Proc. Natl. Acad. Sci. USA
Vol. 82, pp. 2212–2216, April 1985
Mathematics

Padé approximations and diophantine geometry

D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY

Department of Mathematics, Columbia University, New York, NY 10027

Communicated by Herbert Robbins, November 2, 1984

ABSTRACT **Using methods of Padé approximations we prove a converse to Eisenstein's theorem on the boundedness of denominators of coefficients in the expansion of an algebraic function, for classes of functions, parametrized by meromorphic functions. This result is applied to the Tate conjecture on the effective description of isogenies for elliptic curves.**

We use a Padé approximation technique to prove the g-dimensional criterion of algebraicity of a function converse to Eisenstein's theorem: a function $f(\bar{x})$, $\bar{x} = (x_1, \ldots, x_g)$, having algebraic coefficients of the expansion at $\bar{x} = \bar{0}$ from an algebraic number field $\mathbf{K}$ with "controllable" denominators, is an algebraic function over $\mathbf{K}(\bar{x})$, provided that $f(\bar{x})$ and $\bar{x}$ are simultaneously uniformized near $\bar{x} = \bar{0}$ by meromorphic functions in $\mathbf{C}^g$ of finite order of growth. We apply our results to Tate conjectures (1, 2) on the bijectivity of a map $\mathrm{Hom}(A, B) \otimes \mathbf{Z}_l \to \mathrm{Hom}(T_l(A), T_l(B))$ and on the finiteness of isomorphism classes of abelian varieties B isogenous to a fixed abelian variety A defined over $\mathbf{K}$ and having a polarization of a given degree. For elliptic curves, the conjecture on the finiteness of classes of isogeny is a corollary of Siegel's theorem on integral points (3, 4). The first Tate conjecture for elliptic curves was proved by Serre (3) for all cases but the one in which A and B have integral invariants and no complex multiplication. Faltings (5) recently proved (ineffectively) the finiteness of the isogeny classes for arbitrary abelian varieties, thus providing solutions to the Tate, Shafarevich, and Mordell conjectures. We show how our general result yields a simple proof of isogeny of two elliptic curves defined over $\mathbf{Q}$, having identical traces of Frobenious operators for a bounded number of primes. Here we use Honda's theorem (6). The technique from ref. 7 allows us to determine effectively all elliptic curves $\mathbf{K}$-isogenous to a given one. Applications of our methods to Tate conjectures for arbitrary abelian varieties and to the Grothendieck conjecture on linear differential equations will be reported elsewhere (8).

Section 1. The Main Result

Here we prove the criterion of algebraicity and algebraic independence of functions, uniformized by meromorphic functions in $\mathbf{C}^g$, and having "bounded" denominators of algebraic numbers occurring as coefficients of their power series expansions at $\bar{x} = \bar{0}$. We consider n functions $f_1(\bar{x}), \ldots, f_n(\bar{x})$ analytic in $\bar{x} = (x_1, \ldots, x_g)$ at $\bar{x} = \bar{0}$. We assume that there exist n meromorphic functions $U_1(\bar{u}), \ldots, U_n(\bar{u})$ of g variables $\bar{u} = (u_1, \ldots, u_g)$ in $\mathbf{C}^g$ such that there exists a change of variables $\bar{x} \rightleftarrows \bar{u}$ with the following properties. First, $\bar{0} \rightleftarrows \bar{u}_0$ and the Jacobian $D(\bar{u})/D(\bar{x})$ of the transformation is nonsingular at $\bar{x} = \bar{0}$ and all elements of the matrix $(\partial u_i/\partial x_j)_{i,j=1}^g$ at $\bar{x} = \bar{0}$ are bounded by c_0. Second, we assume that in the neighborhood of $\bar{u} = \bar{u}_0$ we have the uniformization

$$f_j(\bar{x}) = U_j(\bar{u}) \text{ and } f_j(\bar{0}) = U_j(\bar{u}_0) \qquad [1.1]$$

for $j = 1, \ldots, n$. Third, we assume that $U_1(\bar{u}), \ldots, U_n(\bar{u})$ are meromorphic functions of finite order of growth $\leq \rho$. This means that there exist entire functions $H(\bar{u})$, $H_1(\bar{u})$, ..., $H_n(\bar{u})$ of $\bar{u}$ in $\mathbf{C}^g$ such that $U_j(\bar{u}) = H_j(\bar{u})/H(\bar{u})$ $(j = 1, \ldots, n)$ and

$$\max\{|H(\bar{u})|, |H_1(\bar{u})|, \ldots, |H_n(\bar{u})|\} \leq \exp\{\alpha T^\rho\} \qquad [1.2]$$

for all $\bar{u}$ in the polydisk $D_T = \{\bar{u} \in \mathbf{C}^g : |u_i - u_{i,0}| \leq T, i = 1, \ldots, g\}$ and $\bar{u}_0 = (u_{1,0}, \ldots, u_{g,0})$. Finally, the analyticity of $U_j(\bar{u})$ at $\bar{u} = \bar{u}_0$ is expressed as

$$|H(\bar{u}_0)| \geq \gamma, \qquad 0 < \gamma \leq 1. \qquad [1.3]$$

These assumptions on $f_1(\bar{x}), \ldots, f_n(\bar{x})$ with $n \geq g + 1$ will be invoked everywhere in this section. We put $\mathbf{m} = (m_1, \ldots, m_g)$ for nonnegative integers $m_i \geq 0$ $(i = 1, \ldots, g)$ and we denote $|\mathbf{m}| = m_1 + \ldots + m_g$, $\mathbf{m}! = m_1! \ldots m_g!$ $\bar{x}^{\mathbf{m}} = x_1^{m_1} \ldots x_g^{m_g}$ and $\partial_{\bar{x}}^{\mathbf{m}} = (\partial/\partial x_1)^{m_1} \ldots (\partial/\partial x_g)^{m_g}$.

LEMMA 1.1. *Under the assumptions above, let* $\mathrm{P}(z_1, \ldots, z_n)$ *be a polynomial in* $z_1, \ldots, z_n$ *of total degree at most* D *and of height at most* H, *such that the function* $\mathrm{R}(\mathbb{x}) \overset{\text{def}}{=} \mathrm{P}(f_1(\mathbb{x}), \ldots, f_n(\mathbb{x}))$ *has a zero at* $\mathbb{x} = \mathbb{x}_0$ *of order at least* M: $\mathrm{R}(\mathbb{x}) = \Sigma_{\mathbf{m}} a_{\mathbf{m}} \bar{x}^{\mathbf{m}}$, $a_{\mathbf{m}} = 0$ *for* $|\mathbf{m}| < \mathrm{M}$. *Then for* $|\mathbf{m}| = \mathrm{M}$, *we have*

$$|a_{\mathbf{m}}| = |\partial_{\bar{x}}^{\mathbf{m}} \mathrm{R}(\bar{x})|_{\bar{x}=\bar{0}}| \leq \gamma^{-\mathrm{D}} (c_0 g)^{\mathrm{M}} \mathrm{H} C_{\mathrm{D}+n}^{n} \exp\{\alpha \mathrm{M}\} (\mathrm{M}/\mathrm{D})^{-\mathrm{M}/\rho} \mathrm{M}!/\Gamma(\mathrm{M}/g + 1)^g. \qquad [1.4]$$

Here $\mathrm{M} \geq \mathrm{D} > g$.

