TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 357, Number 3, Pages 1047–1059
S 0002-9947(04)03520-2
Article electronically published on May 10, 2004

ON THE p^e-TORSION OF ELLIPTIC CURVES AND ELLIPTIC SURFACES IN CHARACTERISTIC p

ANDREAS SCHWEIZER

ABSTRACT. We study the extension generated by the x-coordinates of the p^e-torsion points of an elliptic curve over a function field of characteristic p. If $S \to C$ is a non-isotrivial elliptic surface in characteristic p with a p^e-torsion section, then for $p^e > 11$ our results imply restrictions on the genus, the gonality, and the p-rank of the base curve C, whereas for $p^e \leq 11$ such a surface can be constructed over any base curve C. We also describe explicitly all occurring p^e in the cases where the surface S is rational or $K3$ or the base curve C is rational, elliptic or hyperelliptic.

INTRODUCTION

Let F be a function field (of one variable) with constant field k.

In 1968 M. Levin [Le] showed that the torsion subgroup of any elliptic curve E over F with $j(E) \notin k$ can be uniformly bounded in terms of the genus of F and the characteristic of k. In 1996 [NgSa] refined Levin's method and gave an even more uniform bound in characteristic 0, namely in terms of the gonality of F. A similar argument can be used in characteristic p to bound the prime-to-p torsion in terms of p and the gonality of F.

For a different approach in terms of the genus see [HiSi, Theorem 7.2] in characteristic 0 and [GoSz, Theorem 13] in the case where k is finite. The latter, however, is not completely uniform since it involves the inseparability degree of $j(E)$. Both these references use the fact that if E has a place of additive reduction, then the prime-to-$char(k)$ torsion is bounded by 4, as follows from the description of the bad fibers (see [Si2] or [Ta]). Thus in characteristic p in many cases the p-primary torsion is the more interesting part.

Levin's proof for the p-primary torsion uses an auxiliary function field, generated over $k(\tilde{j})$ by the x-coordinate of a p^e-torsion point of an elliptic curve over $k(\tilde{j})$ with j-invariant $\tilde{j}$. This function field is intrinsic in the sense that it depends only on p and e but not on the elliptic curve. It had been studied before in [Ig], where the ramification is described and an explicit formula for its genus is given.

In Theorem 1.2 we show that the approach via this function field is actually optimal. In fact, we use a slight modification, which we call H_{p^e}. But the difference is merely a matter of convenience and not essential. We derive good upper and lower bounds for the gonality of H_{p^e} and also estimate its p-rank (i.e., the p-rank of its

Received by the editors August 5, 2002 and, in revised form, August 25, 2003.
2000 *Mathematics Subject Classification.* Primary 11G05, 14J27.
Key words and phrases. Elliptic curve, non-isotrivial elliptic surface, p-primary torsion, uniform bound, Hasse invariant, Igusa curve, gonality, $K3$ surface.

Jacobian). This furnishes our first main application: The existence of an elliptic curve E over F with an F-rational p^e-torsion point and $j(E) \notin k$ implies lower bounds (in terms of p and e) for the following invariants of F:

its genus $g(F)$,
its gonality $\gamma(F)$,
the quotient $g(F)/\gamma(F)$,
its p-rank $r(F)$,
the difference $g(F) - r(F)$.

Or, put the other way round, the p-primary torsion of all E over F with $j(E) \notin k$ can be uniformly bounded in terms of these invariants, for example by $24\gamma(F)$. In the cases where F is rational, elliptic, or hyperelliptic, we determine the optimal bounds. See also [CoPa], where for rational F of characteristic different from 2 and 3 all possible prime-to-the-characteristic torsion structures are described.

If k is algebraically closed, our results can be reformulated in the language of non-isotrivial elliptic surfaces $S \to C$ over k, giving relations between the p-primary part of the Mordell-Weil group and invariants of the base curve C. We also determine which p^e-torsion sections are possible on rational elliptic surfaces and on elliptic $K3$ surfaces.

1. Elliptic curves over function fields

If k is a field, we write k^* for its multiplicative group and $\overline{k}$ for its algebraic closure.

Let F be a function field (always of one variable) with constant field k of characteristic $p > 0$. Besides its genus $g(F)$ there are two further invariants of F that are of interest to us.

The (absolute) gonality of $\gamma(F)$ of F is the smallest possible index of a rational subfield $\overline{k}(U)$ in $\overline{k}F$. Equivalently, for a curve C over k the gonality $\gamma(C)$ is the smallest possible degree of a non-constant map (defined over $\overline{k}$) from C to some $\mathbb{P}^1$ over $\overline{k}$.

The p-rank of a smooth, projective curve C over a field k of characteristic p, or equivalently, the p-rank of its function field F, is defined as the dimension of the $\mathbb{F}_p$-vector space formed by the p-torsion points (over $\overline{k}$) of its Jacobian. This dimension can take any value between 0 and $g(C)$.

In this section we are interested in elliptic curves E over F with $j(E) \notin k$. The last condition guarantees, among other things, that E is ordinary. So the p^e-torsion points of E over $\overline{F}$ form a group isomorphic to $\mathbb{Z}/p^e\mathbb{Z}$.

We write $E^{(p^e)}$ for the image of E under the e-th iteration of the Frobenius isogeny. Since $E^{(p^e)}$ is obtained by raising the coefficients in a Weierstraß equation of E to the p^e-th power, we have $j(E^{(p^e)}) = (j(E))^{p^e}$. Conversely, if $j(E) \in (F^*)^{p^e}$, then $E \cong \widetilde{E}^{(p^e)}$ for some $\widetilde{E}$ over F.

By induction it suffices to prove this for $e = 1$. If $p \geq 5$, then $Y^2 = X^3 + a_4X + a_6$ is isomorphic over F to $Y^2 = X^3 + a_4^{p^2}X + a_4^{\frac{3(p^2-1)}{2}}a_6$ and from the formula for the j-invariant we see that if $j(E)$ is a p-th power, then $a_4^{\frac{3(p^2-1)}{2}}a_6$ is also.

Analogous arguments work in characteristic 3, where E has a normal form $Y^2 = X^3 + a_2X^2 + a_6$ (see [Si1, Appendix A]) and in characteristic 2, where $Y^2 + XY = X^3 + a_2X^2 + \frac{1}{j(E)}$ is isomorphic over F to $Y^2 + XY = X^3 + a_2^2X^2 + \frac{1}{j(E)}$ (see also [Si1, Appendix A]).

