
Article:
Khawaja, M. and Siksek, S. (2024) Primitive algebraic points on curves. Research in Number Theory, 10 (3). 57. ISSN: 2363-9555

https://doi.org/10.1007/s40993-024-00543-4

M. Khawaja, S. Siksek *Res. Number Theory (2024) 10:57*
https://doi.org/10.1007/s40993-024-00543-4

Research in Number Theory

RESEARCH

Primitive algebraic points on curves

Maleeha Khawaja[1] and Samir Siksek[2*]

*Correspondence:
s.siksek@warwick.ac.uk
[2]Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK
Full list of author information is available at the end of the article
Khawaja is supported by an EPSRC studentship from the University of Sheffield (EP/T517835/1). Siksek is supported by the EPSRC grant *Moduli of Elliptic curves and Classical Diophantine Problems* (EP/S031537/1)

Abstract

A number field K is primitive if K and $\mathbb{Q}$ are the only subextensions of K. Let C be a curve defined over $\mathbb{Q}$. We call an algebraic point $P \in C(\overline{\mathbb{Q}})$ primitive if the number field $\mathbb{Q}(P)$ is primitive. We present several sets of sufficient conditions for a curve C to have finitely many primitive points of a given degree d. For example, let $C/\mathbb{Q}$ be a hyperelliptic curve of genus g, and let $3 \leq d \leq g-1$. Suppose that the Jacobian J of C is simple. We show that C has only finitely many primitive degree d points, and in particular it has only finitely many degree d points with Galois group S_d or A_d. However, for any even $d \geq 4$, a hyperelliptic curve $C/\mathbb{Q}$ has infinitely many imprimitive degree d points whose Galois group is a subgroup of $S_2 \wr S_{d/2}$.

Keywords: Curves, Jacobians, Primitive points

Mathematics Subject Classification: 11G30

1 Introduction

By a **curve** C over a field K we mean a smooth projective and geometrically irreducible variety defined over K having dimension 1. We say that a curve C defined over a field K is **hyperelliptic** if the genus of C is at least 2 and C admits a degree 2 morphism $C \to \mathbb{P}^1$, defined over K, which we shall refer to as the **hyperelliptic morphism**. We say that C/K has K-**gonality** m if m is the least degree of a non-constant morphism $\pi : C \to \mathbb{P}^1$ defined over K. Thus, for example, a hyperelliptic curve defined over K has K-gonality 2. We say that C/K is **bielliptic** if its genus is at least 2 and it admits a degree 2 morphism $C \to E$, defined over K, where E is a curve of genus 1.

Recall that a number field K is called **imprimitive** if there is some subextension $\mathbb{Q} \subsetneq L \subsetneq K$; if there is no such subextension then K is called **primitive**. Now let C be a curve defined over $\mathbb{Q}$. Let $P \in C$ be an algebraic point; i.e. $P \in C(\overline{\mathbb{Q}})$. We say P has **degree** d if the number field $\mathbb{Q}(P)$ has degree d. We say that P is **primitive** if the number field $\mathbb{Q}(P)$ is primitive, otherwise we say that P is **imprimitive**. A degree d point $P \in C(\overline{\mathbb{Q}})$ is called $\mathbb{P}^1$-**isolated** if there is no degree d non-constant morphism $\phi : C \to \mathbb{P}^1$, defined over $\mathbb{Q}$, such that P is in the preimage of an element of $\mathbb{P}^1(\mathbb{Q})$. The notion of isolated points was introduced in [7] and has become important in understanding low degree points on curves, particularly on modular curves (e.g. [8,18]). It is easy to see that if $d < m$, where m is the $\mathbb{Q}$-gonality of C, then P is $\mathbb{P}^1$-isolated. A key observation we make in this paper is that primitive points are often $\mathbb{P}^1$-isolated even if the degree is greater than the gonality.

Theorem 1 *Let C be a curve defined over $\mathbb{Q}$ with genus g and $\mathbb{Q}$-gonality $m \geq 2$. Let $d \geq 2$ be an integer satisfying*

$$d \neq m, \qquad d < 1 + \frac{g}{m-1}. \tag{1}$$

Let $P \in C(\overline{\mathbb{Q}})$ be a degree d point on C that is not $\mathbb{P}^1$-isolated. Then $\mathbb{Q}(P)$ contains a subfield of index d' satisfying

$$1 < d' < d, \qquad d' \mid \gcd(d, m).$$

In particular, the following hold.

(I) If $\gcd(d, m) = 1$ or d is prime then any degree d point $P \in C(\overline{\mathbb{Q}})$ is $\mathbb{P}^1$-isolated.
(II) If $P \in C(\overline{\mathbb{Q}})$ is a primitive degree d point, then P is $\mathbb{P}^1$-isolated.

Under certain additional assumptions on the Jacobian J of the curve C, it is possible to conclude finiteness of primitive degree d points on C.

Theorem 2 *Let C be a curve defined over $\mathbb{Q}$ with genus g and $\mathbb{Q}$-gonality $m \geq 2$. Let $d \geq 2$ be an integer satisfying (1). Let J be the Jacobian of C. Suppose either of the following hold:*

(a) $J(\mathbb{Q})$ is finite;
(b) or $d \leq g - 1$, and $A(\mathbb{Q})$ is finite for every abelian subvariety $A/\mathbb{Q}$ of J of dimension $\leq d/2$.

Then C has finitely many primitive degree d points. Moreover, if $\gcd(d, m) = 1$ or d is prime then C has finitely many degree d points.

Observe that, for $d \leq g - 1$, assumption (b) is trivially satisfied if J is simple. We moreover note that the inequality $d \leq g - 1$ in (b) follows immediately from (1) if $m \geq 3$.

Example 3 We consider the modular curve $X_0(239)$ which has genus $g = 20$ and $\mathbb{Q}$-gonality $m = 6$ (see [32, Table 3]). We consider degree d points for $d = 2, 3, 4$; we note that (1) is satisfied for these values of d. A straightforward computation in `Magma`, which makes use of modular symbols algorithms due to Cremona [12] and Stein [40], shows that the Jacobian $J_0(239)$ of $X_0(239)$ factors as

$$J_0(239) \sim \mathcal{A}_3 \times \mathcal{A}_{17},$$

where $\mathcal{A}_3$ and $\mathcal{A}_{17}$ are simple abelian varieties of dimension 3 and 17, respectively. Moreover $\mathcal{A}_{17}$ has analytic rank 0, and $\mathcal{A}_3$ has positive analytic rank. Assuming the Birch and Swinnerton–Dyer conjecture, $J_0(239)(\mathbb{Q})$ is infinite, and so hypothesis (a) of Theorem 2 is not satisfied. However, $J_0(239)$, clearly satisfies hypothesis (b) for $d = 2, 3, 4$. By Theorem 2, we conclude that $X_0(239)$ has finitely many quadratic, cubic and primitive quartic points.

We point out the following theorem [17, Proposition 2.3] which gives a stronger conclusion than Theorem 2 under different assumptions.

Theorem 4 *(Derickx and Sutherland) Let C be a curve defined over $\mathbb{Q}$ with genus g and $\mathbb{Q}$-gonality $m \geq 2$. Let J be the Jacobian of C and suppose $J(\mathbb{Q})$ is finite. Suppose $d < m$. Then C has finitely many degree d points.*

The following corollary to Theorem 2 is obtained by restricting Theorem 2 and its proof to the hyperelliptic case.

Corollary 5 *Let C be a hyperelliptic curve defined over $\mathbb{Q}$ with genus g. Let J be the Jacobian of C and let d be a positive integer. Suppose either of the following hold:*

(a) $3 \le d \le g$ *and* $J(\mathbb{Q})$ *is finite;*
(b) or $3 \le d \le g-1$, *and* $A(\mathbb{Q})$ *is finite for every abelian subvariety* $A/\mathbb{Q}$ *of* J *of dimension* $\le d/2$.

Then C has finitely many primitive degree d points. More precisely, the following hold.

(i) If d is odd, then C has finitely many degree d points.
(ii) If d is even, then for all but finitely many degree d points P on C, the field $\mathbb{Q}(P)$ contains a subfield of index 2.

We note that Gunther and Morrow [21, Proposition 2.6] prove that conclusions (i) and (ii) hold for 100% of genus g hyperelliptic curves over $\mathbb{Q}$ with a rational Weierstrass point, provided only that $d \le g-1$, though their proof is rather different.

In contrast to Corollary 5 we note the following.

Lemma 6 *Let C be a hyperelliptic curve defined over $\mathbb{Q}$. Let $d \ge 4$ be an even integer. Then C has infinitely many imprimitive degree d points.*

Proof We may suppose C has an affine model

$$C \ : \ Y^2 = F(X) \tag{2}$$

where $F \in \mathbb{Q}[X]$ is a squarefree polynomial. Let L be any number field of degree $d/2$ and choose $\theta \in L$ such that $L = \mathbb{Q}(\theta)$. By Faltings' theorem, $C(L)$ is finite. Thus we may choose some $a \in \mathbb{Q}$ such that $F(\theta + a)$ is a non-square in L. Let $P = (\theta + a, \sqrt{F(\theta + a)})$. This is a degree d point on C, and is imprimitive as $\mathbb{Q}(P)$ contains the index 2 subfield L. □

Let C be a curve defined over $\mathbb{Q}$. Let $P \in C$ be an algebraic point; i.e. $P \in C(\overline{\mathbb{Q}})$. We define the **Galois group of** P to be the Galois group of the Galois closure of $\mathbb{Q}(P)/\mathbb{Q}$. A degree $d \ge 4$ point whose Galois group is S_d or A_d is primitive (Lemma 29). Thus if d is an even integer and if C, d satisfy the hypotheses of Corollary 5 then C has only finitely many degree d points with Galois group S_d or A_d. However, it follows from the proof of Lemma 6 that C has infinitely many degree d points with Galois group contained in $S_2 \wr S_{d/2}$. In a separate paper [27] we explore Galois groups of algebraic points in more detail. For now, we content ourselves with the following result.

Theorem 7 *Let C be a hyperelliptic curve defined over $\mathbb{Q}$ with genus 2 or 3. Let J be the Jacobian of C and suppose that $J(\mathbb{Q})$ is trivial. Then C has no quartic points with Galois group S_4 or A_4. However, C has infinitely many quartic points with Galois group contained in D_4.*

The above results exploit the gonality map $C \to \mathbb{P}^1$ to make deductions about low degree primitive points. However, the existence of a low degree map $C \to C'$ with C' of positive genus also makes it more likely for low degree primitive algebraic points on C to be $\mathbb{P}^1$-isolated, as illustrated by the following theorem.

