ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 44, Number 5, 2014

A SUPPLEMENT TO MANIN'S PROOF OF THE HASSE INEQUALITY

JASBIR S. CHAHAL, AFZAL SOOMRO AND JAAP TOP

ABSTRACT. In 1956 Yu.I. Manin published an elementary proof of Helmut Hasse's 1933 result stating that the Riemann hypothesis holds in the case of an elliptic function field over a finite field. We briefly explain how Manin's proof relates to more modern proofs of the same result. This enables us to present an analogous elementary proof for the case of finite fields of characteristic two, which was excluded in the original argument.

1. Introduction and motivation. Let $\mathbb{F}_q$ denote a finite field of cardinality q, and let $E/\mathbb{F}_q$ be an elliptic curve. A well-known result is that

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

This is a special case of a more general conjecture which Artin formulated in his thesis, and in fact this thesis already verifies the inequality for some special cases, including all elliptic curves over $\mathbb{F}_3, \mathbb{F}_5$, and $\mathbb{F}_7$. Establishing the inequality for elliptic curves in general became a project of Hasse. His 1933 note **[6]** proves it for the fields $\mathbb{F}_p$ with $p \geq 5$ a prime number. Soon thereafter, in 1934, Hasse **[7]** succeeds for all finite fields, and in 1936 he publishes a simplification **[8]** of his argument. All of this was superseded by the work of Weil in the late forties.

Hasse's result is important for certain primality proofs and integer factorization algorithms, and also in coding theory and in cryptography. In 1956, Manin **[13]** presented a completely elementary proof of Hasse's inequality. However, in his presentation, he restricts himself to the case that the characteristic of the finite field is different from two. Several texts have discussed Manin's proof, including the well-known elementary analytic number theory book by Gel'fond and Linnik **[4]** and also **[1, 2, 3, 9, 12]**. All of these use the same restriction that the characteristic should be > 2. Since the characteristic two case is

Received by the editors on June 25, 2012.
DOI:10.1216/RMJ-2014-44-5-1457

needed in several applications of Hasse's result, it seems appropriate to have an elementary proof for this case as well. This is precisely the aim of this note.

We start by recalling a well-known fact; this is a special case of an assertion given in a famous paper of Safarevic and Tate [**17**]. This only serves to clarify some ideas behind Manin's proof. The constructions in characteristic two presented in the last two sections of this note were found using exactly the same ideas. However, if one is only interested in the elementary proof as such, one does not need it.

Let E/k be an elliptic curve, and let -1 denote the minus one map on E. Using a projection $E \times E \to E$ one obtains a family of curves

$$\frac{E \times E}{(-1) \times (-1)} \longrightarrow E/(-1) \cong \mathbb{P}^1.$$

The generic fiber of this family is an elliptic curve E^{tw} over the function field $k(\mathbb{P}^1) = k(t)$. Over the quadratic extension $k(E)$ of $k(t)$, the elliptic curves E and E^{tw} are isomorphic. In particular, this implies that the associated groups of $k(E)$-rational points are isomorphic:

$$E^{\mathrm{tw}}(k(E)) \cong E(k(E)).$$

Evidently, the group $E(k(E))$ may be regarded as the group $\mathrm{Mor}_k(E, E)$ of all rational maps from E to E defined over k. Hence, via the above isomorphism, the subgroup $E^{\mathrm{tw}}(k(t)) \subset E^{\mathrm{tw}}(k(E))$ is identified with a subgroup of $\mathrm{Mor}_k(E, E)$. It is easy to see, and explicitly mentioned as, formula (13) in [**17**], which is this subgroup:

$$\begin{array}{ccc} E^{\mathrm{tw}}(k(t)) & \subset & E^{\mathrm{tw}}(k(E)) \\ \big\downarrow \wr & & \big\downarrow \wr \\ \{\varphi \in \mathrm{Mor}_k(E,E) \ : \ \varphi \circ (-1) = (-1) \circ \varphi\} & \subset & \mathrm{Mor}_k(E,E). \\ \cup & & \\ \mathrm{End}_k(E) & & \end{array}$$

Note that in the diagram we already indicate a source for points in $E^{\mathrm{tw}}(k(t))$: the ring of k-rational endomorphisms of E.

