A REVIEW OF NON-ARCHIMEDEAN ELLIPTIC FUNCTIONS

John Tate

This expository article consists of two parts. The first is an old manuscript dating from 1959, entitled "Rational points on elliptic curves over complete fields" containing my first proof of the isomorphism $k^*/t^{\mathbb{Z}} \simeq E_t(k)$. The second part is a discussion of some further aspects of the theory. It begins with a sketch of some topics I had hoped to add to the old manuscript before publishing it, namely, the description of the rational functions on E_t as "rigid analytic" meromorphic functions on k^* with multiplicative period t, the construction of these via theta-functions, and the classification of isogenies between the E_t's. Then, after a discussion of some consequences of the isogency classification, there is a description of the kernel $E_t[m]$ of multiplication by m on E_t as finite flat group scheme, and an indication of its relevance to the main theme of this conference. Finally, curves E_t over more general base rings than local fields are discussed, in particular, the "universal curve" E_q over $\mathbb{Z}[[q]][q^{-1}]$, and the connection with moduli. First, here is the old manuscript.

Rational Points on Elliptic Curves Over Complete Fields.

Let k be a field complete with respect to a non-trivial real valued valuation of the type satisfying

$$|x| \geq 0 \ , \quad |xy| = |x|\,|y| \ , \quad |x+y| \leq |x| + |y| \ .$$

According to a theorem of Ostrowski, k is either the real or complex field, with a valuation equivalent to the ordinary one, or else k is 'non-archimedean' in the sense that the valuation satisfies the stronger condition

$$|x+y| \leq \max\{|x|, |y|\} \ .$$

In the 'classical' case when k is the complex field, the group of points on an elliptic curve defined over k can be represented as the quotient of the additive group of k by a discrete subgroup generated by two independent 'periods' ω_1 and ω_2. Passing from the additive group to the multiplicative group by means of the exponential function one can absorb one of these periods and obtain a representation of the group of points as the quotient of the multiplicative group of k by a discrete subgroup generated by one multiplicative period $t = e^{2\pi i \tau}$, where $\tau = \omega_2/\omega_1$. The explicit formulas giving this multiplicative representation are the well-known Fourier expansions of the Weierstrass

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

functions $\wp, g_2, g_3$, etc. These Fourier expansions, suitably normalized, yield 'universal' identities among power series with rational integral coefficients. Our aim in this paper is to show that these identities can be used to obtain an exactly parallel 'multiplicative' representation (Theorem 1) for the group of rational points on certain elliptic curves over an arbitrary complete field k. Unfortunately when k is non-archimedean this method works only for curves whose absolute invariant j satisfies $|j| > 1$. In a second paper we will consider the case $|j| \leq 1$, which is of quite a different nature.[1]

Let t be an element of k such that $0 < |t| < 1$ and consider the series

$$x(w) = \sum_{m=-\infty}^{\infty} \frac{t^m w}{(1-t^m w)^2} - 2\sum_{m=1}^{\infty} \frac{t^m}{(1-t^m)^2} \ , \tag{1}$$

where w is a non-zero variable in k. Using the identity

$$\frac{w}{(1-w)^2} = \frac{1}{w+w^{-1}-2} = \frac{w^{-1}}{(1-w^{-1})^2}$$

we can rewrite our series in the form

$$x(w) = \frac{w}{(1-w)^2} + \sum_{m=1}^{\infty} \left(\frac{t^m w}{(1-t^m w)^2} + \frac{t^m w^{-1}}{(1-t^m w^{-1})^2} - 2\frac{t^m}{(1-t^m)^2} \right) \tag{2}$$

which shows, by comparison with the geometric series $\sum_1^\infty t^m$, that the convergence is absolute for all $w \in k^*$ and is uniform for w in a subset of the form $r_1 \leq |w| \leq r_2$ and $|w - t^m| \geq \varepsilon$ for all $m \in \mathbb{Z}$, with $0 < r_1 < r_2$ and $\varepsilon > 0$. The functional equations

$$x(tw) = x(w) = x(w^{-1}) \tag{3}$$

are now obvious from (1) and (2) respectively. In the restricted range $|t| < |w| < |t|^{-1}$ we have $|t^m w| < 1$ and $|t^m w^{-1}| < 1$ for all positive integers m and can therefore expand the fractions under the summation sign in (2), obtaining

$$\begin{aligned} x(w) &= \frac{w}{(1-w)^2} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} (nt^{mn}w^n + nt^{mn}w^{-n} - 2nt^{mn}) \\ &= \frac{1}{w+w^{-1}-2} + \sum_{n=1}^{\infty} \frac{nt^n}{1-t^n}\ (w^n + w^{-n} - 2)\ , \quad \text{for } \ |t| < |w| < |t|^{-1}\ . \end{aligned} \tag{4}$$

In case k is the complex field the classical Fourier expansions to which we alluded in the first paragraph can be written in the form

$$\wp(u) = x(w) + \frac{1}{12} \qquad (w = e^u) \tag{5}$$

[1] This "second paper," never written, was to have discussed kernel of the reduction map via the formal group, especially in the ordinary case when that group is of height 1, so twisted multiplicative.

and

$$\text{(6)}\qquad \begin{cases} g_2 = \dfrac{1}{12} + 20\displaystyle\sum_{n=1}^{\infty} \dfrac{n^3 t^n}{1-t^n} \\ \\ g_3 = -\dfrac{1}{216} + \dfrac{7}{3}\displaystyle\sum_{n=1}^{\infty} \dfrac{n^5 t^n}{1-t^n} \ , \end{cases}$$

where $\wp(u), g_2$ and g_3 are the Weierstrass functions belonging to the periods $\omega_1 = 2\pi i$ and $\omega_2 = \log t$ (any value). A good reference for this classical theory is [H-C], Abschnitt II; formulas (5) and (6) are proved there in 2, §12. However, we shall pause here to give a direct proof for the sake of completeness. The function $x(w)$ is obviously meromorphic in the domain $k^* = k - \{0\}$, with multiplicative period t, its only singularities being double poles at the points $w = t^m$, $m \in \mathbb{Z}$. Therefore the function $x(e^u)$ is meromorphic in the whole u plane with additive periods $\omega_1 = 2\pi i$ and $\omega_2 = \log t$, its only singularities being double poles at the period points $m_1\omega_1 + m_2\omega_2$; $m_1, m_2 \in \mathbb{Z}$. The same is true of $\wp(u)$. The expansion of $\wp(u)$ in powers of u is

$$\text{(7)}\qquad \wp(u) = \frac{1}{u^2} + \frac{1}{20} g_2 u^2 + \frac{1}{28} g_3 u^4 + \cdots \ .$$

The corresponding expansion of $x(e^u)$ is readily obtained by substituting $w = e^u = 1 + u + \cdots$ in (4), namely

$$\text{(8)}\quad x(w) = \frac{1}{u^2 + \frac{1}{12}u^4 + \frac{1}{360}u^6 + \frac{1}{20160}u^8 + \cdots} + \sum_{n=1}^{\infty} \frac{nt^n}{(1-t^n)} \left(n^2u^2 + \frac{n^4}{12}u^4 + \cdots \right)$$

$$= \frac{1}{u^2} - \frac{1}{12} + \left(\frac{1}{240} + \sum_{n=1}^{\infty} \frac{n^3 t^2}{1-t^n} \right) u^2 + \left(-\frac{1}{6048} + \frac{1}{12} \sum_{n=1}^{\infty} \frac{n^5 t^n}{1-t^n} \right) u^4 + \cdots \ .$$

Since the pole terms cancel, the difference $\wp(u) - x(w)$ is an entire meromorphic function, hence constant. Formulas (5) and (6) now follow by comparison of coefficients in the two expansions (7) and (8).

Differentiating (5) we obtain

$$\text{(9)}\qquad \wp'(u) = w\frac{d}{dw}x(w) = \sum_{m=-\infty}^{\infty} \left(\frac{t^m w}{(1-t^m w)^2} + 2\frac{(t^m w)^2}{(1-t^m w)^3} \right)$$

$$= x(w) + 2y(w) \ ,$$

where

$$\text{(10)}\qquad y(w) = \sum_{m=-\infty}^{\infty} \frac{(t^m w)^2}{(1-t^m w)^3} + \sum_{m=1}^{\infty} \frac{t^m}{(1-t^m)^2}$$

$$\text{(11)}\qquad = \frac{w^2}{(1-w)^3} + \sum_{m=1}^{\infty} \left(\frac{t^{2m} w^2}{(1-t^m w)^3} - \frac{t^m w^{-1}}{(1-t^m w^{-1})^3} + \frac{t^m}{(1-t^m)^2} \right) \ .$$

Substituting (5) and (9) in the identity

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3 \tag{12}$$

we find

$$y^2 + xy = x^3 - b_2x - b_3 \ , \tag{13}$$

where

(14)

$$\begin{cases} b_2 = \dfrac{1}{4}\left(g_2 - \dfrac{1}{12}\right) = 5\displaystyle\sum_{n=1}^{\infty} \frac{n^3t^n}{1-t^n} = 5t + 45t^2 + 140t^3 + \cdots \\ \\ b_3 = \dfrac{1}{4}\left(g_3 + \dfrac{g_2}{12} - \dfrac{1}{432}\right) = \displaystyle\sum_{n=1}^{\infty} \left(\frac{7n^5 + 5n^3}{12}\right)\frac{t^n}{1-t^n} = t + 23t^2 + 154t^3 + \cdots \ . \end{cases}$$

The coefficients of these power series for b_2 and b_3 are integers because

$$7n^5 + 5n^3 = 7n^3(n^2-1) + 12n^3 \equiv 12n^3 \pmod{24} \ .$$

We now abandon the assumption that k is the complex field and see how much of the preceding theory carries over to an arbitrary complete field k, as described in the opening paragraph of this paper. Certainly the series (10) has the same convergence properties as (1) and can therefore be used to define a function $y(w)$ for non-zero $w \in k$. Trivial rearrangements of the defining series show that y satisfies the functional equations

$$y(tw) = y(w) \quad \text{and} \quad y(w^{-1}) + y(w) = -x(w) \ . \tag{15}$$

Moreover we can use the power series (14) to define elements b_2 and b_3 in k, no matter what its characteristic, because the coefficients are rational integers; the convergence for $|t| < 1$ in the non-archimedean case is obvious because the coefficients have absolute value ≤ 1. Thus it is natural to conjecture that for any complete field k and any element $t \in k$ with $0 < |t| < 1$ the equation (13) defines an elliptic curve, and the map $w \to (x(w), y(w))$ gives a parametrization of the points on this curve by the transcendental variable $w \in k^*$.

