Inventiones math. 23, 179–206 (1974)

The Arithmetic of Elliptic Curves*

John T. Tate (Cambridge, Mass.)

§ 1. Introduction

After curves of genus 0 (e.g. lines and conics in the plane) come curves of genus 1, or "elliptic" curves (e.g. plane cubics or intersections of quadric surfaces in three-space). Elliptic curves are the first examples of abelian varieties. Their points of finite order give the first non-trivial examples of étale cohomology groups. The action of Galois groups on these leads both to the classical theory of complex multiplication as well as to systems of non-abelian extensions which may contain clues to non-abelian class field theory. Elliptic curves are intimately connected with the theory of modular forms, in more ways than one.

In the early sections I have tried to give a brief introduction to the fundamentals of the subject, using explicit formulas to by-pass chunks of general theory when possible. The later sections are a survey of recent work with emphasis on three main topics: (1) The problem of rational points, the Shafarevitch group, and the conjecture of Birch and Swinnerton-Dyer. (2) Modular curves and Weil's astounding idea that every elliptic curve over the rational field is "modular". (3) Serre's theorem that the Galois groups obtained from points of finite order on elliptic curves are "as big as possible". I hope to be able to convey some idea of these advances here, illustrating them by numerical examples discussed in the last section.

§ 2. Weierstrass Models

In these lectures we will use the term *elliptic curve* to mean an abelian variety of dimension 1, or, what is the same, an irreducible non-singular projective algebraic curve of genus 1 furnished with a point 0, the origin for the group law. Any such curve E, defined over a field K, has a plane cubic model of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{1}$$

* Revised version of a survey, distributed in conjunction with the Colloquium Lectures given at Dartmouth College, Hannover, August 29–September 1, 1972 (77th summer meeting of the A.M.S.).

The author thanks N.S.F. for its support, and J.-P. Serre for his secretarial and editorial help

where x and y are coordinates in the affine plane and the coefficients a_i are in our ground field K. We call (1) a *Weierstrass equation* because in characteristics $\neq 2, 3$ we can replace x and y by

$$\wp = x + \frac{a_1^2 + 4a_2}{12}, \qquad \wp' = 2y + a_1 x + a_3,$$

and (1) becomes of the form

$$(\wp')^2 = 4\wp^3 - g_2 \wp - g_3.$$

In the projective plane the curve (1) has a unique point at infinity which we call 0 and take as the origin for the group law. It is a point of inflection with the line at infinity as tangent; the other lines through 0 are the "vertical" lines, $x = \text{const}$.

Given an Eq. (1), i.e., given five elements a_1, a_2, a_3, a_4, a_6 in K, we define associated quantities b_i, c_i, Δ, and j by the following formulas. The subscripts indicate weights. The quantity Δ, of weight 12, is called the *discriminant*; its non-vanishing is necessary and sufficient for the curve (1) to be non-singular, hence elliptic.

$$\begin{array}{ll}
b_2 = a_1^2 + 4a_2 & c_4 = b_2^2 - 24b_4 (= 12 g_2) \\
b_4 = a_1 a_3 + 2a_4 & c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6 (= 216 g_3) \\
b_6 = a_3^2 + 4a_6 & \Delta = -b_2^2 b_8 - 8b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6 (= g_2^3 - 27 g_3^2) \\
b_8 = b_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 & j = \dfrac{c_4^3}{\Delta} (= 1728\, J).
\end{array} \tag{2}$$

These quantities are related by

$$4b_8 = b_2 b_6 - b_4^2 \quad \text{and} \quad 1728\Delta = c_4^3 - c_6^2. \tag{3}$$

An invariant differential on (1) is

$$\omega = \frac{dx}{2y + a_1 x + a_3} \left(= \frac{d\wp(z)}{\wp'(z)} = dz \right). \tag{4}$$

A Weierstrass model (1) for an elliptic curve E over K is unique up to a coordinate transformation of the form

$$x = u^2 x' + r, \qquad y = u^3 y' + s u^2 x' + t \tag{5}$$

with $r, s, t, u \in K$, $u \neq 0$. Under such a change we have

$$\omega' = u\,\omega, \tag{6}$$

and the transformation rules for the a's, b's, c's, Δ and j are:

$$\begin{array}{ll}
u\,a_1' = a_1 + 2s & u^8\,b_8' = b_8 + 3r\,b_6 + 3r^2\,b_4 + r^3\,b_2 + 3r^4 \\
u^2\,a_2' = a_2 - s\,a_1 + 3r - s^2 & u^6\,b_6' = b_6 + 2r\,b_4 + r^2\,b_2 + 4r^3 \\
u^3\,a_3' = a_3 + r\,a_1 + 2t & u^4\,b_4 = b_4 + r\,b_2 + 6r^2 \\
u^4\,a_4' = a_4 - s\,a_3 + 2r\,a_2 & u^2\,b_2' = b_2 + 12r \\
\qquad -(t+rs)\,a_1 + 3r^2 - 2st & \\
u^6\,a_6' = a_6 + r\,a_4 + r^2\,a_2 + r^3 - t\,a_3 - rt\,a_1 - t^2 & \\
u^4\,c_4' = c_4, \quad u^6\,c_6' = c_6, & u^{12}\,\Delta' = \Delta, \quad j' = j.
\end{array} \tag{7}$$

If two elliptic curves E and E' are isomorphic, then $j=j'$; the converse is true over an algebraically closed field K, as is not hard to check using the formulas above.

If P is a point on E we denote the corresponding prime divisor by (P). We let $D \sim D'$ denote linear equivalence of divisors. The group law on E, which is commutative and denoted by $+$, is determined intrinsically by the rule

$$\sum_{i=1}^{n} P_i = \sum_{i=1}^{n} Q_i \Leftrightarrow \sum_{i=1}^{n} (P_i) \sim \sum_{i=1}^{n} (Q_i), \tag{8}$$

together with the fact that 0 is the identity element, i.e., $0+P=P$ for all P. On a Weierstrass model (in fact on any plane cubic model in which 0 is a point of inflection) it follows that for three points P, Q, R on E we have $P+Q+R=0 \Leftrightarrow (P)+(Q)+(R) \sim 3(0) \Leftrightarrow (P)+(Q)+(R)$ is the intersection cycle of a line with E. (This means simply P, Q, and R collinear if $P \neq Q \neq R \neq P$; if $P=Q \neq R$, it means that the tangent to E at P meets E also in R; and if $P=Q=R$ it means that P is a point of inflection.)

It is easy to make the addition law on a Weierstrass model (1) very explicit. Let $P_1=(x_1, y_1)$ and $P_2=(x_2, y_2)$ be two points $\neq 0$ on the curve. Then $P_1+P_2=0 \Leftrightarrow x_1=x_2$ and $y_1+y_2+a_1 x+a_3=0$. Otherwise, we find the sum $P_1+P_2=P_3=(x_3, y_3)$ as follows: Let $y=\lambda x+\nu$ be the line through P_1 and P_2 (tangent to E at P_1 if $P_1=P_2$). Then x_1, x_2, x_3 are the roots, with correct multiplicities, of the cubic equation in x obtained by substituting $\lambda x+\nu$ for y in (1). Hence x_3 can be calculated from $x_1+x_2+x_3=\lambda^2+a_1\lambda-a_2$, then y_3 from $-a_1 x_3-a_3-y_3=\lambda x_3+\nu$. Of course, if the coordinates of the points P_1 and P_2 lie in the ground field K, those of P_3 do also. Thus the set $E(K)$ of K-rational points on E, consisting of 0 and the solutions $(x, y) \in K \times K$ of Eq. (1), is a group.

Even if E is not an elliptic curve, but a singular plane cubic of the form (1), the prescription just given makes the set of non-singular points E_{ns} on E into a group. In this case E is a rational curve of genus 0, with one singularity, S, a node or cusp. The situation is as follows:

If $\Delta = 0$ and $c_4 \neq 0$ (so $j = \infty$) then S is a node and is rational over K. If

$$y = \alpha_1 x + \beta_1 \quad \text{and} \quad y = \alpha_2 x + \beta_2$$

are the two tangents to E at S then the map

$$P = (x, y) \mapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2} \tag{9}$$

is an isomorphism of E_{ns} with the multiplicative group $\mathbf{G}_m$. If α_1 and α_2 are in K, this isomorphism is defined over K and $E_{ns}(K) \simeq K^*$; if not, then α_1 and α_2 are conjugate quadratic irrationalities over K and

$$E_{ns}(K) \simeq (\text{gp. of elts. of norm 1 in the quad. ext. } K(\alpha)/K).$$

If $\Delta = 0$ and $c_4 = 0$ (so j indeterminate), then S is a cusp. If S is rational over K (which is automatic if K is perfect or of characteristic $\neq 2, 3$), then the map

$$P \mapsto \frac{1}{(\text{slope } PS) - (\text{slope of tangent at } S)} \tag{10}$$

is an isomorphism of E_{ns} with the additive group $\mathbf{G}_a$, defined over K, and $E_{ns}(K) \simeq K^+$.

By means of the formulas (7) it is easy to determine the structure of the group of automorphisms of an elliptic curve E. If $j \neq 0$, 1728 then the only non trivial automorphism is $P \mapsto -P$. If char $K \neq 2, 3$ and $j = 0$ (resp. $j = 12^3$) then E can be taken in the form $y^2 = x^3 + a_6$ (resp. $y^2 = x^3 + a_4 x$) and the only automorphisms are of the form $(x, y) \mapsto (u^2 x, u^3 y)$ with $u^6 = 1$ (resp. $u^4 = 1$). If char $K = 3$ (resp. char $K = 2$) and $j = 0 = 1728$ then, over an algebraically closed field, E can be taken of the form $y^2 = x^3 - x$ (resp. $y^2 - y = x^3$) and Aut E is a non-commutative group of order 12 (resp. 24). More precisely:

The group of order 12 can be presented by two generators s, t with the relations $s^4 = 1$, $t^3 = 1$, $s t s^{-1} = t^{-1}$; its quotient by $\{\pm 1\} = \{1, s^2\}$ is $\mathbf{SL}_2(\mathbf{F}_2) = \mathfrak{S}_3$, as one sees by considering its action on the 2-division points.