In particular, if E has an F-rational p^e-torsion point, then $j(E)$ must be a p^e-th power in F, since the p^e-torsion point generates an F-rational, cyclic p^e-isogeny whose dual isogeny is the e-th iteration of the Frobenius.

Another advantage of $j(E) \notin k$ is $Aut(E) \cong \{\pm 1\}$. Thus, if p is odd and E in the form $Y^2 = X^3 + a_2X^2 + a_4X + a_6$, then every other elliptic curve over F with the same j-invariant has an equation $Y^2 = X^3 + Da_2X^2 + D^2a_4X + D^3a_6$ with $D \in F^*$ (the so-called D-twist of E). On the points, the isomorphism (over $\overline{F}$) from E to this curve is given by $(x, y) \mapsto (Dx, D\sqrt{D}y)$.

If $p = 2$, every elliptic curve over F with the same j-invariant as $Y^2 + XY = X^3 + a_2X^2 + \frac{1}{j(E)}$ is of the form $Y^2 + XY = X^3 + (a_2 + \alpha)X^2 + \frac{1}{j(E)}$ with $\alpha \in F$, and the point (x, y) maps to $(x, y + \beta x)$ with $\beta^2 + \beta = \alpha$.

To come to the point: First, the extension obtained by adjoining to F the x-coordinate of one primitive p^e-torsion point of E contains the x-coordinates of all p^e-torsion points of E, because for every $n \in \mathbb{N}$ the multiplication-by-n map on E is given on the x-coordinates by a rational function over F. And secondly, the extension does not really depend on E, only on $j(E)$ and p^e.

We define

$$H_{p^e} := \mathbb{F}_p(\tilde{\jmath}, (x(P_e))^{p^e}),$$

where $\tilde{\jmath}$ is transcendental over $\mathbb{F}_p$ and P_e is a primitive p^e-torsion point of an elliptic curve E over $\mathbb{F}_p(\tilde{\jmath})$ with $j(E) = \tilde{\jmath}$.

The fields H_{p^e} will be the major tool throughout this paper. If k is algebraically closed, then $kH_{p^e}/k(\tilde{\jmath})$ is the separable part of the extension investigated in [Ig].

On several occasions we will need the number h_p of supersingular j-invariants in $\overline{\mathbb{F}_p}$, which is given by

$$h_p = \begin{cases} \frac{p-1}{12} & if\ p \equiv 1\ mod\ 12, \\ \lfloor \frac{p+13}{12} \rfloor & if\ p \not\equiv 1\ mod\ 12. \end{cases}$$

Now we are ready to start with some fundamental facts on H_{p^e}, which are almost entirely due to [Ig].

Lemma 1.1. *If $p^e \geq 3$, then $H_{p^e}/\mathbb{F}_p(\tilde{\jmath})$ is a geometric Galois extension of degree*

$$[H_{p^e} : \mathbb{F}_p(\tilde{\jmath})] = \frac{p^{e-1}(p-1)}{2}$$

with

$$Gal(H_{p^e}/\mathbb{F}_p(\tilde{\jmath})) \cong (\mathbb{Z}/p^e\mathbb{Z})^*/\{\pm 1\}.$$

The genus g_{p^e} of H_{p^e} is given by

$$2g_{p^e} - 2 = \frac{1}{24}(p-1)(p^{2e-1} - 12p^{e-1} + 1) - h_p - \frac{3}{8}\delta_{2,p} - \frac{1}{3}\delta_{3,p},$$

where $\delta_{i,p}$ is 1 if $i = p$, and 0 otherwise.

For every supersingular invariant $j_0 \in \overline{\mathbb{F}_p}$ the place $\tilde{\jmath} - j_0$ is totally ramified in $\overline{\mathbb{F}_p}H_{p^e}/\overline{\mathbb{F}_p}(\tilde{\jmath})$. If $p \equiv 1\ mod\ 4$, then $\tilde{\jmath} - 1728$ has ramification index 2; if $p \equiv 1\ mod\ 3$, then $\tilde{\jmath}$ has ramification index 3. All other places are unramified. The place $\frac{1}{\tilde{\jmath}}$ is totally decomposed in $H_{p^e}/\mathbb{F}_p(\tilde{\jmath})$.

Proof. We first prove the last statement.

Let E be an elliptic curve over $\mathbb{F}_p(\tilde{\jmath})$ with j-invariant $\tilde{\jmath}$ and split multiplicative reduction at $\frac{1}{\tilde{\jmath}}$. Then E is a Tate curve over the local field $K = \mathbb{F}_p((\frac{1}{\tilde{\jmath}}))$, i.e.,

there exists a Tate period $t \in K^*$ such that $E(\overline{K}) \cong \overline{K}^*/t^{\mathbb{Z}}$. The p^e-torsion point P_e corresponds to the coset $wt^{\mathbb{Z}}$, where w is a p^e-th root of t. Since the Tate uniformization respects the action of $Aut(\overline{K}/K)$, we see that P_e, like w, is fixed by all elements of $Aut(\overline{K}/K)$. Hence P_e is purely inseparable over K, which means that H_{p^e} is contained in K. (Thanks to Hershy Kisilevsky, from whom I learned this argument a few years ago.)

The fact that $\frac{1}{\tilde{j}}$ is totally decomposed implies that $H_{p^e}/\mathbb{F}_p(\tilde{j})$ is a geometric extension and $[kH_{p^e} : k(\tilde{j})] = [H_{p^e} : \mathbb{F}_p(\tilde{j})]$ for every constant field extension.

All other claims are proved in [Ig]. □

The following theorem is the key fact for almost all results in this paper.

Theorem 1.2. *Let F be a function field with constant field k of characteristic p. Then the necessary and sufficient condition for the existence of an elliptic curve E over F with $j(E) \notin k$ and F-rational p^e-torsion points is that F contains a function field that is k-isomorphic to kH_{p^e}.*

In particular, g_{p^e} is the minimal genus of such a function field. Moreover, if $g(F) = g_{p^e} \geq 2$, then F must be k-isomorphic to kH_{p^e}.

