To appear in the *International Journal of Computer Mathematics*
Vol. 00, No. 00, Month 20XX, 1–13

Elliptic curves with $j = 0, 1728$ *and low embedding degree*

J.M. Miret[a], D. Sadornil[b*] and J.Tena[c]

[a]*Dept. de Matemàtica. Universitat de Lleida. Spain;*
[b]*Dept. de Matemáticas, Estadística y Computación. Universidad de Cantabria. Spain*
[c]*IMUVA and Dept. de Álgebra, Análisis Matemático, Geometría y Topología. Universidad de Valladolid. Spain.*

(*Received 00 Month 20XX; final version received 00 Month 20XX*)

Elliptic curves over a finite field $\mathbb{F}_q$ with j-invariant 0 or 1728, both supersingular and ordinary, whose embedding degree k is low are studied. In the ordinary case we give conditions characterizing such elliptic curves with fixed embedding degree with respect to a subgroup of prime order ℓ. For $k = 1, 2$, these conditions give parameterizations of q in terms of ℓ and two integers m, n. We show several examples of families with infinitely many curves. Similar parameterizations for $k \geq 3$ need a fixed kth root of the unity in the underlying field. Moreover, when the elliptic curve admits distortion maps, an example is provided.

Keywords: Elliptic curves, Embedding degree, Distorsion maps, Pairing-based Cryptography, Bateman-Horn's Conjecture.

2010 AMS Subject Classification: 14H52, 94A60.

1. Introduction

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, with $q = p^r$, p prime, $p \geq 5$, given by its Weiertrass model $y^2 = x^3 + Ax + B$; $A, B \in \mathbb{F}_q$. For general results on elliptic curves we refer to [21] and for their cryptographic applications to [4]. Let us remember that the cardinality $N = \#E(\mathbb{F}_q)$ is given by $N = q + 1 - t$, where t, the trace of the Frobenius endomorphism, satisfies (Hasse theorem) $|t| \leq 2\sqrt{q}$. When $p \nmid t$ the curve $E/\mathbb{F}_q$ is called ordinary and its endomorphism ring $End(E)$ can be embedded as an order in the quadratic imaginary field $K = \mathbb{Q}(\sqrt{t^2 - 4q})$, while if $p \mid t$ the curve is called supersingular and $End(E)$ can be considered as an order in a quaternion algebra.

Let $E(\mathbb{F}_q)$ be the set of rational points of E over the finite field $\mathbb{F}_q$. This set can be endowed with a structure of abelian group. This group was proposed to be used in discrete logarithm cryptosystems instead of the multiplicative group $\mathbb{F}_q^*$ as it is stronger against cryptanalytic attacks. However, Menezes-Okamoto-Vanstone (MOV) and Frey-Rück (FR) algorithms allow, using pairings (Weil, Tate, etc), the translation of the Discrete Logarithm Problem (DLP) on the points of $E(\mathbb{F}_q)$ to the DLP on a field extension $\mathbb{F}_{q^k}$ (see [4] or [16]). The natural number k (the embedding degree) is characterized by the following definition.

This work has been partially supported by the Spanish Ministerio de Ciencia e Innovacion under grants MTM2010-16051 and MTM2013-46949-P and MTM2014-55421-P.

*Corresponding author. Email: daniel.sadornil@unican.es

DEFINITION 1.1 *Let ℓ be a divisor of $N = \#E(\mathbb{F}_q)$ (usually ℓ a prime). The embedding degree of $E/\mathbb{F}_q$ with respect to ℓ is the smallest natural integer k verifying the equivalent conditions:*

i) $\ell \mid (q^k - 1)$.
ii) $\mathbb{F}_{q^k}^*$ *contains a cyclic subgroup of order* ℓ.

If ℓ is the greatest prime divisor of $N = \#E(\mathbb{F}_q)$, then k is called the embedding degree of $E/\mathbb{F}_q$.

It is also worth nothing the following result by Balasubramanian and Koblitz [1]: if $k > 1$ the conditions i) and ii) are equivalent to

iii) $E(\mathbb{F}_{q^k})$ *contains the full ℓ-torsion group* $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

Nevertheless, if $k = 1$, the group $E[\ell](\mathbb{F}_q)$ can be either cyclic (of order ℓ) or the full group $E[\ell]$.

The DLP on elliptic curves with small k could be vulnerable to MOV and FR attacks. However, curves with small embedding degree are suitable in Pairing-based Cryptography [5]. For both destructive and constructive reasons, it is advisable to know the embedding degree of a given elliptic curve. Supersingular elliptic curves have embedding degree less than or equal to 6 (in fact, in this paper, since characteristic $p \neq 2, 3$, $k = 1, 2, 3$), while ordinary curves with small degree are scarce [1].

Elliptic curve cryptosystems work on a cyclic subgroup $\langle P \rangle \subseteq E(\mathbb{F}_q)$ of order ℓ (usually a prime). Nevertheless, the alternating property of the Weil pairing e_ℓ implies that e_ℓ is trivial for every couple of points $Q, R \in \langle P \rangle$. The same happens frequently for the Tate pairing, [5, Chapter IX]. To avoid this obstacle, a modified pairing is used, employing a distortion map.

DEFINITION 1.2 *A distortion map for a point $P \in E(\mathbb{F}_q)$ of prime order ℓ, coprime with p, is an endomorphism σ of E defined over $\mathbb{F}_{q^k}$ such that $\sigma(P) \notin \langle P \rangle$ ($e_\ell(P, \sigma(P)) \neq 1$).*

Distortion maps always exist on supersingular elliptic curves but never for ordinary elliptic curves with embedding degree greater than 1 (see [22]). For ordinary curves with $k = 1$ they can exist only if $E[\ell] \subseteq E(\mathbb{F}_q)$. Nevertheless, in this case, ℓ must satisfy other conditions to guarantee the existence of a distortion map, see Theorem 2.1 of [7].

