Simple geometrically split abelian surfaces over finite fields

Kuo-Ming James Chou and Ernst Kani

1 Introduction

In the search to find curves which are suitable for cryptography, several authors have studied genus 2 curves $C/\mathbb{F}_q$ whose Jacobians have the property of the title of this paper, i.e. the Jacobian J_C of $C/\mathbb{F}_q$ is $\mathbb{F}_q$-simple but $J_C \otimes \overline{\mathbb{F}}_q$ is isogenous to a product surface, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$. For example, Satoh[10] considered the *Legendre curves* $y^2 = x^5 + ux^3 + vx$ which generalize those studied by Furukawa, Kawazoe and Takahashi[4] (where $u = 0$).

A natural question in this connection is to try to classify all abelian surfaces $A/\mathbb{F}_q$ which are simple but geometrically split. This is answered by the following result.

Theorem 1. *Let $A/\mathbb{F}_q$ be a simple, non-supersingular abelian surface. Then $A \otimes \mathbb{F}_{q^n}$ splits for some $n > 1$ if and only if A is ordinary and there is an integer c such that*

$$(1) \qquad \mathrm{tr}_A^2 \;=\; c(s_A - cq + 2q) \quad \textit{with} \quad 0 \le c \le 3,$$

where s_A is the coefficient of the X^2-term of the characteristic polynomial $h_A(X)$ of $A/\mathbb{F}_q$ and tr_A is the trace of A. If this is the case, then $A \otimes \mathbb{F}_{q^n} \sim E_n^2$ for some elliptic curve $E/\mathbb{F}_{q^n}$, where $n = c+2$ for $c < 3$ and $n = 6$ for $c = 3$. Moreover, n is minimal in the sense that $A \otimes \mathbb{F}_{q^m}$ is simple for all $m|n$, $m \ne n$.

Except for the compact formulation of condition (1), this theorem was proved by Maisner and Nart[7] and by Howe and Zhu[6] in the ordinary case. Since the proof of [7] is not entirely self-contained (cf. Remark 4), we present here a more direct proof in section 2.

To actually prove the *existence* of simple, geometrically split abelian surfaces, further work is necessary. To this end we prove in section 3:

Theorem 2. (a) *Let $s \in \mathbb{Z}$. Then there is a simple, ordinary abelian surface $A/\mathbb{F}_q$ with $s_A = s$ such that $A \otimes \mathbb{F}_{q^2}$ splits if and only if*

$$(2) \qquad |s| \le 2q, \quad \gcd(s,q) = 1 \quad \textit{and} \quad 2q - s \ne x^2,\ \forall x \in \mathbb{Z}.$$

If these conditions hold, then we have $h_A(X) = X^4 + sX^2 + q^2$.

(b) *Let $n = 3, 4$ or 6 and put $c = [\frac{n}{2}]$. If $t \in \mathbb{Z}$, then there is a simple, ordinary abelian surface $A/\mathbb{F}_q$ with $\mathrm{tr}_A = t$ such that $A \otimes \mathbb{F}_{q^n}$ splits (but $A \otimes \mathbb{F}_{q^m}$ is simple for $m|n$, $m \ne n$) if and only if*

$$(3) \qquad t^2 \le 4cq, \quad \gcd(t,q) = 1, \quad c|t, \quad \textit{and} \quad 4cq - t^2 \ne \varepsilon x^2,\ \forall x \in \mathbb{Z},$$

where $\varepsilon = 1$ *if* $n = 4$ *and* $\varepsilon = 3$ *otherwise. If these conditions hold, then* $h_A(X) = X^4 - tX^3 + \left(\frac{t^2}{c} - (c-2)q\right)X^2 - tqX + q^2$.

(c) *If* $A/\mathbb{F}_q$ *is any simple, non-supersingular abelian surface which is geometrically split, then it is one of the surfaces listed in parts* (a) *and* (b).

Note that (3) shows that the case $n = 4$ cannot occur when $q = 2^r$ and that $n = 6$ and $q = 7$ cannot occur when $q = 3^r$; cf. Remark 19(a). However, in all other cases there exists a simple ordinary abelian surface $A/\mathbb{F}_q$ such that $A \otimes \mathbb{F}_{q^n}$ is minimally split; cf. Proposition 18.

A related *existence question* is the following: for which ordinary elliptic curves $E/\mathbb{F}_{q^n}$ (where $n \in \{2, 3, 4, 6\}$) is there a simple abelian surface $A/\mathbb{F}_q$ such that $A \otimes \mathbb{F}_{q^n} \sim E^2$? This question is answered in section 3 (cf. Theorem 20 and Proposition 30), and is closely related to the structure of the *Weil restriction* of $E/\mathbb{F}_{q^n}$ with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$. This relation is explained in section 4 (cf. Propositions 21 and 26) and is used to determine all abelian surfaces $B/\mathbb{F}_q$ such that $B \otimes \mathbb{F}_{q^n} \sim E^2$; cf. Proposition 29.

In the last section we apply our results to the Jacobians $J_{u,v}/\mathbb{F}_q$ defined by the genus 2 curves

$$C_{u,v}/\mathbb{F}_q : \qquad y^2 = x^5 + ux^3 + vx$$

which were studied by Legendre (1832) and Satoh[10]. As Satoh showed, we have that $J_{u,v} \otimes \mathbb{F}_{q^4} \sim E^2$, for some (explicit) elliptic curve $E/\mathbb{F}_{q^4}$, and in Theorem 31 we use our previous results to determine when $J_{u,v}$ splits already over $\mathbb{F}_{q^2}$. This allows us to simplify Satoh's algorithm for determining (the largest prime factor of) $|J_{u,v}(\mathbb{F}_q)|$; cf. Algorithm 37. As a result, the algorithm now runs in deterministic polynomial time in place of Satoh's probabilistic polynomial time. Moreover, in place of considering Satoh's 26 possibilities for the group order, we only have to consider 2 possibilities.

This research was supported by an OGS grant held by the first author and by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC) held by the second author.

2 Classification theorems

In this section we classify the simple abelian surfaces $A/\mathbb{F}_q$ which are geometrically split. As was indicated in the introduction, this classification will be given in terms of properties of the coefficients tr_A and s_A of the characteristic polynomial $h_A(X) \in \mathbb{Z}[X]$ of (the Frobenius endomorphism π_A of) $A/\mathbb{F}_q$. A first step towards this classification is the following result.

Theorem 3. *Let $A/\mathbb{F}_q$ be a simple, non-supersingular abelian surface such that*

$$A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \sim E_1 \times E_2,$$

for some integer $n > 1$ and some elliptic curves $E_i/\mathbb{F}_{q^n}$, where $i = 1, 2$. Then

(a) *A, E_1, and E_2 are ordinary, and $E_1 \sim E_2$.*

(b) *$h_A(X)$ is irreducible over $\mathbb{Q}$, and $K := \mathbb{Q}[X]/(h_A(X))$ is biquadratic extension of $\mathbb{Q}$, i.e. $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

(c) *If n is minimal, then $n = 2, 3, 4$ or 6.*

Remark 4. Most of this theorem can already be found in the literature. Specifically, the fact that A has to be ordinary (Theorem 3(a)) follows from Corollary 2.17 of [7] and part (c) is part of Theorem 6 of [6]. However, we feel that our proof of part (a) is more direct than that of [7] which relies on previous work (due to Rück and Xing; see [7]). Indeed, we only use basic facts of abelian varieties as given in Mumford[8] and Waterhouse [11]. For example, we shall use the following well-known fact about simple *ordinary* abelian varieties $A/\mathbb{F}_q$.

Lemma 5. *If $A/\mathbb{F}_q$ is a simple, ordinary abelian variety, then $h_A(X)$ is irreducible over $\mathbb{Q}$ and $\mathrm{End}^0(A) \simeq \mathbb{Q}[X]/(h_A(X))$. In particular, $\mathrm{End}^0(A)$ is a CM-field of degree $2\dim(A)$.*

Proof. Since $A/\mathbb{F}_q$ is simple, we know by Theorem 8 of [11] that $h_A(X) = f(X)^d$, where $f(X) \in \mathbb{Q}[X]$ is some irreducible polynomial and d is determined by $[D : Z(D)] = d^2$, where $D := \mathrm{End}^0(A)$ and $Z(D)$ denotes the centre of D. Now the first part of Theorem 7.2 of [11] asserts that D is commutative, and so $d = 1$, and hence $h_A(X) = f(X)$ is irreducible. Moreover, since $Z(D) = \mathbb{Q}(\pi_A)$ (cf. Theorem 3 (a) on page 256 of [8]), it thus follows that $D = Z(D) = \mathbb{Q}(\pi_A) \simeq \mathbb{Q}[X]/(h_A(X))$. In particular, $e := [Z(D) : \mathbb{Q}] = \deg(h_A) = 2\dim(A)$, and so it follows from the classification theory of skewfields with a positive involution ([8], p. 201) and the restrictions on e (cf. [8], p. 202) that we are in Case IV of [8], p. 201, and so $D = Z(D)$ is a CM-field, i.e. D is a totally imaginary field which contains a totally real subfield of index 2.

Remark 6. In connection with the above-quoted Theorem 7.2 of Waterhouse[11], we note that the second part of that theorem is incorrect as stated: it is *not true* that if $A/\mathbb{F}_q$ is simple and ordinary, then $\mathrm{End}^0(A) = \mathrm{End}^0(A \otimes \overline{\mathbb{F}}_q)$, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$. (This incorrect statement is repeated in [12].) Indeed, if this were true, then A would be absolutely simple, and the above Theorem 3 would be vacuous. However, the examples of [4], [10] (and Example 36 below) provide explicit counterexamples to this assertion.

Corollary 7. *If $A/\mathbb{F}_q$ is an ordinary abelian surface, then the characteristic polynomial of A has the form*

$$(4)\quad h_A(X) = (X-\alpha_1)(X-\alpha_2)\left(X - \frac{q}{\alpha_1}\right)\left(X - \frac{q}{\alpha_2}\right) = X^4 - tX^3 + sX^2 - tqX + q^2$$

where $\alpha_1, \alpha_2 \in \mathbb{C}$ with $\alpha_i \neq \frac{q}{\alpha_i} = \overline{\alpha}_i$, for $i = 1, 2$, and $t, s \in \mathbb{Z}$ with $(s, q) = 1$. Moreover, A is simple if and only if $\Delta_A := t^2 - 4s + 8q$ is not a square in $\mathbb{Z}$. If this is the case, then $K_0 = \mathbb{Q}(\sqrt{\Delta_A})$ is the maximal real subfield of $\mathbb{Q}(\pi_A) \simeq \mathbb{Q}[X]/(h_A)$.

Proof. The assertions of the first sentence follow from Proposition 3.4 of [5]. Next, suppose that A is not simple, so $A \sim E_1 \times E_2$, where $E_i/\mathbb{F}_q$ are two elliptic curves. Then $h_A(X) = h_{E_1 \times E_2}(X) = (X^2 - t_1 X + q)(X^2 - t_2 X + q)$, where $t_i = \mathrm{tr}_{E_i}$, and so

$$(5)\qquad \mathrm{tr}_A = t_1 + t_2, \quad s_A = t_1 t_2 + 2q \quad \text{and} \quad \Delta_A = (t_1 - t_2)^2.$$

Thus, Δ_A is a square if A is not simple.

Conversely, suppose that A is simple. Then by Lemma 5 we know that $h_A(X)$ is irreducible and that $K := \mathbb{Q}(\alpha_1) \simeq \mathrm{End}^0(A)$ is a quartic CM field. Thus, if $K_0 \subset K$ denotes the maximal real subfield of K, then $[K_0 : \mathbb{Q}] = 2$.

Since $\overline{\alpha_1} = \frac{q}{\alpha_1}$, we see that $\alpha_1 + \frac{q}{a_1} \in K \cap \mathbb{R} = K_0$. But since α_1 satisfies the polynomial $X^2 - (a_1 + \frac{q}{a_1})X + q \in K_0[X]$, we see that $[K : \mathbb{Q}(a_1 + \frac{q}{a_1})] \leq 2$, and so $K_0 = \mathbb{Q}(a_1 + \frac{q}{a_2})$. Next we note that

$$(6)\qquad g(X) \;:=\; X^2 - tX + (s - 2q) \;=\; \left(X - \left(\alpha_1 + \tfrac{q}{\alpha_1}\right)\right)\left(X - \left(\alpha_2 + \tfrac{q}{\alpha_2}\right)\right)$$

because by multiplying out the factorization (4) we see that $t = (\alpha_1 + \frac{q}{\alpha_1}) + (\alpha_2 + \frac{q}{\alpha_2})$ and $s = 2q + \alpha_1\alpha_2 + \alpha_1\frac{q}{\alpha_2} + \alpha_2\frac{q}{\alpha_1} + \frac{q^2}{\alpha_1\alpha_2}$, from which (6) follows readily. Thus, $g(X) \in \mathbb{Z}[X]$ has $\alpha_1 + \frac{q}{\alpha_1}$ as a root, and so it follows that $g(X)$ is irreducible over $\mathbb{Q}$. Thus, its discriminant $\mathrm{disc}(g) = t^2 - 4(s - 2q) = \Delta_A$ is not a square in $\mathbb{Q}$, and so $K_0 = \mathbb{Q}(\sqrt{\Delta_A})$.

Remark 8. If $A/\mathbb{F}_q$ is an abelian variety, then its *trace* $\mathrm{tr}_A = \mathrm{tr}(\pi_A) \in \mathbb{Z}$ is the trace of its Frobenius endomorphism π_A (cf. [8], p. 182), i.e. $-\mathrm{tr}_A$ is the coefficient of X^{2g-1} in the characteristic polynomial $h_A(X)$ of π_A, where $g = \dim(A)$. Thus, if $A/\mathbb{F}_q$ is an ordinary surface, then $\mathrm{tr}_A = t$ in the notation of (4), and hence (4) shows that $h_A(X)$ (and also the isogeny class of $A/\mathbb{F}_q$) is uniquely determined by the pair of integers (tr_A, s_A), where s_A denotes the coefficient of X^2 in $h_A(X)$.

In fact, if $A/\mathbb{F}_q$ is *any* abelian surface, then its characteristic polynomial $h_A(X)$ has the form (4), as is easy to see by considering the simple and split cases separately. (This fact is used without proof in [7].) Thus, the pair (tr_A, s_A) characterizes the isogeny class of the abelian surface $A/\mathbb{F}_q$.

Proof of Theorem 3. (a) We will show that the following 3 cases are impossible.

Case 1: $E_1/\mathbb{F}_{q^n}$ and $E_2/\mathbb{F}_{q^n}$ are supersingular.

Here we have by page 259 of [8] that $\overline{E} := E_1 \otimes \overline{\mathbb{F}}_{q^n} \sim E_2 \otimes \overline{\mathbb{F}}_{q^n}$, where $\overline{\mathbb{F}}_{q^n}$ denotes the algebraic closure of $\mathbb{F}_{q^n}$. It follows that $A \otimes \overline{\mathbb{F}}_{q^n} \sim \overline{E}^2$ is supersingular, which implies that $A/\mathbb{F}_q$ is supersingular as well, contrary to the hypothesis. Thus, this case cannot occur.

Case 2: $E_1/\mathbb{F}_{q^n}$ and $E_2/\mathbb{F}_{q^n}$ are ordinary but $E_1/\mathbb{F}_{q^n} \not\sim E_2/\mathbb{F}_{q^n}$.

