Supersingular abelian varieties over finite fields

Hui Zhu
MSRI, 1000 Centennial Drive, Berkeley, CA 94720, USA
Email: zhu@msri.org

Abstract

Let A be a supersingular abelian variety defined over a finite field $\mathbf{k}$. We give an approximate description of the structure of the group $A(\mathbf{k})$ of $\mathbf{k}$-rational points of A in terms of the characteristic polynomial f of the Frobenius endomorphism of A relative to $\mathbf{k}$. Write $f = \prod {g_i}^{e_i}$ for distinct monic irreducible polynomials g_i and positive integers e_i, we show that there is a group homomorphism $\varphi : A(\mathbf{k}) \longrightarrow \prod (\mathbf{Z}/g_i(1)\mathbf{Z})^{e_i}$ that is "almost" an isomorphism in the sense that the size of the kernel and the cokernel of φ are bounded by an explicit function of $\dim A$.

AMS classification: 14K22, 06B15.

1 Introduction

Let A be an abelian variety of dimension d defined over a finite field $\mathbf{k}$ of characteristic p with q elements. Let f be the characteristic polynomial of the Frobenius endomorphism of A relative to $\mathbf{k}$. An abelian variety A over $\mathbf{k}$ is *supersingular* if each complex root of f can be written as $\zeta\sqrt{q}$, the product of some root of unity ζ and the positive square root $\sqrt{q}$. This definition is equivalent to the standard ones as in [6] or [5]. The group structure of rational points on an elliptic curve over a finite field has been well studied (see [9, Chapter V]). We have studied the question for elementary supersingular abelian varieties in [10]. In this paper and [10], an *elementary* abelian variety is a power of a simple abelian variety. Here we study arbitrary supersingular abelian varieties.

For a finite abelian group G we write $\#G$ for its order. Let $\log(\cdot)$ be the natural logarithm. Write $f = \prod_{i=1}^{t} g_i^{e_i}$ for monic irreducible polynomials g_i with integer coefficients and positive integers e_i.

Theorem 1.1. *Let A be an supersingular abelian variety over $\mathbf{k}$ of dimension $d \geq 2$. Write $f = \prod_{i=1}^{t} g_i^{e_i}$ as above. Then there exists a group homomorphism*

$$\varphi : A(\mathbf{k}) \longrightarrow \prod_{i=1}^{t} (\mathbf{Z}/g_i(1)\mathbf{Z})^{e_i}$$

such that $\#\mathrm{Ker}(\varphi) = \#\mathrm{Coker}(\varphi)$

$$\leq \begin{cases} (2\log(2d-2))^{2d-2} & \text{if } d > 4.35 \times 10^7 \\ (2\log(100d-100))^{2d-2} & \text{if } 2 \leq d \leq 4.35 \times 10^7. \end{cases}$$

Further, for every prime $l \neq p$, *the* l*-part of* $\#\mathrm{Ker}(\varphi)$ *divides*

$$\begin{cases} 1 & \text{if } l > d \\ l^{\left[\frac{2d-2}{l-1}\right]} & \text{if } 2 < l \leq d \text{ or } q \text{ is a square} \\ 2^{3d-3} & \text{if } l = 2 \text{ and } q \text{ is a non-square}; \end{cases}$$

Let $\mathbf{Z}[\pi]$ be the $\mathbf{Z}$-algebra generated by the Frobenius π in the endomorphism ring of A. Let $\bar{\mathbf{k}}$ be an algebraic closure of $\mathbf{k}$.

Theorem 1.2. *Let* A *be an supersingular abelian variety over* $\mathbf{k}$ *of dimension* $d \geq 2$. *Write* $f = \prod_{i=1}^{t} g_i^{e_i}$ *as above. Let* $R_i = \mathbf{Z}[\pi]/(g_i(\pi))$ *and* $R_{i(p)}$ *its localization at* p. *There is a surjective* $\mathbf{Z}[\pi]$*-module homomorphism*

$$\varphi : A(\bar{\mathbf{k}}) \longrightarrow \prod_{i=1}^{t} (R_{i(p)}/R_i)^{e_i},$$

$$\text{where } \#\mathrm{Ker}(\varphi) < \begin{cases} (2\log(2d-2))^{2d-2} & \text{if } d > 4.35 \times 10^7 \\ (2\log(100d-100))^{2d-2} & \text{if } 2 \leq d \leq 4.35 \times 10^7. \end{cases}$$

Our theorems essentially demonstrate the following observation: The group structure of a supersingular abelian variety over a finite field is determined by the characteristic polynomial of its Frobenius endomorphism with an "error term" depending only on dim A, not on the size of the base field.

The organization of this paper is as the follows: Sections 2 and 3 are technical. Section 2 contains a lemma (see Lemma 2.1) from analytic number theory which will be used for section 3. In section 3 we will determine all possible irreducible factors of the characteristic polynomial f and compute their mutual resultants so as to give a useful approximation (see Lemma 3.3). In section 4, we consider finitely generated *torsion-free modules* over a *fibre product* of rings by applying Goursat's lemma. Finally, by considering the l-adic Tate module of A as a torsion-free module over $\mathbf{Z}[\pi]$, we apply section 4 to our problem and prove the two theorems.

This paper is based on a portion of the author's Berkeley Ph.D thesis. It is my pleasure to thank Professor Hendrik W. Lenstra, Jr. for his guidance and numerous suggestions. The author is supported as a MSRI postdoctoral fellow while preparing this paper and would like to thank the institute for its wonderful working environment.

2 A variation of Mertens theorem

Here we prove a lemma from analytic number theory that will be used in Lemma 3.3 in the next section. An immediate consequence is Corollary 2.2

which was initially conjectured by Hendrik Lenstra (see [7, §1] for its application). Mertens theorem implies that when n is large enough we have $\prod_{l \le n} l^{\frac{1}{l}} < n$, where l ranges over all primes $\le n$ (see [2, Theorem 425] or [8, (2.5)]). Let $\phi(\cdot)$ denote the Euler phi-function. In this section we will prove that when n is large enough we have $\prod_{l|n} l^{\frac{1}{l-1}} < \log \phi(n)$. The subscript $l \mid n$ denotes that l ranges over all distinct primes dividing n.

Lemma 2.1. *Let* $n_0 := p_{11} \prod_{i=1}^{8} p_i \approx 3.007 \times 10^8$. *Then*

$$\prod_{l|n} l^{\frac{1}{l-1}} < \begin{cases} \log \phi(n) & \text{if } n > n_0, \\ \log(50\phi(n)) & \text{if } 2 \le n \le n_0. \end{cases}$$

Proof. Let C be Euler's constant, and p_i the i-th prime number. Given an integer $n \ge 2$ we find the positive integer t such that $\prod_{i=1}^{t} p_i \le n < \prod_{i=1}^{t+1} p_i$. Since n has at most t distinct prime factors and $\frac{\log l}{l-1}$ is a decreasing function,

$$\sum_{l|n} \frac{\log l}{l-1} \le \sum_{i=1}^{t} \frac{\log p_i}{p_i - 1}. \tag{1}$$

By [8, (2.8) and (3.23)], we have for $t \ge 12$ that

$$\sum_{i=1}^{t} \frac{\log p_i}{p_i - 1} = \sum_{i=1}^{t} \frac{\log p_i}{p_i} + \sum_{m=2}^{\infty} \sum_{i=1}^{t} \frac{\log p_i}{p_i^m} < \log p_t + \frac{1}{\log p_t} - C. \tag{2}$$