The group of order 24 is isomorphic to $\mathbf{SL}_2(\mathbf{F}_3)$, as one sees by considering its action on the 3-division points; it is a semi-direct product of a cyclic group of order 3 by a quaternion group of order 8 (normal subgroup).

§ 3. Expansions near 0; the Formal Group

Let E be defined by a Weierstrass Eq. (1). Let

$$z=-\frac{x}{y}, \quad w=-\frac{1}{y}, \quad \text{so } x=\frac{z}{w}, \quad y=-\frac{1}{w}. \tag{11}$$

The equation for E in the affine (z,w)-plane is

$$w=z^3+a_1 z w+a_2 z^2 w+a_3 w^2+a_4 z w^2+a_6 w^3. \tag{12}$$

The point 0 is given by $(z,w)=(0,0)$, and z is a local parameter at 0. From (12) we get the formal expansion

$$\begin{aligned} w&=z^3+a_1 z^4+(a_1^2+a_2) z^5+(a_1^3+2a_1 a_2+a_3) z^6 \\ &\quad +(a_1^4+3a_1^2 a_2+3a_1 a_3+a_2^2+a_4) z^7+\cdots \\ &=z^3(1+A_1 z+A_2 z^2+\cdots), \end{aligned} \tag{13}$$

where A_n is a polynomial of weight n in the a_i with positive integral coefficients. From (13) and (11) we get

$$\begin{aligned} x&=z^{-2}-a_1 z^{-1}-a_2-a_3 z-(a_4+a_1 a_3) z^2+\cdots, \\ y&=-z^{-1}x=-z^{-3}+a_1 z^{-2}+\cdots, \end{aligned} \tag{14}$$

as the formal expansion of x and y. Clearly, the coefficients of these expansions have coefficients in $\mathbf{Z}[a_1,a_2,a_3,a_4,a_6]$. The same is true for the expansion of the invariant differential ω:

$$\begin{aligned} \omega&=dz\big(1+a_1 z+(a_1^2+a_2) z^2+(a_1^3+2a_1 a_2+2a_3) z^3 \\ &\quad +(a_1^4+3a_1^2 a_2+6a_1 a_3+a_2^2+2a_4) z^4+\cdots\big), \end{aligned} \tag{15}$$

because

$$\begin{aligned} \frac{\omega}{dz}&=\frac{dx/dz}{2y+a_1 x+a_3}=\frac{-2z^{-3}+\cdots}{-2z^{-3}+\cdots} \\ &=\frac{dy/dz}{3x^2+2a_2 x+a_4-a_1 y}=\frac{-3z^{-4}+\cdots}{-3z^{-4}+\cdots} \end{aligned}$$

has coefficients in $\mathbf{Z}[\frac{1}{2},a_1,\ldots,a_6]$, but also in $\mathbf{Z}[\frac{1}{3},a_1,\ldots,a_6]$.

Finally, if $P_3=P_1+P_2$ and $P_i=(z_i,w_i)$, then we can express $z_3=F(z_1,z_2)$ as a formal power series in z_1 and z_2, with coefficients in $\mathbf{Z}[a_1,\ldots,a_6]$. The expansion begins

$$\begin{aligned} F(z_1,z_2)&=z_1+z_2-a_1 z_1 z_2-a_2(z_1^2 z_2+z_1 z_2^2) \\ &\quad -2a_3(z_1^3 z_2+z_1 z_2^3)+(a_1 a_2-3a_3) z_1^2 z_2^2+\cdots. \end{aligned} \tag{16}$$

This is the "formal group on one parameter" associated with E, cf. [4], [7], [16], [59], [79].

For each integer $n \geqq 1$ we have, formally,

$$z(nP)=\psi_n(z(P)), \tag{17}$$

where the series ψ_n are defined inductively by

$$\psi_1(z)=z, \qquad \psi_{n+1}(z)=F(z,\psi_n(z)). \tag{18}$$

For example, we have

$$\psi_2(z)=2z-a_1 z^2-2a_2 z^3+(a_1 a_2-7a_3)z^4+\cdots \tag{19}$$

and

$$\psi_3(z)=3z-3a_1 z^2+(a_1^2-8a_2)z^3+3(4a_1 a_2-13a_3)z^4+\cdots. \tag{20}$$

In characteristic $p>0$, for any formal group on one parameter, the series ψ_p is of the form

$$\psi_p(z)=c_1 z^{p^h}+c_2 z^{2p^h}+c_3 z^{3p^h}+\cdots, \qquad \text{with } c_1 \neq 0,$$

where h is an integer $\geqq 1$, or ∞ ($h=\infty$ means $\psi_p(z)=0$). This h is called the *height*; it determines the formal group up to isomorphism over an algebraically closed ground field [26]. The formal group of an elliptic curve E is of height 1 or 2, because the isogeny p: $E \to E$ is of degree p^2 (see below), and p^h is the inseparable part of that degree. If the height is 1, E is said to be *ordinary*, or to have *non-zero Hasse invariant*; if the height is 2, E is said to be *supersingular*, or to have *Hasse invariant* 0. Concerning the Hasse invariant, cf. e.g. [13]; also [60], [97]. It can be defined as the coefficient of z^p in $\psi_p(z)$, which is equal (in char. p) to the coefficient of $z^{p-1}dz$ in the z-expansion (15) of $\omega=dz(1+\cdots)$, and is determined up to multiplication by an element of $(K^*)^{p-1}$.

Over an algebraically closed field of characteristic $p \neq 0$, there is only a finite number of supersingular curves, up to isomorphism. The number is roughly $p/12$; more precisely we have the following "mass-formula", due to Eichler and Deuring [13]:

$$\sum_{E \text{ supersingular}} \frac{1}{|\operatorname{Aut} E|}=\frac{p-1}{24}. \tag{21}$$

Here $|\operatorname{Aut} E|$ denotes the number of automorphisms of E over the algebraically closed field. In conjunction with the results on aut E stated at the end of §2, this formula is a convenient memory aid, being equivalent to the following: For $p=2, 3$ the only supersingular invariant is $j=0=12^3$. For $p \geqq 5$, there are $[p/12]$ supersingular values of j different from 0 or 12^3, and $j=0$ (resp. 12^3) is supersingular for $p \equiv 11$

or 5 mod 12 (resp. for $p \equiv 11$ or 7 mod 12). It is worth noticing that the number of these supersingular j's is equal (for $p \geqq 3$) to

$$1 + \text{genus of the } \Gamma_0(p) \text{ modular curve}$$

and to

$$\text{dimension of modular forms of weight } p+1 \text{ on } \mathbf{SL}_2(\mathbf{Z}).$$

This is more than simple coincidence (see e.g. the last § of Deligne-Rapoport in [84]).

§ 4. Isogenies and ℓ-Adic Homology

An *isogeny* is a non-zero homomorphism $\varphi\colon E_1 \to E_2$ of elliptic curves. Its *degree*, $\deg \varphi$, can be defined either as the degree of the corresponding function field extension $K(E_1)/K(E_2)$, or as the total intersection multiplicity $\Gamma_\varphi \cdot \Gamma_0$ of the graph of φ with the graph of the 0-homomorphism, on the product $E_1 \times E_2$. More precisely, the separable part of the field extension degree is equal to the number of points of intersection and the inseparable part to their multiplicities. An isogeny $\varphi\colon E_1 \to E_2$ induces a dual isogeny $\varphi'\colon E_2 \to E_1$ in the other direction, because an elliptic curve, being its own Jacobian, is self dual. If s (sum) is the canonical map from divisors of degree 0 to points defined by $s(\sum n_i(P_i)) = \sum n_i P_i$, then we have $\varphi'(s_2(D)) = s_1(\varphi^*(D))$ for a divisor D of degree 0 on E_2, where φ^* denotes "inverse image under φ". We have

$$\begin{aligned} &(\varphi')' = \varphi, && \varphi' \circ \varphi = \text{multn. by } \deg \varphi = \varphi \circ \varphi' \\ &\deg \varphi = \deg \varphi', && \varphi_1' + \varphi_2' = (\varphi_1 + \varphi_2)', \qquad (\varphi \circ \psi)' = \psi' \circ \varphi'. \end{aligned} \tag{22}$$

All these rules are easy consequences of the theory of divisors on the product $E_1 \times E_2$, i.e., of "correspondences". So also is the fundamental fact that $\deg \varphi$ *is a quadratic function* of φ, i.e., if $\varphi_i\colon E_1 \to E_2$ are homomorphisms, then $\deg(\sum m_i \varphi_i)$ is a quadratic form in the integral variables m_i (we put $\deg 0 = 0$). In particular, for any integer $m > 0$ the multiplication by m in E is $m(\mathrm{id})_E$ and is therefore an isogeny of degree m^2. We denote this isogeny by m_E and its kernel by E_m. Granting all this, there follows

Theorem 1. *Let E be an elliptic curve defined over a field K.*

a) *If K is separably closed and m an integer not divisible by the characteristic of K, then $E(K)$ is divisible by m, and its subgroup $E_m(K)$ of elements of order dividing m is isomorphic to $(\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z})$, the product of two cyclic groups of order m.*

b) *If K is algebraically closed of characteristic $p > 0$, then $E(K)$ is divisible by p. If E is ordinary, then $E_{p^r}(K) \approx \mathbf{Z}/p^r\mathbf{Z}$, but if E is supersingular, then $E_{p^r}(K) = 0$.*

For example, if $K=\mathbf{C}$, the complex field, then we have $E(\mathbf{C})\approx\mathbf{C}/L$, where $L=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2$ is a "period lattice" in $\mathbf{C}$. Hence, for any integer $m>0$,

$$E_m(\mathbf{C})=\left(\frac{1}{m}L\right)/L\simeq L/mL=(\mathbf{Z}/m\mathbf{Z})\otimes L\simeq(\mathbf{Z}/m\mathbf{Z})\times(\mathbf{Z}/m\mathbf{Z})$$

is indeed a free module of rank 2 over the ring $\mathbf{Z}/m\mathbf{Z}$. Moreover it has a homological interpretation, as the 1-homology of E with coefficients mod m, because L can be identified with $H_1(\mathbf{C}/L,\mathbf{Z})$. In view of Theorem 1, if E is an elliptic curve over any field K and K_s a separable algebraic closure of K, it is reasonable to view $E_m(K_s)$ as the 1-dimensional homology of E with coefficients in $\mathbf{Z}/m\mathbf{Z}$, which, in fact, it is in the étale cohomology theory of M. Artin and Grothendieck. Taking $m=l^n$, l a prime $\neq\operatorname{char}(K)$, and passing to the projective limit as $n\to\infty$ we get Weil's l-adic space

$$T_l(E)=\varprojlim_n E_{l^n}(K_s)\overset{\substack{\text{if } K=\mathbf{C},\\ \text{as above}}}{=}\varprojlim_n(\mathbf{Z}/l^n\mathbf{Z})\otimes L=\mathbf{Z}_l\otimes L,$$

which is a free module of rank 2 over the ring $\mathbf{Z}_l$ of l-adic integers, and plays the role of $H_1(E,\mathbf{Z}_l)$.

