<table>
<thead>
<tr>
<th>Title</th>
<th>Universal bound for isogenies of elliptic curves over number fields (Algebraic Number Theory and Related Topics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Kawamura, Takashi</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 2003, 1324: 161-173</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2003-05</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/43157">http://hdl.handle.net/2433/43157</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
Universal bound for isogenies of elliptic curves over number fields

東京大学・大学院数理科学研究科 河村 隆 (Takashi Kawamura)
Graduate School of Mathematical Sciences,
University of Tokyo

1 Introduction

Let $E$ and $E'$ be isogenous elliptic curves defined over a number field $k$ of degree $d$. Masser and Wüstholz [6] proved the existence of a constant $c$ depending effectively only on $d$ such that there is an isogeny between $E$ and $E'$ whose degree is at most $c\{w(E)\}^4$, where $w(E) = \max\{1, h(g_2), h(g_3)\}$ when $E$ is identified with its Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$. Here $h$ denotes the absolute logarithmic Weil height. But they did not give an explicit formula of $c$. The purpose of this paper is to express $c$ as an explicit function of $d$ bounded by a polynomial when $E$ has no complex multiplication. The main result is as follows.

**Theorem.** Given a positive integer $d$, there exists a constant $c(d)$ depending only on $d$ with the following property. Let $k$ be a number field of degree at most $d$, and let $E$ be an elliptic curve defined over $k$ without complex multiplication. Suppose $E$ is isogenous to another elliptic curve $E'$ defined over $k$.

(i) Then there is an isogeny between $E$ and $E'$ whose degree is at most $c(d)\{w(E)\}^4$, where

$$c(d) = 6.55 \times 10^{64}\{\max\{1.09 \times 10^7d^{1.45}\{15.5 \max\{\log(88.8d + 2.8), 38.4\} + 342.3\}^{1.45}, 1.82 \times 10^{63}\}\}^{210}\{11.4d + 55.3\}^{20}.$$ 

In particular the function $c(d)$ in $d$ increases as $1.9 \times 10^{1956}d^{325}$ when $d$ goes to infinity.

(ii) $c(1) = 8.2 \times 10^{13415}$ when $d = 1$, i. e., $k = \mathbb{Q}$.

We proceed along the line of [6]. Main devices in calculating $c$ are as follows. First we distinguish five constants which are unified as $c_3$ in [6, Lemma 3.3.] and those in [6, Lemmas 3.4 and 4.4]. Secondly we improve the relative degree of the field generated by the values of Weierstrass $p$-functions and their derivatives over $k$ from 81 to 36.
Pellarin [8] found an upper bound of the form $4.2 \times 10^{61} d^4 \max\{1, \log d\}^2 h(E)^2$, where $h(E) = \max\{1, h(j)\} + \max\{1, h(1, g_2, g_3)\}$ and $j$ is the $j$-invariant of $E$. But his Lemme 3.2 seems to contain some mistakes, because the cardinality of $\mathbb{C}$-linear independent monic monomials $X^\lambda$ on $G$ such that $\lambda \leq D$, $M_D$, is $\prod_n (D_n + 1)$ on line 21 of page 219. This lemma is used in the proof of Proposition 3.1, and plays a crucial role in the main estimate. We hope that his proof will be corrected.

2 Preliminary estimates

Let $\Omega$ be a lattice in the complex plane. Let $(\omega_1, \omega_2)$ be a basis of $\Omega$ such that $\tau = \omega_2/\omega_1$ belongs to the standard fundamental region for the modular group. So $|\tau| \geq 1$, $x = \text{Re} \, \tau$ satisfies $|x| \leq \frac{1}{2}$, and $y = \text{Im} \, \tau$ satisfies $y \geq \frac{\sqrt{3}}{2}$. Let $A$ be the area of the unit of $\Omega$, which equals $y|\omega_1|^2$. Let $g_2$ and $g_3$ be the invariants of $\Omega$, let $p(z)$ be the corresponding Weierstrass function, and $\gamma = \max\{|\frac{1}{4}g_2|^\frac{1}{2}, |\frac{1}{4}g_3|^\frac{1}{3}\}$.

**Lemma 2.1.** There exists a function $\theta_0(z)$ such that $\theta(z) = \gamma \theta_0(z)$ and $\tilde{\theta}(z) = p(z)\theta_0(z)$ are entire functions, with no common zeros, that satisfy

$$|\log \max\{|\theta(z)|, |\tilde{\theta}(z)|\} - \pi|z|^2/A| < 10.5y$$

for all complex $z$.

**Proof.** This is [4, Lemma 3.1] except for the estimation of the constant on the right-hand side of the inequality, which is 10.5. q. e. d.

**Lemma 2.2.** Let $z$ be a complex number not in $\Omega$, and $||z||$ be the distance from $z$ to the nearest element of $\Omega$. Then

$$|p(z) - p(\omega_2/2)| < 77244||z||^{-2}.$$ 

**Proof.** This is [6, Lemma 3.2] except for the estimation of the constant on the right-hand side of the inequality, which is 77244. q. e. d.

Let $d$ be a positive integer, and $k$ be a number field of degree at most $d$. Moreover, $g_2$ and $g_3$ are assumed to lie in $k$, and $w = \max\{1, h(g_2), h(g_3)\}$.

