# The Field of N-Torsion Points of an Elliptic Curve over a Finite Field

by

ADAM LEONARD VAN TUYL

A thesis submitted to the Department of
Mathematics and Statistics in conformity with the requirements
for the degree of Master of Science

Queen's University
Kingston, Ontario, Canada
September, 1997

# Abstract

Let $E$ be an elliptic curve over a finite field $K = \mathbb{F}_q$, and $n \neq \text{char}(K)$ a prime. Then the field of $n$-torsion points is constructed by adjoining the coordinates of all the $n$-torsion points to $K$. In this paper we present two algorithms to calculate the degree of the resulting extension. The first algorithm is based upon the characteristic polynomial of the Frobenius endomorphism; the second relies on the division polynomials of $E$. We also make a comparison between the two algorithms and describe some possible improvements. As well, we explore some possible applications for our algorithms.

# Acknowledgements

First and foremost, I would like to thank may advisor Dr. Ernst Kani for a multitude of things: for always being free with his time to answer my questions, for providing me with inspiration and new direction when I encountered mental blocks, and for insightful comments on this paper, to name just a few.

I would like to thank all my friends and professors here at the Mathematics Department at Queens's University for providing me with inspiration, motivation, and perspective throughout the year.

A special thanks to Queen's University for financial support during the past year.

And finally, though they have no idea what I do, even when I try to explain it, thanks to my friends and family.

# Contents

# List of Tables

# List of Figures

# Introduction

Let $E$ be an elliptic curve over a field $K$ given in the Weierstrass form

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

If $F$ is any field extension of $K$, then the set of $F$-rational points of $E$ is denoted by $E(F)$, i.e,

$$E(F) = \{(x, y) \in F^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ is the the point at infinity. A group structure can be imposed on the set $E(F)$ by defining an operation of addition on the points of $E$ via the chord and tangent method. The identity of this group is $\mathcal{O}$. A point $P \in E(F)$ is called a *n-torsion point* if

$$\underbrace{P + \cdots + P}_{n} = nP = \mathcal{O}.$$

We let $E[n]$ be the set of all $n$-torsion points in $E(\overline{K})$, where $\overline{K}$ is the algebraic closure of $K$. Suppose that for every $P = (x, y) \in E[n]$, we adjoin $P$'s coordinates to the base field $K$. The resulting extension, $K_{E,n}$, is called the *field of n-torsion points of E*. Since it can be shown that $E[n]$ is a finite group, (cf. Theorem 1.1), we can deduce that $K_{E,n}$ is a finite extension. Further, $F = K_{E,n}$ is the smallest extension such that $\mathrm{E}[n] \leq E(F)$.

Interest in the fields $K_{E,n}$ comes from the fact that these fields, or more precisely, the Galois representations described in Chapter 1, played an important role in proving one of the great open questions in number theory, namely, Fermat's Last Theorem. Roughly speaking, the basis of this proof (due to Frey/Ribet/Wiles [**Wi**]) is to show that certain Galois extensions $K$ of $\mathbb{Q}$ cannot be of the form $K = K_{E,n}$, thereby leading to the non-existence of a solution. In his proof, Wiles proves a weak version of Serre's Conjecture to get a precise overview of which Galois extensions $K/\mathbb{Q}$ can be of the form $K_{E,n}$ for an elliptic curve $E/\mathbb{Q}$.

In this paper we will study the analogous problem when $\mathbb{Q}$ is replaced by $K = \mathbb{F}_q$. In this case, $K_{E,n}$ is completely determined by its degree $d = [K_{E,n} : K]$, so the problem becomes one of finding what degrees $d$ are possible. To answer this question we need a method to compute $d$. In particular, we will consider the following problem when $\text{char}(K) \neq 2, 3$:

PROBLEM 1. *Given an elliptic curve $E$ over the field $K = \mathbb{F}_q$, and a prime $n \neq$ char$(K)$, determine an algorithm to compute the degree $d$ of the extension $K_{E,n}$ over $K$, i.e., $d = [K_{E,n} : K]$.*

In this report we present two algorithms that compute $d$. The first algorithm is based upon the Frobenius endomorphism, $\phi_q$, where $\phi_q$ is defined as

$$\begin{aligned} \phi_q : E &\longrightarrow E \\ (x, y) &\mapsto (x^q, y^q). \end{aligned}$$

If we restrict $\phi_q$ to $E[n]$, that is, $\phi_q|_{E[n]}$, it can be shown (Theorem 2.3) that $d = \text{ord}(\phi_q|_{E[n]})$ in the group $\text{Aut}(E[n])$, the group of automorphisms on $E[n]$. Moreover, we use the fact (Theorem 2.12) that $\phi_q|_{E[n]}$ satisfies the equation

$$T^2 - a_E T + q \equiv 0 \pmod{n}.$$

Here, $a_E = (q + 1) - \#E(\mathbb{F}_q)$. As we will show in Theorem 2.14, in most cases the degree $d$ can be found using basic linear algebra. Only in the case where the discriminant of the above equation is divisible by $n$ do we need to turn to more powerful machinery. We will see that in this situation we can find $d$ if we utilize the division polynomials of $E$.

The division polynomials of $E$ form the basis of the second algorithm for computing $d$. By factoring the $n^{th}$ division polynomial of $E$ in the ring $K[x]$, we show in Theorem 3.6 that we can determine $d$ up to a factor of 2. Then, taking the roots $x_i$ of the division polynomial and evaluating the norms of $(x_i^3 + ax_i + b)$, we can distinguish between the two possible values.

Our presentation will be as follows. The first three chapters present established results that form the mathematical basis of our algorithms. Chapter 1 focuses on the extension $K_{E,n}$. Chapter 2 is a discussion on the characteristic polynomial of the Frobenius endomorphism. Finally, Chapter 3 describes the division polynomials of $E$.

The final three chapters use the results of the previous chapters to describe our algorithms. In Chapter 4, we present our two algorithms for computing $d$ given $E$, $n$, and $q$ as input. In Chapter 5, we discuss the implementation of the two algorithms. Also contained in this chapter is a comparison of the two methods. Finally, in Chapter 6, we explore some possible uses for our algorithms. In particular, we discuss the connection between our algorithms and the modular curve $X(n)$. We also discuss the possibility of using the second algorithm to compute $\#E(\mathbb{F}_p)$.

We conclude with an appendix containing a table of our results. A description of how they were generated has also been included.

CHAPTER 1

# The Field of N-Torsion Points

In this chapter, let $K$ be a perfect field with $\mathrm{char}(K) \neq 2, 3$. Then the equation for an elliptic curve $E$ over this field is given by the Weierstrass form

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

Further, let $n$ be a prime such that $n \neq \mathrm{char}(K)$. The goal of this chapter is to present some results about $K_{E,n}$, the field of $n$-torsion points, that form the basis of our algorithms. More precisely, we show that $K_{E,n}$ is a Galois extension of $K$. As well, we show that there exists a 1-1 homomorphism from its Galois group into $GL_2(\mathbb{Z}/n\mathbb{Z})$, that is, there is a Galois representation. We begin with a more formal construction of $K_{E,n}$.

## 1. $E[n]$ and $K_{E,n}$

Integral to the construction of $K_{E,n}$ is $E[n]$, the set of all $n$-torsion points, i.e., the set of all points $P \in E(\overline{K})$ such that $nP = \mathcal{O}$. The following result about $E[n]$ plays an important role throughout this report.

THEOREM 1.1. *$E[n]$ is a finite subgroup of $E(\overline{K})$ of order $n^2$ and hence*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

PROOF. We refer the reader to [**Si**] III.6.2 and III.6.4 for the proof. □

Notice that for all $n$, $\mathcal{O} \in E[n]$. Using Theorem 1.1, we can write $E[n]$ as

$$E[n] = \{\mathcal{O}, (x_1, y_1), \ldots, (x_m, y_m)\},$$

where $m = n^2 - 1$. Taking the coordinates $\{x_i, y_i\}$ for every $1 \leq i \leq m$, and adjoining them to our base field $K$, we construct the field of $n$-torsion points $K_{E,n}$. Explicitly,

$$K_{E,n} = K(E[n]) = K(x_1, y_1, \ldots, x_m, y_m).$$

It is clear that the degree $d$ of the extension of $K_{E,n}$ is finite. Every $x \in \overline{K}$ is algebraic over $K$, that is, $[K(x) : K] < \infty$. By Theorem 1.1, $E[n]$ is finite. Hence, we are adjoining only a finite number of elements to $K$, each of finite degree, so $d = [K_{E,n} : K] < \infty$.

## 2. Galois Action on the Points of $E$

One of the goals of this chapter is to show that $K_{E,n}$ is a Galois extension of $K$. As the following proposition demonstrates, the elements of the Galois group can be extended to act upon the $K$-rational points $E$.

PROPOSITION 1.2. *Let $E$ be an elliptic curve defined by an equation with coefficients in $K$ and let $K'$ be a Galois extension of $K$.*
*i) For $P \in E(K')$ and $\sigma \in Gal(K'/K)$, define $\sigma_E(P)$ by*

$$\sigma_E(P) = \begin{cases} (\sigma(x), \sigma(y)) & \text{if } P = (x, y) \\ \mathcal{O} & \text{if } P = \mathcal{O} \end{cases}$$

*Then $\sigma_E(P) \in E(K')$.*
*ii) For all $P \in E(K')$ and all $\sigma, \tau \in \mathrm{Gal}(K'/K)$,*

$$(\sigma\tau)_E(P) = \sigma_E(\tau_E(P))$$

*iii) For all $P, Q \in E(K')$, and all $\sigma \in \mathrm{Gal}(K'/K)$,*

$$\begin{aligned} \sigma_E(P+Q) &= \sigma_E(P) + \sigma_E(Q) \\ \sigma_E(-P) &= -\sigma_E(P) \end{aligned}$$

PROOF. See [**SiTa**], pp 186-187. □

Observe that the proposition says that every $\sigma \in \mathrm{Gal}(K'/K)$ can be extended to act upon the points $P \in E(K')$. In fact, from Proposition 1.2*iii* we see that the induced map $\sigma_E$ is a homomorphism from $E(K')$ into itself, i.e., $\sigma_E \in \mathrm{End}(E(K'))$. Proposition 1.2*ii* allows us to claim that this is more than a mere endomorphism on $E(K')$. Each induced map has an inverse since $\sigma$ has an inverse, so $\sigma_E$ is actually an element of $\mathrm{Aut}(E(K'))$, the group of all invertible endomorphisms on $E(K')$. So, from Proposition 1.2, we can deduce the following:

COROLLARY 1.3. *The map*

$$\rho_{E/K,K'} : \mathrm{Gal}(K'/K) \longrightarrow \mathrm{Aut}(E(K'))$$

$$\sigma \mapsto \sigma_E$$

*is a group homomorphism.*

Since we have assumed that $K$ is a perfect field, we know that the field extension $\overline{K}$ is Galois over $K$. Let $\mathrm{Gal}(\overline{K}/K)$ be its Galois group, and let

$$\rho_{E/K} = \rho_{E/K,\overline{K}} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E(\overline{K}))$$

denote the associated map defined in Corollary 1.3. But now observe how $\rho_{E/K}(\sigma) = \sigma_E$ acts on the $n$-torsion points. If $P \in \mathrm{E}[n]$ , then $nP = \mathcal{O}$. So, $\sigma_E(nP) = \mathcal{O}$. But then, by Proposition 1.2, we have $n\sigma_E(P) = \mathcal{O}$. Thus, $\sigma_E(P) \in E[n]$. So, by restricting $\sigma_E$ to $E[n]$, we find that the induced map is an element of $\mathrm{Aut}(E[n])$, the group of invertible homomorphisms that take $E[n]$ to itself. So, in effect, we have the homomorphism

$$\rho_{E/K,n} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[n]).$$

$$\sigma \mapsto \sigma_E|_{E[n]}.$$

Recall from Theorem 1.1 that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Picking a basis for $\mathrm{E}[n]$ , we have $\mathrm{Aut}(E[n]) \cong GL_2(\mathbb{Z}/n\mathbb{Z})$, the set of all $2 \times 2$ matrices with coefficients in $\mathbb{Z}/n\mathbb{Z}$. To make this more explicit, suppose that $P_1$ and $P_2$ form a basis for $E[n]$. Then every $P \in E[n]$ can be expressed as

$$P = aP_1 + bP_2,$$

with $a, b \in \mathbb{Z}/n\mathbb{Z}$. If $\sigma \in \mathrm{Aut}(E[n])$, then by definition we will have

$$\sigma(P) = a\sigma(P_1) + b\sigma(P_2).$$

So, to determine $\sigma$, we only need to determine where $\sigma$ takes $P_1$ and $P_2$. That is,

$$\begin{aligned} \sigma(P_1) &= a_1P_1 + a_2P_2 \\ \sigma(P_2) &= b_1P_1 + b_2P_2. \end{aligned}$$

We can now define the following map:

$$\pi = \pi_{P_1,P_2} : \mathrm{Aut}(E[n]) \longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z})$$

$$\sigma \mapsto M_\sigma$$

where $M_\sigma = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$. If $\sigma, \tau \in \mathrm{Aut}(E[n])$, then, as in basic linear algebra, we have $M_{\sigma\tau} = M_\sigma M_\tau$. From this we can show that $\pi$ is in fact a group isomorphism. The next theorem shows that we can use this discussion to show that there exists a homomorphism from $\mathrm{Gal}(\overline{K}/K)$ to $GL_2(\mathbb{Z}/n\mathbb{Z})$. In other words, we have a *Galois representation modulo n* called the *Galois representation of E/K modulo n.*

COROLLARY 1.4. *Let $E$ be an elliptic curve over $K$, and $n \geq 2$ be an prime. Fix generators $P_1$ and $P_2$ for $E[n]$ . Then the map*

$$\rho_n : \mathrm{Gal}(\overline{K}/K) \longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z})$$

$$\rho_n = \pi_{P_1,P_2} \circ \rho_{E/K,n}$$

*is a homomorphism of groups.*

Throughout the remainder of this paper, we shall usually denote $\rho_{E/K,n}$ by $\rho_n$ since the two maps are equivalent, up to a choice of basis for $E[n]$.

## 3. The Galois Extension $K_{E,n}$

The following result shows that $K_{E,n}$, the field of $n$-torsion points, is Galois. As will be seen, it is a consequence of the fact that $\mathrm{Ker}(\rho_n) = \mathrm{Gal}(\overline{K}/K_{E,n})$.

PROPOSITION 1.5. *Let $\rho_n$ be the homomorphism described in Corollary 1.4. Then*

$$\mathrm{Ker}(\rho_n) = \mathrm{Gal}(\overline{K}/K_{E,n}).$$

*In particular, $K_{E,n}$ is a Galois extension of $K$.*

PROOF. Let $\sigma \in \mathrm{Ker}(\rho_n)$. Furthermore, let $\sigma_E = \rho_{E/K,n}(\sigma)$. Since $\rho_n(\sigma) = I_2 \in GL_2(\mathbb{Z}/n\mathbb{Z})$, we have that $\sigma_E = id \in \mathrm{End}(E[n])$. So, for every $P \in E[n]$, $\sigma_E(P) = P$. Thus, if $P \neq \mathcal{O}$, we have $(\sigma(x), \sigma(y)) = (x, y)$. Recall that the coordinates of the $n$-torsion points generate $K_{E,n}$ over $K$. So $\sigma$ leaves $K_{E,n}$ fixed since it acts trivially on each of the generators of $K_{E,n}$. But then $\sigma \in \mathrm{Gal}(\overline{K}/K_{E,n})$.

Conversely, if $\sigma \in \mathrm{Gal}(\overline{K}/K_{E,n})$, then $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Let $\sigma_E = \rho_{E/K,n}(\sigma)$. Then, if $P \neq \mathcal{O} \in E[n]$,

$$\sigma_E(P) = (\sigma(x), \sigma(y)).$$

But because $x, y \in K_{E,n}$, $\sigma(x) = x$ and $\sigma(y) = y$. Then $\sigma_E(P) = P$ for all $P \in E[n]$. In particular, if $P_1$ and $P_2$ are a basis for $E[n]$, then $\sigma_E(P_1) = P_1$, and $\sigma_E(P_2) = P_2$. This implies that $\rho_{E/K,n}(\sigma) = id \in \mathrm{End}(E[n])$. Since $\pi$ is an isomorphism, we have $\rho_n(\sigma) = \pi_{P_1,P_2} \circ \rho_{E/K,n}(\sigma) = I_2$, the identity matrix of $GL_2(\mathbb{Z}/n\mathbb{Z})$, thereby implying that $\sigma \in \mathrm{Ker}(\rho_n)$. This completes the first part of the proof.

Now, $H = \mathrm{Ker}(\rho_n)$ is normal in $G = \mathrm{Gal}(\overline{K}/K)$. But by the above, $H = \mathrm{Gal}(\overline{K}/K_{E,n})$, so by Galois theory, $K_{E,n}/K$ is Galois. □

Using this theorem, we can now introduce the Galois representation of the group $\mathrm{Gal}(K_{E,n}/K)$. For example, see [**SiTa**] p. 196.

COROLLARY 1.6. *Let $E$ be an elliptic curve over $K$ and $n \geq 2$ be an prime $\neq$ char$(K)$. Fix generators $P_1$ and $P_2$ for $E[n]$. Then $\rho_n$ induces an injective homomorphism*

$$\overline{\rho}_n : \mathrm{Gal}(K_{E,n}/K) \hookrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}).$$

*In particular, $\overline{\rho}_n(\sigma|_{K_{E,n}}) = \rho_n(\sigma)$ for $\sigma \in \mathrm{Gal}(\overline{K}/K)$.*

PROOF. From Corollary 1.4, $\rho_n$ induces an injective map

$$\overline{\rho}_n : \frac{\mathrm{Gal}(\overline{K}/K)}{\mathrm{Ker}(\rho_n)} \hookrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}).$$

But by Proposition 1.5 and Galois theory, we deduce that

$$\frac{\mathrm{Gal}(\overline{K}/K)}{\mathrm{Ker}(\rho_n)} \cong \mathrm{Gal}(K_{E,n}/K).$$

The result now follows. □

COROLLARY 1.7.

$$d = [K_{E,n} : K] = |\,\mathrm{Im}(\overline{\rho}_n)|.$$

PROOF. By Galois theory, we have $[K_{E,n} : K] = |\,\mathrm{Gal}(K_{E,n}/K)|$. But the result now follows from the fact that $\overline{\rho}_n$ is injective by Corollary 1.6. □

**Remark:** Before we proceed, we detour briefly to discuss the context out of which this problem arose. As mentioned in the introduction, the origin of this problem is based in part on Wiles' proof [**Wi**] of Fermat's Last Theorem (FLT).

Continuing from the earlier work and ideas of Frey and Ribet, Wiles considered the elliptic curve

$$E : y^2 = x(x - a^n)(x + b^n),$$

where $a^n + b^n = c^n$ is a counterexample to FLT. Then, by examining its field of $n$-torsion points $K_{E,n}$ when $K = \mathbb{Q}$, or more specifically, the associated Galois representation, he derived a contradiction. The proof relied on being able to give a (partial) characterization of those Galois representations modulo $n$ which arise from elliptic curves. This is essentially equivalent to the question as to which field extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \leq GL_2(\mathbb{Z}/n\mathbb{Z})$ are of the form $K = K_{E,n}$.

In this paper, we have chosen to work in a setting that is much more simple than the one used by Wiles. We restrict ourselves to $K = \mathbb{F}_q$, in which case $\mathrm{Gal}(K_{E,n}/K)$ is cyclic (cf. Theorem 1.12). In this context, determining which field extension $K'/K$ with $\mathrm{Gal}(K'/K)$ are of the form $K' = K_{E,n}$ is equivalent to asking what degrees $[K_{E,n} : K]$ are possible. This is because $K_{E,n}$ is uniquely determined up to isomorphism by $d$, since there is only one finite field (up to isomorphism) of given degree over $K$.

## 4. The Weil $e_n$-pairing and Computing $[K_{E,n} : K]$

In this section we describe how the *Weil $e_n$-pairing* provides a partial answer to our question of computing $d$. The Weil $e_n$-pairing is a skew-symmetric, bilinear pairing

$$e_n : E[n] \times E[n] \longrightarrow \mu_n(\overline{K}) = \text{the group of } n^{th} \text{ roots of unity of } \overline{K}.$$

Recall that as before $\mathrm{char}(K) \neq n$, so $\mu_n(\overline{K}) \cong \mathbb{Z}/n\mathbb{Z}$. The actual definition of this pairing is quite involved, so we point the reader to [**Si**] III.8 for a thorough treatment of this topic. We cite the following proposition which describes some of the properties of this pairing.

PROPOSITION 1.8. *The Weil $e_n$-pairing has the following properties:*

a)

$$e_n(P_1 + P_2, Q) = e_n(P_1, Q)e_n(P_2, Q)$$

$$e_n(P, Q_1 + Q_2) = e_n(P, Q_1)e_n(P, Q_2).$$

b)

$$e_n(Q,P) = e_n(P,Q)^{-1}.$$

c) *If* $\mathrm{ord}(P) = n$, *then* $e_n(P,Q) = 1$ *if and only if* $Q = kP$ *for some* $k \in \mathbb{Z}$.

d) *For all* $\sigma \in Gal(\overline{K}/K)$,

$$e_n(P,Q)^\sigma = e_n(\sigma(P), \sigma(Q)).$$

e) *The pairing* $e_n$ *is non-degenerate. In particular, if* $P \in E[n]$ *has order* $n$ *and* $\zeta_n$ *is a primitive* $n^{th}$ *root of unity, then there exists* $Q \in E[n]$, *such that* $e_n(P,Q) = \zeta_n$, *and* $P, Q$ *form a basis of* $E[n]$.

PROOF. See [**Si**] III.8.1 and III.8.1.1. □

The following corollary tells us that all $n^{th}$ roots of unity lie in $K_{E,n}$.

COROLLARY 1.9. *Let* $E$ *be an elliptic curve over* $K$. *Let* $n \neq char(K)$ *and let* $\zeta_n$ *denote a primitive* $n^{th}$ *root of unity. Then* $\zeta_n \in K_{E,n}$.

PROOF. This follows from Proposition 1.8. Let $P, Q \in E(K_{E,n})$ be a basis of $E[n]$. Then $e_n(P,Q) = \zeta_n$ is a primitive $n^{th}$ root of unity since $e_n$ is non-degenerate. Now for every $\sigma \in G = Gal(\overline{K}/K_{E,n})$, $\sigma(P) = P, \sigma(Q) = Q$. Hence, by Proposition 1.8d:

$$\zeta_n^\sigma = e_n(\sigma(P), \sigma(Q)) = e_n(P,Q) = \zeta_n.$$

So, $\zeta_n$ is fixed by all the elements of $G$, which implies that $\zeta_n \in K_{E,n}$. □

COROLLARY 1.10. *If* $K = \mathbb{F}_q$ *and* $d = [K_{E,n} : K]$, *then* $q^d \equiv 1 \pmod{n}$. *In particular,* $\mathrm{ord}(q,n) | d$.

PROOF. By the previous corollary, we have $\zeta_n \in K_{E,n} = \mathbb{F}_{q^d}$. Then $n = \mathrm{ord}(\zeta_n) \mid |\mathbb{F}_{q^d}^*| = q^d - 1$. So $n | q^d - 1$, giving the desired result. □

In the next proposition we show that if we have a point $P$ of order $n$ of $E(\overline{K})$, then we can use the $e_n$-pairing to give us a partial criterion for finding $d$.

PROPOSITION 1.11. *Let* $P = (x,y) \in E(\overline{K})$ *be a point of order* $n$, *where* $n$ *is a prime distinct from char(K). Then,* $K(P, \zeta_n) = K_{E,n}$ *or*

$$[K_{E,n} : K(P, \zeta_n)] = n.$$

PROOF. By Corollary 1.10, we have $K(\zeta_n) \subset K_{E,n}$. Since $P \in E(\overline{K})$ is a point of order $n$, and thus a $n$-torsion point, we deduce that $K(P, \zeta_n) \subset K_{E,n}$. Then it is enough to show:

**Claim:** If $\sigma \in G = \mathrm{Gal}(\overline{K}/K(P, \zeta_n))$, then $\sigma^n \in H = Gal(\overline{K}/K_{E,n})$.

Indeed, since $H$ is normal in $G$ (Proposition 1.5), this claim shows that $G/H$ is a $n$-group. But since $G/H \leq \mathrm{Gal}(K_{E,n}/K) \leq GL_2(\mathbb{Z}/n\mathbb{Z})$ whose $n$-Sylow subgroup has order $n$, we see that $[G : H] = 1$ or $[G : H] = n$.

It thus remains to verify the claim. Using Proposition 1.8e, we pick a point $Q \in E(\overline{K})$ such that $e_n(P, Q) = \zeta_n$. Moreover $P$ and $Q$ will form a basis for $E[n]$, thereby implying that $K(P, Q, \zeta_n) = K_{E,n}$.

Now, let $\sigma \in G$. Then

$$\begin{aligned} e_n(P, \sigma(Q)) &= e_n(\sigma(P), \sigma(Q)) \quad \text{since } P \text{ is invariant under } \sigma \in G \\ &= e_n(P, Q)^\sigma \quad \text{by Prop. 1.8d} \\ &= \zeta_n^\sigma = \zeta_n = e_n(P, Q). \end{aligned}$$

So, we conclude that $e_n(P, \sigma(Q)) = e_n(P, Q)$, or equivalently, $e_n(P, \sigma(Q) - Q) = 1$. But then by Proposition 1.8c, $\sigma(Q) - Q = kP$, so $\sigma(Q) = Q + kP$, with $k = k_\sigma \in \mathbb{Z}/n\mathbb{Z}$. But from this we deduce that

$$\sigma^n(Q) = Q + nkP = Q.$$

Thus $\sigma^n$ is fixes both $P$ and $Q$, and hence $K_{E,n}$, or, in other words, $\sigma^n \in H$. This concludes the proof of the claim. □

If we now specialize to the case that $K = \mathbb{F}_q$, then it is a well know result that $[K(\zeta_n) : K] = \mathrm{ord}(q, n)$ (e.g. [**LiHa**] 2.47). If we know that $[K(P) : K] = r$, then we can calculate $d^* = [K(P, \zeta_n) : K] = \mathrm{lcm}(\mathrm{ord}(q, n), r)$. Then, by applying the above proposition, we know that $d = d^*$ or $d = nd^*$.

In order to use this fact, we need to know how to calculate $[K(P) : K]$. Since $P$ is a point of order $n$, we need to find the smallest $r$ such that $n | \#E(\mathbb{F}_{q^r})$. This implies that $K(P) = \mathbb{F}_{q^r}$. We remark that we can calculate $\#E(\mathbb{F}_{q^r})$ once we know $\#E(\mathbb{F}_q)$. If we know $\#E(\mathbb{F}_q)$, then it can be shown ([**Si**] V.2.4) from the zeta function of $E$ over $\mathbb{F}_q$ that

$$\#E(\mathbb{F}_{q^r}) = (1 + q^r) - (\alpha^r + \beta^r) \tag{1}$$

where $\alpha$ and $\beta$ are the complex roots of

$$T^2 - a_E T + q = 0.$$

and $a_E = (1+q) - \#E(\mathbb{F}_q)$. So, we can use this proposition to compute $d$ up to a factor of $n$.

In Chapter 4 we will use this result in our second algorithm. In this algorithm we first find a point $P$ of order $n$. Or more specifically, we will find $d^* = [K(P, \zeta_n) : K]$. We then will compare $d^*$ to the possible values of $d = [K_{E,n} : K]$ we determined from the division polynomials of $E$ will be described in Chapter 3.

## 5. The Frobenius Automorphism

Suppose that $K = \mathbb{F}_q$ is a finite field. As noted in Corollary 1.7, calculating $d = [K_{E,n} : K]$ is equal to the $|\operatorname{Im}(\overline{\rho}_n)|$. The question of finding $d$ therefore can be translated into one of finding the order of the image of $\overline{\rho}_n$. In fact, we will show that $\operatorname{Im}(\overline{\rho}_n)$ is cyclic, therefore finding $d$ is equivalent to finding the order of the generator of $\operatorname{Im}(\overline{\rho}_n)$.

Now consider the following map:

$$\sigma_q : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q$$

$$x \mapsto x^q.$$

It can be shown quite easily that this map is an automorphism of $\overline{\mathbb{F}}_q$ that leaves $\mathbb{F}_q$ fixed, hence $\sigma_q \in \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. This automorphism $\sigma_q$ is called the *Frobenius automorphism*. As the next theorem shows, if we restrict $\sigma_q$ to the subfield $\mathbb{F}_{q^r}$ with $r \in \mathbb{Z}^+$, then this induced map plays an important role in the group $\operatorname{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$.