Proof. If we take $\tilde{j} = j(E)$, then E is isomorphic over $\overline{F}$ to an elliptic curve defined over $\mathbb{F}_p(\tilde{j})$. Hence the condition is clearly necessary. To prove that it is sufficient we assume that F contains $kH_{p^e}/k(\tilde{j})$ and consider an elliptic curve E over F with j-invariant $\tilde{j}^{p^e}$.

If p is odd we can assume E in the form $Y^2 = X^3 + a_2X^2 + a_4X + a_6$. Let (x_0, y_0) be a p^e-torsion point. Then x_0 and y_0^2 are in F. If $y_0 \notin F$, we simply replace E by the twisted curve $Y^2 = X^3 + y_0^2a_2X^2 + y_0^4a_4X + y_0^6a_6$ which has $(y_0^2x_0, y_0^4)$ as a p^e-torsion point.

In characteristic 2 we can bring E into normal form $Y^2 + XY = X^3 + a_2X^2 + \frac{1}{\tilde{j}^{2^e}}$ with $a_2 \in F$ (see [Si1, Appendix A]). Then $(0, \frac{1}{\tilde{j}^{2^{e-1}}})$ is the 2-torsion point. If $e > 1$ we concentrate on the curve with $a_2 = 0$, which has $(\tilde{j}^{-2^{e-2}}, \tilde{j}^{-2^{e-1}})$ as a 4-torsion point. The x-coordinate of every 2^e-torsion point P is contained in F. If the y-coordinate were not in F, some $\sigma \in Aut(\overline{F}/F)$ would map P to its inverse. But then σ would also map the underlying 4-torsion point to its inverse, a contradiction.

All other claims follow easily. □

The theorem shows that if one wants to bound the genus of F from below in terms of p^e, then the approach in [Le] is optimal. Actually, Levin uses it the other way around to give a uniform bound on the p-primary torsion of E in terms of p and $g(F)$. Before we derive a bound that is even more uniform we recall a result by Voloch that is very useful for the explicit construction of elliptic curves with a p-torsion point.

The Hasse invariant of an elliptic curve $E : Y^2 = X^3 + a_2X^2 + a_4X + a_6$ over a field K of odd characteristic p is the coefficient of X^{p-1} in the polynomial $(X^3 + a_2X^2 + a_4X + a_6)^{\frac{p-1}{2}}$. It is 0 if and only if E is supersingular. For ordinary curves the class of the Hasse invariant in $K^*/(K^*)^{p-1}$ is an isomorphy invariant. If the Hasse invariant of E lies in $(K^*)^{p-1}$, then by [Vo, pp. 248/249] the p-torsion points of the curve $Y^2 = X^3 + a_2^pX^2 + a_4^pX + a_6^p$ are K-rational.

Examples 1.3. a) The Hasse invariant of an ordinary elliptic curve $Y^2 = X^3 + a_4X + a_6$ over a field K of characteristic 11 is $9a_4a_6$. So if we take for example

$a_4 = 5$ and $a_6 = T^{10}$, then by [Vo, pp. 248/249] the 11-torsion points of the curve $Y^2 = X^3 + 5X + T^{110}$ will be $\mathbb{F}_{11}(T)$-rational.

b) In characteristic 17 the Hasse invariant of $Y^2 = X^3 + a_4X + a_6$ is $2a_4(a_4^3 - a_6^2)$. So if F is the function field $\mathbb{F}_{17}(T, Z)$ with $2T^4 - 2TZ^2 = 1$, then the elliptic curve $Y^2 = X^3 + TX + Z$ over F has Hasse invariant 1 by construction. Moreover, its j-invariant $\frac{8T^4}{T^4-4}$ is non-constant. By [Vo, pp. 248/249] the 17-torsion points of $Y^2 = X^3 + T^{17}X + Z^{17}$ are F-rational. To obtain a good normal form for F we change the coordinates to $U = 4T$, $V = 2TZ$.

From Theorem 1.2 we conclude that the genus 2 function field $\mathbb{F}_{17}(U, V)$ with $V^2 = U^5 - 9U$ is isomorphic over $\mathbb{F}_{17}$ to H_{17}.

Actually, the trick in the second example works in general.

Lemma 1.4. *If $p \geq 17$, then H_p is isomorphic to $\mathbb{F}_p(T, Z)$ with $H(T, Z) = 1$, where $H(T, Z)$ is the Hasse invariant of the elliptic curve $Y^2 = X^3 + TX + Z$.*

Proof. A little calculation shows that the terms of $H(T, Z)$ are of the form $c_{m,n}T^mZ^n$ with $m = \frac{p-1}{4} - \frac{3}{2}n$ and $0 \leq n \leq \frac{p-1}{6}$. So the total degree of the polynomial $H(T, Z) - 1$ is at most $\frac{p-1}{4}$.

If this polynomial were not irreducible in $\overline{\mathbb{F}_p}[T, Z]$, then there would be a non-constant, irreducible factor $f(T, Z)$ of total degree $d \leq \frac{p-1}{8}$. Let L be the function field $\overline{\mathbb{F}_p}(T, Z)$ with $f(T, Z) = 0$. By the well-known formula for the genus of plane curves we have $g(L) \leq \frac{(d-1)(d-2)}{2}$. On the other hand, by [Vo, pp. 248/249] the p-torsion points of $Y^2 = X^3 + T^pX + Z^p$ are L-rational, so L contains H_p and hence $g_p \leq g(L)$. Using the easy estimate $\frac{1}{48}(p^2 - 14p + 33) \leq g_p$ (misprint on page 460 of [Le]), we arrive at a contradiction.

Thus $H(T, Z) - 1$ is irreducible in $\overline{\mathbb{F}_p}[T, Z]$ and $\mathbb{F}_p(T, Z)$ is a function field which, by [Vo, pp. 248/249], contains H_p. If the index $[\mathbb{F}_p(T, Z) : H_p]$ were bigger than 1, we would have $2g_p - 1 \leq g(\mathbb{F}_p(T, Z)) \leq \frac{(p-5)(p-9)}{32}$. This is only possible for $p \leq 17$, but the case $p = 17$ was already treated in Example 1.3b). □

We also see that in general the curve $H(T, Z) = 1$ is not smooth, since in general g_p is not of the form $\frac{(d-1)(d-2)}{2}$.

