Families of elliptic curves with rational 3-torsion

Dustin Moody, Hongfeng Wu

July 23, 2012

Abstract

In this paper we look at three families of elliptic curves with rational 3-torsion over a finite field. These families include Hessian curves, twisted Hessian curves, and a new family we call generalized DIK curves. We find the number of $\mathbb{F}_q$-isogeny classes of each family, as well as the number of $\mathbb{F}_q$-isomorphism classes of the generalized DIK curves. We also include some formulas for efficient computation on these curves, improving upon known results. In particular, we find better formulas for doubling and addition on the original tripling-oriented DIK curves and also for addition and tripling on elliptic curves with j-invariant 0.

1 Introduction

Elliptic curves have been the focus of much research, particularly in the past few decades. An elliptic curve defined over a field K is an abelian variety of dimension 1 defined over K. Traditionally, elliptic curves have been represented by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

with the $a_i \in K$. However, the Weierstrass model is simply one way to represent an elliptic curve. Several alternate models have been proposed. For example, Edwards curves [4], [11], Hessian curves [19], [24], Jacobi quartics [9], and Montgomery curves [21] have all been proposed for use in cryptography.

There have been many interesting results for some of these alternate models. For example, the number of isomorphism classes over $\overline{\mathbb{F}}_q$ (or $\mathbb{F}_q$) for various models has been studied in [8], [12], [15], [16], [17], [14]. Recently, Ahmadi and Granger were able to count the number of $\mathbb{F}_q$-isogeny classes [1] for Edwards curves. Their results extend to twisted Edwards curves, Montgomery curves, Huff curves, and Jacobi intersections. In this work we continue along these lines. We focus our study on Hessian curves, and two related alternative models of curves.

Hessian curves are a one-parameter elliptic curve family with a rational point of order 3. They are defined by the equation

$$H_d : x^3 + y^3 + 1 = 3dxy,$$

with $d \in K, d^3 \neq 1$. The point $(-1, 0)$ has order 3 on H_d, for any d. The use of Hessian curves in mathematics and cryptography has been studied in many papers. One of their primary advantages is that they help prevent against information leakage through side channel attacks. For more on these curves see [6], [9], [12], [13], [18], [19], [24]. There is also a generalized Hessian curve, known as a twisted Hessian curve, given by

$$H_{a,d} : ax^3 + y^3 + 1 = 3dxy$$

for some $a \in K$ with $d^3 \neq a$. This curve was introduced in [6] for use in cryptography, and an equivalent version has been further studied in [13].

We mention another family of elliptic curves related to elliptic curves with 3-torsion. Doche, Icart, and Kohel introduced what are known as *tripling-oriented DIK curves*. This family consists of curves given by the equation $y^2 = x^3 + 3u(x + 1)^2$. These curves were first proposed in [10] as curves for which there are efficient formulas to perform arithmetic necessary for cryptography. In comparison with Hessian curves, DIK curves are characterized by the existence of a rational 3-torsion subgroup, rather than a rational 3-torsion point. In this paper, we generalize the original DIK curves so as to include all elliptic curves with a rational 3-torsion subgroup.

In section 4 of this work we give a formula for the number of isogeny classes for Hessian curves, twisted Hessian curves, and generalized DIK curves. The results for Hessian curves were touched on in [7], but without proof. In doing so, we discover some information about the distribution of curves in the isogeny classes of generalized DIK curves. We also count the number of $\mathbb{F}_q$-isomorphism classes of generalized DIK curves. We note that the number

of isomorphism classes of Hessian curves and twisted Hessian are given in [12] and [13] respectively.

We then look at computing on these curves. We are able to give new records for doubling and addition on the original DIK curves. We give formulas to perform efficient arithmetic on the generalized DIK curves. This includes a subfamily with j-invariant 0, where we are able to improve existing formulas for addition and tripling.

2 Elliptic curves with rational 3-torsion

2.1 Generalized DIK curves

Let E/K be an elliptic curve. For a through background on elliptic curves, see [23]. Let $F(x, y)$ be the defining equation for E as given by (1). We introduce a definition from [10].

Definition 1. *A torsion subgroup G of $E(\bar{K})$ is said to be defined over K or to be K-rational if $G\backslash\{\mathcal{O}\}$ is the zero set of a finite set of polynomials*

$$\{f_1(x, y), f_2(x, y), \cdots, f_n(x, y)\} \in K(x, y)/(F(x, y)).$$

It is well known that a finite subgroup G of E is K-rational if and only if G is the kernel of an isogeny $\psi : E \to E'$ defined over K. Similarly, if K is a perfect field, then a subgroup G of E is K-rational if and only if for any point $P \in G$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $\sigma(P) \in G$. Note that E need not have a K-rational point in G. However if $G = \langle P \rangle$, and P is K-rational, then necessarily G is a K-rational subgroup. We now let K be a finite field $\mathbb{F}_q$, and focus on $\mathbb{F}_q$-rational subgroups of order 3. For the remainder of the paper, we also assume that the characteristic of $\mathbb{F}_q$ is greater than 3.

Theorem 2. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with characteristic different from 2 or 3. Then E has an $\mathbb{F}_q$-subgroup of order 3 if and only if it has an $\mathbb{F}_q$-isomorphism to an elliptic curve of the form $y^2 = x^3 + a(cx + 1)^2$, with $a, c \in \mathbb{F}_q$ and $a(4ac^3 - 27) = 0$.*

Proof. As the characteristic of $\mathbb{F}_q$ is greater than 3, we can assume the defining equation of E is $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Let the $\mathbb{F}_q$-rational subgroup be $G = \{\mathcal{O}, P = (x_P, y_P), -P = (x_P, -y_P)\}$. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, we know $\sigma(P) = (\sigma(x_P), \sigma(y_P)) \in G$, thus $\sigma(x_P) = x_P$ and so $x_P \in \mathbb{F}_q$. This implies

that $y_P^2 \in \mathbb{F}_q$. By changing x to $x - x_P$, we can assume that $P = (0, y_P)$ and $y_P = 0$ (else $2P = \mathcal{O}$). So without loss of generality, we have $a_6 = y_P^2 = 0$.

The addition law on E yields

$$x(2P) = \frac{x_P^4 - 4a_4x_P^2 - 8a_6x_P - (4a_2a_6 - a_4^2)}{4a_6} = \frac{a_4^2 - 4a_2a_6}{4y_P^2}.$$

Therefore, as $x(2P) = x(-P) = 0$, then it follows that $a_4^2 - 4a_2a_6 = 0$.

If $a_4 = 0$ then we must have that a_2 equals 0. The curve E is then of the form $y^2 = x^3 + a$, for some $a \in \mathbb{F}_q$. If instead $a_4 = 0$, then we can perform the change of variables

$$\left(\left(\frac{a_4}{2a_6}\right)^2 x, \left(\frac{a_4}{2a_6}\right)^3 y\right) \to (x, y),$$

to obtain an isomorphic curve $y^2 = x^3 + a(x+t)^2$ where $t = a_4/(2a_6), a = a_6t^4$. Note that $y^2 = x^3 + a(x + t)^2$ can be rewritten $y^2 = x^3 + at^2(x/t + 1)^2$. So whether $a_4 = 0$ or not, we have seen that E is $\mathbb{F}_q$-isomorphic to a curve of the form $y^2 = x^3 + a(cx + 1)^2$.

Conversely, suppose E has an $\mathbb{F}_q$-isomorphism to an elliptic curve of the form $E_{a,c} : y^2 = x^3 + a(cx + 1)^2$. Let $P = (0, \sqrt{a})$. Then it is easy to check that $G = \{\mathcal{O}, P, -P\}$ is an $\mathbb{F}_q$-rational subgroup of order 3. □

We give the curves of Theorem 2 a special name.

