ELLIPTIC CURVES WITH SPLIT MULTIPLICATIVE REDUCTION OVER COMPLETE RINGS*

BY ZENAIDA RAMOS

§0. Introduction and Statement of Results.

Consider the formal series in the variables q, v given by:

$$x(v) = \sum_{n\in Z}\frac{q^n v}{(1-q^n v)^2} - 2h(q) \tag{0.1}$$

$$y(v) = \sum_{n\in Z}\frac{(q^n v)^2}{(1-q^n v)^3} + h(q) \tag{0.2}$$

where

$$h(q) = \sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}$$

They have the following properties (see [4])

i) $x(qv) = x(v) = x(v^{-1})$
ii) $y(qv) = y(v) = -y(v^{-1}) - x(v^{-1})$
iii) They satisfy the equation:

$$y^2 + xy = x^3 - A_4 x - A_6 \tag{0.3}$$

where

$$A_4 = 5\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n};\ A_6 = \sum_{n=1}^{\infty}\frac{7n^5+5n^3}{12}\frac{q^n}{1-q^n}$$

the discriminant is given by

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} \tag{0.4}$$

and the invariant is

$$j = \frac{1}{q} + 744 + 196884\, q + \ldots.. \tag{0.5}$$

In an unpublished work, John Tate shows (by means of the series $x(v)$ and $y(v)$) that if B is a field, complete for some non-archimedean valuation, then for each $q \in B$ with $0 < |q| < 1$, the quotient $B^*/q^{\mathbf{Z}}$ (where $q^{\mathbf{Z}}$ is the infinite cyclic discrete subgroup of the multiplicative group B^* generated by q) is an elliptic curve E_q over B. E_q has minimal Weierstrass equation given by (0.3).

* The results in this note are part of the author's doctoral dissertation written at Harvard under the supervision of Professor John Tate, to whom the author wishes to thank for his inspiration and guidance.

It is characterized, up to B-isomorphism, by the fact that it has the given j-invariant together with the fact that its reduction is of split multiplicative type. The purpose of this work is to prove a similar result in case B is the ring of fractions $A[q^{-1}]$ where A is a UFD, complete for the J-adic topology given by a prime ideal J containing q and under certain conditions of the pair (J, A).

Throughout this paper A will be integrally closed domain, q a non-zero non unit element in A, $J \subset A$ an ideal containing q and such that A is J-adically complete. Let K denote the quotient field of A and let $E_q(B)$ denote the B-rational points on the elliptic curve defined by the homogenous equation

$$y^2z + xyz = x^3 - A_4x^2z - A_6z^3. \tag{0.6}$$

In §1 we define a map

$$\theta_q: A(q^{-1})^* \to E_q(B)$$

and prove that it is a homomorphism.

Definition 1. The pair (q, A) will be said to have the *Covering Map Property* if the following two conditions are satisfied:

i) A is a q-adically complete domain

ii) The map θ_q: $A[q^{-1}]^* \to E_q(B)$ is surjective.

We prove two theorems:

THEOREM A (Main Theorem). *Let A be a Noetherian UFD and let q be a non-zero element contained in a prime ideal $J \subset A$, with A complete for the J-adic topology. Suppose the pair (J, A) satisfies the following conditions:*

a) $2 \in A^*$ *and either every unit in A/J is a square or the associated graded ring*

$$Gr_J(A) = A/J \oplus J/J^2 \oplus \cdots \oplus J_,^n/J_,^{n+1} \oplus \cdots$$

is an integrally closed domain.

b) $3 \in A^*$, *A contains a primitive cubic root of* 1 *and either every unit in A/J is a cube or the associated graded ring $Gr_J(A)$ is an integrally closed domain.*

Then the pair (q, A) satisfies the Covering Map Property.

THEOREM B (Reduction Steps). *Suppose the pair (q, A) satisfies one of the following two conditions:*

a) *The ring A is contained in a ring A_1 with (q, A_1) having the Covering Map Property. Also there is a group G, with every element in it being of finite order, such that G acts on A_1 and*

$$A = A_1{}^G = \{a \in A_1: g(a) = a \ \forall \ g \in G\}.$$

b) *The ring A is the intersection of two rings A_1, A_2; both contained in a q-adically complete domain A_3. Also, the pairs (q, A_i) for i = 1, 2 have the Covering Map Property.*

Then the pair (q, A) satisfies the Covering Map Property.