THEOREM 1.12. *The Frobenius automorphism $\sigma_q|_{\mathbb{F}_{q^r}}$ generates* $\operatorname{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, *that is*

$$\langle \sigma_q|_{\mathbb{F}_{q^r}} \rangle = Gal(\mathbb{F}_{q^r}/\mathbb{F}_q).$$

*In particular,* $\operatorname{ord}(\sigma_q|_{\mathbb{F}_{q^r}}) = [\mathbb{F}_{q^r} : \mathbb{F}_q]$.

PROOF. See [**St**]. □

COROLLARY 1.13.

$$d = [K_{E,n} : K] = \operatorname{ord}(\overline{\rho}_n(\sigma_q|_{K_{E,n}})) = \operatorname{ord}(\rho_n(\sigma_q)).$$

PROOF. Let $K_{E,n}$ be the field of $n$-torsion points. So, $K_{E,n} = \mathbb{F}_{q^d}$. Thus, by Theorem 1.12, we have $\text{ord}(\sigma_q|_{K_{E,n}}) = [K_{E,n} : K] = d$. Since $\overline{\rho}_n$ is injective by Corollary 1.6, $\text{ord}(\sigma_q|_{K_{E,n}}) = \text{ord}(\overline{\rho}_n(\sigma_q|_{K_{E,n}}))$. The result now follows. □

This is an important corollary since our first algorithm is based upon this fact. In the next chapter we will show that if we use some information from the elliptic curve $E$, then we can determine the characteristic polynomial of the matrix $\overline{\rho}_n(\sigma_q|_{K_{E,n}}) = \rho_n(\sigma_q)$. From this information we can calculate $d$, or more specifically, the order of $\rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$ in almost all cases.

CHAPTER 2

# The Characteristic Polynomial of the Frobenius Endomorphism

In the previous chapter we saw that the problem of calculating $d = [K_{E,n} : K]$ when $K = \mathbb{F}_q$ is a finite field can be translated into finding the order of $\rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$, i.e., the image of the Frobenius automorphism under the Galois representation of $E/K$ modulo $n$. In this chapter we show that we can use information from the elliptic curve $E$ to determine the characteristic polynomial of the matrix $\rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$. Specifically, the goal of this chapter is to demonstrate that the characteristic polynomial, $ch_{\rho_n(\sigma_q)}(T) \in \mathbb{F}_n[T]$ is congruent modulo $n$ to

$$ch_{\rho_n(\sigma_q)}(T) \equiv T^2 - a_E T + q \pmod{n}$$

where $a_E = (q+1) - \#E(\mathbb{F}_q)$.

## 1. The Frobenius Endomorphism

Vital to this chapter is the concept of an endomorphism of an elliptic curve $E/K$. Endomorphisms are actually a subset of a larger class of morphisms called isogenies. Hence, we begin with a definition of an isogeny.

**Definition 2.1:** Let $E_1$ and $E_2$ be elliptic curves over a field $K$. A *$K$-isogeny* between $E_1$ and $E_2$ is a morphism over $K$

$$\phi : E_1 \longrightarrow E_2$$

satisfying $\phi(\mathcal{O}) = \mathcal{O}$.

Here, the morphism is a morphism between the two *projective* curves $E_1$ and $E_2$. We now specialize to the case that $\phi$ is an isogeny from $E$ to itself, i.e., $E = E_1 = E_2$. Then we say that $\phi$ is an *endomorphism*. It is a fact (e.g. [**Si**] III.4) that if $\phi$ is a $K$-isogeny, then for any field extension $F$ of $K$ we have an induced group

homomorphism

$$\phi_F : E_1(F) \longrightarrow E_2(F)$$

$$\phi_F = \phi|_F.$$

If $\phi$ is an endomorphism, then $\phi_F \in \mathrm{End}(E(F))$.

In the next definition, we define a specific endomorphism, the Frobenius endomorphism.

**Definition 2.2** : Let $K = \mathbb{F}_q$ and $E$ be an elliptic curve over $K$. Then (cf. [**Si**] III.4.6) there is a unique morphism, called the *Frobenius endomorphism of* $E/K$

$$\phi_q : E \longrightarrow E$$

such that its action on the $\overline{K}$-rational points is given by

$$(\phi_q)_{\overline{K}}(P) = \begin{cases} (\ x^q, y^q) & \text{if } P = (x,y) \in E(\overline{K}) \\ \mathcal{O} & \text{if } P = \mathcal{O} \end{cases}$$

The action of the Frobenius endomorphism on $E(\overline{K})$ is linked to the Frobenius automorphism on $\overline{K}$ in the following manner. Since $K$ is perfect in this case, $\overline{K}$ is Galois over $K$. But then by Corollary 1.3 the following map exists:

$$\rho_{E/K} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E(\overline{K}))$$

$$\sigma \mapsto \sigma_E,$$

where $\sigma_E$ is defined as in Proposition 1.2$i$. In particular, since the Frobenius automorphism $\sigma_q \in \mathrm{Gal}(\overline{K}/K)$ then

$$(\rho_{E/K}(\sigma_q))(P) = (\sigma_q)_E(P) = \begin{cases} (\sigma_q(x), \sigma_q(y)) = (x^q, y^q) & \text{if } P = (x,y) \in E(\overline{K}) \\ \mathcal{O} & \text{if } P = \mathcal{O}. \end{cases}$$

Comparing this formula to the one above shows that the action of the Frobenius endomorphism on $E(\overline{K})$ is equal to the induced map of the Frobenius automorphism, i.e,

$$(\phi_q)_{\overline{K}}(P) = \rho_{E/K}(\sigma_q)(P)$$

for all $P \in E(\overline{K})$. For the remainder of this report, $(\phi_q)_{\overline{K}}$ and $\rho_{E/K}(\sigma_q) = (\sigma_q)_E$ will be synonymous.

In the next proposition we show that the order of the induced map $\phi_q|_{E[n]}$ in $\mathrm{End}(E[n])$ is equal to $d = [K_{E,n} : K]$.

PROPOSITION 2.3. *Let $\phi_q \in End(E)$ be the Frobenius endomorphism. Then*

$$\phi_q|_{E[n]} = \rho_n(\sigma_q).$$

*In particular, $d = [K_{E,n} : K] = \mathrm{ord}(\phi_q|_{E[n]})$ in $\mathrm{End}(E[n])$.*

PROOF. As noted in the above discussion, we have that the action of $(\phi_q)_{\overline{K}}$ on the $\overline{K}$-rational points of $E$ is equal to $\rho_{E/K}(\sigma_q) \in \mathrm{End}(\overline{K})$. Therefore, it is clear that $\phi_q|_{E[n]} = \rho_{E/K}(\sigma_q)|_{E[n]}$. But by Corollary 1.6, we have

$$\rho_{E/K}(\sigma_q)|_{E[n]} = \overline{\rho}_n(\sigma_q|_{K_{E,n}}) = \rho_n(\sigma_q).$$

The first statement now follows. The second statement is a consequence of Corollary 1.13. □

If $E$ is a curve defined over a field $K$, then the set $\mathrm{End}_K(E)$ consists of all those endomorphisms defined over $K$. $\mathrm{End}_K(E)$ forms a ring where addition is defined by

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

and multiplication is defined via composition, i.e.,

$$(\phi\psi)(P) = \phi(\psi(P)).$$

The proof of these facts is given in [**Si**] III.3.6. The ring $\mathrm{End}_K(E)$ is called the *endomorphism ring* of $E$.

To every isogeny $\phi$, and specifically every endomorphism, we can assign a degree to $\phi$. From algebraic geometry, any non-constant morphism between two curves $E_1$ and $E_2$ is surjective, i.e., $\phi(E_1) = E_2$. (See [**Ha**], II.6.8.) Thus, every non-zero isogeny is surjective. Given any non-zero isogeny $\phi$ between two curves $E_1$ and $E_2$ defined over $K$, we can construct a map between the two function fields $K(E_2)$ and $K(E_1)$ as follows:

$$\phi^* : K(E_2) \longrightarrow K(E_1)$$

$$\phi^* f = f \circ \phi$$

This is injective and fixes $K$. Further, $K(E_1)$ is a finite extension of $\phi^* K(E_2)$, i.e, $[K(E_1) : \phi^* K(E_2)] < \infty$. (See [**Ha**] II.6.8 for a proof of this fact.) This leads to our next definition in which we attach a degree to every isogeny.

**Definition 2.4:** Let $\phi : E_1 \longrightarrow E_2$ be an isogeny where $E_1$ and $E_2$ are defined over $K$. Then its *degree* is defined as follows: if $\phi = 0$, set $\deg \phi = 0$. Otherwise, put

$$\deg \phi = [K(E_1) : \phi^* K(E_2)]$$

We also call $\phi$ *separable* (respectively, *inseparable*) if the finite field extension in question is *separable* (respectively, *inseparable*).

We conclude this section with a theorem concerning the degree of the Frobenius endomorphism.

THEOREM 2.5. *Let $E/K$ be an elliptic curve over $K = \mathbb{F}_q$, $char(K) \neq 2, 3$. Then*

$$\deg \phi_q = q.$$

PROOF. Recall that the Frobenius endomorphism $\phi_q$ is defined by

$$\phi_q : E \longrightarrow E$$

$$(x, y) \mapsto (x^q, y^q)$$

for all non-zero elements in $E(\overline{K})$. By definition, the map

$$\phi_q^* : K(E) \longrightarrow K(E)$$

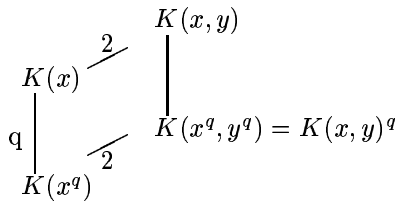
is given by

$$\phi_q^* f = f \circ \phi_q = f(x^q, y^q).$$

Here, $f \in K(E)$, where $K(E)$ is the function field of $E$ defined by

$$K(E) = Quot\left(\frac{K[X,Y]}{(F(X,Y))}\right)$$

where $F(X,Y) \in K[X,Y]$ is a polynomial defining $E$. Since $\mathrm{char}(K) \neq 2, 3$, we can take $F(X,Y) = Y^2 - X^3 - aX - b$. Thus, $K(E) \cong K(x,y)$, where $y^2 = x^3 + ax + b$. Moreover, $\phi_q^* K(E) = K(x^q, y^q) = K(x,y)^q$, where the last identity follows from the fact that $g^q = g$ for every $g \in K$ This leads to the following extensions:




The degrees $[K(x,y) : K(x)] = [K(x^q, y^q) : K(x^q)] = 2$ are a consequence of the relation between $x$ and $y$, namely, $y^2 = x^3 + ax + b$ and $a, b \in \mathbb{F}_q$. The degree of $[K(x) : K(x^q)]$ is $q$ because $x$ satisfies the monic irreducible polynomial

$$T^q - x^q = 0$$

over $K(x^q)$. But then

$$\begin{aligned} [K(x,y) : K(x^q, y^q)][K(x^q, y^q) : K(x^q)] &= [K(x,y) : K(x)][K(x) : K(x^q)] \\ &= 2q \end{aligned}$$

Solving for $[K(x,y) : K(x^q, y^q)]$ gives us $[K(x,y) : K(x^q, y^q)] = \deg\phi_q = q$, the desired result. □

## 2. The Dual Isogeny

In this section we provide some of the tools we need to prove the main result of this chapter. Many results of this section will only be stated, with references given to their proofs (cf. [**Si**] III.6). We begin with the following theorem which motivates our next definition.

PROPOSITION 2.6. *Suppose that* $\phi \in \mathrm{End}(E)$ *and* $\deg \phi = m \neq 0$. *Then there exists a unique isogeny* $\hat{\phi} \in \mathrm{End}(E)$ *satisfying*

$$\phi \circ \hat{\phi} = [m]$$

*where* $[m] = m \cdot 1_E$ *is the multiplication by* $m$ *map and* $1_E$ *is the identity map of* $\mathrm{End}(E)$.

PROOF. See [**Si**] III.6.1. □

**Definition:** Let $\phi \in \mathrm{End}(E)$. Then the *dual isogeny* $\hat{\phi}$ is defined as follows. If $\phi \neq 0$, then $\hat{\phi}$ is the unique isogeny defined in Proposition 2.6. If $\phi = 0$, set $\hat{\phi} = 0$.

The next theorem gives some basic properties of $\phi$ and its dual $\hat{\phi}$.

PROPOSITION 2.7. *Let $\phi, \lambda \in End(E)$. Further, let deg $\phi = m$. Then*

*a)* $\hat{\phi} \circ \phi = \phi \circ \hat{\phi} = [m]$

*b)* $\hat{\phi} \circ \hat{\lambda} = \widehat{\lambda \circ \phi}$

*c)* $\widehat{\phi + \lambda} = \hat{\phi} + \hat{\lambda}$

*d)* $\widehat{[n]} = [n]$, *where* $[n]$ *is the multiplication by* $n$ *map.*

PROOF. See [**Si**] III.6.2. □

Finally, for every $\phi \in \text{End}(E)$ we define $N\phi$, the norm of $\phi$, and the trace of $\phi$, $Tr\phi$, to be the unique integers such that

$$[N\phi] = \phi \circ \hat{\phi} \quad \text{and} \quad [Tr\phi] = \phi + \hat{\phi}$$

While it is clear that $N\phi \in \mathbb{Z}$ by Proposition 2.7a, it is not readily evident that $Tr\phi \in \mathbb{Z}$. But this fact follows from the previous proposition if we rewrite $\phi + \hat{\phi}$ as

$$\begin{aligned} \phi + \hat{\phi} &= 1_E + \phi \circ \hat{\phi} - (1_E - \phi)(1_E - \hat{\phi}) \\ &= 1_E + \phi \circ \hat{\phi} - (1_E - \phi)(\widehat{1_E - \phi}) \\ &= 1_E + [N\phi] - [N(1_E - \phi)] \\ &= [1_E + N\phi - N(1_E - \phi)] \end{aligned}$$

From this we can deduce that $Tr \in \mathbb{Z}$, and furthermore, that

$$Tr\phi = 1 + N\phi - N(1_E - \phi). \tag{2}$$

## 3. The Characteristic Polynomial of the Frobenius

Let $\phi \in \text{End}(E)$ and consider the following polynomial

$$f_\phi(T) = T^2 - (Tr\phi)T + (N\phi) \in \mathbb{Z}[T]. \tag{3}$$

Then, $f_\phi$ factors in $\text{End}(E)$ as

$$f_\phi(T) = (T - \phi)(T - \hat{\phi})$$

So, $\phi$ and its dual, $\hat{\phi}$, are the roots of $f_\phi$.

Now consider an elliptic curve $E$ which is defined over $K$. For every $\phi \in \mathrm{End}(E)$, we can restrict $\phi$ to $E[n]$, thus inducing an element $\phi|_{E[n]} \in \mathrm{End}(E[n])$. We thus have a ring homomorphism,

$$\lambda_n : \mathrm{End}(E) \longrightarrow \mathrm{End}(E[n])$$

$$\phi \mapsto \phi|_{E[n]}$$

Moreover, this induced endomorphism $\phi|_{E[n]}$ will satisfy the polynomial $f_\phi$ in $\mathrm{End}(E[n])$ because of the homomorphism property of the mapping $\lambda_n$.

If we pick a basis of $E[n]$, then by the same argument of that in Chapter 1 which yields a group isomorphism between $\mathrm{Aut}(E[n])$ and $GL_2(\mathbb{Z}/n\mathbb{Z})$, there exists a ring isomorphism

$$\pi : \mathrm{End}(E[n]) \xrightarrow{\sim} M_2(\mathbb{Z}/n\mathbb{Z}).$$

where $M_2(\mathbb{Z}/n\mathbb{Z})$ is the ring of all $2 \times 2$ matrices. Then $M_\phi = \pi(\phi|_{E[n]})$ is a matrix in $M_2(\mathbb{Z}/n\mathbb{Z})$. As the next theorem will show, the characteristic polynomial of this matrix $M_\phi$ is related to the polynomial $f_\phi$.

THEOREM 2.8. *Let $\phi \in \mathrm{End}(E)$. Then the characteristic polynomial of $M_\phi$, where $M_\phi$ is defined as above, is congruent modulo $n$ to $f_\phi$*

$$ch_{\phi|_{E[n]}} = ch_{M_\phi}(T) \equiv f_\phi(T) \pmod{n}$$

*where, as before,*

$$f_\phi(T) = T^2 + (Tr\phi)T + (N\phi) \in \mathbb{Z}[T].$$

PROOF. Let $\overline{f}_\phi$ be the image of $f_\phi$ in $\mathbb{F}_n[T]$. We have already pointed out that $\phi|_{E[n]}$ satisfies $f_\phi$ in $\mathrm{End}(E[n])$. Since there exists an isomorphism $\pi$ from $\mathrm{End}(E[n])$ to $M_2(\mathbb{Z}/n\mathbb{Z})$, by the ring homomorphism properties of $\pi$ we see that $M_\phi$ satisfies $\overline{f}_\phi \in \mathbb{F}_n[T]$. In other words, $\overline{f}_\phi$ annihilates $M_\phi$.

Let $g_\phi$ be the minimal polynomial of $M_\phi$ in $\mathbb{F}_n[T]$. Then $g_\phi | \overline{f}_\phi$ in the ring $\mathbb{F}_n[T]$. If $g_\phi = \overline{f}_\phi$, then we are done since $\deg(g_\phi) = 2 = \deg(ch_{M_\phi})$ and $g_\phi | ch_{M_\phi}$ by the Cayley-Hamilton Theorem, and all polynomials are monic.

Thus, assume $\deg(g_\phi) = 1$. (Without loss of generality, we can assume that $\deg(g_\phi) \neq 0$.) Then $g_\phi(T) = (T - a) \in \mathbb{F}_n[T]$, for some $a \in \mathbb{F}_n$. But this means that

$$\phi|_{E[n]} = [a]|_{E[n]},$$

or in other words, $\phi|_{E[n]}$ acts like multiplication by $a$ on the points of $E[n]$. Thus $(\phi - a)|_{E[n]} = 0$, thereby implying that $\mathrm{Ker}(\phi - a) \supset E[n]$. Therefore, $(\phi - a) = [n] \cdot \psi$ for some $\psi \in \mathrm{End}(E)$, and hence

$$\widehat{[n] \cdot \psi} = [n] \cdot \hat{\psi} = \widehat{(\phi - a)} = \hat{\phi} - a.$$

Thus, $\hat{\phi}|_{E[n]} = [a]|_{E[n]}$. But now, from the definitions of the norm and trace, we have

$$\begin{aligned} N\phi &= \phi \circ \hat{\phi} \equiv [a^2] \pmod{n} \\ Tr\phi &= \phi + \hat{\phi} \equiv [a] + [a] = 2[a] \pmod{n} \end{aligned}$$

From this we can deduce from equation 3 that

$$\overline{f}_{\phi}(T) \equiv (T - a)^2.$$

But since $g_\phi$ and $ch_{M_\phi}$ have the same irreducible factors, we have $ch_{M_\phi} = g_\phi^2 = (T - a)^2$, so $\overline{f}_{\phi} = ch_{M_\phi}$ in $\mathbb{F}_n[T]$. □

We now specialize to the case when $\phi = \phi_q \in \mathrm{End}(E)$, is the Frobenius endomorphism. Then $\phi_q$ satisfies the following polynomial

$$f_{\phi_q} = T^2 - (Tr\phi_q)T + (N\phi_q).$$

in $\mathrm{End}(E)$ by Proposition 2.8. But by Proposition 2.7 and 2.5, we have that $N\phi_q = \deg \phi_q = q$.

To calculate $Tr\phi_q$ we use (2) to get

$$Tr\phi_q = (1 + N\phi_q - N(1_E - \phi_q)) = 1 + q - \deg(1_E - \phi_q).$$

To determine the value of $\deg(1_E - \phi_q)$ we can use the following two results.

LEMMA 2.9. *Let $\phi_q : E \longrightarrow E$ be the Frobenius endomorphism on an elliptic curve $E/K = \mathbb{F}_q$, and let $m, n \in \mathbb{Z}$. Then the map*

$$m + n\phi_q : E \longrightarrow E$$

*is separable if and only if $q \nmid m$. In particular, $1 - \phi_q$ is separable.*

PROOF. See [**Si**] III.5.5. □

LEMMA 2.10. *Assume $\phi$ is separable. Then*

$$\#\operatorname{Ker}(\phi) = \deg \phi$$

PROOF. See [**Si**] III.4.10. □

Using these results, we have

THEOREM 2.11. *Let $E$ be an elliptic curve over $K = \mathbb{F}_q$. Then*

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

*In particular, $Tr\phi_q = 1 + q - \#E(\mathbb{F}_q)$.*

PROOF. Since $\phi_q$ is the Frobenius endomorphism, then $\phi_q(P) \in \mathrm{E}(K)$ if and only if $\phi_q(P) = P$. So $E(\mathbb{F}_q) = \operatorname{Ker}(1 - \phi_q)$. But by the two previous lemmas we have

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

□

We now summarize this discussion in the following theorem

THEOREM 2.12. *Let $E$ be an elliptic curve over $K = \mathbb{F}_q$. If $\phi_q \in \operatorname{End}(E)$ is the Frobenius endomorphism, then $\phi_q$ satisfies the polynomial*

$$f_{\phi_q}(T) = T^2 - a_E T + q$$

*in* $\operatorname{End}(E)$ *where* $a_E = (1 + q) - \#E(\mathbb{F}_q)$.

PROOF. This follows by substituting $Tr\phi_q = (1 + q) - \#E(\mathbb{F}_q)$ and $N\phi_q = q$ into (3). □

If we restrict $\phi_q$ to $E[n]$, then by Proposition 2.3, the induced map $\phi_q|_{E[n]} = \overline{\rho}_n(\sigma_q|_{K_{E,n}}) = \rho_n(\sigma_q)$. But then the following corollary to Theorem 2.12 and Theorem 2.8 tells us the characteristic polynomial of $\overline{\rho}_n(\sigma_q|_{K_{E,n}}) = \rho_n(\sigma_q)$.

COROLLARY 2.13. *The polynomial*

$$f(T) = T^2 - a_E T + q$$

*is congruent modulo $n$ to the characteristic polynomial of $\overline{\rho}_n(\sigma_q|_{K_{E,n}}) = \rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$.*

This gives the desired result of the chapter.

## 4. Towards an algorithm

By Corollary 2.13, we now know how to determine the characteristic polynomial of the matrix $\rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$, where $\rho_n$ is the group homomorphism of Corollary 1.6. As the next proposition shows, from this polynomial we can determine $d = [K_{E,n} : K]$ in a large number of cases.

THEOREM 2.14. *Let $E$ be an elliptic curve over the field $K = \mathbb{F}_q$. Here, $char(K) \neq 2, 3$. Further, pick an odd prime $n \neq char(K)$. Let $\rho_n(\sigma_q)$ be the image of the Frobenius automorphism in $GL_2(\mathbb{Z}/n\mathbb{Z})$ where $\rho_n$ is defined as in Corollary 1.6. Then $d = [K_{E,n} : K] = \operatorname{ord}(\rho_n(\sigma_q))$ and*

$$ch_{\rho_n(\sigma_q)}(T) \equiv T^2 - a_E T + q \pmod{n}$$

*is its corresponding characteristic polynomial. Suppose that $ch_{\rho_n(\sigma_q)}$ factors over $\overline{\mathbb{F}}_n$ as*

$$ch_{\rho_n(\sigma_q)}(T) = (T - \alpha)(T - \beta).$$

*Let $c = \left(\frac{a_E^2 - 4q}{n}\right)$, where $\left(\frac{-}{n}\right)$ is the Legendre symbol. Then,*

- *if $c = 1$, then $\alpha, \beta \in \mathbb{F}_n$ and $d = \operatorname{lcm}(\operatorname{ord}(\alpha, n), \operatorname{ord}(\beta, n))$;*
- *if $c = -1$, then $\alpha, \beta \in \mathbb{F}_{n^2} \setminus \mathbb{F}_n$, $\beta = \alpha^n$, and $d$ is equal to the order of $\alpha \in \mathbb{F}_{n^2}^{\times}$;*
- *if $c = 0$, then $\alpha = \beta \in \mathbb{F}_n$ and $d = \operatorname{ord}(\alpha, n)$ or $d = n \operatorname{ord}(\alpha, n)$.*

*Moreover, if $n > 4q$ or $\left(\frac{q}{n}\right) = -1$, then $c \neq 0$, in which case we can determine $d$ explicitly.*

PROOF. The first statement was proved in Corollary 1.13. The second statement was proved in Corollary 2.13.

Observe that $a_E^2 - 4q$ is the discriminant of the characteristic polynomial. So, if $c = 1$, the first assertion follows from the fact that then $ch_{\rho_n(\sigma_q)}$ factors in $\mathbb{F}_n$ and has two distinct roots, $\alpha$ and $\beta$, in this field. Further, $\alpha$ and $\beta$ are the eigenvalues of the matrix $\rho_n(\sigma_q)$. Thus,

$$\rho_n(\sigma_q) \sim \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

Notice that for $t \in \mathbb{Z}$, then

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}^t = \begin{pmatrix} \alpha^t & 0 \\ 0 & \beta^t \end{pmatrix}$$

So, if $t$ is such that $\rho_n(\sigma_q)^t \sim I_2$ in $GL_2(\mathbb{Z}/n\mathbb{Z})$ where $I_2$ is the identity matrix, then $\text{ord}(\alpha, n)|t$ and $\text{ord}(\beta, n)|t$. Hence, the order of $\rho_n(\sigma_q)$, and consequently, the value of $d$, is equal to $\text{lcm}(\text{ord}(\alpha, n), \text{ord}(\beta, n))$. This gives us the desired result in this case.

In the second assertion, that is, if $c = -1$, then neither $\alpha$ nor $\beta$ are in $\mathbb{F}_n$. So the polynomial $ch_{\rho_n(\sigma_q)}(T)$ is irreducible in $\mathbb{F}_n[x]$. But because $\alpha$ and $\beta$ satisfy this monic polynomial of degree 2, $\alpha, \beta \in \mathbb{F}_{n^2}$. Moreover, since $\beta$ is a conjugate of $\alpha$, we can write it as $\beta = \alpha^n$ since $\sigma_n$ generates $\text{Gal}(\mathbb{F}_{n^2}/\mathbb{F}_n)$. Thus

$$\rho_n(\sigma_q) \sim \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^n \end{pmatrix}.$$

But then it is clear that the order of $\rho_n(\sigma_q)$ is equal to the order of $\alpha$ in $\mathbb{F}_{n^2}$.

Finally, if $c = 0$, then the discriminant $a_E^2 - 4q \equiv 0 \pmod{n}$. In this case there is only one eigenvalue, i.e. $\alpha = \beta \in \mathbb{F}_n$. But then by the Jordan Canonical Form,

$$\rho_n(\sigma_q) \sim \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \quad \text{or} \quad \rho_n(\sigma_q) \sim \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix},$$

depending upon the dimension of the eigenspace. If $\rho_n(\sigma_q)$ is diagonal, i.e. the eigenspace has dimension 2, then it is clear that the order of $\rho_n(\sigma_q)$ is the order of $\alpha$ in $\mathbb{F}_n$. Thus, $d = \text{ord}(\alpha, n)$. However, suppose that the other case occurs. We observe that

$$\rho_n(\sigma_q)^t \sim \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}^t = \begin{pmatrix} \alpha^t & t\alpha^{t-1} \\ 0 & \alpha^t \end{pmatrix}$$

for all $t \in \mathbb{Z}$. Letting $t = n$, we find that $\rho_n(\sigma_q)^t$ is a diagonal matrix with $\alpha$'s along the diagonal since $\rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$. Further, this is the smallest value of $t$ that will give us a diagonal matrix. The order of $\rho_n(\sigma_q)^t$ will then be $\text{ord}(\alpha, n)$. Thus, the order of $\rho_n(\sigma_q)$ must be $n\text{ord}(\alpha, n)$ which in turn implies that $d = n\text{ord}(\alpha, n)$.

To prove the last statement, we use the following fact first proved by Hasse (see [**Si**] V.1.1), namely,

$$|a_E| \leq 2\sqrt{q} \tag{4}$$

So, if $n > 4q$, then $n > |a_E^2 - 4q|$, from which it is clear that $\left(\frac{a_E^2 - 4q}{n}\right) \neq 0$. Thus, the last case cannot occur. Similarly, the last case cannot occur if $\left(\frac{q}{n}\right) = -1$ since $\left(\frac{a_E^2 - 4q}{n}\right) = 0$ implies that the opposite is true, that is, $q$ is a square modulo $n$.