**Lemma 2.3.** There are constants $c_{1,i}$ ($1 \leq i \leq 5$), depending only on $d$, such that

(i) $c_{1,1}^{-w} \leq \gamma < c_{1,1}^w$,

(ii) $y < c_{1,2}w$, 


(iii) $A > c_{1,3}^{-w}$,
(iv) $|\omega_1| > c_{1,4}^{-w}$,
(v) $A^{-1}|\omega_2|^2 < c_{1,5}w$,

where $c_{1,1} = 2e^{0.5d}$, $c_{1,2} = 3.2d + 1.2$, $c_{1,3} = 16.6e^{3.8d}$, $c_{1,4} = 4.37e^{1.9d}$, and $c_{1,5} = 3.2d + 1.5$.

**Proof.** This is [6, Lemma 3.3] except for the estimation of the constants $c_{1,i}$ ($1 \leq i \leq 5$).

Lemma 2.4. There is a constant $c_2$ depending only on $d$ and a positive integer $b < 2.22^w$ with the following properties. Suppose $n$ is a positive integer, $\zeta$ is an element of $\Omega/n$ not in $\Omega$, and write $\xi = p(\zeta)$.

Then

(i) $\xi$ is an algebraic number of degree at most $dn^2$ with $h(\xi) < 8.55w$,
(ii) $bn^2\xi$ is an algebraic integer, and $|\xi| < c_2^w n^2$,

where $c_2 = 2.951 \times 10^6 \exp(3.8d)$.

**Proof.** When $\frac{1}{4}g_2$ and $\frac{1}{4}g_3$ are algebraic integers, from the proof of [6, Lemma 3.4] $\xi$ has degree at most $dn^2$, and $n^2\xi$ is an algebraic integer. In the general case we can find a positive integer $b_0 \leq (\sqrt[3]{2}e^{\frac{1}{6}})^w$ such that $\frac{1}{4}b_0^4g_2$ and $\frac{1}{4}b_0^6g_3$ are algebraic integers. These correspond to the lattice $\Omega_0 = \Omega/b_0$ with Weierstrass function $p_0(z) = b_0^2 p(b_0 z)$. So $\xi_0 = p_0(\zeta/b_0)$ has degree at most $dn^2$, and $n^2\xi_0$ is an algebraic integer. As $\xi = b_0^{-2}\xi_0$, $n^2\xi_0 = b_0^2 n^2 \xi$ is an algebraic integer, $b_0^2 n^2 \xi \leq (\sqrt[3]{4}e^{\frac{1}{3}})^w n^2 < 2.22^w n^2 \xi$, and $\xi$ is an algebraic number of degree at most $dn^2$.

The Néron-Tate height $q(P)$ of the point $P$ in $\mathbb{P}^2$ with projective coordinates $(1, p(\zeta), p'(\zeta))$ satisfies $q(P) = 0$. By [3, Lemme 3.4] the Weil height $h(P)$ satisfies $h(P) \leq q(P) + 3w + 8 \log 2 \leq (3 + 8 \log 2)w$. So $h(\xi) \leq h(P) < 8.55w$.

By Lemma 2.2

$$|\xi| < |p(\omega_2/2)| + c_3 \|\zeta\|^{-2},$$  \hspace{1cm} (1)

where $c_3 = 77244$. As $p(\omega_2/2)$ is a root of $4x^3 - g_2x - g_3 = 0$, from Cardano's Formula $|p(\omega_2/2)| \leq (|g_3| + \sqrt{|g_3|^2 + |g_2|^3/27})^{\frac{1}{3}} < (1.3e^{\frac{3}{2}})^w$.

By Lemma 2.3(iv) $\|\zeta\|^{-2} \leq n^2|\omega_1|^{-2} < n^2 c_{1,4} 2^w$. From (1)

$$|\xi| \leq (1.3e^{\frac{3}{2}})^w + c_3 c_{1,4} 2^w n^2 < \{2.951 \times 10^6 \exp(3.8d)\}^w n^2 = c_2^w n^2.$$
3 The Main Proposition: construction

Let $E$ and $E^*$ be elliptic curves defined over $\mathbb{C}$, and $\Omega$ and $\Omega^*$ be their period lattices respectively. Let $\varphi$ be an isogeny from $E^*$ to $E$. It is said to be normalized if it induces the identity on the tangent spaces. Then $\Omega^* \subset \Omega$, and $[\Omega : \Omega^*]$ is the degree of $\varphi$. It is said to be cyclic if its kernel is a cyclic group.

Main Proposition. Given a positive integer $d$, there exists a constant $c_4(d)$ depending only on $d$, with the following property. Let $k$ be a number field of degree at most $d$, and let $E$ and $E^*$ be elliptic curves defined over $k$ without complex multiplication. Suppose there is a normalized cyclic isogeny $\varphi$ from $E^*$ to $E$ of degree $N$. Then there is an isogeny between $E$ and $E^*$ of degree at most $c_4(d)\{w(E) + w(E^*) + \log N\}^4$, where

$$c_4(d) = 1.47 \times 10^{16} \max\{(5910d15.5 \max\{\log(7.4d + 2.8)\}, 38.4) + 342.3\}^{1.45}, 1.82 \times 10^{63}\}^{42}.$$

Before the proof of Main Proposition we need Lemmas 3.1-3.5. The body of the proof is described in Section 4.