Proof: In the notation above, we put $F(\bar{u}) \overset{\text{def}}{=} H(\bar{u})^D \cdot P(U_1(\bar{u}), \ldots, U_n(\bar{u}))$. Since $f_j(\bar{x}) = U_j(\bar{u}) = H_j(\bar{u})/H(\bar{u})$ $(j = 1, \ldots, n)$ near $\bar{u} = \bar{u}_0$, $F(\bar{u})$ is an entire function and $R(\bar{x}) = F(\bar{u})$ near $\bar{x} = \bar{0}$ (or near $\bar{u} = \bar{u}_0$). Thus, according to the assumptions of *Lemma 1.1*, $F(\bar{u})$ has a zero of order at least M at $\bar{u} = \bar{u}_0$. We can now apply the Cauchy integral formula in the polydisk D_T to an entire function $F(\bar{u})$:

$$\left.\frac{\partial_{\bar{u}}^{\mathbf{m}} F(\bar{u})}{\mathbf{m}!}\right|_{\bar{u}=\bar{u}_0} = \frac{1}{(2\pi i)^g} \int_{\partial_0 D_T} \frac{F(\bar{\xi}) d\bar{\xi}}{(\bar{\xi} - \bar{u}_0)^{\mathbf{m}+1}} \qquad [1.5]$$

where $\partial_0 D_T$ is a hull of the polydisk D_T. It follows from Eq. **1.5** that

$$|\partial_{\bar{u}}^{\mathbf{m}} F(\bar{u})|_{\bar{u}=\bar{u}_0}/\mathbf{m}!| \leq C_{D+n}^{n} \cdot H \cdot \exp\{\alpha D T^\rho\} \cdot T^{-M}, \qquad [1.6]$$

where $|\mathbf{m}| = M$. We can now express $\partial_{\bar{x}}^{\mathbf{m}} R(\bar{x})|_{\bar{x}=\bar{0}}$ for $|\mathbf{m}| = M$ in terms of $\partial_{\bar{u}}^{\mathbf{n}} F(\bar{u})|_{\bar{u}=\bar{u}_0}$, using the fact that $\partial_{\bar{u}}^{\mathbf{n}} F(\bar{u})|_{\bar{u}=\bar{u}_0} = 0$, whenever $|\mathbf{n}| < M$. To do this, we use the formula for partial differentiation, $\partial_{x_i} \varphi = \Sigma_{j=1}^g M_{i,j} \partial_{u_j} \varphi$, where $M(\bar{u}) = (M_{i,j})_{i,j=1}^g$ is the matrix inverse of the Jacobian matrix $J(\bar{u}) = (\partial x_j(\bar{u})/\partial u_i)_{i,j=1}^g$. By our assumptions, absolute values of all elements of $M(\bar{u}_0)$ are bounded by c_0. Thus, by applying the differentiation rule M times and taking into account the fact that $F(\bar{u})$ has a zero at $\bar{u} = \bar{u}_0$ of order at least M, we obtain

$$|\partial_{\bar{x}}^{\mathbf{m}} R(\bar{x})|_{\bar{x}=\bar{0}}| \leq |H(\bar{u}_0)|^{-D} (c_0 g)^M \max\{|\partial_{\bar{x}}^{\mathbf{n}} F(\bar{u})|_{\bar{u}=\bar{u}_0} : |\mathbf{n}| = M\}. \qquad [1.7]$$

We put now $T = (M/D)^{1/\rho}$ in Eq. **1.6** for $M > D$. Then the combination of Eqs. **1.6** and **1.7** implies Eq. **1.4** and the lemma is proved.

The publication costs of this article were defrayed in part by page charge payment. This article must therefore be hereby marked "*advertisement*" in accordance with 18 U.S.C. §1734 solely to indicate this fact.

For an algebraic number field $\mathbf{K}$ of degree $d = [\mathbf{K}:\mathbf{Q}]$ we consider d imbedding $\alpha \mapsto \alpha^{(\sigma)}$ of $\mathbf{K}$ into $\mathbf{C}$: $\sigma = 1, \ldots, d$. Then the size $|\overline{\alpha}|$ of an algebraic number $\alpha \in \mathbf{K}$ is defined as $|\overline{\alpha}| = \max\{|\alpha^{(\sigma)}|: \sigma = 1, \ldots, d\}$. For $\alpha \in \mathbf{K}$ we denote by $d(\alpha)$ the denominator of α—i.e., a rational integer $d(\alpha) \geq 1$ such that $\alpha d(\alpha)$ is an algebraic integer. Also we denote by $\mathrm{den}\{\alpha_0, \ldots, \alpha_N\}$ the common denominator of $\alpha_0, \ldots, \alpha_N$ from $\mathbf{K}$.

THEOREM 1.1. *Let a system of functions* $f_1(\bar{x}), \ldots, f_n(\bar{x})$ *satisfy all the assumptions above with* $n \geq g + 1$. *Denote* $f_i(\bar{x}) = \sum_m a_m^{(i)} \cdot \bar{x}^m$ $(i = 1, \ldots, n)$ *and* $f_1(\bar{x})^{k_1} \ldots f_n(\bar{x})^{k_n} = \sum_m a_{m;k_1,\ldots,k_n} \bar{x}^m$ *for non-negative integers* $k_1, \ldots, k_n$. *Assume that* $a_m^{(i)} \in \mathbf{K}$ $(i = 1, \ldots, n)$ *and denote by* D_M *the common denominator of* $\{a_{m;k_1,\ldots,k_n} : |m| \leq M; k_1 + \ldots + k_n < M\}$. *Let* $\sigma = \limsup_{M\to\infty} \max\{|\overline{a_m^{(i)}}|^{1/M} : |m| \leq M; i = 1, \ldots, n\}$ *and* $\xi = \limsup_{M\to\infty} \log|D_M|/M \log M$. *1. If* $\sigma < \infty$ *and* $\xi < [1 - g/n]/(d\rho)$, *then the functions* $f_1(\bar{x}), \ldots, f_n(\bar{x})$ *are algebraically dependent over* $\mathbf{K}$. *2. Denote* $f_i^{(\sigma)}(\bar{x}) = \sum_m (a_m^{(i)})^{(\sigma)} \bar{x}^m$ *for* $\sigma = 1, \ldots, d$. *Assume that the system of functions* $f_1^{(\sigma)}(\bar{x}), \ldots, f_n^{(\sigma)}(\bar{x})$ *satisfies the uniformization assumptions above for any* $\sigma = 1, \ldots, d$. *Then conditions* $\sigma < \infty$ *and* $\xi < [1 - g/n]/\rho$ *imply that the functions* $f_1(\bar{x}), \ldots, f_n(\bar{x})$ *are algebraically dependent over* $\mathbf{K}$. *3. Assume that the functions* $f_1(\bar{x}), \ldots, f_n(\bar{x})$ *satisfy a system of* g *independent algebraic differential equations in* $\partial/\partial x_1, \ldots, \partial/\partial x_g$. *Then for any* M_0 *there exists an effective constant* M_1 *depending only on this system of differential equations, on* σ, c_0, α, γ, $\mathbf{K}$, *and* M_0 *such that the assumption in case 1 on* ξ *can be weakened to* $\sup_{M_0<M\leq M_1} \log D_M/(M \log M) < [1 - g/n]/(d\rho)$ *and the assumption in case 2 on* ξ *can be weakened to* $\sup_{M_0<M\leq M_1} \log D_M/(M \log M) < [1 - g/n]/\rho$. *Moreover, the statements of 1 and 2 can be improved to "the functions* $f_1(\bar{x}), \ldots, f_n(\bar{x})$ *are related by an algebraic relation over* $\mathbf{K}$ *of total degree* $< M_1$."

Proof: Let us assume that $\sigma < \infty$ and that for some $\delta > 0$, $\xi < [1 - g/(n - \delta)]/(d\rho)$ in case 1 and $\xi < [1 - g/(n - \delta)]/\rho$ in case 2. Thus, we may assume that $\log|D_M| < [1 - g/(n - \delta)] \times M \log M/(d\rho)$ in case 1 and $\log|D_M| < [1 - g/(n - \delta)] \cdot M \log M/\rho$ in case 2 for any sufficiently large M (or for $1 < M \leq M_1$ in case 3).

LEMMA 1.2(4). *Let* M *and* N *be integers,* $N > M > 0$, *and let* $u_{i,j}$ $(i = 1, \ldots, M; j = 1, \ldots, N)$ *be algebraic integers in* $\mathbf{K}$ *with sizes at most* U (≥ 1). *Then there exist algebraic integers* $x_1, \ldots, x_N$ *in* $\mathbf{K}$, *not all zero, satisfying* $\sum_{j=1}^{N} u_{i,j} \cdot x_j = 0$: $i = 1, \ldots, M$ *and such that* $|\overline{x_j}| \leq c_1 (c_1 NU)^{M/(N-M)}$: $j = 1, \ldots, M$. *Here* $c_1 = c_1(\mathbf{K}) > 0$.