Definition 3. *Let $E_{a,c}$ be an elliptic curve over $\mathbb{F}_q$, defined by the equation*

$$y^2 = x^3 + a(cx + 1)^2$$

with $a(4ac^3 - 27) = 0$. Then we call $E_{a,c}$ a generalized DIK curve.

Recall the original DIK curves are of the form $y^2 = x^3 + 3u(x + 1)^2$, and so they are the generalized DIK curves $E_{3u,1}$. Up to twists, every curve with a rational 3-torsion subgroup can be written in the original DIK form. By Theorem 2, we see that the generalized DIK curves are exactly the family of all elliptic curves with rational 3-torsion subgroup, without needing to recourse to twisting.

Corollary 4. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with characteristic different from 2, or 3. Then E has an $\mathbb{F}_q$-rational point of order 3 if and only if E has an $\mathbb{F}_q$-isomorphism to an elliptic curve of the form $W_{a,b} : y^2 = x^3 + (ax + b)^2$, with $a, b \in \mathbb{F}_q, b(4a^3 - 27b) = 0$.*

Proof. Suppose first that E is isomorphic to the elliptic curve $W_{a,b} : y^2 = x^3 + (ax + b)^2$. Then it is easy to check that $(0, b)$ is a point of order 3 on $W_{a,b}/\mathbb{F}_q$. By the isomorphism, then E also has a rational point of order 3.

Now suppose that E has an $\mathbb{F}_q$-rational point P of order 3. We saw in the proof of Theorem 2 that we can assume E has equation $y^2 = x^3 + c$ or $y^2 = x^3 + a(x + t)^2$ for some $t \in \mathbb{F}_q$, with $a = y_P^2 t^4$ a square in $\mathbb{F}_q$. If E is the curve $y^2 = x^3 + c$, it is already in the desired form. Otherwise, we can rearrange the equation for E as $y^2 = x^3 + (y_P t^2 x + y_p t^3)^2$, which completes the proof. □

A better known way to write an elliptic curve with an $\mathbb{F}_q$-rational point of order 3 is $y^2 + a_1xy + a_3y = x^3$, where the point $(0, 0)$ has order 3. We will use the form given in Corollary 4, as it is very similar to the equation for the generalized DIK curves.

3 Hessian and twisted Hessian curves

We now turn our attention to Hessian curves and twisted Hessian curves. Recall that every Hessian curve has a rational point of order 3, namely the point $(-1, 0)$. Thus Hessian curves form a subset of the curves $W_{a,b}$ described in Corollary 4. The following lemma explicitly shows this relationship.

Lemma 5. *Let $\mathbb{F}_q$ be a finite field of characteristic greater than 3, and let $d \in \mathbb{F}_q$ with $d^3 = 1$. In projective coordinates, the Hessian curve*

$$H_d : \ U^3 + V^3 + W^3 = 3dUVW$$

is isomorphic to the elliptic curve

$$W_{a,b} : \ Y^2Z = X^3 + Z(aX + bZ)^2,$$

where $a = (d + 2)$, and $b = 4(d^2 + d + 1)/3$.

Proof. The isomorphism is given by the change of variables

$$\begin{aligned} U &= \frac{3d}{8(d^3-1)}X + \frac{3}{8(d^3-1)}Y + \frac{1}{2(d-1)}Z, \\ V &= \frac{3d}{8(d^3-1)}X + \frac{-3}{8(d^3-1)}Y + \frac{1}{2(d-1)}Z, \\ W &= \frac{-3}{4(d^3-1)}X + \frac{1}{1-d}Z. \end{aligned}$$

The inverse change of variables is

$$\begin{aligned} X &= \frac{(4d^2+4d+4)}{3}U + \frac{(4d^2+4d+4)}{3}V + \frac{(4d^2+4d+4)}{3}W, \\ Y &= \frac{(4d^3-4)}{3}U + \frac{(4-4d^3)}{3}V, \\ Z &= -U - V - dW. \end{aligned}$$

□

The majority of results in this paper will fall into two cases, depending on q mod 3. Note that when $q \equiv 2 \bmod 3$, then every element is a cube in $\mathbb{F}_q$. We will also need the fact that when $q \equiv 1 \bmod 3$, then -3 is a square in $\mathbb{F}_q$.

Theorem 6. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with $q \equiv 2$ mod 3. Then E has a point of order 3 if and only if it is $\mathbb{F}_q$-isomorphic to a Hessian curve $H_d : x^3 + y^3 + 1 = 3dxy$.*

Proof. Suppose first that E is isomorphic to a Hessian curve H_d. As the point $(-1, 0)$ has order 3 on H_d, then E has a point of order 3. Now suppose that E is an elliptic curve with a rational point of order three. By Corollary 4, we can assume that the equation for E is $y^2 = x^3 + (ax + b)^2$. By composing with the isomorphism $(x, y) \to (u^2, u^3 y)$, for some $u = 0$ in $\mathbb{F}_q$, then the curve $E_u : y^2 = x^3 + (aux + bu^3)^2$ is isomorphic to E. If we choose u to be a root of $3bu^3 - 4a^2u^2 + 12au - 12$, then it can be checked that setting $d = au - 2$ satisfies $bu^3 = \frac{4}{3}(d^2 + d + 1)$. Then by Lemma 5, we see E_u is isomorphic to the Hessian curve H_d.

It remains to be checked that $3bu^3 - 4a^2u^2 + 12au - 12 = 0$ has a root in $\mathbb{F}_q$. If $a = 0$ then this is clear. For $a = 0$, let $\beta \in \mathbb{F}_q$ be such that $\beta^3 = \frac{4a^3}{4a^3 - 27b}$, which is possible as $q \equiv 2 \bmod 3$. Then $\frac{3\beta}{a(\beta-1)}$ is a root of $3bu^3 - 4a^2u^2 + 12au - 12 = 0$ in $\mathbb{F}_q$. □

When $q \equiv 1 \bmod 3$, then Theorem 6 is not true. That is, the family of Hessian curves over $\mathbb{F}_q$ is not equivalent to the family of curves with an $\mathbb{F}_q$-rational point of order 3. The next proposition shows this latter family is however, the same as twisted Hessian curves.

Proposition 7. *Let $\mathbb{F}_q$ be a finite field with characteristic greater than 3, and $a, d \in \mathbb{F}_q$ with $d^3 = a$ and $a = 0$. In projective coordinates, the twisted Hessian curve*

$$H_{a,d} : \ aU^3 + V^3 + W^3 = 3dUVW$$

is $\mathbb{F}_q$-isomorphic to an elliptic curve of the form $W_{s,t}: Y^2Z = X^3 + Z(sX + tZ)^2$.

Proof. If $q \equiv 2 \bmod 3$, then every element of $\mathbb{F}_q$ is a cube. Therefore, each curve $au^3 + v^3 + 1 = 3duv$ can be changed into a Hessian curve $u^3 + v^3 + 1 = 3d'uv$ for some d' by a suitable change of variables. The result then follows from Lemma 5.