Suppose $n \ge \prod_{i=1}^{13} p_i$. The two auxiliary functions $F(n) := F_0(n) + \frac{1}{F_0(n)} - C$ and $F_0(n) := \log\log n - \log(1 - \frac{1}{\log\log n - 0.7093})$ are increasing with respect to n. By Bertrand's Postulate (see [2, 22.3]) and [8, (3.32)], we obtain $p_t > \frac{p_{t+1}}{2} > \frac{\log n}{2.0325}$; thus by [8, (3.16)], we have $\log p_t < \log\log n - \log(1 - \frac{1}{\log p_t}) < F_0(n)$. Combining (1) and (2) yields

$$\sum_{l|n} \frac{\log l}{l-1} < F(n). \tag{3}$$

Define $H(n) := \exp(C) \log\log n + \frac{2.5}{\log\log n}$. Since $\frac{n}{H(n)}$ is an increasing function for $n \ge 30$, and by [8, (3.41)], we get

$$\frac{\prod_{i=1}^{t} p_i}{H(\prod_{i=1}^{t} p_i)} < \frac{n}{H(n)} < \phi(n) \quad \text{for all} \quad n \ne \prod_{i=1}^{9} p_i. \tag{4}$$

Suppose $n > \prod_{i=1}^{25} p_i$. It is not hard to show that $n > (H(n))^{21}$, and so

$$n < \phi(n) H(n) < \phi(n) (n/H(n))^{\frac{1}{20}} < \phi(n)^{1.05}. \tag{5}$$

Now $F(n) - \log\log n$ is decreasing, so $F(n) < \log\log n - 0.0529$. Then (3) and (5) yield $\sum_{l|n} \frac{\log l}{l-1} < \log\log n - 0.0529 < \log(1.05 \log \phi(n)) - 0.0529 < \log\log \phi(n)$.

Suppose $\prod_{i=1}^{10} p_i \leq n < \prod_{i=1}^{25} p_i$, by explicit calculation for each $10 \leq t \leq 24$ and by (4), we have

$$\prod_{l|n} l^{\frac{1}{l-1}} \leq \prod_{i=1}^{t} p_i^{\frac{1}{p_i-1}} < \log \frac{\prod_{i=1}^{t} p_i}{H(\prod_{i=1}^{t} p_i)} < \log \phi(n).$$

Suppose $n_0 < n < \prod_{i=1}^{10} p_i$. This implies that n has at most 9 distinct prime factors. Since $l^{\frac{1}{l-1}} > 1$ and $l^{\frac{1}{l-1}}$ is decreasing in l, the product $\prod_{l|n} l^{\frac{1}{l-1}}$ attains its maximum when n is the product of the smallest possible 9 primes among $p_1, \cdots, p_{10}$ such that $n > n_0$. This forces the first inequality below, while the rest follows from explicit computation and (3):

$$\prod_{l|n} l^{\frac{1}{l-1}} \leq \prod_{\substack{1 \leq i \leq 10 \\ i \neq 8}} p_i^{\frac{1}{p_i-1}} < \log n_0 - 1.85 < \log \frac{n_0}{H(\prod_{i=1}^{10} p_i)} < \log \frac{n_0}{n/\phi(n)},$$

which is less than $\log \phi(n)$ and the first part of the lemma is proved.

Suppose $30 \leq n \leq \prod_{i=1}^{10} p_i$ and $n \neq \prod_{i=1}^{9} p_i$. By (1), (5) and explicit computation on each $3 \leq t \leq 9$, we obtain

$$\prod_{l|n} l^{\frac{1}{l-1}} \leq \prod_{i=1}^{t} p_i^{\frac{1}{p_i-1}} < \log \frac{50 \prod_{i=1}^{t} p_i}{H(\prod_{i=1}^{t} p_i)} < \log(50\phi(n)).$$

It is easy to verify for $n = \prod_{i=1}^{9} p_i$ and $2 \leq n < 30$. □

By a similar but easier calculation, we can show $\prod_{l|n} l^{\frac{1}{l-1}} < \log n$ for all n so that $p_8 \prod_{i=1}^{6} p_i < n \leq n_0$ and thus for all $n > n_0$ by the above lemma. This gives the following corollary.

Corollary 2.2. *For all $n > p_8 \prod_{i=1}^{6} p_i = 570570$, we have $\prod_{l|n} l^{\frac{1}{l-1}} < \log n$.*

Remark 2.3. The minimal bounds for n in Lemma 2.1 and Corollary 2.2 are both sharp. It is not hard to verify the following: if $n = n_0 = p_{11} \prod_{i=1}^{8} p_i$, then $\prod_{l|n} l^{\frac{1}{l-1}} > \log \phi(n)$; if $n = p_8 \prod_{i=1}^{6} p_i$, then $\prod_{l|n} l^{\frac{1}{l-1}} > \log n$.

3 Supersingular polynomials

In this section, we will quote algebraic number theory from [1] or [3] without comment. Recall that q is a power of the prime p. An algebraic number in $\mathbf{C}$ is called a *supersingular q-number* if it is of the form $\zeta\sqrt{q}$, the product of some root of unity ζ and the positive square root of q. Obviously it is an algebraic integer. Here we determine all minimal polynomials of supersingular q-numbers, calculate their mutual resultants, and prove Lemma 3.3. This lemma is a core technical point for our proof of Theorems 1.1 and 1.2 in section 5.

Let $(\frac{a}{b})$ be the Jacobi symbol for an integer a and odd integer b, further, define $(\frac{a}{2})=0$ if $2\mid a$ and $(\frac{a}{2})=(-1)^{(a^2-1)/8}$ if $2\nmid a$. Denote by ζ_m the primitive m-th root of unity, $\exp(\frac{2\pi\sqrt{-1}}{m})$. The Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ consists of the σ_i defined by $\sigma_i(\zeta_m)=\zeta_m^i$ with i coprime to m and $1\le i\le m$. We claim that $\sqrt{p}\in\mathbf{Q}(\zeta_m)$ implies $\sigma_i(\sqrt{p})=(\frac{p}{i})\sqrt{p}$. Since they are both multiplicative, it suffices to show $\sigma_l(\sqrt{p})=(\frac{p}{l})\sqrt{p}$ for each prime l dividing i. If l is odd then $\sigma_l(\sqrt{p})\equiv(\sqrt{p})^l=p^{\frac{l-1}{2}}\sqrt{p}\bmod l$ and thus $\sigma_l(\sqrt{p})=(\frac{p}{l})\sqrt{p}$. Suppose $l=2$. Since m is odd, our hypothesis implies $\mathbf{Q}(\sqrt{p})\subseteq\mathbf{Q}(\zeta_p)\subseteq\mathbf{Q}(\zeta_m)$. Denote by $\bar{\sigma}_2$ the image of σ_2 in $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$, then $\sigma_2(\sqrt{p})=\bar{\sigma}_2(\sqrt{p})=\sqrt{p}$ or $-\sqrt{p}$. It equals the former if and only if $\bar{\sigma}_2\in\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}(\sqrt{p}))$, that is, if and only if 2 is a square in $(\mathbf{Z}/p\mathbf{Z})^*$. Thus $\sigma_2(\sqrt{p})=(\frac{p}{2})\sqrt{p}$.

Let Φ_m be the m-th cyclotomic polynomial. We write (m_1,m_2) for the greatest common divisor for integers or polynomials m_1 and m_2. Let $\mathcal{C}(\pi)$ be the conjugacy class of π in $\mathbf{C}$.