Since both E_1 and E_2 are ordinary, $A_n := A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \sim E_1 \times E_2$ is also ordinary, which implies that $A/\mathbb{F}_q$ is ordinary. We thus have by Lemma 5 that that $\mathrm{End}^0(A)$ is a field of degree $2\dim(A) = 4$ over $\mathbb{Q}$. However,

$$\mathrm{End}^0(A) \subset \mathrm{End}^0(A_n) \simeq \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2)$$

because E_1 and E_2 are not isogenous. Since $\mathrm{End}^0(E_1)$ and $\mathrm{End}^0(E_2)$ are imaginary quadratic fields, it follows by comparing dimensions that

$$\mathrm{End}^0(A) \simeq \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2).$$

Since the right hand side is not a field, we have a contradiction, and so this case is impossible as well.

Case 3: $E_1/\mathbb{F}_{q^n}$ supersingular and $E_2/\mathbb{F}_{q^n}$ ordinary.

Here we shall derive a contradiction after establishing the following claims.

Claim 3.1: $h_A(X)$ is irreducible over $\mathbb{Q}$ and $\mathrm{End}^0(A)$ is a field.

Suppose $h_A(X)$ were reducible over $\mathbb{Q}$. Since $A/\mathbb{F}_q$ is simple, we know by Theorem 8 of [12] that $h_A(X) = f(X)^d$ for some $d \in \mathbb{N}$ and some $f(X) \in \mathbb{Z}[X]$. If $\deg(f(X)) = 1$, then Theorem 3 (d) on page 256 of [8] shows that A is $\mathbb{F}_q$-isogenous to a power of a supersingular elliptic curve, which is contrary to the hypothesis that A is non-supersingular. Thus, we must have that $h_A(X) = f(X)^2$, where $\deg(f(X)) = 2$, and so by Theorem 8 of [12], we know that $\mathrm{End}^0(A)$ is a skewfield of degree $[\mathrm{End}^0(A) : \mathbb{Q}] = 2^2 \deg(f(X)) = 8$. On the other hand, since $E_1 \not\sim E_2$, we have that

$$\mathrm{End}^0(A) \subset \mathrm{End}^0(A_n) \simeq \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2) \subseteq \mathrm{End}^0(\overline{E}_1) \times \mathrm{End}^0(\overline{E}_2) = Q \times F,$$

where $\overline{E}_i := E_i \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_{q^n}$, for $i = 1, 2$, and Q is a quaternion algebra, and F is an imaginary quadratic field. By comparing dimensions, we have that $\mathrm{End}^0(A) \simeq Q \times F$, which is a contradiction because $Q \times F$ is not a skewfield. Thus, $h_A(X)$ must be irreducible over $\mathbb{Q}$, and hence has no repeated roots. By Theorem 3 (a) (c) on page 256 of [8], it follows that $\mathrm{End}^0(A) \simeq \mathbb{Q}(\pi_A)$ is a field. This concludes Claim 3.1.

Claim 3.2: $\pi_{E_1} = [\pm q^{\frac{n}{2}}]$

Since E_1 is supersingular, we know that $\mathrm{End}^0(\overline{E}_1) = Q$ is a quaternion algebra, where $\overline{E}_1 := E_1 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_{q^n}$. First we show that $\mathrm{End}^0(E_1) = Q$. If not, then $\mathrm{End}^0(E_1)$ is a skewfield which is properly contained in Q, and so $\mathrm{End}^0(E_1) \leq 2$. Thus, since $A_n := A \otimes \mathbb{F}_{q^n} \sim E_1 \times E_2$, where $E_1 \not\sim E_2$, we have $\mathrm{End}^0(A_n) \simeq \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2) = \mathrm{End}^0(E_1) \times F$, where F is an imaginary quadratic field. Thus $[\mathrm{End}^0(A_n) : \mathbb{Q}] \leq 4$, and so $\mathrm{End}^0(A) = \mathrm{End}^0(A_n) \simeq \mathrm{End}^0(E_1) \times F$ by comparing degrees. This, however, is impossible since the latter is not a field.

We thus have that $\mathrm{End}^0(E_1) = Q$, i.e. all endomorphisms of $\bar{E}_1$ are defined over $\mathbb{F}_{q^n}$. It then follows from Theorem 3 (d) on page 256 of [8] that $h_{E_1}(X) = (X-a)^2$ for some $a \in \mathbb{Q}$. This implies that $a^2 = q^n$, which means that $a = \pm q^{\frac{n}{2}}$ is the eigenvalue of π_{E_1}. Thus, $\pi_{E_1} = [\pm q^{\frac{n}{2}}]$, which verifies Claim 3.2.

Claim 3.3: The minimal polynomial $m_{A_n}(X)$ of π_{A_n} over $\mathbb{Q}$ has degree 3.

By Claim 3.2, we know that the minimal polynomial of π_{E_1} is $m_{E_1}(X) = X \pm q^{\frac{n}{2}}$. On the other hand, since E_2 is ordinary we know that the minimal polynomial of π_{E_2} is irreducible over $\mathbb{Q}$ of degree 2. Thus, the minimal polynomial of $\pi_{E_1 \times E_2}$ is

$$m_{E_1 \times E_2}(X) = \mathrm{lcm}(m_{E_1}(X), m_{E_2}(X)) = m_{E_1}(X) m_{E_2}(X),$$

which has degree 3. Since $m_{A_n}(X) = m_{E_1 \times E_2}(X)$, we have $\deg(m_{A_n}(X)) = 3$ as claimed.

We now combine Claims 3.1 and 3.3 to derive a contradiction. Since $\mathrm{End}^0(A)$ is a field of degree 4 over $\mathbb{Q}$ by Claim 3.1, the minimal polynomials of the elements in $\mathrm{End}^0(A)$ over $\mathbb{Q}$ must have degree either 1, 2, or 4. However, $\pi_{A_n} = \pi_A^n \in \mathrm{End}^0(A)$, so this contradicts the result of Claim 3.3. Hence, we conclude that Case 3 cannot occur either.

Since Cases 1, 2 and 3 cannot occur, we conclude that the only possibility is $A_n = A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \sim E^2$ where $E/\mathbb{F}_{q^n}$ is ordinary. Note that this implies that A is ordinary.

(b) Since A is ordinary by part (a), it follows from Lemma 5 that $h_A(X)$ is irreducible and that $K := \mathrm{End}^0(A) \simeq \mathbb{Q}[X]/(h_A(X))$ is a CM-field of degree 4. Thus, K contains the real quadratic subfield $K_0 = \mathbb{Q}(\sqrt{\Delta_A})$; cf. Corollary 7.

Put $A_n := A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$. Since $\pi_{A_n} = \pi_A^n$ and $A_n \sim E^2$ by part (a), it follows that

$$h_{A_n}(X) = (X - \alpha_1^n)(X - \alpha_2^n)\left(X - \frac{q^n}{\alpha_1^n}\right)\left(X - \frac{q^n}{\alpha_2^n}\right) = h_E(X)^2, \tag{7}$$

where $h_E(X)$ is the characteristic polynomial of $E/\mathbb{F}_{q^n}$. Thus, α_1^n is a root of $h_E(X)$, and so $K_E := \mathbb{Q}(\alpha_1^n)$ is an imaginary quadratic field because K_E is the splitting field of $h_E(X)$ where E is ordinary. But $K_E \subset \mathbb{Q}(\alpha_1) \simeq K$, so K has two distinct quadratic subfields. Since $[K : \mathbb{Q}] = 4$, we see that $K = K_0 K_E$, and so $K/\mathbb{Q}$ is a biquadratic field, as claimed.

(c) From (7) and the fact that $\alpha_i^n \neq \frac{q^n}{\alpha_i}$ for $i = 1, 2$ (cf. Corollary 4), we see that either $\alpha_1^n = \alpha_2^n$ or that $\alpha_1^n = \frac{q^n}{\alpha_2^n}$. Thus, after renaming $\frac{q}{\alpha_2}$ as α_2 if necessary, we may assume that $\alpha_1^n = \alpha_2^n$. Thus, $\alpha_1 = \zeta_n \alpha_2$, for some nth root of unity.

Now if $n \in \mathbb{N}$ is the minimal value such that A_n splits, then ζ_n is a *primitive* nth root. To see this, suppose that $\zeta_n^d = 1$ for some $d|n$ and $d \neq n$. Then $\alpha_1^d = \alpha_2^d$, so by the first equation of (7) (with n replaced by d) we see that h_{A_d} has repeated roots, and so A_d cannot be simple by Lemma 5. This contradicts the minimality of n, and so ζ_n is a primtive nth root.

By part (b) we know that $K/\mathbb{Q}$ is abelian. If $\eta \in \mathrm{Gal}(K/\mathbb{Q})$ denotes the automorphism induced by complex conjugation, then its fixed field is $K^\eta = K_0$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be the unique automorphism such that $\sigma(\alpha_1) = \alpha_2$. Then $\sigma(\alpha_1^n) = \alpha_2^n = \alpha_1^n$, so $K_E = K^\sigma$, and hence the third quadratic subfield is $K^{\sigma\eta}$. Now $\zeta_n = \frac{\alpha_1}{\alpha_2} \in K^{\sigma\eta}$ because $\eta(\frac{\alpha_1}{\alpha_2}) = \frac{q/\alpha_1}{q/\alpha_2} = \frac{\alpha_2}{\alpha_1} = \sigma(\frac{\alpha_1}{\alpha_2})$. Thus $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq [K^{\sigma\eta} : \mathbb{Q}] = 2$, and this implies that $n = 2, 3, 4$ or 6, as claimed.

Remark 9. If $A/\mathbb{F}_q$ is as in Theorem 3, then by part (b) we know that the quartic field $K = \mathbb{Q}[X]/(h_A(X))$ has three quadratic subfields. As was mentioned in the above proof, one is the real quadratic field $K_0 = K^\eta$, where $\eta \in \mathrm{Gal}(K/\mathbb{Q})$ denotes complex conjugation, and the other is the imaginary quadratic subfield $K_E = \mathrm{End}^0(E) = \mathbb{Q}(\sqrt{\mathrm{tr}_E^2 - 4q^n})$, the splitting field of $h_E(X)$. In terms of the roots α_1, α_2 of $h_A(X)$ (which were chosen such that $\alpha_1 = \zeta_n\alpha_2$, for some primitive nth root of unity $\zeta_n \in \mathbb{C}$), we have

$$K_E = \mathbb{Q}(\alpha_1^n) = K^\sigma \quad \text{and} \quad K_0 = \mathbb{Q}\left(\alpha_1 + \tfrac{q}{\alpha_1}\right) = \mathbb{Q}\left(\alpha_2 + \tfrac{q}{\alpha_2}\right) = \mathbb{Q}(\sqrt{\Delta_A}) = K^\eta, \tag{8}$$

where $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ satisfies $\sigma(\alpha_1) = \alpha_2$ and Δ_A is as in Corollary 7. Moreover, from the proof of Theorem 3(c) we see that if $n \neq 2$, then the third subfield of K is

$$K^{\sigma\eta} = \mathbb{Q}(\zeta_n), \quad \text{provided that } n \neq 2.$$

From this we see that if $n = 3$ or $n = 6$, then we must have that $K_E \neq \mathbb{Q}(\zeta_3)$, or equivalently, that E is not isogenous to any curve E_0 with $j(E_0) = 0$. Similarly, if $n = 4$, then we must have that $K_E \neq \mathbb{Q}(i)$, or equivalently, that E is not isogenous to any curve E_0' with $j(E_0') = 1728$.

We now investigate the structure of the characteristic polynomials $h_A(X)$ of a simple, geometrically split abelian surface $A/\mathbb{F}_q$ in more detail. For this we shall make use of the following result which will also be needed in the next section.

Proposition 10. *If $h(X)$ is a quartic polynomial of the form*

$$h(X) \;=\; X^4 - tX^3 + sX^2 - tqX + q^2 \tag{9}$$

where $s, t, q \in \mathbb{Z}$ and $q \neq 0$, then there are $\alpha_1, \alpha_2 \in \mathbb{C}$ such that

$$h(X) = (X - \alpha_1)(X - \alpha_2)\left(X - \frac{q}{\alpha_1}\right)\left(X - \frac{q}{\alpha_2}\right). \tag{10}$$

Furthermore, let $n \geq 1$ and put

$$h_{(n)}(X) := (X-\alpha_1^n)(X-\alpha_2^n)\left(X-\frac{q^n}{\alpha_1^n}\right)\left(X-\frac{q^n}{\alpha_2^n}\right). \tag{11}$$

Then we have

$$h_{(n)}(X) = X^4 - t_nX^3 + s_nX^2 - t_nq^nX + q^{2n} \tag{12}$$

where $t_n = \alpha_1^n + \alpha_2^n + \frac{q^n}{\alpha_1^n} + \frac{q^n}{\alpha_2^n}$ and $s_n = \frac{1}{2}(t_n^2 - t_{2n})$ are integers. Thus, if we put

$$r_n := t^2 - n(s-(n-2)q) \quad \textit{and} \quad \Delta_n := t_n^2 - 4s_n + 8q^n, \tag{13}$$

then we have

$$\begin{array}{rclclcrcl} t_2 & = & r_2 & = & t^2 - 2s, & & s_2 & = & s^2 - 2t^2q + 2q^2 \\ t_3 & = & r_3t & = & t^3 - 3st + 3tq, & & s_3 & = & s^3 - 3q^2s - 3qt^2s + 6q^2t^2, \end{array} \tag{14}$$

and hence

$$\Delta_2 = t^2\Delta_1 = r_0\Delta_1, \quad \Delta_3 = r_1^2\Delta_1, \quad \Delta_4 = r_0r_2^2\Delta_1, \quad \textit{and} \quad \Delta_6 = r_0r_1^2r_3^2\Delta_1. \tag{15}$$

Remark 11. If $A/\mathbb{F}_q$ is an abelian surface, then by Remark 6 we know that its characteristic polynomial $h_A(X)$ has the form (9), and so it follows as in the proof of Theorem 3(a) that the characteristic polynomial of $A_n := A \otimes \mathbb{F}_{q^n}$ is

$$h_{A_n}(X) = (h_A)_{(n)}(X) \quad \text{and that hence} \quad \Delta_{A_n} = \Delta_n. \tag{16}$$

Thus, the above proposition describes in particular how the coefficients of $h_{A_n}(X)$ are related to those of $h_A(X)$ and hence contains Lemma 2.13 of [7] (which is stated there without proof). Note that this more general version of Proposition 10 is needed in the the proof of Proposition 15.

Proof of Proposition 10. We first note that $h(X)$ satisfies the functional equation

$$X^4h\left(\frac{q}{X}\right) = q^2h(X) \tag{17}$$

because $X^4h\left(\frac{q}{X}\right) = q^4 - tq^3X + sq^2X^2 - tq(qX^3) + q^2X^4 = q^2h(X)$. Thus, if a is a root of $h(X)$, then so is $\frac{q}{a}$. (Note that $a \neq 0$ because $q \neq 0$.) To verify that (10) holds, let α_1 be a root of $h(X)$. Suppose first that $\alpha_1 \neq \frac{q}{\alpha_1}$. Then $g_1(X) := (X-\alpha_1)(X-\frac{q}{\alpha_1})|h(X)$, so $h(X) = g_1(X)g_2(X)$. Since $X^2g_1(\frac{q}{X}) = qg_1(X)$, it follows from (17) that $g_2(X)$ has the same property, and so $g_2(X) = (x-\alpha_2)(X-\frac{q}{\alpha_2})$, where a_2 is a root of $g_2(X)$. Thus (10) holds in this case.