Theorem 8 *Let $\pi : C \to C'$ be a morphism of curves defined over $\mathbb{Q}$ of degree $m \geq 2$. Write g, g' for the genera of C, C' respectively, and suppose $g' \geq 1$. Let $d \geq 2$ be an integer satisfying*

$$d < 1 + \frac{g - mg'}{m - 1}. \tag{3}$$

Let $P \in C(\overline{\mathbb{Q}})$ be a degree d point on C that is not $\mathbb{P}^1$-isolated. Then $\mathbb{Q}(P)$ contains a subfield of index d' satisfying

$$1 < d' < d, \qquad d' \mid \gcd(d, m).$$

In particular, the following hold.

(I) If $\gcd(d, m) = 1$ or d is prime then any degree d point $P \in C(\overline{\mathbb{Q}})$ is $\mathbb{P}^1$-isolated.
(II) If $P \in C(\overline{\mathbb{Q}})$ is a primitive degree d point, then P is $\mathbb{P}^1$-isolated.

Theorem 9 *Let $\pi : C \to C'$ be a morphism of curves defined over $\mathbb{Q}$ of degree $m \geq 2$. Write g, g' for the genera of C, C' respectively, and suppose $g' \geq 1$. Let $d \geq 2$ be an integer satisfying (3). Write J for the Jacobian of C and suppose $J(\mathbb{Q})$ is finite. Then C has finitely many primitive degree d points. Moreover, if $\gcd(d, m) = 1$ or d is prime then C has finitely many degree d points.*

Example 10 We illustrate Theorem 9 by giving an example. Consider the modular curve $X_1(45)$. The `LMFDB` [42] gives the following information:

(a) $X_1(45)$ has genus 41;
(b) $X_1(45)$ is a degree 3 cover of a genus 9 curve (the latter has `LMFDB` label `45.576.9-45.a.4.1`);
(c) $J_1(45)$ has analytic rank 0.

Write $J = J_1(45)$. As J has analytic rank 0, a theorem of Kato [25, Corollary 14.3] implies that the Mordell–Weil group $J(\mathbb{Q})$ is finite. Thus, by Theorem 9, the curve $X_1(45)$ has only finitely many degree d points for $d = 2, 3, 4, 5, 7$, and only finitely many primitive degree d points for $d = 6$. We point out that the $\mathbb{Q}$-gonality of $X_1(45)$ appears to be currently unknown; according to the `LMFDB` it belongs to the interval $9 \leq \gamma \leq 18$.

Applying Theorem 9 and its proof to bielliptic curves gives the following.

Corollary 11 *Let C be a bielliptic curve defined over $\mathbb{Q}$ with genus g. Let J be the Jacobian of C and suppose $J(\mathbb{Q})$ is finite. Let $2 \leq d \leq g - 2$. Then C has finitely many primitive degree d points. More precisely, the following hold.*

(i) If $d = 2$ or d is odd, then C has finitely many degree d points.
(ii) If $d \geq 4$ and even, then for all but finitely many degree d points P on C, the field $\mathbb{Q}(P)$ contains a subfield of index 2.

The above theorems are concerned with finiteness criteria for low degree primitive points. In the opposite direction, we show that if the degree d is sufficiently large compared to the genus, then there are infinitely many primitive degree d points, provided there is at least one such point.

Theorem 12 *Let $C/\mathbb{Q}$ be a curve. Let $d \geq g+1$ where g is the genus of C. Suppose there exists a primitive degree d point on C. Then there are infinitely many primitive degree d points on C.*

The paper is organized as follows. In Section 2 we review some standard results regarding Riemann–Roch spaces and we use these to prove Theorem 7. In Section 3 we recall the Castelnuovo–Severi theorem and use it to give proofs of Theorems 1 and 8. In Section 4 we give criteria for when a complete linear series does not contain any primitive divisors (a primitive divisor is simply the Galois orbit of a primitive algebraic point). Let C satisfy the hypotheses of either Theorem 2 or Theorem 9, and write $C^{(d)}$ for the d-th symmetric power of C. In Section 5, using a powerful theorem of Faltings, we show that $C^{(d)}(\mathbb{Q})$ may be decomposed as a finite union of complete linear series. In Section 6 we prove Theorems 2 and 9 and their corollaries, making use of the results developed in previous sections. In Section 7 we recall the relationship between primitive extensions and primitive group actions, and we use this together with Hilbert's irreducibility theorem to give a proof of Theorem 12. Finally, in Sections 8 and 9 we give consequences of Theorems 2 and 9 (and their proofs) for the modular curves $X_1(N)$ and $X_0(N)$ for certain small N.

We are grateful to Nils Bruin, Victor Flynn, Samuel Le Fourn, David Loeffler, Filip Najman, Petar Orlić, Damiano Testa and Bianca Viray for helpful discussions, and to the referees for suggesting many improvements.

2 Proof of Theorem 7

Let C be a curve defined over $\mathbb{Q}$. When we speak of divisors on C we in fact mean rational divisors: a **divisor** on $C/\mathbb{Q}$ is a finite formal integral linear combination $D = \sum a_i P_i$ of algebraic points P_i that is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We call this divisor **effective** and write $D \geq 0$ if and only if $a_i \geq 0$ for all i. An **irreducible divisor** is an effective divisor that cannot be written as the sum of two non-zero effective divisors. Thus an effective degree d divisor D is irreducible if and only if there is a degree d point $P \in C(\overline{\mathbb{Q}})$ such that $D = P_1 + P_2 + \cdots + P_d$ where $\{P_1, \ldots, P_d\}$ is the Galois orbit of P. We say that D is **the irreducible divisor corresponding** to P.

For a divisor D on C we denote by $L(D)$ the corresponding **Riemann–Roch space** defined by

$$L(D) \;=\; \{0\} \cup \{f \in \mathbb{Q}(C)^\times \;:\; \mathrm{div}(f) + D \geq 0\},$$

and we let $\ell(D) = \dim L(D)$. We shall make frequent use of the Riemann–Roch theorem [3, page 13] which asserts that

$$\ell(D) - \ell(K_C - D) \;=\; \deg(D) - g + 1; \tag{4}$$

here K_C is any canonical divisor on C, and g is the genus of C. Recall that $\deg(K_C) = 2g-2$. Therefore, if $\deg(D) \geq 2g-1$ then $K_C - D$ has negative degree and cannot be linearly equivalent to an effective divisor. In that case $\ell(K_C - D) = 0$.

We shall also require Clifford's theorem [22, Theorem IV.5.4] on special effective divisors. Recall that an effective divisor D is **special** if $\ell(K_C - D) > 0$.

Theorem 13 *(Clifford) Let D be an effective special divisor on a curve C. Then*

$$\ell(D) \;\leq\; \frac{\deg(D)}{2} + 1.$$

Moreover, equality occurs if and only if $D = 0$, or D is a canonical divisor, or C is hyperelliptic and D is a multiple of a hyperelliptic divisor.

Recall that a hyperelliptic curve C is equipped with a degree 2 morphism $\pi : C \to \mathbb{P}^1$; a **hyperelliptic divisor** on C is $\pi^*(\alpha)$ for any $\alpha \in \mathbb{P}^1(\mathbb{Q})$.

Proof of Theorem 7 Let C be as in the statement of Theorem 7. We may suppose C has an affine model as in (2) where $F \in \mathbb{Q}[X]$ is a squarefree polynomial of degree $2g+1$ or $2g+2$. It follows from Lemma 6 and its proof that C has infinitely many quartic points with Galois group contained in D_4. To complete the proof it is enough to show that there are no quartic points on C with Galois group S_4 or A_4.

If $\deg(F) = 2g+1$ we let ∞ be the single point at infinity on this model, and write $D_0 = 4\infty$. If $\deg(F) = 2g+2$ we let ∞_+ and ∞_- be the two points at infinity, and write $D_0 = 2\infty_+ + 2\infty_-$. In either case D_0 is twice a hyperelliptic divisor.

Let P be a degree 4 point on C, and let D be the corresponding irreducible divisor. Since $J(\mathbb{Q})$ is trivial, $D - D_0 \sim 0$ where $\sim$ denotes linear equivalence on C. That is,

$$D = D_0 + \mathrm{div}(f),$$

where $f \in L(D_0)$. We claim that $1, X, X^2$ is a $\mathbb{Q}$-basis of $L(D_0)$. Let us first assume our claim and use it to complete the proof. Thus $f = a_0 + a_1X + a_2X^2$ for some $a_0, a_1, a_2 \in \mathbb{Q}$. Moreover, f is non-constant as $D \neq D_0$. Now P is a zero of f. Hence $X(P)$ satisfies the non-constant polynomial $a_0 + a_1U + a_2U^2 \in \mathbb{Q}[U]$. Since $\mathbb{Q}(P) = \mathbb{Q}(X(P), Y(P))$ is a quartic field, and $Y(P)^2 = F(X(P))$, we see that $\mathbb{Q}(X(P))$ is quadratic and contained in the quartic field $\mathbb{Q}(P)$. Therefore the Galois group of P is neither S_4 nor A_4.

It remains to prove our claim. Note that X has a double pole at infinity and no other poles if $\deg(F) = 2g+1$; and also X has a simple pole at ∞_+ and ∞_-, and has no other poles if $\deg(F) = 2g+2$. Therefore, $1, X, X^2$ belong to $L(D_0)$, and so $\ell(D_0) \geq 3$. It is enough to show that $\ell(D_0) = 3$. We now make use of our assumption that $g = 2$ or 3. If $g = 2$ then Riemann–Roch immediately gives $\ell(D_0) = 3$. Suppose $g = 3$. Then Riemann–Roch tells us that D_0 is special, and since it is twice a hyperelliptic divisor, Clifford's theorem gives the equality $\ell(D_0) = 3$. □

3 Proofs of Theorems 1 and 8

We start by recalling the classical Castelnuovo–Severi theorem.

Theorem 14 *(Castelnuovo–Severi theorem) Let k be a perfect field, and let X, Y, Z be curves over k. Denote the genera of these curves by $g(X)$, $g(Y)$ and $g(Z)$ respectively. Let $\pi_Y : X \to Y$ and $\pi_Z : X \to Z$ be non-constant morphisms defined over k, having degrees m and n respectively. Suppose*

$$g(X) > m \cdot g(Y) + n \cdot g(Z) + (m-1)(n-1). \tag{5}$$

Then there is a curve X' defined over k, and a morphism $X \to X'$ also defined over k and of degree > 1 through which both π_Y and π_Z factor.

