Twisted Hessian curves

Daniel J. Bernstein[1,2], Chitchanok Chuengsatiansup[1], David Kohel[3], and Tanja Lange[1]

[1] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
c.chuengsatiansup@tue.nl, tanja@hyperelliptic.org
[2] Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045, USA
djb@cr.yp.to
[3] Institut de Mathématiques de Marseille
Aix-Marseille Université
163, avenue de Luminy, Case 907
13288 Marseille CEDEX 09, France
David.Kohel@univ-amu.fr

Abstract. This paper presents new speed records for arithmetic on a large family of elliptic curves with cofactor 3: specifically, 8.77**M** per bit for 256-bit variable-base single-scalar multiplication when curve parameters are chosen properly. This is faster than the best results known for cofactor 1, showing for the first time that points of order 3 are useful for performance and narrowing the gap to the speeds of curves with cofactor 4.

Keywords: efficiency, elliptic-curve arithmetic, double-base chains, fast arithmetic, Hessian curves, complete addition laws

1 Introduction

> *For efficiency reasons, it is desirable to take the cofactor to be as small as possible.* — "Recommended elliptic curves for federal government use", National Institute of Standards and Technology, 1999 [47]

All of NIST's standard prime-field elliptic curves have cofactor 1. However, by now there is overwhelming evidence that cofactor 1 does not provide the best

This work was supported by the U.S. National Science Foundation under grants 0716498 and 1018836; by the Agence Nationale de la Recherche grant ANR-12-BS01-0010-01; by the Netherlands Organisation for Scientific Research (NWO) under grants 639.073.005 and 613.001.011; and by the European Commission under Contract ICT-645421 ECRYPT-CSA. This work was started during the ESF exploratory workshop "Curves, Coding Theory, and Cryptography" in March 2009; the first and fourth author would like to thank the ESF for financial support. Permanent ID of this document: 1ad9e9d82a9e27e390be46e1fe7b895f. Date: 2015.08.04.

performance/security tradeoff for elliptic-curve cryptography. All of the latest speed records for ECC are set by curves with cofactor divisible by 2, with base fields $\mathbf{F}_q$ where q is a square, and with extra endomorphisms: Faz-Hernández–Longa–Sánchez [27] use a twisted Edwards GLS curve with cofactor 8 over $\mathbf{F}_q$ where $q = (2^{127} - 5997)^2$; Oliveira–López–Aranha–Rodríguez-Henríquez [49] use a GLV+GLS curve with cofactor 2 over $\mathbf{F}_q$ where $q = 2^{254}$; and Costello–Hisil–Smith [20] use a Montgomery $\mathbf{Q}$-curve with cofactor 4 (and twist cofactor 8) over $\mathbf{F}_q$ where $q = (2^{127} - 1)^2$. Similarly, for "conservative" ECC over prime fields without extra endomorphisms, Bernstein [5] uses a Montgomery curve with cofactor 8 (and twist cofactor 4), and Bernstein–Duif–Lange–Schwabe–Yang [7] use an equivalent twisted Edwards curve.

The very fast Montgomery ladder for Montgomery curves [42] was published at the dawn of ECC, and its speed always relied on a cofactor divisible by 4. However, for many years the benefit of such cofactors seemed limited to ladders for variable-base single-scalar multiplication. Cofactor 1 seemed slightly faster than cofactor 4 for signature generation and signature verification; NIST's curves were published in the context of a signature standard. Many years of investigations of addition formulas for a wide range of curve shapes (see, e.g., [17], [19], [34], [41], and [13]) failed to produce stronger arguments for cofactors above 1 — until the advent [24] and performance analysis [9] of Edwards curves.

Cofactor 3. Several papers have tried to exploit a different cofactor, namely 3, as follows. Hessian curves $x^3 + y^3 + 1 = dxy$, which always have points of order 3 over finite fields, have a very simple and symmetric addition law due to Sylvester. Chudnovsky–Chudnovsky in [17] already observed that this law requires just $12\mathbf{M}$ in projective coordinates. However, Hessian doublings were much slower than Jacobian-coordinate Weierstrass doublings, and this slowdown outweighed the addition speedup, since (in most applications) doublings are much more frequent than additions. The best way to handle a curve with cofactor 3 was to forget about the points of order 3 and simply use the same formulas used for curves with cofactor 1.

What we show in this paper, for the first time, is how to use cofactor 3 to beat the best available results for cofactor 1. We do not claim to have beaten cofactor 4, but we have significantly narrowed the gap.

We now review previous speeds and compare them to our speeds. We adopt the following rules to maximize comparability:

- For individual elliptic-curve operations we count multiplications and squarings. $\mathbf{M}$ is the cost of a multiplication, and $\mathbf{S}$ is the cost of a squaring. We do not count additions or subtractions. (Computer-verified operation counts for our formulas, including counts of additions and subtractions, appear in the latest update of EFD [8].)
- In summaries of scalar-multiplication performance we take $\mathbf{S} = 0.8\mathbf{M}$. Of course, squarings are much faster than multiplications in characteristic 2, but we emphasize the case of large characteristic.

- We also count multiplications by curve parameters: e.g., $\mathbf{M}_d$ is the cost of multiplying by d. We assume that curves are sensibly chosen with small d. In summaries we take $\mathbf{M}_d = 0$.
- We do not include the cost of final conversion to affine coordinates. We also assume that inversion is not fast enough to make intermediate inversions useful. Consequently the exact cost of inversion does not appear.
- We focus on the traditional case of variable-base single-scalar multiplication, in particular for average 256-bit scalars. Beware that this is only loosely correlated with other scalar-multiplication tasks. (Other tasks tend to rely more on additions, so the fast complete addition law for twisted Hessian curves should provide an even larger benefit compared to Weierstrass curves.)

Bernstein–Lange in [10] analyzed scalar-multiplication performance on several curve shapes and concluded, under these assumptions, that Weierstrass curves $y^2 = x^3 - 3x + a_6$ in Jacobian coordinates used $9.34\mathbf{M}$ per bit on average, and that Hessian curves were slower. Bernstein–Birkner–Lange–Peters in [6] used double-base chains (doublings, triplings, and additions) to considerably speed up Hessian curves to $9.65\mathbf{M}$ per bit and to slightly speed up Weierstrass curves to $9.29\mathbf{M}$ per bit. Hisil in [32, Table 6.4], without double-base chains, reported more than $10\mathbf{M}$ per bit for Hessian curves.

Our new results are just $8.77\mathbf{M}$ per bit. This means that one actually gains something by taking advantage of a point of order 3. The new speeds require a base field with $6 \neq 0$ and with fast multiplication by a primitive cube root of 1, such as a field of the form $\mathbf{F}_p[\omega]/(\omega^2 + \omega + 1)$ where $p \in 2 + 3\mathbf{Z}$. This quadratic field structure might seem to constrain the applicability of the results, but (1) GLS-curve and $\mathbf{Q}$-curve results already show that a quadratic field structure is desirable for performance; (2) there is also a fast primitive cube root of 1 in, e.g., the prime field $\mathbf{F}_p$ where $7p = 2^{298} + 2^{149} + 1$; (3) we do not lose much speed from more general fields (the cost of a tripling increases by $0.4\mathbf{M}$). Note that the $8.77\mathbf{M}$ per bit does not use the speedups in (1). Our speedups can be combined with the speedups in (1) but we have not quantified the resulting performance.

Completeness, side channels, and precomputation. For a large fraction of curves, the formulas we use have a further benefit not reflected in the multiplication counts stated above: namely, the formulas are *complete*. This means that the formulas work for all curve points. The implementor does not have to waste any time checking for exceptional cases, and does not have to worry that an attacker can generate inputs that trigger exceptional cases: there are no exceptional cases. (For comparison, a *strongly unified* but incomplete addition law works for most additions and works for most doublings, but still has exceptional cases. The traditional addition law for Weierstrass curves is not even strongly unified: it consistently fails for doublings.)

Often completeness is used as part of a side-channel defense; see, e.g., [9, Section 8]. In this paper we focus purely on speed: we do not limit attention to scalar-multiplication techniques that are safe inside applications that expose secret scalars to side-channel attacks. Note that scalars are public in many crypto-

graphic protocols, such as signature verification, and also in many other elliptic-curve computations, such as the elliptic-curve method of integer factorization.

We also allow scalar-multiplication techniques that rely on scalar-dependent precomputation. This is reasonable for applications that reuse a single scalar many times. For example, in the context of signatures, the *signer* can carry out the precomputation and compress the results into the signature. The signer can also choose different techniques for different scalars: in particular, there are some scalars where our cofactor-3 techniques are even faster than cofactor 4. One can easily find, and we suggest choosing, curves of cofactor 12 that simultaneously allow the current cofactor-3 and cofactor-4 methods; these curves are also likely to be able to take advantage of any future improvements in cofactor-3 and cofactor-4 methods.

Tools and techniques. At a high level, we use a tree search for double-base chains, allowing windows and taking account of the costs of doublings, triplings, and additions. At a lower level, we use tripling formulas that take $6\mathbf{M} + 6\mathbf{S}$, doubling formulas that take $6\mathbf{M} + 2\mathbf{S}$, and addition formulas that take $11\mathbf{M}$; in this overview we ignore multiplications by constants. These formulas work in projective coordinates for Hessian curves.

Completeness relies on two further tools. First, we use a rotated addition law. Unlike the standard (Sylvester) addition law, the rotated addition law is strongly unified. In fact, the rotated addition law works in every case where the standard addition law fails; i.e., the two laws together form a complete system of addition laws. Second, we work more generally with twisted Hessian curves $ax^3 + y^3 + 1 = dxy$. If a is not a cube then the rotated addition law by itself is complete. The doubling formulas and tripling formulas are also complete, meaning that they have no exceptional cases. The generalization also provides more flexibility in finding curves with small parameters.

For comparison, Jacobian coordinates for Weierstrass curves $y^2 = x^3 - 3x + a_6$ use $7\mathbf{M} + 7\mathbf{S}$ for tripling, $3\mathbf{M} + 5\mathbf{S}$ for doubling, and $11\mathbf{M} + 5\mathbf{S}$ for addition. This saves $3(\mathbf{M} - \mathbf{S})$ in doubling but loses $\mathbf{M} + \mathbf{S}$ in tripling and loses $5\mathbf{S}$ in addition. Given these operation counts it is not a surprise that we beat Weierstrass curves.

$6\mathbf{M} + 6\mathbf{S}$ triplings were achieved once before, namely by tripling-oriented Doche–Icart–Kohel curves [22]. Those curves also offer $2\mathbf{M} + 7\mathbf{S}$ doublings, competitive with our $6\mathbf{M} + 2\mathbf{S}$. However, the best addition formulas known for those curves take $11\mathbf{M} + 6\mathbf{S}$, even slower than Weierstrass curves.

As noted earlier, Edwards curves are still faster for average scalars, thanks to their particularly fast doublings and additions. However, we do beat Edwards curves for scalars that involve many triplings.

Credits and priority dates. Hessian curves and the standard addition law are classical material. The rotated addition law, the fact that the rotated addition law is strongly unified, the concept of twisted Hessian curves, the generalization of the addition laws to twisted Hessian curves, the complete system of addition laws, and the completeness of the rotated addition law for non-cube a are all due to this paper. We announced the essential details online in July 2009 (e.g., stating

Operation	T	S	2	3	>	Cost	Source
doubling			✓	✓	✓	$6\mathbf{M}+3\mathbf{S} \approx 8.4\mathbf{M}$	1986 Chudnovsky–Chudnovsky [17]
doubling	✓		✓	✓	✓	$6\mathbf{M}+3\mathbf{S} \approx 8.4\mathbf{M}$	our 2009 announcement
doubling				✓	✓	$3\mathbf{M}+6\mathbf{S} \approx 7.8\mathbf{M}$	2007 Hisil–Carter–Dawson [30]
doubling			✓	✓	✓	$7\mathbf{M}+1\mathbf{S} \approx 7.8\mathbf{M}$	2007 Hisil–Carter–Dawson [30]
doubling	✓			✓	✓	$6\mathbf{M}+2\mathbf{S} \approx 7.6\mathbf{M}$	this paper
addition		✓		✓	✓	$9\mathbf{M}+6\mathbf{S} \approx 13.8\mathbf{M}$	2009 Hisil–Wong–Carter–Dawson [31]
addition			✓	✓	✓	$12\mathbf{M} = 12.0\mathbf{M}$	1986 Chudnovsky–Chudnovsky [17]
addition	✓	✓	✓	✓	✓	$12\mathbf{M} = 12.0\mathbf{M}$	our 2009 announcement
addition	✓	✓		✓	✓	$11\mathbf{M} = 11.0\mathbf{M}$	2010 Hisil [32]
tripling				✓	✓	$8\mathbf{M}+6\mathbf{S} \approx 12.8\mathbf{M}$	2007 Hisil–Carter–Dawson [30]
tripling	✓			✓	✓	$8\mathbf{M}+6\mathbf{S} \approx 12.8\mathbf{M}$	our 2009 announcement
tripling	✓		✓			$7\mathbf{M}+6\mathbf{S} \approx 11.8\mathbf{M}$	2010 Farashahi–Joye [25]
tripling	✓			✓		$8\mathbf{M}+4\mathbf{S} \approx 11.2\mathbf{M}$	2013 Farashahi–Wu–Zhao [26]
tripling	✓			✓	✓	$8\mathbf{M}+4\mathbf{S} \approx 11.2\mathbf{M}$	2015 Kohel [39]
tripling	✓		✓	✓	✓	$8\mathbf{M}+4\mathbf{S} \approx 11.2\mathbf{M}$	this paper
tripling	✓		✓		✓	$6\mathbf{M}+6\mathbf{S} \approx 10.8\mathbf{M}$	this paper, assuming fast primitive $\sqrt[3]{1}$

Table 1.1. Costs of various formulas for Hessian curves in projective coordinates. Costs are sorted using the assumption $\mathbf{S} \approx 0.8\mathbf{M}$; note that $\mathbf{S}/\mathbf{M}$ is normally much smaller in characteristic 2. "T" means that the formula was stated for twisted Hessian curves, not just Hessian curves; all of the "T" formulas are complete for suitable curves. "S" means "strongly unified": an addition formula that also works for doubling. "2" means that the formula works in characteristic 2. "3" means that the formula works in characteristic 3. ">" means that the formula works in characteristic above 3.

the completeness result in [4, page 40], and contributing a "twisted Hessian" section to EFD), but this paper is our first formal publication of these results.

