On Various Families of Twisted Jacobi Quartics*

Jérôme Plût

Université de Versailles–Saint-Quentin-en-Yvelines; Versailles, France
jerome.plut@prism.uvsq.fr

Abstract. We provide several results on some families of twisted Jacobi quartics. We give new addition formulæ for two models of twisted Jacobi quartic elliptic curves, which represent respectively 1/6 and 2/3 of all elliptic curves, with respective costs $7\mathbf{M} + 3\mathbf{S} + \mathbf{D}_a$ and $8\mathbf{M} + 3\mathbf{S} + \mathbf{D}_a$. These formulæ allow addition and doubling of points, except for points differing by a point of order two.

Furthermore, we give an intrinsic characterization of elliptic curves represented by the classical Jacobi quartic, by the action of the Frobenius endomorphism on the 4-torsion subgroup. This allows us to compute the exact proportion of elliptic curves representable by various models (the three families of Jacobi quartics, plus Edwards and Huff curves) from statistics on this Frobenius action.

1 Introduction

The interest for elliptic curves in cryptography arises from the fact that, given suitable parameter choices, they provide an efficient representation of the "generic group" model. However, the need for separate formulæ for point addition and doubling in Weierstraß coordinates critically exposes elliptic curve arithmetic to side-channel analysis.

One family of countermeasures protecting against these attacks is the use of a coordinate system that allows point additions and doublings to be performed with the same formulæ. Namely, addition formulæ are said to be *unified* if they also allow doubling of non-zero points, and *complete* if the allow addition of any pair of points, identical or not, zero or not.

Some curve models with such properties, over a field of odd characteristic, are:

- twisted Edwards curves [Edw07, BL07, BBJ+08, HWCD08], with equation $ax^2 + y^2 = 1 + dx^2y^2$, have a unified addition formula, that is complete in some cases, costing $9\mathbf{M} + \mathbf{D}_a + \mathbf{D}_d$ [HWCD08];
- Jacobi quartics, with equation $y^2 = x^4 + 2a\,x^2 + 1$, are unified [BJ03], and have an addition formula costing $7\mathbf{M} + 3\mathbf{S} + \mathbf{D}_a$ [HWCD09];
- Huff cubics [JTV10], with equation $ax(y^2 - 1) = by(x^2 - 1)$, have a unified addition formula costing $11\mathbf{M}$.

* This work was supported by the French *Agence Nationale de la Recherche* through the ECLIPSES project under Contract ANR-09-VERS-018.

A. Miri and S. Vaudenay (Eds.): SAC 2011, LNCS 7118, pp. 373–383, 2012.

Not all elliptic curves transform to the Edwards or Jacobi quartic forms: only the curves with a rational point of order four transform to Edwards curves [BBJ+08, Theorem 3.3][Mor09], whereas the condition for Jacobi quartics is examined in more detail in section 2.2 of this document. Since it is preferred that elliptic curves used in cryptography have a group of prime order (as is the case, for example, of NIST-recommended curves [Nat00]), they are not actually amenable to Edwards or Jacobi quartic form.

Recent research activity has focused on counting elliptic curves in various families using explicit computation of the j-invariant, for example in the families of Doche-Icart-Kohel [DIK06] and Edwards [RFS10], Legendre [FW10], and complete Edwards curves [AG11].

We count the Jacobi quartics using a direct method, relying on the action of the Frobenius on the 4-torsion points of elliptic curves. Throughout this document, k is a finite field of odd characteristic. Let E be an elliptic curve defined over k. The 4-torsion subgroup $E[4]$ of E has coordinates in the algebraic closure of k, and is thus equipped with an action of the Frobenius endomorphism φ of k. Since k has odd characteristic, by [Sil86, 6.4(b)], the group $E[4]$ is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$, and the action $\varphi_E \pmod 4$ of φ is given by a matrix in $GL_2(\mathbb{Z}/4\mathbb{Z})$. Finally, a change of basis of $E[4]$ conjugates the matrix of $\varphi_E \pmod 4$. Therefore, to the curve E, one may canonically attach the conjugacy class of $\varphi_E \pmod 4$ in $GL_2(\mathbb{Z}/4\mathbb{Z})$.