□

COROLLARY 2.15. *Let $E$ be an elliptic curve of $K$ and let $d = [K_{E,n} : K]$, where, as before, $n \neq char(K)$. If $c = \left(\frac{a_E^2 - 4q}{n}\right)$, then we have the following relations between $d$ and $n$:*

- *if $c = 1$, then $d|(n-1)$.*
- *if $c = 0$, then $d|n(n-1)$.*
- *if $c = -1$, then $d|\operatorname{ord}(q,n)(n+1)|n^2-1$*

*In addition, we always have $\operatorname{ord}(q,n)|d$.*

PROOF. The first two assertions are easy to see from Theorem 2.14 since $\operatorname{ord}(\alpha, n)|n-1$ for all $\alpha \in \mathbb{F}_n$. To prove the third statement, we note that since $\left(\frac{a_E^2 - 4q}{n}\right) = -1$, $d$ is equal to the order of $\alpha \in \mathbb{F}_{n^2}$, where $\alpha$ is one of the roots of the characteristic polynomial. Let $g$ be a primitive $(n^2-1)^{th}$ root of unity. So, $\alpha = g^t$ for some $t \in \mathbb{Z}$. Moreover, from Theorem 2.13 we have $\alpha\alpha^n = q \in \mathbb{F}_{n^2}$. Let $b = \operatorname{ord}(q,n)$. Then

$$(g^t)^{(1+n)b} = \alpha^{(1+n)b} = (\alpha^{(1+n)})^b = q^b = 1.$$

Since $d$ is the order of $g^t$, we have $d|\operatorname{ord}(q,n)(n+1)$.

The last assertion was proven in Corollary 1.10. □

In Theorem 2.14, the value of $a_E$ does not determine $d$ completely in the case $c = 0$. However, in many cases, the following criterion allows us to determine $d$.

PROPOSITION 2.16. *Let $E$ be an elliptic curve over $K$ and let*

$$f(T) = T^2 - a_E T + q = (T - \delta)(T - \gamma)$$

*be the factorization of $f(T)$ in $\mathbb{C}[T]$. Suppose that $a_E^2 - 4q \equiv 0 \pmod{n}$. Then $f(T)$ has repeated root $\alpha$ modulo $n$, and put $d^* = ord(\alpha, n)$. Then, if*

$$n^2 \nmid 1 + q^{d^*} - (\delta^{d^*} + \gamma^{d^*})$$

*then $d = [K_{E,n} : K] = nd^*$.*

PROOF. We know from Theorem 2.14 that $d = d^*$ or $d = nd^*$. Suppose that $d = d^*$. Since $E[n]$ is a subgroup of $E(\mathbb{F}_{q^{d^*}})$, we must have

$$n^2 | \#E(\mathbb{F}_{q^{d^*}}).$$

Recall from Chapter 1.4 that $\#E(\mathbb{F}_{q^{d^*}})$ is given by equation (1), that is,

$$\#E(\mathbb{F}_{q^{d^*}}) = (1 + q^{d^*}) - (\delta^{d^*} + \gamma^{d^*}).$$

(It should be clear that the right side is an integer since $\delta$ and $\gamma$ are conjugates.) But now, by hypothesis, we can deduce that $n^2 \nmid \#E(\mathbb{F}_{q^{d^*}})$, providing us with a contradiction. This implies that $d = nd^*$.

□

Unfortunately, this is *not* an if and only if statement. We provide a counterexample to the converse in Example 4.2. In the next chapter we present the division polynomials of an elliptic curve $E$. In Chapter 4 we describe a method by which we can determine $d$ when $a_E^2 - 4q \equiv 0 \pmod{n}$ and Proposition 2.16 fails to determine $d$.

CHAPTER 3

# The Division Polynomials of an Elliptic Curve

Let $E$ be an elliptic curve over the field $K$ with $\mathrm{char}(K) \neq 2, 3$. Thus, $E$ can be written as

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

where the *discriminant* $\Delta = -16(4a^3 - 27b^2) \neq 0$. It is well known that we can define an operation of addition on the points $P \in E(\overline{K})$ by using the cord and tangent method. We can construct explicit formulae for the addition of two points, $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, which depend only on $a, b, x_1, x_2, y_1$, and $y_2$. These formulae, though not difficult to describe, are somewhat messy and involve several cases. Those interested in these formulae are recommended to check out [**Si**], II.2.3.

In this chapter we will describe the division polynomials of an elliptic curve where $E$ is given as above. We will construct an explicit formula for $[n]$, the multiplication by $n$ map, i.e.,

$$[n]P = \left( \frac{\phi_n(P)}{\psi_n^2(P)}, \frac{\omega_n(P)}{\psi_n^3(P)} \right),$$

where $\phi_n, \omega_n$, and $\psi_n$ are polynomials in the coordinates of $P = (x, y)$. From this explicit expression we can determine the $x$-coordinates of the $n$-torsion points, thus providing us with a partial solution to our problem.

## 1. The Division Polynomials

The *division polynomials* $\tilde{\psi}_n \in \mathbb{Z}[a, b, x, y]$ are defined inductively as follows:

$$\begin{aligned}
\tilde{\psi}_{-1} &= -1, \quad \tilde{\psi}_0 = 0, \quad \tilde{\psi}_1 = 1, \quad \tilde{\psi}_2 = 2y \\
\tilde{\psi}_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \\
\tilde{\psi}_4 &= 4y(x^6 - 5ax^4 + 20bx^3 - 5ax^2 - 4abx - 8b^2 - a^3) \\
\tilde{\psi}_n = \tilde{\psi}_{2m+1} &= \tilde{\psi}_{m+2}\tilde{\psi}_m^3 - \tilde{\psi}_{m-1}\tilde{\psi}_{m+1}^3, \qquad m \geq 2 \\
2y\tilde{\psi}_n = 2y\tilde{\psi}_{2m} &= \tilde{\psi}_m(\tilde{\psi}_{m+2}\tilde{\psi}_{m-1}^2 - \tilde{\psi}_{m-2}\tilde{\psi}_{m+1}^2), \qquad m \geq 3.
\end{aligned}$$

The fact that $\tilde{\psi}_{2m}$ is a polynomial follows from the next lemma.

LEMMA 3.1. *Let $\tilde{\psi}_n$ be the $n^{th}$ division polynomial. Then*

$$\begin{aligned} 2y\tilde{\psi}_{2m} &= 4y^2 F_{2m}, \qquad \text{if } n = 2m \\ \tilde{\psi}_{2m+1} &= F_{2m+1}, \qquad \text{if } n = 2m+1 \end{aligned}$$

*where $F_{2m}$ and $F_{2m+1}$ are polynomials in $\mathbb{Z}[a, b, x, y^2]$. In particular, $\tilde{\psi}_n \in \mathbb{Z}[a, b, x, y]$ if $n$ even. Further, if $n$ is odd, then $\tilde{\psi}_n \in \mathbb{Z}[a, b, x, y^2]$, and $(2y)^{-1}\tilde{\psi}_n \in \mathbb{Z}[a, b, x, y^2]$ if $n$ is even.*

PROOF. For the base cases $n = 1, 2, 3$, and 4, the statement holds trivially. Thus, assume $n \geq 5$ and that the result holds for all $k < n$. We demonstrate the statement's validity for $\tilde{\psi}_n$.

If $n$ is odd, then

$$\tilde{\psi}_n = \tilde{\psi}_{2m+1} = \tilde{\psi}_{m+2}\tilde{\psi}_m^3 - \tilde{\psi}_{m-1}\tilde{\psi}_{m+1}^3.$$

By the inductive hypothesis, if $m$ is even,

$$\begin{aligned} \tilde{\psi}_n &= 2yF_{m+2}(2y)^3 F_m^3 - F_{m-1}F_{m+1}^3 \\ &= 16y^4 F_{m+2}F_m^3 - F_{m-1}F_{m+1}^3. \end{aligned}$$

But then, since $F_{m+2}, F_m^3, F_{m-1}, F_{m+1}^3 \in \mathbb{Z}[a, b, x, y^2]$, it is clear that

$$F_n = F_{2m+1} = 16y^4 F_{m+2}F_m^3 - F_{m-1}F_{m+1}^3 \in \mathbb{Z}[a, b, x, y^2].$$

The case for $m$ odd is similar.

If $n$ is even, then

$$2y\tilde{\psi}_n = 2y\tilde{\psi}_{2m} = \tilde{\psi}_m(\tilde{\psi}_{m+2}\tilde{\psi}_{m-1}^2 - \tilde{\psi}_{m-2}\tilde{\psi}_{m+1}^2)$$

Again, there are two subcases, $m$ odd and $m$ even. We do only the first case. By induction

$$2y\tilde{\psi}_n = F_m(F_{m+2}(4y^2)F_{m-1}^2 - F_{m-2}(4y^2)F_{m+1}^2)$$

After rearranging,

$$2y\tilde{\psi}_n = (4y^2)F_n = (4y^2)[F_m(F_{m+2}F_{m-1}^2 - F_{m-2}F_{m+1}^2)]$$

It is clear that $F_n \in \mathbb{Z}[a, b, x, y^2]$, thus completing the proof. □

We now connect this discussion with our elliptic curve $E : y^2 = x^3 + ax + b$ over the finite field $K = \mathbb{F}_q$. The $n^{th}$ division polynomial $\psi_n$ of $E$ is formed by substituting the coefficients $a$ and $b$ into $\tilde{\psi}_n(a, b, x, y)$. So $\psi_n \in K[x, y]$. Moreover, we substitute $x^3 + ax + b$ for $y^2$ in $\psi_n(x, y)$. Notice that once we do this, $\psi_n$ is no longer a polynomial in $K[x, y]$ because we have introduced relations between the indeterminates. In fact,

$$\psi_n \in K[\overline{x}, \overline{y}] \cong K[x, y]/(f(x, y))$$

where $f(x, y) = y^2 - x^3 - ax - b$. In fact, for the remainder of this chapter, we assume that an elliptic curve $E$ has been given and the appropriate substitutions have been made. That is, we will consider $\psi_n$ as an element of $K[\overline{x}, \overline{y}]$. But now applying Lemma 3.1 it is clear that $\psi_n \in K[\overline{x}]$ if $n$ odd, and $(2y)^{-1}\psi_n \in K[\overline{x}]$ if $n$ is even. In fact, we can consider both polynomials as polynomials in the indeterminate $x$ since $K[\overline{x}] \cong K[x]$.

Now define the following polynomials $\phi_n$ and $\omega_n$ by

$$\begin{aligned} \phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1} \\ 4y\omega_n &= \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2. \end{aligned}$$

Using the above discussion, it is clear that $\phi_n \in K[x]$ for both $n$ even and $n$ odd. In the next lemma, we describe the behavior of $\phi_n$ and $\psi_n^2$ as polynomials in $K[x]$

LEMMA 3.2. *Let $\phi_n$ and $\psi_n^2$ be defined as above. Then $\phi_n$ and $\psi_n^2$ are both polynomials in $K[x]$. Furthermore, as polynomials in $x$*

$$\begin{aligned} \phi_n(x) &= x^{n^2} + \textit{ lower order terms} \\ \psi_n^2(x) &= n^2 x^{n^2-1} + \textit{ lower order terms} \end{aligned}$$

PROOF. The first statement follows directly from the previous lemma. Furthermore, the behavior of $\phi_n(x)$ is a direct consequence of the behavior of $\psi_n^2(x)$. Thus, we prove the theorem only for $\psi_n^2$.

The result holds trivially for the base cases $n = 1, 2, 3$, and 4. Suppose that $n > 4$. If $n$ is even, then $n = 2m$. Hence,

$$\psi_n = \psi_{2m} = \frac{\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)}{2y}$$

Squaring both sides gives us

$$\psi_n^2 = \frac{\psi_m^2(\psi_{m+2}^2\psi_{m-1}^4 - 2\psi_{m+2}\psi_{m-2}\psi_{m-1}^2\psi_{m+1}^2 + \psi_{m-2}^2\psi_{m+1}^4)}{4y^2}.$$

By induction

$$\psi_m^2\psi_{m+2}^2\psi_{m-1}^4 = (m+2)^2(m-1)^4m^2x^{4m^2+2} + \dots \tag{5}$$

$$\psi_{m+2}\psi_{m-2}\psi_{m-1}^2\psi_{m+1}^2 = (m+2)(m-2)(m-1)^2(m+1)^2x^{4m^2+2} + \dots \tag{6}$$

$$\psi_{m-2}^2\psi_{m+1}^4 = (m-2)^2(m+1)^4m^2x^{4m^2+2} + \dots \tag{7}$$

Using (5), (6), and (7), we can rewrite $\psi_n^2$ as

$$\psi_n^2 = \frac{16m^2x^{4m^2+2} + \dots}{4y^2}.$$

Since $y^2 = x^3 + ax + b \in K[\overline{x}, \overline{y}]$ and $\psi_n^2 \in K[x]$, we can simplify the above to

$$\psi_n^2 = 4m^2x^{(2m)^2-1} + \text{lower order terms}$$

as desired.

The proof for $n$ odd is similar in style and content, so we omit it. □

As the next theorem shows, the multiplication by $n$ map can be defined in terms of $\phi_n, \omega_n$, and $\psi_n$.

THEOREM 3.3. *Let $P = (x, y) \in E(\overline{K})$. Then,*

$$[n]P = \left(\frac{\phi_n(P)}{\psi_n^2(P)}, \frac{\omega_n(P)}{\psi_n^3(P)}\right)$$

PROOF. We refer to an analytic proof using elliptic functions given in [**La1**] II.2.1. The proof there is done for all fields $K$ where $\text{char}(K) \neq 2, 3$. □

## 2. The $n$-torsion Points

In this section, we connect the division polynomial $\psi_n$ to the $n$-torsion points. From the next proposition, we can deduce that the $x$-coordinates of the $n$-torsion points are the roots of $\psi_n$.

PROPOSITION 3.4. *The polynomials $\phi_n$ and $\psi_n^2$, viewed as elements of $K[x]$, are relatively prime if $\Delta = -16(4a^3 + 27b^3) \neq 0$. (The number $\Delta$ is called the* discriminant *of $E$).*

PROOF. Again, see [**La1**] II.2.3 for a proof of this fact. □

We need the restriction that $\Delta \neq 0$ because we can find polynomials $f, g \in K[x]$ such that

$$f\phi_n - g\psi_n^2 = \Delta.$$

For example, in the case that $n = 2$, then

$$16(3x^2 - 4a)\phi_2 - 4(3x^2 - 5ax - 27b)\psi_2^2 = \Delta$$

where $a$ and $b$ are the coefficients of the elliptic curve $E$. An important corollary of this proposition, combined with the explicit formula for $[n]$, is that the division polynomials provide us with a means to find the $x$-coordinates of the $n$-torsion points.

COROLLARY 3.5. *If $P = (x, y) \in E(\overline{K})$, then*

$$[n]P = \mathcal{O} \quad \text{if and only if} \quad \psi_n^2(x) = 0.$$

PROOF. By Theorem 3.3, we see that the $x$-coordinate of $nP$ is given by $r_n(x) = \frac{\phi_n(x)}{\psi_n^2(x)} \in K(x)$. (The fact that these are polynomials in strictly in $x$ follows from Lemma 3.2.) Thus $nP = \mathcal{O}$ if and only if $r_n(x)$ has a pole at $x$. Since $\phi_n(x)$ and $\psi_n^2(x)$ are relatively prime by Theorem 3.4, the rational function $r_n$ has poles at $x$ if and only if $\psi_n^2(x)$ has a zero at $x$. The result now follows. □

## 3. Using $\psi_n$ to find $[K_{E,n} : K]$

As we have just seen, from the division polynomial $\psi_n$ we can find the $x$-coordinate of the $n$-torsion points. Supposing that $n$ is odd, then $\psi_n$ is a polynomial in $x$. If we now suppose that $K = \mathbb{F}_q$ and factor $\psi_n$ over $\mathbb{F}_q[x]$, we get

$$\psi_n = f_1 \cdots f_r$$

where each $f_i$ is irreducible in $\mathbb{F}_q[x]$. We also notice that the $f_i$s are distinct. This follows from the fact that there are $n^2 - 1$ torsion points of the form $P = (x, y)$. Moreover, there are only two $P \in E[n]$ that will have $x$ has its $x$-coordinate because of the relation $y^2 = x^3 + ax + b$. Since $\psi_n$ has degree $\frac{n^2-1}{2}$ by Lemma 3.2, then it has $\frac{n^2-1}{2}$ roots in $\overline{\mathbb{F}}_q$, But each root must be of multiplicity one because each root $x$ corresponds to the $x$-coordinate of a $n$-torsion point. If there were a root $x$ of multiplicity greater than one, there there would be less than $n^2 - 1$ $n$-torsion points of the form $P = (x, y)$, which cannot be true.

As demonstrated in the next proposition, we can determine $d = [K_{E,n} : K]$ up to a factor of 2 from the way $\psi_n$ factors in $\mathbb{F}_q[x]$.

THEOREM 3.6. *Let $n$ be an odd prime. Also, $K = \mathbb{F}_q$ with $n \neq char(K)$. Suppose that $\psi_n$ factors in $K[x]$ as above. Let $d_i = deg(f_i)$ and $l = lcm(\{d_i\}_{i=1}^r)$. Let $K'_{E,n} = K(x_1, x_2, \ldots, x_{n^2-1})$, where the $x_i$'s are the $x$-coordinates of the $n$-torsion points. Then*

$$[K'_{E,n} : K] = l.$$

*Furthermore, $[K_{E,n} : K'_{E,n}] = 1$ or $2$; alternatively, $d = l$ or $d = 2l$.*

PROOF. We begin by noting that $\psi_n$ is a polynomial in $x$ since $n$ is odd. From Corollary 3.5, we know the roots of $\psi_n$ are precisely the $x$-coordinates of the $n$-torsion points. Thus, $K'_{E,n}$ is the splitting field of $\psi_n$ over $K$. Since $K$ is a finite field $[K'_{E,n} : K]$ is equal to to the least common multiple of the degrees of $\psi_n$'s irreducible factors over $K$, i.e., $[K'_{E,n} : K] = l$.

To prove the second claim, suppose that $K_{E,n} \neq K'_{E,n}$. Then there exists some $x_i$ such that

$$y_i = \sqrt{x_i^3 + ax_i + b} \notin K'_{E,n} = \mathbb{F}_{q^l}.$$

But then $K'_{E,n}(y_i) = \mathbb{F}_{q^{2l}}$, and every element of $x \in \mathbb{F}_{q^l}$ has a square root in $\mathbb{F}_{q^{2l}}$. In particular, all $y_i \in \mathbb{F}_{q^{2l}}$. Thus, in this case $[K_{E,n} : K'_{E,n}] = 2$.

Since $d = [K_{E,n} : K'_{E,n}][K'_{E,n} : K]$, it is apparent that $d = l$ or $d = 2l$. □

As we see from this proposition, we once again have a partial solution to our problem. Solely from the division polynomial, we can determine $d = [K_{E,n} : K]$ up to a factor of 2. In the next chapter we describe two algorithms to calculate $d$. Both algorithms utilize the division polynomial $\psi_n$ to calculate $d$. But as we will see, the importance of $\psi_n$ varies between the two methods. In the first method, $\psi_n$ will only be computed in the special case that $a_E^2 - 4q \equiv 0 \pmod{n}$, whereas in the second method, $\psi_n$ will be computed in all cases. In fact, the second algorithm is a continuation of the discussion of this chapter. Specifically, we present a method to distinguish between the two possibilities, $d = l$ or $d = 2l$.

CHAPTER 4

# Two Algorithms for Computing $[K_{E,n} : K]$

So far we have presented only partial solutions (Theorem 1.11, Theorem 2.14, and Theorem 3.6) to the problem of calculating $d = [K_{E,n} : K]$. However, in this chapter we describe two algorithms which combine these solutions to compute $d = [K_{E,n} : K]$. We assume that the following information has been provided:

- $q = p^r$, where $K = \mathbb{F}_q$, and $\text{char}(K) = p \neq 2, 3$.
- $n$, a prime such that $n \neq \text{char}(K)$ and $n \geq 3$.
- $a$ and $b$, the coefficients of the elliptic curve $E$ over $K$ in Weierstrass form.

Both algorithms are a function of $n, q, a$ and $b$. The algorithms are an amalgamation of our previous partial solutions.

## 1. Algorithm 1

Algorithm 1 is based upon the results of Chapter 2 and 3, in particular, Theorem 2.14 and Theorem 3.6. Recall from Theorem 2.14 that once we know $a_E$, and if $\left(\frac{a_E^2 - 4q}{n}\right) \neq 0$, then we can determine $d = [K_{E,n} : K]$. If $\left(\frac{a_E^2 - 4q}{n}\right) = 0$, then by Theorem 2.14, the characteristic polynomial of $\rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$, i.e.,

$$ch_{\rho_n(\sigma_q)} \equiv T^2 - a_E T + q \pmod{n},$$

has a repeated eigenvalue $\alpha$. Then, we know that $d = n\text{ord}(\alpha, n)$ or $d = \text{ord}(\alpha, n)$. Furthermore, Proposition 2.16 allows us to distinguish $d$ in *some* cases. However, by using the factorization of $\psi_n$ in $K[x]$, i.e.,

$$\psi_n = f_1 \cdots f_r,$$

then we can distinguish between the two possibilities in all cases as exhibited in the following lemma.

LEMMA 4.1. *If* $\left(\frac{a_E^2-4q}{n}\right) = 0$, *then put* $l = \mathrm{lcm}(\{\deg(f_i)\}_{i=1}^r)$ *and let* $d^* = \mathrm{ord}(\alpha, n)$. *Then*

$$d = \begin{cases} d^* & \text{if } d^* = l \text{ or } d^* = 2l \\ nd^* & \text{otherwise.} \end{cases}$$

PROOF. From Theorem 3.6, we know that $d = l$ or $d = 2l$. Suppose that $d^* = l$. Then if $d = nd^*$, then $l \neq d$ and $2l \neq d$ since $n$ is an odd prime. So, $d = d^*$. Similarly suppose that $d^* = 2l$. If $d = nd^*$, then $l \neq d$ and $2l \neq d$. So, $d = d^*$.

Now suppose that $d^* \neq l$ and $d^* \neq 2l$. Then $d \neq d^*$ since $d = l$ or $d = 2l$. So, $d = nd^*$. □

By applying this lemma, that is, by using the division polynomial $\psi_n$ we can determine $d$ in the case that $a_E^2 - 4q \equiv 0 \pmod{n}$. We now have an algorithm to compute $d$. We summarize below.

ALGORITHM 1. *Suppose that* $a, b, q$, *and* $n$ *have been given.*

1. *Compute* $a_E = (1+q) - \#E(\mathbb{F}_q)$ *by computing* $\#E(\mathbb{F}_q)$ *(Sec. 5.1)*
2. *Let* $c = \left(\frac{a_E^2-4q}{n}\right)$, *where* $\left(\frac{-}{n}\right)$ *is the Legendre symbol.*
3. *If* $c = 1$, *then* $T^2 - a_E T + q \equiv (T-\alpha)(T-\beta) \pmod{n}$, *where* $\alpha \neq \beta \in \mathbb{F}_n$, *and*
   $d = \mathrm{lcm}(\mathrm{ord}(\alpha, n), \mathrm{ord}(\beta, n))$
   *else if* $c = -1$, *then* $T^2 - a_E T + q \equiv (x-\alpha)(x-\alpha^n) \in \mathbb{F}_{n^2}$, *and*
   $d =$ *order of* $\alpha$ *in* $\mathbb{F}_{n^2}^{\times}$.
   *else if* $c = 0$, *then* $T^2 - a_E T + q \equiv (T-\alpha)^2, \alpha \in \mathbb{F}_n$. *Then*
   1. $d^* = ord(\alpha, n)$.
   2. $T^2 - a_E T + q = (T-\delta)(T-\gamma) \in \mathbb{C}[x]$.
   3. *If* $n^2 | (1+q^{d^*}) - (\delta^{d^*} - \gamma^{d^*})$ *then*
      1. *Construct* $\psi_n$.
      2. *Factor* $\psi_n$ *in* $\mathbb{F}_q[x]$.
      3. *Let* $l = \mathrm{lcm}(\{\deg(f_i)\}_{i=1}^r)$ *where* $\psi_n = f_1 \cdots f_r$.
      4. *if* $d^* = l$ *or* $d^* = 2l$ *then*
         $d = d^*$.
         *else*
         $d = nd^*$
         *end if*
      *else*
      $d = nd^*$
      *end if*
   *end if*

As we can see, fundamental to Algorithm 1 is $a_E$. By definition, computing $a_E$ is equivalent to computing $\#E(\mathbb{F}_q)$. However, computing the number of points on an elliptic curve over a finite field $K = \mathbb{F}_q$, even when $q = p$, is a non-trivial matter for large $p$. Since the appearance of R. Schoof's ground breaking paper [**Sc1**] on this topic, much work has gone into this question. For a nice expository paper on a variety of methods to compute $\#E(\mathbb{F}_p)$ one is recommended to check out another of Schoof's papers [**Sc2**]. In this second paper, Schoof claims that for prime $p < 200$, a simple brute force method of counting points on the curve is efficient. For $p > 200$, a less naive method must be used. Hence, to use Algorithm 1 for large $p$, one will need to first implement an efficient algorithm for computing $\#E(\mathbb{F}_p)$.

If $n$ is large compared to $q$, we note that Theorem 2.14 says that we can determine $d$ solely from the characteristic polynomial without recourse to $\psi_n$. Specifically, if $n > 4q$ or if $\left(\frac{q}{n}\right) = -1$, then the problem case will not occur.

We conclude our discussion of Algorithm 1 by providing an example of two curves with the same $a_E$ and $a_E^2 - 4q \equiv 0 \bmod n$, but the degree of their field of $n$-torsion points differ by a factor of $n$.

**Example 4.2:** Let $E_1 : y^2 = x^3 + 2$ and $E_2 : y^2 = x^3 + 6x + 2$. Also, let $q = 7$, so $K = \mathbb{F}_7$, and $n = 3$. Then, by counting the number of $K$-rational points on each curve, we find that $a_E = -1$ for both $E_1$ and $E_2$. So, the characteristic polynomials are equal modulo $n$, that is

$$\begin{aligned} ch_{\rho(\sigma_q, E_1)}(T) &\equiv ch_{\rho(\sigma_q, E_2)}(T) \\ &\equiv (T - \alpha)^2 \mod n \end{aligned}$$

Both matrices have repeated eigenvalues since $\left(\frac{a_E^2 - 4q}{n}\right) = 0$. In this example, $\alpha \equiv 1 \pmod 3$, since $\alpha^2 \equiv q \pmod 3$ and $q \equiv 1 \pmod 3$. Since $\mathrm{ord}(\alpha, 3) = 1$, then $[K_{E_1,3} : K] = 1$ or 3 by Theorem 2.14. Similarly for $[K_{E_2,3} : K]$. Forming the 3-division polynomials for each curve and factoring over $\mathbb{F}_q[x]$, we get

$$\begin{aligned} \psi_{3,E_1} &\equiv 3x^4 + 24x \\ &\equiv 3x(x+4)(x+2)(x+1) \pmod 7, \end{aligned}$$

and

$$\begin{aligned}\psi_{3,E_2} &\equiv 3x^4 + 36x^2 + 24x - 36 \\ &\equiv (x+1)(3x^3 + 4x^2 + 4x + 6) \pmod 7.\end{aligned}$$

From $\psi_{3,E_1}$ we deduce that $[K_{E_1,3} : K] = 1$. Moreover, from $\psi_{3,E_2}$ we see that $[K_{E_2,3} : K] = 3$.

Observe also that the curve $E_2 : y^2 = x^3 + 6x + 2$ is a counterexample to the converse of Proposition 2.16. Since $a_{E_2} = -1$, we can deduce that $3^2 \mid 9 = \#E(\mathbb{F}_q)$. However, $d \neq 1$, but $d = 3$, as we have just shown.

## 2. Algorithm 2

Algorithm 2 is a continuation of the discussion begun at the end of Chapter 3 where we showed that if $\psi_n = f_1 \cdots f_r$ in $K[x]$, then $d = l$ or $d = 2l$, where $l = \text{lcm}(\{\deg(f_i)\}_{i=1}^r)$. To determine if $d = l$, we need to show that for every $x_i \in \overline{K}$ such that $x_i$ is a root of $\psi_n^2$, then $y_i = \sqrt{x_i^3 + ax_i + b} \in \mathbb{F}_{q^l}$. If there is some $x_j$ where $y_j \notin \mathbb{F}_{q^l}$, then $y_j \in \mathbb{F}_{q^{2l}}$, implying that $d = 2l$.