The speeds that we announced at that time for twisted Hessian curves were no better than known speeds for standard formulas for Hessian curves: $8\mathbf{M}+6\mathbf{S}$ for tripling, $6\mathbf{M}+3\mathbf{S}$ for doubling, and $12\mathbf{M}$ for addition. Followup work found better formulas for all of these operations. Almost all of those formulas are superseded by formulas that we now announce; the only exception is that we use $11\mathbf{M}$ addition formulas [32] from Hisil. See Table 1.1 for an overview.

Tripling: One of the followup papers [25], by Farashahi–Joye, reported $7\mathbf{M}+6\mathbf{S}$ for twisted Hessian tripling, but only for characteristic 2. Another followup paper [26], by Farashahi–Wu–Zhao, reported 4 multiplications and 4 cubings, overall $8\mathbf{M}+4\mathbf{S}$, for Hessian tripling, but only for characteristic 3. Further followup work [39], by Kohel, reported 4 multiplications and 4 cubings for twisted Hessian tripling in any odd characteristic. In Section 6 we generalize the approach of [39] and show how a better specialization reduces cost to just 6 cubings, assuming that the field has a fast primitive cube root of 1.

Doubling: In Section 6 we present four doubling formulas, starting with $6\mathbf{M}+3\mathbf{S}$ and culminating with $6\mathbf{M}+2\mathbf{S}$. In the case $a=1$, the first formula was already well known before our work. Hisil, Carter and Dawson in [30] had already

introduced doubling formulas using $3\mathbf{M}+6\mathbf{S}$, and also introduced doubling formulas using $7\mathbf{M}+1\mathbf{S}$, using techniques that seem to be specific to small cube a such as $a=1$; see also [32]. Our $6\mathbf{M}+2\mathbf{S}$ is better than $7\mathbf{M}+1\mathbf{S}$ if $\mathbf{S}<\mathbf{M}$, and is better than $3\mathbf{M}+6\mathbf{S}$ if $\mathbf{S}>0.75\mathbf{M}$.

At a higher level, double-base chains have been explored in several papers. The idea of a tree search for double-base chains was introduced by Doche and Habsieger in [21]. The tree search in [21] tries to minimize the number of additions used in a double-base chain, ignoring the cost of doublings and triplings; we do better by using the cost of doublings and triplings to adjust the weights of nodes in the tree.

2 Twisted Hessian curves

Definition 2.0. *Let k be a field. A* **projective twisted Hessian curve over** *k is a curve of the form $aX^3+Y^3+Z^3=dXYZ$ in $\mathbf{P}^2$ with specified point $(0:-1:1)$, where a,d are elements of k with $a(27a-d^3)\neq 0$.*

Theorem 2.1 below states that any projective twisted Hessian curve is an elliptic curve. The correponding affine curve $ax^3+y^3+1=dxy$ with specified point $(0,-1)$ is an **affine twisted Hessian curve**.

We state theorems for the projective curve, and allow the reader to deduce corresponding theorems for the affine curve. When we say "Let H be the twisted Hessian curve $aX^3+Y^3+Z^3=dXYZ$ over k" we mean that a,d are elements of k, that $a(27a-d^3)\neq 0$, and that H is the projective twisted Hessian curve $aX^3+Y^3+Z^3=dXYZ$ in $\mathbf{P}^2$ with specified point $(0:-1:1)$. Some theorems need, and state, further assumptions such as $d\neq 0$.

The special case $a=1$ of a twisted Hessian curve is simply a **Hessian curve**. The twisted Hessian curve $aX^3+Y^3+Z^3=dXYZ$ is isomorphic to the Hessian curve $\bar{X}^3+Y^3+Z^3=(d/a^{1/3})\bar{X}YZ$ over any extension of k containing a cube root $a^{1/3}$ of a: simply take $\bar{X}=a^{1/3}X$. Similarly, taking $\bar{X}=dX$ when $d\neq 0$ shows that the twisted Hessian curve for (a,d) is isomorphic to the twisted Hessian curve for $(a/d^3,1)$; but we retain a and d as separate parameters to allow more curves with small parameters and thus with fast arithmetic.

Hessian curves have a long history, but twisted Hessian curves do not. The importance of twisted Hessian curves, beyond their extra generality, is that they have a complete addition law when a is not a cube. See Theorem 4.5 below.

Proof strategy: twisted Hessian curves as foundations. One can use the first isomorphism stated above to derive many features of twisted Hessian curves from corresponding well-known features of Hessian curves. We instead give direct proofs in the general case, meant as replacements for the older proofs in the special case: in other words, we propose starting with the theory of twisted Hessian curves rather than starting with the theory of Hessian curves. This reduces the total proof length: the extra cost of tracking a through the proofs is smaller than the extra cost of applying the isomorphism.

We do not claim that this tracking involves any particular difficulty. In one case the tracking has been done before: specifically, some of the nonsingularity computations in Theorem 2.1 are special cases of classical discriminant computations for ternary cubics $aX^3 + bY^3 + cZ^3 = dXYZ$. See, e.g., [2] and [16]. However, the classical computations were carried out in characteristic 0, and the range of validity of the computations is not always obvious. Many of the computations fail in characteristic 3, even though Theorem 2.1 is valid in characteristic 3. Since the complete proofs are straightforward we simply include them here.

Similarly, one can derive many features of twisted Hessian curves from corresponding well-known features of Weierstrass curves, but we instead give direct proofs. We do use Weierstrass curves inside Theorem 5.2, which proves a property of all elliptic curves having points of order 3.

Notes on definitions: Hessian curves. There are various superficial differences among the definitions of Hessian curves in the literature. First, often characteristic 3 is prohibited. For example, [50] considers only base fields $\mathbf{F}_q$ with $q \in 2 + 3\mathbf{Z}$, and [34] considers only characteristics larger than 3. Our main interest is in the case $q \in 1 + 3\mathbf{Z}$, and in any event we see no reason to restrict the characteristic in the definition.

Second, often constants are introduced into the parameter d. For example, [34] defines a Hessian curve as $X^3 + Y^3 + Z^3 = 3dXYZ$, and the curve actually considered by Hesse in [29, page 90, formula 54] was $X^3+Y^3+Z^3+6dXYZ = 0$.

Third, the specified point is often taken as a point at infinity, specifically $(-1 : 1 : 0)$; see, e.g., [17]. We use an affine point $(0 : -1 : 1)$ to allow completeness of the *affine* twisted Hessian curve rather than merely completeness of the *projective* twisted Hessian curve; if a is not a cube then there are no points at infinity for implementors to worry about. Converting addition laws (and twists and so on) between these two choices of neutral element is a trivial matter of permuting X, Y, Z.

Notes on definitions: elliptic curves. There are also various differences among the definitions of elliptic curves in the literature.

The most specific definitions would say that Hessian curves are not elliptic curves: for example, Koblitz in [36, page 117] defines elliptic curves to have long Weierstrass form. Obviously we do not use such restrictive definitions.

Two classical definitions that allow Hessian curves are as follows: (1) an elliptic curve is a nonsingular cubic curve in $\mathbf{P}^2$ with a specified point; (2) an elliptic curve is a nonsingular cubic curve in $\mathbf{P}^2$ with a specified *inflection* point. The importance of the inflection-point condition is that it allows the traditional geometric addition law: three distinct curve points on a line have sum 0; more generally, all curve points on a line, counted with multiplicity, have sum 0. If the specified point were not an inflection point then the addition law would be more complicated. See, e.g., [33, Chapter 3, Theorem 1.2].

We take the first of these two definitions. The statement that any twisted Hessian curve H is elliptic (Theorem 2.1) thus means that H is a nonsingular cubic curve with a specified point. We prove separately (Theorem 2.2) that the specified point $(0 : -1 : 1)$ is an inflection point.

These definitions are still not broad enough to allow, e.g., Edwards curves as elliptic curves. Edwards curves in $\mathbf{P}^2$ are singular and not cubic; the Arène–Lange–Naehrig–Ritzenthaler geometric addition law [1] for Edwards curves is not the traditional geometric addition law; etc. "Elliptic curve" is often defined more broadly as "smooth projective genus-1 curve with a specified point", but this leaves ambiguous whether a "projective curve" is a curve for which there *exists* an embedding into projective space or a curve *equipped with* an embedding into projective space. With the first notion, the concept of addition laws for a curve is ill-defined, as is any other concept that relies on choices of coordinates. The second notion does not admit, e.g., Edwards curves in $\mathbf{P}^1 \times \mathbf{P}^1$ as elliptic curves; it does allow Edwards curves in $\mathbf{P}^3$, but the switch from $\mathbf{P}^1 \times \mathbf{P}^1$ to $\mathbf{P}^3$ damages the performance of doublings, so this definition is not broad enough for a serious analysis of performance. We avoid further discussion of ways to define elliptic curves in more generality: all of our theorems are focused on twisted Hessian curves, and then the classical definitions suffice.

Theorem 2.1. *Let H be the twisted Hessian curve $aX^3 + Y^3 + Z^3 = dXYZ$ over a field k. Then H is an elliptic curve.*

Proof. $aX^3 + Y^3 + Z^3 = dXYZ$ is a cubic curve in $\mathbf{P}^2$, and $(0 : -1 : 1)$ is a point on the curve. What remains is to prove that this curve is nonsingular.

Recall that $a(27a - d^3) \neq 0$ by definition of twisted Hessian curves.

A singularity $(X : Y : Z) \in \mathbf{P}^2$ of $aX^3 + Y^3 + Z^3 = dXYZ$ satisfies $3aX^2 = dYZ$, $3Y^2 = dXZ$, and $3Z^2 = dXY$. We will deduce $X = Y = Z = 0$, contradicting $(X : Y : Z) \in \mathbf{P}^2$.

Case 1: $3 \neq 0$ in k. Multiply to obtain $27aX^2Y^2Z^2 = d^3X^2Y^2Z^2$, i.e., $(27a - d^3)X^2Y^2Z^2 = 0$. By hypothesis $27a - d^3 \neq 0$, so $X^2Y^2Z^2 = 0$, so $X = 0$ or $Y = 0$ or $Z = 0$.

Case 1.1: $X = 0$. Then $3Y^2 = 0$ and $3Z^2 = 0$ so $Y = 0$ and $Z = 0$ as claimed.

Case 1.2: $Y = 0$. Then $3aX^2 = 0$ and $3Z^2 = 0$, and $a \neq 0$ by hypothesis, so $X = 0$ and $Z = 0$ as claimed.

Case 1.3: $Z = 0$. Then $3aX^2 = 0$ and $3Y^2 = 0$, and again $a \neq 0$, so $X = 0$ and $Y = 0$ as claimed.

Case 2: $3 = 0$ in k. Then $dYZ = 0$ and $dXZ = 0$ and $dXY = 0$. By hypothesis $a(-d^3) \neq 0$, so $d \neq 0$, so at least two of the coordinates X, Y, Z are 0.

Case 2.1: $X = Y = 0$. Then the curve equation $aX^3 + Y^3 + Z^3 = dXYZ$ forces $Z^3 = 0$ so $Z = 0$ as claimed.

Case 2.2: $X = Z = 0$. Then the curve equation forces $Y^3 = 0$ so $Y = 0$ as claimed.

Case 2.3: $Y = Z = 0$. Then the curve equation forces $aX^3 = 0$, and $a \neq 0$ by hypothesis, so $X = 0$ as claimed. □

Theorem 2.2. *Let H be the twisted Hessian curve $aX^3 + Y^3 + Z^3 = dXYZ$ over a field k. Then $(0 : -1 : 1)$ is an inflection point on H.*

Proof. We claim that $(0 : -1 : 1)$ is the only point of intersection of the line $-3(Y + Z) = dX$ with the curve $aX^3 + Y^3 + Z^3 = dXYZ$ over any extension of

k. Consequently, by Bézout's theorem, this point has intersection multiplicity 3. (An alternative proof, involving essentially the same calculation, computes the multiplicity directly from its definition.)