Let us denote by A the plane cubic curve which is defined over k by equation (13). To show that A is non-singular of genus 1 (rather than singular of genus 0) we must show that the discriminant Δ does not vanish. The expression for Δ as polynomial in b_2 and b_3, and hence as power series in t can be obtained by way of the classical formula in terms of g_2 and g_3:

$$\Delta = g_2^3 - 27g_3^2 = \left(4b_2 + \frac{1}{12}\right)^3 - 27\left(4b_3 - \frac{1}{3}b_2 - \frac{1}{216}\right)^2$$

$$= b_3 + b_2^2 + 72b_2b_3 - 432b_3^2 + 64b_2^3 \tag{16}$$

$$= t - 24t^2 + 252t^3 + \cdots \ . \tag{17}$$

In the classical case, hence also in the real case, we know $\Delta \neq 0$. In the non-archimedean case we see that $\Delta \neq 0$ because $\Delta \equiv t \pmod{t^2}$. Although we shall not require it, we mention here that the classical expansion of Δ as infinite product,

$$\Delta = t \prod_{n=1}^{\infty} (1 - t^n)^{24} \tag{17'}$$

holds for all t with $|t| < 1$ in any complete field, because the validity of this formula in the classical case ensures that it is a formal identity in the power series ring $\mathbb{Z}[\![t]\!]$, resulting from the substitution of (14) in (16). From (17') the non-vanishing of Δ follows without consideration of the different cases. At any rate, our curve A is elliptic, with the absolute invariant

$$j = \frac{(12g_2)^3}{\Delta} = \frac{(1 + 48b_2)^3}{\Delta} = \frac{1 + 240t + 2160t^2 + \cdots}{t - 24t^2 + 252t^3 + \cdots} \tag{18}$$

$$= \frac{1}{t}(1 + 744t + 196884t^2 + \cdots) \ ,$$

just as in the classical case.

In the projective plane our curve A is complete and non-singular with just one point at infinity, where $x/y = 0$. We shall designate this infinite point by 0 and shall from now on view A as an abelian variety in the canonical way, with 0 as origin. Thus the addition of points on A is determined uniquely by the fact that the map which attaches to each point $P \in A$ the linear equivalence class of the divisor $(P) - (0)$ is an isomorphism between the group of points on A and the group of divisor classes of degree 0 on A; that this map is a bijection follows from the Riemann-Roch theorem which assures us that each divisor class of degree 1 on A contains one and only one point. For three points P_i on A we have $P_1 + P_2 + P_3 = 0$ if and only if the divisors $(P_1) + (P_2) + (P_3)$ and $3(0)$ are linearly equivalent. But $3(0)$ is the intersection divisor of A with the infinite line; hence our condition is simply that $(P_1) + (P_2) + (P_3)$ be the intersection divisor of A with some line in the projective plane.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points $\neq 0$ on A and consider the line L joining P_1 and P_2 (or tangent to A at $P_1 = P_2$ if the points coincide). L is parallel to the y-axis in the (x, y) plane if and only if

$$x_1 = x_2 \quad \textit{and} \quad y_1 + y_2 = -x_1 \ . \tag{19}$$

Thus (19) is necessary and sufficient for L to pass through 0, or, equivalently, for $P_1 + P_2 = 0$. If $P_1 + P_2 \neq 0$, then L has an equation of the form

$$y = \lambda x + \nu \ , \tag{20}$$

where

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2} = \frac{x_1^2 + x_1 x_2 + x_2^2 - b_2 - y_2}{y_1 + y_2 + x_1} \tag{21}$$

$$\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2 \ .$$

(Notice that the two expressions for λ are identically equal when both are defined, and that at least one of them is defined since we are assuming (19) is false; in fact the second expression is needed only when $P_1 = P_2$, in which case it reduces to dy/dx at $P = P_1$.) Let $(x_3, \lambda x_3 + \nu)$ be the third intersection of L with A. Then x_3 is the third root of the cubic equation

$$x^3 - (\lambda^2 + \lambda)x^2 - \big(\nu(2\lambda + 1) + b_2\big)x - (b_3 + \nu^2) = 0 \tag{22}$$

which results from substituting (20) in (13). Hence $x_1 + x_2 + x_3 = \lambda^2 + \lambda$. Taking the negative of the third intersection using (19) we find that the sum $P_1 + P_2 = P_3$ has the coordinates

$$\begin{aligned} x_3 &= \lambda^2 + \lambda - x_1 - x_2 \\ y_3 &= -x_3 - \lambda x_3 - \nu \ , \end{aligned} \tag{23}$$

where $\lambda = \lambda(x_1, x_2, y_1, y_2)$ and $\nu = \nu(x_1, x_2, y_1, y_2)$ are given by (21).

Let $t^{\mathbb{Z}} = \{t^m \mid m \in \mathbb{Z}\}$ denote the infinite cyclic discrete subgroup of k^* which is generated by our element t, and let φ be the map of k^* into the projective plane which is defined by

$$\begin{aligned} \varphi(w) &= \big(x(w), y(w)\big) \ , && \text{if } \ w \notin t^{\mathbb{Z}} \\ \varphi(w) &= 0 \ , && \text{if } \ w \in t^{\mathbb{Z}} \ . \end{aligned} \tag{24}$$

Let A_k denote the group of points on A which are rational over k.

Theorem 1. *The map φ is a homomorphism of k^* onto A_k with kernel $t^{\mathbb{Z}}$.*

We prove first that φ maps k^* *into* A. Since $0 \in A$, this amounts to proving that equation (13) is an identity between the functions $x(w)$ and $y(w)$, holding for all values of the argument $w \in k^*$, $w \notin t^{\mathbb{Z}}$, for which the functions are defined. Since these functions have multiplicative period t, it is enough to consider values of w such that $|t| < |w| \leq 1$ and $w \neq 1$. In this range we can use formula (4) which expresses x as a power series in t with coefficients which are rational functions of w. There is an analogous expression for y which is obtained by expanding the fractions under the summation sign in (11) and which we don't bother to write out. Thus our contention will be proved if we can show that (13) is a *formal* identity when we interpret x and y (and b_2 and b_3) as *formal* power series in t with coefficients which are rational functions of an *indeterminate* w. Now in fact the coefficients of the formal power series in question are expressed as elements of the ring $\mathbb{Z}[w, w^{-1}, (1-w)^{-1}]$, *i.e.*, the subring of $\mathbb{Q}(w)$ generated by $1, w, w^{-1}$ and $(1-w)^{-1}$. The canonical homomorphism $\mathbb{Z} \to k$ extends to a homomorphism $\mathbb{Z}[w, w^{-1}, (1-w)^{-1}] \to k(w)$. Hence the formal identity we are trying to establish is a 'universal' one, and will hold in any characteristic provided it holds in characteristic 0. From the classical theory we know that our equation (13) holds true *numerically* if we substitute any pair of complex numbers w and t in the domain of convergence $|t| < |w| < |t|^{-1}$, $w \neq 1$. Fixing first w such that $|w| < 1$ and letting t vary we conclude that the resulting power series in t with complex coefficients are equal coefficient-wise; then letting w vary, we conclude

that the coefficients are formally equal as rational functions of an indeterminate, as was to be shown.

