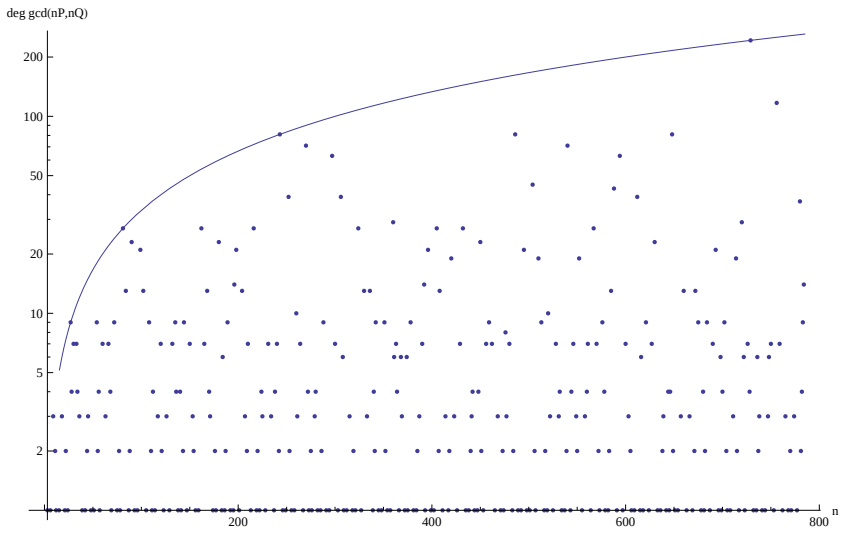
Common Divisors of Elliptic Divisibility Sequences over Function Fields

Jori W. Matthijssen

Master Thesis written at the University of Utrecht,
under the supervision of Prof. Gunther Cornelissen.

September 26, 2011



Pure mathematics is, in its way, the poetry of logical ideas.

Albert Einstein, New York Times, May 1st, 1935.

Abstract

Let $E/k(T)$ be an elliptic curve defined over a rational function field and fix a Weierstrass equation for E. For a point $P \in E(k(T))$, we can write $x_P = \frac{A_P}{B_P^2}$ with relatively prime polynomials $A_P, B_P \in k[T]$. The sequence $(B_{nP})_{n\geq 1}$ is called the *elliptic divisibility sequence* of $P \in E$. For two such elliptic divisibility sequences $(B_{nP})_{n\geq 1}$ and $(B_{nQ})_{n\geq 1}$, we consider the degree of the greatest common divisor of terms in the elliptic divisibility sequences,

$$\deg \gcd(B_{nP}, B_{nQ}).$$

We conjecture a complete theory for how this degree is bounded as n increases, and we support this conjecture with proofs and experiments. In characteristic 0, Silverman already conjectured that this degree is always bounded by a constant, and he gave a proof for curves with constant j-invariant. In characteristic p, Silverman conjectured that there is always a constant c such that there are infinitely many n with

$$\deg \gcd(B_{nP}, B_{nQ}) \geq cn.$$

We conjecture that there are curves that do as well as curves that don't satisfy the stronger bound that

$$\deg \gcd(B_{nP}, B_{nQ}) \geq cn^2$$

for infinitely many n, and that this is still true when we do not allow the field characteristic p to divide n.

Contents

Introduction

Elliptic Divisibility Sequences

Divisibility sequences are not new to mankind. An early example is the well known Fibonacci sequence,

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots,$$

which is given by the linear recurrence relation $F_n = F_{n-1} + F_{n-2}$, and it was used in the metrical sciences in South Asia, its development being attributed in part to Pingala (200 BC), later being associated with Virahanka (circa 700 AD), Gopãla (circa 1135) and Hemachandra (circa 1150) (see [3], pp 226). In the west, the Fibonacci sequence first appears in the book Liber Abaci (1202, see [18]) by Leonardo da Pisa, also known as Fibonacci, who considered the growth of an idealized rabbit population.

A *divisibility sequence* is a sequence

$$n_1, n_2, n_3, \ldots$$

such that $n_i | n_j$ whenever $i|j$. For example, the 10th term of the Fibonacci sequence, 55, is divisible by the 5th term of the Fibonacci sequence, 5. Also, the 12th term of the Fibonacci sequence, 144, is divisible by the 6th term of the Fibonacci sequence, 8. A proof that the Fibonacci sequence is actually a divisibility sequence is given in example 1.1.4.

An *elliptic divisibility sequence* is a special kind of divisibility sequence. The first definition as well as the arithmetic properties of an elliptic divisibility sequence are attributed to Morgan Ward in 1948, and he defined one as

> a sequence of integers,
>
> $$(h) : h_0, h_1, h_2, \ldots, h_n, \ldots$$
>
> which is a particular solution of
>
> $$\omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2$$
>
> and such that h_n divides h_m whenever n divides m,[1]

which he studied using elliptic functions. He directly gives the simple example $h_n = n$, and one easily checks that this is indeed correct. The Fibonacci sequence itself is not an elliptic divisibility sequence: taking $m = 3$ and $n = 2$ we have that the left-hand side gives

$$\omega_{m+n}\omega_{m-n} = 5 \cdot 1 = 5$$

[1] See [25], pp. 1.

while the right-hand side gives

$$\omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2 = 3 \cdot 1 \cdot 1^2 - 2 \cdot 1 \cdot 2^2 = -5.$$

The even terms of the Fibonacci sequence,

$$1, 3, 8, 21, 55, 144 \ldots,$$

do form an elliptic divisibility sequence, and an easy elementary proof that this sequence satisfies the definition given by Ward can be found in [13], example 3.10, pp. 20-21. Moreover, if we would define the Fibonacci sequence up to sign, it would also be an elliptic divisibility sequence: the sign choice

$$1, -1, -2, 3, 5, -8, -13, 21, 34, -55, -89, 144, \ldots$$

makes the Fibonacci sequence into an elliptic divisibility sequence in the definition of Ward.
Elliptic divisibility sequences attracted only sporadic attention until around the year 2000, when they were taken up as a class of nonlinear recurrences that are more amenable to analysis than most such sequences. New applications include a proof of the undecidability of Hilbert's tenth problem over certain rings of integers (logics) by Bjorn Poonen in 2002 (see [14]) and the elliptic curve discrete logarithm problem (cryptography) by Rachel Shipsey in 2000 (see [17]).

In this thesis, we will follow Silverman in using an alternative definition of an elliptic divisibility sequence that is more natural in that it is directly related to elliptic curves. Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^3 + a_4x + a_6.$$

As we will prove in proposition 1.2.1, any nonzero rational point $P \in E(\mathbb{Q})$ can be written in the form

$$P = (x_P, y_P) = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3}\right) \text{ with } \gcd(A_P, B_P) = \gcd(C_P, B_P) = 1,$$

where B_P is defined up to a unit, i.e., up to sign. For P a non-torsion point, the elliptic divisibility sequence associated to $E/\mathbb{Q}$ and P is the sequence of denominators of multiples of P:

$$B_P, B_{2P}, B_{3P}, \ldots.$$

This alternative definition of an elliptic divisibility sequence that we use gives a slightly different collection of divisibility sequences than is given by the classical non-linear recurrence formula. The relationship between these definitions has been formalized in the year 2000 by Rachel Shipsey, see [17].

Above, we described elliptic divisibility sequences for which the elliptic curve

E is defined over $\mathbb{Q}$. We will be looking mostly at elliptic divisibility sequences over function fields; we replace $\mathbb{Q}$ with the rational function field $k(T)$ and replace $\mathbb{Z}$ with the ring of polynomials $k[T]$, and for a point P, we can still write $x_P = \frac{A_P}{B_P^2}$ with $A_P, B_P \in k[T]$ and $\gcd(A_P, B_P) = 1$. Hence we will look at elliptic divisibility sequences $(B_{nP})_{n\geq 1}$ where B_{nP} is the root of the denominator of the x-coordinate of the point nP on an elliptic curve over a function field.

In this thesis, we will look at common divisors of two such elliptic divisibility sequences. More explicitly, given two elliptic divisibility sequences $(B_{nP})_{n\geq 1}$ and $(B_{nQ})_{n\geq 1}$, we look at the degree of $\gcd(B_{nP}, B_{nQ})$, and how this degree behaves as n increases. This means we will look at the following questions:

- What are lower and what are upper bounds for this degree, as n increases?
- In which cases are there infinitely many n such that the degree is bigger than cn for some constant c?
- In which cases are there infinitely many n such that the degree is even bigger than cn^2 for some constant c?
- In which cases are there infinitely many n such that $\gcd(B_{nP}, B_{nQ}) = \gcd(B_P, B_Q)$?

Overview of the Text

Broadly spoken, this thesis can be divided into four parts. Sections 1, 2, 3.1-3.2 and 5.1-5.2 are considered to be preliminaries. Sections 3.3-3.5, 4 and 5.3-5.5 treat what we know from Silverman's article [19] and more. In section 6, we do experiments and examples, and in section 7, a complete theory of bounds on the degree of $\gcd(B_{nP}, B_{nQ})$ is conjectured and explained.

The preliminaries first treat elliptic divisibility sequences in section 1. Here, they are defined over $\mathbb{Q}$ as well as over a function field $k(T)$, and examples are given. In section 2, we introduce elliptic surfaces and several concepts concerning elliptic surfaces and elliptic curves over function fields. At the start of section 3, we define Weil and Cartier divisors, and explore their relationship. At the start of section 5, we treat some additional concepts concerning elliptic curves over a function field in characteristic p. All ideas introduced in the preliminaries can be found in any book about the subject (I mostly used [6], [10], [15], [20] and [21]), and no new or original ideas are created. However, all proofs are mine, unless explicitly stated otherwise.

In the remaining part of section 3, we explore and formalize the relationship between terms in elliptic divisibility sequences B_{nP} arising from a curve over $k(T) = k(\mathbb{P}^1)$ and the pullback divisor $\sigma_P^*(\bar{O})$, and we see how this pullback divisor can be seen as a generalization of elliptic divisibility sequences for curves

over $k(C)$ where C/k is an arbitrary smooth projective curve. Although this relationship is commonly known (on appropriate subsets of the human population), formalizing this relationship is part of my own research.

In section 4, we treat the characteristic 0 case for curves $E/k(C)$ with constant j-invariant as done by Silverman in [19]. Although the proof of the characteristic 0 case is attributed to Silverman, it is important to note that his version is very dense, and I have tried to explain many of the steps in the proof in more detail. Moreover, we finish that section by using the relationship formalized in section 3 to prove a corollary about the case $C = \mathbb{P}^1$, looking at B_{nP} instead of at $\sigma_P^*(\bar{O})$.

In section 5, we treat the characteristic p case for curves $E/k(C)$ with constant j-invariant as done by Silverman in [19]. After doing some additional preliminaries, I have tried to explain many of the steps of his proof in more detail. In 5.6, we take a moment to see if and how this proof can be generalized when taking P and Q on separate curves instead of on a single elliptic curve.

In section 6, the main aim is to get a better grip on the characteristic p case, and to investigate whether or not it is probable that there is a stronger bound such that there are infinitely many n such that the degree of $\gcd(B_{nP}, B_{nQ})$ is bigger than this bound, i.e. a bound of the form cn^2 instead of the cn bound given by the proof of Silverman (where c is a constant).

In chapter 7, we gather all our findings coming from both experiments and proofs, and we conjecture a complete theory for how $\deg \gcd(B_{nP}, B_{nQ})$ is bounded as n increases. Moreover, we recapitulate what is proven so far and we prove some easy additional cases.

Preview

In this thesis, we conjecture a complete theory about the greatest common divisor of elliptic divisibility sequences,

$$\deg \gcd(B_{nP}, B_{nQ}).$$

If P and Q are linearly independent or if one is a torsion point, it seems true that there are infinitely many n such that $\gcd(B_{nP}, B_{nQ}) = \gcd(B_P, B_Q)$. Moreover, we prove that this is the case in characteristic 0 for curves with constant j-invariant in the more general setting

$$\mathrm{GCD}(\sigma_{nP}^*(\bar{O}), \sigma_{nQ}^*(\bar{O})) = \mathrm{GCD}(\sigma_P^*(\bar{O}), \sigma_Q^*(\bar{O}))$$

for infinitely many n. In characteristic p, no proof is given, but the experiments do give a strong inclination to believe this is still the case.
In characteristic 0, the conjecture says that there is a constant c, independent of n, that is an upper bound on $\deg \gcd(B_{nP}, B_{nQ})$. We prove this for curves with

constant j-invariant.
In characteristic p, an obvious quadratic (in n) upper bound is given by the fact that $\deg B_{nP}$ itself grows asymptotically like n^2. We conjecture that for some but not all curves, there are infinitely many n such that

$$\deg \gcd(B_{nP}, B_{nQ}) \geq cn^2$$

for some constant c, and that for all curves the weaker bound

$$\deg \gcd(B_{nP}, B_{nQ}) \geq cn$$

holds. We prove this weaker bound for curves with constant j-invariant.

Acknowledgements

I would like to thank Gunther Cornelissen for suggesting this subject, suggesting many of the used references, as well as taking the time to study difficulties together and to turn unproven lemmas into proven lemmas. I will never forget the time we spend on the fact that "the pullback divisor $\sigma_P^*(\bar{O})$ is, roughly, one half the polar divisor of x_P"([19], pp. 434).
I would also like to thank Rachel for everything non-mathematical during the time I spend on my thesis. I don't think I could have done it without her.

1 Elliptic Divisibility Sequences

1.1 Divisibility Sequences

We start with a standard definition of a divisibility sequence.

Definition 1.1.1. A sequence of integers $(d_n)_{n\geq 1}$ is called a *divisibility sequence*, provided that $d_m|d_n$ when $m|n$.

Here are some easy examples.

Example 1.1.2. The sequence $(n)_{n\geq 1}$ is trivially a divisibility sequence.

Example 1.1.3. The sequence $(a^n-1)_{n\geq 1}$ is a divisibility sequence for every $a \in \mathbb{N}$. For let $m|n$ and $k = \frac{n}{m} \in \mathbb{N}$, then

$$a^n - 1 = a^{k\cdot m} - 1 = (a^m - 1) \cdot \sum_{i=1}^{k} a^{(k-i)m},$$

and thus

$$(a^m - 1)|(a^n - 1).$$

Moreover, this divisibility sequence comes from a rank 1 subgroup of the multiplicative group $\mathbb{G}_m$: we have that $p|a^n - 1$ precisely when $a^n = 1 \bmod p$. There is an analogy between this sequence and elliptic divisibility sequences: with those, we look at $nP = 0 \bmod p$ instead (note that 1 is the identity in the multiplicative group $\mathbb{G}_m$ and that 0 is the identity in additive group E).

Example 1.1.4. The Fibonacci sequence $(F(n))_{n\geq 1}$ is a divisibility sequence. Write $F(1) = 1$, $F(2) = 1$, and $F(n) = F(n-1) + F(n-2)$ and let $m|n$ and $k = n/m \in \mathbb{Z}_{\geq 1}$, then

$$\begin{aligned} F(n) &= F(n-1) + F(n-2) = 2F(n-2) + F(n-3) \\ &= F(2)F(n-1) + F(1)F(n-2) = F(3)F(n-2) + F(2)F(n-3) \\ &= F(m)F(n-m+1) + F(m-1)F(n-m) \\ &= F(m)F((k-1)m+1) + F(m-1)F((k-1)m). \end{aligned}$$

Now, we can continue doing the same again starting with $F((k-1)m)$, and get

$$\begin{aligned} F((k-1)m) &= F(m)F((k-2)m+1) + F(m-1)F((k-2)m)), \\ F(m-1)F((k-1)m) &= F(m)F(m-1)F((k-2)m+1) \\ &\quad + F(m-1)^2F((k-2)m). \end{aligned}$$

Repeating this $k-1$ times, we get

$$\begin{aligned} F(n) &= \left(\sum_{i=1}^{k-1} F(m-1)^{i-1}F(m)F((k-i)m+1)\right) + F(m-1)^{k-1}F(m) \\ &= F(m)\left(\left(\sum_{i=1}^{k-1} F(m-1)^{i-1}F((k-i)m+1)\right) + F(m-1)^{k-1}\right) \end{aligned}$$

and thus $F(m)|F(n)$.

1.2 Elliptic Divisibility Sequences over $\mathbb{Q}$

Let $E/\mathbb{Q}$ be an elliptic curve given by the Weierstrass equation $y^2 = x^3 + Ax + B$ with integer coefficients. To define elliptic divisibility sequences, we need the form of a point on such a curve.

Proposition 1.2.1. *We can write any nonzero rational point $P \in E(\mathbb{Q})$ as*

$$P = (x_p, y_P) = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3}\right),$$

where A_P, B_P and C_P are integers with $\gcd(A_P, B_P) = \gcd(C_P, B_P) = 1$.

Proof. This is a simple elementary proof. Let $(x, y) \in E/\mathbb{Q}$ be a point on some elliptic curve given by the Weierstrass equation $y^2 = x^3 + Ax + B$. Write

$$x = \frac{a}{b} \quad \text{and} \quad y = \frac{c}{d}$$

with $a, b, c, d \in \mathbb{Z}$ and $\gcd(a, b) = \gcd(c, d) = 1$. Then the Weierstrass equation gives us that

$$\frac{c^2}{d^2} = \frac{a^3 + Aab^2 + Bb^3}{b^3}.$$

Since $b|Bb^3$, $b|Aab^2$ and $\gcd(b^3, a^3) = 1$, we have that

$$\gcd(a^3 + Aab^2 + Bb^3, b^3) = 1$$

and hence we have that $d^2 = b^3$. Moreover, this means that $d = \sqrt{b^3}$ and hence that b is a square $b = B_P^2$, and therefore that $d = \sqrt{B_P^6} = B_P^3$. This completes the proof. □

Now, we can define what we mean with an elliptic divisibility sequence, namely a sequence of denominators $(B_{nP})_{n\geq 1}$.

Definition 1.2.2. The *elliptic divisibility sequence* associated to $E/\mathbb{Q}$ and P is the sequence $(B_{nP})_{n\geq 1}$ of denominators of multiples of P.

Remark 1.2.3. In the proof of proposition 1.2.1, B_P is only defined up to sign: we can change the sign of B_P if we also change the sign of C_P. Hence the elliptic divisibility sequence $(B_{nP})_{n\geq 1}$ is also only defined up to sign. Since we will only look at divisibility properties, this is not a problem.

The following proposition says that an elliptic divisibility sequence indeed is a divisibility sequence.

Proposition 1.2.4. *Let $(B_{nP})_{n\geq 1}$ be an elliptic divisibility sequence. Then $B_{mP}|B_{nP}$ when $m|n$. In other words, $(B_{nP})_{n\geq 1}$ is a divisibility sequence.*

Proof. The proof of this proposition is based on formal groups. Since the machinery needed for this proof is very different from the rest of the thesis, it will be omitted. For a proof, see [2], lemma 2.6, pp. 14. □

Remark 1.2.5. As is also shown in [2], an elliptic divisibility sequence even satisfies the stronger condition that

$$\gcd(B_{mP}, B_{nP}) = B_{\gcd(m,n)P},$$

and is therefore often called a *strong divisibility sequence*.

Example 1.2.6. As said in the introduction, we know that the even terms of the Fibonacci sequence,

$$1, 3, 8, 21, 55, 144, \ldots,$$

form an elliptic divisibility sequence as in Wards definition, see [13], example 3.10, pp. 20-21. The elliptic curve associated to this elliptic divisibility sequence (see [22], proposition 4.5.3, pp. 59) is the singular curve

$$E : y^2 + 3xy + 3y = x^3 + 2x^2 + x,$$

with the point $P = (0, 0)$. Since this curve is singular, we have that this sequence is not an elliptic divisibility sequence in our sense of the word.

Example 1.2.7. Let $E : y^2 = x^3 + x + 1$ and look at the point $P = (0, 1)$. We can look at the elliptic divisibility sequence $(B_{nP})_{n\geq 1}$. Its few terms are given in table 1.

$B_1 = 1$
$B_2 = 2$
$B_3 = 1$
$B_4 = 36 = 2^2 \cdot 3^2$
$B_5 = 287 = 7 \cdot 41$
$B_6 = 1222 = 2 \cdot 13 \cdot 47$
$B_7 = 93599 = 11 \cdot 67 \cdot 127$
$B_8 = 2943288 = 2^3 \cdot 3^2 \cdot 40879$
$B_9 = 80653535 = 5 \cdot 503 \cdot 32069$
$B_{10} = 17621453878 = 2 \cdot 7 \cdot 41 \cdot 30699397$
$B_{11} = 2146978731169 = 418 \cdot 5124054251$
$B_{12} = 340830164675988 = 2^2 \cdot 3^3 \cdot 13 \cdot 29 \cdot 37 \cdot 47 \cdot 1721 \cdot 2797$
$B_{13} = 240710769046691137 = 240710769046691137$
$B_{14} = 110719491046597707406 = 2 \cdot 11 \cdot 67 \cdot 127 \cdot 591456591665497$
$B_{15} = 97293858000319762026049 = 7 \cdot 41 \cdot 36097 \cdot 79588361 \cdot 118000231$

Table 1: First 15 terms of the elliptic divisibility sequence $(B_{nP})_{n\geq 1}$ with $y^2 = x^3 + x + 1$ and $P = (0, 1)$.

1.3 Elliptic Divisibility Sequences over Function Fields

Let k be any field. Often we will assume that k is algebraically closed, but in general this assumption is not made. Above, we defined elliptic divisibility

sequences over $\mathbb{Q}$. Instead of working over $\mathbb{Q}$, we can also work over a function field $k(T)$, where we replace the ring of integers $\mathbb{Z}$ with the ring of polynomials $k[T]$. In section 2, we will see how elliptic curves over function fields $k(T)$ correspond to elliptic surfaces over k, and what they are like.
Let $E/k(T)$ be an elliptic curve given by the Weierstrass equation $y^2 = x^3+Ax+B$ with $A, B \in k[T]$. Just like in the case over $\mathbb{Q}$, we can write a point on the elliptic curve as

$$P = (x_p, y_P) = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3}\right)$$

with $A_P, B_P, C_P \in k[T]$ and $\gcd(A_P, B_P) = \gcd(A_P, C_P) = 1$. Moreover, the proof given above carries over completely to this function field case. This means that we have elliptic divisibility sequences over function fields in the same way as over $\mathbb{Q}$.

Definition 1.3.1. Let K be a function field. The *elliptic divisibility sequence* associated to E/K and P is the sequence $(B_{nP})_{n\geq 1}$ of denominators of multiples of P.

Remark 1.3.2. In the proof of proposition 1.2.1, B_P was only defined up to a unit. As we carry that proof to the function field case, we also have that the sequence $(B_{nP})_{n\geq 1}$ is defined up to a unit in the function field. For $K = k(T)$, we have that B_P is defined up to multiplication by a constant in k^*, and as a convention, this means we will choose to always write B_P monic.

Example 1.3.3. Let $E : y^2 = x^3 - T^2x + 1$, take the point $P_1 = (x_P, y_P) = (T, 1)$ and look at the elliptic divisibility sequence $(B_{nP})_{n\geq 1}$ in characteristic 0. Its first few terms are given in table 2.

$B_1 = 1$
$B_2 = 1$
$B_3 = t \cdot (t^3 - 3)$
$B_4 = t^6 - 3t^3 + 1$
$B_5 = t^{12} - 9t^9 + 23t^6 - 15t^3 - 4$
$B_6 = t(t^3 - 3)(t^{12} - 5t^9 + 7t^6 - 3t^3 + 8/3)$
$B_7 = t^{24} - 18t^{21} + 115t^{18} - 348t^{15} + 515t^{12} - 270t^9 - 183t^6 + 252t^3 - 16$
$B_8 = (t^6-3t^3+1)\cdot(t^{24}-12t^{21}+55t^{18}-120t^{15}+135t^{12}-132t^9+209t^6-168t^3-8)$
$B_9 = t \cdot (t^3 - 3) \cdot (t^{36} - 27t^{33} + 264t^{30} - 1344t^{27} + 4038t^{24} - 7254t^{21} + 6204t^{18} + 3672t^{15} - 16623t^{12} + 17817t^9 - 7068t^6 + 576t^3 - 192)$
$B_{10} = (t^{12}-9t^9+23t^6-15t^3-4)(t^{36}-15t^{33}+468/5t^{30}-1548/5t^{27}+2914/5t^{24}-762t^{21}+1544t^{18}-20844/5t^{15}+34929/5t^{12}-30507/5t^9+2620t^6-624t^3+64/5)$

Table 2: First 10 terms of the elliptic divisibility sequence $(B_{nP})_{n\geq 1}$ of $y^2 = x^3 - T^2x + 1$ and $P = (T, 1)$, factored over $\mathbb{Q}$.

2 Elliptic Surfaces

Let k be a field (of characteristic $\neq 2$) and let $A(T)$, $B(T) \in k(T)$ be rational functions of the parameter T. We can look at a family of elliptic curves

$$E_T : y^2 = x^3 + A(T)x + B(T).$$

Substituting $T = t$ for some $t \in \bar{k}$, we get that E_t is an elliptic curve provided that $A(t)$ and $B(t)$ are finite and $\Delta(t) = -16(4A(t)^3 + 27B(t)^2)$ is nonzero.

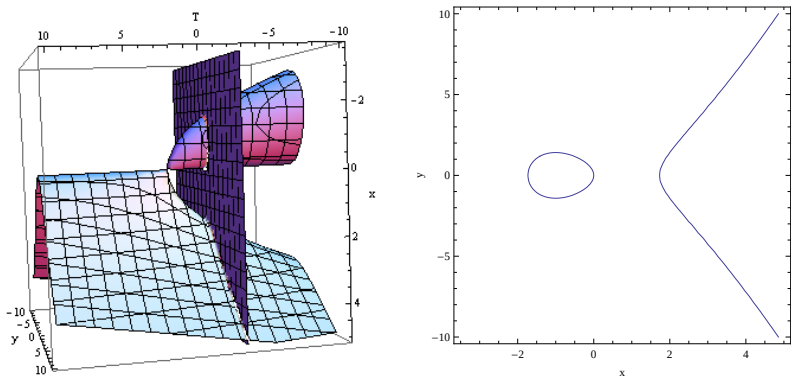


Figure 1: Left: the family of elliptic curves $E_T : y^2 = x^3 + Tx$ intersected with the plane $T = 3$. Right: the elliptic curve E_3.

Instead of looking at it this way, we can also look at the single elliptic curve

$$E : y^2 = x^3 + A(T)x + B(T)$$

defined over the function field $k(T)$. This is an elliptic curve provided that

$$\Delta(T) = -16(4A(T)^3 + 27B(T)^2) \neq 0.$$

For example, we can look at the curve $E : y^2 = x^3 - T^2x + T^2$ and find the point $(T, T) \in E(k(T))$.

We can generalize this even more: above, we assumed that A and B lie in the field of rational functions $k(T)$. $k(T)$ is the function field of the projective line $\mathbb{P}^1$. Instead, we can take any non-singular projective curve C/k and look at elliptic curves E defined over the field $k(C)$. To define the field $k(C)$, we first recall the definition of the local ring of X along Y.

Definition 2.0.4. If x is a point on a variety X, then we define the *local ring of X at x*, denoted $\mathcal{O}_{x,X}$, as the ring of functions that are regular at x, where we identify two such functions if they coincide on some open (using the Zariski topology) neighborhood of x. If X is a variety and $Y \subset X$ is a subvariety, then

we define the *local ring of X along Y*, denoted $\mathcal{O}_{Y,X}$, as the set of pairs (U, f), where U is open in X, $U \cap Y \neq \emptyset$ and $f \in \mathcal{O}(U)$ is a regular function on U, and we identify two pairs $(U_1, f_1) = (U_2, f_2)$ if $f_1 = f_2$ on $U_1 \cap U_2$.

Using this, we can define the function field $\bar{k}(X)$ of X:

Definition 2.0.5. Let X be a variety. The *function field of X*, denoted by $\bar{k}(X)$ (sometimes just $k(X)$), is defined to be $\mathcal{O}_{X,X}$, the local ring of X along X. In other words, $\bar{k}(X)$ is the set of pairs (U, f) where U is a non-empty open subset (in the Zariski topology) of X and f is a regular function on U, subject to the identification $(U_1, f_1) = (U_2, f_2)$ if $f_1|_{U_1 \cap U_2} = f_2|_{U_1 \cap U_2}$.

Remark 2.0.6. Note that the function field of X is indeed a field: in a pair (U, f), f is a regular function, and can be written

$$f = g(x)/h(x),$$

where $h(x) \neq 0$ on U. f has multiplicative inverse $f^{-1} = h(x)/g(x)$ and this is defined on the open $V = X - Z(g)$, hence the inverse of the pair

$$(U, f) = \left(U, \frac{g(x)}{h(x)}\right)$$

is the pair

$$(V, f^{-1}) = \left(X - Z(g), \frac{h(x)}{g(x)}\right).$$

Also, we have that the multiplication is commutative: let $f_1 = g_1/h_1, f_2 = g_2/h_2$ be regular and let $U_1 = X - Z(h_1)$ and $U_2 = X - Z(h_2)$, then $U_1 \cap U_2 \neq \emptyset$ and

$$(U_1, f_1) \cdot (U_2, f_2) = (U_1 \cap U_2, f_1 \cdot f_2) = (U_1 \cap U_2, f_2 \cdot f_1) = (U_2, f_2) \cdot (U_1, f_1).$$

Proposition 2.0.7. *For k algebraically closed, we have that $k(T)$ is the function field of the projective line $\mathbb{P}^1$.*

Proof. $k(T)$ is the rational function field and its elements are rational functions $f = \frac{g(T)}{h(T)}$ with g, h polynomials in $k[T]$. The function field of the projective line is given by pairs (U, f) where U is open in the projective line and f is regular on U, i.e., we have that $f(x) = \frac{g(x)}{h(x)}$ with $h(x) \neq 0$ on U. An element f of $k(T)$ having poles $\alpha_1, \ldots, \alpha_n$ indeed corresponds to any pair (U, f) where U does not contain $\alpha_1, \ldots, \alpha_n$. The other way around, two pairs (U, f) and (V, f) are the same precisely when they're both equal to $(\mathbb{P}^1 - \{\alpha_1, \ldots, \alpha_n\}, f)$, and this last pair corresponds to a rational function in $k(T)$. Thus $k(T)$ is precisely the function field of $\mathbb{P}^1$. □

Intuitively, assuming that $k = \bar{k}$, this means that the function field $k(C)$ of a curve C can be seen as the field of functions $C \to k$, poles allowed, that are regular on some open subsets of C.

Now, fix a non-singular projective curve C/k and take

$$E : y^2 = x^3 + Ax + B$$

with $A, B \in k(C)$ such that $4A^3 + 27B^2 \neq 0$. As mentioned above, for almost all points $t \in C(\bar{k})$ we can evaluate A and B at t and get an elliptic curve E_t. Instead, we can also treat the variable t just like we treat x and y. Then, we look at the surface formed from elliptic curves

$$\mathcal{E} = \{([X : Y : Z], t) \in \mathbb{P}^2 \times C \mid Y^2Z = X^3 + AZ^2 + BZ^3\},$$

where $A, B \in k(C)$. This forms the basis for the formal definition of an elliptic surface.