Proof We are unable to find a reference that gives the precise statement that we need. Indeed the theorem is most often given in the context of complex Riemann surfaces (for example [1]), or the field of definition of the morphism $X \to X'$ is not mentioned (for example [24, Corollary]). We therefore give an explanation of how the version above

follows straightforwardly from a proof due to Mattuck and Tate [28] of the Castelnuovo–Severi inequality.

Let $S = Y \times Z$. Given two divisors D, D' on the surface S, we denote their intersection number by $D \cdot D'$. Let D be the image of X on S under the morphism $(\pi_Y, \pi_Z) : X \to S$, and write $h : X \to D$ for the induced map. Clearly the curve D and the map h are defined over k. Let $u : D \to Y$ and $v : D \to Z$ be the restrictions of the projections $Y \times Z \to Y$ and $Y \times Z \to Z$ to D. Then $\pi_Y = u \circ h$ and $\pi_Z = v \circ h$. We claim that $\deg(h) > 1$. The theorem follows from our claim on letting X' be the normalization of D.

We prove our claim by contradiction. Suppose $\deg(h) = 1$. The h is a birational map, and $g(D) = g(X)$ (where $g(D)$ denotes the geometric genus of D). Mattuck and Tate [28, page 296] show that

$$D \cdot D \ \leq \ 2mn, \qquad D \cdot K_S \ = \ (2g(Y) - 2)m + (2g(Z) - 2)n, \tag{6}$$

where K_S denotes any canonical divisor on S (the inequality on the left is itself referred to as the Castelnuovo–Severi inequality). By the adjunction formula for surfaces [22, Exercise V.1.3] we have

$$2p_a(D) - 2 \ = \ D \cdot (D + K_S),$$

where $p_a(D)$ is the arithmetic genus of D. Thus, from (6),

$$p_a(D) \ \leq \ g(Y)m + g(Z)n + (m-1)(n-1).$$

However, since the geometric genus is bounded by the arithmetic genus,

$$g(X) \ = \ g(D) \ \leq \ p_a(D) \ \leq \ g(Y)m + g(Z)n + (m-1)(n-1).$$

contradicting assumption (5). This establishes our claim. □

Proof of Theorem 1 Let P be a degree d point on C and suppose P is not $\mathbb{P}^1$-isolated. Thus there is a degree d map $f : C \to \mathbb{P}^1$, defined over $\mathbb{Q}$, such that $f(P) = \alpha \in \mathbb{P}^1(\mathbb{Q})$. Observe that $f^*(\alpha)$ consists precisely of the Galois orbit of P. Let $m \geq 2$ be the $\mathbb{Q}$-gonality of C; thus in particular, there is a morphism $\pi : C \to \mathbb{P}^1$ defined over $\mathbb{Q}$, of minimal degree $m \geq 2$. As m and d satisfy (1), the Castelnuovo–Severi theorem immediately implies that the morphisms f, π must simultaneously factor through a common non-trivial morphism of curves. We obtain a commutative diagram of non-constant morphisms of curves

$$\begin{array}{ccccc} & & C & & \\ & \swarrow^{f} & \downarrow{\scriptstyle h} & \searrow^{\pi} & \\ \mathbb{P}^1 & \xleftarrow[u]{} & Y & \xrightarrow[v]{} & \mathbb{P}^1 \end{array} \tag{7}$$

defined over $\mathbb{Q}$, where $\deg(h) > 1$. Write $d' = \deg(h)$. Then d' divides both $d = \deg(f)$ and $m = \deg(\pi)$, so $d' \mid \gcd(d, m)$. If $d' = d$, then $d \mid m$. However, $m \leq d$ by the minimality of m. Therefore $m = d$ contradicting (1). We deduce that $d' < d$.

Let $Q = h(P) \in Y$. Since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts transitively on $f^*(\alpha) \ni P$, it acts transitively on $u^*(\alpha) \ni Q$. Hence Q has degree $\deg(u) = d/d'$ and $\mathbb{Q}(Q) \subseteq \mathbb{Q}(P)$. Thus the field $\mathbb{Q}(P)$ of degree d contains the subfield $\mathbb{Q}(Q)$ of index d'. The theorem follows. □

Proof of Theorem 8 This proof is similar to the proof of Theorem 1. As before, let P be a degree d point on C and suppose that P is not $\mathbb{P}^1$-isolated. Thus there is a degree d map $f : C \to \mathbb{P}^1$, defined over $\mathbb{Q}$, such that $f(P) = \alpha \in \mathbb{P}^1(\mathbb{Q})$.

From assumption (3), the Castelnuovo–Severi theorem gives a commutative diagram of non-constant morphisms of curves

$$\begin{array}{ccccc} & & C & & \\ & \swarrow^{f} & \downarrow{\scriptstyle h} & \searrow^{\pi} & \\ \mathbb{P}^1 & \xleftarrow[u]{} & Y & \xrightarrow[v]{} & C' \end{array} \tag{8}$$

defined over $\mathbb{Q}$, where $\deg(h) > 1$. As before we let $d' = \deg(h)$. If $\deg(u) = 1$ then $Y \cong \mathbb{P}^1$ which contradicts the existence of a non-constant morphism v from Y to the curve C' having genus $g' \geq 1$. Thus $\deg(u) > 1$ and $d' = d/\deg(u) < d$. The rest of the proof is similar to the proof of Theorem 1. □

4 Primitive divisors in complete linear series

Let C be a curve over $\mathbb{Q}$. For an effective divisor D on C the notation $|D|$ denotes the **complete linear series containing** D:

$$|D| = \{D + \operatorname{div}(f) : f \in L(D)\};$$

this is precisely the set of effective divisors linearly equivalent to D. Observe that for effective divisors D, D', we have $D \sim D'$ if and only if $|D| = |D'|$. Recall that $|D| \cong \mathbb{P}^{\ell(D)-1}(\mathbb{Q})$. Note that $\ell(D) \geq 1$ since $\mathbb{Q} \subseteq L(D)$ for any effective divisor D. In particular, $|D| = \{D\}$ if and only if $\ell(D) = 1$.

The following well-known lemma highlights the relationship between a point being not $\mathbb{P}^1$-isolated and the complete linear series of its irreducible divisor having positive dimension.

Lemma 15 *Let C be a curve defined over $\mathbb{Q}$, and let $d \geq 1$. Let D be an irreducible degree d divisor. The following are equivalent.*

(a) $\dim|D| \geq 1$.
(b) $\ell(D) \geq 2$.
(c) There is a degree d morphism $f : C \to \mathbb{P}^1$, defined over $\mathbb{Q}$, such that $f^*(\infty) = D$.
(d) Any $P \in D$ is not $\mathbb{P}^1$-isolated.

Proof Recall that $|D| \cong \mathbb{P}^{\ell(D)-1}(\mathbb{Q})$. Thus $\dim|D| = \ell(D) - 1$ and therefore (a) and (b) are equivalent.

Suppose $\ell(D) \geq 2$. Then there is some non-constant $f \in L(D)$. Thus $f \in \mathbb{Q}(C)^\times$ satisfies $\operatorname{div}(f) + D \geq 0$. Write $\operatorname{div}_\infty(f)$ for the divisor of poles of f. As f is non-constant, $0 < \operatorname{div}_\infty(f)$. As f is defined over $\mathbb{Q}$, we have $\operatorname{div}_\infty(f)$ is a rational divisor. Moreover, $\operatorname{div}_\infty(f) \leq D$ since $\operatorname{div}(f) + D \geq 0$. Since D is irreducible, $\operatorname{div}_\infty(f) = D$. Now we consider f as a morphism $C \to \mathbb{P}^1$ defined over $\mathbb{Q}$. Then $f^*(\infty) = D$. As D has degree d so does f. Thus (b) implies (c).

Conversely, suppose (c). Then $f \in L(D)$ and non-constant giving (b).

It is clear that (c) implies (d). To complete the proof we suppose (d) and prove (c). Thus there is a morphism $f : C \to \mathbb{P}^1$ of degree d defined over $\mathbb{Q}$ with $f(P) = \alpha \in \mathbb{P}^1(\mathbb{Q})$. Composing f with an automorphism of $\mathbb{P}^1$ we may suppose $\alpha = \infty$. Now $P \in \operatorname{div}_\infty(f)$, and so $D \leq \operatorname{div}_\infty(f)$ as $\operatorname{div}_\infty(f)$ is stable under the action of Galois. Thus $D = \operatorname{div}_\infty(f)$ as both divisors have degree d. This completes the proof. □

We will call an irreducible divisor **primitive** if it is the Galois orbit of a primitive point.

Corollary 16 *Let C be a curve defined over $\mathbb{Q}$ with genus g and $\mathbb{Q}$-gonality $m \geq 2$. Let $d \geq 2$ be an integer satisfying (1). Let D' be an effective degree d divisor on C with $\ell(D') \geq 2$. Then $|D'|$ contains no primitive degree d divisors. Moreover, if $\gcd(d, m) = 1$ or d is prime, then $|D'|$ contains no irreducible divisors.*

Proof Suppose $D \in |D'|$ is an irreducible divisor. Then $\ell(D) = \ell(D') \geq 2$. By Lemma 15, any $P \in D$ is not $\mathbb{P}^1$-isolated. By part (II) of Theorem 1 we see that P is imprimitive. Thus $|D'|$ contains no primitive divisors.

Suppose now that $\gcd(d, m) = 1$ or d is prime. Then part (I) of Theorem 1 gives a contradiction, therefore $|D'|$ contains no irreducible divisors. □

The following variant of Corollary 16 has an almost identical proof, but appealing to Theorem 8 instead of Theorem 1.

Corollary 17 *Let $\pi : C \to C'$ be a morphism of curves defined over $\mathbb{Q}$ of degree $m \geq 2$. Write g, g' for the genera of C, C' respectively, and suppose $g' \geq 1$. Let $d \geq 2$ be an integer satisfying (3). Let D' be an effective degree d divisor on C with $\ell(D') \geq 2$. Then $|D'|$ contains no primitive degree d divisors. Moreover, if $\gcd(d, m) = 1$ or d is prime, then $|D'|$ contains no irreducible divisors.*

5 Decomposition of $C^{(d)}$ into complete linear series

We denote the d-th symmetric power of C by $C^{(d)}$. Recall that $C^{(d)}(\mathbb{Q})$ can be identified with the set of effective degree d divisors on C. The purpose of this section is to prove the following proposition.