Let $\omega_1, \omega_2$ and $\omega_1^*, \omega_2^*$ be bases of $\Omega$ and $\Omega^*$ respectively such that $\tau = \omega_2/\omega_1$ and $\tau^* = \omega_2^*/\omega_1^*$ lie in the standard fundamental region. Then there are integers $m_{ij}$ ($i, j = 1, 2$) such that

$$\omega_1^* = m_{11}\omega_1 + m_{12}\omega_2, \quad \omega_2^* = m_{21}\omega_1 + m_{22}\omega_2 \quad (2)$$

and $m_{11}m_{22} - m_{12}m_{21} = N$. Write $h = w(E) + w(E^*) \geq 2$.

Lemma 3.1. We have $|m_{ij}| < (7.4d + 2.8)N1\frac{3}{2}h$ ($i, j = 1, 2$).

Proof. This is [6, Lemma 4.1] except for the estimation of the constant on the right-hand side of the inequality, which is $7.4d + 2.8$. Q. e. d.

Let $C$ be a sufficiently large constant depending only on $d$, $L = h + \log N$, $D = [C^{20}L^2]$ and $T = [C^{39}L^4]$. Let $p(z)$ and $p^*(z)$ be the Weierstrass functions corresponding to $\Omega$ and $\Omega^*$ respectively. For $t > 0$ and independent variables $z_1$ and $z_2$ let $D_1(t)$ be the set of differential operators of the form

$$\partial = (\partial/\partial z_1)^{t_1}(\partial/\partial z_2)^{t_2} \quad (t_1 \geq 0, \ t_2 \geq 0, \ t_1 + t_2 < t).$$

Lemma 3.2. There is a nonzero polynomial $P(X_1, X_2, X_1^*, X_2^*)$ of degree at most $D$ in each variable, whose coefficients are rational integers of absolute values at most $\exp(c_5TL)$, such that the function

$$f(z_1, z_2) = P(p(z_1), p(z_2), p^*(m_{11}z_1 + m_{12}z_2), p^*(m_{21}z_1 + m_{22}z_2))$$
satisfies $\partial f(\omega_1/2, \omega_2/2) = 0$ for all $\partial$ in $D_i(8T)$, where

$$c_5 = 156 \log C + 12 \max\{\log(7.4d + 2.8), \ 38.4\} + 251.3.$$  

Proof. Let $M$ denote any monomial of degree at most $D$ in each of the four functions appearing in $f$, that is,

$$M = \{p(z_1)\}^{d_1}\{p(z_2)\}^{d_2}\{p^*(m_{11}z_1 + m_{12}z_2)\}^{d_3}\{p^*(m_{21}z_1 + m_{22}z_2)\}^{d_4}$$

with $0 \leq d_i \leq D (1 \leq i \leq 4)$, and let $\partial$ be any operator of $D_i(8T)$. Then $\partial M$ can be written as a polynomial in the four numbers $m_{ij} (i, j = 1, 2)$ and the twelve functions obtained from the above four by replacing the Weierstrass functions by their first and second derivatives. From Baker's Lemma [2, Lemma 3]

$$\frac{d^j}{dz^j}\{p(z)\}^{k} = \sum u(t, t', t'', j, k)\{p(z)\}^{t}\{p'(z)\}^{t'}\{p'(z)\}^{t''},$$

where the sum is taken over nonnegative integers $t, t'$ and $t''$ which satisfy $2t + 3t' + 4t'' = j + 2k$, and $u(t, t', t'', j, k)$ are integers of absolute values at most $j!48^j(7!2^8)^k$. So the total degree of $\partial M$ is at most $3D + 8T - 1 + 0.5 \cdot (8T - 1) + D < 12(D + T)$. And its coefficients are integers of absolute values at most $(8T - 1)!48^{8T - 1}(7!2^8)^D < T^{8T}(2^{56} \times 3^8)^{D+T}$.

By Lemma 3.1 we have $\log |m_{ij}| < (\log c_6 + 1)L/2$, where $c_6 = 7.4d + 2.8$. From (2) the twelve functions at $(z_1, z_2) = (\omega_1/2, \omega_2/2)$ take the values

$$p^{(t)}(\omega_j/2), \ p^{*(t)}(\omega_j^*/2) (t = 0, 1, 2; j = 1, 2).$$

By Lemma 2.4 $h(p(\omega_j/2))$ and $h(p^*(\omega_j^*/2))$ are at most $8.55L$. Both $p'(\omega_j/2)$ and $p''(\omega_j^*/2)$ are zero. And

$$h(p''(\omega_j/2)) = h(6p(\omega_j/2)^2 - g_2/2) \leq 2h(p(\omega_j/2)) + h(g_2) + \log 12 + \log 2 < 19.7L.$$ 