Proposition 3.1. *Let g be the minimal polynomial of a given supersingular q-number π.*

(1) If q is a square, then $\mathcal{C}(\pi)=\mathcal{C}(\zeta_m\sqrt{q})$ for some m, and

$$g=\Psi_m(X):=(\sqrt{q})^{\phi(m)}\Phi_m(\tfrac{X}{\sqrt{q}});$$

(2) If q is a non-square, then $\mathcal{C}(\pi)=\mathcal{C}(\zeta_m^\nu\sqrt{q})$ for some primitive m-th root of unity ζ_m^ν with $m\not\equiv 2 \bmod 4$;
(i) if $\mathbf{Q}(\pi)\neq\mathbf{Q}(\pi^2)$, then

$$\begin{aligned} g &= G_m(X):=q^{\frac{\phi(m)}{(2,m)}}\Phi_{m/(2,m)}(\tfrac{X^2}{q}) \\ &= \prod_{\substack{(i,m/(2,m))=1\\ 1\le i\le m/(2,m)}}(X-\zeta^i_{m/(2,m)}\sqrt{q})(X+\zeta^i_{m/(2,m)}\sqrt{q}); \end{aligned}\tag{6}$$

(ii) if $\mathbf{Q}(\pi)=\mathbf{Q}(\pi^2)$, then

$$g = E_{m,\pm 1}(X):=\prod_{\substack{(i,m/(2,m))=1\\ 1\le i\le m/(2,m)}}(X\mp(\tfrac{q}{i})\zeta_m^i\sqrt{q}).\tag{7}$$

Proof. Part (1) is straightforward. We shall show part (2). Write $\pi=\zeta_m^\nu\sqrt{q}$ for some primitive m-th root of unity ζ_m^ν. If $2\|m$, then $\pi=-\zeta_{m/2}^{\nu(m+2)/4}\sqrt{q}$; but since $m/2$ is odd, π is conjugate to $\zeta^\mu_{m/2}\sqrt{q}$ for some primitive $(m/2)$-th root of unity $\zeta^\mu_{m/2}$. Thus we may assume $m\not\equiv 2\bmod 4$ for the rest of the proof.

Now $[\mathbf{Q}(\pi):\mathbf{Q}(\pi^2)]=1$ or 2. It can be shown that $\mathbf{Q}(\pi)=\mathbf{Q}(\pi^2)$ if and only if $\Delta_{\mathbf{Q}(\sqrt{p})/\mathbf{Q}}\mid m$ and $2\Delta_{\mathbf{Q}(\sqrt{p}/\mathbf{Q})}\nmid m$ (see [10, Lemma 2.6]). Suppose $[\mathbf{Q}(\pi):\mathbf{Q}(\pi^2)]=2$. It is not hard to see that π is a root of G_m, and its minimal polynomial is G_m since G_m has degree $2\phi(m)/(2,m)$ and

$$[\mathbf{Q}(\pi):\mathbf{Q}]=\frac{[\mathbf{Q}(\pi):\mathbf{Q}(\zeta_{m/(2,m)})][\mathbf{Q}(\zeta_m):\mathbf{Q}]}{[\mathbf{Q}(\zeta_m):\mathbf{Q}(\zeta_{m/(2,m)})]}=2\phi(m)/(2,m).$$

Suppose $[\mathbf{Q}(\pi) : \mathbf{Q}(\pi^2)] = 1$. Then $\sqrt{p} \in \mathbf{Q}(\zeta_{m/(2,m)})$ and so by the argument preceding this proposition, we have $\sigma_i(\pi) = \sigma_i(\zeta_m^\nu \sqrt{q}) = (\frac{q}{i})\zeta_m^{i\nu}\sqrt{q}$ for all $\sigma_i \in \mathrm{Gal}(\mathbf{Q}(\zeta_{m/(2,m)})/\mathbf{Q})$. The degree of π is $\phi(m/(2,m))$, so its minimal polynomial is $E_{m,(\frac{q}{\nu})} = \prod(X - (\frac{q}{i})\zeta_m^{\nu i}\sqrt{q})$ where the product ranges over i with $(i, m/(2,m)) = 1$ and $1 \le i \le m/(2,m)$. $\square$

Remark 3.2. Let $\mathcal{E}$ denote the set of supersingular q-numbers $\zeta_m^\nu\sqrt{q}$ for some primitive m-th root of unity ζ_m^ν where $p \nmid m$, $p \ne 2$, q is not a square, such that (I) $4 \nmid m$ when $p \equiv 1 \bmod 4$ while (II) $4||m$ when $p \equiv 3 \bmod 4$.

Let $\mathcal{Q}$ be the set of supersingular q-numbers $\zeta_m^\nu\sqrt{q}$ for some primitive m-th root of unity ζ_m^ν where $p \nmid m$ and such that either (I) $m = 1, 2$ or (II) q is a square, $(2,p)p \nmid m$ and $\mathrm{ord}(p \bmod m_{(p)})$ is odd.

We note that $\pi \in \mathcal{Q}$ (respectively, $\mathcal{E}$) if and only if $\mathcal{C}(\pi) \subset \mathcal{Q}$ (respectively, $\mathcal{E}$). In other words, these definitions are independent of the choice of π from its conjugacy class.

For $i = 1, 2, \cdots, t$, let $\mathcal{C}_i$ be conjugacy classes of supersingular q-numbers with minimal polynomials g_i. By Proposition 3.1, $\mathcal{C}_i = \mathcal{C}(\zeta_{m_i}^{\nu_i}\sqrt{q})$ where $m_i \not\equiv 2 \bmod 4$ when q is a non-square. We order the $\mathcal{C}_i$'s so that $m_1 \le \cdots \le m_t$. For $i = 1, 2, \cdots, t$, let e_i be positive integers such that (I) $e_i \le e_{i+1}$ when $m_i = m_{i+1}$; and (II) e_i is even when $\pi_i \in \mathcal{Q}$. Under these conditions, the numbers defined by $d := \sum_{i\ge1} e_i \deg(g_i)/2$ and $d_{\mathcal{E}} := \sum_{i\ge1,\pi_i\in\mathcal{E}} e_i \deg(g_i)/2$ are positive integers (see [10, Proposition 3.3]). These two technically defined numbers will be used in section 5.

Let $\mathcal{R}(\cdot,\cdot)$ denote the resultant of two polynomials. For any prime number l, we write n_l and $n_{(l)}$ for the l-part and the non-l-part of a positive integer n, respectively. For any real number r we denote the largest integer $\le r$ by $[r]$.

Lemma 3.3. *Let the notation be as above, and let $d \ge 2$. Then*

$$(2^{d_{\mathcal{E}}}\prod_{i=2}^{t}\prod_{j=1}^{i-1}|\mathcal{R}(g_i,g_j)|^{e_i})_{(p)} < \begin{cases} (2\log(2d-2))^{2d-2} & \text{if } d > 4.35\times 10^7; \\ (2\log(100d-100))^{2d-2} & \text{if } d \le 4.35 \times 10^7. \end{cases}$$

In particular, for any prime l different from p, then

$$(2^{d_{\mathcal{E}}}\prod_{i=2}^{t}\prod_{j=1}^{i-1}|\mathcal{R}(g_i,g_j)|^{e_i})_{l} \text{ divides } \begin{cases} 1 & \text{if } l > d \\ l^{[\frac{2d-2}{l-1}]} & \text{if } 2 < l \le d \text{ or } q \text{ is a square} \\ 2^{3d-3} & \text{if } l = 2 \text{ and } q \text{ is a non-square.} \end{cases}$$

Remark 3.4. The strategy of our proof is to first compute the resultants of cyclotomic polynomials (in Lemma 3.5), then reduce our problem to the cyclotomic case (see Lemma 3.6). Finally we apply Lemma 2.1 to approximate our desired bounds.