Now we are ready to say more about the gonality of H_{p^e}.

Lemma 1.5. a) *H_{p^e} is rational if and only if $p^e \leq 11$.*

b) *H_{p^e} is elliptic if and only if $p^e = 13$ or 16.*

c) *H_{p^e} is hyperelliptic if and only if $p = 17$.*

d) *For $p \geq 7$ the gonality of H_p is bounded by $\frac{p+13}{24} \leq \gamma(H_p) \leq \frac{p-1}{6}$.*

e) *If $e > 1$, then $\gamma(H_{p^e}) = p\gamma(H_{p^{e-1}})$ except for $p^e \in \{25, 9, 8, 4\}$.*

Proof. Statements a) and b) are due to [Le].

This also implies d) for $p < 17$. If $p \geq 17$, then by the first two lines of the proof of Lemma 1.4, H_p is an extension of degree at most $\frac{p-1}{6}$ of $\mathbb{F}_p(T)$; this furnishes the upper bound for $\gamma(H_p)$.

In the sequel of the proof we will repeatedly exploit the following principle: Let F, F_1 and F_2 be function fields (of one variable) over an algebraically closed constant field k with $F_i \subseteq F$. If M is the compositum of F_1 and F_2 in F and $d_i = [M : F_i]$, then

$$g(M) \leq d_1g(F_1) + d_2g(F_2) + (d_1 - 1)(d_2 - 1).$$

In fact, let C, C_1 and C_2 be the curves corresponding to M, F_1 and F_2. Then the maps $\pi_i : C \to C_i$ factor over the induced map $\pi_1 \times \pi_2 : C \to C_1 \times C_2$. The function field of the image D of this map must be M, so $\pi_1 \times \pi_2$ is birational onto D, and we can apply the inequality of Castelnuovo-Severi ([NgSa, Lemma 1.4]).

To establish the lower bound in statement d), let R be a rational subfield of $\overline{\mathbb{F}_p}H_p$ with $[\overline{\mathbb{F}_p}H_p : R] = \gamma = \gamma(H_p)$. Let M be the compositum of R and $\overline{\mathbb{F}_p}(\tilde{\jmath})$, and put $d_1 = [M : R]$ and $d_2 = [M : \overline{\mathbb{F}_p}(\tilde{\jmath})]$. Then, as discussed above,

$$g(M) \le (d_1 - 1)(d_2 - 1).$$

On the other hand, by Lemma 1.1 and the Hurwitz formula,

$$g(M) \ge 1 - d_2 + \frac{1}{2}h_p(d_2 - 1) = (\frac{h_p}{2} - 1)(d_2 - 1).$$

Since $\gamma \le \frac{p-1}{6}$, we can divide by $(d_2 - 1) \ge 2$ and obtain $d_1 \ge \frac{h_p}{2}$. If $d_1 < \gamma$, then $\gamma \ge 2d_1 \ge h_p \ge \frac{p-1}{12}$, which for $p \ge 17$ is bigger than $\frac{p+13}{24}$. If $d_1 = \gamma$, then $M = \overline{\mathbb{F}_p}H_p$ and we have

$$\frac{1}{48}(p-3)(p-11) \le g(H_p) \le (\gamma - 1)(\frac{p-1}{2} - 1),$$

which also yields $\gamma \ge \frac{p+13}{24}$.

To prove e) let R be a rational subfield of $\overline{\mathbb{F}_p}H_{p^e}$ of index $\gamma = \gamma(H_{p^e})$. If R is contained in $\overline{\mathbb{F}_p}H_{p^{e-1}}$ we are done. So let us suppose this is not the case. Then the same argument as above yields

$$g_{p^e} \le p \cdot g_{p^{e-1}} + (p-1)(\gamma - 1).$$

With the formula for the genus from Lemma 1.1 and some estimates we obtain

$$\frac{(p-1)(p^{2e-2} - 1)}{48} \le \gamma.$$

If $p \ge 7$ we compare this with

$$\gamma \le p^{e-1}\frac{p-1}{6},$$

obtained from d). Similarly, if $p = 2$, 3, or 5, we use $\gamma \le 2^{e-3}$, resp. $\gamma \le 3^{e-2}$ or $\gamma \le 5^{e-1}$. Thus we see that the only values $p^e > 16$ for which R is not necessarily contained in $\overline{\mathbb{F}_p}H_{p^{e-1}}$ are 49 and 25. Nevertheless, the attempt still shows $\gamma(H_{49}) = 7$. From the description of the ramification in $H_{25}/\mathbb{F}_5(\tilde{\jmath})$ we see that the intermediate field with index 2 in H_{25} has genus 2. This shows $\gamma(H_{25}) \le 4$ and at the same time (since $g_{25} = 6$) that H_{25} cannot be hyperelliptic.

This brings us to statement c). Of course, the genus 2 function field H_{17} is hyperelliptic. By d) and e) the only other possibilities are $p^e = 19$, 23, 29, and 31.

From Lemma 1.1 we gather that the inertia field of the place $\tilde{\jmath}$ in the extension $H_{31}/\mathbb{F}_{31}(\tilde{\jmath})$ has genus 2 and index 3 in H_{31}. If H_{31} were hyperelliptic, we would get $g_{31} \le 3 \cdot 2 + 2 \cdot 1 = 8$, but $g_{31} = 12$. Completely analogous arguments show that H_{19} and H_{29} are not hyperelliptic.

By Lemma 1.4 we have $H_{23} \cong \mathbb{F}_{23}(T, Z)$ with $10T^4Z + 9TZ^3 - 1 = 0$. This polynomial is irreducible in $\overline{\mathbb{F}_{23}}(T)[Z]$ (Newton polygon for T), so $[H_{23} : \mathbb{F}_{23}(T)] = 3$. Therefore H_{23} cannot be hyperelliptic because of $g_{23} = 6$. □

As an immediate consequence we obtain the following result (and its obvious improvements for $\gamma(F) \le 2$).