So does $h(p^{*(2)}(\omega_j^*/2))$. Thus $m_{ij}$ and the values of the twelve functions have heights at most $c_7L$, where

$$c_7 = \max\{0.5 + 0.5\log(7.4d + 2.8), \ 19.7\}.$$ 

As $p(\omega_j/2)$ and $p^*(\omega_j^*/2)$ are roots of cubic equations with coefficients in $k$, and $p''(\omega_j/2)$ and $p^{*(2)}(\omega_j^*/2)$ lie in the field generated by $p(\omega_j/2)$ and $p^*(\omega_j^*/2)$ over $k$, these values lie in $k'$ whose degree is at most $36d$. The conditions of Lemma 3.2 amount to $R = 4T(8T + 1)$ homogeneous linear equations in $S = (D + 1)^4$ unknowns with coefficients in $k'$. By
Siegel's Lemma [1, Proposition], if $S \geq 2 \times 36dR$, these can be solved in rational integers, not all zero, of absolute values at most $S \exp(c_8)$, where $c_8$ is the height of linear equations. To satisfy the condition $S \geq 72dR$ it suffices that

$$C^{80}L^8 > 2305dC^{78}L^8,$$

so $C > 48.1\sqrt{d}$. \hfill (3)

Next we calculate $c_8$. By Lemma 2.4 there is a positive integer $b \leq 2.22^w$ such that $4bp(\omega_j/2)$ is an algebraic integer. Since $p''(\omega_j/2) = 6p(\omega_j/2)^2 - g_2/2$, and there is a positive integer $b_2 \leq e^w$ such that $b_2g_2$ is an algebraic integer, $16b^2b_2p''(\omega_j/2)$ is an algebraic integer. If we multiply $\partial M$ at $(z_1, z_2) = (\omega_1/2, \omega_2/2)$ by an integer at most $(16 \times 2.22^2L^e)^{12(D+T)}$, every term is an algebraic integer. As $h(\sum_{i=1}^n a_i) \leq \max h(a_i) + \log n$ for algebraic integers $a_i$,

$$S \exp(c_8) \leq (D+1)^4(16 \times 2.22^2L^e)^{12(D+T)}13H_{12(D+T)}
\exp(12c_8(D+T)L) < \exp(c_5TL).$$

q. e. d.

Let $\theta_0(z)$ and $\theta_0^*(z)$ be the functions in Lemma 2.1 corresponding to $p(z)$ and $p^*(z)$ respectively. So the function

$$\Theta(z_1, z_2) = \{\theta_0(z_1)\theta_0(z_2)\theta_0^*(m_{11}z_1 + m_{12}z_2)\theta_0^*(m_{21}z_1 + m_{22}z_2)\}^D$$

is entire. Let $F(z_1, z_2) = \Theta(z_1, z_2)f(z_1, z_2)$.

**Lemma 3.3.** The function $F(z_1, z_2)$ is entire. Further, for any complex number $z$ and any operator $\partial$ in $D_i(4T+1)$ we have

$$|\partial F(\omega_1z, \omega_2z)| < \exp\{c_9L(T + D|z|^2)\},$$

where

$$c_9 = 234\log C + 154.8d + 2\log(7.4d + 2.8) + 12\max\{\log(7.4d + 2.8),
38.4\} + 423.5.$$

**Proof.** Let $\gamma, \gamma^*, \theta, \theta^*, \tilde{\theta}, \tilde{\theta}^*$ be as in Lemma 2.1 corresponding to $p, p^*$. Then $F(z_1, z_2)$ can be expressed as a polynomial in the eight functions

$$\gamma^{-1}\theta(z_i), \tilde{\theta}(z_i), \gamma^{-1}\theta^*(m_{i1}z_1 + m_{i2}z_2), \tilde{\theta}^*(m_{i1}z_1 + m_{i2}z_2) \ (i = 1, 2),$$

so it is entire. It is the quadrihomogenized version of $P$ in Lemma 3.2.
Let $M_0 = \max |m_{ij}|$, $A_0 = \min(A, A^*)$, and $\delta = M_0^{-1}A_0^{\frac{1}{2}}$, where $A$ and $A^*$ are determinants of $\Omega$ and $\Omega^*$ respectively. For any complex number $z$ let $z_1$ and $z_2$ be complex numbers satisfying

$$|z_i - \omega_i z| = \delta \quad (i = 1, 2). \quad (5)$$

We claim that $|F(z_1, z_2)| < \exp\{c_{10}L(T + D|z|^2)\}$, where $c_{10} = 156\log C + 147.2d + 12\max\{\log(7.4d + 2.8), 38.4\} + 404.3$. By Lemma 2.1

$$\log \max\{|\theta(z_i)|, |\tilde{\theta}(z_i)|\} < 10.5y + \pi A^{-1}|z_i|^2$$

$$\leq 10.5(y + A^{-1}\delta^2 + A^{-1}|\omega_i|^2|z|^2) \quad (i = 1, 2).$$

As $A^{-1}\delta^2 \leq M_0^{-2} \leq 1$, from Lemma 2.3(i)(ii)(v) the first two functions in (4) have absolute values at most

$$c_{1,1}^L \exp\{10.5(c_{1,2}L + 1 + c_{1,5}L|z|^2)\} < \exp\{(11.5c_{1,5} + 5.25)L(1 + |z|^2)\},$$

for $c_{1,5} > c_{1,2} > \log c_{1,1}$.