Lemma 3.5. *For any positive integers $m > n$, we have*

$$\mathcal{R}(\Phi_m, \Phi_n) = \begin{cases} (-1)^{\phi(n)\phi(m)} l^{\phi(n)} & \text{if } m/n \text{ is a power of a prime } l, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let l be a prime number. Write $m = m_{(l)} l^{\alpha}$ and $n = n_{(l)} l^{\beta}$, then

$$\Phi_m(X) = \frac{\Phi_{m_{(l)}}(X^{l^\alpha})}{\Phi_{m_{(l)}}(X^{l^{\alpha-1}})} \equiv \frac{\Phi_{m_{(l)}}(X)^{l^\alpha}}{\Phi_{m_{(l)}}(X)^{l^{\alpha-1}}} = \Phi_{m_{(l)}}(X)^{\frac{\phi(m)}{\phi(m_{(l)})}} \bmod l.$$

Hence, $l \mid \mathcal{R}(\Phi_m, \Phi_n)$ if and only if $m_{(l)} = n_{(l)}$, that is, $m/n \in l^{\mathbf{Z}}$. Thus $|\mathcal{R}(\Phi_m, \Phi_n)| = 1$ if m/n is not a prime power. Now assume $m_{(l)} = n_{(l)}$. Then

$$\mathcal{R}(\Phi_n(X), \tfrac{X^m-1}{X^{m/l}-1}) = \mathcal{R}(\Phi_n(X), \Phi_l(X^{m/l})) = \textstyle\prod_{(i,n)=1} \Phi_l(\zeta_n^{im/l}) = l^{\phi(n)}.$$

According to the factorization $\frac{X^m-1}{X^{m/l}-1} = \Phi_m(X)\prod_s \Phi_{m/s}(X)$ where s ranges over divisors of $m_{(l)}$ that are not equal to 1, we get

$$l^{\phi(n)} = |\mathcal{R}(\tfrac{X^m-1}{X^{m/l}-1}, \Phi_n(X))| = |\mathcal{R}(\Phi_m, \Phi_n)| \prod_s |\mathcal{R}(\Phi_{m/s}, \Phi_n)|.$$

The last product is trivial since $n/(m/s)$ is not a prime power. This proves our assertion up to a sign. It remains to show that $\mathcal{R}(\Phi_m, \Phi_n)$ is positive if and only if $m \neq 2$. Indeed, if $m \geq 3$ then complex conjugation is contained in $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ and so $\mathcal{R}(\Phi_m, \Phi_n) = N_{\mathbf{Q}(\zeta_m)/\mathbf{Q}}(\Phi_n(\zeta_m))$ is positive. If $m = 2$ then it is trivial to see that $\mathcal{R}(\Phi_2, \Phi_1) = -2$. This finishes our proof. $\square$

Recall $\mathcal{E}$ from Remark 3.2. Let $\bar{\mathcal{E}}$ be the complement of $\mathcal{E}$ in the set of all supersingular q-numbers with non-square q.

Lemma 3.6. *Let the notation be as in Lemma 3.3,*

$$(\prod_{i>j} |\mathcal{R}(g_i, g_j)|^{e_i})_{(p)} \quad \textit{divides} \quad 2_{(p)}^{[\frac{\sum_{i\geq 2, \pi_i \in \bar{\mathcal{E}}} e_i \deg(g_i)}{2}]} \prod_{i \geq 2, l \mid 2m_i} l_{(p)}^{[\frac{e_i \deg(g_i)}{l-1}]}.$$

Proof. (a) Denote by $\mathcal{F}$ the set of π_i's with $m_i = m_{i+1}$. Let l be a prime different from p. For any fixed π_i, by Lemma 3.5, the product $\prod |\mathcal{R}(\Phi_{m_i}, \Phi_{m_j})|_l$ over all j with $1 \leq j \leq i-1, \pi_j \notin \mathcal{F}$ attains its maximum when each $m_j = \frac{m_i}{l^{i-j}}$. In this case, we have $\sum_{j=1}^{i-1} \phi(m_j) \leq \phi(\frac{m_i}{l}) + \phi(\frac{m_i}{l^2}) + \cdots + \phi(\frac{m_i}{l^{i-1}}) \leq \frac{\phi(m_i)}{l-1}$. Hence

$$\prod_{1 \leq j \leq i-1, \pi_j \notin \mathcal{F}} |\mathcal{R}(\Phi_{m_i}, \Phi_{m_j})|_l \ \text{ divides } \ l^{\frac{\phi(m_i)}{l-1}} \ \text{ for prime } l \mid m_i. \tag{8}$$

(b) Assume q is a square. Since $\mathcal{F}$ is empty, by Proposition 3.1 (1) and (8),

$$\prod_{i>j} |\mathcal{R}(g_i, g_j)|_{(p)}^{e_i} = \prod_{i>j} |\mathcal{R}(\Psi_{m_i}, \Psi_{m_j})|_{(p)}^{e_i} = \prod_{i>j} |\mathcal{R}(\Phi_{m_i}, \Phi_{m_j})|_{(p)}^{e_i},$$

which divides $\prod_{i \geq 2, l \mid m_i} l_{(p)}^{[\frac{e_i \deg(g_i)}{l-1}]}$.

(c) Assume q is a non-square. If q is a non-square then $\pi_i \in \mathcal{F}$ if and only if the pairs π_i, π_{i+1} have minimal polynomials $g_i = E_{m_i, \pm 1}$ and $g_{i+1} = E_{m_i, \mp 1}$. Since $\prod_{i>j} |\mathcal{R}(g_i, g_j)|_{(p)}^{e_i}$ divides

$$\prod_{\pi_{i-1} \in \mathcal{F}} |\mathcal{R}(E_{m_i,1}, E_{m_i,-1})|_{(p)}^{e_i} \prod_{i>j, \pi_j \notin \mathcal{F}} |\mathcal{R}(g_i, G_{m_j})|_{(p)}^{e_i},$$

it suffices to show the following two divisibilities hold:

$$\prod_{\pi_{i-1}\in\mathcal{F}} |\mathcal{R}(E_{m_i,1},E_{m_i,-1})|_{(p)}^{e_i} \quad \text{divides} \quad 2_{(p)}^{[\frac{\sum_{i\geq 2,\pi_i\in\bar{\mathcal{E}}} e_i \deg(g_i)}{2}]} \tag{9}$$

$$\prod_{i>j,\pi_j\notin\mathcal{F}} |\mathcal{R}(g_i,G_{m_j})|_{(p)}^{e_i} \quad \text{divides} \quad \prod_{i\geq 2, l|2m_i} l_{(p)}^{[\frac{e_i \deg(g_i)}{l-1}]}. \tag{10}$$

We firstly prove (9): Let σ and δ range over the embeddings of $\mathbf{Q}(\pi_i)$ in $\mathbf{C}$, by (7) we have

$$\prod_{\pi_{i-1}\in\mathcal{F}} |\mathcal{R}(E_{m_i,1},E_{m_i,-1})|_{(p)}^{e_i} = \prod_{\substack{\pi_{i-1}\in\mathcal{F}\\ \sigma,\delta}} |\pi_i^\sigma - (-\pi_i)^\delta|_{(p)}^{e_i}.$$