Next we prove that φ is a homomorphism. Given $w_1, w_2 \in k^*$, we put $w_3 = w_1 w_2$ and must prove

$$P_3 = P_1 + P_2 \ , \qquad P_i = \varphi(w_i) \ , \quad i = 1, 2, 3 \ . \tag{25}$$

In view of the periodicity $\varphi(tw) = \varphi(w)$ we can restrict our consideration to values of w_1 and w_2 in the ranges $|t| < |w_1| \leq 1$ and $1 \leq |w_2| < |t|^{-1}$. Then $|t| < |w_3| < |t|^{-1}$, so that all three w_i are within the domain of convergence of the power series expressions for x and y considered in the previous paragraph. Since $\varphi(1) = 0$ by definition, (25) holds trivially if $w_1 = 1$ or $w_2 = 1$. From (3), (15), and (19) we see that it also holds if $w_1 w_2 = 1$. Thus we may assume all three points P_i are different from 0 and write $P_i = (x_i, y_i)$, *i.e.*, put $x_i = x(w_i)$, $y_i = y(w_i)$ for $i = 1, 2, 3$. Suppose $x_1 \neq x_2$. Then, using the first expression for λ in (21), substituting (21) in (23), and clearing denominators we see that (25) is equivalent to the simultaneous identities

$$\begin{aligned} (x_1 - x_2)^2 x_3 &= (y_1 - y_2)^2 + (y_1 - y_2)(x_1 - x_2) - (x_1 - x_2)^2 (x_1 + x_2) \\ (x_1 - x_2) y_3 &= -(x_1 - x_2)(y_1 + x_3) + (y_1 - y_2)(x_1 - x_3) \ . \end{aligned} \tag{25$'$}$$

Now we can argue just as in the preceding paragraph: (25′) holds in the classical case (being in fact just the addition formulas for $\wp(u)$ and $\wp'(u)$). Hence (25′) is an identity in the ring of formal power series in t with coefficients in the ring

$$\mathbb{Z}\big[w_1, w_1^{-1}, w_2, w_2^{-1}, (1 - w_1)^{-1}, (1 - w_2)^{-1}, (1 - w_1 w_2)^{-1}\big] \ ,$$

and is therefore a functional identity in any complete field k. We could take care of the remaining case $x_1 = x_2$ by other explicit formulas, or by a continuity argument, but perhaps the simplest way out is to observe that $x_1 = x_2$ if and only if $P_1 = \pm P_2$ and to appeal to

Lemma 1. *Let φ be a map of a (multiplicative) group into an (additive) group which takes on an infinite number of distinct values and satisfies the identity $\varphi(w_1 w_2) = \varphi(w_1) + \varphi(w_2)$ whenever $\varphi(w_1) \neq \pm\varphi(w_2)$. Then φ is a homomorphism.*

Indeed, given w_1, w_2 we can select w so that

$$\varphi(w) \neq \pm\varphi(w_1) \quad , \quad \varphi(w) + \varphi(w_1) \neq \pm\varphi(w_2) \quad , \quad \varphi(w) \neq \pm\varphi(w_1 w_2)$$

and have then $\varphi(w w_1) = \varphi(w) + \varphi(w_1)$. Then

$$\varphi(w) + \varphi(w_1) + \varphi(w_2) = \varphi(w w_1) + \varphi(w_2) = \varphi(w w_1 w_2) = \varphi(w) + \varphi(w_1 w_2)$$

and the lemma follows upon cancelling $\varphi(w)$. It is obvious that our φ takes an infinity of values; for example (2) shows that $|x(1 + t^r)| = |t|^{-2r}$ in the non-archimedean case.

Thus φ is a homomorphism. That its kernel is $t^{\mathbb{Z}}$ is apparent from its very definition (24), and to complete the proof of Theorem 1 we have only to show that φ is surjective. This is true in the classical case, and the case in which k is the real field can be obtained as a corollary by means of the following lemma, which will also be of assistance in the non-archimedean case.

Lemma 2. *If $w \neq 0$ is separably algebraic over k and $\varphi(w) \in A_k$, then $w \in k$.*

Let K be a finite Galois extension of k containing w. Since k is complete, there is a unique extension of its valuation to K, and K is complete in the extended valuation. Thus we can consider the resulting map $\varphi : K^* \to A_K$. According to what we have already proved (applied to K instead of k), φ is a homomorphism with kernel $t^{\mathbb{Z}}$. Each automorphism σ of K over k preserves the extended valuation and therefore commutes with φ. Thus if $\varphi(w) \in A_k$, then $\varphi(w^\sigma) = \varphi(w)$, and w^σ/w is a power of t. But w^σ and w have the same absolute value so this power of t must be 1. Thus $w^\sigma = w$ for all σ and $w \in k$ as contended.

Before treating the case of non-archimedean k we first recall some facts about power series in such a field. Any non-zero power series can be written in the canonical form

$$f(z) = \alpha z^\nu (1 + a_1 z + a_2 z^2 + \cdots) \quad \text{with} \quad \alpha \neq 0 \ . \tag{26}$$

We define the *norm* of f by

$$\|f\| = \sup_{1 \leq n < \infty} \left\{ |a_n|^{1/n} \right\} \ . \tag{27}$$

Notice that this is a sup rather than a lim sup; $\|f\|$ is the smallest real number such that

$$|a_n| \leq \|f\|^n \quad \text{for } \textit{all} \quad n = 1, 2, 3, \ldots \ , \tag{28}$$

or is $+\infty$ if no such number exists. We call the open circle $|z| < \|f\|^{-1}$ the *inner* circle of convergence of f. Of course f may converge in some larger circle, but if so it does so only hesitantly. In the inner circle the convergence is direct and business-like right from the start, for we have $|a_n z^n| < (\|f\|\,|z|)^n$ for $n = 1, 2, 3, \ldots$ there, and $\|f\|\,|z| < 1$. This shows also that we have $|f(z) - \alpha z^\nu| < |\alpha z^\nu|$ in the inner circle, because the valuation is non-archimedean.

Proposition 1. *The non-zero power series with norm less than or equal to a fixed real number $\rho \geq 0$ form a group under multiplication.*

Let $f(z)$ be as in (26) and $g(z) = \beta z^\mu (1 + b_1 z + b_2 z^2 + \cdots)$. Their quotient is

$$\frac{f(z)}{g(z)} = \frac{\alpha}{\beta} z^{\nu - \mu} (1 + c_1 z + c_2 z^2 + \cdots)$$

where the c_n are determined recursively from the equation

$$a_n = b_n + b_{n-1} c_1 + b_{n-2} c_2 + \cdots + b_1 c_{n-1} + c_n \ .$$

From this equation we can prove inductively that $|c_n| \leq \rho^n$ if we assume $|a_n| \leq \rho^n$ and $|b_n| \leq \rho^n$ for $n = 1, 2, 3, \ldots$. Thus $\|f\| \leq \rho$ and $\|g\| \leq \rho$ implies $\|f/g\| \leq \rho$. This proves Proposition 1.

Proposition 2. *The power series of the form*

$$f(z) = z + a_1 z^2 + a_2 z^3 + \cdots \tag{29}$$

with norm less than or equal to a fixed real number $\rho \geq 0$ form a group with respect to the operation of composition $(f \circ g)(z) = f((g(z))$.

Let $f(z)$ be given by (29), let $g(z) = z + b_1 z^2 + b_2 z^3 + \cdots$ be another series of the same form, and let $h = f \circ \overset{-1}{g}$ be the series such that $f(z) = h(g(z))$. The coefficients c_i of $h(z) = z + c_1 z^2 + c_2 z^3 + \cdots$ are determined uniquely in terms of the a's and b's by comparing coefficients in the identity

$$z + a_1 z^2 + a_2 z^3 + \cdots = g(z) + c_1\big(g(z)\big)^2 + c_2\big(g(z)\big)^3 + \cdots \ .$$

Putting $g(z)^i = z^i + b_1^{(i)} z^{i+1} + b_2^{(i)} z^{i+2} + \cdots$ we can write the recursive equations for the c's in the form

$$a_n = b_n + c_1 b_{n-1}^{(2)} + c_2 b_{n-2}^{(3)} + \cdots + c_{n-1} b^{(n)} + c_n$$

for $n = 1, 2, \ldots$. Assume now $\|f\| \leq \rho$ and $\|g\| \leq \rho$. By Proposition 1 we have $\|g^i\| \leq \rho$ for all i. Thus $|a_n| \leq \rho^n$, $|b_n| \leq \rho^n$ *and* $|b_n^{(i)}| \leq \rho^n$ for all $n \geq 1$, $i \geq 2$, and it follows by induction that $|c_n| \leq \rho^n$ for all n. Hence $\|h\| = \|f \circ \overset{-1}{g}\| \leq \rho$, and the proposition is proved.

In particular if our power series (29) has norm $\leq \rho$ then so does its inverse series

$$\overset{-1}{f}(z) = z - a_1 z^2 - (a_2 - 2a_1^2) z^3 - (a_3 - 5a_2 a_1 + 5a_1^3) z^4 + \cdots \ , \tag{30}$$

and since f is the inverse of its inverse it follows that f and $\overset{-1}{f}$ have the same norm and hence the same inner circle of convergence. Each maps that circle into itself, and the identities $z = \overset{-1}{f}(f(z)) = f(\overset{-1}{f}(z))$ are satisfied for all z in the circle because the absolute convergence ensures the validity of the rearrangements of the series necessary to prove them. Hence:

Corollary 1. *A power series of the form* (29) *maps its inner circle of convergence $|z| < \|f\|^{-1}$ bijectively onto itself, the inverse mapping being given by the formal inverse series* (30).

Consider a power series of the form

$$g(z) = \frac{1}{z} + a_1 + a_2 z + a_3 z^2 + \cdots \ . \tag{31}$$

Its reciprocal $1/g(z)$ is of the form (29) and has the same norm. Applying Corollary 1 to this reciprocal we obtain

Corollary 2. *A power series of the form* (31) *maps its inner circle of convergence* $|z| < \|g\|^{-1}$ *($z = 0$ excluded) bijectively onto the domain* $|z| > \|g\|$.

