Journal of Number Theory **86**, 61–77 (2001)
doi:10.1006/jnth.2000.2562, available online at http://www.idealibrary.com on IDEAL®

Supersingular Abelian Varieties over Finite Fields

Hui June Zhu

Department of Mathematics, University of California, Berkeley, California 94720-3880
E-mail: zhu@alum.calberkely.org

Communicated by K. Rubin

Received April 13, 1999

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 φ: $A(\mathbf{k}) \to \prod (\mathbf{Z}/g_i(1)\,\mathbf{Z})^{e_i}$ that is "almost" an isomorphism in the sense that the sizes of the kernel and the cokernel of φ are bounded by an explicit function of $\dim A$.

1991 Mathematics Subject Classifications: Primary 11G15; Secondary 14G10, 11N37.

Key Words: supersingular abelian variety; finite field; Mertens theorem.

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, Chap. V]). We have studied the question for elementary supersingular abelian varieties in [10]. In this paper and [10], an *elementary* abelian variety means an abelian variety that is $\mathbf{k}$-isogenous to 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 distinct monic irreducible polynomials g_i with integer coefficients and positive integers e_i.

0022-314X/01 $35.00

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

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

such that

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

If q is a nonsquare, the l-part of $\#\mathrm{Ker}(\varphi)$ divides l^{3d-2} if $l=2$, divides $l^{[(2d-2)/(l-1)]}$ if $l>2$, and is trivial if $l>d$ or $l=p$. If q is a square, the l-part of $\#\mathrm{Ker}(\varphi)$ divides $l^{[(2d-2)/(l-1)]}$ if $l \geqslant 2$, and is trivial if $l>2d$ or $l=p$.

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

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

where

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

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 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 3.2). 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 Ph.D thesis. The author thanks Professor Hendrik W. Lenstra, Jr., for his guidance and the Mathematical Science Research Institute (Berkeley) for its excellent working environment and support while she was preparing this paper. The author also thanks the referee for many very helpful comments.

2. A VARIATION OF MERTENS'S THEOREM

Here we prove a lemma from analytic number theory that will be used in Lemma 3.2 in the next section. An immediate consequence is Corollary 2.2 which was initially conjectured by Lenstra (see [7, Sect. 1] for its application). Mertens's theorem implies that when n is large enough we have $\prod_{l\leqslant n} l^{1/l} < n$, where l ranges over all primes $\leqslant n$ (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 $\prod_{l\mid n} l^{1/(l-1)} < \log\phi(n)$. The subscript $l\mid n$ denotes that l ranges over all distinct primes dividing n.

Let C be Euler's constant (≈ 0.5772) and p_i the ith prime number.

LEMMA 2.1. *Let* $n_0 := 2\prod_{i=1}^{9} p_i \approx 4.46\times 10^8$. *Then*

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

Proof. Given an integer $n\geqslant 2$ we find the positive integer t such that $\prod_{i=1}^{t} p_i \leqslant n < \prod_{i=1}^{t+1} p_i$. Since n has at most t distinct prime factors and $(\log l)/(l-1)$ is a decreasing function,

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

By [8, (2.8) and (3.23)], we have for $t\geqslant 12$ 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 $n\geqslant \prod_{i=1}^{13} p_i$. The two auxiliary functions $F(n) := F_0(n) + 1/F_0(n) - C$ and $F_0(n) := \log\log n - \log(1 - 1/(\log\log n - 0.7093))$ are increasing with respect to n. By Bertrand's Postulate (see [2, 22.3]) and

[8, (3.32)], we obtain $p_t > p_{t+1}/2 > (\log n)/2.0325$; thus by [8, (3.16)] we have $\log p_t < \log\log n - \log(1 - 1/(\log p_t)) < F_0(n)$. Combining (1) and (2) yields

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

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

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

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

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

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

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

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

Suppose $n < \prod_{i=1}^{10} p_i$. This implies that n has at most 9 distinct prime factors. Since $l^{1/(l-1)} > 1$ and $l^{1/(l-1)}$ is decreasing in l, we have $\prod_{l\,|\,n} l^{1/(l-1)} \leqslant \prod_{i=1}^{9} p_i^{1/(p_i-1)}$. When $3 \prod_{i=1}^{9} p_i \leqslant n < \prod_{i=1}^{10} p_i$, by explicit computation and (4) we have

$$\prod_{l\,|\,n} l^{1/(l-1)} \leqslant \prod_{i=1}^{9} p_i^{1/(p_i-1)} < \log \frac{3 \prod_{i=1}^{9} p_i}{H(3 \prod_{i=1}^{9} p_i)} < \log \phi(n).$$