Splitting the product into two parts according to $\sigma=\delta$ and $\sigma\neq\delta$, they are

$$\begin{aligned} &= \prod_{\pi_{i-1}\in\mathcal{F},\sigma} |2\pi_i^\sigma|_{(p)}^{e_i} \cdot \prod_{\pi_{i-1}\in\mathcal{F},\sigma\neq\delta} \left|\frac{\pi_i^{2\sigma}-\pi_i^{2\delta}}{\pi_i^\sigma-\pi_i^\delta}\right|_{(p)}^{e_i} \\ &= 2_{(p)}^{\sum_{\pi_{i-1}\in\mathcal{F}} e_i \deg(g_i)} \cdot \prod_{\pi_{i-1}\in\mathcal{F}} \left|\frac{\Delta_{\mathbf{Z}[\pi_i^2]/\mathbf{Z}}}{\Delta_{\mathbf{Z}[\pi_i]/\mathbf{Z}}}\right|_{(p)}^{e_i}, \end{aligned}$$

where $\Delta(\cdot)$ denotes the discriminant. The last product is trivial since the inclusion chain $\mathbf{Z}[\pi_i^2]=\mathbf{Z}[q\zeta_{m_i/(2,m_i)}]\subseteq\mathbf{Z}[\pi_i]\subseteq\mathbf{Z}[\zeta_{m_i/(2,m_i)}]$ has p-power index. Note that $\pi_{i-1}\in\mathcal{F}$ implies $\pi_{i-1},\pi_i\in\bar{\mathcal{E}}$; but $e_{i-1}\leq e_i$ by our hypothesis, so we have $\sum_{\pi_{i-1}\in\mathcal{F}} e_i\deg(g_i)\leq\sum_{i\geq 2,\pi\in\bar{\mathcal{E}}} e_i\deg(g_i)/2$. Then (9) follows.

Secondly we prove (10): Let $n_{(2,p)}$ denote the non-2 and non-p part of the integer n. Now we claim that for any $i>j$ we have

$$|\mathcal{R}(g_i,G_{m_j})|_{(p)} \text{ divides } 2^{\deg(g_i)}|\mathcal{R}(\Phi_{m_i},\Phi_{m_j})|_{(2,p)}^{\frac{\deg(g_i)}{\phi(m_i)}}. \tag{11}$$

By Proposition 3.1 (2), it suffices to consider the following two cases:

Case 1. Suppose $g_i=G_{m_i}$. By the definition in (6), we have

$$|\mathcal{R}(G_{m_i},G_{m_j})|_{(p)} = |\mathcal{R}(\Phi_{m_i}(X^{2/(2,m_i)}),\Phi_{m_j}(X^{2/(2,m_j)}))|_{(p)}.$$

Note $\Phi_{m_i}(X^2)=\Phi_{m_i}(X)\Phi_{2m_i}(X)$ when $2\nmid m_i$. Further calculations via Lemma 3.5 yield that

$$|\mathcal{R}(G_{m_i},G_{m_j})|_{(p)} \quad \text{divides} \quad 2^{\deg(G_{m_i})}|\mathcal{R}(\Phi_{m_i},\Phi_{m_j})|_{(2,p)}^{\frac{2}{(2,m_i)}}.$$

Case 2. Suppose $g_i=E_{m_i,\pm1}$. From (6) and (7), $G_{m_i}=E_{m_i,1}E_{m_i,-1}$ and $|\mathcal{R}(E_{m_i,1},G_{m_j})|_{(p)}=|\mathcal{R}(E_{m_i,-1},G_{m_j})|_{(p)}$, so we have

$$|\mathcal{R}(E_{m_i,\pm1},G_{m_j})|_{(p)} = |\mathcal{R}(G_{m_i},G_{m_j})|_{(p)}^{1/2}.$$

Our claim then follows from Case 1.

By (11) and (8), the product $\prod_{i>j,\pi_j\notin\mathcal{F}} |\mathcal{R}(g_i, G_{m_j})|_{(p)}^{e_i}$ divides

$$2^{\sum_{i\geq 2} e_i \deg(g_i)} \prod_{i\geq 2, l|m_i} l_{(2,p)}^{[\frac{e_i \deg(g_i)}{l-1}]} = \prod_{i\geq 2, l|2m_i} l_{(p)}^{[\frac{e_i \deg(g_i)}{l-1}]}.$$

This finishes our proof. □

Proof of Lemma 3.3. If $t = 1$, then $2^{d_\mathcal{E}} \prod_{i>j} |\mathcal{R}(g_i, g_j)|^{e_i} = 2^{d_\mathcal{E}}$ divides 2^d since $d_\mathcal{E} \leq d$. In this case it is straightforward to verify our assertion. For the rest of the proof we assume $t \geq 2$. We shall prove the local bound first.

(I) Let $l > d$ and $l \neq p$, we claim $\prod_{i>j} |\mathcal{R}(g_i, g_j)|_l^{e_i} = 1$. Suppose the contrary. As $l > d \geq 2$, we know that l is an odd prime. By Lemma 3.6, we have that $l \mid m_i$ for some i. Suppose $m_i = l$ or $2l$. We separate two cases: If q is a square, then e_i is even since $\pi_i \in \mathcal{Q}$, thus $d \geq \deg(g_i) + 1 = \phi(m_i) + 1 = l$ which is a contradiction; If q is a non-square, then $\mathbf{Q}(\pi_i) \neq \mathbf{Q}(\pi_i^2)$ and so $g_i = G_{m_i}$ by Proposition 3.1; thence $d \geq \deg(g_i)/2 + 1 = \phi(m_i) + 1 = l$, which contradicts our assumption that $l > d$. Suppose $m_i \geq 3l$, then $l \leq \phi(m_i)/2 + 1 \leq \deg(g_i)/2 + 1 \leq d$ which is absurd. Secondly, if q is a square or $2 < l \neq p$, then by Lemma 3.6 the l-exponent of $2^{d_\mathcal{E}} \prod_{i>j} |\mathcal{R}(g_i, g_j)|^{e_i} \leq [\frac{\sum_{i\geq 2} e_i \deg(g_i)}{l-1}] \leq [\frac{2d-2}{l-1}]$ since $e_1 \deg(g_1) \geq 2$. Similarly, by Lemma 3.6, the 2-exponent of $2^{d_\mathcal{E}} \prod_{i>j} |\mathcal{R}(g_i, g_j)|_2^{e_i}$ is equal to $[\sum_{\pi_i\in\mathcal{E}} e_i \deg(g_i)] + [\sum_{i\geq 2, \pi_i\in\bar{\mathcal{E}}} e_i \deg(g_i)] + \sum_{i\geq 2} e_i \deg(g_i) \leq 3d - 3$.

