n} -rational points of X for all n . For an elliptic curve E_0/\mathbb{F}_q , we have

$$Z(T, E_0) = \frac{(1 - \alpha T)(1 - \bar{\alpha} T)}{(1 - T)(1 - qT)},$$

with α an algebraic integer such that $|E_0(\mathbb{F}_q)| = 1 - \alpha - \bar{\alpha} + q$. The polynomial in the numerator is called $L(T, E_0)$; it is the L -function of the elliptic curve. Note that the denominator agrees with the denominator of $Z(T, \mathbb{P}^1)$, so in this sense the L -function of \mathbb{P}^1 is simply 1.

We will be concerned with relative curves, that is, normal varieties \mathcal{E} with a surjection to a base curve C such that all fibres are again curves. The generic fibre of \mathcal{E} is then a regular curve E/K . In fact the curve E/K will even be smooth in all our examples. The case where this family of curves is constant, i.e. $\mathcal{E} = C \times E_0$ for some curve E_0/\mathbb{F}_q , will not play a role in the sequel, but let us point out that one can get the zeta and L -function easily in that case. In particular, there are no “bad” fibres. The following result is an exercise, and certainly well known.

Proposition 1.1. *Assume $Z(T, X) = \prod_{i \in I} (1 - \alpha_i T)^{-e_i}$ and $Z(T, Y) = \prod_{j \in J} (1 - \beta_j T)^{-f_j}$, where the α_i, β_j are algebraic integers and the e_i, f_j are integers. (The minus sign in the exponents is intentional.) Then*

$$Z(T, X \times Y) = \prod_{i \in I, j \in J} (1 - \alpha_i \beta_j T)^{-e_i f_j}.$$

We point out two important examples:

- (1) As $Z(T, \mathbb{P}^1) = (1 - T)^{-1}(1 - qT)^{-1}$, we get

$$Z(T, \mathbb{P}^1 \times \mathbb{P}^1) = \frac{1}{(1 - T)(1 - qT)^2(1 - q^2T)}.$$

- (2) If E_0 is an elliptic curve with L -function as above, then

$$Z(T, \mathbb{P}^1 \times E_0) = \frac{(1 - \alpha T)(1 - \bar{\alpha} T)(1 - q\alpha T)(1 - q\bar{\alpha} T)}{(1 - T)(1 - qT)^2(1 - q^2T)}.$$

Note that again this function shares the denominator with $Z(T, \mathbb{P}^1 \times \mathbb{P}^1)$, whose numerator is 1. So the zeta function of $\mathbb{P}^1 \times E_0$ has an obvious part, the denominator, which it shares with $Z(T, \mathbb{P}^1 \times \mathbb{P}^1)$, and an interesting part, the numerator. For nonconstant families arising from curves X over the function field of \mathbb{P}^1 , we will again describe $L(T, E/K)$ as the “nonobvious” factor in the zeta function $Z(T, \mathcal{E})$ of a suitable model $\mathcal{E} \rightarrow \mathbb{P}^1$.

To aid the reader, we will recall what happens in a simple situation discussed in [Ha]; we will call it the Minimal Example. Recall that the base curve is written C , and that it will be $\mathbb{P}_{\mathbb{F}_q}^1$ without indication to the contrary. Write $K = \mathbb{F}_q(C) = \mathbb{F}_q(t)$ and consider the elliptic curve

$$E/K : y^2 = x(x - 1)(x - t).$$

At all finite values of t this same equation defines a minimal model, let us call it $\mathcal{E} \rightarrow \mathbb{P}^1$. For $t \neq 0, 1, \infty$ the fibre in t is an elliptic curve in Legendre form. At 0 and 1 one has multiplicative reduction. At $t = \infty$ the minimal equation is $y_1^2 = x_1(x_1 - s)(x_1 - s^2)$ where $s = 1/t$, $x_1 = s^2x$ and $y_1 = s^3y$, so we have additive reduction. This defines \mathcal{E} near $t = \infty$.

Hall established congruences for the L -function of E/K , using the presence of 2-torsion points. These points arise as follows. Let $X = \mathbb{P}_K^1$ (with coordinate x) and $\mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1 = \mathbb{P}_C^1$, with coordinates t (base) and x (fibre). Then $E \rightarrow X$ is a ramified Galois 2-cover, ramified in $0, 1, t, \infty$. The four points of E lying above these four ramification points are 2-torsion points. Similarly, $\mathcal{E} \rightarrow \mathcal{X}$ is a ramified 2-cover: a finite flat morphism of degree 2, and the ramification locus is a ramified cover of C , consisting of four sections $x = 0$, $x = 1$, $x = t$, $x = \infty$. Recall from the introduction: The first (second) of these sections meets the third in $t = 0$ ($t = 1$ resp.); the first three meet in $t = \infty$. (Note that the last fact is due to the variable change required at $t = \infty$.) At the singular fibres, where t has the values $0, 1, \infty$, we get two nodal curves $y^2 = x^2(x - 1)$, $y^2 = x(x - 1)^2$ and a cuspidal cubic $y^2 = x^3$ respectively. All these singular curves are degree 2 covers of $\mathbb{P}_{\mathbb{F}_q}^1$.

For each closed point $w \in \mathbb{P}^1$, the fibre \mathcal{E}_w is a curve over the field $\mathbb{F}_q(w)$ with $q^{d(w)}$ elements, and just by counting points we get that

$$Z(T, \mathcal{E}) = \prod_{w \in \mathbb{P}^1} Z(T^{d(w)}, \mathcal{E}_w).$$

Let $L(T, E/K)$ be the Hasse–Weil L -function which is defined and discussed in [Ha]. We will come back to its definition in the next subsection; in particular we will say how the L -function splits as a product of factors, one for each point of C . Recall that the L -function of a curve E_0 over the finite base field \mathbb{F}_q is given as the characteristic polynomial of Frobenius acting on $H^1(\bar{\mathbb{F}}_q \otimes E_0, \mathbb{Q}_\ell)$. A similar, somewhat more elaborate interpretation will hold for the Hasse–Weil L -function.

In order to give some background, we mention here how it connects it to the zeta function in the general sense of varieties; but we will not give the proof since the result is not used in the sequel. In slightly different form, the statement is contained in Eq. (3.2.2) in [U12].

Lemma 1.2.

$$Z(T, \mathcal{E}) = L(T, E/K)^{-1} \cdot \frac{1}{(1-T)(1-qT)^2(1-q^2T)}.$$

One nice result of Hall says that in the Minimal Case, the polynomial $L(T, E/K)$ is simply the constant 1. We mention in passing that in this case there is also a proof by point counting (using the previous lemma), but since this argument has no potential of being generalised, we do not give it.

It is important to have two handles on the Hasse–Weil L -function: one via the definition, which involves the Galois action of inertia groups at the “bad” fibres, and a more down-to-earth approach, using the geometry of the fibres directly.

1.2. L -functions of relative curves

For this subsection, let C be any smooth projective curve over \mathbb{F}_q with function field K . (In most of the rest of this paper we take $C = \mathbb{P}^1$.) We recall that we assume q to be odd. Let E/K be a smooth projective curve. We also make the assumption that the K/\mathbb{F}_q -trace of the Jacobian $J_{E/K}$ is trivial. For elliptic curves this is equivalent to X having nonconstant j -invariant.

The L -function of E/K is constructed as follows. Fix a prime ℓ different from the characteristic. Let $U \subset C$ be open and dense such that E has good reduction over U , that is, there is a smooth morphism $\pi : \mathcal{E}_U \rightarrow U$ with generic fibre E . We also need these data base-changed from \mathbb{F}_q to its algebraic closure $\bar{\mathbb{F}}_q$; this will simply be indicated by an overbar. One then has a lisse sheaf \mathcal{G} on \bar{U} defined by $\mathcal{G} = R^1\pi_*\mathbb{Z}_\ell$, a relative version of $H^1(-, \mathbb{Z}_\ell)$. In particular, the stalk at any $w \in \bar{U}$ is $H^1(\bar{\mathcal{E}}_w, \mathbb{Z}_\ell)$. This sheaf, like

all the sheaves to follow, carries an action of Frobenius, the distinguished generator of $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. The sheaf \mathcal{G} is equivalently described as $V = \mathbb{Z}_\ell^{2g_E}$ (the generic fibre) with a continuous action of the absolute Galois group $\Omega = \text{Gal}(K^{sep}/\bar{\mathbb{F}}_q K)$.

Next, one extends \mathcal{G} to a sheaf \mathcal{F} on the whole of \bar{C} as follows: $\mathcal{F} = j_*\mathcal{G}$, with $j : \bar{U} \rightarrow \bar{C}$ the inclusion. The stalk \mathcal{F}_w at any $w \in \bar{C}$ is V^{I_w} , the fixed module under inertia.

Now the L -function $L(T, E/K)$ is defined as the characteristic polynomial of Frobenius on $\mathbb{Q}_\ell \otimes H^1(\bar{C}, \mathcal{F})$. It is very important that this can also be written as a product over all closed points $v \in C$; let us formulate this as a lemma.

Lemma 1.3. *For every closed point $v \in C$, pick a point $w(v) \in \bar{C}$ above it. Then, with notations and assumptions as just explained, we have*

$$L(T, E/K) = \prod_{v \in C} \det(1 - T^{d(v)} F : \mathbb{Q}_\ell \otimes \mathcal{F}_{w(v)})^{-1}.$$

Proof. Since the zeroth and second cohomologies of \mathcal{F} over C vanish according to our assumption on the trace of the Jacobian (cf. [U] Lemma 6.2.2), $L(T, E/K)$ is the inverse of the Frobenius–Euler characteristic $\chi(\mathcal{F})$ of \mathcal{F} , that is, of the alternating product

$$\prod_{i=0}^2 \det(1 - TF : \mathbb{Q}_\ell \otimes H^i(\bar{C}, \mathcal{F}))^{(-1)^i}.$$

An old result of Grothendieck now tells us that this globally defined Frobenius–Euler characteristic has an expression by local factors, one for each $v \in C$, and this exactly gives the formula of the lemma. \square

The inverse of the local factor at $v \in U$ in the preceding lemma is just the numerator of the zeta function of the fibre \mathcal{E}_v . We now want a tangible and geometric interpretation also for $v \in C \setminus U$ (that is, v has bad reduction). For this it is convenient to rewrite \mathcal{G} and \mathcal{F} slightly. There is a canonical isomorphism (cf. [U] p. 39) $\mathcal{G}(-1) \cong T_\ell(\text{Pic}^0(\mathcal{E}_U/U))$. The Tate twist $\dots(-1)$ can be neglected because it will be irrelevant later on. Let us write \mathcal{G} again for this new sheaf, the Tate module of the Jacobian, so \mathcal{G} is the projective limit over ν of the torsion sheaves $\text{Pic}^0(\mathcal{E}_{\bar{U}/\bar{U}})[\ell^\nu]$. Thus, the “bad” stalks of \mathcal{F} (we again write \mathcal{F} for $j_*\mathcal{G}$) are now obtained by taking I_w -invariants of the $G(\bar{K}/\bar{\mathbb{F}}_q K)$ -module afforded by the generic fibre of this sheaf. As is well known from work of Serre and Tate [ST], the fibre \mathcal{F}_w is then the Tate module of the fibre at w of the Néron model of $J_{X/K}$.

Even this is not yet sufficiently explicit, at least for us; we would like to avoid referring to Néron models. For this we need the concept of rational singularities. For the definition (in the case of surfaces) we refer to §1.1 in [Li]. The following criterion of Lipman [Li] is perhaps a little more intuitive: A surface singularity is rational if there is a chain of blow-ups terminating in a regular surface. (In general, when resolving a surface singularity, one has to alternate between blowing up and normalising.)

We assume that the model $\mathcal{E}_U \rightarrow U$, which is a smooth morphism, extends to a proper flat morphism $\mathcal{E} \rightarrow C$, with \mathcal{E} normal. For certain types of curves we will just write down such an \mathcal{E} explicitly. This model \mathcal{E} looks like a minimal Weierstraß model; but we did not check whether it really is a minimal Weierstraß model in case E is an elliptic curve, since we do not need it. For the following theorem, note that \mathcal{E} is 2-dimensional and excellent (locally the coordinate rings are of finite type over a (finite) field), and hence we are assured that it admits a resolution of singularities (this was proved by Lipman in 1978; see e.g. the recent paper [CJS]).