Definition 2.0.8. Let C/k be a nonsingular projective curve. An *elliptic surface* is a triple $(\mathcal{E}, \pi, \sigma)$ with the properties that

1. $\mathcal{E}$ is a surface, i.e., a two-dimensional projective variety over k,
2. π is a morphism
$$\pi : \mathcal{E} \to C$$
over k such that for all but finitely many points $t \in C(\bar{k})$, the fibre
$$\mathcal{E}_t = \pi^{-1}(t)$$
is a non-singular curve of genus 1 over $\bar{k}$,
3. σ is a section
$$\sigma : C \to \mathcal{E}$$
to π, i.e., σ is a morphism such that the composition $\pi \circ \sigma : C \to C$ is the identity map on C.

Often, we will just say that $\mathcal{E}$ is an elliptic surface, implicitly assuming that there is a π and a σ given.

Remark 2.0.9. In geometry, the most common definition of an elliptic surface does not assume the existence of section, our third assumption, which leads to many interesting geometrical questions, such as the possibility of the existence of multiple fibres. Because the emphasis in this thesis lies in number theory rather than in geometry, we will always assume the existence of a section σ.

2.1 Isogenies

Let us recall that an isogeny is a morphism between two elliptic curves, possibly over some function fields, that respects the point at infinity.

Definition 2.1.1. Let E_1, E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism

$$\phi : E_1 \to E_2$$

satisfying $\phi(O_1) = O_2$, where O_1 and O_2 are the points at infinity of E_1 and E_2 respectively. E_1 and E_2 are called *isogenous* if there is an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{O_2\}$.

An isogeny turns out to commute with the group operations.

Theorem 2.1.2. *Let*

$$\phi : E_1 \to E_2$$

be an isogeny of elliptic curves. Then

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

for all $P, Q \in E_1$.

Proof. See [21], theorem III.4.8, pp.71. □

From the definition, it is not directly clear that being isogenous is an equivalence relation. The following theorem says that given a non-zero isogeny $\phi : E_1 \to E_2$, we can always construct the dual isogeny $\hat{\phi} : E_2 \to E_1$. With this, it follows that being isogenous is indeed an equivalence relation.

Theorem 2.1.3. *Let* $\phi : E_1 \to E_2$ *be a nonconstant isogeny of degree* m. *Then there exists a unique isogeny*

$$\hat{\phi} : E_2 \to E_1$$

satisfying $\hat{\phi} \circ \phi = [m]$, *where* $[m]$ *is the multiplication-by-*m *map.*

Proof. See [21], theorem III.6.1, pp. 81. □

Definition 2.1.4. Let $\phi : E_1 \to E_2$ be an isogeny. The *dual isogeny to* ϕ is the isogeny $\hat{\phi}$ given above, unless ϕ is constant, then the dual isogeny is [0].

2.2 Birational Equivalence

We would like to be able to associate an elliptic surface $\mathcal{E}$ to an elliptic curve $E/k(C)$, because as we've seen before, an elliptic surface and an elliptic curve over a function field are rather two ways of looking at 'the same thing'. For this, we will first define birational equivalence - first for projective varieties, then for elliptic surfaces.

Definition 2.2.1. Let V and W be projective varieties. A *rational map* from V to W is an equivalence class of pairs (U, ϕ_U), where U is non-empty open in V and $\phi_U : U \to W$ is a morphism, and two pairs $(U_1, \phi_{U_1}), (U_2, \phi_{U_2})$ are deemed equivalent if $\phi_{U_1} = \phi_{U_2}$ on $U_1 \cap U_2$.
A rational map $\phi : V \to W$ is a *birational isomorphism* if it has rational inverse

$\psi : W \to V$; that is, $\overline{\phi(V)} = W$, $\overline{\psi(W)} = V$ and the maps $\phi \circ \psi : W \to W$ and $\psi \circ \phi : V \to V$ are the identity maps at all points for which they are defined. If there is a birational isomorphism between V and W, then V and W are said to be *birationally equivalent*.

Remark 2.2.2. Note that we require for a rational inverse not only that the compositions are identity maps at all points for which they are defined, but also that $\overline{\phi(V)} = W$ and $\overline{\psi(W)} = V$. This is to exclude cases like the following: let V be some curve and let $W = \text{curve} \cup \{pt\}$ consist of a point and a curve, and assume that there is a rational map from V to the curve of W with the property that there is a rational map from W to V such that the compositions are identity maps at all points for which they are defined (i.e. assume that V and the curve of W are isomorphic). We do not want to call this map a birational isomorphism: it does nothing with the separate point of W. To avoid cases in which isolated parts of W or V aren't mapped to at all, we require that $\overline{\phi(V)} = W$ and $\overline{\psi(W)} = V$ before we call something a birational isomorphism.

We are now ready to say when two elliptic surfaces are birational equivalent.

Definition 2.2.3. Let $(\mathcal{E}_1, \pi_1, \sigma_1)$, $(\mathcal{E}_2, \pi_2, \sigma_2)$ be two elliptic surfaces over C. A *rational map from $\mathcal{E}_1$ to $\mathcal{E}_2$ over C* is a rational map $\phi : \mathcal{E}_1 \to \mathcal{E}_2$ which commutes with the projection maps, i.e., with the property that $\pi_2 \circ \phi = \pi_1$. The surfaces $\mathcal{E}_1$ and $\mathcal{E}_2$ are *birational equivalent over C* if there is a birational isomorphism $\phi : \mathcal{E}_1 \to \mathcal{E}_2$ which commutes with the projection maps.

Now, we can state the proposition that explains precisely how the theory of elliptic curves over a function fields $k(C)$ is the same as the birational theory of elliptic surfaces over C.

Proposition 2.2.4. *Let $E/k(C)$ be an elliptic curve. To each Weierstrass equation for E,*

$$E : y^2 = x^3 + Ax + B$$

with $A, B \in k(C)$, we associate an elliptic surface

$$\mathcal{E}(A, B) = \{([X : Y : Z], t) \in \mathbb{P}^2 \times C : Y^2Z = X^3 + AXZ^2 + BZ^3\}.$$

Then all of the $\mathcal{E}(A, B)$ associated to E are k-birationally equivalent over C. Let $\mathcal{E}$ be an elliptic surface over C/k, then $\mathcal{E}$ is k-birationally equivalent over C to $\mathcal{E}(A, B)$ for some $A, B \in k(C)$. Furthermore, the elliptic curve $E : y^2 = x^3 + Ax + B$ is uniquely determined (up to $k(C)$-isomorphism) by $\mathcal{E}$.

Proof. See [20], Proposition 3.8, pp. 206. □

Definition 2.2.5. Let $\mathcal{E}$ be an elliptic surface over k. For a point P on the corresponding elliptic curve over $k(C)$, there is a map

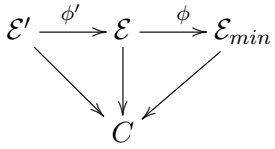
$$\sigma_P : C \to \mathcal{E} : t \to (P_t, t)$$

that sends t to P evaluated at t.

2.3 Minimal Elliptic Surfaces

Now, we will define what it means for an elliptic surface to be minimal.

Theorem 2.3.1. *Let $\mathcal{E} \to C$ be an elliptic surface. Then there exists an elliptic surface $\mathcal{E}_{min} \to C$ and a birational map $\phi : \mathcal{E} \to \mathcal{E}_{min}$ commuting with the maps to C with the following property:*
Let $\mathcal{E}' \to C$ be an elliptic surface, and let $\phi' : \mathcal{E}' \to \mathcal{E}$ be a birational map commuting with the maps to C. Then the rational map $\phi \circ \phi'$ extends to a morphism. In other words, the top line of the following commutative diagram extends to a morphism:



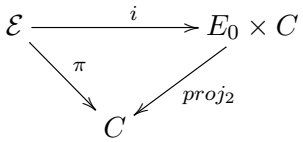
Proof. See [20], theorem 8.4, p. 244. □

Definition 2.3.2. Let $\mathcal{E} \to C$ be an elliptic surface. We say that this elliptic surface is minimal, if it is equal to some $\mathcal{E}_{min}$.

2.4 Split Elliptic Surfaces

An elliptic surface $\mathcal{E}$ over a field k is said to split if it is isomorphic to the product of an elliptic curve over k and the curve C, with an additional constraint on π.

Definition 2.4.1. An elliptic surface $\mathcal{E}$ *splits* over k if there is an elliptic curve E_0/k and a birational isomorphism $i : \mathcal{E} \to E_0 \times C$ such that the following diagram commutes:



Example 2.4.2. Let $\mathcal{E} : y^2 = x^3 + T^4x$ be an elliptic surface with $C = \mathbb{P}^1$ and let $E_0 : y^2 = x^3 + x$ be an elliptic curve, then there is an isomorphism

$$i : \mathcal{E} \to E_0 \times \mathbb{P}^1 : ((x, y), t) \to ((t^{-2}x, t^{-3}y), t),$$

where for $((x, y), t) \in \mathcal{E}$, we have

$$(t^{-2}x)^3 + (t^{-2}x) = t^{-6}(x^3 + t^4x) = t^{-6}y^2 = (yt^{-3})^2,$$

so i indeed maps to $E_0 \times \mathbb{P}^1$. Moreover, we have that $\pi : ((x, y), t) \to t$ factors through $E_0 \times \mathbb{P}^1$, thus we have that $\mathcal{E}$ splits over k.

Example 2.4.3. Let $\mathcal{E} : y^2 = x^3 + Tx$ be an elliptic surface with $C = \mathbb{P}^1$ and let $E_0 : y^2 = x^3 + x$ be an elliptic curve, then there is an isomorphism

$$i : \mathcal{E} \to E_0 \times \mathbb{P}^1 : ((x, y), t) \to ((t^{-1/2}x, t^{-1/4}y), t),$$

but this isomorphism is not defined over k, so $\mathcal{E}$ does not split over k. However, it does split if we replace the base field $k(T)$ by the finite field extension $k(T^{1/4})$.

Example 2.4.4. Let $\mathcal{E} : y^2 = x^3 + Tx + T$ be an elliptic surface with $C = \mathbb{P}^1$. This surface does not split over k, not even when we replace the base field by some larger field. This is because its j-invariant is not constant, see remark 2.5.4 below.

Proposition 2.4.5. *Let $\mathcal{E} \to C$ be an elliptic surface over k, and let E/K be the associated elliptic curve over the function field $K = k(C)$. Then $\mathcal{E} \to C$ splits over k if and only if there is an elliptic curve E_0/k and an isomorphism $E \to E_0$ defined over K.*

Proof. This proof comes from [20], proposition 5.1, pp. 221.
Suppose first that $\pi : \mathcal{E} \to C$ splits. This means that there is a birational isomorphism

$$i : \mathcal{E} \to E_0 \times C$$

so that $proj_2 \circ i = \pi$. A dominant rational map induces a corresponding map on function fields (see [20], proposition 3.7, pp. 205), so we obtain an isomorphism

$$k(\mathcal{E}) \simeq k(E_0 \times C)$$

which is compatible with the inclusions $k(C) \to k(\mathcal{E})$ and $k(C) \to k(E_0 \times C)$.
In other words, writing $K = k(C)$, the fields $k(\mathcal{E}) = K(E)$ and $k(E_0 \times C) = K(E_0)$ are isomorphic as K-algebras. Each of them is a field of transcendence degree 1 over K, so each corresponds to a unique non-singular curve defined over K(see [6], I.6.12). In other words, there is an isomorphism $E \simeq E_0$ defined over K.
Now assume that we are given an elliptic curve E_0/k and an isomorphism $E \to E_0$ defined over K. Then $K(E) \simeq K(E_0)$ as K-algebras, which is the same as saying that

$$k(\mathcal{E}) \simeq k(E_0 \times C)$$

as $k(C)$-algebras. Again using [20], proposition 3.7, this isomorphism of fields induces a birational isomorphism of varieties $\mathcal{E} \to E_0 \times C$ commuting with the maps to C, which shows that $\mathcal{E} \to C$ splits over k. This completes the proof. □

Definition 2.4.6. Let $\mathcal{E} \to C$ be an elliptic surface over k, and let E/K be the associated elliptic curve over the function field $K = k(C)$. We say that E/K *splits over* K if $\mathcal{E} \to C$ splits over k, or in other words, if there is an elliptic curve E_0/k and an isomorphism $E \to E_0$ defined over K.

2.5 J-Invariant

In this subsection, we will first recall the definition of the j-invariant of an elliptic curve, and after that, we will use this definition to see the j-invariant of an elliptic surface as the j-invariant of $\mathcal{E}_t$ at each $t \in C$. Then we will be able to state a theorem that tells us how the splitting of an elliptic surface depends on this j-invariant.

Definition 2.5.1. Fix an elliptic curve $E : y^2 = x^3 + Ax + B$. We define *the j-invariant of E* as

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Let $\mathcal{E}$ be an elliptic surface over k. We define *the j-invariant of $\mathcal{E}$* as the map

$$j_{\mathcal{E}} : C \to \mathbb{P}^1 : t \to j(\mathcal{E}_t).$$

More precisely, $j_{\mathcal{E}}(t)$ is the j-invariant of the elliptic curve $\mathcal{E}_t$ provided that the fiber $\mathcal{E}_t$ is non-singular, and at the remaining points of C, it is defined by extending $j_{\mathcal{E}}$ to a morphism as in the following proposition.

Proposition 2.5.2. *$j_{\mathcal{E}}$ is an algebraic map, and it extends to a morphism from C to $\mathbb{P}^1$.*

Proof. We know that the fiber $\mathcal{E}_t$ is non-singular if and only if the discriminant $4A(t)^3 + 27B(t)^2$ is not equal to zero. This means that if the fiber $\mathcal{E}_t$ is non-singular, then we have that $j_{\mathcal{E}}(t) \in \mathbb{A}^1 \subset \mathbb{P}^1$. Hence the map we defined so far is a map

$$j_{\mathcal{E}} : \{t \in C | 4A(t)^3 + 27B(t)^2 \neq 0\} \to \mathbb{A}^1 \subset \mathbb{P}^1 : t \to j(\mathcal{E}_t)$$

Since A and B are elements of the function field $k(C)$ of C, we now indeed have that

$$1728\frac{4A(t)^3}{4A(t)^3 + 27B(t)^2}$$

is regular on

$$\{t \in C | 4A(t)^3 + 27B(t)^2 \neq 0\},$$

and hence $j_{\mathcal{E}}$ is an algebraic map. It extends to a morphism from C to $\mathbb{P}^1$ by letting it send a point $t \in C$ for which $\mathcal{E}_t$ is singular to the point $\infty = (1 : 0) \in \mathbb{P}^1$. □

Now we have an important proposition, which says that an elliptic surface splits over some finite field extension of $K = k(C)$ provided that its j-invariant is constant.

Proposition 2.5.3. *Let $\mathcal{E} \to C$ be an elliptic surface defined over k, and choose a Weierstrass equation*

$$\mathcal{E} : y^2 = x^3 + Ax + B$$

with $A, B \in k(C)$. Assume that the j-invariant is constant, i.e., assume that there is a constant c such that $j_{\mathcal{E}}(C) = \{c\}$. Then E/K splits over a finite field extension of $K = k(C)$.

Remark 2.5.4. The reverse of this proposition is also true, and is very easy: if an elliptic surface splits over a finite field extension, we have an E_0 and a C' such that $\mathcal{E} \simeq E_0 \times C'$, and hence $j_{\mathcal{E}}(t) = j_{E_0 \times C'}(t) = j(E_0)$ is constant.

The following lemma is an elementary result. Since the proof would require us to dive into long elementary algebra calculations, we will assume it without proof.

Lemma 2.5.5. *Let $\mathcal{E} \to C$ be an elliptic curve over k, and choose a Weierstrass equation*

$$\mathcal{E} : y^2 = x^3 + Ax + B$$

with $A, B \in k(C)$. Then $\mathcal{E} \to C$ splits over k if and only if one of the following is true:

- *$j_{\mathcal{E}}(C) = \{0\}$ and c_6 is a 6th power,*
- *$j_{\mathcal{E}}(C) = \{1728\}$ and c_4 is a 4th power,*
- *$j_{\mathcal{E}}(C) = \{a\}$ with $a \neq 0, 1728$ and c_6/c_4 is a square,*

where c_4 and c_6 are the usual constants form [21], pp. 42, namely $c_4 = 16(A^2 - 3A)$ and $c_6 = -64A^3 + 288A^2 - 864B$.

Proof of proposition 2.5.3. The proposition is a corollary of the above lemma: take a finite field extension K' of $K = k(C)$ in which c_6 is a 6th power, c_4 is a 4th power and c_6/c_4 is a square and assume that the j-invariant is constant. Then $\mathcal{E} \to C$ splits over k by the lemma, and E/K splits over the finite field extension K' of $K = k(C)$. □

2.6 Heights on Elliptic Curves over Function Fields

In this subsection, we will give a criterium for an elliptic surface over a closed field k to split over k. It makes use of the height function on the function field K.

Definition 2.6.1. Let $K = k(C)$ be the function field of a non-singular algebraic curve C/k. The *height of an element $f \in K$* is defined to be the degree of the assiciated map from C to $\mathbb{P}^1$,

$$h(f) = \deg(f : C \to \mathbb{P}^1).$$

In particular, if $f \in k$, then the map is constant and we set $h(f) = 0$.
For an elliptic curve E/K given by some Weierstrass equation, the *height of a point $P \in E(K)$* is defined to be

$$h(P) = \begin{cases} 0 & \text{if } P = O \\ h(x) & \text{if } P = (x, y). \end{cases}$$

We now have the following criterium for an elliptic surface to split.

Theorem 2.6.2. *Let $\mathcal{E} \to C$ be an elliptic surface over an algebraically closed field k, let E/K be the corresponding elliptic curve over the function field $K = k(C)$, and let d be a constant. If the set*

$$\{P \in E(K) | h(P) \leq d\}$$

contains infinitely many points, then $\mathcal{E}$ splits over k.

Proof. See [20], theorem III.5.4, pp. 222. □

2.7 Twisting

By a twist of a curve E/K we mean another curve E'/K such that they are isomorphic over $\bar{K}$.

Definition 2.7.1. Let E/K be a smooth projective curve. *A twist of E/K* is a smooth curve E'/K that is isomorphic to E over $\bar{K}$. We treat two twists as equivalent if they are isomorphic over K. *The set of twists of E/K*, modulo K-isomorphism, is denoted by $\mathrm{Twist}(E/K)$.
If E/K is an elliptic curve, then a twist of E/K is another elliptic curve E'/K that is isomorphic to E over $\bar{K}$ as an elliptic curve - that is, the isomorphism must preserve the base point O. *The set of twists of E/K*, modulo K-isomorphism, is then denoted by $\mathrm{Twist}((E,O)/K)$.

If the characteristic of K is not 2 or 3, then the elements of $\mathrm{Twist}((E,O)/K)$ can be described quite explicitly.

Proposition 2.7.2. *Assume that* $\mathrm{char}(K) \neq 2, 3$ *and let*

$$n = \begin{cases} 2 & \text{if } j(E) \neq 0, 1728 \\ 4 & \text{if } j(E) = 1728 \\ 6 & \text{if } j(E) = 0. \end{cases}$$

Then $\mathrm{Twist}((E,O)/K)$ *is canonically isomorphic to $K^*/(K^*)^n$. More precisely, choose a Weierstrass equation $E : y^2 = x^3 + Ax + B$ for E/K and let $D \in K^*$, then the elliptic curve $E_D \in \mathrm{Twist}((E,O)/K)$ corresponding to $D(\mathrm{mod}(K^*)^n)$ has Weierstrass equation*

$$E_D : \begin{cases} y^2 = x^3 + D^2Ax + D^3B & \text{if } j(E) \neq 0, 1728 \\ y^2 = x^3 + DAx & \text{if } j(E) = 1728 \\ y^2 = x^3 + DB & \text{if } j(E) = 0. \end{cases}$$

Proof. See [21], proposition X.5.4, pp. 343. □

3 Divisors and their GCD

We will work mostly with Weil divisors. Because the pullback of a divisor is more natural using Cartier divisors, we will also introduce them and their relation to Weil divisors. After that, we introduce the pullback divisor $\sigma_P^*(\bar{O})$ for $\sigma_P^* : C \to \mathcal{E} : t \to (P_t, t)$ and $\bar{O}$ the divisor of the curve at infinity on $\mathcal{E}$. Furthermore, we will show the relation between this pullback divisor $\sigma_P^*(\bar{O})$ and elliptic divisibility sequences $(B_{nP})_{n\geq 1}$ explicitly.

3.1 Weil Divisors

We start with the definition of a Weil divisor.

Definition 3.1.1. Let X be an algebraic variety. A *Weil divisor* is a finite formal sum of subvarieties of codimension one, and the *group of Weil divisors* $\mathrm{Div}(X)$ on X is the free abelian group generated by the closed subvarieties of codimension one on X.

This means that we can write a divisor as a finite formal sum of the form

$$D = \sum n_Y Y,$$

where the n_Y's are integers and the Y's are subvarieties of X of codimension one. In the case of elliptic surfaces, the Y's are the irreducible curves lying on the surface.
The *support of a divisor* is the union of all the Y's for which the multiplicity n_Y is nonzero, and a divisor is called *effective* (or *positive*) if every $n_Y \geq 0$. The *degree* of a divisor D is

$$\deg(D) = \sum n_P.$$

We recall that the *local ring of X along Y*, denoted $\mathcal{O}_{Y,X}$, is the set of pairs (U, f), where U is open in X with $U \cap Y \neq \emptyset$ and f is regular on U, where we identify two pairs $(U_1, f_1) = (U_2, f_2)$ whenever $f_1|_{U_1 \cap U_2} = f_2|_{U_1 \cap U_2}$. For a rational function, we would like to define its order at a point, as the multiplicity of the zero at that point, or minus the multiplicity of the pole if the function has a pole at that point. For this, we first need the definition of a discrete valuation ring.

Definition 3.1.2. Let k be a field. A *valuation of k* is a map

$$k \to \Gamma \cup \{0\} : x \to |x|$$

where Γ is an ordered group, such that

1. $|x| = 0$ iff $x = 0$,
2. $|xy| = |x|\,|y|$ for all $x, y \in k$,

3. $|x+y| \leq \max(|x|, |y|)$ for all $x, y \in k$.

A subring $\mathcal{R}$ of k is called a *valuation ring* if it has the property that for any $x \in X$, we have $x \in \mathcal{R}$ or $x^{-1} \in \mathcal{R}$.
A valuation ring is called *discrete* if it gives rise to a valuation into a cyclic group Γ.

Proposition 3.1.3. *If $\mathcal{R} \subset K$ is a valuation ring, then the non-units of $\mathcal{R}$ form a maximal ideal of $\mathcal{R}$.*

Proof. Let $\mathcal{R}$ be a valuation ring of K. Suppose that $x, y \in \mathcal{R}$ are not units. Since $\mathcal{R}$ is a valuation ring, we either have that $x/y \in \mathcal{R}$ or that $y/x \in \mathcal{R}$. Since the situation is completely symmetrical, we can assume that $x/y \in \mathcal{R}$. Then

$$1 + x/y = (x+y)/y \in \mathcal{R}.$$

If $x+y$ were a unit, then $1/y \in \mathcal{R}$, contradicting the assumption that y is not a unit, hence $x+y$ is not a unit. Also, if $z \in \mathcal{R}$ and x is not a unit, then zx is also not a unit (that would imply that $x^{-1} \in \mathcal{R}$). Hence the non-units of $\mathcal{R}$ form a maximal ideal of $\mathcal{R}$. □

Remark 3.1.4. A valuation ring $\mathcal{R}$ gives rise to a valuation in the following way: the non-units of $\mathcal{R}$ form a maximal ideal of $\mathcal{R}$, and we will denote it by m. Then, for $x, y \in k$, we can define

$$|x| < |y| \leftrightarrow |x/y| \geq 1 \leftrightarrow x/y \in m^*.$$

Note that this indeed satisfies the properties of a valuation.
For a discrete valuation ring $\mathcal{R}$, there is an element π in this maximal ideal of $\mathcal{R}$ such that its value $|\pi|$ generates the value group. Then, every element $x \in k$ can be written $x = u\pi^r$ with u a unit of $\mathcal{R}$ and r an integer. We call r *the order of x at v*, and we say that x has a *zero of order r*, or when r is negative, that x has a *pole of order $-r$*.

Proposition 3.1.5. *If Y is an irreducible divisor on X and X is nonsingular along Y, then $\mathcal{O}_{Y,X}$ is a discrete valuation ring.*

To prove this, we will use a classical result, stated in the following theorem.

Theorem 3.1.6. *Let R be a local noetherian domain of dimension 1. Then R is integrally closed if and only if R is a discrete valuation ring.*

Proof. This is a classical result and the proof requires a considerable amount of commutative algebra. See theorem 5.3 in [4], pp. 7-8 or proposition 9.2 in [1], pp. 94-95. □

Proof of proposition 3.1.5. The idea of the proof is to show that $\mathcal{O}_{Y,X}$ is an integrally closed one-dimensional Noetherian local ring, and then use the classical result that any such ring is a discrete valuation ring.

Let Y be an irreducible divisor on X with X nonsingular along Y. Since Y has codimension 1 in X, we know that the local ring of X along Y, $\mathcal{O}_{Y,X}$, has dimension 1. Since the localization of a Noetherian ring is Noetherian, we know that $\mathcal{O}_{Y,X}$ is Noetherian, and since the localization of an integrally closed domain is integrally closed, we also know that $\mathcal{O}_{Y,X}$ is integrally closed. Now, the above classical result applies, and we are done. □

Definition 3.1.7. As $\mathcal{O}_{Y,X}$ is a discrete valuation ring, for $f \in \mathcal{O}_{Y,X}$ we can define *the order of f at Y*, $\text{ord}_Y : \mathcal{O}_{Y,X} - \{0\} \to \mathbb{Z}$, as the normalized order r from the above remark 3.1.4. Now, by letting

$$\text{ord}_Y(f/g) := \text{ord}_Y(f) - \text{ord}_Y(g),$$

we can extend ord_Y to $k(X) - \{0\}$, and get the *order at Y*,

$$\text{ord}_Y : k(X) - \{0\} \to \mathbb{Z}.$$

Moreover, we define *the positive order at Y* ord_Y^+ as

$$\text{ord}_Y^+ : k(X) - \{0\} \to \mathbb{Z} : f \to \max(0, \text{ord}_Y(f)).$$

As we have now defined what the order of a function at Y is, we can define the divisor of a rational function $f \in k(X) - \{0\}$.

Definition 3.1.8. Let X be a variety and let $f \in k(X) - \{0\}$ be a rational function on X. The *divisor of f* is the divisor

$$\text{div}(f) = \sum_Y \text{ord}_Y(f)Y \in \text{Div}(X).$$

A divisor is called *principal* if it is the divisor of a function. Two divisors are called *linearly equivalent*, denoted $D \sim D'$, if their difference is a principal divisor. Sometimes, we write (f) for the divisor of f. The divisor class group $Cl(X)$ is the group of divisor classes modulo linear equivalence. Also, we can define *the positive divisor of f* as

$$\text{div}^+(f) = \sum_Y \text{ord}_Y^+(f)Y \in \text{Div}(X).$$

3.2 Cartier Divisors and their Relation to Weil Divisors

Alternatively, we can start with the idea that a divisor should be something which locally looks like the divisor of a rational function. Although not trivially true, it turns out that a subvariety of codimension one on a normal variety is defined locally as the zeros and poles of a single function. We use this idea in the definition of Cartier divisors.

Definition 3.2.1. Let X be a variety. A *Cartier divisor* on X is a collection of pairs $(U_i, f_i)_{i \in I}$ satisfying the following conditions:

1. The U_i's are open in X and cover X.
2. The f_i's are nonzero rational functions $f \in k(U_i)^* = k(X)^*$.
3. $f_i f_j^{-1} \in \mathcal{O}(U_i \cap U_j)$, so $f_i f_j^{-1}$ has no poles or zeros on $U_i \cap U_j$.

Two pairs $(U_i, f_i)_{i\in I}$, $(V_j, g_j)_{j\in J}$ are considered the same if $f_i g_j^{-1} \in \mathcal{O}(U_i \cap V_j)$ for all i and j.
We define *the sum of two Cartier divisors* as

$$(U_i, f_i)_{i\in I} + (V_j, g_j)_{j\in J} = (U_i \cap V_j, f_i g_j)_{j\in I\times J}.$$

With this operation, the Cartier divisors form a group, called $\mathrm{CaDiv}(X)$. The *support* of a Cartier divisor is the set of zeros and poles of the f_i's. A Cartier divisor is called *effective* (or *positive*) if it is equal to some $(U_i, f_i)_{i\in I}$ with every $f_i \in \mathcal{O}(U_i)$ (that is, f_i has no poles on U_i).
Associated to a function $f \in k(X)^*$ is the Cartier divisor $\mathrm{div}(f) = (X, f)$. Such a divisor is called a *principal Cartier divisor*, and two divisors are called *linearly equivalent* if their difference is principal. The group of Cartier divisor classes modulo linear equivalence is called the *Picard group* of X, and is denoted $\mathrm{Pic}(X)$.

To connect the notion of a Cartier divisor to the notion of a Weil divisor, we need to define the order of a Cartier divisor D along an irreducible subvariety Y of codimension 1 in X.

Definition 3.2.2. Let D be a Cartier divisor, let Y be an irreducible subvariety of codimension 1 in X, and choose i such that $U_i \cap Y \neq \emptyset$. We define *the order of D along Y* as

$$\mathrm{ord}_Y(D) = \mathrm{ord}_Y(f_i).$$

Remark 3.2.3. Note that $\mathrm{ord}_Y(D)$ does not depend on the choice of i: this follows from the fact that the f_i are rational functions that fit together properly.

The following theorem gives us a connection between Cartier divisors and Weil divisors.

Theorem 3.2.4. *Let X be a smooth variety. Then the maps*

$$\begin{aligned} \mathrm{CaDiv}(X) \to \mathrm{Div}(X): \quad & D \to \sum_Y \mathrm{ord}_Y(D) Y, \\ \mathrm{CaPrinc}(X) \to \mathrm{WeilPrinc}(X): \quad & \mathrm{div}_{Cartier}(f) = (X, f) \\ & \to \sum_Y \mathrm{ord}_Y(f) Y = \mathrm{div}_{Weil}(f) \end{aligned}$$

are isomorphisms, and they induce an isomorphism $\mathrm{Pic}(X) \to \mathrm{Cl}(X)$.

Proof. See [6], II 6.11 (pp. 141). □

Given a morphism $g : X \to Y$ and a Cartier divisor D over Y, we can pullback this divisor to a divisor over X. This pullback is defined in the natural way.

