New York Journal of Mathematics

New York J. Math. **17** (2011) 163–172.

On the pre-image of a point under an isogeny and Siegel's theorem

Jonathan Reynolds

Abstract. Consider a rational point on an elliptic curve under an isogeny. Suppose that the action of Galois partitions the set of its pre-images into n orbits. It is shown that all but finitely many such points have their denominator divisible by at least n distinct primes. This generalizes Siegel's theorem and more recent results of Everest et al. For multiplication by a prime l, it is shown that if $n > 1$ then either the point is l times a rational point or the elliptic curve admits a rational l-isogeny.

Contents

1. Introduction

Let (E, O) denote an elliptic curve defined over a number field K with Weierstrass coordinate functions x, y. Siegel [24] proved that there are only finitely many $P \in E(K)$ with $x(P)$ belonging to the ring of integers $\mathcal{O}_K$. Given a finite set S of prime ideals of $\mathcal{O}_K$, the ring of S-integers in K is

$$\mathcal{O}_{KS} := \{x \in K : \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

Mahler [21] conjectured that there are finitely many $P \in E(K)$ with $x(P) \in \mathcal{O}_{KS}$ and proved his conjecture for $K = \mathbb{Q}$. Lang [19] gave a modernized exposition and proved Mahler's conjecture for number fields. A corollary to this is that there are finitely many $P \in E(K)$ with $f(P) \in \mathcal{O}_{KS}$, where

Received January 11, 2010.

2000 *Mathematics Subject Classification.* 11G05, 11A51.

Key words and phrases. Isogeny; elliptic curve; Siegel's theorem.

The author is supported by a Marie Curie Intra European Fellowship (PIEF-GA-2009-235210).

ISSN 1076-9803/2011

$f \in K(E)$ is any function having a pole at O (see Corollary 3.2.2 in Chapter IX of [26]). It is unknown how much further these S-integral points can be generalized before finiteness fails. For example, in [13] Everest and Mahé suggest that, in rank one subgroups, only the size of S has to be fixed and not the primes in the set.

Everest, Miller and Stephens [14] proved under an additional hypothesis for $K = \mathbb{Q}$ that there are finitely many multiples mP of a nontorsion point P which have the denominator of $x(mP)$ divisible by a single prime not belonging to a fixed set. These denominators generate an elliptic divisibility sequence, a genus-1 analogue of more classical sequences such as Fibonacci or Mersenne, and the hypothesis, which they called *magnified*, is that the nontorsion point P has a preimage defined in a number field of degree less than the degree of the isogeny (see Definition 2.1). The finiteness result concerning primes in elliptic divisibility sequences was generalized to number fields under an extra assumption that the pre-image lie in a Galois extension [12]. In what follows this extra assumption is removed, there is no restriction to rank one subgroups and, analogous to the results for integral points, S and f are arbitrary (see Theorem 1.1). Moreover, using the division polynomia ls of E, the magnified condition is replaced with a factorization criterion which can be checked more readily (see Theorem 2.4). This leads to a proof that the magnified condition often fails for prime degrees. In particular, either the magnified point is l times a rational point or the elliptic curve admits a rational l-isogeny for some prime l (see Theorem 1.2). Hence, Theorem 1.1 supports the afore mentioned conjecture of Everest and Mahé but Theorem 1.2 shows that Theorem 1.1 is unlikely to resolve the conjecture in general.

1.1. Division polynomials. Let E be an elliptic curve defined over a field K with Weierstrass coordinate functions x, y. For any integer $m \in \mathbb{Z}$, the mth division polynomial of E is the polynomial $\psi_m \in K[x, y] \subset K(E)$ as given on p. 39 of [1]. Moreover, $\psi_m^2 \in K[x]$ and there exists $\theta_m \in K[x]$ with

$$[m]x = \frac{\theta_m}{\psi_m^2}.$$

Given $P \in E(K)$, define $\delta_m^P \in K[x]$ by

$$\delta_m^P = \begin{cases} \theta_m - x(P)\psi_m^2 & \text{if } P \neq O \\ \psi_m^2 & \text{otherwise.} \end{cases}$$

The zeros of δ_m^P give the values of $x(R)$ for which $mR = P$.