Proposition 18 *Let C be a curve over $\mathbb{Q}$ of genus $g \geq 1$, and let J be the Jacobian of C. Let d be a positive integer. Suppose either of the following two conditions hold:*

(a) $J(\mathbb{Q})$ is finite;
(b) or $d \leq g - 1$, and $A(\mathbb{Q})$ is finite for every abelian subvariety $A/\mathbb{Q}$ of J of dimension $\leq d/2$.

Then there are finitely many effective degree d divisors $D_1, D_2, \ldots, D_n$ such that

$$C^{(d)}(\mathbb{Q}) = \bigcup_{i=1}^{n} |D_i|. \tag{7}$$

To prove the proposition we shall need the following famous theorem of Faltings [19].

Theorem 19 *(Faltings) Let B be an abelian variety defined over a number field K, and let $V \subset B$ be a subvariety defined over K. Then there is a finite number of abelian subvarieties $B_1, \ldots, B_m$ of B, defined over K, and a finite number of points $x_1, \ldots, x_m \in V(K)$ such that the translates $x_i + B_i$ are contained in V, and, moreover, such that*

$$V(K) = \bigcup_{i=1}^{m} x_i + B_i(K). \tag{8}$$

We shall also need the following theorem of Debarre and Fahlaoui [13, Corolllary 3.6].

Theorem 20 *(Debarre and Fahlaoui) Let $C/\mathbb{C}$ be a curve of genus $g \geq 1$ with Jacobian J, and let $d \leq g-1$. Let D_0 be a fixed divisor of degree d on C. Let $W_d(C)$ be the image of $C^{(d)}$ under the Abel–Jacobi map*

$$\iota : C^{(d)} \to J, \qquad D \mapsto [D - D_0]. \tag{9}$$

Let A be an abelian subvariety of J with a translate contained in $W_d(C)$. Then $\dim(A) \leq d/2$.

Proof of Proposition 18 If $C^{(d)}(\mathbb{Q}) = \emptyset$ then we take $n = 0$ and there is nothing to prove. So suppose $C^{(d)}(\mathbb{Q}) \neq \emptyset$ and fix $D_0 \in C^{(d)}(\mathbb{Q})$. Let $W_d(C)$ be the image of $C^{(d)}$ under the Abel–Jacobi map (9), which is defined over $\mathbb{Q}$. We claim that $W_d(C)(\mathbb{Q})$ is finite. This is trivially true if (a) holds, so suppose (b). In particular $d \leq g-1$ and so $W_d(C)$ is birational to $C^{(d)}$ (e.g. [31, Theorem 5.1]) and so has dimension d. We apply Falting's Theorem with $B = J$ and $V = W_d(C)$. Thus, there are $x_1, \ldots, x_m \in W_d(C)(\mathbb{Q})$ and $B_1, \ldots, B_m$ abelian subvarieties of J defined over $\mathbb{Q}$ such that $x_i + B_i \subset W_d(C)$ and

$$W_d(C)(\mathbb{Q}) = \bigcup_{i=1}^{m} x_i + B_i(\mathbb{Q}).$$

By the theorem of Debarre and Fahlaoui, $\dim(B_i) \leq d/2$. However, by assumption (b), $B_i(\mathbb{Q})$ is finite. Hence $W_d(C)(\mathbb{Q})$ is finite, proving our claim.

Let $W_d(C)(\mathbb{Q}) = \{R_1, \ldots, R_n\}$ and choose $D_1, \ldots, D_n \in C^{(d)}(\mathbb{Q})$ mapping to $R_1, \ldots, R_n$ respectively. If $D \in C^{(d)}(\mathbb{Q})$ then $\iota(D) = R_i$ for some i, and so $[D - D_0] = [D_i - D_0]$. Hence $[D - D_i] = 0$, so $D \in |D_i|$. This completes the proof. □

Observe that if C and d satisfy the hypotheses of either Theorem 2 or 9 then they satisfy the hypotheses of Proposition 18 and therefore $C^{(d)}(\mathbb{Q})$ can be decomposed into the union of finitely many complete linear series as in (7).

6 Proofs of Theorems 2 and 9 and their corollaries

Proof of Theorem 2 Let C, m, d be as in the statement of Theorem 2. By Proposition 18,

$C^{(d)}(\mathbb{Q})$ has a finite decomposition, as in (7) where $D_1, \ldots, D_n$ are effective degree d divisors. If $\ell(D_i) \geq 2$ then, by Corollary 16, the complete linear series $|D_i|$ does not contain primitive divisors. On the other hand, if $\ell(D_i) = 1$ then $|D_i| = \{D_i\}$. Hence there are only finitely many primitive degree d points on C.

Suppose now that $\gcd(d, m) = 1$ or d is prime. Again, if $\ell(D_i) \geq 2$ then, by Corollary 16, the complete linear series $|D_i|$ does not contain irreducible divisors. The theorem follows. □

Proof of Corollary 5 Let $C/\mathbb{Q}$ be hyperelliptic of genus g. This has gonality $m = 2$. Suppose either of hypotheses (a), (b) of Corollary 5 is satisfied. Then C, g, m, d satisfy the hypotheses of Theorem 2. In particular, if d is odd then C has finitely many degree d points.

Suppose d is even. By Proposition 18, we have that (7) holds where $D_1, \ldots, D_n$ is a finite set of effective degree d divisors on C. Let P be a degree d point and let D be the corresponding irreducible divisor. Then $D \in |D_i|$ for some i. Suppose $D \neq D_i$. Then $\ell(D) \geq 2$ and so by Lemma 15 the point P is not $\mathbb{P}^1$-isolated. It follows from Theorem 1 that $\mathbb{Q}(P)$ contains a subfield of index $d' = 2$. Thus, for all but finitely many degree d points P we have that $\mathbb{Q}(P)$ contains a subfield of index 2. □

Proof of Theorem 9 This follows from Proposition 18 and Corollary 17 by trivial modifications to the proof of Theorem 2. □

Proof of Corollary 11 The proof is a straightforward modification of preceding arguments. □

6.1 A remark on effectivity

Let C and d satisfy the hypotheses of Theorem 2 or Theorem 9. Then $C^{(d)}(\mathbb{Q})$ can be decomposed into a finite union of complete linear systems as in (7). Suppose that we are able to explicitly compute the representatives D_i in (7). Then we have an effective strategy for computing all primitive degree d points. Indeed, if $\ell(D_i) \geq 2$ then $|D_i|$ contains no primitive divisors by Corollary 16. We are left to consider $|D_i|$ for $\ell(D_i) = 1$. However, if $\ell(D_i) = 1$, then $|D_i| = \{D_i\}$ and we simply need to test D_i to determine if it is the Galois orbit of a primitive degree d point. Moreover, if $\gcd(d, m) = 1$ or d is prime then we can compute all degree d points by a slight modification of the strategy: if $\ell(D_i) = 1$ then simply test D_i for irreducibility.

We remark that the decomposition (7) can often be computed using symmetric power Chabauty (e.g. [39] or [10]) provided $r + d \leq g$ where r is the rank of the Mordell–Weil group $J(\mathbb{Q})$.

6.2 A remark on the assumptions of Corollary 5

As noted previously, assumption (b) of Corollary 5 is satisfied for $d \leq g - 1$ whenever the Jacobian J is simple. We remark that almost all hyperelliptic curves have simple Jacobians, in a sense that we make precise shortly. For this we will need the following theorem of Zarhin [44, Theorem 1.1].

Theorem 21 *(Zarhin) Let k be a field, $\mathrm{char}(k) \neq 2$. Let $C : Y^2 = f(X)$, where $f \in k[X]$ is a separable polynomial of degree $n \geq 5$, and let J denote the Jacobian of C. Suppose $\mathrm{char}(k) \neq 3$ or $n \geq 7$, and that f has Galois group either S_n or A_n. Then $\mathrm{End}(J) \cong \mathbb{Z}$, and in particular J is absolutely simple.*

We fix a genus $g \geq 2$. Let $n = 2g + 1$ or $2g + 2$. The set of all polynomials of degree $\leq n$ can be naturally identified with $\mathbb{A}^{n+1}(\mathbb{Q})$: here $\mathbf{a} = (a_0, a_1, \ldots, a_n) \in \mathbb{A}^{n+1}(\mathbb{Q})$ corresponds to the polynomial

$$f_{\mathbf{a}}(X) \;=\; a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0.$$

Hilbert's irreducibility theorem asserts the existence of a thin set $S \subset \mathbb{A}^{n+1}(\mathbb{Q})$ such that for $\mathbf{a} \in \mathbb{A}^{n+1}(\mathbb{Q}) \setminus S$, the polynomial $f_{\mathbf{a}}$ is irreducible of degree n and has Galois group S_n. See [38, Chapter 9] for a statement of Hilbert's irreducibility theorem as well as the definition of thin sets.

Therefore, for $\mathbf{a} \in \mathbb{A}^{n+1}(\mathbb{Q}) \setminus S$, the genus g hyperelliptic curve $Y^2 = f_{\mathbf{a}}(X)$ has a simple Jacobian by Zarhin's theorem.

We point out that there is no shortage of hyperelliptic curves satisfying the finite Mordell–Weil group condition of Corollary 5. This immediately follows from the preceding remarks together with the following Theorem of Yu [43, Theorem 3], applied with $r = 0$.

Theorem 22 *(Yu) Let K be a number field with at least one real embedding. Let $f \in K[X]$ be a separable degree n polynomial such that $n \equiv 3 \pmod 4$ and $\mathrm{Gal}(f) \cong S_n$ or A_n. Let $C : Y^2 = f(X)$ be a hyperelliptic curve over K with Jacobian J. Then for every $r \geq 0$, there are infinitely many quadratic twists J_b of J such that $\dim_{\mathbb{F}_2}(\mathrm{Sel}_2(J_b/K)) = r$.*

7 Proof of Theorem 12

The proof of Theorem 12 relies on the following proposition, which is in fact a consequence of Hilbert's Irreducibility Theorem.