If instead $q \equiv 1 \bmod 3$, then there exists an $\varepsilon \in K$ such that $\varepsilon^2 + \varepsilon + 1 = 0$. In projective coordinates, the curve $H_{a,d}$ is isomorphic to the elliptic curve $W_{s,t}$ with $s = d/2, t = (d^3 - a)/54$ via the change of variables

$$\begin{aligned} U &= X, \\ V &= -s\epsilon X - (\epsilon + 2)Y - 3t\epsilon Z, \\ W &= s(1 + \epsilon)X + (\epsilon - 1)Y + 3t(\epsilon + 1)Z. \end{aligned}$$

The inverse change of variables is given by

$$\begin{aligned} X &= U, \\ Y &= -\tfrac{1+\epsilon}{2(1+2\epsilon)}V - \tfrac{\epsilon}{2(1+2\epsilon)}W, \\ Z &= -\tfrac{s}{3t}U + \tfrac{\epsilon-1}{6t(1+2\epsilon)}V + \tfrac{\epsilon+2}{6t(1+2\epsilon)}W. \end{aligned}$$

□

The previous proposition shows that over $\mathbb{F}_q$, the family of twisted Hessian curves is equivalent to the family of curves $W_{a,b}: y^2 = x^3 + (ax + b)^2$ in the sense of isomorphism over $\mathbb{F}_q$. Thus twisted Hessian curves are exactly the curves with a rational point of order 3. We note that Farashahi and Joye have an equivalent result in [13].

Observe that the curve $y^2 = x^3 + (ax + b)^2$ may be rewritten $y^2 = x^3 + b^2(a/bx + 1)^2$, showing that every curve with a rational point of order 3 is a generalized DIK curve. Therefore

$$\{\text{Hessian curves}\} \subseteq \{\text{Twisted Hessian curves}\} \subseteq \{\text{generalized DIK curves}\}. \tag{2}$$

If $q \equiv 2 \bmod 3$, then the three sets are equal. The first equality is clear, since every element in $\mathbb{F}_q$ is a cube. We now prove the second equality.

Proposition 8. *Let $E_{a,c}: y^2 = x^3 + a(cx + 1)^2$ be a generalized DIK curve over $\mathbb{F}_q$, with $q \equiv 2$ mod 3. Then $E_{a,c}$ has a rational point of order 3. In other words, the family of generalized DIK curves over $\mathbb{F}_q$ is the same as the family of Hessian, or twisted Hessian curves.*

Proof. Let $E_{a,c}$ be an elliptic curve $E_{a,c} : y^2 = x^3 + a(cx+1)^2$ over $\mathbb{F}_q$. Suppose first that $a = s^2$, for some s. Then $E_{a,c} : y^2 = x^3 + (csx+s)^2$, and by Corollary 4 then $E_{a,c}$ has a rational point of order 3.

So we now assume that a is not a square in $\mathbb{F}_q$. If we twist $E_{a,c}$ by a, then we get a curve $E' : y^2 = x^3 + a^2c^2x^2 + 2a^3cx + a^4$, or $y^2 = x^3 + (acx + a^2)^2$. We see that E' has a rational point of order 3 by Corollary 4. Then, as E and E' are twists, their cardinalities N and N' sum to $2q+2$ which is $\equiv 0$ mod 3. As $N' \equiv 0$ mod 3, then likewise $N \equiv 0$ mod 3. Thus E has a point of order 3. □

When $q \equiv 1$ mod 3, then the three families in (2) are not equal. We already noted that an elliptic curve with rational 3-torsion subgroup need not have an $\mathbb{F}_q$-rational point of order 3. Explicitly, if E is the curve $y^2 = x^3 + a(cx+1)^2$, and a is a non-square, then the point $P = (0, \sqrt{a})$ generates a rational 3-torsion subgroup, despite P not being $\mathbb{F}_q$-rational. This shows that the generalized DIK curves are not the same as the family of twisted Hessian curves, when $q \equiv 1$ mod 3. To see that Hessian curves and twisted Hessian curves yield different families, we need a theorem from [22].

Theorem 9. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over a finite field K with $\sqrt{-3} \in K$. Then E has as its torsion subgroup $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ if and only if a and b can parameterized by $\alpha \in K$, $\alpha = 3, -\frac{3}{2}(1 \pm \sqrt{-3})$, with*

$$\begin{aligned} a &= -\tfrac{1}{3^3}\alpha(\alpha+6)(\alpha^2 - 6\alpha + 36), \\ b &= -\tfrac{2}{3^6}(\alpha^2 - 6\alpha - 18)(\alpha^4 + 6\alpha^3 + 54\alpha^2 - 108\alpha + 324). \end{aligned}$$

This allows us to prove the following theorem.

Theorem 10. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with $q \equiv 1$ mod 3. Then E has two independent points of order 3 if and only if it has an $\mathbb{F}_q$-isomorphism to a Hessian curve $x^3 + y^3 + 1 = 3dxy$.*

Proof. We saw in the proof of Proposition 7 that when $q \equiv 1$ mod 3, then the Hessian curve $x^3 + y^3 + 1 = 3dxy$ is isomorphic to the curve $y^2 = x^3 + (dx/2 + (d^3-1)/54)^2$. This curve is in turn isomorphic to $y^2 = x^3 + (3dx + 4(d^3-1))^2$ via $(x, y) \to (6^2x, 6^3y)$. Putting this in short Weierstrass form, this is the curve

$$y^2 = x^3 - 3d(d^3+8)x - 2(d^6 - 20d^3 - 8).$$

So we only need to prove E has two points with order 3 if and only if it is $\mathbb{F}_q$-isomorphic to some curve of the form $y^2 = x^3 - 3d(d^3+8)x - 2(d^6 - 20d^3 - 8)$.

Assuming that $E : y^2 = x^3 + ax + b$ has two points with order 3, then from Theorem 9, let $\beta = \alpha/3$, then

$$\begin{cases} a &= -3\beta(\beta^3 + 8), \\ b &= -2(\beta^6 - 20\beta^3 - 8). \end{cases}$$

Hence, $E : y^2 = x^3 + ax + b$ isomorphic to some Hessian curve.

For the converse, since $\sqrt{-3} \in \mathbb{F}_q$, then it is easily checked that $(3d^2, 4(d^3-1))$ and $(-(d+2)^2, 4\sqrt{-3}(d^2+d+1))$ are two linearly independent points of order 3 on $E/\mathbb{F}_q : y^2 = x^3 - 3d(d^3+8)x - 2(d^6 - 20d^3 - 8)$. □

So for $q \equiv 1 \bmod 3$, Hessian curves have two independent points of order 3, while twisted Hessian curves need only have 1. Thus the two families are not the same, as is the case when $q \equiv 2 \bmod 3$.

4 Isogeny and isomorphism classes

4.1 The number of isogeny classes

In this section we find the number of isogeny classes of the families from the previous section. This includes Hessian curves, twisted Hessian curves, and generalized DIK curves. To do so, we look at the possible cardinalities of these curves over $\mathbb{F}_q$. Tate's theorem states that two elliptic curves are isogenous over $\mathbb{F}_q$ if and only if they have the same number of $\mathbb{F}_q$-rational points [25]. So we can count isogeny classes by counting cardinalities. The following theorem is proved in [27] and appears as stated in [26].

Theorem 11. *Let $q = p^n$ be a power of a prime p and let $N = q + 1 - t$. There is an elliptic curve E defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = N$ if and only if $t \leq 2\sqrt{q}$ and t satisfies one of the following:*

1. *$gcd(t, p) = 1$*
2. *n is even and $t = \pm 2\sqrt{q}$*
3. *n is even, $p \not\equiv 1 \bmod 3$, and $t = \pm\sqrt{q}$*
4. *n is odd, $p = 2$, or 3, and $t = \pm p^{(n+1)/2}$*
5. *n is even, $p \not\equiv 1 \bmod 4$, and $t = 0$*
6. *n is odd and $t = 0$.*

The condition $t \leq 2\sqrt{q}$ is known as Hasse's condition. In particular, we observe that every possible trace t between the Hasse bounds is allowable, when $(t, p) = 1$. These are the ordinary curves. The rest of the conditions describe what supersingular traces are possible, i.e. when $(t, p) > 1$.

We separate our study into two cases, depending on q mod 3. When $q \equiv 2 \bmod 3$, then we observed in the last section that the families of Hessian curves, twisted Hessian curves, and generalized DIK curves are the same. We now give the formula for the number of isogeny classes of these families. We denote this number by M_q.