Theorem 1.4. *Assume that $\bar{\mathcal{E}}$ has only rational singularities, and that all fibres are reduced. Let \mathcal{N}/\bar{C} be the Néron model of the Jacobian of $\bar{E}/\bar{\mathbb{F}}_q K$ (recall E is the generic fibre of \mathcal{E}). Then:*

- (a) *The connected component of 0 in \mathcal{N} identifies with the relative Picard variety $\mathrm{Pic}^0(\bar{\mathcal{E}}/C)$.*
- (b) *For every $w \in \bar{C}$, we have $T_\ell(\mathcal{N}_w) \cong T_\ell(\mathrm{Pic}^0(\bar{\mathcal{E}}_w))$.*
- (c) *The local factor of $L(T, E/K)$ at v is the inverse of $\det(1 - TF : T_\ell(\mathrm{Pic}^0(\bar{\mathcal{E}}_w)))$.*

Proof. (a) This is Theorem 9.7.1 in [BLR]. Comments: (1) The theorem in [BLR] is stated with the spectrum of a DVR instead of a curve as a basis, but this is no problem, the question being local on the basis. (2) Condition (ii) in [BLR] is fulfilled: the residue class fields of the closed points of the base \bar{C} are all $\bar{\mathbb{F}}_q$, hence perfect. (3) Condition (iii) in [BLR] is fulfilled, since we assume the closed fibres to be actually reduced, so all multiplicities are 1.

(b) This follows from (a) since the fibre of $\mathrm{Pic}^0(\mathcal{E}/C)$ in w is $\mathrm{Pic}^0(\bar{\mathcal{E}}_w)$.

(c) The inverse of the local factor is by definition the characteristic polynomial of Frobenius on \mathcal{F}_w ; by the above discussion (Serre–Tate), this sheaf is $T_\ell(\mathcal{N}_w)$. By (b), the latter identifies with $T_\ell(\mathrm{Pic}^0(\bar{\mathcal{E}}_w))$, so we are done. \square

The conditions of the preceding theorem look complicated. But in practice we will use the criterion of Lipman [Li] mentioned above. We will impose suitable conditions on our curve E and then ensure the rationality of the singularities, plus existence of a resolution of singularities, by producing a series of blow-ups of \mathcal{E} terminating in a smooth surface. It should be said that the singularities in \mathcal{E} cannot be expected to be rational in general.

2. Models of relative curves, and rational singularities

For the rest of the paper we assume $C = \mathbb{P}^1$. Recall that $K = \mathbb{F}_q(t)$ is the function field of C . Fix an integer $r \geq 2$, and assume $q \equiv 1$ modulo r . We consider curves E/K given by equations of the form

$$y^r = \prod_{i=1}^d (x - f_i(t)),$$

where the f_i are pairwise distinct polynomials in t . These curves are called *superelliptic* (hyperelliptic for $r = 2$). They are degree r covers of $X = \mathbb{P}_K^1$, the projective line over K with coordinate x . We will always assume that r is coprime to d . To avoid trivial cases we assume $d > 1$. Often we will assume $f_1 = 0$; this can always be achieved by a change of variables $x \mapsto x - f_1$. This only gives the affine part of E ; to get the point(s) over $x = \infty$, one has to pass to projective coordinates (introducing z), then put $x = 1$ and normalise. (For $r = 2$ and $d = 3$ the equation will already be normal.) Then E will have exactly one point at $x = \infty$.

The obvious morphism $E \rightarrow X$ (given by forgetting y) turns E into a G -covering of X , with cyclic Galois group G of order r . If we fix a primitive r -th root ζ of unity in \mathbb{F}_q , we get a generator σ of G , with $\sigma(y) = \zeta y$. This covering is ramified in the K -points $x = f_1, \dots, x = f_d$ and $x = \infty$ of the K -curve X .

We now discuss models $\mathcal{E} \rightarrow C$ of E . Recall that X was defined as \mathbb{P}_K^1 (with coordinate x). Then X/K has an obvious model \mathcal{X} , the relative \mathbb{P}_C^1 over C . This is simply the direct product $\mathbb{P}^1 \times \mathbb{P}^1$, with coordinates x and t respectively. All models \mathcal{E} considered will be ramified G -covers of $\mathcal{X} = \mathbb{P}_C^1$.

For $x \neq \infty$, $t \neq \infty$, \mathcal{E} will be given by exactly the same equation as above. It remains to discuss the model near $x = \infty$ and then near $t = \infty$. The discussion “near $x = \infty$ ” will be brief. Let us first treat $r < d$. Passing to homogeneous coordinates (everything over $\mathbb{F}_q[t]$) one gets $y^r z^{d-r} = (x - f_1 z) \cdots (x - f_d z)$. We set $y = 1$, and we are interested in points having $z = 0$. Replacing z by z/x (this is a step towards the normalisation!) we get $z^{d-r} = x^r \prod (1 - f_i z)$. We rename $d - r$ to k , and replace $f_i z$ by the more generic term $O(z)$, meaning any polynomial in x and z divisible by z . Hence k and r are coprime; we show by induction over $\max(r, k)$ that the normalisation of this curve over $\mathbb{F}_q[t]$ has only one point above $(0, 0)$ and is smooth there. As soon as one of r and k is 1, we are done. If $r > k$: replacing z by z/x produces $z^k = x^{r-k} \prod (1 + O(xz))$, done by inductive hypothesis. If $r < k$: replacing x by x/z produces $z^{k-r} = x^r \prod (1 + O(xz))$, done again by inductive hypothesis. – It remains to treat $r > d$; this is rather similar and left to the reader.

Our next task is to extend \mathcal{E} to a neighbourhood of $t = \infty$. Let $\delta_i = \deg(f_i)$ and let e be the smallest multiple of r that is not smaller than any of the δ_i . (If one f_i is zero, which is permitted, we take its degree to be $-\infty$.) Putting m to be the number of i such that $e > \delta_i$ and changing variables $y_1 = y/t^d$ and $x_1 = x/t^{e/r}$ we get an equation of the above curve near $t = \infty$, writing $s = 1/t$:

$$y_1^r = (x_1 - s^{e-\delta_1} g_1(s)) \cdots (x_1 - s^{e-\delta_d} g_d(s)),$$

with g_i the reciprocal polynomial of f_i . Without loss of generality we assume that $e > \delta_i$ iff $i \leq m$, for some well-determined $0 \leq m < d$. Then at $s = 0$ the equation reduces to

$y_1^r = x_1^m \prod_{j=1}^{d-m} (x_1 - a_j)$, where a_j is the leading coefficient of f_j ($m < j \leq d$). In Hall's setup with elliptic curves we recover that the fibre over $t = \infty$ has a node for $m = 2$ and a cusp for $m = 3$; $m = 0$ or 1 does not arise among his Legendre curves. We note here for later use: If $m = 0$ (this forces all δ_i to be multiples of r) and the a_j are all distinct, then the fibre at $t = \infty$ is nonsingular.

Let $\mathcal{E} \rightarrow C$ be the projective variety over C defined by the equation $y^r = \prod_{i=1}^d (x - f_i)$ for the part with $t \neq \infty$, $x \neq \infty$, by the above equation for a neighbourhood of $t = \infty$, $x \neq \infty$, and described by the preceding discussion near $x = \infty$; we will never need explicit equations there. This is our analog of a minimal Weierstraß model. The ramification locus (at $t \neq \infty$) is the union of the sections $x = \infty$ and $x = f_i(t)$, $1 \leq i \leq d$. A similar description holds near $(1/t =)s = 0$. In another section we will discuss the singular fibres of \mathcal{E} in detail.

For now, the task at hand is to give sufficient criteria for \mathcal{E} to have only rational singularities. The relevance of this was discussed in Subsection 1.2. It is clear that all points of \mathcal{E} which are not above points where two or more sections of the ramification locus intersect will be nonsingular. So the potential singularities of \mathcal{E} all occur above points of $\mathcal{X} = \mathbb{P}_C^1$ where sections meet, and they are all isolated.

A little terminology before we look at details: Consider the fibre \mathcal{X}_τ at $t = \tau \in \bar{\mathbb{F}}_q$, and assume that exactly $m \geq 2$ of the $f_i(\tau)$ share the same value ξ (so the other $f_j(\tau)$ are different from ξ). Then we write $m = n(\tau, \xi)$ and say that m sections (of the ramification locus) meet at $(t, x) = (\tau, \xi)$. There is then a unique point $(\tau, \xi, \eta) \in \mathcal{E}$ above (τ, ξ) . All singular points of \mathcal{E} arise this way. If $\tau = \xi = 0$ (which is no real loss of generality), and (say) the sections $x = f_1, \dots, x = f_m$ meet there, then we say that they *meet with different tangents* if $f_i = a_i t + O(t^2)$ ($t = 1, \dots, b$) with distinct $a_i \in \mathbb{F}_q$. For $m = 2$, we say that the sections *touch with order 2* if they do meet in $(0, 0)$ (so f_1 and f_2 are multiples of t), and $f_1 - f_2$ is divisible by t^2 but not by t^3 .

Proposition 2.1. *Let $\tau, \xi \in \bar{\mathbb{F}}_q$ and assume $m := n(\tau, \xi) \geq 2$ (otherwise there is no singularity). Let $P = (\tau, \xi, \eta)$ be the unique point in $\bar{\mathcal{E}}$ over (τ, ξ) . Then P is a rational singularity if one of the following conditions is met:*

- (1) $m \leq r + 1$; r is congruent to 0 or ± 1 modulo m , and the sections meet with different tangents.
- (2) $m = 2$ (any kind of meeting or touching) and $r = 2$.
- (3) $m \leq 3$ with two or three different tangents, and $r = 2$.
- (4) $m = 2$, the two sections touch with order 2, and $r = 3$.

Remark 2.2. Part (3) of this proposition covers Hall's Minimal Example.

Proof of Proposition 2.1. In all cases we can assume that it is exactly the first m sections that meet, that $(\tau, \xi) = (0, 0)$ and (by change of variables) that $f_1 = 0$. The strategy will always be the same: we perform a series of blowups in the singular point at hand

(which is simply $(0, 0, 0)$), never taking normalisations in between, until we arrive at a smooth surface, or more precisely a surface that is smooth at all points Q over $(0, 0, 0)$. Such points Q are called “relevant”.

We need a little shorthand for the blowing-up steps. Everything will happen in 3-space with coordinates t, x, y . One step consists, in principle, of three substeps: in the first, t and y are replaced by xt' and xy' respectively, and all possible powers of x are removed from the equation (this amounts in geometric language to taking the “strict transform” of our surface in one affine piece of the blow-up of the ambient space). We will indicate this procedure by a label (x) , which precedes the transformed equation. The second and third substeps are entirely similar, with t (y respectively) taking the role of t . (The slightly odd ordering, (x) coming before (t) , has entirely technical reasons.) It is well known that the three affine pieces of the blow-up corresponding to the labels (x) , (t) , (y) are far from disjoint. In fact, if we are in the (t) -piece (say) with coordinates t, x', y' , then every point where x' does not vanish is also in the (x) -piece, and so on. So in discussing one substep one is often able to eliminate points, because they were already done in a previous substep.

There will be some more minor offences concerning notation. First, the primes at the new variables (t', y' for example) will be omitted instantly. Second, the generic letter u will always denote a function that is nonzero at all relevant points. (For instance if only $x = t = y = 0$ is relevant, then $u = 1 + x$ or $u = 1 - x^2t$ are such.) Third, when blowups are iterated, we just concatenate labels: (xt) means “first perform (x) , and then perform (t) ”.

Before we treat our cases (1)–(4), we discuss a class of singularities known as “ordinary double points” as a subsidiary lemma. (The lemma seems to be known, but the author did not find a good reference, so the short proof is given for the reader’s convenience. For $P = (0, 0, 0)$, the singularity in the lemma is $y^2 = xt$; there the rationality is a special case of Proposition 3.1 in Singh and Spiroff [SS].)