Going back to the case $K=\mathbf{C}$ we note that the intersection pairing of 1-cycles induces an alternating form on $L=H_1$ with values on $\mathbf{Z}$, making $\Lambda^2L\simeq\mathbf{Z}$. The algebraic analog is Weil's "e_m-pairing"

$$e_m\colon\ E_m(K_s)\times E_m(K_s)\to\mu_m(K_s)\tag{23}$$

with values in m-th roots of unity. Passage to the limit with $m=l^n$ furnishes identifications

$$\Lambda^2_{\mathbf{Z}_l}T_l(E)\simeq T_l(\mu).\tag{24}$$

An endomorphism $\varphi\colon E\to E$ induces an endomorphism φ_l of $T_l(E)$ which can be represented by a 2×2 l-adic matrix, once a base for T_l is chosen, and which has a determinant, trace, and characteristic polynomial independent of that choice. Naturally φ' is adjoint to φ with respect to the e_m-pairings, so we have $\varphi_l t_1\wedge t_2=t_1\wedge\varphi'_l t_2$ in the sense of (24). Replacing t_2 by $\varphi_l t_2$ and using $\varphi'\varphi=\deg\varphi$ gives $\varphi_l t_1\wedge\varphi_l t_2=(\deg\varphi)(t_1\wedge t_2)$, i.e., $\det\varphi_l=\deg\varphi$. Replacing φ by $m-\varphi$, $m\in\mathbf{Z}$, we get that $\deg(m-\varphi)=f_l(m)$ for all m, where $f_l(X)=\det(X-\varphi_l)$ is the characteristic polynomial of φ_l. *Hence* $f_l(X)=X^2-(\operatorname{Tr}\varphi)X+(\deg\varphi)$ *has coefficients in* $\mathbf{Z}$, *independent of* l. Call it $f(X)$. Since $\deg(m-n\varphi)\geqq0$ all m,n we have $(\operatorname{Tr}\varphi)^2-4\deg\varphi\leqq0$, or, what is the same, *the complex roots of* $f(X)=0$ ("eigenvalues of φ") *are conjugate, of absolute value* $\sqrt{\deg\varphi}$; if $\varphi\notin\mathbf{Z}$, these two roots generate an imaginary quadratic field. It is customary (although slightly abusive) to identify φ with one of these roots, hence to speak of φ as a "number" in some quadratic imaginary field; one then writes $\operatorname{Tr}\varphi = \varphi + \bar{\varphi}$ and $\deg\varphi = \varphi\bar{\varphi}$.

Let N_φ be the number of fixed points of φ acting on $E(K_s)$. If $1-\varphi$ is separable, then the fixed points have multiplicity 1 and

$$N_\varphi = \deg(1-\varphi) = 1 - \operatorname{Tr}\varphi + \deg\varphi = (1-\varphi)(1-\bar{\varphi}), \tag{25}$$

a "Lefschetz fixed point formula".

For a concrete discussion of how to compute isogenies on Weierstrass models, see Vélu [78].

§ 5. Finite Ground Field

Let k be a finite field of characteristic p with $q = p^a$ elements. In characteristic p the map $x \mapsto x^q$ is a field isomorphism, and $x = x^q \Leftrightarrow x \in k$. Hence, if V is an algebraic variety defined by equations $f_i(x_1, \dots, x_n) = 0$ with coefficients in k, the map $(x_1, \dots, x_n) \mapsto (x_1^q, \dots, x_n^q)$ induces a rational map $\pi_{V/k}$ of V into itself, called the *Frobenius endomorphism of V relative to k*, whose fixed point set is just the set $V(k)$ of k-rational points on V.

Let E be an elliptic curve over k. Then $\pi = \pi_{E/k}$ is a purely inseparable isogeny of degree q of E.

Theorem 2. *The order of the group $E(k)$ is*

$$|E(k)| = 1 - \operatorname{Tr}\pi + q. \tag{26}$$

It differs from $1+q$ by at most $2\sqrt{q}$.

This theorem, conjectured by E. Artin in his thesis, was proved by Hasse in the 1930's, and later generalized to curves of higher genus and abelian varieties by Weil. It is an immediate consequence of the considerations at the end of the last section. Indeed, π being purely inseparable has differential 0, so $1-\pi$ has differential the identity and is separable.

Remark. We may identify π with an integer of an imaginary quadratic field (or of $\mathbf{Q}$), with $|\pi| = q^{\frac{1}{2}}$, cf. § 4. Conversely, any such integer is "the Frobenius endomorphism" of an elliptic curve over $\mathbf{F}_q$, determined up to $\mathbf{F}_q$-isogeny; this follows from Deuring [13] and has been generalized to abelian varieties by Honda and Tate [75], [77].

The zeta function of the curve E/k (cf. e.g. [54]) is:

$$\zeta_{E/k}(s) = \frac{f_{E/k}(q^{-s})}{(1-q^{-s})(1-q^{1-s})}, \tag{27}$$

where

$$f_{E/k}(X) = \det(1-\pi X) = 1 - (\operatorname{Tr}\pi)X + qX^2 = (1-\pi X)(1-\bar{\pi}X), \tag{28}$$

and Theorem 2 implies that its zeros are on the line $\operatorname{Re}(s) = \frac{1}{2}$.

We define $f_{E/k}(X)$ also when E is not an elliptic curve, but a curve of Weierstrass type (1) with a singularity, S. There are three cases as discussed at the end of §1. We put

$$f_{E/k}(X)=\begin{cases}1-X, & \text{if } S \text{ a node with tangents rational over } k\\ 1+X, & \text{if } S \text{ a node with tangents quadratic over } k\\ 1, & \text{if } S \text{ a cusp.}\end{cases} \tag{29}$$

Then (27) holds in all cases, E singular or not. So does the relationship

$$|E_{ns}(k)|=qf(q^{-1}). \tag{30}$$

§ 6. Local Fields

The group $E(\mathbf{C})$ of points on an elliptic curve over the complex field is a connected compact complex Lie group of complex dimension 1, so is isomorphic to the product of two circles.

The group $E(\mathbf{R})$ of points on an elliptic curve over the real field is a compact real Lie group of dimension 1 with one or two components (according as $\Delta<0$ or $\Delta>0$), and is therefore isomorphic to the circle group or to its product with a group of order 2.

Suppose now that K is a field complete with respect to a discrete valuation, v. Let R denote the ring of integers in K, ρ a prime element in R, and $k=R/\rho R$ the residue field. Assume v normalized so that $v(\rho)=1$. Let E be an elliptic curve over K. There exist Weierstrass Eqs. (1) for E with coefficients $a_i\in R$. Among all such, choose one for which $v(\Delta)$ is minimal. We call such an equation a *minimal Weierstrass equation* for E. Using the Eqs. (7) it is a simple matter to check that *any two such minimal equations are related by a transformation* (5) *with r, s, $t\in R$ and u invertible in R*. This will mean that the following considerations are essentially independent of our choice of minimal Eq. (1). In particular, the Weierstrass curve $\tilde{E}$ over k got by reducing (1) modulo the prime in R is unique up to a transformation of the form (5) over k.

A point P in projective n-space over K can be represented by a set of coordinates $(x_0, \ldots, x_n)$ such that $x_i\in R$ all i and x_i invertible in R for some i (i.e., such that $0=\operatorname{Min} v(x_i)$), and then on reducing the x_i mod ρR we get a point $\tilde{P}=(\tilde{x}_0, \ldots, \tilde{x}_n)$ in projective n-space. For $n=2$ this "reduction map" $P\mapsto\tilde{P}$ from $\mathbf{P}_2(K)$ to $\mathbf{P}_2(k)$ obviously carries $E(K)$ to $\tilde{E}(k)$. We put

$$E_0(K)=\{P\in E(K)\,|\,\tilde{P}\in\tilde{E}_{ns}(k)\}, \tag{31}$$

$$E_1(K)=\{P\in E(K)\,|\,\tilde{P}=\tilde{0}\}. \tag{32}$$

Recall (cf. §1) that $\tilde{E}_{ns}$ denotes the non-singular part of $\tilde{E}$, and is a group.

Theorem 3. a) *The set $E_0(K)$ is a subgroup of finite index in $E(K)$.*

b) *The reduction map is a homomorphism of $E_0(K)$ onto $\tilde{E}_{ns}(k)$ with kernel $E_1(K)$.*

c) *The map $P \to z(P) = -x(P)/y(P)$ is an isomorphism between $E_1(K)$ and the group of points on the formal group* (16) *with coordinate z in the prime ideal of R.*

That $E_0(K)$ is a subgroup and is mapped homomorphically to $\tilde{E}_{ns}(k)$ by reduction follows from the fact that reduction carries lines into lines. The homomorphism is onto by Hensel's lemma, and its kernel is $E_1(K)$ by definition. The finiteness of index in a) depends on the minimality of the Eq. (1); see the discussion following the "addendum toTheorem 3" below. Part (c) is clear; a point $P=(x,y)$ in $E(K)$ is in $E_1(K)$ if and only if x and y are *not* in R, i.e., $v(x), v(y)<0$. Then (1) shows $3\,v(x)=2\,v(y)$ and consequently $v(z)>0$. Conversely, if $v(z)>0$ then formulas (14) define a point $P=(x,y)$ such that $z(P)=z$.

Corollary 1. *The group $E_1(K)$ is uniquely divisible by integers m not divisible by* char(k).

Because such an m is invertible in R, and hence the series $\psi_m(z) = m\,z + \cdots$ (cf. (18)) has an inverse function in $R[[z]]$.