Definition 3.2.5. Let $g : X \to Y$ be a morphism of varieties, let $D \in \text{CaDiv}(Y)$ be a Cartier divisor defined by $(U_i, f_i)_{i\in I}$, and assume that $g(X)$ is not contained in the support of D. Then *the pullback* $g^*(D) \in \text{CaDiv}(X)$, defined as a Cartier divisor, is the divisor defined by

$$g^*(D) = (g^{-1}(U_i), f_i \circ g)_{i\in I}$$

Using the isomorphism given above between CaDiv(X) and Div(X) for some smooth X, we can define the pullback of a Weil divisor through the definition of the pullback of a Cartier divisor.

Definition 3.2.6. Let $g : X \to Y$ be a morphism of smooth varieties. Let $D \in \text{CaDiv}(Y)$ be a Cartier divisor and let

$$D_{Weil} = \sum_y \text{ord}_y(D)(y)$$

be the corresponding Weil divisor (where the sum is taken over all subvarieties of codimension 1 of Y). Then *the pullback* $g^*(D_{Weil}) \in \text{Div}(X)$, defined as a Weil divisor, is defined by

$$g^*(D_{Weil}) = \sum_x \text{ord}_x(g^*(D))(x)$$

whenever $g^*(D)$ is defined, where the sum is over all the subvarieties of codimension 1 of X.

3.3 Pullback Divisor $\sigma_P^*(\bar{O})$

Recall that given an elliptic surface $\mathcal{E}$, we have morphisms

$$\sigma_P : C \to \mathcal{E} : t \to (P_t, t).$$

Using the definition given above, this means that we can construct the pullback σ_P^*. Write $\bar{O}$ for the divisor of the curve at infinity.
In this thesis, we are interested in the terms B_{nP} in an elliptic divisibility sequence. There is a tight relationship between these denominators and the pullback divisor $\sigma_{nP}^*(\bar{O})$, and in this subsection, we will formalize this relationship. After that, we can see $\sigma_{nP}^*(\bar{O})$ as a generalization of the terms B_{nP}; where the denominator B_{nP} is only defined for an elliptic curve over the function field of $\mathbb{P}^1$, $k(T) = k(\mathbb{P}^1)$, we have that $\sigma_{nP}^*(\bar{O})$ is also defined for an elliptic curve over a more general function field $k(C)$, where C/k is any smooth projective curve.

First, we will define the zero divisor as a Weil divisor.

Definition 3.3.1. For $K = k(C)$, let $O \in E(K)$ be the point at infinity, then we have the corresponding section $\sigma_O : C \to \mathcal{E} : t \to (O_t, t)$, where O_t is the point at infinity on the curve E_t. Denote the irreducible curve at infinity $\{(O_t, t)|t \in C\}$ on the surface $\mathcal{E}$ by Y_O. Now, define *the zero divisor* $\bar{O}$ as $\bar{O} = \sigma_O(C) = Y_O \in \text{Div}(\mathcal{E})$.

We want to be able to pull this zero divisor back over a morphism $\sigma_P : C \to \mathcal{E}$, and we want to get a divisor $\sigma_P^*(\bar{O}) \in \mathrm{Div}(C)$. This means that first, we will need to write $\bar{O}$ as a Cartier divisor. Recall that we can write any elliptic surface $\mathcal{E}$ (up to birational equivalence) as

$$\mathcal{E}(A,B) = \{((X:Y:Z),t) \in \mathbb{P}^2 \times C | Y^2Z = X^3 + AXZ^2 + BZ^3\}$$

This leads us to the following definition.

Definition 3.3.2. As $\mathcal{E}$ is a two-dimensional projective variety, we have the standard opens

$$\begin{aligned} U_0 &= \{((X:Y:Z),t) \in \mathcal{E} | X \neq 0\} \\ U_1 &= \{((X:Y:Z),t) \in \mathcal{E} | Y \neq 0\} \\ U_2 &= \{((X:Y:Z),t) \in \mathcal{E} | Z \neq 0\}. \end{aligned}$$

These three opens cover $\mathcal{E}$. We also have rational functions

$$\begin{aligned} f_0 &= \frac{Z}{X} \\ f_1 &= \frac{Z}{Y} \\ f_2 &= 1 \end{aligned}$$

on U_0, U_1 and U_2 respectively. Now put

$$\bar{O}_{Car} = \{(U_0, f_0), (U_1, f_1), (U_2, f_2)\}.$$

Remark 3.3.3. We have to check that this indeed defines a Cartier divisor. The U_i's are indeed opens that cover $\mathcal{E}$, and the f_i's are indeed nonzero rational functions over the U_i's. On $U_0 \cap U_1$ we indeed have that $f_0 f_1^{-1} = \frac{Y}{X}$ and $f_1 f_0^{-1} = \frac{X}{Y}$ have no poles or zeros. On $U_0 \cap U_2$ we have that $\frac{Z}{X}$ and $\frac{X}{Z}$ have no poles or zeros, and on $U_1 \cap U_2$ we have that $\frac{Z}{Y}$ and $\frac{Y}{Z}$ have no poles or zeros.
Also we want to know how this divisor relates to the zero divisor. If ϕ is not the curve at infinity, we can use f_2 to see that $\mathrm{ord}_\phi(\bar{O}_{Car}) = \mathrm{ord}_\phi(f_2) = 0$, and for ϕ_O the curve at infinity, we can use f_1 to see that $\mathrm{ord}_{\phi_O}(\bar{O}_{Car}) = \mathrm{ord}_{\phi_O}(f_1) = 3$, and hence we have that

$$\sum_\phi \mathrm{ord}_\phi(\bar{O}_{Cart})(\phi) = 3\bar{O}.$$

Now we are able to do the pullback σ_P^*. For any $P \in E(K)$, we have $\sigma_P : C \to \mathcal{E} : t \to (P_t, t)$, so the Cartier divisor $\sigma_P^*(\bar{O}_{Cart})$ is defined as

$$\sigma_P^*(\bar{O}_{Cart}) = \{(\sigma_P^{-1}(U_0), \frac{Z}{X} \circ \sigma_P), (\sigma_P^{-1}(U_1), \frac{Z}{Y} \circ \sigma_P), (\sigma_P^{-1}(U_2), 1 \circ \sigma_P)\}.$$

Translating this back to a Weil divisor on C (where C can be any smooth projective curve), we have the following proposition.

Proposition 3.3.4. *Let $\mathcal{E}/C$ be an elliptic surface over a smooth projective curve C, and write a Weierstrass equation for $E/K = E/k(C)$. Take a point $P = (x_P, y_P) = \left(\frac{A_p}{B_P^2}, \frac{C_P}{B_P^3}\right)$ where $\gcd(C_P, B_P) = 1$, then for all $t \in C$ for which the coefficients of the Weierstrass equation are regular, we have that*

$$\mathrm{ord}_t(\sigma_P^*(\bar{O})) = \frac{1}{3}\mathrm{ord}_t^+(y_P^{-1})$$

and equivalently, we have

$$\mathrm{ord}_t(\sigma_P^*(\bar{O})) = \frac{1}{2}\mathrm{ord}_t^+(x_P^{-1}).$$

To prove this proposition, we first have a lemma that says what it means that the coefficients of the Weierstrass equation are regular.

Lemma 3.3.5. *Let $\mathcal{E}/C$ be an elliptic surface over a curve C, and write a Weierstrass equation $y^2 = x^3 + Ax + B$ for $E/K = E/k(C)$, and assume that A and B are regular at $t \in k(C)$. Then any point at infinity at t, $P_t = (x_{P_t} : y_{P_t} : 0)$, satisfies $x_{P_t} = 0$.*

Proof. Take $Y^2Z = X^3 + AXZ^2 + BZ$ with A and B regular at t and a point $P_t = (x_{P_t} : y_{P_t} : z_{P_t})$ at infinity at t. This implies that $z_t = 0$ and that x_{P_t} and y_{P_t} are finite (or at least they can be chosen finite). Hence $B_t z_t = 0$, $A_t x_t z_t^2 = 0$ and $y_t^2 z_t = 0$, thus we have that $x_{P_t}^3 = 0$, and since we don't have zero divisors, $x_{P_t} = 0$. This completes the proof. □

Proof of proposition 3.3.4. Let $C_{reg} \subseteq C$ be the set of all $t \in C$ for which the coefficients of the Weierstrass equation are regular. We have

$$\sum_{t \in C_{reg}} \mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t) = \sum_{\substack{t \in C_{reg} \\ Z_{P_t} \neq 0}} \mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t) + \sum_{\substack{t \in C_{reg} \\ Z_{P_t} = 0}} \mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t).$$

All t with $Z_{P_t} \neq 0$ are inside $\sigma_P^{-1}(U_2)$, and in the last sum, we have that $Z_{P_t} = 0$ implies that $X_{P_t} = 0$ (note that we use here that the coefficients of the Weierstrass equation are regular), thus we have

$$\begin{aligned}
\sum_{t \in C_{reg}} \mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t) &= \sum_{\substack{t \in C_{reg} \\ Z_{P_t} \neq 0}} \mathrm{ord}_t(1)(t) + \sum_{\substack{t \in C_{reg} \\ P_t = (0:1:0)}} \mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t) \\
&= \sum_{\substack{t \in C_{reg} \\ Z_{P_t} \neq 0}} 0 \cdot (t) + \sum_{\substack{t \in C_{reg} \\ P_t = (0:1:0)}} \mathrm{ord}_t(Z_P/Y_P)(t) \\
&= \sum_{\substack{t \in C_{reg} \\ P_t = (0:1:0)}} \mathrm{ord}_t(Z_P/Y_P)(t).
\end{aligned}$$

Now, we can write $y_P = Y_P/Z_P$, and we have

$$\sum_{t\in C_{reg}} \mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t) = \sum_{\substack{t\in C_{reg}\\ P_t=(0:1:0)}} \mathrm{ord}_t(y_P^{-1})(t) = \sum_{\substack{t\in C_{reg}\\ P_t=(0:1:0)}} \mathrm{ord}_t^+(y_P^{-1})(t).$$

Moreover,

$$\sum_{\substack{t\in C_{reg}\\ P_t\neq(0:1:0)}} \mathrm{ord}_t^+(y_P^{-1})(t) = 0,$$

and hence we have that

$$\mathrm{ord}_t(\sigma_P^*(\bar{O})) = \frac{1}{3}\sum_{t\in C_{reg}} \mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t) = \frac{1}{3}\sum_{t\in C_{reg}} \mathrm{ord}_t^+(y_P^{-1})(t).$$

Also, we have that

$$\begin{aligned}\sum_{\substack{t\in C_{reg}\\ P_t=(0:1:0)}} \mathrm{ord}_t^+(Z_P/Y_P)(t) &= \sum_{\substack{t\in C_{reg}\\ P_t=(0:1:0)}} \mathrm{ord}_t^+(Z_P/(X_P^{3/2}/Z_P^{1/2}))(t)\\ &= \frac{3}{2}\sum_{\substack{t\in C_{reg}\\ P_t=(0:1:0)}} \mathrm{ord}_t^+(x_P^{-1})(t)\end{aligned}$$

and hence in the same way as above,

$$\mathrm{ord}_t(\sigma_P^*(\bar{O})) = \frac{1}{3}\sum_{t\in C_{reg}} \mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t) = \frac{1}{2}\sum_{t\in C_{reg}} \mathrm{ord}_t^+(x_P^{-1})(t).$$

□

For $C = \mathbb{P}^1$, this proposition has an easy corollary for when the coefficients of the Weierstrass equation are constant.

Corollary 3.3.6. *Let $\mathcal{E}/\mathbb{P}^1$ be an elliptic surface over $\mathbb{P}^1$, and write a Weierstrass equation for $E/K = E/k(T)$. Take a point $P = (x_P, y_P) = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3}\right)$ satisfying $\gcd(C_P, B_P) = 1$. If the coefficients of the Weierstrass equation are constant, then*

$$\sigma_P^*(\bar{O}) = \frac{1}{3}\mathrm{div}^+(y^{-1}) = \frac{1}{2}\mathrm{div}^+(x^{-1}).$$

Proof. The coefficients of the Weierstrass equation are constant precisely when for all $t \in \mathbb{P}^1$, these coefficients are regular. That being said, the corollary is immediate from proposition 3.3.4. □

Now, we will take a look at what happens when for some $t \in C$, the coefficients of the Weierstrass equation are not regular. First, we will have an example that shows that the equation $\mathrm{ord}_t(\sigma_P^*(\bar{O})) = \frac{1}{3}\mathrm{ord}_t^+(y_P^{-1})$ does *not* always hold for $t \in C = \mathbb{P}^1$ for which the coefficients of the Weierstrass equation are *not* regular at t.

Example 3.3.7. Consider the curve

$$E : y^2 = x^3 - T^2x + 1$$

with the point $P = (x_P, y_P) = (T, 1) \in E(k(T))$ over the rational function field $k(T)$. If we try and compute $\sigma_p^*(\bar{O})$ at $T = \infty$, we see that the x-coordinate T of P is not regular at ∞. Moreover, the coefficient $-T^2$ of the Weierstrass equation is not regular. Looking at the surface

$$Y^2Z = X^3 - T^2XZ^2 + Z^3$$

and the point

$$P = (T : 1 : 1) = (1 : T^{-1} : T^{-1}),$$

trying to calculate $\mathrm{ord}_\infty(\sigma_P^*(\bar{O}))$ directly gives us the problem that $P_\infty = (1 : 0 : 0)$ is not the usual point at infinity (and this is where the above proof of $\mathrm{ord}_t(\sigma_P^*(\bar{O})) = \frac{1}{3}\mathrm{ord}_t^+(y_P^{-1})$ would go wrong).
What we can do is use a change of variables. Write $(x, y) = (T^2u, T^3v)$, then the new equation is

$$v^2 = u^3 - T^{-2}u + T^{-6}$$

and the point P has coordinates $(u_P, v_P) = (T^{-2} \cdot T, T^{-3} \cdot 1) = (T^{-1}, T^{-3})$. Now, both coefficients $-T^{-2}$ and T^{-6} are regular at ∞, and the coordinates of P in these new variables are also regular at ∞. Calculating $\mathrm{ord}_\infty(\sigma_P^*(\bar{O}))$ with the method developed above, gives us that

$$\mathrm{ord}_\infty(\sigma_P^*(\bar{O})) = \frac{1}{3}\mathrm{ord}_\infty^+(T^3) = 0$$

while

$$\mathrm{ord}_\infty^+ x_P^{-1} = \mathrm{ord}_\infty^+ T^{-1} = 1$$

and

$$\mathrm{ord}_\infty B_{2P} = \mathrm{ord}_\infty 1 = 0$$

and

$$\mathrm{ord}_\infty^+ y_P^{-1} = \mathrm{ord}_\infty^+(1) = 0.$$

Now, looking at $2P = (x_{2P}, y_{2P}) = (T^4 - 2T : -T^6 + 3T^3 - 1 : 1)$, we see that after changing coordinates, we have $2P = (u_{2P}, v_{2P}) = \left(\frac{T^4-2T}{T^2} : \frac{-T^6+3T^3-1}{T^3} : 1\right)$. At infinity, this has order

$$\mathrm{ord}_\infty(\sigma_P^*(\bar{O})) = \frac{1}{3}\mathrm{ord}_\infty^+\left(\frac{T^3}{-T^6 + 3T^3 - 1}\right) = 1$$

while

$$\mathrm{ord}_\infty^+ x_P^{-1} = \mathrm{ord}_\infty^+\left(\frac{1}{T^4 - 2T}\right) = 4$$

and

$$\mathrm{ord}_\infty B_{2P} = \mathrm{ord}_\infty 1 = 0$$

and

$$\mathrm{ord}_\infty^+ y_P^{-1} = \mathrm{ord}_\infty^+ \left(\frac{1}{-T^6 + 3T^3 - 1} \right) = 6.$$

Remark 3.3.8. As the previous example shows, there are three things of interest, namely $\sigma_P^*(\bar{O})$, $\frac{1}{2}\mathrm{div}^+(x_P^{-1})$ and $\mathrm{div}^+(B_P)$, and in general, all three are different. $\sigma_P^*(\bar{O})$ is intrinsically defined and doesn't depend on the Weierstrass equation chosen, while $\mathrm{div}^+(x_P^{-1})$ and $\mathrm{div}^+(B_P)$ clearly depend on the Weierstrass equation. Furthermore, $x_P^{-1} = \frac{B_P^2}{A_P}$ has an order different from B_P^2 at t for which A_P is not regular.

Fortunately, as the following proposition tells us, the difference between $\frac{1}{2}\mathrm{ord}_t^+(x_P^{-1})$ and $\mathrm{ord}_t(\sigma_P^*(\bar{O}))$ is always small. Furthermore, for $C = \mathbb{P}^1$, we can relate $\mathrm{ord}_t(B_P)$ to $\frac{1}{2}\mathrm{ord}_t^+(x_P^{-1})$.

Proposition 3.3.9. *Let $\mathcal{E}/C$ be an elliptic surface over a curve C, and write a Weierstrass equation for $E/K = E/k(C)$. Take a point $P = (x_P, y_P)$. Then:*

1. *$\frac{1}{2}\mathrm{ord}_t^+(x^{-1})$, $\frac{1}{3}\mathrm{ord}_t^+(y^{-1})$ and $\mathrm{ord}_t(\sigma_P^*(\bar{O}))$ are the same for all but finitely many $t \in C$.*

2. *there is a constant c, only depending on the Weierstrass equation for E, such that for all $t \in C$,*

$$0 \leq \frac{1}{2}\mathrm{ord}_t^+(x^{-1}) - \mathrm{ord}_t(\sigma_P^*(\bar{O})) \leq c.$$

3. *using the same constant c, we also have for all $t \in C$ that*

$$0 \leq \frac{1}{3}\mathrm{ord}_t^+(y^{-1}) - \mathrm{ord}_t(\sigma_P^*(\bar{O})) \leq c.$$

Furthermore, if $C = \mathbb{P}^1$, then:

4. *if A_P, B_P and C_P are regular at t, then*

$$\mathrm{ord}_t(B_P) = \mathrm{ord}_t^+(B_P) = \frac{1}{2}\mathrm{ord}_t^+(x^{-1}) = \frac{1}{3}\mathrm{ord}_t^+(y^{-1}).$$

5. *if A_P, B_P and C_P are not all regular at t, then $\mathrm{ord}_t(B_P) \leq 0$.*

Proof. Let $\mathcal{E}/C$ be an elliptic surface over a curve C, write a Weierstrass equation $y^2 = x^3 + Ax + B$ for $E/K = E/k(C)$ and take a point $P = (x_P, y_P)$. The coefficients of the Weierstrass equation are regular at all but finitely many $t \in C$, thus by proposition 3.3.4, we have that $\frac{1}{2}\mathrm{ord}_t(x^{-1})$, $\frac{1}{3}\mathrm{ord}_t(y^{-1})$ and $\mathrm{ord}_t(\sigma_P^*(\bar{O}))$ are the same for all but finitely many $t \in C$.
Now we will show that the difference for other t is always bounded by a constant. Let t be such that the coefficients of the Weierstrass equation are not regular at t, let m be the order of the pole at t of A and let n be the order of the pole at t of B and write $u_t = T - t$. Let c_t be $\max(m/4, n/6)$ rounded up to an integer,

then the change-of-variables $(x, y) = (u^{-2c_t}X, u^{-3c_t}Y)$ changes the Weierstrass equation to

$$Y^2 = y^2u^{6c_t} = x^3u^{6c_t} + Au^{6c_t}x + Bu^{6c_t} = X^3 + Au^{4c_t}X + Bu^{6c_t} = X^3 + A'X + B'$$

where $A' = Au^{4c_t}$ and $B' = Bu^{6c_t}$ are regular at t. The point $P = (x_P, y_P)$ becomes $P = (X_P, Y_P) = (u^{2c_t}x_P, u^{3c_t}y_P)$ in the new variables. Now,

$$\mathrm{ord}_t(\sigma_P^*(\bar{O})) = \frac{1}{2}\mathrm{ord}_t^+(u^{-2c_t}x_P^{-1}) \leq \mathrm{ord}_t^+(u_t^{-c_t}) + \frac{1}{2}\mathrm{ord}_t^+(x_P^{-1}) = \frac{1}{2}\mathrm{ord}_t^+(x_P^{-1})$$

while since $\mathrm{ord}_t(u_t^{-c_t}) < 0$, we also have

$$\mathrm{ord}_t(\sigma_P^*(\bar{O})) = \frac{1}{2}\mathrm{ord}_t^+(u^{-2c_t}x_P^{-1}) \geq \mathrm{ord}_t(u_t^{-c_t}) + \frac{1}{2}\mathrm{ord}_t^+(x_P^{-1}) = -c_t + \frac{1}{2}\mathrm{ord}_t^+(x_P^{-1})$$

and hence

$$0 \leq \frac{1}{2}\mathrm{ord}_t^+(x_P^{-1}) - \mathrm{ord}_t(\sigma_P^*(\bar{O})) \leq c_t.$$

Now, the second statement follows by taking $c = \max_t(\{c_t\})$. The third statement follows analogously from the fact that $\mathrm{ord}_t(\sigma_P^*(\bar{O})) = \frac{1}{3}\mathrm{ord}_t^+\left(u^{-3c_t}y_P^{-1}\right)$.

For the 4th statement, let $C = \mathbb{P}^1$ and assume that A_P, is regular at t, then A_P has no pole at t and hence

$$\frac{1}{2}\mathrm{ord}_t^+(x_P^{-1}) = \frac{1}{2}\mathrm{ord}_t^+\left(\frac{B_P^2}{A_P}\right) = \frac{1}{2}\mathrm{ord}_t^+(B_P^2) = \mathrm{ord}_t^+(B_P).$$

In the same way, if C_P is regular at t, then

$$\frac{1}{3}\mathrm{ord}_t^+(y_P^{-1}) = \frac{1}{3}\mathrm{ord}_t^+\left(\frac{B_P^3}{C_P}\right) = \frac{1}{3}\mathrm{ord}_t^+(B_P^3) = \mathrm{ord}_t^+(B_P).$$

Furthermore, if B_P is regular at t, then $\mathrm{ord}_t(B_P) = \mathrm{ord}_t^+(B_P)$. This completes the proof of the 4th statement.

For the 5th statement, first note that if B_P is not regular at t, that then B_P has a pole at t and hence $\mathrm{ord}_t(B_P) < 0$. Now assume that A_P is not regular at t, then A_P has a pole at t, and hence B_P is nonzero at t, meaning that $\mathrm{ord}_t(B_P) \leq 0$. Now, assume that C_P is not regular at t, then we have in the same way that $\mathrm{ord}_t(B_P) \leq 0$. This completes the proof of the last statement and the proof of the proposition. □

To formalize the relationship between the pullback divisor $\sigma_{nP}^*(\bar{O})$ and $\mathrm{div}^+(B_{nP})$ in the case that $C = \mathbb{P}^1$, we need the following lemma.

Lemma 3.3.10. *Let $C = \mathbb{P}^1$ and $\mathcal{E}/\mathbb{P}^1$ be an elliptic surface over $\mathbb{P}^1$, and write a Weierstrass equation for $E/K = E/k(T)$. Take a point $P = (x_P, y_P)$. Then $\mathrm{ord}_t(B_P) \leq 0$ for some $t \in C$ implies that $t = \infty$, and for this t, there is a constant c_2 only depending on the curve E such that $\frac{1}{2}\mathrm{ord}_t^+(x^{-1}) \leq c_2$.*

Proof. This lemma is a direct corollary of the function field analogue to Siegels finiteness theorem for integral points on elliptic curves. The characteristic 0 case of this theorem is proven in part by Lang, see [11], and in part by Manin, see [24]. The characteristic p case is done by Voloch, see [23]. □

The following theorem now formalizes the relation between B_{nP} and $\sigma^*_{nP}(\bar{O})$.

Theorem 3.3.11. *For any elliptic divisibility sequence $(B_{nP})_{n\geq 1}$, we have that the difference between $\mathrm{div}^+(B_{nP})$ and $\sigma^*_{nP}(\bar{O})$ is bounded by a single divisor $D \in \mathrm{Div}(C)$, only depending on the Weierstrass equation for E:*

$$\left|\sigma^*_{nP}(\bar{O}) - \mathrm{div}^+(B_{nP})\right| \leq D.$$

Proof. This follows from combining the first, second, fourth and fifth statement of the previous proposition and the previous lemma.
Put $\mathrm{ord}_t(D) = max(c, c_2)$ for all $t \in C$ for which the coefficients of the Weierstrass equation are not regular at t (finitely many by the first statement), and $\mathrm{ord}_t(D) = 0$ everywhere else. By the 4th and the 5th statement if follows that either $\mathrm{ord}^+_t(B_P) = \mathrm{ord}^+_t(x^{-1})$ or that $\mathrm{ord}^+_t(B_P) = 0$, and in this last case, the lemma above tells us that $\frac{1}{2}\mathrm{ord}^+_t(x^{-1}) \leq c_2$. Then by combining the first and the second statement, the corollary follows. □

Thus we have that $\sigma^*_{nP}(\bar{O})$ is, roughly (i.e. up to a single divisor only depending on the Weierstrass equation), equal to half the polar divisor of nP. Since $\sigma^*_{nP}(\bar{O})$ is defined for an elliptic divisibility sequence on $E/k(C)$ where C is any smooth curve, we have that $\sigma^*_{nP}(\bar{O})$ generalizes the concept of elliptic divisibility sequences for arbitrary smooth projective curves C.

3.4 Examples

3.4.1 A Singular Surface

Take $C = \mathbb{P}^1$ and look at the surface

$$\mathcal{E} = \{([X : Y : Z], t) \in \mathbb{P}^2 \times C | Y^2Z = X^3\}.$$

This is *not* an elliptic surface: for every $t \in C$, the fibre $\mathcal{E}_t = \pi^{-1}(t)$ is singular. Still, we can look at the point $P = ([T, 1, T^3], T) = ([\frac{1}{T^2}, \frac{1}{T^3}, 1], T)$ and we have a map

$$\sigma_P : \mathbb{P}^1 \to \mathcal{E} : t \to P_t.$$

Furthermore, we can still construct the pullback

$$\begin{aligned}\sigma^*_P(\bar{O}_{cart}) &= \{(\sigma_P^{-1}(U_0), \frac{Z}{X} \circ \sigma_P), (\sigma_P^{-1}(U_1), \frac{Z}{Y} \circ \sigma_P), (\sigma_P^{-1}(U_2), 1 \circ \sigma_P)\} \\ &= \{(\mathbb{P}^1 - \{0\}, T \to T^2), (\sigma_P^{-1}(U_1), T \to T^3), (\mathbb{P}^1 - \{0\}, T \to 1)\}\end{aligned}$$

and hence

$$\begin{aligned}\sigma_P^*(\bar{O}) &= \frac{1}{3}\sum_{t\in\mathbb{P}^1}\mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t) = \frac{1}{3}\sum_{t\in\mathbb{P}^1-\{0\}}\mathrm{ord}_t(T^2)(t) + \frac{1}{3}\sum_{t=0}\mathrm{ord}_t(T^3)(t)\\ &= 0 + \frac{1}{3}3(0) = (0) = \mathrm{div}(T) = \mathrm{div}(B_P)\end{aligned}$$

Since for every $t \in \mathbb{P}^1$, we do have that the non-singular points of $\mathcal{E}_t$ form a group, we can still add points, and it turns out that $nP = \left(\frac{1/n^2}{T^2}, \frac{1/n^3}{T^3}\right)$ and hence

$$\mathrm{div}(B_{nP}) = (0) = \sigma_{nP}^*(\bar{O})$$

for all $n \geq 1$.

3.4.2 An Elliptic Surface with Constant J-invariant

Let

$$\mathcal{E} = \{([X:Y:Z], t) \in \mathbb{P}^2 \times C | Y^2Z = X^3 - T^2(T^2-1)X\}$$

with the point $P = (1-T^2, 1-T^2)$. We can construct the pullback

$$\begin{aligned}\sigma_P^*(\bar{O}_{cart}) &= \{(\sigma_P^{-1}(U_0), \frac{Z}{X}\circ\sigma_P), (\sigma_P^{-1}(U_1), \frac{Z}{Y}\circ\sigma_P), (\sigma_P^{-1}(U_2), 1\circ\sigma_P)\}\\ &= \{(V, T\to\frac{1}{1-T^2}), (V, T\to\frac{1}{1-T^2}), (\mathbb{P}^1, T\to 1)\}\end{aligned}$$

where $V = \{t \in \mathbb{P}^1 | 1-t^2 \neq 0\}$, and hence

$$\begin{aligned}\sigma_P^*(\bar{O}) &= \frac{1}{3}\sum_{t\in\mathbb{P}^1}\mathrm{ord}_t(\sigma_P^*(\bar{O}_{cart}))(t)\\ &= \frac{1}{3}\mathrm{ord}_\infty(\sigma_P^*(\bar{O}_{cart}))(\infty) + \frac{1}{3}\sum_{t\in\mathbb{P}^1-\{\infty\}}\mathrm{ord}_t(1)(t)\\ &= \frac{1}{3}\mathrm{ord}_\infty(\sigma_P^*(\bar{O}_{cart}))(\infty).\end{aligned}$$

To calculate the order at infinity, we need to do a change of variables

$$(x,y) = ((T^2(T^2-1))^2u, (T^2(T^2-1))^3v),$$

and we get that $P = (u_P, v_P) = \left(\frac{-1}{T^4(T^2-1)}, \frac{-1}{T^6(T^2-1)^2}\right)$ on

$$v^2 = u^3 - (T^2(T^2-1))^{-3}u.$$

Hence

$$\mathrm{ord}_\infty(\sigma_P^*(\bar{O}_{cart})) = \mathrm{ord}_\infty(1) = 0,$$

and $\sigma_P^*(\bar{O})$ is the empty divisor, and is equal to $\mathrm{div}(B_P) = \mathrm{div}(1)$.
We can calculate multiples nP of P, and their B_{nP} is denoted in the table below.

point nP	B_{nP}
P	1
$2P$	1
$3P$	$T^4 - \frac{3T^2}{4} - \frac{3}{16}$
$4P$	$T^6 - \frac{3T^4}{2} + \frac{T^2}{2} + \frac{1}{64}$
$5P$	$T^{12} - \frac{9T^{10}}{4} + \frac{5T^8}{8} + \frac{107T^6}{64} - \frac{155T^4}{128} + \frac{167T^2}{1024} + \frac{5}{4096}$

Figure 2: B_{nP} for $E : y^2 = x^3 - T^2(T^2-1)x$ and $P = (1-T^2, 1-T^2)$.