Theorem 1.1. *Let K be a number field, S a finite set of prime ideals of $\mathcal{O}_K$ and $f \in K(E)$ a function having a pole at O. Suppose that δ_m^P has n factors over K for some $P \in E(K)$. Then for all but finitely many such points,*

$$\{\textit{primes } \mathfrak{p} \notin S : \operatorname{ord}_{\mathfrak{p}}(f(P)) < 0\} \tag{1.1}$$

contains at least n distinct primes.

By Siegel's theorem, along with the generalizations of it by Mahler and Lang, (1.1) contains at least one prime for all $P \in E(K)$ of sufficiently large height. So Theorem 1.1 extends Siegel's result whenever δ_m^P factorizes for some nontorsion point P. In Section 3 it shown that the finitely many exceptional points are m times a U-integral point for some finite set U of prime ideals of $\mathcal{O}_L$, where U and L are given explicitly. Quantitative results for the number of exceptional points can be found using [16].

In addition to being conjectured finite [12, 14, 15], the number of prime terms in an elliptic divisibility sequence coming from a minimal Weierstrass equation is believed to be uniformly bounded [10, 20]. Similarly, the number of terms without a primitive divisor is believed to be uniformly bounded [11, 17, 18]. There are also links between primitive divisors and extensions of Hilbert's tenth problem [5, 9]. However, most results in these directions have also used that δ_m^P factorizes for some m. Therefore it seems reasonable to give a detailed study of this condition.

Let K be a number field and E/K an elliptic curve. If Lehmer's conjecture holds (see [25]), and $\epsilon > 0$ is such that $\hat{h}(Q) \geq \frac{\epsilon}{[K(Q):K]}$ for all $Q \in E(\overline{K})$, then for all $R \in E(\overline{K})$ with $mR = P$ we have

$$[K(R) : K] \geq \frac{\epsilon}{\hat{h}(R)} = \frac{\epsilon}{\hat{h}(P)} m^2.$$

In other words, the number of factors of δ_m^P is bounded in terms of $\hat{h}(P)$, and independent of m. Sookdeo [27] has used a similar argument in a dynamical context. Since ϵ is unknown, Lehmer's conjecture gives no way of knowing whether or not δ_m^P is irreducible for all m. For prime degrees this issue is resolved by the following:

Theorem 1.2. *Let l be a prime, E an elliptic curve defined over a field K with* $\operatorname{char} K \nmid l$ *and P a K-rational point on E. Then either*

(i) *δ_l^P is irreducible, or*
(ii) *E admits a K-rational l-isogeny, or*
(iii) *$[l]^{-1}P$ contains a K-rational point.*

Given an elliptic curve $E/\mathbb{Q}$, the set of all curves E' isogenous to E over $\mathbb{Q}$ is finite (up to isomorphism) and is known as an isogeny class. Vélu's formulae [28] and the Weierstrass parameterization of the elliptic curve can be used to find an isogeny class. This is best illustrated in an algorithm developed by Cremona [7]. He has used his algorithm to produce tables of isogeny classes [6]. For each curve in the class, nontorsion generators of the Mordell–Weil group are also given. For a number field the primes which can occur as orders of isogenies have been well studied [3]. Applying a famous result of Mazur [22] gives:

Corollary 1.3. *Let $K = \mathbb{Q}$ and $P \in E(\mathbb{Q})$. If δ_l^P factorizes for some prime l then either P is l times a rational point, or $l \leq 19$, or l=37, 43, 67, or 163.*

The criterion in Corollary 1.3 can readily be checked using, for example, `MAGMA` [2] and so gives a way to determine if δ_l^P is irreducible for all primes l. What is known for composite m is discussed in Section 5; note that if δ_m^P factorizes then δ_d^P does not necessarily factorize for some proper divisor $d > 1$ of m, but counter-examples have only been found when $m = 4$.

Acknowledgement. The author thanks the referee for recommending various improvements in exposition.