To prove the claim, assume that $-3(Y+Z) = dX$ and $aX^3+Y^3+Z^3 = dXYZ$. Then $(27a-d^3)X^3 = 27aX^3-(-3(Y+Z))^3 = 27(aX^3+(Y+Z)^3) = 27(aX^3+Y^3+Z^3+3(Y+Z)YZ) = 27(dXYZ-dXYZ) = 0$ so $X^3 = 0$ so $X = 0$. Now $Y+Z = 0$: this follows from $-3(Y+Z) = dX = 0$ if $3 \neq 0$ in k, and it follows from $Y^3+Z^3 = 0$ if $3 = 0$ in k. Thus $(X:Y:Z) = (0:-1:1)$. □

3 The standard addition law

Theorem 3.2 states an addition law for twisted Hessian curves. We originally derived this addition law as follows:

- Start from Sylvester's addition law for $X^3+Y^3+Z^3 = dXYZ$. See, e.g., [17, page 425, equation 4.21i].
- Observe, as noted in [17], that the addition law is independent of d.
- Conclude that the addition law also works for $X^3+Y^3+Z^3 = (d/c)XYZ$, where c is a cube root of a.
- Permute X, Y, Z to our choice of neutral element.
- Replace X with cX.
- Rescale the outputs X_3, Y_3, Z_3 by a factor c.

The resulting polynomials X_3, Y_3, Z_3 are identical to Sylvester's addition law: they are independent of curve parameters, and in particular are independent of a. We refer to this addition law as the **standard addition law**. For reasons explained in Section 2, we prove Theorem 3.2 here by giving a direct proof of the standard addition law for the general case, rather than deriving the general case from the special case $a = 1$.

The standard addition law is never complete: it fails whenever $(X_2:Y_2:Z_2) = (X_1:Y_1:Z_1)$. More generally, it fails if and only if $(X_2:Y_2:Z_2)-(X_1:Y_1:Z_1)$ has the form $(0:-\omega:1)$ where $\omega^3 = 1$, or equivalently $(X_2:Y_2:Z_2) = (\omega^2X_1:\omega Y_1:Z_1)$. See Theorem 4.6 for the equivalence, and Theorem 3.3 for the failure analysis.

A different way to analyze the failure cases, with somewhat less calculation, is as follows. First prove that $(X_2:Y_2:Z_2)$ has the form $(0:-\omega:1)$ if and only if the addition law fails to add the neutral element $(0:-1:1)$ to $(X_2:Y_2:Z_2)$. Then use a theorem of Bosma and Lenstra [14, Theorem 2] stating that the set of failure cases of a degree-$(2,2)$ addition law for a cubic elliptic curve in $\mathbf{P}^2$ is a union of shifted diagonals $\Delta_S = \{(P_1, P_1+S)\}$. The theorems in [14] are stated only for Weierstrass curves, but they are invariant under linear equivalence and thus also apply to twisted Hessian curves. See [38] for a generalization to elliptic curves embedded in projective space of any dimension.

Theorems 4.2 and 4.5 below introduce a new addition law that (1) works for all doublings on any twisted Hessian curve and (2) is complete for any twisted Hessian curve with non-cube a.

Theorem 3.1. *Let H be the twisted Hessian curve $aX^3 + Y^3 + Z^3 = dXYZ$ over a field k. Let X_1, Y_1, Z_1 be elements of k such that $(X_1 : Y_1 : Z_1) \in H(k)$. Then $-(X_1 : Y_1 : Z_1) = (X_1 : Z_1 : Y_1)$.*

Proof. Recall that the specified neutral element of the curve is $(0 : -1 : 1)$.

Case 1: $(X_1 : Y_1 : Z_1) \neq (X_1 : Z_1 : Y_1)$. Then $X_1(Y + Z) = X(Y_1 + Z_1)$ is a line in $\mathbf{P}^2$: if all its coefficients $-Y_1 - Z_1, X_1, X_1$ are 0 then $(X_1 : Y_1 : Z_1) = (0 : -1 : 1) = (X_1 : Z_1 : Y_1)$, contradiction. This line intersects the curve at the distinct points $(0 : -1 : 1)$, $(X_1 : Y_1 : Z_1)$, and $(X_1 : Z_1 : Y_1)$. Hence $-(X_1 : Y_1 : Z_1) = (X_1 : Z_1 : Y_1)$.

Case 2: $(X_1 : Y_1 : Z_1) = (X_1 : Z_1 : Y_1)$ and $X_1 \neq 0$. Again $(X_1 : Y_1 : Z_1) \neq (0 : -1 : 1)$, and again $X_1(Y + Z) = X(Y_1 + Z_1)$ is a line. This line intersects the curve at both $(0 : -1 : 1)$ and $(X_1 : Y_1 : Z_1)$, and we show in a moment that it is the tangent to the curve at $(X_1 : Y_1 : Z_1)$. Hence $-(X_1 : Y_1 : Z_1) = (X_1 : Y_1 : Z_1) = (X_1 : Z_1 : Y_1)$.

For the tangent calculation we take coordinates $y = Y/X$ and $z = Z/X$. The curve is then $a + y^3 + z^3 = dyz$; the point P_1 is $(y_1, z_1) = (Y_1/X_1, Z_1/X_1)$, which by hypothesis satisfies $y_1 = z_1$; and the line is $y + z = y_1 + z_1$. The curve is symmetric between y and z, so its slope at $(y_1, z_1) = (z_1, y_1)$ must be -1, which is the same as the slope of the line.

Case 3: $(X_1 : Y_1 : Z_1) = (X_1 : Z_1 : Y_1)$ and $X_1 = 0$. Then $Y_1^3 + Z_1^3 = 0$ by the curve equation so $Y_1 = \lambda Z_1$ for some λ with $\lambda^3 = -1$; but $(Y_1 : Z_1) = (Z_1 : Y_1)$ implies $\lambda = 1/\lambda$, so $\lambda = -1$, so $(X_1 : Y_1 : Z_1) = (0 : -1 : 1)$. Hence $-(X_1 : Y_1 : Z_1) = (0 : -1 : 1) = (0 : 1 : -1) = (X_1 : Z_1 : Y_1)$. □

Theorem 3.2. *Let H be the twisted Hessian curve $aX^3 + Y^3 + Z^3 = dXYZ$ over a field k. Let $X_1, Y_1, Z_1, X_2, Y_2, Z_2$ be elements of k such that $(X_1 : Y_1 : Z_1), (X_2 : Y_2 : Z_2) \in H(k)$. Define*

$$\begin{aligned} X_3 &= X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1, \\ Y_3 &= Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1, \\ Z_3 &= Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1. \end{aligned}$$

If $(X_3, Y_3, Z_3) \neq (0, 0, 0)$ then $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$.

Proof. The polynomial identity

$$\begin{aligned} &aX_3^3 + Y_3^3 + Z_3^3 - dX_3Y_3Z_3 \\ &= (X_1^3Y_2^3Z_2^3 + Y_1^3X_2^3Z_2^3 + Z_1^3X_2^3Y_2^3 - 3X_1Y_1Z_1X_2^2Y_2^2Z_2^2)(aX_1^3 + Y_1^3 + Z_1^3 - dX_1Y_1Z_1) \\ &- (X_2^3Y_1^3Z_1^3 + Y_2^3X_1^3Z_1^3 + Z_2^3X_1^3Y_1^3 - 3X_2Y_2Z_2X_1^2Y_1^2Z_1^2)(aX_2^3 + Y_2^3 + Z_2^3 - dX_2Y_2Z_2) \end{aligned}$$

implies that $(X_3 : Y_3 : Z_3) \in H(k)$. The rest of the proof uses the chord-and-tangent definition of addition to show that $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$.

If $(X_1 : Y_1 : Z_1) = (X_2 : Y_2 : Z_2)$ then $(X_3, Y_3, Z_3) = (0, 0, 0)$, contradiction. Assume from now on that $(X_1 : Y_1 : Z_1) \neq (X_2 : Y_2 : Z_2)$.

The line through $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ is $(Z_1Y_2 - Z_2Y_1)X + (X_1Z_2 - X_2Z_1)Y + (X_2Y_1 - X_1Y_2)Z = 0$. The polynomial identity

$$(Z_1Y_2 - Z_2Y_1)X_3 + (X_1Z_2 - X_2Z_1)Z_3 + (X_2Y_1 - X_1Y_2)Y_3 = 0$$

shows that $(X_3 : Z_3 : Y_3)$ is also on this line.

One would now like to conclude that $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = -(X_3 : Z_3 : Y_3)$, so $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$ by Theorem 3.1. The only difficulty is that $(X_3 : Z_3 : Y_3)$ might be the same as $(X_1 : Y_1 : Z_1)$ or $(X_2 : Y_2 : Z_2)$; the rest of the proof consists of verifying that, in these two cases, the line is the tangent to the curve at $(X_3 : Z_3 : Y_3)$.

We use two other easy polynomial identities. First, $X_1Y_2Y_3 + Y_1Z_2X_3 + Z_1X_2Z_3 = 0$. Second, $aX_1X_2X_3 + Z_1Z_2Y_3 + Y_1Y_2Z_3 = (aX_1^3 + Y_1^3 + Z_1^3)X_2Y_2Z_2 - (aX_2^3 + Y_2^3 + Z_2^3)X_1Y_1Z_1$. The curve equations for $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ then imply $aX_1X_2X_3 + Z_1Z_2Y_3 + Y_1Y_2Z_3 = 0$.

Case 1: $(X_3 : Z_3 : Y_3) = (X_1 : Y_1 : Z_1)$. The two identities above then imply $X_1Y_2Z_1 + Y_1Z_2X_1 + Z_1X_2Y_1 = 0$ and $aX_1^2X_2 + Z_1^2Z_2 + Y_1^2Y_2 = 0$ respectively. Our line is $(Z_1Y_2 - Z_2Y_1)X + (X_1Z_2 - X_2Z_1)Y + (X_2Y_1 - X_1Y_2)Z = 0$, while the tangent to the curve at $(X_1 : Y_1 : Z_1)$ is $(3aX_1^2 - dY_1Z_1)X + (3Y_1^2 - dX_1Z_1)Y + (3Z_1^2 - dX_1Y_1)Z = 0$. To see that these lines are the same, observe that the cross product

$$\begin{pmatrix} (3Y_1^2 - dX_1Z_1)(X_2Y_1 - X_1Y_2) - (3Z_1^2 - dX_1Y_1)(X_1Z_2 - X_2Z_1) \\ (3Z_1^2 - dX_1Y_1)(Z_1Y_2 - Z_2Y_1) - (3aX_1^2 - dY_1Z_1)(X_2Y_1 - X_1Y_2) \\ (3aX_1^2 - dY_1Z_1)(X_1Z_2 - X_2Z_1) - (3Y_1^2 - dX_1Z_1)(Z_1Y_2 - Z_2Y_1) \end{pmatrix}$$

is exactly

$$\begin{pmatrix} 3X_2 & -3X_1 & dX_1 \\ 3Y_2 & -3Y_1 & dY_1 \\ 3Z_2 & -3Z_1 & dZ_1 \end{pmatrix} \begin{pmatrix} aX_1^3 + Y_1^3 + Z_1^3 - dX_1Y_1Z_1 \\ aX_1^2X_2 + Z_1^2Z_2 + Y_1^2Y_2 \\ X_1Y_2Z_1 + Y_1Z_2X_1 + Z_1X_2Y_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Case 2: $(X_3 : Z_3 : Y_3) = (X_2 : Y_2 : Z_2)$. Exchanging $(X_1 : Y_1 : Z_1)$ with $(X_2 : Y_2 : Z_2)$ replaces (X_3, Y_3, Z_3) with $(-X_3, -Y_3, -Z_3)$ and moves to case 1. □

Theorem 3.3. *In the situation of Theorem 3.2,* $(X_3, Y_3, Z_3) = (0, 0, 0)$ *if and only if* $(X_2 : Y_2 : Z_2) = (\omega^2X_1 : \omega Y_1 : Z_1)$ *for some* $\omega \in k$ *with* $\omega^3 = 1$.

Proof. If $(X_2 : Y_2 : Z_2) = (\omega^2X_1 : \omega Y_1 : Z_1)$ and $\omega^3 = 1$ then (X_3, Y_3, Z_3) is proportional to $(X_1^2\omega Y_1Z_1 - \omega^4X_1^2Y_1Z_1, Z_1^2\omega^2X_1\omega Y_1 - Z_1^2X_1Y_1, Y_1^2\omega^2X_1Z_1 - \omega^2Y_1^2X_1Z_1) = (0, 0, 0)$.

Conversely, assume that $(X_3, Y_3, Z_3) = (0, 0, 0)$. Then $X_1^2Y_2Z_2 = X_2^2Y_1Z_1$, $Z_1^2X_2Y_2 = Z_2^2X_1Y_1$, and $Y_1^2X_2Z_2 = Y_2^2X_1Z_1$.

If $X_1 = 0$ then $Y_1^3 + Z_1^3 = 0$ by the curve equation, so $Y_1 \neq 0$ and $Z_1 \neq 0$. Write $\lambda_1 = Y_1/Z_1$; then $(X_1 : Y_1 : Z_1) = (0 : \lambda_1 : 1)$ and $\lambda_1^3 = -1$. Furthermore $X_2^2Y_1Z_1 = 0$ so $X_2 = 0$ so $(X_2 : Y_2 : Z_2) = (0 : \lambda_2 : 1)$ where $\lambda_2^3 = -1$. Define

$\omega = \lambda_2/\lambda_1$; then $\omega^3 = \lambda_2^3/\lambda_1^3 = 1$ and $(X_2 : Y_2 : Z_2) = (0 : \lambda_2 : 1) = (0 : \omega\lambda_1 : 1) = (\omega^2 X_1 : \omega Y_1 : Z_1)$.

