COMPOSITIO MATHEMATICA

J. H. SILVERMAN
J. F. VOLOCH

Multiple Weierstrass points

Compositio Mathematica, tome 79, n° 1 (1991), p. 123-134
<http://www.numdam.org/item?id=CM_1991__79_1_123_0>

Compositio Mathematica **79**: 123–134, 1991.

Multiple Weierstrass points

J.H. SILVERMAN[1] and J.F. VOLOCH[2]

[1]*Mathematics Department, Brown University, Providence, RI 02912, U.S.A. and* [2]*IMPA, Estr. Dona Castorina, 110, 22.460 Rio de Janeiro, Brazil*

Received 25 June 1990; accepted 26 October 1990

In this note we study the question of when a point on a curve of genus $g \geqslant 2$ can be an nth order Weierstrass point for infinitely many n. We start by setting some notation:

k	a field.
C/k	a curve of genus $g \geqslant 2$ defined over k.
D	an effective divisor of degree d on C.
n	a positive integer.
s	$= l(nD)$. (If $nd \geqslant 2g-1$, then $s = nd - g + 1$.)
$C[nD]$	$= \{P \in C : l(nD - sP) \geqslant 1\}$, the set of nth order Weierstrass points associated to D.
$N(D,P)$	$= \{n \in \mathbb{N} : P \in C[nD]\}$.

A point P which lies in infinitely many of the $C[nD]$'s, $n = 1, 2, \ldots$, will be called a *multiple D-Weierstrass point*. Multiple Weierstrass points do exist, the simplest example being the branch points on a hyperelliptic curve. More generally, a number of authors [1, 4, 6, 8, 9, 10, 14] have given criteria under which fixed points of non-trivial automorphisms are multiple Weierstrass points. We observe, however, that a Riemann surface of genus at least 2 has only a finite number of automorphisms, and so looking at fixed points of automorphisms can yield only finitely many multiple Weierstrass points.

In fact, a little thought suggests that at least in characteristic zero, the multiple Weierstrass points should be rather rare. Our first theorem shows that this is indeed the case.

THEOREM 1. *With notation as above, assume that k has characteristic zero. Assume further that the Jacobian variety J of C is simple; or, more generally, that the theta divisor* $\Theta \subset J$ *contains no translates of non-trivial abelian subvarieties of J.*

[1]Research partially supported by NSF DMS-8842154 and a Sloan Foundation Fellowship.

(a) *If* $N(D, P)$ *is infinite, then there is an integer* $m \geqslant 1$ *such that*

$$md(P) \sim mD.$$

(*Here* $\sim$ *denotes linear equivalence of divisors.*)

(b) *The set* $N(D, P)$ *is finite for all but finitely many points* $P \in C$. (*That is,* C *has only finitely many multiple* D*-Weierstrass points.*)

Theorem 1 is essentially an assertion concerning Riemann surfaces defined over the complex numbers. However, our proof of Theorem 1 will depend on two deep arithmetic results, Raynaud's proof of the Manin–Mumford conjecture and Faltings' proof of part of the Lang–Mordell conjecture. It would be extremely interesting to give a purely analytic proof.

The Lang–Mordell conjecture says (roughly) that if a subvariety of an abelian variety contains infinitely many rational points, then those points lie on finitely many translates of abelian subvarieties. Faltings [5] has proven this conjecture in the case that the subvariety contains no translates of abelian subvarieties. It seems quite likely that Faltings' proof will be adapted to give a proof of the full Lang–Mordell conjecture, in both its absolute and relative forms. We will then be able to prove (b) of Theorem 1 with no restrictions on C.

THEOREM 2. *Assume that* k *has characteristic zero. Assume further that the absolute and relative Lang–Mordell conjectures are true.* (*For the precise statement of these conjectures, see below.*) *Then* $N(D, P)$ *is finite for all but finitely many points* $P \in C$.

In positive characteristic, Weierstrass points often behave quite differently from characteristic zero. As a contrast to Theorem 1, we will prove the following result.

THEOREM 3. *Let* k *be a finite field, and let* $P \in C(\bar{k})$.