2. The action of Galois on preimages

Let E be an elliptic curve defined over a field K with Weierstrass coordinate functions x, y. Given a Galois extension L/K, $\sigma \in \mathrm{Gal}(L/K)$ and $R \in E(L)$, $\sigma(R)$ is defined by $\sigma(R) = (x(R)^\sigma, y(R)^\sigma)$.

Definition 2.1 ([12])**.** Let K be a field, E/K an elliptic curve, $P \in E(K)$ and $\phi : E' \to E$ an isogeny. Suppose that E', ϕ and a point in $\phi^{-1}(P)$ are all defined over a finite extension L/K. If $[L : K] < \deg \phi$ then P is called *magnified*.

Below (Theorem 2.4) it is shown that for a perfect field (which includes the applications referenced above) the magnified condition is equivalent to δ_m^P factorizing for some m.

Lemma 2.2. *Assume that* $\mathrm{char}\, K \neq 2$ *or K is perfect. Suppose that $P \in E(K)$ is not a 2-torsion point, E'/K is an elliptic curve with Weierstrass coordinate functions x', y' and $\phi : E' \to E$ is an isogeny defined over K with $\phi(R) = P$ for some $R \in E'(\overline{K})$. Then $K(x'(R), y'(R)) = K(x'(R))$.*

Proof. Put $L = K(x'(R))$ and $L' = K(x'(R), y'(R))$. Then $[L' : L] \leq 2$. The assumptions on K make L'/L Galois. Suppose that $[L' : L] = 2$ and choose σ to be the generator of $\mathrm{Gal}(L'/L)$. Then $T = \sigma(R) - R$ is in the kernel of ϕ since $\sigma(\phi(R)) - \phi(R) = O$. But σ fixes $x'(R)$ so $R + T = \pm R$. Since P is not a 2-torsion point it follows that $\sigma(R) = R$ and $L' = L$. □

Lemma 2.3. *Assume that K is perfect. If $P \in E(K) \setminus E[2]$ is magnified by an isogeny $\phi : E' \to E$ of degree m then it is magnified by $[m]$.*

Proof. Suppose that E', ϕ and $Q \in \phi^{-1}(P)$ are all defined over a finite extension L/K with $[L : K] < m$. The dual $\hat{\phi} : E \to E'$ of ϕ is defined over L. Let $R \in \hat{\phi}^{-1}(Q)$. Lemma 2.2 gives $L(x(R), y(R)) = L(x(R))$. Now $f = x' \circ \hat{\phi} \in L(E) = L(x, y)$ is an even function. Hence, $f \in L(x)$ and $f(x) = x'(Q)$ gives a polynomial in $L[x]$ whose roots determine the values

of $x(R)$. Since $\#\hat{\phi}^{-1}(Q) \leq \deg \hat{\phi} = m$ and K is perfect, this polynomial cannot have an irreducible factor of degree larger than m. Thus,

$$[L(x(R)) : K] = [L(x(R)) : L][L : K] < m^2. \qquad \square$$

Theorem 2.4. *For K a perfect field and an elliptic curve E/K, $P \in E(K)$ is magnified if and only if δ_m^P factorizes over K for some m.*

Proof. If $P \in E[2]$ then $3P = P$ so δ_3^P factorizes. So assume that $P \notin E[2]$. By Lemma 2.3, P is magnified if and only if it is magnified by $[m]$ for some $m > 1$. The result now follows from Lemma 2.2. $\square$

3. Proof of Theorem 1.1

Proof of Theorem 1.1. Suppose firstly that f is an x-coordinate function relative to some Weierstrass equation for E. Fix a set of generators of $E(K)/mE(K)$ and for every P_j in the set, adjoin to K the coordinates of the points in $[m]^{-1}P_j$. Note that this finite extension L does not depend on P and that the splitting field of δ_m^P is contained within it. Let U be a finite set of prime ideals of $\mathcal{O}_L$ containing:

- those which lie above the ideals in S,
- those at which the coefficients of the Weierstrass equation are not integral,
- those which make $x(T)$ a U-integer for all nonzero $T \in E[m]$, and
- those which make $\mathcal{O}_{LU}$ a principal ideal domain.