This work gives an intrinsic characterization of representability of elliptic curves by the Jacobi quartic model (Theorem 5); this is given by a list of allowed conjugacy classes for $\varphi_E \pmod 4$. In particular, this does not depend on the representation chosen for the curve. Thus, it allows us to give an asymptotic count of the elliptic curves that can be represented as Jacobi quartics. This method generalizes to other quadrics intersection models such as Edwards, Jacobi, and Huff (Theorem 11).

Billet and Joye [BJ03, §3] also define a twist of the Jacobi model that represents all curves with at least one rational point of order two, and give unified addition formulæ for these curves with a cost of $10\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$. We give here improved addition formulæ for the two following variants of the twisted Jacobi model:

- A $7\mathbf{M}+3\mathbf{S}+\mathbf{D}_a$ multiplication for the *(2,2)-Jacobi quartic*, which represents all curves whose point group has $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ as a subgroup (1/6 of all elliptic curves);
- A $8\mathbf{M} + 3\mathbf{S} + \mathbf{D}_a$ multiplication for the *(2)-Jacobi quartic*, which represents all curves whose point group has $(\mathbb{Z}/2\mathbb{Z})$ as a subgroup (2/3 of all elliptic curves).

These formulæ, as well as the Jacobi quartic formula from [HWCD09], are not unified. They are, however, "complete except at 2": any points P, Q such that the formulæ don't allow the computation of $P + Q$ differ by a point of order two (Propositions 6 and 8). Thus, these formulæ are usable for all computations in

the subgroup of $E(k)$ of points of order coprime to 2, and in particular in the largest subgroup of $E(k)$ of prime order, which the subgroup of cryptographic significance.

2 Jacobi Quartics

2.1 Curve Equation

A *Jacobi quartic* is a projective curve with the quartic equation

$$y^2 = x^4 + 2ax^2 + 1, \tag{1}$$

where $a \in k$ is a parameter. The discriminant of the right-hand side polynomial is $2^8(a^2-1)^2$; therefore, if $a \notin \{-1, 1\}$, then the curve has the tacnode at the point at infinity $(0:1:0)$ as its only singular point. Resolution of this singularity yields the intersection of two quadrics

$$JQ_a: \quad y^2 = z^2 + 2ax^2 + t^2, \quad x^2 = z \cdot t, \tag{2}$$

where the tacnode $(0:1:0)$ has the two antecedents $(0:1:\pm 1:0)$.

The curve JQ_a contains the four points with coordinates $(x:y:z:t)$ equal to $(0:1:0:\pm 1)$ and $(0:1:\pm 1:0)$. We fix $\varepsilon = (0:1:0:1)$ as the neutral point; the three others are then the three points of order two.

As JQ_a is a smooth intersection of two quadrics in the projective space of dimension three, it is an elliptic curve, and the group law is defined by coplanarity [Ono94, LS01]. Namely, let ε be the neutral point; then any three points P_1, P_2, P_3 have zero sum if the four points $(\varepsilon, P_1, P_2, P_3)$ are coplanar. Of course, when two of the points, say P_1 and P_2, are identical, we replace P_2 by the direction of the tangent line at P_1 to JQ_a.

We may then check that the addition formulæ for $P_3 = P_1 + P_2$, where $P_i = (x_i : y_i : z_i : t_i)$, are

$$\begin{aligned} x_3 &= (x_1y_2 + y_1x_2) \cdot (t_1t_2 - z_1z_2); \\ y_3 &= (y_1y_2 + 2ax_1x_2)(z_1z_2 + t_1t_2) + 2x_1x_2(z_1t_2 + t_1z_2); \\ z_3 &= (x_1y_2 + y_1x_2)^2; \\ t_3 &= (t_1t_2 - z_1z_2)^2. \end{aligned} \tag{3}$$

The negative of the point $(x:y:z:t)$ is $(-x:y:z:t)$.

A speed-up of one multiplication is achieved [HWCD09] by observing that

$$z_3 = (z_1z_2 + t_1t_2)(z_1t_2 + t_1z_2) + 2x_1x_2(2ax_1x_2 + y_1y_2), \tag{4}$$

so that $y_3 + z_3$ factorizes as

$$y_3 + z_3 = (z_1z_2 + 2x_1x_2 + t_1t_2)(y_1y_2 + 2ax_1x_2 + z_1t_2 + t_1z_2). \tag{5}$$

The cost of a point addition using (5) is $7\mathbf{M} + 3\mathbf{S} + \mathbf{D}_a$.