In the proof below D denotes an integer parameter satisfying a finite set of inequalities $D \geq D_i$ for effective constants $D_i = D_i(\mathbf{K}, \delta, g, n, \sigma, \ldots)$.

LEMMA 1.3. *Let* $1/4 > \delta > 0$ *and* $n - g > \varepsilon > 0$. *Then for any* $D \geq D_0(\mathbf{K}, \delta, g, n, \sigma, \varepsilon)$ *there exists a nonzero polynomial* $P(x_1, \ldots, x_n) \in \mathbf{K}[x_1, \ldots, x_n]$ *with integral coefficients of total degree in* $x_1, \ldots, x_n$ *at most* D *and with the following properties. The sizes of the coefficients of* $P(x_1, \ldots, x_n)$ *are bounded by* $D^{c_1 D^{(n-\varepsilon)/(g-\varepsilon)}}$, *where* $c_1 = c_1(\mathbf{K}, n, g, \delta, \varepsilon) > 0$. *The function* $R(x_1, \ldots, x_g) \overset{def}{=} P(f_1(x_1, \ldots, x_g), \ldots, f_n(x_1, \ldots, x_g))$ *has a zero of order at least* $D^{(n-\varepsilon)/g}$ *at* $\bar{x} = \bar{0}$.

Proof of Lemma 1.3: Let $p(x_1, \ldots, x_n) = \sum_{k_1\geq 0} \ldots \sum_{k_n\geq 0, k_1+\ldots+k_n\leq D} p_{k_1,\ldots,k_n} \cdot x_1^{k_1} \ldots x_n^{k_n}$, where $p_{k_1,\ldots,k_n}$ $(k_1 + \ldots + k_n \leq D)$ are undetermined integers from $\mathbf{K}$. Then, in the notation of *Theorem 1.1* we have the following expansion of $R(\bar{x})$ at $\bar{x} = \bar{0}$: $R(\bar{x}) = \sum_m \bar{x}^m \{\sum_{k_1\geq 0} \ldots \sum_{k_n\geq 0, k_1+\ldots+k_n\leq D} p_{k_1,\ldots,k_n} \cdot a_{m;k_1,\ldots,k_n}\}$. Hence, the system of linear equations on $p_{k_1,\ldots,k_n}$ equivalent to $\mathrm{ord}_{\bar{x}=\bar{0}} R(\bar{x}) \geq S$ has the form

$$\sum_{k_1\geq 0} \ldots \sum_{k_n\geq 0, k_1+\ldots+k_n\leq D} D_S \cdot a_{m;k_1,\ldots,k_n} \cdot p_{k_1,\ldots,k_n} = 0 \qquad [1.8]$$

for all $\mathbf{m} = (m_1, \ldots, m_g)$ with $|\mathbf{m}| < S$, when $S \geq D$. In Eq. **1.8** all coefficients at $p_{k_1,\ldots,k_n}$ are algebraic integers from $\mathbf{K}$ of sizes bounded by $S^{[1-g/(n-\delta)]S/\rho} \cdot c_2^S$, according to the assumptions of *Theorem 1.1*. The system of Eqs. **1.8** has C_{S-1+g}^{g} equations on $(D + 1)^n$ unknowns $p_{k_1,\ldots,k_n}$ $(k_1 + \ldots + k_n \leq D)$. We can put $S = [D^{(n-\varepsilon)/g}]$. Then for sufficiently large D, we apply *Lemma 1.2* and deduce the existence of a system of algebraic integers $p_{k_1,\ldots,k_n}$ from $\mathbf{K}$, not all zero, satisfying all Eqs. **1.8** and such that

$$\max\{\overline{|p_{k_1,\ldots,k_n}|}: k_1 + \ldots + k_n \leq D\} \leq D^{c_3 D^{(n-\varepsilon)/(g-\varepsilon)}}.$$

Let us assume that $R(\bar{x}) \not\equiv 0$, where $R(\bar{x})$ is defined as in *Lemma 1.3*. Let $M = \mathrm{ord}_{\bar{x}=\bar{0}} R(\bar{x}) < \infty$. If we put $R(\bar{x}) = \sum_m c_m \bar{x}^m$, then, by the definition of M, $c_m = 0$, whenever $|\mathbf{m}| < M$. Also there exists $\mathbf{m}_0$ such that $|\mathbf{m}_0| = M$ and $c \overset{def}{=} c_{\mathbf{m}_0} \neq 0$. Following the formula given in the proof of *Lemma 1.3*, we have the following representation of the number c in terms of coefficients of the expansions of $f_1(\bar{x})^{k_1} \ldots f_n(\bar{x})^{k_n}$ and the coefficients of the polynomial $p(x_1, \ldots, x_n)$:

$$c = \sum_{k_1\geq 0} \ldots \sum_{k_n\geq 0, k_1+\ldots+k_n\leq D} p_{k_1,\ldots,k_n} \cdot a_{\mathbf{m}_0;k_1,\ldots,k_n}. \qquad [1.9]$$

Obviously, the denominator of $c \in \mathbf{K}$ divides D_M because $M \geq D^{(n-\varepsilon)/g}$. Also, $\overline{|c|} \leq C_{D+n}^{n} \cdot H \cdot c_4^M$, for $c_4 = c_4(\sigma, g, n, \varepsilon) > 0$, where H bounds the sizes of the coefficients of the polynomials $P(x_1, \ldots, x_n)$:

$$H \leq D^{c_1 D^{(n-\varepsilon)/(g-\varepsilon)}} \qquad [1.10]$$

Consequently, we have

$$d(c) \leq D_M, \ \overline{|c|} \leq c_4^M \cdot D^{c_5 D^{(n-\varepsilon)/(g-\varepsilon)}}. \qquad [1.11]$$

To bound $|c|$ from above, we use the estimates of *Lemma 1.1* and the representation of c: $c = \partial_{\bar{x}}^{\mathbf{m}_0} R(\bar{x})/\mathbf{m}_0!|_{\bar{x}=\bar{0}}$. We remark that $M \geq D^{(n-\varepsilon)/g}$, according to *Lemma 1.3*, and that $(n - \varepsilon)/g > 1$, by the choice of ε. Thus, for a sufficiently large D, $D \geq D_1(\mathbf{K}, \delta, g, n, \varepsilon, \alpha, \gamma, c_0)$, the estimate **1.4** implies

$$|c| \leq c_6^M \cdot (M/D)^{-M/\rho} \cdot D^{c_1 D^{(n-\varepsilon)/(g-\varepsilon)}}, \qquad [1.12]$$

where we use the bound **1.10** on H.

In case 2, together with the function $R(\bar{x})$, we consider functions $R^{(\sigma)}(\bar{x}) \overset{def}{=} P^{(\sigma)}(f_1^{(\sigma)}(\bar{x}), \ldots, f_n^{(\sigma)}(\bar{x}))$, where $P^{(\sigma)}(x_1, \ldots, x_n)$ is obtained from $P(x_1, \ldots, x_n)$ by application of the isomorphism σ to all of its coefficients, $\sigma = 1, \ldots, d$. Then from the definitions of functions $f_1^{(\sigma)}(\bar{x}), \ldots, f_n^{(\sigma)}(\bar{x})$, it follows that $\{\partial_{\bar{x}}^{\mathbf{m}} R(\bar{x})|_{\bar{x}=\bar{0}}\}^{(\sigma)} = \partial_{\bar{x}}^{\mathbf{m}} R^{(\sigma)}(\bar{x})|_{\bar{x}=\bar{0}}$. In particular, $c^{(\sigma)} = \partial_{\bar{x}}^{\mathbf{m}_0} R^{(\sigma)}(\bar{x})|_{\bar{x}=\bar{0}}/\mathbf{m}_0!$. Thus, under the assumptions of case 2 on the uniformization of $f_1^{(\sigma)}(\bar{x}), \ldots, f_n^{(\sigma)}(\bar{x})$, we deduce from *Lemma 1.1* an inequality similar to **1.12**:

$$|c^{(\sigma)}| \leq c_7^M \cdot (M/D)^{-M/\rho} \cdot D^{c_1 D^{(n-\varepsilon)/(g-\varepsilon)}}, \qquad [1.13]$$

for $\sigma = 1, \ldots, d$ (true only under the assumptions of case 2). We use product formula $d(c)^d \cdot |\prod_{\sigma=1}^{d} c^{(\sigma)}| \geq 1$ to $c \in \mathbf{K}$, $c \neq 0$. In case 1, combining inequalities **1.11** and **1.12** together with the bound on D_M, we obtain $M^{[1-g/(n-\delta)]M/\rho} \cdot c_8^M \cdot (M/D)^{-M/\rho} \cdot D^{c_9 D^{(n-\varepsilon)/(g-\varepsilon)}} \geq 1$. Since $M \geq D^{(n-\varepsilon)/g}$,

$$M^{[1-g/(n-\delta)]/\rho} \cdot c_8 \cdot M^{c_{10} M^{-g\varepsilon/(n-\varepsilon)}} \geq M^{[1-g/(n-\varepsilon)]/\rho}. \qquad [1.14]$$