We are left with the case that $\alpha_i = \frac{q}{\alpha_i}$ for all roots α_i of $h(X)$. Thus $\alpha_i^2 = q$, so we have at most two distinct roots. If all roots are the same, then clearly (10) holds with $\alpha_1 = \alpha_2$, so assume that $\alpha_1 \neq \alpha_2$. Then $\alpha_2 = -\alpha_1$, so $h(X) = (x-\alpha_1)^{m_1}(X+\alpha_1)^{m_2}$, which has constant term $(-1)^{m_1}\alpha_1^4 = (-1)^{m_1}q^2$. Since $h(0) = q^2$, we see that m_1 is even and hence $m_1 = m_2 = 2$, and so $h(X) = (x-\alpha_1)^2(x+\alpha_1)^2$. Thus (10) holds in this case as well.

To show that equation (12) holds, write $\alpha_3 := \frac{q}{\alpha_1}$ and $\alpha_4 := \frac{q}{\alpha_2}$, and put

$$\begin{aligned} t_n &:= \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n \\ s'_n &:= \alpha_1^n\alpha_2^n + \alpha_1^n\alpha_3^n + \alpha_1^n\alpha_4^n + \alpha_2^n\alpha_3^n + \alpha_2^n\alpha_4^n + \alpha_3^n\alpha_4^n \\ t'_n &:= \alpha_1^n\alpha_2^n\alpha_3^n + \alpha_1^n\alpha_2^n\alpha_4^n + \alpha_1^n\alpha_3^n\alpha_4^n + \alpha_2^n\alpha_3^n\alpha_4^n. \end{aligned}$$

Expanding the right hand side of (11), we see that the coefficients of X^3, X^2, and X are $-t_n$, s'_n and $-t'_n$, respectively. Since $t_n^2 - t_{2n} = (\alpha_1^n + \ldots + \alpha_4^n)^2 - (\alpha_1^{2n} + \ldots + \alpha_4^{2n}) = 2(\alpha_1^n\alpha_2^n + \alpha_1^n\alpha_3^n + \alpha_1^n\alpha_4^n + \alpha_2^n\alpha_3^n + \alpha_2^n\alpha_4^n + \alpha_3^n\alpha_4^n) = 2s'_n$, we have that $s_n = s'_n$. Moreover, since $\alpha_1\alpha_3 = \alpha_2\alpha_4 = q$, we see that $t'_n = q^n\alpha_2^n + \alpha_1^n q^n + q^n\alpha_4^n + q^n\alpha_3^n = q^n t_n$, and so (12) holds because $h_{(n)}(X)$ is clearly monic with constant term q^{2n}.

Note that Newton's recursive formulae (cf. [2], page 161) show that t_n and s_n can be expressed in terms of polynomials in s, t, and q^2, for we have

$$t_n = -nc_n - (c_1 t_{n-1} + \ldots + c_{n-1}t_1), \tag{18}$$

where $c_1 := -t$, $c_2 := s$, $c_3 := -tq$, $c_4 = q^2$ and $c_n = 0$ if $n > 4$. Hence, since $s, t, q^2 \in \mathbb{Z}$, it follows that $t_n \in \mathbb{Z}$ for $n \geq 1$ and that $s_n \in \mathbb{Q}$. Since $s_n = s'_n \in \mathbb{Q}$ is also an algebraic integer (because the α_i's are algebraic integers), we see that $s_n \in \mathbb{Z}$.

From (18) we have that $t_2 = -2c_2 - c_1t_1 = t^2 - 2s = r_2$, and similarly one obtains that

$$\begin{aligned} t_3 &= t^3 + 3tq - 3st \;=\; t(t^2 - 3(s+q)) \;=\; tr_3 \\ t_4 &= -4q^2 + s^4 + 4s^2q - 4ts^2 + 2t^2 \\ t_5 &= -5sq^2 + s^5 + 5s^3q - 5s^3q - 5ts^3 + 5st^2 - 5stq \\ t_6 &= -3s^2q^2 + s^6 + 6s^4q - 6ts^4 + 9t^2s^2 + 6tq^2 - 2t^3 - 12s^2tq. \end{aligned} \tag{19}$$

From these it follows that $s_2 = \frac{1}{2}(t_2^2 - t_4) = \frac{1}{2}((t^2-2s)^2 + 4q^2 - t^4 - 4t^2q + 4st^2 - 2s^2) = s^2 - 2t^2q + 2q^2$, and similarly $s_3 = \frac{1}{2}(t_3^2 - t_6) = s^3 - 3q^2s - 3qt^2s + 6q^2t^2$, as claimed.

Substituting the above expressions for t_2 and s_2 in Δ_2 yields $\Delta_2 = (t^2-2s)^2 - 4(s^2 - 2t^2q + 2q^2) + 8q^2 = t^2(t^2 - 4s + 8q) = t^2\Delta_1 = r_0\Delta_1$, and similarly $\Delta_3 = r_1^2\Delta_1$. Now since $h_{(4)}(X) = (h_{(2)})_{(2)}(X)$, it follows from what was just proved that $\Delta_4 = t_2^2\Delta_2 = r_2^2\Delta_2 = r_2^2r_0\Delta_1$. Similarly, since $h_{(6)}(X) = (h_{(3)})_{(2)}(X)$, we have $\Delta_6 = t_3^2\Delta_3 = t^2r_3^2\Delta_3 = r_0r_3^2r_1^2\Delta_1$, which proves (15).

The following result characterizes the simple, geometrically split abelian surfaces $A/\mathbb{F}_q$ in terms of relations satisfied by the coefficients tr_A and s_A of the characteristic polynomial $h_A(X)$. Except for its compact formulation, this result is originally due to Howe and Zhu[6].

Theorem 12. *Let $\mathbb{A}/\mathbb{F}_q$ be a simple ordinary abelian surface. Then A is not absolutely simple if and only if there exists an integer $c \in \mathbb{Z}$ such that*

$$\mathrm{tr}_A^2 = c(s_A + cq - 2q) \quad \textit{and} \quad 0 \le c \le 3. \tag{20}$$

Proof. Suppose first that (20) holds, i.e. that $r_c = 0$ in the notation (13) (with $t = \mathrm{tr}_A$ and $s = s_A$) for some $c \in \{0, 1, 2, 3\}$. Then by (15) and (16) we have that $\Delta_{A_n} = \Delta_n = 0$ for some $n \in \{2, 3, 4, 6\}$, and hence A_n is split by Corollary 7.

Conversely, suppose that A_n is split, and assume that n is minimal with this property. Then by Theorem 3 we have that $n \in \{2, 3, 4, 6\}$ and that $A_n \sim E^2$, for some elliptic curve $E/\mathbb{F}_{q^n}$. By (5) we thus have that $\Delta_{A_n} = 0$, and so from (15) we see that $r_c = 0$ for some $c \in \mathbb{Z}$ with $0 \le c \le 3$, and so (20) holds.

By combining Theorem 3 with Theorem 12 we obtain the following result.

Corollary 13. *Let $A/\mathbb{F}_q$ be a simple abelian surface. Then A is absolutely simple if and only if A is either non-ordinary and non-supersingular or A is ordinary and relation* (20) *does not hold for A.*

Proof. Suppose first that A is absolutely simple. Then A cannot be supersingular (because then $A \otimes \overline{\mathbb{F}}_q \sim \overline{E}^2$, where $\overline{E}$ is supersingular), so either A is non-ordinary and non-supersingular or A is ordinary and condition (20) does not hold by Theorem 12. Conversely, if A non-ordinary and non-supersingular, then A is absolutely simple by Theorem 3(a), and if A is ordinary and (20) does not hold, then A is absolutely simple by Theorem 12.

Proof of Theorem 1. The first assertion is contained in Corollary 13. By Theorem 3 we know that if A_n is (minimally) split, then $A_n \sim E_n^2$ for $n \in \{2, 3, 4, 6\}$ and some elliptic curve $E_n/\mathbb{F}_{q^n}$, and by the proof of Theorem 12 we know that n is related to c as stated in Theorem 1.

For later reference, we note that we have also proved the following result.

Corollary 14. *In the situation of* Theorem 1, *the isogeny class of $E = E^{(n)}/\mathbb{F}_{q^n}$ is determined by the formula*

$$-\mathrm{tr}_{E^{(n)}} = \begin{cases} s_A, & \textit{if } n = 2 \\ \mathrm{tr}_A^3 - 3q\,\mathrm{tr}_A, & \textit{if } n = 3 \\ (\frac{\mathrm{tr}_A^2}{2} - 2q)^2 - 2q^2, & \textit{if } n = 4 \\ (\frac{\mathrm{tr}_A^2}{3} - 2q)^3 - 3q^2(\frac{\mathrm{tr}_A^2}{3} - 2q), & \textit{if } n = 6. \end{cases} \tag{21}$$

Proof. From (5) and Remark 11 we know that $2\,\mathrm{tr}_{E^{(n)}} = \mathrm{tr}_{A_n} = t_n$, where t_n is as in Proposition 10. If $n=2$, then $2\,\mathrm{tr}_{E^{(2)}} = t_2 = t^2-2s = -2s$ by (14) and (20) (with $c=0$), so (21) holds for $n=2$. Similarly, for $n=3$ we obtain by from (14) and (20) (with $c=1$) that $2\,\mathrm{tr}_{E^{(3)}} = t_3 = t(t^2+3q-3s) = t(t^2+3q-3(t^2-q)) = t(6q-2t^2)$, and so (21) holds for $n=3$. The cases $n=4$ and 6 are proved similarly by using (19) in place of (14).

3 Existence theorems

In the previous section we had classified the simple ordinary abelian surfaces $A/\mathbb{F}_q$ which are geometrically split in terms of the relation (20) satisfied by $h_A(X)$. We now refine this by determining precisely which polynomials $h(X)$ of the form (9) actually belong to an abelian surface of this type. For this, we first prove the following result.

Proposition 15. *For $n \in \{2,3,4,6\}$, define s, t, u_n by the following rules. If $n=2$, then put*

$$t = 0, \quad u_2 = s, \quad \text{where } s\in\mathbb{Z} \text{ is arbitrary,} \tag{22}$$

and if $n = 3$, 4 or 6, then let $t\in\mathbb{Z}$ be arbitrary and define s and u_n by

$$s = \frac{t^2}{c}+(c-2)q \quad \text{and} \quad u_n = T_n^{\frac{n}{k}} - \frac{n}{k}q^kT_n^{\frac{n}{k}-2}, \quad \text{where } T_n = \frac{t^k}{c}-2(k-1)q, \tag{23}$$

and where $c = \left[\frac{n}{2}\right]$ and $k = [\frac{n+2}{3}]$, i.e. s and u_n are given by the following table:

(24)

n	s	u_n
3	t^2-q	t^3-3qt
4	$\frac{t^2}{2}$	$\frac{1}{4}t^4-2qt^2+2q^2$
6	$\frac{t^2}{3}+q$	$\frac{1}{27}t^6-\frac{2}{3}qt^4+3q^2t^2-2q^3.$

Then there exists an ordinary abelian surface $A/\mathbb{F}_q$ such that

$$\mathrm{tr}_A = t, \quad s_A = s \quad \text{and} \quad A\otimes\mathbb{F}_{q^n}\sim E^2, \tag{25}$$

for some elliptic curve $E/\mathbb{F}_{q^n}$, if and only if

$$s\in\mathbb{Z}, \quad |u_n|\le 2\sqrt{q^n} \quad \text{and} \quad \gcd(u_n,q)=1. \tag{26}$$

If this is the case, then $\mathrm{tr}_E = -u_n$ and A is simple if and only if $\Delta_A = t^2-4s+8q = (4-c)(4q-\frac{t^2}{c})$ is not a square in $\mathbb{Z}$.

Proof. Let s and t be as in (22) and (23). Define $h(X)$ by (9), and let t_n and s_n be defined as in Proposition 10. We then claim that we have that

(27) $-2u_n = t_n,\ u_n^2+2q^n = s_n,$ or, equivalently, that $h_{(n)}(X) = (X^2+u_nX+q^n)^2$.

To verify this, suppose first that $n = 2$. Substituting $t = 0$ and $s = u_2$ into the formulae (14) for t_2 and s_2 yields $t_2 = (0)^2 - 2u_2 = -2u_2$ and $s_2 = u_2^2 - 2(0)^2q + 2q^2 = u_2^2 + 2q^2$, and so (27) holds for $n = 2$. Thus we have shown:

$$h(X) = X^4 + uX^2 + q^2 \quad \Rightarrow \quad h_{(2)}(X) = (X^2 + uX + q^2)^2. \tag{28}$$

Similarly, if $n = 3$, then we substitute t and $s = t^2 - q$ into the formulae (14) of s_3, t_3 to get $t_3 = t^3 - 3(t^2 - q)t + 3tq = -2u_3$ and $s_3 = (t^2 - q)^3 - 3q^2(t^2 - q) - 3qt^2(t^2 - q) + 6q^2t^2 = (t^3 - 3tq)^2 + 2q^3 = u_3^2 + 2q^3$, which verifies (27) for $n = 3$.

If $n = 4$, then we substitute t and $s = \frac{t^2}{2}$ into the formulae (14) of t_2 and s_2 to obtain $t_2 = t^2 - 2\left(\frac{t^2}{2}\right) = 0$ and $s_2 = \frac{t^4}{4} - 2t^2q + 2q^2 = u_4$, so $h_{(2)}(X) = X^4 + u_4X^2 + q^4$. Thus, by (28) applied to $h_{(2)}(X)$ in place of $h(X)$ (and q^2 in place of q), we see that $h_{(4)}(X) = (h_{(2)})_{(2)}(X) = (X^2 + u_4X + q^4)^2$, and so (27) holds for $n = 4$.

Finally, if $n = 6$, then $s = \frac{t^2}{3} + q$ and so by the formulae (14) for t_3 and s_3 we obtain $t_3 = t^3 - 3\left(\frac{t^2}{3} + q\right)t + 3tq = 0$ and $s_3 = \left(\frac{t^2}{3} + q\right)^3 - 3q^2\left(\frac{t^2}{3} + q\right) - 3qt^2\left(\frac{t^2}{3} + q\right) + 6q^2t^2 = \frac{1}{27}t^6 - \frac{2}{3}t^4q + 3q^2t^2 - 2q^3 = u_6$. Thus, applying (28) to $h_{(3)}(X)$ (in place of $h(X)$), we obtain that $h_{(6)}(X) = (h_{(3)})_{(2)}(X) = (X^2 + u_6 + q^6)^2$, and so (27) holds for $n = 6$. This proves (27) in all cases.

We next prove the equivalence of conditions (25) and (26). Suppose first that $A/\mathbb{F}_q$ and $E/\mathbb{F}_{q^n}$ satisfying (25) exist. Since $h(X) = h_A(X) \in \mathbb{Z}[X]$, it follows that $t \in \mathbb{Z}$. Moreover, since $A_n \sim E^2$, we know by Remark 11 that $h_{(n)}(X) = h_{A_n}(X) = h_E(X)^2$. Comparing this to (27), we see that $h_E(X) = X^2 + u_nX + q^n$ and so $\mathrm{tr}_E = -u_n$. Thus, by Hasse's bound we have $|u_n| \le 2\sqrt{q^n}$. Moreover, since A and hence E are ordinary, we have that $(u_n, q^n) = 1$. Thus (26) holds.