Remark 1. The formulæ (3) are not unified. One checks that these formulæ yield

$$(x:y:z:t) + (-x:y:t:z) = (0:0:0:0). \tag{6}$$

This situation is examined in more detail in the proposition 6 below.

2.2 Representability

Proposition 2. *Let E be an elliptic curve over the field k of characteristic $\neq 2$. Then E is isomorphic to a Jacobi quartic if, and only if, it has an equation of the form*

$$\eta^2 = (\xi - r_1)(\xi - r_2)(\xi - r_3)$$

such that r_1, r_2 and $r_3 \in k$ and at least one of the $r_i - r_j$ for $i, j \in \{1, 2, 3\}$, $i \neq j$, is a square.

Proof. Let E be such an elliptic curve and assume for example that $r_2 - r_3$ is a square in k. We may then define parameters $a, c, d \in k$ by

$$a = \frac{r_2 + r_3 - 2r_1}{r_2 - r_3}, \quad c = \frac{r_2 - r_3}{2}, \quad 4d^2 = r_2 - r_3. \tag{7}$$

The equation of E may then be simplified to

$$2\left(\frac{\eta}{d}\right)^2 = \left(\frac{\xi - r_1}{c}\right)\left(\frac{\xi - r_1}{c} - a - 1\right)\left(\frac{\xi - r_1}{c} - a + 1\right). \tag{8}$$

We define coordinates (x, y, z, t) by the matrix relation

$$\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 - a^2 \\ -2a & 0 & 1 & a^2 - 1 \\ 2 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{\xi - r_1}{c} \\ \frac{\eta}{d} \\ \left(\frac{\xi - r_1}{c}\right)^2 \\ 1 \end{pmatrix}. \tag{9}$$

Then (x, y, z, t) satisfy the Jacobi quartic equations for JQ_a.

Conversely, the above computation shows that JQ_a is birationally equivalent to the elliptic curve with equation $2\eta^2 = \xi(\xi - a + 1)(\xi - a + 1)$, which amounts to the Weierstraß equation in $(\frac{\xi}{2}, \frac{\eta}{2})$:

$$\left(\frac{\eta}{2}\right)^2 = \frac{\xi}{2}\left(\frac{\xi}{2} - \frac{a-1}{2}\right)\left(\frac{\xi}{2} - \frac{a+1}{2}\right). \tag{10}$$

The right-hand side has the roots $\frac{a+1}{2}$ and $\frac{a-1}{2}$, the difference of which is 1, which is a square in k. □

Remark 3. If -1 is not a square in k, then exactly one of $r_1 - r_2$ and $r_2 - r_1$ is a square. Over such a field, an elliptic curve can be represented by a Jacobi quartic if, and only if, it has a rational 2-torsion subgroup.

Remark 4. If E has full rational 2-torsion subgroup, then so does its quadratic twist $\widetilde{E}$, and at least one of E or $\widetilde{E}$ can be represented by a Jacobi quartic.

Theorem 5. *Let k be a finite field of characteristic $\neq 2$, E be an elliptic curve over k. Let φ_E be the representation of the Frobenius automorphism of k on $E(\overline{k})$ and $\varphi_E \pmod 4$ be the action of φ_E on the 4-torsion group $E[4]$.*

Then E can be represented by a Jacobi quartic if, and only if, $\varphi_E \pmod 4$ belongs to one of the following conjugacy classes in $GL_2(\mathbb{Z}/4\mathbb{Z})$:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix} = \mathrm{id}, \begin{pmatrix}1&2\\0&1\end{pmatrix}, \begin{pmatrix}-1&2\\0&-1\end{pmatrix}, \begin{pmatrix}1&0\\0&-1\end{pmatrix}, \begin{pmatrix}1&2\\2&-1\end{pmatrix}. \tag{11}$$

Proof. The condition that E has a rational 2-torsion subgroup is equivalent to $\varphi_E \equiv \mathrm{id} \pmod 2$. It may be checked, for example by enumeration, that there are exactly six such conjugacy classes of matrices in $GL_2(\mathbb{Z}/4\mathbb{Z})$: namely, the five classes of (11) and the class of $-\mathrm{id}$.