(II) Now we prove the global bound. Let m_i' be the non-2-part of m_i. Let the notation be as in Lemma 3.6, $(2^{d_\mathcal{E}} \prod_{i>j} |\mathcal{R}(g_i, g_j)|^{e_i})_{(p)}$ divides

$$2^{[\frac{\sum_i e_i \deg(g_i)}{2}]} \prod_{i\geq 2, l|2m_i'} l^{[\frac{e_i \deg(g_i)}{l-1}]} \quad < \quad 2^d \prod_{i\geq 2}(\prod_{l|2m_i'} l^{\frac{1}{l-1}})^{e_i \deg(g_i)};$$

Note $\phi(2m_i') = \phi(m_i') \leq 2d - 2$, so by Lemma 2.1 we have

$$\begin{aligned}\prod_{l|2m_i'} l^{\frac{1}{l-1}} &< \log(50\phi(2m_i')) < \log(100d - 100) \\ &< 2^d(\log(100d-100))^{\sum_{i\geq 2} e_i \deg(g_i)} \leq (2\log(100d-100))^{2d-2}.\end{aligned}$$

Now assume that $d > 4.35 \times 10^7$. If $2m_i' > n_0$ then Lemma 2.1 implies that $\prod_{l|2m_i'} l^{\frac{1}{l-1}} < \log(2d-2)$; otherwise, by inequality (1) in the proof of the same lemma and explicit computation, $\prod_{l|2m_i'} l^{\frac{1}{l-1}} \leq \prod_{i=1}^{9} p_i^{\frac{1}{p_i-1}} \leq \log(2d-2)$. Therefore,

$$2^d \prod_{i\geq 2}(\prod_{l|2m_i'} l^{\frac{1}{l-1}})^{e_i \deg(g_i)} < 2^d(\log(2d-2))^{2d-2} \leq (2\log(2d-2))^{2d-2}.$$

This finishes our proof. □

Example 3.7. Those local upper bounds in Lemma 3.3 (1) are sharp. The second bound is achieved in the following example: Let q be a square. Let l be an odd prime different from p. Let $\pi_i = \zeta_{l^{i-1}}\sqrt{q}$ and e_i even positive integers for $i = 1, \cdots, t$. Then we have $2^{d\varepsilon}\prod_{i>j}|\mathcal{R}(g_i, g_j)|_l^{e_i} = l^{\frac{2d-2}{l-1}}$.

Here is a non-trivial example in which the third bound is approached very closely: Consider $\pi_1 = \zeta_3\sqrt{3}, \pi_2 = \zeta_{12}\sqrt{3}, \pi_3 = \zeta_{12}^7\sqrt{3}$ It can be checked that $\pi_i \in \bar{\mathcal{E}}$ so $2^{d\varepsilon}\prod_{i>j}\mathcal{R}(g_i, g_j)^{e_i} = 2^{2e_2+4e_3}$; while $2^{3d-3} = 2^{6e_1+3e_2+3e_3-3}$. Note $e_2 \geq e_3$ by our hypothesis.

4 Torsion-free modules and fibre products

All rings are commutative with 1. Let $t \geq 2$. Let $\mathfrak{a}_i$ be an ideal of a ring R_i for $i = 1, \cdots, t$. Inductively the fibre product $R_1 \times_{R_2/\mathfrak{a}_2} R_2 \times \cdots \times_{R_t/\mathfrak{a}_t} R_t$ is

$$R'_{t-1} \times_{R_t/\mathfrak{a}_t} R_t := \{(r'_{t-1}, r_t) \in R'_{t-1} \times R_t \mid \gamma_t(r'_{t-1} + \mathfrak{a}'_{t-1}) = r_t + \mathfrak{a}_t\},$$

where $R'_{t-1} = R_1 \times_{R_2/\mathfrak{a}_2} R_2 \times \cdots \times_{R_{t-1}/\mathfrak{a}_{t-1}} R_{t-1}$ has an ideal $\mathfrak{a}'_{t-1}$ such that there is an isomorphism $R'_{t-1}/\mathfrak{a}'_{t-1} \xrightarrow{\gamma_t} R_t/\mathfrak{a}_t$.

Given an R_i-module M_i with a submodule $N_i \supseteq \mathfrak{a}_i M_i$ for $i = 1, \cdots, t$, define the fibre product of modules $M_1 \times_{M_2/N_2} M_2 \times \cdots \times_{M_t/N_t} M_t$ analogously as

$$M'_{t-1} \times_{M_t/N_t} M_t := \{(x'_{t-1}, x_t) \in M'_{t-1} \times M_t \mid \theta_t(x'_{t-1} + N'_{t-1}) = (x_t + N_t)\};$$

where $M'_{t-1} = M_1 \times_{M_2/N_2} M_2 \times \cdots \times_{M_{t-1}/N_{t-1}} M_{t-1}$ has a submodule $N'_{t-1} \supseteq \mathfrak{a}_{t-1}M_{t-1}$ such that there is a γ_t-linear isomorphism $\theta_t : M'_{t-1}/N'_{t-1} \to M_t/N_t$. (Note: γ_t-linear means $\theta_t r'_{t-1} = (\gamma_t r'_{t-1})\theta_t$ for every $r'_{t-1} \in R'_{t-1}$.) Then $M_1 \times_{M_2/N_2} M_2 \times \cdots \times_{M_t/N_t} M_t$ is a module over $R_1 \times_{R_2/\mathfrak{a}_2} R_2 \times \cdots \times_{R_t/\mathfrak{a}_t} R_t$.

We have the following Goursat's Lemma for rings (also see [4, Exercise 5, page 75] for Goursat's lemma for groups).

Lemma 4.1. *Let $R_1, \ldots, R_t$ be rings. Suppose R is a subring of $\prod_{i=1}^t R_i$ such that the projections $R \xrightarrow{\rho_i} R_i$ are surjective. Let R'_i be the image of the projection $R \to \prod_{i=1}^j R_i$. Denote the projection maps from R'_i to R'_{i-1} and R_i by ρ'_{i-1} and ρ''_i, respectively. We may identify $\mathfrak{a}_i = \mathrm{Ker}(\rho'_{i-1})$ and $\mathfrak{a}'_{i-1} = \mathrm{Ker}(\rho''_i)$ as ideals in R_i and R'_{i-1}, respectively. We obtain isomorphisms $R'_{i-1}/\mathfrak{a}'_{i-1} \xrightarrow{\gamma_i} R_i/\mathfrak{a}_i$ for $i = 2, \cdots, t$ which define an isomorphism $R \cong R_1 \times_{R_2/\mathfrak{a}_2} R_2 \times \cdots \times_{R_t/\mathfrak{a}_t} R_t$. As abelian groups, $(R'_{i-1} \times R_i)/R'_i \cong R_i/\mathfrak{a}_i$ for $i = 2, \ldots, t$.*

Proof. From the inductive definition of fibre product, it suffices to prove for $t = 2$. It is clear that $\mathfrak{a}_1 = R \cap (R_1 \times \{0\})$, and by assumption, it can be identified as an ideal in R_1. Similarly we identify $\mathfrak{a}_2$ with an ideal in R_2. Thus $\mathfrak{a}_1 \times \mathfrak{a}_2$ is the largest ideal of $R_1 \times R_2$ that is also an ideal in R. The natural map $\theta : R \to R_1/\mathfrak{a}_1 \times R_2/\mathfrak{a}_2$ defines an isomorphism $\gamma : R_1/\mathfrak{a}_1 \to R_2/\mathfrak{a}_2$ as the image of R. If two elements $(r_1, r_2), (r_1, r_3) \in R_1 \times R_2$ lie in R, then $(0, r_2 - r_3) \in R$. Hence $r_2 - r_3 \in \mathfrak{a}_2$, otherwise contradicting the fact that $\mathfrak{a}_1 \times \mathfrak{a}_2$ is the largest ideal of $R_1 \times R_2$ which is also an ideal in R. This shows that γ is well-defined. Using the same argument, we see that γ is injective and surjective. From our construction $R_1 \times_{R_2/\mathfrak{a}_2} R_2$ is exactly the pullback of the map θ and hence identical with R. $\square$

We have an analogous Goursat's lemma for modules.