(a) $N(D, P)$ *is an infinite set.*

(b) *Assume that* D *is non-special. Then the complement of* $N(D, P)$ *in* $\mathbb{N}$ *is either empty or infinite.*

REMARK. Recall that in characteristic p a divisor is called classical if not every point is a Weierstrass point. Continuing the notation of Theorem 3, suppose that the divisor class $\langle D - d(P) \rangle$ has order prime to p in $\mathrm{Pic}^0(C)$, that $P \notin C[K_C]$, and that $p > 2g - 2$. Then using the results in [13], it is not hard to show that there are infinitely many multiples mD such that mD is classical and $P \in C[mD]$.

Theorem 1(a) answers in the affirmative a question raised by Fernando Cukierman and Joe Harris, at least for curves satisfying the assumptions of Theorem 1. More generally, they have asked about the validity of the following

two statements (in characteristic zero):

(i) If $N(K_C, P) = \mathbb{N}$, then $(2g-2)(P) \sim K_C$. (Here K_C is a canonical divisor on C.)

(ii) If $\#N(K_C, P) = \infty$, then there exists an integer $m \geqslant 1$ such that $m(2g-2)(P) \sim mK_C$.

We will show that both of these statements are false. In fact, we will give an example showing that the stronger assumption of (i) does not even imply the weaker conclusion of (ii).

PROPOSITION 4. *There exist curves $C/\mathbb{C}$ of arbitrarily high genus which contain points $P \in C$ satisfying $N(K_C, P) = \mathbb{N}$ and $m(2g-2)(P) \not\sim mK_C$ for all $m \geqslant 1$.*

Before starting the proof of our theorems, we set a bit more notation and prove a useful alternative characterization of Weierstrass points.

J the Jacobian variety of C.

i_P the embedding $C \hookrightarrow J$, $Q \mapsto \langle (Q) - (P) \rangle$. We extend i_P linearly to divisors.

W_P $= i_P(C^{g-1}) = \underbrace{i_P(C) + \cdots + i_P(C)}_{g-1 \text{ times}}$.

LEMMA 5. *Assume that nD is non-special. Then*

$$P \in C[nD] \Leftrightarrow n \cdot i_P(D) \in W_P.$$

Proof. Since nD is non-special, we have

$$\deg(nD - sP) = nd - s = nd - l(nD) = g - 1 - l(K_C - nD) = g - 1.$$

We compute

$$\begin{aligned} P \in C[nD] &\Leftrightarrow l(nD - sP) \geqslant 1 \\ &\Leftrightarrow nD - sP \text{ is effective} \\ &\Leftrightarrow nD - sP \sim P_1 + \cdots + P_{g-1} \quad \text{for some } P_1, \ldots, P_{g-1} \in C, \\ &\Leftrightarrow n \cdot i_P(D) = i_P(P_1) + \cdots + i_P(P_{g-1}) \in i_P(C^{g-1}) \subset W_P. \end{aligned}$$

□

Proof of Theorem 1. Since k has characteristic zero, we may assume that k is a finitely generated subfield of $\mathbb{C}$ (Lefschetz principle), and then by specialization we may assume that k is a number field. Let

$$T(D) = \{P \in C : N(D, P) \text{ is infinite}\}.$$

Our aim is to prove that $T(D)$ is finite.

Riemann's theorem [7, p. 338] says that for any point $P \in C$, the divisor W_P is a translate of Θ, say $W_P = \Theta + y_P$. By assumption, Θ contains no translates of non-trivial abelian subvarieties of J, so the same is true of W_P. By Faltings' theorem [5], the intersection of W_P with any finitely generated subgroup of J is finite.

Lemma 5 says that

$$n \in N(D,P) \Leftrightarrow n \cdot i_P(D) \in W_P,$$

at least if nD is non-special. In particular, this is true for all $n \geqslant 2g-1$. So if we let

$$N'(D,P) = \{n \in N(D,P) : n \geqslant 2g-1\},$$

then the set

$$N'(D,P) \cdot i_P(D) = \{n \cdot i_P(D) : n \in N'(D,P)\}$$

is contained in W_P. By Faltings' theorem, the intersection of the finitely generated (in fact, cyclic) group $\mathbb{Z} \cdot i_P(C)$ with W_P is finite, so we conclude that $N(D,P) \cdot i_P(D)$ is finite.

It follows that every $P \in T(D)$ has the property that $i_P(D)$ has finite order in J. This means that there is some $m \geqslant 1$ such that $m i_P(D) = O$; or equivalently that $m(D - d(P)) \sim 0$. This completes the proof of (a).