Lemma 2.3. *Every singularity of type $y^2 = xt + P(x, t)$ with $P(x, t) \in (x, t)^3$ is rational at $x = y = t$ in characteristic different from 2.*

Proof. We blow up once and consider the equations obtained by the substeps (x) and (t) . By symmetry, the former suffices. We get $(x) : y^2 = t + xQ(x, t)$, at $x = 0$. (For the last time we remind the reader that the letters y, t have changed their meaning!) Now every point with $t \neq 0$ is smooth: we are extracting the square root of a unit in the local ring of the point. At $t = 0$ one sees easily that the RHS of the equation is not in $(x, t)^2$, whatever the value $Q(0, 0)$, so the equation is again smooth. Likewise, the substep (y) only leads to smooth points: one gets $y^2 = 1 + y^{-2}P(yx, ty)$. The right hand side is a unit in the local ring of every point with $y = 0$. \square

We now come back to the proof of the proposition.

(1) We blow up systematically, treating the substeps (x) , (t) , (y) in turn. Sometimes we get a smooth surface directly, in other cases we find a surface with only ordinary double points. In these cases we will be done after the first blow-up. But sometimes we only obtain a surface with an equation of the same type, with r replaced by $r - m$. So the whole proof of (1) is an induction over r , with m being fixed.

Our hypothesis means that we have an equation

$$y^r = x(x - a_2t + O(t^2)) \cdots (x - a_mt + O(t^2))u,$$

where $a_2, \dots, a_m \in \mathbb{F}_q$ are nonzero and distinct, and $u = u(x, t)$ does not vanish at $t = x = y = 0$.

First substep: Let us first assume $m \leq r$. We get

$$(x) : y^r x^{r-m} = (1 - a_2t + O(t^2x)) \cdots (1 - a_mt + O(t^2x))u,$$

only points with $x = 0$ being relevant. If $r > m$, this means $t = 1/a_i$ for some $i \in \{2, \dots, m\}$, and it is easy to check that all such points are smooth, as follows. Let \mathfrak{m} be the maximal ideal attached to such a point. Then modulo \mathfrak{m}^2 , the RHS is a nonzero scalar times $(1 - t/a_i + \alpha x)$, where $1 - t/a_i$ and x are linearly independent in $\mathfrak{m}/\mathfrak{m}^2$, and the LHS is a scalar multiple of x , so the equation as a whole is in $\mathfrak{m} \setminus \mathfrak{m}^2$. For $r = m$ one has to distinguish: there are points with y and the RHS both zero, and these are dealt with as before (with small changes); at every point (t, x, y) where the RHS is not zero, we are extracting the r -th root of a unit in the local ring at this point, which is smooth again.

Now (still in the first substep) we assume $m = r + 1$. Then we obtain

$$(x) : y^r = x(1 - a_2t + O(t^2x)) \cdots (1 - a_mt + O(t^2x))u,$$

where again only points with $x = 0$ are relevant. Hence also $y = 0$ for these points. At points with $t = 1/a_i$ for some $i \in \{2, \dots, m\}$, we claim that we have an ordinary double point. Indeed: say $t = 1/a_2$ and let \mathfrak{m} be the maximal ideal at this point. Then one finds that the factors x and $1 - a_2t + O(t^2x)$ are in \mathfrak{m} and linearly independent modulo \mathfrak{m}^2 , and all other factors $1 - a_mt + O(t^2x)$ for $i = 3, \dots, m$ are outside \mathfrak{m} , as well as u . This suffices to show that the point is an ordinary double point.

It is easy to show that for t not equal to any $1/a_i$ we even get smooth points. This completes the substep (x) . (Remark which can be ignored but which may help to understand our hypotheses on r and m : If we had taken $m = r + 2$, we would have gotten a factor x^2 instead of the factor x right next to the $=$ sign, leading to a non-normal equation; so we would be stuck!)

The second substep, with (t) in the place of (x) , is so similar, including the case distinction $m \leq r$ versus $m = r + 1$, that we feel safe omitting the details.

Now for the third substep. This time we begin with the case $m = r + 1$. We obtain

$$(y) : 1 = y \cdot x \cdot (x - a_2 t + O(t^2)) \cdots (x - a_m t + O(t^2)) u,$$

and only points with $y = 0$ matter. But obviously there are no such points. So we turn to the case $m \leq r$. This gives, on putting $r' = r - m$:

$$(y) : y^{r'} = x \cdot (x - a_2 t + O(t^2)) \cdots (x - a_m t + O(t^2)) u.$$

If we still have $m \leq r' + 1$ and $r' \geq 2$, we can invoke our inductive hypothesis; note that the congruence $r' \equiv 0, \pm 1 \pmod m$ holds again. If $r' = 1$, it is easy to see that the equation is smooth at all points with $y = 0$. So we are left with the cases $2 \leq r' < m - 1$. But by our congruence hypothesis, this cannot happen. So we are done.

We now turn to part (2) of the proposition. Here we are facing an equation

$$y^2 = x(x - g)u(x, t),$$

where g is a polynomial in t vanishing at 0, and $u(0, 0) \neq 0$. We get in the first substep

$$(x) : y^2 = (1 - \tilde{g})u$$

with $\tilde{g} = g(xt)/x$; this is already a smooth equation at all points with $x = 0$. (Distinguish cases: if $g(t)$ has no linear term, then $1 - \tilde{g}$ is a unit at all relevant points, and the equation is smooth. If the linear term of $g(t)$ is ct , we get an equation $y^2 = (1 - ct - xh(x, t))u$. At every point with $t \neq 1/c$ we again extract the square root of a unit in the local ring of the point, a smooth equation. At the point $(t, x) = (1/c, 0)$, one easily checks that $1 - ct - xh(x, t)$ and hence the whole right hand side $(1 - ct - xh(x, t))u$ is in $\mathfrak{m} \setminus \mathfrak{m}^2$.)

Now let's do the second substep:

$$(t) : y^2 = x(x - g/t)u.$$

Only points with $t = 0$ are relevant. We either have a smooth equation (if g/t does not vanish at $t = 0$), or a similar equation with decreased degree (if g/t still vanishes at $t = 0$), so we are done by induction.

The third substep (y) leads to $1 = x(x - \tilde{g})u$. Hence $x \neq 0$, and all relevant points are already caught by the (x) -piece of the blow-up.

Remark: In this case there is an alternative argument, appealing to the theory of semistable curves.

(3) Here we are looking at an equation

$$y^2 = (x - f_1)(x - f_2)(x - f_3)u$$

where the f_i vanish at $t = 0$, but they are not all three congruent modulo t^2 . The case where they are mutually incongruent modulo t^2 is contained in case (1) above. So let us assume $f_1 \equiv f_3$ modulo t^2 and $f_1 \not\equiv f_2$ modulo t^2 . By a change of variables one can transform the equation to

$$y^2 = x(x - t + O(t^2))(x - t^2h)u$$

for some $h = h(t) \in \mathbb{F}_q[t]$. Exactly as in step (2) it turns out: As soon as the pieces (x) and (t) are done (actually (x) is enough), all relevant points of the piece (y) are already covered – we skip the details this time. So we only have to do two pieces.

First piece:

$$(x) : y^2 = x(1 - t + O(t^2x))(1 - t^2xh(xt))u,$$

at $x = y = 0$, t a priori undetermined. But this is an easy case. The factor $(1 - t^2xh(xt))$ is also a unit at all points with $x = y = 0$; the only singular point arises by setting $t = 1$, and this gives an ordinary double point (see [Lemma 2.3](#)). Second piece:

$$(t) : y^2 = xt(x - 1 + O(t))(x - th)u = xt(x - th)u'$$

at $t = y = 0$. The only singular points arise at $x = 0$ or $x = 1$. In the latter case the singularity is an ordinary double point. (Note that x and $x - th$ are units at points with $x = 1$ and $t = 0$.) In the former case we can put the factor $x - 1 + O(t)$ into the unit factor and get $y^2 = xt(x - th)u$. (We remind the reader that by abuse of notation u stands for a unit, which may well change from one step to another.) We now prove by induction over the order e of vanishing of the polynomial $g = g(t)$ at $t = 0$ that the singularity $y^2 = xt(x - g)u$ at $x = y = t = 0$ is rational; this will finish the argument.

If $g(0) \neq 0$, i.e. $e = 0$, then the singularity is an ordinary double point. So assume $e > 1$.

We have to blow up again. By exactly the same argument as before, it suffices to do the (x) - and the (t) -piece. Performing (x) gives $y^2 = t(x - g(xt)) = tx(1 - t\tilde{g}(tx))$, with $\tilde{g}(t) = g(t)/t$. At $t = 0$ this is an ordinary double point. If $\tilde{g}(0) = 0$, this is the only t -value that gives a singularity (recall $x = y = 0$). If $\tilde{g}(0) = a \neq 0$, then the only other singular t -value is $1/a$, and this is again an ordinary double point. So the essential part of the blow-ups where induction is needed is the substep (t) . This gives the equation $y^2 = xt(x - g/t)u$, to be considered at $t = y = 0$. For $x \neq 0$ we again only get ordinary double points. At $x = 0$, the singularity is rational by induction hypothesis.

(4) Here we are looking at

$$y^3 = x(x - g)u,$$

with g divisible by t but not by t^3 . If g is not divisible by t^2 , then we have two sections meeting with different tangents, so this is already covered by (1). So we assume $t^2|g$.

First blowup.

$$(x) : y^3x = (1 - \tilde{g})u$$

with $\tilde{g} = g(xt)/x$, relevant only at $x = 0$. But since \tilde{g} vanishes at $x = 0$, there are no relevant points here.

$$(t) : y^3t = x(x - g/t)u.$$

Relevant only at $t = 0$. Since $g'(0) = 0$, we may replace g by g/t in our notation and we have an equation $y^3t = x(x - g)u$ similar to the initial one, but there is an extra t on the left. We continue from here. Note that now $g(t)$ is divisible by t but not by t^2 .

$$(y) : y = x(x - \tilde{g})u$$

with $\tilde{g} = g(yt)/y$ divisible by t^2y . Only $y = 0$ is relevant, hence also $x = 0$. Thus the RHS is in \mathfrak{m}^2 and the LHS is in $\mathfrak{m} \setminus \mathfrak{m}^2$, hence the equation is smooth in all points having $y = 0$, and need not be pursued further.

Second blow-up.

$(tx) : y^3tx^2 = (1 - g(xt)/x)u$, relevant only at $x = 0$. Put $\alpha = g'(0) \neq 0$. The relevant points then have $x = 0$, $t = 1/\alpha$, and at these points (whatever y) the RHS is not in the square of the maximal ideal and the LHS is, so we have smoothness.

$(tt) : y^3t^2 = x(x - g/t)u$, with points having $t = 0$. Again, $\alpha = g'(0) \neq 0$. So we must have $x = 0$ or $x = \alpha$, and both of these are smooth points.

$(ty) : y^2t = x(x - \tilde{g})u$ with $\tilde{g} = g(ty)/y$, points having $y = 0$ only. Let $c = g'(0)$ be the linear coefficient of g , so $\tilde{g} = ct + O(t^2y)$. Then all relevant points have $x = 0$ or $x = tc$. Since $c \neq 0$, one can check that only $y = x = t = 0$ is singular. We continue from here.

$(tyx) : y^2tx = (1 - ct + O(t^2yx^2))u$, only points with $x = 0$ are relevant. So t must have value $1/c$. Whatever the value of y , this is smooth.

$(tyt) : y^2t = x(x - c - O(t^2y))u$, only points with $t = 0$ are relevant. Here x must be 0 or 1, and whatever the value of y , this is smooth.

$(tyy) : yt = x(x - ct + O(t^2y))u$, only points with $y = 0$ are relevant. Points with $x \neq 0$, $x - t = 0$, are smooth. Among the points with $x = 0$, only $y = t = x = 0$ is singular. So we have a similar equation as at the end of stage (ty) , with y^2 replaced by y . We continue from here.