In this paper, we will study the embedding degree and distortion maps for curves with invariant $j = 1728$ (i.e. with Weiertrass equation $y^2 = x^3 + Ax$) and $j = 0$ (curves with equation $y^2 = x^3 + B$). These curves are well studied in the classical theory of elliptic curves [21]. Since the Weierstrass form of these curves is very simple, addition and doubling can be computed efficiently. These curves can be supersingular or ordinary and we consider both cases separately. Elliptic curves with $j = 0$ and embedding degree 1 have been studied recently in [13] by Kirlar.

Our interest is focused on the characterization of families of curves for different small embedding degrees and not on implementation considerations, such as performance and cryptographic security requirements.

The paper is structured as follows. Section 2 recalls some basic information on elliptic curves with j-invariant 0 and 1728. Section 3 is devoted to supersingular curves, while ordinary elliptic curves are studied in Section 4. Finally, some particular families and examples are given in Section 5. From numerical experiments, we can deduce that the number of elliptic curves of the families with embedding degree 1 or 2 closely approaches the expected value given by the Bateman-Horn's conjecture [3].

2. Elliptic curves with j-invariant 0 and 1728

Isomorphism classes and some information about the cardinality of the elliptic curves with j-invariant 1728 or 0 were provided in [19]. In the present paper we will use those number theoretic results as a tool and apply them to the aim stated above. In order to be self-contained, in this section we recall such results from [19].

PROPOSITION 2.1 *([19, Proposition 3.1]) The number of isomorphim classes of elliptic curves with j-invariant 1728 over $\mathbb{F}_q$, $q = p^r$ is given by*

i) If $q \equiv 3 \pmod 4$ (so $p \equiv 3 \pmod 4$ and r odd) then there exist two isomorphism classes with representatives,

$$y^2 = x^3 + x, \qquad y^2 = x^3 - x. \tag{1}$$

Both curves are supersingular.

ii) If $q \equiv 1 \pmod 4$ then there exist four isomorphism classes with representatives,

$$E_i : y^2 = x^3 + \omega^i x, \quad 0 \leq i \leq 3, \tag{2}$$

where ω is a generator of $\mathbb{F}_q^*$. For $p \equiv 3 \pmod 4$, so r even, these curves are supersingular, otherwise the curves are ordinary.

Remark. The curve E_0 and its quadratic twisted E_2 are independent of the particular generator ω, but E_1, E_3 can be interchanged when changing it.

LEMMA 2.2 *([19, Proposition 3.5]) The traces t_i of the Frobenius endomorphisms of the curves E_i given in (2) verify:*

$$t_0, t_2 \equiv 2 \pmod 4, \ t_1, t_3 \equiv 0 \pmod 4,$$

$$t_0/2 \equiv 1 \pmod 4 \ \text{ and } \ t_2/2 \equiv 3 \pmod 4.$$

PROPOSITION 2.3 *([19, Proposition 2.1]) The number of isomorphim classes of elliptic curves with j-invariant 0 over $\mathbb{F}_q$, $q = p^r$ is given by*

i) If $q \equiv 2 \pmod 3$ then there exist two isomorphism classes with representatives,

$$y^2 = x^3 + 1, \qquad y^2 = x^3 + B, \ \ B \in \mathbb{F}_q^* - (\mathbb{F}_q^*)^2. \tag{3}$$

Both curves are supersingular.

ii) If $q \equiv 1 \pmod 3$ then there exist six isomorphism classes with representatives,

$$E_i' : y^2 = x^3 + \omega^i, \ 0 \leq i \leq 5, \tag{4}$$

where ω is a generator of $\mathbb{F}_q^*$. For $p \equiv 2 \pmod 3$, so r even, these six curves are supersingular, otherwise the curves are ordinary.

Remark. E_0', E_1' and E_2' are respectively a quadratic twist of E_3', E_1' and E_5'. There is an ambiguity in the identification of $E_1^{'}$ or $E_5{'}$ (resp. $E_2^{'}$ and $E_4{'}$). They depend on

the generator ω we take for $\mathbb{F}_q^*$. For instance, giving two generators ω, ω' such that $\omega = (\omega')^j$; $j \equiv 5 \pmod 6$ then the curve $E_1' : y^2 = x^3 + \omega$ could be also read as $E_5' : y^2 = x^3 + (\omega')^5$. Only E_0', E_3' are independent of the particular generator ω.

LEMMA 2.4 *([19, Proposition 2.3]) The traces t_i' of the Frobenius endomorphisms of the curves E_i' given in (4) verify:*

$$t_0' \equiv 2 \pmod 6,\ t_3' \equiv 4 \pmod 6,\ t_1', t_5' \equiv 1 \pmod 6 \text{ and } t_2', t_4' \equiv -1 \pmod 6.$$

3. The supersingular case

The taxonomy of supersingular elliptic curves and their embedding degree is well established, see for instance [16]. The determination of the cardinality of supersingular curves with $j = 1728$ or 0 is already given in [19] and consequently their insertion in such classification is easy. We summarize those results in the following subsections, giving also a distortion map for each curve. Some of these distortions can be found in [5], while others are adaptations of the general method suggested in [22].

3.1 *Supersingular curves with $j = 1728$*

The cardinality of these curves is given by the following result.

LEMMA 3.1 *([19, Section 3]) For the supersingular elliptic curves given in Proposition 2.1 we have:*

i) $y^2 = x^3 + x$, $y^2 = x^3 - x$ *have cardinality* $q + 1$ *over* $\mathbb{F}_q$, $q \equiv 3 \pmod 4$.
ii) E_1 *and* E_3 *have cardinality* $q+1$, E_0 *has cardinality* $q+1\pm 2\sqrt{q}$ *and* E_2 *has cardinality* $q+1\mp 2\sqrt{q}$ *over* $\mathbb{F}_q$, $q \equiv 1 \pmod 4$, $q = p^r$ *(the sign corresponds to* $r \equiv 2, 0 \pmod 4$*).*

Curves with equation (1) have embedding degree $k = 2$. According to [16] their groups of points are isomorphic to either $\mathbb{Z}/(q+1)\mathbb{Z}$ or $\mathbb{Z}/(q+1)/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For any prime divisor $\ell \neq 2$ of their group order and for any $P = (x, y)$ of order ℓ a distortion map is given by

$$\sigma(x, y) = (-x, \sqrt{-1}y). \tag{5}$$

Since $\sqrt{-1} \notin \mathbb{F}_q$, both points P and $\sigma(P)$ are linearly independent over $\mathbb{F}_q$.