If $X_2 = 0$ then similarly $X_1 = 0$. Assume from now on that $X_1 \neq 0$ and $X_2 \neq 0$. Write $y_1 = Y_1/X_1$, $z_1 = Z_1/X_1$, $y_2 = Y_2/X_2$, and $z_2 = Z_2/X_2$. Rewrite the three equations $X_3 = 0$, $Y_3 = 0$, and $Z_3 = 0$ as $y_2 z_2 = y_1 z_1$, $z_1^2 y_2 = z_2^2 y_1$, and $y_1^2 z_2 = y_2^2 z_1$. The first two equations imply $z_1^3 y_1 = z_1^2 y_2 z_2 = z_2^3 y_1$, so $(z_1^3 - z_2^3) y_1 = 0$; the first and third equations imply $y_1^3 z_1 = y_1^2 y_2 z_2 = y_2^3 z_1$, so $(y_1^3 - y_2^3) z_1 = 0$.

If $y_1 = 0$ then $z_1^2 y_2 = 0$ by the second equation. The curve equation $a + y_1^3 + z_1^3 = d y_1 z_1$ forces $a + z_1^3 = 0$ so $z_1 \neq 0$; hence $y_2 = 0$. The curve equation $a + y_2^3 + z_2^3 = d y_2 z_2$ similarly forces $a + z_2^3 = 0$ so $z_2^3 = z_1^3$. Write $\omega = z_2/z_1$; then $\omega^3 = 1$ and $(X_2 : Y_2 : Z_2) = (1 : y_2 : z_2) = (1 : 0 : z_2) = (1 : 0 : \omega z_1) = (\omega^2 : \omega y_1 : z_1) = (\omega^2 X_1 : \omega Y_1 : Z_1)$.

If $z_1 = 0$ then similar logic applies. Assume from now on that $y_1 \neq 0$ and $z_1 \neq 0$. Then $z_1^3 = z_2^3$ and $y_1^3 = y_2^3$. Write $\omega = y_1/y_2$; then $\omega^3 = 1$. The equation $X_3 = 0$ forces $\omega = z_2/z_1$. Hence $(X_2 : Y_2 : Z_2) = (1 : y_2 : z_2) = (1 : \omega^{-1} y_1 : \omega z_1) = (\omega^2 X_1 : \omega Y_1 : Z_1)$. □

4 The rotated addition law

Theorem 4.2 states a new addition law for twisted Hessian curves. This addition law is obtained as follows:

- Subtract $(1 : -c : 0)$ from one input, using Theorem 4.1, where c is a cube root of a.
- Use the standard addition law in Theorem 3.2.
- Add $(1 : -c : 0)$ to the output, using Theorem 4.1 again.

The formulas in Theorem 4.1 are linear, so the resulting addition law has the same bidegree as the standard addition law. This is an example of what Bernstein and Lange in [11, Section 8] call **rotation** of an addition law.

This rotated addition law is new, even in the case $a = 1$. Unlike the standard addition law, the rotated addition law works for doublings. Specializing the rotated addition law to doublings, and further to $a = 1$, produces exactly the Joye–Quisquater doubling formula from [34, Proposition 2]. Even better, the rotated addition law is complete when a is not a cube; see Theorem 4.5 below.

Theorem 4.7 states that the standard addition law and the rotated addition law form a complete system of addition laws for any twisted Hessian curve: any pair of input points can be added by at least one of the two laws. This system is vastly simpler than the Bosma–Lenstra complete system [14] of addition laws for Weierstrass curves, and arguably even simpler than the Bernstein–Lange complete system [11] of addition laws for twisted Edwards curves: each output coordinate here is a difference of just two degree-$(2,2)$ monomials, as in [11], but here there are just three output coordinates while in [11] there were four.

One can easily rotate the addition law again (or, equivalently, exchange the two inputs) to obtain a third addition law with the same features as the second

addition law. One can also prove that these three addition laws are a basis for the space of degree-$(2,2)$ addition laws for H: it is easy to see that the laws are linearly independent, and Bosma and Lenstra showed in [14, Section 4] that the whole space has dimension 3.

Theorem 4.1. *Let H be the twisted Hessian curve $aX^3 + Y^3 + Z^3 = dXYZ$ over a field k. Assume that $c \in k$ satisfies $c^3 = a$. Then $(1 : -c : 0) \in H(k)$. Furthermore, if X_1, Y_1, Z_1 are elements of k such that $(X_1 : Y_1 : Z_1) \in H(k)$, then $(X_1 : Y_1 : Z_1) + (1 : -c : 0) = (Y_1 : cZ_1 : c^2X_1)$.*

Proof. First $a(1)^3 + (-c)^3 + (0)^3 = 0$ so $(1 : -c : 0) \in H(k)$.

Case 1: $Z_1 \neq 0$. Write $(X_2, Y_2, Z_2) = (1, -c, 0)$, and define (X_3, Y_3, Z_3) as in Theorem 3.2. Then $X_3 = -Y_1Z_1$, $Y_3 = -cZ_1^2$, and $Z_3 = -c^2X_1Z_1$, so $(X_3 : Y_3 : Z_3) = (Y_1 : cZ_1 : c^2X_1)$, so $(X_1 : Y_1 : Z_1) + (1 : -c : 0) = (Y_1 : cZ_1 : c^2X_1)$ by Theorem 3.2.

Case 2: $Z_1 = 0$. (Note that Theorem 3.2 is not useful in this case, since it defines $(X_3, Y_3, Z_3) = (0, 0, 0)$.) Then $aX_1^3 + Y_1^3 = 0$ by the curve equation, so $X_1 \neq 0$ and $Y_1 \neq 0$. Write $\omega = Y_1/(-cX_1)$; then $\omega^3 = Y_1^3/(-aX_1^3) = 1$, and $(X_1 : Y_1 : Z_1) = (1 : -\omega c : 0)$.

Case 2.1: $\omega \neq 1$. The line $Z = 0$ intersects the curve at the three distinct points $(1 : -c : 0)$, $(1 : -\omega c : 0)$, and $(1 : -\omega^{-1}c : 0)$, so $(1 : -c : 0) + (1 : -\omega c : 0) = -(1 : -\omega^{-1}c : 0) = (1 : 0 : -\omega^{-1}c) = (-\omega c : 0 : c^2) = (Y_1 : cZ_1 : c^2X_1)$ by Theorem 3.1.

Case 2.2: $\omega = 1$, i.e., $(X_1 : Y_1 : Z_1) = (1 : -c : 0)$. The line $3c^2X + 3cY + dZ = 0$ intersects the curve at $(1 : -c : 0)$. We will see in a moment that it has no other intersection points. Consequently $3(1 : -c : 0) = 0$; i.e., $(X_1 : Y_1 : Z_1) + (1 : -c : 0) = 2(1 : -c : 0) = -(1 : -c : 0) = (1 : 0 : -c) = (-c : 0 : c^2) = (Y_1 : cZ_1 : c^2X_1)$ by Theorem 3.1.

We finish by showing that the only intersection is $(1 : -c : 0)$. Assume that $3c^2X + 3cY + dZ = 0$ and $aX^3 + Y^3 + Z^3 = dXYZ$. Then $-dZ = 3c(cX + Y)$, but also $(cX + Y)^3 = aX^3 + Y^3 + 3c^2X^2Y + 3cXY^2 = -Z^3$, so $-d^3Z^3 = 27a(cX + Y)^3 = -27aZ^3$. By hypothesis $27a \neq d^3$, so $Z^3 = 0$, so $Z = 0$, so $cX + Y = 0$, so $(X : Y : Z) = (1 : -c : 0)$. □

Theorem 4.2. *Let H be the twisted Hessian curve $aX^3 + Y^3 + Z^3 = dXYZ$ over a field k. Let $X_1, Y_1, Z_1, X_2, Y_2, Z_2$ be elements of k such that $(X_1 : Y_1 : Z_1), (X_2 : Y_2 : Z_2) \in H(k)$. Define*

$$\begin{aligned} X_3' &= Z_2^2X_1Z_1 - Y_1^2X_2Y_2, \\ Y_3' &= Y_2^2Y_1Z_1 - aX_1^2X_2Z_2, \\ Z_3' &= aX_2^2X_1Y_1 - Z_1^2Y_2Z_2. \end{aligned}$$

If $(X_3', Y_3', Z_3') \neq (0, 0, 0)$ then $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3' : Y_3' : Z_3')$.

Proof. Fix a field extension K of k containing a cube root c of a. Replace k, X_1, Y_1, Z_1 with K, Z_1, c^2X_1, cY_1 respectively throughout Theorem 3.2. This

replaces X_3, Y_3, Z_3 with $-Z_3', -c^2X_3', -cY_3'$ respectively. Hence $(Z_1 : c^2X_1 : cY_1) + (X_2 : Y_2 : Z_2) = (Z_3' : c^2X_3' : cY_3')$ if $(X_3', Y_3', Z_3') \neq (0,0,0)$.

Now add $(1 : -c : 0)$ to both sides. Theorem 4.1 implies $(1 : -c : 0) + (Z_1 : c^2X_1 : cY_1) = (c^2X_1 : c^2Y_1 : c^2Z_1) = (X_1 : Y_1 : Z_1)$ and similarly $(1 : -c : 0) + (Z_3' : c^2X_3' : cY_3') = (X_3' : Y_3' : Z_3')$. Hence $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3' : Y_3' : Z_3')$ if $(X_3', Y_3', Z_3') \neq (0,0,0)$. □

Theorem 4.3. *In the situation of Theorem 4.2,* $(X_3', Y_3', Z_3') = (0,0,0)$ *if and only if* $(X_2 : Y_2 : Z_2) = (Z_1 : \gamma^2X_1 : \gamma Y_1)$ *for some* $\gamma \in k$ *with* $\gamma^3 = a$.

Proof. Fix a field extension K of k containing a cube root c of a. Replace k, X_1, Y_1, Z_1 with K, Z_1, c^2X_1, cY_1 respectively throughout Theorem 3.2 and Theorem 3.3 to see that $(-Z_3', -c^2X_3', -cY_3') = (0,0,0)$ if and only if $(X_2 : Y_2 : Z_2) = (\omega^2Z_1 : \omega c^2X_1 : cY_1)$ for some $\omega \in K$ with $\omega^3 = 1$.

If $(X_2 : Y_2 : Z_2) = (Z_1 : \gamma^2X_1 : \gamma Y_1)$ for some $\gamma \in k$ with $\gamma^3 = a$ then this condition is satisfied by the ratio $\omega = \gamma/c \in K$ so $(X_3', Y_3', Z_3') = (0,0,0)$.

Conversely, if $(X_3', Y_3', Z_3') = (0,0,0)$ then $(X_2 : Y_2 : Z_2) = (\omega^2Z_1 : \omega c^2X_1 : cY_1)$ for some $\omega \in K$ with $\omega^3 = 1$, so $(X_2 : Y_2 : Z_2) = (Z_1 : \gamma^2X_1 : \gamma Y_1)$ where $\gamma = c\omega$. To see that $\gamma \in k$, note that at least two of X_1, Y_1, Z_1 are nonzero. If X_1, Y_1 are nonzero then Y_2, Z_2 are nonzero and $(\gamma^2X_1)/(\gamma Y_1) = Y_2/Z_2$ so $\gamma = (Y_2/Z_2)(Y_1/X_1) \in k$. If Y_1, Z_1 are nonzero then X_2, Z_2 are nonzero and $(\gamma Y_1)/Z_1 = Z_2/X_2$ so $\gamma = (Z_2/X_2)(Z_1/Y_1) \in k$. If X_1, Z_1 are nonzero then X_2, Y_2 are nonzero and $(\gamma^2X_1)/Z_1 = Y_2/X_2$ so $\gamma^2 = (Y_2/X_2)(Z_1/X_1) \in k$; but also $\gamma^3 = c^3 = a \in k$, so $\gamma = a/\gamma^2 \in k$. □

Theorem 4.4. *In the situation of Theorem 4.2,* $(X_3', Y_3', Z_3') \neq (0,0,0)$ *if* $(X_2 : Y_2 : Z_2) = (X_1 : Y_1 : Z_1)$.

Proof. Suppose $(X_3', Y_3', Z_3') = (0,0,0)$. Then $(X_2, Y_2, Z_2) = (Z_1, \gamma^2X_1, \gamma Y_1)$ for some $\gamma \in k$ with $\gamma^3 = a$ by Theorem 4.3, so $(X_2 : Y_2 : Z_2) + (1 : -\gamma : 0) = (\gamma^2X_1 : \gamma^2Y_1 : \gamma^2Z_1) = (X_1 : Y_1 : Z_1)$ by Theorem 4.1. Subtract $(X_2 : Y_2 : Z_2) = (X_1 : Y_1 : Z_1)$ to obtain $(1 : -\gamma : 0) = (0 : -1 : 1)$, contradiction.

Alternative proof, showing more directly that $Y_3' \neq 0$ or $Z_3' \neq 0$: Write (X_2, Y_2, Z_2) as $(\lambda X_1, \lambda Y_1, \lambda Z_1)$ for some $\lambda \neq 0$. Then $Y_3' = \lambda^2Z_1(Y_1^3 - aX_1^3)$ and $Z_3' = \lambda^2Y_1(aX_1^3 - Z_1^3)$.

Case 1: $Y_1 = 0$. Then $aX_1^3 = -Z_1^3$ by the curve equation, so $Y_3' = -\lambda^2Z_1^4$. If $Y_3' = 0$ then $Z_1 = 0$ so $aX_1^3 = 0$ so $X_1 = 0$ so $(X_1, Y_1, Z_1) = (0,0,0)$, contradiction. Hence $Y_3' \neq 0$.