For $\varepsilon < \delta$ and sufficiently large M (or D), inequality **1.14** is impossible. This shows that $R(\bar{x}) \equiv 0$ and that the functions $f_1(\bar{x}), \ldots, f_n(\bar{x})$ are related over $\mathbf{K}$ by an algebraic relation of total degree at most $D < M$. Let us now consider case 2. We apply product formula using inequality **1.13** and the bound $D_M < M^{[1-g/(n-\delta)]M/\rho}$ on $d(c) \leq D_M$. We obtain $M^{d[1-g/(n-\delta)]M/\rho} \cdot c_7^{dM} \cdot (M/D)^{-Md/\rho} \cdot D^{c_1 d D^{(n-\varepsilon)/(g-\varepsilon)}} \geq 1$. This im-

plies the bound **1.14**, as above, with perhaps, different constants c_8 and c_{10}. Again for $\varepsilon < \delta$ and M sufficiently large with respect to g, n, δ, ε, ρ, c_8, and c_{10}, this implies $R(\bar{x}) \equiv 0$. Thus *Theorem 1.1* is established in cases 1 and 2. We observe that, under the assumptions of case 3, any function of the form $R(\bar{x}) = P(f_1(\bar{x}), \ldots, f_n(\bar{x}))$ with $\deg(P) \le D$, which is not identically zero can have a zero at $\bar{x} = \bar{0}$ of order at most $D^{c_{11}}$. Here c_{11} is a certain effective constant depending only on the system of g algebraic differential equations satisfied by $f_1(\bar{x}), \ldots, f_n(\bar{x})$ (and on the maximal order of zeroes of $f_i(\bar{x})$ at $\bar{x} = \bar{0}$); see ref. 9. This result bounds M in terms of D and c_{11}. Consequently, in both cases 1 and 2, under the assumptions of case 3, we need bounds on D_M only for $M_0 < M \le M_1$ for effective constants M_0 and M_1.

Section 2. Formal Groups of Elliptic Curves Over Q

In this section, we give a simple solution to Tate's problem on the isogeny of two elliptic curves defined over **Q** that have isomorphic Tate modules (see chapter 4 of ref. 3). We will use mainly *Theorem 1.1* for $g = 1$ and Honda's result on formal group laws of elliptic curves defined over **Q**.

We start with an arbitrary plane cubic model of an elliptic curve E defined by the equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. The Weierstrass elliptic function parametrization of this model of E is given by the formulas $\mathcal{P}(u) = x + (a_1^2 + 4a_2)/12$, $\mathcal{P}'(u) = 2y + a_1x + a_3$; $\mathcal{P}'(u)^2 = 4\mathcal{P}(u)^3 - g_2\mathcal{P}(u) - g_3$, see ref. 10; so we have two meromorphic functions $x = x_E(u)$, $y = y_E(u)$ of u. An invariant differential ω on E has the form $\omega = dx/(2y + a_1x + a_3) = d\mathcal{P}(u)/\mathcal{P}'(u) = du$. Tate (10) has chosen the local parameter $z = -x/y$. Then the expansion of the invariant differential ω at $z = 0$ has the form (10) $\omega = dz \cdot f(z)$, $f(z) = \sum_{m=1}^{\infty} b_m z^{m-1}$, $b_1 = 1$, where b_m belong to $\mathbf{Z}[a_1, a_2, a_3, a_4, a_6]$: $m = 1, 2, \ldots$. Thus $du/dz = f(z)$ and we have the following expansion of the "elliptic logarithm" u:

$$u(\stackrel{\text{def}}{=} L(z)) = \int f(z)dz = \sum_{m=1}^{\infty} b_m z^m/m. \qquad [2.1]$$

Let E be defined over **Q**—i.e., $a_i \in \mathbf{Z}$ for $i = 1, 2, 3, 4, 6$. We assume, without loss of generality, that the E is in its Neron's minimal model. We denote by c_p for every p the trace of the Frobenious isomorphism of $\tilde{E}(p) = E(\text{mod } p)$. The L-function of $E/\mathbf{Q}$ has the form (10) $L(E; s) = \sum_{m=1}^{\infty} c_m m^{-s}$, $c_1 = 1$. To the L-function $L(E; s)$ corresponds a formal logarithm $l(z) = \sum_{m=1}^{\infty} c_m z^m/m$. Two power series $L(z)$ and $P(z)$ define formal group laws $G(x, y) = l^{-1}(l(x) + l(y))$, $F(x, y) = L^{-1}(L(x) + L(y))$ in the neighborhood of $x = y = 0$. Our main auxiliary result is Honda's (6).

THEOREM 2.1. *The two formal group laws* G(x, y) *and* F(x, y) *are strictly isomorphic over* **Z**. *This means that there exists a power series* $h_E(z) \in \mathbf{Z}[[z]]$, $h_E(z) = z + O(z^2)$ *such that* $L^{-1}(l(z)) \equiv h_E(z)$.

COROLLARY 2.2. *If two curves* $E_1/\mathbf{Q}$ *and* $E_2/\mathbf{Q}$ *have the same* L-*functions* (*or, equivalently, if they have the same number of solutions mod* p *for all* p), *then* $E_1/\mathbf{Q}$ *and* $E_2/\mathbf{Q}$ *are isogenous over* **Q**.

Proof: Consider the two elliptic logarithms $L_{E_1}(z)$ and $L_{E_2}(z)$, corresponding to E_1 and E_2 according to Eq. **2.1**. From Honda's theorem **2.1** and the assumptions of *Corollary 2.2*, there exists a convergent power series $f(z) \in \mathbf{Z}[[z]]$, $f(z) = z + O(z^2)$ such that $f(z) \equiv L_{E_1}^{-1}(L_{E_2}(z))$. We can now apply *Theorem 1.1* with $g = 1$, $n = 2$, $f_1(x) = x$, and $f_2(x) = f(x)$. We define

$$z_i(u) = -x_{E_i}(u)/y_{E_i}(u) \qquad [2.2]$$

for the elliptic functions $x_{E_i}(u)$, $y_{E_i}(u)$ associated with E_i: $i = 1, 2$. Then by Eq. **2.1**, $L_{E_i}(z_i(u)) \equiv u$: $i = 1, 2$. Thus we obtain the following uniformization of $(x, f(x))$: $f(x) = z_1(u)$, $x = z_2(u)$, where $z_1(u)$, $z_2(u)$ are meromorphic functions of order of growth two—i.e., $\rho = 2$ in *Theorem 1.1*. We also have $\sigma < \infty$ and $\xi = 0$, since $f(x)$ is an integral power series. Thus *Theorem 1.1* implies that $f(x)$ is an algebraic function. In view of the parametrization and the representation **2.2**, the Weierstrass elliptic functions $\mathcal{P}_1(u)$ and $\mathcal{P}_2(u)$ are algebraically dependent over **Q**. The lattices $\mathcal{L}_i = 2\omega_i\mathbf{Z} \oplus 2\omega_i'\mathbf{Z}$ of E_i: $i = 1, 2$ are related by a rational transformation. This transformation induces the isogeny between E_1 and E_2.