We now want to think of the divisor D as fixed and the point P as varying, so we consider the map

$$\mu_D : C \to J, \qquad P \mapsto \langle d(P) - D \rangle.$$

Notice that $i_P(D) = -\mu_D(P)$. Thus

$$\mu_D(T(D)) \subset \mu_D(C) \cap J_{\text{tors}}.$$

Next we observe that μ_D is a composition (for any basepoint $P_0 \in C$)

$$C \overset{\mu_{P_0}}{\hookrightarrow} J \xrightarrow{\text{mult. by } d} J \xrightarrow{\text{translation}} J.$$

$$P \mapsto \langle (P) - (P_0) \rangle$$

Hence

$$\mu_D(C^g) = d \cdot \mu_{P_0}(C^g) + g \cdot \mu_D(P_0).$$

But $\mu_{P_0}(C^g)$ is all of J [7, page 235], so also $\mu_D(C^g) = J$. Thus the image $\mu_D(C)$ generates J. In particular, $\mu_D(C)$ must be a curve of genus at least 2, and the map $\mu_D : C \to \mu_D(C)$ is finite.

Since $\mu_D(C)$ has genus at least 2, Raynaud's theorem [12] says that

$$\mu_D(C) \cap J_{\text{tors}}$$

is finite. This implies that $\mu_D(T(D))$ is finite; and since $\mu_D: C \to J$ is finite-to-one, we finally conclude that the set $T(D)$ is finite. This completes the proof of (b). □

Before commencing the proof of Theorem 2, we must remind the reader of the statement of the Lang–Mordell conjecture. There are two forms of this conjecture, one for finitely generated fields and one for finitely generated extensions of arbitrary fields.

ABSOLUTE LANG–MORDELL CONJECTURE. *Let K be a field finitely generated over $\mathbb{Q}$ or $\mathbb{F}_p$, let A/K be an abelian variety, and let $V/K \subset A/K$ be a subvariety. Then there is a finite collection $U_1, \dots, U_r \subset A$ of abelian subvarieties of A and a finite set of points $u_1, \dots, u_r \in A$ such that*

$$V(K) \subset \bigcup_{i=1}^{r} (U_i + u_i) \subset V.$$

RELATIVE LANG–MORDELL CONJECTURE. *Let k be an (algebraically closed) field, let K/k be a regular extension, let A/K be an abelian variety, let (A_0, τ) be a K/k trace for A/K, and let $V/K \subset A/K$ be a subvariety. Then there is a finite collection $U_1, \dots, U_r \subset A$ of abelian subvarieties of A and a finite set of points $u_1, \dots, u_r \in A$ such that*

$$V(K) \subset \bigcup_{i=1}^{r} (U_i + u_i) + \tau(A_0) \subset V + \tau(A_0).$$

REMARK. In both versions of the Lang–Mordell Conjecture, it is possible to choose the U_i's to be defined over K and the u_i's to be in $A(K)$. To see this, suppose that A/K is an abelian variety, and that $U \subset A$ is an abelian subvariety defined over some extension of K. Let

$$B = \bigcap_{\sigma \in G(\bar{K}/K)} U^{\sigma}$$

be the largest abelian subvariety of U which is defined over K. Then one easily sees that $A(K) \cap U = B(K)$. Hence if we choose some $x \in A(K) \cap (U + u)$, then

$$V(K) \cap (U + u) \subset A(K) \cap (U + u) = (A(K) \cap U) + x = B(K) + x.$$

Now suppose that $V(K) \subset \bigcup (U_i + u_i) \subset V$ as in the Absolute Lang–Mordell Conjecture. Let $B_i \subset U_i$ be the maximal K-abelian subvariety of U_i, and choose points $x_i \in V(K) \cap (U_i + u_i)$. Then the computation we just did shows that

$$V(K) = \bigcup_{i=1}^{r} (V(K) \cap (U_i + u_i)) \subset \bigcup_{i=1}^{r} B_i(K) + x_i.$$

Since also $B_i + x_i \subset U_i + x_i = U_i + u_i \subset V$, this shows we may replace the U_i's by the B_i's and the u_i's by the x_i's. The argument for the Relative Lang–Mordell Conjecture is similar, the main difference being that the inclusion

$V(K) \cap (U + u) \subset B(K) + x$ is replaced by the relative inclusion

$$V(K) \cap (U + u + \tau(A_0)) \subset B(K) + x + \tau(A_0).$$

The Lang–Mordell Conjecture involves translates of abelian subvarieties contained in a given subvariety. This prompts us to make the following definitions:

DEFINITION. Let A be an abelian variety, $B \subset A$ an abelian subvariety, and $V \subset A$ an arbitrary subvariety. We define

$$V^B = \{x \in A : B + x \subset V\}.$$

We say that B is *a V-maximal abelian subvariety of A* if $\dim B \geqslant 1$, $V^B \neq \varnothing$, but $V^{B'} = \varnothing$ for all abelian subvarieties $B \subsetneq B' \subset A$.