These general facts about inversion of power series in a complete non-archimedean field will enable us to prove

Lemma 3. *If k is non-archimedean then for each $x \in k$ there exists an element w in a quadratic extension of k such that $x = x(w)$. Moreover w is separable over k except possibly if $x = 0$ and the characteristic of k is 2.*

The surjectivity of $\varphi : k^* \to A_k$ follows directly from Lemmas 2 and 3. Given a point $P = (x, y)$ in A_k we choose w as in Lemma 3 such that $x = x(w)$. Then $\varphi(w)$ and $\varphi(w^{-1}) = -\varphi(w)$ are points on A with the same x-coordinate as P. Since they are opposites, they are the only such points, so one of them is our given point P. By Lemma 2 we have $w \in k$ if w is separable. Thus every point of A_k is the image of some $w \in k^*$, except possibly the point $(0, \sqrt{b_3}\,)$ in characteristic 2. But the image of k^* under φ is a subgroup of A_k consisting of more than one element and its complement, which is a union of cosets, cannot possibly consist of one point. Thus the exception does not occur.

To prove Lemma 3 we treat the cases $|x| > |t|^{1/2}$ and $|x| < 1$ by different but analogous methods. In the first case we use the new variable

$$r = w + w^{-1} - 2\ . \tag{32}$$

Each fixed value $r \in k$ determines two reciprocal values of w, namely the roots of the quadratic equation

$$w^2 - (r+2)w + 1 = 0 \tag{33}$$

and these roots are separable over k because $w = w^{-1}$ implies $w = \pm 1 \in k$. For all integers $n \geq 1$ we have

$$w^n + w^{-n} - 2 = F_n(r) = r^n + c_{n,1}r^{n-1} + \cdots + c_{n,n-1}r \tag{34}$$

where $F_n(r)$ is a monic polynomial of degree n with rational integral coefficients $c_{n,i}$ and without constant term. (For example, this follows from the recurrence relation $F_{n+1} = (z+2)F_n - F_{n-1} + 2r$.) Substituting (34) in (4) and rearranging the resulting series in powers of r we obtain

$$x(w) = f(r) = \frac{1}{r} + a_1 r + a_2 r^2 + \cdots\ , \tag{35}$$

where the coefficients

$$a_n = \frac{nt^n}{1-t^n} + c_{n+1,1}\frac{(n+1)t^{n+1}}{1-t^{n+1}} + c_{n+2,2}\frac{(n+2)t^{n+2}}{1-t^{n+2}} + \cdots$$

are elements of k satisfying $|a_1| = |t|$, and $|a_n| \leq |t|^n$ for all $n \geq 1$. Notice that the numbering of the coefficients in (35) is shifted by one from that in the canonical form

(31), so that the norm of f, being the supremum of the numbers $|a_n|^{1/(n+1)}$, is $|t|^{1/2}$ rather than $|t|$. Thus, although $f(r)$ converges for $|r| < |t|^{-1}$, the inner circle of convergence is only $|r| < |t|^{-1/2}$. Corollary 2 shows now that given $x \in k$, $|x| > |t|^{1/2}$, there exists $r \in k$, $|r| < |t|^{-1/2}$ such that $x = f(r)$ and consequently $x = x(w)$, where w is a root of (33). For values of x such that $|x| < 1$ we shall expand $x(w)$ in terms of another variable, namely

$$s = w + tw^{-1} \ . \tag{36}$$

Each value of $s \in k$ determines two values of w, namely the roots of the quadratic equation

$$w^2 - sw + t = 0 \ . \tag{37}$$

These roots are separable over k except in the case $s = 0$, characteristic of $k = 2$, and $t \notin (k^*)^2$. For all integers $n \geq 1$ we have

$$w^n + (tw^{-1})^n = G_n(s,t) = s^n + d_{n,2}ts^{n-2} + d_{n,4}t^2s^{n-4} + \cdots \ , \tag{38}$$

where $G_n(s,t)$ is a polynomial in s and t with rational integral coefficients $d_{n,i}$ of the form indicated. This follows for example from the recursion relation $G_{n+1} = sG_n - tG_{n-1}$ and the initial conditions $G_0 = 2$, $G_1 = s$. From (2) we have

$$\begin{aligned} x(w) + 2\sum_{m=1}^{\infty} \frac{t^m}{(1-t^m)^2} &= \sum_{m=0}^{\infty} \left(\frac{t^m}{(1-t^m w)^2} + \frac{t^m(tw^{-1})}{(1-t^m(tw^{-1}))^2} \right) \\ &= \sum_{m=0}^{\infty} \sum_{n=1}^{\infty} nt^{mn}w^n + nt^{mn}(tw^{-1})^n \\ &= \sum_{n=1}^{\infty} \frac{n}{1-t^n}(s^n + d_{n,2}ts^{n-2} + d_{n,4}t^2s^{n-4} + \cdots) \\ &= a_0 + a_1 s + a_2 s^2 + \cdots \ , \end{aligned} \tag{39}$$

where

$$a_m = \frac{m}{1-t^m} + d_{m+2,2}\frac{m+2}{1-t^{m+2}}t + d_{m+4,4}\frac{m+4}{1-t^{m+4}}t^2 + \cdots \ . \tag{40}$$

In particular,

$$a_0 = d_{2,2}\frac{2t}{1-t^2} + d_{4,4}\frac{4t^2}{1-t^4} + \cdots$$

is divisible by $2t$, *i.e.*, $|a_0| \leq |2t|$, and

$$a_1 = \frac{1}{1-t} + d_{3,2}\frac{3t}{1-t^3} + d_{5,4}\frac{5t^2}{1-t^5} + \cdots$$

is a unit, *i.e.*, $|a_1| = 1$, and all a_n are integers, *i.e.*, $|a_n| \leq 1$ for all $n \geq 1$. Thus we have

$$x(w) = 2t\alpha + \beta f(s) \ , \tag{41}$$

where $|\alpha| \leq 1$, $|\beta| = 1$, and where $f(s) = s + (a_2/a_1)s^2 + \cdots$ is a power series of the form (29) with norm 1. Since the map $z \to 2t\alpha + \beta z$ is a bijection of the circle $|z| < 1$ with itself we conclude from Corollary 1 that, given any $x \in k$ with $|x| < 1$, there exists $s \in k$ with $x = 2t\alpha + \beta f(s)$ and consequently $x = x(w)$ where w is a root of (37). This concludes the proof of Lemma 3 and Theorem 1.

Let us have a closer look at our homomorphism $\varphi : k^* \to A_k$ in the non-archimedean case. Because of the periodicity $\varphi(tw) = \varphi(w)$ we can restrict our attention to values of w such that $|t| < w \leq 1$. For these we have by formulas (2) and (8′)

$$\left| x(w) - \frac{w}{(1-w)^2} \right| < 1 \quad \text{and} \quad \left| y(w) - \frac{w^2}{(1-w)^3} \right| < 1 \ . \tag{42}$$

Hence

$$\begin{aligned} &|t| < |w| < 1 \Longrightarrow |x(w)| < 1 \ \text{ and } \ |y(w)| < 1 \\ &|w| = 1 \Longrightarrow |x(w)| = \frac{1}{|1-w|^2} \geq 1 \ \text{ and } \ |y(w)| = \frac{1}{|1-w|^3} \geq 1 \ . \end{aligned} \tag{43}$$

Let us denote the ring of integers in k by $R_k = \{z \in k; |z| \leq 1\}$, and the group of units of R_k by $U_k = \{z \in k; |z| = 1\}$. Corresponding to each real number ρ, $0 < \rho \leq 1$, we have subgroups of U_k defined and denoted by

$$\begin{aligned} U_k[\rho] &= \left\{ z \in U_k \, ; \, |z-1| \leq \rho \right\} \\ U_k(\rho) &= \left\{ z \in U_k \, ; \, |z-1| < \rho \right\} \ . \end{aligned} \tag{44}$$

According to (43) the image of U_k under φ is the subset of A_k consisting of 0 and the points $P = (x, y)$ such that $|x| \geq 1$ and $|y| \geq 1$. This subset, which we shall denote by B_k, is therefore a subgroup of A_k, isomorphic to U_k. It also follows from (43) that the images under φ of the subgroups $U_k[\rho]$ and $U_k(\rho)$ are, respectively,

$$\begin{aligned} B_k[\rho] &= \left\{ P = (x,y) \in A_k \, ; \, |x| \geq \rho^{-2} \right\} \\ B_k(\rho) &= \left\{ P = (x,y) \in A_k \, ; \, |x| > \rho^{-2} \right\} \ . \end{aligned} \tag{45}$$

The fact that these subsets of A_k are subgroups can of course be proved directly from the algebraic addition formulas, without resort to our transcendental parameter w; the necessary argument becomes quite transparent if one uses the new variables $\xi = x/y$ and $\eta = 1/y$ which put 0 at the origin of the (ξ, η)-plane. Notice that ξ is a uniformizing parameter at 0. B_k is the subset of the (ξ, η)-plane where $|\xi| \leq 1$ and $|\eta| \leq 1$, and $B_k[\rho]$ is the subset of B_k where $|\xi| \leq \rho$. We don't go into details here.

The quotient group A_k/B_k is isomorphic to $k^*/\varphi^{-1}(B_k) = k^*/\langle t \rangle U_k$, and therefore to the quotient group of all absolute values of elements of k^* (the "value group" of k) by

the group of powers of $|t|$. Thus, A_k/B_k is finite if and only if the valuation is discrete, in which case A_k/B_k is a cyclic group of order e, where e is the ordinal number of t in k. In particular, we have $A_k = B_k$ if and only if t is a prime element in R_k.