Thus, to distinguish between $d = l$ and $d = 2l$, we need to check whether $x^3 + ax + b$ is a square in $\mathbb{F}_{q^l}$, where $x$ is a root of $\psi_n$. In the next definition, we define a function analogous to the Legendre symbol for arbitrary finite fields.

**Definition 4.3:** Let $K = \mathbb{F}_q$, and $x \in K$. Then the *quadratic character* $\left(\frac{}{K}\right)$ is defined as follows:

$$\left(\frac{x}{K}\right) = \begin{cases} 1 & \text{if } \exists y \in K \text{ such that } y^2 = x \\ -1 & \text{if } \nexists y \in K \text{ such that } y^2 = x \\ 0 & \text{if } x = 0. \end{cases}$$

So, to distinguish between $d = l$ and $d = 2l$, we need to evaluate

$$\left(\frac{x_i^3 + ax_i + b}{\mathbb{F}_{q^l}}\right)$$

for each root $x_i$ of $\psi_n^2$. Recall from Theorem 3.6, $d = 2l$ if there exists at least one $x_i$ such that $y_i \notin \mathbb{F}_{q^l}$. So, to determine $d$, we need to determine if all $y_i \in \mathbb{F}_{q^l}$.

However, we notice that $x_i$ is the root of some $f_i$, where $f_i$ is an irreducible factors of $\psi_n$ in $K[x]$. Let $d_i = \deg(f_i)$. Then $y_i^2 = x_i^3 + ax_i + b \in \mathbb{F}_{q^{d_i}}$ since $f_i$ is the minimal polynomial of $x_i$ over $K$. If $2d_i | l$, then all the $x \in \mathbb{F}_{q^{d_i}}$ have a

square root in $\mathbb{F}_{q^l}$. So, in particular, $y_i \in \mathbb{F}_{q^l}$. Thus, if $x_i$ is the root of $f_i$ such that $2d_i|l$, then $y_i \in \mathbb{F}_{q^l}$. So, we need only consider all $x_i$ such that $x_i$ is the root of an irreducible factor $f_i$ such that $2d_i \nmid l$. It is clear that such a factor will exist since $l = \text{lcm}(\{\deg(f_i)\}_{i=1}^r)$.

In next lemma, we show that we can find $d$ if we consider only one irreducible factor $f_i$ of $\psi_n$, such that $2d_i \nmid l$. Moreover, this result uses the partial solution of Theorem 1.11

LEMMA 4.4. *Let $f_i$ be an irreducible factor of $\psi_n$ such that $2d_i \nmid l$, where $d_i = deg(f_i)$. Put $d^* = lcm(ord(q,n), d_i)$ and $c = \left(\frac{x_i^3+ax_i+b}{\mathbb{F}_{q^{d_i}}}\right)$, where $f_i(x_i) = 0$. Then,*

$$d = \begin{cases} l & \text{if } c = 1 \text{ and } d^*|l \\ 2l & \text{otherwise.} \end{cases}$$

PROOF. Recall that $d = l$ or $2l$ and that $\text{ord}(q,n)|d$. Then, if $d^* \nmid l$, then $d \neq l$, so $d = 2l$. Similarly, if $c = -1$, then by the definition of the quadratic character, $y_i \notin \mathbb{F}_{q^{d_i}}$, thus implying that $y_i \in \mathbb{F}_{q^{2d_i}}$. Since $y_i \in K_{E,n} = \mathbb{F}_{q^d}$, then $2d_i|d$. But $2d_i \nmid l$, so $l \neq d$, hence $d = 2l$.

If $c = 1$ and $d^*|l$, then $P = (x_i, y_i) \in \mathbb{F}_{q^{d_i}}$, so $\mathbb{F}_{q^{d^*}} = K(P, \zeta_n)$. Thus, by Theorem 1.11, $d = d^*$ or $d = nd^*$. Then if $d = 2l$, either $2l = d^*$ or $2l = nd^*$. But in both case, $d^* \nmid l$. Thus, $d = l$. □

Notice that this proof makes implicit use of the fact that $n \geq 3$. We now have a way to determine $d$ from the way the division polynomial factors by using this lemma. We now explicitly write out our algorithm.

ALGORITHM 2. *Suppose that $n, q, a$, and $b$ have been given.*

1. *Construct $\psi_n$.*
2. *Factor $\psi_n = f_i \cdots f_r$ into its irreducible factors over $\mathbb{F}_q[x]$*
3. *Calculate $l = \text{lcm}(\{\deg(f_i)\}_{i=1}^r)$.*
4. *Pick an $f_i$, where $2\deg(f_i) \nmid l$.*
5. *Calculate $c = \left(\frac{x_i^3+ax_i+b}{\mathbb{F}_{q^{d_i}}}\right)$ where $d_i = deg(f_i)$ and $x_i \in \overline{K}$ is a root of $f_i$.*
6. *If $c = -1$ then*
   *$d = 2l$.*
   *else*
   *Put $d^* = \text{lcm}(\text{ord}(q,n), d_i)$.*
   *if $l = d^*$ or $l = nd^*$ then*
   *$d = l$.*

*else*
$d = 2l$.
*end if.*
*end if.*

An immediate problem one will encounter when trying to implement Algorithm 2 is the factorization of $\psi_n$ in $\mathbb{F}_q[x]$ in Step 2. By Lemma 3.2, we know that $\psi_n^2$ behaves like

$$\psi_n^2 = nx^{n^2-1} + \text{lower order terms}$$

as a polynomial in $x$. That is, the degree of the division polynomials grows like $n^2$. Thus, Algorithm 2 would seem suited for small $n$. Compare this to Algorithm 1 which works well for large $n$ compared to $q$. In the next chapter we will provide a more detailed comparison of the algorithms for various $n$ and $q$ when $q = p$ is a prime.

In the next chapter, we discuss in more detail the computation of $\left(\frac{x^3+ax+b}{\mathbb{F}_{q^d}}\right)$ of Step 5. We will see in Proposition 5.2 that quadratic residues in a field extension can be related to quadratic residues in subfields. We will also look into the implementation of these algorithms when $K = \mathbb{F}_p$. As well, we consider the question of computing $d$ for all elliptic curves over the finite field $\mathbb{F}_p$. For now, we conclude this chapter with a brief discussion concerning the case $n = 2$.

## 3. $[K_{E,n} : K]$ when $n = 2$

In the preceding, we avoided the discussion of the case $n = 2$. This is not because this case is more difficult than when $n \geq 3$. In fact, rather the opposite is true. Recall that a 2-torsion point is a point $P$ such that $2P = \mathcal{O}$, or alternatively, $P = -P$. But now if $Q = (x, y)$, then $-Q = (x, -y)$. This implies that $P$ is a 2-torsion point if and only if $y = 0$. Hence, the $x$-coordinates of the 2-torsion points are merely the roots of

$$y = \sqrt{x^3 + ax + b}.$$

Notice that agrees with our criterion of Corollary 3.5 that the $x$-coordinates of the $n$-torsion points are the roots of $\psi_n$ since $\psi_2 = 2y$.

There are three ways in which $f(x) = x^3 + ax + b$ factors over $K = \mathbb{F}_q$. First, all three roots are in $K$, that is,

$$x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3).$$

In this case, $E[2] \leq E(\mathbb{F}_q)$, that is, $d = 1$. In the second case, only one root is in $K$. But then

$$x^3 + ax + b = (x - e_1)(x^2 + sx + t).$$

Then, $K_{E,2} = \mathbb{F}_{q^2}$. In the finally case, $f(x)$ is irreducible. But then $K_{E,2} = \mathbb{F}_{q^3}$. Thus, the case $n = 2$ is ignored in this project since the solution is relatively straight forward.

CHAPTER 5

# Implementing the Algorithms

In this penultimate chapter we describe the implementation of the two algorithms described in Chapter 4. In particular, we discuss the implementation when $K = \mathbb{F}_p$. We describe some methods that will decrease the run time of the algorithms. As well, we point out some possible problems one may encounter. We also compare the running time of the two algorithms for various $n$ and $p$. Finally, we discuss the problem of computing the degree $d = [K_{E,n} : K]$ for *all* elliptic curves over $K = \mathbb{F}_p$.

**Remark:** We emphasize the fact that the algorithms we implemented assume that $K = \mathbb{F}_p$. While the algorithms are true for $K = \mathbb{F}_{p^r}$, implementation becomes difficult since we need to utilize the arithmetic of $\mathbb{F}_{p^r}$. Furthermore, both algorithms were implemented in Maple V Release 4 on a Packard Bell Pentium/66 using Windows 3.1. Since some of the discussions of the chapter hold for $q = p^r$, we continue with this generality, specializing to $p$ only when necessary.

## 1. Implementation of Algorithm 1

As noted in Section 4.1, one of the major stumbling blocks of this algorithm is the computation of $a_E$, or equivalently, of $\#E(\mathbb{F}_q)$. If $E$ is an elliptic curve over $\mathbb{F}_q$ given in Weierstrass form, i.e.,

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

then for every $x \in \mathbb{F}_q$, there exist either $0, 1$, or $2$ solutions for $y$. The number of solutions of $y$ is determined by

$$1 + \left(\frac{x^3 + ax + b}{\mathbb{F}_q}\right),$$

where $\left(\frac{}{\mathbb{F}_q}\right)$ is the quadratic character defined in Definition 4.3. In the case that $q = p$, then the symbol on the right is the well known Legendre symbol. As Schoof

points out in his paper [**Sc2**], if we sum the above expression over all $x \in \mathbb{F}_q$, remembering to count the point at infinity, we have

$$\#E(\mathbb{F}_q) = 1 + q + \sum_{x \in \mathbb{F}_q} \left( \frac{x^3 + ax + b}{\mathbb{F}_q} \right).$$

From this, we deduce that

$$a_E = -\sum_{x \in \mathbb{F}_q} \left( \frac{x^3 + ax + b}{\mathbb{F}_q} \right). \tag{8}$$

Hence, to calculate $a_E$, one can use the above expression.

In the case that $q = p$ and for $p > 200$ there do exist more efficient algorithms. For a variety of methods, see [**Sc2**], [**Sc1**], and [**At**]. However, for this paper we have stayed within this bound, i.e., we have chosen to work with primes $p < 200$. In this context, this brute force method is efficient enough for computing $a_E$. To further increase efficiency, we first compile a table of a squares modulo $p$. Then, for each $x = 0, 1, \ldots, p-1$, we check if $x^3 + ax + b$ is in this list. As Schoof claims in [**Sc2**], this provides us with an algorithm with a running time of $O(p^{1+\epsilon})$ for every $\epsilon > 0$. For those who wish to deal with the problem of calculating $d$ when $p > 200$, it will be first necessary to implement a quicker method for counting $\#E(\mathbb{F}_p)$. Our implementation of Algorithm 1 makes use of (8) to calculate $a_E$.

We also consider the case that $\left( \frac{a_E^2 - 4q}{n} \right) = -1$. As was shown in Theorem 2.14, under this hypothesis $d$ is equal to the order of $\alpha \in \mathbb{F}_{n^2}$, where $\alpha$ is a root of

$$f(T) \equiv T^2 + a_E T + q \pmod{n}.$$

Of course, to calculate the order of $\alpha$ we need to first construct $\mathbb{F}_{n^2}$ and identify $\alpha$ with an element in this field. To construct $\mathbb{F}_{n^2}$, we use the fact that $f$ is irreducible in the ring $\mathbb{F}_n[T]$. Hence

$$\mathbb{F}_{n^2} \cong \frac{\mathbb{F}_n[T]}{(f)}.$$

Since $f(\alpha) \equiv 0 \pmod{n}$ we have $T \equiv \alpha \pmod{f}$. So, we need to discern the order of $T$ in $\mathbb{F}_n[T]/(f)$, i.e., find the minimum of all $d$ such that $T^d \equiv 1 \pmod{f}$. In our implementation, we have used `GF`, the finite field Maple package to calculate $d$.

We observe that Algorithm 1 relies on $\psi_n$ to distinguish between the two possible values for $d$ in the case that $a_E^2 - 4q \equiv 0 \pmod{n}$. As noted in Lemma 3.2, $\psi_n$ is a polynomial of degree $\frac{n^2-1}{2}$. This is unfortunate since this implies that the

degree grows at very rapid rate. The question arises if there are any alternatives to $\psi_n$.

The answer to this question is yes. The *modular equation* $\Phi_n(S,T) \in \mathbb{Z}[S,T]$ where $n$ is prime is a possible candidate for an alternative to $\psi_n$. The modular equation is a symmetric polynomial which is equal to

$$\Phi_n(S,T) = S^{n+1} - S^n T^n + T^{n+1} + \text{lower order terms},$$

where the lower order term are of the form $S^i T^j$ with $i, j \leq n$ and $i + j < 2n$. The modular equation also satisfies

$$\Phi_n(S,T) \equiv (S^n - T)(T - S^n) \pmod{n}.$$

This relationship is called the *Kronecker congruence relation*. Let $E$ be an elliptic curve over $K = \mathbb{F}_p$ and suppose that the $j$-invariant is such that $j \neq 0, 1728$. Substituting $j$ for $S$ in $\Phi_n(S,T)$, we a get a new polynomial $\Phi_n(j,T)$ which is a polynomial strictly in $T$ and of degree $n+1$. Moreover, we have

PROPOSITION 5.1. *The polynomial $\Phi_n(j,T)$ splits completely in $\mathbb{F}_{p^r}[T]$ if and only if $\rho_n(\sigma_q)^r$ acts as a scalar matrix on $E[n]$ in $GL_2(\mathbb{Z}/n\mathbb{Z})/\pm 1 \cong PGL_2(\mathbb{Z}/n\mathbb{Z})$.*

PROOF. See [**Sc2**] 6.1. □

But now consider how this proposition can improve Algorithm 1. In Algorithm 1 we use $\psi_n$ to determine if $\rho_n(\sigma_q)$ is similar to a diagonal matrix or not. But by Proposition 5.1, if $\Phi_n(j,T)$ splits in $\mathbb{F}_p[T]$, then $\rho_n(\sigma_q)$ acts as a scalar matrix on $E[n]$ in $PSL_2(\mathbb{Z}/n\mathbb{Z})$, or in other words, the dimension of the eigenspace is 2. Notice that there will be a marked improvement in the algorithm since the degree of $\Phi_n(j,T)$ grows at a linear rate.

Unfortunately, while using the modular equation will increase the running time, no nice method exists for constructing $\Phi_n(S,T)$. Unlike $\psi_n$, there is no recursive definition for $\Phi_n(S,T)$. Another problem with this polynomial is that the coefficients have a tendency to become very large. For example, consider the modular

equation $\Phi_n(S,T)$ with $n=3$:

$$\begin{aligned}\Phi_3(S,T) &= S^4+S^3T^3+T^4+2232(S^3T^2+T^3S^2)\\ &\quad -1069956(S^3T+T^3S)+36864000(S^3+T^3)\\ &\quad +2587918086S^2T^2+8900222976000(S^2T+T^2S)\\ &\quad +452984832000000(S^2+T^2)-770845966336000000ST\\ &\quad +1855425871872000000000(S+T).\end{aligned}$$

Of course, we only need to calculate the coefficients modulo $p$. For a discussion of the problem of computing these coefficients over $\mathbb{Z}$, see Yui's paper [**Yu**]. Whether $\Phi_n(S,T)$ presents a viable alternative to $\psi_n$ remains to be seen. Further, one may ask whether there exist other polynomials that can be used to distinguish between the two possible values of $d$.

## 2. Implementation of Algorithm 2

Suppose that $\psi_n$ is the $n^{th}$ division polynomial, and that $\psi_n$ factors in $\mathbb{F}_q[x]$ as

$$\psi_n = f_1 \cdots f_r.$$

If $d_i = \deg(f_i)$ and $l = \operatorname{lcm}(\{d_i\}_{i=1}^r)$, we know from Theorem 3.6 that $d = l$ or $d = 2l$. In Algorithm 2 we distinguish between these two possibilities. If $f_i$ is an irreducible factor such that $2d_i \nmid l$, then this distinction boils down to the computation of

$$\left(\frac{x_i^3+ax_i+b}{\mathbb{F}_{q^{d_i}}}\right), \tag{9}$$

where $f_i(x_i)=0$ and

$$\mathbb{F}_{q^{d_i}} \cong \frac{\mathbb{F}_q[x]}{(f_i)}.$$

Here, $\left(\frac{}{\mathbb{F}_{q^{d_i}}}\right)$ is the quadratic character. This section describes how one evaluates this expression.

As remarked at the end of Section 4.2, but not proved, quadratic residues in a field extension can be related to quadratic residues in subfields. We now prove this statement.

PROPOSITION 5.2. *Let $H \supset F$ be finite fields of characteristic $p \neq 2$ and $[H : F] = m$. Let $x \in H$. Then*

$$\left(\frac{x}{H}\right) = \left(\frac{N_{H/K}(x)}{F}\right)$$

*where $N_{H/K}(x) = x^{\Sigma}$ is the* norm *of $x$. Here, $\Sigma = \frac{q^m-1}{q-1}$, where $q = |F|$.*

PROOF. This result is based upon Exercise 1.12 in [**Sm**]. Suppose that $\left(\frac{x}{H}\right) = 1$. Then there exists $y \in H$ such that $y^2 = x$. But then $N_{H/F}(x) = N_{H/F}(y^2) = N_{H/F}(y)^2$. Since $N_{H/F}(y) \in F$, we must have $\left(\frac{N_{H/F}(x)}{F}\right) = 1$.

Conversely, suppose that $\left(\frac{N_{H/F}(x)}{F}\right) = 1$. Let $x = g^t$, where $g$ is a primitive element of $H$. We want to show that $t$ is even. Since $\left(\frac{N_{H/F}(x)}{F}\right) = 1$, there exists $y \in F$ such that $y^2 = N_{H/F}(x) = x^{\frac{q^m-1}{q-1}}$. So $1 = y^{q-1} = x^{\frac{q^m-1}{2}}$. Thus $1 = g^{t(q^m-1)/2}$. Since $g$ has order $q^m - 1$, we have $2|t$. □

Applying this proposition to the calculation of (9), we see that we only need to evaluate

$$\left(\frac{N_{\mathbb{F}_{q^{d_i}}/\mathbb{F}_q}(x_i^3 + ax_i + b)}{\mathbb{F}_q}\right),$$

where $\left(\frac{}{\mathbb{F}_q}\right)$ is the quadratic character. But if we now specialize to $q = p$, we need to evaluate

$$\left(\frac{N_{\mathbb{F}_{p^{d_i}}/\mathbb{F}_p}(x_i^3 + ax_i + b)}{p}\right),$$

where $\left(\frac{}{p}\right)$ is the Legendre Symbol. So, using Algorithm 2 involves the evaluation of $N_{\mathbb{F}_{p^{d_i}}/\mathbb{F}_p}(x_i^3 + ax_i + b)$. (We drop the subscript $\mathbb{F}_{p^{d_i}}/\mathbb{F}_p$ for the remainder of our discussion.) Recall that if $\alpha \in \mathbb{F}_{p^{d_i}}$, then $N(\alpha) \equiv \alpha^{\frac{p^{d_i}-1}{p-1}} \pmod{p}$. Unfortunately, as both $p$ and $d_i$ increase, the calculation of $N(\alpha)$ can become very involved! However, we can make use of the fact that $f_i$ is the minimal polynomial of $x_i$. The next proposition shows that calculating $N(x_i^3 + ax_i + b)$ is equivalent to evaluating

$$(-1)^{d_i} f_i(e_1) f_i(e_2) f_i(e_3),$$

where the $e_i$'s are the three roots of $x^3 + ax + b$.

PROPOSITION 5.3. *Let $H/F$ be a finite field extension of degree $n$, $\alpha \in H$, and $f(x) = char_{\alpha/F}(x) = \prod_{i=1}^{n}(x - \alpha_i)$ where $\alpha_i \in \overline{H}$. Then for every $g(x) \in F[x]$,*

1) $char_{g(\alpha)/F}(x) = \prod_{i=1}^{n}(x - g(\alpha_i))$

2) $N_{H/F}(g(\alpha)) = \prod_{i=1}^{n} g(\alpha_i) = c^m(-1)^{nm}\prod_{j=1}^{m} f(\beta_j)$
*where* $g(x) = c\prod_{j=1}^{m}(x-\beta_j)$ *in* $\overline{F}[x]$.

PROOF. By definition we have

$$char_{g(\alpha)/F}(x) = char_{g(A)}(x)$$

where $A$ is any $n \times n$ matrix representing the endomorphism $\lambda \mapsto \alpha\lambda \in \mathrm{End}_F(H)$. Now, for any matrix $A$,

$$char_{g(A)}(x) = \prod_{i=1}^{n}(x - g(\alpha_i))$$

by the Jordan Canonical Form ([**HoKu**] 7.3), so 1) follows.

For 2), by definition, for any $\beta \in H$,

$$N_{H/F}(\beta) = (-1)^n char_{\beta/F}(0).$$

Thus, by 1),

$$\begin{aligned} N_{H/F}(g(\alpha)) &= (-1)^n\prod_{i=1}^{n}(-g(\alpha_i)) = \prod_{i=1}^{n} g(\alpha_i) \\ &= \prod_{i=1}^{n}\prod_{j=1}^{m} c(\alpha_i - \beta_j) = c^n\prod_{j=1}^{m}\prod_{i=1}^{n}(\alpha_i - \beta_j) \\ &= c^n(-1)^{nm}\prod_{j=1}^{m}\prod_{i=1}^{n}(\beta_j - \alpha_i) = c^n(-1)^{nm}\prod_{j=1}^{m} f(\beta_j) \end{aligned}$$

This gives us the desired result. □

COROLLARY 5.4. *Suppose that* $f(x) = x^3 + ax + b$ *is a polynomial over* $K = \mathbb{F}_q$ *and that* $f$ *factors in* $\overline{K}[x]$ *as*

$$x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3).$$

*Suppose further that* $f_i$ *is an irreducible factor of* $\psi_n$, $d_i = \deg(f_i)$, *and* $f(x_i) = 0$. *Let* $\mathbb{F}_{q^{d_i}} = \mathbb{F}_q[x]/(f_i)$. *Then*

$$\left(\frac{x_i^3 + ax_i + b}{\mathbb{F}_q^{d_i}}\right) = \left(\frac{(-1)^{d_i}\prod_{j=1}^{3} f_i(e_j)}{\mathbb{F}_q}\right).$$

To further shorten the running time of this algorithm, we can impose the condition that we pick $f_i$ such that $d_i$ is minimal among all $d_i$ such that $2d_i \nmid l$. When we implemented Algorithm 2, we used this corollary to evaluate (9).

However, in some cases it is not necessary to go all the trouble of computing the quadratic character in (9). In fact, we can sometimes determine $d$ from the way $\psi_n$ factors in $\mathbb{F}_p[x]$, or more precisely, from the way $\psi_n$ does not factor.

PROPOSITION 5.5. *Let $E$ be an elliptic curve of $\mathbb{F}_q$, and $n \neq char(K)$ is prime. Suppose that the division polynomial $\psi_n$ of $E$ is irreducible in $\mathbb{F}_q[x]$. Then $\left(\frac{a_E^2-4q}{n}\right) = -1$. Furthermore, if $ord(q,n) = n-1$, then $d = n^2-1$. Otherwise, $d = \frac{(n^2-1)}{2}$.*

PROOF. Since $\psi_n$ is irreducible, $l = \deg(\psi_n) = \frac{(n^2-1)}{2}$. So $d = \frac{(n^2-1)}{2}$ or $d = n^2-1$. If $\left(\frac{a_E^2-4q}{n}\right) = 1$, then by Corollary 2.15, $d|(n-1)$. However, neither $\frac{(n^2-1)}{2}$ nor $(n^2-1)$ meet this condition. Similarly, if $\left(\frac{a_E^2-4q}{n}\right) = 0$, then $d|n(n-1)$. But again, neither of our two possible values meet this criterion. Thus, the first statement follows.

To prove the second statement, we recall the $d|\operatorname{ord}(q,n)(n+1)$ by Corollary 2.15. So, if $\operatorname{ord}(q,n) < (n-1)$, then it must be the case that $d = \frac{(n^2-1)}{2}$. Finally, if $\operatorname{ord}(q,n) = n-1$ we show that $d = n^2-1$. Suppose, to the contrary, that $d = \frac{(n^2-1)}{2}$. Then $\alpha^d = \alpha^{\frac{(n^2-1)}{2}} = 1 \in \mathbb{F}_{n^2}$, where $\alpha$ is a solution to

$$T^2 - a_E T + q \equiv 0 \pmod{n},$$

that is, $\alpha$ is one of the eigenvalues of $\rho_n(\sigma_q)$. But $\alpha^{\frac{(n^2-1)}{2}} = 1 \in \mathbb{F}_{n^2}$ implies that $\alpha$ is a square in $\mathbb{F}_{n^2}$. But then, by Proposition 5.2,

$$1 = \left(\frac{\alpha}{\mathbb{F}_{n^2}}\right) = \left(\frac{N(\alpha)}{\mathbb{F}_n}\right) = \left(\frac{\alpha\alpha^n}{\mathbb{F}_n}\right) = \left(\frac{q}{n}\right).$$

But the last statement implies that $\left(\frac{q}{n}\right) = 1$, or in other words, $q^{\frac{n-1}{2}} \equiv 1 \pmod{n}$. But this contradicts the hypothesis that $\operatorname{ord}(q,n) = n-1$. So, $d = n^2-1$. □

From this proposition, we see that we can determine $d$ in some cases from the way $\psi_n$ factors in the ring $\mathbb{F}_q[x]$. This produces a considerable savings in the running time of Algorithm 2 since we avoid the process of calculating norms. It is hoped, but not known, that there exist other such short cuts, i.e., methods of determining $d$ strictly from the way $\psi_n$ factors. Our implementation of Algorithm 2 incorporated this proposition by first checking if $\psi_n$ was irreducible in $\mathbb{F}_p[x]$; if it was, then we would use this result to calculate $d$.

Before we continue with the next section, we note that one of the most time consuming pieces of this algorithm is the factorization of $\psi_n$ in the the polynomial ring $\mathbb{F}_p[x]$. To increase the overall efficiency of the algorithm, an efficient algorithm for factoring in $\mathbb{F}_p[x]$ should be used.

## 3. A Comparison of the two Algorithms

In this section we compare the performance of the two algorithms. For our test curve, we will use the INRIA curve

$$E : y^2 = x^3 + 105x + 78153,$$

which was first named and studied by Atkin [**At**]. The curve is inspired by the address of the INRIA institute: Domaine de Voluceau-Rocquencurt, B.P. 105, 78153 Le Chesney cedex. The curve was first used by Atkin in computing $\#E(\mathbb{F}_p)$, where $p$ was the first 200 digit prime. See [**Sc2**] and [**At**] for a discussion of this topic.

It should be noted that the above curve is not an elliptic curve when the $\text{char}(K) = p$ divides the discriminant of $E$. As usual, the discriminant is defined to be $\Delta = -16(4a^3 + 27b^2)$. Now, for the INRIA curve we have

$$\Delta = -16(4(105)^3 + 27(78153)^2) = -(2)^4(3)^3(13)(167)(2813479).$$

Therefore, if $p \neq 2, 3, 13, 167$, or 2813479, then the INRIA curve is an elliptic curve over $\mathbb{F}_p$.

As noted, both algorithms were implemented for the case $K = \mathbb{F}_p$ in Maple V Release 4 on a Packard Bell Pentium/66 using Windows 3.1 as its operating system. In comparing the algorithms, we stayed within a small window of allowable input. That is, we compared the algorithms for all primes $p, n < 101$. In comparing the two algorithms, the first thing we immediately noticed was that Algorithm 1 is vastly superior to Algorithm 2.

When using Algorithm 1, we found that for a fixed $n$, whether $n = 5, 53$, or 101, for all $p < 101$ the algorithm took less than 1 second of CPU time. Even if $p < 200$ the algorithm still needed less than 2 seconds of CPU time. However, as $p$ increased, there was a marked difference in running time. In fact, there appears to be a linear increase in running time as $p$ grows, as evident in Figure 1. This is due mainly to the fact that the calculation of $a_E$ grows at roughly a linear rate. However,

FIGURE 1. Algorithm 1 for the INRIA curve: $p$ versus CPU Time (seconds), when $n = 5$.

when we fixed $p$ and varied $n$, we found that in most case the time involved stay constant, regardless of the value of $n$. For example, when we fixed $p = 53$ and let $n$ run through all the primes less than 100 (Figure 2), we found that in the majority of cases, the time involved was between 0.25 and 0.3 seconds CPU time.