Theorem 1.6. *Let F be a function field with constant field k of characteristic p. Then the p-primary torsion of every elliptic curve E over F with $j(E) \notin k$ is uniformly bounded by $24\gamma(F)$.*

Proof. If E has an F-rational p^e-torsion point, then F contains kH_{p^e}. For $p \geq 7$ this implies $\gamma(F) \geq \gamma(H_{p^e}) \geq p^{e-1}\frac{p+13}{24}$. Similarly for $p \in \{2,3,5\}$. □

If there is an E/F with F-rational p^e-torsion, then the upper bound on $\gamma(H_p)$ yields another restriction on F. Since every finite, purely inseparable extension of a function field L (in one variable!) over a perfect constant field is isomorphic to L itself by some power of the Frobenius map, we can suppose that $\overline{k}F$ is a separable extension of $\overline{k}H_{p^e}$, of degree d say. Then by the Hurwitz formula $g(F) - 1 \geq d(g_{p^e} - 1)$, whereas for the gonality we trivially have $\gamma(F) \leq dp^{e-1}\gamma(H_p)$. Using the formula for g_{p^e} and Lemma 1.5d) we can bound $\frac{g(F)}{\gamma(F)}$ from below by something which is roughly of order $\frac{p^e}{8}$. Note that for most function fields the gonality is about half of the genus.

We discuss yet another invariant of H_{p^e}.

Lemma 1.7. *The p-rank r_{p^e} of H_{p^e} satisfies*

$$r_{p^e} = p^{e-1}(r_p + h_p - 1) + 1 - h_p,$$

where h_p is the number of supersingular j-invariants in $\overline{\mathbb{F}_p}$.

If $p \in \{2,3,5,7\}$, then $r_{p^e} = 0$. If $p \geq 11$ and $e \geq 2$, then $0 < r_{p^e} < g_{p^e}$.

Proof. Since $H_{p^{e+1}}$ is a Galois extension of degree p of H_{p^e}, ramified exactly at the supersingular values of $\tilde{j}$, we have

$$r_{p^{e+1}} - 1 = p(r_{p^e} - 1) + h_p(p-1)$$

by the well-known formula for the p-rank in such extensions. We refer to [Ro] for an elementary proof in the situation where the constant field is finite, which clearly suffices for our purposes. From this inductive formula the closed formula for r_{p^e} follows immediately.

Then the vanishing of r_{p^e} for $p \in \{2,3,5,7\}$ is clear. For $p \geq 11$ the positivity of r_{p^e} for $e \geq 2$ follows from $h_p \geq 2$ (for $p \neq 13$) resp. from $r_{13} = 1$. (Compare the proof of Proposition 2.7a) for the last claim.) Finally, the inequality $r_{p^e} < g_{p^e}$ is obtained by using $r_p \leq g_p$ and comparing with the formula for g_{p^e}. □

We suspect that the function fields H_p are ordinary, i.e., that $r_p = g_p$. In any case, putting $r_p = g_p$ in the formula provides a good upper bound for r_{p^e}, and it is clear that for fixed p the genus of H_{p^e} (roughly $\frac{p^{2e}}{48}$) grows much faster than its p-rank (more like $\frac{p^{e+1}}{48}$). This is interesting because of the following criterion.

We write $r(F)$ for the p-rank of a function field F with constant field k of characteristic p. The functoriality of the Jacobian implies that if there exists an elliptic curve E over F with $j(E) \notin k$ and F-rational p^e-torsion points, then necessarily

$$r(F) \geq r_{p^e}$$

and

$$g(F) - r(F) \geq g_{p^e} - r_{p^e}.$$

Coming back to the Hasse invariant, the following lemma will allow us to prove the converse to the statement in [Vo, pp. 248/249].

Lemma 1.8. *If $char(k) = p \geq 3$, then $kH_p = k(\tilde{\jmath}, W)$, where $W^{\frac{p-1}{2}}$ is the Hasse invariant of any elliptic curve over $k(\tilde{\jmath})$ with j-invariant $\tilde{\jmath}$.*

Proof. If $E:\ Y^2 = X^3 + a_2X^2 + a_4X + a_6$ is such a curve and $W^{\frac{p-1}{2}}$ its Hasse invariant, we consider its W-twist $\widetilde{E}:\ Y^2 = X^3 + Wa_2X^2 + W^2a_4X + W^3a_6$ over $k(\tilde{\jmath}, W)$. The Hasse invariant of $\widetilde{E}$ is W^{p-1}, so by [Vo, pp. 248/249] the p-torsion points of the curve $Y^2 = X^3 + W^pa_2^pX^2 + W^{2p}a_4^pX + W^{3p}a_6^p$ are $k(\tilde{\jmath}, W)$-rational. In particular, $k(\tilde{\jmath}, W)$ contains kH_p.

On the other hand $\frac{p-1}{2} = [kH_p : k(\tilde{\jmath})] \leq [k(\tilde{\jmath}, W) : k(\tilde{\jmath})] \leq \frac{p-1}{2}$. □

Proposition 1.9. *If F is a function field with constant field k of characteristic $p \geq 3$ and E is an elliptic curve over F with $j(E) \notin k$, then the p-torsion points of E are F-rational if and only if $j(E)$ lies in $(F^*)^p$ and the Hasse invariant of E lies in $(F^*)^{p(p-1)}$.*

Proof. At the beginning of this section we showed that if $j(E) \in (F^*)^p$, then E is the image under Frobenius of an elliptic curve $\widetilde{E}$ over F. Clearly, if the Hasse invariant of E lies in $(F^*)^{p(p-1)}$, then the Hasse invariant of $\widetilde{E}$ lies in $(F^*)^{p-1}$, and hence the p-torsion points of E are F-rational by [Vo, pp. 248/249].

Conversely, suppose the p-torsion points of E are F-rational. Then, as discussed at the beginning of this section, $j(E)$ is a p-th power in F^* and $E \cong \widetilde{E}^{(p)}$ for some $\widetilde{E}$ over F.

Obviously, F must contain kH_p. Since there exists a twist of $\widetilde{E}$ that is defined over $k(j(\widetilde{E}))$ and since twisting with $D \in F^*$ changes the Hasse invariant by $D^{\frac{p-1}{2}}$, we see from Lemma 1.8 that the Hasse invariant of $\widetilde{E}$ must be a $\frac{p-1}{2}$-th power in F. Thus the Hasse invariant of E is $w^{\frac{p(p-1)}{2}}$ for some $w \in F^*$.