The curves E_1, E_3 have cyclic groups and embedding degree $k = 2$. Now as $\sqrt{-1} \in \mathbb{F}_q$, then (5) is not a distortion map. Nevertheless, we can take (for any prime $\ell \neq 2$) the map,

$$\sigma(x, y) = \left(\omega^{i(\frac{1-p}{2})}x^p, \sqrt{\omega^{i(\frac{3(1-p)}{2})}}y^p\right). \tag{6}$$

The curves E_0, E_2 have rational groups $\mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z}$ and embedding degree $k = 1$. Since these groups contain the full group of ℓ-torsion, the map given in (5) is also a distortion map for any point P of order ℓ, except if P is an eigenvector for the endomorphism σ.

3.2 *Supersingular curves with $j = 0$*

The cardinality of these curves is given by the following result.

LEMMA 3.2 *([19, Section 2] For the curves of Proposition 2.3 we have:*

i) $y^2 = x^3 + 1$, $y^2 = x^3 + B$ *have cardinality* $q + 1$ *over* $\mathbb{F}_q$, $q \equiv 2 \pmod 3$.
ii) E'_0 *has cardinality* $q + 1 \pm 2\sqrt{q}$ *and* E'_3 *has cardinality* $q + 1 \mp 2\sqrt{q}$ *over* $\mathbb{F}_q$, $q \equiv 1 \pmod 3$, $q = p^r$ *(the sign corresponds to* $r \equiv 2, 0 \pmod 4$*).*
iii) E'_1 *and* E'_4 *are quadratic twist. The same occurs with* E'_2 *and* E'_5. E'_1 *and* E'_5 *have cardinality* $q + 1 \pm \sqrt{q}$ *and* E'_2 *and* E'_4 *have cardinality* $q + 1 \mp \sqrt{q}$ *over* $\mathbb{F}_q$, $q \equiv 1 \pmod 3$, $q = p^r$ *(the sign corresponds to* $r \equiv 2, 0 \pmod 4$*).*

Curves with equation (3) have embedding degree $k = 2$ and group cyclic or isomorphic to $\mathbb{Z}/(q+1)/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For any prime divisor $\ell \neq 3$ dividing the cardinality and for any $P = (x, y)$ of order ℓ a distortion map is given by

$$\sigma(x, y) = (\zeta_3 x, y) \tag{7}$$

with $\zeta_3^2 + \zeta_3 + 1 = 0$ over $\mathbb{F}_q$.

E'_0, E'_3 have groups isomorphic to $\mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z}$ and embedding degree $k = 1$. For any prime $\ell \neq 3$ dividing $\#E(\mathbb{F}_q)$ the above map is a distortion map for any point $P = (x, y)$ not eigenvector of σ.

The four curves E'_1, E'_2, E'_4, E'_5 have cyclic groups, embedding degree $k = 3$ and if $\alpha \in \mathbb{F}_{q^3}$ such that $\alpha^3 = \omega^i$, $i = 1, 2, 4, 5$, a distortion map is:

$$\sigma(x, y) = \left(\frac{x^p}{\alpha \omega^{i(p-2)/3}}, \frac{y^p}{\omega^{i(p-1)/2}} \right). \tag{8}$$

4. The ordinary case

Several constructions of ordinary elliptic curves with small embedding degree can be found in the literature, for example [2], [5, Chapter IX], [9], [17], [13], [14] or [11]. Most of them are based on the following idea: Given an embedding degree k, look for a suitable equation $t^2 - 4q = Dh^2$ with a small D and then determine an elliptic curve with discriminant D and cardinality $q + 1 - t$ using the complex multiplication method. Our approach is, in some way, opposite to this because we impose $D = -1, -3$ (i.e. $j = 1728, 0$) and we look for suitable values of ℓ and q that guarantee the desired k.

According to Propositions 2.1 and 2.3, elliptic curves over $\mathbb{F}_q$ are ordinary if $j = 1728$ and $p \equiv 1 \pmod 4$ and if $j = 0$ and $p \equiv 1 \pmod 3$. To characterize when these elliptic curves have low embedding degree we will take advantage of the following result, given by Cocks and Pinch [6].

LEMMA 4.1 *An elliptic curve E has embedding degree k with respect to ℓ if and only if $t \equiv 1 + \zeta_k \pmod \ell$, for ζ_k a kth root of unity modulo ℓ.*

Thus, as t is the trace of the Frobenius endomorphism π, first we have to impose conditions for it, so that one of four elements in $\mathbb{Z}[\sqrt{-1}]$ (respectively six elements in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$), with norm q has the right trace. Then we have to decide which of the four curves E_i (respectively six curves E'_i) corresponds to such π. For this purpose Lemmas

2.2 and 2.4 will be useful.

To continue, we will study separately the cases of embedding degree $k = 1, 2$ and higher.

4.1 *Embedding degree 1*

According to Lemma 4.1, the trace of the Frobenius endomorphism of an elliptic curve with embedding degree $k = 1$ with respect to ℓ must be $t \equiv 2 \pmod{\ell}$.

We first consider elliptic curves with $j = 1728$. In this case, the endomorphism ring $\mathcal{O}$ is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$.

THEOREM 4.2 *One of the four curves $E_i : y^2 = x^3 + \omega^i x$ has embedding degree 1 with respect to ℓ if and only if*

$$q = (m^2 + n^2)\ell^2 + 2m\ell + 1, \quad m, n \in \mathbb{Z},\ m \equiv n \pmod 2. \tag{9}$$

Such a curve has cardinality $(m^2 + n^2)\ell^2$.