When $n_0 < n < 3 \prod_{i=1}^{9} p_i$, by similar computation we have

$$\prod_{l\,|\,n} l^{1/(l-1)} \leqslant p_{10}^{1/(p_{10}-1)} \prod_{i=1}^{8} p_i^{1/(p_i-1)} < \log \frac{n_0}{H(n_0)} < \log \phi(n).$$

This proves the first half of the lemma.

Suppose $30 \leqslant n \leqslant n_0$ and $n \neq \prod_{i=1}^{9} p_i$. By (1), (4), and explicit computation on each $3 \leqslant t \leqslant 9$, we obtain

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

This is easy to verify for $n = \prod_{i=1}^{9} p_i$ and $2 \leqslant n < 30$. ∎

By a similar but easier calculation, we can show that $\prod_{l \mid n} l^{1/(l-1)} < \log n$ for all n so that $p_8 \prod_{i=1}^{6} p_i < n \leqslant n_0$ 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* $\prod_{l \mid n} l^{1/(l-1)} < \log n$.

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 $n = n_0 = 2 \prod_{i=1}^{9} p_i$, then $\prod_{l \mid n} l^{1/(l-1)} > \log \phi(n)$; if $n = p_8 \prod_{i=1}^{6} p_i$, then $\prod_{l \mid n} l^{1/(l-1)} > \log n$.

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 3.2. 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 $(\frac{a}{1}) = 1$ and 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 mth root of unity, $\exp(2\pi\sqrt{-1}/m)$. 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 $1 \leqslant i \leqslant m$. 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 that $\sigma_l(\sqrt{p}) = (\frac{p}{l})\sqrt{p}$ for each prime l dividing i. If l is odd then $\sigma_l(\sqrt{p}) \equiv (\sqrt{p})^l = p^{(l-1)/2}\sqrt{p} \bmod l$ and thus $\sigma_l(\sqrt{p}) = (\frac{p}{l})\sqrt{p}$. Suppose $l = 2$. Since m is odd, our hypothesis implies that $\mathbf{Q}(\sqrt{p}) \subseteq \mathbf{Q}(\zeta_p) \subseteq \mathbf{Q}(\zeta_m)$. 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 mth cyclotomic polynomial. We write (m_1, m_2) for the greatest common divisor for integers or polynomials m_1 and m_2. Let $\mathscr{C}(\pi)$ 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.*

I. *If q is a squar, then $\mathscr{C}(\pi) = \mathscr{C}(\zeta_m \sqrt{q})$ for some m, and*

$$g = \Psi_m(X) := (\sqrt{q})^{\phi(m)} \Phi_m\left(\frac{X}{\sqrt{q}}\right).$$

II. *If q is a nonsquare, then $\mathscr{C}(\pi) = \mathscr{C}(\zeta_m^v \sqrt{q})$ for some primitive mth root of unity ζ_m^v with $m \not\equiv 2 \bmod 4$. Define*

$$G_m(X) := q^{\phi(m)/(2,m)} \Phi_{m/(2,m)}(X^2/q). \tag{6}$$

(i) *If $\mathbf{Q}(\pi) \neq \mathbf{Q}(\pi^2)$, then $g = G_m(X)$.*

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

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

Proof. Part I is straightforward. We shall show part II. Write $\pi = \zeta_m^v \sqrt{q}$ for some primitive mth root of unity ζ_m^v. If $2 \parallel m$, then $\pi = -\zeta_{m/2}^{v(m+2)/4} \sqrt{q}$; but since $m/2$ is odd, π is conjugate to $\zeta_{m/2}^{\mu} \sqrt{q}$ for some primitive $(m/2)$th root of unity $\zeta_{m/2}^{\mu}$. 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. Let Δ denote the discriminant of a number field extension. 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 $\sqrt{p} \in \mathbf{Q}(\zeta_m)$ and so by the argument preceding this proposition we have $\sigma_i(\pi) = \sigma_i(\zeta_m^v \sqrt{q}) = (\frac{q}{i}) \zeta_m^{iv} \sqrt{q}$ 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 $E_{m, (\frac{q}{v})} = \prod (X - (\frac{q}{i}) \zeta_m^{vi} \sqrt{q})$ where the product ranges over i with $(i, m/(2,m)) = 1$ and $1 \leqslant i \leqslant m/(2,m)$. ∎

We introduce some notation here. 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.