LEMMA 6. *Let A be an abelian variety, and let $V \subset A$ be a subvariety. Assume that the Relative Lang–Mordell Conjecture is true. Then A contains only finitely many V-maximal abelian subvarieties.*

Proof. Let k be an algebraically closed field of definition for A and V. We suppose that A contains infinitely many V-maximal abelian subvarieties, say $B_1, B_2, \ldots$, and derive a contradiction. Note that in any case the abelian subvarieties of A fall into only finitely many isogeny classes. This follows, for example, from Poincaré's Complete Reducibility Theorem [11, Corollary 1, p. 174]. So taking a subsequence of the B_i's, we may assume that they are all isogenous to some fixed abelian variety Y. We will also fix isogenies $\phi_i : Y \to B_i$.

We now extend scalars and look at A and V as varieties over the function field $k(Y)$ of Y. Equivalently, we let $\mathscr{A} = A \times Y$ and $\mathscr{V} = V \times Y$, so $\pi_2 : \mathscr{A} \to Y$ exhibits $\mathscr{A}$ as an abelian scheme over Y. The sections

$$(\phi_i \times 1) : Y \to \mathscr{A}, \qquad y \mapsto (\phi_i(y), y)$$

correspond to points $P_i \in A(k(Y))$. Notice that the image of this section is $B_i \times Y$.

By assumption, $V^{B_i} \neq \varnothing$, so we can choose some $b_i \in A(k)$ so that $B_i + b_i \subset V$. By abuse of notation, we also let b_i represent the point in $A(k(Y))$ corresponding to the constant section

$$Y \to \mathscr{A}, \qquad y \mapsto (b_i, y).$$

In other words, we have a natural inclusion $A(k) \subset A(k(Y))$, since A/k is a $k(Y)/k$ trace for $A/k(Y)$.

The point $P_i + b_i \in A(k(Y))$ corresponds to the section

$$\psi_i : Y \to \mathscr{A}, \qquad y \mapsto (\phi_i(y) + b_i, y);$$

and we see that $\psi_i(Y) = (B_i + b_i) \times Y \subset \mathscr{V}$. Hence $P_i + b_i \in V(k(Y))$.

Now we apply the Relative Lang–Mordell Conjecture. This says that after replacing the set of $P_i + b_i$'s by some infinite subsequence, there is an abelian

subvariety $U/k(Y) \subset A/k(Y)$ and a point $u \in A(k(Y))$ so that

$$\{P_i + b_i : i = 1, 2, \ldots\} \subset U + u + A(k) \subset V + A(k).$$

[N.B. These are points and varieties defined over the function field $k(Y)$. The fact that we can choose U and u defined over $k(Y)$ rather than some extension is explained in the remark given above after the statement of the Relative Lang–Mordell Conjecture.]

We claim that in fact U is defined over k. To see this, take a model for U over Y, say $\mathscr{U} \to Y$, with $\mathscr{U} \subset \mathscr{A}$. Since U is an abelian subvariety of A over $k(Y)$, we can find an open subvariety $Y^0 \subset Y$ so that $\mathscr{U}^0 \to Y^0$ is an abelian subscheme of $\mathscr{A}^0 \to Y^0$. But $\mathscr{A}^0$ splits as $A \times Y^0$, so taking fibers of the map $\mathscr{U}^0 \to Y^0$ we get an algebraic map

$$Y^0 \to \left\{\begin{matrix}\text{abelian subvarieties} \\ \text{of } A\end{matrix}\right\}.$$

More precisely, fix a projective embedding of A. By continuity, every fiber of $\mathscr{U}^0 \to Y^0$ is a subvariety of A of a fixed degree. Then we get a rational map from Y^0 into the Chow scheme of subvarieties of A of that fixed degree; and further, the image of that rational map consists of *abelian* subvarieties of A. But it is easy to see (e.g. again using Poincaré Reducibility) that A contains only finitely many abelian subvarieties of bounded degree, so the image of Y^0 in the Chow scheme is finite, hence constant.