In each case, we have that the divisor of B_{nP} and $\sigma^*_{nP}(\bar{O})$ are equal everywhere except maybe at ∞. To find the order of $\sigma^*_{nP}(\bar{O})$ at infinity, we can do the same change of variables $(x, y) = ((T^2(T^2-1))^2 u, (T^2(T^2-1))^3 v)$ as before. For example, we have that

$$2P = (t^4 - t^2 + 1/4, t^6 - 3/2t^4 + 1/4t^2 + 1/8)$$

and after change of variables, we have that

$$2P = \left(\frac{t^4 - t^2 + 1/4}{(t^2(t^2-1))^2}, \frac{t^6 - 3/2t^4 + 1/4t^2 + 1/8}{(t^2(t^2-1))^3} \right)$$

and has regular coordinates at $t = \infty$, so the order at infinity $\sigma^*_{nP}(\bar{O})$ is again zero, and $\mathrm{div}(B_{nP}) = \sigma^*_{nP}(\bar{O})$.

3.5 Greatest Common Divisor of Points on Elliptic Curves

We have the standard definition of the greatest common divisor of two polynomials (the largest polynomial that divides both), and using that, we can define the greatest common divisor of two points P and Q on an elliptic curve over $k(T)$ as the greatest common divisor of their denominators B_P and B_Q. Now, we want to generalize that idea to elliptic curves over the function field of an arbitrary curve $k(C)$, and for that, we will use the pullback divisor $\sigma^*_P(\bar{O})$ instead of B_P. For this, we first need the definition of the greatest common divisor of two Weil divisors.

Definition 3.5.1. Let C be a smooth projective curve. For effective divisors $D_1, D_2 \in \mathrm{Div}(C)$, we define the *greatest common divisor of* D_1 *and* D_2 as

$$\mathrm{GCD}(D_1, D_2) = \sum_{\gamma \in C} \min(\mathrm{ord}_\gamma(D_1), \mathrm{ord}_\gamma(D_2))(\gamma) \in \mathrm{Div}(C).$$

Remark 3.5.2. In the case that $C = \mathbb{P}^1$, taking two polynomials $f, g \in k[T]$, we have that

$$\mathrm{div}(\gcd(f, g)) = \sum_{\gamma \in C} \min(\mathrm{ord}_\gamma(f), \mathrm{ord}_\gamma(g))(\gamma) = \mathrm{GCD}(\mathrm{div}^+(f), \mathrm{div}^+(g)).$$

Using the pullback divisor $\sigma_P^*(\bar{O})$, we can now define the greatest common divisor of two points on elliptic curves.

Definition 3.5.3. Let E_1/K and E_2/K be two elliptic curves over a function field $K = k(C)$, and let $P_1 \in E_1(K)$ and $P_2 \in E_2(K)$ be nonzero points. The *elliptic greatest common divisor* (or just greatest common divisor) *of* P_1 *and* P_2 is the divisor

$$\mathrm{GCD}(P_1, P_2) = \mathrm{GCD}(\sigma_{P_1}^*(\bar{O}_{\mathcal{E}_1}), \sigma_{P_2}^*(\bar{O}_{\mathcal{E}_2})) \in \mathrm{Div}(C)$$

In the case that $C = \mathbb{P}^1$, we want this definition to correspond to the other definition of the greatest common divisor of two points as the greatest common divisor of their B_P. As it turns out, the two definitions are not precisely the same; they can differ up to a constant, only depending on the Weierstrass equations chosen. The following proposition gives a precise formulation.

Proposition 3.5.4. *Let two elliptic curves $E_1/k(T)$ and $E_2/k(T)$ in Weierstrass form and two nonzero points $P = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^2}\right) \in E_1$ and $Q = \left(\frac{A_Q}{B_Q^2}, \frac{C_Q}{B_Q^2}\right) \in E_2$ be given. Then there is a divisor $D = D(E_1, E_2)$, only depending on the Weierstrass equations, such that*

$$|\mathrm{GCD}(P, Q) - \mathrm{div}(\gcd(B_P, B_Q))| \leq D.$$

Proof. We have $\mathrm{GCD}(P, Q) = \mathrm{GCD}(\sigma_P^*(\bar{O}_{\mathcal{E}_1}), \sigma_Q^*(\bar{O}_{\mathcal{E}_2}))$. Now, corollary 3.3.11 gives us that $|\sigma_P^*(\bar{O}_{\mathcal{E}_1}) - \mathrm{div}^+(B_P)| \leq D_1$ and $|\sigma_P^*(\bar{O}_{\mathcal{E}_2}) - \mathrm{div}^+(B_Q)| \leq D_2$, and using remark 3.5.2 we know that

$$\mathrm{GCD}(\mathrm{div}^+(B_P), \mathrm{div}^+(B_Q)) \quad = \quad \mathrm{div}(\gcd(B_P, B_Q))$$

Hence

$$\begin{aligned} |\mathrm{GCD}(P, Q) - \mathrm{div}(\gcd(B_P, B_Q))| &= |\mathrm{GCD}(\sigma_P^*(\bar{O}_{\mathcal{E}_1}), \sigma_Q^*(\bar{O}_{\mathcal{E}_2})) \\ &\quad -\mathrm{GCD}(\mathrm{div}^+(B_P), \mathrm{div}^+(B_Q))| \\ &\leq D_1 + D_2 = D \end{aligned}$$

This completes the proof. □

We also need the notion of independent points; when we look at common divisors of elliptic divisibility sequences, we will need to distinguish between the case that the points P and Q are and the case that they are not in essence the same point.

Definition 3.5.5. Two points $P_1 \in E_1/K$ and $P_2 \in E_2/K$ are called *dependent points* if there are isogenies $F : E_1 \to E_1$ and $G : E_2 \to E_1$, not both zero, such that $F(P_1) = G(P_2)$; otherwise, they are called *independent points*. We say that P_1 and P_2 are K-independent if the isogenies F and G can be defined over K.

4 Common Divisors of Elliptic Divisibility Sequences in Characteristic 0

In this section we will look at common divisors of elliptic divisibility sequences in characteristic 0. Instead of working with $(B_{nP})_{n\geq 1}$, we will work with the sequences $(\sigma^*_{nP}(\bar{O}))_{n\geq 1}$. As we've seen, they only differ by a constant if $C = \mathbb{P}^1$, and if $C \neq \mathbb{P}^1$, then we see $(\sigma^*_{nP}(\bar{O}))_{n\geq 1}$ as a generalization of $(B_{nP})_{n\geq 1}$.

The following theorem says that if the j-invariant is constant, then the degree the greatest common divisor of multiples of two independent points is always bounded by a constant. It thus gives the strongest possible bound for $\deg \mathrm{GCD}(n_1P_1, n_2P_2)$. Also, the theorem says that $\deg \mathrm{GCD}(n_1P_1, n_2P_2)$ is equal to the lower bound $\deg \mathrm{GCD}(P_1, P_2)$ for infinitely many n. This theorem is proven by Silverman in [19]. In this section, our main goal is to give and explain the proof, and to give some details that Silverman omits.

Theorem 4.0.6. *Let $K = k(C)$ be a characteristic zero function field of a smooth projective curve C/k, let E_1/K and E_2/K be elliptic curves, and let $P_1 \in E_1(K)$ and $P_2 \in E_2(K)$ be K-independent points. Assume further that the elliptic curves E_1/K and E_2/K both have constant j-invariant, i.e., $j(E_1), j(E_2) \in k$. Then:*

1. *there is a constant $c = c(K, E_1, E_2, P_1, P_2)$ so that*

$$\deg \mathrm{GCD}(n_1P_1, n_2P_2) \leq c \qquad \text{for all } n_1, n_2 \geq 1.$$

2. *the set*

$$\{n \geq 1 : \mathrm{GCD}(nP_1, nP_2) = \mathrm{GCD}(P_1, P_2)\}$$

has positive density.

The proof of this theorem consists of four parts: first, there is a general part, where the assumption of the constant j-invariant is used by taking a finite field extension over which the elliptic curves over the function fields split. After that, there are three cases: two 'easy' cases and one 'hard' case that uses Raynaud's theorem.

Before we start with the general part, we will first do an elementary result that is used in both 'easy' cases.

Lemma 4.0.7. *Let $\gamma \in C$ and let $P \in E(K) = E(k(C))$ be a nontorsion point.*

- *If $\mathrm{ord}_\gamma \sigma^*_P(\bar{O}) \geq 1$, then for all $m \neq 0$ we have*

$$\mathrm{ord}_\gamma \sigma^*_{mP}(\bar{O}) = \mathrm{ord}_\gamma \sigma^*_P(\bar{O}).$$

- *There is an integer $m' = m'(E/K, P, \gamma)$ so that for all $m \neq 0$,*

$$\mathrm{ord}_\gamma \sigma^*_{mP}(\bar{O}) \in \{0, m'\}.$$

In particular, $\mathrm{ord}_\gamma \sigma_{mP}(\bar{O})$ *is bounded independently of* m.

Proof. Let $[m] : \mathcal{E} \to \mathcal{E}$ be the multiplication-by-m map. We have that

$$[m]^* \bar{O} = \bar{O} + D_m$$

where $D_m \in \mathrm{Div}(\mathcal{E})$ is the divisor of nonzero m-torsion points.
Now I claim that $\bar{O} \cap D_m = \emptyset$, i.e. that the divisors $\bar{O}$ and D_m do not intersect. For a nonsingular fiber $\mathcal{E}_\gamma$, we know that the intersection of D_m and $\mathcal{E}_\gamma$ consists of the nonzero m-torsion points of the elliptic curve $\mathcal{E}_\gamma$, so on the nonsingular fibers, the divisors $\bar{O}$ and D_m do not intersect(note that we use that the characteristic of k is zero - moreover, it is enough to know that m is relatively prime to the field characteristic p, see [21], VII.3.1, pp. 192). On a singular fiber $\mathcal{E}_\gamma$, the map $[m] : \mathcal{E} \to \mathcal{E}$ is étale in a neighborhood of the zero point O_γ of $\mathcal{E}_\gamma$ (the map behaves well locally around O_γ: there is no singularity there). Hence we indeed have $\bar{O} \cap D_m = \emptyset$, and we have

$$\sigma^*_{mP}(\bar{O}) = \sigma^*_P([m]^*(\bar{O})) = \sigma^*_P(\bar{O}) + \sigma^*_P(D_m)$$

Using this, we can prove both statements of the lemma. First assume that $\mathrm{ord}_\gamma \sigma^*_P(\bar{O}) \geq 1$, then this means that $\sigma_P(\gamma) = O_\gamma \in \mathcal{E}_\gamma$. Since $\bar{O} \cap D_m = \emptyset$, it follows that the support of $\sigma^*(D_m)$ does not contain γ, so

$$\mathrm{ord}_\gamma \sigma^*_{mP}(\bar{O}) = \mathrm{ord}_\gamma \sigma^*_P(\bar{O}) + \mathrm{ord}_\gamma \sigma^*_P(D_m) = \mathrm{ord}_\gamma \sigma^*_P(\bar{O}).$$

This completes the proof of the first statement.
For the second statement, we may suppose without loss of generality that there exists some $m \neq 0$ such that $\mathrm{ord}_\gamma \sigma^*_{mP} \geq 1$, since otherwise we may take $m' = 0$. Now suppose that $\mathrm{ord}_\gamma \sigma^*_{m_1 P}(\bar{O}) \geq 1$ and $\mathrm{ord}_\gamma \sigma^*_{m_2 P}(\bar{O}) \geq 1$. Then applying the first statement first to $m_1 P$ with $m = m_2$ and then to $m_2 P$ with $m = m_1$, we find that

$$\mathrm{ord}_\gamma \sigma^*_{m_1 P}(\bar{O}) = \mathrm{ord}_\gamma \sigma^*_{m_1 m_2 P}(\bar{O}) = \mathrm{ord}_\gamma \sigma^*_{m_2 P}(\bar{O}).$$

This completes the proof of the lemma. □

4.1 General Part of the Proof

We will now start the proof of theorem 4.0.6. Let $K = k(C)$ be a characteristic zero function field, let E_1/K and E_2/K be elliptic curves and let $P_1 \in E_1(K)$ and $P_2 \in E_2(K)$ be K-independent points. Assume that the elliptic curves E_1 and E_2 have constant j-invariant. Then, by 2.5.3, we know that they split over some finite extension of K. Taking a common splitting field K', there is a finite cover $C' \to C$ and there are elliptic curves E'_1/k, E'_2/k such that

$$\mathcal{E}_i \times_C C' \simeq_{/k} E'_i \times_k C'.$$

For $i = 1, 2$, we then get commutative diagrams

$$\begin{array}{ccc} E_i' \times_k C' & \xrightarrow{s} & \mathcal{E}_i \\ \downarrow & & \downarrow \\ C' & \xrightarrow{f} & C. \end{array}$$

For each point $P_i \in E_i(K)$, we have a section $\sigma_{P_i} : C \to \mathcal{E}_i$ which in turn lifts to a unique section

$$\tau_{P_i} \times 1 : C' \to E_i' \times_k C'.$$

In other words, each point $E_i(K)$ gives a unique morphism $\tau_{P_i} : C' \to E_i'$ so that the following diagram commutes:

$$\begin{array}{ccc} E_i' \times_k C' & \xrightarrow{s} & \mathcal{E}_i \\ \uparrow_{\tau_{P_i} \times 1} & & \uparrow_{\sigma_{P_i}} \\ C' & \xrightarrow{f} & C. \end{array}$$

Now we can define a morphism

$$\phi = \tau_{P_1} \times \tau_{P_2} : C' \to E_1' \times_k E_2'.$$

The general part of the proof ends by showing the statement that I've put in the following lemma. The proof of the lemma mainly consists of tracing around the above commutative diagrams.

Lemma 4.1.1. *If*

$$\gamma \in \text{Support}(\text{GCD}(n_1 P_1, n_2 P_2)),$$

then for all $\gamma' \in f^{-1}(\gamma)$ *we have that*

$$\phi(\gamma') \in E_1'[n_1] \times E_2'[n_2] \subset (E_1' \times E_2')_{tors}.$$

Proof. Suppose that γ is in the support of $\text{GCD}(n_1 P_1, n_2 P_2)$ for some integers n_1, n_2. Then by definition of this GCD, we have that $\gamma \in \text{Support}(\sigma^*_{n_1 P_1}(\bar{O}_{\mathcal{E}_1}))$ and $\gamma \in \text{Support}(\sigma^*_{n_2 P_2}(\bar{O}_{\mathcal{E}_2}))$.
Tracing around the commutative diagrams, this means that for every point $\gamma' \in f^{-1}(\gamma) \subset C'$, we have $\tau_{n_1 P_1}(\gamma') = O_1$ and $\tau_{n_2 P_2}(\gamma') = O_2$ where $O_i \in E_i'(K)$ is the zero point. Equivalently, we have $\tau_{P_1}(\gamma') \in E_1'[n_1]$ and $\tau_{P_2}(\gamma') \in E_2'[n_2]$, so in particular, $\tau_{P_1}(\gamma')$ and $\tau_{P_2}(\gamma')$ are torsion points of E_1' and E_2' respectively. Hence $\phi(\gamma') = (\tau_{P_1}(\gamma'), \tau_{P_2}(\gamma'))$ is a torsion point of the abelian surface $E_1' \times E_2'$. This completes the proof of the lemma. □

Now, there will be three cases. In case 1 and 2 we will prove the theorem, and we will prove that case 3 does not occur.

4.2 Case 1: τ_{p_1} and τ_{p_2} are Constant

We start with an 'easy' case, namely by assuming that the maps τ_{p_1} and τ_{p_2} defined in the general part above are constant. Write $\tau_{P_i}(C') = \{c_i\} \subset E_i'$. First, we have a short lemma, of which the proof is due to Cornelissen.

Lemma 4.2.1. *In this case, the divisor $\sigma_{P_i}^*(\bar{O}_{\mathcal{E}_i})$ is supported on the set of ramification points R_f of the map $f : C' \to C$. Moreover, we also have that $\sigma_{nP_i}^*(\bar{O}_{\mathcal{E}_i})$ is supported on the set of ramification points R_f.*

Proof. Write

$$E : y^2 = x^3 + Ax + B,$$

where E has constant j-invariant, and take a point $P = (x_P, y_P) \in E(K)$. Since E splits, there is a transformation $(x, y) = (Xu^2, Yu^3)$ that changes E to its twist

$$Y^2 = X^3 + Au^{-4} + Bu^{-6} = X^3 + A_0X + B_0$$

with $Au^{-4} = A_0$ and $Bu^{-6} = B_0$ constant and $P' = (X, Y)$ constant.
Now, with $P = (X, Y)$ constant and hence $(x, y) = (Xu^2, Yu^3)$ on the original curve, a constant non-zero divisor, coming from a constant point P', intersects the curve at infinity on $\mathcal{E}$ only when t is a pole of u.
The curve over which $\mathcal{E}$ splits is given by extending K with $u = \sqrt[4]{A/A_0}$, and this extension $C' \to C$ ramifies above the poles and zeros of u. Hence the support of the pullback divisor $\sigma_{nP}^*(O)$ is contained in the support of the polar divisor of u, and this support is contained in the set of ramification points of the map $C' \to C$. Noting that the proof still works for $j = 0, 1728$, this completes the proof. □

Returning to the proof of our original theorem, we have that lemma 4.0.7 gives us that for any particular point $\gamma \in R_f$, the multiplicity $\mathrm{ord}_\gamma \sigma_{nP_i}^*(\bar{O}_{\mathcal{E}_i})$ is bounded independently of n. Hence by above lemma, $\deg \sigma_{nP_i}^*(\bar{O}_{\mathcal{E}_i})$ is bounded for all $n \geq 1$. Thus $E_i(K)$ contains infinitely many points of bounded degree. Now, using that

$$h(P) = h(x_P) = \sum_{t \in C} \max\{-\mathrm{ord}_t(x), 0\} = \sum_{t \in C} \mathrm{ord}_t^+(x^{-1})$$

(see [20], III.4.1, pp. 212), using that $\frac{1}{2}\mathrm{ord}_t^+(x_P^{-1}) = \mathrm{ord}_t(\sigma_P^*(\bar{O}))$ for all but finitely many t and using that the difference between $\frac{1}{2}\mathrm{ord}_t^+(x^{-1})$ and $\mathrm{ord}_t(\sigma_P^*(\bar{O}))$ is bounded by a constant (see proposition 3.3.9), we have that

$$h(P) = 2 \deg \sigma_P^*(\bar{O}) + O(1).$$

Hence $E_i(K)$ contains infinitely many points of bounded height. It then follows from theorem 2.6.2 that $\mathcal{E}_i \to C$ splits over k.

Thus this case leads to the conclusion that both E_1 and E_2 are K-isomorphic to elliptic curves defined over k, so we may replace them with curves that are defined over k. Then $\mathcal{E}_i = E_i \times_k C$, and any point $Q_i \in E_i(K)$ is associated to a k-morphism $\tau_{Q_i} : C \to E_i$. Our assumption that τ_{P_i} is constant is equivalent to saying that $P_i \in E_i(k)$. Now, $\sigma_{nP_i}^*(\bar{O}_{\mathcal{E}_i})$ is supported on $t \in C$ for which there is a point $(nP, t) \in E_i \times_k C'$ that is zero at t. But

$$(nP_i \times C') \cap (O_i \times C') = \emptyset,$$

so we have that

$$\text{Support}(\sigma^*_{nP_i}(\bar{O}_{\mathcal{E}_i})) = \emptyset.$$

This means that for all n_1, n_2,

$$\text{GCD}(n_1P_1, n_2P_2) = 0$$

which gives a strong form of both statements in the theorem.

4.3 Case 2: τ_{P_1} or τ_{P_2} is Nonconstant, and $\phi(C') \cap (E'_1 \times E'_2)_{tors}$ is Finite

The first statement of the theorem is in this case almost trivial from lemma 4.0.7. We will show how this lemma is applied.
The assumption that τ_{P_1} or τ_{P_2} is nonconstant implies that the map $\phi = \tau_{P_1} \times \tau_{P_2} : C' \to E'_1 \times_k E'_2$ is nonconstant, and hence that $\phi : C' \to \phi(C')$ is finite-to-one. Now, lemma 4.1.1 gives us that

$$\text{Support}(\text{GCD}(n_1P_1, n_2P_2)) \subset f(\phi^{-1}(\phi(C') \cap (E'_1 \times E'_2)_{tors})).$$

Using that $\phi(C') \cap (E'_1 \times E'_2)_{tors}$ is finite and $\phi : C' \to \phi(C')$ is finite-to-one, we then have that

$$f(\phi^{-1}(\phi(C') \cap (E'_1 \times E'_2)_{tors}))$$

is finite hence that

$$\text{Support}(\text{GCD}(n_1P_1, n_2P_2))$$

is a subset of a finite set of points that is independent of n_1 and n_2. Now we can apply lemma 4.0.7 to complete the proof of the first statement: the lemma tells us that for any $\gamma \in C$, the order of $\text{GCD}(n_1P_1, n_2P_2)$ at γ is bounded independently of n_1 and n_2, thus we have that $\text{GCD}(n_1P_1, n_2P_2)$ is bounded.

We will now prove the second statement of the theorem in this case. We've already seen that

$$\text{Support}(\text{GCD}(n_1P_1, n_2P_2)) \subset f(\phi^{-1}(\phi(C') \cap (E'_1 \times E'_2)[n])).$$

Since $\phi(C') \cap (E'_1 \times E'_2)_{tors}$ is finite by assumption, we can find an integer N so that $\phi(C') \cap (E'_1 \times E'_2)_{tors})$ is contained in $(E'_1 \times E'_2)[N]$. It follows that

$$\phi(C') \cap (E'_1 \times E'_2)[n] = \phi(C') \cap (E'_1 \times E'_2)[\gcd(n, N)]$$

for all $n \geq 1$, and hence in particular that

$$\phi(C') \cap (E'_1 \times E'_2)[n] = \phi(C') \cap \{0\}$$

for all n with $\gcd(n, N) = 1$. For those n, this means, since we're dealing with divisibility sequences, that

$$\text{Support}(\text{GCD}(P_1, P_2)) \subseteq \text{Support}(\text{GCD}(nP_1, nP_2)) \subseteq f(\phi^{-1}(\phi(C') \cap \{0\}))$$

Now I claim that $\mathrm{Support}(\mathrm{GCD}(nP_1, nP_2)) = \mathrm{Support}(\mathrm{GCD}(P_1, P_2))$ for all n with $\gcd(n, N) = 1$. If $0 \notin \phi(C')$ this is trivial, so assume that $0 \in \phi(C')$. Then we know that

$$\mathrm{Support}(\mathrm{GCD}(P_1, P_2)) \subseteq \mathrm{Support}(\mathrm{GCD}(nP_1, nP_2)) \subseteq f(\phi^{-1}(\{0\}))$$

On the other hand, we also know that when $\gamma \in f(\phi^{-1}(\{0\}))$, the commutative diagrams in the general part give us that $\gamma \in \mathrm{Support}(\sigma_{P_i}^*(s(\{0\}, C'))) = \mathrm{Support}(\sigma_{P_i}^*(\bar{O}))$, what means that

$$f(\phi^{-1}(\{0\})) \subseteq \mathrm{Support}(\mathrm{GCD}(P_1, P_2)),$$

and hence indeed that

$$\mathrm{Support}(\mathrm{GCD}(nP_1, nP_2)) = \mathrm{Support}(\mathrm{GCD}(P_1, P_2))$$

for all n with $\gcd(n, N) = 1$.
Now,we can apply the first part of lemma 4.0.7, amd this says that the multiplicities of $\mathrm{GCD}(nP_1, nP_2)$ and $\mathrm{GCD}(P_1, P_2)$ are the same at every point in the support of $\mathrm{GCD}(P_1, P_2)$, and hence we have that

$$\mathrm{GCD}(nP_1, nP_2) = \mathrm{GCD}(P_1, P_2)$$

for all n with $\gcd(n, N) = 1$. This proves the second statement of the theorem in this case.

4.4 Case 3: τ_{P_1} or τ_{P_2} is Nonconstant, and $\phi(C') \cap (E_1' \times E_2')_{tors}$ is Infinite

The idea here is to show that this case cannot occur. Having seen the proof of case 2, in this case we do not have that $\mathrm{GCD}(n_1P_1, n_2P_2)$ is supported on a finite set of points that is independent of n_1 and n_2, and this means that the degree of $\mathrm{GCD}(n_1P_1, n_2P_2)$ could most probably become arbitrary large.

To show that this case cannot occur, Raynaud's theorem is applied, and it is shown that P_1 and P_2 cannot be K-independent points.

Theorem 4.4.1 (Raynaud's theorem)**.** *Let k be a field of characteristic zero, and A/k be an abelian variety, and let $V \subset A$ be a subvariety. Then the Zariski closure of $V \cap A_{tors}$ is equal to a finite union of translates of abelian subvarieties of A by torsion points.*

Proof. For the case that V is a curve, which is the case that we need, see Raynaud, M.: Sous-variété d'un variété abélienne et points de torsion. Invent. Math. 71, 207-233 (1983). □

The assumption that τ_{P_1} or τ_{P_2} is nonconstant implies that $V = \phi(C')$ is an irreducible curve, what means that we can apply Raynaud's theorem which tells us that $V \cap (E_1' \times E_2')_{tors}$ can only be infinite if it is contained in the translate of an elliptic curve (an abelian subvariety of $E_1' \times E_2'$) by a torsion point of $E_1' \times E_2'$. Thus there is an elliptic curve $W \subset E_1' \times E_2'$ and a torsion point $t \in E_1' \times E_2'$ so that $v = W + t$. Let N be the order of the point t. Then composing with the multiplication-by-N map yields

$$[N] \circ \phi = [N] \circ (\tau_{P_1} \times \tau_{P_2}) = \tau_{NP_1} \times \tau_{NP_2}.$$

Since W is an elliptic curve, we have that $[N] \circ \phi$ maps C' onto $NV = N(W+t) = NW = W$. Hence we get a commutative diagram:

$$\begin{array}{ccccc} & & C & & \\ & \swarrow^{\tau_{NP_1}} & \downarrow{\scriptstyle [N]\circ\phi} & \searrow^{\tau_{NP_2}} & \\ E_1' & \xleftarrow[\pi_1]{} & W & \xrightarrow[\pi_2]{} & E_2' \end{array}$$

where π_1 and π_2 are the projections $\pi_i : E_1' \times E_2' \to E_i'$.
Write $d_2 = \deg(\pi_2)$. Since W is an elliptic curve, there is a dual isogeny $\hat{\pi}_2 : E_2' \to W$ with the property that $\hat{\pi}_2 \circ \pi_2 = [d_2]$. Now we compute

$$\begin{aligned} [d_2] \circ \tau_{NP_1} &= [d_2] \circ \pi_1 \circ [N] \circ \phi \\ &= \pi_1 \circ [d_2] \circ [N] \circ \phi \\ &= \pi_1 \circ \hat{\pi}_2 \circ \pi_2 \circ [N] \circ \phi \\ &= \pi_1 \circ \hat{\pi}_2 \circ \tau_{NP_2} \\ &= \pi_1 \circ \hat{\pi}_2 \circ [N] \circ \tau_{P_2} \end{aligned}$$

Let $G' : E_2' \to E_1'$ be the isogeny

$$G' = \pi_1 \circ \hat{\pi}_2 \circ [N] \in \mathrm{Hom}_k(E_2', E_1').$$

Recall that $K' = k(C')$ is the extension of K over which E_1 and E_2 become isomorphic to E_1' and E_2' respectively. Thus G' induces an isogeny

$$G : E_2 \to E_1$$

defined over K', but a priori, there is no reason that G needs to be defined over K. However, the relation $\tau_{d_2 NP_1} = [d_2] \circ \tau_{NP_1} = \pi_1 \circ \hat{\pi}_2 \circ [N] \circ \tau_{P_2}$ gives a commutative diagram

$$\begin{array}{ccc} E_2' \times_k C' & \xrightarrow[G'\times 1]{} & E_1' \times_k C' \\ \uparrow{\scriptstyle \tau_{P_2}\times 1} & & \uparrow{\scriptstyle \tau_{d_2 NP_1}\times 1} \\ C' & = & C' \end{array}$$

which is equivalent to the equality

$$G(P_2) = d_2 N P_1$$

of points in $E_1(K)$.
The curves E_1 and E_2 and the points P_1 and P_2 are rational over K by assumption, hence the same is true of the multiple d_1NP_1 of P_1. Thus the above equality says that the isogeny G maps at least one K-rational point of E_2 to a K-rational point of E_1. Further, the independence assumption on P_1 and P_2 ensures that they are not torsion points. Now, the following lemma gives us that G is indeed defined over K:

Lemma 4.4.2. *Let K be a field of characteristic 0, let E_1/K and E_2/K be elliptic curves, and let $G : E_2 \to E_1$ be an isogeny defined over $\bar{K}$. Suppose that there is a K-rational point $P \in E_2(K)$ so that the image $G(P)$ is also K-rational, i.e. $G(P) \in E_1(K)$. Then either P has finite order or else G is defined over K.*

Proof. For each $s \in \mathrm{Gal}(\bar{K}/K)$, define an isogeny g_s be

$$g_s : E_2 \to E_1, g_s(Q) = G^s(Q) - G(Q).$$

The assumption on the point P implies that

$$G(P) = (G(P))^s = G^s(P^s) = G^s(P)$$

so we can see that $P \in ker(g_s)$ for all $s \in \mathrm{Gal}(\bar{K}/K)$. Let $d_s = \deg(g_s)$. Applying the dual isogeny, it follows that $P \in E_2[d_s]$ for all $s \in \mathrm{Gal}(\bar{K}/K)$. Hence either P is a torsion point, or else $d_s = 0$ for all $s \in \mathrm{Gal}(\bar{K}/K)$. But

$$d_s = 0 \leftrightarrow g_s = [0] \leftrightarrow G^s = G$$

so

$$d_s = 0 \text{ for all } s \in \mathrm{Gal}(\bar{K}/K) \leftrightarrow \ G \text{ is defined over } K.$$

This completes the proof that P is either a torsion point or that G is defined over K. □

Continuing with the proof of theorem 4.0.6, we now know that G is indeed defined over K. But now the relation $G(P_2) = d_1NP_1$ tells us that P_1 and P_2 are linearly K-dependent, which is a contradiction. The conclusion is that this case, having τ_{P_1} or τ_{P_2} nonconstant and $\phi(C') \cap (E_1' \times E_2')_{tors}$ infinite, cannot occur. Having proven all three cases, the proposition now follows.

4.5 A Corollary for $C = \mathbb{P}^1$

For $C = \mathbb{P}^1$, Silverman's theorem also applies when we look at the denominators B_{nP} of points on a curve $E/k(T)$.

Corollary 4.5.1. *Take k algebraically closed of characteristic 0. Let $C = \mathbb{P}^1$ and let $P, Q \in E(k(T))$ be independent points on an elliptic curve over $k(T)$, and assume that it has constant j-invariant. Then there is a constant $c = c(E, P, Q)$ so that*

$$\deg \gcd(B_{nP}, B_{nQ}) \leq c.$$

Further, there is an equality

$$\gcd(B_{nP}, B_{nQ}) = \gcd(B_P, B_Q)$$

for infinitely many $n \geq 1$.