Theorem 1.1 (case 3) gives us bounds on the degree of the isogeny between E_1 and E_2 and an effective bound on P, such that E_1 and E_2 are isogenous when they have the same number of solutions (mod p) for all $p \le P$. The bound on P was established in ref. 11 assuming the generalized Riemann hypothesis. For an elliptic curve $E/\mathbf{Q}$ with the Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$ ($g_2, g_3 \in \mathbf{Z}$) and the period lattice $\mathcal{L}$ we denote by $\Delta(E)$ the area of the fundamental parallelogram of $\mathcal{L}$ and $H(E) = \max(|g_2|^{1/4}, |g_3|^{1/6})$, so that $H(E) \le \gamma_1\Delta(E)^{-2} \max(1, \log H(E))^{1/2}$.

PROPOSITION 2.3. *Let* $E_1/\mathbf{Q}$ *and* $E_2/\mathbf{Q}$ *be elliptic curves defined over* **Q**. *Then for every* $\varepsilon > 0$, *there exist an effective constant* $c_\varepsilon > 0$ *depending only on* ε *such that the following conditions are satisfied. If* E_1 and E_2 *have the same number of rational points* (*mod* p) *for any* $p \le c_\varepsilon max\{1, \Delta(E_1)^{-1} \cdot \Delta(E_2)^{-1}\}^{1+\varepsilon}$, *then* E_1 *and* E_2 *are isogenous over* **Q** *and, moreover, the degree of isogeny between* E_1 *and* E_2 *is bounded by* $c_\varepsilon max\{1, \Delta(E_1)^{-1} \cdot \Delta(E_2)^{-1}\}^{1+\varepsilon}$.

Section 3. The Uniformization of Formal Groups

Let A be a (finitely generated over **Z**) subring of an algebraic number field **K**. A g-dimensional commutative formal group law (12) over ring A is a g-tuple of power series $F(\bar{x}, \bar{y}) = (F(1)(\bar{x}, \bar{y}), \ldots, F(g)(\bar{x}, \bar{y}))$ in $2g$ variables $\bar{x} = (x_1, \ldots, x_g)$; $\bar{y} = (y_1, \ldots, y_g)$ such that $F(i)(\bar{x}, \bar{y}) \equiv x_i + y_i \text{ mod(deg 2)}$; $F(i)(F(\bar{x}, \bar{y}), \bar{z}) \equiv F(i)(\bar{x}, F(\bar{y}, \bar{z}))$ and $F(i)(\bar{x}, \bar{y}) \equiv F(i)(\bar{y}, \bar{x})$, $i = 1, \ldots, g$. One defines the homomorphisms $[n]_F(\bar{x})$: $F(\bar{x}, \bar{y}) \to F(\bar{x}, \bar{y})$ as follows: $[1]_F(\bar{x}) = \bar{x}$, $[n]_F(\bar{x}) = F(\bar{x}, [n-1]_F(\bar{x}))$, if $n \ge 2$; $[0]_F(\bar{x}) = 0$, $[n]_F(\bar{x}) = i([-n]_F(\bar{x}))$, if $n < 0$; and $i(\bar{x})$ is the "minus" operators: $F(\bar{x}, i(\bar{x})) \equiv 0$. One defines endomorphisms $[m/n]_F(\bar{x})$ over $\mathbf{Z}[1/n] \otimes A$, looking at the inverse of $[n]_F(\bar{x})$.

In cases arising from abelian varieties, the formal group law $F(\bar{x}, \bar{y})$ is an algebraic function in $\bar{x}, \bar{y}$. This allows us to evaluate the sizes and the denominators of expressions such as $\partial_{\bar{u}}^{\mathbf{m}} R(z_1(\bar{u}), \ldots, z_g(\bar{u}), z_1(a\bar{u}), \ldots, z_g(a\bar{u}))$ for polynomials $R(\bar{x}, \bar{y})$. The corresponding device was presented in ref. 7. The assumption that the group law is defined algebraically is as follows.

ASSUMPTION 3.1. *Assume that the formal group law* $F(\bar{x}, \bar{y})$ *is an algebraic function over* $\mathbf{K}(\bar{x}, \bar{y})$. *This means that there exists an algebraic equation defining* x_0 *as a function of* $\bar{x}$: $q(x_0, \bar{x}) = 0$ *and similarly defining* y_0 *as a function of* $\bar{y}$: $q(y_0, \bar{y}) = 0$, *such that* (*near* $\tilde{x} = \tilde{0}$, $\tilde{y} = \tilde{0}$)

$$F(\bar{x}, \bar{y}) = \bar{P}(\tilde{x}, \tilde{y})/Q(\tilde{x}, \tilde{y}) \qquad [3.1]$$

for $\tilde{x} = (x_0, \bar{x})$ $(= (x_0, x_1, \ldots, x_g))$ *and* $\tilde{y} = (y_0, \bar{y})$ $(= (y_0, y_1, \ldots, y_g))$. *Here* $\bar{P}(\tilde{x}, \tilde{y}) = (P(1)(\tilde{x}, \tilde{y}), \ldots, P(g)(\tilde{x}, \tilde{y}))$ *and* $P(i)(\tilde{x}, \tilde{y})$ $(i = 1, \ldots, g)$, $Q(\tilde{x}, \tilde{y})$ *are polynomials in* $2(g+1)$ *variables* $\tilde{x}, \tilde{y}$ *from* $\mathbf{K}[\tilde{x}, \tilde{y}]$ *with integral coefficients. For normalization, assume that the Taylor expansion of the branch* $x_0 = x_0(\bar{x})$ *of the root* x_0 *of* $q(x_0, \bar{x}) = 0$ *with the initial condition* $x_0(\bar{0}) = 0$ *in powers of* $\bar{x}$ (*near* $\bar{x} = 0$) *has integral coefficients from* **K** *and that* $Q(\bar{0}, \bar{0}) = 1$.

ASSUMPTION 3.2. *Assume that there is a meromorphic uniformization of the group law* **3.1** *by functions of the variable* $\bar{u} = (u_1, \ldots, u_g)$ *in* $\mathbf{C}^g$. *This means that there are* $g + 1$ *func-*

tions $z_0(\bar{u})$ *and* $\bar{z}(\bar{u}) = (z_1(\bar{u}), \ldots, z_g(\bar{u}))$ *that are analytic at* $\bar{u} = \bar{0}$ *and meromorphic in* $\mathbf{C}^g$ *such that* $\bar{z}(\bar{u} + \bar{v}) \equiv F(\bar{z}(\bar{u}), \bar{z}(\bar{v}))$ *for* $\tilde{z}(\bar{u}) \equiv (z_0(\bar{u}), \bar{z}(\bar{u}))$. *In the notation of Eq.* **3.1**,

$$\bar{z}(\bar{u} + \bar{v}) = \bar{P}(\tilde{z}(\bar{u}), \tilde{z}(\bar{v}))/Q(\tilde{z}(\bar{u}), \tilde{z}(\bar{v})) \qquad [3.2]$$

and $x_0(\bar{z}(\bar{u})) \equiv z_0(\bar{u})$. *The normalization of the uniformization* **3.2** *is the following*: $z_i(\bar{u}) = u_i mod(deg\ 2)$ $(i = 1, \ldots, g)$ *and* $z_0(\bar{u}) = 0\ mod(deg\ 2)$.

Under these assumptions, the formal group law **3.1** is defined over the ring A of integers of **K**.