$(tyyx) : yt = (1 - ct + O(t^2yx^2))u$, only points with $x = 0$ to be considered. This can be rewritten as $(y + c)t = \text{unit}$, and is smooth.

$(tyyt) : y = x(x - c + O(t^2y))u$, only points with $t = 0$ are relevant. So the $O(t^2y)$ -term is always in the square of the maximal ideal, and we can ignore it when checking smoothness. Without it, smoothness of the equation is obvious.

$(tyyy) : t = x(x - ct + O(t^2y^2))u$, only points with $y = 0$ to be considered. The reasoning is exactly the same as in the preceding case. So finally after four blow-ups, we

have smoothness, and the rationality of the original singularity, and we are done with part (4) of [Proposition 2.1](#) as well. \square

Our final job in this section is to discuss these criteria in the light of the explicit formulas at $t = \infty$, since we of course want *all* singularities of \mathcal{E} to be rational. As mentioned before, we don't have to worry any more about $x = \infty$. Recall $\delta_i = \deg(f_i)$ and e is the smallest multiple of ℓ majorising all δ_i . We assume $f_1 = 0$ (letting its degree be $-\infty$) and we denote the leading coefficient of f_i by a_i . (So a_1 is undefined.) Recall $s = t^{-1}$ and the equation for \mathcal{E} near $s = 0$:

$$y_1^r = (x_1 - s^{e-\delta_1}g_1(s)) \cdots (x_1 - s^{e-\delta_d}g_d(s)),$$

with g_i the reciprocal polynomial of f_i . The following result speaks about singularities of \mathcal{E} which lie in the fibre at $t = \infty$. These should not be confused with the singularities of that fibre, which play no role at this moment.

Proposition 2.4. *Any of the following conditions insures that all singularities of \mathcal{E} over $t = \infty$ are rational.*

- (1) $r|\delta$, and there exists $1 \leq b \leq \min(d-1, m+1)$ satisfying $r \equiv 0, \pm 1 \pmod{b}$ and such that f_2, \dots, f_b have degree $\delta-1$, f_{b+1}, \dots, f_d have degree δ ; moreover a_2, \dots, a_b are pairwise distinct and a_{b+1}, \dots, a_d are pairwise distinct.
- (2) $r = 2$: f_3, \dots, f_d have even degree δ , $\deg(f_2) < \delta$, and a_3, \dots, a_d are pairwise distinct.
- (3a) $r = 2$: f_4, \dots, f_d have even degree δ , $\deg(f_3) = \delta-1$, $\deg(f_2) \leq \delta-1$ and a_4, \dots, a_d are pairwise distinct.
- (3b) $r = 2$, $d = 3$, f_3 has odd degree δ , $\deg(f_2) < \delta$. (This captures Hall's Legendre curves.)
- (4) $r = 3$, f_3, \dots, f_d have degree δ which is divisible by 3, and $\deg(f_2)$ is $\delta-1$ or $\delta-2$.

In all these cases, sections intersect only at $x = 0$.

Remark 2.5. The condition that sections meet only at $x = 0$ is a restriction we put in for the sake of simplicity. We also can have sections run together at $s = 0$ but $x \neq 0$, but then the rationality conditions have to be checked separately, by changing variables.

Proof of Proposition 2.4. (1) Note that $e = \delta$ and δ_i is either $\delta-1$ or δ , according to whether $i \leq b$ or $i > b$. We get that the first b sections of the ramification locus meet at $s = 0 = x = y$; indeed, the polynomials $s^{e-\delta_i}g_i(s)$ for $i = 1, \dots, b$ vanish at $s = 0$, but have different first derivatives $0, a_2, \dots, a_b$. Thus $(0, 0, 0)$ is rational by part (1) of [Proposition 2.1](#) (note that b plays the role of m). The condition concerning f_{b+1}, \dots, f_d ensures that no other points with $s = 0$ are singular; no other meeting of sections occurs.

- (2) follows in a similar way from part (2) of [Proposition 2.1](#).
 (3a) and (3b) are consequences of part (3) of [Proposition 2.1](#).
 (4) comes down to part (4) of [Proposition 2.1](#). \square

3. Singular coverings of curves and c.t. modules

We will sketch as succinctly as possible the construction of [\[GP\]](#), which comes from the theory of 1-motives and attaches a cohomologically trivial module M to a ramified Galois covering of curves $E \rightarrow X$ over \mathbb{F}_q . (In [\[GP\]](#) the notation is $X \rightarrow Y$, but this would not fit at all with our present setup. Also note that many authors understand a “Galois covering” of curves to be étale; in this parlance, we would have to say “generically Galois”.) So E and X continue to denote curves over a field, but this is now a finite field, in contrast with previous usage. For the sake of simplicity let us assume G (the Galois group of E/X) to be cyclic of order ℓ , a chosen prime number which may well be 2, and let S be a finite non-empty set of points of X so that $E \rightarrow X$ is unramified outside S . We need to review a certain amount of notation, asking the reader for a little patience. Full details of the construction are given in Section 2 of [\[GP\]](#).

To begin with, we need another finite nonempty set Σ of points of X , disjoint with S . (It only plays an auxiliary role.) This leads to the so-called generalised Jacobian $J_{E,\Sigma}$. For the reader’s convenience we give a brief description: its \mathbb{F} -points (for \mathbb{F} any field containing \mathbb{F}_q) are given as the group of degree zero divisors on $E_{\mathbb{F}}$ modulo the following equivalence relation: two divisors are equivalent iff their difference is the divisor of a function f which evaluates to 1 in every point above a point of Σ . Then $J_{E,\Sigma}$ as an algebraic group is the extension of the usual Jacobian variety J_E by a torus $\mathbb{T}(\Sigma)$ depending only on Σ .

We also need Tate modules. For any \mathbb{Z}_{ℓ} -module J one puts $T_{\ell}(J) = \varprojlim J[\ell^{\nu}]$, the limit being taken along the transition maps $J[\ell^{\nu+1}] \rightarrow J[\ell^{\nu}]$ given by multiplication by ℓ . If we take J to be the ℓ -part of $J_{E,\Sigma}(\bar{\mathbb{F}}_q)$, the resulting Tate module is simply written $T_{\ell}(J_{E,\Sigma})$ as usual.

A few more definitions: \bar{S} stands for the set of points in $E_{\bar{\mathbb{F}}_q}$ above points in S (please note the slight abuse of notation, suppressing E). Let $\mathbb{Z}_{\ell}\bar{S}$ denote the free \mathbb{Z}_{ℓ} -module with basis \bar{S} and let $(\mathbb{Z}_{\ell}\bar{S})^0$ be the kernel of the map $\mathbb{Z}_{\ell}\bar{S} \rightarrow \mathbb{Z}_{\ell}$ which sends every $x \in \bar{S}$ to 1.

The module M that plays a central role in [\[GP\]](#) now arises as middle term of a short exact sequence

$$0 \rightarrow T_{\ell}(J_{E,\Sigma}) \rightarrow M \rightarrow (\mathbb{Z}_{\ell}\bar{S})^0 \rightarrow 0.$$

All modules carry a G -action and the maps are compatible with it, so we do have an extension of $\mathbb{Z}_{\ell}[G]$ -modules. It remains to specify the class of this extension in the relevant Ext group.

Lemma 3.1. *Let V be any $\mathbb{Z}_\ell[G]$ -module isomorphic to $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^n$ over \mathbb{Z}_ℓ for some $n < \infty$. Then $T_\ell(V) \cong \mathbb{Z}_\ell^n$, and for any $\mathbb{Z}_\ell[G]$ -module N there is a canonical epimorphism*

$$\psi : \operatorname{Hom}_{\mathbb{Z}_\ell[G]}(N, V) \rightarrow \operatorname{Ext}_{\mathbb{Z}_\ell[G]}^1(N, T_\ell(V)).$$

If $\operatorname{Hom}_{\mathbb{Z}_\ell[G]}(N, T_\ell(V)) = 0$, then ψ is an isomorphism.

Proof. Use that $V \cong (\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} T_\ell(V)$, and the long exact sequence for Ext coming from the s.e.s. $0 \rightarrow T_\ell(V) \rightarrow \mathbb{Q} \otimes_{\mathbb{Z}} T_\ell(V) \rightarrow V \rightarrow 0$. The term $\operatorname{Ext}_{\mathbb{Z}_\ell[G]}^1(N, \mathbb{Q} \otimes T_\ell(V))$ is zero since the second argument is an injective $\mathbb{Z}_\ell[G]$ -module. \square

Using this lemma, we now can describe the class of the extension defining M : it is $\psi(\operatorname{div})$, where $\operatorname{div} : (\mathbb{Z}_\ell \bar{S})^0 \rightarrow J_{E, \Sigma}$ is the natural divisor class map, associating to each degree zero divisor supported on \bar{S} its class in the generalised Jacobian. The main result of [GP] on the algebraic side (Theorem 3.9 (1)) says that M is cohomologically trivial over G . Equivalently, M has projective dimension at most 1 over $\mathbb{Z}_\ell[G]$.

Later we will extend most of this construction to families of curves (in other words, we are going to sheafify it over a base C), but it turns out that the auxiliary set Σ causes technical problems, so we need a slightly different version of the above construction, with Σ removed. Recall that $\mathbb{T}(\Sigma)$ is a torus, defined to be the kernel of the surjection $J_{E, \Sigma} \rightarrow J_E$, and put $M_\Sigma = T_\ell(\mathbb{T}(\Sigma)(\bar{\mathbb{F}}_q))$. Over $\bar{\mathbb{F}}_q$, the torus $\mathbb{T}(\Sigma)$ is the cokernel of an injection $\mathbb{G}_m \rightarrow \mathbb{G}_m^{\bar{\Sigma}}$, where $\bar{\Sigma}$ is the set of points over Σ in $E_{\bar{\mathbb{F}}_q}$. The group G acts without fixed points (that is, freely) on $\bar{\Sigma}$. One then obtains two short exact sequences:

$$0 \rightarrow M_\Sigma \rightarrow M \rightarrow M' \rightarrow 0$$

and

$$0 \rightarrow T_\ell(J_E) \rightarrow M' \rightarrow (\mathbb{Z}_\ell \bar{S})^0 \rightarrow 0.$$

This latter extension comes from a divisor class map exactly as before. The module M' no longer depends on Σ ; it will be our substitute for M . From the above description of the torus as a cokernel, and since $T_\ell(\mathbb{G}_m(\bar{\mathbb{F}}_q)) = \mathbb{Z}_\ell$, one sees that there is another s.e.s. $0 \rightarrow \mathbb{Z}_\ell \rightarrow P \rightarrow M_\Sigma \rightarrow 0$ for some free $\mathbb{Z}_\ell[G]$ -module P . As a consequence, we get a four-term exact sequence

$$0 \rightarrow \mathbb{Z}_\ell \rightarrow P \rightarrow M \rightarrow M' \rightarrow 0,$$

with P free and M of projective dimension ≤ 1 over $\mathbb{Z}_\ell[G]$; in particular both P and M are cohomologically trivial (c.t. for short) over G . This motivates the following definition:

Definition.

- (1) Any $\mathbb{Z}_\ell[G]$ -module A admitting an exact sequence $0 \rightarrow \mathbb{Z}_\ell \rightarrow P \rightarrow Q \rightarrow A \rightarrow 0$ with P and Q c.t. over G will be called *almost cohomologically trivial* (almost c.t. for short).
- (2) A $\mathbb{Z}_\ell[G][[\Gamma]]$ -module A will be called *almost c.t. in the strict sense* if the same condition holds where \mathbb{Z}_ℓ , P and Q are likewise $\mathbb{Z}_\ell[G][[\Gamma]]$ -modules, and the module \mathbb{Z}_ℓ is $\mathbb{Z}_\ell(1)$ when taking also the Γ -action into account, that is, the Tate module of the roots of unity. So the (geometric) Frobenius F just acts as multiplication by $1/q$.