Proof. This follows from the above theorem and the fact from corollary 3.5.4 that there is a divisor D, only depending on the elliptic curve, such that

$$|\mathrm{GCD}(P, Q) - \mathrm{div}(\gcd(B_P, B_Q))| \leq D.$$

To see the first statement explicitly, note that for a divisor of a function $D = \mathrm{div}(f)$, we know that $\deg(D) = \deg(f)$. Hence we know that

$$|\deg(\mathrm{GCD}(nP, nQ)) - \deg(\gcd(B_{nP}, B_{nQ}))| \leq deg(D) = c_1,$$

and from the above theorem we have that $\deg \mathrm{GCD}(nP_1, nQ) \leq c_2$, so combining the two statements and putting $c = c_1 + c_2$, the first statement follows.

For the second statement, first note that from the above theorem, we know that the set

$$\{n \geq 1 : \mathrm{GCD}(nP, nQ) = \mathrm{GCD}(P, Q)\}$$

has positive density. Assume for some n that $\mathrm{GCD}(nP, nQ) = \mathrm{GCD}(P, Q)$. For all $t \in \mathbb{P}^1 - \{\infty\}$, we have by proposition 3.3.9 that

$$\mathrm{ord}_t \gcd(B_{nP}, B_{nQ}) = \mathrm{ord}_t \mathrm{GCD}(nP, nQ).$$

For $t = \infty$, the difference between $\mathrm{ord}_t \gcd(B_{nP}, B_{nQ})$ and $\mathrm{ord}_t \mathrm{GCD}(nP, nQ)$ is either 0 or c, where c is a constant only depending on the Weierstrass equation. If $\mathrm{ord}_\infty \gcd(B_P, B_Q) = \mathrm{ord}_\infty \mathrm{GCD}(P, Q) + c$, then since B_P and B_Q are divisibility sequences, we know that for all n with the property that $\mathrm{GCD}(nP_1, nP_2) = \mathrm{GCD}(P_1, P_2)$, we have that

$$\begin{aligned} \mathrm{ord}_\infty \gcd(B_{nP}, B_{nQ}) &= \mathrm{ord}_\infty \mathrm{GCD}(nP, nQ) + c = \mathrm{ord}_\infty \mathrm{GCD}(P, Q) + c \\ &= \mathrm{ord}_\infty \gcd(B_P, B_Q) \end{aligned}$$

and hence

$$\gcd(B_{nP}, B_{nQ}) = \gcd(B_P, B_Q).$$

If on the other hand

$$\mathrm{ord}_\infty \gcd(B_P, B_Q) = \mathrm{ord}_\infty \mathrm{GCD}(P, Q),$$

then for above n, we either have that

$$\mathrm{ord}_\infty \gcd(B_{nP}, B_{nQ}) = \mathrm{ord}_\infty \mathrm{GCD}(nP, nQ)$$

or that

$$\mathrm{ord}_\infty \gcd(B_{nP}, B_{nQ}) = \mathrm{ord}_\infty \mathrm{GCD}(nP, nQ) + c.$$

Since both sequences are strong divisibility sequences, we know that

$$\gcd(B_{p_1 P}, B_{p_2 P}) = B_P$$

for all primes p_1, p_2. Hence this constant c at infinity can only be contained in B_{pP} for one prime number p, and not for any other. More generally, the constant c can only be contained in B_{nP} for $n = kp$ for integers k and a single prime p. Since in the proof of the above theorem (see case 2 mostly), the equality is for all n with $\gcd(n, N) = 1$, we know that there are infinitely many such n with the property that our prime number p does not divide n, and hence for infinitely many n,

$$\gcd(B_{nP}, B_{nQ}) = \gcd(B_P, B_Q).$$

This completes the proof.

□

5 Common Divisors of Elliptic Divisibility Sequences in Characteristic p

The previous section did the case for which the characteristic was zero. When we change the perspective to characteristic p, the results seem to change rather drastically. Most importantly, lemma 4.0.7 does not hold, and this lemma was a fundamental lemma needed for both the 'easy' cases of the proof.
Before we start with elliptic divisibility sequences over function fields in characteristic p, we will first take a closer look at surjective morphisms of curves in general and the Frobenius map in particular.

5.1 Surjective Morphisms of Curves

We recall that a morphism of curves $\phi : E_1 \to E_2$ is either surjective or constant, and that if it is surjective, then it induces an injection of function fields

$$\phi^* : k(E_2) \to k(E_1), \qquad \phi^*(g) = g \circ \phi \text{ for all } g \in k(E_2).$$

Similarly, we can define maps of divisor groups as follows:

$$\phi^* : \mathrm{Div}(E_2) \to \mathrm{Div}(E_1) : (Q) \to \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P),$$

where e_ϕ is the ramification index (see [6], pp. 299), and extend $\mathbb{Z}$-linearly to arbitrary divisors. Recall that we write $\hat{\phi}$ for the dual of ϕ, and note that we write $\hat{\phi}^*$ for the dual of ϕ^*. Now, we have the following proposition.

Proposition 5.1.1. *Let $\phi : E_1 \to E_2$ be a nonconstant (or equivalently, surjective) map of smooth curves. Then the following hold:*

1. $\deg(\phi^* D) = (\deg(\phi))(\deg(D))$ *for all* $D \in \mathrm{Div}(E_2)$.
2. $\phi^*(\mathrm{div}(g)) = \mathrm{div}(\phi^*(g))$ *for all* $g \in \bar{k}(E_2)^*$.
3. *If $\psi : E_2 \to E_3$ is another such map, then $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.*

Proof. See [21], II.3.6, pp. 29. □

5.2 Frobenius Morphism and the Hasse Estimate

Let k be a field of characteristic $p > 0$ and let $q = p^r$. For a polynomial $f \in k[X]$, we write $f^{(q)}$ for the polynomial obtained from f by raising each coefficient to the q^{th} power. For any curve E/k, we can define a new curve $E^{(q)}/k$ as the curve whose homogeneous ideal is given by $I(E^{(q)})$, i.e. the ideal generated by $\{f^{(q)} : f \in I(E)\}$. The Frobenius morphism is a natural map from E to $E^{(q)}$.

Definition 5.2.1. The q^{th}*-power Frobenius morphism* is the map

$$F : E \to E^{(q)} : F([x_0, \ldots, x_n]) = [x_0^q, \ldots, x_n^q].$$

Remark 5.2.2. Note that the q^{th}-power Frobenius morphism indeed maps to $E^{(q)}$: for every point $P = [x_0, \ldots, x_n] \in E$, the image $\phi(P)$ of each generator $f^{(q)}$ of $I(E^{(q)})$ is

$$f^{(q)}(\phi(P)) = f^{(q)}(x_0^q, \ldots, x_n^q) = (f(x_0, \ldots, x_n))^q = 0.$$

Note that we used that $\text{char}(k)|q$.

Using what we know from nonconstant morphisms, we have that the Frobenius morphism induces an injection

$$F^* : k(E^{(q)}) \to k(E), \qquad F^*g = g \circ F \text{ for all } g \in k(E^{(q)})$$

and that there is a map of divisor groups generated by

$$F^* : \text{Div}(E^{(q)}) \to \text{Div}(E) : (Q) \to \sum_{P \in F^{-1}(Q)} e_F(P)(P).$$

The following result is a standard result about the multiplication-by-$[m]$ map and the m-torsion subgroup.

Proposition 5.2.3. *Let E be an elliptic curve and let $m \in \mathbb{Z} - \{0\}$. Then:*

1. $\deg[m] = m^2$,
2. *if $m \neq 0$ in K, i.e. if either $\text{char}(K) = 0$ or $\text{char}(K) = p$ and $p \nmid m$, then*

$$E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},$$

3. *if $\text{char}(K) = p \geq 0$, then one of the following is true:*
   - $E[p] = \{O\}$,
   - $E[p] = \mathbb{Z}/p\mathbb{Z}$.

Proof. See [21], corollary III.6.4, pp. 86. □

Definition 5.2.4. An elliptic curve in characteristic p is called *supersingular* if $E[p] = \{O\}$, and it is called *ordinary* otherwise, i.e. if $E[p] = \mathbb{Z}/p\mathbb{Z}$.

The following proposition about the pullback of the Frobenius map is a key proposition that we will use to show Silverman's conjecture in characteristic p when we do allow p to divide n, see section 5.3.

Proposition 5.2.5. *Let E be an elliptic curve over $k(T)$, let $\bar{O}$ denote the zero divisor on a model of E over $\mathbb{P}^1$ and let $\bar{O}'$ denote the zero divisor on a model of $E^{(p)}$. Then:*

- *we have $F^*(\bar{O}') = p\bar{O}$,*
- *we have $\hat{F}^*(\bar{O}) = \bar{O}' + D$ for some effective divisor D.*

Proof. Since $F^{-1}(\bar{O}') = \{\bar{O}\}$, we have that

$$F^*(\bar{O}') = e_F(\bar{O})\bar{O}.$$

Moreover, $\deg(F^*(\bar{O}')) = (\deg(F))(\deg(\bar{O}')) = p$, and hence we have that

$$F^*(\bar{O}') = p\bar{O}.$$

To show the second statement, we have that

$$F^* \circ \hat{F}^* = (\hat{F} \circ F)^* = [p]^*$$

where $[p]$ is the multiplication-by-p map. Moreover, $[p]^*(\bar{O}) = k\bar{O} + D_P$ for some integer k, where D_p is the divisor of p-torsion points. From proposition 5.2.3, we know that $\deg([p]) = p^2$ and hence

$$\deg([p]^*(\bar{O})) = \deg([p]) \cdot 1 = p^2,$$

and we know that $\#D_P$ is either 0 or p, thus we must have that

$$[p]^*(\bar{O}) = p\bar{O} + D'$$

where D' is some effective divisor (containing the p-torsion subgroup).
Now write $\hat{F}^*(\bar{O}) = \bar{O}' + D$ for some divisor D. We need to show that D is effective. We can calculate

$$\begin{aligned} p\bar{O} + D' &= [p]^*(\bar{O}) = F^* \circ \hat{F}^*(\bar{O}) \\ &= F^*(\bar{O}' + D) = F^*(\bar{O}') + F^*(D) = p\bar{O} + F^*(D) \end{aligned}$$

and hence we know that $F^*(D) = D'$ is effective, and this is only possible when D is also effective. This completes the proof. □

The Hasse bound is a classical result that bounds the number of points on an elliptic curve over a finite field.

Theorem 5.2.6. *Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. Then*

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

Proof. Since we haven't proven all ingredients for the Hasse bound, I will give a short sketch, which is based on the proof given in [21], V.1.1, pp. 138.
Choose a Weierstrass equation for E with coefficients in $\mathbb{F}_q$ and let F denote the usual q^{th} power Frobenius morphism. Since the Galois group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is topologically generated by the q^{th}-power map on $\bar{\mathbb{F}}_q$, we know that for any point $P \in E(\bar{\mathbb{F}}_q)$, we have that

$$P \in E(\mathbb{F}_q) \text{ if and only if } F(P) = P.$$

Thus we have that $E(\mathbb{F}_q) = \ker(1 - F)$ and

$$\#E(\mathbb{F}_q) = \#\ker(1 - F) = \deg(1 - F).$$

Since the degree map on $\mathrm{End}(E)$ is a positive quadratic form and since $\deg(F) = q$, we have that the Cauchy-Schwarz inequality gives us that

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

□

5.3 Silverman's Conjecture

The following theorem is proven by Silverman in his paper [19], which is a strong form of his conjecture for elliptic curves with constant j-invariant.

Theorem 5.3.1. *Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 5$, let $E/\mathbb{F}_q(T)$ be an elliptic curve with constant j-invariant, and let $P, Q \in E(\mathbb{F}_q(T))$ be non-torsion points. Then*

$$\deg \mathrm{GCD}(nP, nQ) \geq cn + O(\sqrt{n}) \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n,$$

for some constant c.
Moreover, this constant c is given by

$$c = \begin{cases} \frac{1}{2} & \text{if } j \neq 0, 1728, \\ 1 & \text{if } j = 1728 \text{ with } q = 3 \bmod 4 \text{ or if } j = 0 \text{ with } q = 2 \bmod 3, \\ \frac{1}{4} & \text{if } j = 1728 \text{ with } q = 1 \bmod 4, \\ \frac{1}{6} & \text{if } j = 0 \text{ with } q = 1 \bmod 3. \end{cases}$$

Remark 5.3.2. Note that Silverman claims that he proves that in all cases,

$$\deg \mathrm{GCD}(nP, nQ) \geq n + O(\sqrt{n}) \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

However, reading the proof carefully, above theorem gives all that can be concluded.

We will go over the proof of this theorem in a minute. First, let us see that the theorem is relatively easy to see if one allows p to divide n, and the assumption of a constant j-invariant is not needed in this case. Since the Frobenius map $F : E^{(p)} \to E$ is an isogeny of degree p, we can factor the multiplication-by-p map $[p]$ as $[p] = F \circ \hat{F}$, where $\hat{F}$ is the dual of F. Let $\bar{O}$ denote the zero divisor on a model of E over $\mathbb{P}^1$ and let $\bar{O}'$ denote the zero divisor on a model of $E^{(p)}$. From proposition 5.2.5, we now know that $F^*(\bar{O}') = p\bar{O}$, and that $\hat{F}^*(\bar{O}) = \bar{O}' + D$ for some effective divisor D, and we can estimate

$$\begin{aligned} \deg \mathrm{GCD}(p^i P, p^i Q) &= \deg \mathrm{GCD}(\sigma_P^* \circ F^{i*} \circ \hat{F}^{i*}(\bar{O}), \sigma_Q^* \circ F^{i*} \circ \hat{F}^{i*}(\bar{O})) \\ &\geq \deg \mathrm{GCD}(\sigma_P^* \circ F^{i*}(\bar{O}'), \sigma_Q^* \circ F^{i*}(\bar{O}')) \\ &= p^i \deg \mathrm{GCD}(\sigma_P^*(\bar{O}), \sigma_Q^*(\bar{O})) \end{aligned}$$

and hence

$$\deg \mathrm{GCD}(nP, nQ) \geq n \cdot \deg \mathrm{GCD}(P, Q)$$

for all $n = p^i$, $i = 1, 2, 3, \ldots$. Hence if $\deg \mathrm{GCD}(P, Q) \neq 0$, then the theorem indeed follows if we would allow p to divide n. However, if $\deg \mathrm{GCD}(P, Q) = 0$, then it doesn't follow. An example of such a case is given in the experiments, see remark 6.5.1.

Remark 5.3.3. As Silverman states, it seems tempting to conjecture a stronger lower bound of the form cn^2. The only obvious upper bound comes from the fact that deg D_{nP} grows asymptotically as fast as n^2 (this is a corollary of Siegel's theorem, see [21], theorem IX.3.1, pp. 276). In section 6, we experiment on this hypothesis, and it seems probable that there are curves for which there is a stronger lower bound of the form cn^2, as well as curves for which no such bound exists.

5.4 Proof of Silverman's Theorem

This proof of the characteristic p case is rather different in nature from the proof of the characteristic zero case: this proof is number-theoretical, while in the characteristic zero case, the proof was almost entirely geometric.

Proof of theorem 5.3.1. Take $E/\mathbb{F}_q(T)$ any elliptic curve, and fix a minimal Weierstrass equation for E. For each integer $N \geq 1$, let

$$S_{q,N} = \{\pi \in \mathbb{F}_q[T] : \pi \text{ is monic, irreducible, and deg } \pi = N\}$$

be the set of monic irreducible polynomials of degree N in $\mathbb{F}_q[T]$. Given any $\pi \in S_{q,N}$, we can reduce E modulo π to obtain an elliptic curve $\tilde{E}_\pi$ defined over the finite field $\mathbb{F}_\pi = \mathbb{F}_q[T]/(\pi)$. The residue fields $\mathbb{F}_\pi \simeq \mathbb{F}_{q^N}$ associated to the various $\pi \in S_{q,N}$ are all isomorphic, but the elliptic curves $\tilde{E}_\pi$ for different primes need not and generally will not be isomorphic. The Hasse estimate now gives us that

$$n_\pi(E) = \#\tilde{E}_\pi(\mathbb{F}_\pi) = q^N + 1 - a_\pi(E)$$

where $|a_\pi(E)| \leq 2q^{N/2}$.
Now suppose that $j(E) \in \mathbb{F}_q$ and assume for now that $j(E) \neq 0, 1728$. This means that there is an elliptic curve $E'/\mathbb{F}_q$ so that E is a quadratic twist of E'. In other words, if E' is given by a Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_q^*$, then E has a Weierstrass equation

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

for some squarefree $D \in \mathbb{F}_q[T]$ (note that this is where the $\text{char}(k) \geq 5$ assumption is used, see proposition 2.7.2). Replacing a, b by r^2a, r^3b and $D(T)$ by $r^{-1}D(T)$ for an appropriate $r \in \mathbb{F}_q^*$, we may assume that $D(T)$ is monic. For now, we assume that $D(T) \neq 1$, so E is a nontrivial twist of E'.
For any $\pi \in S_{q,N}$ with $\pi \nmid D$, the curve $\tilde{E}_\pi/\mathbb{F}_\pi$ is isomorphic over $\mathbb{F}_\pi$ to either $E'/\mathbb{F}_{q^N}$ or to its unique quadratic twist. More precisely, $\tilde{E}_\pi/\mathbb{F}_\pi$ is isomorphic over $\mathbb{F}_\pi$ to $E'/\mathbb{F}_{q^N}$ if $D \in \mathbb{F}_\pi^{*^2}$ and to its twist if $D \in \mathbb{F}_\pi^* \backslash \mathbb{F}_\pi^{*^2}$.
Write $a_N(E') := q^N + 1 - \#E'(\mathbb{F}_{q^N})$. Hence if D is a square in $\mathbb{F}_\pi$, then we have $a_\pi(E) = a_N(E')$. If on the other hand D is not a square, then $\tilde{E}_\pi/\mathbb{F}_\pi$ is isomorphic to the quadratic twist of $E'/\mathbb{F}_{q^N}$, and $\#E'/\mathbb{F}_{q^N} + \#\text{twist}(E'/\mathbb{F}_{q^N}) = 2(q^N + 1)$

(see [16], 3, pp. 224), where $\text{twist}(E'/\mathbb{F}_{q^N})$ is the twist of $E'/\mathbb{F}_{q^N}$. Hence in this case we have that

$$a_\pi(E) = q^N+1-\#\text{twist}(E'/\mathbb{F}_{q^N}) = q^N+1-2(q^N+1)+(q^N+1-a_N(E')) = -a_N(E').$$

Therefore, we have that

$$a_\pi(E) = \left(\frac{D}{\pi}\right) a_N(E')$$

where $\left(\frac{D}{\pi}\right)$ is the Legendre symbol. We divide the set of primes $S_{q,N}$ into two subsets,

$$\begin{aligned} S^+_{q,N}(D) &= \{\pi \in S_{q,N} | \left(\frac{D}{\pi}\right) = 1\}, \\ S^-_{q,N}(D) &= \{\pi \in S_{q,N} | \left(\frac{D}{\pi}\right) = -1\}. \end{aligned}$$

Then

$$n_\pi(E) = \begin{cases} q^N + 1 - a_N(E') & \text{for all } \pi \in S^+_{q,N} \\ q^N + 1 + a_N(E') & \text{for all } \pi \in S^-_{q,N}. \end{cases}$$

For a fixed D, the quadratic reciprocity law for $\mathbb{F}_q[T]$ (see [15], 3.5, pp. 27) says that

$$\left(\frac{D}{\pi}\right) = (-1)^{\frac{q-1}{2}\cdot N\cdot \deg(D)} \left(\frac{\pi}{D}\right).$$

This means that for fixed D, the power of -1 only depends on N, the degree of π. For fixed D and N, this means that we either have $\left(\frac{D}{\pi}\right) = \left(\frac{\pi}{D}\right)$ or we have $\left(\frac{D}{\pi}\right) = -\left(\frac{\pi}{D}\right)$ for all π of degree N, and thus we can write

$$S^+_{q,N}(D) = \{\pi \in S_{q,N} | \left(\frac{\pi}{D}\right) = 1\} \text{ or } S^+_{q,N}(D) = \{\pi \in S_{q,N} | \left(\frac{\pi}{D}\right) = -1\}.$$

Now, $\left(\frac{\pi}{D}\right) = 1$ implies that $\pi \mod D \in \{a_1, \ldots, a_r\}$, where $a_1, \ldots, a_r$ are the squares mod D, and there are $r = \Phi(D)/2$ of them, where $\Phi(D)$ is the number of nonzero polynomials of degree less then $\deg(D)$ and relatively prime to D. By Dirichlets theorem (see [15], theorem 4.8, pp. 40), writing

$$S_N(a_i, D) := \{\pi \in S_{q,N} | \pi = a_i \mod D\},$$

we have that

$$\#S_N(a_i, D) = \frac{1}{\Phi(D)}\frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right),$$

hence we have that

$$\#S^+_{q,N} = \#\bigcup_{i=1}^{r} S_N(a_i, D) = \frac{\Phi(D)}{2}\left(\frac{1}{\Phi(D)}\frac{q^N}{N} + O(\frac{q^{N/2}}{N})\right) = \frac{q^N}{2N} + O\left(\frac{q^{N/2}}{N}\right).$$

Moreover, if $\left(\frac{\pi}{D}\right) = -1$, then the same thing follows analogously. Now, doing precisely the same for $S^-_{q,N}(D)$, we get that

$$\#S^-_{q,N} = \frac{q^N}{2N} + O\left(\frac{q^{N/2}}{N}\right).$$

Let $P, Q \in E(\mathbb{F}_q(T))$ be non-torsion points, and let $n = n_\pi(E) = q^N + 1 - a_N(E')$. Since n is the number of points on the curve $\tilde{E}_\pi(\mathbb{F}_\pi)$, we know that n annihilates $\tilde{E}_\pi(\mathbb{F}_\pi)$ (i.e. n times a point on $\tilde{E}_\pi(\mathbb{F}_\pi)$ is the point at infinity). Write $nP = \left(\frac{A_{nP}}{B^2_{nP}} : \frac{C_{nP}}{B^3_{nP}} : 1\right) = (A_{nP}B_{nP} : C_{nP} : B^3_{nP})$, then we know that if we reduce nP modulo π, we will get the point at infinity on $\tilde{E}_\pi(\mathbb{F}_\pi)$, i.e. we know that B_{nP} is divisible by all such π. Since the same is true for nQ, we obtain a lower bound

$$\deg \mathrm{GCD}(B_{nP}, B_{nQ}) \geq \sum_{\pi \in S^+_{q,N}} \deg(\pi) = \#S^+_{q,N} \cdot N = \frac{q^N}{2} + O(q^{N/2}) = n/2 + O(\sqrt{n}).$$

Similarly, if $n = q^N + 1 + a_N(E')$, then the same argument using the primes $\pi \in S^-_{q,N}$ yield the same lower bound. Hence we have that

$$\deg \mathrm{GCD}(B_{nP}, B_{nQ}) \geq n/2 + O(\sqrt{n}) \text{ for all } n = q^N + 1 \pm a_N(E')$$

with $N = 1, 2, 3, \ldots$. This estimate is exactly the lower bound that we are trying to prove, subject to the additional constraint that we want n to be relatively prime to p. However, it is clear that at least one of the numbers $n = q^N + 1 + a_N(E')$ and $n = q^N + 1 - a_N(E')$ is prime to p, since otherwise p would divide their sum $2q^N + 2$, which is only possible when $p = 2$, contrary to assumption. Therefore, the bound holds for infinitely many values if n with $p \nmid n$, which completes the proof.

Now consider the case that E is a trivial twist of E'. Then E is $\mathbb{F}_q(T)$-isomorphic to a curve defined over $\mathbb{F}_q$, and thus $E(\mathbb{F}_q(T)) = E'(\mathbb{F}_q(T)) = E'(\mathbb{F}_q)$, since a nonconstant point in $E'(\mathbb{F}_q(T))$ would correspond to a nonconstant morphism $\mathbb{P}^1 \to E'$. But the group $E'(\mathbb{F}_q(T))$ is finite, so $E(\mathbb{F}_q(T))$ has no non-torsion points, and the statement of the theorem is vacuously true.

Let $j(E) = 1728$, then there is an elliptic curve $E'/\mathbb{F}_q$ so that E is a twist of E'. In other words, if E' is given by a Weierstrass equation $y^2 = x^3 + ax$ with $a \in \mathbb{F}^*_q$, then E has a Weierstrass equation

$$E : y^2 = x^3 + Dax$$

for some $D \in \mathbb{F}_q[T]$. Replacing a by ra and $D(T)$ by $r^{-1}D(T)$, we may assume that $D(T)$ is monic.

First assume that $q = 3 \bmod 4$. Then, for odd N, we also have that $q^N = 3 \bmod 4$. Using Jacobi sums (see [8], theorem 18.5.5, pp. 307), it is not hard to show that

$$n_\pi(E) = q^N + 1$$

for all $\pi \in S_{q,N}$, where N is odd.
Hence just as in the above proof, we have that q^N+1 annihilates $\tilde{E}_\pi$, and $B_{(q^N+1)P}$ is divisible by all such π. Thus

$$\deg \mathrm{GCD}(B_{nP}, B_{nQ}) \geq \sum_{\pi \in S_{q,N}} \deg(\pi) = \#S_{q,N} \times N = q^N + O(q^{N/2}) = n + O(\sqrt{n})$$

for all $n = q^N + 1$ with N odd. Noting that $p \not| \, q^N + 1$, this completes the proof of this case.
Now assume that $q = 1 \bmod 4$, then for all N, $q^N = 1 \bmod 4$. Write $q^N = \phi\bar{\phi}$ with $\phi = a + bi \in \mathbb{Z}[i]$ such that $\phi = 1 \bmod 2 + 2i$, then, again using [8], theorem 18.5, pp. 307, we have that

$$n_\pi(E) = q^N + 1 - \left(\frac{\overline{D_\pi}}{\phi}\right)_4 \phi - \left(\frac{D_\pi}{\phi}\right)_4 \bar{\phi}$$

where D_π is D modulo π, i.e., it is the D in the equation for $\tilde{E}_\pi$, and $()_4$ is the 4-th power residue symbol. Hence $\left(\frac{D_\pi}{\phi}\right)_4 \in \{1, -1, i, -i\}$ and

$$-\left(\frac{\overline{D_\pi}}{\phi}\right)_4 \phi - \left(\frac{D_\pi}{\phi}\right)_4 \bar{\phi} \in \{2a, -2a, 2b, -2b\}.$$

Using the same argument as above, again by using Dirichlet's theorem to show that all four subsets are roughly equal in size, it follows that

$$\deg \mathrm{GCD}(B_{nP}, B_{nQ}) \geq \frac{1}{4}\#S_{q,N} \times N = \frac{1}{4}q^N + O(q^{N/2}) = n/4 + O(\sqrt{n}).$$

Let $j(E) = 0$, then there are again two cases. If $q = 2 \bmod 3$, then

$$n_\pi(E) = q^N + 1$$

for all $\pi \in S_{q,N}$ where N is odd (see [8], theorem 18.4, pp. 305) and we again have that

$$\deg \mathrm{GCD}(B_{nP}, B_{nQ}) \geq \sum_{\pi \in S_{q,N}} \deg(\pi) = \#S_{q,N} \times N = q^N + O(q^{N/2}) = n + O(\sqrt{n})$$

for all $n = q^N + 1$ with N odd.
If on the other hand $q = 1 \bmod 3$, writing $q^N = \phi\bar{\phi}$ with $\phi = a + b\omega + c\omega^2 \in \mathbb{Z}[\omega]$ where $\omega = e^{2\pi i/3}$ and $\phi = 2 \bmod 3$, we have that

$$n_\pi(E) = q^N + 1 + \left(\frac{\overline{4D_\pi}}{\phi}\right)_6 \phi + \left(\frac{4D_\pi}{\phi}\right)_6 \bar{\phi},$$

where $()_6$ is the 6-th power residue symbol. Now, $\left(\frac{4D_\pi}{\phi}\right)_6 \in \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$ and

$$\left(\frac{\overline{4D_\pi}}{\phi}\right)_6 \phi + \left(\frac{4D_\pi}{\phi}\right)_6 \bar{\phi} \in \{2a-2b-2c, -2a+2b+2c, -a-b+2c, a+b-2c, -a+2b-c, a-2b+c\}.$$

Then,in the same way as above, we have

$$\deg \mathrm{GCD}(B_{nP}, B_{nQ}) \geq \frac{1}{6}\#S_{q,N} \times N = \frac{1}{6}q^N + O(q^{N/2}) = n/6 + O(\sqrt{n}).$$

□

Remark 5.4.1. Silverman claims that he proves that

$$\deg \mathrm{GCD}(nP, nQ) \geq n + O(\sqrt{n}) \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

However, in his prove, he uses that

$$\frac{q^N}{2} + O(q^{N/2}) = n + O(\sqrt{n})$$

for $n = q^n + 1 \pm a_N(E')$, which is incorrect. If we replace this with

$$\frac{q^N}{2} + O(q^{N/2}) = n/2 + O(\sqrt{n}),$$

as we did in our version of the proof above, then the conclusion is the slightly weaker, namely that

$$\deg \mathrm{GCD}(nP, nQ) \geq n/2 + O(\sqrt{n}) \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

Also, for $j = 0, 1728$, the result is weaker.

Remark 5.4.2. In characteristic 3, we expect that there is a similar proof of the above theorem using the characteristic 3 analogue of proposition 2.7.2.

5.5 Points on Different Elliptic Curves

In characteristic 0, the proof we've seen was also valid when taking the points P and Q on two different elliptic curves, as well as allowing n to be chosen differently on both curves. In this subsection, we discuss the question whether this is also the case with above proof in characteristic p.

Take P and Q on two different elliptic curves. The above proof does *not* generalize to this case. If P and Q lie on different elliptic curves with constant j-invariant $j \neq 0, 1728$, then the n for which B_{nP} is divisible by all primes in $S^-_{q,N}$ is $n_\pi(E) = q^N + q - a_N(E')$. Arguing heuristically, the chance that this happens for the same n around q^N for both P and Q is 1 over the size of the Hasse bound on $a_N(E')$. This means that we can calculate the chance that after some $N = N_0$, it never happens again that $a_N(E'_1) = \pm a_N(E'_2)$, and this chance is

$$\prod_{N=N_0}^{\infty} (1 - \frac{1}{2\sqrt{q^{N/2}}}) \geq \prod_{N=N_0}^{\infty} (1 - \frac{1}{2\sqrt{2^{N/2}}}).$$

This product converges, and as N_0 goes up, it converges to a value that converges to 1. For example if we take $N_0 = 50$, then there is over a 99.9% chance that $a_N E_1' \neq \pm a_N E_2'$ for all $N > N_0$.

There is one case for which the result does generalize.