Let $\mathscr{E}$ denote the set of supersingular q-numbers $\zeta_m^v\sqrt{q}$ for some primitive mth root of unity ζ_m^v where $p \nmid m$, $p \neq 2$, and q is not a square, such that (I) $4 \nmid m$ when $p \equiv 1 \bmod 4$ while (II) $4 \parallel m$ when $p \equiv 3 \bmod 4$.

Let $\mathscr{Q}$ be the set of supersingular q-numbers $\zeta_m^v\sqrt{q}$ for some primitive mth root of unity ζ_m^v such that either (I) $m=1, 2$ or (II) q is a square, $(2, p)\ p \nmid m$ and $\operatorname{ord}(p \bmod m_{(p)})$ is odd. We note that $\pi \in \mathscr{Q}$ (respectively, $\mathscr{E}$) if and only if $\mathscr{C}(\pi) \subset \mathscr{Q}$ (respectively, $\mathscr{E}$). In other words, these definitions are independent of the choice of π from its conjugacy class.

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

Let $\mathscr{R}(\cdot, \cdot)$ denote the resultant of two polynomials. For any real number r we denote the largest integer $\leqslant r$ by $[r]$.

Lemma 3.2. *Let the notation be as above and let $d \geqslant 2$. Then*

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

Let l be a prime different from p. If q is a nonsquare, we have

$$\left(2^{d_{\mathscr{E}}} \prod_{i=2}^{t} \prod_{j=2}^{i-1} |\mathscr{R}(g_i, g_j)|^{e_i}\right)_{l} \text{ divides } \begin{cases} 1 & \text{if } l > d; \\ l^{[(2d-2)/(l-1)]} & \text{if } 2 < l \leqslant d; \\ 2^{3d-2} & \text{if } l = 2. \end{cases}$$

If q is a square, we have

$$\left(2^{d_{\mathscr{E}}} \prod_{i=2}^{t} \prod_{j=1}^{i-1} |\mathscr{R}(g_i, g_j)|^{e_i}\right)_{l} \text{ divides } \begin{cases} 1 & \text{if } l > 2d; \\ l^{[(2d-2)/(l-1)]} & \text{if } l \leqslant 2d. \end{cases}$$

Remark 3.3. The strategy of our proof is first to compute the resultants of cyclotomic polynomials (in Lemma 3.4) and then to reduce our problem to the cyclotomic case (see Lemma 3.5). Finally, we apply Lemma 2.1 to approximate our desired bounds.

LEMMA 3.4. *For any positive integers $m > n$, we have*

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

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

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

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

$$\mathscr{R}\left(\Phi_n(X), \frac{X^m - 1}{X^{m/l} - 1}\right) = \mathscr{R}(\Phi_n(X), \Phi_l(X^{m/l})) = \prod_{(i,n)=1} \Phi_l(\zeta_n^{im/l}) = l^{\phi(n)}.$$

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

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

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 $\mathscr{R}(\Phi_m, \Phi_n)$ is positive if and only if $m \neq 2$. Indeed, if $m \geqslant 3$ then complex conjugation is contained in $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ and so $\mathscr{R}(\Phi_m, \Phi_n) = N_{\mathbf{Q}(\zeta_m)/\mathbf{Q}}(\Phi_n(\zeta_m))$ is positive. If $m = 2$ then it is trivial to see that $\mathscr{R}(\Phi_2, \Phi_1) = -2$. This finishes our proof. ∎

Let $\overline{\mathscr{E}}$ be the complement of $\mathscr{E}$ in the set of all supersingular q-numbers with nonsquare q.