We now need to use cohomology groups explicitly. Let us agree that all group cohomology is Tate cohomology and that we omit the hat accent over H . So $H^0(G, M)$ is not M^G but the quotient $M^G/N_G M$. This also fits well with the notion of cohomologically trivial modules: M is c.t. over G iff $H^i(U, M) = 0$ for all $i \in \mathbb{Z}$ and all subgroups U of G . For any almost c.t. G -module A and any $i \in \mathbb{Z}$ we have

$$H^i(G, A) \cong H^{i+2}(G, \mathbb{Z}_\ell).$$

The module M' constructed above is almost c.t., even in the strict sense, since the \mathbb{Z}_ℓ term arose as $T_\ell(\bar{\mathbb{F}}_q^*)$, so the action of Frobenius is the cyclotomic one.

This slightly modified construction can now be adapted to certain *singular curves* E which are Galois covers of $X = \mathbb{P}^1$. This all happens over the algebraic closure $\bar{\mathbb{F}}_q$, and to lighten notation we will just write E , not $E_{\bar{\mathbb{F}}_q}$. All the modules we construct will carry two commuting actions, one of the Galois group G , and another of $\Gamma = \text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. The curve E will be defined by an equation $y^\ell = f(x)$, where x is the coordinate of $X = \mathbb{P}^1$, ℓ divides $q - 1$, $f(x)$ may have multiple roots. Note that ℓ (a fixed prime) now takes the role of r in previous sections. While one could strive for more generality, we think $\ell = r$ is a fundamental case, and we want to keep things simple. Thus the group G is cyclic of order ℓ ; at the time being we cannot deal with noncyclic groups. (Very likely, cyclic groups of nonprime order could be treated by similar methods.)

We *assume* that no root of $f(x)$ has multiplicity more than $\ell + 1$, and that the degree of $f(x)$ is coprime to ℓ . One may transform the equation into

$$y^\ell = x^e g(x), \quad 0 < e \leq \ell + 1, \quad g(0) \neq 0, \quad \gcd(\ell, e + \deg(g)) = 1.$$

(This mirrors what happens in a fibre of \mathcal{E} (see previous sections) when exactly e sections of the ramification locus meet at $x = 0$.) The action of the cyclic group G of order ℓ is clear: a fixed generator σ sends y to ζy . (Recall that ζ is a fixed primitive ℓ -th root of unity.) We will not need an explicit equation near $x = \infty$; it is enough to know that there is exactly one point at ∞ and it is smooth.

There is a fundamental dichotomy of cases: (I) e is coprime to ℓ and (II) $\ell = e$. There is a finite covering $\tilde{E} \rightarrow E \rightarrow X = \mathbb{P}^1$ with $\tilde{E} \rightarrow E$ a birational morphism, and \tilde{E}

still a G -covering of X , which is an isomorphism outside $(0, 0)$ and locally at $(0, 0)$ the normalisation of E . (The normalisation is understood inside the function field. If $g(x)$ is without repeated factors, then \tilde{E} is already the global normalisation of E in its function field.) In case (I) we do not need to know \tilde{E} explicitly; it suffices to know that it has exactly one point above the singular point $(0, 0)$, and consequently for later use, the kernel of $\text{Pic}(\tilde{E}) \rightarrow \text{Pic}(E)$ is a successive extension of additive groups $\alpha_{\mathbb{F}_q}$. We record an immediate consequence of this, since it will be important in the sequel.

Lemma 3.2. *In case (I) the Tate module $T_\ell(\ker(\text{Pic}(\tilde{E}) \rightarrow \text{Pic}(E)))$ is zero.*

In the more interesting case (II), \tilde{E} is given by the equation $\tilde{y}^\ell = g(x)$, by setting $\tilde{y} = y/x$.

We now continue our discussion, treating the case (I) and (II) together for a while. The ramification divisor $R(E/X)$ consists of 0, the zeros of $g(x)$, and ∞ . We repeat that we are now working over $\overline{\mathbb{F}}_q$, so E now stands for the object that was $E_{\overline{\mathbb{F}}_q}$ before. Therefore $\mathbb{Z}_\ell \tilde{S}$ is the free \mathbb{Z}_ℓ -module on $R(E/X)$, where each point of $R(E/X)$ is considered as a point of E , not of X ; the distinction is important even though $E \rightarrow X$ is bijective on ramified points. We introduce the divisor class map on the degree zero submodule $(\mathbb{Z}_\ell \tilde{S})^0$ in such a way that it is consistent with the degeneration of smooth fibres into singular fibres that will occur later. To each finite point $\xi \in R(E/X)$ we attach the degree $\text{ord}_\xi(x^e g)$ (the vanishing order of $x^e g$ at ξ). In particular 0 is given the degree e . To ∞ we give degree 1.

The degree zero divisor $0 - e\infty$ is mapped to the class of the following Cartier divisor D on E : Near $(0, 0)$, the local equation is $y = 0$. No other points outside infinity give any contribution; at infinity we take the $-e$ -th power of a local parameter. Then D has degree 0 and is by construction locally principal. We claim that in case II ($e = \ell$) the preimage \tilde{D} of D in \tilde{E} is principal. Indeed, the function \tilde{y} is invertible at all ℓ points of \tilde{E} above $(0, 0)$, so \tilde{D} is given there by $x = 0$, and hence $\tilde{D} = \text{Div}(x)$. This will be important later. Note that 0 is no longer ramified in \tilde{E}/\mathbb{P}^1 . (Remark: In case (I) 0 remains ramified after normalising in $(0, 0)$. Here \tilde{D} need not be principal, but it can be easily described: take e times the (smooth) point above $(0, 0)$ and $-e$ times infinity on \tilde{E} .)

For other finite points $\xi \in R(E/X)$ with degree e' , the divisor class map $\text{div}(\xi - e'\infty)$ is defined similarly; if one wants formulas, one simply moves ξ to 0. We no longer claim that D becomes principal in \tilde{E} .

This divisor class map $\text{div} = \text{div}_E : (\mathbb{Z}_\ell \tilde{S})^0 \rightarrow \text{Pic}^0(E)$ gives rise to an extension

$$0 \rightarrow T_\ell(J_E) \rightarrow M_E \rightarrow (\mathbb{Z}_\ell \tilde{S})^0 \rightarrow 0,$$

via Lemma 3.1. Note that M_E was M' a little ago; we now omit the prime, since the old unprimed M will not appear again. We have similar data $\tilde{S}_{\tilde{E}}$, $\text{div}_{\tilde{E}}$, $M_{\tilde{E}}$ attached to \tilde{E} instead of E . (Now \tilde{S} will be written \tilde{S}_E , to emphasise the roles of E and \tilde{E} .) This leads to a natural map $\pi : M_{\tilde{E}} \rightarrow M_E$.

Proposition 3.3. *The map $\pi : M_{\tilde{E}} \rightarrow M_E$ induces isomorphisms on G -cohomology.*

Proof. The canonical map $\beta : J_E(\bar{\mathbb{F}}_q) \rightarrow J_{\tilde{E}}(\bar{\mathbb{F}}_q)$, induced by pullback of line bundles, is well known to be onto. (One may see this as follows: Every line bundle on \tilde{E} is isomorphic to a line bundle attached to a divisor whose support lies in the locus of bijectivity of $\tilde{E} \rightarrow E$, and such a bundle of course comes from a bundle on E .) Let $J(\tilde{E}/E)$ be the kernel of β .

There is also a canonical map $\alpha : (\mathbb{Z}_\ell \bar{S}_E)^0 \rightarrow (\mathbb{Z}_\ell \bar{S}_{\tilde{E}})^0$. In case (I), α is an identity on divisors whose support does not contain (0) . Note that the ramification sets $R(\tilde{E}/\mathbb{P}^1)$ and $R(E/\mathbb{P}^1)$ are in 1–1 correspondence. We declare that α sends the divisor $(0) - e\infty$ to $e(0) - \infty$. (With this definition, the diagram below will commute.) Then α is injective, and after ℓ -completion an isomorphism. In case (II), α is just the restriction map $(\mathbb{Z}_\ell \bar{S}_E)^0 = \text{Maps}^0(R(E/\mathbb{P}^1), \mathbb{Z}_\ell) \rightarrow \text{Maps}^0(R(\tilde{E}/\mathbb{P}^1), \mathbb{Z}_\ell) = (\mathbb{Z}_\ell \bar{S}_{\tilde{E}})^0$. Then α is onto, and its kernel is the \mathbb{Z} -span of the divisor $D = (0) - e\infty$.

Let $Z_{\tilde{E}/E}$ be the kernel of α in either case. Then we obtain a commutative diagram:

$$\begin{array}{ccc} Z_{\tilde{E}/E} & \xrightarrow{\tilde{div}} & J(\tilde{E}/E) \\ \downarrow & & \downarrow \\ (\mathbb{Z}_\ell \bar{S}_E)^0 & \xrightarrow{div_E} & J_E(\bar{\mathbb{F}}_q) \\ \alpha \downarrow & & \beta \downarrow \\ (\mathbb{Z}_\ell \bar{S}_{\tilde{E}})^0 & \xrightarrow{div_{\tilde{E}}} & J_{\tilde{E}}(\bar{\mathbb{F}}_q) \end{array}$$

The map \tilde{div} is well-defined since the class of D becomes trivial when pulled back to \tilde{E} , as explained above.

Translating the divisor class maps into extensions as before, we now get the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & T_\ell(J(\tilde{E}/E)) & \longrightarrow & \tilde{M} & \longrightarrow & Z_{\tilde{E}/E} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & T_\ell(J_E) & \longrightarrow & M_E & \longrightarrow & (\mathbb{Z}_\ell \bar{S}_E)^0 \longrightarrow 0 \\ & & \downarrow & & \pi \downarrow & & \downarrow \\ 0 & \longrightarrow & T_\ell(J_{\tilde{E}}) & \longrightarrow & M_{\tilde{E}} & \longrightarrow & (\mathbb{Z}_\ell \bar{S}_{\tilde{E}})^0 \longrightarrow 0 \end{array}$$

Since the T_ℓ -column is short exact and the S -column is short exact, so is the middle column. Now in case (I) (e coprime to ℓ), $T_\ell(J(\tilde{E}/E))$ is zero by [Lemma 3.2](#), and $Z_{\tilde{E}/E}$ is zero since α is injective as said a little earlier. Hence \tilde{M} is zero in case (I), and we even get that $\pi : M_E \rightarrow M_{\tilde{E}}$ is an isomorphism. In case (II) we do not claim this to be the case. However for π to induce isomorphisms on G -cohomology, it suffices that \tilde{M} has

no G -cohomology. The rest of the proof will establish this. So we may and will focus on case (II) from now on. We are actually going to show that \tilde{M} is $\mathbb{Z}_\ell[G]$ -free of rank one.

Recall that we are working over $\bar{\mathbb{F}}_q$. We have to understand the “relative Picard group” $J(\tilde{E}/E)$. If $e = 2$ (recall $e = \ell$ since we are in case (II)), then E arises from \tilde{E} by glueing two points P_0 and P_1 into one point P , and then it is well known, by an argument of Mayer–Vietoris type, that $J(\tilde{E}/E)$ identifies with the multiplicative group \mathbb{G}_m , even functorially, so $\ker(\mathrm{Pic}(E) \rightarrow \mathrm{Pic}(\tilde{E})) \cong \bar{\mathbb{F}}_q^*$. (The Mayer–Vietoris sequence that is attached to the relevant Cartesian square of schemes is more visible when one writes $(\mathbb{G}_m \times \mathbb{G}_m)/\mathrm{diag}(\mathbb{G}_m)$ instead of \mathbb{G}_m .) The identification goes as follows: given a line bundle \mathcal{N} on E that trivialises on \tilde{E} , take a generating section u of the pullback of \mathcal{N} to \tilde{E} , and a generating section v of \mathcal{N} near the node P . Then $w := v/u$ is invertible in P_0 and P_1 , and the class of \mathcal{N} maps to the class of the pair $(w(P_0), w(P_1))$ modulo the diagonal.