Thus there is an abelian subvariety $U'/k \subset A/k$ so that $U' \times Y$ is birational to $\mathscr{U}$. Equivalently, U' is isomorphic to U over $k(Y)$, which is just another way of saying that U itself can be defined over k.

We now know that as varieties over $k(Y)$, we have an inclusion $U + u \subset V + A(k)$. This means the following. For any extension $K/k(Y)$ and any point $P \in U(K)$, there is a point $a \in A(k)$ such that $P + u - a \in V(K)$. The crucial point here is that the point a is defined over k. We apply this by taking $K = k(U \times Y)$, with $k(Y) \hookrightarrow K$ corresponding to the projection $U \times Y \to Y$.

Note that there is a generic point $P \in U(k(U))$, and we can consider P to be a point of $U(K)$ via the inclusion $k(U) \subset K$ coming from the projection $U \times Y \to U$. For this P we choose an $a \in A(k)$ so that $P + u - a \in V(K)$. What does this mean in terms of maps between varieties?

The point $P \in U(K) = U(k(U \times Y))$ corresponds to the map

$$U \times Y \to U, \qquad P(t, y) = t.$$

The point $u \in A(k(Y))$ corresponds to a rational map $\lambda : Y \to A$; and if we want to treat u as a point in $A(K)$, then it is the map

$$U \times Y \to A, \qquad (t, y) \mapsto \lambda(y).$$

The point $a \in A(k) \subset A(K)$ corresponds to the constant map

$$U \times Y \to A, \qquad (t, y) \mapsto a.$$

So the inclusion $P + u - a \in V(K)$ means that when we combine these three maps, we end up lying in V:

$$U \times Y \to V, \qquad (t, y) \mapsto t + \lambda(y) + a.$$

In other words,

$$U(k) + \lambda(Y)(k) + a \subset V(k).$$

Next we observe that Y and A are abelian varieties, so $\lambda: Y \to A$ is a homomorphism followed by a translation [11, Corollary 1, p. 43]. Hence we can write

$$\lambda(Y) = X + x$$

for some abelian subvariety $X/k \subset A/k$ and some point $x \in A(k)$. (We allow the possibility that X consists of a single point.) Hence

$$U + X + x + a \subset V$$

as subvarieties over A/k. Now $U + X$ is an abelian subvariety of A, and we have just shown that a translate of $U + X$ lies in V. Therefore

$$V^{U+X} \neq \varnothing.$$

On the other hand, we know from above that

$$\{P_i + b_i : i = 1, 2, \ldots\} \subset U + u + A(k).$$

Since the b_i's are in $A(k)$, we see that

$$\{P_i : i = 1\,2, \ldots\} \subset U + u + A(k).$$

Recalling that the point P_i corresponds to the section $(\phi_i \times 1): Y \to \mathscr{A}$, and that $u \in A(k(Y))$ corresponds to the map $\lambda: Y \to A$ with image $\lambda(Y) = X + x$, this means that $\phi_i(Y) = B_i$ is contained in a translate of $U + X$. But B_i and $U + X$ are subgroups of A, so B_i itself is contained in $U + X$:

$$B_i \subset U + X \quad \text{for all } i = 1, 2, \ldots$$

Further, since the B_i's are distinct, we see that $U + X$ has dimension strictly larger than the B_i's, so

$$B_i \subsetneqq U + X \quad \text{for all } i = 1, 2, \ldots.$$

This combined with $V^{U+X} \neq \varnothing$ contradicts the assumption that the B_i's are V-maximal, which completes the proof of Lemma 6. □

Proof of Theorem 2. As in the proof of Theorem 1, we may assume that k is

finitely generated over $\mathbb{Q}$. We again let

$$T(D) = \{P \in C: N(D, P) \text{ is infinite}\},$$

and we will show that $T(D)$ is finite. We know W_P is a translate of Θ. Hence the W_P-maximal abelian subvarieties of J are the same as the Θ-maximal abelian subvarieties of J. We denote this set by $\mathscr{M}(\Theta)$. From Lemma 6, $\mathscr{M}(\Theta)$ is finite.