Let q be the cardinality of k. Then, by the Hasse-Weil theorem [Sil86, Theorem 2.4], we have $\det(\varphi_E) = q$. Therefore, if $q \equiv -1 \pmod 4$, then $\det \varphi_E \equiv -1 \pmod 4$ and thus $\varphi_E \pmod 4$ is conjugate to one of the latter two matrices of (11). In this case, Remark 3 shows that E is representable by a Jacobi quartic.

It remains to prove the case when $q \equiv +1 \pmod 4$. In this case, there exists $i \in k$ such that $i^2 = -1$. Let $(r_n, 0)$, for $n = 1, 2, 3$, be the (rational) points of order two of E and (ξ_n, η_n) be (not necessarily rational) points of order four such that $2(\xi_n, \eta_n) = (r_n, 0)$. The condition on (ξ_1, η_1) is equivalent to

$$(\xi_1 - r_1)^2 = (r_1 - r_2)(r_1 - r_3), \qquad \eta_1^2 = (r_1 - r_2)(r_1 - r_3)(2\xi_1 - r_2 - r_3). \tag{12}$$

Define $d_1 = r_2 - r_3$, $d_2 = r_3 - r_1$, and $d_3 = r_1 - r_2$; by Proposition 2, representability by a Jacobi quartic is equivalent to at least one of the d_n being a square in k. Two cases may occur:

(i) all d_n reduce to the same class modulo squares in $k^\times$: then there exist $c_n \in k$ and $d \in k$ such that $d_n = c_n^2 d$. The equations (12) may be rewritten as:

$$(\xi_1 - r_1)^2 = -(c_2 c_3 d)^2, \qquad \eta_1^2 = -(c_2 c_3 d)^2 (c_3 \pm i c_2)^2 d. \tag{13}$$

We see that all ξ_n are rational, and therefore $\varphi_E(\xi_n, \eta_n) = (\xi_n, \pm\eta_n)$. Thus, $\varphi_E \pmod 4$ is diagonalizable, and thus belongs to $\{\mathrm{id}, -\mathrm{id}\}$. The case $\varphi_E \equiv +\mathrm{id} \pmod 4$ is equivalent to $\eta_1 \in k$ and thus to d being a square. Therefore, in the case (i), E is representable by a Jacobi quartic if, and only if, $\varphi_E \equiv \mathrm{id} \pmod 4$.

(ii) not all the d_n reduce to the same class modulo squares: then E can be represented by a Jacobi quartic. Moreover, if for example d_1 is a square and d_2 is not, then $(\xi_3 - r_3)^2 = -d_1 d_2$ is not a square, and therefore $\xi_3 \notin k$. Thus, $\varphi_E \pmod 4$ is not diagonalizable and belongs to one of the conjugacy classes $\begin{pmatrix}1&2\\0&1\end{pmatrix}, \begin{pmatrix}-1&2\\0&-1\end{pmatrix}$.

This shows that the cases where E transforms to a Jacobi quartic are exactly the cases where $\varphi_E \pmod 4$ is one of the five matrices listed above. □

3 (2, 2) Jacobi Quartics

3.1 Curve Equation

We expand the definition of the Jacobi quartics to allow representability of all curves with rational 2-torsion subgroup. To do this, we relax the condition that d, as defined in equation (7), belong to k. We then obtain the quadric intersection

$$JQ^{(2,2)}_{a,b}: \qquad b\,x^2 = zt, \qquad y^2 = z^2 + 2a\,x^2 + t^2. \tag{14}$$

It is smooth when $(a^2-1)b \neq 0$. We note that for all $\lambda \in k^\times$, the curve $JQ^{(2,2)}_{\lambda^2 a, \lambda^2 b}$ is isomorphic to $JQ^{(2,2)}_{a,b}$ by the coordinate change $(\lambda x : y : z : t)$. Therefore, we may choose b to be either one or a (small) preset quadratic non-residue in k.