For $\ell = e > 2$ there is a slight difficulty. The curve E is obtained from \tilde{E} first by identifying e points P_0, \dots, P_{e-1} into one, which gives a singularity of embedding dimension e (the tangents of the e points are linearly independent), and then making the tangent space two-dimensional (the tangents remain pairwise distinct but no longer independent if $e > 2$). The second process corresponds to a morphism of curves that is bijective on points, so the associated kernel of Picard groups is annihilated by a power of the characteristic, and will therefore be irrelevant for us. There is an epimorphism $J(\tilde{E}/E) \rightarrow (\bar{\mathbb{F}}_q^* \times \dots \times \bar{\mathbb{F}}_q^*)/\mathrm{diag}(\bar{\mathbb{F}}_q^*)$, where the product has ℓ factors, cyclically permuted by G , and the kernel of this epimorphism has no ℓ -torsion. So the kernel disappears on taking Tate modules, and T_ℓ of the target is naturally isomorphic to $\mathbb{Z}_\ell[G]/\mathbb{Z}_\ell N_G$. The description of the epimorphism is analogous to the case $e = 2$: given a line bundle \mathcal{N} on E that trivialises on \tilde{E} , take a generating section u of the pullback of \mathcal{N} to \tilde{E} , and a generating section v of \mathcal{N} near the node P . Then $w := v/u$ is invertible in the points P_i ($i = 0, \dots, \ell - 1$), and the class of \mathcal{N} maps to the class of the ℓ -tuple $(w(P_0), \dots, w(P_{\ell-1}))$ modulo the diagonal.

We are going to show that the extension module \tilde{M} attached to the map $\widetilde{\mathrm{div}}$ is free of rank one over $\mathbb{Z}_\ell[G]$. The term preceding (following) \tilde{M} in the top row of the last diagram is isomorphic to $\mathbb{Z}_\ell[G]/\mathbb{Z}_\ell N_G$ (\mathbb{Z}_ℓ respectively). One easily calculates that $\mathrm{Ext}_{\mathbb{Z}_\ell[G]}^1(\mathbb{Z}_\ell, \mathbb{Z}_\ell[G]/\mathbb{Z}_\ell N_G)$ is cyclic of order ℓ , and that all nonsplit elements of this Ext have middle term isomorphic to $\mathbb{Z}_\ell[G]$. Thus it suffices that the class of the extension is not zero.

We claim: If D is the divisor on E constructed above (the generator of $Z_{\tilde{E}/E}$), then $\widetilde{\mathrm{div}}(D)$ is of order ℓ in $(\bar{\mathbb{F}}_q^* \times \dots \times \bar{\mathbb{F}}_q^*)/\mathrm{diag}(\bar{\mathbb{F}}_q^*)$. Indeed, the pullback of D to \tilde{E} is defined by $x = 0$, and locally at the singular point $(0, 0)$, D is defined by $y = 0$. The quotient y/x evaluated at all the points P_i above $(0, 0)$ runs through the values $\zeta^i \alpha$, fixing some ℓ -th root α of $g(0)$. The resulting tuple $(1, \zeta, \dots, \zeta^{\ell-1})\alpha$ is not in the image of the diagonal. By Lemma 3.1, the extension class associated to $\widetilde{\mathrm{div}}$ is not the trivial class, since $\mathrm{Hom}_{\mathbb{Z}_\ell[G]}(\mathbb{Z}_\ell, \mathbb{Z}_\ell[G]/\mathbb{Z}_\ell N_G)$ is zero, so ψ is an isomorphism. As seen in the

previous paragraph, this suffices to make \tilde{M} free. So we certainly have established that \tilde{M} is cohomologically trivial over G . This concludes the proof of [Proposition 3.3](#). \square

4. Construction of the almost cohomologically trivial sheaf, and the main congruence

We now come back to our superelliptic curve E/K and its model $\mathcal{E} \rightarrow C = \mathbb{P}^1$. For the form of the equation and the construction of \mathcal{E} we refer back to [Section 2](#). For the whole of this section, we will assume that the singularities of \mathcal{E} are all rational. Conditions ensuring this are listed in [Propositions 2.1 and 2.4](#). In the next section we will look at concrete examples. Note that we will take r (the exponent of y in the defining equation) equal to ℓ from now on, in accordance with the preceding section, so G will always be cyclic of order ℓ .

Recall that we constructed an étale sheaf \mathcal{F} on the base C such that $L(T, E/K)$ is the characteristic polynomial of Frobenius on $H^1(C, \mathcal{F})$. (Abuse of notation: of course we mean the char. pol. of Frobenius acting on $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} H^1(C, \mathcal{F})$.) We also explained that $L(T, E/K)$ can be seen as the inverse of $\prod_{i=0}^2 \det(1 - TF : \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} H^i(C, \mathcal{F}))^{(-1)^i}$, simply because the H^0 - and H^2 -terms vanish. Therefore $L(T, E/K)$ can be calculated as a product over the points of $C = \mathbb{P}_{\mathbb{F}_q}^1$ as explained earlier.

Now \mathcal{F} carries a G -action, and we are interested in the so-called G -equivariant L -function. (Equivariant L -functions, also known as equivariant zeta-functions, have been studied by D. Burns and many other authors; as a background, we refer to [Section 2.2](#) in [\[Bu\]](#).) We get the equivariant L -function by taking the characteristic polynomial over $\mathbb{Q}_\ell[G]$ instead of over \mathbb{Q} as follows:

$$L_G(T, E/K) = \det_{\mathbb{Q}_\ell[G]}(1 - TF : \mathbb{Q}_\ell \otimes H^1(C, \mathcal{F}))^{-1}.$$

Again we can formally put in H^0 - and H^2 -terms; therefore we get a formula representing $L_G(T, E/K)$ as a product indexed with $v \in C$ (we recall one last time that $C = \mathbb{P}^1$):

$$L_G(T, E/K) = \prod_{v \in C} \det_{\mathbb{Q}_\ell[G]}(1 - T^{d(v)} F : \mathbb{Q}_\ell \otimes \mathcal{F}_v)^{-1}.$$

The connection with the non-equivariant L -function is the following: Every ℓ -adic character χ of the abelian group G extends to an algebra map $\mathbb{Q}_\ell[G][T] \rightarrow \mathbb{Q}_\ell(\zeta_{|G|})[T]$ (just being identity on T), and with this understanding we have the product formula

$$L(T, E/K) = \prod_{\chi \in \hat{G}} \chi(L_G(T, E/K)).$$

More conveniently for us, we let χ_0 be the trivial character and fix one nontrivial character χ_1 of G ; this character has values in $\mathbb{Q}(\zeta)$. Then we get $L(T, E/K) = \chi_0(L_G(T, E/K)) \cdot N(\chi_1(L_G(T, E/K)))$, where $N : \mathbb{Z}_\ell[\zeta_\ell][T] \rightarrow \mathbb{Z}_\ell[T]$ is the norm map,

induced from the usual norm $\mathbb{Q}(\zeta_\ell) \rightarrow \mathbb{Q}$. For $\ell = 2$, this norm is just the identity map, and can be omitted.

As the $\mathbb{Z}_\ell[G]$ -module $H^1(C, \mathcal{F})$ need not be free, we should not expect good integrality properties of the equivariant L -function. The central point of this section (one may say, of the whole paper) is to remedy this by modifying the sheaf \mathcal{F} . Ideally, all stalks \mathcal{F}_v should become c.t.; this will be achieved up to a controllable error term. In our parlance, \mathcal{F}_v will become *almost cohomologically trivial*.

To this purpose, we discuss the ramification sheaf \mathcal{S}_0 and the divisor class map. Recall $S \subset \mathcal{E}$ is the ramification locus of the ramified degree ℓ covering $\mathcal{E} \rightarrow \mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1$. The sections of S are given by $x = f_i(t)$, plus one component at infinity. We put $\mathcal{S}_\nu = \text{Hom}_{\mathbb{P}^1}(S, \mathbb{Z}/\ell^\nu)$ (morphisms of schemes over \mathbb{P}^1 , the target being the constant scheme \mathbb{Z}/ℓ^ν). Then we let \mathcal{S} be the projective limit of the \mathcal{S}_ν , and \mathcal{S}_0 be the kernel of augmentation. These are constructible sheaves on \mathbb{P}^1 . Generically they are just \mathbb{Z}_ℓ^S . Elements (sections) of \mathcal{S}_0 should be thought of as linear combinations of sections of S such that the coefficients sum to zero. At values τ of t where the fibre is singular (equivalently: two or more sections, say S_1, \dots, S_e of the ramification locus meet) the following happens. The fibre $\mathcal{S}_{0,\tau}$ consists, again, of zero-sum linear combinations of sections, but the coefficients of S_1, \dots, S_e have to be equal. So in the case of elliptic curves the following happens: S has four sections, \mathcal{S}_0 is generically of rank three, and at points of multiplicative (additive) bad reduction, the rank drops by one (respectively two).

The divisor class map is generically exactly what one expects: a linear combination of sections S_i , that is, of points in the generic curve, is mapped to the class of the corresponding divisor. This gives the map $\text{div} : \mathcal{S}_0|U \rightarrow \text{Pic}^0(\mathcal{E}|U)$. We need this map to land in a certain ℓ^ν -torsion part. But this is easy. In the hyperelliptic case $\ell = 2$ all divisor classes $[D] = [S_i] - [S_j]$ are 2-torsion, since $2D$ is a degree zero divisor coming from the base curve \mathbb{P}^1 . For general prime numbers ℓ the argument is exactly the same. We see that ν can be taken to be 1.

At points $t = \tau$ with smooth fibre, div becomes exactly the divisor class map $\text{div}_{\mathcal{E}_\tau}$ attached to the fibre \mathcal{E}_τ , which is a G -cover of \mathbb{P}^1 , ramified in S_τ .

By functoriality div gives a map, still denoted div , from \mathcal{S}_0 into $j_* \text{Pic}^0(\mathcal{E}_U/U)[\ell^\nu]$. It can be described explicitly as follows. Suppose the sections S_1, \dots, S_e run together into one point P at $t = \tau$ (and the other sections stay clear of that point). We want to explain what div does to the linear combination $D = S_1 + \dots + S_e - eS_*$, where S_* is any section distinct from the S_i . The S_i are principal divisors on a punctured neighbourhood of P . Now while the closure of S_i need not be principal near P , we will see by explicit calculation that the principal divisor $S_1 + \dots + S_e$ in a punctured neighbourhood of P extends to a principal divisor near P . The class of this principal divisor near P , together with the contribution coming from $-eS_*$, is the image of D in the fibre.

This definition of the divisor class map in the fibre is consistent with the previous description for an individual singular curve. The \mathbb{Z}_ℓ -valued functions on S that take the same value on S_1, \dots, S_e are in canonical bijection with the \mathbb{Z}_ℓ -valued functions on S_τ ,

which arises from S by identifying the sections S_1, \dots, S_e into one element. Likewise, the degrees of points and the kernels of augmentation are in correct correspondence.

Example. Take the Minimal Example $y^2 = x(x-1)(x-t)$ at $t=0$, where the two sections $S_1 : x=0=y$ and $S_2 : x-t=0=y$ run together. The section S_1 defines a locally principal ideal outside P , generated by x and y . This does not extend to a locally free ideal at P . The ideal (x, y) is “divisorial” at P but not principal. But if we take the two sections together, the equations are $y=0=x(x-t)$; this extends to a locally principal ideal, with generator y at P .