We can now modify the arguments of lemma 1.5 of chapter 7, §11 of ref. 7. We start with a polynomial $R(\bar{z}, \bar{y})$ in $2g$ variables $\bar{z} = (z_1, \ldots, z_g)$, $\bar{y} = (y_1, \ldots, y_g)$ of total degree D_0 in $\bar{z}$ and of total degree D_1 in $\bar{y}$. We also consider a function

$$r(\bar{u}) \stackrel{\text{def}}{=} R(\bar{z}(\bar{u}/N), \bar{z}(\bar{u})) \qquad [3.3]$$

for an integer $N \geq 1$. Let us assume that a point $\bar{u}_0$ is a zero of order M of the function $r(\bar{u})$. This means that for all $\mathbf{m}$ with $|\mathbf{m}| < M$, $\partial_{\bar{u}}^{\mathbf{m}} r(\bar{u})|_{\bar{u}=\bar{u}_0} = 0$. We are interested in the number $c = \partial_{\bar{u}}^{\mathbf{n}} r(\bar{u})|_{\bar{u}=\bar{u}_0}/\mathbf{n}!$, where $|\mathbf{n}| = M$. We have first of all, $\partial_{\bar{u}}^{\mathbf{n}} r(\bar{u})|_{\bar{u}=\bar{u}_0} = N^{-M} \cdot \partial_{\bar{w}}^{\mathbf{n}} r(\bar{u}_0 + N\bar{w})|_{\bar{w}=\bar{0}}$. Applying the law of addition **3.2** to $r(\bar{u} + N\bar{w})$ in **3.3**, we get

$$\begin{aligned} r(\bar{u} + N\bar{w}) &= Q(\tilde{z}(\bar{u}/N), \tilde{z}(\bar{w}))^{-D_0} \cdot Q(\tilde{z}(\bar{u}), \tilde{z}(N\bar{w}))^{-D_1} \\ &\quad \cdot H(\tilde{z}(\bar{u}/N), \tilde{z}(\bar{w}), \tilde{z}(\bar{u}), \tilde{z}(N\bar{w})), \\ H(\tilde{z}_1, \ldots, \tilde{z}_4) &\stackrel{\text{def}}{=} Q(\tilde{z}_1, \tilde{z}_2)^{D_0} \cdot Q(\tilde{z}_3, z_4)^{D_1} \qquad [3.4] \\ &\quad \cdot R(\bar{P}(\tilde{z}_1, \tilde{z}_2)/Q(\tilde{z}_1, \tilde{z}_2), \bar{P}(\tilde{z}_3, \tilde{z}_4)/Q(\tilde{z}_3, \tilde{z}_4)). \end{aligned}$$

According to the assumption on M we get

$$\begin{aligned} \partial_{\bar{u}}^{\mathbf{n}} r(\bar{u})|_{\bar{u}=\bar{u}_0} &= N^{-M} \cdot Q(\tilde{z}(\bar{u}_0/N), \tilde{0})^{-D_0} \cdot Q(\tilde{z}(\bar{u}_0), \tilde{0})^{-D_1} \\ &\quad \cdot \partial_{\bar{w}}^{\mathbf{n}} H(\tilde{z}(\bar{u}_0/N), \tilde{z}(\bar{w}), \tilde{z}(\bar{u}_0), \tilde{z}(N\bar{w}))|_{\bar{w}=\bar{0}}, \end{aligned}$$

provided that neither $\bar{u}_0$ nor $\bar{u}_0/N$ is a singularity (pole) of $z_i(\bar{u})$ $(i = 1, \ldots, g)$. We put $x_i = z_i(\bar{w})$ $(i = 1, \ldots, g)$ and we denote $\tilde{x}_N \stackrel{\text{def}}{=} (x_0([N]_F(\bar{x})), [N]_F(\bar{x}))$. According to the uniformization, $\tilde{z}(N\bar{w}) = \tilde{x}_N$, whenever $\tilde{z}(\bar{w}) = \tilde{x}$. Thus we obtain

$$\begin{aligned} \partial_{\bar{u}}^{\mathbf{n}} r(\bar{u})|_{\bar{u}=\bar{u}_0} &= N^{-M} \cdot Q(\tilde{z}(\bar{u}_0/N), \tilde{0})^{-D_0} \cdot Q(\tilde{z}(\bar{u}_0), 0)^{-D_1} \\ &\quad \cdot \partial_{\bar{x}}^{\mathbf{n}} H(\tilde{z}(\bar{u}_0/N), \tilde{x}, \tilde{z}(\bar{u}_0), \tilde{x}_N)|_{\bar{x}=\bar{0}}. \end{aligned}$$

From Eisenstein's theorem and *Assumption 3.1* it follows that all numbers $\partial_{\bar{x}}^{\mathbf{m}} x_0(\bar{x})/\mathbf{m}!$, $\partial_{\bar{x}}^{\mathbf{m}} x_0([N]_F(\bar{x}))/\mathbf{m}!$, $\partial_{\bar{x}}^{\mathbf{m}} [N]_F(\bar{x})/\mathbf{m}!$ at $\bar{x} = \bar{0}$ are algebraic integers from **K**. Thus

THEOREM 3.1. *Suppose that* Assumptions 3.1 *and* 3.2 *are valid. Let* $R(\bar{z}, \bar{y})$ *be a polynomial in* $2g$ *variables* $\bar{z}, \bar{y}$ *of total degree* D_0 *in* $\bar{z}$ *and of total degree* D_1 *in* $\bar{y}$. *Define* $r(\bar{u}) \stackrel{\text{def}}{=} R(\bar{z}(\bar{u}/N), \bar{z}(\bar{u}))$ *for* $N \geq 1$ *and assume that for* $\bar{u}_0$ *(which is not a pole of* $z_i(\bar{u})$, $z_i(N\bar{u})$; $i = 0, \ldots, g$*) we have* $\partial_{\bar{u}}^{\mathbf{m}} r(\bar{u})|_{\bar{u}=\bar{u}_0} = 0$ *whenever* $|\mathbf{m}| < M$. *Then, for any* $\mathbf{n}$, $|\mathbf{n}| = M$, *we have the representation* $\partial_{\bar{u}}^{\mathbf{n}} r(\bar{u})|_{\bar{u}=\bar{u}_0}/\mathbf{n}! = N^{-M} \cdot Q(\tilde{z}(\bar{u}_0/N), \tilde{0})^{-D_0} \cdot Q(\tilde{z}(\bar{u}_0), \tilde{0})^{-D_1} \cdot H_n(\tilde{z}(\bar{u}_0/N), \tilde{z}(\bar{u}_0))$. *Here* $H_n(\tilde{z}_1, \tilde{z}_2)$ *is a polynomial of degree at most* $D_0 d$ *in* $\tilde{z}_1$ *and of degree at most* $D_1 d$ *in* $\tilde{z}_2$. *Moreover, if* $R(\bar{z}, \bar{y})$ *has integral coefficients from* **K** *of sizes bounded by* H, *then all coefficients of the polynomial* $H_n(\tilde{z}_1, \tilde{z}_2)$ *are also integral numbers from* **K**. *The sizes of the coefficients of* $H_n(\tilde{z}_1, \tilde{z}_2)$ *are bounded from above by* $H(c_{12})^{D_0+D_1} \cdot (c_{12} + c_{13}N)^M$. *If* $z_i(\bar{u}_0/N)$, $z_i(\bar{u}_0)$ $(i = 0, \ldots, g)$ *are algebraic numbers from* **K** *and if* Δ_1 *is the denominator of* $\{z_i(\bar{u}_0/N) : i = 0, \ldots, g\}$ *and* Δ_2 *is the denominator of* $\{z_i(\bar{u}_0) : i = 0, \ldots, g\}$, *then the number* $N^M \cdot \Delta_1^{D_0 d} \cdot \Delta_2^{D_1 d} \cdot Q(\tilde{z}(\bar{u}_0/N), \tilde{0})^{D_0} \cdot Q(\tilde{z}(\bar{u}_0), \tilde{0})^{D_1} \cdot \partial_{\bar{u}}^{\mathbf{n}} r(\bar{u})|_{\bar{u}=\bar{u}_0}$ *is an algebraic integer from* **K**.

Section 4. The Effective Bounds on Isogenies

We now present a self-contained proof of an effective bound on the degree of **K**-isogeny that an elliptic curve defined over **K** can have, along the lines of *Theorem 1.1*.

THEOREM 4.1. *Let an elliptic curve* E *be defined over a real algebraic field* **K** *and let there exist a cyclic subgroup* A *in* E *of order* n *defined over* **K**. *Then* $n < C(E, \mathbf{K})$, *where* $C(E, \mathbf{K})$ *is an effective constant depending only on the discriminant of* **K** *and on the algebraic equation defining* E.