Proof. Since $j = 1728$, the Frobenius endomorphism can be written as $\pi = a + b\sqrt{-1}$ for some integers a, b, in the ring $\mathcal{O}_K$. From Lemma 4.1, its trace satisfies $t = 2a = 2 + 2m\ell$, hence $a = 1 + m\ell$, for some $m \in \mathbb{Z}$. On the other hand, ℓ divides $\#E(\mathbb{F}_q)$, so $\ell \mid (q - 1)$, then $q = N(\pi) = a^2 + b^2 \equiv 1 \pmod{\ell}$. Consequently, $\ell \mid b$ and there exists an integer n such that $b = n\ell$. Hence, $q = (1 + m\ell)^2 + (n\ell)^2 = (m^2 + n^2)\ell^2 + 2m\ell + 1$. Taking into account that q is odd then m and n have the same parity. ■

Theorem 4.2 does not specify which of the four curves E_i has embedding degree 1, but from Lemma 2.2 we can give more information. If m is even, $t_i \equiv 2 \pmod 4$ and $i = 0$ or 2. Moreover, for ℓ an odd prime, we can distinguish between the curves: E_0 corresponds to $m \equiv 0 \pmod 4$ and E_2 to $m \equiv 2 \pmod 4$. So, we can establish a necessary and sufficient condition to ensure that the elliptic curve E_0 or E_2 has embedding degree 1 with respect to ℓ. On the other hand, if m is odd, the curve would be E_1 or E_3. These last curves can not be distinguished since the correct trace depends on the chosen generator of $\mathbb{F}_q^*$.

Koblitz and Menezes show in [14] that over any prime field $\mathbb{F}_p$, $p = 1 + b^2$, the curve $y^2 = x^3 - x$ has embedding degree 1 for any prime divisor of b if $4 \mid b$ and also the curve $y^2 = x^3 - 4x$ if $b \equiv 2 \pmod 4$. It is worth noticing that over $\mathbb{F}_p$ both curves are isomorphic to E_0 and they are precisely those obtained taking in Theorem 4.2 the values $m = 0$ and $b = n\ell$ (n even). A special case is also presented in [11].

In order to provide distortion maps for these curves, we must check that $E[\ell] \subseteq E(\mathbb{F}_q)$. Lenstra ([15]) describes how to compute the group structure of an elliptic curve via its endomorphism ring.

LEMMA 4.3 *The corresponding curve in Theorem 4.2 has group isomorphic to $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$, where $d_1 = \gcd(m, n)\ell$ and $d_2 = \frac{(m^2+n^2)\ell}{\gcd(m,n)}$.*

Proof. As $\mathbb{Z}[\sqrt{-1}]$-module, $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}[\sqrt{-1}]/(\pi - 1)\mathbb{Z}[\sqrt{-1}]$ (see [15]). Since $\mathbb{Z}[\sqrt{-1}]$ is a principal ideal domain, $E(\mathbb{F}_q)$ is a $\mathbb{Z}[\sqrt{-1}]$-module, then there exists a basis $\langle e_1, e_2\rangle$ of $\mathbb{Z}[\sqrt{-1}]$ and integers d_1, d_2 (invariant factors) with $d_1 \mid d_2$ such that $(\pi - 1)\mathbb{Z}[\sqrt{-1}] = \langle d_1 e_1, d_2 e_2\rangle$. Moreover, $E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$. These invariant factors can be computed using the Smith Normal Form of the matrix $\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}$ where $\langle a_1 +$

$a_2\sqrt{-1}, b_1 + b_2\sqrt{-1}\rangle$ is any basis of $(\pi - 1)\mathbb{Z}[\sqrt{-1}]$ ([20]).

Now, $(\pi - 1)\mathbb{Z}[\sqrt{-1}] = \langle \ell(m + n\sqrt{-1}), \ell(m\sqrt{-1} - n)\rangle$ and the result follows because the Smith Normal Form of $\begin{pmatrix} \ell m & \ell n \\ -\ell n & \ell m \end{pmatrix}$ is precisely $\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$. where $d_1 = gcd(m, n)\ell$ and $d_2 = \frac{(m^2+n^2)\ell}{\gcd(m,n)}$.

■

Thus, distortion maps can exist for a ℓ-torsion group, but it is also necessary to check the behaviour of ℓ in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$ as mentioned in [7].

COROLLARY 4.4 *If E_i is an elliptic curve with $j = 1728$ and embedding degree 1, the map $\sigma(x, y) = (-x, \sqrt{-1}y)$ will be a distortion map for any point P of prime order $\ell \neq 2$, except if $\ell \equiv 1 \pmod 4$ and P is eigenvector for σ (there are $2\ell - 2$ such points).*

Proof. Following [7], there are distortion maps for every subgroup (of order ℓ) of $E[\ell]$ if and only if ℓ is inert in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$, that is $\ell \equiv 3 \pmod 4$. For $\ell \equiv 1 \pmod 4$, ℓ splits and there exist distortion maps for all but two subgroups.

Let $\sigma(x, y) = (-x, \sqrt{-1}y)$, clearly σ is an endomorphism of E. Since the action of σ on $E[\ell]$ has characteristic polynomial $X^2 + 1$ it is clear that σ is a distorsion map for any point P such that is not a eigenvector for it, which only occurs if $\ell \equiv 1 \pmod 4$. ■

Now we consider the case $j = 0$. The endomorphism ring for an elliptic curve with $j = 0$ is the maximal order in $K = \mathbb{Q}(\sqrt{-3})$, that is $\mathcal{O}_K = \mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

THEOREM 4.5 *One of the six curves $E'_i : y^2 = x^3 + \omega^i$ has embedding degree 1 with respect to ℓ if and only if*

$$q = (m\ell + 2)^2 + 3(n\ell + 1)(\ell(n - m) - 1), \quad m, n \in \mathbb{Z}. \tag{10}$$

Such a curve has cardinality $(3n(n - m) + m^2)\ell^2$.