The last two expressions in (4) are estimated similarly. From (2) and (5) $z_i^* := m_{i1}z_1 + m_{i2}z_2$ satisfy $|z_i^* - \omega_i^* z| \leq 2M_0\delta \quad (i = 1, 2)$. Thus

$$\log \max\{|\theta^*(z_i^*)|, |\tilde{\theta}^*(z_i^*)|\} < 10.5(y^* + 4M_0^2A^{*-1}\delta^2 + A^{*-1}|\omega_i^*|^2|z|^2)$$

$$\quad (i = 1, 2).$$

By Lemma 2.3 the last two functions have absolute values at most

$$c_{1,1}^L \exp\{10.5(c_{1,2}L + 4 + c_{1,5}L|z|^2)\} < \exp\{(11.5c_{1,5} + 21)L(1 + |z|^2)\}.$$ 

By Lemma 3.2

$$|F(z_1, z_2)| < \exp(c_5TL) \exp\{(46c_{1,5} + 84)DL(1 + |z|^2)\}(D + 1)^4$$

$$< \exp\{c_{10}L(T + D|z|^2)\},$$

which is the claim.

By the Cauchy Integral Formula

$$|\partial F(\omega_1 z, \omega_2 z)| = \left| \frac{t_1!t_2!}{(2\pi i)^2} \oint \oint \frac{F(z_1, z_2)}{(z_1 - \omega_1 z)^{t_1+1}(z_2 - \omega_2 z)^{t_2+1}} dz_1 dz_2 \right|$$

$$< t_1!t_2!\delta^{-(t_1+t_2)} \exp\{c_{10}L(T + D|z|^2)\},$$

where the integrals are around the circles (5). From Lemma 2.3(iii) and Lemma 3.1

$$\delta = M_0^{-1}A_0^{\frac{1}{2}} > (7.4d + 2.8)^{-1}N^{-\frac{1}{2}}h^{-1}c_{1,3}^{-\frac{1}{2}}$$

$$> \{6.72(7.4d + 2.8)^{\frac{1}{2}} \exp(1.9d)\}^{-L} =: c_{11}^{-L}.$$
$|\partial F(\omega_1 z, \omega_2 z)| < (4T)!c_{11}^{4LT} \exp\{c_{10}L(T + D|z|^2)\} \exp\{c_9 L(T + D|z|^2)\}.$

q. e. d.

Let $Q$ be the unique integral power of 2 that satisfies

$C^{17/8} < Q \leq 2C^{17/8}.$

**Lemma 3.4.** For any odd integer $q$ and $\zeta = q/Q$, we have

$|\Theta(\omega_1\zeta, \omega_2\zeta)| > \exp(-84DLQ^2).$

Further, for any $\partial$ in $D_i(4T + 1)$ such that $\partial f(\omega_1\zeta, \omega_2\zeta) \neq 0$, we have

$|\partial f(\omega_1\zeta, \omega_2\zeta)| > \exp(-c_{12}TLQ^6),$

where $c_{12} = 16d[290 \log C + 15.5 \max\{\log(7.4d + 2.8), 38.4\} + 342.3].$

**Proof.** By Lemma 2.3(i) and Lemma 2.4(i)

$$\max\{\gamma, |p(\omega_j\zeta)|\} < \exp(8.55dhQ^2) (j = 1, 2).$$

From Lemma 3.1 and Lemma 2.3(ii)

$$|\theta_0(\omega_j\zeta)| > \exp(-10.5y - 8.55dhQ^2) > \exp(-10.5d(1 + c_{1,2}/Q^2)hQ^2),$$

and the same bound holds for $|\theta_0^* (\omega_j^* \zeta)| (j = 1, 2).$ Thus

$$|\Theta(\omega_1\zeta, \omega_2\zeta)| > \exp(-4D \times 10.5d(1 + c_{1,2}/Q^2)hQ^2) > \exp(-84DLQ^2),$$

for by (3) $Q^2 > C^{11/4} > 48^4d^2 > 3.2d + 1.2 = c_{1,2}$.

$\alpha := \partial f(\omega_1\zeta, \omega_2\zeta)$ is estimated as in the proof of Lemma 3.2. $\alpha$ is a polynomial in the $m_{ij}$ ($i, j = 1, 2$) and the twelve numbers $p^{(t)}(\omega_j\zeta)$, $p^{*(t)}(\omega_j^* \zeta)$ ($j = 1, 2; t = 0, 1, 2$). Let $\partial M$ be as in the proof of Lemma 3.2, and $\partial$ be any operator of $D_i(4T + 1).$ From Baker's Lemma the total degree of $\partial M$ is at most $6(D + T)$, and the absolute values of its coefficients are at most $T^{4T}(2^{24} \times 3^4)^{D+T}$.