Now let $\mathcal{F} = T_\ell(\mathrm{Pic}_{\mathcal{E}/\mathbb{P}^\infty}^0)$. The divisor class map $\mathcal{S}_0 \rightarrow \mathrm{Pic}_{\mathcal{E}/\mathbb{P}^\infty}^0$ then gives rise to an extension of constructible sheaves

$$0 \rightarrow \mathcal{F} \rightarrow \mathcal{M} = \mathcal{M}_{\mathcal{E}} \rightarrow \mathcal{S}_0 \rightarrow 0.$$

As shown in Section 3, for every smooth fibre \mathcal{E}_τ the fibre \mathcal{M}_τ is almost cohomologically trivial over $G = \mathrm{Gal}(X/\mathbb{P}^1)$. We claim the same is true for singular fibres. Let τ be a value where \mathcal{E}_τ is singular, and let $M = \mathcal{M}_\tau$. Then we showed in Section 3 (with \mathcal{E}_τ playing the role of E): if \tilde{E} arises from \mathcal{E}_τ by resolving one singularity, and \tilde{M} is the analog of M for \tilde{E} , then M and \tilde{M} are linked by a s.e.s. $0 \rightarrow (\text{c.t.}) \rightarrow M \rightarrow \tilde{M} \rightarrow 0$. It is an easy algebraic matter to deduce that the same is true if \tilde{E} is obtained by resolving a finite number of singularities, one at a time. Thus we can assume that \tilde{E} is smooth, so \tilde{M} is almost c.t. Now again it is an easy argument using pullbacks to see that this implies: M is almost c.t. as well. We restate this as a theorem, introducing a shorthand: A sheaf \mathcal{N} on C will be called almost c.t. if all its stalks over closed points of C are.

Theorem 4.1. *The sheaf $\mathcal{M} = \mathcal{M}_{\mathcal{E}}$ is almost cohomologically trivial.*

This has consequences for equivariant characteristic polynomials. For every C -sheaf \mathcal{N} with commuting actions of G and Frobenius, we abbreviate

$$\chi_G(\mathcal{N}, T) = \prod_{v \in C} \det_{\mathbb{Q}_\ell[G]}(1 - T^{d(v)} F : \mathbb{Q}_\ell \otimes \mathcal{N}_v).$$

A priori, this is an element in $\mathbb{Q}_\ell[G][[T]]$; its image under any $\chi \in \hat{G}$ is in $\mathbb{Z}_\ell(\chi)[[T]]$.

For any $f \in \mathbb{Q}_\ell[T]$ let $f_* \in \mathbb{Q}_\ell[G][T]$ be the unique element with $\chi_0(f_*) = f$ and $\chi(f_*) = 1$ for all nontrivial χ . We then have the following integrality property:

Lemma 4.2. *If M is an almost c.t. module over $\mathbb{Z}_\ell[G][[T]]$, then there is some element $P(T) \in 1 + T\mathbb{Z}_\ell[G][[T]]$ such that*

$$\det_{\mathbb{Q}_\ell[G]}(1 - TF : \mathbb{Q}_\ell M) = (1 - q^{-1}T)_* \cdot P(T).$$

Proof. One first shows that if P is c.t. over G , then $f_M := \det_{\mathbb{Q}_\ell[G]}(1 - TF : \mathbb{Q}_\ell P)$ lies in $1 + T\mathbb{Z}_\ell[G][[T]]$. (Reduce to the case that P is $\mathbb{Z}_\ell[G]$ -free.) Then one looks at a sequence which testifies that M is almost c.t. (in the sharp sense, involving also the action of Frobenius):

$$0 \rightarrow \mathbb{Z}_\ell(1) \rightarrow P \rightarrow Q \rightarrow M \rightarrow 0,$$

where the $\mathbb{Z}_\ell[G][[T]]$ -modules P and Q are c.t. over G . Recall that G acts trivially on $\mathbb{Z}_\ell(1)$. By multiplicativity one then gets

$$\det_{\mathbb{Q}_\ell[G]}(1 - TF : \mathbb{Q}_\ell M) = f_Q \cdot f_P^{-1} \cdot \det_{\mathbb{Q}_\ell[G]}(1 - TF : \mathbb{Q}_\ell(1)).$$

It is now easy to see that the last det is precisely $(1 - q^{-1}T)_*$. \square

We now combine the preceding results, using the following somewhat abusive notation: for $z \in \mathbb{Q}_\ell[G]$, the character values $\chi_0(z)$ and $\chi_1(z)$ will be written z^+ and z^- respectively. (Of course this notation is suggested by the case $\ell = 2$.)

Theorem 4.3. *There is an element $\tilde{L}(T) \in 1 + T\mathbb{Z}_\ell[G][[T]]$ such that $\chi_G(\mathcal{M}, T) = ((1 - q^{-1}T)(1 - T))_* \tilde{L}(T)$. In more explicit terms:*

$$\begin{aligned}\chi_G(\mathcal{M}, T)^+ &= (1 - q^{-1}T)(1 - T) \cdot \tilde{L}(T)^+; \\ \chi_G(\mathcal{M}, T)^- &= \tilde{L}(T)^-.\end{aligned}$$

Proof. We use the product representation for $\chi_G(\mathcal{M}, T)$ and [Lemma 4.2](#). The element \tilde{L} is the product of the factors $P_v(T^{\deg(v)})$ arising there (one for each $v \in C$). The factor $(1 - q^{-1}T)_*$ gets replaced by $\prod_{v \in C} (1 - q^{-1}T^{\deg(v)})_*$, and from the formalism of the zeta function for \mathbb{P}^1 one knows that this product is $(1 - q^{-1}T)(1 - T)_*$. This shows the first equality; the rest is only a restatement. \square

It remains to get back from the module \mathcal{M} to the module \mathcal{F} . To explain what is going on let us begin by an observation. Recall that ζ is a fixed primitive ℓ -th root of unity. Now if we are given two series $f \in \mathbb{Z}_\ell[[T]]$, $g \in \mathbb{Z}_\ell(\zeta)[[T]]$, there is $h \in \mathbb{Z}_\ell[G][[T]]$ such that $h^+ = f$ and $h^- = g$ if and only if $f \equiv g$ modulo $(1 - \zeta)$. That is, the image of f modulo ℓ (which lies in $\mathbb{F}_\ell[[T]]$) has to agree with the image of g modulo $1 - \zeta$ (which again lies in $\mathbb{F}_\ell[[T]]$). Thus, integrality in the group-ring sense is equivalent to a congruence of character components. In particular the preceding theorem implies the congruence

$$\chi_G(\mathcal{M}', T)^- \equiv \frac{1}{(1 - q^{-1}T)(1 - T)} \chi_G(\mathcal{M}', T)^+ \quad (1)$$

modulo $1 - \zeta$. Actually, since $q \equiv 1$ modulo ℓ , we may, and we will, omit the factor q^{-1} in front of one of the T 's.

We now come back to the “defining” short exact sequence for \mathcal{M} :

$$0 \rightarrow \mathcal{F} \rightarrow \mathcal{M} \rightarrow \mathcal{S}_0 \rightarrow 0.$$

This will lead to a congruence concerning $L_G(T, E/K)$. By the s.e.s. and by construction, we have

$$\chi_G(\mathcal{M}) = \chi_G(\mathcal{S}_0)L_G(T, E/K)^{-1}. \quad (2)$$

Now the plus part of $L_G(T, E/K)$ is 1, since this plus part is simply the L -function of the relative curve $Y \rightarrow C$, which is a relative \mathbb{P}^1 . On the other hand, G acts trivially on S and on \mathcal{S}_0 , so the minus part of $\chi_G(\mathcal{S}_0)$ is again 1. Thus we get (all congruences mod $(1 - \zeta)$):

$$\begin{aligned} (L_G(T, E/K)^{-1})^- &\equiv \chi_G(\mathcal{S}_0)^-(L_G(T, E/K)^{-1})^- \\ &\equiv \chi_G(\mathcal{M})^- \\ &\equiv \frac{1}{(1-T)^2} \chi_G(\mathcal{M}, T)^+ \\ &\equiv \frac{1}{(1-T)^2} \chi_G(\mathcal{S}_0, T)^+(L_G(T, E/K)^{-1})^+ \\ &\equiv \frac{1}{(1-T)^2} \chi_G(\mathcal{S}_0, T)^+. \end{aligned}$$

This means

$$L_G(T, E/K) \equiv (1-T)^2 / \chi_G(\mathcal{S}_0, T)^+,$$

and the last χ_G -term can also be written without the action of G , simply as $\prod_{v \in C} \det(1 - T^{\deg(v)} F : \mathbb{Q}_\ell \otimes \mathcal{S}_{0,v})$. It remains to calculate this equivariant characteristic polynomial.

The ramification sheaf \mathcal{S}_0 is easily described. Generically it turns out to be $\mathbb{Z}_\ell^{|S|-1} = \mathbb{Z}_\ell^d$, a free \mathbb{Z}_ℓ -sheaf whose rank is the number of sections of S minus one. Over values $t = v$ where sections meet (that is, the fibre \mathcal{E}_v is singular), the rank drops. More precisely, if $n = n(v, \xi)$ sections meet at $(t, x) = (v, \xi)$, the rank of $\mathcal{S}_{0,v}$ drops by $n - 1$. Still more precisely there is a s.e.s.

$$0 \rightarrow \mathcal{S}_0 \rightarrow (\mathbb{Z}_\ell^d)_C \rightarrow \bigoplus_{(v, \xi)} i_{v*} \mathbb{Z}_\ell^{n(v, \xi)-1} \rightarrow 0.$$

Here $i_{v*} \mathbb{Z}_\ell$ denotes the skyscraper sheaf supported in the closed point v , and the sum is over all the finitely many (v, ξ) such that $n(v, \xi) > 1$.

Now the Euler characteristic of the constant sheaf $(\mathbb{Z}_\ell)_C$ is $(1-T)(1-qT)$ (the same product occurring in the zeta function of \mathbb{P}^1) and if we assume that all relevant v, ξ

are \mathbb{F}_q -rational, the Euler characteristic of the skyscraper sheaf $i_{v*}\mathbb{Z}_\ell$ is simply $1 - T$, since the cohomology is concentrated in degree zero, and Frobenius acts trivially. (We will deal with nonrational intersection points later on.) This gives

$$\chi(\mathcal{S}_0, T) \equiv (1 - T)^{2d} / (1 - T)^\kappa,$$

where the “total intersection multiplicity of sections” κ is defined as $\sum_{v, \xi} (n(v, \xi) - 1)$. In the Minimal Example $y^2 = x(x - 1)(x - t)$ this number is 4: the section $x - t$ meets the first section $x = 0$ in $t = 0$, and the second section $x = 1$ in $t = 1$. Both of these events produce multiplicative bad reduction of the fibre, and hence a contribution of 1 to the term κ . On the other hand, the three sections $x = 0, 1, t$ all meet at $x = 0$ and $t = \infty$, as was explained early on in the paper. This contributes a 2 towards κ .

In the general situation we finally get:

Theorem 4.4. *We make the following assumptions: The curve E/K is superelliptic with model $\mathcal{E} \rightarrow C$ (recall $C = \mathbb{P}^1$ and K is the function field of C); the \mathbb{F}_q -trace of the Jacobian of E is trivial; \mathcal{E} has only rational singularities (for more on this refer back to Section 2), and the intersection points of the sections of S are \mathbb{F}_q -rational. Then we have the following congruence:*

$$L_G(T, E/K)^- \equiv (1 - T)^{2-2d} (1 - T)^\kappa = (1 - T)^{2-2d+\kappa} \pmod{1 - \zeta_\ell}.$$

Hence, since $L(T, E/K)$ is the $\mathbb{Z}[\zeta_\ell]/\mathbb{Z}$ -norm of $L_G(T, E/K)$, we also get a congruence

$$L(T, E/K) \equiv (1 - T)^{(\ell-1)(2-2d+\kappa)} \pmod{\ell}.$$

In the Minimal Example the exponent of $1 - T$ in the last congruence is zero, so we have reproved Hall’s result that the L -function is 1 in this case. Further consequences and examples will be given in the ensuing final section.

5. Consequences and examples

We keep the assumption that all singularities of the model \mathcal{E} of the superelliptic curve E/K are rational. Let us begin by recording a corollary to Theorem 4.4, which will remain correct if the intersection points are not \mathbb{F}_q -rational, see below. For $\ell = 2$ this is again due to Hall.