As an application we have that, if A is a local *UFD*, complete for the topology generated by the maximal ideal J and the field A/J is algebraically closed, then Theorem A shows that for all non-zero $q \in J$, the pair (q, A) has the Covering Map Property.

§1. The Uniformization Map

LEMMA 1.0. *The formal series $x(v)$ and $y(v)$ have their poles in the set $q^{\mathbf{Z}} = \{q^n \colon n \in \mathbf{Z}\}$ which is the set of zeroes of the theta function:*

$$\theta(v) = \textstyle\sum_{n=-\infty}^{\infty} (-1)^n q^{(n^2-n)/2} v^n \tag{1.1}$$

which has a product expansion:

$$\theta(v) = [\textstyle\prod_{n=1}^{\infty} (1 - q^n)](1 - v) \prod_{n=1}^{\infty} (1 - q^n v)(1 - q^n v{-}1) \tag{1.2}$$

Proof. For a proof see [6, Ch. XXI].

LEMMA 1.3. *The functions $\theta^3(v)$, and $\theta^3 y(v)$ satisfy the functional equation $\phi(v) = -v^3\phi(qv)$. Also $\theta^2 x(v)$ satisfies the functional equation $\phi(v) = v^2\phi(qv)$.*

Proof. The series expansion for $\theta(v)$ shows that $\theta(v) = -v\theta(qv)$. The lemma follows from this fact and the properties $x(qv) = x(v)$ and $y(qv) = y(v)$.

We define the map

$$\theta_q \colon A[q^{-1}]^* \to E_q(B)$$

as $v \to$ point of coordinates, $(\theta^3 x(v), \theta^3 y(v), \theta^3(v))$. Given $v \in A[q^{-1}]^*$ there is an integer n s.t. $q^n v$, $q^n v^{-1} \in A$ so that the expressions $1 - q^s v$, $1 - q^s v^{-1}$ are units in A $\forall$ $s > n$. From this it can be shown that the Laurent series defining the functions $\theta^3 x(v)$, $\theta^3 y(v)$, $\theta^3(v)$ converge to an element in $A[q^{-1}]$ whenever $v \in A[q^{-1}]^*$. Also from the product expansion for $\theta(v)$ we see that $\theta^3(v) = 0 \Leftrightarrow v \in q^{\mathbf{Z}}$ and in this case $\theta^3 x(v) = 0$ but $\theta^3 y(v) = \prod_{n=1} (1 - q^n)^9 \in A^*$.

Hence $\theta^3(v)$ and $\theta^3 y(v)$ do not have common zeroes so that the map θ_q is well defined.

PROPOSITION 1.4 *The map θ_q is an homomorphism with Kernel $q^{\mathbf{Z}}$.*

Proof. To show that θ_q is a homomorphism we use classical formulae.

For example, in the case when $0 < |q| < 1$ and $v \in \mathbf{C}^*$ we have the identity

$$\begin{vmatrix} \theta^3 x(u) & \theta^3 y(u) & \theta^3(u) \\ \theta^3 x(v) & \theta^3 y(v) & \theta^3(v) \\ \theta^3 x(u^{-1}v^{-1}) & \theta^3 y(u^{-1}v^{-1}) & \theta^3(u^{-1}v^{-1}) \end{vmatrix} = 0$$

which shows that

$$\theta_q(u) + \theta_q(v) + \theta_q(u^{-1}v^{-1}) = 0,$$

when u, $vA[q^{-1}]^*$ and $\theta_q(u) \neq \theta_q(v)$, and so on.

To find the Kernel of θ_q we observe that the zero of $E_q(B)$ corresponds to the point (0, 1, 0). Then $\theta_q(v) = 0 \Leftrightarrow \theta^3(v) = 0$ and $\theta^3 x(v) = 0 \Leftrightarrow v \in q^{\mathbf{Z}}$.

2. The Image of Proper q-divisors

Let $\sqrt{J}$ denote the radical of the ideal J in A, i.e. the set of $x \in A$ such that $x^n \in J$ for some positive integer n.

Definition: A proper q-divisor in A is an element $v \in \sqrt{J}$ such that $v \neq 0$ and $qv^{-1} \in \sqrt{J}$.

PROPOSITION 2.1 *If v is a proper q-divisor in A, then $\theta_q(v)$ is given by coordinates in $(\sqrt{J}, \sqrt{J}, 1)$. Conversely, every point of that form is the image $\theta_q(v)$ of some proper q-divisor v.*

Proof. The first statement is clear from the expressions for the coordinate theta functions.