The identity endomorphism $1 = id$ is a nonzero element of $\mathrm{End}_k(E)$. Hence, it corresponds to a point in $E^{\mathrm{tw}}(k(t))$, which we denote as Q. Note that, since $\mathrm{End}_k(E)$ is torsion free, $Q \in E^{\mathrm{tw}}(k(t))$ is a point of

infinite order. This rather simple observation is one of the basic ideas in a well-known paper by Gouvêa and Mazur [**5**], see also [**16**].

From now on, we assume that $k = \mathbb{F}_q$ is a finite field of cardinality q. In this case, $\mathrm{End}_k(E)$ also contains the qth power Frobenius endomorphism π. This corresponds to another point in $E^{\mathrm{tw}}(k(t))$, which we denote as P_0. Except possibly in the case that E/k is a supersingular elliptic curve, the two endomorphisms 1 and π are linearly independent, which implies that Q and P_0 generate a rank 2 subgroup of $E^{\mathrm{tw}}(k(t))$.

In Manin's elementary proof, he introduces the points

$$P_n = P_0 + nQ \in E^{\mathrm{tw}}(k(t)).$$

By construction, these correspond to

$$\pi + n \in \mathrm{End}_k(E).$$

Using the assumption that the characteristic of k is not 2, Manin now uses an explicit equation for $E^{\mathrm{tw}}/k(t)$, and he defines a naive height $h_n = h(P_n)$ of the points P_n. To see the relation with $\mathrm{End}_k(E)$, put

$$d_n := \deg(\pi + n).$$

Lemma 1.1. *With notations as above, for every integer n, one has $h_n = d_n$.*

Proof. Recall from any of the descriptions of Manin's proof that the sequence $(h_n)_{n\in\mathbb{Z}}$ is determined by the three properties:

(1) $h_0 = q$;
(2) $h_{-1} = \#E(\mathbb{F}_q)$;
(3) For every $n \in \mathbb{Z}$ one has $h_{n-1} + h_{n+1} = 2h_n + 2$.

So it suffices to show that $(d_n)_{n\in\mathbb{Z}}$ satisfies the same properties. It is amusing to note that this can already be found in Hasse's 1936 paper [**8**]. We indicate the standard approach.
(1) Obviously, $d_0 = \deg(\pi) = q$.
(2) One has $d_{-1} = \deg(\pi - 1) = \#E(\mathbb{F}_q)$ (compare [**15,** Chapter IV]).
(3) Here one uses dual isogenies; for notations and properties see [**15**].

In the ring $\mathrm{End}_k(E) \supset \mathbb{Z}$, one has

$$\begin{aligned} d_{n-1} + d_{n+1} &= (\pi \widehat{+ n - 1})(\pi + n - 1) + (\pi \widehat{+ n + 1})(\pi + n + 1) \\ &= (\widehat{\pi} + n - 1)(\pi + n - 1) + (\widehat{\pi} + n + 1)(\pi + n + 1) \\ &= 2\widehat{\pi}\pi + 2n(\widehat{\pi} + \pi) + 2n^2 + 2 \\ &= 2(\widehat{\pi} + n)(\pi + n) + 2 = 2d_n + 2. \end{aligned}$$

This proves the lemma. □

One could replace the elementary but somewhat intricate proofs that Manin and others have for the fundamental properties of the sequence $(h_n)_{n\in\mathbb{Z}}$, by a more direct interpretation of h_n as the degree of the associated endomorphism. However, the point of the proof was that it is elementary, while the approach via endomorphisms requires more theory. In the remainder of this note we work out the details of an elementary proof in characteristic two, guided by the exposition presented above.