Theorem 5.1. *Under the rationality assumption, the degree of the L -function $L(T, X/K)$ is $2 - 2d + \kappa$, where κ is defined at the end of the preceding section.*

Example 1. We now discuss a hyperelliptic example (so $\ell = 2$) in detail. Let E_2 be given by the following equation

$$y^2 = x(x-t)(x-2t)(x-(t^2+1))(x-(t^2+2))$$

over \mathbb{F}_q with $q \equiv 1$ modulo 24, so $\zeta_6, \sqrt{2}, \sqrt{-1} \in \mathbb{F}_q$. The five polynomials f_i are $0, t, 2t, t^2+1, t^2+2$ in this precise order. We list the loci $A(i, j) = \{\tau : f_i(\tau) = f_j(\tau)\}$. For the moment we exclude $\tau = \infty$; this will be treated separately.

i, j	elements in $A(i, j)$
1, 2	0
1, 3	0
1, 4	$\pm\sqrt{-1}$
1, 5	$\pm\sqrt{-2}$
2, 3	0
2, 4	$\pm\zeta_6$
2, 5	$-1, 2$
3, 4	1
3, 5	$1 \pm \sqrt{-1}$
4, 5	none

It is clear from this list that there is just one point over $t = 0$ where three sections meet, and otherwise at most two sections will meet. At the triple intersection, we have three distinct tangents, since $f_1 = 0, f_2 = t, f_3 = 2t$ are not congruent modulo t^2 . So Proposition 2.1 assures us that all singular points with $t \neq \infty$ are rational singularities. At $t = \infty$ we rewrite the equation as described in Section 2 in the form $y^2 = \prod_{i=1}^5 (x - s^{e-\delta_i} g_i(s))$, with $e = 2$ and $\delta_i = \deg(f_i)$. Then we see that exactly three polynomials $s^{e-\delta_i} g_i$ (the first three) vanish at $s = 0$, and they are incongruent modulo s^2 . The last two are g_4 and g_5 . They happen to share the value 1 at $s = 0$, which is no problem. Proposition 2.4 gives us rationality of these singularities as well. So this is an example of a curve whose model has only rational singularities. It was not hard to find.

Now let us look at the L -function of this curve E_2 of genus 2. It happens exactly twice that $n(\tau, \xi) = 3$ (at $(0, 0)$ and at exactly one point with $t = \infty$), and it happens exactly 10 times that $n(\tau, \xi) = 2$. This totals up to $\kappa = 14$, and so $\mathcal{L}(T) = L(T, E_2/K)$ has degree $2 - 2 \cdot 5 + 14 = 6$.

Example 2. Now for a change, let us deal with a truly superelliptic curve with $\ell = d = 5$. So the genus will be 6 (the same as of the Fermat curve of degree 5). We take $E_6 : y^5 = x \prod_{i=2}^5 (x - f_i(t))$, with $f_2 = t^4 - t, f_3 = 2t^4 - 3t, f_4 = t^5 + 1$ and $f_5 = 2t^5 + 1$. These choices (which were not hard to find) were made to ensure the rationality of singularities, that is, the intersection behaviour in the ramification locus. At $t = \infty$, the first three sections meet, but with different tangent directions, because f_2 and f_3 have degree 4 (one less than the maximal degree 5) and have distinct leading coefficients. No further

meeting occurs in this fibre since f_4 and f_5 have maximal degree 5 and distinct leading coefficients. Examining the behaviour for finite values of t needs a little help from the computer. It is visible that the three first sections meet at $t = 0$ (and $x = 0$), with different tangents since the linear coefficients of f_2 and f_3 are nonzero and distinct. As in the hyperelliptic example we let A_{ij} be the locus of all t where sections number i and j intersect, more simply put: A_{ij} is the set of zeros of $f_j - f_i$. We claim that apart from $t = x = 0$, no more than two sections meet, and always transversally (i.e. with distinct tangents). For this it suffices that A_{ij} has the maximum number of points, i.e. $f_j - f_i$ has no repeated roots, and that $A_{ij} \cap A_{ik} \subset \{0\}$ for every index triple i, j, k without repetition. It suffices to check this for $i < j < k$. The fastest way to check this in one fell blow is to calculate the discriminant of $(f_j - f_i)(f_k - f_i)$. We did this with PARI, and found that everything is fine provided the characteristic p is not on a finite list of bad primes that reads 2, 3, 5, 11, 13, 23, 43, 103, 349, 23879. For example $(f_2 - f_1)(f_4 - f_1) = f_2 f_4$ has discriminant $-337500 = 2^2 3^3 5^5$, which puts 2, 3, 5 on the bad list. Of course 5 was bad to begin with, because of the shape of our equation. If we want all intersection points be \mathbb{F}_q -rational, this imposes further conditions on q , which we do not spell out; of course infinitely many primes p with this property can be found. The smallest seems to be $p = 3121$.

We now calculate the total intersection number κ . It is almost the sum of the cardinals of the A_{ij} (which is $3 \cdot 4 + 6 \cdot 5 = 42$; note $A_{4,5}$ is empty). There are two corrections: we have to subtract 1 since the contribution of $(0,0)$ has to be corrected from 3 to 2; and we have to add 2, for the triple crossing at $t = \infty$. This gives $\kappa = 43$. Hence the degree of $L(T, E_6/K)$ is $(\ell - 1) \cdot 35 = 140$.

So far we have been assuming that all the points (v, ξ) where sections $f_i = 0$ meet are \mathbb{F}_q -rational. This is not necessary. If for instance $f_1 - f_2$ is irreducible of degree δ and coprime to all other differences $f_i - f_j$, we have two sections meeting in a set $A_{ij} = V(f_1 - f_2)$ of points rational over \mathbb{F}_{q^δ} , transitively permuted by the \mathbb{F}_q -Frobenius. For every rational point where two sections meet we had a correction term: the skyscraper sheaf \mathbb{Z}_ℓ on that point, corresponding to a factor $1 - T$. This is now replaced by a skyscraper sheaf on the δ points of A_{ij} , corresponding to a factor $1 - T^\delta$.

With this small generalisation of the main result at our disposal, let us look at one class of elliptic curves related to Hall's work, so $\ell = 2$ and $d = 3$.

Example 3. Suppose $f(t)$ and $g(t)$ are cubic irreducible over \mathbb{F}_q with different leading coefficients, not scalar multiples of each other, and such that $f - g$ is again irreducible (and cubic of course), and take $E : y^2 = x(x - f)(x - g)$. At $t = \infty$ we get additive reduction. The number κ is then $\deg(fg(f - g)) + 2$. The deg term counts the number of events where two sections meet (multiplicative reduction), and the $+2$ comes from $t = \infty$. So $\kappa = 11$. Again, if all intersection points were rational, the corresponding factor would be $(1 - T)^{11}$; now it is $(1 - T)^5(1 + T + T^2)^3$. We obtain $L(T, E/K) \equiv (1 - T)(1 + T + T^2)^3$ modulo 2, so the analytic rank is at most 1. By “analytic rank” of the curve, or rather

its Jacobian, we mean the order of vanishing of $L(T, E/K)$ at $T = 1/q$. The factors $1 + T + T^2$ cannot contribute to this vanishing order since $1/q \equiv 1$ modulo ℓ and 1 is not a root of $1 + T + T^2$. Unfortunately we cannot see the sign ϵ of the functional equation via this congruence modulo 2.

Example 4. Let us give a variant with $\ell = 3$ and still $d = 3$; we make exactly the same assumptions on f and g , only replacing “cubic” by “quadratic”. This is still an elliptic curve: $E' : y^3 = x(x - f)(x - g)$. The singularities are OK. For $t = \infty$ see discussion above; the three sections run together. (We should not call this “additive reduction”; in fact we get three lines that intersect in a point.) Similar calculations as just above give $\kappa = 8$, with corresponding factor $(1 - T)^5(1 + T)^3$ and $L(T, E'/K) \equiv (1 - T)(1 + T)^3$ modulo 3. Here we can read off $\epsilon = -1$, and the analytic rank is exactly 1. It would be interesting to actually find a non-torsion point on the curve.

Example 5. We give one final class of curves: take d general, but prime to ℓ as always, $f_1 = 0$ as usual, and the remaining f_i of degree ℓ . Assume that all $f_i - f_j$ (including $j = 1$) are of the form: a linear factor times an irreducible polynomial, and all leading terms of the f_i ($i > 1$) are distinct. Assume moreover that there are no triple meeting points, that is, $f_i - f_j$ is coprime to $f_i - f_k$ for $\{i, j\} \neq \{i, k\}$. Then the model \mathcal{E} is smooth at $t = \infty$. We have $\kappa = \ell \binom{d}{2}$, the corresponding factor is

$$(1 - T)^{2\binom{d}{2}}(1 + T + \dots + T^{\ell-2})^{\binom{d}{2}},$$

and the congruence is (note that $2\binom{d}{2} - 2d + 2 = (d - 1)(d - 2)$)

$$L(T, E/K) \equiv (1 - T)^{(\ell-1)(d-1)(d-2)}(1 + T + \dots + T^{\ell-2})^{(\ell-1)\binom{d}{2}} \pmod{\ell}.$$

So the analytic rank is at most $(\ell - 1)(d - 1)(d - 2)$, and the sign of the functional equation is $+1$, except perhaps if $\ell = 2$.

To finish, let us indicate a tentative change of scenario. So far we have always assumed that the sections of the ramification divisor S are defined over K . This seems unnecessary. We will just discuss one prototype $E : y^2 = x^3 - t$. Here the sections of S only exist after a cubic extension of K . Still, the sheaf \mathcal{S}_0 exists. One should check whether the divisor class map again extends to the fibre $t = 0$. (I think it does.) There is one great advantage: the obvious minimal model is smooth at $x = y = t = 0$, much in contrast with earlier examples. At $t = \infty$ ($s = 1/t = 0$) we get $y^2 = x^3 - s^5$, which means additive reduction. So we just have additive reduction twice, and $L(T, E/K) \equiv 1$ modulo 2. Hence the L -function is 1, which forces the rank of $X(K)$ to be zero, by Tate’s work (cf. [Ha]). It is not too hard to show this directly.

Acknowledgments

A first very rough draft of this paper was written when W. Gajda, S. Petersen and myself were in the application stage of a joint research project, which then did receive funding by DFG, grant no. GR998/5-1. I would like to thank DFG for this grant and in particular for funding the AVGA meeting 2011 in Poznań. I am grateful to Wojtek Gajda, Chris Hall and Sebastian Petersen for very helpful discussions during that workshop and afterwards, and an extra word of thanks goes to S. Petersen and W. Gajda for their perusal of this text at several stages and their helpful criticism. Last but certainly not least, I would like to thank the referee very much for his painstaking reading and his numerous comments, both insightful and critical, which again led to many improvements.

References

- [BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, *Ergebnisse der Mathematik*, vol. 21, Springer, 1989.
- [Bu] D. Burns, On the values of equivariant zeta functions of curves over finite fields, *Doc. Math.* 9 (2004) 357–399.
- [CJS] V. Cossart, U. Jannsen, Shuji Saito, Canonical embedded and non-embedded resolution of singularities for excellent two-dimensional schemes, preprint, arXiv:0905.2191.
- [GP] C. Greither, C. Popescu, The Galois module structure of ℓ -adic realizations of Picard 1-motives and applications, *Int. Math. Res. Not. IMRN* 2012 (2012) 986–1036.
- [Ha] C. Hall, L -functions of twisted Legendre curves, *J. Number Theory* 119 (2006) 128–147.
- [Li] J. Lipman, Rational singularities, with applications to algebraic surfaces and unique factorization, *Publ. Math. Inst. Hautes Études Sci.* 36 (1969) 195–279.
- [ST] J.-P. Serre, J. Tate, Good reduction of abelian varieties, *Ann. Math.* 88 (1969) 492–517.
- [SS] A. Singh, S. Spiroff, Divisor class groups of graded hypersurfaces, in: *Algebra, Geometry and Their Interactions*, in: *AMS Contemporary Mathematics*, vol. 448, 2007, pp. 237–243.
- [U12] D. Ulmer, Explicit points on the Legendre curve II, *Math. Res. Lett.* 21 (2014) 261–280.
- [U1] D. Ulmer, Curves and Jacobians over function fields, in: *Arithmetic Geometry over Global Function Fields*, in: *Advanced Courses in Mathematics – CRM Barcelona*, ISBN 978-3-0348-0852-1, Birkhäuser, 2015, pp. 283–335.