This curve has the rational points of order two

$$\omega_1 = (0:1:0:-1), \quad \omega_2 = (0:1:1:0), \quad \omega_2' = \omega_2 + \omega_1 = (0:1:-1:0). \tag{15}$$

The point addition formulæ are deduced from (3):

$$\begin{aligned} x_3 &= (x_1y_2 + y_1x_2)\,(z_1z_2 - t_1t_2) \\ y_3 &= (y_1y_2 + 2a\,x_1x_2)\,(z_1z_2 + t_1t_2) + 2b\,x_1x_2\,(z_1t_2 + t_1z_2) \\ z_3 &= (z_1z_2 - t_1t_2)^2 \quad\; = (z_1z_2 + t_1t_2)^2 - (2b\,x_1x_2)^2 \\ t_3 &= b\,(x_1y_2 + y_1x_2)^2 \end{aligned} \tag{16}$$

$$y_3 + t_3 = (z_1z_2 + 2b\,x_1x_2 + t_1t_2)\,(y_1y_2 + 2a\,x_1x_2 + z_1t_2 + t_1z_2)$$

The full cost for a point addition is seen to be $7\mathbf{M}+3\mathbf{S}+\mathbf{D}_a+2\mathbf{D}_b$. The advantage of choosing a parameter b such that multiplication by b is fast is apparent. The probability that all $b < N$ are squares modulo p is asymptotically equivalent to e^{-N}, so that in practice we shall almost always be able to find such a b; moreover, whether this is the case is easy to check by quadratic reciprocity.

Proposition 6. *Let P_1, P_2 be two points of $JQ^{(2,2)}_{a,b}$ such that the addition formulæ (16) yield $P_3 = P_1 + P_2 = (0:0:0:0)$. Then we either have $P_2 = P_1 + \omega_2$ or $P_2 = P_1 + \omega_2'$, where ω_i are the points of order two defined in (15).*

Proof. Let $(x_i : y_i : z_i : t_i)$ be the coordinates of P_i. If $x_1 = x_2 = 0$, then both points belong to the 2-torsion group and the result follows by enumeration, so we may assume for example $x_1 \neq 0$. Since $bx_1^2 = z_1t_1$, this implies $z_1 \neq 0$ and $t_1 \neq 0$.

The relations $t_3 = 0$ and $z_3 = 0$ then imply that there exist $\alpha, \beta \in k$ such that $P_1 = (x_1 : \alpha x_1 : \beta t_1 : t_1)$ and $P_2 = (x_2 : -\alpha x_2 : z_2 : \beta z_2)$. Since $bx_1^2 = \beta t_1^2$, there exists $\xi \in k$ such that $\beta = b\xi^2$ and $x_1 = \xi t_1$. Let $\eta = \xi\alpha$; then

$$P_1 = (\xi : \eta : b\xi^2 : 1), \qquad P_2 = (\sigma\xi : -\sigma\eta : 1 : b\xi^2) \qquad \text{for } \sigma = \pm 1.$$

We then see that $\sigma = 1$ implies $P_2 = P_1 + \omega_2$ whereas $\sigma = -1$ implies $P_2 = P_1 + \omega_2'$. □

3.2 Representability

Proposition 7. *The $(2,2)$-Jacobi quartics represent exactly all elliptic curves E with rational 2-torsion subgroup.*

Proof. Let E be a curve with three rational points of order two and the equation $\eta^2 = (\xi - r_1)(\xi - r_2)(\xi - r_3)$ and define, for any $c \in k$,

$$a = c^{-2}(r_2 + r_3 - 2r_1), \quad b = c^{-2}(r_2 - r_3), \tag{17}$$

and coordinates $(x : y : z : t)$ by

$$\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 & c & 0 & 0 \\ -2r_1 & 0 & 1 & r_1(r_2 + r_3) - r_2 r_3 \\ -r_2 - r_3 & 0 & 1 & r_2 r_3 \\ r_2 - r_3 & 0 & 0 & -r_1(r_2 - r_3) \end{pmatrix} \begin{pmatrix} \xi \\ \eta \\ \xi^2 \\ 1 \end{pmatrix}. \tag{18}$$

Then we see that $(x : y : z : t)$ satisfy the quadric equations (14). □

4 (2)-Jacobi Quartics

4.1 Curve Equation

The (2)-*Jacobi quartic* is the intersection of the two quadrics

$$JQ^{(2)}_{a,b} : \qquad x^2 = zt, \qquad y^2 = z^2 + 2a\,x^2 + b\,t^2. \tag{19}$$

It is smooth (and thus an elliptic curve) whenever $(a^2 - 1)b \neq 0$. For all $\lambda \in k^\times$, $JQ^{(2)}_{\lambda^2 a, \lambda^4 b}$ is isomorphic to $JQ^{(2)}_{a,b}$ by the coordinate change $(\lambda x : y : z : \lambda^2 t)$.