Case 2: $Z_1 = 0$. Then $aX_1^3 = -Y_1^3$ by the curve equation, so $Z_3' = -\lambda^2Y_1^4$. If $Z_3' = 0$ then $Y_1 = 0$ so $aX_1^3 = 0$ so $X_1 = 0$ so $(X_1, Y_1, Z_1) = (0,0,0)$, contradiction. Hence $Z_3' \neq 0$.

Case 3: $Y_1 \neq 0$ and $Z_1 \neq 0$. If $Y_3' = 0$ and $Z_3' = 0$ then $aX_1^3 = Y_1^3$ and $aX_1^3 = Z_1^3$; in particular $X_1 \neq 0$. so $3aX_1^3 = dX_1Y_1Z_1$ by the curve equation, so $27a^3X_1^9 = dX_1^3Y_1^3Z_1^3 = da^2X_1^9$, so $27a = d^3$, contradiction. Hence $Y_3' \neq 0$ or $Z_3' \neq 0$. □

Theorem 4.5. *In the situation of Theorem 4.2, assume that* a *is not a cube in* k. *Then* $(X_3', Y_3', Z_3') \neq (0,0,0)$ *and* $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3' : Y_3' : Z_3')$.

Proof. By hypothesis no $\gamma \in k$ satisfies $\gamma^3 = a$. By Theorem 4.3, $(X_3', Y_3', Z_3') \neq (0,0,0)$. By Theorem 4.2, $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3' : Y_3' : Z_3')$.

We also give a second, more direct, proof that $Z_3' \neq 0$. The curve equation forces $Z_1 \neq 0$ and $Z_2 \neq 0$. Write $x_1 = X_1/Z_1$, $y_1 = Y_1/Z_1$, $x_2 = X_2/Z_2$, and $y_2 = Y_2/Z_2$. Suppose that $Z_3' = 0$, i.e., $y_2 = ax_1y_1x_2^2$. Eliminate y_2 in the curve equation $ax_2^3+y_2^3+1 = dx_2y_2$ to obtain $ax_2^3+(ax_1y_1x_2^2)^3+1 = dax_1y_1x_2^3$. Use the curve equation at (x_1, y_1) to eliminate d and rewrite $(ax_1y_1x_2^2)^3 = -ax_2^3 - 1 + ax_2^3(ax_1^3+y_1^3+1) = ax_2^3(ax_1^3+y_1^3)-1$ which factors as $(a^2x_1^3x_2^3-1)(ax_2^3y_1^3-1) = 0$, implying that a is a cube in k. □

Theorem 4.6. *Let H be the twisted Hessian curve $aX^3 + Y^3 + Z^3 = dXYZ$ over a field k. Assume that $\omega \in k$ satisfies $\omega^3 = 1$. Then $(0 : -\omega : 1) \in H(k)$. Furthermore, if X_1, Y_1, Z_1 are elements of k such that $(X_1 : Y_1 : Z_1) \in H(k)$, then $(X_1 : Y_1 : Z_1) + (0 : -\omega : 1) = (\omega^2 X_1 : \omega Y_1 : Z_1)$.*

Proof. Take $(X_2, Y_2, Z_2) = (0, -\omega, 1)$ in Theorem 3.2 to obtain $(X_3, Y_3, Z_3) = (-\omega X_1^2, -X_1Y_1, -\omega^2 X_1Z_1)$. If $X_1 \neq 0$ then $(X_3, Y_3, Z_3) \neq (0,0,0)$ and $(X_1 : Y_1 : Z_1) + (0 : -\omega : 1) = (X_3 : Y_3 : Z_3) = (\omega^2 X_1 : \omega Y_1 : Z_1)$.

Also take $(X_2, Y_2, Z_2) = (0, -\omega, 1)$ in Theorem 4.2 to obtain $(X_3', Y_3', Z_3') = (X_1Z_1, \omega^2 Y_1Z_1, \omega Z_1^2)$. If $Z_1 \neq 0$ then $(X_3', Y_3', Z_3') \neq (0,0,0)$ and $(X_1 : Y_1 : Z_1) + (0 : -\omega : 1) = (X_3' : Y_3' : Z_3') = (\omega^2 X_1 : \omega Y_1 : Z_1)$.

At least one of X_1, Z_1 must be nonzero, so at least one of these cases applies. □

Theorem 4.7. *Let H be the twisted Hessian curve $aX^3+Y^3+Z^3 = dXYZ$ over a field k. Let $X_1, Y_1, Z_1, X_2, Y_2, Z_2$ be elements of k such that $(X_1 : Y_1 : Z_1), (X_2 : Y_2 : Z_2) \in H(k)$. Define (X_3, Y_3, Z_3) as in Theorem 3.2, and (X_3', Y_3', Z_3') as in Theorem 4.2. Then $(X_3, Y_3, Z_3) \neq (0,0,0)$ or $(X_3', Y_3', Z_3') \neq (0,0,0)$.*

Proof. Suppose that $(X_3, Y_3, Z_3) = (0,0,0)$ and $(X_3', Y_3', Z_3') = (0,0,0)$. Then $(X_2 : Y_2 : Z_2) = (\omega^2 X_1 : \omega Y_1 : Z_1)$ for some $\omega \in k$ with $\omega^3 = 1$ by Theorem 3.3, so $(X_2 : Y_2 : Z_2) = (X_1 : Y_1 : Z_1) + (0 : -\omega : 1)$ by Theorem 4.6. Furthermore $(X_2 : Y_2 : Z_2) = (Z_1 : \gamma^2 X_1 : \gamma Y_1)$ for some $\gamma \in k$ with $\gamma^3 = a$ by Theorem 4.3, so $(X_2 : Y_2 : Z_2) = (X_1 : Y_1 : Z_1) - (1 : -\gamma : 0)$ by Theorem 4.1. Hence $(0 : -\omega : 1) = -(1 : -\gamma : 0) = (1 : 0 : -\gamma)$, contradiction. □

5 Points of order 3

Each projective twisted Hessian curve over $\mathbf{F}_q$ has a rational point of order 3. See Theorem 5.1. In particular, for $q \in 1+3\mathbf{Z}$, the point $(0 : -\omega : 1)$ is a rational point of order 3, where ω is a primitive cube root of 1 in $\mathbf{F}_q$.

Conversely, if $q \in 1 + 3\mathbf{Z}$, then each elliptic curve over $\mathbf{F}_q$ with a point P_3 of order 3 is isomorphic to a twisted Hessian curve via an isomorphism that takes P_3 to $(0 : -\omega : 1)$. We prove this converse in two steps:

- Over any field, each elliptic curve with a point P_3 of order 3 is isomorphic to a curve of the form $y^2 + dxy + ay = x^3$, where $a(27a - d^3) \neq 0$, via

an isomorphism taking P_3 to $(0,0)$. This is a standard fact; see, e.g., [23, Section 13.1.5.b]. To keep this paper self-contained we include a proof as Theorem 5.2. We refer to $y^2+dxy+ay=x^3$ as a **triangular curve** because its Newton polygon is a triangle of minimum area (equivalently, minimum number of boundary lattice points) among all Newton polygons of Weierstrass curves.

– Over a field with a primitive cube root ω of 1, this triangular curve is isomorphic to the twisted Hessian curve $(d^3-27a)X^3+Y^3+Z^3=3dXYZ$ via an isomorphism that takes $(0,0)$ to $(0:-\omega:1)$. See Theorem 5.3.

Furthermore, over any field, this triangular curve is 3-isogenous to the twisted Hessian curve $aX^3+Y^3+Z^3=dXYZ$, provided that $d\neq 0$. See Theorem 5.4. This gives an alternate proof, for $d\neq 0$, that $aX^3+Y^3+Z^3=dXYZ$ has a point of order 3 over $\mathbf{F}_q$: the triangular curve $y^2+dxy+ay=x^3$ has a point of order 3, namely $(0,0)$, so its group order over $\mathbf{F}_q$ is a multiple of 3; the isogenous twisted Hessian curve $aX^3+Y^3+Z^3=dXYZ$ has the same group order, and therefore also a point of order 3. This isogeny also leads to extremely fast tripling formulas; see Section 6.

For comparison: Over a field where all elements are cubes, such as a field $\mathbf{F}_q$ with $q\in 2+3\mathbf{Z}$, Smart in [50, Section 3] states an isomorphism from the triangular curve to a Hessian curve, taking $(0,0)$ to the point $(-1:0:1)$ of order 3 (modulo permutation of coordinates to put the neutral element at infinity). We instead emphasize the case $q\in 1+3\mathbf{Z}$ since this is the case that allows completeness.

Theorem 5.1. *Let H be the twisted Hessian curve $aX^3+Y^3+Z^3=dXYZ$ over a finite field k. Then $H(k)$ has a point of order 3.*

Proof. Case 1: $\#k\in 1+3\mathbf{Z}$. There is a primitive cube root ω of 1 in k. The point $(0:-\omega:1)$ is in $H(k)$ by Theorem 4.6, is nonzero since $\omega\neq 1$, satisfies $2(0:-\omega:1)=(0:-\omega^2:1)=(0:1:-\omega)$ by Theorem 4.6, and satisfies $-(0:-\omega:1)=(0:1:-\omega)$ by Theorem 3.1, so it is a point of order 3.

Case 2: $\#k\notin 1+3\mathbf{Z}$. There is a cube root c of a in k. The point $(1:-c:0)$ is in $H(k)$ by Theorem 4.1, is visibly nonzero, satisfies $2(1:-c:0)=(-c:0:c^2)=(1:0:-c)$ by Theorem 4.1, and satisfies $-(1:-c:0)=(1:0:-c)$ by Theorem 3.1, so it is a point of order 3. □

Theorem 5.2. *Let E be an elliptic curve over a field k. Assume that $E(k)$ has a point P_3 of order 3. Then there exist a,d,ϕ such that $a,d\in k$; $a(27a-d^3)\neq 0$; ϕ is an isomorphism from E to the triangular curve $y^2+dxy+ay=x^3$; and $\phi(P_3)=(0,0)$.*

Proof. Write E in long Weierstrass form $v^2+e_1uv+e_3v=u^3+e_2u^2+e_4u+e_6$. The point P_3 is not the neutral element so it is affine, say (u_3,v_3).

Substitute $u=x+u_3$ and $v=t+v_3$ to obtain an isomorphic curve C in long Weierstrass form $t^2+c_1xt+c_3t=x^3+c_2x^2+c_4x+c_6$. This isomorphism takes P_3 to the point $(0,0)$. This point has order 3, so the tangent line to C at $(0,0)$

intersects the curve at that point with multiplicity 3, so it does not intersect the point at infinity, so it is not vertical; i.e., it has the form $t = \lambda x$ for some $\lambda \in k$.

Substitute $y = t - \lambda x$ to obtain an isomorphic curve A in long Weierstrass form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. This isomorphism preserves $(0,0)$, and now the line $y = 0$ intersects A at $(0,0)$ with multiplicity 3. Hence $a_2 = a_4 = a_6 = 0$; i.e., the curve is $y^2 + a_1xy + a_3y = x^3$. Write $d = a_1$ and $a = a_3$.

The discriminant of this curve is $a^3(d^3 - 27a)$ so $a \neq 0$ and $27a - d^3 \neq 0$. More explicitly, if $a = 0$ then $(0,0)$ is singular; if $d^3 = 27a$ and $3 = 0$ in k then $(-(a^2/4)^{1/3}, -a/2)$ is singular; if $d^3 = 27a$ and $3 \neq 0$ in k then $(-d^2/9, a)$ is singular. □

Theorem 5.3. *Let a, d be elements of a field k such that $a(27a - d^3) \neq 0$. Let ω be an element of k with $\omega^3 = 1$ and $\omega \neq 1$. Let E be the triangular curve $VW(V + dU + aW) = U^3$. Then there is an isomorphism ϕ from E to the twisted Hessian curve $(d^3 - 27a)X^3 + Y^3 + Z^3 = 3dXYZ$, defined by $\phi(U : V : W) = (X : Y : Z)$ where $X = U$, $Y = \omega(V + dU + aW) - \omega^2V - aW$, $Z = \omega^2(V + dU + aW) - \omega V - aW$. Furthermore $\phi(0 : 0 : 1) = (0 : -\omega : 1)$.*

Proof. Note that $3 \neq 0$ in k: otherwise $(\omega - 1)^3 = \omega^3 - 1 = 0$ so $\omega - 1 = 0$, contradiction.

Write H for the curve $a'X^3+Y^3+Z^3 = d'XYZ$, where $a' = d^3-27a$ and $d' = 3d$. Then $a'(27a'-(d')^3) = (d^3-27a)(27(d^3-27a)-27d^3) = 27^2a(27a-d^3) \neq 0$, so H is a twisted Hessian curve over k.

The identity $a'X^3 + Y^3 + Z^3 - d'XYZ = 27a(VW(V + dU + aW) - U^3)$ in the ring $\mathbf{Z}[a, d, U, V, W, \omega]/(\omega^2 + \omega + 1)$ shows that ϕ maps E to H.

The map ϕ is invertible on $\mathbf{P}^2$: specifically, $\phi^{-1}(X : Y : Z) = (U : V : W)$ where $U = X$, $V = -(dX + \omega Y + \omega^2 Z)/3$, and $W = -(dX + Y + Z)/(3a)$. The same identity shows that ϕ^{-1} maps H to E.

Hence ϕ is an isomorphism of curves from H to E. To see that it is an isomorphism of elliptic curves, observe that it maps the neutral element of E to the neutral element of H: specifically, $\phi(0 : 1 : 0) = (0 : \omega - \omega^2 : \omega^2 - \omega) = (0 : -1 : 1)$.