Theorem 12. *The number of isogeny classes of Hessian curves over $\mathbb{F}_q$ is*

$$M_q = 1 + 2\Big\lfloor \frac{2\sqrt{q}}{3} \Big\rfloor - 2\Big\lfloor \frac{2\sqrt{q}}{3p} \Big\rfloor,$$

when $q \equiv 2$ mod 3.

Proof. Let t be such that $N = q + 1 - t$ is a multiple of 3, and $|t| \leq 2\sqrt{q}$. If $(t, q) = 1$ then by Theorem 11 we know there is an elliptic curve with trace t. As $3|\#E(\mathbb{F}_q)$, then there is a rational point of order 3, and by Theorem 6, E is $\mathbb{F}_q$-isomorphic to a Hessian curve. This takes care of all the ordinary curves.

Let p be the characteristic of $\mathbb{F}_q$, so q is a power of p. As $q \equiv 2 \bmod 3$, then we must have that $p \equiv 2 \bmod 3$ and $q = p^{2k+1}$ for some k. The only allowable trace with $(t, q) > 1$ is when $t = 0$. When $t = 0$ then $N \equiv 0 \bmod 3$, so we see that curves with trace 0 are $\mathbb{F}_q$-isomorphic to Hessian curves.

Conversely, if E is a Hessian curve then by Theorem 6 E has a point of order 3, and so its cardinality N is divisible by three. If E is supersingular then the trace of E must be 0. Thus the number of isogeny classes is the number of multiples of 3 between the Hasse bounds which yield ordinary curves, and we add one for the supersingular curves with cardinality $N = q + 1$.

If we write $q = 3k + 2$, then by Lemma 13, we have

$$\begin{aligned} M_q &= \frac{q+1+2\sqrt{q}}{3} - \frac{q+1-2\sqrt{q}}{3} - \frac{2\sqrt{q}}{3p} - \frac{-2\sqrt{q}}{3p} + 1 \\ &= k+1+\frac{2\sqrt{q}}{3} - k+1+\frac{-2\sqrt{q}}{3} - 1+2\ \frac{2\sqrt{q}}{3p} + 1 \\ &= \frac{2\sqrt{q}}{3} - \frac{-2\sqrt{q}}{3} - 2\ \frac{2\sqrt{q}}{3p} \\ &= 1+2\ \frac{2\sqrt{q}}{3} - 2\ \frac{2\sqrt{q}}{3p}\ . \end{aligned}$$

□

Lemma 13. *The number of t satisfying $a \leq t \leq b$ with $t \equiv c \bmod m$ is*

$$\frac{b-c}{m} - \frac{a-c}{m}\ .$$

Proof. This is elementary. □

We now turn our attention to when $q \equiv 1 \bmod 3$. In this case, we have that

$$\{\text{Hessian curves}\} \subsetneq \{\text{twisted Hessian curves}\} \subsetneq \{\text{generalized DIK curves}\}.$$

We start with Hessian curves. Before we give the number of Hessian isogeny classes, we need a preliminary result.

Proposition 14. *Let $q \equiv 1$ mod 3, and $E(\mathbb{F}_q)$ an elliptic curve. If $9|\#E(\mathbb{F}_q)$, then E is isogenous to a curve over $\mathbb{F}_q$ containing a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

Proof. As $9|\#E(\mathbb{F}_q)$, then E contains either $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$ as a subgroup. If $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is the subgroup, then we are done, so we assume that E has the subgroup $\mathbb{Z}/9\mathbb{Z}$. Let P be a point of order 9 on E.

By Corollary 4, we can write the equation for E as $y^2 = x^3 + (ax + b)^2$, for some $a, b \in \mathbb{F}_q$, with a point of order 3 given by $3P = (0, b)$. Using Vélu's formula, we can construct a 3-isogeny ϕ whose kernel is the subgroup $\langle 3P \rangle$:

$$\phi(x, y) = \frac{x^3 + 4abx + 4a^2}{x^2}, y\frac{x^3 - 4abx - 8a^2}{x^3}\ .$$

The image of ϕ is the curve

$$E' : \ y^2 = x^3 + a^2x^2 - 18abx - b(16a^3 + 27b).$$

Now let $Q = \phi(P)$, which is necessarily a point of order 3 on E', since $3Q = 3\phi(P) = \phi(3P) = \infty$. Denote the dual of ϕ by $\hat{\phi}$. Then $\hat{\phi}(Q) = \hat{\phi}(\phi(P)) = 3P$, so we see Q is not in the kernel of $\hat{\phi}$.

Consider the point

$$R = \quad -\frac{4a^2}{3}, \frac{4a^3 - 27b}{3\sqrt{-3}} \quad .$$

A calculation checks that R is on E', and that $2R = -R$, so that R is a point of order 3. As $q \equiv 1 \bmod 3$, then -3 is a square in $\mathbb{F}_q$, and hence $R \in E'(\mathbb{F}_q)$. It is easy to see that $\hat{\phi}(R) = \infty$, and so the kernel of $\hat{\phi} = \langle R \rangle$. Thus $R = \pm Q$, and we have two independent points of order 3 on $E'(\mathbb{F}_q)$. So E is isogenous to a curve E' which contains $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ as a subgroup. This proves the proposition. □

Corollary 15. *Let $q \equiv 1$ mod 3, and $0 \leq c \leq 8$ be the residue class of $(q+1)/p$ mod 9. Then the number of isogeny classes of Hessian curves over $\mathbb{F}_q$ is*

$$M_q = \frac{q+1+2\sqrt{q}}{9} - \frac{q+1-2\sqrt{q}}{9} - \frac{2\sqrt{q}-cp}{9p} - \frac{-2\sqrt{q}-cp}{9p} + S_q,$$

where $S_q = 0$ if $q = p^{2k+1}$ and $S_q = 1$ if $q = p^{2k}$.

Proof. By Tate's Theorem, we need only count the possible number of different cardinalities that Hessian curves can have. When $q \equiv 1 \bmod 3$, then every Hessian curve has cardinality divisible by 9 by Theorem 10. Conversely suppose that E is an elliptic curve over $\mathbb{F}_q$ such that $9|\#E(\mathbb{F}_q)$. By Proposition 14 and Theorem 10, then E is isogenous to a Hessian curve.

We now look at the possible supersingular traces. As $q \equiv 1 \bmod 3$ and $N \equiv 0 \bmod 3$, then $t \equiv 2 \bmod 3$. So we cannot have $t = 0$ as a possible trace. Thus if $q = p^{2k+1}$, then there are no supersingular Hessian curves. We now can assume that $q = p^{2k}$. Let $\epsilon = \pm 1$ such that $p^k \equiv \epsilon \bmod 3$. Then $\epsilon 2p^k$ is a valid trace, while $-\epsilon 2p^k$ is not. Neither $\pm p^k$ can be a valid trace, which can be seen by considering p mod 9: running through the various possibilities, we see that $p^{2k} + 1 \pm p^k \not\equiv 0 \bmod 9$, when $p \equiv 2 \bmod 3$.

The supersingular trace condition can be summarized by $t \equiv q+1 \bmod 9$ and $t \equiv 0 \bmod p$. These can be combined into the condition $t \equiv cp \bmod 9p$, where $c = (q+1)/p \bmod 9$. The formulas given in the statement of the theorem now follow by Lemma 13.

□

We next look at twisted Hessian curves.