By the Siegel–Mahler theorem we can assume that no $R \in [m]^{-1}P$ is U-integral. Write $x(R) = A_R/B_R^2$, where A_R and B_R are coprime in $\mathcal{O}_{LU}$. Then

$$x(P) = \frac{\theta_m(x(R))}{\psi_m^2(x(R))} = \frac{B_R^{2m^2}\theta_m\left(\frac{A_R}{B_R^2}\right)}{B_R^2\left(B_R^{2(m^2-1)}\psi_m^2\left(\frac{A_R}{B_R^2}\right)\right)}, \tag{3.1}$$

where B_R is coprime with the numerator. Let R and R' be two distinct points in $[m]^{-1}P$. Then $R' = R + T$ for some nonzero $T \in E[m]$. From the addition formula it can be seen that B_R and $B_{R'}$ are coprime in $\mathcal{O}_{LU}$. Any conjugate of a prime in the factorization of B_R over $\mathcal{O}_{LU}$ divides the denominator of some element in the orbit $\{\sigma(x(R)) : \sigma \in \mathrm{Gal}\,(L/K)\}$. Hence, using (3.1), the number of distinct prime ideals $\mathfrak{p} \notin S$ of $\mathcal{O}_K$ with $\mathrm{ord}_{\mathfrak{p}}(x(P)) < 0$ is at least equal to the number of factors of δ_m^P over K.

Finally, suppose that $f \in K(E)$ has a pole at O. We may assume that a Weierstrass equation for E/K is of the the form y^2 equal to a monic cubic in $K[x]$. Now $f \in K(C) = K(x, y)$ and $[K(x, y) : K(x)] = 2$ give

$$f(x, y) = \frac{\phi(x) + \psi(x)y}{\eta(x)},$$

where $\phi(x), \psi(x), \eta(x) \in K[x]$. Now $\operatorname{ord}_O(\phi) = \operatorname{ord}_O(x^{\deg \phi}) = -2 \deg \phi$. Similarly, $\operatorname{ord}_O(\psi) = -2 \deg \psi$ and $\operatorname{ord}_O(\eta) = -2 \deg \eta$. Since O is a pole of f,

$$\operatorname{ord}_O(f) = \operatorname{ord}_O(\phi + \psi y) - \operatorname{ord}_O(\eta) < 0.$$

But $\operatorname{ord}_O(\phi + \psi y) \geq \min\{\operatorname{ord}_O(\phi), \operatorname{ord}_O(\psi) + \operatorname{ord}_O(y)\}$ and $\operatorname{ord}_O(y) = -3$, thus

$$2 \deg \eta < \max\{2 \deg \phi, 2 \deg \psi + 3\}. \tag{3.2}$$

Enlarge S so that:

- $\mathcal{O}_{KS}$ is a a principal ideal domain;
- the coefficients of the Weierstrass equation are S-integers;
- $\phi(x), \psi(x), \eta(x) \in \mathcal{O}_{KS}[x]$ and their leading coefficients are S-units.

Write $(x(P), y(P)) = \left(A_P/B_P^2, C_P/B_P^3\right)$, where $A_P C_P$ and B_P are coprime in $\mathcal{O}_{KS}$. The condition (3.2) gives that B_P divides the denominator and is coprime the numerator of $f(P)$ in $\mathcal{O}_{KS}$. Thus the result follows from the case $f = x$ above. □

4. Proof of Theorem 1.2

The condition that $\operatorname{char} K \nmid m$ ensures that multiplication by m is separable and that $\#[m]^{-1}P = m^2$ (see 4.10 and 5.4 in Chapter III of [26]). Hence, for $P \notin E[2]$ the splitting of field of δ_m^P is Galois over K. Note that $(\mathbb{Z}/m\mathbb{Z})^2$ is isomorphic to $E[m]$ and bijective with $[m]^{-1}P$. The actions of Galois on $E[m]$ and on $[m]^{-1}P$ are described by homomorphisms $\operatorname{Gal}(\bar{K}/K) \to \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and $\operatorname{Gal}(\bar{K}/K) \to \operatorname{AGL}_2(\mathbb{Z}/m\mathbb{Z})$. Let G_m and $\mathcal{G}_m$ be the images of these maps. Consider the homomorphism $\alpha_m : \mathcal{G}_m \to G_m$ given by $\alpha_m((A, v)) = A$, where $A \in \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and $v \in (\mathbb{Z}/m\mathbb{Z})^2$.