Algorithm 2 was a completely different story. For $n > 20$, Algorithm 2 rarely completed under 60 seconds of CPU time, regardless of the value of $p$. We did find, however, that when we fixed $n$ and varied $p$ over all all primes $< 200$, the time involved stayed relatively constant. For example, for $n = 17$, Algorithm 2 took roughly 40 seconds to finish for most of the primes under 100 (Figure 3). Swapping the place of $n$ and $p$, that is, fixing $p$ and varying $n$, we found that as $n$ increased, the time needed for the algorithm to quit grew exponentially. Indeed, when we tried the case that $p = 5$ and varied $n$, we found for all $n \leq 23$ the time involved was less then 30 seconds. For $n > 23$, the time involved jumped up past 5 minutes of CPU time (Figure 4).

FIGURE 2. Algorithm 1 for the INRIA curve: $n$ versus CPU Time (seconds), when $p = 5$.

In the appendix, we compute $d$ for all elliptic curves (up to $\mathbb{F}_p$-isomorphism) over the finite field $\mathbb{F}_p$. We do this for all $n, p \leq 37$. We also included the total running time for the algorithms to calculate $d$ over all curves. As well, the average time for computing $d$ for each curve is included. We see from these table that the observed times for INRIA curve are similar to the average times.

It should be duly noted that each algorithm incorporated some of the inbuilt Maple procedures. This prevents us from declaring Algorithm 1 the better method since it is not clear whether the Maple code can be further optimized. This may the case for Algorithm 2. Algorithm 2 relies, in part, on Maple's subroutine for factoring polynomials over finite fields. Better algorithms may exist though this question was not fully looked into. Of course, one way to increase the efficiency of both algorithms is to divorce them from symbolic programs like Maple or Mathematica and rewrite them completely as specialized programs.

FIGURE 3. Algorithm 2 for the INRIA curve: $p$ versus CPU Time (seconds), when $n = 17$.

In general, it would appear that Algorithm 1 is the superior of the two methods. In fact, for most curves under the conditions we consider, i.e, $n, p < 100$ the runtime was usually less 2 seconds of CPU time. Algorithm 2 appears to be limited to very small $n$, due in part to its dependence upon the factoring of a polynomial over a finite field.

## 4. Finding all Elliptic Curves over $\mathbb{F}_q$

The material in this section will lead into the final chapter in we which count the number of $K$-isomorphism classes of curves $E$ over $K = \mathbb{F}_q$ whose field of $n$-torsion points have a given degree, that is,

$$Z_q(n, d) = \#\{E/K = \mathbb{F}_q : [K_{E,n} : K] = d\}/\simeq_K .$$

But to do so, we need a way in which to list all given curves up to $\mathbb{F}_q$-isomorphism. This is the focus of of this section.

FIGURE 4. Algorithm 2 for the INRIA curve: $n$ versus CPU Time (seconds), when $p = 5$.

Let $E$ be an elliptic curve over $K = \mathbb{F}_q$ given in Weierstrass form,

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

We can associate with every curve $E$ an invariant, called the *j-invariant*, where

$$j_E = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

If $j \in K$ and $j \neq 0, 1728$, we can construct a curve $E$ with this $j$-invariant, namely,

$$E_j : y^2 = x^3 - \frac{27j}{j - 1728}x + \frac{54j}{j - 1728}. \tag{10}$$

In fact, under the hypothesis that $j \neq 0, 1728$, then there are only two curves up to $K$-isomorphism over $K$ with this $j$-invariant: the above curve and its quadratic twist,

$$E_{j,twist} : y^2 = x^3 - \frac{27j}{j - 1728}g^2x + \frac{54j}{j - 1728}g^3,$$

where $g$ is not a square in $K$. For a more thorough analysis of twisting, see [**Si**] X.5.

The cases where $j = 0$ and $j = 1728$ are more involved. We see from the formula for $j_E$ that $j = 0$ if and only if $a = 0$, that is,

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

Over $K$, there may be 6 or 2 non-isomorphic curves with $j = 0$. More precisely, there are always $k = |\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^6|$ curves, and we have $k = 6$ if $q \equiv 1 \pmod 3$ and $k = 2$ if $q \not\equiv 1 \pmod 3$. If $q \equiv 1 \pmod 3$ these curves are

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

where $g \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^6$, that is, $g$ runs through the representatives of $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^6$. If $q \not\equiv 1 \pmod 3$, then there are only two curves, $E : y^2 = x^3 + 1$ and its quadratic twist $E' : y^2 = x^3 + g$, where $g$ is not a square in $\mathbb{F}_q$.

The case for $j = 1728$ is similar. We see that this situation occurs when $b = 0$, i.e,

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

There may be 2 or 4 curves with this $j$-invariant; the number is dependent upon the value $k = |\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^4|$. If $q \equiv 1 \pmod 4$, then $k = 4$. So the four curves with $j = 1728$ are

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

where $g \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^4$. If $q \not\equiv 1 \pmod 4$, then there are two curves, $E : y^2 = x^3 + x$, and its quadratic twist $E'$.

Therefore, to construct all curves $E$ over $K$, we can run through all $j \in \mathbb{F}_q$ and construct the corresponding curve using (10), or in the case that $j = 0$ and $j = 1728$, $E : y^2 = x^3 + 1$ and $E : y^2 = x^3 + x$ respectively. Then, depending upon the $q$, we form the twists of the curves. Observe that there will be at least $2q$ elliptic curves over $\mathbb{F}_q$ because for each $j \in \mathbb{F}_q$, there are at least two curves with this $j$-invariant. At most, however, there will be $2q + 6$ curves. This will occur when $q \equiv 1 \pmod{12}$. Under this hypothesis, there will be six curves of $j = 0$ and four curves with $j = 1728$. Adding this total to $2(q-2)$, the number of elliptic curves with $j \neq 0, 1728$, we get the desired result. In fact, we can write an explicit formula for the number of curves over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism:

$$\#\{\text{elliptic curves over } \mathbb{F}_q\}/\simeq = 2(q-2) + \left(4 + 2\left(\frac{q}{3}\right)\right) + \left(3 + \left(\frac{-1}{q}\right)\right),$$

where $\left(\frac{\cdot}{q}\right)$ is the Legendre symbol.

The method to construct the tables found in the appendix used this approach; for each $j \in \mathbb{F}_q$ we found the coefficients $a$ and $b$ of the curve $E_j$, storing the results in an array. Once all the coefficients had been found, we would pass each pair $a$ and $b$ to our algorithm to compute $d$.

However, as the next two propositions show, sometimes all that is necessary is to compute $d = [K_{E,n} : K]$ for one curve in the twist class. From this result, we may be able to deduce the degree $d' = [K_{E',n} : K]$ for the twist as well.

PROPOSITION 5.6. *Let $E$ be an elliptic curve over $K = \mathbb{F}_q$. Further, let $E'$ be the quadratic twist of $E$ over $K$, and suppose that $n \neq char(K)$. Then $a_E = -a_{E'}$.*

PROOF. Let $E$ be defined by $y^2 = x^3 + ax + b$ and $E'$, so $E'$ is given by $y^2 = x^3 + g^2ax + bg^3$ where $g$ is not a square in $\mathbb{F}_q$. But then by formula (8) of Chapter 5, we have

$$\begin{aligned} a_{E'} &= -\sum_{x \in \mathbb{F}_q} \left( \frac{x^3 + g^2ax + bg^3}{\mathbb{F}_q} \right) \\ &= -\sum_{gx \in \mathbb{F}_q} \left( \frac{(gx)^3 + g^2a(gx) + bg^3}{\mathbb{F}_q} \right) \\ &= -\left(\frac{g}{\mathbb{F}_q}\right) \sum_{x \in \mathbb{F}_q} \left( \frac{x^3 + ax + b}{\mathbb{F}_q} \right) \\ &= -a_E. \end{aligned}$$

□

PROPOSITION 5.7. *Let $E$ be an elliptic curve over $K = \mathbb{F}_q$. Let $E'$ be the quadratic twist of $E$ over $K$, and suppose that $n \neq char(K)$ is prime. Let $d = [K_{E,n} : K]$ and $d' = [K_{E',n} : K]$. Then*

1) *If $2 \nmid d$, then $d' = 2d$.*
2) *If $4|d$, then $d' = d$.*
3) *If $2|d$ but $4 \nmid d$, then*

$$d' = \begin{cases} \frac{d}{2} & \text{if } ord(q,n) \equiv 1 \pmod 2 \\ d & \text{if } ord(q,n) \equiv 0 \pmod 2 \end{cases}$$

PROOF. By Proposition 5.6, we have $a_E = -a_{E'}$. Let $\sigma_E$ be the Frobenius automorphism that generates $\mathrm{Gal}(K_{E,n}/K)$ and $\sigma_{E'}$ the automorphism that generates $\mathrm{Gal}(K_{E',n}/K)$. Furthermore, let $\overline{\rho}_n$ be the injective homomorphism from $\mathrm{Gal}(K_{E,n}/K)$ to $GL_2(\mathbb{Z}/n\mathbb{Z})$ as given in Corollary 1.6. Similarly, let $\overline{\rho}'_n$ be the injective homomorphism from $\mathrm{Gal}(K_{E',n}/K)$ to $GL_2(\mathbb{Z}/n\mathbb{Z})$. To prove this proposition, we need the following:

**Claim:**

$$\mathrm{ord}(\overline{\rho}_n(\sigma_E)) = \mathrm{ord}(-\overline{\rho}'_n(\sigma_{E'})).$$

We first observe that $\overline{\rho}_n(\sigma_E)$ is a solution to

$$T^2 - a_E T + q \equiv 0 \pmod{n}$$

and $\overline{\rho}'_n(\sigma_{E'})$ satisfies

$$T^2 + a_E T + p \equiv 0 \pmod{n}.$$

Factoring the above polynomials over $\overline{\mathbb{F}}_n[x]$ gives

$$(T-\alpha)(T-\beta) = 0 \quad \text{and} \quad (T+\alpha)(T+\beta) = 0$$

respectively. If $\overline{\rho}_n(\sigma_E)$ and $\overline{\rho}'_n(\sigma_{E'})$ are diagonable, we will have

$$\overline{\rho}_n(\sigma_E) \sim \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \quad \text{and} \quad \overline{\rho}'_n(\sigma_{E'}) \sim \begin{pmatrix} -\alpha & 0 \\ 0 & -\beta \end{pmatrix}.$$

From this we deduce that $\overline{\rho}_n(\sigma_E) \sim -\overline{\rho}'_n(\sigma_E)$, thereby implying that $\mathrm{ord}(\overline{\rho}_n(\sigma_E)) = \mathrm{ord}\ (-\overline{\rho}'_n(\sigma_{E'}))$ in $GL_2(\mathbb{Z}/n\mathbb{Z})$.

In the case that $\overline{\rho}_n(\sigma_E)$ and $\overline{\rho}'_n(\sigma_{E'})$ are not diagonable, we have

$$\overline{\rho}_n(\sigma_E) \sim \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix} \quad \text{and} \quad \overline{\rho}'_n(\sigma_{E'}) \sim \begin{pmatrix} -\alpha & 1 \\ 0 & -\alpha \end{pmatrix}.$$

In this case, $\overline{\rho}_n(\sigma_E) \not\sim -\overline{\rho}'_n(\sigma_{E'})$ but $\overline{\rho}_n(\sigma_E)^n \sim -\overline{\rho}'_n(\sigma_{E'})^n$. But from this we can deduce that $\mathrm{ord}(\overline{\rho}_n(\sigma_E)) = \mathrm{ord}(-\overline{\rho}'_n(\sigma_{E'}))$. This completes the proof of the claim.

To prove 1), we suppose that $2 \nmid d$. Then by the claim, we have that

$$\mathrm{ord}(-\overline{\rho}'_n(\sigma_{E'})) = \mathrm{ord}(-I_2)\,\mathrm{ord}(\overline{\rho}'_n(\sigma_{E'})) = d.$$

From this and the fact that $2 \nmid d$, we can deduce that

$$(-I_2)^d\,\overline{\rho}'_n(\sigma_{E'})^d = (-I_2)\,\overline{\rho}'_n(\sigma_{E'})^d = I_2.$$

So, $\overline{\rho}'_n(\sigma_{E'})^d = -I_2$ So, $d' = 2d$, and thus, 1) follows.

Now suppose that $4|d$. By the claim, we have the fact that

$$(-I_2)^d \overline{\rho}'_n(\sigma_{E'})^d = \overline{\rho}'_n(\sigma_{E'})^d = \overline{\rho}_n(\sigma_E)^d = I_2.$$

So, $d'|d$. We wish to show that $d' = d$. Suppose that $d' < d$. If $d'$ where even, then we would have an immediate contradiction since this implies that $\overline{\rho}_n(\sigma_E)^{d'} = I_2$ which is false. So suppose that $d'$ is odd. But then this implies $\overline{\rho}_n(\sigma_E)^{d'} = -I_2$ from which we deduce that $\overline{\rho}_n(\sigma_E)^{2d'} = I_2$. But this is a contradiction since the order of $\overline{\rho}_n(\sigma_E)$ has order divisible by 4, but $2d'$ does not have this property. Thus, 2) follows.

Finally, suppose that $2|d$ but $4 \nmid d$. We will first show that $d' = d$ or $d' = \frac{d}{2}$ where $d' = [K_{E',n} : K]$. We have

$$\mathrm{ord}(-\overline{\rho}'_n(\sigma_{E'})) = \mathrm{ord}(\overline{\rho}_n(\sigma_E)).$$

Therefore,

$$-I_2^d \overline{\rho}'_n(\sigma_{E'})^d = \overline{\rho}'_n(\sigma_{E'})^d = \overline{\rho}_n(\sigma_E)^d = I_2.$$

So, $\overline{\rho}'_n(\sigma_{E'})^d = I_2$ which implies that $d' = \mathrm{ord}(\overline{\rho}'_n(\sigma_{E'}))|d$. Now suppose that $d'$ is even. Since

$$\mathrm{ord}(\overline{\rho}'_n(\sigma_{E'})) = \mathrm{ord}(-\overline{\rho}_n(\sigma_E)),$$

this implies that

$$\overline{\rho}'_n(\sigma_{E'})^{d'} = -I_2^{d'} \overline{\rho}_n(\sigma_E)^{d'} = \overline{\rho}_n(\sigma_E)^{d'} = I_2.$$

Thus, $d|d'$, from which we deduce that $d' = d$.

Suppose that $d'$ is odd. Then

$$\overline{\rho}'_n(\sigma_{E'})^{d'} = -I_2^{d'} \overline{\rho}_n(\sigma_E)^{d'} = -I_2 \overline{\rho}_n(\sigma_E)^{d'} = I_2.$$

From this we deduce that $\overline{\rho}_n(\sigma_E)^{d'} = -I_2$ which implies that $2d' = d$. So, $d' = \frac{d}{2}$

We will now show that if we know the parity of $\mathrm{ord}(q, n)$, then we can distinguish between the two possibilities. We make use of the fact that $\mathrm{ord}(q, n)$ divides both $d$ and $d'$ by Corollary 1.10. Suppose that $\mathrm{ord}(q, n) \equiv 0 \pmod 2$. We wish to show that $d' = d$. Suppose not, i.e., $d' = \frac{d}{2}$. Since $[K_{E',n} : K] = \frac{d}{2}$, this implies that $\mathrm{ord}(q, n)|\frac{d}{2}$. But since $\frac{d}{2} \equiv 1 \pmod 2$ and $\mathrm{ord}(q, n) \equiv 0 \pmod 2$, $\mathrm{ord}(q, n) \nmid \frac{d}{2}$, a contradiction. So $d' = d$.

Now assume that $\text{ord}(q,n) \equiv 1 \pmod 2$. We first observe that $\text{ord}(q,n) | \frac{d}{2}$. Furthermore, both matrices $\overline{\rho}_n(\sigma_E)$ and $\overline{\rho}'_n(\sigma_{E'})$ have determinant $\equiv q \pmod n$. So, in particular,

$$\det(\overline{\rho}_n(\sigma_E)^{\frac{d}{2}}) \equiv 1 \pmod n.$$

Since $\overline{\rho}_n(\sigma_E)^d = I_2$, we can deduce that

$$\overline{\rho}_n(\sigma_E)^{\frac{d}{2}} \sim I_2, -I_2, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \text{ or } \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

But $\overline{\rho}_n(\sigma_E)^{\frac{d}{2}} \not\sim \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, or $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, because these two matrices do not have determinant $\equiv 1 \pmod n$. Moreover, $\overline{\rho}_n(\sigma_E)^{\frac{d}{2}} \not\sim I_2$ since this implies that $d \neq \text{ord}(\overline{\rho}_n(\sigma_E))$. Hence, $\overline{\rho}_n(\sigma_E)^{\frac{d}{2}} \sim -I_2$. But from this, we have

$$\overline{\rho}'_n(\sigma_{E'})^{\frac{d}{2}} = -I_2^{\frac{d}{2}} \overline{\rho}_n(\sigma_E)^{\frac{d}{2}} = I_2.$$

Thus, $d' = \frac{d}{2}$. □

As we can see from the above proposition, the calculation of $d$ for one elliptic curve $E$ can always give us the value of $d'$ for the twist with little or no extra work. Using this result, we can reduce the amount of computation in the problem of computing $d$ for all curves over $\mathbb{F}_q$.

CHAPTER 6

# Exploring Possible Applications of the Algorithms

In this final chapter we move away from questions of efficiency and theory to a discussion on possible uses for these algorithms. One natural use of these algorithms is to count the number of elliptic curves over $K = \mathbb{F}_q$, $\mathrm{char}(K) = p$, whose field of $n$-torsion points is degree $d \in \mathbb{Z}^+$. We also discuss the connection between this counting procedure and the modular curve $X(n)$ over a finite field $\mathbb{F}_q$. Finally, we conclude this chapter with an open question about the possibility of using Algorithm 2 to compute $\#E(\mathbb{F}_p)$.

## 1. A Remark on Counting Curves

Let $K = \mathbb{F}_q$ and $n \neq \mathrm{char}(K)$ be a prime. If for each elliptic curve $E$ over $K$ we compute $[K_{E,n} : K]$ using either of our two methods, then we can count the number of elliptic curves over $K$ (up to $K$-isomorphism classes) whose field of $n$-torsion points is a field extension of degree $d \in \mathbb{Z}^+$. We express this number by $Z_q(n,d)$ where

$$Z_q(n,d) = \#\{E/\mathbb{F}_q \mid d = [K_{E,n} : K]\}/\simeq .$$

The tables in the appendix, therefore, allow one to compute $Z_p(n,d)$ for primes $p, n \leq 37$. Note that the tables only consist of curves over $\mathbb{F}_p$, not $\mathbb{F}_q = \mathbb{F}_{p^r}$. Moreover, from earlier facts about the relationships between $q, n$, and $d$, we can deduce that

$$Z_q(n,d) = 0 \quad \text{if } d \nmid n^2 - 1 \text{ and } d \nmid n(n-1)$$

by Corollary 2.15. Also, if $Z_q(n,d) > 0$, it will be the case that $q^d \equiv 1 \pmod{n}$. In the next section we will show that the value of $Z_q(n,1)$ can be connected to the modular curve $X(n)$ defined over $\mathbb{F}_q$. We also remark that there is also a connection between the numbers $Z_q(n,d)$ the number of $\mathbb{F}_q$-rational points on the reductions of the modular diagonal quotient surfaces as considered in [**KaSc**].

## 2. $Z_q(n,1)$ and Counting $\#X(n)(\mathbb{F}_q)$

In this section we will sketch out how we can use $Z_q(n,1)$ to count the number of $\mathbb{F}_q$-rational points on the modular curve $X(n)/\mathbb{F}_q$, i.e., $\#X(n)(\mathbb{F}_q)$. A possible application of this discussion is the ability to determine the coefficients of the zeta function for $X(n)$. As well, the material of this section allows us to partially verify the tables of the appendix for the special cases of $n = 3$ and $n = 5$, and $q = p$ when $p \equiv 1 \pmod{n}$. We will also consider the first interesting case for $n$, that is, when $n = 7$. In this case, we will compare our results to the tables of Cremona [**Cr**].

For this section we will be appealing to the theory concerning the modular curve $X(n)$ [**Ig**] [**De**]. For this entire discussion we will be assuming the following conditions hold. First, $n \neq \mathrm{char}(K) = p$ is a prime. And secondly, $K = \mathbb{F}_q$ contains all the $n^{th}$ roots of unity $\zeta_n \in K$, or equivalently, $q \equiv 1 \pmod{n}$. We fix a primitive $n^{th}$ root of unity $\zeta_n$ from now on.

The curve $X(n)$ is a smooth, geometrically irreducible, projective curve over the field $K$. We now let $Y(n) = X(n)\backslash\text{cusps}$, where the cusps are $K$-rational points. Then, for any $K' \supset K$, the $K'$-rational points of $Y(n)$ can be interpreted in terms of 3-tuples $(E,P,Q)_{/K'}$. Here $E$ is an elliptic curve over $K'$, and $P, Q \in E(\overline{K})$ are $K'$-rational points which form a basis for $E[n]$ satisfying the condition that $e_n(P,Q) = \zeta_n$, where $e_n$ is the pairing described in Section 1.4. For any extension $K' \supset K$, there exists [**Ig**] a natural bijection between the points $x \in Y(n)(K')$ and the isomorphism classes of 3-tuples, i.e.,

$$Y(n)(K') \longleftrightarrow \text{Iso. Classes}(E,P,Q)_{/K'}.$$

In other words, we can identify each $y \in Y(n)(K')$ with a 3-tuple $(E,P,Q)_{/K'}$, where $(E,P,Q)_{/K'}$ is a representative of its isomorphism class. We note that $(E,P,Q)_{/K'} \sim (E',P',Q')_{/K'}$ if there exists a $K$-isomorphism $\phi : E/K' \xrightarrow{\sim} E'/K'$ such that $\phi(P) = P'$ and $\phi(Q) = Q'$. For example, if $j_E \neq 0, 1728$ then the isomorphism class of $(E,P,Q)_{/K'}$ consists of itself and $(E,-P,-Q)_{/K'}$.

We now observe that the group $G_n = Sl_2(\mathbb{Z}/n\mathbb{Z})/\pm 1$ naturally acts on $X(n)$ and on $Y(n)$ via the the above bijection as follows:

$$M \cdot (E,P,Q) = (E, aP + cQ, bP + dQ)$$

if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_n$. In addition there is $G_n$-equivariant morphism $f$ from this projective curve $X(n)$ to $X(1) \cong \mathbb{P}^1_K$ defined by

$$\begin{aligned} f : X(n) &\longrightarrow X(1) \\ (E,P,Q) &\mapsto j_E \\ \text{cusps} &\mapsto \infty, \end{aligned}$$

such that $G_n \backslash X(n) \cong X(1)$. In other words, the point $x = (E,P,Q)$ is taken to the $j$-invariant of the elliptic curve $E$. Further, the cusps of $X(n)$, which are $K$-rational, are taken to $\infty$, the point at infinity of $\mathbb{P}^1_K$.

Recall from Definition 2.4 that we can assign a degree to a morphism. Since $G_n$ acts faithfully we have

$$\deg(f) = |SL_2(\mathbb{Z}/n\mathbb{Z})/\pm 1| = \frac{n(n^2-1)}{2}.$$

Moreover, if $K(X(n))$ and $K(X(1))$ are the functions field of $X(n)$ and $X(1)$ respectively, then it can be shown that $K(X(n))^{G_n} = K(X(1))$. In particular, $K(X(n))/K(X(1))$ is Galois. Since $K(X(n))/K(X(1))$ is Galois [**Ig**], the ramification index $e_x(f)$ of $f : X(n) \to X(1)$ and $x \in X(n)$ depends only on $f(x) = y$, so we can write $e_y = e_x(f)$. From Igusa's paper [**Ig**] we have

$$e_y = \begin{cases} n & \text{if } y = \infty \\ 3 & \text{if } y = 0 \\ 2 & \text{if } y = 1728 \end{cases}$$

where $e_y = 1$ otherwise.

Using the following formula due to Hurwitz, we can compute the genus of $X(n)$:

$$2g(X(n)) - 2 = \deg(f)\left(2g(X(1)) - 2 + \sum_{y \in X(1)} (1 - \frac{1}{e_y})\right). \tag{11}$$

Here, $g(X(n))$ and $g(X(1))$ refer to the genus of $X(n)$ and $X(1)$ respectively. (See [**Ha**] IV.2.4 and exercise IV.2.4 for a proof of this formula.) Since $X(1)_{/K} \cong \mathbb{P}^1_K$, we know that $g(X(1)) = 0$. Simplifying the above formula gives us

$$\begin{aligned} 2g(X(n)) - 2 &= \deg(f)\left(-2 + (1 - \frac{1}{2}) + (1 - \frac{1}{3}) + (1 - \frac{1}{n})\right) \\ &= \frac{(n^2-1)(n-6)}{12}. \end{aligned}$$

We now relate the number of $K$-rational points of $X(n)_{/K}$ to $Z_q(n,1)$. We note that for every tuple $(E,P,Q)_{/K}$ that since $P,Q \in E(K)$, then $E[n] \leq E(K)$, thereby implying $[K_{E,n} : K] = 1$. In particular, if $(E,P,Q) \in X(n)(K)$, then $[K_{E,n} : K] = 1$. Conversely, if $E$ is an elliptic curve with $[K_{E,n} : K] = 1$, then $E$ gives rise to to precisely $\frac{deg(f)}{e_{j_E}}$ rational points on $X(n)$. Thus, this gives us the following formula:

$$\#X(n)(\mathbb{F}_q) = \frac{\deg(f)}{e_\infty} + c_0\frac{\deg(f)}{e_0} + c_{1728}\frac{\deg(f)}{e_{1728}} + c\deg(f) \tag{12}$$

where

$$\begin{aligned} c_0 &= \#\{E/\mathbb{F}_q \mid [K_{E,n} : K] = 1 \text{ and } j_E = 0\}, \\ c_{1728} &= \#\{E/\mathbb{F}_q \mid [K_{E,n} : K] = 1 \text{ and } j_E = 1728\}, \\ c &= \#\{E/\mathbb{F}_q \mid [K_{E,n} : K] = 1 \text{ and } j_E \neq 0, 1728\}. \end{aligned}$$

Observe how this should compare with $Z_q(n,1)$, namely,

$$Z_q(n,1) = c_0 + c_{1728} + c. \tag{13}$$

We may summarize our discussion as follows:

PROPOSITION 6.1. *Let*

$$Z_q^*(n) = 6\left(\frac{1}{3}c_0 + \frac{1}{2}c_{1728} + c\right). \tag{14}$$

*Then*

$$\#X(n)(\mathbb{F}_q) = \frac{n^2-1}{2} + \frac{n(n^2-1)}{12}Z_q^*(n). \tag{15}$$

PROOF. This is immediate by substituting (14) into (12). □

Notice that from this discussion, our algorithms could be used to compute some of the coefficients of the zeta function of $X(n)/\mathbb{F}_q$. Recall that

$$Z_{X(n)/\mathbb{F}_q}(T) = \exp\left(\sum_{i=1}^{\infty} \frac{\#X(n)(\mathbb{F}_{q^i})}{i}T^i\right).$$

Since $Z_{X(n)/\mathbb{F}_q}(T)$ is a rational function, we need to compute only finitely many $\#X(n)(\mathbb{F}_{q^i})$ to determine *all* the coefficients. Unfortunately, there is a question of whether this is a practical method of determining these coefficients. Recall that our algorithms were only implemented for the case that $K = \mathbb{F}_p$. While the theory

remains the same for $K = \mathbb{F}_q$, implementation becomes more difficult since we need to use the arithmetic of $\mathbb{F}_q$.

We now specialize to the case that $n = 3$ and $n = 5$ and $X(n)_{/K}$ where $K = \mathbb{F}_q$. Recall that $q \equiv 1 \pmod{n}$. We will show how the above discussion allows us to check our tables in a limited sense. Using Hurwitz's formula (11), we find that $g(X(3)) = g(X(5)) = 0$. So, $X(n) \cong \mathbb{P}^1_K$ for $n = 3, 5$. We then deduce that

$$\#X(n)(\mathbb{F}_q) = q + 1$$

for both $n = 3, 5$.