2. The ordinary case. Let $d > 0$ be an integer, and put $q = 2^d$. Suppose $E/\mathbb{F}_q$ is an elliptic curve with j-invariant $j(E) \neq 0$. It is easily verified (see **[15,** Appendix A], see also Hasse's 1934 paper **[7]**) there are $a, b \in \mathbb{F}_q$, with $b \neq 0$, such that E corresponds to the equation:

$$E : y^2 + xy = x^3 + ax^2 + b.$$

The function field $\mathbb{F}_q(E)$ is written as $\mathbb{F}_q(t, s)$, where s satisfies the quadratic equation

$$s^2 + ts + t^3 + at^2 + b = 0$$

over the rational function field $\mathbb{F}_q(t)$. Define the elliptic curve $E^{\mathrm{tw}}/\mathbb{F}_q(t)$ by the equation

$$E^{\mathrm{tw}} : y^2 + txy = t^2x^3 + t^3x^2 + bx^2 + bt^2.$$

Then E and E^{tw} are not isomorphic over $\mathbb{F}_q(t)$, but they are isomorphic over $\mathbb{F}_q(t, s)$. Indeed, an isomorphism is given by

$$E \longrightarrow E^{\mathrm{tw}} : (x, y) \longmapsto (x, sx + ty).$$

Note that E and E^{tw} have a unique rational point of exact order 2, defined by $x = 0$.

We view the identity map on E as a point $(t,s) \in E(\mathbb{F}_q(t,s))$. Via the given isomorphism, this becomes the point

$$Q := (t,0) \quad \text{on } E^{\mathrm{tw}}.$$

We do the same with the Frobenius map. This gives $(t^q, s^q) \in E(\mathbb{F}_q(t,s))$; hence, the point

$$P_0 := (t^q, st^q + ts^q) \quad \text{on } E^{\mathrm{tw}}.$$

Note that both Q, P_0 are $\mathbb{F}_q(t)$-rational points. This is evident from the discussion in the previous section; a direct proof follows from the observation that the unique automorphism of the quadratic extension $\mathbb{F}_q(t,s)$ over $\mathbb{F}_q(t)$ is defined by $s \mapsto s+t$. Clearly this automorphism fixes $st^q + ts^q$. We can actually say more.

Lemma 2.1. *One has that $st^q + ts^q \in \mathbb{F}_q[t]$ has degree $(3q+2)/2$.*

Proof. Note that the function $st^q + ts^q$ on E is well-defined at every point of E except the point O at infinity. We already showed that this function is in $\mathbb{F}_q(t)$. If it had a denominator, then every zero of the denominator would produce points $\neq O$ on E where $st^q + ts^q$ is undefined. This shows that, indeed, $st^q + ts^q$ is a polynomial in t.

To find the degree of this polynomial one uses the valuation v (order of vanishing) corresponding to O. As is well-known, $v(t) = -2$ and $v(s) = -3$, hence $v(st^q + ts^q) = -3q - 2$. Since a nonzero polynomial $f \in \mathbb{F}_q[t]$ of degree d has valuation $v(f) = -2d$, the lemma follows. □

One of the properties of the points Q and P_0 is that their x-coordinate is a nonconstant polynomial. This implies that, even if one would write this x-coordinate as a quotient of polynomials, the numerator would have a larger degree than the denominator. A natural way to interpret this observation is in terms of the discrete valuation v on $\mathbb{F}_q[t]$, given as

$$v(f) := -\deg(f),$$

for nonzero polynomials f. This is extended in the usual way to $\mathbb{F}_q(t)$ by $v(f/g) = v(f) - v(g)$. Note that $\tau = 1/t$ has the properties $\mathbb{F}_q(\tau) = \mathbb{F}_q(t)$ and $v(\tau) = 1$. We will use τ as a coordinate of this field.