To prove the second statement, set $(a, b, 1) \in E_q(B)$ with $a, b \in \sqrt{J}$. If there is a proper q-divisor v with $\theta_q(v) = (a, b, 1)$ then we should have $x(v) = a$, but

$$x(v) = \frac{v}{(1-v)^2} + \sum_{n=1}^{\infty} \frac{q^n v}{(1-q^n v)^2} + \frac{q^n v^{-1}}{(1-q^n v^{-1})^2} - 2h(g)$$

$$= \sum_{n=0}^{\infty} \frac{q^n v}{(1-q^n v)^2} + \frac{q^n (qv^{-1})}{(1-q^n (qv^{-1}))^2} - 2h(g)$$

taking common denominators for the two fractions and putting $w = v + qv^{-1}$, we get formally

$$x(v) = \sum_{n=0}^{\infty} \frac{(q^n + q^{3n+1})w - 4q^{2+1}}{(1 - q^n w + q^{2n+1})^2} - 2h(g)$$

$$= c_0 + c_1 w + c_2 w^2 + \cdots + c_n w^n + \cdots,$$

where

$$c_0 = -2h(q) - 4\sum_{n=0}^{\infty} \frac{q^{2n+1}}{(1-q^{2n+1})^2} \in qA$$

$$c_1 = \sum_{n=0}^{\infty} \frac{q^n - 6q^{3n+1} + q^{5n+1}}{(1-q^{2n+1})^3} \in 1 + qA$$

$$c_2 = \sum_{n=0}^{\infty} \frac{4q^{2n} - 15^{2n+1} + 3q^{6n+1} + 3q^{6n+2} + q^{8n+3}}{(1-q^{2n+1})^4}$$

$$\vdots$$

Since $c_0 \in \sqrt{J}$, $c_1 \in A^*$ and $c_n \in A$ for all n, the equation

$$a = c_0 + c_1 w + c_2 w^2 + \cdots + c_n w^n + \cdots \tag{2.2}$$

has a unique solution $w \in \sqrt{J}$, for each $a \in \sqrt{J}$. (In fact, inverting this series we find w expressed as a power series in $(a - c_0)c_1^{-1}$, and from this we obtain a power series in a:

(2.3) $$w = d_0 + d_1 a + \cdots + d_n a^n + \cdots$$

where the coefficient d_i belongs to A and $d_0 \in qA$. Since $a \in \sqrt{J}$ this series is convergent so that w is well defined in $\sqrt{J}$.)

Now let w be the solution of (2.2) where a is the x-coordinate of our point $P = (a, b, 1) \in E_q(B)$. If there is a $v \in A$ with $v + qv^{-1} = w$, then we are done. Indeed, suppose v and $qv^{-1} = u$ are elements of A such that $uv = q$ and u + v = w. Then first of all, $u, v \in \sqrt{J}$. To see this, recall that $\sqrt{J}$ is the intersection of the ideals of A containing J. Since $q \in J$ it follows from $uv = q$ that for each such prime ideal $\mathscr{P}$ either $u \in \mathscr{P}$ or $v \in \mathscr{P}$. Then from $w \in \mathscr{P}$ and $u + v = w$ we conclude that both u and v are in $\mathscr{P}$. This being true for each $\mathscr{P}$ containing J, we have $u, v \in \sqrt{J}$.

Next, we claim that either $\theta_q(v) = P$ or $\theta_q(u) = P$. Indeed, by our construction of w $\theta_q(v)$ has the same "x-coordinate", $x(v) = a$ as P. Hence $P = \theta_q(v)$ or $P = - \theta_q(v)$. But $- \theta_q(v) = \theta_q(qv^{-1}) = \theta_q(u)$.

To complete the proof of the proposition, we must show that the equation $v + qv^{-1} = w$, i.e.,

$$v^2 - wv + q = 0$$

has a solution $v \in A$. If it did not, then it would not have a solution in K, because A is integrally closed. Suppose therefore that it has no solution $v \in K$, and let $L = K(v)$ be the quadratic extension of K obtained by adjoining a root v. Let $A_L = A[v] = A + Av$ and let $J_L = JA_L = J + Jv$. Then

$$J_L{}^n = (JA_L)^n = J^n + J^n v,$$

from which we conclude that

$$A_L = \varprojlim A_L / J_L{}^n.$$

Hence we can consider the map

$$\theta_q : B_L{}^* \to E_q(K_L)$$

where $B_L = A_L[q^{-1}]$ and K_L is the quotient field of B_L. As above, we have $\theta_q(v) = \pm P \in E_q(B)$.