Conversely, suppose that (26) holds. Then $u_n^2 - 4q^n < 0$, so the roots of $f(X) := X^2 + u_nX + q^n$ are complex conjugates of each other and hence both have absolute value $q^{n/2}$. From this it follows that $h(X)$ is a q-Weil polynomial, i.e. that $h(X) \in \mathbb{Z}[X]$ and that $|\alpha_i| = \sqrt{q}$ for all roots α_i of $h(X)$. Indeed, since $s, t \in \mathbb{Z}$, we see that $h(X) \in \mathbb{Z}[X]$. Moreover, if $\alpha_i \in \mathbb{C}$ is a root of $h(X)$, then by definition and (27) we know that α_i^n is a root of $h_{(n)}(X) = f(X)^2$, and hence it is also a root of $f(X)$. Thus, $|\alpha_i^n| = q^{n/2}$ and so $|\alpha_i| = \sqrt{q}$. Thus, $h(X)$ is a q-Weil polynomial.

Moreover, $h(X)$ is also an ordinary q-Weil polynomial in the sense of [5], i.e. $(s, q) = 1$. Indeed, for $n = 2$ this is clear from (26) because $s = u_2$. For $n \neq 2$ we see that the formulae for u_n imply that $(t, q) = 1$ and hence also that $(s, q) = 1$. Thus, $h(X)$ is an ordinary q-Weil polynomial, and so by the Honda-Tate theorem (Theorem 3.3. of [5]), there exists an ordinary abelian surface $A/\mathbb{F}_q$ such that $h_A(X) = h(X)$.

Moreover, it follows from (27) that $A_n = A\otimes\mathbb{F}_{q^n}$ splits because by Remark 11 we have that $h_{A_n}(X) = (h_A)_{(n)}(X) = h_{(n)}(X) = f(X)^2$ is not irreducible. Thus $A_n \sim E^2$, where $h_E(X) = f(X)$.

This proves the equivalence of conditions (25) and (26) and the fact that $\mathrm{tr}_E = -u_n$. The last assertion follows directly from Corollary 7.

We will now use the above proposition to prove the *Existence Theorem* (Theorem 2) stated in the introduction. For this, we first observe the following simple fact.

Lemma 16. *Let $a, b \in \mathbb{R}$ with $b \geq 0$. Then we have*

$$(29) \qquad (a^2-2b)^2 \;\leq\; 4b^2 \quad\Leftrightarrow\quad a^2 \;\leq\; 4b \quad\Leftrightarrow\quad (a^3-3ab)^2 \;\leq\; 4b^3.$$

Proof. Since $(a^2-2b)^2 - 4b^2 = a^2(a^2-4b)$, the first assertion is clear if $a \neq 0$. But if $a = 0$, then the first two inequalities are trivially true, so the first assertion holds.

Similarly, since $(a^3-3ab)^2 - 4b^3 = (a^2-4b)(a^2-b)^2$, the second equivalence is clear if $a^2 \neq b$. But if $a^2 = b$, then the last two inequalities hold, and so (29) follows.

Corollary 17. *In the situation of* Proposition 15 *suppose that $n \neq 2$. Then*

$$(30) \qquad |u_n| \;\leq\; 2\sqrt{q^n} \quad\Leftrightarrow\quad T_n^2 \;\leq\; 4q^k \quad\Leftrightarrow\quad t^2 \;\leq\; 4cq.$$

Proof. If $n = 3$, then $c = 1$, $k = 1$ and $u_3 = T_3^3 - 3qT_3$, so (30) follows from the second equivalence of (29) by taking $a = T_3 = t$ and $b = q$.

If $n = 4$, then $u_4 = T_4^2 - 2q^2$, so the first equivalence of (30) follows from the first equivalence of (29) by taking $a = T_4$ and $b = q^2 = q^k$. Moreover, since $T_4 = \frac{t^2}{2} - 2q$, we see that $T_4^2 \leq 4q^2 \Leftrightarrow \frac{t^4}{4} - 2qt^2 \leq 0 \Leftrightarrow t^2 \leq 8q = 4cq$, and so (30) holds for $n = 4$.

Finally, if $n = 6$, then $u_6 = T_6^2 - 3q^2T_6$, so the first equivalence of (30) follows from the second equivalence of (29) by taking $a = T_6$ and $b = q^2 = q^k$. Moreover, since $T_6 = \frac{t^2}{3} - 2q$, we see that $T^6 \leq 4q^2 \Leftrightarrow \frac{t^4}{9} - \frac{4}{3}qt^2 \leq 0 \Leftrightarrow t^2 \leq 12q = 4cq$, which proves (30).

Proof of Theorem 2. (a) If $A/\mathbb{F}_q$ is simple and ordinary but $A \otimes \mathbb{F}_{q^2}$ splits, then $\mathrm{tr}_A = 0$ by Theorem 1, and so it follows from Proposition 15 that $|s_A| = |u_2| \leq 2q$ and that $\Delta_A = 8q - 4s_A$ is not square, and hence (2) holds. Conversely, if (2) holds, then it follows from Proposition 15 that there is a simple, ordinary abelian surface $A/\mathbb{F}_q$ with $s_A = s$ such that $A \otimes \mathbb{F}_{q^2}$ splits.

(b) We first observe that condition (3) is equivalent to condition (26) together with the condition that $\Delta = t^2 - 4s + 8q \notin \mathbb{Z}^2$ (when $s = \frac{t^2}{c} + (c-2)q$). Indeed, by (30) we know that $t^2 \leq 4cq \Leftrightarrow |u_n| \leq 2\sqrt{q^n}$, and clearly $s \in \mathbb{Z} \Leftrightarrow c|t^2 \Leftrightarrow c|t$ (because $c = 1, 2$ or 3). Moreover, under the hypothesis that $c|t$, it is clear from (24) that $(u_n, q) = 1 \Leftrightarrow (t, q) = 1$. Finally, we show that $\Delta \in \mathbb{Z}^2 \Leftrightarrow \exists x \in \mathbb{Z} : 4cq - t^2 = \varepsilon x^2$ by distinguishing cases: (i) if $n = 3$, then $\Delta = 12q - 3t^2$, so $\Delta \in \mathbb{Z}^2 \Leftrightarrow \exists x \in \mathbb{Z}$

with $12q-3t^2=(3x)^2 \Leftrightarrow 4q-t^2=3x^2=\varepsilon x^2$; (ii) if $n=4$, then $\Delta=8q-t^2$, so $\Delta \in \mathbb{Z}^2 \Leftrightarrow \exists x \in \mathbb{Z}$ with $8q-t^2=x^2=\varepsilon x^2$; (iii) if $n=6$, then $\Delta=4q-\frac{t^2}{3}$ (and $3|t$), so $\Delta \in \mathbb{Z}^2 \Leftrightarrow \exists x \in \mathbb{Z}$ with $12q-t^2=3x^2=\varepsilon x^2$.

From this observation we see that if (3) holds, then it follows from Proposition 15 that there is a simple, ordinary abelian surface $A/\mathbb{F}_q$ with $\mathrm{tr}_A=t$ such that $A\otimes\mathbb{F}_{q^n}$ splits (and $A\otimes\mathbb{F}_{q^m}$ is simple, for all $m|n$, $m\neq n$). Conversely, suppose that there is an abelian surface $A/\mathbb{F}_q$ with these properties. Then by Theorem 1 we know that (1) holds with $c=n-2$ for $n=3,4$ and $c=3$ for $n=6$ or, equivalently, for $c=[\frac{n}{2}]$, for $n=3,4$ or 6. Thus $s_A=\frac{\mathrm{tr}_A^2}{c}+(c-2)q$, and so it follows that condition (24) holds. By Proposition 15 this means that (25) holds and that $\Delta_A\notin\mathbb{Z}^2$, and by the above observation we obtain that (3) holds, as claimed.

(c) If $A/\mathbb{F}_q$ is such an abelian surface, then by Theorem 1 there is an integer c with $0\leq c\leq 3$ such that (1) holds. Thus $A\otimes\mathbb{F}_{q^n}$ splits minimally for $n=c+2$, if $c<3$ and for $n=6$, if $c=3$. If $c=0$, then we are in the situation of part (a), and if $c>0$, then $c=[\frac{n}{2}]$ and so we are in the situation of part (b).

We can use Theorem 2 to prove the following existence result.

Proposition 18. *Let $n\in\{2,3,4,6\}$ and suppose that $n\neq 4$ if $q=2^r$ and that $n\neq 6$ if $q=3^r$ or $q=7$. Then there exists a simple ordinary abelian surface $A/\mathbb{F}_q$ such that $A\otimes\mathbb{F}_{q^n}$ is* minimally split, *i.e. $A\otimes\mathbb{F}_{q^n}$ is split, but $A\otimes\mathbb{F}_{q^m}$ is simple, for all $m|n$, $m\neq n$.*

Proof. Here we shall use repeatedly the following obvious fact:

$$x_1>x_2>0,\ x_i\in\mathbb{Z} \quad\Rightarrow\quad x_1^2-x_2^2 \ \geq\ 2x_2+1\ \geq\ 3. \tag{31}$$

From this we see that at least one of $s=\pm1$ satisfies (2), for if $2q+1=x_1^2$ and $2q-1=x_2^2$ are both square, then $2=x_1^2-x_2^2$, which contradicts (31). Thus, by Theorem 2(a), there is a simple, ordinary abelian surface $A/\mathbb{F}_q$ with $s_A\in\{\pm1\}$ such that $A\otimes\mathbb{F}_{q^n}$ splits, and hence the assertion is true for $n=2$.

Now suppose that $n>2$. Then by Theorem 2(b) it is enough to find a $t\in\mathbb{Z}$ satisfying condition (3). For this, we distinguish the following cases.

Suppose first that $n=3$. If $q=2^r$, then every odd t with $t^2\leq 4q$ satisfies (3) because $4q-t^2\equiv -1 \pmod 8$, whereas $3x^2\equiv 3 \pmod 8$, if x is odd, so $4q-t^2\neq 3x^2$, $\forall x\in\mathbb{Z}$. On the other hand, if $q\neq 2^r$, then at least one $t\in\{1,2\}$ satisfies (3), for otherwise there exist $x_1>x_2>0$ such that $4q-1=3x_1^2$ and $4q-4=3x_2^2$, and then $3=3(x_1^2-x_2^2)$, which contradicts (31).

Next suppose that $n=4$, so q is odd by hypothesis. Here at least one $t\in\{2,4\}$ satisfies (3), for otherwise there exist integers $x_1>x_2>0$ such that $8q-4=(2x_1)^2$ and $8q-16=(2x_2)^2$, and then $3=x_1^2-x_2^2\geq 2x_2+1$ by (31), so $x_2=1$ and $8q=20$, contradiction.

Finally, suppose that $n = 6$, so $q \neq 3^r, 7$ by hypothesis. If $q = 2^r$ or $q \equiv 2 \pmod 3$, then every $t = \pm 3t_1$ with $t^2 \leq 12q$ and $(t, q) = 1$ satisfies (3). Indeed, in the former case (i.e. if $q = 2^r$) we have $12q - t^2 \equiv -1 \pmod 8$, whereas $3x^2 \equiv 3 \pmod 8$, and in the latter case we have $4q - 3t_1^2 \equiv 2 \pmod 3$, whereas $x^2 \equiv 1 \pmod 3$. In particular, (3) holds for $t = \pm 3$ in these cases.

Now assume that $q \equiv 1 \pmod 3$ and that $q \neq 7$ is odd. Here at least one $t \in \{3, 6\}$ satisfies (3). If not, then there exist integers $x_1 > x_2 > 0$ such that $12q - 9 = 3x_1^2$ and $12q - 36 = 3x_2^2$, and then $18 = x_1^2 - x_2^2 \geq 2x_2 + 1$ by (31), so $x_2 \leq 8$ and $4q \leq 8^2 + 9$, or $q \leq 20$. Thus $q = 13$ or $q = 19$. But then (3) holds for $t = 6$ and $t = 3$, respectively, because $4 \cdot 13 - 12 = 40$ and $4 \cdot 19 - 3 = 73$ are non-squares.

Remark 19. (a) It is clear that the case $n = 4$ cannot occur if $q = 2^r$ because in this case there is no integer t such that $2|t$ and $(t, q) = 1$, and so there is no $t \in \mathbb{Z}$ which satisfies condition (3). Similarly, the case $n = 6$ cannot occur if $q = 3^r$. Finally, if $q = 7$, then the case $n = 6$ cannot not occur because $(12 \cdot 7 - (3t_1)^2)/3 \in \{7^2, 5^2, 1^2\}$ is a square for $t_1 = \pm 1, \pm 2, \pm 3$.

(b) Note that if q is large, then there are only very few exceptional t's which satisfy the first conditions of (3) but fail the last condition. Indeed, if $q = 2^r$, then then there are no exceptions (as the above proof of Proposition 18 showed), and if $q = p^r$ is odd, then the equations $2q = t_1^2 + t_2^2$ and $4q = t_1^2 + 3t_2^2$ have at most $4(r+1)$ and $6(r+1)$ integer solutions (t_1, t_2), respectively, and so there are at most $6(r+1)$ such exceptional t's.

It is useful to observe that condition (3) implies that there exists an elliptic curve $E_0/\mathbb{F}_{q^k}$ such that $E_0 \otimes_{\mathbb{F}_{q^k}} \mathbb{F}_{q^n} \sim E^\chi$, where E^χ denotes the (unique) nontrivial *quadratic twist* of $E = E_n$. This observation leads to the following "descent result".

Theorem 20. (a) *If $E/\mathbb{F}_{q^2}$ is an ordinary elliptic curve, then there exists an abelian surface $A/\mathbb{F}_q$ such that $A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2} \sim E^2$. Moreover, A is simple if and only if $2q + \mathrm{tr}_E$ is not a square or, equivalently, if $E_1 \otimes \mathbb{F}_{q^n} \not\sim E$, for any elliptic curve $E_1/\mathbb{F}_q$.*

(b) *Let $n = 3, 4$ or 6 and put $c = [\frac{n}{2}]$ and $k = [\frac{n+2}{3}]$. If $E/\mathbb{F}_{q^n}$ is an ordinary elliptic curve, then the following conditions are equivalent:*

(i) *There is an abelian surface $A/\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^n} \sim E^2$ such that $A \otimes \mathbb{F}_{q^m}$ is simple for all $m|n$, $m \neq n$;*

(ii) *there is an integer $t \in \mathbb{Z}$ such that $(4-c)(4q - \frac{t^2}{c})$ is not a square in $\mathbb{Z}$ and such that $-\mathrm{tr}_E = t_0^{\frac{n}{k}} - \frac{n}{k} q^k t_0^{\frac{n}{k}-2}$, where $t_0 = \frac{t^k}{c} - 2(k-1)q$.*

(iii) *there is an elliptic curve $E_0/\mathbb{F}_{q^k}$ with $E_0 \otimes \mathbb{F}_{q^n} \sim E^\chi$ and an integer $t \in \mathbb{Z}$ such that $\mathrm{tr}_{E_0} = \frac{t^k}{c} - 2(k-1)q$ but $(4-c)(4q - \frac{t^2}{c})$ is not a square in $\mathbb{Z}$.*

Proof. (a) Put $s = u_2 = -\mathrm{tr}_E$ and $t = 0$. Then $(u_2, q) = 1$ because E is ordinary and $|u_2| \leq 2\sqrt{q^2}$ by Hasse's bound. Thus (25) holds for $n = 2$ and so by Proposition 15 there is an abelian surface $A/\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^2} \sim E_2^2$ for some elliptic curve $E_2/\mathbb{F}_{q^2}$ with $\mathrm{tr}_{E_2} = -u_2$. Thus $\mathrm{tr}_{E_2} = \mathrm{tr}_E$, and hence $E_2 \sim E$ by Tate. By Corollary 7 we have that A is simple if and only if $\Delta_A = t^2 - 4s + 8q = 4(2q + \mathrm{tr}_E)$ is not a square. If this is the case, then $E \not\sim E_1 \otimes \mathbb{F}_{q^2}$, for otherwise $\mathrm{tr}_E = \mathrm{tr}_{E_1}^2 - 2q$. Conversely, if $2q + \mathrm{tr}_E = t_1^2$ is a square, then $t_1^2 \leq 2q + |\,\mathrm{tr}_E\,| \leq 4q$ (by Hasse's bound) and $(t_1^2, q) = (\mathrm{tr}_E, q) = 1$, so by the Tate-Honda Theorem ([11], Theorem 4.1(1)), there exists an elliptic curve $E_1/\mathbb{F}_q$ such that $\mathrm{tr}_{E_1} = t_1$, and then $\mathrm{tr}_{E_1 \otimes \mathbb{F}_{q^2}} = t_1^2 - 2q = \mathrm{tr}_E$, so $E_1 \otimes \mathbb{F}_{q^2} \sim E$ by Tate's Theorem.