In order to make reduction modulo τ more explicit, write

$$\xi := t^{-2}x \quad \text{and} \quad \eta := t^{-4}y.$$

In these coordinates, the equation for E^{tw} is

$$\eta^2 + \tau\xi\eta = \xi^3 + \tau\xi^2 + b\tau^4\xi^2 + b\tau^6.$$

The reduction modulo τ of this equation is the curve

$$\overline{E}/\mathbb{F}_q : \eta^2 = \xi^3.$$

Moreover, one has a well-defined map

$$E^{\mathrm{tw}}(\mathbb{F}_q(t)) \xrightarrow{\mathrm{mod}\,\tau} \overline{E}(\mathbb{F}_q).$$

With the usual notations (see, e.g., **[15,** Chapter VII, Section 2]) let $\overline{E}_{\mathrm{ns}} := \overline{E} - \{(0,0)\}$, and let $E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$ be the set of points in $E^{\mathrm{tw}}(\mathbb{F}_q(t))$ whose reduction modulo τ is in $\overline{E}_{\mathrm{ns}}(\mathbb{F}_q)$. It is well known that

$$E_0^{\mathrm{tw}}(\mathbb{F}_q(t)) \xrightarrow{\mathrm{mod}\,\tau} \overline{E}_{\mathrm{ns}}(\mathbb{F}_q)$$

is a homomorphism of groups. The kernel of this homomorphism is denoted $E_1^{\mathrm{tw}}(\mathbb{F}_q(t))$. By definition, this kernel consists of the point O at infinity and all affine points which, in the (ξ, η) coordinates, satisfy $v(\xi) < 0$. In the original (x, y) coordinates, using $t^{-2}x = \xi$, this means $2 + v(x) < 0$. So, writing x as a quotient of polynomials in t, this means

$$2 - \deg(\mathrm{numer}\,(x)) + \deg(\mathrm{denom}\,(x)) < 0.$$

This argument shows the following.

Lemma 2.2. *Let $P \in E^{\mathrm{tw}}(\mathbb{F}_q(t))$ have x-coordinate $x(P) = f/g$ for polynomials $f, g \in \mathbb{F}_q[t]$. Then*

$$P \in E_1^{\mathrm{tw}}(\mathbb{F}_q(t)) \Longleftrightarrow \deg(f) > \deg(g) + 2$$

and

$$P \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t)) \Longleftrightarrow \deg(f) \geq \deg(g) + 2.$$

As an easy example, observe that $P_0 \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$ for all q, and $P_0 \in E_1^{\mathrm{tw}}(\mathbb{F}_q(t))$ precisely when $q \neq 2$. Moreover, $Q \notin E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$.

One can do an analogous calculation for the reduction modulo t. In this case, both P_0 and Q reduce modulo t to the singular point of the reduction.

Remark 2.3. An easy calculation (compare **[14]** for a more intrinsic way of seeing this) shows that the only places of $\mathbb{F}_q(t)$ where E^{tw} has singular reduction, are $t = 0$ and $t = \infty$. In both cases, the reduction is of type I_4^* in Kodaira's terminology **[15,** Appendix C, Section 15]. In particular, this implies that

$$2E^{\mathrm{tw}}(\mathbb{F}_q(t)) \subset E_0^{\mathrm{tw}}(\mathbb{F}_q(t)).$$

This also follows from a direct, elementary calculation. Hence, considering reduction modulo τ, $2Q \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$ whereas $Q \notin E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$.

Remark 2.4. Note that the situation for odd characteristic is somewhat simpler, as we will briefly indicate here.

Assume k is a finite field of odd cardinality r. Let E/k be an elliptic curve defined by an equation

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Put $f(t) := t^3 + at^2 + bt + c \in k[t]$, and define $E^{\mathrm{tw}}/k(t)$ by

$$E^{\mathrm{tw}} : f(t)y^2 = x^3 + ax^2 + bx + c.$$

As before, elements in $\mathrm{End}_k(E)$ provide points in $E^{\mathrm{tw}}(k(t))$, so one obtains points $Q = (t, 1)$ and $P_0 = (t^r, f(t)^{(r-1)/2})$ corresponding to the identity and the Frobenius endomorphisms, respectively.