Lemma 4.1. *Let E be an elliptic curve defined over a field K with* $\operatorname{char} K \neq 2$ *and let P be a K-rational point on E. Then either*

(i) *δ_2^P is irreducible,*
(ii) *P is a 2-torsion point,*
(iii) *$[2]^{-1}P$ has a K-rational point, or*
(iv) *P is the image of a K-rational point under a K-rational 2-isogeny.*

Proof. Let $2R = P$. Suppose that P is not a 2-torsion point. Using Lemma 2.2, let $L = K(x(R), y(R)) = K(x(R))$. If δ_2^P factorizes then we may choose R so that $[L : K] \leq 2$. If $[L : K] = 1$ then we are in case (iii). If $[L : K] = 2$ then choose $\sigma \in \operatorname{Gal}(L/K)$ to be nontrivial. Then $T = \sigma(R) - R$ is a 2-torsion point since $\sigma(2R) - 2R = \mathcal{O}$. Also $T \in E(K)$ since $\sigma(T) = -T$. Using this torsion point, we can construct an elliptic curve E'/K and a 2-isogeny $\phi : E \to E'$ with $\ker \phi = \{\mathcal{O}, T\}$ (see 8.2.1 of [4]). Moreover, both ϕ and its dual $\hat{\phi} : E' \to E$ are defined over K. Put $\phi(R) = Q$. It follows that $\sigma(Q) = \phi(\sigma(R)) = \phi(R + T) = \phi(R)$. Hence $Q \in E'(K)$ and $\hat{\phi}(Q) = P$. □

Note that, for $l = 2$, Lemma 4.1 is stronger than Theorem 1.2.

Proof of Theorem 1.2. If $P \in E[2]$ then we are in case (ii) or (iii). So assume that $P \notin E[2]$. If $\#\ker\alpha_l > 1$ then there exists a non zero l-torsion point T and $\sigma \in \mathrm{Gal}(\bar{K}/K)$ with $\sigma(R) = R + T$ for all $R \in [l]^{-1}P$. Hence $\tau\sigma\tau^{-1}(R) = R + \tau(T)$ for any $\tau \in \mathrm{Gal}(\bar{K}/K)$. If $\tau(T) \in \langle T\rangle$ for all $\tau \in \mathrm{Gal}(\bar{K}/K)$ then we are in case (ii) (see 4.12 and 4.13 in Chapter III of [26]). Otherwise, Galois acts transitively on $[l]^{-1}P$ and we are in case (i).

Thus, it remains to consider the case where $\alpha_l : \mathcal{G}_l \to G_l$ is an isomorphism and, by Lemma 4.1, $l > 2$. So α_l has an inverse $A \to (v \to Av + b_A)$ and the map $\beta_l : G_l \to E[l]$ given by $\beta_l(A) = b_A$ is a crossed homomorphism because $\beta_l(AB) = Ab_B + b_A$. The map β_l is said to be principal if for some fixed $v \in (\mathbb{Z}/l\mathbb{Z})^2$, $\beta_l(A) = Av - v$ for all $A \in G_l$. The group $H^1(G_l, E[l])$ is the quotient of the group of crossed homomorphisms $G_l \to E[l]$ and the group of principal ones. If l does not divide $\#G_l$ then the orders of G_l and $E[l]$ are coprime, so it follows that $H^1(G_l, E[l]) = 0$. So assume that $l \mid \#G_l$ and apply Proposition 15 of [23]. Either G_l is contained in a Borel subgroup and so we are in case (ii) since then the span of some point of order l is fixed by Galois, or G_l contains $H_l = \mathrm{SL}_2(\mathbb{Z}/l\mathbb{Z})$. For the second possibility construct an inflation-restriction sequence as in the proof of Lemma 4 in [8]. Note that H_l is normal since it is the kernel of the determinant on G_l. There is an exact sequence