Finally $\phi(0 : 0 : 1) = (0 : \omega a - a : \omega^2 a - a) = (0 : \omega - 1 : \omega^2 - 1) = (0 : -\omega : 1)$. □

Theorem 5.4. *Let H be the twisted Hessian curve $aX^3+Y^3+Z^3 = dXYZ$ over a field k. Assume that $d \neq 0$. Let E be the triangular curve $VW(V+dU+aW) = U^3$. Then there is an isogeny ι from H to E defined by $\iota(X : Y : Z) = (-XYZ : Y^3 : X^3)$; there is an isogeny ι' from E to H defined by*

$$\iota'(U : V : W) = \left(\frac{R^3+S^3+V^3-3RSV}{d} : RS^2+SV^2+VR^2-3RSV : RV^2+SR^2+VS^2-3RSV \right)$$

where $Q = dU$, $R = aW$, and $S = -(V + Q + R)$; and $\iota'(\iota(P)) = 3P$ for each point P on H.

Proof. If $U = -XYZ$, $V = Y^3$, and $W = X^3$ then $VW(V + dU + aW) - U^3 = X^3Y^3(aX^3 + Y^3 + Z^3 - dXYZ)$. Hence ι is a rational map from H to E. The neutral element $(0 : -1 : 1)$ of H maps to the neutral element $(0 : 1 : 0)$ of E, so ι is an isogeny from H to E. Note that ι is defined everywhere on H: each point $(X : Y : Z)$ on H has $X \neq 0$ or $Y \neq 0$, so $(-XYZ, Y^3, X^3) \neq (0, 0, 0)$.

If $Q = dU$, $R = aW$, $S = -(V + Q + R)$, $X = (R^3 + S^3 + V^3 - 3RSV)/d$, $Y = RS^2 + SV^2 + VR^2 - 3RSV$, and $Z = RV^2 + SR^2 + VS^2 - 3RSV$ then the following identities hold:

$$\begin{aligned}
&aX^3 + Y^3 + Z^3 - dXYZ \\
&\quad = a(Q^2 + 3QR + 3R^2 + 3QV + 3VR + 3V^2)^3(VW(V + dU + aW) - U^3); \\
&a(R + S + V)^3 - d^3RSV = ad^3(VW(V + dU + aW) - U^3); \\
&dX + 3Y + 3Z = (R + S + V)^3 - 27RSV.
\end{aligned}$$

The first identity implies that ι' is a rational map from E to H. The neutral element $(0 : 1 : 0)$ of E maps to the neutral element $(0 : -1 : 1)$ of H, so ι' is an isogeny from E to H. The remaining identities imply that ι' is defined everywhere on E. Indeed, if $(X, Y, Z) = (0, 0, 0)$ then $a(R+S+V)^3 - d^3RSV = 0$ and $(R+S+V)^3 - 27RSV = dX + 3Y + 3Z = 0$ so $(d^3 - 27a)RSV = 0$, implying $R = 0$ or $S = 0$ or $V = 0$. If $R = 0$ then $0 = Y = SV^2$ so $S = 0$ or $V = 0$; if $S = 0$ then $0 = Y = VR^2$ so $V = 0$ or $R = 0$; if $V = 0$ then $0 = Y = RS^2$ so $R = 0$ or $S = 0$. In all cases at least two of R, S, V are 0, but also $R+S+V = 0$, so all three are 0. This implies $W = 0$, $Q = 0$, and $U = 0$, contradicting $(U : V : W) \in \mathbf{P}^2$.

What remains is to prove that $\iota' \circ \iota$ is tripling on H. Take a point $(X_1 : Y_1 : Z_1)$ on H. Define $(X_2, Y_2, Z_2) = ((Z_1^3 - Y_1^3)X_1, (Y_1^3 - aX_1^3)Z_1, (aX_1^3 - Z_1^3)Y_1)$; then $(X_2 : Y_2 : Z_2) = 2(X_1 : Y_1 : Z_1)$ by Theorem 4.2 and Theorem 4.3. Define (X_3, Y_3, Z_3) and (X_3', Y_3', Z_3') as in Theorem 3.2 and Theorem 4.2 respectively. Define $(U, V, W) = (-X_1Y_1Z_1, Y_1^3, X_1^3)$; then $(U : V : W) = \iota(X_1 : Y_1 : Z_1)$. Define $Q = dU$, $R = aW$, $S = -(V + Q + R)$, $X = (R^3 + S^3 + V^3 - 3RSV)/d$, $Y = RS^2 + SV^2 + VR^2 - 3RSV$, and $Z = RV^2 + SR^2 + VS^2 - 3RSV$; then $\iota'(\iota(X_1 : Y_1 : Z_1)) = (X : Y : Z)$. Write C for the polynomial $aX_1^3 + Y_1^3 + Z_1^3 - dX_1Y_1Z_1$.

Case 1: $X_1 \neq 0$. The identities

$$\begin{aligned}
X_3 &= X_1(-X + C(2aX_1^3 + 2Y_1^3 - Z_1^3 - dX_1Y_1Z_1)X_1Y_1Z_1), \\
Y_3 &= X_1(-Y + C(a^2X_1^6 - adX_1^4Y_1Z_1 - aX_1^3Z_1^3 + 4aX_1^3Y_1^3 - Y_1^6)), \\
Z_3 &= X_1(-Z + C(-a^2X_1^6 - dX_1Y_1^4Z_1 - Y_1^3Z_1^3 + 4aX_1^3Y_1^3 + Y_1^6))
\end{aligned}$$

show that $(X_3 : Y_3 : Z_3) = (X : Y : Z)$. In particular, $(X_3, Y_3, Z_3) \neq (0, 0, 0)$, so $3(X_1 : Y_1 : Z_1) = (X_3 : Y_3 : Z_3)$ by Theorem 3.2, so $3(X_1 : Y_1 : Z_1) = (X : Y : Z)$.

Case 2: $Y_1 \neq 0$. The identities

$$\begin{aligned}
X_3' &= Y_1(X - C(2aX_1^3 + 2Y_1^3 - Z_1^3 - dX_1Y_1Z_1)X_1Y_1Z_1), \\
Y_3' &= Y_1(Y - C(a^2X_1^6 - adX_1^4Y_1Z_1 - aX_1^3Z_1^3 + 4aX_1^3Y_1^3 - Y_1^6)), \\
Z_3' &= Y_1(Z - C(-a^2X_1^6 - dX_1Y_1^4Z_1 - Y_1^3Z_1^3 + 4aX_1^3Y_1^3 + Y_1^6))
\end{aligned}$$

show that $(X_3' : Y_3' : Z_3') = (X : Y : Z)$. In particular, $(X_3', Y_3', Z_3') \neq (0, 0, 0)$, so $3(X_1 : Y_1 : Z_1) = (X_3' : Y_3' : Z_3')$ by Theorem 4.2, so $3(X_1 : Y_1 : Z_1) = (X : Y : Z)$.

At least one of X_1 and Y_1 must be nonzero, so at least one of these cases applies. □

6 Cost of additions, doublings, and triplings

This section analyzes the cost of various formulas for arithmetic on twisted Hessian curves. Input and output points are assumed to be represented in projective coordinates $(X : Y : Z)$.

All of the formulas in this section are complete when a is not a cube. In particular, the addition formulas use the rotated addition law (Theorem 4.2) rather than the standard addition law (Theorem 3.2). Switching back to the standard addition law is a straightforward rotation exercise and saves $1\mathbf{M}_a$ in addition, at the expense of completeness. If incomplete formulas are acceptable then one can achieve the same savings in the rotated addition law by taking $a = 1$, although this would force somewhat larger constants in doublings and triplings.

Addition. The following formulas compute addition $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ in $12\mathbf{M} + 1\mathbf{M}_a$.

$$A = X_1 \cdot Z_2;\ B = Z_1 \cdot Z_2;\ C = Y_1 \cdot X_2;\ D = Y_1 \cdot Y_2;\ E = Z_1 \cdot Y_2;$$
$$F = aX_1 \cdot X_2;\ X_3 = A \cdot B - C \cdot D;\ Y_3 = D \cdot E - F \cdot A;\ Z_3 = F \cdot C - B \cdot E.$$

Mixed addition, computing $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : 1)$, takes only $10\mathbf{M}+1\mathbf{M}_a$: eliminate the two multiplications by Z_2 in the above formulas.

In followup work, Hisil has saved $1\mathbf{M}$ as follows, achieving $11\mathbf{M} + 1\mathbf{M}_a$ for addition (and $9\mathbf{M} + 1\mathbf{M}_a$ for mixed addition), assuming $2 \neq 0$ in the field:

$$A = X_1 \cdot Z_2;\ B = Z_1 \cdot Z_2;\ C = Y_1 \cdot X_2;\ D = Y_1 \cdot Y_2;\ E = Z_1 \cdot Y_2;$$
$$F = aX_1 \cdot X_2;\ G = (D + B) \cdot (A - C);\ H = (D - B) \cdot (A + C);$$
$$J = (D + F) \cdot (A - E);\ K = (D - F) \cdot (A + E);$$
$$X_3 = G - H;\ Y_3 = K - J;\ Z_3 = J + K - G - H - 2(B - F) \cdot (C + E).$$

Theorem 4.5 shows that all of these formulas are complete if a is not a cube. In particular, these formulas can be used to compute doublings. This is one way to reduce side-channel leakage in twisted Hessian coordinates. However, faster doublings are feasible as we show below.

Doubling. Each of the following formulas is a complete doubling formula, i.e., correctly doubles all curve points, whether or not a is a cube. To see this, substitute $(X_2, Y_2, Z_2) = (X_1, Y_1, Z_1)$ in Theorem 4.2, and observe that the resulting vector (X_3', Y_3', Z_3') is, up to sign (and scaling by a power of 2 for the formulas labeled as requiring $2 \neq 0$), the same as the vector (X_3, Y_3, Z_3) computed here. Recall that Theorem 4.2 is always usable for doublings by Theorem 4.4.

The first doubling formulas use $6\mathbf{M} + 3\mathbf{S} + 1\mathbf{M}_a$. Note that the formulas compute the squares of all input values as a step towards cubing them. They are not used individually, so the formulas would benefit from dedicated cubings.

$$A = X_1^2;\ B = Y_1^2;\ C = Z_1^2;\ D = A \cdot X_1;\ E = B \cdot Y_1;\ F = C \cdot Z_1;\ G = aD;$$
$$X_3 = X_1 \cdot (E - F);\ Y_3 = Z_1 \cdot (G - E);\ Z_3 = Y_1 \cdot (F - G).$$

The second doubling formulas require $2 \neq 0$ in the field and require the field to contain an element i with $i^2 = -1$. These formulas use $8\mathbf{M} + 1\mathbf{M}_i + 1\mathbf{M}_d$.

$$J = iZ_1;\ A = (Y_1 - J) \cdot (Y_1 + J);\ P = Y_1 \cdot Z_1;$$
$$C = (A - P) \cdot (Y_1 + Z_1);\ D = (A + P) \cdot (Z_1 - Y_1);\ E = 3C - 2dX_1 \cdot P;$$
$$X_3 = -2X_1 \cdot D;\ Y_3 = (D - E) \cdot Z_1;\ Z_3 = (D + E) \cdot Y_1.$$

The third doubling formulas eliminate the multiplication by i, further improve cost to $7\mathbf{M} + 1\mathbf{S} + 1\mathbf{M}_d$, and eliminate the requirement for the field to contain i, although they still require $2 \neq 0$ in the field.

$$P = Y_1 \cdot Z_1;\ Q = 2P;\ R = Y_1 + Z_1;$$
$$A = R^2 - P;\ C = (A - Q) \cdot R;\ D = A \cdot (Z_1 - Y_1);\ E = 3C - dX_1 \cdot Q;$$
$$X_3 = -2X_1 \cdot D;\ Y_3 = (D - E) \cdot Z_1;\ Z_3 = (D + E) \cdot Y_1.$$

The fourth doubling formulas, also requiring $2 \neq 0$ in the field, improve cost even more, to $6\mathbf{M} + 2\mathbf{S} + 1\mathbf{M}_d$.

$$R = Y_1 + Z_1;\ S = Y_1 - Z_1;\ T = R^2;\ U = S^2;\ V = T + 3U;\ W = 3T + U;$$
$$C = R \cdot V;\ D = S \cdot W;\ E = 3C - dX_1 \cdot (W - V);$$
$$X_3 = -2X_1 \cdot D;\ Y_3 = (D + E) \cdot Z_1;\ Z_3 = (D - E) \cdot Y_1.$$

In most situations the fastest approach is to choose small d and use the fourth doubling formulas. Characteristic 3 typically has fast cubings, making the first doubling formulas faster. Characteristic 2 allows only the first doubling formulas.

Tripling. Assume that $d \neq 0$. The 3-isogenies in Theorem 5.4 then lead to efficient tripling formulas that compute $(X_3 : Y_3 : Z_3) = 3(X_1 : Y_1 : Z_1)$ significantly faster than a doubling followed by an addition. This is useful in, e.g., scalar multiplications using double-base chains; see Section 7.