(b) (i) $\Rightarrow$ (ii): Let $A/\mathbb{F}_q$ be given, and put $t = \mathrm{tr}_A$ and $s = s_A$. Then by Theorem 1 we know that $s = \frac{t^2}{c} + (c-2)q$ and by Corollary 14 we have $-\mathrm{tr}_E = t_0^{\frac{n}{k}} - \frac{n}{k} q^k t_0^{\frac{n}{k}-2}$, where $t_0 := \frac{t^k}{c} - 2(k-1)q$. Moreover, $\Delta_A = t^2 - 4s + 8q = (4-c)(4q - \frac{t^2}{c})$ is not a square by Corollary 7, so (ii) holds.

(ii) $\Rightarrow$ (iii): By hypothesis, $\mathrm{tr}_E = -u_n$ and $t_0 = T_n$ where u_n and T_n are as in (23). Thus, since $|\,\mathrm{tr}_E\,| \leq 2\sqrt{q^n}$ by Hasse's Theorem, we see that $t_0^2 = T_n^2 \leq 4q^k$ by (30). Moreover, $(t_0, q) = 1$, for otherwise $(\mathrm{tr}_E, q) > 1$, contradiction. It thus follows from the Tate-Honda Theorem ([11], Theorem 4.1(1)) that there is an elliptic curve $E_0/\mathbb{F}_{q^k}$ such that $\mathrm{tr}_{E_0} = t_0$. Since $\mathrm{tr}_{E_0 \otimes \mathbb{F}_{q^n}} = t_0^{\frac{n}{k}} - \frac{n}{k} q^k t_0^{\frac{n}{k}-2} = -\mathrm{tr}_E = \mathrm{tr}_{E^\chi}$, it follows by Tate that $E_0 \otimes \mathbb{F}_{q^n} \sim E^\chi$, and so (iii) follows.

(iii) $\Rightarrow$ (i): Put $t_0 = \mathrm{tr}_{E_0}$, so by hypothesis there is a $t \in \mathbb{Z}$ such that $t_0 = \frac{t^k}{c} - 2(k-1)q$. Moreover, since $E_0 \otimes \mathbb{F}_{q^n} \sim E^\chi$, we have $t_0^{\frac{n}{k}} - \frac{n}{k} q^k t_0^{\frac{n}{k}-2} = \mathrm{tr}_{E^\chi} = -\mathrm{tr}_E$, and so we have $\mathrm{tr}_E = -u_n$, where u_n is as defined in (23). By Hasse's bound we thus have $|u_n| = |\,\mathrm{tr}_E\,| \leq 2\sqrt{q^n}$, and so (26) holds. Thus, by Proposition 15 there is an abelian surface $A/\mathbb{F}_q$ and an elliptic curve $E_1/\mathbb{F}_{q^n}$ with $A \otimes \mathbb{F}_{q^n} \sim E_1^2$ such that $\mathrm{tr}_A = t$, $s_A = \frac{t^2}{c} + (c-2)q$. Moreover, since $\mathrm{tr}_{E_1} = -u_n = \mathrm{tr}_E$, we have that $E \sim E_1$ by Tate, and hence $A \otimes \mathbb{F}_{q^n} \sim E^2$. Furthermore, since $\Delta_A = (4-c)(4q - \frac{t^2}{c})$ is not a square by hypothesis, we also know that A is simple. Now since $s_A = \frac{t^2}{c} + (c-2)q$ and $t = \mathrm{tr}_A$, we see that (1) holds and so it follows from Theorem 1 that $A \otimes \mathbb{F}_{q^m}$ is simple, for all $m|n$ with $m \neq n$.

4 Connection with the Weil restriction

In order to further analyze the abelian surfaces whose existence is asserted in Theorem 20, we observe that there is a close connection between A and the *Weil restriction* $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ of E with respect to the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$.

Proposition 21. *Let $A/\mathbb{F}_q$ be an abelian surface with $A \otimes \mathbb{F}_{q^n} \sim E^2$, where $E/\mathbb{F}_{q^n}$ is an elliptic curve. If A is simple, then A is isogenous to a factor of* $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$. *Otherwise, A has a factor $E_1/\mathbb{F}_q$ with $E_1 \otimes \mathbb{F}_{q^n} \sim E$ which is isogenous to a factor of* $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$.

Proof. Recall (cf. [1]) that the Weil restriction satisfies the following universal property: for any abelian variety $B/\mathbb{F}_q$, there is an isomorphism (of abelian groups)

$$\mathrm{Hom}(B, \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)) \quad \xrightarrow{\sim} \quad \mathrm{Hom}(B \otimes \mathbb{F}_{q^n}, E). \tag{32}$$

Applying this to $B = A$ we see that $\mathrm{Hom}(A, R) \simeq \mathrm{Hom}(A \otimes \mathbb{F}_{q^n}, E)$, where $R := \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$. Since $A \otimes \mathbb{F}_{q^n} \sim E^2$, we have $\mathrm{Hom}(A \otimes \mathbb{F}_{q^n}, E) \otimes \mathbb{Q} \simeq \mathrm{Hom}(E^2, E) \otimes \mathbb{Q} \neq 0$. Thus $\mathrm{Hom}(A, R) \neq 0$ and so there exists a *non-zero* homomorphism $h : A \to R$.

If A is simple, then it follows that $\mathrm{Ker}(h)$ is finite, and so $h : A \to h(A)$ is an isogeny onto the abelian subvariety $h(A)$ of R, which proves the first assertion.

Now suppose that A is not simple, i.e. $A \sim E_1 \times E_2$, where E_i are two elliptic curves on A. Note that $E_i \otimes \mathbb{F}_{q^n} \sim E$, for $i = 1, 2$, because $A \otimes \mathbb{F}_{q^n} \sim E^2$. Now since $\mathrm{Ker}(h) \neq A$, there is at least one $i = 1, 2$, such that $E_i \not\subset \mathrm{Ker}(h)$. Renumbering if necessary, we may assume that $i = 1$. Then $h_{|E_1} : E_1 \to h(E_1)$ is an isogeny, and so the second assertion follows.

Remark 22. Note that if $E/\mathbb{F}_{q^n}$ is an elliptic curve, then we have

$$\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E) \otimes \mathbb{F}_{q^n} \;\sim\; E^n.$$

This follows from the fact that $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E) \otimes \mathbb{F}_{q^n} \simeq \prod_{\sigma \in G} E^\sigma$, where $G = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ and the fact that each Galois conjugate E^σ is isogenous to E because E^σ and E have the same number of $\mathbb{F}_{q^n}$-rational points.

Corollary 23. *Let $E/\mathbb{F}_{q^2}$ be an elliptic curve and let* $\mathrm{Res}(E) = \mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E)$ *be its Weil restriction. Then the following conditions are equivalent:*

(i) *Every abelian surface $A/\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^2} \sim E^2$ is split;*

(ii) *there is a split abelian surface $A/\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^2} \sim E^2$;*

(iii) $\mathrm{Res}(E)$ *is not simple;*

(iv) $\mathrm{Res}(E) \sim E_1 \times E_1^\chi$*, for some elliptic curve $E_1/\mathbb{F}_q$;*

(v) *$E \sim E_1 \otimes \mathbb{F}_{q^2}$, for some elliptic curve $E_1/\mathbb{F}_q$.*

In particular, there is a simple abelian surface $A/\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^2} \sim E^2$ if and only if $\mathrm{Res}(E)$ *is simple. If this is the case, then every such A is isogenous to* $\mathrm{Res}(E)$ *and $h_A(X) = h_E(X^2)$.*

Proof. (i) $\Rightarrow$ (v): By Remark 22, $A = \mathrm{Res}(E)$ is a surface over $\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^2} \sim E^2$. Since A is split by hypothesis, we have $A \sim E_1 \times E_2$ for some elliptic curves $E_i/\mathbb{F}_q$, and so $E_i \otimes \mathbb{F}_{q^2} \sim E$ because $A \otimes \mathbb{F}_{q^2} \sim E^2$.

(v) $\Rightarrow$ (iv): Since $\mathrm{Hom}(E_1, \mathrm{Res}(E)) \simeq \mathrm{Hom}(E_1 \otimes \mathbb{F}_{q^2}, E) \neq 0$, we see that E_1 is a factor of $\mathrm{Res}(E)$, and so $\mathrm{Res}(E) \sim E_1 \times E_2$ is split. Note that since $\mathrm{Res}(E) \otimes \mathbb{F}_{q^2} \sim E^2$, it follows that $E_2 \otimes \mathbb{F}_{q^2} \sim E$ and so $\mathrm{tr}_{E_2} = \pm\,\mathrm{tr}_{E_1}$. Now since $E_1^\chi \otimes \mathbb{F}_{q^2} \sim E_1 \otimes \mathbb{F}_{q^2} \sim E$, we see that E_1^χ is also a factor of $\mathrm{Res}(E)$. If $\mathrm{tr}_{E_1} \neq 0$, then $E_1^\chi \not\sim E_1$, and so $E_1^\chi \sim E_2$, and (iv) follows. If $\mathrm{tr}_{E_1} = 0$, then $\mathrm{tr}_{E_1^\chi} = -\mathrm{tr}_{E_1} = \pm\,\mathrm{tr}_{E_2}$ are all 0, so $E_1^\chi \sim E_1 \sim E_2$ and hence (iv) holds in this case as well.

(iv) $\Rightarrow$ (iii): Trivial.

(iii) $\Rightarrow$ (ii): By Remark 22 we can take $A = \mathrm{Res}(E)$.

(ii) $\Rightarrow$ (i): Let $A/\mathbb{F}_q$ satisfy condition (ii). If (i) is false, then there is a simple $B/\mathbb{F}_q$ with $B \otimes \mathbb{F}_{q^2} \sim E^2$, and then $B \sim \mathrm{Res}(E)$ by Proposition 21 because $\dim(B) = \dim(\mathrm{Res}(E)) = 2$. Thus $\mathrm{Res}(E)$ is simple and so Proposition 21 shows that $A \sim \mathrm{Res}(E)$ because $A \otimes \mathbb{F}_{q^2} \sim E^2$.

This proves the equivalence of conditions (i) – (v), and so by the equivalence of (i) and (iii) we see that there is a simple $A/\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^2} \sim E^2$ if and only if $\mathrm{Res}(E)$ is simple. If this is the case, then by Proposition 21 we know that A is isogenous to a factor of $\mathrm{Res}(E)$, and so $A \sim \mathrm{Res}(E)$ because $\dim(A) = \dim(\mathrm{Res}(E)) = 2$. Thus $h_A(X) = h_{\mathrm{Res}(A)}(X) = h_E(X^2)$.

Remark 24. If the equivalent conditions (i)–(iv) of Corollary 23 hold, then there are (at most) 3 possibilities for the isogeny class of an abelian surface $A/\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^2} \sim E^2$: either $A \sim \mathrm{Res}(E)$ or $A \sim E_1^2$ or $A \sim (E_1^\chi)^2$, where $E_1/\mathbb{F}_q$ is as in (v). Thus

$$h_A(X) = h_E(X^2) \quad \text{or} \quad h_A(X) = h_{E_1}(X)^2 \quad \text{or} \quad h_A(X) = h_{E_1^\chi}(X)^2. \tag{33}$$

Corollary 25. *Let $A/\mathbb{F}_q$ be an abelian surface such that $A \otimes \mathbb{F}_{q^n} \sim E^2$, for some elliptic curve $E/\mathbb{F}_{q^n}$. If $n = 2m$ is even, then $A \otimes \mathbb{F}_{q^m}$ splits if and only if there is an elliptic curve $E_1/\mathbb{F}_{q^m}$ with $E_1 \otimes \mathbb{F}_{q^n} \sim E$.*

Proof. Put $A' = A \otimes \mathbb{F}_{q^m}$. Since $A' \otimes \mathbb{F}_{q^n} \sim E^2$, the assertion follows from Corollary 23 (applied to $A'/\mathbb{F}_{q^m}$).

By using the above proposition, we can analyze the isogeny structure of $\mathrm{Res}(E)$. For this, it is useful to introduce the following notation which partially generalizes the notation E^χ for elliptic curves which was introduced earlier.

Notation. If $A/\mathbb{F}_q$ is an abelian variety, then let $A^\chi/\mathbb{F}_q$ denote any abelian variety such that $h_{A^\chi}(X) = h_A(-X)$. (Note that A^χ exists by Honda-Tate.) Thus, $\mathrm{tr}_{A^\chi} = -\mathrm{tr}_A$ and so if $\dim A = 2$ then $A^\chi \sim A$ if and only if $\mathrm{tr}_A = 0$. Moreover, we note that $A^\chi \otimes \mathbb{F}_{q^2} \sim A \otimes \mathbb{F}_{q^2}$, so A^χ is isogenous to a quadratic twist of A.

Proposition 26. *Let $E/\mathbb{F}_{q^n}$ be an elliptic curve and suppose there is a simple abelian surface $A/\mathbb{F}_q$ with $A \otimes \mathbb{F}_{q^n} \sim E^2$. Then the Weil restriction $\mathrm{Res}(E) = \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ of E has the following structure.*

(a) *If $n = 2$, then $\mathrm{Res}(E) \sim A \sim A^\chi$.*

(b) *If $n = 3$, then $\mathrm{Res}(E) \sim A \times E_0$, where $E_1/\mathbb{F}_q$ is an elliptic curve whose isogeny class is uniquely determined by the condition that $E_1 \otimes \mathbb{F}_{q^3} \sim E$.*

(c) *If* $n = 4$ *and* $A^\chi \not\sim A$, *then* $\mathrm{Res}(E) \sim A \times A^\chi$.

(c) *If* $n = 6$ *and* $A^\chi \not\sim A$, *then* $\mathrm{Res}(E) \sim A \times A^\chi \times \mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E_1)$, *where* $E_1/\mathbb{F}_{q^2}$ *is an elliptic curve with* $E_1 \otimes \mathbb{F}_{q^6} \sim E$.

Proof.(a) By Corollary 23 we know that $A \sim \mathrm{Res}(E)$. Moreover, since A^χ is also simple, and since $A^\chi \otimes \mathbb{F}_{q^2} \sim A \otimes \mathbb{F}_{q^2} \sim E^2$, it also follows that $A^\chi \sim \mathrm{Res}(E)$.