The addition formulæ are given by

$$\begin{aligned} x_3 &= (x_1 y_2 + y_1 x_2)\,(z_1 z_2 - b t_1 t_2) \\ y_3 &= (y_1 y_2 + 2a x_1 x_2)\,(z_1 z_2 + b t_1 t_2) + 2b x_1 x_2\,(z_1 t_2 + t_1 z_2) \\ z_3 &= (z_1 z_2 - b t_1 t_2)^2 \\ t_3 &= (x_1 y_2 + y_1 x_2)^2 \end{aligned} \tag{20}$$

The factorisation trick from [HWCD09] does not apply here, thus the total point addition cost is $8\mathbf{M} + 3\mathbf{S} + \mathbf{D}_a + 2\mathbf{D}_b$.

The point $\omega_1 = (0 : 1 : 0 : -1)$ is of order two.

Proposition 8. *Let P_1, P_2 be two points of $JQ^{(2)}_{a,b}$ such that the addition formulæ (20) yield $P_3 = (0 : 0 : 0 : 0)$. Then $P_1 - P_2$ is a point of order two, distinct from ω_1.*

Proof. After extending the scalars to $k(\sqrt{b})$, the curve $JQ^{(2)}_{a,b}$ becomes isomorphic to $JQ^{(2,2)}_{ab,\sqrt{b}}$. The result follows from Proposition 6 on that curve. □

4.2 Representability

Proposition 9. *The* (2)*-Jacobi quartics represent exactly all elliptic curves* E *with at least one rational point of order two.*

Proof. Let E be a curve with one rational point of order two; then there exist $r, s, p \in k$ such that E has the equation

$$E : \eta^2 \;=\; (\xi - r)(\xi^2 - s\xi + p). \tag{21}$$

We then define

$$a = s - 2r, \quad b = s^2 - 4p, \tag{22}$$

and coordinates $(x : y : z : t)$ by

$$\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \;=\; \begin{pmatrix} 0 & 1 & 0 & 0 \\ -2r & 0 & 1 & rs - p \\ -s & 0 & 1 & p \\ 1 & 0 & 0 & -r \end{pmatrix} \begin{pmatrix} \xi \\ \eta \\ \xi^2 \\ 1 \end{pmatrix}. \tag{23}$$

We then see that these coordinates satisfy equations (19). □

5 Asymptotic Count of Various Elliptic Curve Models

This section gives the asymptotic probability that a random elliptic curve is represented by one of the quadric intersection models presented above.

5.1 Statistics for the Frobenius Modulo 4

We use the fact that, given an elliptic curve E over a field k of characteristic $\neq 2$, the representability of E by the Jacobi, Edwards or Huff models is determined by the conjugacy class of $\varphi_E \pmod 4$.

For any real number x, let $\mathscr{E}(x)$ be the (finite) set of all isomorphism classes of elliptic curves over finite fields $\mathbb{F}_q$ with $q \leq x$ and q odd.

Proposition 10. *Let* $S \subset GL_2(\mathbb{Z}/4\mathbb{Z})$ *be a conjugacy class. For any elliptic curve* E *over a finite field* k *(of characteristic* $\neq 2$*), let* $\varphi_E \pmod 4$ *be the conjugacy class of the representation of the Frobenius endomorphism of* k *on the* 4*-torsion subgroup of* E*.*

Then we have the asymptotic probability

$$\lim_{x \to \infty} P(\varphi_E \equiv S \pmod 4 \mid E \in \mathscr{E}(x)) \;=\; \frac{\#S}{96}.$$