Proposition 23 *Let $d \geq 2$ be an integer. Let $f : C \to \mathbb{P}^1$ be a degree d morphism of curves defined over $\mathbb{Q}$, and let $\alpha \in \mathbb{P}^1(\mathbb{Q})$. Suppose that α is not a branch value for f, and that the fibre $f^{-1}(\alpha)$ consists of a single Galois orbit of points. Let $P \in f^{-1}(\alpha)$ and suppose the extension $\mathbb{Q}(P)$ is primitive. Then there is a thin set $S \subset \mathbb{P}^1(\mathbb{Q})$ such that for $\beta \in \mathbb{P}^1(\mathbb{Q}) \setminus S$, the fibre $f^{-1}(\beta)$ consists of a single Galois orbit of points and, for any $Q \in \pi^{-1}(\beta)$, the extension $\mathbb{Q}(Q)$ is primitive of degree d.*

Before proving Proposition 23 we show that it implies Theorem 12.

Proof of Theorem 12 Let $C/\mathbb{Q}$ be a curve of genus g. Suppose $P \in C(\overline{\mathbb{Q}})$ is primitive of degree $d \geq g+1$, and let D be the corresponding irreducible divisor.

By Riemann–Roch,

$$\ell(D) \;\geq\; d - g + 1 \;\geq\; 2.$$

It follows from Lemma 15 that there is a degree d morphism $f : C \to \mathbb{P}^1$ defined over $\mathbb{Q}$ such that $f^*(\infty) = D$. We apply Proposition 23 with $\alpha = \infty \in \mathbb{P}^1(\mathbb{Q})$. The theorem follows. □

The proof of Proposition 23 makes use of the relationship between primitive extensions and primitive Galois groups. Whilst this relationship is known, we are unable to find a convenient reference, and we therefore give the details. Let X be a non-empty set, and let G be a group acting transitively on X. The **trivial** partitions of X are $\{X\}$ and $\{\{x\} : x \in X\}$. A partition $\mathcal{P}$ of X is said to be G-**stable** if $\sigma(Z) \in \mathcal{P}$ for all $\sigma \in G$ and $Z \in \mathcal{P}$. Observe, as the action of G on X is transitive, that G also acts transitively on any G-stable partition $\mathcal{P}$, and that any two elements of $\mathcal{P}$ therefore have the same cardinality.

We say that G **acts imprimitively** on X if X admits a G-stable non-trivial partition. If X does not have a G-stable non-trivial partition then we say that G **acts primitively on** X. The following lemma is an immediate consequence of this definition.

Lemma 24 *Let G be a group acting transitively on a set X. Let G' be a subgroup of G and suppose that G' acts primitively on X. Then G acts primitively on X.*

The following result is well-known, and in particular implies that S_d and A_d act primitively on $\{1, \ldots, d\}$, for $d \geq 1$ and $d \geq 3$ respectively.

Lemma 25 *Let G be a group acting 2-transitively on a set X. Then the action is primitive.*

Proof Let $\mathcal{P}$ be a G-stable partition of X and suppose $Y \in \mathcal{P}$ has at least two elements. We would like to show that $Y = X$. Let $a, b \in Y$ be distinct, and let $c \in X$ be distinct from a, b. Then there is some $\sigma \in G$ such that $\sigma(a) = a$ and $\sigma(b) = c$. Thus $a \in Y \cap \sigma(Y)$ which forces $\sigma(Y) = Y$, and therefore $c \in Y$. Hence $Y = X$. □

Lemma 26 *Let G be a group acting transitively on a set X. The action is imprimitive if and only if there is a proper subset Y of X, with at least two elements, such that*

$$\forall \sigma \in G, \qquad \text{if } \sigma(Y) \cap Y \neq \emptyset \text{ then } \sigma(Y) = Y. \tag{10}$$

Proof Given a G-stable non-trivial partition $\mathcal{P}$ we can take Y to be any element of $\mathcal{P}$. As $\mathcal{P}$ is a partition, Y clearly satisfies (10), and as $\mathcal{P}$ is non-trivial, Y is a proper subset of X with at least two elements.

Conversely, suppose Y is a proper subset of X containing at least two elements and satisfying (10). We easily check that $\mathcal{P} = \{\tau(Y) : \tau \in G\}$ is a G-stable non-trivial partition. □

Lemma 27 *Let G be a finite group acting transitively on a non-empty finite set X. Let $x \in X$, and write* Stab(x) *for the stabilizer of x in G. The action of G on X is imprimitive if and only if* Stab(x) *is a non-maximal proper subgroup of G.*

Proof Let $x \in X$ and assume the existence of a subgroup $\mathrm{Stab}(x) \subsetneq H \subsetneq G$. Let $Y = \{\tau(x) : \tau \in H\}$. Then, $\#Y = [H : \mathrm{Stab}(x)]$ and so $2 \leq \#Y < [G : \mathrm{Stab}(x)] = \#X$. Moreover, suppose $\sigma \in G$ and $\sigma(Y) \cap Y \neq \emptyset$. Let $z \in \sigma(Y) \cap Y$. Then there are $\tau_1, \tau_2 \in H$ such that $\sigma\tau_2(x) = z = \tau_1(x)$. Thus $\tau_1^{-1}\sigma\tau_2 \in \mathrm{Stab}(x) \subseteq H$. Hence $\sigma \in H$, and so $\sigma(Y) = Y$. Therefore (10) is satisfied and so the action is imprimitive.

Conversely, suppose the existence of a proper subset Y of X with at least two elements satisfying (10). As the action is transitive, we may in fact suppose that $x \in Y$. Let $H = \{\sigma \in G : \sigma(Y) = Y\}$. As G is transitive, H is a proper subgroup of G. Moreover, Stab(x) is contained in H. Let $x' \in Y, x' \neq x$. Then there is some $\sigma \in G$ such that $\sigma(x) = x'$. Thus $\sigma(Y) = Y$, and so $\sigma \in H$ but $\sigma \notin \mathrm{Stab}(x)$. It follows that Stab($x$) is a proper in H, and so is non-maximal as a subgroup of G. □

Lemma 28 *Let $K = \mathbb{Q}(\theta)$ be a number field and let $\tilde{K}$ be its Galois closure over $\mathbb{Q}$. Let $G = \mathrm{Gal}(\tilde{K}/\mathbb{Q})$. Let $d = [K : \mathbb{Q}]$ and let $\theta_1, \ldots, \theta_d \in \tilde{K}$ be the Galois conjugates of θ. Then G acts primitively on $\{\theta_1, \ldots, \theta_d\}$ if and only if the extension $K/\mathbb{Q}$ is primitive.*

Proof Let $X = \{\theta_1, \ldots, \theta_d\}$. Then G acts transitively on X. We let $x = \theta \in X$ and note that the stabilizer Stab(θ) is in fact $\mathrm{Gal}(\tilde{K}/K)$. By the Galois correspondence, K is imprimitive if and only if the subgroup $\mathrm{Gal}(\tilde{K}/K)$ is proper and non-maximal in G, which by Lemma 27 if equivalent to the action of G being imprimitive. □

The following result was assumed in the introduction.

Lemma 29 *Let $C/\mathbb{Q}$ be a curve, let $d \geq 3$ and let P be a degree d point on C with Galois group S_d or A_d. Then P is primitive.*

Proof The lemma follows from Lemma 28, and for this we need the fact that S_d and A_d act primitively on $\{1, \ldots, d\}$. This is trivially true if $d = 3$, and for $d \geq 4$ follows from Lemma 25. □

Proof of Proposition 23 By composing f with a suitable automorphism of $\mathbb{P}^1$ we may suppose that $\alpha = 0 \in \mathbb{P}^1(\mathbb{Q})$. Write $\mathbb{K} = \mathbb{Q}(C)$ for the function field of C. We may regard f as a non-constant element of $\mathbb{K}$, and with this interpretation $\mathbb{Q}(f) = \mathbb{Q}(\mathbb{P}^1)$ is a subfield of $\mathbb{K}$ of index d.

By hypothesis, $\alpha = 0$ is not a branch value for f, and $f^{-1}(0)$ consists of a single Galois orbit containing P. Write $D = f^*(0)$ which we think of as a degree d place of $\mathbb{K}$, unramified in the extension $\mathbb{K}/\mathbb{Q}(\mathbb{P}^1)$. Write

$$\mathcal{O}_D = \{h \in \mathbb{K} \ : \ \mathrm{ord}_D(h) \geq 0\}, \qquad \mathfrak{m}_D = \{h \in \mathbb{K} \ : \ \mathrm{ord}_D(h) \geq 1\},$$

for the valuation ring of D and its maximal ideal. Then the residue field $\mathcal{O}_D/\mathfrak{m}_D$ can be identified with $K = \mathbb{Q}(P)$ where the identification is given by $g + \mathfrak{m}_D \mapsto g(P)$. Now fix $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. Then there is some $g \in \mathcal{O}_D$ such that $g(P) = \theta$. As $g \in \mathbb{K}$ and $\mathbb{K}$ has degree d over $\mathbb{Q}(f)$, there is a polynomial $F(U, V) \in \mathbb{Q}[U, V]$,

$$F(U, V) = \sum_{i=1}^{n} a_i(V)U^i, \qquad a_i(V) \in \mathbb{Q}[V] \tag{11}$$

of degree $n \mid d$, such that $\gcd(a_0(V), \ldots, a_n(V)) = 1$, and $F(g,f) = 0$. Now, $F(\theta, 0) = F(g(P),f(P)) = 0$, and so θ is a root of the polynomial $F(U, 0) \in \mathbb{Q}[U]$; this polynomial is non-zero as $\gcd(a_0(V), \ldots, a_n(V)) = 1$. As θ has degree d, it follows that $n = d$, and that $F(U, V)$ is irreducible over $\mathbb{Q}(V)$. In particular $F(U, V) = 0$ is a (possibly singular) plane model for C. As C is absolutely irreducible, $F(U, V)$ is irreducible over $\overline{\mathbb{Q}}$. Write $\tilde{\mathbb{K}}$ for the Galois closure of $\mathbb{K}/\mathbb{Q}(\mathbb{P}^1)$, and let $g_1, \ldots, g_d$ be the roots of $F(U,f) = 0$ in $\tilde{\mathbb{K}}$; then $\tilde{\mathbb{K}} = \mathbb{Q}(\mathbb{P}^1)(g_1, \ldots, g_d)$.