Theorem 16. *Let $q \equiv 1$ mod 3, and $0 \leq c \leq 2$ be the residue class of p mod 3. Then the number of isogeny classes of twisted Hessian curves over $\mathbb{F}_q$ is*

$$M_q = \frac{q+1+2\sqrt{q}}{3} - \frac{q+1-2\sqrt{q}}{3} - \frac{2\sqrt{q}+cp}{3p} - \frac{-2\sqrt{q}+cp}{3p} + S_q,$$

where $S_q = 0$ if $q = p^{2k+1}$ and $S_q = c$ if $q = p^{2k}$.

Proof. We previously demonstrated that the family of twisted Hessian curves is the same as elliptic curves with a rational point of order 3, when $q \equiv 1 \bmod 3$. Thus, if E is a twisted Hessian curve over $\mathbb{F}_q$, then $3|\#E(\mathbb{F}_q)$. Conversely, if $q+1-2\sqrt{q} \leq N \leq q+1+2\sqrt{q}$ is a multiple of 3, then by Corollary 4 E may be written $y^2 = x^3 + (ax+b)^2$. From section 2, we saw this curve is $\mathbb{F}_q$-isomorphic to a twisted Hessian curve.

As $q+1 \equiv 2 \bmod 3$, then $t \equiv 2 \bmod 3$. Thus $t = 0$ is not a possible trace, and so for $q = p^{2k+1}$ there are no supersingular twisted Hessian curves. We can now assume $q = p^{2k}$. Let $\epsilon = \pm 1$ such that $\epsilon \equiv p^k \bmod 3$. Then $\epsilon 2p^k$ is a valid trace, while $-\epsilon 2p^k$ is not. If $p \equiv 2 \bmod 3$, then $-\epsilon p^k$ will be a valid trace, while ϵp^k is not.

Let $c = p \bmod 3$, so $c = 1$ or 2. Then the supersingular trace conditions may be summarized as $t \equiv -cp \bmod 3p$. The results given in the statement of the theorem now follow. □

And finally, for generalized DIK curves we are able to prove the following theorem.

Theorem 17. *Let $q \equiv 1$ mod 3. For generalized DIK curves, i.e., curves with a rational 3-torsion subgroup, then the number of isogeny classes is*

$$M_q = 2\lfloor 2\sqrt{q} \rfloor - 2\,\frac{2\sqrt{q}}{3} - 2\,\frac{2\sqrt{q}}{p} + 2\,\frac{2\sqrt{q}}{3p} + S_q,$$

where $S_q = 0$ if $q = p^{2k+1}$, $S_q = 2$ if $q = p^{2k}$, $p \equiv 1$ mod 3, and $S_q = 4$ if $q = p^{2k}, p \equiv 2$ mod 3.

Proof. Let N be the cardinality of a generalized DIK curve E. We may write E as $y^2 = x^3 + a(cx+1)^2$. If a is a square, then the proof of Theorem 2 shows that $(0, \sqrt{a})$ is a point of order 3. We then have $3|N$. Now suppose that a is a non-square in $\mathbb{F}_q$, from which it follows that $3 \mid N$. Let E' denote the elliptic curve obtained by twisting E by a. That is, $E' : y^2 = x^3 + a(ac^2x^2) + a^2(2acx) + a^3(a)$. Then E' is a generalized DIK curve, with a rational point of order 3, since $E' : y^2 = x^3 + (acx + a^2)^2$. As E and E' are quadratic twists, then we know $N + N' = 2q + 2$. As $N' \equiv 0 \bmod 3$, then we see that $N \equiv 1 \bmod 3$. So we see that if E is a generalized DIK curve, then $N \equiv 0$ or $1 \bmod 3$.

Conversely, suppose $N \equiv 0 \bmod 3$. Then Corollary 4 shows E can be written in the form $y^2 = x^3 + (ax + b)^2$, with $b = 0$, or equivalently $y^2 = x^3 + b^2\left(\frac{a}{b}x + 1\right)^2$. This is a generalized DIK curve.

Now suppose $N \equiv 1 \bmod 3$. Then let $N' = 2q + 2 - N$, and hence $N' \equiv 0 \bmod 3$. Then we have a generalized DIK curve $E' : y^2 = x^3 + a(cx + 1)^2$ with cardinality N'. If we twist E' by a quadratic non-residue $t = 0$, we get the curve $E : y^2 = x^3 + at^2\left(\frac{c}{t}x + 1\right)^2$ and E is a generalized DIK curve with cardinality N.

We now examine the possible supersingular traces. As $t = q + 1 - N$, then we see $t \not\equiv 0 \bmod 3$. So there can be no supersingular curves with $t = 0$. Thus for $q = p^{2k+1}$, any generalized DIK curve is an ordinary curve. The number of isogeny classes in this case is

$$\begin{aligned} M_q = \; & q + 1 + 2\sqrt{q} \; - \; q + 1 - 2\sqrt{q} \; - \; \frac{2\sqrt{q}}{3} \; - \; \frac{-2\sqrt{q}}{3} \\ & - \; \frac{2\sqrt{q}}{p} \; - \; \frac{-2\sqrt{q}}{p} \; + \; \frac{2\sqrt{q}}{3p} \; - \; \frac{-2\sqrt{q}}{3p} \\ = \; & 2 \; 2\sqrt{q} \; - 2 \; \frac{2\sqrt{q}}{3} \; - 2 \; \frac{2\sqrt{q}}{p} \; + 2 \; \frac{2\sqrt{q}}{3p} \; . \end{aligned}$$

For $q = p^{2k}$, then both $t = \pm 2p^k$ are valid traces. When $p \equiv 2 \bmod 3$, then $t = \pm p^k$ are also valid. The stated result now follows. □

4.2 Trace ratio results

For the generalized DIK curve $E_{a,c}(\mathbb{F}_q) : y^2 = x^3 + c(ax + 1)^2$, let $A(E_{a,c}, \mathbb{F}_q)$ denote the trace of the Frobenius endomorphism. Then it is well known that

$\#E_{a,c}(\mathbb{F}_q) = q + 1 - A(E_{a,c}, \mathbb{F}_q)$, with $|A(E_{a,c}, \mathbb{F}_q)| \leq 2\sqrt{q}$. When the context is clear, we will just write A. Let

$$N(A) = \#\{(a, c) \in \mathbb{F}_q \times \mathbb{F}_q | A(E_{a,c}, \mathbb{F}_q) = A\,, a(4ac^3 - 27) = 0\}.$$

Note that $N(A)$ can be analogously defined for any elliptic curve. Katz looked at these quantities for Legendre curves, and showed several results concerning their ratios. [20]. For Edwards curves, Ahmadi and Granger were able to demonstrate certain relationships hold between $N(A)$ and $N(-A)$ [1]. For generalized DIK curves, we have the following result.

Proposition 18. *For the family of generalized DIK curves over $\mathbb{F}_q$, then $N(A) = N(-A)$.*

Proof. We create a bijection between the generalized DIK curves with trace A and $-A$. Let t be a fixed non-square in $\mathbb{F}_q$. Given a curve $E_{a,c}; y^2 = x^3 + a(cx + 1)^2$, let $\phi_t(E_{a,c})$ be the curve obtained by twisting by t. That is $\phi_t(E_{a,c}) = y^2 = x^3 + atc^2x^2 + 2act^2x + at^3 = E_{at^3,c/t}$. We see ϕ_t is injective.