Case 1. L/K separable. Let $(1, \sigma)$ be the Galois group. Clearly $\sigma A_L = A_L$ and $\sigma J_L = J_L$ so σ commutes with θ_q. Since $\sigma P = P$, we conclude that

$$v^\sigma / v \in \operatorname{Ker} \theta_q = q^{\mathbf{Z}}$$

Say $v^\sigma = q^n v$. Applying σ again gives $q^{2n} v = v$, hence $q^{2n} = 1$. This means $n = 0$, because $q \in J$, so $v^\sigma = v$, and $v \in K$, a contradiction.

Case 2. L/K not separable. Then K is of characteristic 2 and $w = 0$. By (2.2) we have then

$$a = c_0 = -2h(q) - 4 \sum_{n=0}^{\infty} \frac{q^{2n+1}}{(1 - q^{2n+1})^2} = 0$$

and the relation

$$b^2 + ab = a^3 - A_4 a - A_6$$

becomes

$$b^2 = A_6 = \sum_{n=0}^{\infty} \frac{q^{2n+1}}{1-q^{2n+1}} = \sum_{n=1}^{\infty} g_n q^n,$$

say,

$$= q_n \sum_{\text{odd}} g_n q^{n-1} + \sum_{n \text{ even}} g_n q^n,$$
$$= q(\sum_{n \text{ odd}} g_n q^{(n-1)/2})^2 + (\sum_{n \text{ even}} g_n q^{n/2})^2,$$
$$= qc^2 + d^2,$$

with $c, d \in A$ and $c = 1 + \cdots \neq 0$. On the other hand, $v^2 = q$. So $b^2 = v^2c^2 + d^2$ and hence $v = (b + d)/c \in K$, a contradiction. This concludes the proof of the Proposition.

3. The Isogeny

By abuse of notation E_q will stand for the defining equation

$$zy^2 + xyz = x^3 - A_4xz^2 - A_6z^3$$

corresponding to the parameter q.

Define the map

$$\phi\colon E_{q^2}(B) \to E_q(B)$$

as follows: Take Q to be the point on $E_{q^2}(B)$ of order 2 given by $\theta_{q^2}(q)$; its coordinates are $(2e_q, -e_q, 1)$ where $e_q = h(q) - 2h(q^2)$ [($h(q)$ as defined on Introduction)]. Put

$$\phi(0) = \phi(Q) = 0.$$

For any other point P: $(x_2, y_2, 1)$ in $E_{q^2}(B)$ we set

$$\phi(x_2, y_2, 1) = (x_1, y_2, 1)$$

with

$$x_1 + 4e_q = \lambda^2 + \lambda$$

where

$$\lambda = \frac{y_2 + e_q}{x_2 - 2e_q}$$

is the slope of the line PQ. Put

$$y_1 = y_2 + (1 + \lambda)(x_2 - x_1).$$

We can check directly that $(x_1, y_1, 1)$ satisfies the equation E_q. Clearly, ϕ is an isogeny from E_{q^2} to E_q with kernel $\{0, Q\}$.

PROPOSITION 3.1. *The map ϕ has the following properties:*

i) $\phi \circ \theta_{q^2} = \theta_q$.

ii) A point $(x_1, y_1, 1) \in E_q(B)$ is in the image of $\phi \Leftrightarrow x_1$ is of the form $\lambda^2 + \lambda - 4e_q$ for some $\lambda \in K$.

Proof. (i) follows from the identities

$$x_q(v) = x_{q^2}(v) + x_{q^2}(qv) - 2e_q$$

$$y_q(v) = y_{q^2}(v) + y_{q^2}(qv) + e_q .$$

Proof of (ii). Set $(x_1, t_1, 1) \in E_q(K)$ with $x_1 = \lambda^2 + \lambda - 4e_q$ for some $\lambda \in K$. We can solve the system of equations