For $n = 3$, we used our algorithms and (15) to compute $\#X(n)(\mathbb{F}_p)$ for all primes $p < 100$ and $p \equiv 1 \pmod{3}$. Comparing this to the expected result of $p + 1$, we see that in all cases they agree. The following table (Table 1) contains our results for this comparison. The first column contains all primes $p < 100$ such that $p \equiv 1 \pmod{3}$. Columns two through four contain the values of $c_0, c_{1728}$, and $c$ that were obtained via our algorithms. The fifth column is the value of $Z_p(n, d)$. The sixth column contains the value of $Z_p^*(n)$ as defined in (14). In the last column, we use our observed data to evaluate (15), that is,

$$\#X(3)(\mathbb{F}_p) = 4 + 2 \cdot Z_p^*(3)$$

since $n = 3$. Notice that each entry in the last column of the table is equal to $p+1$, which is what we expected.

Moreover, the case of $n = 5$ is very similar. The only differences are that we must use $p \equiv 1 \pmod{5}$ and the formula for (15) becomes

$$\#X(5)(\mathbb{F}_p) = 12 + 10 \cdot Z_p^*(5).$$

The observed results again agree with the expected results for all $p < 100$. We include a table (Table 2) for this situation.

Therefore, from these two tables we see that the output from our algorithms gives the correct value under these special conditions. This provides a basis of confidence that our algorithms were implemented correctly.

For the cases $n > 5$, we encounter a difficulty on the theoretical side. For $n > 5, X(n)$ is a curve with genus $> 0$. In fact, by (11) we can deduce that $g(X(n))$

| prime $p$ | $c_0$ | $c_{1728}$ | $c$ | $Z_p(3,1)$ | $Z_p^*(3)$ | $4+2\cdot Z_p^*(3)$ |
|---|---|---|---|---|---|---|
| 7 | 1 | 0 | 0 | 1 | 2 | 8 |
| 13 | 1 | 1 | 0 | 2 | 5 | 14 |
| 19 | 1 | 0 | 1 | 2 | 8 | 20 |
| 31 | 1 | 0 | 2 | 3 | 14 | 32 |
| 37 | 1 | 1 | 2 | 4 | 17 | 38 |
| 43 | 1 | 0 | 3 | 4 | 20 | 44 |
| 61 | 1 | 1 | 4 | 6 | 29 | 62 |
| 67 | 1 | 0 | 5 | 6 | 32 | 68 |
| 73 | 1 | 1 | 5 | 7 | 35 | 74 |
| 79 | 1 | 0 | 6 | 7 | 38 | 80 |
| 97 | 1 | 1 | 7 | 9 | 47 | 98 |

TABLE 1. Comparing the Output of the Algorithms to $\#X(3)(\mathbb{F}_p)$

| prime $p$ | $c_0$ | $c_{1728}$ | $c$ | $Z_p(5,1)$ | $Z_p^*(5)$ | $12+10\cdot Z_p^*(5)$ |
|---|---|---|---|---|---|---|
| 11 | 0 | 0 | 0 | 0 | 0 | 12 |
| 31 | 1 | 0 | 0 | 1 | 2 | 32 |
| 41 | 0 | 1 | 0 | 1 | 3 | 42 |
| 61 | 1 | 1 | 0 | 2 | 5 | 62 |
| 71 | 0 | 0 | 1 | 1 | 6 | 72 |

TABLE 2. Comparing the Output of the Algorithms to $\#X(5)(\mathbb{F}_p)$

grows like $n^3$. This makes it very difficult to determine a nice expected result for $\#X(n)(\mathbb{F}_q)$.

To get a flavor of this problem, we consider the first non-trivial case, $n = 7$. By (11), we calculate the genus to be $g(X(7)) = 3$. Now consider the Jacobian of $X(7)$, that is, $J = Jac(X(7))$. Then it can be shown ([**Ka**] based upon the results of [**KaRo**]) that $J$ is isogenous to the cube of an elliptic curve $E$ over $K$, i.e.,

$$Jac(X(7)) \sim E^3. \tag{16}$$

Moreover, it can be shown that $E = X_0(49)_{/\mathbb{F}_q}$, an elliptic curve with conductor $N = 49$. From the tables of Cremona [**Cr**], we can write an explicit equation for

$E$, namely,

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

If we now write out the zeta function for $E$ and $X(7)$, we will have

$$\begin{aligned} Z_{X(7)/K}(T) &= \frac{L_{X(7)/K}(T)}{(1-T)(1-qT)} \\ Z_{E/K}(T) &= \frac{L_{E/K}(T)}{(1-T)(1-qT)} \end{aligned}$$

where $L_{X(7)/K}(T)$ and $L_{E/K}(T)$ are the $L$-series of $X(7)$ and $E$ respectively. By the isogeny relation of (16), we can deduce that

$$L_{X(7)/K}(T) = L_{E/K}(T)^3.$$

But

$$L_{E/K}(T) = (1 - a_E T + qT^2),$$

hence, the zeta function of $X(7)_{/K}$ becomes

$$Z_{X(7)/K}(T) = \frac{(1 - a_E T + qT^2)^3}{(1-T)(1-qT)}.$$

Suppose that $(1 - a_E T + qT^2) = (1-\alpha T)(1-\beta T) \in \overline{K}[T]$. Then we can rewrite the above zeta function as

$$Z_{X(7)/K}(T) = \exp\left(\sum_{i=1}^{\infty} \frac{1 + q^i - 3(\alpha^i + \beta^i)}{i} T^i\right).$$

From this we deduce that

$$\#X(7)(K) = 1 + q - 3(\alpha + \beta) = 1 + q - 3a_E. \tag{17}$$

If we specialize to $K = \mathbb{F}_p$, then we can use this result in two ways. First, we can use this result in combination with (15) to check the output of our algorithms with known values of $a_E$, which, by Eichler-Shimura, is the $p^{th}$-coefficient of the unique cusp form of $S_2(\Gamma_0(49))$. And second, since we can compute $\#X(7)(\mathbb{F}_p)$ for all $p \equiv 1 \pmod 7$ with our algorithms, this gives us a new way in which to calculate $a_E$ (for $p \equiv 1 \pmod 7$).

In Table 3, we use our results for all primes $p < 100$ and $p \equiv 1 \pmod 7$ to calculate $a_E$ using (17). We then compare this result to the value of $a_E$ given in [**Cr**]. We also use our algorithms to compute $a_E$ for the first two primes $p > 100$ and $p \equiv 1 \pmod 7$. These results go beyond the tables of [**Cr**]. The first column

| prime $p$ | $c_0$ | $c_{1728}$ | $c$ | $Z_p(7,1)$ | $Z_p^*(7)$ | $\#X(7)(\mathbb{F}_p)$ | $\frac{(1+p)-\#X(n)(\mathbb{F}_p)}{3}$ | $a_E$ |
|---|---|---|---|---|---|---|---|---|
| 29 | 0 | 0 | 0 | 0 | 0 | 24 | 2 | 2 |
| 43 | 1 | 0 | 0 | 1 | 2 | 80 | -12 | -12 |
| 71 | 0 | 0 | 0 | 0 | 0 | 24 | 16 | 16 |
| 113 | 0 | 1 | 0 | 1 | 3 | 108 | 2 | - |
| 127 | 1 | 0 | 0 | 1 | 2 | 80 | 16 | - |

TABLE 3. Comparing the Output of the Algorithms to $\#X(7)(\mathbb{F}_p)$

list the primes $p$ such that $p \equiv 1 \pmod 7$. Columns two through four contain the values for $c_0, c_{1728}$, and $c$ respectively. Column five has the value of $Z_p(7,1)$, while column six is $Z_p^*(7)$. In the seventh column, we evaluate $\#X(7)(\mathbb{F}_p)$ using (15). In the next column, we compute $a_E$ by using (17). Finally, the last column gives the value for $a_E$ as listed in the tables of [**Cr**]. Observe that this value agrees with the previous column. There is no entry in this column for the last two rows since the tables of [**Cr**] only contain $a_E$ for $p < 100$.

## 3. Computing $\#E(\mathbb{F}_p)$ and Algorithm 2: an Open Question

As with all questions in mathematics, answers inevitable lead to more questions. We conclude with a question that is suggested by this paper.

QUESTION 1. *Can Algorithm 2 be used in the calculation of $a_E$, or equivalently, of $\#E(\mathbb{F}_p)$?*

This question is closely related to the work of Schoof and Atkins [**Sc2**],[**Sc1**][**At**]. While Algorithm 1 utilizes $a_E$ to calculate $d$, Algorithm 2 does not depend upon $a_E$. Algorithm 1, therefore, shows that $d$ and $a_E$ are related; this question asks whether we can work backwards from $d$ to get $a_E$.

Suppose that an elliptic curve $E$ over $\mathbb{F}_p$ has been given. Now using Algorithm 2 we can compute $d = [K_{E,n} : K]$ given some prime $n \neq p$. Suppose that $\alpha$ and $\beta$ are the roots in $\overline{\mathbb{F}}_n$ of the characteristic polynomial of the Frobenius endomorphism. By Corollary 2.12, we have

$$T^2 - a_E T + p = (T - \alpha)(T - \beta).$$

Now since $d$ is the degree, $\alpha^d \equiv \beta^d \equiv 1 \pmod{n}$, then,

$$\alpha^d + \beta^d \equiv 2 \pmod{n}. \tag{18}$$

Let $a_{E,m} = \alpha^m + \beta^m$, for $m \leq 1$. Then it is a possible to write a recursive definition for $a_{E,m}$ in terms of $a_{E,1} \equiv \alpha + \beta \pmod{n}$, namely,

$$\begin{aligned} a_{E,1} &\equiv \alpha + \beta \pmod{n} \\ a_{E,m} &\equiv a_{E,\frac{m}{2}}^2 - 2p^{\frac{m}{2}} \pmod{n} \quad m \text{ even} \\ a_{E,m} &\equiv a_{E,\frac{m+1}{2}} a_{E,\frac{m-1}{2}} - p^{\frac{m-1}{2}} a_{E,1} \pmod{n} \quad m > 1 \text{ odd} \end{aligned}$$

Notice that the above formulae rely on the fact that $\alpha\beta \equiv p \pmod{n}$. Now consider the following polynomials $f_m \in \mathbb{Z}[x]$ which are defined similarly, that is,

$$\begin{aligned} f_1 &= x \\ f_m &= f_{\frac{m}{2}}^2 - 2p^{\frac{m}{2}} \quad m \text{ even} \\ f_m &= f_{\frac{m+1}{2}} \cdot f_{\frac{m-1}{2}} - p^{\frac{m-1}{2}} x \quad m > 1 \text{ odd}. \end{aligned}$$

But then if substitute $a_{E,1}$ into $f_d$, we have

$$a_{E,d} \equiv f_d(a_{E,1}) \pmod{n}.$$

We can then rewrite (18) as

$$f_d(a_{E,1}) \equiv 2 \pmod{n}. \tag{19}$$

But then notice that $a_E \equiv a_{E,1} \pmod{n}$ will also satisfy this polynomial. So, if we take all solutions to the equation $f_d(x) \equiv 2 \pmod{n}$, the desired value (up to a congruence modulo $n$) will be in the solution set.

So now suppose that we find $d_i$ for a number of $n_i$. Then we know that $a_E \pmod{n_i}$ will satisfy

$$f_{d_i}(x) \equiv 2 \pmod{n_i}.$$

That is, $a_E \pmod{n_i}$ will be in the solution set to the above polynomial. It is the hope that if we consider enough $d_i$ and $n_i$, we can pick out $a_E$. To make this more clear, we work through the following example.

| $n$ | $d$ | roots of $f_d(x) - 2 \pmod{n}$ |
|---|---|---|
| 3 | 8 | -1,0,1 |
| 5 | 5 | 2 |
| 7 | 48 | $0, \pm 1, \pm 2, \pm 3$ |
| 11 | 10 | -3,-1,0,1,3 |
| 13 | 84 | $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6$ |
| 17 | 68 | -8,0,8 |

TABLE 4. Computing Possible Values for $a_E$

**Example 6.2:** Let $E : y^2 = x^3 + 52x + 95$ be an elliptic curve over $\mathbb{F}_p$ when $p = 101$. Now, using a well know result due to Hasse (see [**Si**]V.1.1) we have

$$|a_E| \leq 2\sqrt{p}$$

Since $p = 101$, we know that $a_E$ is an integer in the interval $-20 \leq a_E \leq 20$. We now use Algorithm 2 to compute $d$ for the primes $n \leq 17$. Then for each $d$ and $n$, we compute the solutions to $f_d(x) \equiv 2 \pmod{n}$. The results are summarized in Table 4.

Notice that when $n = 3, 7, 13$, we do not get any information about $a_E$. However, when $n = 5$, we find that $a_E \equiv 2 \pmod{5}$. When $n = 7$, we find that either $a_E \equiv 0, -1, 1, -3$ or $3 \pmod{11}$. Finally, we see that $a_E \equiv -8, 0$ or $8 \pmod{17}$. Checking all integers in our range, we will find that there is only only one possible value for $a_E$, namely, $a_E = -8$, which is, in fact, the correct result. (The reader is invited to verify this: write out all integers in the interval [-20,20] and use the above results to eliminate each integer that fails to meet one of the above conditions. For example, $-20$ cannot be $a_E$ because $-20 \not\equiv 2 \pmod{5}$.)

While the above example shows that we can use Algorithm 2 to calculate $a_E$, there are many more questions that need to be answered. First of all, will this method always provide a unique result? In the case that for each $n$ we find that the degree $d$ is such that $4|d$, then both the curve and its twist have the same degree. So, $\pm a_E$ will always be a solution to the equation $f_d(x) \equiv 2 \pmod{n}$. In this case, it would seem that we could only find $a_E$ up to a sign. Second, how many $n$ do

we need to check before we can distinguish $a_E$? We can quit in our example after checking $n = 17$. However, in some cases, we may need to check very large $n$ before we can determine $a_E$. And finally, is this any improvement over other algorithms for computing $a_E$? This question is linked to the previous. If we can keep $n$ small, then by our discussion in Chapter 5, we know that Algorithm 2 is fairly quick. But as $n$ grows, the running time in Algorithm 2 also increases.

APPENDIX A

# Tables

Each table corresponds to a prime $5 \leq p \leq 37$, where $p$ is the characteristic of $K = \mathbb{F}_p$. For each $p$, we constructed all elliptic curves over the field $K$ as described in Section 5.4. In the tables, the first four columns correspond to information about elliptic curves:

- $j$ is the $j$-invariant of the curve.
- $a$ and $b$ are the coefficients of the Weierstrass equation for $E$, that is, $E : y^2 = x^3 + ax + b$.
- $a_p = (p+1) - \#E(\mathbb{F}_p)$. From this column, we can also deduce $\#E(\mathbb{F}_p)$.

The remaining columns give the value of $d_n$, where

$$d_n = [K_{E,n} : K],$$

and $n$ is a prime $\leq 37$. Reading across the table, we get an elliptic curve and the value of $d_n$ for this curve for various $n$.

For example, the third row of Table 1 (the table consisting of all curves over $\mathbb{F}_5$) tells us that

$$y^2 = x^3 + x + 3$$

is an elliptic curve over $\mathbb{F}_5$ with $j$-invariant 1. Reading across the row, we see that the degree of the field of 11-torsion points is 60.

The last five rows of each table contain the following information:

- $\mathrm{ord}(p, n)$ is the order of $p$ in $\mathbb{Z}/n\mathbb{Z}$.
- *Alg1: Total* lists the total running time for Algorithm 1 to generate $d_n$ for every elliptic curve $E$ over $\mathbb{F}_p$ up to $\mathbb{F}_p$-isomorphism.
- *Alg1: Avg.* contains the average running time for Algorithm 1 for each curve. It was determined by taking the total time and dividing by the number of curves over $\mathbb{F}_p$.

- *Alg2: Total* lists the total running time for Algorithm 2 to generate $d_n$ for every elliptic curve $E$ over $\mathbb{F}_p$. Note that we found the time only for $n \leq 17$ when $p \leq 11$, and for $n \leq 11$ otherwise.
- *Alg2: Avg.* contains the average running time for Algorithm 2 for each curve. It was determined by taking the total time and dividing by the number of curves over $\mathbb{F}_p$.

The tables were generated using Algorithm 1 implemented in Maple V Release 4. The computations were done on a Packard Bell Pentium/66 with the Windows 3.1 operating system.

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 2 | - | 6 | 20 | 8 | 32 | 36 | 22 | 14 | 12 | 72 |
| 0 | 0 | 2 | 0 | 2 | - | 6 | 20 | 8 | 32 | 36 | 22 | 14 | 12 | 72 |
| 1 | 1 | 3 | 2 | 8 | - | 48 | 60 | 12 | 16 | 90 | 528 | 14 | 96 | 36 |
| 1 | 4 | 4 | -2 | 8 | - | 48 | 60 | 12 | 16 | 45 | 528 | 14 | 96 | 36 |
| 2 | 4 | 2 | 3 | 2 | - | 48 | 110 | 56 | 288 | 180 | 22 | 140 | 30 | 36 |
| 2 | 1 | 1 | -3 | 2 | - | 48 | 55 | 56 | 288 | 180 | 22 | 140 | 15 | 36 |
| 1728 | 1 | 0 | 2 | 8 | - | 48 | 60 | 12 | 16 | 90 | 528 | 14 | 96 | 36 |
| 1728 | 2 | 0 | 4 | 8 | - | 48 | 30 | 12 | 16 | 180 | 528 | 28 | 96 | 36 |
| 1728 | 3 | 0 | -4 | 8 | - | 48 | 15 | 12 | 16 | 180 | 528 | 28 | 96 | 36 |
| 1728 | 4 | 0 | - 2 | 8 | - | 48 | 60 | 12 | 16 | 45 | 528 | 14 | 96 | 36 |
| 4 | 2 | 1 | -1 | 8 | - | 6 | 10 | 56 | 16 | 171 | 22 | 420 | 48 | 1368 |
| 4 | 3 | 3 | 1 | 8 | - | 6 | 5 | 56 | 16 | 342 | 22 | 420 | 48 | 1368 |
| ord$(p,n)$ | | | | 2 | - | 6 | 5 | 4 | 16 | 9 | 22 | 14 | 3 | 36 |
| Alg1: Total (sec) | | | | .549 | - | .549 | .824 | .494 | .714 | .714 | .769 | .659 | 1.044 | .605 |
| Alg1: Avg. (sec) | | | | .042 | - | .042 | .633 | .038 | .055 | .055 | .059 | .051 | .080 | .047 |
| Alg2: Total (sec) | | | | 10.49 | - | 15.27 | 106.1 | 113.9 | 211.297 | * | * | * | * | * |
| Alg2: Avg. (sec) | | | | .807 | - | 1.175 | 8.159 | 8.758 | 16.253 | * | * | * | * | * |

Table 1: Elliptic curves over $\mathbb{F}_p$, where $p = 5$

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | -4 | 3 | 24 | - | 120 | 12 | 288 | 18 | 528 | 105 | 15 | 36 |
| 0 | 0 | 2 | -1 | 1 | 24 | - | 120 | 12 | 288 | 18 | 528 | 35 | 15 | 36 |
| 0 | 0 | 3 | -5 | 6 | 8 | - | 40 | 12 | 288 | 9 | 176 | 210 | 30 | 36 |
| 0 | 0 | 4 | 5 | 3 | 8 | - | 40 | 12 | 288 | 18 | 176 | 105 | 15 | 36 |
| 0 | 0 | 5 | 1 | 2 | 24 | - | 120 | 12 | 288 | 9 | 528 | 70 | 30 | 36 |
| 0 | 0 | 6 | 4 | 6 | 24 | - | 120 | 12 | 288 | 9 | 528 | 210 | 30 | 36 |
| 1 | 4 | 6 | -3 | 4 | 4 | - | 10 | 168 | 16 | 114 | 22 | 210 | 480 | 342 |
| 1 | 1 | 1 | 3 | 4 | 4 | - | 10 | 168 | 16 | 57 | 22 | 105 | 480 | 171 |
| 2 | 3 | 1 | -4 | 3 | 24 | - | 120 | 12 | 288 | 18 | 528 | 105 | 15 | 36 |
| 2 | 6 | 6 | 4 | 6 | 24 | - | 120 | 12 | 288 | 9 | 528 | 210 | 30 | 36 |
| 3 | 6 | 2 | -1 | 3 | 24 | - | 120 | 12 | 288 | 18 | 528 | 35 | 15 | 36 |
| 3 | 5 | 5 | 1 | 6 | 24 | - | 120 | 12 | 288 | 9 | 528 | 70 | 30 | 36 |
| 4 | 5 | 4 | -2 | 6 | 4 | - | 10 | 168 | 96 | 30 | 528 | 28 | 15 | 171 |
| 4 | 3 | 3 | 2 | 3 | 4 | - | 10 | 168 | 96 | 15 | 528 | 28 | 30 | 342 |
| 5 | 2 | 3 | 2 | 3 | 4 | - | 10 | 168 | 96 | 15 | 528 | 28 | 30 | 342 |
| 5 | 4 | 4 | -2 | 6 | 4 | - | 10 | 168 | 96 | 30 | 528 | 28 | 15 | 171 |
| 1728 | 1 | 0 | 0 | 4 | 8 | - | 10 | 24 | 32 | 12 | 22 | 28 | 60 | 36 |
| 1728 | 3 | 0 | 0 | 4 | 8 | - | 10 | 24 | 32 | 12 | 22 | 28 | 60 | 36 |
| ord$(p,n)$ | | | | 1 | 4 | - | 10 | 12 | 16 | 3 | 22 | 7 | 15 | 9 |
| Alg1: Total (sec) | | | | .989 | .824 | - | .879 | .879 | 1.373 | .934 | 1.318 | 1.098 | 1.263 | .989 |
| Alg1: Avg. (sec) | | | | .052 | .043 | - | .046 | .046 | .072 | .049 | .069 | .058 | .066 | .052 |
| Alg2: Total (sec) | | | | 20.82 | 24.41 | - | 40.01 | 127.3 | 449.5 | * | * | * | * | * |
| Alg2: Avg. (sec) | | | | 1.096 | 1.286 | - | 2.110 | 6.700 | 23.65 | * | * | * | * | * |

Table 2: Elliptic curves over $\mathbb{F}_p$, where $p = 7$

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 2 | 4 | 12 | - | 24 | 32 | 12 | 22 | 56 | 30 | 6 |
| 0 | 0 | 2 | 0 | 2 | 4 | 12 | - | 24 | 32 | 12 | 22 | 56 | 30 | 6 |
| 1728 | 1 | 0 | 0 | 2 | 4 | 12 | - | 24 | 32 | 12 | 22 | 56 | 30 | 6 |
| 1728 | 2 | 0 | 0 | 2 | 4 | 12 | - | 24 | 32 | 12 | 22 | 56 | 30 | 6 |
| 2 | 1 | 9 | 4 | 8 | 3 | 21 | - | 168 | 96 | 60 | 22 | 28 | 960 | 36 |
| 2 | 4 | 6 | -4 | 8 | 6 | 42 | - | 168 | 96 | 60 | 22 | 28 | 960 | 36 |
| 3 | 9 | 4 | -6 | 2 | 3 | 24 | - | 168 | 16 | 18 | 176 | 840 | 960 | 228 |
| 3 | 3 | 10 | 6 | 2 | 6 | 24 | - | 168 | 16 | 9 | 176 | 840 | 960 | 228 |
| 4 | 8 | 6 | 3 | 2 | 10 | 42 | - | 12 | 16 | 15 | 528 | 28 | 960 | 228 |
| 4 | 10 | 4 | -3 | 2 | 5 | 21 | - | 12 | 16 | 30 | 528 | 28 | 960 | 228 |
| 5 | 2 | 7 | 5 | 8 | 4 | 3 | - | 168 | 16 | 114 | 22 | 280 | 960 | 228 |
| 5 | 8 | 1 | -5 | 8 | 4 | 6 | - | 168 | 16 | 57 | 22 | 280 | 960 | 228 |
| 6 | 5 | 1 | 1 | 8 | 6 | 24 | - | 12 | 16 | 60 | 22 | 280 | 30 | 228 |
| 6 | 9 | 8 | -1 | 8 | 3 | 24 | - | 12 | 16 | 60 | 22 | 280 | 30 | 228 |
| 7 | 7 | 8 | -2 | 8 | 10 | 3 | - | 12 | 288 | 18 | 22 | 168 | 960 | 18 |
| 7 | 6 | 9 | 2 | 8 | 5 | 6 | - | 12 | 288 | 9 | 22 | 168 | 960 | 18 |
| 8 | 10 | 2 | 4 | 8 | 3 | 21 | - | 168 | 96 | 60 | 22 | 28 | 960 | 36 |
| 8 | 7 | 5 | -4 | 8 | 6 | 42 | - | 168 | 96 | 60 | 22 | 28 | 960 | 36 |
| 9 | 4 | 3 | -2 | 8 | 10 | 3 | - | 12 | 288 | 18 | 22 | 168 | 960 | 18 |
| 9 | 5 | 2 | 2 | 8 | 5 | 6 | - | 12 | 288 | 9 | 22 | 168 | 960 | 18 |
| 10 | 3 | 5 | 3 | 2 | 10 | 42 | - | 12 | 16 | 15 | 528 | 28 | 960 | 228 |
| 10 | 1 | 7 | -3 | 2 | 5 | 21 | - | 12 | 16 | 30 | 528 | 28 | 960 | 228 |
| ord$(p,n)$ | | | | 2 | 1 | 3 | - | 12 | 16 | 3 | 22 | 28 | 30 | 6 |
| Alg1: Total (sec) | | | | 1.483 | 2.032 | 1.593 | - | 2.032 | 1.538 | 2.252 | 1.483 | 1.867 | 2.306 | 1.867 |
| Alg1: Avg. (sec) | | | | .064 | .088 | .069 | - | .088 | .067 | .098 | .065 | .081 | .100 | .081 |
| Alg2: Total (sec) | | | | 32.68 | 33.18 | 56.35 | - | 191.633 | 854.1 | * | * | * | * | * |
| Alg2: Avg. (sec) | | | | 1.421 | 1.442 | 2.450 | - | 8.332 | 37.13 | * | * | * | * | * |

Table 3: Elliptic curves over $\mathbb{F}_p$, where $p = 11$

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 24 | 6 | 40 | - | 72 | 18 | 264 | 140 | 30 | 36 |
| 0 | 0 | 2 | -5 | 2 | 8 | 6 | 120 | - | 72 | 18 | 264 | 420 | 30 | 36 |
| 0 | 0 | 3 | 5 | 1 | 8 | 6 | 120 | - | 72 | 18 | 264 | 420 | 30 | 36 |
| 0 | 0 | 4 | -7 | 3 | 24 | 2 | 120 | - | 72 | 18 | 88 | 420 | 30 | 36 |
| 0 | 0 | 5 | -2 | 6 | 24 | 6 | 40 | - | 72 | 18 | 264 | 140 | 30 | 36 |
| 0 | 0 | 6 | 7 | 6 | 24 | 2 | 120 | - | 72 | 18 | 88 | 420 | 30 | 36 |
| 1 | 6 | 1 | 6 | 4 | 4 | 16 | 120 | - | 16 | 360 | 66 | 28 | 960 | 36 |
| 1 | 11 | 8 | -6 | 4 | 4 | 16 | 120 | - | 16 | 360 | 33 | 28 | 960 | 36 |
| 2 | 8 | 10 | 1 | 6 | 4 | 16 | 10 | - | 136 | 18 | 11 | 28 | 960 | 1368 |
| 2 | 6 | 2 | -1 | 3 | 4 | 16 | 10 | - | 136 | 18 | 22 | 28 | 960 | 1368 |
| 3 | 9 | 8 | 5 | 3 | 8 | 6 | 120 | - | 72 | 18 | 264 | 420 | 30 | 36 |
| 3 | 10 | 12 | -5 | 6 | 8 | 6 | 120 | - | 72 | 18 | 264 | 420 | 30 | 36 |
| 4 | 7 | 12 | -2 | 6 | 24 | 6 | 40 | - | 72 | 18 | 264 | 140 | 30 | 36 |
| 4 | 2 | 5 | 2 | 3 | 24 | 6 | 40 | - | 72 | 18 | 264 | 140 | 30 | 36 |
| 5 | 10 | 6 | 0 | 4 | 8 | 2 | 10 | - | 8 | 18 | 44 | 14 | 30 | 72 |
| 5 | 1 | 9 | 0 | 4 | 8 | 2 | 10 | - | 8 | 18 | 44 | 14 | 30 | 72 |
| 6 | 1 | 11 | 2 | 3 | 24 | 6 | 40 | - | 72 | 18 | 264 | 140 | 30 | 36 |
| 6 | 4 | 10 | -2 | 6 | 24 | 6 | 40 | - | 72 | 18 | 264 | 140 | 30 | 36 |
| 7 | 4 | 5 | 4 | 6 | 4 | 16 | 120 | - | 16 | 360 | 132 | 14 | 960 | 36 |
| 7 | 3 | 1 | -4 | 3 | 4 | 16 | 120 | - | 16 | 360 | 132 | 14 | 960 | 36 |
| 8 | 2 | 9 | -3 | 4 | 24 | 16 | 10 | - | 4 | 360 | 11 | 420 | 30 | 1368 |
| 8 | 8 | 7 | 3 | 4 | 24 | 16 | 10 | - | 4 | 360 | 22 | 420 | 30 | 1368 |
| 9 | 3 | 7 | 1 | 6 | 4 | 16 | 10 | - | 136 | 18 | 11 | 28 | 960 | 1368 |
| 9 | 12 | 4 | -1 | 3 | 4 | 16 | 10 | - | 136 | 18 | 22 | 28 | 960 | 1368 |
| 10 | 5 | 3 | -4 | 3 | 4 | 16 | 120 | - | 16 | 360 | 132 | 14 | 960 | 36 |
| 10 | 7 | 11 | 4 | 6 | 4 | 16 | 120 | - | 16 | 360 | 132 | 14 | 960 | 36 |
| 11 | 11 | 4 | 2 | 3 | 24 | 6 | 40 | - | 72 | 18 | 264 | 140 | 30 | 36 |
| 11 | 5 | 6 | -2 | 6 | 24 | 6 | 40 | - | 72 | 18 | 264 | 140 | 30 | 36 |
| 1728 | 1 | 0 | -6 | 4 | 4 | 16 | 120 | - | 16 | 360 | 33 | 28 | 960 | 36 |
| 1728 | 2 | 0 | 4 | 2 | 4 | 16 | 120 | - | 16 | 360 | 132 | 14 | 960 | 36 |
| 1728 | 4 | 0 | 6 | 4 | 4 | 16 | 120 | - | 16 | 360 | 66 | 28 | 960 | 36 |
| 1728 | 7 | 0 | -4 | 1 | 4 | 16 | 120 | - | 16 | 360 | 132 | 14 | 960 | 36 |
| ord$(p,n)$ | | | | 1 | 4 | 2 | 10 | - | 4 | 18 | 11 | 14 | 30 | 36 |
| Alg1: Total (sec) | | | | 2.472 | 2.197 | 2.417 | 2.637 | - | 2.637 | 2.361 | 2.801 | 2.801 | 2.691 | 2.691 |
| Alg1: Avg. (sec) | | | | .077 | .068 | .076 | .0824 | - | .0824 | .074 | .086 | .087 | 0.084 | .084 |
| Alg2: Total (sec) | | | | 43.94 | 45.53 | 52.84 | 90.74 | - | * | * | * | * | * | * |
| Alg2: Avg. (sec) | | | | 1.373 | 1.423 | 1.65 | 2.836 | - | * | * | * | * | * | * |