Corollary 5.5.1. *Let $P_1 \in E_1$ and $P_2 \in E_2$ be non-torsion points on elliptic curves $E_1/\mathbb{F}_q(T)$, $E_2/\mathbb{F}_q(T)$, with $j = 0$ and $q = 2$ mod 3 or $j = 1728$ and $q = 3$ mod 4. Then*

$$\deg \ \mathrm{GCD}(nP_1, nP_2) \geq n + O(\sqrt{n}) \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

Proof. Using the notation of the above proof, we have that

$$n_\pi(E_i) = q^N + 1$$

for all $\pi \in S_{q,N}$, which is valid for E_1 as well as for E_2. Hence the same way as in the above proof,

$$\deg \mathrm{GCD}(B_{nP}, B_{nQ}) \geq \sum_{\pi \in S_{q,N}} \deg(\pi) = \#S_{q,N} \times N = q^N + O(q^{N/2}) = n + O(\sqrt{n}).$$

□

If we also allow to look at multiples $n_1 P$ and $n_2 Q$ with n_1 not necessarily equal to n_2, the result does generalize, and this is made precise in the following corollary.

Corollary 5.5.2. *Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 5$, let $E_1/\mathbb{F}_q(T)$ and $E_2/\mathbb{F}_q(T)$ be elliptic curves with constant j-invariant $j \neq 0, 1728$, and let $P_1 \in E_1(\mathbb{F}_q(T))$ and $P_2 \in E_2(\mathbb{F}_q(T))$ be non-torsion points. Then writing $n = max(n_1, n_2)$,*

$$\deg \ \mathrm{GCD}(n_1 P_1, n_2 P_2) \geq n/4 + O(\sqrt{n})$$

for infinitely many pairs (n_1, n_2), $n_i \geq 1$ with $p \nmid n_i$, where the big-O constant only depends on $E_1/\mathbb{F}_q(T)$ and $E_2/\mathbb{F}_q(T)$.

Proof. For each N, using the notation from the proof above, let $n_1 = q^N + 1 + a_N(E_1')$ and $n_2 = q^N + 1 + a_N(E_2')$. Because D is different for both elliptic curves, also the sets $S^+_{q,N}(D)$ and $S^-_{q,N}(D)$ are different for both curves. Still, if D_1 corresponds to E_1 and D_2 corresponds to E_2, then either

$$\#\left(S^+_{q,N}(D_1) \cap S^+_{q,N}(D_2)\right) \geq \frac{1}{2} \#S^+_{q,N}(D_1)$$

or

$$\#\left(S^+_{q,N}(D_1) \cap S^-_{q,N}(D_2)\right) \geq \frac{1}{2} \#S^+_{q,N}(D_1).$$

Hence potentially matching $S^+_{q,N}(D_1)$ of the first curve with $S^-_{q,N}(D_2)$ of the second curve, we can assume that at least half of the π in $S^+_{q,N}(D_1)$ are also in

the corresponding set for E_2. Hence in the same way as in the proof above, we have that

$$\mathrm{GCD}(B_{n_1 P_1}, Bn_2 P_2) \geq \frac{1}{2} \cdot \#S^{+}_{q,N} \cdot N = \frac{q^N}{4} + O(q^{N/2}) = n/4 + O(\sqrt{n}).$$

□

If $j = 0$ or $j = 1728$, an analogue to above corollary is possible, and this is left to the reader.

6 Experiments and Examples

We will first take a short moment to dwell on what is proven so far, what is most probably true, and what is still an open question. After that, we will do some experiments for all three parts: for what we have proven, the experiments can be thought of as examples; for what is most probably true they are something between examples and support; and for the open questions, they are support to state conjectures.

We started with the characteristic zero case, and in this case, at least when the j-invariant is constant, we know that the degree of the greatest common divisor of multiples of points,

$$\deg \mathrm{GCD}(n_1P_1, n_2P_2),$$

is bounded by a constant independent of n_1 and n_2. Thus we have a very strong upper bound on the size of $\deg \mathrm{GCD}(n_1P_1, n_2P_2)$ in the characteristic zero case. Furthermore, we've seen that $\mathrm{GCD}(nP_1, nP_2)$ is equal to $\mathrm{GCD}(P_1, P_2)$ for infinitely many n, or even stronger, that the set

$$\{n \geq 1 : \mathrm{GCD}(nP_1, nP_2) = \mathrm{GCD}(P_1, P_2)\}$$

has positive density.
The constant upper bound in this characteristic zero case is as good as we could hope for, and there are no open questions here - the only thing that remains open, but is thought to be precisely the same, is the case of a non-constant j-invariant.

In the characteristic p case, we've seen a proof of a lower bound, that holds for infinitely many n with $p \nmid n$. This lower bound grows linearly in n, and gives a real difference between the characteristic p and the characteristic 0 case: this lower bound shows that a constant upper bound cannot exists in the characteristic p case. Again, we've only seen a proof that assumed that the j-invariant of the elliptic curve over the function field was constant - if it is not constant, then the proof does not work, but still we are very tempted to think that the lower bound will still hold. Also, the proof assumed that $p \geq 5$, but for lower characteristic, similar results are expected.

Hence in characteristic p we showed that there are infinitely many n with $p \nmid n$ such that $\deg \mathrm{GCD}(nP_1, nP_2)$ lies somewhere between $n + \mathcal{O}(\sqrt{n})$ and cn^2 for some c, where the upper bound comes from the fact that $\deg B_{nP}$ grows asymptotically as n^2.
Now, it is still an open question whether or not there are always infinitely many n, with or without $p \nmid n$, such that $\deg \mathrm{GCD}(nP_1, nP_2)$ has a lower bound of the form cn^2. Also, it is an open question whether or not we have $\mathrm{GCD}(nP_1, nP_2) = \mathrm{GCD}(P_1, P_2)$ for infinitely many n. Moreover, we can wonder which of these things are true when we take P_1 and P_2 on two different elliptic

curves instead of on the same one.

In this section, our main focus will be to try and conjecture the answers to these three open questions. Along the way, we will see examples of all the other cases as comparison, and we will also look at curves with non-constant j-invariant, to see if we can spot any apparent differences.

Except for their specific properties, the surfaces chosen can be thought of as "randomly chosen", whatever that can mean, and different "randomly chosen" surfaces are expected to give similar results. All calculations are done in Magma, and the pictures are made in Mathematica. Tables with the results of the experiments can be found in appendix A.

6.1 Examples in Characteristic Zero

When starting experiments on deg $\mathrm{GCD}(nP, nQ)$ in characteristic 0, it is directly apparent that this degree always stays very low. Of course, this is what we should expect, because it is bounded by a constant independent of n. For example, if we take the curves

$$\begin{aligned}
E_1 : y^2 &= x^3 - T^2x + 1 \text{ with the point } P_1 = (x_{P_1}, y_{P_1}) = (T, 1),\\
E_2 : y^2 &= x^3 - T^2(T^2-1)x \text{ with the point } P_2 = (x_{P_2}, y_{P_2}) = (1-T^2, 1-T^2),\\
E_3 : y^2 &= x^3 - (T^2-1)x + T^2 \text{ with the point } P_3 = (x_{P_3}, y_{P_3}) = (0, T),\\
E_4 : y^2 &= x^3 - T^2x + T^2 \text{ with the point } P_4 = (x_{P_4}, y_{P_4}) = (T, T),
\end{aligned}$$

then we can calculate deg $\mathrm{GCD}(nP, nQ)$ for all 6 combinations, and for all n at least up to 32, all of those degrees are zero. The denominators of the x-coordinates of the points nP and nQ never share any root.

Let's construct an example in which the degree of $\mathrm{GCD}(nP, nQ)$ is not always zero. E_1, as defined above, also has the point $P = (T^{-2}, T^{-3})$ where the denominator has 0 as a root. It is not hard to construct another elliptic curve and a point with this property. Let

$$E_5 : y^2 = x^3 + T^4x - 1$$

with the point $Q = (T^{-4}, T^{-6})$. Calculating, we find that $\mathrm{GCD}(nP, nQ)$ is, for all n at least up to 12, equal to T, with degree 1. By lemma 4.0.7, we indeed have that

$$\mathrm{ord}_0\sigma^*_{mP}(\bar{O}) = \mathrm{ord}_0\sigma^*_P(\bar{O}) = 1 = \mathrm{ord}_0\sigma^*_Q(\bar{O}) = \mathrm{ord}_0\sigma^*_{mQ}(\bar{O}),$$

so the order at 0 is indeed always just 1.

If we take E_5 with $Q = (T^{-4}, T^{-6})$ and E_1 using the other point $P_1 = (T, 1)$, calculations seem to give, at least for all n up to 12, that $\mathrm{GCD}(nP_1, nQ) = t$ whenever n is a multiple of 3, and $\mathrm{GCD}(nP_1, nQ) = 0$ otherwise. Something like this is to be expected; again using lemma 4.0.7, we have that

$$\mathrm{ord}_0\sigma^*_{mP}(\bar{O}) \in \{0, 1\}$$

and

$$\mathrm{ord}_0\sigma^*_{mQ}(\bar{O}) \in \{0, 1\}$$

for all m, and the sequences are strong divisibility sequences, i.e.,

$$gcd(B_{nP}, B_{mP}) = B_{gcd(m,n)P}.$$

In all cases, $\mathrm{GCD}(nP, nQ)$ seems to be very bounded indeed, and the fact that many curves used here do not have a constant j-invariant does not seem to matter.

6.2 Two Points on $E : y^2 = x^3 + T^2x + T$ in Characteristic 3

We will start with the curve

$$E : y^2 = x^3 + T^2x + T$$

having independent non-torsion points

$$P = \left(\frac{T^2 + T + 1}{(T+1)^2}, \frac{2T^4 + 2T + 1}{(T+1)^3}\right) \quad \text{and} \quad Q = (1, T + 2).$$

We calculated $\deg \mathrm{GCD}(nP, nQ)$ for all n up to 390, and the results can be found in figure 3. It is apparent from the graphs that this degree seems to grow quadratically. Looking at the top picture, one can notice that the three points on or near the top line have $n = 3^k$ with $k = 1, 2, 3, \ldots$.
When we instead decide to look only at points with n not a multiple of 3, we still see high points lying on the second quadratic line, and they turn out to be the points with

$$n = 3^k \pm 1.$$

This thus gives strong evidence that there are elliptic curves with two independent points in characteristic 3 such that for infinitely many n,

$$\deg \mathrm{GCD}(nP, nQ) \geq cn^2$$

for some constant c, and that this is still true if we do not allow the characteristic 3 to divide n.

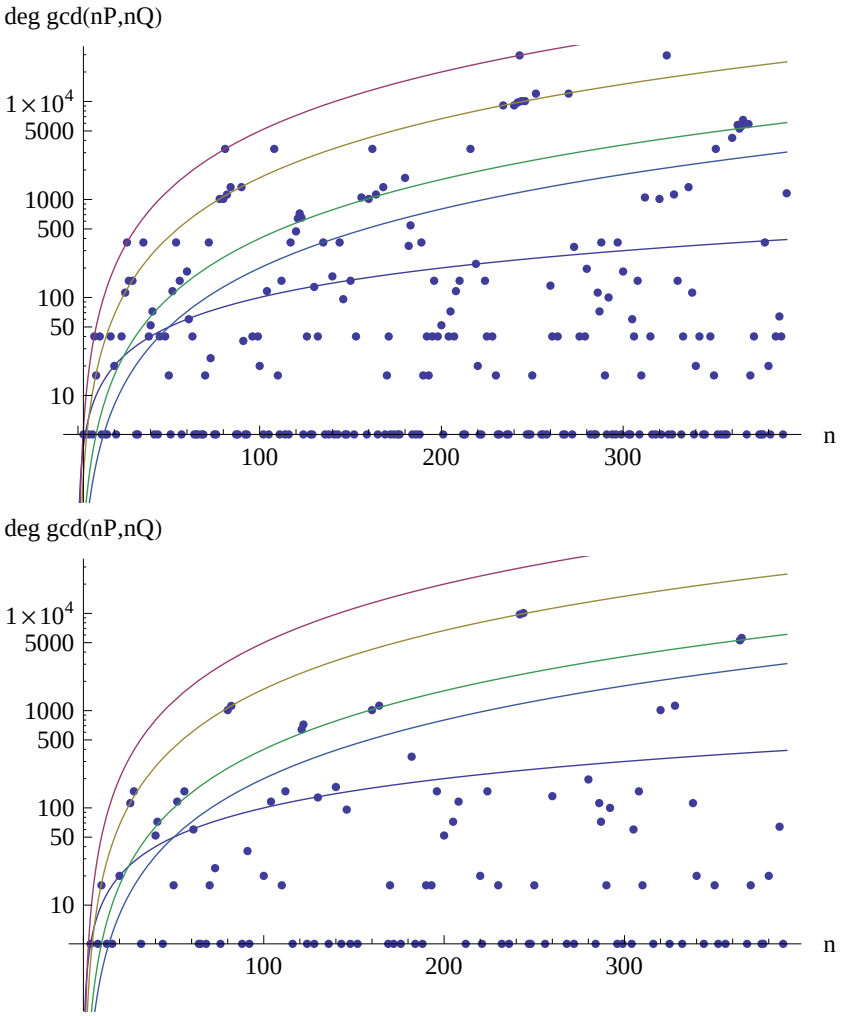


Figure 3: Graphs of the degree of the GCD of nP and nQ on $y^2 = x^3 + T^2x + T$ on a logarithmic scale, where $P = \left(\frac{T^2+T+1}{(T+1)^2}, \frac{2T^4+2T+1}{(T+1)^3}\right)$ and $Q = (1, T+2)$, over a function field with characteristic 3. The top picture shows all n, the bottom picture shows n that are not a multiple of 3. The lines are, starting from top going down, the functions $x^2/70$ (red), $x^2/200$ (yellow), $x^2/500$ (green), $x^2/1000$ (blue) and $x/5$ (dark blue).

```
p:=3;
F:=GF(p);
K<t>:=FunctionField(F);
E:=EllipticCurve([0,0,0,t^2,t]);
point:= E![1,t+2,1];
pt:= C![(t^2+t+1)/((t+1)^2),(2*t^4+2t+1)/(t+1)^3,1];
Q<t> := PolynomialRing(GF(p));
newpoint:=point;
newpt:=pt;
set:=<Degree(Gcd(Q!(Denominator((newpoint)[2])/Denominator((newpoint)[1])),
Q!(Denominator((newpt)[2])/Denominator((newpt)[1])))>;
for k:=2 to 200 do
newpoint:=newpoint+point;
newpt:=newpt+pt;
a:=Gcd(Q!(Denominator((newpoint)[2])/Denominator((newpoint)[1])),
Q!(Denominator((newpt)[2])/Denominator((newpt)[1]))); set:=Append(set,Degree(a));
end for;
set;
```

Figure 4: Magma code used to calculate $\deg \mathrm{GCD}(nP, nQ)$ for n up to 200 for $E : y^2 = x^3+T^2x+T$ and $P = \left(\frac{T^2+T+1}{(T+1)^2}, \frac{2T^4+2T+1}{(T+1)^3}\right)$ and $Q = (1, T+2)$. The code used in the characteristic 0 case is similar with $F := \mathit{RationalField}()$; instead. In the characteristic 3 case, most machine time is spend calculating the sums newpoint:=newpoint+point; and newpt:=newpt+pt;.

6.3 Dependent Points

Here we will give an example of what the graph looks like for dependent points. Take

$$E_1 : y^2 \quad = \quad x^3 - T^2x + 1 \text{ with the point } P_1 = (x_{P_1}, y_{P_1}) = (T, 1)$$

and

$$E_4 : y^2 \quad = \quad x^3 - T^2x + T^2 \text{ with the point } P_4 = (x_{P_4}, y_{P_4}) = (T, T)$$

in characteristic 3. Take a look at figure 5. From this figure, we see that there is something peculiar going on with E_1 and E_4: the numbers are high, and increasing with few exceptions. Closer examination shows that 168 of the 201 calculated points lie on the line $x^2/6$ rounded down, and when we only look at points with n not a multiple of 3, all points lie on the line $x^2/6$ rounded down. Furthermore, closer examination also shows that in all cases, the degree of the GCD is just a big as the degree of the point on E_1.
The difference between this case an all the others, is that in characteristic 3, the points we've chosen on E_1 and E_4 are not linearly independent. To see this, let us construct an isogeny. Recall that $E_1 : y^2 = x^3 - T^2x + 1$ with the point

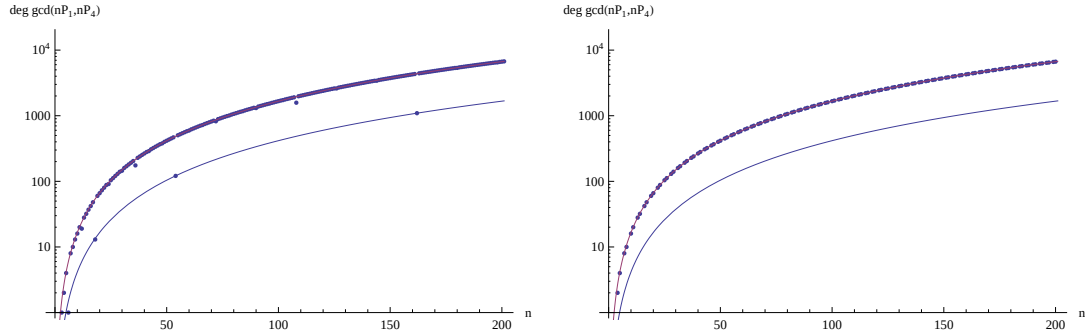


Figure 5: The degree of the GCD of the sequences on E_1 and E_4 over a function field with characteristic 3. The picture on the left shows all n, the picture on the right only show n that are not a multiple of 3. The lines are the functions $x^2/6$ (red) and $x^2/24$ (blue). Note that the scale on the degree is logarithmic.

$P_1 = (T, 1)$ and $E_4 : y^2 = x^3 - T^2x + T^2$ with the point $P_4 = (T, T)$
Let

$$\phi : E_4 \to E_1 : (x, y) \to (x^3/t^2, y^3/t^3).$$

If $(x, y) \in E_4$ is a point on E_4, then, using that the field has characteristic 3,

$$\left(\frac{y^3}{t^3}\right)^2 = \frac{(x^3 - t^2x + t^2)^3}{t^6} = \frac{x^9 - t^6x^3 + t^6}{t^6} = \left(\frac{x^3}{t^2}\right)^3 - t^2\left(\frac{x^3}{t^2}\right) + 1$$

and hence $(x^3/t^2, y^3/t^3)$ indeed lies on E_4. Thus ϕ is a morphism from E_4 to E_1 satisfying $\phi(O_1) = O_2$, so it is an isogeny. Furthermore, we have that $\phi(P_4) = \phi((t, t)) = \left(\frac{t^3}{t^2}, \frac{t^3}{t^3}\right) = (t, 1) = P_1$, hence we indeed have, in characteristic 3, that P_4 and P_1 are linearly dependent points.

6.4 Points on Different Elliptic Curves

One can wonder if what we just saw on $E : y^2 = x^3 + T^2 + T$ taking two points on the same curve, is still probable when we take the two independent points on separate elliptic curves. To have a good look at this, we will have two examples. Let the field characteristic be 3 and look at the curves

$$\begin{aligned}
E_1 : y^2 &= x^3 - T^2x + 1 \text{ with the point } P_1 = (x_{P_1}, y_{P_1}) = (T, 1), \\
E_2 : y^2 &= x^3 - T^2(T^2 - 1)x \text{ with the point } P_2 = (x_{P_2}, y_{P_2}) = (1 - T^2, 1 - T^2), \\
E_3 : y^2 &= x^3 - (T^2 - 1)x + T^2 \text{ with the point } P_3 = (x_{P_3}, y_{P_3}) = (0, T).
\end{aligned}$$

We will look at $\deg \mathrm{GCD}(nP_1, nP_2)$ and at $\deg \mathrm{GCD}(nP_1, nP_3)$, see figures 6 and 7.

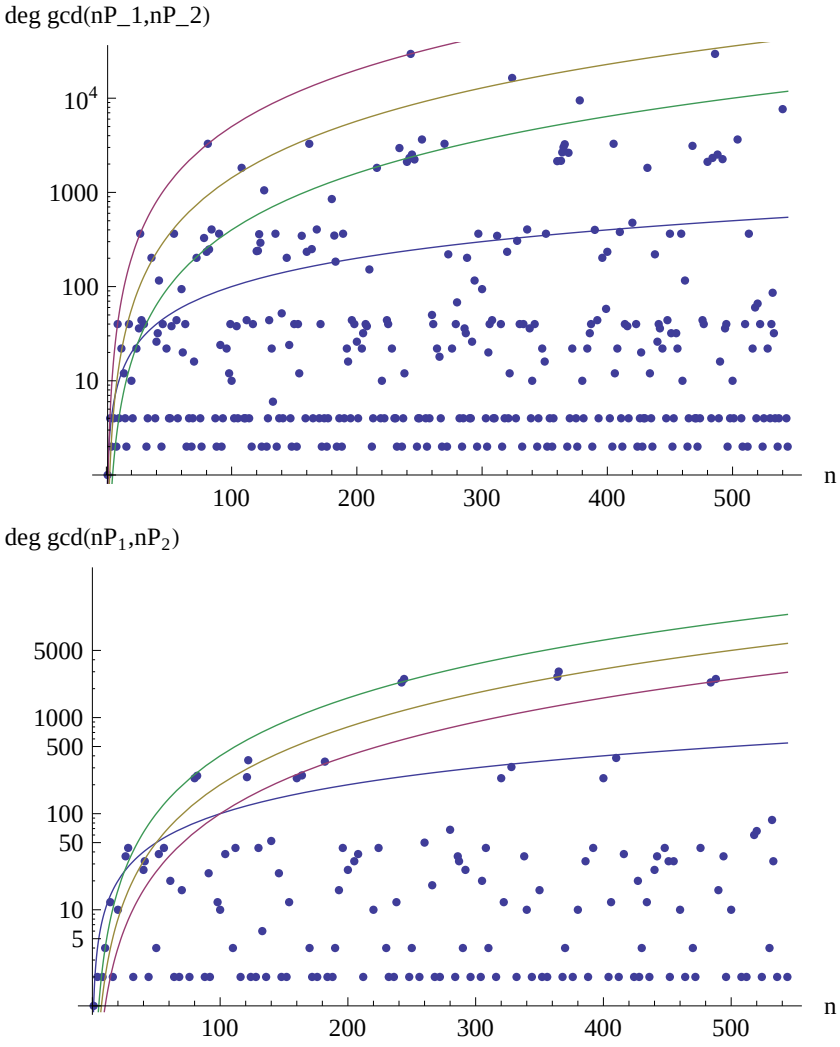


Figure 6: Graphs of the degree of the GCD of nP_1 and nP_2 over a function field with characteristic 3. The top picture shows all n, the bottom picture shows n that are not a multiple of 3. The lines are $\{x, x^2/2, x^2/7, x^2/25\}$ and $\{x, x^2/25, x^2/50, x^2/100\}$ respectively.

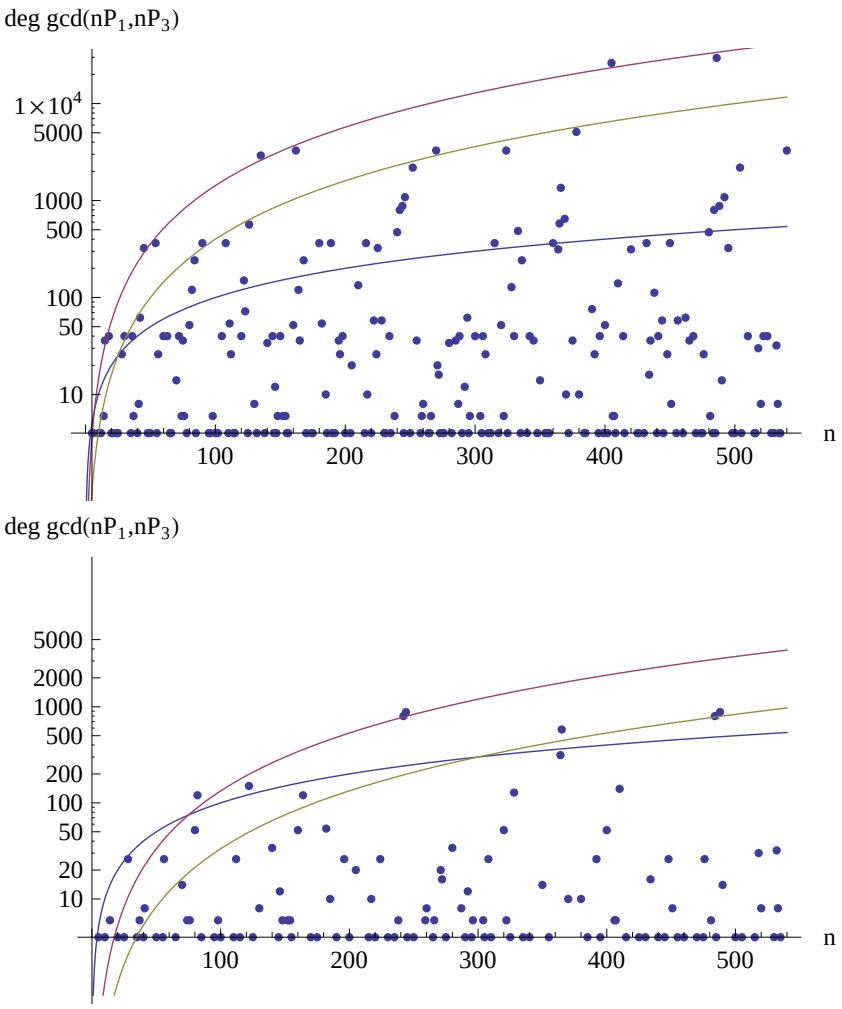


Figure 7: Graphs of the degree of the GCD of nP_1 and nP_3 over a function field with characteristic 3. The top picture shows all n, the bottom picture shows n that are not a multiple of 3. The lines are $\{x, x^2/7, x^2/25\}$ and $\{x, x^2/75, x^2/300\}$ respectively.

Recall that Silverman conjectured for two points on a single curve, and proved for some cases, that even if we don't allow p to divide n (i.e. even if we look at the picures on the bottom), that there is a c such that there are infinitely many n with the property that $\deg \mathrm{GCD}(nP, nQ) \geq cn$. Looking at the pictures on the bottom, it seems very probable that this is still the case for some pairs of non-isomorphic curves, when we take two points on two different curves: the lowest blue line (the function x) seems to grow slower than the degrees.

We also wondered whether or not there are infinitely many n with the property that $\deg \mathrm{GCD}(nP, nQ) \geq cn^2$ for some c. When we allow p to divide n (i.e. look at the pictures on the top), the stronger bound seems very probable. There even seems to be some structure in most of the graphs: take for example E_1 and E_2, then we see that there are 3 points, each time with increasing distance, on or near the red line in the top graph. Moreover, closer inspection gives that these points are at

$$n = 3^k, \quad k = 1, 2, 3, 4.$$

In the same way, there is a point just above and shortly after that a point just beneath the yellow line, each time with increasing distance. These points lie at

$$n = 2 \cdot 3^k$$

and

$$n = 4 \cdot 3^k.$$

Note that analogous things can be said about the graph of E_1 and E_3, where we allow p to divide n.

If we do not allow p to divide n, i.e. look at the pictures on the bottom, the constant c, the constant such that there are infinitely many n with a degree above cn^2, will be lower then in the other case, but it still seems probable that there is such a cn^2 bound. In both examples, this degree seems to be rather high at the points

$$n = 3^k \pm 1,$$

and also at similar n, and the degree seems to grow quadratically for those n. Further calculations indeed show that for $n = 728$,

$$\deg \mathrm{GCD}(728P_1, 728P_2) = 21596 > 21199 = 728^2/25$$

and

$$\deg \mathrm{GCD}(728P_1, 728P_3) = 7106 > 7066 = 728^2/75.$$

Hence also for $k = 6$, the points at $n = 3^k - 1$ lie above our quadratic line.

We will now see a pair of curves where the results seem to be drastically different.

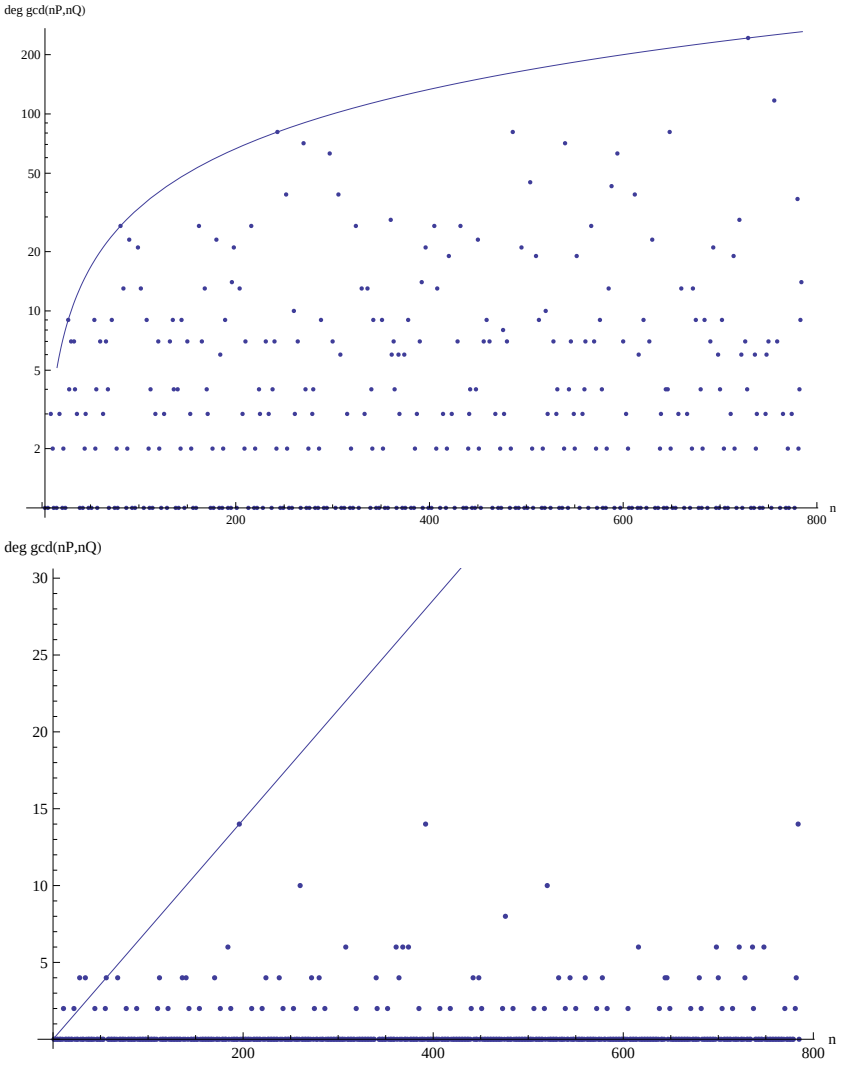


Figure 8: Graphs of the degree of the GCD of nP and nQ over a function field with characteristic 3, where $P = (1, T+1)$ on $E : y^2 = x^3 + (t+1)x^2 + (t^2+t+2)$ and $Q = (1, T+2)$ on $E' : y^2 = x^3 + (2t+1)x^2 + (t^2+2t+2)$. The top picture shows all n, the bottom picture shows n that are not a multiple of 3. The line is $x/3$ and $x/14$ respectively.