Proof. Let π be the Frobenius endomorphism of an elliptic curve with embedding degree 1 with respect to ℓ. We have now $\pi = a + b\frac{1+\sqrt{-3}}{2}$ for some integers a, b. So, from Lemma 4.1 there exists $m \in \mathbb{Z}$ such that $t = 2a + b = 2 + m\ell$. Since $q = N(\pi) = a^2 + b^2 + ab$, then $q = (m\ell + 2)^2 + 3a(a - m\ell - 2)$. On the other hand, ℓ divides $\#E(\mathbb{F}_q)$, hence $\ell \mid (q - 1)$. This is equivalent to $\ell \mid 3(a - 1)^2$ and, assuming $\ell > 3$, we can write $a = n\ell + 1$ for some $n \in \mathbb{Z}$. Replacing these values for a, b in the norm of π the result follows. ■

From Lemma 2.4 if m is even, the specific curve with embedding degree 1 is E'_0 or E'_3. Moreover, since $\ell > 3$, E'_0 corresponds to $m \equiv 0 \pmod 6$ and E'_3 corresponds to $m \equiv 2, 4 \pmod 6$. The curve E'_4 is a quadratic twist of E'_1 and E'_5 of E'_2. Hence $t'_1 \equiv t'_5 \pmod 6$ and $t'_2 \equiv t'_4 \pmod 6$. However, these curves cannot be distinguished since the trace depends on the generator ω.

Kirlar studies in [13] the curves $y^2 = x^3 - c$ over $\mathbb{F}_p$ and he shows that $y^2 = x^3 - 1$ has embedding degree $k = 1$ over $\mathbb{F}_p$, where $p = 1 + 27c^2$ for some natural c. Over $\mathbb{F}_p$, Kirlar's curve is exactly E'_0 and it corresponds to $m = 0$ and $c = n\ell$ in Theorem 4.5. A different case is also presented in [11], the curve $y^2 = x^3 + b$ over $\mathbb{F}_p$, $p = r^2 + r + 1$, $r \equiv 2 \pmod 3$ where b is neither a square nor a cube. This curve is isomorphic to E'_1 or E'_5 (it depends on ω) and it corresponds to the case $m = n = 1$.

As for the $j = 1728$ case, group structure of the elliptic curve can be computed.

LEMMA 4.6 *The corresponding curve in Theorem 4.5 has group isomorphic to* $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$, *where* $d_1 = \gcd(m,n)\ell$ *and* $d_2 = \frac{(3n(n-m)+m^2)\ell}{\gcd(m,n)}$.

Proof. This proof is similar to that of Lemma 4.3 taking into account that now the endomorphism ring is $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and $(\pi-1)\mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \langle n\ell + \ell(m-2n)\frac{1+\sqrt{-3}}{2}, (-m+2n)\ell + \ell(m-n)\frac{1+\sqrt{-3}}{2}\rangle$.

■

As before a distortion map can be given using the results of [7].

COROLLARY 4.7 *If* E_i' *is an elliptic curve with* $j=0$ *and embedding degree 1, the map* $\sigma(x,y) = (\zeta_3 x, y)$, *where* ζ_3 *is a cubic root of unity modulo* ℓ, *will be a distortion map for any point* P *of prime order* $\ell > 3$, *except if* $\ell \equiv 1 \pmod 3$ *and* P *is an eigenvector for* σ *(there are* $2\ell - 2$ *such points).*

4.2 *Embedding degree 2*

An elliptic curve with embedding degree $k=2$, with respect to an odd prime ℓ, must have trace $t \equiv 0 \pmod \ell$ (Lemma 4.1). Similarly, like the case $k=1$, we can obtain conditions to ensure that the curves E_i or E_i' have embedding degree $k=2$. Proofs for these results are similar to those of the results in Section 4.1 and we omit them for simplicity.

For $j = 1728$, we have:

THEOREM 4.8 *One of the four curves* $E_i : y^2 = x^3 + \omega^i x$ *has embedding degree 2 with respect to* ℓ *if and only if*

$$q = m^2\ell^2 + n\ell - 1,\ m \equiv n \pmod 2 \text{ and } n\ell - 1 \text{ is a square.} \tag{11}$$

The cardinality of the suitable curve is $(m^2\ell + n - 2m)\ell$.

For odd integers m, the obtained curve would be E_0 or E_2, and both cases can be distinguished according to the congruence of $t/2$ modulo 4. That is, for $m\ell \equiv 1 \pmod 4$ the curve is E_0, otherwise it is E_2. For even integers m the corresponding curve is E_1 or E_3 (depending on the generator ω). Since $k=2$ there are no distortion maps in this case. The group structure can be easily computed.

LEMMA 4.9 *The corresponding curve in Theorem 4.8 has group isomorphic to* $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ *where* $d_1 = \gcd(m\ell - 1, C)$ *with* $C^2 = n\ell - 1$ *and* $d_2 = \frac{(m^2\ell+n-2m)}{d_1}\ell$.

Now, for $j=0$, we have:

THEOREM 4.10 *One of the six curves* $E_i' : y^2 = x^3 + \omega^i$ *has embedding degree 2 with respect to* ℓ *if and only if*

$$q = (m\ell)^2 + 3C(C - n\ell),\ m \not\equiv 0 \pmod 3 \text{ and } 3C^2 = \ell n - 1. \tag{12}$$

The cardinality of the suitable curve is $q + 1 - m\ell$.

As the trace for these curves is $m\ell$, the involved curves are E_0' or E_3' if and only if m is even. Moreover, not all values of m, n are admissible, for example, if $n=1$ and m is

even then q is an even integer. Also, if $n = 2, 3, 6$ then ℓ is not a prime number (not even an integer).

LEMMA 4.11 *The corresponding curve in Theorem 4.10 has group isomorphic to* $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$, *where* $d_1 = \gcd(C-1, -m\ell + 2C)$ *and* $d_2 = \frac{(q+1-n\ell)}{d_1}$.