If char$(k)=p>0$ the Newton polygon of $\psi_p(z)$ gives information about points of order p^ν in $E_1(K)$; cf. [30], [59]. In particular, if p is unramified in R, e.g. if $R=\mathbf{Z}_p$, then $E_1(K)$ is torsion-free unless $p=2$ and a_1 is odd, in which case its torsion subgroup is of order 2.

We say E has *good*, or *stable, reduction at v*, if $\tilde{E}$ is an elliptic curve, i.e., if $\tilde{\Delta} \neq 0$, i.e., if $v(\Delta)=0$. Then $j \in R$ and its residue $\tilde{j}$ is the modular invariant of $\tilde{E}$. If $\tilde{E}$ is singular with a node we say E has *multiplicative*, or *semistable*, reduction at v. This happens if and only if $v(\Delta)>0$, but $v(c_4)=0$, and then $j \notin R$. If $\tilde{E}$ has a cusp, then E has *additive*, or *unstable reduction at v*, this occurs if and only if $v(\Delta)>0$ and $v(c_4)>0$. In this case there is a finite (ramified) extension K' of K over which E has either good reduction (if $j \in R$), or multiplicative reduction (if $j \notin R$).

Let K_{unr} and K_s denote the maximal unramified extension of K and the separable closure of K, respectively. Thus the residue field of K_{unr} (for the unique extension of v) is k_s, and we have

$$\mathrm{Gal}(k_s/k) \simeq \mathrm{Gal}(K_{\text{unr}}/K) \simeq G_v/I_v,$$

where $G_v = \mathrm{Gal}(K_s/K)$ is the Galois group of K_s over K and $I_v = \mathrm{Gal}(K_s/K_{\text{unr}})$ its inertia subgroup. If G_v acts on a set T we say T is *unramified at v* if I_v acts trivially on it. This being said we can state the "criterion of Ogg-Néron-Shafarevitch":

Theorem 4. *The following conditions are equivalent*

(a) *E has good reduction at v,*

(b) *$E_m(K_s)$ unramified at v for all m not divisible by* $\operatorname{char}(k)$,

(c) *$T_l(E)$ is unramified at v for some prime $l \neq \operatorname{char}(k)$.*

When these conditions hold, the reduction homomorphism induces an isomorphism $E_m(K_{\mathrm{unr}}) \simeq \tilde{E}_m(k_s)$ for all m not divisible by $\operatorname{char}(k)$.

For the proof, see [45] and [56]. Corollaries are, that *good reduction at v is invariant under K-isogeny,* and that *if $T_l(E)$ is unramified at v for one prime $l \neq \operatorname{char}(k)$, it is so for all such l.*

In case of potential good reduction ($j \in R$), I_v acts on $T_l(E)$ (for $l \neq \operatorname{char}(k)$) through a finite quotient group, tamely if $\operatorname{char}(k) \neq 2, 3$, and the quotient group and the character of the representation are independent of l (cf. [56], but note that the functorial argument with Néron's model made there can be replaced by Weierstrass equation calculations in the case of elliptic curves).

In case $j \notin R$ many aspects of the situation are made transparent by the existence of an analytic uniformization covering all of E, not just E_1. Consider the classical formulas

$$c_4 = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1-q^n}, \qquad \Delta = q \prod_{n=1}^{\infty} (1-q^n)^{24} \tag{33}$$

and

$$j = \frac{c_4^3}{\Delta} = \frac{1}{q} + 744 + 196884\, q + \cdots. \tag{34}$$

These make sense for $q \in K$ with $0 < v(q) < \infty$ (i.e., $1 > |q| > 0$) and, in our non-archimedean field K, the relation (34) gives a bijection between the set of all such q and the set of $j \in K$ with $v(j) < 0$ (i.e., $j \notin R$). Any such q generates an infinite cyclic discrete subgroup $q^{\mathbf{Z}}$ of the multiplicative group $\mathbf{G}_m$. In the classical case, $\mathbf{C}^*/q^{\mathbf{Z}}$ is an elliptic curve with invariant j given by (34). The same is true over K!

Theorem 5. *For q as above, $\mathbf{G}_m/q^{\mathbf{Z}} = E_q$ is an elliptic curve over K. It has a minimum Weierstrass equation with c_4, Δ, and j as above. It is characterized, up to K-isomorphism by the fact that it has the given j-invariant, together with the fact that its reduction is of split multiplicative type (i.e., $\tilde{E}_q$ has a node with tangents rational over K).*

I found this theorem in 1959 and would like to apologize for never having officially published it. The most complete reference for it at present is [51]. Mumford [38] has found a very non-obvious generalization to curves of higher genus. For the generalization to abelian varieties, see McCabe [88] and Raynaud [96].

Theorem 5 gives an isomorphism $E_q(K) \simeq K^*/q^{\mathbf{Z}}$ under which the subgroup $(E_q)_0(K)$ corresponds to the group of units in R, and $(E_q)_1(K)$ to the group of units $\equiv 1$.

If E is another elliptic curve over K with the same j-invariant as E_q, then there is a unique separable quadratic extension K_E/K such that E becomes isomorphic to E_q over K_E, and then $E(K) \simeq A/q^{\mathbf{Z}}$, where A is the group of elements in K_E whose norm to K is a power of q. The extension K_E/K is unramified if and only if E has multiplicative reduction, in which case the residue field extension of K_E/K is generated by the tangents at the node of $\tilde{E}$.

Addendum to Theorem 3. *Let E be an elliptic curve over K. If E has split multiplicative reduction, then $E(K)/E_0(K)$ is cyclic of order $v(\Delta) = -v(j)$. In all other cases $E(K)/E_0(K)$ is of order $\leqq 4$.*

If E has split multiplicative reduction, then $E \approx E_q$ for some q, and the claim follows from the discussion above, because $v(\Delta) = v(q)$. The other cases can be checked out laboriously working with Weierstrass equations (following an algorithm given in a letter to Cassels, see [85]), but more insight can be gained by considering *Néron's minimal model*. Indeed, the projective two-dimensional scheme over R defined by a minimal Weierstrass equation may not be regular at the singular point of its special fiber $\tilde{E}$ (if $\tilde{E}$ is singular). By resolving this possible singularity, one obtains a regular projective scheme $\mathscr{E}$ over R whose special fiber $\tilde{\mathscr{E}}$ may be any one of the 10 well-known types consisting of several irreducible components with multiplicities as pictured, e.g., in [21] and [39]. The non-singular points on the special fiber $\tilde{\mathscr{E}}$ form an algebraic group $\tilde{\mathscr{E}}_{ns}$ over k whose connected component is $\tilde{E}_{ns}$, and we have $E(K)/E_0(K) \approx \tilde{\mathscr{E}}_{ns}(k)/\tilde{E}_{ns}(k)$. The addendum above now follows, because, except for Kodaira's type I_m (Néron's (b_m)), which corresponds to our E_q, with $v(q) = m$, no other type of special fiber has strictly more than 4 components of multiplicity 1.

We can do no more here than mention briefly the duality, in case k is finite, between the compact profinite group $E(K)$ and the discrete torsion group $H^1(\mathrm{Gal}(K_s/K), E(K_s))$, cf. [73], [93].

We close this section by mentioning the *exponent of the conductor of E at v*. This is a certain integer $f = f_v \geqq 0$ which is a measure of the badness the reduction of E at v and is invariant under isogeny. It is 0 for good reduction and 1 for multiplicative reduction. For additive reduction we have $f = 2 + \delta$ where $\delta \geqq 0$ is a certain "measure of wild ramification" which can be defined in terms of the action of the inertia group I_v on the points of finite order, and which is 0 except in case char $k = 2$ or 3, cf. [45], [49], and [56]. If n is the total number of irreducible components of the special fiber of Néron's model (not counting their multiplicities) over the algebraic closure $\bar{k}$ of k, Ogg has shown, by checking case by case, that

$$f = v(\Delta) + 1 - n.$$

It would be interesting to know what is behind this mysterious equality.

§ 7. Global Fields; the Group $E(\mathbf{Q})$

Global fields are finite extensions of the rational field $\mathbf{Q}$ or of a field $k(T)$, k finite. But we shall usually simply illustrate the ideas with the example $K = \mathbf{Q}$. Let E be an elliptic curve over $\mathbf{Q}$.

Theorem 6. *The group $E(\mathbf{Q})$ is finitely generated.*

This was proved by Mordell 50 years ago. Soon after, Weil, in his thesis, generalized it to abelian varieties over number fields. Néron proved it for abelian varieties over any finitely generated field (cf. [23] and [24]).

We give only the briefest outline of the proof. A full account, and further references, can be found in Cassel's survey [9], and also in Mordell's recent book on Diophantine equations. The first step is to construct a "height" function. After Néron [40], it is natural to use the *canonical height*. If $x = m/n$ is a rational number in lowest terms, we define $h(x) = \log \operatorname{Max}(|m|, |n|)$. One shows then that there is a unique real-valued function h on $E(\mathbf{Q})$ such that $h(2P) = 4h(P)$, and such that the difference $h(P) - h(x(P))$ is bounded as P runs over $E(\mathbf{Q})$, where x is the "x-coordinate" function in any Weierstrass equation for E over $\mathbf{Q}$. Moreover, the bound is effectively calculable in terms of the coefficients of the equation (see e.g. Manin-Zarkin [90], where however the elliptic curve is not given by a Weierstrass equation, but as an intersection of two quadrics in 3-space). The function h is *quadratic*, in the sense that the function

$$\langle P, Q \rangle \overset{\text{defn}}{=} \tfrac{1}{2}(h(P+Q) - h(P) - h(Q)) \tag{35}$$

is biadditive on $E(\mathbf{Q}) \times E(\mathbf{Q})$.

Now it is straightforward to show that if, for some integer $m \geqq 2$, the points P_i represent all cosets of $mE(\mathbf{Q})$ in $E(\mathbf{Q})$, and if $h_0 > h(P_i)$ all i, then $E(\mathbf{Q})$ is generated by the set of points P such that $h(P) < h_0$. Since that set is finite for any h_0, Theorem 1 will follow if we prove that $E(\mathbf{Q})/mE(\mathbf{Q})$ is finite; that is the second part of the proof.