Now consider a generalized DIK curve $E_{b,d}$ with trace $-A$. Twisting by t gives the curve $E_{bt^3,d/t}$, which has trace A. Under the transformation $(x, y) \to (t^2x, t^3y)$, then this curve is isomorphic to $E_{b/t^3,td}$. But then $\phi_t(E_{b/t^3,td}) = E_{b,d}$, showing ϕ_t is surjective. □

Proposition 18 is not valid for the family of Hessian curves or twisted Hessian curves (unless $q \equiv 2 \bmod 3$). From experimental observations, we did not notice any noticeable patterns between $N(A)$ and $N(-A)$ for Hessian or twisted Hessian curves in the case when $q \equiv 1 \bmod 3$. For Hessian curves, when $q \equiv 1 \bmod 3$, then $3|N(A)$ for any A. This follows as on a given Hessian curve there are two independent points of order 3, hence two 3-isogenies to two other Hessian curves. These three curves all share the same trace A. When $q = p^{2k}$ there is exactly one supersingular trace. It appears the number of supersingular curves in this case is $p - 1$ when $p \equiv 1 \bmod 3$, and $p - 2$ when $p \equiv 2 \bmod 3$. It might be possible to prove this using the Hasse polynomial (see section V.4 of [23]).

For twisted Hessian curves with $q \equiv 1 \bmod 3$, then $N(A)$ is always even. This follows as on any twisted Hessian curve there is always a point of order 3. So there is likewise always a 3-isogeny to another twisted Hessian curve, resulting in pairs for each isogeny class.

We saw in section 3 that the Hessian curve H_d has a birational transformation to the curve $y^2 = x^3 - 3d(d^3+8)x - 2(d^6 - 20d^3 - 8)$, $d^3 = 1$. We use this representation over finite fields $\mathbb{F}_q$, with $q \equiv 2 \bmod 3$, and let d vary. Based on numerical evidence, it appears that the number of supersingular curves is jh, where h is the class number of $\mathbb{Q}(\sqrt{-q})$, and j is 1,2, or 4. It seems $j = 1$ when $q \equiv 5 \bmod 12$, $j = 2$ when $q \equiv 23 \bmod 24$, and $j = 4$ when $q \equiv 11 \bmod 24$.

4.3 Isomorphism classes of generalized DIK curves

In this section, we determine the number N_q of $\mathbb{F}_q$-isomorphism classes of generalized DIK curves. The results for Hessian and twisted Hessian curves are known [12], [13]. We re-state the twisted Hessian result, as we can easily determine N_q from it.

Theorem 19. *Let N'_q denote the number of $\mathbb{F}_q$-isomorphism classes of twisted Hessian curves. Then*

$$N'_q = \begin{cases} q-1 & \text{if } q \equiv 2 \bmod 3, \\ (3q+9)/4 & \text{if } q \equiv 1 \bmod 12, \\ (3q+7)/4 & \text{if } q \equiv 7 \bmod 12. \end{cases}$$

Theorem 20. *Let N_q denote the number of $\mathbb{F}_q$-isomorphism classes of generalized DIK curves. Then*

$$N_q = \begin{cases} q-1 & \text{if } q \equiv 2 \bmod 3, \\ (3q+9)/2 & \text{if } q \equiv 1 \bmod 12, \\ (3q+7)/2 & \text{if } q \equiv 7 \bmod 12. \end{cases}$$

Proof. When $q \equiv 2 \bmod 3$, then by Proposition 8 we know the family of generalized DIK curves is the same as the family of twisted Hessian curves. For $q \equiv 1 \bmod 3$, then consider first the generalized DIK curves $E_{a,c} : y^2 = x^3 + a(cx+1)^2$ with $a = 0$ a square in $\mathbb{F}_q$, say $a = d^2$. Then we can rewrite $E_{a,c} : y^2 = x^3 + (cdx + d)^2$. By Proposition 7, these curves are $\mathbb{F}_q$-isomorphic to twisted Hessian curves.

Now consider the curves $E_{a,c}$ with a a non-square in $\mathbb{F}_q$. Each such curve is a non-trivial quadratic twist of a generalized DIK curve $E_{b,d}$ with b a square. It is easy to check as we run over all the non-square a, then we run over all the square b in $\mathbb{F}_q^*$. This implies that N_q is exactly twice the number of $\mathbb{F}_q$-isomorphism classes of the $E_{a,c}$ with a square. Thus $N_q = 2N'_q$, when $q \equiv 1 \bmod 3$. This completes the proof. □

Remark: it seems difficult to count the number of $\mathbb{F}_q$-isomorphism classes of the original tripling-oriented DIK curves $y^2 = x^3 + 3a(x+1)^2$. Farashahi and Shparlinski [15] obtained the number of $\overline{\mathbb{F}}_q$-isomorphism classes, but not the number of $\mathbb{F}_q$-isomorphism classes. From numerical observations, this number is approximately $5q/6$ when $q \equiv 1 \bmod 3$, and $3q/4$ when $q \equiv 2 \bmod 3$.

5 Arithmetic on generalized DIK curves

In this section, we look at how to efficiently perform arithmetic on a generalized DIK curve. Let M and S respectively denote the cost of a multiplication and a squaring in the finite field $\mathbb{F}_q$. We also use C to denote the cost of a multiplication by a constant in the finite field. We are assuming the cost of an addition in $\mathbb{F}_q$ is negligible in comparison to M, S, or C.

Throughout this section we use Jacobian, or extended Jacobian coordinates. With these coordinates, the elliptic curve $E_{a,c}$ has the form $E_{a,c}; Y^2 = X^3 + ac^2X^2Z^2 + 2acXZ^4 + aZ^6$. Points in Jacobian coordinates are represented by the triple (X, Y, Z) which corresponds to the affine point $(X/Z^2, Y/Z^3)$, when $Z = 0$. The extended Jacobian coordinate for the same point is (X, Y, Z, Z^2).

5.1 Improved formulae for the original DIK curves

For the original tripling-oriented DIK curves $y^2 = x^3 + 3u(x+1)^2$, the record for doubling and addition formulae is $2M + 7S$ and $11M + 6S$ respectively [3]. We are able to present faster formulas. The count for our new formula for doubling on an original DIK curve is $1M + 8S + 3C$, while for addition it is $11M + 4S + 3C$.

Doubling For the curve $y^2 = x^3 + 3u(x+1)^2$, the new doubling formula is $2(X_1, Y_1, Z_1, Z_1^2) = (X_3, Y_3, Z_3, Z_3^2)$:

$$\begin{aligned}
C_1 &= u,\ C_2 = 6u - 3u^2, \\
A &= Z_1^2,\ B = X_1 + C_1 * A,\ D = B^2,\ E = Y_1^2,\ F = E^2, \\
S &= 2((B+E)^2 - D - F),\ M = 3D + C_2 * A^2,\ T = M^2 - 2S, \\
Z_3 &= (Y_1 + Z_1)^2 - A - E,\ R = Z_3^2 \\
X_3 &= T - C_1 * R,\ Y_3 = M \cdot (S - T) - 8F.
\end{aligned}$$

The new formula costs $1M+8S+3C$. The $3C$ are multiplications by C_1 and C_2.

Addition On the curve $y^2 = x^3+3u(x+1)^2$, our new proposed addition formula for $(X_1, Y_1, Z_1, Z_1^2) + (X_2, Y_2, Z_2, Z_2^2) = (X_3, Y_3, Z_3, Z_3^2)$ is

$$\begin{aligned}
C_1 &= u,\ A = Z_1^2,\ M = X_1 + C_1 * A,\\
B &= Z_2^2,\ N = X_2 + C_1 * B,\ U_1 = M \cdot B,\ U_2 = N \cdot A,\\
S_1 &= Y_1 \cdot Z_2 \cdot B,\ S_2 = Y_2 \cdot Z_1 \cdot A,\ H = U_2 - U_1,\\
I &= (2H)^2,\ J = H \cdot I,\ R = 2(S_2 - S_1),\ V = U_1 \cdot I,\\
Z_3 &= ((Z_1 + Z_2)^2 - A - B) \cdot H,\ T = Z_3^2,\ W = R^2 - J - 2V,\\
X_3 &= W - C_1 * T,\ Y_3 = R \cdot (V - W) - 2S_1 \cdot J.
\end{aligned}$$

The new formulae cost $11M+4S+3C$. The $3C$ are all multiplications by C_1.