$$0 \to H^1(G_l/H_l, E[l]^{H_l}) \to H^1(G_l, E[l]) \to H^1(H_l, E[l]).$$

For $l > 2$ the first cohomology group is trivial since $E[l]^{H_l}$ is trivial. By [8, Lemma 3], the third cohomology group is also trivial. Hence $H^1(G_l, E[l]) = 0$ and so β_l must be principal. But then $-v = -Av + \beta_l(A)$ for all $A \in G_l$ gives a fixed point for the action on $[l]^{-1}P$ so we are in case (iii). □

5. Multiplication by a composite

Let α_m be as in Section 4. A result for all composite m is:

Theorem 5.1. *Let $m > 1$ be a composite integer, E an elliptic curve defined over a field K with $\mathrm{char}\, K \nmid m$ and P a K-rational point on E. Then either*

(i) *δ_m^P is irreducible,*
(ii) *δ_d^P factorizes, where $d > 1$ is a proper divisor of m,*
(iii) *E admits a K-rational l-isogeny for some prime $l \mid m$, or*
(iv) *α_m is an isomorphism.*

Proof. If $\#\ker\alpha_m > 1$ then there exists a nonzero m-torsion point T and $\sigma \in \mathrm{Gal}(\bar{K}/K)$ with $\sigma(R) = R+T$ for all $R \in [m]^{-1}P$. If T has order d_1 then write $d_1 = ld_2$ where l is prime. Now $\sigma^{d_2}R = R + d_2T$ for all $R \in [m]^{-1}P$. Hence $\tau\sigma^{d_2}\tau^{-1}(R) = R + \tau(d_2T)$ for any $\tau \in \mathrm{Gal}(\bar{K}/K)$. Assume that $\tau(d_2T)$ is not a multiple of d_2T for some $\tau \in \mathrm{Gal}(\bar{K}/K)$; otherwise we are in case (iii). Then we can always find a Galois element which will take R to $R + T_1$, where T_1 is any l-torsion point. Assume that $P \notin E[2]$ and δ_m^P factorizes over K. Let $R_1, R_2 \in [m]^{-1}P$ correspond to roots of two

different factors. By assumption for any $T_1 \in E[l]$, $R_2 + T_1$ corresponds to a root of the same polynomial. Thus, $\rho(R_1) - R_2$ is not a l-torsion point for any $\rho \in \mathrm{Gal}(\bar{K}/K)$. So $\rho(lR_1) \neq lR_2$ for any $\rho \in \mathrm{Gal}(\bar{K}/K)$. Since $lR_1, lR_2 \in [m/l]^{-1}P$, Galois does not act transitively on $[m/l]^{-1}P$ and so we are in case (ii). □

Let D_m be the square-free polynomial whose roots are the x-coordinates of the points of order m on E. Then the action of Galois on $E[m]$ is given by the Galois group of D_m. Note that, for $m = 4$, all of the cases in Theorem 5.1 are necessary. For example, taking the curve "117a4" with $P = (8, 36)$ we see that (iv) is false because the Galois groups of δ_4^P and D_4 have different orders; moreover, only (iii) is true. For the curve "55696ba1" and the generator Cremona gives, by checking that the curve has a trivial isogeny class, we see that only (iv) is true. When m has two coprime proper divisors we have:

Theorem 5.2. *Suppose that $m > 1$ is composite and $m = d_1 d_2$ where d_1, d_2 are coprime proper divisors. If δ_m^P factorizes then either $\delta_{d_1}^P$ or $\delta_{d_2}^P$ factorizes.*