To do this, one produces an exact sequence

$$E(\mathbf{Q}) \xrightarrow{m} E(\mathbf{Q}) \xrightarrow{\alpha} S^{(m)} \to III_m \to 0, \tag{36}$$

in which $S^{(m)}$, the *Selmer group for m*, is *finite* and *effectively computable*, and in which III_m is the set of elements of order dividing m in the *Shafare-*

vitch group Ш of $E/\mathbf{Q}$. This takes care of the finiteness statement, but does not yet give an effective method of constructing generators. The trouble is that there is no known method of computing Ш_m! However, for each integer $n \geq 1$ there is a commutative diagram

$$\begin{tikzcd}
E(\mathbf{Q}) \arrow[r] \arrow[d, "\mathrm{id.}"] & S^{(m^n)} \arrow[r] \arrow[d, "\beta_n"'] & \text{Ш}_{m^n} \arrow[r] \arrow[d, "\text{multn by } m^{n-1}"] & 0 \\
E(\mathbf{Q}) \arrow[r, "\alpha"] & S^{(m)} \arrow[r] & \text{Ш}_m \arrow[r] & 0
\end{tikzcd} \tag{37}$$

in which the middle column is effectively computable (in principle). Computing it is called *making the n-th descent*, if I understand the classical terminology properly, and yields a refinement of (36), namely

$$E(\mathbf{Q}) \xrightarrow{m} E(\mathbf{Q}) \xrightarrow{\alpha} S^{(m,n)} \to m^{n-1}\,\text{Ш}_{m^n} \to 0, \tag{38}$$

where $S^{(m,n)}$ is the image of $S^{(m^n)}$ under β_n.

Now the standard procedure for finding generators for $E(\mathbf{Q})$ is, as Barry Mazur puts it, the following: By day, one makes descents, computing $S^{(m)} = S^{(m,1)} \supset S^{(m,2)} \supset S^{(m,3)} \supset \cdots$. By night, one computes $T_1 \subset T_2 \subset T_3 \subset \cdots$ where T_n is the subgroup of $S^{(m)}$ generated by the images under α of the points $P = (x, y)$ on E for which $h(x) \leq n$. If, some happy day or night, one arrives at $T_n = S^{(m,j)}$, then one knows that $m^{j-1}\,\text{Ш}_{m^j} = 0$ and that the points $P = (x, y)$ with $h(x) \leq n$ generate $E(\mathbf{Q})/mE(\mathbf{Q})$. From these it is easy to get generators for $E(\mathbf{Q})$, as described above. On the other hand, if Ш_m contains an infinitely divisible element, $\xi \neq 0$, such that for all j there exists $\xi_j \in \text{Ш}$ with $\xi = m^j \xi_j$, then we are doomed to continue computing through all eternity[1].

Being optimistic, we suppose that this does not happen, and in fact make

Conjecture 1. *The Shafarevitch group* Ш *is finite.*

This is not known to be true for a single elliptic curve. However, in thousands of special cases one has shown that the 2 or 3 primary component (Ш is a torsion group) is finite, as a result of the successful carrying out of the above procedure for $m = 2$ or 3. Moreover the conjectures of Birch and Swinnerton-Dyer produce an integer which is naturally interpreted as the order of Ш (see below).

If Ш is finite, then its order is a square, for Cassels [8] has constructed a canonical alternating biadditive map $\text{Ш} \times \text{Ш} \to \mathbf{Q}/\mathbf{Z}$ which is non-degenerate if Ш is finite.

While we are on the subject of rational points and constructibility, let us mention that C.L. Siegel's famous theorem to the effect that on

[1] Or give up *(edit.)*.

any affine model for E there are only finitely many points with *integral* coordinates, which was non-constructive for so long, has recently been made constructive by A. Baker and J. Coates [3]. They prove

Theorem 7. *Let $F(x, y)$ be an absolutely irreducible polynomial of degreee n with integer coefficients having absolute values at most M such that the curve $F(x, y)=0$ has genus 1. Then all integer solutions $F(x, y)=0$ satisfy*

$$\operatorname{Max}(|x|, |y|) < \exp\exp\exp(2M)^{10^{n^{10}}}. \tag{39}$$

Incidentally, their method of proof is to reduce to the Weierstrass equation case, which had been treated earlier by Baker, with a somewhat better bound. But this problem of integral points involves completely different concepts from those we are discussing and we mention it only in passing.

Let $E(\mathbf{Q})_{\text{tors}}$ denote the torsion subgroup of $E(\mathbf{Q})$. In view of Theorem 6, $E(\mathbf{Q})_{\text{tors}}$ is finite and

$$E(\mathbf{Q}) \simeq Z^r \times E(\mathbf{Q})_{\text{tors}}, \tag{40}$$

where r is a certain integer $\geqq 0$ called the *rank* of E over $\mathbf{Q}$. In all known explicit examples the rank is quite small.

The curve $y^2 = x^3 + Ax^2 + Bx$ has rank $\geqq 7$ (very probably 7) for

$$A = -3.5.11.13.17.19.23.29.31.37$$

with $B = 1692602$, $B = 2843738$ or $B = 2877338$.

These curves were recently discovered by C. Pomerance and D.E. Penney [95] by computer search. I don't know of any explicit example of rank >7. However, by spezialisation arguments, Néron [94] has shown there must be elliptic curves over $\mathbf{Q}$ with rank $\geqq 11$, and I would guess that there is no bound on the rank. Shafarevitch and I [64] have shown that the rank can be arbitrarily large if we take as ground field the field of rational functions in one variable over a finite constant field instead of the field of rational numbers.

Perhaps one reason that questions about $E(\mathbf{Q})$ are so difficult is that the adele methods which are so successful with linear algebraic groups look like a mess in the case of elliptic curves. Since E is a *projective* variety, the groups $E(\mathbf{R})$ and $E(\mathbf{Q}_p)$ are *compact*. Hence the map

$$E(\mathbf{Q}) \to E(\mathbf{R}) \times \prod_p E(\mathbf{Q}_p)$$

takes $E(\mathbf{Q})$ to a non-closed subgroup of the product (except in case of rank 0). One good thing about the situation, however, is that the closure of $E(\mathbf{Q})$ in $\prod E(\mathbf{Q}_p)$ is the biggest profinite group in which $E(\mathbf{Q})$ can be dense, i.e. the "congruence subgroup problem" has an affirmative answer for E (Serre [52]).

The torsion subgroup of $E(\mathbf{Q})$ is effectively computable in the practical as well as theoretical sense, by well-known means (cf. [9], Thms. 17.2 and 22.1). By far the best way to get an upper bound for the amount of torsion on a specific curve is to reduce mod p for various primes p. For example, if E is given by a Weierstrass equation with integer coefficients whose reduction mod p for some prime p gives a non-singular curve $\tilde{E}$, then $E(\mathbf{Q})_{\mathrm{tors}}$ is mapped injectively into $\hat{E}(\mathbf{Z}/p\mathbf{Z})$ if p odd, and with a kernel of order at most 2 if $p=2$, for the kernel is in the group of points on a formal group over $\mathbf{Z}_p$ by Theorem 3. For example, if the equation for E is congruent to $y^2 \equiv x^3 - x - 1 \pmod 3$ then $E(\mathbf{Q})$ has no torsion, because that congruence has no solutions.

It is conjectured that, for each number field K of finite degree, the order of $E(K)_{\mathrm{tors}}$ is bounded as E ranges over all elliptic curves defined over K. In 1969, Manin [31] proved that, for each prime p, the order of the p-primary part of $E(K)_{\mathrm{tors}}$ is bounded. More recently, Demjanenko has published proofs of the full conjecture [12], and of an even stronger one [86]. However, there seem to be gaps in his arguments, and the status of the conjecture is unclear at the moment; it deserves clarification[2].

Over the rational field, it is known that, if $E(\mathbf{Q})$ has a point of order m, then either $m \leqq 10$, $m=12$, or m is divisible by a prime $p \geqq 23$. Using methods of Demjanenko, Kubert [87] also proves that m is not divisible by the square of any prime $l \geqq 5$ for which Fermat's last theorem is true. An excellent account of the problem is given by Ogg in [46] and [47], where he explains the connection with the modular curve $X_1(m)$ which parametrizes pairs (E, P) consisting of an elliptic curve E with a point P of order m. For $m \leqq 10$ and $m=12$, $X_1(m)$ is a rational curve, so it is trivial to get plenty of elliptic curves over $\mathbf{Q}$ with a point of those orders. For example, the point $P=(0,0)$ is of order 7 on the curve

$$y^2 + (1+d-d^2)\,xy + (d^2-d^3)\,y = x^3 + (d^2-d^3)\,x^2$$

for any d, and that curve is elliptic if

$$\Delta = d^7(d-1)^7(d^3-8d^2+5d+1) \neq 0.$$

§ 8. L-Series

Let E be an elliptic curve over $\mathbf{Q}$, and let (1) be a global minimal Weierstrass equation for E. (In general, if K is the field of fractions of a Dedekind ring R, there is for each E over K a certain ideal class in R,

[2] About [12], Cassels wrote in Math. Reviews (vol. 44, 1972, n° 2755). " .. Unfortunately, the exposition is so obscure that the reviewer has yet to meet someone who would vouch for the validity of the proof, on the other hand he has yet to be shown a mistake that unambiguously and irretrievably vitiates the argument." *(edit.)*

who's 12th power is 1, which is the obstruction to the existence of a Weierstrass equation for E with coefficients in R which is simultaneously minimal for all primes of R. Hence, if R is a principal ideal domain like $\mathbf{Z}$, or more generally if the class group of R has no 2- or 3-torsion, there is such a "global minimal equation".) For each prime p the reduction of (1) (mod p) defines a curve $\tilde{E}(p)$ over the prime field $\mathbf{F}_p$. Let A_p denote the number of points of $\tilde{E}(p)$ rational over $\mathbf{F}_p$. Note that A_p is *one more than* (because of the point 0 at infinity) *the number of solutions of the congruence*

$$y^2+a_1xy+a_3y\equiv x^3+a_2x^2+a_4x+a_6 \pmod p.$$

Put

$$t_p=1+p-A_p. \tag{41}$$

If $p\nmid\Delta$, then t_p is the "trace of Frobenius" and satisfies $|t_p|\leqq 2\sqrt{p}$. If $p\mid\Delta$, then $t_p=1,\,-1$, or 0, according as $\tilde{E}(p)$ has a node with rational tangents, a node with tangents quadratic over $\mathbf{F}_p$, or a cusp.