Lemma 4.2. *Let R be as in Lemma 4.1. Let M_i be an R_i-module and M be an R-submodule of $\prod_{i=1}^t M_i$ such that the projections $M \xrightarrow{\varrho_i} M_i$ are surjective. Let M_i' denote the image of the projection $M \to \prod_{i=1}^j M_i$. Denote the projection maps from M_i' to M_{i-1}' and M_i by ϱ_{i-1}' and ϱ_i'', respectively. We may identify $N_i = \mathrm{Ker}(\varrho_{i-1}')$ and $N_{i-1}' = \mathrm{Ker}(\varrho_i'')$ as submodules of M_i and M_{i-1}, respectively. We obtain ρ_i-linear isomorphisms $M_{i-1}'/N_{i-1}' \xrightarrow{\theta_i} M_i/N_i$ which define an R-module isomorphism $M \cong M_1 \times_{M_2/N_2} M_2 \times \cdots \times_{M_t/N_t} M_t$.*

Remark 4.3. Any subring R of $\prod_{i=1}^t R_i$ with surjective projections $R \to R_i$ is isomorphic to a fibre product of $R_1, \cdots, R_t$ as defined in Lemma 4.1. For the rest of the paper, we define the fibre product $R = R_1 \times_{R_2/\mathfrak{a}_2} R_2 \times \cdots \times_{R_t/\mathfrak{a}_t} R_t$ by the projections $R \xrightarrow{\rho_i} R_i$. Similarly we define a fibre product of R_i-modules M_i by the projections $M \xrightarrow{\rho_i} M_i$.

Assume all modules are finitely generated. Let l be a prime. Suppose K is a finite dimensional separable $\mathbf{Q}_l$-algebra. Let R be an $\mathbf{Z}_l$*-order* in K, that is, a $\mathbf{Z}_l$-algebra that spans K over $\mathbf{Q}_l$. An R-module M is *torsion-free* if $\alpha m \neq 0$ for all $\alpha \in R - \{0\}$ and $m \in M - \{0\}$. (If R is a domain then this is equivalent to the standard notation.) If M is a torsion-free R-module, then there is a natural injective map $M \to M \otimes_R K$; if moreover $M \otimes_R K \cong K^e$ for some integer e then we say that M is of *rank* e. See [10, Lemma 3.6] for the proof of the following auxiliary lemma.

Lemma 4.4. *Let R, K be as above. Let $r \in R - \{0\}$. Let $M \subseteq M'$ be torsion-free R-modules of rank e, then $\#M/rM = (\#(R/rR))^e$. There exist homomorphisms $\rho : M/rM \to M'/rM'$ and $\rho' : M'/rM' \to M/rM$ with $\#\mathrm{Ker}(\rho) = \#\mathrm{Coker}(\rho)$ and $\#\mathrm{Ker}(\rho') = \#\mathrm{Coker}(\rho')$ dividing $\#(M'/M)$.*

Proposition 4.5. *For $i = 1, \cdots, t$, let R_i be a $\mathbf{Z}_l$-order in a separable $\mathbf{Q}_l$-algebra K_i. Let $\mathfrak{a}_i$ be an ideal in R_i such that $R = R_1 \times_{R_2/\mathfrak{a}_2} R_2 \times \cdots \times_{R_t/\mathfrak{a}_t} R_t$. Let M be a torsion-free R-module and denote by M_i the image of the injection $M \otimes_R R_i \to M \otimes_K K_i$. The projections $M \to M_i$ define an R-module isomorphism $M \cong M_1 \times_{M_2/N_2} M_2 \times \cdots \times_{M_t/N_t} M_t$ for some R_i-submodules N_i in M_i. Further, if M_i is of rank e_i then $\#((\prod_{i=1}^t M_i)/M)$ divides $\prod_{i=2}^t \#(R_i/\mathfrak{a}_i)^{e_i}$.*

Proof. By hypothesis, $M \subseteq \prod_{i=1}^t M_i$. We use induction on t to show that M is the desired fibre product and $\#((\prod_{i=1}^t M_i)/M) = \prod_{i=2}^t \#(M_i/N_i)$. Suppose $t = 2$. By Lemma 4.2, $M \cong M_1 \times_{M_2/N_2} M_2$ for some submodule N_2. Write $\mathfrak{a} = \mathfrak{a}_1 \times \mathfrak{a}_2$. Since $M_1 \times_{M_2/N_2} M_2 = M \supseteq \mathfrak{a}M = \mathfrak{a}(R_1 \times R_2)M = \mathfrak{a}(M_1 \times M_2) = \mathfrak{a}_1 M_1 \times \mathfrak{a}_2 M_2$, we get $\mathfrak{a}_1 M_1 \subseteq N_1$, $\mathfrak{a}_2 M_2 \subseteq N_2$, and $\#((M_1 \times M_2)/M) = \#(M_2/N_2)$. Denote by M_i' the image of the projection $M \to \prod_{j=1}^i M_j$. Suppose there are R_i-submodules N_i in M_i such that, for $i = 2, \cdots, t-1$, we have $M_i' = M_1 \times_{M_2/N_2} M_2 \times \cdots \times_{M_i/N_i} M_i$, and $\#(\prod_{j=1}^{i-1} M_j)/M_{i-1}' = \prod_{j=2}^{i-1}(\#M_j/N_j)$.

Then $M \cong M'_{t-1} \times_{M_t/N_t} M_t$ and

$$\begin{aligned}\#((\prod_{i=1}^{t} M_i)/M) &= \#((\prod_{i=1}^{t-1} M_i)/M'_{t-1}) \cdot \#((M'_{t-1} \times M_t)/M) \\ &= (\prod_{i=2}^{t-1} \#(M_i/N_i)) \cdot \#(M_t/N_t) \\ &= \prod_{i=2}^{t} \#(M_i/N_i).\end{aligned}$$

This finishes our induction. But $\#M_i/N_i \mid \#(M_i/\mathfrak{a}_i M_i) = \#(R_i/\mathfrak{a}_i)^{e_i}$ by Lemma 4.4, so our assertion follows. □

Below is an explicit example of a fibre product of rings.

Proposition 4.6. *Let $g_1, \ldots, g_t \in \mathbf{Z}[X]$ be arbitrary monic polynomials in one variable such that $(g_i, g_j) = 1$ in $\mathbf{Q}[X]$ for $i \neq j$. Denote by π and π_i the images of X in the $\mathbf{Z}$-algebras $\mathbf{Z}[X]/(\prod_{i=1}^{t} g_i)$ and $\mathbf{Z}[X]/(g_i)$, respectively. Let $R = \mathbf{Z}[\pi]_l$, $R_i = \mathbf{Z}[\pi_i]_l$ and $\mathfrak{a}_i = (\prod_{j=1}^{i-1} g_j(\pi_i))R_i$. The natural projections $R \xrightarrow{\rho_i} R_i$ define an isomorphism $R \cong R_1 \times_{R_2/\mathfrak{a}_2} R_2 \times \cdots \times_{R_t/\mathfrak{a}_t} R_t$ such that $\#R_i/\mathfrak{a}_i = \prod_{j=1}^{i-1} |\mathcal{R}(g_i, g_j)|_l$ for all $i \geq 2$.*

Proof. Sending π to $(\pi_1, \cdots, \pi_t)$ defines a ring homomorphism $R \to \prod_{i=1}^{t} R_i$. It is injective since $(g_i, g_j) = 1$ for all $i \neq j$. For each i, this map induces surjective projections $R \to R_i$. The asserted isomorphism follows from induction on t by invoking Lemma 4.1. Thus $\#R_i/\mathfrak{a}_i = \#R_i/(\prod_{j=1}^{i-1} g_j(\pi_i)) = \prod_{j=1}^{i-1} |N_{\mathbf{Q}(\pi_i)/\mathbf{Q}}(g_j(\pi_i))|_l = \prod_{j=1}^{i-1} |\mathcal{R}(g_j, g_i)|_l$. □