(b) By Proposition 21 (and Poincaré's Complete Reducibility Theorem) we know that $\mathrm{Res}(E) \sim A \times A'$, for some abelian variety $A'/\mathbb{F}_q$. Since $\dim A' = \dim(\mathrm{Res}(E)) - \dim A = 1$, we see that $A' = E_1$ is an elliptic curve. Thus $0 \neq \mathrm{Hom}(E_1, \mathrm{Res}(E)) \simeq \mathrm{Hom}(E_1 \otimes \mathbb{F}_{q^3}, E)$ by (32), and hence $E_1 \otimes \mathbb{F}_{q^3} \sim E$. Note that if $E'/\mathbb{F}_q$ is any elliptic curve with $E' \otimes \mathbb{F}_{q^3} \sim E$, then by reversing this argument we see that E' is a factor of $\mathrm{Res}(E) \sim E_1 \times A$ and hence $E' \sim E_1$ because A is simple.

(c) Since $A^\chi \otimes \mathbb{F}_{q^4} \sim A \otimes \mathbb{F}_{q^4} \sim E^2$ it follows from Proposition 21 that $\mathrm{Res}(E)$ has two abelian subvarieties B and B' with $B \sim A$ and $B' \sim A^\chi$. Since $B \not\sim B'$ and B is simple, we see that $\dim(B + B') = 4$. Thus $\mathrm{Res}(E) = B + B' \sim A \times A^\chi$.

(d) Put $R = \mathrm{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(E)$. Then $\mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(R) = \mathrm{Res}(E)$, so $\mathrm{Hom}(A \otimes \mathbb{F}_{q^2}, R) \simeq \mathrm{Hom}(A, \mathrm{Res}(E)) \simeq \mathrm{Hom}(A \otimes \mathbb{F}_{q^6}, E) \neq 0$. Thus R is not simple, and hence $R \sim A' \times E_1$, for some elliptic curve $E_1/\mathbb{F}_{q^2}$ and some (possibly split) abelian surface $A'/\mathbb{F}_{q^2}$. Note that by the same argument as in (b) we have that $E_1 \otimes \mathbb{F}_{q^6} \sim E$.

Thus, $\mathrm{Res}(E) \sim A_0 \times R_0$, where $A_0 := \mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(A')$ and $R_0 := \mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E_1)$. We claim that $\mathrm{Hom}(A, R_0) = 0$. If not, then $A \sim R_0$ because A is simple and then $A \otimes \mathbb{F}_{q^2} \sim R_0 \otimes \mathbb{F}_{q^2} \sim E_1^2$, the latter by Remark 22. But then by part (a) we have $A \sim A^\chi$, contradiction. Thus, $\mathrm{Hom}(A, R_0) = 0$ and hence A is a factor of A_0 because A is a (simple) factor of $\mathrm{Res}(E)$ by Proposition 21. Similarly, A^χ is a factor of A_0. Since A and A^χ are non-isogenous and simple, it follows that $A_0 \sim A \times A^\chi$ and hence $\mathrm{Res}(E)$ has the asserted form.

Corollary 27. *Let* A_1 *and* $A_2/\mathbb{F}_q$ *be two simple abelian surfaces with* $A_i \otimes \mathbb{F}_{q^n} \sim E^2$. *If* $n = 2$ *or* $n = 3$, *then* $A_1 \sim A_2$. *If* $n = 4$ *or* $n = 6$ *and if* $A_i^\chi \not\sim A_i$ *for* $i = 1, 2$, *then* $A_2 \sim A_1$ *or* $A_2 \sim A_1^\chi$.

Proof. If $n = 2$, then Proposition 26(a) applied to A_i gives $A_i \sim \mathrm{Res}(E)$ and so $A_1 \sim A_2$. For $n = 3$ we have by Proposition 26(b) that $A_i \times E_i \sim \mathrm{Res}(E)$ for some elliptic curves E_1, E_2 and so $A_1 \sim A_2$ and $E_1 \sim E_2$. For $n = 4$ we have by Proposition 26(c) that $A_i \times A_i^\chi \sim \mathrm{Res}(E)$ and so either $A_1 \sim A_2$ or $A_1 \sim A_2^\chi$. Finally, for $n = 6$ we obtain from Proposition 26(d) that $A_i \times A_i^\chi \times R_i \sim \mathrm{Res}(E)$, where $R_i = \mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E_i)$ for some elliptic curve $E_i/\mathbb{F}_{q^2}$. Now by the same argument as in the proof of Proposition 26(d) we see that $\mathrm{Hom}(A_2, R_1) = 0$, so $A_2 \sim A_1$ or $A_2 \sim A_1^\chi$.

Note that the above results also apply in the case that E is supersingular. However, if we impose the extra condition that E is ordinary, then we can use the results of the previous section to say more. We begin with the following observation.

Proposition 28. *If $A/\mathbb{F}_q$ is a simple ordinary abelian surface, then $A \otimes \mathbb{F}_{q^2}$ splits if and only if $A^\chi \sim A$.*

Proof. As was mentioned above, we have that $A^\chi \sim A$ if and only if $\mathrm{tr}_A = 0$. By Theorem 1 this is equivalent to the condition that $A \otimes \mathbb{F}_{q^2}$ splits.

We can use the above results to classify the abelian varieties $B/\mathbb{F}_q$ with $B \otimes \mathbb{F}_{q^n} \sim E^2$ when E is as in Theorem 20(b).

Proposition 29. *Let $E/\mathbb{F}_{q^n}$ be an ordinary elliptic curve, where $n = 3, 4$ or 6. If E satisfies the equivalent conditions of* Theorem 20(b), *then there are $[\frac{n+1}{2}]$ isogeny classes of abelian surfaces $B/\mathbb{F}_q$ such that $B \otimes \mathbb{F}_{q^n} \sim E^2$. More precisely, if $A/\mathbb{F}_q$ and $E_0/\mathbb{F}_{q^k}$ satisfy the conditions* (i) *and* (iii) *of* Theorem 20(b), *respectively, and if $t_0 = \mathrm{tr}_{E_0}$ and t are as in* Theorem 20(b), *and if $E_1 = E_0^\chi$, then these isogeny classes are given by the following table:*

n	$B \sim$	(tr_B, s_B)	condition
3	A, E_1^2	$(t, t^2 - q), (-2t, t^2 + 2q)$	$t_0^3 - 3qt_0 = -\mathrm{tr}_E,\ t = t_0$
4	A, A^χ	$(\pm t, \frac{1}{2}t^2)$	$t_0^2 - 2q^2 = -\mathrm{tr}_E,\ t^2 = 4q + 2t_0$
6	$A, A^\chi, \mathrm{Res}(E_1)$	$(\pm t, \frac{t^2}{3} + q), (0, t_0)$	$t_0^3 - 3q^2t_0 = -\mathrm{tr}_E,\ t^2 = 12q + 6t_0$

Furthermore, B is simple except in the case that $n = 3$ and $B \sim E_1^2$.

Proof. Suppose first that $n = 3$. Since $E_0 \otimes \mathbb{F}_{q^3} \sim E^\chi$, we know that $t = t_0 = \mathrm{tr}_{E_0}$ satisfies $t^3 - 3qt = -\mathrm{tr}_E$ and that $E_1 \otimes \mathbb{F}_{q^3} \sim E$. We observe that t is the unique rational root of $g_3(X) := X^3 - 3qX + \mathrm{tr}_E$ because $g_3(X) = (X - t)(X^2 + tX + t^2 - 3q)$ and the discriminant of $X^2 + tX + t^2 - 3q$ is $t^2 - 4(t^2 - 3q) = 3(4q - t^2)$, which is not a square by condition (ii) of Theorem 20. Moreover, by the proof of (iii) $\Rightarrow$ (i) we know that there is a simple abelian surface $A_0/\mathbb{F}_q$ with $\mathrm{tr}_{A_0} = t$ and $s_{A_0} = t^2 - q$ such that $A_0 \otimes \mathbb{F}_{q^3} \sim E^2$.

Now if $B/\mathbb{F}_q$ is simple, then $B \sim A_0$ by Corollary 27; in particular, $A \sim A_0$. If B splits, then $B \sim E_1' \times E_2'$ for some $E_i'/\mathbb{F}_q$ with $E_i' \otimes \mathbb{F}_{q^3} \sim E$. Then by Proposition 26(b) we know that $E_1' \sim E_2' \sim E_1$, so $B \sim E_1^2$. Thus $h_B(X) = h_{E_1}(X)^2 = (X^2 + tX + q)^2$, and so $\mathrm{tr}_B = -2t$ and $s_B = t^2 + 2q$.

Next, consider the case that $n = 4$. Since $A \otimes \mathbb{F}_{q^2}$ is simple by condition (i), we have that $A^\chi \not\sim A$ by Proposition 28, and so $\mathrm{Res}(E) = A \times A^\chi$ by Proposition 26(c). It thus follows from Proposition 21 that $B \sim A$ or $B \sim A^\chi$. Moreover, by the proof of (iii) $\Rightarrow$ (i) of Theorem 20 we know that $s_A = \frac{t^2}{2}$, where $t = \mathrm{tr}_A$ satisfies $(\frac{t^2}{2} - 2q)^2 - 2q^2 = -\mathrm{tr}_E$. Note that this property characterizes t uniquely up to sign, for we have that $g_4(X) := (X^2 - 4q)^2 + 4\,\mathrm{tr}_E = (X^2 - t^2)(X^2 - (8q - t^2))$, and $8q - t^2$ is not a square by condition (ii).

Finally, suppose that $n = 6$. Since $A_3 := A \otimes \mathbb{F}_{q^3}$ is simple by condition (i), it follows from Corollary 23 that $B_3 = B \otimes \mathbb{F}_{q^3}$ is also simple, and hence B is simple as well. Moreover, since $A_2 := A \otimes \mathbb{F}_{q^2}$ satisfies condition (i) for $n = 3$ (with q replaced by q^2), it follows from what was proved above that $t_0 = \mathrm{tr}_{E_0}$ is the unique rational root of $\tilde{g}_3(X) = X^3 - 3q^2X + \mathrm{tr}_E$, and that $B_2 := B \otimes \mathbb{F}_{q^2}$ is isogenous to A_2 or to E_1^2. In the latter case we have by Theorem 1 and Corollary 14 that $\mathrm{tr}_B = 0$ and $s_B = -\mathrm{tr}_{E_1} = t_0$. In the former case we have that $B \not\sim B^\chi$ by Proposition 28, and so it follows from Corollary 27 that $B \sim A$ or $B \sim A^\chi$. By Theorem 1 and Corollary 14 it follows that $s_B = \frac{\mathrm{tr}_B^2}{3} + q$ where $t_1 := \frac{\mathrm{tr}_B^2}{3} - 2q$ satisfies $t_1^3 - 3q^2t_1 = -\mathrm{tr}_E$. By the above uniqueness result for t_0 we have that $t_1 = t_0$, and so the assertion follows.

We observe that the conditions of Theorem 20(b) can also be expressed in the following way.

Proposition 30. *Let $E/\mathbb{F}_{q^n}$ be an ordinary elliptic curve, where $n = 3, 4$ or 6. Then the equivalent conditions* (i)–(iii) *of* Theorem 20(b) *are equivalent to condition* (iv)$_n$ *which is given by*

(iv)$_3$ $\mathrm{End}^0(E) \not\simeq \mathbb{Q}(\sqrt{-3})$ *and $E \sim E_1 \otimes \mathbb{F}_{q^3}$, for some elliptic curve $E_1/\mathbb{F}_q$;*

(iv)$_4$ $\mathrm{End}^0(E) \not\simeq \mathbb{Q}(i)$, *$E^\chi \sim E_0 \otimes \mathbb{F}_{q^4}$, for some elliptic curve $E_0/\mathbb{F}_{q^2}$, and $E^2 \sim A \otimes \mathbb{F}_{q^4}$, for some abelian surface $A/\mathbb{F}_q$;*

(iv)$_6$ $\mathrm{End}^0(E) \not\simeq \mathbb{Q}(\sqrt{-3})$, *$E \sim E_1 \otimes \mathbb{F}_{q^6}$, for some an elliptic curve $E_1/\mathbb{F}_{q^2}$ but $E \not\sim E_1' \otimes \mathbb{F}_{q^6}$, for any elliptic curve $E_1'/\mathbb{F}_{q^3}$, and $E^2 \sim A \otimes \mathbb{F}_{q^4}$, for some abelian surface $A/\mathbb{F}_q$ with* $\mathrm{tr}_A \neq 0$.

Proof. (i) $\Rightarrow$ (iv)$_n$: By Remark 9 we know that $\mathrm{End}^0(E) \not\simeq \mathbb{Q}(\zeta_n)$. In view of this, (iv)$_3$ is a special case of (iii) and (iv)$_4$ follows from (i) and (iii). Finally, the existence of $E_1/\mathbb{F}_{q^2}$ in (iv)$_6$ follows from (iii) and the existence of A follows from (i). Note that in the latter case we have $\mathrm{tr}_A \neq 0$ for otherwise A splits over $\mathbb{F}_{q^2}$ by Theorem 1. Moreover, since $A_3 := A \otimes \mathbb{F}_{q^3}$ is simple and $A_3 \otimes \mathbb{F}_{q^6} \sim E^2$, it follows from Corollary 23 that $E \not\sim E_1' \otimes \mathbb{F}_6$, for any $E_1'/\mathbb{F}_{q^3}$. Thus (iv)$_6$ holds.

(iv)$_3$ $\Rightarrow$ (iii): Put $E_0 = E_1^\chi$, so $E_0 \otimes \mathbb{F}_{q^3} \sim E^\chi$ and $\mathrm{End}^0(E_0) \simeq \mathrm{End}^0(E_1) = \mathrm{End}^0(E)$ because E is ordinary. Put $t = \mathrm{tr}_{E_0}$. If $3(4q - t^2) = t_1^2$ were a square, then $\mathrm{End}^0(E) \simeq \mathrm{End}^0(E_0) = \mathbb{Q}(\sqrt{t^2 - 4q}) = \mathbb{Q}(\sqrt{-3})$, contradiction. Thus (iii) holds.

(iv)$_4$ $\Rightarrow$ (i): Put $t_0 = \mathrm{tr}_{E_0}$. Then (as in the proof of (ii) $\Rightarrow$ (i) of Theorem 20) we have that $2q^2 - \mathrm{tr}_E = t_0^2$. Now if $A \otimes \mathbb{F}_{q^2}$ were split, then by Theorem 20(a) (with q replaced by q^2) we would have $2q^2 + \mathrm{tr}_E = t_1^2$, for some $t_1 \in \mathbb{Z}$. Thus $4q^4 - \mathrm{tr}_E^2 = (t_0t_1)^2$, and so $\mathrm{End}^0(E) = \mathbb{Q}(\sqrt{\mathrm{tr}_E^2 - 4q^4}) = \mathbb{Q}(i)$, contradiction. Thus $A \otimes \mathbb{F}_{q^2}$ is simple, and hence condition (i) holds.