One associates with $E/\mathbf{Q}$ an "L-function"

$$L_E(s)=\prod_{p\mid\Delta}\frac{1}{(1-t_p p^{-s})}\prod_{p\nmid\Delta}\frac{1}{1-t_p p^{-s}+p^{1-2s}}. \tag{42}$$

This "Euler product" converges for $\mathrm{Re}\,s>\frac{3}{2}$. Expanded out, it is a Dirichlet series $\sum c_n n^{-s}$ whose p-th coefficient for p prime is $c_p=t_p$.

The *conductor*, N, of E is defined by

$$N=\prod_{p\mid\Delta}p^{f_p}, \tag{43}$$

where f_p is the exponent defined at the end of §6. Let

$$\xi_E(s)=N^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s). \tag{44}$$

Conjecture 2. *The function $\xi_E(s)$ is holomorphic in the whole s plane and satisfies a functional equation*

$$\xi_E(s)=w\,\xi_E(2-s), \qquad \textit{with } w=\pm 1.$$

This is a special case of a vast conjecture about zeta functions attached to the cohomology of any dimension of any algebraic variety over any global field (cf. Serre's discussion [57] and Deligne's appendix to it). For elliptic curves with complex multiplication, over any number field, the conjecture is true (Weil [81], Deuring [14]) and is proved by showing L_E is a Hecke L-series with Grössencharacter. For certain modular curves over $\mathbf{Q}$ the conjecture is true (Eichler, Shimura [65]) and is proved by showing L_E is the Mellin transform of a modular form. The philosophy of Weil and Langlands seems to be that every zeta function associated with any algebraic variety is some sort of transform of a modular form on a semisimple or reductive algebraic group. I don't know anything more definite in general, but in the case of elliptic curves over **Q**, Weil [82] has the following precise conjecture, for which overwhelming evidence has already accumulated.

Conjecture 3. *Let E be an elliptic curve over* **Q**. *Let N be its conductor, and $L_E=\sum c_n n^{-s}$ its zeta function. Then the function $f(\tau)=\sum c_n e^{2\pi i n\tau}$, for τ in the upper half plane, is a cusp form of weight 2 for the congruence subgroup $\Gamma_0(N)$ of the modular group* $\mathrm{SL}_2(\mathbf{Z})$, *which is an eigenfunction for the Hecke operators T_p, $p\nmid N$, and satisfies $f|W=-wf$, where $W\tau=-1/N\tau$ and $w=\pm 1$ is the sign in the functional equation of conjecture 2. Moreover there is a rational map $\varphi\colon X_0(N)\to E$ defined over* **Q** *such that $\omega\circ\varphi$ is a multiple of the differential form represented by $f(\tau)\,d\tau$ on $X_0(N)$.*

Here $X_0(N)$ is the modular curve over **Q** which, over **C**, is the compactification of the quotient of the upper half plane by $\Gamma_0(N)$. (Concerning modular forms see Hecke's collected work, Ogg's Benjamin notes, Shimura [67], and the Proceedings of the Antwerp Summer School [84], [85].)

The forms $f(\tau)$ obtained from elliptic curves of conductor N should be "new-forms" for $\Gamma_0(N)$, in the sense of Atkin-Lehner [2]. Thus, the number of such forms which are eigenfunctions for the Hecke operators with rational eigenvalues should be equal to the number of isogeny classes of elliptic curves over **Q** with conductor N. A lot of experimental evidence points to the truth of this. A computer search for elliptic curves of small conductor was initiated by Swinnerton-Dyer, and continued by Birch, Tingley, Vélu (cf. [85]); for each $N<200$, the right number of isogeny classes was found. Moreover, much theoretical work has been done (e.g. [44], [61]) to determine the elliptic curves over **Q** with given conductor. All of this supports Conjecture 3.

For any given N it is possible, in principle, to check Conjecture 3 for curves of conductor N. The point is that Baker's methods now make effective (cf. remark in Coates [11]) the theorem of Siegel used by Shafarevitch [62] to prove

Theorem 8. *Let K be an algebraic number field and S a finite set of places of K. Then, up to isomorphism, there is only a finite number of elliptic curves over K with good reduction outside S.*

Incidentally, the corresponding theorem should be true for abelian varieties of any dimension, with a fixed polarization degree. If it were true for dimension 2 and degree 1 then, as Serre remarks, one could prove the isogeny conjecture stated at the end of § 9, by the methods of [75].

For formal group considerations related to Conjecture 3, see [7] and [17].

Shimura ([69], [68]) has recently verified Conjecture 3 for the elliptic curves over **Q** with complex multiplication.

The part of Conjecture 3 before the word "moreover" has a generalization from **Q** to arbitrary global fields which has been proved by Deligne in the function field case (cf. [83]).

In view of Conjecture 3, it is natural to study elliptic curves over **Q** which do come from modular functions, since presumably all do. Such curves have an incredibly rich structure whose exploitation may well lead to progress on the question of rational points; cf. Birch [6], Manin [33], [89], Mazur [34], [91], and Mazur-Swinnerton-Dyer [92].

Another conjecture for which there is overwhelming evidence is that of Birch and Swinnerton-Dyer [5], concerning the behavior of $L_E(s)$ at $s=1$.

For each prime $p|\Delta$, let $c_p=(E(\mathbf{Q}_p):E_0(\mathbf{Q}_p))$ where E_0 is as defined in (31); in other words, let c_p be the number of components of multiplicity 1 rational over $\mathbf{F}_p$ on the special fiber of Néron's minimum model for E at p (cf. end of § 6). Also, let ω be the differential form (4) associated with a global minimal model for E (note that it is unique up to sign, because ± 1 are the only units in **Z**), and put

$$\alpha=\int_{E(\mathbf{R})}|\omega|.$$

In other words, α is either the positive real period of ω or twice that period, depending on whether $E(\mathbf{R})$ is connected or has two components.

Conjecture 4. a) *The order of the zero of $L_E(s)$ at $s=1$ is equal to the rank r of the group $E(\mathbf{Q})$.*

b) *Let $P_1, P_2, \ldots, P_r$ be r independent points in $E(\mathbf{Q})$ and let $B=\sum \mathbf{Z}P_i$ be the subgroup of $E(\mathbf{Q})$ which they generate. Then*

$$\lim_{s\to 1}\frac{L_E(s)}{(s-1)^r}=\alpha[\text{Ш}]\frac{\det\langle P_i,P_j\rangle}{(E(\mathbf{Q}):B)^2}\prod_{p|\Delta}c_p,$$

where $[\text{Ш}]$ is the order of the Shafarevitch group of E over **Q**, *where α and the c_p are as defined just above, and where $\langle\ ,\ \rangle$ is the height pairing* (35).

This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group Ш which is not known to be finite! It has been corroborated numerically in thousands of cases ([5], [71]), and it fits well with the modular point of view [6], [34]. Other evidence is reviewed in [9] and [72]. Recently Razar [50] checked it (mod 2) for some infinite families of curves over **Q**.

The generalization to abelian varieties over arbitrary global fields is discussed in [76]. The situation over functions fields is encouraging. There, part (a) implies part (b), up to a power of the characteristic. Furthermore, Milne [36] has proved both parts in char$\neq 2$ for elliptic curves with *constant* $j\neq 0, 12^3$. And M. Artin and H. Swinnerton-Dyer [1] have proved (a) for an elliptic curve defined over a field of rational functions $k(t)$, k finite, by an Eq. (1) in which the coefficients $a_i=a_i(t)$ are polynomials in t with degree $a_i\leqq 2i$.

For the super-generalization of part (a), see [74].

§ 9. Action of Galois on Points of Finite Order

Let K be a number field, $\bar{K}$ an algebraic closure of K and G the Galois group of $\bar{K}$ over K. Let E be an elliptic curve over K. The group G operates naturally on $E(\bar{K})$. If n is an integer $\geqq 1$, let $E_n=E_n(\bar{K})$ denote the set of points $P\in E(\bar{K})$ such that $nP=0$. As we have seen (§ 4), E_n is a free $(\mathbf{Z}/n\,\mathbf{Z})$-module of rank 2, and the action of G on E_n is given by a homomorphism

$$\varphi_n\colon\ G\rightarrow \mathrm{Aut}(E_n)\simeq \mathbf{GL}_2(\mathbf{Z}/n\,\mathbf{Z}).$$

The group $\varphi_n(G)$ is the Galois group of the extension of K obtained by adjunction of the coordinates of the points of E_n.

The properties of φ_n are well known in case E has complex multiplication (cf. [15]). Suppose therefore that E *does not have complex multiplication*. Then Serre [55], [59], has proved:

Theorem 9. *The index of* $\varphi_n(G)$ *in* $\mathrm{Aut}(E_n)\simeq \mathbf{GL}_2(\mathbf{Z}/n\,\mathbf{Z})$ *is bounded by a constant depending only on E and K, not on n.*

Note the analogy with the theory of cyclotomic extensions. For each integer $n\geqq 1$, the group μ_n of n-th roots of 1 in $\bar{K}$ is a free $(\mathbf{Z}/n\,\mathbf{Z})$-module of rank 1, and the action of G on it is given by a homomorphism

$$\chi_n\colon\ G\rightarrow \mathrm{Aut}(\mu_n)\simeq \mathbf{GL}_1(\mathbf{Z}/n\,\mathbf{Z}).$$

The boundedness of the index of $\chi_n(G)$ in $\mathrm{Aut}(\mu_n)$ is an immediate consequence of the fact that χ_n is surjective if $K=\mathbf{Q}$ ("irreducibility of the cyclotomic polynomial"). Moreover, the cyclotomic theory is part of the elliptic theory. Since Weil's e_n-pairing (23) gives a G-isomorphism $\Lambda^2 E_n\simeq\mu_n$, we have

$$\det\varphi_n(\sigma)=\chi_n(\sigma)\qquad \text{for } \sigma\in G.$$

Thus the $\mathbf{GL}_2/\mathbf{SL}_2$ part of the story is just cyclotomic theory.