The quotient group $B_k/B_k(1)$ is isomorphic to $U_k/U_k(1)$ and therefore to the multiplicative group of the residue class field $\bar{k} = R_k/P_k$. (Here $P_k = \{z; |z| < 1\}$ is the maximal ideal of R_k.) Now the coefficients of the defining equation (9) of our curve A lie in R_k; reducing them mod y_k we obtain

$$\bar{y}^2 + \bar{x}\,\bar{y} = \bar{x}^3 \tag{46}$$

as the equation for the "reduced curve" $\bar{A}$, defined over the residue class field. $\bar{A}$ is singular, having an ordinary double point at the origin $\bar{x} = 0$, $\bar{y} = 0$. There is one point at infinity on $\bar{A}$, which we shall denote by $\bar{0}$. The set of *non-singular* points on $\bar{A}$ forms a group with $\bar{0}$ as neutral element, the addition of non-singular points on $\bar{A}$ being defined geometrically in the same way as the addition of points on A, by the rule $\bar{P}_1 + \bar{P}_2 + \bar{P}_3 = \bar{0}$ if and only if $(\bar{P}_1) + (\bar{P}_2) + (\bar{P}_3)$ is the intersection of $\bar{A}$ with a line in the projective plane not passing through the singular point $(0, 0)$. Being singular and cubic, $\bar{A}$ must be of genus 0. In fact, the map

$$\bar{\varphi}(\bar{w}) = (\bar{w}, \bar{y}) \ , \quad \text{where} \quad \bar{x} = \frac{\bar{w}}{(1-\bar{w})^2} \quad , \quad \bar{y} = \frac{\bar{w}^2}{(1-\bar{w})^3} \ , \tag{47}$$

gives a birational transformation of the $\bar{w}$-line onto $\bar{A}$, the inverse transform being $\bar{w} = \bar{y}^2/\bar{x}^3$. This transformation $\bar{\varphi}$ carries the points $\bar{w} = 0$ and $\bar{w} = \infty$ onto the singular point of $\bar{A}$; for the remaining points it is an isomorphism of the multiplicative group onto the group of non-singular points of $\bar{A}$. Applying the place $k \to \bar{k}$ to coordinates of points we obtain a *reduction map* $\theta : A \to \bar{A}$. Specifically, we have $\theta(P) = \bar{0}$ if and only if $P \in B(1)$, and for the remaining points $P = (x, y)$, $\theta(P) = (\bar{x}, \bar{y})$ where bar denotes the residue class of whatever is under it. Thus B is just the set of points P on A such that $\theta(P)$ is a simple point of $\bar{A}$, and we shall denote the group formed by these simple points by $\bar{B}$. The diagram

$$\begin{array}{ccc} U_k & \xrightarrow{\varphi} & B_k \\ \downarrow & & \downarrow \theta \\ \bar{k}^* & \xrightarrow{\bar{\varphi}} & \bar{B}_{\bar{k}} \end{array} \tag{48}$$

is commutative, as one sees from (47) and (42). Thus our homomorphism φ can be viewed as a transcendental "lifting" of the birational transformation $\bar{\varphi}$, and from this point of view the success of our method becomes more understandable.

Reference

[H-C] A. Hurwitz and R. Courant, Funktionentheorie, Springer, Berlin, 1929.

In the following discussion we will denote the curve (13) of the above manuscript by E or E_t instead of A, and its group of k-rational points by $E(k)$ instead of A_k. We also assume that k is non-archimedean, and let C denote the completion of the algebraic closure of k.

The field of rational functions on E via theta functions.

We will denote by $K = k(x, y)$ the field of rational functions on E which are defined over k. In the classical case $k = \mathbb{C}$, K can be identified with the field of meromorphic functions f on $\mathbb{C}^*$ which have multiplicative period t, that is, satisfy f(tw)=f(w) for all w in $\mathbb{C}^*$. The same is true for our non-archimedean k if we add "defined over k" and define "meromorphic function on C^* defined over k" to be an element of the field of fractions of the ring of holomorphic ones, where by "holomorphic function on C^* defined over k" we mean a function $f : C^* \to C^*$ which is representable by an everywhere convergent Laurent series with coefficients in k. For a non-zero such series, the number of zeros in an annulus $r \leq |w| \leq R$ is finite, and in fact, the exact number of such zeros (multiplicities counted) can be read off the Newton Polygon of the series in the usual way; see e.g., [D-G-S, Ch.II]. The divisor of such a function is a collection of points c_i in C^* with multiplicities, such that each annulus contains only a finite number of c_i, and which is "defined over k" in the sense that the c_i are algebraic over k, and points conjugate over k have the same multiplicity, which is a multiple of the degree of inseparability of the point over k. Every such divisor is the divisor of a holomorphic function. In contrast to the classical case, the only holomorphic functions on k^* with no zeros in $\bar{k}$ are the monomials aw^n, $a \in k^*$, and in the Weierstrass product

$$\prod_{i,|c_i|\geq 1} \left(1 - \frac{w}{c_i}\right) \prod_{i,|c_i|<1} \left(1 - \frac{c_i}{w}\right)$$

showing the existence of a function with a given divisor $\{c_i\}$, no convergence factors are needed.

By an elliptic function (with period t) defined over k we mean a function meromorphic on C^* which is defined over k and invariant under $w \mapsto tw$. The above considerations show that the divisor of such a function $f(w)$ is the difference of two disjoint divisors with multiplicities > 0, each of which is invariant by $w \mapsto tw$ and defined over k. Consequently, $f = g/h$, where g and h are holomorphic functions on C^* defined over k, which satisfy a functional equation of the form $g(w) = aw^n g(tw)$. The monomial aw^n is the same for g and for h, since $f(w) = f(tw)$. Such functions are called theta functions of type aw^n, and n is called their degree. The dimension of the space of theta functions of a given type aw^n is n for $n > 0$, and is 0 for $n < 0$ (for $n = 0$ it is 1 if $a = t^m$ for some m in $\mathbb{Z}$, in which case the thetas are the monomials of degree $-m$, and is 0 otherwise, as is easily checked). Indeed, for $n \neq 0$, the space of *formal* Laurent series f satisfying $f(w) = aw^n f(tw)$ is of dimension $|n|$, because $|n|$ successive coefficients of the series can be arbitrarily prescribed, and the remaining ones are then determined by the relation $f(w) = aw^n f(tw)$. The resulting series converge everywhere if $n > 0$, but diverge if $n < 0$. The Newton Polygon of such a series is invariant under the map $(x, y) \mapsto (x + n, y - \log|a| - x \log|t|)$. From this it follows easily that a theta function $g(w)$ of degree $n > 0$ has exactly n zeros in an annulus of the form $r|t| < |w| \leq r$. Hence, an elliptic function f has the same number of zeros as poles in such a "period annulus", and if that number is n, then f is the quotient of two theta functions of degree n of the same type. For $n = 0$ or 1, the ratio of two such thetas is constant. Hence, an elliptic

function with no pole is constant, and there is no elliptic function with just one simple pole in a period annulus.

Now one can proceed as in the classical Weierstrass theory. The role of the Weierstrass sigma function is played by a theta function of type $-w$, for example, the function

$$\theta(w) = \sum_{n\in\mathbb{Z}} (-1)^n t^{\frac{n^2-n}{2}} w^n \ .$$

The zeros of $\theta(w)$ are the points $w = t^n$, $n \in \mathbb{Z}$, each with multiplicity one. This follows from consideration of the Newton Polygon as above, together with the fact that $\theta(1) = 0$. It also follows from the classical identity

$$\theta(w) = (1-w) \prod_{m=1}^{\infty} \left[(1-t^m)(1-t^m w)(1-t^m w^{-1})\right]$$

Using that identity it is easy to show that $\theta(w)^2 x(w)$ and $\theta(w)^3 y(w)$ are holomorphic, and consequently, $x(w)$ and $y(w)$ are elliptic functions in the above sense. In fact, the differential operators $D := wd/dw$ and $D_2 := \frac{1}{2}(D^2 - D)$ act on the ring of holomorphic functions, and, putting

$$\zeta(w) = -\frac{D\theta(w)}{\theta(w)}$$

we have $\zeta(tw) = 1 + \zeta(w)$, and

$$x(w) = D\zeta(w) \quad , \quad y(w) = D_2\zeta(w) \ .$$

Thus $Dx = 2y + x$, or, in terms of differentials,

$$dx/(2y + x) = dw/w \ .$$

Further details (e.g., the fact that elliptic functions are rational functions of x and y, the expression of elliptic functions in terms of $\theta(w)$, etc.) are left to the reader; references are [R] and [S]. Everything is as in the classical case, except perhaps for some questions of rationality, like the surjectivity of the homomorphism $\varphi : k^* \to E(k)$. A shorter proof of that than the one in the manuscript above is as follows. Let $P = (x_0, y_0)$ be a point on $E(k)$. The function $x - x_0$ has zeros only at P and $-P$. If P is not in the image of φ, then the function $w \mapsto x(w) - x_0$ has no zero in k^*. That function has a pole at $w = 1$, hence it has a zero at some point w_0 in C^*. Then $\varphi(w_0) = P$ or $-P$, and, replacing w_0 by $1/w_0$ if necessary, we can assume $\varphi(w_0) = P$, i.e., that $w = w_0$ is a common zero of $x(w) - x_0$ and of $y(w) - y_0$. These two functions can't have two common zeros in a period annulus — otherwise the function $y(w)/x(w)$ would have exactly one pole there, which is impossible. Thus the divisor consisting of the points $w_0 t^n$, $n \in \mathbb{Z}$, with multiplicity one, is rational over k, i.e., w_0 is in k^*, as was to be shown.