LEMMA 3.5. *Let the notation be as in Lemma* 3.2,

$$\left(\prod_{i > j} |\mathscr{R}(g_i, g_j)|^{e_i}\right)_{(p)} \text{ divides } 2^{[\sum_{\pi_i \in \overline{\mathscr{E}}} e_i \deg(g_i)/2]}_{(p)} \prod_{i \geqslant 2,\, l \mid 2m_i} l^{[e_i \deg(g_i)/(l-1)]}_{(p)}.$$

Proof. (a) Denote by $\mathscr{F}$ 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 $\prod |\mathscr{R}(\Phi_{m_i}, \Phi_{m_j})|_l$ over all j with $1 \leqslant j \leqslant i-1$, $\pi_j \notin \mathscr{F}$ attains its maximum when each $m_j = m_i/l^{i-j}$. In this case we have $\sum_{j=1}^{i-1} \phi(m_j) \leqslant \phi(m_i/l) + \phi(m_i/l^2) + \cdots + \phi(m_i/l^{i-1}) \leqslant \phi(m_i)/(l-1)$. Hence

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

(b) Assume q is a square. Since $\mathscr{F}$ is empty, by Proposition 3.1(I),

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

which divides $\prod_{i \geqslant 2,\, l \mid m_i} l_{(p)}^{[e_i \deg(g_i)/(l-1)]}$ by (8). This proves the lemma in the case.

(c) Assume q is a nonsquare. Then $\pi_i \in \mathscr{F}$ 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 the product $\prod_{i>j} |\mathscr{R}(g_i, g_j)|_{(p)}^{e_i}$ divides

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

it suffices to show that the two divisibilities

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

$$\prod_{i>j,\, \pi_j \notin \mathscr{F}} |\mathscr{R}(g_i, G_{m_j})|_{(p)}^{e_i} \text{ divides } l_{(p)}^{[e_i \deg(g_i)/(l-1)]} \tag{10}$$

hold. We first prove (9): Let σ and δ range over the embeddings of $\mathbf{Q}(\pi_i)$ in $\mathbf{C}$. By (7) we have

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

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

$$= \prod_{\pi_{i-1} \in \mathscr{F},\, \sigma} |2\pi_i^\sigma|_{(p)}^{e_i} \cdot \prod_{\pi_{i-1} \in \mathscr{F},\, \sigma \neq \delta} \left| \frac{\pi_i^{2\sigma} - \pi_i^{2\delta}}{\pi_i^\sigma - \pi_i^\delta} \right|_{(p)}^{e_i}$$

$$= 2_{(p)}^{[\sum_{\pi_{i-1} \in \mathscr{F}} e_i \deg(g_i)]} \cdot \prod_{\pi_{i-1} \in \mathscr{F}} \left| \frac{\Delta_{\mathbf{Z}[\pi_i^2]/\mathbf{Z}}}{\Delta_{\mathbf{Z}[\pi_i]/\mathbf{Z}}} \right|_{(p)}^{e_i}.$$

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 $\pi_{i-1} \in \mathscr{F}$ implies $\pi_{i-1}, \pi_i \in \bar{\mathscr{E}}$; but $e_{i-1} \geqslant e_i$ by our hypothesis, so we have

$$\sum_{\pi_{i-1} \in \mathscr{F}} e_i \deg(g_i) \leqslant \sum_{\pi_i \in \bar{\mathscr{E}}} e_i \deg(g_i)/2.$$

Then (9) follows.

Second, 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 $i > j$,

$$\prod_{\pi_j \notin \mathscr{F}} |\mathscr{R}(g_i, G_{m_j})|_{(p)} \text{ divides } 2^{\deg(g_i)} \prod_{\pi_j \notin \mathscr{F}} |\mathscr{R}(\Phi_{m_i}, \Phi_{m_j})|_{(2,p)}^{\deg(g_i)/\phi(m_i)}.$$

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

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

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

Note that $\Phi_{m_i}(X^2) = \Phi_{m_i}(X)\,\Phi_{2m_i}(X)$ when $2 \nmid m_i$. Further calculations via Lemma 3.4 and (8) yield that

$$\prod_{\pi_j \notin \mathscr{F}} |\mathscr{R}(G_{m_i}, G_{m_j})|_{(p)} \text{ divides } 2^{\deg(G_{m_i})} \prod_{\pi_j \notin \mathscr{F}} |\mathscr{R}(\Phi_{m_i}, \Phi_{m_j})|_{(2,p)}^{2/(2,m_i)}.$$

Note that $\deg(G_{m_i})/\phi(m_i) = 2/(2, m_i)$. Thus (11) holds.