Proof. There exists $x, y \in \mathbb{Z}$ such that $xd_1 + yd_2 = 1$. Consider the homomorphism $\mathcal{G}_m \to \mathcal{G}_{d_1} \times \mathcal{G}_{d_2}$ given by $\rho \to (\rho, \rho)$. If ρ is in the kernel of this map then $\rho(d_2 R) = d_2 R$ and $\rho(d_1 R) = d_1 R$ for all $R \in [m]^{-1}P$. But then $x\rho(d_1 R) + y\rho(d_2 R) = \rho(R) = R$ for all $R \in [m]^{-1}P$. So $\mathcal{G}_m \cong \mathcal{G}_{d_1} \times \mathcal{G}_{d_2}$. Assume that $P \notin E[2]$ and $\delta_{d_1}^P$ is irreducible. Then for any $R \in [m]^{-1}P$ and $T \in E[d_1]$ there exists $\sigma \in \mathcal{G}_{d_1}$ with $\sigma(d_2 R) = d_2 R + T$. Define (σ, Id) by $(\sigma, \mathrm{Id})(R) = n_2\sigma(d_2 R) + n_1(d_1 R)$. Since $\mathcal{G}_m \cong \mathcal{G}_{d_1} \times \mathcal{G}_{d_2}$, $(\sigma, \mathrm{Id}) \in \mathcal{G}_m$. For any $R \in [m]^{-1}P$, $(\sigma, \mathrm{Id})(R) = R + n_2 T$. So, since d_1 and n_2 are coprime, R and $R+T$ must correspond to roots of the same polynomial. Suppose that δ_m^P factorizes and let $R_1, R_2 \in [m]^{-1}P$ correspond to roots of two different factors. Then $\rho(R_1) - R_2 \notin E[d_1]$ or $\rho(d_1 R_1) \neq \rho(d_1 R_2)$ for all $\rho \in \mathrm{Gal}(\bar{K}/K)$. Since $d_1 R_1, d_1 R_2 \in [d_2]^{-1}P$ it follows that $\delta_{d_2}^P$ factorizes. □

Hence the case where m is a composite prime power remains. Although no further results could be proven it is perhaps worth noting that, in all of Cremona's data, an example where (i) and (ii) are false in Theorem 5.1 could not be found when $4 < m \leq 25$.

References

[1] Blake, Ian F.; Seroussi, Gadiel; Smart, Nigel P. Elliptic curves in cryptography. London Mathematical Society Lecture Note Series, 265. *Cambridge University Press, Cambridge*, 2000. xvi+204 pp. ISBN: 0-521-65374-6. MR1771549 (2001i:94048), Zbl 0937.94008.

[2] Bosma, Wieb; Cannon, John; Playoust, Catherine. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997), no. 3-4, 235–265. MR1484478, Zbl 0898.68039.

[3] Brown, M. L. A note on orders of isogenies of elliptic curves. *Bull. London Math. Soc.* **20** (1988), no. 3, 221–227. MR931181 (89g:11044), Zbl 0667.14012.

[4] Cohen, Henri. Number theory. Vol. I. Tools and Diophantine equations. Graduate Texts in Mathematics, 239. *Springer, New York*, 2007. xxiv+650 pp. ISBN: 978-0-387-49922-2. MR2312337 (2008e:11001), Zbl 1119.11001.

[5] Cornelissen, Gunther; Zahidi, Karim. Elliptic divisibility sequences and undecidable problems about rational points. *J. Reine Angew. Math.* **613** (2007), 1–33. MR2377127 (2009h:11196), Zbl 1178.11076.

[6] Cremona, J. E. Elliptic curve data, available at `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/`.

[7] Cremona, J. E. Algorithms for modular elliptic curves. Second edition. *Cambridge University Press, Cambridge*, 1997. vi+376 pp. ISBN: 0-521-59820-6. MR1628193 (99e:11068), Zbl 0872.14041.

[8] Djabri, Z.; Schaefer, Edward F.; Smart, N. P. Computing the p-Selmer group of an elliptic curve. *Trans. Amer. Math. Soc.* **352** (2000), no. 12, 5583–5597. MR1694286 (2001b:11047), Zbl 0954.11022.