At one point later on it will be convenient to consider the group of points of our curve E_t not only with coordinates in k or C, but also in a finite commutative k-algebra A.

Any such algebra is a product of local ones, so it suffices to consider that case. We leave to the reader the exercise of showing that for a local A, our functions x and y, or perhaps better, the theta functions of type $-w^3$, give a surjective homomorphism

$$\varphi : A^* \to E_t(A)$$

with kernel $t^{\mathbb{Z}}$, so induce an isomorphism

$$A^*/t^{\mathbb{Z}} \simeq E(A) \ ,$$

which is of course functorial in A. One can argue by induction on the length of A. If I is an ideal of square zero and $B = A/I$, the induction step from B to A can be made with the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Lie}(\mathbb{C}_m) \otimes I & \longrightarrow & A^*/t^{\mathbb{Z}} & \longrightarrow & B^*/t^{\mathbb{Z}} & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{Lie}(\varphi)\otimes \mathrm{id}}\downarrow & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} & & \\ 0 & \longrightarrow & \mathrm{Lie}(E_t) \otimes I & \longrightarrow & E_t(A) & \longrightarrow & E_t(B) & \longrightarrow & 0 \end{array}$$

For non local A it follows that $E(A) = A^*/t^{\mathbb{Z}(A)}$, where $\mathbb{Z}(A)$ is the group of continuous maps $i : \mathrm{Spec}(A) \to \mathbb{Z}$.

Isogenies.

Suppose $t_1, t_2 \in k$, with $0 < |t_1|, |t_2| < 1$. We will say t_1 and t_2 are "commensurable" if there exist non-zero integers m, n such that $t_2^m = t_1^n$. When this is the case the left hand square of the following diagram is commutative

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{1\mapsto t_1} & C^* & \xrightarrow{\varphi} & E_{t_1}(C) & \longrightarrow & 0 \\ & & {\scriptstyle m}\downarrow & & {\scriptstyle n}\downarrow & & \downarrow{\scriptstyle \alpha_{m,n}} & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow[1\mapsto t_2]{} & C^* & \xrightarrow{\varphi} & E_{t_2}(C) & \longrightarrow & 0 \end{array}$$

and consequently there is a unique homomorphism

$$\alpha_{m,n} : E_{t_1}(C) \to E_{t_2}(C)$$

making the right hand square commutative. This map $\alpha_{m,n}$ is in fact an isogeny defined over k, because composition with $w \mapsto w^n$ takes meromorphic functions on C^* with period t_2 into those with period t_1 and preserves the field of definition of such functions, and therefore composition with $\alpha_{m,n}$ carries rational functions on E_{t_2} defined over k into those on E_{t_1}.

Theorem. *The degree of $\alpha_{m,n}$ is mn. Every isogeny between curves of type E_t is of the form $\alpha_{m,n}$; the map $(m, n) \mapsto \alpha_{m,n}$ is an isomorphism*

$$\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid t_2^m = t_1^n\} \simeq \mathrm{Hom}_k(E_{t_1}, E_{t_2}) = \mathrm{Hom}_C(E_{t_1}, E_{t_2}) \ .$$

In particular, E_{t_1} is isogenous to E_{t_2} if and only if t_1 and t_2 are commensurable.

Proof. If $t = t_2^m = t_1^n$, with $m > 0$, hence $n > 0$, then we have a commutative triangle.

$$\begin{array}{ccc} & E_t & \\ {\scriptstyle \alpha_{1,n}}\nearrow & & \searrow{\scriptstyle \alpha_{m,1}} \\ E_{t_1} & \xrightarrow[\alpha_{m,n}]{} & E_{t_2} \end{array}$$

The degree of $\alpha_{m,1}$ is m, because the corresponding function field extension is cyclic of degree m, with Galois group generated by the automorphism translation by t_2 on the field of meromorphic functions with period $t = t_2^m$. In case $m = n$ and $t_2 = t_1$ the map $\alpha_{n,n}$ is multiplication by n on E_{t_1}, which shows that $\alpha_{n,1}$ is dual to $\alpha_{1,n}$ and has therefore degree n. Hence the degree of $\alpha_{m,n}$ is mn, as claimed. (Note that $\alpha_{-m,-n} = -\alpha_{m,n}$.)

To prove the rest we can assume the ground field is C, since we have already noted that $\alpha_{m,n}$ is defined over k if t_1 and t_2 are in k. Since C is algebraically closed, every isogeny over C is a product of isogenies of prime degree. Since it is obvious that the composition of maps of the form $\alpha_{m,n}$ is of that same form, we are reduced to proving that an isogeny $\beta : E_t \to E_{t'}$ of prime degree p is of the form $\alpha_{p,1}$, or $\alpha_{1,p}$. The j-invariants of our curves are not 0 or 1728 because they satisfy $|j| > 1$. Consequently the only automorphisms of the curves (preserving the group structure) are ± 1, and it follows that an isogeny is determined up to sign by its kernel. Since $-\alpha_{m,n} = \alpha_{-m,-n}$, it suffices to show that the only finite subgroup-schemes of order p of E_t are the kernel of $\alpha_{1,p}$ and the kernels of the various $\alpha_{p,1}$'s. If p is not the characteristic of C, then this amounts to the fact that a subgroup of order p of $C^*/t^{\mathbb{Z}}$ is either the group of pth roots of 1, or is generated by one of the pth roots of t. Suppose $p = \mathrm{char}(C)$. Then $\alpha_{1,p} : E_t \to E_{t^p}$ is the Frobenius, and $\alpha_{p,1} : E_t \to E_{t^{1/p}}$ is the Verschiebung. The kernels of these two maps are the only subgroupschemes of order p, because their product is the kernel of multiplication by p and they are not isomorphic, being isomorphic to μ_p and $\mathbb{Z}/p\mathbb{Z}$, respectively. This concludes the proof of the Theorem.

Applications.

An immediate corollary is the fact that $\mathrm{Hom}(E_t, E_t) = \mathbb{Z}$, i.e., our curves do not have nontrivial endomorphisms. When I first told Serre about the existence of the curves E_t, he noted that if the curve is defined over a finite extension of $\mathbb{Q}_p$ the non-existence of non-trivial endomorphisms can be seen from the action of Galois on points of finite order, and that this gives a nice proof that the j-invariant of an elliptic curve with complex multiplication is an algebraic integer. Indeed, if j were not an integer at a place above a prime p, then there would be a finite extension of $\mathbb{Q}_p$ over which the curve is isomorphic to E_t for $t = j^{-1} + 744j^{-2} + 750420j^{-3} + \cdots$, contradicting the fact that E_t does not have non trivial endomorphisms. Incidentally, a generalization to abelian varieties of CM type is the fact that such a variety has potential good reduction at every place [S-T, Thm. 6(a)].

Another corollary of the theorem is that if $\ell : k^* \to V$ is a homomorphism of k^* into a $\mathbb{Q}$-vector space V, and if the valuation v satisfies $v(k^*) \subset \mathbb{Q}$, then $\ell(t)/v(t)$ is an isogeny invariant of the curves of type E_t. The special case $k = \mathbb{Q}_p$, $V = k$, $\ell : k^* \to k$ is the p-adic logarithm $\log_p$, and $v = \mathrm{ord}_p$ is of interest. In that case, if E_t arises by base change

from an elliptic curve E over $\mathbb{Q}$, Greenberg and Stevens have proved [G-S], at least for $p > 3$, that

$$L_p'(1) = \frac{\log_p(t)}{\mathrm{ord}_p(t)} \ \frac{L(1)}{\Omega}$$

where L_p is the p-adic and L the ordinary L-function of E, and Ω is the real period of E. This relation is predicted by the p-adic Birch and Swinnerton-Dyer conjecture proposed in [M-T-T]. The usual Birch and Swinnerton-Dyer conjecture involves the discriminant of a real-valued height pairing on the Mordell-Weil group $E(\mathbb{Q})$. The p-adic conjecture involves the discriminant of a p-adic height pairing on the so-called extended Mordell-Weil group which is the extension of $E(\mathbb{Q})$ by $\mathbb{Z}$ obtained by taking the inverse image of $E(\mathbb{Q})$ under the map $\varphi : \mathbb{Q}_p^* \to E(\mathbb{Q}_p)$. Call this inverse image $E'(\mathbb{Q})$, and let $E'(\mathbb{Q})_0$ denote its intersection with $\mathbb{Z}_p^*$. Then for a, b $E_0'(\mathbb{Q})$ and $c \in E'(\mathbb{Q})$, the p-adic height pairing satisfies

$$\langle a, b\rangle = \text{usual } p\text{-adic } \langle (a), (b)\rangle$$
$$\langle c, t\rangle = \log_p(c)/\mathrm{ord}_p(t)$$

In particular, $\langle t, t\rangle$ is the isogeny invariant $\log_p(t)/\mathrm{ord}_p(t)$ occurring in the result of Greenberg and Stevens mentioned above. In case the rank of $E(\mathbb{Q})$ is 0, their result is the p-adic Birch and Swinnerton-Dyer conjecture.