$$y_2 + e_q = \lambda(x_2 - 2e_q)$$

$$y_2 = y_1 + (1 + \lambda)(x_2 - x_1)$$

for x_2, y_2. Then

$$x_2 = x_1 + e_q + \frac{y_1 - \lambda x_1}{1 + 2\lambda}$$

and from this

$$y_2 = \lambda x_2 - (1 + 2\lambda) e_q .$$

To prove that $(x_2, y_2, 1) \in E_{q^2}(K)$, put $L = K(y)$ where y is a root of the equation

$$y^2 + x_2 y = x_2^3 - A_4(q^2) x_2 - A_6(q^2).$$

Then, $(x_2, y, 1) = (x_1, y_1, 1)$, so that

$$x_1 = u^2 + u - 4e_q$$

where

$$u = \frac{y + e_q}{x_2 - 2e_q}.$$

Thus either $\lambda = u$ or $u = -(1 + \lambda)$. If $\lambda = u$, then $y = y_2$. If $u = -(1 + \lambda)$ then $y = -x_2 - y_2$. In any case $(x_2, y_2, 1) \in E_{q^2}(K)$. This ends the proof.

Comment. Suppose A is a *UFD*. Then if $(x_1, y_1, 1) \in E_q(K)$ there exist L, M, $N \in A$ with $(L, M) = 1$. (This symbol means L and M do not have a common prime divisor), $(N, M) = 1$ and such that

$$x_1 = L/M^2, \qquad y_1 = N/M^3.$$

This is called a canonical expression for $(x_1, y_1, 1)$.

PROPOSITION 3.2. *Suppose A is a UFD. Let* $(x_1, y_1, 1)$ $E_q(K)$ *with*

$$\phi^{-1}(x_1, y_1, 1) = \{(x_2, y_2, 1), (x_2', y_2', 1)\}.$$

a) If $L/M^2 = x_1$ *is a canonical expression, then* x_2 *and* x_2' *can be written canonically as*

$$x_2 = U/V^2, \qquad x_2' = U'/V'^2$$

with $VV' = M$ *and* $(V, V') = 1$.

b) Suppose $\sqrt{J}$ *is a prime ideal. Then at least one of the numerators U and U' belongs to* $\sqrt{J}$.

Proof. The defining equations for ϕ show that

$$(x_2 - 2e_q) + (x_2' - 2e_q) = x_1 - 2e_q \tag{3.3}$$

$$(x_2 - 2e_q)(x_2' - 2e_q) = e_q + 12e_{q^2} - A_4(q^2). \tag{3.4}$$

Put

$$x_2 = U/V^2 \quad \text{and} \quad x_2' = U'/V'^2$$

with $(U, V) = U', V') = 1$. Then (3.4) shows that V and V' cannot have a common prime divisor. Then $VV' = M$ follows from (3.3). This is assertion (a). Now, equation (3.4) shows that

$$UU' \in qA \subset J \in \sqrt{J}.$$

Hence at least one of U, U' belongs to $\sqrt{J}$.

THEOREM 3.5. *Assume A is a UFD with* $2 \in A^*$ *and such that either*
a) The associated graded ring

$$Gr_J(A) = A/J \oplus J/J^2 \oplus \cdots \oplus J^n/J^{n+1} \oplus \cdots$$

is an integrally closed integral domain, or
b) Every unit in A/J is a square. Then the map

$$\phi: E_{q^2}(K) \to E_q(K)$$

is surjective.

Proof. By Proposition 3.1 it will be enough to prove that if $(x_1, y_1, 1) \in E_q(K)$ then $x_1 + 4e_q$ is of the form $\lambda^2 + \lambda$; i.e. $x_1 + \frac{1}{4} + 4e_q$ should be a square; noticing that $\frac{1}{4} + 4e_q = -x_q(-1)$ we apply the transformation

$$\bar{y} = y_1 + \tfrac{1}{2}x_1$$

$$\bar{x} = x_1 - x_q(-1)$$

to the equation and get

$$y^2 = -x^3 - 2a_2\bar{x}^2 + (a_2^2 - 4a_4)\bar{x} \tag{3.6}$$

where

$$a_2 = \tfrac{1}{4} + 6e_q \tag{3.7}$$

$$a_4 = 3e_{q^2} + [A_4(q) - e_q]/4 \tag{3.8}$$

Note that $a_2 \in A^*$, and $a_4 \in qA \subset J$.

Now we just need to show that if $(\bar{x}, \bar{y}, 1)$ is a solution to (3.6) then $\bar{x}$ is a square. Writing

$$\bar{x} = U/V^2, \qquad \bar{y} = W/V^3$$

in (3.6).