Let $\tilde{C}/\mathbb{Q}$ be the algebraic curve associated to $\tilde{\mathbb{K}}$. Let $\tilde{D}$ be an extension of the place D of $\mathbb{K}$ to $\tilde{\mathbb{K}}$. As D is unramified in $\mathbb{K}/\mathbb{Q}(\mathbb{P}^1)$, the place $\tilde{D}$ is unramified in the Galois closure $\tilde{\mathbb{K}}/\mathbb{Q}(\mathbb{P}^1)$ (see for example [41, Corollary III.8.4]). We claim that $g_1, \ldots, g_d \in \mathcal{O}_{\tilde{D}}$. To see this, note that $G = \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{Q}(\mathbb{P}^1))$ acts transitively on the g_i. Thus we would like to show $\mathrm{ord}_{\tilde{D}}(\tau(g)) \geq 0$ for all $\tau \in G$. However,

$$\mathrm{ord}_{\tilde{D}}(\tau(g)) \ = \ \mathrm{ord}_{\tau^{-1}(\tilde{D})}(g) \ = \ \mathrm{ord}_D(g) \ \geq \ 0,$$

where the second equality follows as $g \in \mathbb{K}$ and $\tau^{-1}(\tilde{D})$ is an unramified place of $\tilde{\mathbb{K}}$ above D. This proves the claim.

The place $\tilde{D}$ corresponds to a Galois orbit of points on $\tilde{C}$ and we let $\tilde{P}$ be a representative point chosen above P. Write $G_{\tilde{D}}$ for the decomposition group corresponding to $\tilde{D}$ in $G = \mathrm{Gal}(\tilde{\mathbb{K}}/\mathbb{Q}(\mathbb{P}^1))$; by definition this is

$$G_{\tilde{D}} = \{\sigma \in G \ : \ \sigma(\mathfrak{m}_{\tilde{D}}) = \mathfrak{m}_{\tilde{D}}\}.$$

As $\tilde{D}$ is unramified in the Galois closure $\tilde{\mathbb{K}}/\mathbb{Q}(\mathbb{P}^1)$, the theory of decomposition groups allows us to identify the decomposition group $G_{\tilde{D}}$ with $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$, where $\tilde{K}$ is the Galois closure of $K/\mathbb{Q}$. Here we shall in fact need the details of the precise identification. Let $\sigma \in G_{\tilde{D}}$. We associate σ to $\sigma' \in \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ as follows. We let $\gamma \in \tilde{K} \cong \mathcal{O}_{\tilde{D}}/\mathfrak{m}_{\tilde{D}}$. Then $\gamma = h(\tilde{P})$ for some $h \in \mathcal{O}_{\tilde{D}}$, and we define $\sigma'(\gamma) = \sigma(h)(\tilde{P})$. It immediately follows from the definition of $G_{\tilde{D}}$ that σ' is well-defined. The map $G_{\tilde{D}} \to \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ given by $\sigma \mapsto \sigma'$ is in fact an isomorphism [41, Theorem III.8.2], and from now on we shall identify $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ with $G_{\tilde{D}}$ via this identification.

Let $\theta_1, \ldots, \theta_d$ be the conjugates of θ in $\tilde{K}$, where we take $\theta_1 = \theta$. Now $\theta = g(P) = g(\tilde{P})$. Let $1 \leq i \leq d$. Then there is some $\sigma_i \in G_{\tilde{D}}$ such that $\sigma_i(\theta) = \theta_i$ and therefore $\sigma_i(g)(\tilde{P}) = \theta_i$. Thus there is a conjugate of g sending $\tilde{P}$ to θ_i. As the θ_i are pairwise distinct, we may after reordering the g_i suppose that $g_i(\tilde{P}) = \theta_i$. Now $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) = G_{\tilde{D}}$ is a subgroup of $G = \mathrm{Gal}(\tilde{\mathbb{K}}/\mathbb{Q}(\mathbb{P}^1))$ and both act on $\{g_1, \ldots, g_d\}$. As $K/\mathbb{Q}$ is primitive, Lemma 28 tells us

that $G_{\tilde{D}}$ acts primitively on the θ_i and therefore on the g_i. Thus by Lemma 24, the action of G on $\{g_1, \ldots, g_d\}$ is primitive.

Finally we apply Hilbert's Irreducibility Theorem [38, Chapter 9] to $f : C \to \mathbb{P}^1$. For $\beta \in \mathbb{P}^1(\mathbb{Q})$ we shall make a standard abuse of language and speak of the decomposition group G_β by which we mean the decomposition group $G_{\tilde{Q}}$ for any point $\tilde{Q} \in \tilde{C}$ above β. As usual, G_β is only defined up to conjugation in G. Now, Hilbert's Irreducibility Theorem applied to $f : C \to \mathbb{P}^1$ asserts the existence of a thin set $S \subset \mathbb{P}^1(\mathbb{Q})$, which includes all branch values, such that $G_\beta = G$ for $\beta \in \mathbb{P}^1(\mathbb{Q}) \setminus S$. We enlarge S by adjoining finitely many values in $\mathbb{P}^1(\mathbb{Q})$: the roots of $a_d(V)$ (which is the leading coefficient of F regarded as an element of $\mathbb{Q}[V][U]$); the V-coordinate of any singular point of the plane model $F(U, V) = 0$; and the point $\infty \in \mathbb{P}^1(\mathbb{Q})$. As we have added finitely many points to the set S it remains thin. Let $\beta \in \mathbb{P}^1(\mathbb{Q}) \setminus S$. Let $\phi_1, \ldots, \phi_d$ be the roots of $F(U, \beta)$. Let $Q = (\phi_1, \beta)$; this is a smooth point on the plane model, and so may be regarded as a point on C. Let $\tilde{Q}$ be a point of $\tilde{C}$ above Q. Then as before, we can identify the action of G_β on $\{\phi_1, \ldots, \phi_d\}$ with the action of G on $\{g_1, \ldots, g_d\}$. As G is acting transitively and primitively on $\{g_1, \ldots, g_d\}$, we have that $G_\beta = \mathrm{Gal}(\mathbb{Q}(f^{-1}(\beta))/\mathbb{Q})$ is acting transitively and primitively on $\{\phi_1, \ldots, \phi_d\}$. Hence, the Galois action on the fibre $f^{-1}(\beta) = \{(\phi_1, \beta), \ldots, (\phi_d, \beta)\}$ is primitive and, by Lemma 28, the field $\mathbb{Q}(Q) = \mathbb{Q}(\phi_1)$ is primitive of degree d. The proposition follows. □

Let $C/\mathbb{Q}$ be a curve and let $d \geq g + 1$ where g is the genus of C. Theorem 12 asserts the existence of infinitely many primitive degree d points on C provided there is at least one. However, the existence of a primitive degree d point is not guaranteed, as illustrated by the following lemma.

Lemma 30 *Let $g \geq 2$ be even. Let C be a degree $2g + 1$ genus g curve defined over $\mathbb{Q}$*

$$C : Y^2 = a_{2g+1}X^{2g+1} + a_{2g}X^{2g} + \cdots + a_0.$$

Suppose $J(\mathbb{Q}) = 0$ where J is the Jacobian of C. Then C has no points of degree $g + 1$ points.

Proof Write ∞ for the single point at infinity on the given model. Write $D_0 = (g + 1)\infty$. Note that X has a double pole at ∞. Thus $1, X, \ldots, X^{g/2} \in L(D_0)$. We claim that $1, X, \ldots, X^{g/2}$ is a basis for $L(D_0)$. We first explain how our claim implies the lemma. Let D be an effective degree $g + 1$ divisor. Since $J(\mathbb{Q}) = 0$, we have $D - D_0 = \mathrm{div}(f)$ for some $f \in L(D_0)$. Thus, $f = \alpha_0 + \alpha_1 X + \cdots + \alpha_{g/2}X^{g/2}$, for some $\alpha_0, \ldots, \alpha_{g/2} \in \mathbb{Q}$. In particular $f \in L(g\infty)$. Thus

$$D - \infty = D_0 + \mathrm{div}(f) - \infty = g\infty + \mathrm{div}(f)$$

is effective. Hence D is reducible. It follows that C has no degree $g + 1$ points.

It remains to prove our claim. Since $1, X, \ldots, X^{g/2} \in L(D_0)$, our claim is equivalent to showing that $\ell(D_0) \leq g/2 + 1$. If $g = 2$, the Riemann–Roch theorem immediately implies that $\ell(D_0) = 2 = g/2 + 1$ as required. We may therefore suppose $g > 2$, and as g is even, $g \geq 4$. It follows from the Riemann–Roch theorem (4) that $\ell(K_C - D_0) = \ell(D_0) - 2 \geq g/2 - 1 > 0$. In particular, D_0 is a special divisor. By Clifford's theorem (Theorem 13) we have $\ell(D_0) \leq g/2 + 3/2$. However, since g is even and $\ell(D_0)$ is an integer, we have $\ell(D_0) \leq g/2 + 1$, completing the proof. □

In a positive direction, we can use Theorem 12 to construct curves with infinitely many primitive points.

Lemma 31 *Let $g \geq 2$. Let $d = g + 1$. Then there is a hyperelliptic curve $C/\mathbb{Q}$ of genus g with infinitely many primitive degree d points.*

Proof Let $K = \mathbb{Q}(\theta)$ be any primitive number field of degree d. Let $\theta_1, \ldots, \theta_d$ be the conjugates of θ in a fixed Galois closure $\tilde{K}$ of K. Choose a rational number α such that $2\alpha \neq \theta_i + \theta_j$ for any pair $1 \leq i, j \leq d$. Let $\phi = \theta - \alpha$. The conjugates of ϕ are $\phi_i = \theta_i - \alpha$ with $1 \leq i \leq d$, and satisfy $\phi_i \neq \pm\phi_j$ for any pair i, j. Note that $\mathbb{Q}(\phi^2) \subseteq K$. As K is primitive, either $\mathbb{Q}(\phi^2) = \mathbb{Q}$ or $\mathbb{Q}(\phi^2) = K$. However, if $\mathbb{Q}(\phi^2) = \mathbb{Q}$, then $K = \mathbb{Q}(\theta) = \mathbb{Q}(\phi)$ has degree at most 2, contradicting the fact that K has degree $d = g + 1 \geq 3$. Thus $K = \mathbb{Q}(\phi^2)$. Let $f \in \mathbb{Q}[X]$ be the minimal polynomial of ϕ^2, which must be irreducible of degree d. Let $h = f(X^2)$. The roots of h are $\pm\phi_1, \ldots, \pm\phi_d$ which are pairwise distinct and hence h is separable of degree $2d = 2g + 2$. Let C be the genus g hyperelliptic curve

$$C : Y^2 = h(X).$$

Note that this has the primitive degree d point $(\phi, 0)$. Hence by Theorem 12 there are infinitely many primitive degree d points. □