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

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

But $\deg(E_{m_i,\pm 1}) = \deg(G_{m_i})/2$, thus (11) follows from Case 1.

By (11) and (8), the divisibility in (10) follows. This finishes our proof. ∎

Proof of Lemma 3.2. If $t = 1$, then $2^{d_{\mathscr{E}}} \prod_{i>j} |\mathscr{R}(g_i, g_j)|^{e_i} = 2^{d_{\mathscr{E}}}$ divides 2^d since $d_{\mathscr{E}} \leqslant d$. In this case it is straightforward to verify our assertion. For the rest of the proof we assume that $t \geqslant 2$. We shall prove the local bound first. Below let $l \neq p$.

(I) Let q be a nonsquare. Let $l > d \geqslant 2$. We claim that $\prod_{i>j} |\mathscr{R}(g_i, g_j)|_l^{e_i} = 1$. Suppose the contrary. By Lemma 3.5, we have that $l \mid m_i$ for some i. Suppose $m_i = l$ or $2l$, then $\mathbf{Q}(\pi_i) \neq \mathbf{Q}(\pi_i^2)$ and so $g_i = G_{m_i}$ by Proposition 3.1(III). Thence $d \geqslant \deg(g_i)/2 + 1 = \phi(m_i) + 1 = l$, which contradicts our assumption that $l > d$. Suppose $m_i \geqslant 3l$, then $l \leqslant \phi(m_i)/2 + 1 \leqslant \deg(g_i)/2 + 1 \leqslant d$ which is absurd.

Let q be a square. Let $l > 2d$. We claim that $\prod_{i>j} |\mathscr{R}(g_i, g_j)|_l^{e_i} = 1$. Suppose the contrary, that there are i and j such that $m_i/m_j = l^s$ for some integer $s > 0$. Then $2d \geqslant \phi(m_i) + \phi(m_j) = \phi(l^s m_j) + \phi(m_j) \geqslant l$, which leads to a contradiction.

Second, if $l > 2$ or q is a square, then by Lemma 3.5 the l-exponent of $2^{d_{\mathscr{E}}} \prod_{i>j} |\mathscr{R}(g_i, g_j)|^{e_i} \leqslant [(\sum_{i \geqslant 2} e_i \deg(g_i))/(l-1)] \leqslant [(2d-2)/(l-1)]$ since $e_1 \deg(g_1) \geqslant 2$.

Similarly, by Lemma 3.5, the 2-exponent of $2^{d_{\mathscr{E}}} \prod_{i>j} |\mathscr{R}(g_i, g_j)|_2^{e_i}$ is less than or equal to $\sum_{\pi_i \in \mathscr{E}} e_i \deg(g_i)/2 + \sum_{\pi_i \in \bar{\mathscr{E}}} e_i \deg(g_i)/2 + \sum_i e_i \deg(g_i) \leqslant 3d-2$.

(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 3.5; $(2^{d_{\mathscr{E}}} \prod_{i>j} |\mathscr{R}(g_i, g_j)|^{e_i})_{(p)}$ divides

$$2^{[(\sum_i e_i \deg(g_i))/2]} \prod_{l \mid 2m'_i} l^{[(e_i \deg(g_i))/(l-1)]}$$
$$< 2^d \prod_i \Bigg(\prod_{l \mid 2m'_i} l^{1/(l-1)} \Bigg)^{e_i \deg(g_i)}.$$

Note that $\phi(2m'_i) = \phi(m'_i) \leqslant 2d-2$, so by Lemma 2.1 we have

$$\prod_{l \mid 2m'_i} l^{1/(l-1)} < \log(50\phi(2m'_i)) < \log(100d - 100).$$

Thus

$$\Bigg(2^{d_{\mathscr{E}}} \prod_{i>j} |\mathscr{R}(g_i, g_j)|^{e_i} \Bigg)_{(p)} < 2^d (\log(100d-100))^{\sum_i e_i \deg(g_i)}$$
$$\leqslant (2 \log(100d-100))^{2d}.$$

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

$$2^d \prod_i \Bigg(\prod_{l \mid 2m'_i} l^{1/(l-1)} \Bigg)^{e_i \deg(g_i)} < 2^d (\log(2d-2))^{2d} < (2 \log(2d-2))^{2d}.$$

This finishes our proof. ∎

EXAMPLE 3.6. Those local upper bounds in Lemma 3.2 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 be even positive integers for $i = 1, ..., t$. Then we have $2^{d_{\mathscr{E}}} \prod_{i>j} |\mathscr{R}(g_i, g_j)|_l^{e_i} = l^{(2d-2)/(l-1)}$.