Proof. Let $X(n)$ be the moduli space of elliptic curves over $\mathbb{F}_q$ equipped with a basis for the n-torsion subgroup. Then the forgetful map $X(4) \to X(1)$ is a covering with Galois group $GL_2(\mathbb{Z}/4\mathbb{Z})$. According to the Artin-Čebotarev theorem [Ser65, Theorem 7][CH11, Theorem 2] applied to this covering map,

the set of elliptic curves over $\mathbb{F}_q$ with Frobenius class equal to S has a Dirichlet density equal to $\#S/\#GL_2(\mathbb{Z}/4\mathbb{Z})$. Finally, the group $GL_2(\mathbb{Z}/4\mathbb{Z})$ is an extension of $GL_2(\mathbb{F}_2)$, which is isomorphic to the symmetric group $\mathfrak{S}_3$, by the group of matrices $\equiv 0 \pmod 2$, which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$; thus, it is a group of order 96. □

We note that the Huff cubic $ax(y^2-1) = by(x^2-1)$ is birationally equivalent to the homogenous quadric intersection form $uz = vt, zt = ab(u^2+v^2)-(a^2+b^2)uv$ by the variable change $t = (a^2-b^2)$, $z = (a^2-b^2)xy$, $u = ax-by$, $v = bx-ay$.

Theorem 11. *The asymptotic proportion of elliptic curves in odd characteristic representable by twisted Edwards, Jacobi quartics, or Huff models are listed in the table below.*

Curve	q odd	$q \equiv +1 \pmod 4$	$q \equiv -1 \pmod 4$
Twisted Edwards	17/48	1/3	3/8
Jacobi quartic	5/32	7/48	1/6
$(2,2)$-Jacobi quartic	1/6	1/6	1/6
(2)-Jacobi quartic	2/3	2/3	2/3
Huff	5/48	1/12	1/8

Proof. These elliptic curve models are all characterized by a set of conjugacy classes of the Frobenius in $GL_2(\mathbb{Z}/4\mathbb{Z})$; namely:

(i) the Jacobi quartics are characterized by the list of conjugacy classes of Theorem 5;
(ii) the $(2,2)$-Jacobi quartics are exactly the curves E satisfying $\varphi_E \equiv \mathrm{id} \pmod 2$ (by Proposition 7);
(iii) the (2)-Jacobi quartics are exactly the curves such that φ_E has a fixed point modulo 2 (by Proposition 9);
(iv) the twisted Edwards curves are exactly the curves with a rational 4-torsion point [BBJ+08, Theorem 3.3], which means that φ_E has a fixed point modulo 4;
(v) the Huff curves are the curves that contain $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ as a subgroup [JTV10, Theorem 2] and are thus the intersection of $(2,2)$-Jacobi quartics and Edwards curves.

In each case, the results follow by counting the number of such matrices in $GL_2(\mathbb{Z}/4\mathbb{Z})$. By the Hasse-Weil theorem, $q = \det(\varphi_E)$; consequently, the conditional results on $q \pmod 4$ are derived by counting the number of such matrices with the suitable determinant.

For instance, the Jacobi quartics in the case where $q \equiv +1 \pmod 4$ correspond to the conjugacy classes of $\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\begin{pmatrix}1&2\\0&1\end{pmatrix}$ and $\begin{pmatrix}-1&2\\0&-1\end{pmatrix}$, with respective cardinalities 1, 3 and 3. Therefore, asymptotically, 7/48 of all elliptic curves with $q \equiv +1$ are isomorphic to a Jacobi quartic. □

Remark 12. If the field k is a prime field then the results about some of these families of curves may also be derived, in a similar way, from statistics about the group structure of elliptic curves [Gek06, 2.18].

5.2 Summary of Quadrics Intersections

All coordinate systems in the following list may be represented as the smooth intersection of two three-dimensional quadrics. For each, we list the cost for a point addition according to literature, the condition for representability of a curve by such a model, and the asymptotic probability that this model represents a random curve, in the sense of Theorem 11.