Again we observe from Lemma 5 that the set

$$N'(D, P) \cdot i_P(D) = \{n \cdot i_P(D): n \in N(D, P), n \geqslant 2g - 1\}$$

is contained in W_P. By the Absolute Lang–Mordell Conjecture, the intersection

$$\mathbb{Z} \cdot i_P(D) \cap W_P$$

is contained in finitely many translates of abelian subvarieties of J which lie in W_P. More precisely, there are points $y_{B,P} \in J$, one for each $B \in \mathscr{M}(\Theta)$, such that

$$N(D, P) \cdot i_P(D) \subset \mathbb{Z} \cdot i_P(D) \cap W_P \subset \bigcup_{B \in \mathscr{M}(\Theta)} (B + y_{B,P}) \cup \{\text{finite set}\} \subset W_P.$$

We can thus divide $N(D, P)$ into a finite union of sets

$$N(D, P) = \bigcup_{B \in \mathscr{M}(\Theta)} \{n \geqslant 2g-1: n \cdot i_D(P) \in B + y_{B,P}\} \cup \{n \in N(D, P): n \leqslant 2g-2\}.$$

Suppose that $N(D, P)$ is infinite, i.e. $P \in T(D)$. This means that for some $B \in \mathscr{M}(\Theta)$, there are infinitely many $n \in \mathbb{N}$ such that $n \cdot i_D(P) \in B + y_{B,P}$. If n_1 and n_2 are two such integers, then $(n_2 - n_1) \cdot i_D(P) \in B$. Thus if $N(D, P)$ is infinite, then there is some $B \in \mathscr{M}(\Theta)$ such that infinitely many multiples of $i_D(P)$ lie on B. We are thus reduced to the following assertion:

For each $B \in \mathscr{M}(\Theta)$ and each $P \in C$, let

$$N(D, P, B) = \{n \in \mathbb{Z}: n \cdot i_D(P) \in B\}.$$

Then the set

$$T(D, B) = \{P \in C: N(D, P, B) \text{ is infinite}\}$$

is a finite subset of C.

Note that since B is a group, we could equally well have defined $T(D, B)$ to consist of those points such that $n \cdot i_D(P) \in B$ for some $n \neq 0$. For the remainder of this proof we fix some $B \in \mathscr{M}(\Theta)$. The idea of the proof is to apply the Lang–Mordell Conjecture and Raynaud's Theorem to the quotient variety J/B.

We consider the map

$$\mu_D: C \to J, \qquad P \mapsto \langle d(P) - D \rangle$$

as in the proof of Theorem 1, and the projection map

$$\pi: J \to J/B.$$

Since $i_P(D) = -\mu_D(P)$, we have

$$\begin{aligned} P \in T(D, B) &\Leftrightarrow n \cdot i_D(P) \in B \text{ for some integer } n \neq 0 \\ &\Leftrightarrow n \cdot (\pi\mu_D)(P) = 0 \text{ for some integer } n \neq 0 \\ &\Leftrightarrow (\pi\mu_D)(P) \in (J/B)_{\text{tors}}. \end{aligned}$$

This shows that

$$(\pi\mu_D)(T(D, B)) \subset (\pi\mu_D)(C) \cap (J/B)_{\text{tors}}.$$

We claim that $(\pi\mu_D)\colon C \to J/B$ is finite onto its image. We need to show that $(\pi\mu_D)(C)$ is not a point, which is equivalent to showing that $\mu_D(C)$ is not contained in a translate of B. During the proof of Theorem 1, we showed that $\mu_D(C^g) = J$, so the image $\mu_D(C)$ generates J. In particular, since B is a proper abelian subvariety of J, $\mu_D(C)$ cannot be contained in any translate of B. This proves our claim that $(\pi\mu_D)\colon C \to J/B$ is finite onto its image.

We next claim that the image $(\pi\mu_D)(C)$ has genus at least 2. Suppose not. Since an abelian variety contains no rational curves, it would follow that $E = (\pi\mu_D)(C)$ is a curve of genus 1. Let X be the connected component of the inverse image $\pi^{-1}(E)$ which contains $\mu_D(C)$. Then $X \to E$ exhibits X as a fiber product over an elliptic curve with fibers isomorphic to the abelian variety B. It follows that X is the translate of an abelian subvariety of J, and that X is isogenous to $E \times B$.