By Lemma 2.4 there is a positive integer $b < 2.22^w$ such that $bQ^2 p(\omega_j\zeta)$ is an algebraic integer. Since $p'(\omega_j\zeta)^2 = 4p(\omega_j\zeta)^3 - g_2 p(\omega_j\zeta) - g_3$, and there is a positive integer $b_3 \leq e^w$ such that $b_3g_3$ is an algebraic integer, $(b^3 b_2 b_3)\frac{1}{3} Q^3 p'(\omega_j\zeta)$ is an algebraic integer. And $2b^2 b_2 Q^4 p''(\omega_j\zeta)$ is an algebraic integer. If we multiply $\partial M$ at $(z_1, z_2) = (\omega_1\zeta, \omega_2\zeta)$ by
a positive integer at most \((2 \times 2.22^{2L} e^{1.5L} Q^{4})^{6(D+T)}\), every term is an algebraic integer. By Lemma 2.4 \(h(p(\omega_j \zeta))\) and \(h(p^*(\omega_j^* \zeta))\) are at most \(8.55L\),

\[
h(p'(\omega_j \zeta)) \leq \frac{1}{2} \{2h(p(\omega_j \zeta)) + \log 4 + h(g_2) + h(p(\omega_j \zeta)) + h(g_3) + \log 3\} < 2 \times 8.55L + L + \log 3 < 19.7L,
\]

and \(h(p''(\omega_j^* \zeta)), h(p'''(\omega_j^* \zeta))\) and \(h(p'\prime\prime(\omega_j^* \zeta))\) are at most \(19.7L\). Thus at \((z_1, z_2) = (\omega_1 \zeta, \omega_2 \zeta)\),

\[
\exp(h(\partial M)) \leq (2 \times 2.22^{2L} e^{1.5L} Q^{4})^{12(D+T)} 17H_{6(D+T)} T^{4T}(2^{24} \times 3^{4})^{D+T} \exp\{6c_7(D + T)L\}.
\]

\(\alpha\) is a linear combination of \(\partial M\) with rational integer coefficients whose absolute values are at most \(\exp(c_5 T L)\). So

\[
h(\alpha) \leq \log(D + 1)^4 + c_5 TL + h(\partial M)
\]

\[
< [290 \log C + 15.5 \max\{\log(7.4d + 2.8), 38.4\} + 342.3]TL.
\]

Next we estimate the degree of \(\alpha\), \(\deg \alpha\). Since

\[
Q(\alpha) = Q(p^{(t)}(\omega_j \zeta), p^{*^{(t)}}(\omega_j^* \zeta)) (j = 1, 2; t = 0, 1, 2)
\]

\[
\subset k(p(\omega_j \zeta), p^*(\omega_j^*), p'(\omega_j \zeta), p''(\omega_j^* \zeta)),
\]

the degrees of \(p(\omega_j \zeta)\) and \(p^*(\omega_j^* \zeta)\) are at most \(dQ^2\) by Lemma 2.4(i), and \([k(p(\omega_j \zeta), p'(\omega_j \zeta)) : k(p(\omega_j \zeta))]\leq 2\),

\[
\deg \alpha = [Q(\alpha) : Q] \leq d(Q^2)^4 2^4 = 16dQ^8.
\]

Hence \(|\alpha| \geq \exp\{-(\deg \alpha)h(\alpha)\} > \exp(-c_{12} T L Q^8)\). q.e.d.

**Lemma 3.5.** If \(C\) satisfies \(C > (256/\log 2)c_{12}\) with the constant \(c_{12}\) in Lemma 3.4, then for any odd integer \(q\) and any \(\partial\) in \(D_t(4T + 1)\) we have \(\partial f(q \omega_1/Q, q \omega_2/Q) = 0\).

**Proof.** Assume that there exist an odd integer \(q\) and an operator \(\partial\) in \(D_t(4T + 1)\) such that \(\alpha = \partial f(\omega_1 \zeta, \omega_2 \zeta) \neq 0\) for \(\zeta = q/Q\). We can suppose that \(0 < \zeta < 1\), and that

\[
\alpha \Theta(\omega_1 \zeta, \omega_2 \zeta) = G(\zeta),
\]

where \(G(z) = \partial F(\omega_1 z, \omega_2 z)\) and \(\partial\) is of minimal order.

\(G^{(t)}(z)\) is a linear combination of the \(\partial f(\omega_1 z, \omega_2 z)\) for \(\partial\) in \(D_t(t + 1 + 4T)\), so by Lemma 3.2 and periodicity

\[
G^{(t)}(s + 1/2) = 0
\]
for any integer \( t \) with \( 0 \leq t < 4T \) and any integer \( s \). We apply the Schwarz Lemma to (7) for \( 0 \leq s < S \), where \( S = |C^{18}L| \). Then \( |G(\zeta)| \leq 2^{-4TS} M_1 \), where \( M_1 \) is the supremum of \( |G(z)| \) for \( |z| \leq 5S \). By Lemma 3.3 \( M_1 < \exp\{25c_9 L(T + DS^2)\} \) \( < \exp(50c_9 LDS^2) \). If \( C > (25/\log 2)c_9 \), then \( \exp(50c_9 LDS^2) < 2^{2TS} \), so \( |G(\zeta)| < 2^{-2TS} \). By (6) and Lemma 3.4

\[
|\alpha| < 2^{-2TS} \exp(84DLQ^2) < 2^{-TS},
\]

where the second inequality follows, because \( C > (84/\log 2)^{4/131} \). But also from Lemma 3.4 we have the lower bound

\[
|\alpha| > \exp(-c_{12}TLQ^8).
\]

If

\[
C > (256/\log 2)c_{12}
\]

\[
= 5909d[290 \log C + 15.5 \max\{\log(7.4d + 2.8), 38.4\}
+ 342.3],
\]

then \( 2^{TS} > \exp(c_{12}TLQ^8) \), which contradicts (8) and (9). As \( 256c_{12} > 25c_9 \), (10) implies that \( C > (25/\log 2)c_9 \). q. e. d.