Serre's methods are quite effective when j is not an algebraic integer, for then the v-adic analytic theory for a place v with $v(j)<0$ furnishes transvections in $\varphi_n(G)$. For example:

Proposition. *Let E be an elliptic curve over $\mathbf{Q}$ with discriminant $\Delta=\prod p_i^{e_i}$ and with square free conductor $N=\prod p_i$. Suppose l is a prime not dividing one of the e_i, or >5. Then $\varphi_l(G)=\operatorname{Aut}(E_l)\simeq \mathrm{GL}_2(\mathbf{F}_l)$ unless $A_p\equiv 0 \pmod{l}$ for all $p\nmid\Delta$.* (A_p is the number of points on the reduction of $E \bmod p$.)

Of course G operates on the l-adic modules $T_l(E)=\varprojlim E_{l^n}$ and on the vector spaces $V_l(E)=\mathbf{Q}_l\otimes_{\mathbf{Z}_l}T_l(E)$. If E and E' are K-isogenous, then $V_l(E)$ and $V_l(E')$ are isomorphic G-modules. Is the converse true?

Conjecture 5. *Suppose E and E' are elliptic curves over K such that $V_l(E)$ and $V_l(E')$ are G-isomorphic for some prime l* (hence for all l). *Then E and E' are K-isogenous.*

Serre has proved this in case the modular invariant j of E is not an algebraic integer, using the v-adic analytic theory (cf. [55], ch. IV, § 2.3). It would be very interesting to prove it in general.

§ 10. Examples

Here are some examples of curves over $\mathbf{Q}$ which illustrate various points of the general theory we have discussed. Weil's conjecture predicts that there is no elliptic curve E over $\mathbf{Q}$ with conductor $N<11$. There are three known curves with $N=11$ (cf. [78]), all isogenous as they should be. Two of them are

$$y^2+y=x^3-x^2 \qquad (\Delta=-11, j=-2^{12}/11)$$

and

$$y^2+y=x^3-x^2-10x-20 \qquad (\Delta=-11^5, j=-2^{12}31^3/11^5).$$

They correspond to the modular groups $\Gamma_1(11)$ and $\Gamma_0(11)$ respectively. They have rank 0, and the conjecture of Birch and Swinnerton-Dyer is true for them if the latter has trivial Ш ([27], [72]). Serre's theory (see prop. above) shows that for primes $l\neq 5$ one has $\varphi_l(G)=\operatorname{Aut}E_l$. The prime $l=5$ is an exception, because each curve has a rational point of order 5. But the most striking thing about them is their L-function: if we define integers c_n by

$$q\prod_{n=1}^{\infty}(1-q^n)^2\prod_{n=1}^{\infty}(1-q^{11n})^2=\sum_{n=1}^{\infty}c_nq^n,$$

then

$$L_E(s)=\sum_{n=1}^{\infty}\frac{c_n}{n^s}.$$

To prove this is the same as to show that the number of solutions of the congruence $y^2+y\equiv x^3-x^2 \pmod{p}$ is $p-c_p$ for every prime p. Eichler showed this for all p outside an unknown finite exceptional set, and it follows from Igusa [19], [20] that Eichler's exceptional set is in fact empty (see also Deligne-Rapoport's paper in [84]).

Our next example is the curve

$$u^3 + v^3 = w^3 .$$

To get it in minimal Weierstrass form, put

$$x = \frac{3w}{u+v}, \qquad y = \tfrac{9}{2}\left(\frac{u-v}{u+v}\right) + \tfrac{1}{2}$$

and it becomes

$$y^2 - y = x^3 - 7 \qquad (N = 27, \Delta = -3^9, j = 0).$$

There are only three rational points (i.e., Fermat's last theorem is true for exponent 3), and there is convincing numerical evidence that the conjecture of Birch and Swinnerton-Dyer is true for it (cf. [71]). In the *Disquisitiones* Gauss proved that the number of rational points on the curve (mod p) is

$$p+1, \qquad \text{if } p \equiv -1 \pmod 3),$$

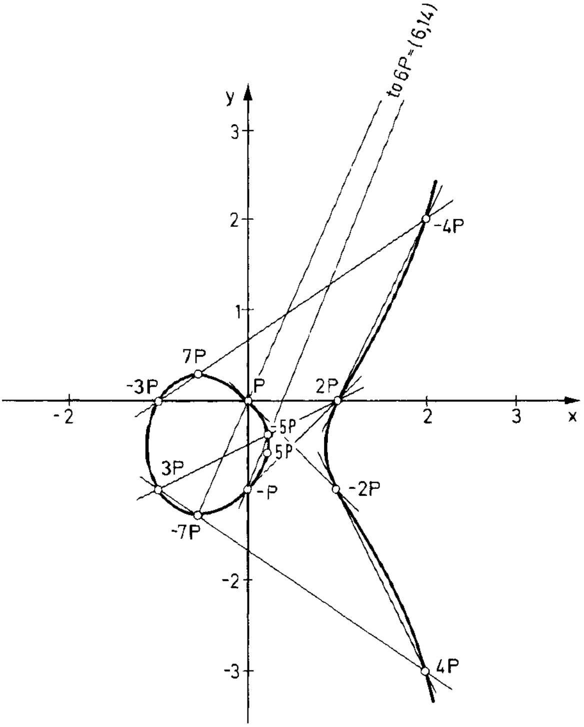

Fig. 1. The curve $y^2 + y = x^3 - x$

and is

$$p+1-t_p, \quad \text{if } p \equiv 1 \pmod 3,$$

where t_p is the unique integer $\equiv -1 \pmod 3$ such that $4p = t_p^2 + 27B^2$ for some integer B. Weil interpreted Gauss' result as meaning that $L_E(s)$ was a certain Hecke L-series for the field $\mathbf{Q}(\sqrt{-3})$. The curve has complex multiplication by the third roots of unity, and the points of finite order generate abelian extensions over that field.

The group of rational points on the curve

$$y^2 + y = x^3 - x \qquad (N=37,\ \Delta=37,\ j=2^{12}\,3^3/37)$$

is infinite cyclic, generated by $P=(0,0)$. We have

$$\begin{array}{llll} P=(0,0) & 3P=(-1,-1) & 5P=(\frac{1}{4},-\frac{5}{8}) & 7P=(-\frac{5}{9},\frac{8}{27}) \\ 2P=(1,0) & 4P=(2,-3) & 6P=(6,14) & 8P=(\frac{21}{25},-\frac{69}{125}), \end{array}$$

"etc.". There are 5 points (mod 2) and 7 (mod 3). This shows there is no torsion, but in fact, by Serre's proposition above, it shows much more, namely that $\varphi_l(G) = \mathrm{Aut}(E_l)$ for every prime l!

References

Most works cited below are post-1960, but no attempt at completeness has been made even for this recent period. An excellent guide to the earlier literature is the bibliography in Cassels' survey article [9]

1. Artin, M., Swinnerton-Dyer, H.P.F.: The Shafarevitch-Tate conjecture for pencils of elliptic curves on $K3$ surfaces. Inventiones math. **20**, 249–266 (1973)
2. Atkin, A.O.L., Lehner, J.: Hecke operators on $\Gamma_0(m)$ Math. Ann. **185**, 134–160 (1970)
3. Baker, A., Coates, J.: Integer points on curves of genus 1. Proc. Camb. Phil. Soc **67**, 595–602 (1970)
4. Barsotti, I · Analytical methods for abelian varieties in positive characteristic. Colloque de Bruxelles, pp. 77–85, 1962
5. Birch, B.J., Swinnerton-Dyer, H.P.F.. Notes on elliptic curves (II) J reine u angewandte Math. **218**, 79–108 (1965)
6. Birch, B.J.: Elliptic curves A progress report. Proceedings of the 1969 Summer Institute on Number Theory held at Stony Brook, New York, A.M.S pp. 396–400 (1971)
7. Cartier, P.: Groupes formels, fonctions automorphes et fonctions zeta des courbes elliptiques Actes, Congres Intern. Math. T. 2, 291–299 (1970)
8. Cassels, J W S.: Arithmetic on curves of genus 1, (IV). Proof of the Hauptvermutung. J. reine u. angewandte Math. **211**, 95–112 (1962)
9. Cassels, J W.S.: Diophantine equations with special reference to elliptic curves Survey Article. Journ. London Math. Soc. **41**, 193–291 (1966)
10 Cassels, J W.S., Ellison, W J., Pfister, A · On sums of squares and on elliptic curves over functions fields. Journ. Number Theory 3, 125–149 (1971)
11. Coates, J.: An effective p-adic analog of a theorem of Thue III. The Diophantine Equation $y^2 = x^3 + k$. Acta Arithmetica XVI, 425–435 (1970)
12. Demjanenko, V.A.· On the torsion of elliptic curves (in Russian). Isv. Acad Nauk U.S.S.R. **35**, 280–307 (1971) (English trans. in Math. of U.S.S R., Isv., AMS)

13 Deuring, M : Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Hamb. **16**, 32–47 (1949)

14 Deuring, M.: Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, I, II, III, IV Gott. Nach., 1953, 1955, 1956, 1957

15 Deuring, M.: Die Klassenkörper der komplexen Multiplikation. Enz. Math Wiss, 12, 23 Stuttgart: Teubner 1958

16 Frohlich, A : Formal groups. Lecture Notes in Mathematics **74**. Berlin-Heidelberg-New York: Springer 1968

17. Honda, T.: Formal groups and zeta functions Osaka J. Math. **5**, 199–213 (1968)

18 Honda, T.: On the theory of commutative formal groups Journ Math. Soc Japan **22**, 213–246 (1970)

19. Igusa, J : On the transformation theory of elliptic functions Amer. J. Math. **81**, 436–452 (1959)

20. Igusa, J.: Kroneckerian model of fields of elliptic modular functions Amer J. Math **81**, 561–577 (1959)

21 Kodaira, K : On compact analytic surfaces Annals of Math Studies **24**, 121–135 Princeton Univ. Press 1960

22. Lang, S., Tate, J.: Principal homogeneous spaces over abelian varieties. Amer J Math. **80**, pp. 659–684 (1958)

23. Lang, S., Néron, A.: Rational points of abelian varieties over function fields Amer J. Math. 95–118 (1959)

24 Lang, S : Diophantine Geometry. New York: Interscience 1962

25. Lang, S.. Elliptic Functions. Reading: Addison-Wesley 1973

26 Lazard, M. Sur les groupes de Lie formels à un paramètre. Bull Soc Math. France **83**, 251–274 (1955)

27. Ligozat, G.: Fonctions *L* des courbes modulaires Séminaire Delange-Pisot-Poitou. Jan. 1970, 10 p.

28. Lubin, J., Serre, J.-P, Tate, J.T.: Elliptic curves and formal groups A.M.S. Summer Institute on Algebraic Geometry, Woods Hole, 1964