Next we note that $\mu_D(C) \subset X$. As observed above, $\mu_D(C)$ generates J, from which it follows that $X = J$. But

$$\dim X = \dim(E \times B) = 1 + \dim B \leqslant \dim J - 1.$$

(The last inequality follows from the fact that some translate of B is contained in the divisor Θ, and Θ itself is not an abelian variety, so B must have codimension at least 2 in J.) This contradiction shows that $(\pi\mu_D)(C)$ cannot have genus 1, so its genus must be at least 2.

We can now finish the proof of Theorem 2. Since $(\pi\mu_D)(C)$ has genus at least 2, Raynaud's theorem [12] says that

$$(\pi\mu_D)(C) \cap (J/B)_{\text{tors}}$$

is finite. From above, this implies that $(\pi\mu_D)(T(D, B))$ is finite. But the map $\pi\mu_D\colon C \to J/B$ is finite, so we conclude that $T(D, B)$ is finite. □

The easiest way to prove Theorem 3 is to observe that points of C which map to torsion points of J (under the map $P \to i_P(D)$) are always multiple Weierstrass points for D. This leads us to make the following slight generalization of a notion introduced by Coleman [3].

DEFINITION. The *torsion packet associated to the divisor* D is the set

$$\begin{aligned} \mathscr{T}(D) &= \{P \in C\colon mD \sim md(P) \text{ for some } m \geqslant 1\} \\ &= \{P \in C\colon \langle d(P) - D \rangle \in J_{\text{tors}}\}. \end{aligned}$$

(As usual, $\sim$ denotes linear equivalence of divisors.)

Notice that Raynaud's theorem says that if k has characteristic 0, then every torsion packet $\mathscr{T}(D)$ is finite.

LEMMA 7. *If $P \in \mathscr{T}(D)$, then P is a multiple D-Weierstrass point. More precisely, there is an integer $m \geqslant 1$ so that $N(D, P)$ contains $m\mathbb{N}$.*

Proof. We have

$$P \in \mathscr{T}(D) \Leftrightarrow i_P(D) \in J_{\text{tors}} \Leftrightarrow m \cdot i_P(D) = 0 \quad \text{for some } m \geqslant 1.$$

Since $0 \in W_P$, we see that $nm \cdot i_P(D) \in W_P$ for all $n \geqslant 1$. By Lemma 5, this means that $P \in C[nmD]$ for all $n \in \mathbb{N}$, at least provided that nmD is non-special. Replacing m by a multiple of m (such as $(2g-1)m$), we can ensure that nmD is non-special. Then $N(D, P)$ contains $m\mathbb{N}$. □

Proof of Theorem 3. (a) Since $i_P(D) \in J(\bar{k})$, and every element of $J(\bar{k})$ has finite order (since k is a finite field), we see that every point $P \in C(\bar{k})$ is in $\mathscr{T}(D)$. Hence from Lemma 7, $N(D, P)$ is infinite.

(b) Suppose $N(D, P) \neq \mathbb{N}$, and choose some $r \in \mathbb{N}$ with $r \notin N(D, P)$. This means that $P \notin C[rD]$, so from Lemma 5 (note D is non-special by assumption), we see that $r \cdot i_P(D) \notin W_P$. As in (a), we also know that $i_P(D)$ has finite order in $J(\bar{k})$, say $m \cdot i_P(D) = 0$. Then for every integer $j = 1, 2, \ldots$ we have

$$(r + jm) i_P(D) = r \cdot i_P(D) \notin W_P, \quad \text{so } P \notin C[(r + jm)D].$$

Hence the arithmetic progression $r + m\mathbb{N}$ is contained in the complement of $N(D, P)$. □

Proof of Proposition 4. Let $X/\mathbb{C}$ be a curve of genus at least 1, let $s \geqslant 5$ be an integer, and choose s generic points $x_1, \ldots, x_s \in X$. [In fact, it is only necessary to choose points so that the differences $(x_i) - (x_j)$ do not have finite order in $\text{Pic}^0(X)$.] Let $\pi: C \to X$ be a double cover of X which is ramified above each of the x_i's. For example, take any function $f \in \mathbb{C}(X)$ with simple zeros at the x_i's, and let C be a smooth model for the field $\mathbb{C}(X)(\sqrt{f})$.