5 Arbitrary supersingular abelian varieties

In this section, we shall prove Theorems 1.1 and 1.2. Let l be a prime $\neq p$. Let $T_l := T_l(A)$ be the l-adic Tate module of A and $V_l := T_l \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$. There is a $\mathbf{k}$-isogeny $A \xrightarrow{\gamma} \prod_{i=1}^{t} A_i$, where A_i is an elementary abelian variety with characteristic polynomial $g_i^{e_i}$. Let $\mathbf{Q}[\pi]$ be the $\mathbf{Q}$-subalgebra generated by π in the endomorphism algebra of A. Write $R := \mathbf{Z}[\pi]$ and $R_i := \mathbf{Z}[\pi]/g_i(\pi)\mathbf{Z}[\pi]$. Let R_l and $R_{l,i}$ be the l-adic completions of R and R_i, respectively. The isogeny γ gives an isomorphism of $\mathbf{Q}[\pi]$-modules, $\gamma : V_l \xrightarrow{\sim} \prod_{i=1}^{t} V_l(A_i)$. On T_l, the isogeny γ induces an injective map of R-modules $T_l \longrightarrow \prod_{i=1}^{t} T_{l,i}$ where $T_{l,i} = T_l(A_i)$, it can be identified as the image of T_l in the projection $V_l \to V_l(A_i)$. Clearly, T_l is a torsion-free R_l-module. Let π_i denote the image of π in $\mathbf{Q}[\pi]/(g_i(\pi))$, then $\mathbf{Q}[\pi]/(g_i(\pi)) = \mathbf{Q}(\pi_i)$ is actually a field, and we fix their embedding in $\mathbf{C}$. Since $V_l(A_i) \cong_{\mathbf{Q}(\pi_i)_l} \mathbf{Q}(\pi_i)_l^{e_i}$, we note that $T_{l,i}$ is a torsion-free $R_{l,i}$-module of rank e_i for each i.

Lemma 5.1. *Let the notation be as above. Let $r \in R$. There is an R_l-module homomorphism*

$$\varphi_l : T_l/rT_l \xrightarrow{\alpha_l} \prod_{i=1}^{t} (T_{l,i}/rT_{l,i}) \xrightarrow{\beta_l} \prod_{i=1}^{t} (R_l/rR_l)^{e_i}$$

with $\#\mathrm{Ker}(\varphi_l) = \#\mathrm{Coker}(\varphi_l)$ *dividing* $(2^{d_\mathcal{E}} \prod_{i=2}^{t} \prod_{j=1}^{i-1} |\mathcal{R}(g_i, g_j)|^{e_i})_l$.

Proof. By Propositions 4.5 and 4.6, $R_l = R_{l,1} \times_{R_{l,2}/\mathfrak{a}_2} R_{l,2} \times \cdots \times_{R_{l,t}/\mathfrak{a}_t} R_{l,t}$ and $T_l \cong T_{l,1} \times_{T_{l,2}/N_{l,2}} T_{l,2} \times \cdots \times_{T_{l,t}/N_{l,t}} T_{l,t}$ for some $R_{l,i}$-submodules $N_{l,i}$ in $T_{l,i}$ such that

$$\#((\prod_{i=1}^{t} T_{l,i})/T_l) \quad \text{divides} \quad \prod_{i=2}^{t}\prod_{j=1}^{i-1} |\mathcal{R}(g_i,g_j)|_l^{e_i}. \tag{12}$$

Applying Lemma 4.4, there is a map α_l with $\#\mathrm{Ker}(\alpha_l) = \#\mathrm{Coker}(\alpha_l)$ dividing $\prod_{i=2}^{t}\prod_{j=1}^{i-1} |\mathcal{R}(g_i,g_j)|_l^{e_i}$. On the other hand, by [10, Proposition 3.11], we have $\#(T_{l,i}/R_{l,i}^{e_i}) \mid 2^{e_i \deg(g_i)/2}$ if $(l,\pi_i) \in \{2\}\times\mathcal{E}$; and it equals 1 otherwise. Applying Lemma 4.4 again, we get a map β_l with $\#\mathrm{Ker}(\beta_l) = \#\mathrm{Coker}(\beta_l)$ dividing

$$\prod_{i=1}^{t} \#(T_{l,i}/R_{l,i}^{e_i}) = \prod_{\pi\in\mathcal{E}} 2_l^{e_i \deg(g_i)/2} = 2_l^{d_\mathcal{E}}. \tag{13}$$

Hence the composition map $\varphi_l = \beta_l \cdot \alpha_l$ has $\#\mathrm{Ker}(\varphi_l) = \#\mathrm{Coker}(\varphi_l)$ dividing the product of the last numbers of (12) and (13). ☐

Remark 5.2. If we order the e_i such that $e_1 \geq e_2 \geq \ldots \geq e_t$, and denote by $R'_{l,i}$ the image of the projection $R_l \to R_{l,1} \times \cdots \times R_{l,i}$, then the divisibility in (12) is actually equality if $T_{l,i} \cong_{R_{l,i}} R_{l,i}^{e_i}$ and

$$T_l \cong_{R_l} R_{l,1}^{e_1-e_2} \times (R'_{l,2})^{e_2-e_3} \times (R'_{l,3})^{e_3-e_4} \times \ldots \times (R'_{l,t-1})^{e_{t-1}-e_t} \times R_l^{e_t}.$$

Proof of Theorem 1.1: Suppose $d = \dim A \geq 2$. Noting that the l-Sylow subgroup of $A(\mathbf{k})$ is isomorphic to $T_l/(\pi-1)T_l$ and that the p-Sylow subgroup is trivial, we define $\varphi := \prod_{l\neq p} \varphi_l$, the φ_l as in Lemma 5.1. Our assertion follows from Lemma 3.3. Now suppose $d = 1$, then f has only one irreducible factor g. By [10, Theorem 1.1] there is a group homomorphism $\varphi : A(\mathbf{k}) \to (\mathbf{Z}/g(1)\mathbf{Z})^e$ with $\#\mathrm{Ker}(\varphi) = \#\mathrm{Coker}(\varphi)$ dividing $2_{(p)}$. Our assertion follows. ☐

The proof of Theorem 1.2 is almost identical to that of [10, Theorem 1.2]. We provide a sketch of its proof. For any integer n coprime to p, we find an R-module homomorphism $A[n] \to \prod_{i=1}^{t}(R_i/nR_i)^{e_i}$ with kernel and cokernel bounded as in the assertion. These bounds do not depend on n. After taking the suitable injective limit on both sides over n we get the desired homomorphism φ having the same bounds.

References

[1] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, 1993.

[2] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, fifth ed., Oxford Science Publications, 1979.

[3] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer, 1992.

[4] S. Lang, *Algebra*, third ed., Addison-Wesley, 1993.

[5] K-Z Li and F. Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Math., vol. 1680, Springer-Verlag, 1998.

[6] F. Oort, *Subvarieties of moduli spaces*, Invent. Math. **24** (1974), 95–119.

[7] C. Powell, *Bounds for multiplicative cosets over fields of prime order*, Math. Comp. **66** (1997), 807–822.

[8] J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[9] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1986.

[10] H. Zhu, *Group structures of elementary supersingular abelian varieties over finite fields*, MSRI Preprint #1998-065.