Proof: Let E be given in its Weierstrass form by the equation $y^2 = 4x^3 - g_2 x - g_3$ for algebraic integers $a_4 = -g_2/4$, $a_6 = -g_3/4$ in **K**. We consider the uniformization of E by elliptic functions, presented in *Section 2*, and the uniformization of the formal group law $F(x, y)$ (for $g = 1$), associated with E in *Section 2*, satisfying the assumptions of *Section 3*. Let $\mathcal{P}(u)$ be a Weierstrass elliptic function with parameters g_2, g_3 and let $z(u) = -2\mathcal{P}(u)/\mathcal{P}'(u)$. As in *Section 3*, $z(u)$ is a uniformization of $F(x, y)$ and $z_0(u)$ is defined by the algebraic equation $z_0 = z^3 + a_4 z_0^2 z + a_6 z_0^3$ with an expansion $z_0 = z^3 + \ldots$. For the series $[1/n]_F(x) = x/n + \ldots$, describing the division by n near the origin, we have $[1/n]_F = \sum_{m=1}^{\infty} a_m x^m$, $n^{2m-1} a_m \in \mathbf{Z}[a_4, a_6]$ $(m = 1, \ldots)$. According to Eq. **2.2**,

$$z(u) = g(u)/h(u), \qquad [4.1]$$

where $g(u)$ and $h(u)$ are entire functions of u of order of growth 2, and

$$\max_{|u|=R} \max\{|g(u)|, |h(u)|\} \leq \exp\{\beta R^2\}, \qquad [4.2]$$

where β is an effective constant.

Let $0 < \delta < 1/2$. We assume that n is a sufficiently large (with respect to sizes of g_2, g_3, $\Delta(K)$, $[\mathbf{K}:\mathbf{Q}]$, and δ) positive integer such that there exists a cyclic subgroup A of order n in E, defined over **K**. Then A is generated by a torsion point $(z(\omega/n), z_0(\omega/n))$ of order n exactly for a period ω. Since **K** is real and $g_2, g_3 \in \mathbf{K}$, the lattice $\mathcal{L} = 2\omega_1\mathbf{Z} + 2\omega_2\mathbf{Z}$ of periods is invariant under the complex conjugation $\mathcal{L}^* = \mathcal{L}$. Thus, either $Im(\omega_1) = 0$, $Re(\omega_2) = 0$, or $\omega_2 = \omega_1^\dagger$. Since A is invariant under complex conjugation, $\omega^* = \alpha\omega \bmod(n\mathcal{L})$ for α, $(\alpha, n) = 1$, and ω can be taken as $2\omega_1$, $2\omega_2$, $2(\omega_1 + \omega_2)$, or $2(\omega_1 - \omega_2)$. In either case ω is independent of n.

LEMMA 4.2. *Let* D *be a sufficiently large integer,* $D \geq D_0(n, \mathbf{K}, E, \delta)$. *Then there exists a nonzero polynomial* $P(x_0, x_1) \in \mathbf{K}[x_0, x_1]$ *with integral coefficients of degree at most* D *in* x_1 *and of degree less than* n^2 *in* x_0 *with the following properties. The sizes of coefficients of* $P(x_0, x_1)$ *are bounded by* $n^{4Dn^{2-2\delta}}$. *The function* $R(x) \stackrel{\text{def}}{=} P([1/n]_F(x), x)$ *has a zero of order at least* $Dn^{2-\delta}$ *at* $x = 0$.

Proof of Lemma 4.2: Let $P(x_0, x_1) = \sum_{m_0=0}^{n^2-1} \sum_{m_1=0}^{D} p_{m_0,m_1} x_0^{m_0} x_1^{m_1}$, where p_{m_0,m_1} are undetermined integers from **K**. In the notation above: $\{[1/n]_F(x)\}^i = \sum_{m=1}^{\infty} a_m^{(i)} x^m$ $(i = 1, 2, \ldots)$. Then we have $R(x) = \sum_{m=0}^{\infty} x^m \cdot \{\sum_{m_0=0}^{n^2-1} \sum_{0 \leq k \leq m, k \leq D} p_{m_0,k} a_{m-k}\}$. Here, by the properties of the expansion of $[1/n]_F(x)$, $n^{2m} a_m^{(s)}$ are integers from **K** $(m, s = 1, \ldots)$. Hence, the system of linear equations on p_{m_0,m_1} $(m_0 = 0, \ldots, n^2 - 1; m_1 = 0, \ldots, D)$, equivalent to the condition $\mathrm{ord}_{x=0} R(x) \geq S$, is

$$\sum_{m_0=0}^{n^2-1} \sum_{0 \leq k \leq \min(m,D)} n^{2m} \cdot a_{m-k}^{(m_0)} \cdot p_{m_0,k} = 0 \qquad [4.3]$$

$m = 0, \ldots, S - 1$. The coefficients at $p_{m_0,k}$ are algebraic integers from **K**. To estimate their sizes we note that, in the expansion $[1/N]_F(x) = \sum_{m=1}^{\infty} a_m x^m$, we have $|a_m| \leq c_1^m$ for $c_1 \geq 1$ (effectively depending on E and **K** only). Thus the sizes of the coefficients at $p_{m_0,k}$ in Eq. **4.3** are bounded from above by $c_2^D n^{2S}$ for $c_2 \geq 1$ (effectively depending on E and **K** only) and $D \geq n^2$. We set $S = [D \cdot n^{2-\delta}]$. Then the system **4.3** has

at most $Dn^{2-\delta}$ equations on $n^2(D+1)$ unknown p_{m_0,m_1} ($m_0 = 0, \ldots, n^2-1$; $m_1 = 0, \ldots, D$). Thus for sufficiently large D we can apply *Lemma 1.2* and obtain a system of algebraic integers p_{m_0,m_1} ($m_0 = 0, \ldots, n^2-1$, $m_1 = 0, .., D$) from $\mathbf{K}$, not all zero, such that all Eqs. **4.3** are satisfied and such that

$$\max\{\overline{|p_{m_0,m_1}|}: m_0 = 0, \ldots, n^2-1;\ m_1 = 0, \ldots, D\} \le (c_2^D n^{2Dn^{2-\delta}})^{Dn^{2-\delta}/(Dn^2-Dn^{2-\delta})} \le n^{4Dn^{2-2\delta}}$$

for a sufficiently large D, $D \ge D_0(n, \mathbf{K}, E, \delta)$ and $n \ge n_0(\mathbf{K}, E, \delta)$. Hence, all conditions of *Lemma 4.2* are satisfied.

We define $r(u) \stackrel{\text{def}}{=} P(z(u/n), z(u))$, where $P(x_0, x_1)$ is a polynomial satisfying all conditions of *Lemma 4.2* and $F(u) = h(u)^D h(u/n)^{n^2-1} r(u)$. In the notation of the proof of *Lemma 4.2*, $F(u) = \sum_{m_0=0}^{n^2-1} \sum_{m_1=0}^{D} p_{m_0,m_1}\, g(u/n)^{m_0}\, h(u/n)^{n^2-1-m_0}\, g(u)^{m_1} h(u)^{D-m_1}$. Consequently, $|F(u)|$ can be estimated via Eq. **4.2** in the following way:

$$|F(u)| \le n^2(D+1)\cdot H \times \exp\{\beta(D+1)R^2\} \qquad [4.4]$$

for $|u| = R$, where H bounds the height (maximum of the absolute values of the coefficients) of $P(x_0, x_1)$ and β depends only on $2\omega_1$, $2\omega_2$ (see Eq. **4.2**). Let $G(u) \stackrel{\text{def}}{=} F(u)/u^S$, $S = [Dn^{2-\delta}]$. According to *Lemma 4.2*, the function $G(u)$ is an entire function (no poles at $u = 0$). Thus the maximum modulus principle $|G|_r \le |G|_R$ for $r \le R$ implies

$$|F^{(M)}(u)/M!| \le |F|_r \le |F|_R\cdot(r/R)^S,\ S = [Dn^{2-\delta}], \qquad [4.5]$$

where $|u| \le r-1$, $r \le R$. Let us choose $R = n^{1-\delta/2}$ and a small $\varepsilon > 0$. Then for a sufficiently large integer n, $n \ge n_1(\beta, \delta, \varepsilon)$ and for $D \ge n^2$, it follows from Eqs. **4.4** and **4.5** and *Lemma 4.2* that, for $|u| \le n^{1-\delta/2-\varepsilon}$,