Now we consider the elliptic curve E_{w^p} obtained from E by twisting with w^p. Its Hasse invariant is $w^{p(p-1)}$. Hence, by the first part of the proof, its p-torsion points are F-rational. But these p-torsion points are of the form $(w^px_0, w^{\frac{3p}{2}}y_0)$, where (x_0, y_0) are the p-torsion points of E, which are F-rational by assumption. As $y_0 \neq 0$ (because $p > 2$), we see that $\sqrt{w} \in F$. So the Hasse invariant of E is in $(F^*)^{p(p-1)}$ (and E_{w^p} is isomorphic to E already over F). □

If $j(E) \in k$ and k is algebraically closed, then an argument similar to the one on the last few lines shows that the p-primary torsion of E over F is bounded by 2 unless E is isomorphic over F to an elliptic curve defined over k.

2. Elliptic surfaces with a p-torsion section

For the rest of the paper k is an algebraically closed field of characteristic $p > 0$. We consider elliptic surfaces $S \to C$, i.e., C is a smooth, projective curve over k and S is a smooth, projective surface with a relatively minimal elliptic fibration $S \to C$ which has a section $C \to S$. We always suppose the elliptic surface to be non-isotrivial, i.e., even after base change the elliptic fibration does not split.

If F is the function field of C over k, then the generic fiber of $S \to C$ is an elliptic curve E over F, and the non-isotriviality condition is equivalent to $j(E) \notin k$.

The group of sections $C \to S$ is isomorphic to the group of F-rational points of E, called Mordell-Weil group in both settings. We write $MW_p(S/C)$ for the p-primary part of the Mordell-Weil group. Then $|MW_p(S/C)| = p^e$ for some $e \geq 0$.

The results of Section 1 can be reformulated in terms of elliptic surfaces. For example, given C, the necessary and sufficient condition for the existence of a non-isotrivial $S \to C$ with a p^e-torsion section is that C is a cover of a curve whose function field is isomorphic to kH_{p^e}. Moreover, $|MW_p(S/C)|$ is uniformly bounded in terms of invariants of C; for example,

$$|MW_p(S/C)| \leq 24\gamma(C),$$

where γ denotes the gonality.

Now we are mainly interested in which values $|MW_p(S/C)|$ can take if we impose conditions on the surface S.

If an elliptic surface $S \to C$ is a rational surface or a $K3$ surface, then the base curve C must necessarily be rational because $b_1(S) = 0$. More precisely, an elliptic surface $S \to \mathbb{P}^1$ is a rational surface if and only if $c_2(S) = 12$, and S is a $K3$ surface if and only if $c_2(S) = 24$.

The second Chern number $c_2(S)$ can be calculated by

$$c_2(S) = deg(conductor(S)) + \sum_{\nu \in \mathbb{P}^1} (n_\nu - 1),$$

where n_ν is the number of irreducible components of the special fiber at ν. See [Si2, Chapter IV] or [Ta] for the description of the special fibers.

Lemma 2.1. *Let $S \to \mathbb{P}^1$ be a non-isotrivial elliptic surface in characteristic 3 and suppose that it has a 9-torsion section. Then $c_2(S) \geq 27$. In particular, S is neither rational nor a $K3$ surface.*

Proof. By Lemma 1.1 the place $\frac{1}{j}$ decomposes into 3 different places in H_9. This implies that the j-invariant of S has at least 3 different poles. Moreover, $j(S)$ must be a 9-th power, so the order of each pole is divisible by 9. Hence, from the contribution of the fibers of type I_n and I_n^* we get $c_2(S) \geq 27$. □

For rational S the same reasoning also excludes the possibilities $p^e = 7$, 8 or 11. Thus for non-isotrivial rational elliptic surfaces in characteristic p we have $|MW_p(S/C)| \leq 5$. This can also be seen (even without the assumption of non-isotriviality) from [OgSh, Corollary 2.1]. See also [Ke, p. 57], which provides more information on the bad fibers.

Examples 2.2. The following examples, which all essentially go back to [La1] and [La2], show that the remaining possible values for $|MW_p(S/C)|$ actually occur. The base curve is always the projective line with coordinate T.

a) If an elliptic surface $S \to \mathbb{P}^1$ in characteristic 5 has a 5-torsion section, then, as in the proof of Lemma 2.1, its j-invariant must have at least two different poles, each with an order divisible by 5. Thus, if $c_2(S) = 12$, then the singular fibers of S can only be of type II, I_5, I_5. By [La2] there is, up to isomorphism, exactly one surface of this type. From [Ito1] we take the simple equation $Y^2 = X^3 + X + T^5$ and that over $\overline{\mathbb{F}_5}(T)$ the Mordell-Weil group is indeed $\mathbb{Z}/5\mathbb{Z}$.

b) Using the duplication formula ([Si1, p. 59]) it is not difficult to check that $(0, 0)$ is a 4-torsion point of the characteristic 2 curve $Y^2 + TXY + TY = X^3 + X^2$. This is the surface III from [La2] with singular fibers of type III, I_8.

This also indicates an error in the table of the Main Theorem in [OgSh]; in Case 70 the Mordell-Weil group should be $\mathbb{Z}/4\mathbb{Z}$.

c) By [Ito2] the characteristic 3 surface VII from [La2], given by the equation $Y^2 = X^3+T^2X^2+TX$, has Mordell-Weil group $\mathbb{Z}/6\mathbb{Z}$ and hence a 3-torsion section.

This surface has singular fibers of type III, I_3, I_6. Its existence contradicts the statement on the last page of [Ke] that Case 66 in the table of the Main Theorem in [OgSh] cannot occur in characteristic 2 or 3. Apparently, the error in the argumentation in [Ke] is due to the somewhat misleading notation in [OgSh] (see pages 83 and 87) that makes singular fibers of type I_2 or I_3 appear as if they were of type III or IV. Also note that in the table singular fibers of type I_1 or II remain hidden.

d) There are presumably many rational elliptic surfaces in characteristic 2 with a 2-torsion section. We just mention the surface VIII from [La2] with equation $Y^2 + TXY + TY = X^3$ and singular fibers of type IV, I_2, I_6, because it shows that Case 66 of [OgSh] also exists in characteristic 2. (Compare the comment in the last example.)

e) In every characteristic p there are many non-isotrivial rational elliptic surfaces without a p-torsion section. Any Beauville surface (see [La1]) will do, because it has fibers I_n with $p \not| n$. For example in odd characteristic we might take the Beauville surface with singular fibers I_8, I_2, I_1, I_1, which again shows that in Case 70 in [OgSh] the Mordell-Weil group should be $\mathbb{Z}/4\mathbb{Z}$.