We note that if we use expanded coordinates (X_1, Y_1, Z_1, uZ_1^2), then the cost for the doubling and addition formulae on DIK curves are $1M+8S+2C$ and $11M + 4S + 1C$ respectively.

5.2 Efficient Point Multiplication on general DIK curves

Earlier we introduced the family of elliptic curves

$$E_{a,c} : y^3 = x^3 + a(cx + 1)^2,$$

which we called generalized DIK curves. By Theorem 2, every curve with a rational 3-torsion subgroup can be written in this form. We now give efficient formulas for the group law on these curves.

Doubling and Addition Given $P = (X_1, Y_1, Z_1)$, let $2P = (X_3, Y_3, Z_3)$. Then

$$\begin{aligned}
X_3 &= (3X_1^2 + 2ac^2X_1Z_1^2 + 2acZ_1^4)^2 - 8X_1Y_1^2 - ac^2Z_3^2,\\
Y_3 &= (3X_1^2 + 2ac^2X_1Z_1^2 + 2acZ_1^4)(4X_1Y_1^2 - X_3) - 8Y_1^4,\\
Z_3 &= 2Y_1Z_1.
\end{aligned}$$

Using the same sorts of tricks as in [5, 10], we obtain the following addition formula. Let $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$, and $P + Q = (X_3, Y_3, Z_3)$. Then

$$\begin{aligned}
X_3 &= (Y_2Z_1^3 - Y_1Z_2^3)^2 - (X_2Z_1^2 - X_1Z_2^2)^2(X_1Z_2^2 + X_2Z_1^2 + ac^2Z_1^2Z_2^2),\\
Y_3 &= (Y_2Z_1^3 - Y_1Z_2^3)(X_1Z_2^2(X_2Z_1^2 - X_1Z_2^2)^2 - X_3) - Y_1Z_2^3(X_2Z_1^2 - X_1Z_2^2)^3,\\
Z_3 &= Z_1Z_2(X_2Z_1^2 - X_1Z_2^2).
\end{aligned}$$

Therefore, we have the following efficient algorithms. Compared to the original DIK curves, our new doubling formula increases the computational cost by only needing 1 more C. Our new tripling requires 2 more C.

Doubling. We give explicit formulae to compute $2(X_1, Y_1, Z_1, Z_1^2) = (X_3, Y_3, Z_3, Z_3^2)$ for $E_{a,c}$.

$$\begin{aligned}
C_1 &= ac^2/3,\ C_2 = 2ac - (1/3)a^2c^4, \\
A &= Z_1^2,\ B = X_1 + C_1 * A,\ D = B^2,\ E = Y_1^2,\ F = E^2, \\
S &= 2((B+E)^2 - D - F),\ M = 3D + C_2 * A^2,\ T = M^2 - 2S, \\
Z_3 &= (Y_1 + Z_1)^2 - A - E,\ R = Z_3^2 \\
X_3 &= T - C_1 * R,\ Y_3 = M \cdot (S - T) - 8F.
\end{aligned}$$

The new formula costs $1M + 8S + 3C$. The $3C$ are multiplications by C_1 and C_2.

Addition The following formulae, given $P = (X_1, Y_1, Z_1, Z_1^2)$ and $Q = (X_2, Y_2, Z_2, Z_2^2)$, computes the sum $P + Q = (X_3, Y_3, Z_3, Z_3^2)$ on $E_{a,c}$.

$$\begin{aligned}
C_1 &= ac^2/3,\ A = Z_1^2,\ M = X_1 + C_1 * A, \\
B &= Z_2^2,\ N = X_2 + C_1 * B,\ U_1 = M \cdot B,\ U_2 = N \cdot A, \\
S_1 &= Y_1 \cdot Z_2 \cdot B,\ S_2 = Y_2 \cdot Z_1 \cdot A,\ H = U_2 - U_1, \\
I &= (2H)^2,\ J = H \cdot I,\ R = 2(S_2 - S_1),\ V = U_1 \cdot I, \\
Z_3 &= ((Z_1 + Z_2)^2 - A - B) \cdot H,\ T = Z_3^2,\ W = R^2 - J - 2V, \\
X_3 &= W - C_1 * T,\ Y_3 = R \cdot (V - W) - 2S_1 \cdot J.
\end{aligned}$$

The new formulae cost $11M + 4S + 3C$. The $3C$ are all multiplications by C_1.

Mixed-Addition Let $P = (X_1, Y_1, Z_1, Z_1^2)$, $Q = (X_2, Y_2, 1, 1^2)$, $P + Q = (X_3, Y_3, Z_3, Z_3^2)$. Then the operations for mixed-addition can be organized as follows:

$$\begin{aligned}
M &= Z_1^2,\ A = X_2 M,\ R = Z_1 M,\ B = Y_2 \cdot R, \\
D &= A - X_1,\ E = 2(B - Y_1),\ G = D^2,\ H = 4D \cdot G, \\
V &= 4X_1 \cdot G,\ Z_3 = (Z_1 + D)^2 - M - G,\ F = Z_3^2 \\
X_3 &= E^2 - H - ac^2 * F - 2V,\ Y_3 = E \cdot (V - X_3) - 2Y_1 \cdot H.
\end{aligned}$$

The formulae cost $4S + 7M + C$. The C is a multiplication by ac^2.

5.3 Tripling on the curve $E_{a,c}$

In this subsection, we show the tripling formula on $E_{a,c}$. We again use Jacobian coordinates, let $P = (X_1, Y_1, Z_1)$ and $3P = (X_3, Y_3, Z_3)$. By a long and straightforward calculation, it can be checked that

$$X_3 = U^2 + V,\ Y_3 = U(X_3 - 4V),\ Z_3 = X_1 Z_1 W,$$

where

$$\begin{aligned} U &= Y_1\left(Y_1^2 - ac^2X_1^2Z1^2 - 6acX_1Z_1^4 - 9aZ_1^6\right), \\ V &= -aX_1^2Z_1^2\ \ \frac{4ac^3-27}{3}X_1^2Z_1^2 - c(Y_1^2 + \frac{ac^2}{3}X_1^2Z_1^2 + 2acX_1Z_1^4 + 3aZ_1^6)\ \ ^2, \\ W &= 3Y_1^2 + aZ_1^2(c^2X_1^2 + 6cX_1Z_1^2 + 9Z_1^4). \end{aligned}$$

Now we have the following algorithm

$$\begin{aligned} A &= Z_1^2,\ B = (a/3) * A,\ D = 3A,\ E = X_1 \cdot Z_1,\ F = E^2,\ G = (c * X_1 + D)^2, \\ M &= B \cdot G,\ U = Y_1 \cdot (Y_1^2 - 3M),\ J = Y_1^2 + M, \\ V &= -a * F \cdot (\tfrac{4ac^3-27}{3} * F - c \cdot J)^2, \\ X_3 &= U^2 + V,\ Y_3 = U(X_3 - 4V),\ Z_3 = 3EJ. \end{aligned}$$

The cost is $6S + 6M + 5C$. The $5C$ are multiplications by $a/3$, a, c, and $\frac{4ac^3-27}{3}$. If $c = 0$, then one could also compute $H = ac^2 * F$, and $V = -H \cdot (\frac{4}{3}H - (9/c) * F - J)^2$. The cost is then $6S + 6M + 4C$, saving one multiplication by a constant.