We again put $\tau = 1/t$. An equation for E^{tw} which is minimal at τ is obtained by introducing $\xi := x/t$. The new equations reads

$$(1 + a\tau + b\tau^2 + c\tau^3)y^2 = \xi^3 + a\tau\xi^2 + b\tau^2\xi + c\tau^3.$$

In the new coordinates, $Q = (1, 1)$ and P_0 has ξ-coordinate equal to τ^{1-r}. Hence, both points are in the subgroup $E_0^{\mathrm{tw}}(k(t))$. As in Lemma 2.2, this subgroup consists of the point O and of all points P such that the valuation at τ of $\xi(P)$ is at most 0. Writing $x(P) = f/g$ for polynomials $f, g \in k[t]$, this translates into $1 - \deg(f) + \deg(g) \leq 0$, in other words,

$$\deg(f) > \deg(g).$$

In particular, since $E_0^{\mathrm{tw}}(k(t))$ is a group, this property holds for the x-coordinate of any nonzero point $P_0 + nQ$. Note that this fact is proven in all published versions of Manin's elementary argument without a reference to reduction theory.

We now continue with the case $j \neq 0$ in characteristic 2.

Lemma 2.5. *Suppose $P \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$. Then*

$$\deg(\mathrm{numer}\,(x(P+Q))) = \deg(\mathrm{denom}\,(x(P+Q))) + 1.$$

Proof. This is obvious when $P = O$. Hence, assume $P \neq O$, and write $P = (f/g, y)$ for polynomials $f, g \in \mathbb{F}_q[t]$. The rational function $y \in \mathbb{F}_q(t)$ then satisfies

$$(*) \qquad (g^2y)^2 + tfg(g^2y) + t^2f^3g + t^2bg^4 + t^3f^2g^2 + bf^2g^2 = 0,$$

which implies $g^2y \in \mathbb{F}_q[t]$.

The assumption $P \in E_0^{\mathrm{tw}}$ means by Lemma 2.2 that $\deg(g) \leq \deg(f) - 2$. This implies

$$\deg(g^2y) < \deg(tf^2),$$

since otherwise the first term on the left-hand-side of $(*)$ would have strictly larger degree than any of the other terms. A calculation shows

$$x(P+Q) = \frac{g^2y + t^2fg + tf^2}{f^2 + g^2t^2}.$$

The discussion above implies that the numerator in this expression has degree $\deg(tf^2)$ while the denominator has degree $\deg(f^2)$. This proves the lemma. □

The following is a consequence of Lemma 2.5.

Corollary 2.6. *For $P_n := P_0 + nQ$, we have $P_n \neq O$ and*

$$\deg(\mathrm{numer}\,(x(P_n))) > \deg(\mathrm{denom}\,(x(P_n))).$$

Proof. The point P_n corresponds to $\pi + n \in \mathrm{End}\,(E)$, which is nonzero because E is ordinary. Hence, $P_n \neq O$.

If n is even, then both P_0 and nQ are in $E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$ since $E^{\mathrm{tw}}/E_0^{\mathrm{tw}}$ is a group of exponent 2. Hence, also $P_n = P_0 + nQ \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$. Lemma 2.2 implies

$$\deg(\mathrm{numer}\,(x(P_n))) \geq \deg(\mathrm{denom}\,(x(P_n))) + 2$$

in this case.

If n is odd, write $P_n = P_{n-1} + Q$. The argument above shows that $P_{n-1} \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$, and Lemma 2.5 therefore implies

$$\deg(\mathrm{numer}\,(x(P_n))) = \deg(\mathrm{denom}\,(x(P_n))) + 1.$$

This proves the corollary. □

As in the characteristic > 2 case, put

$$d_n := \deg(\mathrm{numer}\,(x(P_n))).$$

Proposition 2.7. *The integers d_n have the following three properties.*

(i) $d_0 = q$.
(ii) $d_{-1} = \#E(\mathbb{F}_q)$.
(iii) $d_{n-1} + d_{n+1} = 2d_n + 2$.

Proof. (i) is obvious from the definition.