(iv)$_6$ $\Rightarrow$ (i): First note that the third hypothesis of (iv)$_6$ implies that $A_3 := A \otimes \mathbb{F}_{q^3}$ is simple; cf. Corollary 23. In particular, A is simple. Moreover, the first two hypotheses of (iv)$_6$ imply that (iv)$_3$ holds (with q replaced by q^2), and so, by what was shown above, we see that (i) holds for E and $n = 3$. Thus, by Proposition 29 we know that either $A_2 := A \otimes \mathbb{F}_{q^2}$ is simple or that $A_2 \sim E_1^2$. However, in the latter case $\mathrm{tr}_A = 0$ by Theorem 1, contradiction. Thus A_2 is also simple and hence (i) holds.

5 Application to the Legendre/Satoh Jacobians

In his recent paper, Satoh[10] proposed to study genus 2 curves of the form

$$C_{u,v}: \quad y^2 = x^5 + ux^3 + vx, \tag{34}$$

where $u, v \in \mathbb{F}_q$; these curves generalize those of [4], where it is assumed that $u = 0$. (Here, as in [10], we assume that $(q, 2) = 1$.) Note that $C_{u,v}$ is a genus 2 curve if and only if $x^5 + ux^3 + vx$ has five distinct roots over $\overline{\mathbb{F}}_q$; this is the case if and only if $v \neq 0$ and $u^2 - 4v \neq 0$, which we assume henceforth. Note also that

$$C_{u',v'} \simeq C_{u,v}, \quad \text{if } u' = c^4 u \text{ and } v' = c^8 v, \text{ for some } c \in \mathbb{F}_q^\times,$$

because the substitution $x' = c^2 x$ and $y' = c^5 y$ transforms $C_{u,v}$ into $C_{u',v'}$.

It is interesting to observe that if $u = -(1 + v)$, then $C_{u,v}$ has the form

$$C_v := C_{-1-v,v}: \quad y^2 = x(x^2 - 1)(x^2 - v)$$

which is precisely the family of curves which were studied by Legendre in 1832: these were the first known examples of curves whose Jacobians are split (over the ground field $\mathbb{C}$); cf. Krazer[9], p. 477. Note that the family of curves C_v is *geometrically* the same as the family $C_{u,v}$ because we have

$$C_{u,v} \otimes \mathbb{F}_{q^8} \simeq C_{c^8 v}, \quad \text{where } c \in \mathbb{F}_{q^8} \text{ satisfies } c^8 v + c^4 u + 1 = 0.$$

We thus refer to the curves $C_{u,v}$ as *Legendre/Satoh curves.*

Fix $\sigma \in \mathbb{F}_{q^4}^\times$ such that $\sigma^4 = v$, and (as in [10]) let

$$x^4 + ux^2 + v = (x^2 - \alpha^2)(x^2 - \beta^2)$$

be the factorization of $x^4 + ux^2 + v$ in $\mathbb{F}_{q^4}$, so $\alpha^2 + \beta^2 = -u$ and $(\alpha\beta)^2 = v$. Thus $\sigma^2 = \pm\alpha\beta$, and so by replacing β by $-\beta$ if necessary, we can assume that $\sigma^2 = \alpha\beta$. Put

$$\gamma = 2\frac{u - 6\sigma^2}{u + 2\sigma^2} \in \mathbb{F}_{q^2} \quad \text{and} \quad \chi = -\frac{(\alpha - \beta)^2}{64\sigma^3} = \frac{u + 2\sigma^2}{64\sigma^3} \in \mathbb{F}_{q^4}, \tag{35}$$

and consider the elliptic curves

$$E_{u,v}/\mathbb{F}_{q^2}: \quad y^2 = (x - 1)(x^2 - \gamma x + 1) \quad \text{and} \quad E_\chi/\mathbb{F}_{q^4}: \quad y^2 = \chi(x - 1)(x^2 - \gamma x + 1).$$

Note that these are indeed elliptic curves because $\gamma \neq \pm 2$ (for otherwise $v = 0$ or $u = 2\sigma^2$, so $u^2 = 4v$). In addition, we note that E_χ is a quadratic twist of $E_{u,v} \otimes \mathbb{F}_{q^4}$ because if we let $c \in \mathbb{F}_{q^8}$ be such that $c^2 = \chi$, then the map $(x, y) \mapsto (x, cy)$ defines an isomorphism between $E_\chi \otimes \mathbb{F}_{q^8}$ and $E_{u,v} \otimes \mathbb{F}_{q^8}$. We also remark that a somewhat tedious computation shows that the j-invariant of $E_{u,v}$ (and hence also of E_χ) is

$$j(E_{u,v}) \;=\; j(E_\chi) \;=\; 256\frac{(\gamma+1)^3}{\gamma+2}, \tag{36}$$

but we don't need this fact.

Let $J_{u,v} = J_{C_{u,v}}$ denote the Jacobian of $C_{u,v}/\mathbb{F}_q$. By combining the above results with those of Satoh[10], we obtain the following result.

Theorem 31. (a) *The Jacobian $J_{u,v}$ of $C_{u,v}$ splits over a degree 4 extension of $\mathbb{F}_q$; more precisely, we have*

$$J_{u,v} \otimes \mathbb{F}_{q^4} \;\sim\; E_\chi^2.$$

(b) *If $q \equiv 3 \pmod 4$ or if v is a square in $\mathbb{F}_q^\times$ or if $\mathrm{End}^0(E_{u,v} \otimes \overline{\mathbb{F}}_q) \simeq \mathbb{Q}(i)$, then $J_{u,v}$ splits over $\mathbb{F}_{q^2}$. Moreover, the converse holds if $E_{u,v}$ is ordinary.*

(c) *Suppose that $q \equiv 1 \pmod 4$ and that v is not a square in $\mathbb{F}_q^\times$, and that $E := E_{u,v}$ is ordinary. Then $J_{u,v} \otimes \mathbb{F}_{q^2}$ is simple if and only if precisely one of $4q \pm 2\,\mathrm{tr}_E$ is a square in $\mathbb{Z}$. If this is the case and if $t \in \mathbb{Z}$ and $\varepsilon = \pm 1$ are such that $4q + 2\varepsilon\,\mathrm{tr}_E = t^2$, then*

$$h_{J_{u,v}}(X) = X^4 \pm tX^3 + \frac{t^2}{2}X^2 \pm tqX + q^2.$$

Proof. (a) This is proven in Satoh[10], p. 541. More precisely, Satoh shows that the rules

$$\varphi_1(x,y) = \left(\left(\frac{x+\sigma}{x-\sigma}\right)^2, \frac{y}{(x-\sigma)^3}\right), \quad \varphi_2(x,y) = \left(\left(\frac{x-\sigma}{x+\sigma}\right)^2, \frac{y}{(x+\sigma)^3}\right) \tag{37}$$

define morphisms $\varphi_i : C_{u,v} \otimes \mathbb{F}_{q^4} \to E_i$, where $E_1 = E_\chi$ and $E_2 = E_{-\chi}$ is the quadratic twist of E_χ by (-1). In addition, he shows that the induced homomorphism $\varphi_1^* + \varphi_2^* : E_1 \times E_2 \to J_{u,v} \otimes \mathbb{F}_{q^4}$ is an isogeny.

(b) We first observe that

$$\chi \in (\mathbb{F}_{q^4}^\times)^2 \quad \Leftrightarrow \quad \sigma \in (\mathbb{F}_{q^4}^\times)^2 \quad \Leftrightarrow \quad q \equiv 3 \pmod 4 \;\text{ or }\; v \in (\mathbb{F}_q^\times)^2. \tag{38}$$

Indeed, the first equivalence is clear from the definition (35) of χ because $-1 \in (\mathbb{F}_{q^4}^\times)^2$. To prove the second, note that σ is a square in $\mathbb{F}_{q^4}$ if and only if its norm $N(\sigma) = N_{\mathbb{F}_{q^4}/\mathbb{F}_q}(\sigma) = \sigma^{1+q+q^2+q^3}$ is a square in $\mathbb{F}_q^\times$. Since $1+q+q^2+q^3 \equiv 1+q+1+q \equiv 2+2q \pmod 8$, we can write $1+q+q^2+q^3 = 4k$ with $k \in \mathbb{N}$ and so $N(\sigma) = v^k$. Furthermore, k is even if and only if $q \equiv 3 \pmod 4$ and so $N(\sigma)$ is always a square in this case. If $q \equiv 1 \pmod 4$, then k is odd, and so in this case $N(\sigma) \in (F_q^\times)^2$ if and only if $v \in (\mathbb{F}_q^\times)^2$. This proves (38).

We thus see that the first two hypotheses of (b) imply that $\chi \in (\mathbb{F}_{q^4}^\times)^2$, and so $E_\chi \simeq E_{u,v} \otimes \mathbb{F}_{q^4}$. Thus, by part (a) we see that $E_0 = E_{u,v}$ satisfies the hypothesis of Corollary 25 for $m = 2$ and so $J_{u,v} \otimes \mathbb{F}_{q^2}$ is split.

Next, suppose that $\mathrm{End}^0(E_{u,v} \otimes \overline{\mathbb{F}}_q) \simeq \mathbb{Q}(i)$. Then $E_{u,v}$ and hence E_χ is ordinary and $\mathrm{End}^0(E_\chi) \simeq \mathrm{End}^0(E_{u,v}) \simeq \mathbb{Q}(i)$. Thus condition (iv)$_4$ of Proposition 30 does not hold for $E = E_\chi$, and so it follows from that proposition together with part (a) that $J_{u,v} \otimes \mathbb{F}_{q^2}$ is split.

Now suppose that $E_{u,v}$ is ordinary and that $J_{u,v} \otimes \mathbb{F}_{q^2}$ is split. If none of the three conditions of (b) hold, then $\chi \notin (\mathbb{F}_{q^4}^\times)^2$ by (38), so $E_\chi \sim (E_{u,v} \otimes \mathbb{F}_{q^4})^\chi$, and hence $(E_\chi)^\chi \sim E_{u,v} \otimes \mathbb{F}_{q^4}$. Thus, the condition (iv)$_4$ of Proposition 30 holds for $E = E_\chi$, and so by Proposition 30 (and Corollary 23) we have that $J_{u,v} \otimes \mathbb{F}_{q^2}$ is simple, contradiction. This proves the converse.

(c) Here $\chi \notin (\mathbb{F}_{q^4}^\times)^2$ by (38), so $E_\chi \sim (E \otimes \mathbb{F}_{q^4})^\chi$, and hence $(E_\chi)^\chi \sim E \otimes \mathbb{F}_{q^4}$.

Suppose first that $4q + 2\,\mathrm{tr}_E$ is a square in $\mathbb{Z}$ but $4q - 2\,\mathrm{tr}_E$ is not. Then in view of part(a) we see that $E_0 := E$ satisfies condition (iii) of Theorem 20(b), and so it follows from that theorem together with Corollary 23 that $J_{u,v} \otimes \mathbb{F}_{q^2}$ is simple. Similarly, if $4q - 2\,\mathrm{tr}_E$ is a square in $\mathbb{Z}$ but $4q + 2\,\mathrm{tr}_E$ is not, then $E_0 := E^\chi$ satisfies condition (iii) of Theorem 20(b) (because $E^\chi \otimes \mathbb{F}_{q^4} \sim E \otimes \mathbb{F}_{q^4}$ and $\mathrm{tr}_{E^\chi} = -\,\mathrm{tr}_E$) and so $J_{u,v} \otimes \mathbb{F}_{q^2}$ is simple in this case as well.

Conversely, suppose that $J_{u,v} \otimes \mathbb{F}_{q^2}$ is simple. Then by part (a) we have that condition (i) of Theorem 20(b) holds for E_χ and so by that theorem there is an elliptic curve $E_0/\mathbb{F}_{q^2}$ such that $E_0 \otimes \mathbb{F}_{q^4} \sim (E_\chi)^\chi$ with $4q + 2\,\mathrm{tr}_{E_0}$ a square and $4q - 2\,\mathrm{tr}_{E_0}$ a non-square. Now since $(E_\chi)^\chi \sim E \otimes \mathbb{F}_{q^2}$, we see that either $E_0 \sim E$ or $E_0 \sim E^\chi$, and so it follows that precisely one of $4q \pm 2\,\mathrm{tr}_E$ is a square.

The last assertion follows directly from Proposition 29.

In the following corollary we further analyze some of the cases of Theorem 31(b).

Corollary 32. (a) *If $v \in (\mathbb{F}_q^\times)^4$, then $\gamma, \chi \in \mathbb{F}_q$ and $J_{u,v} \sim E_\chi^0 \times E_{-\chi}^0$, where $E_{\pm\chi}^0/\mathbb{F}_q$ is defined by the equation $y^2 = \pm\chi(x-1)(x^2 - \gamma x + 1)$. Thus $h_{J_{u,v}}(X) = h_{E_\chi^0}(X) h_{E_\chi^0}((-1)^{\frac{q-1}{2}} X)$.*

(b) *If $v \in (\mathbb{F}_q^\times)^2 \setminus (\mathbb{F}_q^\times)^4$, then $\gamma \in \mathbb{F}_q$ and $J_{u,v} \otimes \mathbb{F}_{q^2} \sim ((E' \otimes \mathbb{F}_{q^2})^\chi)^2$, where $E'/\mathbb{F}_q$ is the elliptic curve defined by the equation $y^2 = (x-1)(x^2 - \gamma x + 1)$. If E' is ordinary, then $J_{u,v}$ is simple if and only if $4q - \mathrm{tr}_{E'}^2$ is not a square in $\mathbb{Z}$ or, equivalently, if and only if $\mathrm{End}^0(E') \not\simeq \mathbb{Q}(i)$. If this is the case, then $h_{J_{u,v}}(X) = x^4 + (\mathrm{tr}_{E'}^2 - 2q)X^2 + q^2$.*

Proof. (a) Since $v \in (\mathbb{F}_q^\times)^4$, then we can choose $\sigma \in \mathbb{F}_q$ and so also $\chi \in \mathbb{F}_q^\times$. It thus follows as in the proof of Theorem 31(a) that the rule (37) defines morphisms $\varphi_i^0 : C_{u,v} \to E_i^0$, where $E_1^0 = E_\chi^0$ and $E_2^0 = E_{-\chi}^0$, and that $J_{u,v} \sim E_1^0 \times E_2^0$. Thus $h_{J_{u,v}}(X) = h_{E_1^0}(X) h_{E_2^0}(X)$. If $q \equiv 1 \mod 4$, then $-1 \in (\mathbb{F}_q^\times)^2$ and so $E_1^0 \simeq E_2^0$. If $q \equiv 3 \mod 4$, then $-1 \notin (\mathbb{F}_q^\times)^2$, and so E_2^0 is the nontrivial quadratic twist of E_1^0, and hence $h_{E_2^0}(X) = h_{E_1^0}(-X)$. This proves (a).