4.3 *Higher embedding degree*

Here, we will sketch the general method to find an elliptic curve E with embedding degree $k \geq 3$ for some ℓ and j-invariant 1728 or 0.

Now, in Lemma 4.1, the kth-root of the unity ζ_k depends on the value of ℓ. Assume we have fixed a particular value of ℓ and ζ_k. So, the trace of E can be written as $1+\zeta_k+m\ell$ for some integer m. If $j = 1728$, then it follows that $a = ((1+\zeta_k)/2 \pmod{\ell}) + m\ell$, and for $j = 0$, we have $b = (1 + \zeta_k - 2a \pmod{\ell}) + n\ell$ where a, b are the coefficients of the Frobenius endomorphism π. Since ℓ divides the cardinality of the curve it is easy to check that $q \equiv \zeta_k \pmod{\ell}$. Replacing the previous expressions in $q = N(\pi)$, when $j = 1728$ we have $b^2 = (-(1-\zeta_k)^2/4 \pmod{\ell}) + n\ell$ for some integer n. When $j = 0$, a must satisfy the equation $0 \equiv 3a(a - \zeta_k - 1) + \zeta_k^2 + \zeta_k + 1 \pmod{\ell}$. Finally, for the computed values of a and b, q must be expressed in a particular form (as in Theorems 4.2, 4.5, 4.8 and 4.10).

For instance, for $k = 3$, we have the following.

THEOREM 4.12 *Let* $\ell > 3$ *be an odd prime and* ζ_3 *a cubic root of the unity modulo* ℓ.

i) One of the four curves $E_i : y^2 = x^3 + \omega^i x$ *has embedding degree 3 with respect to* ℓ *if and only if*

$$q = \left(\frac{1+\zeta_3}{2} \pmod{\ell} + m\ell\right)^2 + \left(\frac{3\zeta_3}{4} \pmod{\ell}\right) + n\ell \tag{13}$$

and $(3\zeta_3/4 \pmod{\ell}) + n\ell$ *is a square in the integers.*

ii) One of the six curves $E_i' : y^2 = x^3 + \omega^i$ *has embedding degree 3 with respect to* ℓ *if and only if*

$$q = a^2 + ab + b^2, \quad a = m\ell, \quad b = 1 + \zeta_3 + \ell(n - 2m). \tag{14}$$

The group structure for the corresponding curves can also be computed for specific values ℓ, m, n and the correct ζ_3.

5. Numerical Examples

In this section we present examples of ordinary elliptic curves with low embedding degree (1, 2, 3 or higher) and j-invariant 0 or 1728. The construction of these curves is based on the above theorems. Tables 1 and 2 list some families of elliptic curves constructed following Theorems 4.2, 4.5, 4.8, 4.10, while Table 3 lists elliptic curves with embedding degree 3 following Theorem 4.12. In Table 4 we present some examples of elliptic curves with embedding degree k, $4 \leq k \leq 10$, and $k = 12, 16, 24$ following the general method (see Section 4.3).

These tables are divided into two blocks. In the first block elliptic curves with j-invariant 1728 are presented, while the second one corresponds to curves with j-invariant

Table 1. Ordinary elliptic curves over $\mathbb{F}_q$ with embedding degree 1 with respect to ℓ

ℓ	m,n	q	Curve	Group Structure
ℓ	0,2	$4\ell^2+1$	E_0	$\mathbb{Z}/2\ell\mathbb{Z}\times\mathbb{Z}/2\ell\mathbb{Z}$
73	0,2	21317	E_0	$\mathbb{Z}/146\mathbb{Z}\times\mathbb{Z}/146\mathbb{Z}$
ℓ	2,2	$(2\ell+1)^2+4\ell^2$	E_2	$\mathbb{Z}/2\ell\mathbb{Z}\times\mathbb{Z}/4\ell\mathbb{Z}$
41	2,2	13613	E_2	$\mathbb{Z}/82\mathbb{Z}\times\mathbb{Z}/164\mathbb{Z}$
ℓ	1,1	$(\ell+1)^2+\ell^2$	$E_1\,(E_3)$	$\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/2\ell\mathbb{Z}$
79	1,1	12641	$E_1\,(E_3)$	$\mathbb{Z}/79\mathbb{Z}\times\mathbb{Z}/158\mathbb{Z}$
ℓ	2,0	$4\ell^2+2\ell+1$	E_3'	$\mathbb{Z}/2\ell\mathbb{Z}\times\mathbb{Z}/2\ell\mathbb{Z}$
31	2,0	3907	E_3'	$\mathbb{Z}/62\mathbb{Z}\times\mathbb{Z}/62\mathbb{Z}$
ℓ	1,0	$\ell^2+\ell+1$	$--$	$\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$
59	1,0	3541	$E_1'\,(E_5')$	$\mathbb{Z}/59\mathbb{Z}\times\mathbb{Z}/59\mathbb{Z}$
ℓ	-3,1	$21\ell^2-3\ell+1$	$--$	$\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/21\ell\mathbb{Z}$
53	-3,1	58831	$E_2'\,(E_4')$	$\mathbb{Z}/13\mathbb{Z}\times\mathbb{Z}/273\mathbb{Z}$

Table 2. Ordinary elliptic curves over $\mathbb{F}_q$ with embedding degree 2 with respect to ℓ