Let τ be the involution of C given by switching the sheets of $\pi: C \to X$. Then the points $P_i = \pi^{-1}(x_i)$ are fixed points of τ. Since there are at least 5 fixed points, Lewittes' theorem [10] implies that the P_i's are ordinary Weierstrass points. That is, $P_i \in C[K_C]$. Further, a result of Accola [2, Theorem 6.20], applied to our automorphism of order 2, implies that $P_i \in C[nK_C]$ for all $n \geqslant 2$. Hence each P_i satisfies $N(K_C, P_i) = \mathbb{N}$.

On the other hand, suppose that there are integers $m_i, m_j \geqslant 1$ for indices $i \neq j$ such that

$$m_i(2g - 2)P_i \sim m_i K_C \quad \text{and} \quad m_j(2g - 2)P_j \sim m_j K_C.$$

Subtracting appropriate multiples of these equations yields

$$m_i m_j (2g - 2)((P_i) - (P_j)) \sim 0.$$

Hence $(P_i)-(P_j)$ has finite order in $\mathrm{Pic}^0(C)$.

But the covering $\pi: C \to X$ induces a map $\hat{\pi}: \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(C)$ with finite kernel; and $\hat{\pi}((x_i)-(x_j)) \sim (\deg \pi)((P_i)-(P_j))$. It would follow that $(x_i)-(x_j)$ has finite order in $\mathrm{Pic}^0(X)$, contradicting the choice of the x_i's. Therefore at most one of the P_i's can satisfy $m(2g-2)(P) \sim mK_C$; and all of the other P_i's provide examples which prove Proposition 4. □

Acknowledgements

We would like to thank the NSF and CNPq for sponsoring the Workshop on Algebraic Geometry (IMPA, April 1990) at which the authors started this research. We would also like to thank Bob Accola, Joe Harris, and Fernando Cukierman for a number of helpful suggestions.

References

1. Accola, R.: On generalized Weierstrass points on Riemann surfaces. Modular Functions in Analysis and Number Theory, ed. by T. A. Metzger, *Lecture Notes in Math. and Stat.*, Univ. of Pittsburgh, Pittsburgh, PA: 1978.
2. ——: Topics in the Theory of Riemann Surfaces. Brown University: Lecture Notes September, 1989, to appear.
3. Coleman, R.: Torsion points on curves, Galois Representations and Arithmetic Geometry. *Adv. Stud. in Pure Math.* 12, 235–247 (1987).
4. Duma, A.: Holomorphe Differentiale höherer Ordnung auf kompakten Riemannischen Flächen. Schrift. Univ. Münster 14, 00–00 (1978).
5. Faltings, G.: Diophantine approximation on Abelian varieties, *Annals of Math.*, to appear.
6. Farkas, H. M., Kra, I.: Riemann surfaces, *Grad. Texts Math.* 71. New York: Springer-Verlag, 1980.
7. Griffiths, P., Harris, J.: Principles of Algebraic Geometry. New York: John Wiley & Sons, 1978.
8. Guerrero, I.: Automorphisms of compact Riemann surfaces and Weierstrass points. Riemann Surfaces and Related Topics, Proc. 1978 Stony Brook Conference. Princeton: Princeton Univ. Press, 1980.
9. Horiuchi, R., Tanimoto, T.: Fixed points of automorphisms of compact Riemann surfaces and higher order Weierstrass points. *Proc. Amer. Math. Soc.* 105, 856–860 (1989).
10. Lewittes, J.: Automorphisms of compact Riemann surfaces. *Amer. J. Math.* 85, 734–752 (1963).
11. Mumford, D.: Abelian varieties. Bombay: Oxford University Press, 1970.
12. Raynaud, M.: Courbes sur une variété abélienne et points de torsion. *Invent. Math.* 71, 207–233 (1983).
13. Stöhr, K.-O., Voloch, J. F.: Weierstrass points and curves over finite fields. *Proc. London Math. Soc.* 52, 1–19 (1986).
14. Takigawa, N.: Weierstrass points on compact Riemann surfaces with non-trivial automorphisms. *J. Math. Soc. Japan* 33, 235–246 (1981).

Note Added in Proof. The authors would like to thank Dan Abramovich for pointing out that their conditional Lemma 6 follows unconditionally from Theorem 4 in Kawamata, Y., On Bloch's conjecture, *Invent. Math.* 57, 97–100 (1980).