29. Lubin, J., Tate, J.: Formal moduli for one-parameter formal Lie groups. Bull. Soc. Math. France **94**, 49–60 (1966)

30. Lubin, J.: Finite subgroups and isogenies of one-parameter formal Lie groups Annals of Math. **85**, 296–302 (1967)

31. Manin, V.T.: Uniform bound for the *p*-torsion of elliptic curves (in Russian). Isv. Acad. Nauk. U.S.S.R. **33**, 459–465 (1969) (English translation in Math of the U S.S.R., Isv., AMS)

32. Manin, Y.I.: Le groupe de Brauer-Grothendieck en géométrie diophantienne. Actes, Congres Intern. Math. **1**, 401–411 (1970)

33. Manin, Y.I. Parabolic points and zeta functions of modular curves (in Russian). Isv. Acad. Nauk., pp. 19–66 (1972)

34. Mazur, B. Courbes elliptiques et symboles modulaires Sém. Bourbaki, No 414 – June 1972, 18 p.

35. Milne, J S : The Tate-Shafarevitch group of a constant abelian variety. Inventiones math. **6**, 91–105 (1968)

36. Milne, J.S.. On the arithmetic of abelian varieties. Inventiones math **17**, 177–190 (1972)

37. Mumford, D. Abelian Varieties. Oxford Univ. Press 1970

38. Mumford, D.: An analytic construction of degenerating curves over complete local rings. Comp Math. **24**, 129–174 (1972)

39. Néron, A.: Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. IHES, Publ. Math. pp 361–483 (1964)

40. Néron, A.: Quasi-fonctions et hauteurs sur les variétés abeliennes Annals of Math. **82**, 249–331 (1965)

41. Neumann, O. Zur Reduktion der elliptischen Kurven. Math. Nach. **46**, 285–310 (1970)
42. Ogai, S V : On rational points on the curve $y^2=x(x^2+ax+b)$ (Russian) Trudy, Math. Inst. Steklov **80** (1965). Translated by A.M.S.
43. Ogg, A.P.: Cohomology of abelian varieties over function fields. Annals of Math. pp. 185–212 (1962)
44 Ogg, A.P.: Abelian curves of small conductor. J. reine und angew. Math. **226**, 204–215 (1967)
45. Ogg, A.P.: Elliptic curves and wild ramification. Amer. J pp. 1–21 (1967)
46. Ogg, A.P.: Rational points of finite order on elliptic curves Isv. Math. **12**, 105–111 (1971)
47. Ogg, A.P.: Rational points on certain elliptic modular curves. (A talk given in St Louis on March 29, 1972, at the AMS Symposium on Analytic Number Theory and Related Parts of Analysis)
48. Rajwade, A.R.: Arithmetic on curves with complex multiplication by $\sqrt{-2}$ Proc. Camb Phil. Soc. **64**, 659–672 (1968)
49. Raynaud, M.: Caractéristique d'Euler – Poincaré d'un faisceau et cohomologie des variétés abéliennes Sém. Bourbaki, 286, Février 1965
50. Razar, M.: The non-vanishing of $L(1)$ for certain elliptic curves. Harvard Ph. D Thesis, June 1971
51. Roquette, P.· Analytic theory of elliptic functions over local fields. Hamb. Math. Einzelschriften Neue Folge, Heft 1, Göttingen 1970
52 Serre, J-P.: Sur les groupes de congruences des variétés abéliennes Isv. Akad. Nauk, Math Series **28**, 3–20 (1964)
53. Serre, J-P.: Groupes de Lie l-adiques attachés aux courbes elliptiques. Coll. Internat. du C N R.S., No. 143 a Clermont-Ferrand, Editions du C.N.R.S., Paris 1966
54 Serre, J-P.: Zeta- and L-functions, in Arithmetical Algebraic Geometry. New York: Harper and Row 1966
55. Serre, J-P.: Abelian l-adic representations and elliptic curves. New York· Benjamin 1968
56 Serre, J-P., Tate, J.: Good reduction of abelian varieties. Annals of Math pp. 492–517 (1968)
57. Serre, J-P.: Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). Séminaire Delange-Pisot-Poitou, 15 p., Mai 1970
58. Serre, J-P.: p-torsion des courbes elliptiques (d'après Y Manin). Sém. Bourbaki, n° 380, 14 p., Mai-Juin 1970
59 Serre, J-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Inventiones math. **15**, 259–331 (1972)
60 Serre, J-P.: Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer), Sém. Bourbaki, No. 416, 20 p., Juin 1972
61. Setzer, C.B.: Elliptic curves of prime conductor. Harvard Ph D. Thesis, June 1972
62. Shafarevitch, I.R.. Algebraic number fields Proc. Int Cong. Math., Stockholm 1962, pp. 163–176 (A M.S. Translation, Ser 2, Vol. 31, pp. 25–39)
63. Shafarevitch, I.R. Principal homogeneous spaces defined over a function-field. Amer. Math. Soc. Transl. **37**, 85–114 (1964)
64. Shafarevitch, I.R., Tate, J T.: The rank of elliptic curves. Dokl. Akad Nauk. USSR 175 (1967), pp. 770–773 (in Russian). (A.M S. Translations Vol. **8**, 917–920 (1967))
65. Shimura, G.: On the zeta functions of the algebraic curves uniformized by certain automorphic functions Jour Math. Soc. Japan **13**, 275–331 (1961)
66. Shimura, G.: A reciprocity law in non-solvable extensions. J. reine and angew. Math **221**, 209–220 (1966)
67. Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions. Publ Math. Soc. Japan 11, Iwanomi Shoten Publishers, and Princeton Univ Press, 267 p. (1971)

68. Shimura, G.. On the zeta-function of an abelian variety with complex multiplication Ann Math **94**, 504–533 (1971)
69. Shimura, G.: On elliptic curves with complex multiplication as factors of the jacobians of modular function fields. Nagoya Math. J. **43**, 199–208 (1971)
70. Shioda, T. On rational points of the generic elliptic curve with level N structure over the field of modular functions of level N (to appear)
71. Stephens, N. M · The diophantine equation $x^3+y^3=DZ^3$ and the conjectures of Birch and Swinnerton-Dyer J. Reine Angew Math. **231**, 121–162 (1968)
72. Swinnerton-Dyer, H. P. F . The conjectures of Birch and Swinnerton-Dyer, and of Tata. Proc. of a conference on local fields, pp 132–157. Berlin-Heidelberg-New York: Springer 1967
73 Tate, J.: W. C. groups over P-adic fields Séminaire Bourbaki, No. **156**, 13 p., Déc. 1957
74 Tate, J.· Algebraic cycles and poles of zeta functions. Arithmetical Algebraic Geometry New York: Harper and Row 1966
75. Tate, J.: Endomorphisms of abelian varieties over finite fields. Inventiones math. **2**, 134–144 (1966)
76 Tate, J.: On the conjecture of Birch and Swinnerton-Dyer and a geometric analog. Sém. Bourbaki, No. 306, 26 p., Fév. 1966
77. Tate, J.: Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda) Sém Bourbaki, No. 352, 16 p., Nov. 1968
78. Vélu, J.: Courbes elliptiques sur **Q** ayant bonne réduction en dehors de (11). C. R Acad. Sc. Paris, pp 73–75 (1971)
79. Vélu, J.· Isogénies entre courbes elliptiques. C. R. Acad. Sc Paris, pp 238–241 (1971)
80. Waterhouse, W. C., Milne, J. S.: Abelian varieties over finite fields. A. M. S. Summer Institute on Number Theory, Stony Brook, 1969, Proc of Symposia in pure mathematics, Vol. XX, AMS, 1971
81 Weil, A.· Jacobi sums as „Grossencharaktere". Trans. Amer. Math. Soc. **75**, 487–495 (1952)
82. Weil, A.: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Annalen **168**, 149–156 (1967)
83. Weil, A.: Dirichlet Series and Automorphic Forms Lecture Notes in Mathematics **189**. Berlin-Heidelberg-New York. Springer 1971

Additional Bibliography

84 Modular Functions of One Variable Vol. II. Lecture Notes in Mathematics **349**. Berlin-Heidelberg-New York: Springer 1973
85. Modular Functions of One Variable Vol. IV. Lecture Notes in Math. Berlin-Heidelberg-New York: Springer 1974
86. Demjanenko, V. A. On the uniform boundedness of the torsion of elliptic curves over algebraic number fields (in Russian). Izv. Akad. Nauk SSSR **36** (1972)
87. Kubert, D.: Universal bounds on the torsion and isogenies of elliptic curves Harvard Ph. D. thesis, May 1973
88. McCabe, John. p-adic theta functions. Harvard Ph. D. thesis, pp. 1–222 (1968)
89. Manin, Y. I : Cyclotomic fields and modular curves (in Russian). Usp Mat. Nauk **26**, 7–71 (1971)
90. Manin, Y. I , Zarkin, Y G.: Heights on families of abelian varieties (in Russian). Mat. Sbornik **89**, 171–181 (1972)
91. Mazur, B.: Rational points of abelian varieties with values in towers of number fields. Inventiones math. **18**, 183–266 (1972)
92. Mazur, B , Swinnerton-Dyer, H. P. F.: Arithmetic of Weil curves. To appear in Inventiones math.
93. Milne, J.: Weil-Châtelet groups over local fields. Ann Sci. ENS, **3**, 273–284 (1970); *Addendum*, ibid. **5**, 261–264 (1972)

94. Néron, A.: Propriétés arithmétiques de certaines familles de courbes algébrıques. Proc. Int. Congress Amsterdam, **III**, 481–488 (1954)

95. Penney, D.E., Pomerance, C.· A search for elliptıc curves wıth large rank. In preparation

96. Raynaud, Michel· Variétés abéliennes et géométrie rıgıde. Proc Int. Congress Nice, **I**, 473–477 (1970)

97. Robert, A.: Elliptıc curves. Lecture Notes ın Mathematics **326**. Berlin-Heidelberg-New York Sprınger 1973

John T Tate
Harvard Unıversıty
Department of Mathematics
1 Oxford Street
Cambridge, MA 02138, USA

(Receiıed October 30, 1973)