In figure 8, we again see the graphs for two independent points on two non-isomorphic curves,

$$\begin{aligned} P = (1, T+1) \quad &\text{on} \quad E : y^2 = x^3 + (t+1)x^2 + (t^2+t+2) \\ Q = (1, T+2) \quad &\text{on} \quad E' : y^2 = x^3 + (2t+1)x^2 + (t^2+2t+2). \end{aligned}$$

Here, there seems to be a linear upper bound

$$\deg \mathrm{GCD}(nP, nQ) \leq n/3$$

for all n. Closer inspection at the high points in the upper graph show that

$$\deg \mathrm{GCD}(3^k P, 3^k Q) = 3^{k-1}$$

for all k up to 6, and thus lie on this upper bound.
Moreover, if we instead look at n so that p does not divide n, i.e. look at the lower graph, $\deg \mathrm{GCD}(nP, nQ)$ does not even seem to grow linearly, i.e. I don't think that there is a constant c such that for infinitely many n,

$$\deg \mathrm{GCD}(nP, nQ) \geq cn.$$

One might even think that there is a constant upper bound, maybe as low as 14, but our experiments do not give any strong evidence for such a bound. Moreover, 14 as a lower bound is easily disproved: we have (see appendix A, table 7) that

$$\deg \mathrm{GCD}(196P, 196Q) = 14$$

and

$$\deg \mathrm{GCD}(184P, 184Q) = 6,$$

but strong divisibility gives us that

$$\mathrm{GCD}(196P, 184P) = B_{4P}$$

and

$$\mathrm{GCD}(196Q, 184Q) = B_{4Q},$$

where

$$\mathrm{GCD}(4P, 4Q) = 0.$$

Hence irreducible parts of $\mathrm{GCD}(184P, 184Q)$ do not divide $\mathrm{GCD}(196P, 196Q)$, and writing $9016 = \mathrm{lcm}(196, 184)$, we have that

$$\deg \mathrm{GCD}(9016P, 9016Q) \geq 20.$$

6.5 Two Points on E_4 in Characteristic 5

Above, we saw two points on a curve in characteristic 3 that seemed to satisfy the strong bound that there are infinitely many n with $p \nmid n$ and

$$\deg \mathrm{GCD}(nP, nQ) \geq cn^2$$

for some constant c.
Here, we give an experiment on a curve in characteristic 5, where such a strong bound is not probable. We use

$$E_4 : y^2 = x^3 - T^2x + T^2$$

with $P = (1, 1)$ and $Q = (T, T)$, see figure 9.
From the graphs, it seems probable that there only is a weaker bound that there are infinitely many n with $p \nmid n$ and

$$\deg \mathrm{GCD}(nP, nQ) \geq cn$$

for some constant c.

Remark 6.5.1. In section 5.3, we've shown that

$$\deg \mathrm{GCD}(p^iP, p^iQ) \geq p^i \cdot \deg \mathrm{GCD}(P, Q)$$

for all i. As we can see in this experiment, a priori this does not need to mean that $\deg \mathrm{GCD}(nP, nQ)$ grows at least linearly for $n = p^i$: this experiment is an example of the case that

$$\deg \mathrm{GCD}(P, Q) = 0.$$

Moreover,

$$\deg \mathrm{GCD}(5P, 5Q) = \deg \mathrm{GCD}(5^2P, 5^2Q) = 0.$$

However, we do have that

$$\deg \mathrm{GCD}(5^3P, 5^3Q) = 6,$$

and therefore that

$$\deg \mathrm{GCD}(5^kP, 5^kQ) \geq 5^{k-3} \cdot 6$$

for all $k \geq 3$. This means that $\frac{6}{125}n$ is a proven lower bound such that there are infinitely many n with the property that

$$\deg \mathrm{GCD}(nP, nQ) \geq cn,$$

where we do allow $p = 5$ to divide n.

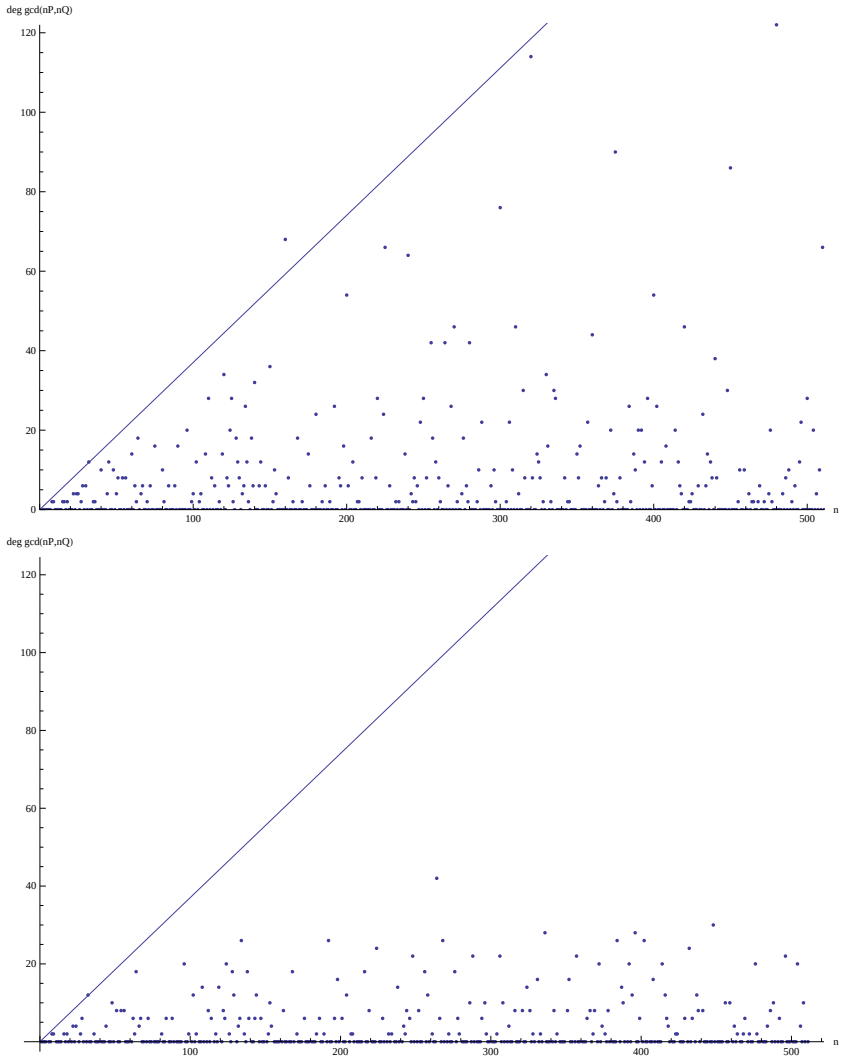


Figure 9: Graphs of the degree of the GCD of nP and nQ on E_4 over a function field with characteristic 5. The top picture shows all n, the bottom picture shows n that are not a multiple of 5. The line is $x/2.7$.

6.6 High Points at $n = p^k$ and $n = p^k \pm 1$

In figures 3, 6 and 7, we saw the degree of the GCD of nP and nQ grow quadratically in n for $n = p^k$. Moreover, in the same figures, we also saw the degree grow quadratically for $n = p^k \pm 1$. As we see neither occur in figures 8 and 9, there seems to be a correlation between these two occurrences, i.e., between quadratic growth in points at $n = p^k$ and quadratic growth in points at $n = p^k \pm 1$.

Let's first have a closer look at what happens for $n = p^k$. In section 5.3, we've already shown that

$$\deg \mathrm{GCD}(nP, nQ) \geq n \cdot \mathrm{GCD}(P, Q)$$

for $n = p^k$. Moreover, we've shown this using the Frobenius morphism and its dual, and the estimate was based on the fact that

$$\deg \mathrm{GCD}(\sigma_P^* \circ F^{i^*} \circ \hat{F}^{i^*}(\bar{O}), \sigma_Q^* \circ F^{i^*} \circ \hat{F}^{i^*}(\bar{O})) \geq \deg \mathrm{GCD}(\sigma_P^* \circ F^{i^*}(\bar{O}'), \sigma_Q^* \circ F^{i^*}(\bar{O}')).$$

For some classes of curves, it can be expected that there is a stronger, quadratic bound, based on how $\hat{F}$ can be related to F.

When we look at the points at $n = p^k \pm 1$, one might be tempted to think that this apparent correlation between quadratic growth at $n = p^k$ and quadratic growth at $n = p^k \pm 1$ is somehow caused by them sharing roots. Nothing is less true: since we are dealing with strong divisibility sequences, we have that

$$\gcd(B_{p^k P}, B_{p^k \pm 1 P}) = B_{\gcd(p^k, p^k \pm 1)P} = B_P,$$

and thus that

$$\gcd\Big(\gcd(B_{p^k P}, B_{p^k Q}), \gcd(B_{(p^k \pm 1)P}, B_{(p^k \pm 1)Q})\Big) = \gcd(B_P, B_Q).$$

However, we do believe that there is some relation between quadratic growth at $n = p^k$ and quadratic growth at $n = p^k \pm 1$. The search for this relation and the class of curves for which points at $n = p^k \pm 1$ grow quadratically is an interesting subject for a follow-up study.

7 A Complete Theory

In section 4 and 5, we saw proofs by Silverman concerning the behavior of the degree of the greatest common divisor of multiples of points, deg GCD(nP, nQ), as n increases. In section 6 we did experiments to get a better grip on unsolved cases. In this section, we will use these experiments and the proofs to conjecture a complete theory about the behavior of deg GCD(nP, nQ) as n increases.

7.1 Characteristic 0

Independent Points and Torsion Points

In the characteristic 0 case, Silverman already conjectured[2] the following.

Conjecture 7.1.1. Let K be a characteristic 0 function field, let $P_1 \in E_1/K$ and $P_2 \in E_2/K$ be K-independent points.

1. There is a constant $c = c(K, E_1, E_2, P_1, P_2)$ so that

$$\deg \text{GCD}(n_1P_1, n_2P_2) \leq c \text{ for all } n_1, n_2 \geq 1.$$

2. Further, there is an equality

$$\text{GCD}(nP_1, nP_2) = \text{GCD}(P_1, P_2) \text{ for infinitely many } n \geq 1$$

Our experiments support this conjecture, see section 6.1. Furthermore, it is true for curves with constant j-invariant.
The conjecture is also valid if either P_1 or P_2 is a torsion point. This is done in the following proposition.

Proposition 7.1.2. *Let K be a characteristic 0 function field, let $P_1 \in E_1/K$ and $P_2 \in E_2/K$ where at least one of them is a torsion point.*

1. *There is a constant $c = c(K, E_1, E_2, P_1, P_2)$ so that*

$$\deg \text{GCD}(n_1P_1, n_2P_2) \leq c \text{ for all } n_1, n_2 \geq 1.$$

2. *Further there is an equality*

$$\text{GCD}(nP_1, nP_2) = \text{GCD}(P_1, P_2) \text{ for infinitely many } n \geq 1$$

Proof. Let $K = k(C)$ be a characteristic 0 function field, let $P_1 \in E_1/K$ and $P_2 \in E_2/K$ and assume for simplicity that P_1 is torsion. Then $nP_1 = O$ for some $n \in \mathbb{N}_{\geq 1}$, and hence

$$\deg \text{GCD}(n_1P_1, n_2P_2) \leq \max\left(\deg(\sigma^*_{P_1}(\bar{O})), \deg(\sigma^*_{2P_1}(\bar{O})), \ldots, \deg(\sigma^*_{nP_1}(\bar{O}))\right) = c$$

[2] See [19], conjecture 7, pp. 437.

for some constant $c = c(K, E_1, P_1)$.

For the second statement, assume that P_1 is torsion and that $n_1 P_1 = O$. Then the set[3]

$$\{\pi \in \mathrm{Div}(C) | \pi \text{ divides } \mathrm{GCD}(nP_1, nP_2) \text{ for some } n\}$$

is finite, since it contains at most all the roots of the denominators of x-coordinates of the finite number of points $P_1, 2P_1, \ldots, n_1 P_1$ (more precisely, it contains at most all divisors dividing all $\sigma^*_{nP_2}(\bar{O})$, $1 \leq n \leq n_1$).
Take any such π and take n_π the smallest integer such that that

$$\pi | \mathrm{GCD}(n_\pi P_1, n_\pi P_2).$$

Since we have strong divisibility, we have that

$$\pi \not| \mathrm{GCD}(n' P_1, n' P_2)$$

for all n' coprime to n_π. This means that for all n that are coprime to all $n_\pi \neq 1$, we have that

$$\mathrm{GCD}(nP_1, nP_2) = \mathrm{GCD}(P_1, P_2).$$

Since there are infinitely many such n, this completes the proof.

□

Dependent Nontorsion Points

The only case we did not yet look at in characteristic 0, is the case of dependent nontorsion points. For K-dependent nontorsion points P_1 and P_2, we expect something completely different from the above. For instance, we can choose $P_1 = P_2$, and we would have that deg $\mathrm{GCD}(nP_1, nP_2)$ has a lower and an upper bound that is quadratic in n. We conjecture that this is generally true for dependent nontorsion points.

Conjecture 7.1.3. Let K be a characteristic 0 function field, let $P_1 \in E_1/K$ and $P_2 \in E_2/K$ be K-dependent nontorsion points.

1. There is a constant $c_1 = c_1(K, E_1, E_2, P_1, P_2)$ so that

$$\deg \mathrm{GCD}(nP_1, nP_2) \leq c_1 n^2 \text{ for all } n \geq 1.$$

2. Further, there is a constant $c_2 = c_2(K, E_1, E_2, P_1, P_2)$ so that

$$\deg \mathrm{GCD}(nP_1, nP_2) \geq c_2 n^2 \text{ for all } n \geq 1.$$

[3]By "π divides $\mathrm{GCD}(nP_1, nP_2)$" we mean that the divisor $\mathrm{GCD}(nP_1, nP_2) - \pi$ is positive.

7.2 Characteristic p

Nontorsion Points

In characteristic p, Silverman conjectured[4] the following.

Conjecture 7.2.1. Let $\mathbb{F}_q$ be a finite field of characteristic p, let $E/\mathbb{F}_q(T)$ be an elliptic curve, and let $P, Q \in E(\mathbb{F}_q(T))$ be nontorsion points. Then there is a constant $c = c(q, E, P, Q)$ so that

$$\deg \mathrm{GCD}(nP, nQ) \geq cn \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

We can support this conjecture with our experiments, and it is proven in the case of a constant j-invariant.
Also, Silverman stated that it is tempting to conjecture a lower bound of the form cn^2, but that there was really no evidence for or against the stronger bound. In the experiments, we saw that there both seem to be curves that satisfy this stronger bound and curves that do not satisfy the stronger bound. That leads us to the following conjecture.

Conjecture 7.2.2. Let $\mathbb{F}_q$ be a finite field of characteristic p, then there exists:

1. an elliptic curve $E/\mathbb{F}_q(T)$ and nontorsion points $P, Q \in E(\mathbb{F}_q(T))$ such that there is a constant $c = c(q, E, P, Q)$ so that

$$\deg \mathrm{GCD}(nP, nQ) \geq cn^2 \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n,$$

2. an elliptic curve $E/\mathbb{F}_q(T)$ and nontorsion points $P, Q \in E(\mathbb{F}_q(T))$ such that there is a constant $c = c(q, E, P, Q)$ so that

$$\deg \mathrm{GCD}(nP, nQ) \leq cn \text{ for all } n \geq 1,$$

Two Non-Isomorphic Elliptic Curves

In the above, we took P and Q from the same elliptic curve. If we allow that they come from different elliptic curves, there seems to be even a greater variety of possibilities.

Conjecture 7.2.3. Let $\mathbb{F}_p$ be a finite field of characteristic p, then

1. there exist two non-isomorphic elliptic curves $E_1/\mathbb{F}_q(T)$ and $E_2/\mathbb{F}_q(T)$ with independent non-torsion points $P \in E_1(\mathbb{F}_q(T))$ and $Q \in E_2(\mathbb{F}_q(T))$ such that there is a constant $c = c(q, E_1, E_2, P, Q) \geq 0$ so that

$$\deg \mathrm{GCD}(nP, nQ) \geq cn^2 \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

[4] See [19], conjecture 9, pp. 442

2. there exist two non-isomorphic elliptic curves $E_1/\mathbb{F}_q(T)$ and $E_2/\mathbb{F}_q(T)$ with non-torsion points $P \in E_1(\mathbb{F}_q(T))$ and $Q \in E_2(\mathbb{F}_q(T))$ such that there is a constant $c_1 = c_1(q, E_1, E_2, P, Q) \geq 0$ so that

$$\deg \mathrm{GCD}(nP, nQ) \leq c_1 n \text{ for all } n \geq 1$$

while at the same time, there is a constant $c_2 = c_2(q, E_1, E_2, P, Q) \geq 0$ such that

$$\deg \mathrm{GCD}(nP, nQ) \geq c_2 n \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

3. there exist two non-isomorphic elliptic curves $E_1/\mathbb{F}_q(T)$ and $E_2/\mathbb{F}_q(T)$ with non-torsion points $P \in E_1(\mathbb{F}_q(T))$ and $Q \in E_2(\mathbb{F}_q(T))$ such that for all $c \in \mathbb{R}_{>0}$, there are only finitely many n so that

$$\deg \mathrm{GCD}(nP, nQ) \geq cn.$$

Torsion Points

In characteristic p, the proof of above proposition 7.1.2 is still valid. Therefore, we have the same proposition for torsion points in characteristic p as we had in characteristic 0.

Proposition 7.2.4. *Let K be a characteristic p function field and let $P_1 \in E_1/K$ and $P_2 \in E_2/K$ be such that one of them be a torsion point.*

1. *There is a constant $c = c(K, E_1, E_2, P_1, P_2)$ so that*

$$\deg \mathrm{GCD}(n_1 P_1, n_2 P_2) \leq c \text{ for all } n_1, n_2 \geq 1.$$

2. *Further, there is an equality*

$$\mathrm{GCD}(nP_1, nP_2) = \mathrm{GCD}(P_1, P_2) \text{ for infinitely many } n \geq 1$$

Proof. The proof is identical to the proof of proposition 7.1.2. □

Lower Bound

For the lower bound, we conjecture the following.

Conjecture 7.2.5. Let E_1 and E_2 be two elliptic curves over a function field, and let $P \in E_1$ and $Q \in E_2$ be independent points. Then

$$\mathrm{GCD}(nP, nQ) = \mathrm{GCD}(P, Q) \text{ for infinitely many } n \geq 1$$

Moreover, this is also true if at least one of them is a torsion point instead.

The final thing we need now is a lower bound for dependent non-torsion points.

Conjecture 7.2.6. Let E_1 and E_2 be two elliptic curves over a function field, and let $P \in E_1$ and $Q \in E_2$ be dependent nontorsion points. Then there is a constant c such that

$$\deg \mathrm{GCD}(nP, nQ) \geq cn^2 \text{ for all } n \geq 1.$$

7.3 Flow Charts

The main conjectures are summarized into two flowcharts: one for the upper and one for the lower bounds.

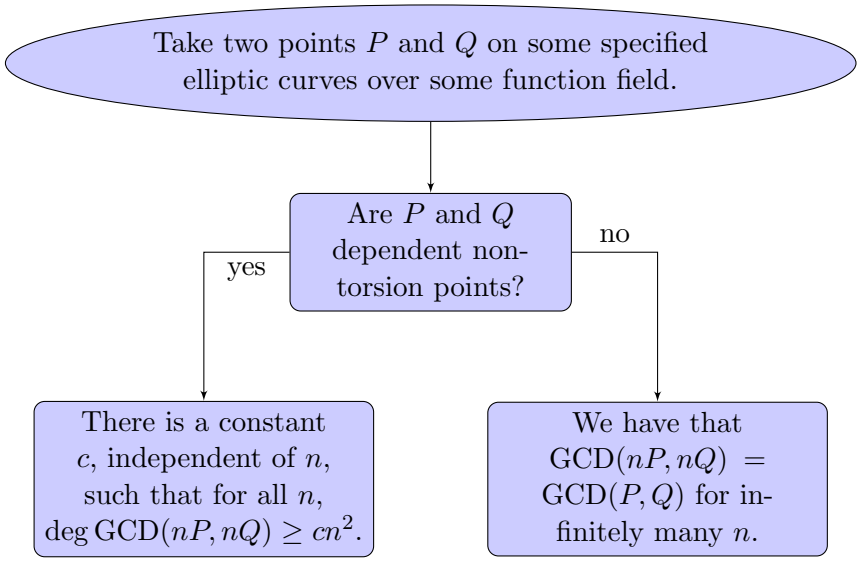


Figure 10: Conjecture of the flow chart for the lower bound on $\deg \mathrm{GCD}(nP, nQ)$ over a function field.

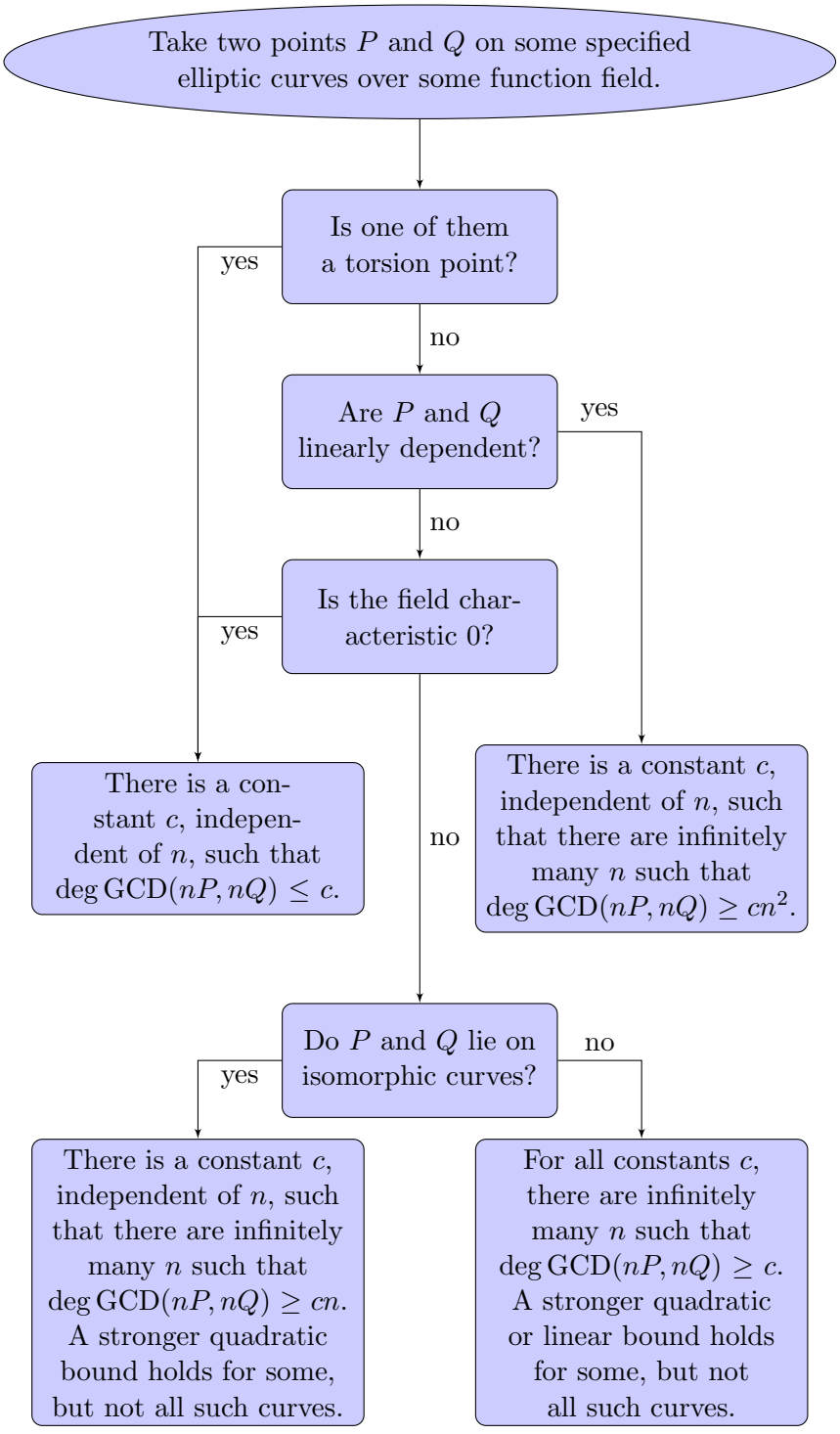


Figure 11: Conjecture of the flow chart for the upper bound on $\deg \mathrm{GCD}(nP, nQ)$ over a function field.

Conclusions

For two points on elliptic curves P_1, P_2, we looked at

$$\deg \text{GCD}(nP_1, nP_2)$$

for increasing n.

We sketched a complete theory of how $\deg \text{GCD}(nP_1, nP_2)$ is bounded as n increases, and this theory is proposed in conjectures.
In characteristic 0, our experiments confirm Silverman's conjecture that there is a constant c, independent of n_i, such that

$$\deg \text{GCD}(n_1P_1, n_2P_2) \leq c \text{ for all } n_1, n_2 \geq 1.$$

Also, they confirm that for infinitely many n such that

$$\deg \text{GCD}(nP_1, nP_2) = \deg \text{GCD}(P_1, P_2).$$

Furthermore, we've seen a proof of both statements for curves with constant j-invariant.

In characteristic p, taking P_1 and P_2 from a single elliptic curve, our experiments confirm Silverman's conjecture that there is a constant c such that

$$\deg \text{GCD}(nP_1, nP_2) \geq cn \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

Again, we've seen a proof of this for curves with constant j-invariant.
Also, it is probable that there exists curves that satisfy as well as curves that do not satisfy the stronger bound

$$\deg \text{GCD}(nP_1, nP_2) \geq cn^2 \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

Allowing P_1 and P_2 to lie on different curves, it even seems probable that there exists curves with points P_1, P_2, such that *there is no constant* c with the property that

$$\deg \text{GCD}(nP_1, nP_2) \geq cn \text{ for infinitely many } n \geq 1 \text{ with } p \nmid n.$$

References

[1] Atiyah, Michael F. and MacDonald, Ian G. *Introduction to Commutative Algrabra*. 1969. Addison-Wesley Publishing company, Reading.

[2] Cornelissen, Gunther and Zahidi, Karim. "Elliptic divisibility sequences and undecidable problems about rational points". In: J. reine angew, Math. 613 (2007), pp 1-33.

[3] Goonatilake, Susantha. *Toward a Global Science: Mining Civilizational Knowledge*. 1998, Indana University Press, Bloomington.

[4] Goren, Eyal Z. "Integral Dependence and Normal Varieties". Downloadable from http://www.math.mcgill.ca/goren/AG/normality4.pdf (last visited 31-5-2011). November 1999.

[5] Griffiths, Philip and Harris, Joseph. *Principles of Algebraic Geometry*. 1978. John Wiley & Sons, New York.

[6] Hartshorne, Robin. *Algebraic Geometry* (Graduate Texts in Mathematics; v. 52). 1977. Springer Science + Business Media, New York.

[7] Hindry, Marc and Silverman, Joseph H. *Diophantine Geometry: An Introduction* (Graduate Texts in Mathematics; v. 201). 2000. Springer-Verlag, New York.

[8] Ireland, Kenneth and Rosen, Michael. *A Classical Introduction to Modern Number Theory* (Graduate Texts in Mathematics; v. 84). 1990, Springer-Verlag, New York.

[9] Ingram, Patrick, Mahé, Valéry, Silverman, Joseph H., Stange, Katherine E. and Streng, Marco. "Algebraic divisibility sequences over function fields". 2011. arXiv:1105.5633v1 [math.NT].

[10] Lang, Serge. *Algebra* (Graduate Texts in Mathematics; v. 211). Corrected printing 2005. Springer Science + Business Media LLC, New York.

[11] Lang, Serge. "Integral points on curves". In: publications mathématiques de l'I.H.É.S., tome 6 (1960), pp. 27-43.

[12] Lehmer, Derrick H. "The Mathematical Work of Morga Ward". In: Mathematics of Computation, vol 61, no. 203, Special issue Dedicated to Derrick Henry Lehmer (July 1993), pp. 307-311.

[13] Looij, Rutger de. *Elliptic divisibility sequences*. Masters thesis supervised by prof. dr. Gunther Cornelissen, Universiteit of Utrecht, May 28, 2010.

[14] Poonen, Bjorn. "Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers". In: Algorithmic

Number Rheory, volume 2369 of Lecture Notes in Comput. Sci. (Sydney, 2002), pp. 3342.

[15] Rosen, Michael. *Number Theory in Function Fields* (Graduate Texts in Mathematics; v. 210). 2002, Springer-Verlag, New York.

[16] Schoof, René. "Counting points on elliptic curves over finite fields". In:journal de Théorie des Nombres de Bordeaux 7 (1995), 219-254.

[17] Shipsey, Rachel. *Elliptic Divisibility Sequences*. Ph. D. thesis, Goldsmiths College, University of londen, 2000.

[18] Sigler, L.E. *Fibonaccis Liber Abaci : A Translation into Modern English of Leonardo Pisanos Book of Calculation*. 2002, Springer, New York.

[19] Silverman, Joseph H. "Common divisors of elliptic divisibility sequences over function fields". In: manuscripta math. 114, 431-446 (2004). Publisched online 16 Juli 2004, Springer-Verlag.

[20] Silverman, Joseph H. *Advanced topics in the Arithmetic of Elliptic Curves* (Graduate Texts in Mathematics; v. 151). Corrected second printing, 1999 (first printing 1994). Springer-Verlag, New York.

[21] Silverman, Joseph H. *The Arithmetic of Elliptic Curves* (Graduate Texts in Mathematics; v. 106). Second edition, 2009 (first edition 1986). Springer, New York.

[22] Swart, Christine S. *Elliptic curves and related sequences*. Ph. D. thesis, University of Londen, 2003.

[23] Voloch, José Felipe. "Explicit p-descent for elliptic curves in characteristic p". In: Compositio Mathematica, tome 74, no 3 (1990), pp 247-258.

[24] Voloch, José Felipe. "Siegel's theorem for complex function fields". In: Proceedings of the amercian mathematical society, volume 121, number 4 (August 1994), pp 1307-1308.

[25] Ward, Morgan. "Memoir on Elliptic Divisibility Sequences". In: American Journal of Mathematics, vol 70, No. 1 (Jan. 1948), pp. 31-74.