Specifically, define

$$U = -X_1Y_1Z_1; \qquad V = Y_1^3; \qquad W = X_1^3; \qquad Q = dU = -dX_1Y_1Z_1;$$
$$R = aW = aX_1^3; \qquad S = -(V + Q + R) = -(Y_1^3 - dX_1Y_1Z_1 + aX_1^3) = Z_1^3;$$
$$X_3 = (R^3 + S^3 + V^3 - 3RSV)/d;$$
$$Y_3 = RS^2 + SV^2 + VR^2 - 3RSV; \qquad Z_3 = RV^2 + SR^2 + VS^2 - 3RSV.$$

Then the isogenies ι and ι' in Theorem 5.4 satisfy $\iota(X_1 : Y_1 : Z_1) = (U : V : W)$ and $3(X_1 : Y_1 : Z_1) = \iota'(U : V : W) = (X_3 : Y_3 : Z_3)$. All tripling formulas that

we consider begin by computing $R = aX_1^3$, $V = Y_1^3$, and $S = Z_1^3$ with three cubings (normally $3\mathbf{M} + 3\mathbf{S}$, except for fields supporting faster cubing) and then compute X_3, Y_3, Z_3 from R, S, V. Note that computing S as Z_1^3 is faster than computing U as $-X_1Y_1Z_1$, and there does not seem to be any benefit in computing U or $Q = dU$.

The following straightforward formulas compute X_3, Y_3, Z_3 from R, S, V in $5\mathbf{M} + 3\mathbf{S} + \mathbf{M}_{1/d}$, assuming $2 \neq 0$ in the field, where $\mathbf{M}_{1/d}$ means the cost of multiplying by the curve parameter $1/d$:

$$\begin{aligned} A &= (R - V)^2;\ B = (R - S)^2;\ C = (V - S)^2;\ D = A + C;\ E = A + B; \\ X_3 &= (1/d)(R + V + S) \cdot (B + D);\ Y_3 = 2RC - V \cdot (C - E); \\ Z_3 &= 2VB - R \cdot (B - D). \end{aligned}$$

The total cost for tripling this way is $8\mathbf{M} + 6\mathbf{S} + \mathbf{M}_a + \mathbf{M}_{1/d}$. For the case $a = 1$ the same cost had been achieved by Hisil, Carter, and Dawson in [30]. One can of course scale X_3, Y_3, Z_3 by a factor of d, replacing $\mathbf{M}_{1/d}$ with $2\mathbf{M}_d$.

Here is a technique to produce faster formulas, building upon the structure used in the proofs in Section 5. Start with the polynomial identity

$$\begin{aligned} &(\alpha R + \beta S + \gamma V)(\alpha S + \beta V + \gamma R)(\alpha V + \beta R + \gamma S) \\ &\quad = \alpha\beta\gamma d X_3 + (\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) Y_3 + (\beta\alpha^2 + \gamma\beta^2 + \alpha\gamma^2) Z_3 + (\alpha + \beta + \gamma)^3 RSV. \end{aligned}$$

Specialize this identity to three choices of constants (α, β, γ), and use the curve equation $d^3RSV = a(R + S + V)^3$ appearing in the proof of Theorem 5.4, to obtain four linear equations for dX_3, Y_3, Z_3, RSV. If the constants are sensibly chosen then the equations are independent.

We now give three examples of this technique. First: Taking $(\alpha, \beta, \gamma) = (1, 1, 1)$ gives $(R + S + V)^3 = dX_3 + 3Y_3 + 3Z_3 + 27RSV$, as already used in the proof of Theorem 5.4. Taking $(\alpha, \beta, \gamma) = (1, -1, 0)$ gives $(R - S)(S - V)(V - R) = Y_3 - Z_3$, and taking $(\alpha, \beta, \gamma) = (1, 1, 0)$ gives $(R + S)(S + V)(V + R) = Y_3 + Z_3 + 8RSV$. These equations, together with $a(R+S+V)^3 = d^3RSV$, are linearly independent except in characteristic 2: we have

$$\begin{aligned} dX_3 &= (1 - 3a/d^3)(R+S+V)^3 - 3(R+S)(S+V)(V+R), \\ 2Y_3 &= (R+S)(S+V)(V+R) + (R-S)(S-V)(V-R) - 8(a/d^3)(R+S+V)^3, \\ 2Z_3 &= (R+S)(S+V)(V+R) - (R-S)(S-V)(V-R) - 8(a/d^3)(R+S+V)^3. \end{aligned}$$

Computing $(2X_3, 2Y_3, 2Z_3)$ from these formulas takes one cubing for $(R+S+V)^3$, $2\mathbf{M}$ for $(R+S)(S+V)(V+R)$, $2\mathbf{M}$ for $(R-S)(S-V)(V-R)$, one multiplication by a/d^3 (or, alternatively, a multiplication of $R+S+V$ by $1/d$ and a subsequent multiplication by a), one multiplication by $1/d$, and several additions, for a total cost of $8\mathbf{M} + 4\mathbf{S} + \mathbf{M}_a + \mathbf{M}_{a/d^3} + \mathbf{M}_{1/d}$; i.e., $8\mathbf{M} + 4\mathbf{S}$ when both a and $1/d$ are chosen to be small. As noted in the introduction, this result is due to Kohel [39], as a followup to our preliminary announcements of results in this paper.

Second example: For characteristic 2 one must take at least one vector (α, β, γ) outside $\mathbf{F}_2^3$, creating more multiplications by constants. The overall cost is still $8\mathbf{M}+4\mathbf{S}$ if all constants are chosen to be small and $(1, 1, 1)$ is used as an (α, β, γ).

Third example: Assume that the base field k is $\mathbf{F}_p[\omega]/(\omega^2+\omega+1)$ where $p \in 2+3\mathbf{Z}$, or more generally has any primitive cube root ω of 1 for which multiplications by ω are fast. Now take the vectors $(\alpha,\beta,\gamma) = (1,\omega^i,\omega^{2i})$ and observe that the left side of the above identity is always a cube:

$$(R+\omega S+\omega^2 V)^3 = dX_3 + 3\omega^2 Y_3 + 3\omega Z_3,$$
$$(R+\omega^2 S+\omega V)^3 = dX_3 + 3\omega Y_3 + 3\omega^2 Z_3.$$

These equations and $(1-27a/d^3)(R+S+V)^3 = dX_3+3Y_3+3Z_3$ are linearly independent; the matrix of coefficients of $dX_3, 3Y_3, 3Z_3$ is a Fourier matrix. We apply the inverse Fourier matrix to obtain $dX_3, 3Y_3, 3Z_3$ with a few more multiplications by ω. Overall this tripling algorithm costs just 6 cubings, i.e., $6\mathbf{M}+6\mathbf{S}$.

One way to understand the appearance of the Fourier matrix here is to observe that the polynomial $dX_3 + 3Y_3t + 3Z_3t^2 + 9(1+t+t^2)RSV$ is the cube of $V+St+Rt^2$ modulo t^3-1. We compute the cube of $V+St+Rt^2$ separately modulo $t-1$, $t-\omega$, and $t-\omega^2$.

7 Cost of scalar multiplication

This section analyzes the cost of scalar multiplication using twisted Hessian curves. In particular, this section explains how we obtained a cost of just $8.77\mathbf{M}$ per bit for average 256-bit scalars.

Since our new twisted-Hessian formulas provide very fast tripling and reasonably fast doubling, the results of [6] suggest that it will be fastest to represent scalars using $\{2,3\}$-double-base chains. Scalar multiplication then involves not only doubling and addition but also tripling. A well-known advantage of double-base representations is that the number of additions is smaller than in the binary representation.

We use a newer algorithm to generate double-base chains, shown in Figure 7.1. This algorithm is an improved version of the basic "tree-based" algorithm proposed and analyzed by Doche and Habsieger in [21].

In the basic algorithm, n is computed recursively from either $(n-1)/(2^{\cdots}3^{\cdots})$ or $(n+1)/(2^{\cdots}3^{\cdots})$, where the exponents of 2 and 3 are chosen to be as large as possible. The algorithm explores the branching tree of possibilities in breadth-first fashion until it reaches $n=1$. To limit time and memory usage, the algorithm keeps only the smallest B nodes at each level. We chose $B=200$.

We use an extension to this algorithm mentioned but not analyzed in [21]. The extension uses not just $n-1$ and $n+1$, but all $n-c$ where c is in a precomputed set (including both positive and negative values). We include the cost of precomputing this set. We chose 21 different possibilities for the precomputed set, namely the 21 sets listed in [6].

We change the way to add new nodes as follows:

- n has *one* child node $n/2$ if n is divisible by 2;
- otherwise, n has *one* child node $n/3$ if n is divisible by 3;
- otherwise, n has *several* child nodes $n-c$, one for each $c \in S$.

Input: An integer n, precomputation set S, and bounds B and C
Output: A double-base chain computing n

```
for each precomputation set S do
    counter ← 0
    Initialize a tree T with root node n
    while (counter < C) do
        for each leaf node m in T do
            if m divisible by 2 then
                Insert child ← f2(m)                    ▷ f2(m) = m/2^v2(m)
                if f2(m) equals 1 then
                    counter ← counter +1
            else if m divisible by 3 then
                Insert child ← f3(m)                    ▷ f3(m) = m/3^v3(m)
                if f3(m) equals 1 then
                    counter ← counter +1
            else
                for each element c in precomputation set S do
                    if m − c > 0 then
                        Insert child ← f(m − c)
                        if m − c equals 1 then
                            counter ← counter + 1
        Discard all but the B smallest weight leaf nodes
return The smallest cost chain
```

Fig. 7.1. The algorithm we used to generate double-base chains. "End" statements are implied by indentation, as in Python.

We improve the algorithm by continuing to search the tree until we have found C chains, rather than stopping with the first chain; we then take the lowest-cost chain. We chose $C = 200$.

We further improve the algorithm by taking the lowest-weight B nodes at each level instead of the smallest B nodes at each level; here "weight" takes account not just of smallness but also of the cost of operations used to reach the node. More precisely, we define "weight" as cost $+ 8 \cdot \log_2(n)$.

We ran this algorithm for 10000 random 256-bit scalars, i.e., integers between 2^{255} and $2^{256} - 1$, using as input the costs of twisted Hessian operations. The average cost of the resulting chain was 8.77**M** per bit.

To more precisely assess the advantage of cofactor 3 over cofactor 1, we carried out a larger series of experiments for smaller scalars, comparing the cost of twisted Hessian curves to the cost of short Weierstrass curves $y^2 = x^3 - 3x + a_6$ in Jacobian coordinates. Specifically, for each b from 2 through 16, we constructed double-base chains for all b-bit integers; for each b from 17 through 64, we constructed double-base chains for 1000 randomly chosen b-bit integers. The top of Figure 7.2 plots pairs (x, y) where x is the cost to multiply by n on a twisted Hessian curve and $x + y$ is the cost to multiply by the same integer n on a

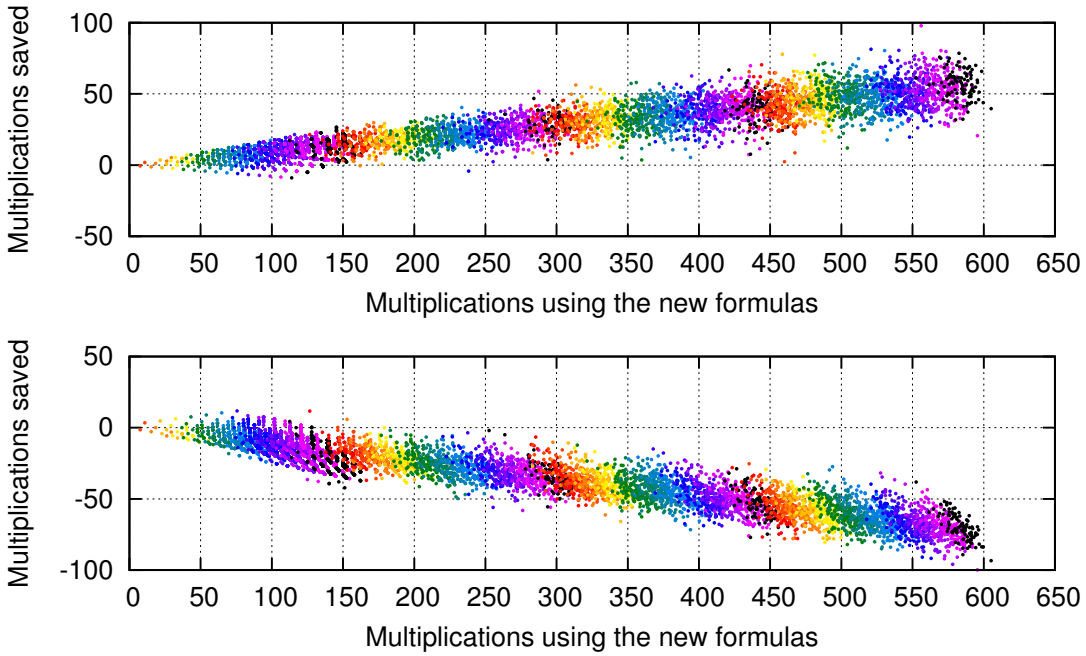

Fig. 7.2. Top: Points (x, y) for 100 randomly sampled b-bit integers n for each $b \in \{2, 3, \ldots, 64\}$. Here $x\mathbf{M}$ are used to compute $P \mapsto nP$ on a twisted Hessian curve in projective coordinates; $(x + y)\mathbf{M}$ are used to compute $P \mapsto nP$ on a Weierstrass curve $y^2 = x^3 - 3x + a_6$ in Jacobian coordinates; and the color is a function of b. Bottom: Similar, but using a twisted Edwards curve rather than a Weierstrass curve.

Weierstrass curve; i.e., switching from Weierstrass to twisted Hessian saves $y\mathbf{M}$. We reduced the number of dots plotted in this figure to avoid excessive PDF file sizes and display times, but a full plot is similar. Dots along the x-axis represent integers with the same cost for both curve shapes. Different colors are used for different bit-sizes b.