[9] Eisenträger, Kirsten; Everest, Graham. Descent on elliptic curves and Hilbert's tenth problem. *Proc. Amer. Math. Soc.* **137** (2009), no. 6, 1951–1959. MR2480276 (2009k:11201), Zbl pre05558381.

[10] Everest, Graham; Ingram, Patrick; Mahé, Valéry; Stevens, Shaun. The uniform primality conjecture for elliptic curves. *Acta Arith.* **134** (2008), no. 2, 157–181. MR2429645 (2009d:11088), Zbl pre05306449.

[11] Everest, Graham; Ingram, Patrick; Stevens, Shaun. Primitive divisors on twists of Fermat's cubic. *LMS J. Comput. Math.* **12** (2009), 54–81. MR2486632 (2010b:11060).

[12] Everest, Graham; King, Helen. Prime powers in elliptic divisibility sequences. *Math. Comp.* **74** (2005), no. 252, 2061–2071 (electronic). MR2164113 (2006d:11057), Zbl 1080.11043.

[13] Everest, Graham; Mahé, Valéry. A generalization of Siegel's theorem and Hall's conjecture. *Experiment. Math.* **18** (2009), no. 1, 1–9. MR2548983 (2010i:11082), Zbl pre05587795.

[14] Everest, Graham; Miller, Victor; Stephens, Nelson. Primes generated by elliptic curves. *Proc. Amer. Math. Soc.* **132** (2004), no. 4, 955–963 (electronic). MR2045409 (2005a:11076), Zbl 1043.11051.

[15] Everest, Graham; Reynolds, Jonathan; Stevens, Shaun. On the denominators of rational points on elliptic curves. *Bull. Lond. Math. Soc.* **39** (2007), no. 5, 762–770. MR2365225 (2008g:11098), Zbl 1131.11034.

[16] Gross, Robert; Silverman, Joseph. S-integer points on elliptic curves. *Pacific J. Math.* **167** (1995), no. 2, 263–288. MR1328329 (96c:11057), Zbl 0824.11038.

[17] Ingram, Patrick. Elliptic divisibility sequences over certain curves. *J. Number Theory* **123** (2007), no. 2, 473–486. MR2301226 (2007k:11090), Zbl 1170.11010.

[18] Ingram, Patrick; Silverman, Joseph H. Uniform estimates for primitive divisors in elliptic divisibility sequences. to appear in a forthcoming memorial volume for Serge Lang, published by Springer-Verlag.

[19] Lang, Serge. Integral points on curves. *Inst. Hautes Études Sci. Publ. Math.* **6** (1960), 27–43. MR0130219 (24 #A86), Zbl 0112.13402.

[20] Mahé, Valéry. Prime power terms in elliptic divisibility sequences. arXiv:1002.4202v1.

[21] Mahler, Kurt. Über die rationalen Punkte auf Kurven vom Geschlecht Eins. *J. Reine Angew. Math.* **170** (1934), 168–178. JFM 60.0159.03.

[22] Mazur, B. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.* **44** (1978), no. 2, 129–162. MR482230 (80h:14022), Zbl 0386.14009.

[23] Serre, Jean-Pierre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), no. 4, 259–331. MR0387283 (52 #8126), Zbl 0235.14012.

[24] Siegel, Carl Ludwig. Über einige Anwendungen Diophantischer Approximationen. *Abh. Preussischen Akademie der Wissenshaften* (1929).

[25] Silverman, Joseph H. A lower bound for the canonical height on elliptic curves over abelian extensions. *J. Number Theory* **104** (2004), no. 2, 353–372. MR2029512 (2004k:11106), Zbl 1053.11052.

[26] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. *Springer, Dordrecht*, 2009. xx+513 pp. ISBN: 978-0-387-09493-9. MR2514094 (2010i:11005), Zbl 1194.11005.

[27] Sookdeo, Vijay A. Integer points in backward orbits. arXiv:0808.2679.

[28] Vélu, Jacques. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), A238–A241. MR0294345 (45 #3414), Zbl 0225.14014.

Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht, Nederland
J.M.Reynolds@uu.nl

This paper is available via http://nyjm.albany.edu/j/2011/17-9.html.