To see (ii), a calculation shows

$$x(P_{-1}) = \frac{N(t)}{(t^q + t)^2},$$

where $N(t) = t^{2q+1} + t^{q+2} + t^{q+1} + st^q + ts^q \in \mathbb{F}_q[t]$. Using Lemma 2.1, $\deg(N(t)) = 2q + 1$. Furthermore, $(t^q + t)^2 = \prod_{\alpha \in \mathbb{F}_q}(t + \alpha)^2$. To compute d_{-1}, we have to examine which of these factors $t + \alpha$ divide $N(t)$, i.e., satisfy $N(\alpha) = 0$. Now

$$N(\alpha) = \alpha^2 + \alpha(\beta + \beta^q),$$

with $\beta \in \mathbb{F}_{q^2}$ satisfying $\beta^2 + \alpha\beta = \alpha^3 + a\alpha^2 + b$. So, if $(\alpha, \beta) \in E(\mathbb{F}_q)$, then $N(\alpha) = \alpha^2 \neq 0$ unless $\alpha = 0$. And if $\beta \notin \mathbb{F}_q$, then $\beta^q = \beta + \alpha$; hence, $N(\alpha) = 0$.

This describes all relevant zeroes of $N(t)$. To say something about their multiplicity, first extend the derivation $' = d/dt$ from $\mathbb{F}_q(t)$ to

$\mathbb{F}_q(t,s)$ using

$$ts' + s = t^2.$$

This yields

$$N'(t) = t^{2q} + t^q + st^{q-1} + t^{q+1} + s^q.$$

Hence, $N'(0) = \sqrt{b} \neq 0$, so 0 is a simple zero of $N(t)$. For any $\alpha \in \mathbb{F}_q$ which is *not* the x-coordinate of a rational point on E, we find $N'(\alpha) = 0$. So these α's are zeroes of $N(t)$ of multiplicity at least 2. The number of such α's equals $q - 1 - \#E(\mathbb{F}_q) - 2/2$. Hence,

$$d_{-1} = 2q + 1 - 1 - 2\left(q - 1 - \frac{\#E(\mathbb{F}_q) - 2}{2}\right) = \#E(\mathbb{F}_q).$$

It remains to prove (iii). For this, write $P_n = (f_n/g_n, y_n)$ for coprime polynomials f_n, g_n, and $y_n \in \mathbb{F}_q(t)$. Using $P_{n\pm1} = P_n \pm Q$, one calculates

$$\frac{f_{n-1}}{g_{n-1}} = \frac{tf_n(tg_n + f_n) + tf_ng_n + g_n^2y_n}{(tg_n + f_n)^2}$$

and

$$\frac{f_{n+1}}{g_{n+1}} = \frac{tf_n(tg_n + f_n) + g_n^2y_n}{(tg_n + f_n)^2};$$

hence,

$$\frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{t^2f_n^2 + bg_n^2}{(tg_n + f_n)^2}.$$

From this, the result follows by comparing degrees, using an argument as presented in, e.g., **[1, 4]**. □

Using Proposition 2.7, an easy argument as presented in all literature on Manin's elementary proof shows how Hasse's inequality for $E/\mathbb{F}_q$ follows.

3. The supersingular case. As before, put $q = 2^d$ for some integer $d \geq 1$. Let $E/\mathbb{F}_q$ be an elliptic curve with j-invariant $j(E) = 0$. By **[15,** Appendix A], we may assume that E is given by an equation

$$E : y^2 + ay = x^3 + bx + c$$

for some $a, b, c \in \mathbb{F}_q$ with $a \neq 0$. The function field $\mathbb{F}_q(E)$ is written as $\mathbb{F}_q(t,s)$, with $s^2 + as = t^3 + bt + c$. The quadratic twist of $E/\mathbb{F}_q(t)$ via

the extension $\mathbb{F}_q(t,s) \supset \mathbb{F}_q(t)$ is:

$$E^{\mathrm{tw}}/\mathbb{F}_q(t) : y^2 + ay = x^3 + bx + t^3 + bt.$$

An isomorphism $E \xrightarrow{\sim} E^{\mathrm{tw}}$ over $\mathbb{F}_q(t,s)$ is given by $(x,y) \mapsto (x, y+s)$. Corresponding to (t,s) and (t^q, s^q) in $E(\mathbb{F}_q(t,s))$ we have the points:

$$Q := (t, 0) \quad \text{and} \quad P_0 := (t^q, s^q + s)$$

in $E^{\mathrm{tw}}(\mathbb{F}_q(t))$. As in Lemma 2.1, one obtains

Lemma 3.1. *The polynomial $s^q + s \in \mathbb{F}_q[t]$ has degree $3q/2$.*

The only place of $\mathbb{F}_q(t)$, where E^{tw} has singular reduction, is the place with uniformizer $\tau := 1/t$. A Weierstrass minimal model at τ is obtained using the variables $\xi := t^{-2}x$ and $\eta := t^{-3}y$. The corresponding equation is:

$$\eta^2 + a\tau^3\eta = \xi^3 + b\tau^4\xi + \tau^3 + b\tau^5.$$

Note that $P_0 \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$ while $Q \notin E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$.

The reduction at τ is of type I_0^*. In particular, this implies that $2E^{\mathrm{tw}}(\mathbb{F}_q(t)) \subset E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$, a fact that also follows from a direct calculation.

We remark in passing that the equation for E^{tw} is of degree 3 in the variables x, y, t. Hence, it defines a (cubic) rational elliptic surface over $\mathbb{F}_q$. Such surfaces, including their possible configurations of singular fibers, were studied by Lang **[10, 11]**.

Observing that $P = (f/g, *)$ is in E_0^{tw} precisely when $\deg(f) \geq \deg(g) + 2$, an argument as given in the proof of Corollary 2.6 shows the following.

Lemma 3.2. *If $P_n := P_0 + nQ \neq O$, then write $x(P_n) = f_n/g_n$ for polynomials $f_n, g_n \in \mathbb{F}_q[t]$.*

One has $\deg(f_n) > \deg(g_n)$.

Write

$$d_n := \begin{cases} 0 & \text{if } P_n = O; \\ \deg(f_n) & \text{if } P_n = \left(\frac{f_n}{g_n}, y_n\right) \text{ with } \gcd(f_n, g_n) = 1. \end{cases}$$

Proposition 3.3. *The integers d_n have the following three properties.*

(i) $d_0 = q$.
(ii) $d_{-1} = \#E(\mathbb{F}_q)$.
(iii) $d_{n-1} + d_{n+1} = 2d_n + 2$.

Proof. (i) is clear. As for (ii), one calculates

$$x(P_0 - Q) = \frac{N(t)}{(t^q + t)^2},$$

where $N(t) = t^{2q+1} + t^{q+2} + b(t^q + t) + a(s^q + s) + a^2$. By Lemma 3.1, $N(t) \in \mathbb{F}_q[t]$ has degree $2q + 1$.

Let $\alpha \in \mathbb{F}_q$ and choose $\beta \in \mathbb{F}_{q^2}$ such that $(\alpha, \beta) \in E(\mathbb{F}_{q^2})$. Then

$$\begin{aligned} N(\alpha) &= a(\beta^q + \beta) + a^2 \\ &= \begin{cases} a^2 \neq 0 & \text{if } (\alpha, \beta) \in E(\mathbb{F}_q); \\ 0 & \text{if } (\alpha, \beta) \notin E(\mathbb{F}_q). \end{cases} \end{aligned}$$

The derivation $' = d/dt$ extends to $\mathbb{F}_q(t, s)$ as

$$as' = t^2 + b.$$

Therefore,

$$N'(t) = t^{2q} + t^2,$$

which vanishes for all $\alpha \in \mathbb{F}_q$. This shows

$$d_{-1} = 2q + 1 - 2 \cdot \left(q - \frac{\#E(\mathbb{F}_q) - 1}{2} \right) = \#E(\mathbb{F}_q).$$