Table 4: Elliptic curves over $\mathbb{F}_p$, where $p = 13$

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 2 | 8 | 6 | 10 | 6 | - | 36 | 22 | 8 | 30 | 72 |
| 0 | 0 | 3 | 0 | 2 | 8 | 6 | 10 | 6 | - | 36 | 22 | 8 | 30 | 72 |
| 1 | 1 | 15 | -6 | 2 | 24 | 48 | 10 | 84 | - | 9 | 528 | 40 | 960 | 1368 |
| 1 | 9 | 14 | 6 | 2 | 24 | 48 | 10 | 84 | - | 18 | 528 | 40 | 960 | 1368 |
| 2 | 6 | 5 | -3 | 2 | 4 | 6 | 120 | 84 | - | 9 | 528 | 28 | 960 | 1368 |
| 2 | 3 | 16 | 3 | 2 | 4 | 6 | 120 | 84 | - | 18 | 528 | 28 | 960 | 1368 |
| 3 | 8 | 1 | -1 | 8 | 24 | 48 | 40 | 84 | - | 9 | 22 | 28 | 960 | 36 |
| 3 | 4 | 10 | 1 | 8 | 24 | 48 | 40 | 84 | - | 18 | 22 | 28 | 960 | 36 |
| 4 | 13 | 8 | 4 | 8 | 24 | 6 | 10 | 156 | - | 9 | 528 | 28 | 30 | 1368 |
| 4 | 15 | 12 | -4 | 8 | 24 | 6 | 10 | 156 | - | 18 | 528 | 28 | 30 | 1368 |
| 5 | 14 | 6 | 4 | 8 | 24 | 6 | 10 | 156 | - | 9 | 528 | 28 | 30 | 1368 |
| 5 | 7 | 9 | -4 | 8 | 24 | 6 | 10 | 156 | - | 18 | 528 | 28 | 30 | 1368 |
| 6 | 12 | 10 | 6 | 2 | 24 | 48 | 10 | 84 | - | 18 | 528 | 40 | 960 | 1368 |
| 6 | 6 | 15 | -6 | 2 | 24 | 48 | 10 | 84 | - | 9 | 528 | 40 | 960 | 1368 |
| 7 | 9 | 16 | -3 | 2 | 4 | 6 | 120 | 84 | - | 9 | 528 | 28 | 960 | 1368 |
| 7 | 13 | 7 | 3 | 2 | 4 | 6 | 120 | 84 | - | 18 | 528 | 28 | 960 | 1368 |
| 8 | 4 | 9 | 0 | 2 | 8 | 6 | 10 | 6 | - | 36 | 22 | 8 | 30 | 72 |
| 8 | 2 | 5 | 0 | 2 | 8 | 6 | 10 | 6 | - | 36 | 22 | 8 | 30 | 72 |
| 9 | 11 | 12 | 2 | 8 | 4 | 48 | 120 | 12 | - | 180 | 176 | 28 | 960 | 36 |
| 9 | 14 | 1 | -2 | 8 | 4 | 48 | 120 | 12 | - | 180 | 176 | 28 | 960 | 36 |
| 10 | 15 | 4 | -6 | 2 | 24 | 48 | 10 | 84 | - | 9 | 528 | 40 | 960 | 1368 |
| 10 | 16 | 6 | 6 | 2 | 24 | 48 | 10 | 84 | - | 18 | 528 | 40 | 960 | 1368 |
| 1728 | 1 | 0 | 2 | 8 | 4 | 48 | 120 | 12 | - | 180 | 176 | 28 | 960 | 36 |
| 1728 | 2 | 0 | -2 | 8 | 4 | 48 | 120 | 12 | - | 180 | 176 | 28 | 960 | 36 |
| 1728 | 3 | 0 | -8 | 8 | 4 | 48 | 120 | 6 | - | 90 | 176 | 28 | 960 | 36 |
| 1728 | 6 | 0 | 8 | 8 | 4 | 48 | 120 | 6 | - | 45 | 176 | 28 | 960 | 36 |
| 12 | 16 | 2 | -7 | 8 | 4 | 6 | 10 | 84 | - | 171 | 22 | 40 | 960 | 1368 |
| 12 | 8 | 3 | 7 | 8 | 4 | 6 | 10 | 84 | - | 342 | 22 | 40 | 960 | 1368 |
| 13 | 3 | 11 | -3 | 2 | 4 | 6 | 120 | 84 | - | 9 | 528 | 28 | 960 | 1368 |
| 13 | 10 | 8 | 3 | 2 | 4 | 6 | 120 | 84 | - | 18 | 528 | 28 | 960 | 1368 |
| 14 | 10 | 14 | -2 | 8 | 4 | 48 | 120 | 12 | - | 180 | 176 | 28 | 960 | 36 |
| 14 | 5 | 4 | 2 | 8 | 4 | 48 | 120 | 12 | - | 180 | 176 | 28 | 960 | 36 |
| 15 | 5 | 7 | -5 | 8 | 8 | 48 | 10 | 6 | - | 90 | 22 | 120 | 30 | 1368 |
| 15 | 11 | 2 | 5 | 8 | 8 | 48 | 10 | 6 | - | 45 | 22 | 120 | 30 | 1368 |
| 16 | 2 | 13 | 2 | 8 | 4 | 48 | 120 | 12 | - | 180 | 176 | 28 | 960 | 36 |
| 16 | 1 | 11 | -2 | 8 | 4 | 48 | 120 | 12 | - | 180 | 176 | 28 | 960 | 36 |
| ord$(p,n)$ | | | | 2 | 4 | 6 | 10 | 6 | - | 9 | 22 | 4 | 30 | 36 |
| Alg1: Total (sec) | | | | 3.680 | 3.680 | 3.735 | 3.680 | 3.845 | - | 3.735 | 3.955 | 3.900 | 4.009 | 4.009 |
| Alg1: Avg. (sec) | | | | .099 | .099 | .101 | .099 | .103 | - | .109 | .106 | .105 | .108 | .108 |
| Alg2: Total (sec) | | | | 54.21 | 56.90 | 60.47 | 124.1 | * | - | * | * | * | * | * |
| Alg2: Avg. (sec) | | | | 1.465 | 1.538 | 1.634 | 3.356 | * | - | * | * | * | * | * |

Table 5: Elliptic curves over $\mathbb{F}_p$, where $p = 17$

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 8 | 3 | 12 | 6 | 120 | 12 | 144 | - | 176 | 840 | 30 | 36 |
| 0 | 0 | 2 | 7 | 2 | 12 | 6 | 40 | 12 | 144 | - | 528 | 840 | 15 | 36 |
| 0 | 0 | 4 | -1 | 3 | 4 | 6 | 120 | 12 | 144 | - | 528 | 280 | 30 | 36 |
| 0 | 0 | 5 | -7 | 1 | 12 | 6 | 40 | 12 | 144 | - | 528 | 840 | 30 | 36 |
| 0 | 0 | 8 | -8 | 6 | 12 | 6 | 120 | 12 | 144 | - | 176 | 840 | 15 | 36 |
| 0 | 0 | 10 | 1 | 6 | 4 | 6 | 120 | 12 | 144 | - | 528 | 280 | 15 | 36 |
| 1 | 15 | 8 | 2 | 1 | 12 | 48 | 10 | 168 | 16 | - | 528 | 840 | 240 | 1368 |
| 1 | 3 | 7 | -2 | 2 | 12 | 48 | 10 | 168 | 16 | - | 528 | 840 | 240 | 1368 |
| 2 | 1 | 17 | -8 | 6 | 12 | 6 | 120 | 12 | 144 | - | 176 | 840 | 15 | 36 |
| 2 | 4 | 3 | 8 | 3 | 12 | 6 | 120 | 12 | 144 | - | 176 | 840 | 30 | 36 |
| 3 | 13 | 12 | 7 | 6 | 12 | 6 | 40 | 12 | 144 | - | 528 | 840 | 15 | 36 |
| 3 | 14 | 1 | -7 | 3 | 12 | 6 | 40 | 12 | 144 | - | 528 | 840 | 30 | 36 |
| 4 | 5 | 9 | 1 | 6 | 20 | 6 | 120 | 12 | 144 | - | 528 | 280 | 15 | 36 |
| 4 | 1 | 15 | -1 | 3 | 20 | 6 | 120 | 12 | 144 | - | 528 | 280 | 30 | 36 |
| 5 | 6 | 7 | 4 | 6 | 20 | 48 | 40 | 168 | 8 | - | 22 | 840 | 30 | 1368 |
| 5 | 5 | 18 | -4 | 3 | 20 | 48 | 40 | 168 | 8 | - | 22 | 840 | 15 | 1368 |
| 6 | 4 | 11 | -1 | 3 | 20 | 6 | 120 | 12 | 144 | - | 528 | 280 | 30 | 36 |
| 6 | 16 | 12 | 1 | 6 | 20 | 6 | 120 | 12 | 144 | - | 528 | 280 | 15 | 36 |
| 7 | 12 | 14 | 0 | 4 | 2 | 6 | 10 | 24 | 16 | - | 22 | 56 | 60 | 72 |
| 7 | 10 | 17 | 0 | 4 | 2 | 6 | 10 | 24 | 16 | - | 22 | 56 | 60 | 72 |
| 8 | 14 | 10 | 3 | 4 | 12 | 48 | 120 | 168 | 8 | - | 22 | 28 | 480 | 36 |
| 8 | 18 | 4 | -3 | 4 | 12 | 48 | 120 | 168 | 8 | - | 22 | 28 | 480 | 36 |
| 9 | 8 | 3 | -4 | 3 | 20 | 48 | 40 | 168 | 8 | - | 22 | 840 | 15 | 1368 |
| 9 | 13 | 5 | 4 | 6 | 20 | 48 | 40 | 168 | 8 | - | 22 | 840 | 30 | 1368 |
| 10 | 10 | 18 | 5 | 3 | 2 | 48 | 10 | 12 | 272 | - | 22 | 28 | 480 | 1368 |
| 10 | 2 | 11 | -5 | 6 | 2 | 48 | 10 | 12 | 272 | - | 22 | 28 | 480 | 1368 |
| 11 | 18 | 2 | 6 | 4 | 20 | 6 | 10 | 12 | 48 | - | 22 | 280 | 480 | 36 |
| 11 | 15 | 16 | -6 | 4 | 20 | 6 | 10 | 12 | 48 | - | 22 | 280 | 480 | 36 |
| 12 | 16 | 6 | -6 | 4 | 20 | 6 | 10 | 12 | 48 | - | 22 | 280 | 480 | 36 |
| 12 | 7 | 10 | 6 | 4 | 20 | 6 | 10 | 12 | 48 | - | 22 | 280 | 480 | 36 |
| 13 | 17 | 4 | 2 | 3 | 12 | 48 | 10 | 168 | 16 | - | 528 | 840 | 240 | 1368 |
| 13 | 11 | 13 | -2 | 6 | 12 | 48 | 10 | 168 | 16 | - | 528 | 840 | 240 | 1368 |
| 14 | 9 | 1 | 2 | 3 | 12 | 48 | 10 | 168 | 16 | - | 528 | 840 | 240 | 1368 |
| 14 | 17 | 8 | -2 | 6 | 12 | 48 | 10 | 168 | 16 | - | 528 | 840 | 240 | 1368 |
| 15 | 2 | 15 | 4 | 6 | 20 | 48 | 40 | 168 | 8 | - | 22 | 840 | 30 | 1368 |
| 15 | 8 | 6 | -4 | 3 | 20 | 48 | 40 | 168 | 8 | - | 22 | 840 | 15 | 1368 |
| 16 | 7 | 5 | 5 | 3 | 2 | 48 | 10 | 12 | 272 | - | 22 | 28 | 480 | 1368 |
| 16 | 9 | 2 | -5 | 6 | 2 | 48 | 10 | 12 | 272 | - | 22 | 28 | 480 | 1368 |
| 17 | 3 | 13 | -4 | 3 | 20 | 48 | 40 | 168 | 8 | - | 22 | 840 | 15 | 1368 |
| 17 | 12 | 9 | 4 | 6 | 20 | 48 | 40 | 168 | 8 | - | 22 | 840 | 30 | 1368 |
| 1728 | 1 | 0 | 0 | 4 | 2 | 6 | 10 | 24 | 16 | - | 22 | 56 | 60 | 72 |
| 1728 | 2 | 0 | 0 | 4 | 2 | 6 | 10 | 24 | 16 | - | 22 | 56 | 60 | 72 |
| ord$(p,n)$ | | | | 1 | 2 | 6 | 10 | 12 | 8 | - | 22 | 28 | 15 | 36 |
| Alg1: Total (sec) | | | | 5.273 | 5.383 | 4.998 | 5.273 | 5.054 | 5.712 | - | 5.218 | 5.547 | 5.327 | 5.218 |
| Alg1: Avg. (sec) | | | | .122 | .125 | .116 | .122 | .117 | .132 | - | .121 | .129 | .124 | .121 |
| Alg2: Total (sec) | | | | 71.347 | 77.883 | 84.20 | 166.8 | * | * | - | * | * | * | * |
| Alg2: Avg. (sec) | | | | 1.659 | 1.811 | 1.958 | 3.879 | * | * | - | * | * | * | * |

Table 6: Elliptic curves over $\mathbb{F}_p$, where $p = 19$

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 2 | 8 | 12 | 4 | 6 | 32 | 36 | - | 28 | 10 | 24 |
| 0 | 0 | 5 | 0 | 2 | 8 | 12 | 4 | 6 | 32 | 36 | - | 28 | 10 | 24 |
| 1 | 2 | 19 | 2 | 8 | 24 | 24 | 11 | 6 | 288 | 9 | - | 7 | 10 | 456 |
| 1 | 4 | 6 | -2 | 8 | 24 | 24 | 22 | 6 | 288 | 18 | - | 14 | 10 | 456 |
| 2 | 8 | 7 | -4 | 8 | 4 | 3 | 5 | 84 | 16 | 171 | - | 35 | 320 | 456 |
| 2 | 16 | 1 | 4 | 8 | 4 | 6 | 10 | 84 | 16 | 342 | - | 70 | 320 | 456 |
| 1728 | 1 | 0 | 0 | 2 | 8 | 12 | 4 | 6 | 32 | 36 | - | 28 | 10 | 24 |
| 1728 | 5 | 0 | 0 | 2 | 8 | 12 | 4 | 6 | 32 | 36 | - | 28 | 10 | 24 |
| 4 | 7 | 9 | 1 | 8 | 4 | 21 | 6 | 156 | 96 | 9 | - | 28 | 30 | 456 |
| 4 | 14 | 21 | -1 | 8 | 4 | 42 | 3 | 156 | 96 | 18 | - | 28 | 30 | 456 |
| 5 | 13 | 20 | 4 | 8 | 4 | 6 | 10 | 84 | 16 | 342 | - | 70 | 320 | 456 |
| 5 | 3 | 16 | -4 | 8 | 4 | 3 | 5 | 84 | 16 | 171 | - | 35 | 320 | 456 |
| 6 | 15 | 16 | -8 | 8 | 24 | 42 | 5 | 84 | 288 | 45 | - | 28 | 320 | 36 |
| 6 | 7 | 22 | 8 | 8 | 24 | 21 | 10 | 84 | 288 | 90 | - | 28 | 320 | 36 |
| 7 | 16 | 14 | -9 | 2 | 4 | 24 | 11 | 84 | 288 | 45 | - | 42 | 30 | 36 |
| 7 | 9 | 2 | 9 | 2 | 4 | 24 | 22 | 84 | 288 | 90 | - | 21 | 30 | 36 |
| 8 | 12 | 22 | -8 | 8 | 24 | 42 | 5 | 84 | 288 | 45 | - | 28 | 320 | 36 |
| 8 | 1 | 13 | 8 | 8 | 24 | 21 | 10 | 84 | 288 | 90 | - | 28 | 320 | 36 |
| 9 | 17 | 12 | -7 | 8 | 24 | 12 | 10 | 12 | 16 | 180 | - | 105 | 10 | 456 |
| 9 | 11 | 5 | 7 | 8 | 24 | 12 | 5 | 12 | 16 | 180 | - | 210 | 10 | 456 |
| 10 | 14 | 18 | 4 | 8 | 4 | 6 | 10 | 84 | 16 | 342 | - | 70 | 320 | 456 |
| 10 | 5 | 19 | -4 | 8 | 4 | 3 | 5 | 84 | 16 | 171 | - | 35 | 320 | 456 |
| 11 | 6 | 11 | 5 | 8 | 8 | 24 | 12 | 84 | 16 | 9 | - | 14 | 320 | 36 |
| 11 | 12 | 18 | -5 | 8 | 8 | 24 | 12 | 84 | 16 | 18 | - | 7 | 320 | 36 |
| 12 | 10 | 3 | 3 | 2 | 24 | 3 | 5 | 84 | 16 | 180 | - | 28 | 30 | 12 |
| 12 | 20 | 7 | -3 | 2 | 24 | 6 | 10 | 84 | 16 | 180 | - | 28 | 30 | 12 |
| 13 | 4 | 15 | 4 | 8 | 4 | 6 | 10 | 84 | 16 | 342 | - | 70 | 320 | 456 |
| 13 | 8 | 12 | -4 | 8 | 4 | 3 | 5 | 84 | 16 | 171 | - | 35 | 320 | 456 |
| 14 | 20 | 6 | -6 | 2 | 4 | 21 | 12 | 12 | 288 | 9 | - | 105 | 320 | 456 |
| 14 | 17 | 14 | 6 | 2 | 4 | 42 | 12 | 12 | 288 | 18 | - | 210 | 320 | 456 |
| 15 | 18 | 10 | -3 | 2 | 24 | 6 | 10 | 84 | 16 | 180 | - | 28 | 30 | 12 |
| 15 | 13 | 8 | 3 | 2 | 24 | 3 | 5 | 84 | 16 | 180 | - | 28 | 30 | 12 |
| 16 | 11 | 1 | -1 | 8 | 4 | 42 | 3 | 156 | 96 | 18 | - | 28 | 30 | 456 |
| 16 | 22 | 10 | 1 | 8 | 4 | 21 | 6 | 156 | 96 | 9 | - | 28 | 30 | 456 |
| 17 | 5 | 13 | 2 | 8 | 24 | 24 | 11 | 6 | 288 | 9 | - | 7 | 10 | 456 |
| 17 | 10 | 15 | -2 | 8 | 24 | 24 | 22 | 6 | 288 | 18 | - | 14 | 10 | 456 |
| 18 | 9 | 5 | 6 | 2 | 4 | 42 | 12 | 12 | 288 | 18 | - | 210 | 320 | 456 |
| 18 | 18 | 4 | -6 | 2 | 4 | 21 | 12 | 12 | 288 | 9 | - | 105 | 320 | 456 |
| 19 | 1 | 21 | 0 | 2 | 8 | 12 | 4 | 6 | 32 | 36 | - | 28 | 10 | 24 |
| 19 | 2 | 3 | 0 | 2 | 8 | 12 | 4 | 6 | 32 | 36 | - | 28 | 10 | 24 |
| 20 | 21 | 4 | -6 | 2 | 4 | 21 | 12 | 12 | 288 | 9 | - | 105 | 320 | 456 |
| 20 | 19 | 17 | 6 | 2 | 4 | 42 | 12 | 12 | 288 | 18 | - | 210 | 320 | 456 |
| 21 | 3 | 17 | 3 | 2 | 24 | 3 | 5 | 84 | 16 | 180 | - | 28 | 30 | 12 |
| 21 | 6 | 9 | -3 | 2 | 24 | 6 | 10 | 84 | 16 | 180 | - | 28 | 30 | 12 |
| 22 | 22 | 2 | -6 | 2 | 4 | 21 | 12 | 12 | 288 | 9 | - | 105 | 320 | 456 |
| 22 | 21 | 20 | 6 | 2 | 4 | 42 | 12 | 12 | 288 | 18 | - | 210 | 320 | 456 |
| ord$(p,n)$ | | | | 2 | 4 | 3 | 1 | 6 | 16 | 9 | - | 7 | 10 | 12 |
| Alg1: Total (sec) | | | | 7.145 | 6.920 | 7.689 | 7.470 | 7.086 | 7.085 | 7.909 | - | 7.800 | 7.085 | 7.469 |
| Alg1: Avg. (sec) | | | | .157 | .147 | .164 | .159 | .151 | .151 | .168 | - | .166 | .151 | .159 |
| Alg2: Total (sec) | | | | 75.63 | 94.75 | 110.4 | 146.38 | * | * | * | - | * | * | * |
| Alg2: Avg. (sec) | | | | 1.609 | 2.016 | 2.349 | 3.114 | * | * | * | - | * | * | * |

Table 7: Elliptic curves over $\mathbb{F}_p$, where $p = 23$

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 2 | 2 | 4 | 10 | 12 | 32 | 18 | 44 | - | 10 | 24 |
| 0 | 0 | 2 | 0 | 2 | 2 | 4 | 10 | 12 | 32 | 18 | 44 | - | 10 | 24 |
| 1 | 18 | 22 | 5 | 8 | 2 | 14 | 40 | 39 | 288 | 18 | 11 | - | 30 | 456 |
| 1 | 14 | 2 | -5 | 8 | 2 | 7 | 40 | 78 | 288 | 18 | 22 | - | 30 | 456 |
| 2 | 21 | 16 | 0 | 2 | 2 | 4 | 10 | 12 | 32 | 18 | 44 | - | 10 | 24 |
| 2 | 26 | 12 | 0 | 2 | 2 | 4 | 10 | 12 | 32 | 18 | 44 | - | 10 | 24 |
| 3 | 12 | 5 | -4 | 8 | 20 | 8 | 120 | 6 | 16 | 360 | 264 | - | 320 | 36 |
| 3 | 19 | 11 | 4 | 8 | 20 | 8 | 120 | 3 | 16 | 360 | 264 | - | 320 | 36 |
| 4 | 15 | 28 | -1 | 8 | 20 | 3 | 120 | 21 | 16 | 72 | 506 | - | 10 | 36 |
| 4 | 2 | 21 | 1 | 8 | 20 | 6 | 120 | 42 | 16 | 72 | 253 | - | 10 | 36 |
| 5 | 4 | 21 | 6 | 2 | 20 | 3 | 40 | 42 | 96 | 360 | 22 | - | 320 | 456 |
| 5 | 16 | 23 | -6 | 2 | 20 | 6 | 40 | 21 | 96 | 360 | 11 | - | 320 | 456 |
| 6 | 20 | 18 | 6 | 2 | 20 | 3 | 40 | 42 | 96 | 360 | 22 | - | 320 | 456 |
| 6 | 22 | 28 | -6 | 2 | 20 | 6 | 40 | 21 | 96 | 360 | 11 | - | 320 | 456 |
| 7 | 16 | 26 | -4 | 8 | 20 | 8 | 120 | 6 | 16 | 360 | 264 | - | 320 | 36 |
| 7 | 6 | 5 | 4 | 8 | 20 | 8 | 120 | 3 | 16 | 360 | 264 | - | 320 | 36 |
| 8 | 24 | 10 | 1 | 8 | 20 | 6 | 120 | 42 | 16 | 72 | 253 | - | 10 | 36 |
| 8 | 9 | 22 | -1 | 8 | 20 | 3 | 120 | 21 | 16 | 72 | 506 | - | 10 | 36 |
| 9 | 5 | 19 | -8 | 8 | 12 | 3 | 10 | 39 | 16 | 18 | 132 | - | 30 | 456 |
| 9 | 20 | 7 | 8 | 8 | 12 | 6 | 10 | 78 | 16 | 18 | 132 | - | 30 | 456 |
| 10 | 22 | 14 | 3 | 2 | 12 | 8 | 10 | 12 | 288 | 18 | 11 | - | 320 | 36 |
| 10 | 1 | 25 | -3 | 2 | 12 | 8 | 10 | 12 | 288 | 18 | 22 | - | 320 | 36 |
| 11 | 6 | 17 | 5 | 8 | 2 | 14 | 40 | 39 | 288 | 18 | 11 | - | 30 | 456 |
| 11 | 24 | 20 | -5 | 8 | 2 | 7 | 40 | 78 | 288 | 18 | 22 | - | 30 | 456 |
| 12 | 1 | 27 | 6 | 2 | 20 | 3 | 40 | 42 | 96 | 360 | 22 | - | 320 | 456 |
| 12 | 4 | 13 | -6 | 2 | 20 | 6 | 40 | 21 | 96 | 360 | 11 | - | 320 | 456 |
| 13 | 8 | 13 | -9 | 2 | 20 | 14 | 10 | 3 | 16 | 360 | 88 | - | 320 | 456 |
| 13 | 3 | 17 | 9 | 2 | 20 | 7 | 10 | 6 | 16 | 360 | 88 | - | 320 | 456 |
| 14 | 10 | 9 | 6 | 2 | 20 | 3 | 40 | 42 | 96 | 360 | 22 | - | 320 | 456 |
| 14 | 11 | 14 | -6 | 2 | 20 | 6 | 40 | 21 | 96 | 360 | 11 | - | 320 | 456 |
| 15 | 14 | 1 | 2 | 8 | 12 | 7 | 10 | 42 | 288 | 360 | 11 | - | 320 | 36 |
| 15 | 27 | 8 | -2 | 8 | 12 | 14 | 10 | 21 | 288 | 360 | 22 | - | 320 | 36 |
| 16 | 26 | 6 | -2 | 8 | 12 | 14 | 10 | 21 | 288 | 360 | 22 | - | 320 | 36 |
| 16 | 17 | 19 | 2 | 8 | 12 | 7 | 10 | 42 | 288 | 360 | 11 | - | 320 | 36 |
| 1728 | 1 | 0 | 10 | 8 | 2 | 8 | 120 | 12 | 16 | 360 | 264 | - | 320 | 36 |
| 1728 | 2 | 0 | 4 | 8 | 4 | 8 | 120 | 3 | 16 | 360 | 264 | - | 320 | 36 |
| 1728 | 4 | 0 | -10 | 8 | 2 | 8 | 120 | 12 | 16 | 360 | 264 | - | 320 | 36 |
| 1728 | 8 | 0 | -4 | 8 | 4 | 8 | 120 | 6 | 16 | 360 | 264 | - | 320 | 36 |
| 18 | 7 | 15 | 2 | 8 | 12 | 7 | 10 | 42 | 288 | 360 | 11 | - | 320 | 36 |
| 18 | 28 | 4 | -2 | 8 | 12 | 14 | 10 | 21 | 288 | 360 | 22 | - | 320 | 36 |
| 19 | 19 | 20 | 10 | 8 | 2 | 8 | 120 | 12 | 16 | 360 | 264 | - | 320 | 36 |
| 19 | 18 | 15 | -10 | 8 | 2 | 8 | 120 | 12 | 16 | 360 | 264 | - | 320 | 36 |

Table 8: Elliptic curves over $\mathbb{F}_p$, where $p = 29$, $j = 0, \ldots, 19$.