For each integer $n > 0$, let K_n be the field of elliptic functions on k^* with period t^n, isomorphic to the field of rational functions on E_{t^n} defined over k. Let K_∞ be the union of the K_n, and let s denote the automorphism of K_∞ given by translation by t. This automorphism s is of infinite order and its fixed field is $K_1 = K$. The extension K_∞/K is Galois with group $\widehat{\mathbb{Z}}$ and the powers of s form a canonically determined dense subgroup. (K_n/k, as abstract function field, determines the elliptic curve E_{t^n} over k, its j-invariant, hence its period t^n, and then, up to sign, the parametrization $\varphi : k^* \to E_{t^n}$, and the automorphism s.) The finite subextensions of K_∞/K are the K_n/K, and they have the remarkable property to be not only unramified, but split completely at every place of K, even though k may be far from algebraically closed.

Points of finite order.

For an integer $m > 0$ let $E_t[m]$ denote the kernel of multiplication by m on E_t. This is a finite flat group scheme over k whose structure is easy to describe. Let R be an arbitrary ground ring, and let u be an invertible element of R. Consider the functor from commutative R-algebras A to abelian groups which associates to A the quotient group of the group of pairs $(a, i) \in A^* \times \mathbb{Z}(A)$ such that $a^m = u^i$, modulo the subgroup of pairs of the form (u^i, im). (Here $\mathbb{Z}(A)$ denotes the group of locally constant functions $i : \mathrm{Spec}\, A \to \mathbb{Z}$.) An element of that quotient is represented by a unique pair (a, i) such that $0 \le i(x) < m$ for $x \in \mathrm{Spec}\, A$, and consequently the functor is represented by the scheme

$$\coprod_{i=0}^{m-1} \mathrm{Spec}(B_i) = \mathrm{Spec}\left(\prod_{i=0}^{m-1} B_i\right)$$

where $B_i = R[X]/(X^m - u^i)$. The group law on the functor makes this scheme a group-scheme which we denote by $G = G_{R,u,m}$. There is an exact sequence

$$0 \to \mu_m \to G_{R,u,m} \to \mathbb{Z}/m\mathbb{Z} \to 0 \ ,$$

the maps being $z \mapsto (z, 0)$ and $(a, i) \mapsto i \pmod m$. Since $H^1(R, G_m) = 0$ in the flat topology ("Hilbert theorem 90"), every $(\mathbb{Z}/m\mathbb{Z})$-module scheme over R which is an extension of $\mathbb{Z}/m\mathbb{Z}$ by μ_m is of the form $G_{R,u,m}$ for some $u \in R^*$. The class of the extension is determined by the image of u in $R^*/(R^*)^m = H^1(R, \mu_m)$. It is easy to see that an isomorphism $G_{R,u,m} \to G_{R,v,m}$ which induces identity on μ_m and on $\mathbb{Z}/m\mathbb{Z}$ is of the form $(a, i) \to (ar^i, i)$, where $r \in R$ and $r^m = v/u$. More generally, for integers e, f, a homomorphism $G_{r,u,m} \to G_{r,v,m}$ which induces multiplication by e on μ_m and by f on $\mathbb{Z}/m\mathbb{Z}$ is of the form

$$(a, i) \mapsto (a^e r^i, fi) \ , \quad \text{where } r \in R \text{ satisfies } u^e r^m = v^f \ .$$

If u is of infinite order in A^* in the sense that $i \mapsto u^i$ is an isomorphism $\mathbb{Z}(A) \simeq u^{\mathbb{Z}(A)}$, then a pair (a, i) is determined by a alone and

$$G_{R,u,m}(A) = \text{ points of order dividing } m \text{ in the group } A^*/u^{\mathbb{Z}(A)} \ .$$

Now take $R = k$, $u = t$. The functorial isomorphism $\varphi : A^*/t^{\mathbb{Z}(A)} \simeq E_t(A)$ for finite dimensional k-algebras A induces an isomorphism of functors, and hence of finite flat group schemes,

$$G_{k,t,m} \simeq E_t[m] \ .$$

Of course, if m is prime to the characteristic of k, then we do not need the isomorphism $A^*/t^{\mathbb{Z}(A)} \simeq E_t(A)$ for all finite A, but only for A's which are (products of) fields. Indeed in that case, the group scheme $E_t[m]$ is etale and is determined by the Galois module $E_t[m](\bar{k})$. In any case, there is a canonical exact sequence of finite flat k-group schemes, or Galois modules,

$$0 \to \mu_m \to E_t[m] \xrightarrow{a} \mathbb{Z}/m\mathbb{Z} \to 0 \ .$$

The Weil pairing

$$E_t[m] \times E_t[m] \to \mu_m$$

is given by $(P, Q) \mapsto a(P)Q - a(Q)P$, or by the negative of that expression, according to one's convention.

The case $E_t[m]$ has good reduction.

Let R be the ring of integers in k. The elliptic curve E_t over k does not have good reduction, that is, there is no elliptic curve over R whose general fiber is E_t. However, it may happen for some m that $E_t[m]$ has good reduction, i.e., is the general fiber of a finite flat group scheme over R. From the above discussion it is clear that this happens if $|t| \in |k^*|^m$; then $t = ua^m$ with $u \in R^*$, $a \in k^*$, and $E_t[m]$ is isomorphic to the general fiber of $G_{R,u,m}$. This would be the situation at each place ℓ of bad reduction of the Frey curve corresponding to a counterexample to Fermat for a prime exponent m. That fact plays an essential role in the relation between the modularity of curves over $\mathbb{Q}$ and Fermat's last theorem suggested by Frey, made more precise by Serre [S2], proved by Ribet [R] and recently exploited by Wiles.

Serre's isogeny theorem.

Suppose p is a prime and k is locally compact with residue characteristic p. Let E_{t_1} and E_{t_2} be two curves over k of our type, and let $E_{t_i}[p^\infty]$ denote the p-divisible group of E_{t_i} over k for $i = 1, 2$. Then the natural map

$$\mathbb{Z}_p \otimes \mathrm{Hom}(E_{t_1}, E_{t_2}) \to \mathrm{Hom}(E_{t_1}[p^\infty], E_{t_2}[p^\infty]) \ ,$$

is an isomorphism. This was proved by Serre [S1, A1.4] in case k is of characteristic 0 and used by him to prove [S1, 2.3] the global isogeny theorem for elliptic curves over a number field with non-integral j-invariant. The global theorem was later proved for all abelian varieties by Faltings, but Serre's result is all that is needed to show for semistable elliptic curves over $\mathbb{Q}$ that the modularity of their Galois representation implies that they are modular in the stronger sense of being covered by a modular curve.

We will prove the local isogeny theorem above by giving an explicit description of the two groups involved as indicated by the following diagram

$$\begin{array}{ccc} \mathrm{Hom}(E_{t_1}, E_{t_2}) & \longrightarrow & \mathrm{Hom}(E_{t_1}[p^\infty], E_{t_2}[p^\infty]) \\ {\scriptstyle \alpha_{m,n}}\uparrow \quad \wr\uparrow & & \downarrow\wr \quad \downarrow{\scriptstyle h} \\ {\scriptstyle (m,n)} & & {\scriptstyle (e,f)} \\ \{(m,n) \in \mathbb{Z}\times\mathbb{Z} \mid t_2^m = t_1^n\} & \longrightarrow & \{(e,f) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid t_2^e = t_1^f \in \widehat{k^*}\} \end{array}$$

$$(m,n) \longmapsto (m,n)$$

Here,

$$\widehat{k^*} := \varprojlim_r (k^*/(k^*)^{p^r}) \ .$$

The right hand vertical map is explained by the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_{p^\infty} & \longrightarrow & E_{t_1}[p^\infty] & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle e} & & \\ 0 & \longrightarrow & \mu_{p^\infty} & \longrightarrow & E_{t_2}[p^\infty] & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & 0 \end{array}$$

Here h is an arbitrary homomorphism of the p-divisible groups. It must respect the filtrations because there is no non-trivial homomorphism $\mu_{p^\infty} \to \mathbb{Q}_p/\mathbb{Z}_p$. (In characteristic p, μ_{p^∞} is connected and the connected component of $\mathbb{Q}_p/\mathbb{Z}_p$ is trivial; in characteristic 0 it is clear from the fully faithful representation of the situation by Galois modules, since the Galois action on μ_{p^∞} is non-trivial.) The endomorphisms induced by h on the submodule and quotient module are multiplications by p-adic integers f and e, respectively, because those groups have no other endomorphisms than such multiplications. Thus the restriction of h to the finite group schemes $E_t[p^r] \simeq G_{k,t}, p^r$ is of the type considered above and consequently $t_2^f = t_1^e$ in $k^*/(k^*)^{p^r}$ for all r. In other words, the equality $t_2^f = t_1^e$ holds in the multiplicatively written $\mathbb{Z}_p$-module

$$\widehat{k^*} := \varprojlim_r (k^*/(k^*)^{p^r})$$

The map $h \mapsto (e, f)$ is injective because there is no non-trivial homomorphism $\mathbb{Q}_p/\mathbb{Z}_p \to \mu_{p^\infty}$. It is surjective because by the above discussion, for given (e, f) satisfying $t_2^e = t_1^f$ in $\widehat{k^*}$, there is a homomorphism

$$h_j : E_{t_1}[p^j] \longrightarrow E_{t_2}[p^j]$$

for each j inducing e on the quotient module and f on the submodule, and h_j is unique up to the addition of homomorphisms $\mathbb{Z}/p^j\mathbb{Z} \to \mu_{p^i}$. Therefore if $p^c = \#(\mu_{p^\infty}(k))$ is the number of p-power roots of 1 in k, then all choices of h_j (for a given pair (e, f)) induce the same homomorphism on $E_{t_1}[p^{j-c}]$. Hence these latter homomorphisms are coherent and give the desired h which maps to (e, f).