Take a prime p in A dividing U, then a $p^{2m} \mid W^2$ for some integer m; if $p^{2m} \nmid U$ then $p \mid (a_2^2 - 4a_4) V^4$ but $(p, V) = 1$ and $a_2^2 - 4a_4 \in A^*$, is not possible, so $U = c^2 b$ with $c \in A^*$, $b \in A$. Now $\bar{x}$ is a square if c is a square. This is true in case (b) by Hensel's lemma.

In case (a) set $d = Wb^{-1} \in A$. Then $c^{-1}d^{-2} = (U - a_2V^2)^2 - 4a_4V^4$.

Digression. If $a \in A = \mathrm{Lim}_{\leftarrow} A/J^n$, and $a \neq 0$, we say deg $a = r$ if $a \notin J^r$ and $a \notin J^{r+1}$; the image $\bar{a} \in J^r/J^{r+1}$ is called the leading form of a. We put deg 0 $= \infty$ and $\bar{0} = 0$. Then deg (ab) = deg a + deg b (because $Gr_J(A)$ is an integral domain). We have $a = 0 \Leftrightarrow \bar{a} = 0$.

Now to prove that c or c^{-1} is a square, we consider two cases:

i) deg $(U - a_2V^2)^2 <$ deg $4a_4V^4$.
ii) deg $(U - a_2V^2)^2 \geq$ deg $4a_4V^4$.

In the first case:

$$\begin{aligned} &\text{leading form of } (U - a_2V^2)^2 - 4a_4V_4 \\ &= \text{leading form of } (U - a_2V^2)^2 \\ &= [\text{Leading form of } (U - a_2V^2)]^2 \\ &= f_r^2, \text{ say.} \end{aligned}$$

Then, leading form of $c^{-1}d^2 = f_r^2$, i.e. $c_0 d_r^2 = f_r^2$

where

$$\begin{aligned} c_0 &= \text{leading form of } c^{-1} \in A^*/J \\ d_r &= \text{leading form of } d. \end{aligned}$$

Hence

$$c_0 = (f_r/d_r)^2$$

is a square in the quotient field of $Gr_J(A)$; but $Gr_J(A)$ is integrally closed. Hence $c_0 \in (A^*/J)^2$ and as 2 is invertible in A, Hensel's lemma shows that $c^{-1} \in (A^*)^2$. So $U = \mu\alpha^2 \in A^2$ and x is a square.

Case (ii) is proved in a similar way.

We can prove now part (a) of Theorem A. Let $P = (x_1, y_1, 1) \in E_q(K)$. By Theorem 3.5 the map

$$\phi : E_{q^2}(K) \to E_q(K)$$

is surjective. Let

$$\phi^{-1}(P) = \{P_1, P_2\}.$$

If $x_1 = L/M^2$, $y_1 = N/M^3$ is a canonical expression, we say M is the denominator associated to the point P. Let V_i be the denominator associated to P_i. By part (a) of Proposition 3.2 we know that $(V_1, V_2) = 1$ and $V_1 V_2 = M$. Suppose V_1 is the one with the smaller set of primes in it (this set can be empty if $V_1 \in A^*$). Then $V_1 \mid M$ and set of primes in V_1 is contained in, but not equal to the set of primes in M.

Put $Q = P_1$. Now using the surjectivity of the map

$$\phi : E_{q^4}(K) \to E_{q^2}(K)$$

and repeating the process we find a point $Q_2 \in E_{q^4}(K)$ with $\phi(Q_2) = Q_1$ and with denominator of $Q_2 \mid$ denominator of Q_1. Repeating this process several times we arrive at a point $Q_n \in A^*$, i.e., $Q_n = (a, b, 1)$ with $a, b \in A$. Let

$$\phi^{-1}(Q_n) = \{R_1, R_2\} \subset E_{q^{2^{n+1}}}(K).$$

Then, R_i is of the form $(a_i, b_i, 1)$ with $a_i, b_i \in A$. Now, part (b) of Proposition 3.2 shows that one of a_1, a_2 belongs to $\sqrt{J}$; let us say $a_1 \in \sqrt{J}$. Then the equation

$$b_1^2 + a_1 b_1 = a_1^3 - A_4(q^{2^{n+1}})a_1 - A_6(q^{2^{n+1}})$$

shows $b_1 \in \sqrt{J}$. Proposition 2.1 shows that there is a $v_0 \in A[q^{-1}]^*$ with

$$\theta_{q^{2^{n+1}}}(v_0) = (a_1, b_1, 1).$$

As each diagram

$$\begin{array}{ccc} E_{q^{2(k+1)}}(K) & \longrightarrow & E_{q^2}(K) \\ & {\scriptstyle \theta_{q^{2^{k+1}}}} \searrow \quad \swarrow {\scriptstyle \theta_{q^{2^k}}} & \\ & A[q^{-1}]^* & \end{array}$$

is commutative, we have $\theta_q(v_0) = P$ and the theorem is proved in case (a).