(b) Here $\sigma^2 \in \mathbb{F}_q$ and so it follows from their definitions that $\gamma \in \mathbb{F}_q^\times$ and $\chi \in \mathbb{F}_{q^2}^\times$. Thus, the equation $y^2 = \pm\chi(x-1)(x^2 - \gamma x + 1)$ defines an elliptic curve $E'_{\pm\chi}/\mathbb{F}_{q^2}$. Similar to part (a), we thus see that the rule (37) defines morphisms $\varphi'_i : C_{u,v} \otimes \mathbb{F}_{q^2} \to E'_i$, where $E'_1 = E'_\chi$ and $E'_2 = E'_{-\chi}$, and $E'_{\pm\chi}/\mathbb{F}_{q^2}$, and that hence $J_{u,v} \otimes \mathbb{F}_{q^2} \sim E'_1 \times E'_2$. But since $q^2 \equiv 1 \mod 4$, we see that -1 is a square in $\mathbb{F}_{q^2}$, and so $E_1^0 \simeq E_2^0$. Thus $J_{u,v} \otimes \mathbb{F}_{q^2} \sim (E'_\chi)^2$. Now the hypothesis on v implies that σ and hence $\chi \notin (\mathbb{F}_{q^2}^\times)^2$, and so $E'_\chi \sim (E' \otimes \mathbb{F}_{q^2})^\chi$. This proves the first assertion. In addition, we have that $\mathrm{tr}_{E'_\chi} = -\mathrm{tr}_{E' \otimes \mathbb{F}_{q^2}} = -(\mathrm{tr}_{E'}^2 - 2q) = 2q - \mathrm{tr}_{E'}^2$, and so from Theorem 20(a) we see that if E' is ordinary, then $J_{u,v}$ is simple if and only if $2q + \mathrm{tr}_{E'_\chi} = 4q - \mathrm{tr}_{E'}^2$ is not a square. This latter condition is equivalent to the fact that $\mathrm{End}^0(E') \not\simeq \mathbb{Q}(i)$ because $\mathrm{End}^0(E') \simeq \mathbb{Q}(\sqrt{\mathrm{tr}_{E'}^2 - 4q})$. If this is the case, then the formula for $h_{J_{u,v}}(X)$ follows from Corollary 23 (with $E = E'_\chi$).

We can use the above theorem to obtain an "almost-deterministic" polynomial-time algorithm for computing the order $|J_{u,v}(\mathbb{F}_q)| = h_{J_{u,v}}(1)$ of the group $J_{u,v}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of the Jacobian of $C_{u,v}$. Here "almost-deterministic" means that we can compute two numbers $\{m, n\}$ such that either $|J_{u,v}(\mathbb{F}_q)| = m$ or $|J_{u,v}(\mathbb{F}_q)| = n$ (and the other number is the order of $J_{u,v}^\chi(\mathbb{F}_q)$, where $J_{u,v}^\chi$ is the quadratic twist of $J_{u,v}$). Unfortunately, this algorithm cannot decide (without further information) which of the two numbers equals the order of $J_{u,v}(\mathbb{F}_q)$.

Algorithm 33 (Non-degenerate Case)**.**

Input: $u, v \in \mathbb{F}_q$ with $v, u^2 - 4v \neq 0$.

Output: The unordered pair $J^* := \{|J_{u,v}(\mathbb{F}_q)|, |J_{u,v}^\chi(\mathbb{F}_q)|\}$, if $J_{u,v} \otimes \mathbb{F}_{q^2}$ is simple and ordinary, and "Fail" otherwise.

Steps: 1. If either $q \equiv 3 \pmod 4$ or v is a square in $\mathbb{F}_q^\times$, then return "Fail".

2. Let θ be a root of $X^2 - v$ in $\mathbb{F}_{q^2}$, and put $\gamma = 2\frac{u-6\theta}{u+2\theta} = 2\frac{u^2+12v-8u\theta}{u^2-4v}$. Apply a point counting algorithm (e.g. the SEA-algorithm) to the elliptic curve $E/\mathbb{F}_{q^2}$ defined by the equation $y^2 = (x-1)(x^2 - \gamma x + 1)$ to find $t_0 := \mathrm{tr}_E$. If $(q, t_0) \neq 1$, then return "Fail".

3. If $4q \pm 2t_0$ are both squares in $\mathbb{Z}$ or if neither is a square, then return "Fail".

4. Find $t \in \mathbb{Z}$ and $\varepsilon = \pm 1$ such that $4q + \varepsilon t_0 = t^2$ and return

$$J^* = \{1 - t + \tfrac{t^2}{2} - tq + q^2,\ 1 + t + \tfrac{t^2}{2} + tq + q^2\}.$$

Remark 34. (a) It is easy to see that $J_{u,v}^\chi$ is isogenous to the Jacobian of the quadratic twist $C_{u,v}^\chi$ of $C_{u,v}$. (Indeed, since $\mathrm{tr}_{J_{u,v}} = 1 + q - |C_{u,v}(\mathbb{F}_q)|$, this follows from the fact that $|C_{u,v}(\mathbb{F}_q)| + |C_{u,v}^\chi(\mathbb{F}_q)| = 2q + 2$.) Thus, if $v \notin (\mathbb{F}_q^\times)^2$, then $C_{u,v}^\chi$ is given by the equation $y^2 = v^{-1}(x^5 + ux^3 + vx)$, and so $C_{u,v}^\chi \simeq C_{uv^2,v^5}$ and $J_{u,v}^\chi \sim J_{uv^2,v^5}$.

(b) If the above algorithm "fails", then either $J_{u,v}$ is supersingular or $J_{u,v} \otimes \mathbb{F}_{q^2}$ splits. In both these cases the curve $C_{u,v}$ is considered to be cryptographically insecure by some authors (cf. [4]), but opinions differ. We shall consider the degenerate case below (cf. Algorithm 35).

(c) The most laborious step in the above algorithm is the point-counting algorithm (SEA-algorithm) applied to $E_{u,v}/\mathbb{F}_{q^2}$. Since this is a polynomial time algorithm, we see that Algorithm 33 is also of polynomial time.

In the degenerate case (cf. Corollary 32) we can compute the order of $J_{u,v}(\mathbb{F}_q)$ exactly.

Algorithm 35 (Degenerate Case)**.**
Input: $u, v = w^2 \in \mathbb{F}_q$ with $w \neq 0$ and $u \neq \pm 2w$.
Output: $|J_{u,v}(\mathbb{F}_q)|$, if $J_{u,v}$ is simple and ordinary, and "Fail" otherwise.
Steps: 1. If either $q \equiv 3 \pmod 4$ or w is a square in $\mathbb{F}_q^\times$, return "Fail".

2. Put $\gamma = 2\frac{u-6w}{u+2w}$. Apply a point counting algorithm (e.g. the SEA-algorithm) to the elliptic curve $E/\mathbb{F}_q$ defined by the equation $y^2 = (x-1)(x^2 - \gamma x + 1)$ to find $t_0 := \mathrm{tr}_E$. If $(q, t_0) \neq 1$, then return "Fail".

3. If $4q - t_0^2$ is a square in $\mathbb{Z}$, then $\mathrm{End}^0(E) \simeq \mathbb{Q}(i)$ and $J_{u,v}$ splits, so return "Fail". Otherwise, $J_{u,v}$ is simple and return $|J_{u,v}(\mathbb{F}_q)| = (1-q)^2 + t_0^2$.

Here we present some small numerical examples.

Example 36. (a) $C_{1,2}/\mathbb{F}_{29}$.
Here $u = 1$, $v = 2$ and $q = p = 29$. Note that $C_{1,2}/\mathbb{F}_{29}$ is a genus 2 curve because $u^2 - 4v \equiv -7 \pmod{29}$.

Since $p = 29 \equiv 1 \pmod 4$ and $(\frac{v}{p}) = -1$, we pass step 1 of Algorithm 33. Thus $\mathbb{F}_{p^2} = \mathbb{F}_{29}(\theta)$, where $\theta^2 = v = 2$ and $\gamma = 2\frac{1+12(2)-8\theta}{-7} = -3 - 6\theta$, so $E_{u,v}$ is given by $y^2 = (x-1)(x^2 + (3+6\theta)x + 1)$. Applying a point counting algorithm to $E_{u,v}/\mathbb{F}_{p^2}$, we obtain that $t_0 := \mathrm{tr}_{E_{u,v}} = 8$, which is coprime to 29. Since $4p - 2t_0 = 100 = (\pm 10)^2$ and $4p + 2t_0 = 132$, we pass step 3 and hence we can take $t = 10$ and $\varepsilon = -1$ in step 4. Thus, we obtain that $J^* = \{592, 1192\}$. In fact, a naive point count shows that $|C_{1,2}(\mathbb{F}_{29})| = 1 + 29 - 10 = 20$, so $\mathrm{tr}_{J_{1,2}} = 10$ and hence $|J_{1,2}(\mathbb{F}_{29})| = 1192$.

(b) $C_{1,2}/\mathbb{F}_{37}$.
Again $u^3 - 4v \equiv -7 \pmod{37}$, so $C_{1,2}/\mathbb{F}_{37}$ is a genus 2 curve. Since $p = 37 \equiv 1 \pmod 4$ and $(\frac{v}{p}) = -1$, we pass step 1. Here $\gamma = 2\frac{1+12(2)-8\theta}{-7} = 14 - 3\theta$, and a point counting algorithm yields that $t_0 := \mathrm{tr}_{E_{u,v}} = -24$. Since $(t_0, p) = 1$, we pass step 2. But $4p + 2t_0 = 100 = 10^2$ and $4p - 2t_0 = 196 = 14^2$ are both squares, so step 3 fails, and we conclude that $J_{1,2} \otimes \mathbb{F}_{37^2}$ splits. Thus, the algorithm returns "Fail".

(c) $C_{1,9}/\mathbb{F}_{41}$.

Here $u = 1$ and $v = w^2$ with $w = 3$, so we can apply Algorithm 35. Note that $u \not\equiv \pm 6 \equiv \pm 2w \pmod{41}$, so this is a genus 2 curve.

Since $p = 41 \equiv 1 \pmod 4$ and $(\frac{3}{41}) = -1$, we pass step 1. Here $\gamma = 2\frac{u-6w}{u+2w} \equiv 1 \pmod{41}$, and so $E/\mathbb{F}_{41}$ is $y^2 = (x-1)(x^2-x+1)$. A point counting algorithm gives $\mathrm{tr}_E = -6$. Since $(6, 41) = 1$ and $4p - \mathrm{tr}_E^2 = 128$ is not a square, we see that $J_{1,9}/\mathbb{F}_{41}$ is simple and that $|J_{1,9}(\mathbb{F}_{41})| = (-40)^2 + (-6)^2 = 1636 = 2^2 409$.

(d) Satoh's example[10]: $C_{3,7}/\mathbb{F}_{509}$.
Here $u^2 - 4v \equiv -19 \pmod{509}$, so $C_{3,7}/\mathbb{F}_{509}$ is a genus 2 curve.

Since $q = p = 509 \equiv 1 \pmod 4$ and $(\frac{7}{509}) = -1$, we pass step 1. Thus $\mathbb{F}_{p^2} = \mathbb{F}_p(\theta)$, where $\theta^2 = 7 \in \mathbb{F}_p$, and $\gamma = 2\frac{3^2+12(7)-8(3)\theta}{-19} = 17 - 185\theta$. Applying a point counting algorithm to $E_{u,v}/\mathbb{F}_{p^2}$ yields $\mathrm{tr}_{E_{u,v}} = -626$, which is coprime to 509, so we pass step 2. Since $4p + 2\,\mathrm{tr}_{E_{u,v}} = 4\cdot 509 + 2(-626) = (\pm 28)^2$ and $4p + 2\,\mathrm{tr}_{E_{u,v}} = 4\cdot 509 - 2(-626) = 3288 \notin \mathbb{Z}^2$, we pass step 3. Thus $t = 28$ and $\varepsilon := 1$ and so the algorithm returns $J^* = \{245194, 273754\}$.

Note that this agrees with two of the 4 values that are considered by Satoh[10] in his example on p. 546. More precisely, by applying the SEA algorithm to $E_\chi/\mathbb{F}_{p^4}$, Satoh obtains (by his algorithm) that $|J_{3,7}(\mathbb{F}_{509})| \in \{274538, 273754, 245978, 245194\}$. He discards the first three numbers because they do not have a sufficiently large prime divisor. He is thus left with $245194 = 2\cdot 122597$, which he accepts because by a random point check he found a point $P \in J_{3,7}(\mathbb{F}_{509})$ of order 122597.

We can use the above Algorithm 33 to obtain the following *deterministic polynomial time* variant of Satoh's *probabilistic polynomial time* algorithm.

Algorithm 37 (Variant of Satoh's Algorithm)**.**
Input: (i) $u, v \in \mathbb{F}_q$ with $v, u^2 - 4v \neq 0$;
(ii) a cofactor bound $M < (\sqrt{q} - 1)^2$;
(iii) a subset D of $J(\mathbb{F}_q)$ which generates a subgroup of order $> M$.
Output: The largest prime factor r of $|J_{u,v}(\mathbb{F}_q)|$, if $r > |J_{u,v}(\mathbb{F}_q)|/M$, and if $J_{u,v} \otimes \mathbb{F}_{q^2}$ is simple and ordinary, and "Fail" otherwise.
Steps: 1.–4. See Algorithm 33.

5. Write $J^* = \{n_1, n_2\}$. For $i = 1, 2$, determine the largest divisor $d_i | n_i$ with $d_i \leq M$. Put $n_i' = n_i/d_i$. If n_i' is prime and if there is a point $P \in \langle D \rangle$ such that $d_i P \neq 0$, then return n_i', otherwise return "Fail".

Remark 38. (a) The above algorithm is slightly more restrictive than that of Satoh[10] because we exclude here the cryptographically uninteresting cases that $J_{u,v}$ is supersingular or that $J_{u,v} \otimes \mathbb{F}_{q^2}$ splits; cf. Remark 34(b). However, if these cases are of interest, then we can easily include them by using Algorithm 35. Note that the condition on M automatically excludes the case that $J_{u,v}$ splits (cf. [10], p. 537).

(b) By the proof of Theorem 1 of Satoh[10], we see that the above algorithm computes the largest prime factor of $J_{u,v}(\mathbb{F}_q)$ subject to the given conditions. We observe that the steps of Satoh's original algorithm which led to probabilistic polynomial time have been eliminated, and so we now have a deterministic polynomial time algorithm. Here we use the fact (due to Agrawal, Kayal and Saxena) that we can test the primality of n'_i in deterministic polynomial time.

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models.* Springer-Verlag, Berlin, 1990.

[2] H. Cohen, *A course in computational algebraic number theory.* Springer-Verlag, New York, 1993.

[3] P. Deligne, Variétés abéliennes ordinaires sur un corps fini. *Invent. Math.* **6** (1969), 238-243.

[4] E. Furukawa, M. Kawazoe, T. Takahashi, Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields. In: *SAC 2003* (Matsui, M., Zuccherato, R. J., eds.), LNCS, vol. 3006, pp 26-41. Springer, Heidelberg, 2004.

[5] E. W. Howe, Principally polarized ordinary abelian varieties over finite fields. *Trans. Amer. Math. Soc.* **347** (1995), 2361-2401.

[6] E. W. Howe, H. J. Zhu, On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. *J. Number Theory* **92** (2002), 139–163.

[7] D. Maisner, E. Nart, Abelian surfaces over finite fields as Jacobians (with an appendix by E.W. Howe). *Experim. Math.* 11 (2002), 321–337.

[8] D. Mumford, *Abelian varieties*, Second Edition. Oxford University Press, Bombay, 1970.

[9] A. Krazer, *Lehrbuch der Thetafunktionen.* Leipzig, 1903; Chelsea Reprint, New York, 1970.

[10] T. Satoh, Generating genus two hyperelliptic curves over large characteristic finite fields. *EUROCRYPT 2009*, Lect. Notes in Comput. Sci., vol. 5479, pp. 536-553, Springer, 2009.

[11] W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.* (4), **2** (1969), 521-560.

[12] W. C. Waterhouse and J. S. Milne, Abelian varieties over finite fields. In: 1969 Number Theory Institute *Proc. Sympos. Pure Math.*, Vol. XX, State Univ. New York, Stony Brook, N.Y., Amer. Math. Soc., Providence, RI, 1971, page 53-64.