4 Proof of Main Proposition: deconstruction

Let \( G = E^2 \times E^{*2} \) embedded in \( \mathbb{P}^{81} \) by Segre embedding. Let \( \epsilon \) be the exponential map from \( \mathbb{C}^4 \) to \( G \) obtained from the functions \( p(z_1), p(z_2), p^*(z_1^*), p^*(z_2^*) \) and their derivatives for independent complex variables \( z_1, z_2, z_1^*, z_2^* \). Define a subspace \( Z \) of \( \mathbb{C}^4 \) by the equations

\[
z_1^* = m_{11}z_1 + m_{12}z_2, \quad z_2^* = m_{21}z_1 + m_{22}z_2.
\]

Write \( O_G \) for the zero of \( G \), and let \( \Sigma \) and \( \Sigma_0 \) be the sets of even and odd multiples of the point \( \sigma = \epsilon(\omega_1/Q, \omega_2/Q, \omega_1^*/Q, \omega_2^*/Q) \) in \( G \) respectively. We use Philippon’s zero estimate.

**Lemma 4.** There is a connected algebraic subgroup \( H = \epsilon(W) \neq G \) of \( G \) such that

\[
T^\rho R \Delta < c_{13} D^r,
\]

where \( W \) is a subspace of \( \mathbb{C}^4 \), \( \rho \) is the codimension of \( Z \cap W \) in \( Z \), \( R \) is the number of points in \( \Sigma \) distinct modulo \( H \), \( \Delta \) is the degree of \( H \), \( r \) is the codimension of \( H \) in \( G \), and \( c_{13} = 4.032 \times 10^7 \).
Proof. By Lemma 3.5 there is a polynomial, homogeneous of degree $D$, that vanishes to order at least $4T + 1$ along $\epsilon(Z)$ at all points of $\Sigma_0$, but does not vanish identically on $G$. Let $\Sigma(4) = \{\sum_{i=1}^{4} \sigma_i | \sigma_i \in \Sigma\}$, so $\Sigma_0 = \sigma + \Sigma(4)$. From [5, Lemma 1] translations on an elliptic curve are described by homogeneous polynomials of degree 2. Accroding to Philippon's zero estimate [9, Theorème 1], there exists a connected algebraic subgroup $H = \epsilon(W) \neq G$ of $G$ such that

$$T^r \Delta \leq \deg G \times 2^\dim G (2D)^r.$$

As $\deg G = 3^{2\dim G} \times 4! = 2^3 \times 3^9$ and $r \leq 4$, $T^r \Delta < c_{13} D^r$. q. e. d.

Now we can give the proof of Main Proposition. We want to find a nontrivial graph subgroup of an isogeny $E \to E^*$ of small degree. We consider the three cases $\rho = 2, 1, 0$ in (11).

When $\rho = 2$, $T^2 \Delta < c_{13} D^2$. So

$$R < c_{13} D^2 \Delta < 4.04 \times 10^7 C^2 D^{r-4} = c_{14} C^2 D^{r-4}.$$  (12)

Thus $r = 4$, $H = O_G$, and $R = Q/2$. If

$$C > 2^8 c_{14}^8 \approx 1.817 \times 10^{63},$$  (13)

then $Q/2 > C^{17/8}/2 > c_{14} C^2$ contradicting (12). Hence the case $\rho = 2$ is ruled out under (13).

Next when $\rho = 1$, $Z \cap W$ has dimension 1, so $r \leq 3$. If $H$ is nonsplit, then by [8, Lemma 2.2] there is an isogeny of degree at most $9\Delta^2$ between $E$ and $E^*$. From (11) $\Delta < c_{13} D^2 \Delta < 9c_{13} C^{40} L^2$. Thus we get an isogeny of degree at most

$$9 \times (4.04 \times 10^7)^2 C^{42} L^4 \approx 1.469 \times 10^{16} C^{42} L^4.$$  (14)

If $H$ is split, we can not have $r = 3$ by the proof of [6, Proposition]. If $r \leq 2$, then $R = Q/2$ by [6, Lemma 5.2], and $R < c_{13} D^2 \Delta < c_{14} C$. The assumption of no complex multiplication is used to prove [6, Lemma 5.2] in applying Kolchin’s Theorem. Since $C > (2c_{14})^{8/9}$ from (13), $Q/2 > C^{17/8}/2 > c_{14} C$. Hence a contradiction.

Lastly when $\rho = 0$, then $Z \subset W$ and $r \leq 2$. If $r = 2$, then from the proof of [6, Proposition] $N \leq 9\Delta < 9c_{13} D^2 \leq 9c_{13} C^{40} L^4$, so the original isogeny $\phi$ satisfies the required estimate.