C	ℓ	m,n	q	Curve	Group Structure
C	C^2+1	1,1	$\ell^2+\ell+1$	E_0	$\mathbb{Z}/C\mathbb{Z}\times\mathbb{Z}/C\ell\mathbb{Z}$
10	101	1,1	10301	E_0	$\mathbb{Z}/10\mathbb{Z}\times\mathbb{Z}/1010\mathbb{Z}$
C	C^2+1	3,1	$9\ell^2+\ell-1$	E_2	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/\ell(9\ell^2-5)/2\mathbb{Z}$
10	101	3,1	91909	E_2	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/45652\mathbb{Z}$
C	$(C^2+1)/2$	2,2	$4\ell^2+2\ell-1$	$E_1\,(E_3)$	$\mathbb{Z}/C\mathbb{Z}\times\mathbb{Z}/2\ell C\mathbb{Z}$
45	1013	2,2	4106701	$E_1\,(E_3)$	$\mathbb{Z}/45\mathbb{Z}\times\mathbb{Z}/91170\mathbb{Z}$
C	$3C^2+1$	1,1	$\ell^2+3C^2-3C\ell$	$--$	$\mathbb{Z}/\ell(\ell-3C)\mathbb{Z}$
20	1201	1,1	1371541	$E_1'(E_5')$	$\mathbb{Z}/1370341\mathbb{Z}$
C	$3C^2+1$	-1,1	$\ell^2+3C^2+3C\ell$	$--$	$\mathbb{Z}/\gcd(C-1,6)\mathbb{Z}\times\mathbb{Z}/\frac{3\ell(C^2+C+1)}{\gcd(C-1,6)}\mathbb{Z}$
8	193	-1,1	42073	$E_2'(E_4')$	$\mathbb{Z}/42267\mathbb{Z}$
C	$(3C^2+1)/4$	4,4	$16\ell^2+3C^2-12C\ell$	E_3'	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\ell(4\ell-3C)\mathbb{Z}$
13	127	4,4	238759	E_3'	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/119126\mathbb{Z}$

0. For embedding degree 1 or 2 we show three different families of elliptic curves. For each family we present the general form (for some values of m,n) (on odd numbered lines) as well as a toy example for a particular prime ℓ (on even lines) with the same parameters for m,n and the same curve as the previous line.

For these families of elliptic curves with embedding degree 1, we always take ℓ to be an odd prime number, but we could also give elliptic curves for ℓ any natural number in the above constructions. In these cases, the embedding degree is taken over an odd prime divisor of ℓ. For example, if we take $m=-1$, $n=1$ in Theorem 4.2, we obtain for $\ell=4060$ that the elliptic curve E_0 over $\mathbb{F}_q$, $q=p^2$ where $p=5741$ has embedding degree 1 for the primes 5, 7 and 29. In this way, different values for m,n,ℓ can produce the same curve. For example, taking $m=-20$, $n=20$, the same curve arises for $\ell=203$ and Theorem 4.2 asserts that E_0 has embedding degree 1 with respect to 7 or 29.

The following two examples for embedding degree $k=1$, are taken from the families of Table 1, searching for ℓ which is a Solinas prime (i.e. sum or difference of a small number of powers of 2).

- For $\ell=2^{169}+2^{90}+1$ or $\ell=2^{258}+2^{242}-1$ and $p=4\ell^2+1$, E_0 has embedding degree 1 with respect to ℓ.
- For $\ell=2^{170}-2^{154}-1$ or $\ell=2^{257}-2^{185}-1$ and $p=\ell^2+\ell+1$, E_3' has embedding degree 1 with respect to ℓ.

Note that the group structure for elliptic curves in the families in Table 2 with $j=1728$ is never cyclic. However, there are other examples where it is cyclic. If we take $m=4$ and $n=2$ in Theorem 4.8 and $\ell=(C^2+1)/2$ a prime, the corresponding curve has

Table 3. Ordinary elliptic curves over $\mathbb{F}_q$ with embedding degree 3 with respect to ℓ

ℓ	ζ_3	m,n	q	Curve	ℓ	ζ_3	m,n	q	Curve
73	64	-1,1	137	$E_1\,(E_3)$	103	56	-2,-2	57427	$E_1'(E_5')$
73	8	-1,3	1249	$E_1\,(E_3)$	109	63	1,1	9001	$E_2'(E_4')$
97	35	1,2	13421	E_2	73	8	2,1	6067	$E_2'(E_4')$
193	84	2,1	275881	E_0	163	104	2,2	83071	$E_2'(E_4')$

Table 4. Ordinary elliptic curves over $\mathbb{F}_q$ with embedding degree greater than 3 with respect to ℓ

k	ℓ	ζ_k	q	Curve	ℓ	ζ_k	q	Curve
4	73	46	3769	$E_1\,(E_3)$	433	179	16633	$E_2'(E_4')$
5	61	20	569	$E_1\,(E_3)$	271	10	21961	$E_2'(E_4')$
6	313	99	3229	$E_1\,(E_3)$	43	7	523	E_0'
7	757	453	51929	E_2	421	33	11821	E_3'
8	1697	1296	43721	$E_1\,(E_3)$	457	170	21649	E_0'
9	181	39	401	$E_1\,(E_3)$	883	641	18301	$E_2'(E_4')$
10	3541	1381	482957	E_2	271	171	7759	E_3'
12	157	22	4889	E_0	337	265	2287	$E_1'(E_5')$
16	673	512	6569	$E_1\,(E_3)$	433	168	140893	$E_2'(E_4')$
24	937	163	9533	$E_1\,(E_3)$	313	168	13627	$E_1'(E_5')$

cyclic structure. This is never possible for embedding degree 1, as is shown in Lemma 4.3.

For higher embedding degrees, as the finite field depends on the k-root of the unity modulo ℓ, in Tables 3 and 4 we present some particular examples (not a general family).