Here is a nontrivial 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 $\pi_i\in\overline{\mathscr{E}}$, so $2^{d_{\mathscr{E}}}\prod_{i>j}\mathscr{R}(g_i, g_j)^{e_j}=2^{2e_2+4e_3}$, while $2^{3d-2}=2^{6e_1+3e_2+3e_3-2}$.

4. TORSION-FREE MODULES AND FIBRE PRODUCTS

All rings are commutative with 1. Let $t\geqslant 2$. Let $\mathfrak{a}_i$ be an ideal of a ring R_i for $i=1, ..., t$. 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 $N_i\supseteq\mathfrak{a}_iM_i$ for $i=1, ..., t$, 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

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

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 θ_t: $M'_{t-1}/N'_{t-1}\to M_t/N_t$. (Note that γ_t-linear means that $\theta_t r'_{t-1}=(\gamma_t r'_{t-1})\,\theta_t$ for every $r'_{t-1}\in R'_{t-1}$.) Then we see that $M_1\times_{M_2/N_2} M_2\times\cdots\times_{M_t/N_t} M_t$ 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, p. 75] for Goursat's Lemma for groups).

LEMMA 4.1. *Let $R_1, ..., R_t$ 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 $R\to\prod_{j=1}^i R_j$. 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 $\mathfrak{a}'_{i-1}=\mathrm{Ker}(\rho''_i)$ with 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 $i=2, ..., t$ 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 $i=2, ..., t$.*

Proof. From the inductive definition of the fibre product, it suffices to prove the lemma for $t=2$. It is clear that $\mathfrak{a}'_1=R\cap(R_1\times\{0\})$, and by assumption it can be identified with 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 $\gamma: R_1/\mathfrak{a}'_1 \to R_2/\mathfrak{a}_2$ whose graph is the image of R. In fact, 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 $r_2 - r_3 \in \mathfrak{a}_2$. 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 is identical to R. ∎

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 $M \to \prod_{j=1}^i M_j$. 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 $N'_{i-1} = \mathrm{Ker}(\varrho''_i)$ with submodules of M_i and M'_{i-1}, respectively. We obtain γ_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 $R_1, \dots, R_t$ 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 that 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 non-zerodivisor $\alpha \in R - \{0\}$ 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 $r \in R - \{0\}$ be a nonzero divisor. 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 $i = 1, \dots, t$, 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 $M \to (M \otimes_{\mathbf{Z}_p} \mathbf{Q}_p) \otimes_K K_i$. 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 $i = 2, ..., t-1$, 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

$$\#\left(\left(\prod_{i=1}^t M_i\right)\Big/ M\right) = \#\left(\left(\prod_{i=1}^{t-1} M_i\right)\Big/ M'_{t-1}\right) \cdot \#\left(\left(M'_{t-1} \times M_t\right)\Big/ M\right)$$

$$= \left(\prod_{i=2}^{t-1} \#(M_i/N_i)\right) \cdot \#(M_t/N_t)$$

$$= \prod_{i=2}^{t} \#(M_i/N_i).$$

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

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

PROPOSITION 4.6. *Let $g_1, ..., g_t \in \mathbf{Z}[X]$ 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 $\# R_i/\mathfrak{a}_i = \prod_{j=1}^{i-1} |\mathscr{R}(g_i, g_j)|_l$ for all $i \geqslant 2$.*

Proof. Sending π to $(\pi_1, ..., \pi_t)$ 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 $\# R_i/\mathfrak{a}_i = \# R_i/\prod_{j=1}^{i-1} g_j(\pi_i)) = \prod_{j=1}^{i-1} |N_{\mathbf{Q}(\pi_i)/\mathbf{Q}}(g_j(\pi_i))|_l = \prod_{j=1}^{i-1} |\mathscr{R}(g_j, g_i)|_l$. ∎