We summarize:

Theorem 2.3. *The order of the p-primary part of the Mordell-Weil group of a non-isotrivial rational elliptic surface $S \to C$ in characteristic p is bounded by $|MW_p(S/C)| \leq 5$, and each of the orders $1, 2, 3, 4, 5$ can be realized by an extremal rational elliptic surface.*

Next we consider non-isotrivial elliptic $K3$ surfaces. The fact that in this case p-torsion sections cannot exist for $p > 11$ was also obtained in [DoKe, Corollary 5.9] as a by-product of more general results on $K3$ surfaces. Actually, $p = 11$ cannot occur because then by the same argument as in Lemma 2.1 we would have $c_2(S) \geq 55$. Thus we are left with $|MW_p(S/C)| \leq 8$.

Examples 2.4. a) In order to obtain a non-isotrivial elliptic $K3$ surface with $|MW_p| = 1$ one can proceed as follows.

We take a Beauville surface (see [La1]) and choose the parameter t of the base curve $\mathbb{P}^1$ in such a way that there are no bad fibers at the places $t = 0$ and $\frac{1}{t}$.

If p is odd, we base change the Beauville surface to an elliptic surface S over a projective line C with parameter T where $T^2 = t$. Equivalently, in the equation of the generic fiber over $k(t)$ we replace t by T^2 and obtain an elliptic curve over $k(T)$. Since the cover $C \to \mathbb{P}^1$ is unramified outside t and $\frac{1}{t}$, each bad fiber of the Beauville surface will give two bad fibers of the same type on S. Hence S must be a $K3$ surface, and since the fibers are still of type I_n with $p \not| n$, it cannot have a p-torsion section.

Similarly, in characteristic 2 we apply the base change $T^2 + T = t$ which is unramified outside $\frac{1}{t}$.

b) We want to construct a non-isotrivial elliptic $K3$ surface in characteristic 2 with an 8-torsion section. By [Si1, Appendix A] there is a model $Y^2 + XY = X^3 + a_2X^2 + a_6$ with $j = \frac{1}{a_6}$. If (x_0, y_0) is a 4-torsion point, then the duplication formula [Si1, p. 59] shows $a_6 = x_0^4$. Hence $a_2 = (\frac{y_0}{x_0} + x_0)^2 + (\frac{y_0}{x_0} + x_0)$ and we can transform to $Y^2 + XY = X^3 + a_6$.

If there is an 8-torsion point, then $a_6 = \lambda^8$ and as in the proof of Lemma 2.1 we see that λ has exactly two zeroes, each of order 1. Again by the duplication formula $\zeta^4 + \lambda^2\zeta^2 = \lambda^8$, where ζ is the x-coordinate of the 8-torsion point. Substituting $V = \frac{\zeta^2}{\lambda^2} + \lambda^2 + \lambda$, we obtain $V(V+1) = \lambda$, which shows that λ cannot have a simple pole. We choose the parameter T of the base curve C so that the double pole of λ is at ∞ and the zeroes are at $T = 0$ and $T = 1$. Thus $\lambda = cT(T+1)$ with $c \in k^*$. The substitution $V = W + dT$ with $d^2 = c$ yields $W(W+1) = (d^2+d)T$, which is only possible for $d = 1$ (since T has a simple pole).

It is straightforward to check that the elliptic surface

$$Y^2 + XY = X^3 + T^8(T+1)^8$$

has conductor $\infty^3 \cdot T(T+1)$ and singular fibers I_1^*, I_8, I_8, is indeed a $K3$ surface, and that $(T^4 + T^3, T^8 + T^5)$ is an 8-torsion point.

By the argument above this surface is unique up to isomorphism.

c) By Proposition 1.9 an elliptic curve in characteristic 7 with a 7-torsion point comes via Frobenius from an elliptic curve $\widetilde{E}: Y^2 = X^3 + AX + B$ such that $3B$ (the Hasse invariant of $\widetilde{E}$) is a 6-th power. Thus $B = 5\beta^6$ and $\widetilde{E}$ is isomorphic to $Y^2 = X^3 + UX + 5$, where U is a non-constant function in $k(T)$.

As in the proof of Lemma 2.1, the j-invariant of a non-isotrivial elliptic $K3$ surface in characteristic 7 with a 7-torsion section has exactly 3 poles, each of order 7. Together with $j(\widetilde{E}) = \frac{-U^3}{U^3-1}$ this implies that U is a function of degree 1 in $k(T)$, i.e. $k(U) = k(T)$. We conclude that

$$Y^2 = X^3 + T^7X + 5,$$

which has conductor $\infty^2 \cdot (T^3 - 1)$ and singular fibers III, I_7, I_7, I_7, is (up to isomorphism) the only such surface.

d) By an analogous argument one sees that every non-isotrivial elliptic $K3$ surface in characteristic 5 with a 5-torsion section is a quadratic base change of the rational elliptic surface $R: Y^2 = X^3 + 3X + U^5$.

We leave it to the reader to work out all equations and their bad fibers (which depend on how the two ramified places in $k(T)/k(U)$ relate to the bad fibers of R).

e) By a quadratic base change of the charcteristic 3 surface in Example 2.2c) we can, for instance, obtain the $K3$ surface $Y^2 = X^3 + T^4X^2 + T^2X$ with conductor $\infty \cdot T^2(T^2-1)$ and singular fibers I_{12}, I_0^*, I_3, I_3.

Examples of elliptic $K3$ surfaces in characteristic 2 with $|MW_2(S/C)| = 2$ or 4 are already in Table 1 of [Ito2].

Thus we have proved

Theorem 2.5. *The p-primary part of the Mordell-Weil group of a non-isotrivial elliptic $K3$ surface in characteristic p can only have order $1, 2, 3, 4, 5, 7$ or 8, and all these orders actually occur (for suitable p).*

For general non-isotrivial elliptic surfaces S over a rational base curve we have $|MW_p(S/\mathbb{P}^1)| \leq 11$, and the values 9 and 11 actually also occur (Theorem 1.2 in connection with Lemma 1.5). We prove even more.