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 | 23 | 12 | -6 | 2 | 20 | 6 | 40 | 21 | 96 | 360 | 11 | - | 320 | 456 |
| 20 | 5 | 9 | 6 | 2 | 20 | 3 | 40 | 42 | 96 | 360 | 22 | - | 320 | 456 |
| 21 | 25 | 8 | 7 | 8 | 12 | 4 | 120 | 21 | 16 | 18 | 11 | - | 320 | 12 |
| 21 | 13 | 6 | -7 | 8 | 12 | 4 | 120 | 42 | 16 | 18 | 22 | - | 320 | 12 |
| 22 | 3 | 23 | -3 | 2 | 12 | 8 | 10 | 12 | 288 | 18 | 22 | - | 320 | 36 |
| 22 | 12 | 10 | 3 | 2 | 12 | 8 | 10 | 12 | 288 | 18 | 11 | - | 320 | 36 |
| 23 | 27 | 4 | 6 | 2 | 20 | 3 | 40 | 42 | 96 | 360 | 22 | - | 320 | 456 |
| 23 | 21 | 3 | -6 | 2 | 20 | 6 | 40 | 21 | 96 | 360 | 11 | - | 320 | 456 |
| 24 | 11 | 7 | -9 | 2 | 20 | 14 | 10 | 3 | 16 | 360 | 88 | - | 320 | 456 |
| 24 | 15 | 27 | 9 | 2 | 20 | 7 | 10 | 6 | 16 | 360 | 88 | - | 320 | 456 |
| 25 | 28 | 2 | 0 | 2 | 2 | 4 | 10 | 12 | 32 | 18 | 44 | - | 10 | 24 |
| 25 | 25 | 16 | 0 | 2 | 2 | 4 | 10 | 12 | 32 | 18 | 44 | - | 10 | 24 |
| 26 | 9 | 11 | 3 | 2 | 12 | 8 | 10 | 12 | 288 | 18 | 11 | - | 320 | 36 |
| 26 | 7 | 1 | -3 | 2 | 12 | 8 | 10 | 12 | 288 | 18 | 22 | - | 320 | 36 |
| 27 | 17 | 24 | -2 | 8 | 12 | 14 | 10 | 21 | 288 | 360 | 22 | - | 320 | 36 |
| 27 | 10 | 18 | 2 | 8 | 12 | 7 | 10 | 42 | 288 | 360 | 11 | - | 320 | 36 |
| 28 | 13 | 3 | 8 | 8 | 12 | 6 | 10 | 78 | 16 | 18 | 132 | - | 30 | 456 |
| 28 | 23 | 24 | -8 | 8 | 12 | 3 | 10 | 39 | 16 | 18 | 132 | - | 30 | 456 |
| ord$(p,n)$ | | | | 2 | 2 | 1 | 10 | 3 | 16 | 18 | 11 | - | 10 | 12 |
| Alg1: Total (sec) | | | | 12.52 | 12.69 | 11.75 | 12.742 | 11.86 | 12.63 | 12.03 | 12.91 | - | 12.58 | 12.19 |
| Alg1: Avg. (sec) | | | | .205 | .208 | .193 | .209 | .194 | .207 | .197 | .217 | - | .203 | .200 |
| Alg2: Total (sec) | | | | 110.2 | 120.1 | 128.2 | 263.4 | * | * | * | * | - | * | * |
| Alg2: Avg. (sec) | | | | 1.806 | 1.967 | 2.102 | 4.318 | * | * | * | * | - | * | * |

Table 8(continued): Elliptic curves over $\mathbb{F}_p$, where $p = 29$, $j = 20, \ldots, 28$.

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | -4 | 1 | 6 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 0 | 0 | 3 | -11 | 6 | 3 | 6 | 20 | 12 | 288 | 18 | 264 | 840 | - | 36 |
| 0 | 0 | 5 | -7 | 3 | 2 | 6 | 60 | 4 | 288 | 18 | 264 | 840 | - | 36 |
| 0 | 0 | 7 | 11 | 3 | 6 | 6 | 20 | 12 | 288 | 18 | 264 | 840 | - | 36 |
| 0 | 0 | 11 | 7 | 6 | 1 | 6 | 60 | 4 | 288 | 18 | 264 | 840 | - | 36 |
| 0 | 0 | 15 | 4 | 2 | 3 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 1 | 28 | 6 | -9 | 4 | 6 | 48 | 10 | 12 | 16 | 24 | 22 | 280 | - | 152 |
| 1 | 4 | 7 | 9 | 4 | 3 | 48 | 5 | 12 | 16 | 24 | 11 | 280 | - | 152 |
| 2 | 7 | 17 | 0 | 4 | 4 | 6 | 20 | 8 | 32 | 6 | 44 | 56 | - | 8 |
| 2 | 1 | 25 | 0 | 4 | 4 | 6 | 20 | 8 | 32 | 6 | 44 | 56 | - | 8 |
| 3 | 18 | 26 | -2 | 6 | 10 | 48 | 5 | 12 | 16 | 120 | 11 | 28 | - | 12 |
| 3 | 7 | 20 | 2 | 3 | 5 | 48 | 10 | 12 | 16 | 120 | 22 | 28 | - | 12 |
| 4 | 22 | 18 | 0 | 4 | 4 | 6 | 20 | 8 | 32 | 6 | 44 | 56 | - | 8 |
| 4 | 12 | 21 | 0 | 4 | 4 | 6 | 20 | 8 | 32 | 6 | 44 | 56 | - | 8 |
| 5 | 23 | 16 | 2 | 3 | 5 | 48 | 10 | 12 | 16 | 120 | 22 | 28 | - | 12 |
| 5 | 21 | 29 | -2 | 6 | 10 | 48 | 5 | 12 | 16 | 120 | 11 | 28 | - | 12 |
| 6 | 15 | 1 | -7 | 3 | 10 | 6 | 60 | 4 | 288 | 18 | 264 | 840 | - | 36 |
| 6 | 11 | 27 | 7 | 6 | 5 | 6 | 60 | 4 | 288 | 18 | 264 | 840 | - | 36 |
| 7 | 6 | 19 | 10 | 6 | 4 | 6 | 5 | 56 | 288 | 24 | 33 | 28 | - | 152 |
| 7 | 23 | 17 | -10 | 3 | 4 | 6 | 10 | 56 | 288 | 24 | 66 | 28 | - | 152 |
| 8 | 2 | 27 | 3 | 4 | 10 | 6 | 30 | 56 | 16 | 120 | 253 | 28 | - | 12 |
| 8 | 18 | 16 | -3 | 4 | 5 | 6 | 15 | 56 | 16 | 120 | 506 | 28 | - | 12 |
| 9 | 24 | 14 | -2 | 6 | 10 | 48 | 5 | 12 | 16 | 120 | 11 | 28 | - | 12 |
| 9 | 30 | 6 | 2 | 3 | 5 | 48 | 10 | 12 | 16 | 120 | 22 | 28 | - | 12 |
| 10 | 16 | 30 | -1 | 3 | 3 | 48 | 5 | 56 | 16 | 120 | 132 | 28 | - | 36 |
| 10 | 20 | 4 | 1 | 6 | 6 | 48 | 10 | 56 | 16 | 120 | 132 | 28 | - | 36 |
| 11 | 17 | 28 | -8 | 6 | 5 | 48 | 30 | 56 | 16 | 18 | 11 | 168 | - | 152 |
| 11 | 29 | 12 | 8 | 3 | 10 | 48 | 15 | 56 | 16 | 18 | 22 | 168 | - | 152 |
| 12 | 21 | 20 | -5 | 6 | 4 | 48 | 55 | 56 | 96 | 120 | 22 | 840 | - | 4 |
| 12 | 3 | 13 | 5 | 3 | 4 | 48 | 110 | 56 | 96 | 120 | 11 | 840 | - | 4 |
| 13 | 1 | 29 | -8 | 6 | 5 | 48 | 30 | 56 | 16 | 18 | 11 | 168 | - | 152 |
| 13 | 9 | 8 | 8 | 3 | 10 | 48 | 15 | 56 | 16 | 18 | 22 | 168 | - | 152 |
| 14 | 11 | 9 | 2 | 3 | 5 | 48 | 10 | 12 | 16 | 120 | 22 | 28 | - | 12 |
| 14 | 6 | 26 | -2 | 6 | 10 | 48 | 5 | 12 | 16 | 120 | 11 | 28 | - | 12 |
| 15 | 8 | 15 | -6 | 4 | 3 | 48 | 110 | 4 | 288 | 6 | 22 | 28 | - | 152 |
| 15 | 10 | 2 | 6 | 4 | 6 | 48 | 55 | 4 | 288 | 6 | 11 | 28 | - | 152 |
| 16 | 13 | 5 | -6 | 4 | 3 | 48 | 110 | 4 | 288 | 6 | 22 | 28 | - | 152 |
| 16 | 24 | 11 | 6 | 4 | 6 | 48 | 55 | 4 | 288 | 6 | 11 | 28 | - | 152 |
| 17 | 30 | 2 | -8 | 6 | 5 | 48 | 30 | 56 | 16 | 18 | 11 | 168 | - | 152 |
| 17 | 22 | 23 | 8 | 3 | 10 | 48 | 15 | 56 | 16 | 18 | 22 | 168 | - | 152 |
| 18 | 29 | 4 | -4 | 3 | 6 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 18 | 13 | 15 | 4 | 6 | 3 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 19 | 12 | 7 | -8 | 6 | 5 | 48 | 30 | 56 | 16 | 18 | 11 | 168 | - | 152 |
| 19 | 15 | 3 | 8 | 3 | 10 | 48 | 15 | 56 | 16 | 18 | 22 | 168 | - | 152 |

Table 9: Elliptic curves over $\mathbb{F}_p$, where $p = 31$, $j = 0, \ldots, 19$.

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 | 25 | 12 | 5 | 3 | 4 | 48 | 110 | 56 | 96 | 120 | 11 | 840 | - | 4 |
| 20 | 8 | 14 | -5 | 6 | 4 | 48 | 55 | 56 | 96 | 120 | 22 | 840 | - | 4 |
| 21 | 20 | 22 | -4 | 3 | 6 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 21 | 25 | 5 | 4 | 6 | 3 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 22 | 5 | 21 | 10 | 6 | 4 | 6 | 5 | 56 | 288 | 24 | 33 | 28 | - | 152 |
| 22 | 14 | 9 | -10 | 3 | 4 | 6 | 10 | 56 | 288 | 24 | 66 | 28 | - | 152 |
| 1728 | 1 | 0 | 0 | 4 | 4 | 6 | 20 | 8 | 32 | 6 | 44 | 56 | - | 8 |
| 1728 | 3 | 0 | 0 | 4 | 4 | 6 | 20 | 8 | 32 | 6 | 44 | 56 | - | 8 |
| 24 | 3 | 25 | 1 | 6 | 6 | 48 | 10 | 56 | 16 | 120 | 132 | 28 | - | 36 |
| 24 | 27 | 24 | -1 | 3 | 3 | 48 | 5 | 56 | 16 | 120 | 132 | 28 | - | 36 |
| 25 | 19 | 24 | 7 | 6 | 5 | 6 | 60 | 4 | 288 | 18 | 264 | 840 | - | 36 |
| 25 | 16 | 28 | -7 | 3 | 10 | 6 | 60 | 4 | 288 | 18 | 264 | 840 | - | 36 |
| 26 | 14 | 3 | 4 | 6 | 3 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 26 | 2 | 19 | -4 | 3 | 6 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 27 | 27 | 8 | -3 | 4 | 5 | 6 | 15 | 56 | 16 | 120 | 506 | 28 | - | 12 |
| 27 | 26 | 30 | 3 | 4 | 10 | 6 | 30 | 56 | 16 | 120 | 253 | 28 | - | 12 |
| 28 | 10 | 11 | 4 | 6 | 3 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 28 | 28 | 18 | -4 | 3 | 6 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 29 | 9 | 13 | -4 | 1 | 6 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 29 | 19 | 10 | 4 | 2 | 3 | 6 | 60 | 12 | 288 | 18 | 88 | 280 | - | 36 |
| 30 | 26 | 10 | 5 | 1 | 4 | 48 | 110 | 56 | 96 | 120 | 11 | 840 | - | 4 |
| 30 | 17 | 22 | -5 | 2 | 4 | 48 | 55 | 56 | 96 | 120 | 22 | 840 | - | 4 |
| ord$(p,n)$ | | | | 1 | 1 | 6 | 5 | 4 | 16 | 6 | 11 | 28 | - | 4 |
| Alg1: Total (sec) | | | | 15.27 | 15.65 | 15.00 | 15.27 | 15.16 | 15.43 | 15.43 | 15.54 | 15.87 | - | 15.60 |
| Alg1: Avg. (sec) | | | | .228 | .234 | .224 | .228 | .226 | .230 | .230 | .232 | .237 | - | .233 |
| Alg2: Total (sec) | | | | 127.6 | 134.0 | 130.7 | 1090.0 | * | * | * | * | * | - | * |
| Alg2: Avg. (sec) | | | | 1.905 | 2.000 | 1.950 | 16.28 | * | * | * | * | * | - | * |

Table 9 (continued): Elliptic curves over $\mathbb{F}_p$, where $p = 31$, $j = 20, \ldots, 30$.

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | -10 | 3 | 8 | 6 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 0 | 0 | 2 | -11 | 2 | 24 | 3 | 20 | 12 | 288 | 18 | 176 | 280 | 30 | - |
| 0 | 0 | 3 | -1 | 3 | 24 | 42 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 0 | 0 | 5 | 1 | 6 | 24 | 3 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 0 | 0 | 6 | 10 | 6 | 8 | 3 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 0 | 0 | 9 | 11 | 1 | 24 | 6 | 20 | 12 | 288 | 18 | 176 | 280 | 30 | - |
| 1 | 7 | 23 | 3 | 4 | 4 | 3 | 10 | 12 | 96 | 40 | 528 | 28 | 30 | - |
| 1 | 28 | 36 | -3 | 4 | 4 | 6 | 5 | 12 | 96 | 40 | 528 | 28 | 30 | - |
| 2 | 30 | 14 | 8 | 3 | 4 | 21 | 5 | 168 | 16 | 18 | 22 | 280 | 30 | - |
| 2 | 9 | 1 | -8 | 6 | 4 | 42 | 10 | 168 | 16 | 18 | 22 | 280 | 30 | - |
| 3 | 18 | 1 | 8 | 3 | 4 | 21 | 5 | 168 | 16 | 18 | 22 | 280 | 30 | - |
| 3 | 35 | 8 | -8 | 6 | 4 | 42 | 10 | 168 | 16 | 18 | 22 | 280 | 30 | - |
| 4 | 15 | 7 | 4 | 6 | 24 | 6 | 110 | 168 | 16 | 6 | 22 | 28 | 192 | - |
| 4 | 23 | 19 | -4 | 3 | 24 | 3 | 55 | 168 | 16 | 6 | 22 | 28 | 192 | - |
| 5 | 17 | 3 | -7 | 3 | 4 | 12 | 110 | 168 | 288 | 40 | 22 | 840 | 6 | - |
| 5 | 31 | 24 | 7 | 6 | 4 | 12 | 55 | 168 | 288 | 40 | 22 | 840 | 6 | - |
| 6 | 34 | 6 | -2 | 2 | 4 | 24 | 30 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 6 | 25 | 11 | 2 | 1 | 4 | 24 | 15 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 7 | 8 | 21 | -8 | 6 | 4 | 42 | 10 | 168 | 16 | 18 | 22 | 280 | 30 | - |
| 7 | 32 | 20 | 8 | 3 | 4 | 21 | 5 | 168 | 16 | 18 | 22 | 280 | 30 | - |
| 8 | 12 | 13 | 0 | 4 | 8 | 12 | 20 | 24 | 32 | 2 | 22 | 56 | 6 | - |
| 8 | 11 | 30 | 0 | 4 | 8 | 12 | 20 | 24 | 32 | 2 | 22 | 56 | 6 | - |
| 9 | 23 | 28 | 2 | 3 | 4 | 24 | 15 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 9 | 18 | 2 | -2 | 6 | 4 | 24 | 30 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 10 | 3 | 31 | 6 | 4 | 24 | 42 | 10 | 168 | 288 | 8 | 22 | 28 | 192 | - |
| 10 | 12 | 26 | -6 | 4 | 24 | 21 | 5 | 168 | 288 | 8 | 22 | 28 | 192 | - |
| 11 | 5 | 27 | 6 | 4 | 24 | 42 | 10 | 168 | 288 | 8 | 22 | 28 | 192 | - |
| 11 | 20 | 31 | -6 | 4 | 24 | 21 | 5 | 168 | 288 | 8 | 22 | 28 | 192 | - |
| 12 | 2 | 33 | -4 | 3 | 24 | 3 | 55 | 168 | 16 | 6 | 22 | 28 | 192 | - |
| 12 | 8 | 5 | 4 | 6 | 24 | 6 | 110 | 168 | 16 | 6 | 22 | 28 | 192 | - |
| 13 | 27 | 20 | 4 | 6 | 24 | 6 | 110 | 168 | 16 | 6 | 22 | 28 | 192 | - |
| 13 | 34 | 12 | -4 | 3 | 24 | 3 | 55 | 168 | 16 | 6 | 22 | 28 | 192 | - |
| 14 | 13 | 11 | 7 | 2 | 4 | 12 | 55 | 168 | 288 | 40 | 22 | 840 | 6 | - |
| 14 | 15 | 14 | -7 | 1 | 4 | 12 | 110 | 168 | 288 | 40 | 22 | 840 | 6 | - |
| 15 | 20 | 34 | -2 | 6 | 4 | 24 | 30 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 15 | 6 | 13 | 2 | 3 | 4 | 24 | 15 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 16 | 21 | 32 | 1 | 6 | 24 | 21 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 16 | 10 | 34 | -1 | 3 | 24 | 42 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 17 | 14 | 9 | 10 | 6 | 8 | 3 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 17 | 19 | 35 | -10 | 3 | 8 | 6 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 18 | 33 | 8 | -2 | 6 | 4 | 24 | 30 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 18 | 21 | 27 | 2 | 3 | 4 | 24 | 15 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 19 | 31 | 12 | -5 | 6 | 8 | 24 | 10 | 168 | 16 | 40 | 528 | 28 | 30 | - |
| 19 | 13 | 22 | 5 | 3 | 8 | 24 | 5 | 168 | 16 | 40 | 528 | 28 | 30 | - |

Table 10: Elliptic curves over $\mathbb{F}_p$, where $p = 37$, $j = 0, \ldots, 19$.

| $j$ | $a$ | $b$ | $a_p$ | $d_3$ | $d_5$ | $d_7$ | $d_{11}$ | $d_{13}$ | $d_{17}$ | $d_{19}$ | $d_{23}$ | $d_{29}$ | $d_{31}$ | $d_{37}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 | 16 | 5 | 4 | 6 | 24 | 6 | 110 | 168 | 16 | 6 | 22 | 28 | 192 | - |
| 20 | 27 | 3 | -4 | 3 | 24 | 3 | 55 | 168 | 16 | 6 | 22 | 28 | 192 | - |
| 21 | 32 | 10 | 2 | 3 | 4 | 24 | 15 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 21 | 17 | 6 | -2 | 6 | 4 | 24 | 30 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 22 | 19 | 36 | -7 | 3 | 4 | 12 | 110 | 168 | 288 | 40 | 22 | 840 | 6 | - |
| 22 | 2 | 29 | 7 | 6 | 4 | 12 | 55 | 168 | 288 | 40 | 22 | 840 | 6 | - |
| 23 | 22 | 30 | -3 | 4 | 4 | 6 | 5 | 12 | 96 | 40 | 528 | 28 | 30 | - |
| 23 | 14 | 18 | 3 | 4 | 4 | 3 | 10 | 12 | 96 | 40 | 528 | 28 | 30 | - |
| 24 | 28 | 18 | -10 | 3 | 8 | 6 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 24 | 1 | 33 | 10 | 6 | 8 | 3 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 25 | 9 | 19 | 5 | 3 | 8 | 24 | 5 | 168 | 16 | 40 | 528 | 28 | 30 | - |
| 25 | 36 | 4 | -5 | 6 | 8 | 24 | 10 | 168 | 16 | 40 | 528 | 28 | 30 | - |
| 1728 | 1 | 0 | 2 | 1 | 4 | 24 | 15 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 1728 | 2 | 0 | -12 | 4 | 4 | 24 | 60 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 1728 | 3 | 0 | -2 | 2 | 4 | 24 | 30 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 1728 | 5 | 0 | 12 | 4 | 4 | 24 | 60 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 27 | 11 | 15 | 3 | 4 | 4 | 3 | 10 | 12 | 96 | 40 | 528 | 28 | 30 | - |
| 27 | 7 | 9 | -3 | 4 | 4 | 6 | 5 | 12 | 96 | 40 | 528 | 28 | 30 | - |
| 28 | 29 | 16 | -8 | 6 | 4 | 42 | 10 | 168 | 16 | 18 | 22 | 280 | 30 | - |
| 28 | 5 | 17 | 8 | 3 | 4 | 21 | 5 | 168 | 16 | 18 | 22 | 280 | 30 | - |
| 29 | 35 | 4 | 6 | 4 | 24 | 42 | 10 | 168 | 288 | 8 | 22 | 28 | 192 | - |
| 29 | 29 | 32 | -6 | 4 | 24 | 21 | 5 | 168 | 288 | 8 | 22 | 28 | 192 | - |
| 30 | 1 | 35 | -2 | 6 | 4 | 24 | 30 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 30 | 4 | 21 | 2 | 3 | 4 | 24 | 15 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 31 | 25 | 24 | 6 | 4 | 24 | 42 | 10 | 168 | 288 | 8 | 22 | 28 | 192 | - |
| 31 | 26 | 7 | -6 | 4 | 24 | 21 | 5 | 168 | 288 | 8 | 22 | 28 | 192 | - |
| 32 | 4 | 29 | 10 | 6 | 8 | 3 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 32 | 16 | 10 | -10 | 3 | 8 | 6 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 33 | 26 | 22 | 11 | 3 | 24 | 6 | 20 | 12 | 288 | 18 | 176 | 280 | 30 | - |
| 33 | 30 | 28 | -11 | 6 | 24 | 3 | 20 | 12 | 288 | 18 | 176 | 280 | 30 | - |
| 34 | 24 | 26 | -2 | 6 | 4 | 24 | 30 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 34 | 22 | 23 | 2 | 3 | 4 | 24 | 15 | 12 | 16 | 40 | 176 | 28 | 192 | - |
| 35 | 6 | 25 | 1 | 6 | 24 | 21 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 35 | 24 | 15 | -1 | 3 | 24 | 42 | 60 | 12 | 288 | 18 | 528 | 840 | 30 | - |
| 36 | 36 | 2 | -9 | 4 | 24 | 24 | 15 | 168 | 16 | 18 | 22 | 28 | 192 | - |
| 36 | 33 | 16 | 9 | 4 | 24 | 24 | 30 | 168 | 16 | 18 | 22 | 28 | 192 | - |
| ord$(p,n)$ | | | | 1 | 4 | 3 | 5 | 12 | 16 | 2 | 22 | 28 | 6 | - |
| Alg1: Total (sec) | | | | 23.45 | 21.97 | 22.35 | 22.30 | 22.08 | 21.09 | 22.74 | 22.85 | 22.57 | 22.68 | - |
| Alg1: Avg. (sec) | | | | .293 | .275 | .279 | .279 | .276 | .264 | .284 | .286 | .282 | .284 | - |
| Alg2: Total (sec) | | | | 169.2 | 117.7 | 226.3 | 977.1 | * | * | * | * | * | * | - |
| Alg2: Avg. (sec) | | | | 2.115 | 2.221 | 2.827 | 12.21 | * | * | * | * | * | * | - |

Table 10(continued): Elliptic curves over $\mathbb{F}_p$, where $p = 37$, $j = 19, \ldots, 36$.

# Vita

| | |
|---|---|
| **Name** | Adam Leonard Van Tuyl |
| **Place and Date of Birth** | Welland, Ontario, March 20, 1974 |
| **Education** | Bachelor of Science (Honours in Mathematics) |
| | Majored in Mathematics and Philosophy |
| | Calvin College, Grand Rapids, Michigan |
| | (1992-96) |
| **Experience** | •Teaching Assistant (Queen's University) |
| | (Sept. 1996 - May 1997) |
| | •Research Assistant (Simon Fraser University) |
| | (May 1995 - Aug. 1995) |
| | •Tutor (Calvin College) |
| | (Sept. 1994 - May 1996) |
| | •Grader (Calvin College) |
| | (Sept. 1993 - May 1996) |
| | •Computer Lab Assistant (Calvin College) |
| | (Sept. 1993 - May 1996) |
| **Awards** | •R.S. McLaughlin Fellowship (Queen's University) |
| | (Sept. 1996 - May 1997) |
| | •William Rink Memorial Prize (Calvin College) |
| | (May 1996) |
| | •NSERC Undergraduate Research Award (Simon Fraser University) |
| | (May 1995 - Aug. 1995) |
| | •Presidential Scholarship (Calvin College) |
| | (Sept. 1992 - May 1996) |

# Bibliography


[At] A.O.L. Atkin, Public email messages. 1990-1992.

[Ca] J.W.S. Cassels, *Lectures on Elliptic Curves.* Cambridge University Press: Cambridge, 1991.

[Cr] J.E. Cremona, *Algorithms for Modular Elliptic Curves.* Cambridge University Press: Cambridge, 1992.

[De] Pierre Deligne, Formes Modulaires et Représentations $l$-adiques, Seminaire Bourbaki, no. 355. (1968/69).

[Ha] Robin Hartshorne, *Algebraic Geometry.* Springer-Verlag: New York, 1977.

[HoKu] Kenneth Hoffman, Ray Kunze, *Linear Algebre.* Prentice-Hall, Inc.: Englewood Cliffs, New Jersey, 1971.

[Ig] Jun-ichi Igusa, Fibre systems of Jacobian varieties III. (Fibre systems of elliptic curves). *Amer. J. Math.* **81** (1959) 453-476.

[Ka] Ernst Kani, Private Conversation, August 1997.

[KaSc] Ernst Kani, Wolfgang Schanz, Modular diagonal quotient surfaces, to appear in *Math. Z.*

[KaRo] Ernst Kani, Micheal Rosen, Idempotent relations and factors of Jacobians. *Math. Ann.* **284** (1989) 307-327.

[La1] Serge Lang, *Elliptic Curves: Diophantine Analysis.* Springer-Verlag, 1983.

[La2] Serge Lang, *Elliptic Functions. 2nd ed.* Springer-Verlag, 1987.

[LiHa] Rudolf Lidl, Harald Niederreiter, *Introduction to finite fields and their applications.* Cambridge University Press: Cambridge, 1986

[Sc1] Rene Schoof, Ellptic curves over finite fields and the computation of square roots mod p. *Math. Comp.* **44** (1985), 483-494.

[Sc2] Rene Schoof, Counting Points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux* **7** (1995), 219-254.

[Si] Joseph H. Silverman, *The Arithmetic of Elliptic Curves.* Springer-Verlag: New York, 1986.

[SiTa] Joseph H. Silverman, John Tate, *Rational Points on Elliptic Curves.* Springer-Verlag: New York, 1992.

[Sm] Charles Small, *Arithmetic of Finite Fields.* Marcel Dekker, Inc.: New York, 1991.

[St] Ian Stewart, *Galois Theory.* Chapman and Hall: London, 1973.

[Wi] Andrew Wiles, Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)* **141** (1995), no. 3, 443–551

[Yu] Noriko Yui, Explicit form of the modular equation. *J. Reine Angew. Math.* **299/300** (1978), 185-200.