5. ARBITRARY SUPERSINGULAR ABELIAN VARIETIES

In this section, we shall prove Theorems 1.1 and 1.2. We denote by $A[n]$ the subgroup of $A(\bar{\mathbf{k}})$ consisting of all points of order dividing n. 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 $g_i^{e_i}$ as in Section 1. 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, $V_l \xrightarrow{\sim} \prod_{i=1}^t V_l(A_i)$, and an injective map of R-modules, $T_l \xrightarrow{\gamma} \prod_{i=1}^t T_l(A_i)$. The image of γ in $T_l(A_i)$, denoted by $T_{l,i}$, is an $R_{l,i}$-submodule of finite index. We assume that A_i has been chosen in such a way that γ maps surjectively onto $T_l(A_i)$, that is $R_{l,i} = T_l(A_i)$. This can be seen from an elementary lemma below.

Lemma 5.1. *For every $\mathbf{Z}[\pi]_l$-submodule M of finite index in $T_l A$, there is an abelian variety A' over $\mathbf{k}$ and a $\mathbf{k}$-isogeny $A' \xrightarrow{\alpha} A$ such that $\alpha T_l A' = M$.*

Proof. Choose n so large that $l^n T_l A \subseteq M$. Let G be the image of $M/l^n T_l A$ in the isomorphism $T_l A/l^n T_l A \xrightarrow{\rho} A[l^n]$. Since G has a $\mathrm{Gal}(\bar{\mathbf{k}}/\mathbf{k})$-module structure and has order dividing l^n (coprime to p), it determines a finite étale subgroup scheme $\mathscr{G}$ of A over $\mathbf{k}$ with $\mathscr{G}(\bar{\mathbf{k}}) = G$. Let $A' := A/\mathscr{G}$. So the isogeny $A \xrightarrow{l^n} A$ factors through $A \xrightarrow{\beta} A'$ and we have $A \xrightarrow{\beta} A' \xrightarrow{\alpha} A$ with $\alpha\beta = l^n$. Note that $\alpha T_l A' \supseteq l^n T_l A$. It is clear that α maps $T_l A'/\beta T_l A$ onto $\alpha T_l A'/l^n T_l A$, whose image in ρ is exactly $G = \mathrm{Ker}(\beta)(\bar{\mathbf{k}})$. Therefore, we have $\alpha T_l A' = M$. ∎

Clearly, T_l is a torsion-free R_l-module. Let π_i be 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 5.2. *Let the notation be as above. Let $r \in R$ be a non-zerodivisor. There is an R_l-module homomorphism*

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

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

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

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

Applying Lemma 4.4., there is a map α_l with $\#\mathrm{Ker}(\alpha_l) = \#\mathrm{Coker}(\alpha_l)$ dividing $\prod_{i=2}^{t} \prod_{j=1}^{i-1} |\mathscr{R}(g_i, g_j)|_l^{e_i}$. 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 $(l, \pi_i) \in \{2\} \times \mathscr{E}$: 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

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

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 5.3. If we order the e_i such that $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_t$ 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

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

Proof of Theorem 1.1. Suppose $d = \dim A \geqslant 2$. 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 $\varphi := \prod_{l \neq p} \varphi_l$, with the φ_l as in Lemma 5.2. Our assertion follows from Lemmas 5.2 and 3.2. ∎

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 with the same bounds.

REFERENCES

1. H. Cohen, "A Course in Computational Algebraic Number Theory," Graduate Texts in Mathematics, Vol. 138, Springer-Verlag, New York/Berlin, 1993.
2. G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 5th ed., Oxford Science Publ., Oxford, UK, 1979.

3. K. Ireland and M. Rosen, “A Classical Introduction to Modern Number Theory,” 2nd ed., Graduate Texts in Mathematics, Vol. 84, Springer, New York/Berlin, 1992.
4. S. Lang, “Algebra,” 3th ed., Addison–Wesley, Reading, MA, 1993.
5. K.-Z. Li and F. Oort, “Moduli of Supersingular Abelian Varieties,” Lecture Notes in Mathematics, Vol. 1680, Springer-Verlag, New York/Berlin, 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, New York/Berlin, 1986.
10. H. June Zhu, Group structures of elementary supersingular abelian varieties over finite fields, *J. Number Theory* **81** (2000), 292–309.