Now the key idea in Serre's proof is that the valuation gives a homomorphism $v : \widehat{k^*} \to \mathbb{Z}_p$ which applied to the condition on e and f gives

$$ev(t_2) = fv(t_1)$$

Since $v(t_1)$ and $v(t_2)$ are non-zero rational integers, it follows that we can multiply the pair (e, f) by a p-adic unit so that it becomes a pair of ordinary integers. Then $t_2^e t_1^{-f}$ is in the kernel of the map $k^* \to \widehat{k^*}$ so is a root of unity of order prime to p in k. Multiplying the pair (e, f) by that order, we get a pair (m, n) such that and our original pair is a p-adic unit times (m, n), which is what we needed to show.

More general ground rings.

Suppose R is a commutative ring and I an ideal in R such that R is I-adically complete and separated. Suppose $t \in I$ is a non-zero-divisor in R, and put $k = R[1/t]$. Formulas (14) define elements b_2 and b_3 in I, and equation (13) defines an elliptic curve over k which we will denote by E_t. Putting

$$u = \frac{y + x}{y} = 1 + \frac{x}{y} \quad , \quad v = \frac{1}{y}$$

the equation for E_t becomes

$$F(u, v) := uv - (u - 1)^3 + b_2(u - 1)v^2 + b_3v^3 = 0 \ .$$

Let $E_t^0(k) = \{P = (u, v) \in E_t(k) \mid u \in R^* \text{ and } v \in R\}$. Then the map $(u, v) \mapsto u$ is a bijection from $E_t^0(k) \to R^*$. The inverse map can be defined by $v = v(u) := \lim(v_n(u))$, where the functions $v_n : R^* \to R$ are defined inductively by

$$v_1(u) = \frac{(u - 1)^3}{u} \ , \quad \text{and } v_{n+1}(u) = v_n(u) - F(u, v_n(u))/u \ , \quad \text{for } n > 0 \ .$$

By induction, one proves that $F(u, v_n(u))$ is in I^n.

In fact, $E_t^0(k)$ is a subgroup of $E_t(k)$, "analytically" isomorphic to R^* in the following sense. There is a Laurent series $f(u)$ with coefficients in R, convergent for all $u \in R^*$, such that $f(u) \equiv u \pmod{I}$, and such that the map $P = (u, v) \mapsto f(u)$ is an isomorphism

$E_t^0(k) \to R^*$. In case R is a discrete valuation ring this map is just the inverse of the negative of the map $\varphi : R^* \to E_t^0(k)$, and we can use the same formulas in the present more general setting. Formulas (2) and (11) yield

$$x + y = \frac{w}{(1-w)^3} + g(w)$$
$$y = \frac{w^2}{(1-w)^3} + h(w)$$

where $g(w)$ and $h(w)$ are Laurent series with coefficients in I which are Laurent polynomials modulo I^n for every n. Hence

$$\begin{aligned} u = (x+y)/y &= (w^{-1} + g(w)(1-w)^3/w^2)/(1 + h(w)(1-w)^3/w^2) \\ &= F(w^{-1}) \text{ , say,} \end{aligned}$$

where $F(z)$ is a Laurent series in z with coefficients in R, $\equiv z \pmod I$ and polynomial $\pmod{I^n}$ for every n. Such an F maps R^* bijectively to R^*, and the inverse function is of the same type. To see this, note that all positive and negative powers of $F(z)$ are functions of a similar type, the monomial z being replaced by z^n in the nth power, so that we can define functions $f_n(Z)$ inductively by

$$f_1(z) = 1 \text{ and } f_{n+1}(z) = f_n(z) + H_n(z) \text{ , where } H_n(z) := z - f_n(F(z)) \text{ ,}$$

for $n > 0$. Then $H_{n+1}(z) = H_n(z) - H_n(F(z))$, hence $H_n(z) \equiv 0 \pmod{I^n}$, and the f_n's converge to an f such that $f(F(z)) = z$.

We leave to the reader the task of showing that the map : $w \mapsto P = (u, v(u))$, with $u = f(w)$ is a group homomorphism. I do not know to what extent this isomorphism $R^* \simeq E_t^0(k)$ can be extended to $k^*/q^{\mathbb{Z}} \to E_t(k)$ in this more general situation, as it can in the case k is a local field. Presumably it can at least be extended to points $w \in k^*$, some power of which is in $R^*q^{\mathbb{Z}}$, with the image being the points in $E_t(k)$, some multiple of which is in $E_t^0(k)$. That would enable us to show that the isomorphism $G_{k,t,m} \simeq E_t[m]$ still holds in this more general situation. But that is known anyway, as we indicate in the next section.

The modular point of view.

All of the elliptic curves which we have discussed so far are obtainable by base change from one single curve, E_q, defined over the ring $\mathbb{Z}[[q]][1/q]$ of finite-tailed Laurent series in an indeterminate q with coefficients in $\mathbb{Z}$. Indeed, given any R, t as above, there is a unique homomorphism from $\mathbb{Z}[[q]][1/q]$ to $k = R[1/t]$ taking $q \to t$, and continuous from the q-adic topology in $\mathbb{Z}[[q]]$ to the I-adic topology in R, and thus E_t can be obtained as a base change of E_q. A more sophisticated and algebraic construction of E_q than the one we give here, due to Raynaud, is explained in detail in [D-R, VII]. That construction, which involves no specific powerseries at all, uses the notion of "generalized elliptic curve" and Grothendieck's existence theorem. It produces E_q as the generalized elliptic curve over $\mathbb{Z}[[q]]$ which algebrizes a formal such curve which is obtained as the limit of schemes over

$\mathbb{Z}[q]/(q^n)$ which are quotients by the action of $\mathbb{Z}$ on schemes whose geometric fibers are infinite strings of copies of P^1 indexed by $\mathbb{Z}$, the point ∞ of the ith copy being identified with the point 0 on the $(i+1)$th. This approach yields an isomorphism $G_{k,q,m} \to E_q[m]$ for each m, where here $k = \mathbb{Z}[[q]][1/q]$.

The curve E_q is used to study the modular curves in the neighborhood of cusps. For example, it identifies $\mathbb{Z}[[q]]$ with the formal completion of $\mathcal{M}_1$ at $j = \infty$, and if a modular form f of level 1 defined over a ring R is viewed as a function which attaches to every pair (E, ω) consisting of an elliptic curve E over an R-algebra A, together with a nowhere vanishing differential ω on E, an element $f(E, \omega) \in A$, then the Fourier expansion of f is the series $f(E_q \otimes R, dq/q) \in \mathbb{Z}[[q]][1/q] \otimes R$. Thus the coefficients of the expansion are contained in a finitely generated $\mathbb{Z}$-submodule of R. Working over $\mathbb{Z}[[q^{1/n}]][1/q][z]/(z^n - 1)$ one can similarly define the expansions of forms of higher level. But the story of the arithmetic of modular curves and modular forms is very long and all we can do here is to refer the reader to such accounts as [D-R], [K] and [K-M], where it is admirably told.

References

[D-R] Deligne, P. and Rapoport, M., Les schémas de modules de courbes elliptiques, in Modular Functions of One Variable II, Springer Lecture Notes in Math. **349** (1973), 143–316.

[D-G-S] Dwork, B., Gerotto, G. and Sullivan, F.J., An Introduciton to G-functions, Annals of Math. Studies **133**, Princeton U. Press, 1994.

[G-S] Greenberg, R. and Stevens, G., p-adic L-functions and p-adic periods of modular forms, Invent. Math. **111** (1993), 407–447.

[K] Katz, N., p-adic properties of modular schemes and modular forms, in Modular Functions of One Variable III, Springer Lecture Notes in Math. **350** (1973), 69–190.

[K-M] Katz, N. and Mazur, B., Arithmetic Moduli of Elliptic Curves, Annals of Math. Studies **108**, Princeton U. Press, 1985.

[M-T-T] Mazur, B., Tate, J., Teitelbaum, J., On p-adic analogs of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. **84** (1986), 1–48.

[R] Ribet, K. A., On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Invent. Math. **100** (1989), 359–407.

[Ro] Roquette, P., Analytic theory of elliptic functions over local fields, Hamburger Math. Einzelschriften, Neue Folge - Heft 1, Vandenhoeck & Ruprecht, Gottingen.

[S1] Serre, J-P., Abelian l-adic representations and elliptic curves. W. A. Benjamin, 1968.

[S2] Serre, J-P., Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math J. **54** (1987), 179–230.

[S-T] Serre, J-P. and Tate, J., Good Reduction of Abelian Varieties, Annals of Math. **88** (1968), 492–517.

[Si] Silverman, J., Advanced Topics in the Arithmetic of Elliptic Curves, Springer, 1994.