If $r = 1$, then by the proof of [6, Proposition] $H$ is nonsplit, and there is an isogeny of degree at most $9\Delta^2$ between $E$ and $E^*$. As by (11)
\[ \Delta < c_{13}D \leq c_{13}C^{20}L^{2} \text{, we get an isogeny of degree at most } 9 \times (4.04 \times 10^{7})^2C^{40}L^{4} = 1.469 \times 10^{16}C^{40}L^{4}. \]

Next we estimate \( C \), the conditions for which are (10) and (13), for (10) implies (3). Let \( C_0 \) be the solution of the equation

\[ C_0 = 5910d[290 \log C_0 + 15.5 \max\{\log(7.4d + 2.8), 38.4\} + 342.3]. \]

Let \( x_0 = \log C_0 \), \( A_1 = 5910 \times 290d \), \( A_2 = 5910d[15.5 \max\{\log(7.4d + 2.8), 38.4\} + 342.3] \), and \( f(x) = e^x - A_1x - A_2 \), so \( f(x_0) = 0 \). If \( x_1 = \{A_2/(A_2-A_1)\} \log A_2 \), then \( f(x_1) > 0 \). As \( f(x) \) increases monotonously, \( x_0 < x_1 \), that is, \( C_0 < \exp x_1 < A_2^{1.45} \).

Thus \( C = \max\{A_2^{1.45}, 1.82 \times 10^{63}\} \) satisfies both (10) and (13). From (14) we have proved Main Proposition with \( c_4(d) = 1.47 \times 10^{16}C^{42} \).

5 Proof of Theorem

We normalize the isogeny by Lemma 5 to apply Main Proposition.

**Lemma 5.** Given a positive integer \( d \), there exists a constant \( c_{15} \) with the following property. Let \( k \) be a number field of degree at most \( d \), let \( E \) and \( E_1^{*} \) be elliptic curves defined over \( k \), and let \( \varphi \) be an isogeny from \( E \) to \( E_1^{*} \) of degree \( N \). Suppose \( k' \) is the smallest extension field of \( k \) over which \( \varphi \) is defined. Then \( [k' : k] \leq 12 \), and there is an elliptic curve \( E^{*} \), defined over \( k' \) and isomorphic over \( k' \) to \( E_1^{*} \), such that the induced isogeny from \( E \) to \( E^{*} \) is normalized. Further we have

\[ w(E^{*}) < (11.4d + 54.3)w(E) + 13 \log N =: c_{15}w(E) + 13 \log N. \]

**Proof.** This is [6, Lemma 3.2] except for the estimation of the constant on the right-hand side of the inequality, which is \( 11.4d + 54.3 \). q. e. d.

Now we give the proof of Theorem. Let \( N \) be the smallest degree of any isogeny between \( E \) and \( E' \). By [6, Lemma 6.2] there is a cyclic isogeny from \( E \) to \( E' \) of degree \( N \). According to Lemma 5 there are an extension \( k' \) of \( k \) with \([k' : k] \leq 12\) and an elliptic curve \( E^{*} \) defined over \( k' \) and isomorphic to \( E' \) such that the induced isogeny \( \varphi \) from \( E \) to \( E^{*} \) is normalized and \( w(E^{*}) < c_{15}\{w(E) + \log N\} \).

As \( \varphi \) is cyclic, by Main Proposition there is an isogeny between \( E \) and \( E^{*} \) whose degree \( N_1 \) satisfies

\[ N_1 \leq c_4(12d)\{w(E)+w(E^{*})+\log N\}^4 < c_4(12d)(c_{15}+1)^4\{w(E)+\log N\}^4. \]
So there is an isogeny of degree $N_1$ between $E$ and $E'$, and

\[ N \leq N_1 < c_4(12d)(c_{15} + 1)^4\{w(E) + \log N\}^4. \]

Thus $N < c_{16}\{w(E)\}^4$ for a constant $c_{16}$ depending only on $d$.

Lastly we estimate $c_{16}$. Let $c_{17} = c_4(12d)(c_{15} + 1)^4$, $w = w(E)$, $N_0$ satisfy $N_0 = c_{17}(w + \log N_0)^4$, and $c_{18} = N_0/w^4$. Then $N < N_0$, and $c_{18}w^4 = c_{17}(w + 4\log w + \log c_{18})^4$. Therefore

\[ c_{18} = c_{17}(1 + 4\log w/w + \log c_{18}/w)^4 < c_{17}(5 + \log c_{18})^4. \]

Let $c_{19}$ satisfy $c_{19} = c_{17}(5 + \log c_{19})^4$. Then $c_{18} < c_{19}$, and $c_{19}$ is estimated similarly as $C_0$ in the proof of Main Proposition. So $c_{19} < 5^{20}c_{17}^5$, and $N < N_0 = c_{18}w^4 < c_{19}w^4 < 5^{20}c_{17}^5w^4 = 5^{20}\{c_4(12d)\}^5(c_{15} + 1)^{20}w^4$.

Hence $c_{16} = 5^{20}\{c_4(12d)\}^5(c_{15} + 1)^{20} < c(d)$.

Acknowledgements. The author is most grateful to Professor Takayuki Oda for helpful advice. He thanks Professor David W. Masser, Professor Sinnou David and Professor Noriko Hirata-Kohno for valuable advice about the estimation of heights.

References