8 Low degree primitive points on some $X_1(N)$

Mazur [29] showed that all rational points on $X_1(p)$ are cuspidal for prime $p \geq 11$. Merel's uniform boundedness theorem [30] asserts that for prime p, and for d satisfying $(3^{d/2} + 1)^2 \leq p$, the only degree d points on $X_1(p)$ are cuspidal. We now know, for each $1 \leq d \leq 8$, the exact set of primes p such that $X_1(p)$ has degree d non-cuspidal points, thanks to the efforts of Kamienny [23], Parent [36,37], Derickx, Kamienny, Stein and Stoll [15], and Khawaja [26]. Less is known about the low degree points on $X_1(N)$ for composite N, though several authors consider the somewhat easier problem of determining the values of N such $X_1(N)$ has infinitely many degree d points for given small d (see for example [7] and [17] for two different approaches to studying this problem). Example 10 illustrates how our results can be applied to modular curves $X_1(N)$ provided the analytic rank of $J_1(N)$ is 0 and we have information about the quotients or gonality of $X_1(N)$. The `LMFDB` [42] contains a database of modular curves $X_1(N)$ for $1 \leq N \leq 70$. For 61 of these curves the Jacobian $J = J_1(N)$ has analytic rank 0. It follows from a theorem of Kato [25, Corollary 14.3] that the Mordell–Weil group $J(\mathbb{Q})$ is finite. We are able to apply Theorem 9 to around half of these curves in order to deduce the finiteness of primitive points of certain low degrees. We note that it is common for $X_1(N)$ to cover multiple curves, and in these instances we apply Theorem 9 to the covered curve C' that gives the most generous range for d in inequality (3). We record the results in Table 1.

In [14, Theorem 3.1] the authors give a complete list of N for which $J_1(N)$ has analytic rank 0. There are in total 83 such values of N, the largest of which is $N = 180$.

9 Low degree primitive points on some $X_0(N)$

The computational study of quadratic points on modular curves is an active area of research (see e.g. [2,11,20,33,35], to name but a few works). Comparatively less is known about points defined over number fields of higher degree. Still, there is reason to be hopeful. Establishing the modularity of all elliptic curves over totally real cubic fields [16], and totally real quartic fields not containing $\sqrt{5}$ [9] required the study of cubic, and quartic points on certain modular curves. Banwait and Derickx [4] have determined all cubic

Table 1 The table summarizes our conclusions upon applying Theorem 9 to $C = X_1(N)$ for the values of N in the first column. Here g denotes the genus of $X_1(N)$; the integer m denotes the degree of the morphism $X_1(N) \to C'$; g' denotes the genus of C'. The sixth column gives the values of d furnished by the theorem for which there are only finitely many points of degree d. The final column gives the values of d (not appearing in the previous column) for which the theorem asserts that there are only finitely primitive degree d points

N	g	C' (LMFDB label)	g'	m	$X_1(N)$ has finitely many degree d points	$X_1(N)$ has finitely many primitive degree d points
19	7	19.120.1-19.a	1	3	$d = 2$	-
22	6	$X_1(11)$	1	3	$d = 2$	-
24	5	24.192.1-24.dg.2.1	1	2	$2 \le d \le 3$	-
26	10	$X_1(13)$	2	3	$d = 2$	-
27	13	27.216.1-27.a.1.1	1	3	$2 \le d \le 5$	-
28	10	28.288.4-28.d.1.1	4	2	$d = 2$	-
30	9	$X_1(15)$	1	3	$2 \le d \le 3$	-
31	26	31.320.6-31.c.1.2	6	3	$2 \le d \le 4$	-
32	17	32.384.5-32.bu.1.1	5	2	$2 \le d \le 7$ $d \ne 4, 6$	$d = 4, 6$
34	21	$X_1(17)$	5	3	$2 \le d \le 3$	-
36	17	36.288.3-36.c.1.1	3	3	$2 \le d \le 4$	-
38	28	$X_1(19)$	7	3	$2 \le d \le 4$	-
39	33	39.448.9-39.a.3.1	9	3	$2 \le d \le 3$	-
40	25	40.576.9-40.bh.1.1	9	2	$2 \le d \le 7$ $d \ne 4, 6$	$d = 4, 6$
42	25	$X_1(21)$	5	3	$2 \le d \le 5$	-
44	36	44.720.16-44.e.1.1	16	2	$2 \le d \le 3$	$d = 4$
45	41	45.576.9-45.a.4.1	9	3	$2 \le d \le 7$ $d \ne 6$	$d = 6$
46	45	$X_1(23)$	12	3	$2 \le d \le 5$	-
48	37	48.768.13-48.nt.1.1	13	2	$2 \le d \le 11$ $d \ne 4, 6, 8, 10$	$d = 4, 6, 8, 10$
49	69	49.336.3-49.b.1.2	3	7	$2 \le d \le 8$	-
50	48	50.360.4-50.a.2.2	4	5	$2 \le d \le 7$	-
52	55	52.1008.25-52.p.1.1	25	2	$2 \le d \le 5$ $d \ne 4$	$d = 4$
54	52	54.648.10-54.a.1.1	10	3	$2 \le d \le 11$ $d \ne 6, 9$	$d = 6, 9$
56	61	56.1152.25-56.bq.1.1	25	2	$2 \le d \le 11$ $d \ne 4, 6, 8, 10$	$d = 4, 6, 8, 10$
60	57	60.1152.25-60.eb.2.1	25	2	$2 \le d \le 7$ $d \ne 4, 6$	$d = 4, 6$
62	91	$X_1(31)$	26	3	$2 \le d \le 7$ $d \ne 6$	$d = 6$
64	93	64.1536.37-64.ef.1.1	37	2	$d = 2$ $3 \le d \le 19$, odd d	$4 \le d \le 18$ even d
66	81	$X_1(33)$	21	3	$2 \le d \le 9$ $d \ne 6, 9$	$d = 6, 9$
68	105	68.1728.49-68.ba.1.1	49	2	$2 \le d \le 7$ $d \ne 4, 6$	$d = 4, 6$
70	97	$X_1(35)$	25	3	$2 \le d \le 11$ $d \ne 6, 9$	$d = 6, 9$

points on $X_0(N)$ for $N \in \{41, 47, 59, 71\}$. Box, Gajović, and Goodman [10] have determined all cubic points on $X_0(N)$ for $N \in \{53, 57, 61, 65, 67, 73\}$, and all quartic points on $X_0(65)$. A famous theorem of Ogg [34] asserts that there are 19 values of N for which which $X_0(N)$ is hyperelliptic. Of these, the only one for which $J_0(N)(\mathbb{Q})$ is infinite is $N = 37$. The remaining 18 values are

- genus 2: $N = 22, 23, 26, 28, 29, 31, 50$;
- genus 3: $N = 30, 33, 35, 39, 40, 41, 48$;
- genus 4: $N = 47$;
- genus 5: $N = 46, 59$;
- genus 6: $N = 71$.

For these N, the quadratic points on $X_0(N)$ have been determined by Bruin and Najman [11]. It is easy to apply Corollary 5 to these curves and derive conclusions about algebraic points of degree $3 \le d \le g$, where g is the genus of $X_0(N)$. For example, consider $C = X_0(71)$ with genus $g = 6$. By Corollary 5 we know that there are only finitely many points on $X_0(71)$ of degrees 3 and 5, and finitely many primitive points of degrees 4, 6. We point out that we can in fact go further and compute these finite sets of points, as sketched in Remark 6.1. We illustrate this by giving some details of the computation of primitive degree 6 points on $X_0(71)$, making use of information found in [11] concerning

Table 2 This table gives the conclusions of our computations of primitive points on $X_0(N)$ of certain low degrees d and for the values of N is the first column. Here g is the genus of $X_0(N)$, and $J(\mathbb{Q})$ is in fact the structure of the Mordell–Weil group where $J = J_0(N)$. The table gives the number of primitive degree d points on $X_0(N)$ up to Galois conjugacy. The symbol — indicates that our method is inapplicable for that particular N and d

N	g	$J(\mathbb{Q})$	Number of primitive degree d points on $X_0(N)$			
			$d = 3$	$d = 4$	$d = 5$	$d = 6$
46	5	$\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/22\mathbb{Z}$	2	4	88	—
47	4	$\mathbb{Z}/23\mathbb{Z}$	2	12	—	—
59	5	$\mathbb{Z}/29\mathbb{Z}$	1	2	16	—
60	7	$\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/24\mathbb{Z})^3$	0	0	120	—
62	7	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$	2	0	0	—
71	6	$\mathbb{Z}/35\mathbb{Z}$	0	0	0	22

the model and the Mordell–Weil group. A model for $X_0(71)$ is given by

$$X_0(71) \ : \ Y^2 \ = \ X^{14} + 4X^{13} - 2X^{12} - 38X^{11} - 77X^{10} - 26X^9 + 111X^8 \\ +148X^7 + X^6 - 122X^5 - 70X^4 + 30X^3 + 40X^2 + 4X - 11.$$

The only rational points are the two rational points at infinity which we denote by ∞_+ and ∞_- (these are in fact the two cusps of $X_0(71)$). Write

$$D_0 = \infty_+ - \infty_-, \qquad D_\infty = \infty_+ + \infty_-.$$

Then,

$$J(\mathbb{Q}) \ = \ (\mathbb{Z}/35\mathbb{Z}) \cdot [D_0],$$

where $J = J_0(71)$. Let P be a primitive degree 6 point on $X_0(71)$, and let D be the corresponding effective irreducible degree 6 divisor. Hence $[D - 3D_\infty] \in J(\mathbb{Q})$. It follows that

$$D \in |D_a|, \qquad D_a = a \cdot D_0 + 3D_\infty, \qquad -17 \le a \le 17.$$

We find that $\ell(D_a)$ is 4 for $a = 0$, is 3 for $a = \pm 1$, is 2 for $a = \pm 2$ and is 1 for all other values of a. If $\ell(D_a) \ge 2$ then, by Corollary 16, we know that $|D_a|$ does not contain primitive divisors. Thus $D \in |D_a|$ for $-17 \le a \le -3$ or $3 \le a \le 17$ whence $\ell(D_a) = 1$. For each of these values, $L(D_a) = \mathbb{Q} \cdot f_a$ where f_a is a non-zero function on $X_0(71)$. Moreover, if $D \in |D_a|$ then $D = D_a + \mathrm{div}(f_a)$. We obtain 30 potential possibilities for the divisor D. We find that for $a = \pm 3$, the divisor $D_a + \mathrm{div}(f_a)$ is reducible, and for $a = \pm 5, \pm 7, \pm 12$, the divisor $D_a + \mathrm{div}(f_a)$ is the Galois orbit of an imprimitive point. The remaining 22 values of a yield the Galois orbit of a primitive degree 6 point. We conclude that there are precisely 22 primitive degree 6 points on $X_0(71)$ up to Galois conjugacy.