$$|F^{(M)}(u)/M!| \le n^{-\varepsilon Dn^{(2-\delta/4)}}. \qquad [4.6]$$

For $u = \alpha\omega$ and an integer α, $1 \le \alpha \le n$, let M_α denote the largest integer m such that $r^{(m')}|_{u=\alpha\omega} = 0$ for all $m' < m$. From this definition of M_α it follows that $F^{(M_\alpha)}(u) = h(u)^D \times h(u/n)^{n^2-1}\cdot r^{(M_\alpha)}(u)$ for $u = \alpha\omega$. Thus if $u = \alpha\omega$ for an integer α, $1 \le \alpha \le n$, $\alpha\omega/n$ is not a half-period of $\mathcal{P}(u)$ and if $|\alpha\omega| \le n^{1-\delta/2-\varepsilon}$, then Eq. **4.6** implies that, for $n \ge n_2(\beta, |\omega|, \delta, \varepsilon)$ and $D \ge D_1(n)$,

$$|r^{(M_\alpha)}(\alpha\omega)/M_\alpha!| \le n^{-\varepsilon Dn^{(2-\delta/8)}}. \qquad [4.7]$$

We can apply now *Theorem 3.1* with $g = 1$, $R(z; y) \stackrel{\text{def}}{=} P(z, y)$, $u_0 = \alpha\omega$, $M = M_\alpha$, and $N = n$. Let us denote by $\mathcal{D}_n$ a (rational) integer such that $\mathcal{D}_n z(\alpha\omega/n)$ and $\mathcal{D}_n z_0(\alpha\omega/n)$ are algebraic integers: $1 \le \alpha \le n$. Consequently,

$$\frac{r^{(M_\alpha)}(\alpha\omega)}{M_\alpha!}\cdot n^{M_\alpha}\cdot Q\left(z_0\left(\frac{\alpha\omega}{n}\right), z\left(\frac{\alpha\omega}{n}\right); 0, 0\right)^{n^2}\cdot\mathcal{D}_n^{n^2 d} \qquad [4.8]$$

is an algebraic integer from L of the size bounded by $n^{M_\alpha}\cdot c_{14}^{M_\alpha+D}\cdot n^{4Dn^{2-2\delta}}$ for an effective constant c_{14} and a sufficiently large D, $D \ge D_2(n)$.

We now need some trivial information on the Galois group G_n of the extension $L = \mathbf{K}(E(A)) = \mathbf{K}(\{z(\alpha\omega/n), z_0(\alpha\omega/n)\colon \alpha = 1, \ldots, n-1\})$ over $\mathbf{K}$. Since A is defined over $\mathbf{K}$, the action of $g \in G_n$ on $(z(\alpha\omega/n), z_0(\alpha\omega/n))$ is the following: $(z(\alpha\omega/n), z_0(\alpha\omega/n))^g = (z(\alpha_g\cdot\alpha\omega/n), z_0(\alpha_g\cdot\alpha\omega/n))$, where $\alpha_g \in \{1, \ldots, n-1\}$ is defined mod(n). Let us denote the number in **4.8** by c_α, so that c_α is an algebraic integer from L. All numbers conjugate to c_α over $\mathbf{K}$ have the form $c_{\alpha\alpha_g}$: $g \in G_n$.

LEMMA 4.3. The total number of zeroes (counted with their multiplicities) of $r(u)$ inside the fundamental parallelogram generated by $2n\omega_1$ and $2n\omega_2$ is at most $3(n^2D + n^2 - 1)$.

Proof: The function $z(u/n)$ does not satisfy any algebraic equation of degree less than n^2 over $\mathbf{C}(z(u))$. Consequently, $r(u) \not\equiv 0$. The number of poles and zeroes of $r(u)$ incongruent mod$(2\omega_1\mathbf{Z} + 2\omega_2\mathbf{Z})$ is bounded by $3(n^2D + n^2 - 1)$.

To prove that n is bounded, we introduce the following nonzero integral number from $\mathbf{K}$: $c \stackrel{\text{def}}{=} \prod^*_{1\le\alpha<n} c_\alpha$, where $*$ means that the product is taken over all α such that $\alpha\omega/n$ is not a half-period of $\mathcal{P}(u)$. Because A is defined over $\mathbf{K}$, the number c belongs to $\mathbf{K}$ and is integral. We estimate the size of c by estimating the sizes of numbers c_α from **4.8** according to the description above. Thus the size of c is bounded by $\prod^*_{1\le\alpha<n}\{n^{M_\alpha}\cdot c_{14}^{M_\alpha+D}\cdot n^{4Dn^{2-2\delta}}\}$.

We now represent c as the product $c = \prod^*_{1\le\alpha<n^{1-\delta/2-\varepsilon|\omega|^{-1}}} c_\alpha \prod^*_{n^{1-\delta/2-\varepsilon|\omega|^{-1}}\le\alpha<n} c_\alpha$. The first factor is bounded, according to the representation **4.8** by **4.7**, and the second factor is bounded by the product of the sizes of c_α. This gives $\{n^{-\varepsilon Dn^{2-\delta/8}}\}^{[n^{1-\delta/2-\varepsilon|\omega|^{-1}]-1}} \times \prod^*_{1\le\alpha<n}\{n^{M_\alpha}c_{14}^{M_\alpha+D}\cdot n^{4Dn^{2-2\delta}}\} \ge |c|$. Since $c \ne 0$ we have $|\overline{c}|^{[\mathbf{K}:\mathbf{Q}]-1}|c| \ge 1$. Using the bound on the size of c and on $|c|$ we obtain

$$\prod^*_{1\le\alpha<n}\{n^{M_\alpha}c_{14}^{M_\alpha+D}\cdot n^{4Dn^{2-2\delta}}\}^{[\mathbf{K}:\mathbf{Q}]} \times \{n^{-\varepsilon Dn^{2-\delta/8}}\}^{[n^{1-\delta/2-\varepsilon|\omega|^{-1}]-1}} \ge 1. \qquad [4.9]$$

Now let ε be sufficiently small, $\varepsilon < \delta/4$. Then for a large n and D sufficiently large with respect to n, **4.9** implies

$$\sum^*_{1\le\alpha<n} M_\alpha > c_{16}Dn^{3-3\delta/2-\varepsilon}, \qquad [4.10]$$

for c_{15} depending only on c_{14}, $|\omega|^{-1}$, $[\mathbf{K}:\mathbf{Q}]$, δ, and ε. However $\sum^*_{1\le\alpha<n} M_\alpha$ is a lower bound for the number of zeroes of $r(u)$ incongruent mod$(n\mathcal{L})$. Comparing **4.10** with the bound of *Lemma 4.3* we conclude that n is bounded whenever $3\delta/2 + \varepsilon < 1$. *Theorem 4.1* is proved.

We dedicate this paper to our father.

1. Tate, J. (1965) *Proceedings of the Purdue University Conference 1963* (Springer, New York), pp. 93–195.
2. Tate, J. (1966) *Invent. Math.* **2**, 134–144.
3. Serre, J.-P. (1968) *Abelian l-adic Representations and Elliptic Curves* (Benjamin, New York).
4. Baker, A. (1979) *Transcendental Number Theory* (Cambridge University Press, Cambridge, England).
5. Faltings, G. (1983) *Invent. Math.* **73**, 349–366.
6. Honda, T. (1970) *J. Math. Soc. Jpn.* **22**, 213–246.
7. Chudnovsky, G. V. (1984) *Contributions To the Theory of Transcendental Numbers* (Am. Math. Soc., Rhode Island).
8. Chudnovsky, D. V. & Chudnovsky, G. V. (1984) *New York Number Theory Seminar* (Springer, New York).
9. Schmidt, W. M. (1977) *Acta Arith.* **32**, 275–296.
10. Tate, J. (1974) *Invent. Math.* **23**, 179–206.
11. Serre, J.-P. (1981) *Publ. Math. IHES* **54**, 323–401.
12. Hazewinkel, U. (1978) *Formal Groups and Applications* (Academic, New York).