5.4 Elliptic curves with j=0

Let E be an elliptic curve over finite field $\mathbb{F}_q$ with j-invariant $j = 0$. Then we can write E as $y^2 = x^3 + a$ for some $a \in \mathbb{F}_q^*$. Note this is the generalized DIK curve $E_{a,0}$. Elliptic curves with $j = 0$ are used in elliptic curve cryptography. For example, the Barreto-Naehrig (BN) curve has $j = 0$ [2]. When using Jacobian coordinates, the previous records for the lowest costs of addition, doubling, and tripling are $11M + 5S$, $2M + 5S$ and $5M + 10S$, respectively [3]. Here, we present new formulae for addition and tripling using extended Jacobian coordinates (X, Y, Z, Z^2).

Addition The following formulae, given $P = (X_1, Y_1, Z_1, Z_1^2)$ and $Q = (X_2, Y_2, Z_2, Z_2^2)$, computes the sum $P + Q = (X_3, Y_3, Z_3, Z_3^2)$.

$$\begin{aligned} A &= Z_1^2,\ B = Z_2^2,\ U_1 = X_1 \cdot B,\ U_2 = X_2 \cdot A,\ H = U_2 - U_1, \\ S_1 &= Y_1 \cdot Z_2 \cdot B,\ S_2 = Y_2 \cdot Z_1 \cdot A, \\ F &= (2H)^2,\ J = H \cdot F,\ R = 2(S_2 - S_1),\ V = U_1 \cdot F, \\ Z_3 &= ((Z_1 + Z_2)^2 - A - B) \cdot H,\ T = Z_3^2, \\ X_3 &= R^2 - J - 2V,\ Y_3 = R \cdot (V - X_3) - 2S_1 \cdot J. \end{aligned}$$

The new formula costs $11M + 4S$.

Tripling The following formulae, given $P = (X_1, Y_1, Z_1, Z_1^2)$ computes $3P = (X_3, Y_3, Z_3, Z_3^2)$.

$$\begin{aligned} A &= Z_1^2,\ B = a * A,\ D = 3A,\ E = X_1 \cdot Z_1,\ F = E^2,\ G = D^2 \\ M &= B \cdot G,\ U = Y_1 \cdot (Y_1^2 - M),\ J = 3Y_1^2 + M,\ V = -a * F \cdot (9F)^2, \\ X_3 &= U^2 + V,\ Y_3 = U(X_3 - 4V),\ Z_3 = EJ. \end{aligned}$$

The cost is $6M + 6S + 2C$. The $2C$ are multiplications by a.

6 Conclusion

In this paper, we proved various results for three families of elliptic curves: Hessian curves, twisted Hessian curves, and generalized DIK curves. These families all have properties relating to when the 3-torsion subgroup is rational. When $q \equiv 2 \bmod 3$, we saw these families are the same family, while when $q \equiv 1 \bmod 3$, then they are distinct. In particular, we looked at the number of isogeny classes of these families, as well as the number of isomorphism classes (for generalized DIK curves). It would be interesting to find formulas for the number of isogeny classes of other families, or to extend the known results for the various models to characteristic 2 and 3. We still do not know how to explain some of the data we observed for supersingular curves in section 4.2. Finally, we examined performing efficient arithmetic on these curves, and found some faster formulas in various cases. It is possible the formulas we gave can be further improved on, leading to lower operation counts.

We would like to thank the anonymous reviewers for their comments. Their suggestions greatly improved the paper, particularly section 4.2.

References

[1] O. Ahmadi, R. Granger. On isogeny classes of Edwards curves over finite fields, available at `http://eprint.iacr.org/2011/135.pdf`.

[2] P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order, in: Selected Areas in Cryptography SAC 2005, Lecture Notes in Computer Science 3897, pp. 319–331, Springer-Verlag, 2005.

[3] D. J. Bernstein, and T. Lange. Explicit-formulae database, available at `http://www.hyperelliptic.org/EFD`.

[4] D. J. Bernstein and T. Lange. Faster Addition and Doubling on Elliptic Curves, in: Asiacrypt 2007, Lecture Notes in Computer Science 4833, pp. 29–50, Springer-Verlag, 2007.

[5] D. J. Bernstein and T. Lange. Analysis and optimization of elliptic-curve single-scalar multiplication, available at `http://eprint.iacr.org/2007/455.pdf`.

[6] D. J. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters. Twisted Edwards curves, in: Africacrypt 2008, Lecture Notes in Computer Science 5023, pp. 389–405, Springer-Verlag, 2008.

[7] W. Castryck, F. Vercauteren. Toric forms of elliptic curves and their arithmetic, Journal of Symbolic Computation 46 (7), pp. 943–966, 2011.

[8] Y. Choie, E. Jeong. Isomorphism classes of elliptic and hyperelliptic curves over finite fields, Finite Fields and Their Applications, **10** 4, pp. 583–614, 2004.

[9] D. Chudnovsky, and G. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests, Advances in Applied Mathematics 7, pp. 385–434, 1986.

[10] C. Doche, T. Icart and D.R. Kohel. Efficient Scalar Multiplication by Isogeny Decompositions, in: International Conference on Practice and Theory in Public Key Cryptography – PKC 2006, Lecture Notes in Computer Science 3958, pp. 191–206, Springer-Verlag, 2006.

[11] H. Edwards. A normal form for elliptic curves, Bulletin of the American Mathematical Society **44** , pp. 393–422, 2007.

[12] R. Farashahi. On the number of distinct Legendre, Jacobi and Hessian curves, in: Workshop on coding and cryptography–WCC 2011, pp. 37–46, 2011.

[13] R. Farashahi, M. Joye. Efficient Arithmetic on Hessian Curves, in: International Conference on Practice and Theory in Public Key Cryptography – PKC 2010, Lecture Notes in Computer Science 6056, pp.243–260, Springer-Verlag, 2010.

[14] R. Farashahi, D. Moody, H. Wu. Isomorphism classes of Edwards and twisted Edwards curves over finite fields, available at `http://eprint.iacr.org/2011/206.pdf`.

[15] R. Farashahi, I. Shparlinski. On the number of distinct elliptic curves in some families, Des. Codes Cryptography, **54**(1), pp. 83–99, 2010.

[16] R. Feng, and H. Wu. Elliptic Curves in Huff's model, available at `http://eprint.iacr.org/2010/390.pdf`.

[17] R. Feng, and H. Wu. On the isomorphism classes of Legendre elliptic curves over finite fields, available at `http://eprint.iacr.org/2010/390.pdf`.

[18] O. Hess. Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln. Journal für die reine und angewandte Mathematik 10, pp. 68–96, 1844.

[19] M. Joye and J.-J. Quisquater. Hessian elliptic curves and side-channel attacks, in: Workshop on Cryptographic Hardware and Embedded Systems–CHES 2001, Lecture Notes in Computer Science 2162, pp. 402–410, Springer, 2001.

[20] Nicholas M. Katz. 2, 3, 5, Legendre: $\pm$ trace ratios in families of elliptic curves, Experiment. Math., 19 (3), pp. 267–277, 2010.

[21] P. Montgomery. Speeding up the Pollard and elliptic curve methods of factorization, Mathematics of Computation 48, pp. 243–264, 1987.

[22] S. Schmitt, H. G. Zimmer. Elliptic Curves: A Computational Approach, de Gruyter, 2003.

[23] J. H. Silverman. The arithmetic of elliptic curves, Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[24] N. P. Smart. The Hessian form of an elliptic curve, in: Workshop on Cryptographic Hardware and Embedded Systems–CHES 2001, Lecture Notes in Computer Science 2162, pp. 118–125, Springer, 2001.

[25] J. Tate. Endomorphisms of abelian varieties over finite fields, Invent. Math. 2, pp. 134–144, 1966.

[26] L. Washington. Elliptic curves: Number theory and cryptography, Chapman & Hall/CRC, Boca Raton, FL, 2003.

[27] W.C. Waterhouse. Abelian varieties over finite fields, Ann. sci. ÉEcole Norm. sup. (4) 2, pp. 521–560, 1969.