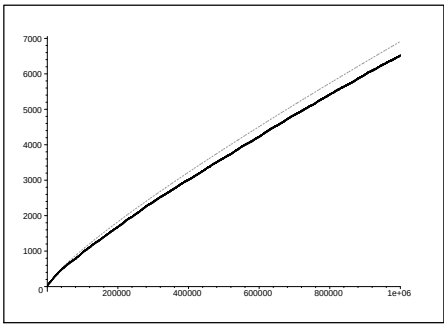
It is known that pairing-friendly elliptic curves are sparse (see [1, 10, 12]). Moreover, since elliptic curves with j-invariant 1728 or 0 are exactly those whose endomorphism ring is $\mathbb{Z}[\sqrt{-1}]$ or $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, then their presence is quite rare. Bateman-Horn's conjecture [3] allows us to suggest that there exist elliptic curves in the families presented in Tables 1 and 2 for any bit length size of the prime ℓ (and so for q). Indeed, the Bateman-Horn's conjecture provides a conjectured density for the positive integers at which a given system of polynomials all have prime values. Figure 1 shows, for each N up to 10^6, the number of values $\ell \leq N$ (and so the number of elliptic curves in the corresponding family) such that the involved polynomials (in two of our families) simultaneously take prime values (continous line). Moreover, we show the corresponding value given by the Bateman-Horn's conjecture (dashed line). More precisely, Figure 1.a) shows the case ℓ and $q = 4\ell^2 + 1$ are prime numbers (first family in Table 1) and Figure 1.b) shows the case $\ell = 3C^2 + 1$, $q = \ell^2 + 3C^2 - 3C\ell$ are primes (fourth family in Table 2). Hence, we can conclude, for its concordance with the Bateman-Horn's conjecture, that there are infinitely many elliptic curves in our families.

A challenging open question is to prove directly the existence of infinitely many curves in some of our families (disregarding the Bateman-Horn's conjecture). For instance, in Table 2 we can find quadratic binary forms $a\ell^2 + bC\ell + cC^2$ for expressing q. Relaxing the condition ℓ prime, we could apply well-known results over the theory of primes represented by binary quadratic forms (see for example [8]). However, since C and ℓ are not independent, it is not so simple to prove it (see Theorem 4.10).

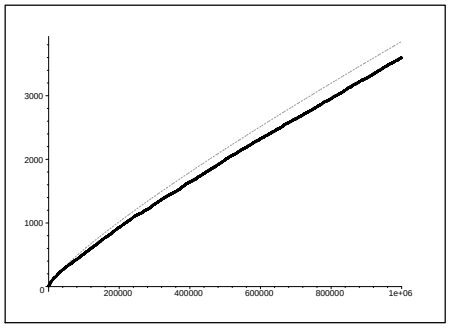
Acknowledgements

We thank the anonymous referee for the helpful comments and suggestions.

An extended abstract including some results of this manuscript (only for elliptic curves with j-invariant 1728) was previously presented at the conference Recsi 2014, [18].



a) ℓ, $q = 4\ell^2 + 1$ primes



b) $\ell = 3C^2 + 1$, $q = \ell^2 + 3C^2 - 3C\ell$ primes

Figure 1. Number of pairs (ℓ, q), $\ell \leq N$, which are primes

References

[1] R. Balasubramanian and N. Koblitz *The improbability that an elliptic curve has subexponential log problem under the Menezes-Okamoto-Vanstone algorithm*, Journal of Cryptology 11, no 2, 141-145, 1998.

[2] P. Barreto, B. Lynn and M. Scott, *Efficient implementation of pairing-based cryptosystems*, Journal of Cryptology 17, 321-334, 2004.

[3] P.T. Bateman and R.A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Mathematics of Computation 16, 363–367, 1962.

[4] I. Blake, G. Seroussi and N. Smart, *Elliptic Curves in Cryptography*. London Mathematical Society, LNS 265. University Press, 1999.

[5] I. Blake, G. Seroussi and N. Smart, *Advances in Elliptic curve Cryptography*. London Mathematical Society, LNS 371. University Press, 2005.

[6] F. Brezing and A. Weng, *Elliptic curves suitable for pairings based cryptography*, Designs, Codes and Cryptography 37, 133–141, 2005.

[7] D. Charles, *On the existence of distortion maps on ordinary elliptic curves*, IACR Cryptology ePrint Archive 2006: 128, 2006.

[8] D.A. Cox, *Primes of the form $x^2 + ny^2$, Fermat, Class Field Theory, and Complex Multiplication.* Wiley-Interscience, 1989.

[9] D. Freeman, M. Scott and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, Journal of Cryptology 23, no. 2, 224–280, 2010.

[10] S.D. Galbraith, J.F. McKee and P.C. Valença, *Ordinary abelian varieties having small embedding degree*, Finite Fields Appl. 13, 800–814, 2007.

[11] Z. Hu, M. Xu and Z. Zhou, *A generalization of Verheul's theorem for some ordinary curves*, LNCS 6584, 105–114, Springer, 2011.

[12] J. Jiménez Urroz, F. Luca and I. Shparlinski, *On the number of isogeny classes and pairing friendly elliptic curves and statistics for MNT curves*, Mathematics of Computation 81, 1093–1110, 2012.

[13] B.B. Kirlar, *On the elliptic curves $y^2 = x^3 - c$ with embedding degree 1*, Journal of Computational and Applied Mathematics 235, 4724–4728, 2011.

[14] N. Koblitz, A. Menezes, *Pairing-based Cryptography at high security level*, Cryptography and Coding, LNCS 3796, 13–36, Springer, 2005.

[15] H.W. Lenstra, *Complex multiplication structure of elliptic curves*, Journal of Number Theory, 56 (2), 227–241, 1995.

[16] A. Menezes, *Elliptic Curves Public Key Cryptography*, Kluwer, 1993.

[17] A. Miyaji, M. Nakabayashi and S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Trans. Fundamentals, E84-A (5), 2001.

[18] J.M. Miret, D. Sadornil and J. Tena, *Familias de curvas elípticas adecuadas para Criptografía Basada en la Identidad* In Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información RECSI XIII, Ed. R. Alvarez et al. Alicante, Spain 2-5 September 2014, Pub. Universidad de Alicante, ISBN: 978-84-9717-323-0, 35–38, 2014.

[19] C. Munuera and J. Tena, *An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite field*, Rendiconti del Circolo Matematico di Palermo, Serie 2, tomo XLII, 106-116, 1993.
[20] C. Norman, *Finitely Generated Abelian Groups and Similarity of Matrices over a Field*, Springer Undergraduate Mathematics Series, 2012.
[21] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, GTM 106, 1986.
[22] E.R. Verheul, *Evidence that XTR is more secure than supersingular elliptic curves cryptosystems*, Journal of Cryptology 17, no. 4, 277–296, 2004.