We have generated similar plots for some other pairs of curve shapes. For example, the bottom of Figure 7.2 shows that Edwards is faster than Hessian for most values of n. In some cases, such as Hessian vs. tripling-oriented Doche–Icart–Kohel curves, the plots are concentrated much more narrowly around a line, since these curve shapes favor similar integers that use many triplings; the line has a positive slope, i.e., Hessian is faster.

References

[1] Christophe Arène, Tanja Lange, Michael Naehrig, Christophe Ritzenthaler, *Faster computation of the Tate pairing*, Journal of Number Theory **131** (2011), 842–857. URL: https://eprint.iacr.org/2009/155. Citations in this document: §2.

[2] Siegfried Heinrich Aronhold, *Zur Theorie der homogenen Functionen dritten Grades von drei Variabeln*, Crelles Journal für die reine und angewandte Mathematik **1850 (39)** (1850), 140–159. URL: http://www.degruyter.com/

view/j/crll.1850.issue-39/crll.1850.39.140/crll.1850.39.140.xml. Citations in this document: §2.

[3] Josh Benaloh (editor), *Topics in cryptology — CT-RSA 2014 — the cryptographer's track at the RSA Conference 2014, San Francisco, CA, USA, February 25–28, 2014, proceedings*, Lecture Notes in Computer Science, vol. 8366, Springer, 2014. ISBN 978-3-319-04851-2. See [27].

[4] Daniel J. Bernstein, *Complete addition laws for all elliptic curves over finite fields (talk slides)* (2009). URL: http://cr.yp.to/talks/2009.07.17/slides.pdf. Citations in this document: §1.

[5] Daniel J. Bernstein, *Curve25519: new Diffie-Hellman speed records*, in PKC 2006 [**52**] (2006), 207–228. URL: http://cr.yp.to/papers.html#curve25519. Citations in this document: §1.

[6] Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters, *Optimizing double-base elliptic-curve single-scalar multiplication*, in Indocrypt 2007 [**51**] (2007), 167–182. URL: https://eprint.iacr.org/2007/414. Citations in this document: §1, §7, §7.

[7] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, Bo-Yin Yang, *High-speed high-security signatures*, Journal of Cryptographic Engineering **2** (2012), 77–89. URL: https://eprint.iacr.org/2011/368. Citations in this document: §1.

[8] Daniel J. Bernstein, Tanja Lange, *Explicit-formulas database* (2007). URL: https://hyperelliptic.org/EFD. Citations in this document: §1.

[9] Daniel J. Bernstein, Tanja Lange, *Faster addition and doubling on elliptic curves*, in Asiacrypt 2007 [**40**] (2007), 29–50. URL: http://cr.yp.to/papers.html#newelliptic. Citations in this document: §1, §1.

[10] Daniel J. Bernstein, Tanja Lange, *Analysis and optimization of elliptic-curve single-scalar multiplication*, in Fq8 [**44**] (2008), 1–19. URL: https://eprint.iacr.org/2007/455. Citations in this document: §1.

[11] Daniel J. Bernstein, Tanja Lange, *A complete set of addition laws for incomplete Edwards curves*, Journal of Number Theory **131** (2011), 858–872. URL: http://cr.yp.to/papers.html#completed. Citations in this document: §4, §4, §4, §4.

[12] Guido Bertoni, Jean-Sébastien Coron (editors), *Cryptographic hardware and embedded systems — CHES 2013 — 15th international workshop, Santa Barbara, CA, USA, August 20–23, 2013, proceedings*, Lecture Notes in Computer Science, vol. 8086, Springer, 2013. ISBN 978-3-642-40348-4. See [49].

[13] Olivier Billet, Marc Joye, *The Jacobi model of an elliptic curve and side-channel analysis*, in AAECC 2003 [**28**] (2003), 34–42. MR 2005c:94045. URL: eprint.iacr.org/2002/125. Citations in this document: §1.

[14] Wieb Bosma, Hendrik W. Lenstra, Jr., *Complete systems of two addition laws for elliptic curves*, Journal of Number Theory **53** (1995), 229–240. ISSN 0022–314X. MR 96f:11079. Citations in this document: §3, §3, §4, §4.

[15] Ljiljana Brankovic, Willy Susilo (editors), *Australasian information security conference (AISC 2009), Wellington, New Zealand, January 2009*, Conferences in Research and Practice in Information Technology (CRPIT), vol. 98, Australian Computer Society, Inc., 2009. See [31].

[16] Arthur Cayley, *On the 34 concomitants of the ternary cubic*, American Journal of Mathematics **4** (1881), 1–15. Citations in this document: §2.

[17] David V. Chudnovsky, Gregory V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Advances in Applied Mathematics **7** (1986), 385–434. MR 88h:11094. Citations in this document: §1, §1, §1, §1, §2, §3, §3.

[18] Henri Cohen, Gerhard Frey (editors), *Handbook of elliptic and hyperelliptic curve cryptography*, CRC Press, 2005. ISBN 1-58488-518-1. MR 2007f:14020. See [23].

[19] Henri Cohen, Atsuko Miyaji, Takatoshi Ono, *Efficient elliptic curve exponentiation using mixed coordinates*, in Asiacrypt 1998 [**48**] (1998), 51–65. MR 1726152. URL: http://www.math.u-bordeaux.fr/~cohen/asiacrypt98.dvi. Citations in this document: §1.

[20] Craig Costello, Huseyin Hisil, Benjamin Smith, *Faster compact Diffie–Hellman: endomorphisms on the x-line*, in Eurocrypt 2014 [**45**] (2014), 183–200. URL: https://eprint.iacr.org/2013/692. Citations in this document: §1.

[21] Christophe Doche, Laurent Habsieger, *A tree-based approach for computing double-base chains*, in ACISP 2008 [**43**] (2008), 433–446. Citations in this document: §1, §1, §7, §7.

[22] Christophe Doche, Thomas Icart, David R. Kohel, *Efficient scalar multiplication by isogeny decompositions*, in PKC 2006 [**52**] (2006), 191–206. Citations in this document: §1.

[23] Christophe Doche, Tanja Lange, *Arithmetic of elliptic curves*, in HEHCC [**18**] (2005), 267–302. Citations in this document: §5.

[24] Harold M. Edwards, *A normal form for elliptic curves*, Bulletin of the American Mathematical Society **44** (2007), 393–422. URL: http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html. Citations in this document: §1.

[25] Reza Rezaeian Farashahi, Marc Joye, *Efficient arithmetic on Hessian curves*, in PKC 2010 [**46**] (2010), 243–260. Citations in this document: §1, §1.

[26] Reza Rezaeian Farashahi, Hongfeng Wu, Chang-An Zhao, *Efficient arithmetic on elliptic curves over fields of characteristic three*, in SAC 2012 [**35**] (2013), 135–148. Citations in this document: §1, §1.

[27] Armando Faz-Hernández, Patrick Longa, Ana H. Sánchez, *Efficient and secure algorithms for GLV-based scalar multiplication and their implementation on GLV-GLS curves*, in CT-RSA 2014 [**3**] (2013), 1–27. URL: https://eprint.iacr.org/2013/158. Citations in this document: §1.

[28] Marc Fossorier, Tom Hoeholdt, Alain Poli (editors), *Applied algebra, algebraic algorithms and error-correcting codes*, Lecture Notes in Computer Science, vol. 2643, Springer, 2003. ISBN 3-540-40111-3. MR 2004j:94001. See [13].

[29] Otto Hesse, *Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln*, Journal für die Reine und Angewandte Mathematik **28** (1844), 68–96. ISSN 0075-4102. Citations in this document: §2.

[30] Huseyin Hisil, Gary Carter, Ed Dawson, *New formulae for efficient elliptic curve arithmetic*, in Indocrypt 2007 [**51**] (2007), 138–151. Citations in this document: §1, §1, §1, §1, §6.

[31] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, Ed Dawson, *Faster group operations on elliptic curves*, in AISC 2009 [**15**] (2009), 7-19. URL: https://eprint.iacr.org/2007/441. Citations in this document: §1.

[32] Huseyin Hisil, *Elliptic curves, group law, and efficient computation*, Ph.D. thesis, Queensland University of Technology, 2010. Citations in this document: §1, §1, §1, §1.

[33] Dale Husemöller, *Elliptic curves*, 2nd edition, Graduate Texts in Mathematics, vol. 111, Springer, 2003. ISBN 978-0387954905. Citations in this document: §2.

[34] Marc Joye, Jean-Jacques Quisquater, *Hessian elliptic curves and side-channel attacks*, in CHES 2001 [**37**] (2001), 402–410. MR 2003k:94032. URL: http://joye.site88.net/. Citations in this document: §1, §2, §2, §4.

[35] Lars R. Knudsen, Huapeng Wu (editors), *Selected areas in cryptography, 19th international conference, SAC 2012, Windsor, ON, Canada, August 15–16, 2012, revised selected papers*, Lecture Notes in Computer Science, vol. 7707, Springer, 2013. ISBN 978-3-642-35998-9. See [26].

[36] Neal Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, vol. 3, Springer, 1998. ISBN 978-3-540-63446-1. Citations in this document: §2.

[37] Çetin Kaya Koç, David Naccache, Christof Paar (editors), *Cryptographic hardware and embedded systems—CHES 2001, third international workshop, Paris, France, May 14–16, 2001, proceedings*, Lecture Notes in Computer Science, vol. 2162, Springer, 2001. ISBN 3-540-42521-7. MR 2003g:94002. See [34], [41], [50].

[38] David Kohel, *Addition law structure of elliptic curves*, Journal of Number Theory **131** (2011), 894–919. Citations in this document: §3.

[39] David Kohel, *The geometry of efficient arithmetic on elliptic curves*, in Arithmetic, Geometry, Coding Theory and Cryptography **637** (2015). Citations in this document: §1, §1, §1, §6.

[40] Kaoru Kurosawa (editor), *Advances in cryptology—ASIACRYPT 2007, 13th international conference on the theory and application of cryptology and information security, Kuching, Malaysia, December 2–6, 2007, proceedings*, Lecture Notes in Computer Science, vol. 4833, Springer, 2007. ISBN 978-3-540-76899-9. See [9].

[41] Pierre-Yvan Liardet, Nigel P. Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form*, in CHES 2001 [**37**] (2001), 391–401. MR 2003k:94033. Citations in this document: §1.

[42] Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of Computation **48** (1987), 243–264. ISSN 0025-5718. MR 88e:11130. Citations in this document: §1.

[43] Yi Mu, Willy Susilo, Jennifer Seberry (editors), *Information security and privacy — 13th Australasian conference, ACISP 2008, Wollongong, Australia, July 7–9, 2008, proceedings*, Lecture Notes in Computer Science, vol. 5107, Springer, 2008. ISBN 978-3-540-69971-2. See [21].

[44] Gary L. Mullen, Daniel Panario, Igor E. Shparlinski (editors), *Finite fields and applications: papers from the 8th international conference held in Melbourne, July 9–13, 2007*, Contemporary Mathematics, vol. 461, American Mathematical Society, 2008. ISBN 978-0-8218-4309-3. MR 2009h:11004. See [10].

[45] Phong Q. Nguyen, Elisabeth Oswald (editors), *Advances in cryptology — EUROCRYPT 2014 — 33rd annual international conference on the theory and applications of cryptographic techniques, Copenhagen, Denmark, May 11–15, 2014, proceedings*, Lecture Notes in Computer Science, vol. 8441, Springer, 2014. ISBN 978-3-642-55219-9. See [20].

[46] Phong Q. Nguyen, David Pointcheval (editors), *Public key cryptography—PKC 2010, 13th international conference on practice and theory in public key cryptography, Paris, France, May 26–28, 2010, proceedings*, Lecture Notes in Computer Science, vol. 6056, Springer, 2010. ISBN 978-3-642-13012-0. See [25].

[47] National Institute of Standards and Technology, *Recommended elliptic curves for federal government use* (1999). URL: http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf. Citations in this document: §1.

[48] Kazuo Ohta, Dingyi Pei (editors), *Advances in cryptology — ASIACRYPT'98: proceedings of the International Conference on the Theory and Application of Cryptology and Information Security held in Beijing*, Lecture Notes in Computer Science, vol. 1514, Springer, 1998. ISBN 3-540-65109-8. MR 2000h:94002. See [19].

[49] Thomaz Oliveira, Julio López, Diego F. Aranha, Francisco Rodríguez-Henríquez, *Lambda coordinates for binary elliptic curves*, in CHES 2013 [**12**] (2013), 311–330. URL: https://eprint.iacr.org/2013/131. Citations in this document: §1.

[50] Nigel P. Smart, *The Hessian form of an elliptic curve*, in CHES 2001 [**37**] (2001), 118–125. Citations in this document: §2, §5.

[51] Kannan Srinathan, C. Pandu Rangan, Moti Yung (editors), *Progress in cryptology—INDOCRYPT 2007, 8th international conference on cryptology in India, Chennai, India, December 9–13, 2007, proceedings*, Lecture Notes in Computer Science, vol. 4859, Springer, 2007. ISBN 978-3-540-77025-1. See [6], [30].

[52] Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, Tal Malkin (editors), *Public key cryptography — 9th international conference on theory and practice in public-key cryptography, New York, NY, USA, April 24–26, 2006, proceedings*, Lecture Notes in Computer Science, vol. 3958, Springer, 2006. ISBN 978-3-540-33851-2. See [5], [22].