Finally, (iii) is evident in case one of $P_n, P_{n\pm1}$ equals O. In the remaining case, using $P_{n\pm1} = P_n \pm Q$ one calculates

$$\frac{f_{n-1}}{g_{n-1}} = \frac{(tf_n + bg_n)(tg_n + f_n) + ag_n^2(y_n + a)}{(tg_n + f_n)^2}$$

and

$$\frac{f_{n+1}}{g_{n+1}} = \frac{(tf_n + bg_n)(tg_n + f_n) + ag_n^2 y_n}{(tg_n + f_n)^2};$$

hence,

$$\frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{t^2 f_n^2 + b^2 g_n^2 + a^2 g_n(tg_n + f_n)}{(tg_n + f_n)^2}.$$

As in Proposition 2.7, this implies the result. □

Again, Hasse's inequality for $E/\mathbb{F}_q$ follows, as explained in all published accounts on Manin's elementary proof.

Acknowledgments. Most of this paper was written while its first and last author enjoyed the hospitality of BIRS in Banff, Alberta. In particular, we are grateful to Mike Bennett, Nils Bruin, Yann Bugeaud, Bjorn Poonen, and Samir Siksek for organizing a very successful BIRS instructional conference on Temporary Methods for Solving Diophantine Equations.

REFERENCES

1. Jasbir S. Chahal, *Topics in number theory*, Plenum Press, New York, 1988.

2. ———, *Manin's proof of the Hasse inequality revisited*, Nieuw Arch. Wisk., 4th Series **13** (1995), 219–232.

3. Jasbir S. Chahal and Brian Osserman, *The Riemann hypothesis for elliptic curves*, Amer. Math. Month. **115** (2008), 431–442.

4. A.O. Gel'fond and Yu.V. Linnik, *Elementary methods in the analytic theory of numbers*, Inter. Ser. Mono. Math. **92**, Pergamon Press, Oxford, 1966.

5. F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.

6. H. Hasse, *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen*, Nachr. Gesell. Wissen. Göttingen (1933), 253–262.

7. ———, *Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern*, Abh. Math. Sem. Hamburg **10** (1934), 325–348.

8. ———, *Zur Theorie der abstrakten elliptischen Funktionenkörper* III, J. reine angew. Math. **175** (1936), 193–208.

9. Anthony W. Knapp, *Elliptic curves*, Math. Notes **40**, Princeton University Press, Princeton, 1993.

10. William E. Lang, *Extremal rational elliptic surfaces in characteristic p* II, *Surfaces with three or fewer singular fibres*, Ark. Mat. **32** (1994), 423–448.

11. ———, *Configurations of singular fibres on rational elliptic surfaces in characteristic two*, Comm. Alg. **28** (2000), 5813–5836.

12. Marios Magioladitis, *Algebraic curves, Riemann hypothesis and coding*, Dipl. Th., Department of Mathematics, University of Crete, 2001. `http://www.exp-math.uni-essen.de/~magiolad/ergasia/essay.htm`

13. Yu.I. Manin, *On cubic congruences to a prime modulus*, Izv. Akad. Nauk SSSR Ser. Mat. **20** (1956), 673–678.

14. Roland Miyamoto and Jaap Top, *Reduction of elliptic curves in equal characteristic* 3 (*and* 2), Canad. Math. Bull. **48** (2005), 428–444.

15. J.H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts Math. **106**, Springer, New York, 1986.

16. C.L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

17. J.T. Tate and I.R. Safarevic, *The rank of elliptic curves*, Soviet Math. Dokl. **8** (1967), 917–920.

Department of Mathematics, Brigham Young University, Provo, UT 84602
Email address: **jasbir@mathematics.byu.edu**

JBI-RuG, Nijenborgh 9, 9747 AG Groningen, the Netherlands
Email address: **m.a.soomro3@gmail.com**

JBI-RuG, Nijenborgh 9, 9747 AG Groningen, the Netherlands
Email address: **j.top@rug.nl**