We carried out similar computations for the hyperelliptic $X_0(N)$ with $N \in \{46, 47, 59, 71\}$, and for degrees d in the range $3 \le d \le \min(g, 6)$ where g is the genus of $X_0(N)$. The outcome of these computations is summarized in Table 2. Here we were helped by the fact that these values of N, the Mordell–Weil group $J_0(N)(\mathbb{Q})$ has been computed by Bruin and Najman [11]. Furthermore, models for the curves are readily available in `Magma` [6] via the `Small Modular Curve package`.

In view of Corollary 11, it is natural to also consider bielliptic $X_0(N)$. Bars [5] shows that $X_0(N)$ is bielliptic for precisely 41 values of N. Of these, $J_0(N)$ has analytic rank 0 for 30 of these values:

Table 3 For each pair (N, d), the table gives a description of the effective degree d divisors D with $\ell(D) = 1$ on the modular curve $X_0(N)$. We denote by $n_{d,r}$ the number of such divisors that are reducible, $n_{d,p}$ the number of such divisors that are irreducible and primitive, and $n_{d,i}$ the number of such divisors that are irreducible but imprimitive. The symbol — indicates that we did not carry out the computation for the pair (N, d)

N	$d = 3$		$d = 4$			$d = 5$		$d = 6$		
	$n_{3,p}$	$n_{3,r}$	$n_{4,p}$	$n_{4,i}$	$n_{4,r}$	$n_{5,p}$	$n_{5,r}$	$n_{6,p}$	$n_{6,i}$	$n_{6,r}$
46	2	20	4	10	42	88	128	—	—	—
47	2	2	12	2	6	—	—	—	—	—
59	1	2	2	0	4	16	8	—	—	—
60	0	364	0	22	1349	120	4440	—	—	—
62	2	28	0	0	58	0	100	—	—	—
71	0	2	0	0	2	0	2	22	6	2

- genus 2: $N = 22, 26, 28, 50$;
- genus 3: $N = 30, 33, 34, 35, 39, 40, 45, 48, 64$;
- genus 4: $N = 38, 44, 54, 81$;
- genus 5: $N = 42, 51, 55, 56, 63, 72, 75$;
- genus 7: $N = 60, 62, 69$;
- genus 9: $N = 95$;
- genus 11: $N = 94, 119$.

Again, it is straightforward to apply Corollary 11 to these curves. We computed all primitive points of certain low degrees on the genus 7 bielliptic curves $X_0(60)$ and $X_0(62)$. For these two curves the size of the Mordell–Weil group has been computed by Najman and Vukorepa [33]. We computed models for these curves and Mordell–Weil generators using a `Magma` package developed by Ozman and Siksek [35], Adžaga, Keller, Michaud-Jacobs, Najman, Ozman and Vukorepa [2], and Najman and Vukorepa [33]. All computations were performed in `Magma`. We summarize our results in Table 2, and refer the reader to

https://github.com/MaleehaKhawaja/Primitive

for the supporting code as well as a description of the points.

We also give a description of all effective degree d divisors D with $\ell(D) = 1$, and refer the reader to Table 3 for this summary.

Data availability The data related to this paper is available at https://github.com/MaleehaKhawaja/Primitive

Author details
[1] School of Mathematics and Statistics, Hicks Building, University of Sheffield, Sheffield S3 7RH, UK, [2] Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK.

Received: 5 January 2024 Accepted: 17 May 2024
Published online: 05 June 2024

References

1. Accola, R.D.M.: On the Castelnuovo-Severi inequality for Riemann surfaces. Kodai Math. J. **29**(2), 299–317 (2006)
2. Adžaga, N., Keller, T., Michaud-Jacobs, P., Najman, F., Ozman, E., Vukorepa, B.: Computing quadratic points on modular curves $X_0(N)$. Math. Comput. **93**(347), 1371–1397 (2024)
3. Arbarello, E., Cornalba, M., Griffiths, P.A., Harris, J.: Geometry of Algebraic Curves, vol. I. Springer, New York (1985)
4. Banwait, B.S., Derickx, M.: Explicit isogenies of prime degree over number fields (2022). arXiv:2203.06009
5. Bars, F.: Bielliptic modular curves. J. Number Theory **76**(1), 154–165 (1999)
6. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The User Language. Volume 24, pp. 235–265. 1997. Computational Algebra and Number Theory London (1993)

7. Bourdon, A., Ejder, O., Liu, Y., Odumodu, F., Viray, B.: On the level of modular curves that give rise to isolated j-invariants. Adv. Math. **357**, 106824, 33 (2019)
8. Bourdon, A., Gill, D.R., Rouse, J., Watson, L.D.: Odd degree isolated points on $X_1(N)$ with rational j-invariant. Res. Number Theory. **10**(1), Paper No. 5, 32 (2024)
9. Box, J.: Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular. Trans. Am. Math. Soc. **375**(5), 3129–3172 (2022)
10. Box, J., Gajović, S., Goodman, P.: Cubic and quartic points on modular curves using generalised symmetric Chabauty. Int. Math. Res. Not. **2023**(7), 5604–5659 (2022)
11. Bruin, P., Najman, F.: Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields. LMS J. Comput. Math. **18**(1), 578–602 (2015)
12. Cremona, J.E.: Algorithms for Modular Elliptic Curves, 2nd edn. Cambridge University Press, Cambridge (1997)
13. Debarre, O., Fahlaoui, R.: Abelian varieties in $W^r_d(C)$ and points of bounded degree on algebraic curves. Compos. Math. **88**(3), 235–249 (1993)
14. Derickx, M., Etropolski, A., van Hoeij, M., Morrow, J.S., Zureick-Brown, D.: Sporadic cubic torsion. Algebra Number Theory **15**(7), 1837–1864 (2021)
15. Derickx, M., Kamienny, S., Stein, W., Stoll, M.: Torsion points on elliptic curves over number fields of small degree. Algebra Number Theory **17**(2), 267–308 (2023)
16. Derickx, M., Najman, F., Siksek, S.: Elliptic curves over totally real cubic fields are modular. Algebra Number Theory **14**(7), 1791–1800 (2020)
17. Derickx, M., Sutherland, A.V.: Torsion subgroups of elliptic curves over quintic and sextic number fields. Proc. Am. Math. Soc. **145**(10), 4233–4245 (2017)
18. Ejder, O.: Isolated points on $X_1(\ell^n)$ with rational j-invariant. Res. Number Theory. **8**(1), Paper No. 16, 7 (2022)
19. Faltings, G.: The general case of S. Lang's conjecture. In: Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Volume 15 of Perspect. Math. Academic Press, San Diego, pp. 175–182 (1994)
20. Freitas, N., Le Hung, B.V., Siksek, S.: Elliptic curves over real quadratic fields are modular. Invent. Math. **201**(1), 159–206 (2015)
21. Gunther, J., Morrow, J.S.: Irrational points on random hyperelliptic curves (2019). arXiv:1709.02041
22. Hartshorne, R.: Algebraic Geometry. Graduate Texts in Mathematics, vol. 52. Springer, New York (1977)
23. Kamienny, S.: Torsion points on elliptic curves and q-coefficients of modular forms. Invent. Math. **109**(2), 221–229 (1992)
24. Kani, E.: On Castelnuovo's equivalence defect. J. Reine Angew. Math. **352**, 24–70 (1984)
25. Kato, K.: p-adic Hodge theory and values of zeta functions of modular forms. Number 295, pages ix, 117–290. 2004. Cohomologies p-adiques et applications arithmétiques. III
26. Khawaja, M.: Torsion primes for elliptic curves over degree 8 number fields. Res. Number Theory **10**(2), 48 (2024)
27. Khawaja, M., Siksek, S.: A single source theorem for primitive points on curves (2024). arXiv:2401.03091
28. Mattuck, A., Tate, J.: On the inequality of Castelnuovo-Severi. Abh. Math. Sem. Univ. Hamburg **22**, 295–299 (1958)
29. Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. (47), 33–186 (1977). With an appendix by Mazur and M, Rapoport (1978)
30. Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. **124**(1–3), 437–449 (1996)
31. Milne, J.S.: Jacobian varieties. In: Arithmetic Geometry (Storrs, Conn., 1984), pp. 167–212. Springer, New York (1986)
32. Najman, F., Orlić, P.: Gonality of the modular curve $X_0(N)$. Math. Comput. **93**(346), 863–886 (2024)
33. Najman, F., Vukorepa, B.: Quadratic points on bielliptic modular curves. Math. Comput. **92**, 1791–1816 (2023)
34. Ogg, A.P.: Hyperelliptic modular curves. Bull. Soc. Math. Fr. **102**, 449–462 (1974)
35. Ozman, E., Siksek, S.: Quadratic points on modular curves. Math. Comput. **88**(319), 2461–2484 (2019)
36. Parent, P.: Torsion des courbes elliptiques sur les corps cubiques. Ann. Inst. Fourier (Grenoble) **50**(3), 723–749 (2000)
37. Parent, P.: No 17-torsion on elliptic curves over cubic number fields. J. Théor. Nombres Bordeaux **15**(3), 831–838 (2003)
38. Serre, J.-P.: Lectures on the Mordell-Weil theorem. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, (1989). Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt
39. Siksek, S.: Chabauty for symmetric powers of curves. Algebra Number Theory **3**(2), 209–236 (2009)
40. Stein, W.: Modular Forms, A Computational Approach, Volume 79 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI (2007). With an Appendix by Paul E. Gunnells
41. Stichtenoth, H.: Algebraic Function Fields and Codes. volume 254 of Graduate Texts in Mathematics, 2nd edn. Springer, Berlin (2009)
42. The LMFDB Collaboration.: The L-functions and modular forms database. http://www.lmfdb.org (2023). Accessed 4 May 2023
43. Yu, M.: Selmer ranks of twists of hyperelliptic curves and superelliptic curves. J. Number Theory **160**, 148–185 (2016)
44. Zarhin, Y.G.: Families of absolutely simple hyperelliptic Jacobians. Proc. Lond. Math. Soc.(3) **100**(1), 24–54 (2010)

Publisher's Note