Theorem 2.6. *Fix a curve C over an algebraically closed field k of characteristic p. If e is a non-negative integer such that $p^e \leq 11$, then one can construct a non-isotrivial elliptic surface $S \to C$ with $|MW_p(S/C)| = p^e$.*

Proof. There exists a covering $C \to \mathbb{P}^1$ of finite degree. We can simply take a non-isotrivial elliptic surface over this $\mathbb{P}^1$ with a p^e-torsion section and then base-change it to C. If the elliptic surface $S_0 \to C$ we obtain has even a p^{e+1}-torsion section, we apply the separable p-isogeny, i.e., divide by the p-torsion section. The resulting surface $S_1 \to C$ will still have a p^e-torsion section. And since $j(S_1)$ is a p-th root of $j(S_0)$ we can continue until we reach an $S_n \to C$ which does not have a p^{e+1}-torsion section. □

In contrast, for $p^e > 11$ there are conditions on the base curve C. For elliptic C we have $|MW_p(S/C)| \leq 16$ and the conditions are the following.

Proposition 2.7. a) *If k is an algebraically closed field of characteristic* 13 *and C is an elliptic curve over k, then the necessary and sufficient condition for the existence of a non-isotrivial elliptic surface $S \to C$ with a* 13*-torsion section is that C has complex multiplication by an order in the cyclotomic field $\mathbb{Q}(\sqrt{-3})$.*

b) *If C is an elliptic curve over an algebraically closed field of characteristic* 2*, then there exists a non-isotrivial elliptic surface $S \to C$ with a* 16*-torsion section if and only if C is supersingular.*

Proof. a) In the extension $H_{13}/\mathbb{F}_{13}(\tilde{\jmath})$ the supersingular place $\tilde{\jmath} - 5$ is totally ramified. Hence $Gal(H_{13}/\mathbb{F}_{13}(\tilde{\jmath}))$ fixes the place $\wp$ of H_{13} lying above $\tilde{\jmath} - 5$. Therefore the curve $\widetilde{C}$ of H_{13} over k with $\wp$ chosen as its origin is an elliptic curve with an automorphism group of order 6. Consequently $\widetilde{C}$ is ordinary and has complex multiplication by $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

Now the assertion follows from Theorem 1.2 and the fact that the elliptic curves C over k that are isogenous to $\widetilde{C}$ are exactly those with complex multiplication by an order in $\mathbb{Q}(\sqrt{-3})$.

The proof of b) is practically the same. □

For hyperelliptic C we have $|MW_p(S/C)| \leq 17$. In characteristic 17 the condition for the existence of a surface S over C with a 17-torsion section is that C is a covering of the curve $V^2 = U^5 - 9U$. In characteristic 13 or 2 a surface with a 13-torsion section, resp. a 16-torsion section, can be realized if and only if the Jacobian of C contains a factor isogenous to an elliptic curve with j-invariant 0.

We conclude with the following general result, which follows from Theorem 1.2 and Lemma 1.7.

Proposition 2.8. *If C is an ordinary curve in characteristic p (i.e., the p-rank of its Jacobian is $g(C)$), then for every non-isotrivial elliptic surface $S \to C$ we have $|MW_p(S/C)| \leq \max\{p, 9\}$.*

Note in this context that most curves are ordinary.

References

[CoPa] D. Cox and W. Parry, *Torsion in elliptic curves over $k(t)$*, Compositio Math. **41** (1980), 337-354. MR81k:14035

[DoKe] I. Dolgachev and J. Keum, *Wild p-cyclic actions on $K3$-surfaces*, J. Algebraic Geom. **10** (2001), 101-131. MR2001i:14049

[GoSz] D. Goldfeld and L. Szpiro, *Bounds for the order of the Tate-Shafarevich group*, Compositio Math. **97** (1995), 71-87. MR97a:11102

[HiSi] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419-450. MR89k:11044

[Ig] J. Igusa, *On the algebraic theory of elliptic modular functions*, J. Math. Soc. Japan **20** (1968), 96-106. MR39:1457

[Ito1] H. Ito, *On unirationality of extremal elliptic surfaces*, Math. Annalen **310** (1998), 717-733. MR99f:14045

[Ito2] H. Ito, *On extremal elliptic surfaces in characteristic* 2 *and* 3, Hiroshima Math. J. **32** (2002), 179-188. MR2003g:14050

[Ke] J. Keum, *Wild p-cyclic actions on smooth surfaces with* $p_g = q = 0$, J. Algebra **244** (2001), 45-58. MR2002g:14060

[La1] W. Lang, *Extremal rational elliptic surfaces in characteristic p. I: Beauville surfaces*, Math. Z. **207** (1991), 429-438. MR92f:14032

[La2] W. Lang, *Extremal rational elliptic surfaces in characteristic p. II: Surfaces with three or fewer singular fibres*, Ark. Mat. **32** (1994), 423-448. MR96d:14034

[Le] M. Levin, *On the group of rational points of elliptic curves over function fields*, Amer. J. Math. **90** (1968), 456-462. MR37:6283

[NgSa] K. V. Nguyen and M.-H. Saito, *d-gonality of modular curves and bounding torsions*, preprint arXiv:alg-geom/9603024, 29Mar96.

[OgSh] K. Oguiso and T. Shioda, *The Mordell-Weil lattice of a rational elliptic surface*, Comment. Math. Univ. St. Paul. **40** (1991), 83-99. MR92g:14036

[Ro] M. Rosen, *Some remarks on the p-rank of an algebraic curve*, Arch. Math. (Basel) **41** (1983), 143-146. MR85b:14030

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM 106, Berlin-Heidelberg-New York, 1986. MR87g:11070

[Si2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer GTM 151, Berlin-Heidelberg-New York, 1994. MR96b:11074

[Ta] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable IV, Springer LNM 476, Berlin-Heidelberg-New York, 1975, pp. 33-52. MR52:13850

[Vo] J.F. Voloch, *Explicit p-descent for elliptic curves in characteristic p*, Compositio Math. **74** (1990), 247-258. MR91f:11042

Korea Institute for Advanced Study (KIAS), 207-43 Cheongnyangni 2-dong, Dongdaemun-gu, Seoul 130-722, Korea

E-mail address: schweiz@kias.re.kr