Index

Appendix A: Experiments

n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg
1	0	51	4	101	0	151	0	201	4	251	0	301	0	351	3280
2	0	52	116	102	4	152	4	202	0	252	12028	302	0	352	4
3	4	53	0	103	0	153	40	203	0	253	0	303	4	353	0
4	4	54	364	104	116	154	0	204	40	254	0	304	4	354	4
5	0	55	0	105	4	155	0	205	72	255	4	305	60	355	0
6	4	56	148	106	0	156	1048	206	0	256	4	306	40	356	4
7	0	57	4	107	0	157	0	207	40	257	0	307	0	357	4
8	4	58	0	108	3280	158	0	208	116	258	4	308	148	358	0
9	40	59	0	109	0	159	4	209	0	259	0	309	4	359	0
10	16	60	184	110	16	160	1012	210	148	260	132	310	16	360	4252
11	0	61	60	111	4	161	0	211	0	261	40	311	0	361	0
12	40	62	0	112	148	162	3280	212	4	262	0	312	1048	362	0
13	4	63	40	113	0	163	0	213	4	263	0	313	0	363	5764
14	0	64	4	114	4	164	1124	214	0	264	40	314	0	364	5284
15	4	65	4	115	0	165	4	215	0	265	0	315	40	365	5592
16	4	66	4	116	4	166	0	216	3280	266	0	316	4	366	6484
17	0	67	0	117	364	167	0	217	0	267	4	317	0	367	0
18	40	68	4	118	0	168	1336	218	0	268	4	318	4	368	4
19	0	69	4	119	0	169	4	219	220	269	0	319	0	369	5872
20	20	70	16	120	472	170	16	220	20	270	12028	320	1012	370	16
21	4	71	0	121	640	171	40	221	4	271	0	321	4	371	0
22	0	72	364	122	720	172	4	222	4	272	4	322	0	372	40
23	0	73	24	123	652	173	0	223	0	273	328	323	0	373	0
24	40	74	0	124	4	174	4	224	148	274	0	324	29524	374	0
25	0	75	4	125	0	175	0	225	40	275	0	325	4	375	4
26	112	76	4	126	40	176	4	226	0	276	40	326	0	376	4
27	364	77	0	127	0	177	4	227	0	277	0	327	4	377	4
28	148	78	1012	128	4	178	0	228	40	278	0	328	1124	378	364
29	0	79	0	129	4	179	0	229	0	279	40	329	0	379	0
30	148	80	1012	130	128	180	1660	230	16	280	196	330	148	380	20
31	0	81	3280	131	0	181	0	231	4	281	0	331	0	381	4
32	4	82	1120	132	40	182	336	232	4	282	4	332	4	382	0
33	4	83	0	133	0	183	544	233	0	283	0	333	40	383	0
34	0	84	1336	134	0	184	4	234	9112	284	4	334	0	384	40
35	0	85	0	135	364	185	0	235	0	285	4	335	0	385	0
36	364	86	0	136	4	186	4	236	4	286	112	336	1336	386	64
37	0	87	4	137	0	187	0	237	4	287	72	337	0	387	40
38	0	88	4	138	4	188	4	238	0	288	364	338	112	388	4
39	40	89	0	139	0	189	364	239	0	289	0	339	4	389	0
40	52	90	1336	140	164	190	16	240	9112	290	16	340	20	390	1156
41	72	91	36	141	4	191	0	241	0	291	4	341	0		
42	4	92	4	142	0	192	40	242	9760	292	100	342	40		
43	0	93	4	143	4	193	16	243	29524	293	0	343	0		
44	4	94	0	144	364	194	0	244	10084	294	4	344	4		
45	40	95	0	145	0	195	40	245	0	295	0	345	4		
46	0	96	40	146	96	196	148	246	10084	296	4	346	0		
47	0	97	0	147	4	197	0	247	4	297	364	347	0		
48	40	98	0	148	4	198	40	248	4	298	0	348	40		
49	0	99	40	149	0	199	0	249	4	299	4	349	0		
50	16	100	20	150	148	200	52	250	16	300	184	350	16		

Table 3: $\deg \gcd(B_{nP}, B_{nQ})$ for all n up to 390 for $P = (1, T+2)$ and $Q = (\frac{T^2+T+1}{(T+1)^2}, \frac{2T^4+2T+1}{(T+1)^3})$ on $E : y^2 = x^3 + T^2X + T$ in characteristic 3.

n	deg	n	deg	n	deg	n	deg	n	deg	n	deg
1	0	35	204	69	793	103	1768	137	3128	171	4873
2	0	36	175	70	816	104	1802	138	3169	172	4930
3	1	37	228	71	840	105	1837	139	3220	173	4988
4	2	38	240	72	823	106	1872	140	3266	174	5041
5	4	39	253	73	888	107	1908	141	3313	175	5104
6	1	40	266	74	912	108	1579	142	3360	176	5162
7	8	41	280	75	937	109	1980	143	3408	177	5221
8	10	42	289	76	962	110	2016	144	3415	178	5280
9	13	43	308	77	988	111	2053	145	3504	179	5340
10	16	44	322	78	1009	112	2090	146	3552	180	5359
11	20	45	337	79	1040	113	2128	147	3601	181	5460
12	19	46	352	80	1066	114	2161	148	3650	182	5520
13	28	47	368	81	1093	115	2204	149	3700	183	5581
14	32	48	379	82	1120	116	2242	150	3745	184	5642
15	37	49	400	83	1148	117	2281	151	3800	185	5704
16	42	50	416	84	1171	118	2320	152	3850	186	5761
17	48	51	433	85	1204	119	2360	153	3901	187	5828
18	13	52	450	86	1232	120	2395	154	3952	188	5890
19	60	53	468	87	1261	121	2440	155	4004	189	5953
20	66	54	121	88	1290	122	2480	156	4051	190	6016
21	73	55	504	89	1320	123	2521	157	4108	191	6080
22	80	56	522	90	1309	124	2562	158	4160	192	6139
23	88	57	541	91	1380	125	2604	159	4213	193	6208
24	91	58	560	92	1410	126	2605	160	4266	194	6272
25	104	59	580	93	1441	127	2688	161	4320	195	6337
26	112	60	595	94	1472	128	2730	162	1093	196	6402
27	121	61	620	95	1504	129	2773	163	4428	197	6468
28	130	62	640	96	1531	130	2816	164	4482	198	6493
29	140	63	661	97	1568	131	2860	165	4537	199	6600
30	145	64	682	98	1600	132	2899	166	4592	200	6666
31	160	65	704	99	1633	133	2948	167	4648	201	6733
32	170	66	721	100	1666	134	2992	168	4699		
33	181	67	748	101	1700	135	3037	169	4760		
34	192	68	770	102	1729	136	3082	170	4816		

Table 4: $\deg \gcd(B_{nP}, B_{nQ})$ for all n up to 201 for the dependent points $P = (T, 1)$ on $E_1 : y^2 = x^3 - T^2x + 1$ and $Q = (T, T)$ on $E_4 : y^2 = x^3 - T^2x + T^2$ in characteristic 3.

n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg
1	0	69	4	137	0	205	32	273	220	341	0	409	0	477	40
2	0	70	16	138	4	206	0	274	0	342	40	410	380	478	0
3	4	71	0	139	0	207	40	275	0	343	0	411	4	479	0
4	2	72	202	140	52	208	38	276	22	344	2	412	2	480	2110
5	0	73	0	141	4	209	0	277	0	345	4	413	0	481	0
6	4	74	0	142	0	210	152	278	0	346	0	414	40	482	0
7	0	75	4	143	0	211	0	279	40	347	0	415	0	483	4
8	2	76	2	144	202	212	2	280	68	348	22	416	38	484	2322
9	40	77	0	145	0	213	4	281	0	349	0	417	4	485	0
10	4	78	328	146	24	214	0	282	4	350	16	418	0	486	29524
11	0	79	0	147	4	215	0	283	0	351	364	419	0	487	0
12	22	80	234	148	2	216	1822	284	2	352	2	420	476	488	2522
13	0	81	3280	149	0	217	0	285	4	353	0	421	0	489	4
14	12	82	248	150	40	218	0	286	36	354	4	422	0	490	16
15	4	83	0	151	0	219	4	287	32	355	0	423	40	491	0
16	2	84	404	152	2	220	10	288	202	356	2	424	2	492	2254
17	0	85	0	153	40	221	0	289	0	357	4	425	0	493	0
18	40	86	0	154	12	222	4	290	4	358	0	426	4	494	36
19	0	87	4	155	0	223	0	291	4	359	0	427	20	495	40
20	10	88	2	156	346	224	44	292	26	360	2146	428	2	496	2
21	4	89	0	157	0	225	40	293	0	361	0	429	4	497	0
22	0	90	364	158	0	226	0	294	116	362	0	430	4	498	4
23	0	91	24	159	4	227	0	295	0	363	2164	431	0	499	0
24	22	92	2	160	234	228	22	296	2	364	2660	432	1822	500	10
25	0	93	4	161	0	229	0	297	364	365	3012	433	0	501	4
26	36	94	0	162	3280	230	4	298	0	366	3244	434	12	502	0
27	364	95	0	163	0	231	4	299	0	367	0	435	4	503	0
28	44	96	22	164	250	232	2	300	94	368	2	436	2	504	3644
29	0	97	0	165	4	233	0	301	0	369	2632	437	0	505	0
30	40	98	12	166	0	234	2956	302	0	370	4	438	220	506	0
31	0	99	40	167	0	235	0	303	4	371	0	439	0	507	4
32	2	100	10	168	404	236	2	304	2	372	22	440	26	508	2
33	4	101	0	169	0	237	4	305	20	373	0	441	40	509	0
34	0	102	4	170	4	238	12	306	40	374	0	442	36	510	40
35	0	103	0	171	40	239	0	307	0	375	4	443	0	511	0
36	202	104	38	172	2	240	2110	308	44	376	2	444	22	512	2
37	0	105	4	173	0	241	0	309	4	377	0	445	0	513	364
38	0	106	0	174	4	242	2320	310	4	378	9476	446	0	514	0
39	4	107	0	175	0	243	29524	311	0	379	0	447	4	515	0
40	26	108	1822	176	2	244	2522	312	346	380	10	448	44	516	22
41	32	109	0	177	4	245	0	313	0	381	4	449	0	517	0
42	116	110	4	178	0	246	2236	314	0	382	0	450	364	518	60
43	0	111	4	179	0	247	0	315	40	383	0	451	32	519	4
44	2	112	44	180	850	248	2	316	2	384	22	452	2	520	66
45	40	113	0	181	0	249	4	317	0	385	0	453	4	521	0
46	0	114	4	182	348	250	4	318	4	386	32	454	0	522	40
47	0	115	0	183	184	251	0	319	0	387	40	455	32	523	0
48	22	116	2	184	2	252	3644	320	234	388	2	456	22	524	2
49	0	117	40	185	0	253	0	321	4	389	0	457	0	525	4
50	4	118	0	186	4	254	0	322	12	390	400	458	0	526	0
51	4	119	0	187	0	255	4	323	0	391	0	459	364	527	0
52	38	120	238	188	2	256	2	324	16402	392	44	460	10	528	22
53	0	121	240	189	364	257	0	325	0	393	4	461	0	529	0
54	364	122	360	190	4	258	4	326	0	394	0	462	116	530	4
55	0	123	292	191	0	259	0	327	4	395	0	463	0	531	40
56	44	124	2	192	22	260	50	328	306	396	202	464	2	532	86
57	4	125	0	193	16	261	40	329	0	397	0	465	4	533	32
58	0	126	1052	194	0	262	0	330	40	398	0	466	0	534	4
59	0	127	0	195	4	263	0	331	0	399	58	467	0	535	0
60	94	128	2	196	44	264	22	332	2	400	234	468	3118	536	2
61	20	129	4	197	0	265	0	333	40	401	0	469	0	537	4
62	0	130	44	198	40	266	18	334	0	402	4	470	4	538	0
63	40	131	0	199	0	267	4	335	0	403	0	471	4	539	0
64	2	132	22	200	26	268	2	336	404	404	2	472	2	540	7654
65	0	133	6	201	4	269	0	337	0	405	3280	473	0	541	0
66	4	134	0	202	0	270	3280	338	36	406	12	474	4	542	0
67	0	135	364	203	0	271	0	339	4	407	0	475	0	543	4
68	2	136	2	204	22	272	2	340	10	408	22	476	44	544	2

Table 5: $\deg \gcd(B_{nP}, B_{nQ})$ for all n up to 544 for $P = (T, 1)$ on $E_1 : y^2 = x^3 - T^2x + 1$ and $Q = (1 - T^2, 1 - T^2)$ on $E_2 : y^2 = x^3 - T^2(T^2 - 1)x$ in characteristic 3.

n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg
1	0	69	0	137	0	205	20	273	4	341	0	409	0	477	0
2	0	70	14	138	4	206	0	274	0	342	40	410	140	478	0
3	0	71	0	139	0	207	0	275	4	343	0	411	0	479	0
4	0	72	40	140	34	208	0	276	4	344	0	412	0	480	472
5	4	73	0	141	0	209	0	277	0	345	36	413	0	481	6
6	4	74	6	142	0	210	134	278	0	346	0	414	40	482	0
7	0	75	36	143	0	211	0	279	0	347	0	415	4	483	4
8	0	76	6	144	40	212	0	280	34	348	4	416	0	484	800
9	0	77	0	145	4	213	0	281	0	349	0	417	0	485	4
10	4	78	4	146	12	214	0	282	4	350	14	418	0	486	29524
11	0	79	0	147	4	215	4	283	0	351	0	419	0	487	0
12	4	80	52	148	6	216	364	284	0	352	0	420	314	488	880
13	0	81	0	149	0	217	10	285	36	353	0	421	0	489	0
14	6	82	120	150	40	218	0	286	0	354	4	422	0	490	14
15	36	83	0	151	0	219	0	287	8	355	4	423	0	491	0
16	0	84	242	152	6	220	4	288	40	356	0	424	0	492	1084
17	0	85	4	153	0	221	0	289	0	357	4	425	4	493	0
18	40	86	0	154	6	222	58	290	4	358	0	426	4	494	0
19	0	87	0	155	4	223	0	291	0	359	0	427	0	495	324
20	4	88	0	156	4	224	26	292	12	360	364	428	0	496	0
21	4	89	0	157	0	225	324	293	0	361	0	429	0	497	0
22	0	90	364	158	0	226	0	294	62	362	0	430	4	498	4
23	0	91	0	159	0	227	0	295	4	363	0	431	0	499	0
24	4	92	0	160	52	228	58	296	6	364	314	432	364	500	4
25	4	93	0	161	0	229	0	297	0	365	580	433	0	501	0
26	0	94	0	162	3280	230	4	298	0	366	1354	434	16	502	0
27	0	95	4	163	0	231	4	299	0	367	0	435	36	503	0
28	26	96	4	164	120	232	0	300	40	368	0	436	0	504	2186
29	0	97	0	165	36	233	0	301	0	369	648	437	0	505	4
30	40	98	6	166	0	234	40	302	0	370	10	438	112	506	0
31	0	99	0	167	0	235	4	303	0	371	0	439	0	507	0
32	0	100	4	168	242	236	0	304	6	372	4	440	4	508	0
33	0	101	0	169	0	237	0	305	4	373	0	441	40	509	0
34	0	102	4	170	4	238	6	306	40	374	0	442	0	510	40
35	4	103	0	171	0	239	0	307	0	375	36	443	0	511	0
36	40	104	0	172	0	240	472	308	26	376	0	444	58	512	0
37	6	105	40	173	0	241	0	309	0	377	0	445	4	513	0
38	0	106	0	174	4	242	800	310	4	378	5102	446	0	514	0
39	0	107	0	175	4	243	0	311	0	379	0	447	0	515	4
40	4	108	364	176	0	244	880	312	4	380	10	448	26	516	4
41	8	109	0	177	0	245	4	313	0	381	0	449	0	517	0
42	62	110	4	178	0	246	1084	314	0	382	0	450	364	518	30
43	0	111	54	179	0	247	0	315	364	383	0	451	8	519	0
44	0	112	26	180	364	248	0	316	0	384	4	452	0	520	8
45	324	113	0	181	0	249	0	317	0	385	4	453	0	521	0
46	0	114	4	182	54	250	4	318	4	386	0	454	0	522	40
47	0	115	4	183	0	251	0	319	0	387	0	455	4	523	0
48	4	116	0	184	0	252	2186	320	52	388	0	456	58	524	0
49	0	117	0	185	10	253	0	321	0	389	0	457	0	525	40
50	4	118	0	186	4	254	0	322	6	390	76	458	0	526	0
51	0	119	0	187	0	255	36	323	0	391	0	459	0	527	0
52	0	120	40	188	0	256	0	324	3280	392	26	460	4	528	4
53	0	121	0	189	364	257	0	325	4	393	0	461	0	529	0
54	364	122	150	190	4	258	4	326	0	394	0	462	62	530	4
55	4	123	72	191	0	259	6	327	0	395	4	463	0	531	0
56	26	124	0	192	4	260	8	328	128	396	40	464	0	532	32
57	0	125	4	193	0	261	0	329	0	397	0	465	36	533	8
58	0	126	566	194	0	262	0	330	40	398	0	466	0	534	4
59	0	127	0	195	36	263	0	331	0	399	4	467	0	535	4
60	40	128	0	196	26	264	4	332	0	400	52	468	40	536	0
61	0	129	0	197	0	265	4	333	486	401	0	469	0	537	0
62	0	130	8	198	40	266	6	334	0	402	4	470	4	538	0
63	40	131	0	199	0	267	0	335	4	403	0	471	0	539	0
64	0	132	4	200	4	268	0	336	242	404	0	472	0	540	3280
65	4	133	0	201	0	269	0	337	0	405	26244	473	0		
66	4	134	0	202	0	270	3280	338	0	406	6	474	4		
67	0	135	2916	203	0	271	20	339	0	407	6	475	4		
68	0	136	0	204	4	272	16	340	4	408	4	476	26		

Table 6: $\deg \gcd(B_{nP}, B_{nQ})$ for all n up to 540 for $P = (T, 1)$ on $E_1 : y^2 = x^3 - T^2x + 1$ and $Q = (0, T)$ on $E_3 : y^2 = x^3 - (T^2 - 1)x + T^2$ in characteristic 3.

n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg
1	0	80	0	159	1	238	4	317	0	396	21	475	0	554	0	633	1	712	0
2	0	81	27	160	0	239	0	318	1	397	0	476	8	555	1	634	0	713	0
3	1	82	0	161	0	240	7	319	2	398	0	477	3	556	0	635	0	714	19
4	0	83	0	162	27	241	0	320	0	399	1	478	0	557	0	636	1	715	2
5	0	84	13	163	0	242	2	321	1	400	0	479	0	558	3	637	0	716	0
6	1	85	0	164	0	243	81	322	0	401	0	480	7	559	0	638	2	717	1
7	0	86	0	165	7	244	0	323	0	402	1	481	0	560	4	639	3	718	0
8	0	87	1	166	0	245	0	324	27	403	0	482	0	561	7	640	0	719	0
9	3	88	2	167	0	246	1	325	0	404	0	483	1	562	0	641	0	720	29
10	0	89	0	168	13	247	0	326	0	405	27	484	2	563	0	642	1	721	0
11	2	90	23	169	0	248	0	327	1	406	0	485	0	564	1	643	0	722	6
12	1	91	0	170	4	249	1	328	0	407	2	486	81	565	0	644	4	723	1
13	0	92	0	171	3	250	0	329	0	408	13	487	0	566	0	645	1	724	0
14	0	93	1	172	0	251	0	330	13	409	0	488	0	567	27	646	4	725	0
15	1	94	0	173	0	252	39	331	0	410	0	489	1	568	0	647	0	726	7
16	0	95	0	174	1	253	2	332	0	411	1	490	0	569	0	648	81	727	0
17	0	96	1	175	0	254	0	333	3	412	0	491	0	570	7	649	2	728	4
18	3	97	0	176	2	255	1	334	0	413	0	492	1	571	0	650	0	729	243
19	0	98	0	177	1	256	0	335	0	414	3	493	0	572	2	651	1	730	0
20	0	99	21	178	0	257	0	336	13	415	0	494	0	573	1	652	0	731	0
21	1	100	0	179	0	258	1	337	0	416	0	495	21	574	0	653	0	732	1
22	2	101	0	180	23	259	0	338	0	417	1	496	0	575	0	654	1	733	0
23	0	102	13	181	0	260	10	339	1	418	2	497	0	576	9	655	0	734	0
24	1	103	0	182	0	261	3	340	4	419	0	498	1	577	0	656	0	735	1
25	0	104	0	183	1	262	0	341	2	420	19	499	0	578	4	657	3	736	6
26	0	105	1	184	6	263	0	342	9	421	0	500	0	579	1	658	0	737	2
27	9	106	0	185	0	264	7	343	0	422	0	501	1	580	0	659	0	738	3
28	4	107	0	186	1	265	0	344	0	423	3	502	0	581	0	660	13	739	0
29	0	108	9	187	2	266	0	345	1	424	0	503	0	582	1	661	0	740	0
30	7	109	0	188	0	267	1	346	0	425	0	504	45	583	2	662	0	741	1
31	0	110	2	189	9	268	0	347	0	426	1	505	0	584	0	663	1	742	0
32	0	111	1	190	0	269	0	348	1	427	0	506	2	585	13	664	0	743	0
33	7	112	4	191	0	270	71	349	0	428	0	507	1	586	0	665	0	744	1
34	4	113	0	192	1	271	0	350	0	429	7	508	0	587	0	666	3	745	0
35	0	114	1	193	0	272	4	351	9	430	0	509	0	588	43	667	0	746	0
36	3	115	0	194	0	273	1	352	2	431	0	510	19	589	0	668	0	747	3
37	0	116	0	195	1	274	0	353	0	432	27	511	0	590	0	669	1	748	6
38	0	117	3	196	14	275	2	354	1	433	0	512	0	591	1	670	0	749	0
39	1	118	0	197	0	276	1	355	0	434	0	513	9	592	0	671	2	750	7
40	0	119	0	198	21	277	0	356	0	435	1	514	0	593	0	672	13	751	0
41	0	120	7	199	0	278	0	357	1	436	0	515	0	594	63	673	0	752	0
42	1	121	2	200	0	279	3	358	0	437	0	516	1	595	0	674	0	753	1
43	0	122	0	201	1	280	4	359	0	438	1	517	2	596	0	675	9	754	0
44	2	123	1	202	0	281	0	360	29	439	0	518	0	597	1	676	0	755	0
45	3	124	0	203	0	282	1	361	6	440	2	519	1	598	0	677	0	756	117
46	0	125	0	204	13	283	0	362	0	441	3	520	10	599	0	678	1	757	0
47	0	126	3	205	0	284	0	363	7	442	4	521	0	600	7	679	0	758	0
48	1	127	0	206	0	285	1	364	4	443	0	522	3	601	0	680	4	759	7
49	0	128	0	207	3	286	2	365	0	444	1	523	0	602	0	681	1	760	0
50	0	129	1	208	0	287	0	366	1	445	0	524	0	603	3	682	2	761	0
51	1	130	0	209	2	288	9	367	0	446	0	525	1	604	0	683	0	762	1
52	0	131	0	210	7	289	0	368	6	447	1	526	0	605	2	684	9	763	0
53	0	132	7	211	0	290	0	369	3	448	4	527	0	606	1	685	0	764	0
54	9	133	0	212	0	291	1	370	0	449	0	528	7	607	0	686	0	765	3
55	2	134	0	213	1	292	0	371	0	450	23	529	0	608	0	687	1	766	0
56	4	135	9	214	0	293	0	372	1	451	2	530	0	609	1	688	0	767	0
57	1	136	4	215	0	294	1	373	0	452	0	531	3	610	0	689	0	768	1
58	0	137	0	216	27	295	0	374	6	453	1	532	4	611	0	690	7	769	0
59	0	138	1	217	0	296	0	375	1	454	0	533	0	612	39	691	0	770	2
60	7	139	0	218	0	297	63	376	0	455	0	534	1	613	0	692	0	771	1
61	0	140	4	219	1	298	0	377	0	456	7	535	0	614	0	693	21	772	0
62	0	141	1	220	2	299	0	378	9	457	0	536	0	615	1	694	0	773	0
63	3	142	0	221	0	300	7	379	0	458	0	537	1	616	6	695	0	774	3
64	0	143	2	222	1	301	0	380	0	459	9	538	0	617	0	696	1	775	0
65	0	144	9	223	0	302	0	381	1	460	0	539	2	618	1	697	0	776	0
66	7	145	0	224	4	303	1	382	0	461	0	540	71	619	0	698	6	777	1
67	0	146	0	225	3	304	0	383	0	462	7	541	0	620	0	699	1	778	0
68	4	147	1	226	0	305	0	384	1	463	0	542	0	621	9	700	4	779	0
69	1	148	0	227	0	306	39	385	2	464	0	543	1	622	0	701	0	780	37
70	0	149	0	228	1	307	0	386	0	465	1	544	4	623	0	702	9	781	2
71	0	150	7	229	0	308	6	387	3	466	0	545	0	624	1	703	0	782	4
72	9	151	0	230	0	309	1	388	0	467	0	546	7	625	0	704	2	783	9
73	0	152	0	231	7	310	0	389	0	468	3	547	0	626	0	705	1	784	14
74	0	153	3	232	0	311	0	390	7	469	0	548	0	627	7	706	0	785	0
75	1	154	2	233	0	312	1	391	0	470	0	549	3	628	0	707	0		
76	0	155	0	234	3	313	0	392	14	471	1	550	2	629	0	708	1		
77	2	156	1	235	0	314	0	393	1	472	0	551	0	630	23	709	0		
78	1	157	0	236	0	315	3	394	0	473	2	552	19	631	0	710	0		
79	0	158	0	237	1	316	0	395	0	474	1	553	0	632	0	711	3		

Table 7: $\deg \gcd(B_{nP}, B_{nQ})$ for all n up to 785 for $P = (1, T+1)$ on $E : y^2 = x^3 + (T+1)x^2 + (T^2+T+2)$ and $Q = (1, T+2)$ on $E' : y^2 = x^3 + (2T+1)x^2 + (T^2+2T+2)$ in characteristic 3.

n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg	n	deg
1	0	66	4	131	0	196	6	261	2	326	8	391	0	456	10
2	0	67	6	132	4	197	0	262	0	327	0	392	20	457	0
3	0	68	0	133	6	198	16	263	0	328	2	393	0	458	0
4	0	69	0	134	26	199	0	264	42	329	0	394	12	459	10
5	0	70	2	135	12	200	54	265	0	330	34	395	0	460	0
6	0	71	0	136	2	201	6	266	6	331	16	396	28	461	0
7	0	72	6	137	0	202	0	267	0	332	0	397	0	462	4
8	2	73	0	138	18	203	0	268	26	333	2	398	0	463	0
9	2	74	0	139	6	204	12	269	0	334	0	399	6	464	2
10	0	75	16	140	32	205	0	270	46	335	30	400	54	465	2
11	0	76	0	141	0	206	0	271	0	336	28	401	0	466	0
12	0	77	0	142	0	207	2	272	2	337	0	402	26	467	0
13	0	78	0	143	6	208	2	273	0	338	0	403	0	468	2
14	0	79	0	144	12	209	0	274	0	339	0	404	0	469	6
15	2	80	10	145	0	210	8	275	4	340	0	405	12	470	0
16	2	81	2	146	0	211	0	276	18	341	0	406	0	471	0
17	0	82	0	147	6	212	0	277	0	342	8	407	0	472	2
18	2	83	0	148	0	213	0	278	6	343	0	408	16	473	0
19	0	84	6	149	0	214	0	279	2	344	2	409	0	474	0
20	0	85	0	150	36	215	0	280	42	345	2	410	0	475	4
21	0	86	0	151	0	216	18	281	0	346	0	411	0	476	20
22	4	87	0	152	2	217	0	282	0	347	0	412	0	477	2
23	0	88	6	153	10	218	0	283	0	348	0	413	0	478	0
24	4	89	0	154	4	219	8	284	0	349	0	414	20	479	0
25	4	90	16	155	0	220	28	285	2	350	14	415	0	480	122
26	0	91	0	156	0	221	0	286	10	351	8	416	12	481	0
27	2	92	0	157	0	222	0	287	0	352	16	417	6	482	0
28	6	93	0	158	0	223	0	288	22	353	0	418	4	483	0
29	0	94	0	159	0	224	24	289	0	354	0	419	0	484	4
30	6	95	0	160	68	225	66	290	0	355	0	420	46	485	0
31	0	96	20	161	0	226	0	291	0	356	0	421	0	486	8
32	12	97	0	162	8	227	0	292	0	357	22	422	0	487	0
33	0	98	0	163	0	228	6	293	0	358	0	423	2	488	10
34	0	99	2	164	0	229	0	294	6	359	0	424	2	489	0
35	2	100	4	165	2	230	0	295	0	360	44	425	4	490	2
36	2	101	0	166	0	231	0	296	10	361	0	426	0	491	0
37	0	102	12	167	0	232	2	297	2	362	0	427	0	492	6
38	0	103	0	168	18	233	0	298	0	363	0	428	0	493	0
39	0	104	2	169	0	234	2	299	0	364	6	429	6	494	0
40	10	105	4	170	0	235	0	300	76	365	0	430	0	495	12
41	0	106	0	171	2	236	0	301	0	366	8	431	0	496	22
42	0	107	0	172	0	237	0	302	0	367	0	432	24	497	0
43	0	108	14	173	0	238	14	303	0	368	2	433	0	498	0
44	4	109	0	174	0	239	0	304	2	369	8	434	6	499	0
45	12	110	28	175	14	240	64	305	0	370	0	435	14	500	28
46	0	111	0	176	6	241	0	306	22	371	0	436	0	501	0
47	0	112	8	177	0	242	4	307	0	372	20	437	12	502	0
48	10	113	0	178	0	243	2	308	10	373	0	438	8	503	0
49	0	114	6	179	0	244	8	309	0	374	4	439	0	504	20
50	4	115	0	180	24	245	2	310	46	375	90	440	38	505	0
51	8	116	0	181	0	246	6	311	0	376	2	441	8	506	4
52	0	117	2	182	0	247	0	312	4	377	0	442	0	507	0
53	0	118	0	183	0	248	22	313	0	378	8	443	0	508	10
54	8	119	14	184	2	249	0	314	0	379	0	444	0	509	0
55	0	120	34	185	0	250	28	315	30	380	0	445	0	510	66
56	8	121	0	186	6	251	0	316	8	381	0	446	0	511	0
57	0	122	8	187	0	252	8	317	0	382	0	447	0		
58	0	123	6	188	0	253	0	318	0	383	0	448	30		
59	0	124	20	189	2	254	0	319	0	384	26	449	0		
60	14	125	28	190	0	255	42	320	114	385	2	450	86		
61	0	126	2	191	0	256	18	321	8	386	0	451	0		
62	6	127	0	192	26	257	0	322	0	387	14	452	0		
63	2	128	18	193	0	258	12	323	0	388	10	453	0		
64	18	129	12	194	0	259	0	324	14	389	0	454	0		
65	0	130	8	195	8	260	8	325	12	390	20	455	2		

Table 8: $\deg \gcd(B_{nP}, B_{nQ})$ for all n up to 511 for $P = (1, 1)$ and $Q = (T, T)$ on $E_4 : y^2 = x^3 - T^2x + T^2$ in characteristic 5.