Curve	Condition	Cost	Probability
Twisted Edwards	$(\mathbb{Z}/4\mathbb{Z})$	$9\mathbf{M} + \mathbf{D}_a + \mathbf{D}_d$	$17/48$
Jacobi quartic	$(\mathbb{Z}/2\mathbb{Z})^2$, $\sqrt{r_1 - r_2}$	$7\mathbf{M} + 3\mathbf{S} + \mathbf{D}_a$	$9/32$
$(2,2)$-Jacobi	$(\mathbb{Z}/2\mathbb{Z})^2$	$7\mathbf{M} + 3\mathbf{S} + \mathbf{D}_a + 2\mathbf{D}_b$	$1/6$
(2)-Jacobi	$(\mathbb{Z}/2\mathbb{Z})$	$8\mathbf{M} + 3\mathbf{S} + \mathbf{D}_a + 2\mathbf{D}_b$	$2/3$
Huff	$(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$	$11\mathbf{M}$	$5/48$

References

[AG11] Ahmadi, O., Granger, R.: On isogeny classes of edwards curves over finite fields. Arxiv preprint arXiv:1103.3381 (2011)

[BBJ+08] Bernstein, D.J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards Curves. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 389–405. Springer, Heidelberg (2008), doi:10.1007/978-3-540-68164-9_26

[BJ03] Billet, O., Joye, M.: The Jacobi Model of an Elliptic Curve and Side-Channel Analysis. In: Fossorier, M., Høholdt, T., Poli, A. (eds.) AAECC 2003. LNCS, vol. 2643, pp. 34–42. Springer, Heidelberg (2003), doi:10.1007/3-540-44828-4_5

[BL07] Bernstein, D.J., Lange, T.: Inverted Edwards Coordinates. In: Boztaş, S., Lu, H.-F. (eds.) AAECC 2007. LNCS, vol. 4851, pp. 20–27. Springer, Heidelberg (2007)

[CH11] Castryck, W., Hubrechts, H.: The distribution of the number of points modulo an integer on elliptic curves over finite fields (Preprint, 2011)

[DIK06] Doche, C., Icart, T., Kohel, D.R.: Efficient Scalar Multiplication by Isogeny Decompositions. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 191–206. Springer, Heidelberg (2006)

[Edw07] Edwards, H.M.: A normal form for elliptic curves. Bulletin-American Mathematical Society 44(3), 393–422 (2007)

[FW10] Feng, R., Wu, H.: On the isomorphism classes of legendre elliptic curves over finite fields. Arxiv preprint arXiv:1001.2871 (2010)

[Gek06] Gekeler, E.-U.: The distribution of group structures on elliptic curves over finite prime fields. Documenta Mathematica 11, 119–142 (2006)

[HWCD08] Hisil, H., Wong, K.K.-H., Carter, G., Dawson, E.: Twisted Edwards Curves Revisited. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 326–343. Springer, Heidelberg (2008)

[HWCD09] Hisil, H., Wong, K.K.-H., Carter, G., Dawson, E.: Faster group operations on elliptic curves. In: Proceedings of the Seventh Australasian Conference on Information Security, AISC 2009, vol. 98, pp. 7–20. Australian Computer Society, Inc., Darlinghurst (2009)

[JTV10] Joye, M., Tibouchi, M., Vergnaud, D.: Huff's Model for Elliptic Curves. In: Hanrot, G., Morain, F., Thomé, E. (eds.) ANTS-IX. LNCS, vol. 6197, pp. 234–250. Springer, Heidelberg (2010)

[LS01] Liardet, P.-Y., Smart, N.P.: Preventing SPA/DPA in ECC Systems using the Jacobi Form. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 391–401. Springer, Heidelberg (2001), doi:10.1007/3-540-44709-1_32

[Mor09] Morain, F.: Edwards curves and cm curves. Arxiv preprint arXiv:0904.2243 (2009)

[Nat00] National Institute of Standards and Technology. FIPS PUB 186-2: Digital Signature Standard (DSS) (January 2000)

[Ono94] Ono, T.: Variations on a theme of Euler: quadratic forms, elliptic curves, and Hopf maps. Plenum. Pub. Corp. (1994)

[RFS10] Farashahi, R.R., Shparlinski, I.: On the number of distinct elliptic curves in some families. Designs, Codes and Cryptography 54, 83–99 (2010), doi:10.1007/s10623-009-9310-2

[Ser65] Serre, J.-P.: Zeta and L functions. In: Proc. Conf. on Arithmetical Algebraic Geometry, Purdue Univ., pp. 82–92. Harper & Row, New York (1965)

[Sil86] Silverman, J.H.: The arithmetic of elliptic curves. Springer, Heidelberg (1986)