Part (b) can be proved by means of the isogeny $E_{q^2}(K) \to E_q(K)$ and proving similar results.

§4. Proof of Theorem B

In any case, A is q-adically complete

Case (a). Let K_1 denote the quotient field of A_1. Let $P \in E_q(K) \subset E_q(K_1)$. Then, as (q, A_1) has the Covering Map Property, there is a $v \in A_1[q^{-1}]^*$ such that $\theta_q(v) + P$. Choose $\sigma \in G$. Then $[\theta_q(v)]^\sigma = P^\sigma$, i.e. $\theta_q(v^\sigma) = P^\sigma = P$ so that $v^\sigma/v \in \operatorname{Ker} \theta_q$. Hence there is an integer n such that $v^\sigma = q^n v$. Suppose $s =$ order of σ. Then

$$v = v^{\sigma^s} = q^n v^{\sigma^{s-1}} = q^{n^2} v^{\sigma^{s-2}} = q^{n^s} v, \qquad \text{i.e. } q^{n^s} = 1.$$

If $s \neq 0 (\sigma \neq 1)$ then $n = 0$, which shows that $v^\sigma = v$ $v \in G$. Hence $v \in (A_1 [q^{-1}]^*)^G$ and (q, A) has the Covering Map Property.

Case (b). Let K_i denote the quotient field of A_i for $i = 1, 2, 3$. Let $P \in E_q(K) \subset E_q(K_i)$. As (q, A_i) satisfies the Covering Map Property for $i = 1, 2$ there are units

$$v_i \in A_i[q^{-1}]^*, \qquad (i = 1, 2)$$

such that $\theta_q(v_i) = P$. As $v_1, v_2 \in A_3[q^{-1}]^*$ and as

$$\theta_q : A_3[q^{-1}]^* \to E_q(K_3)$$

has kernel $q^{\mathbf{Z}}$, then $v_1 = q^n v_2$ for some integer n. Hence we can take

$$v_1 = v_2 \in A_1[q^{-1}]_* \cap A_2[q^{-1}]_* \subset A_3[q^{-1}]_* .$$

Multiplying by a power of q, we take $v_1 \in A_1 \cap A_2$. Hence $v_1 \in A[q^{-1}]^*$. This shows that (q, A) has the Covering Map Property.

A final comment. The following counter example given by Mumford shows that when A is just integrally closed, (q, A) does not always have the Covering Map Property.

Let k be a field of characteristic $\neq 2$, and $A = K[[u, v, w]]$ where u, v, w satisfy

$$w^2 = u[u^2 - 2a_2 uv^2 + (a_2^2 - 4a_4)] v^4$$

where a_2, a_4 are as in (3.7) and (3.8). Then $(u/v^2, w/v^3, 1)$ corresponds to a point $P(x_1, y_1, 1) \in E_q(K)$ and as u/v^2 is not a square. Hence $P \notin \operatorname{Im} \theta_q$.

INSTITUTO DE MATEMATICAS
UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

REFERENCES

[1] L. EULER, Opera Omnia (1) XX, Leipzig, 1912.
[2] D. MUMFORD, *An analytic construction of degenerating curves over complete local rings*, Compositio Math. **24** (1972), 129–174.
[3] ———, *An analytic construction of degenerating abelian varieties over complete rings.* Compositio Math. **24** (1972), 239–272.
[4] P. ROQUETTE, *Analytic theory of elliptic functions over local fields*, Hamb. Math. Einzelschriften Neue Folge, Heft 1, Göttingen, 1970.
[5] J. T. TATE, *The arithmetic of elliptic curves*, Invent. Math., **23** (1974), 179–206.
[6] E. T. WHITTAKER AND G. N. WATSON, A Course of Modern Analysis, Cambridge Univ. Press, 1943.