COMPOSITIO MATHEMATICA

MICHAEL HARRIS

Kubert-lang units and elliptic curves without complex multiplication

Compositio Mathematica, tome 41, nº 1 (1980), p. 127-136

<http://www.numdam.org/item?id=CM_1980__41_1_127_0>

COMPOSITIO MATHEMATICA, Vol. 41, Fasc. 1, 1980, pag. 127–136

KUBERT-LANG UNITS AND ELLIPTIC CURVES WITHOUT COMPLEX MULTIPLICATION

Michael Harris*

Introduction

In the series of papers [5], Kubert and Lang have described the groups of units in the fields of modular functions of all levels, and have determined the ranks of these groups in general. Various authors, including Ramachandra [8] and Robert [9], have considered the specializations of these units at elliptic curves with complex multiplication; by application of Kronecker's Second Limit Formula, they have proved deep results about the multiplicative independence of these specializations. More recently, Kubert and Lang have proved that specialization to an elliptic curve with non-integral j-invariant introduces no additional relations, under some mild additional hypotheses; their proof in this case, as in the generic case, depends on the q-expansions of the modular units at the various cusps.

In this note I obtain asymptotic lower bounds for the ranks of the groups of specialized Kubert-Lang units of level p^n, when the elliptic curve involved is defined over a number field K, and is such that its p^n-division points generate a $GL(2, Z/p^nZ)$- extension of K, for all n. These bounds are derived from the p-adic representation theory of $GL(2, Z_p)$, and use no other information than the generic independence results of Kubert-Lang, and the distribution relations of Robert and Kubert-Lang. Consequently, they are not nearly so deep, nor so sharp, as the bounds obtained by the analytic methods of the previous authors; however, they apply to every elliptic curve without complex multiplication over a number field, for almost all primes p.

In the last section, I show how the p-adic L-functions studied by

* Research partially supported by NSF Grant MCS77-04951

0010-437X/80/04/0127-10$00.20/0

Katz can be used to improve the estimates derived from representation theory in the general case.

I wish to thank D. Goss, S. Lang, B. Mazur, and A. Wiles for helpful discussions.

1. Verma Modules

Let p be an odd prime number. If H is a p-adic group and X is a topological space, we let $C(H, X)$ be the space of continuous X-valued functions on H, and let $C^\infty(H, X) \subset C(H, X)$ be the space of *locally constant* X-valued functions on H.

Let $G = \mathrm{GL}(2, \mathbf{Z}_p)$, $B =$ upper triangular Borel subgroup of G, $B^1 =$ the group of matrices of the form $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ $b \in \mathbf{Z}_p$, $d \in \mathbf{Z}_p^\times$, $Z =$ the center of G, and C a "Cartan subgroup" as in Kubert-Lang [5, II]: i.e., the intersection with G of the image of any embedding in the algebra of two-by-two matrices over $\mathbf{Q}_p$ of the multiplicative group of the unramified quadratic extension of $\mathbf{Q}_p$. Let $G_n = \mathrm{Ker}(G \to \mathrm{GL}(2, \mathbf{Z}/p^{n+1}\mathbf{Z}))$, for $n = 0, 1, 2, \ldots$; let H_n, where $H = B$, B^1, C, etc. be $H \cap G_n$. For each such H, let Λ_H be the *Iwasawa algebra* of H: $\Lambda_H = \varprojlim_n \mathbf{Z}_p[H/H_n]$.

Define the *Verma module* $M = \Lambda_G \otimes_{\Lambda_{B^1}} \mathbf{Z}_p$, where B^1 acts trivially on $\mathbf{Z}_p$. The *Pontryagin dual* of M is then $M^* = \{f \in C^\infty(G, \mathbf{Q}_p/\mathbf{Z}_p) \mid f(bg) = f(g),\ b \in B^1,\ g \in G\}$; the contragredient of M is $M^t = \{f \in C(G, \mathbf{Z}_p) \mid f(bg) = f(g),\ b \in B^1,\ g \in G\}$; we let $M' = M^t \cap C^\infty(G, \mathbf{Z}_p)$. Each of these groups is naturally a left module for Λ_G.

Let X be a finitely generated Λ_{C_0}-module. The *rank* of X is the dimension over the fraction field $\mathcal{K}$ of Λ_{C_0} of $\mathcal{K} \otimes_{\Lambda_{C_0}} X$. (That $\mathcal{K}$ exists follows from the non-canonical isomorphism $\Lambda_{C_0} \simeq \mathbf{Z}_p[[T_1, T_2]]$ – cf. [5, V].)

Let $I_{H_n} \subset \Lambda_H$, for any subgroup H of G, be the kernel of the natural map $\Lambda_H \to \mathbf{Z}_p[H/H_n]$.

LEMMA 1: *If X is a Λ_{C_0}-module of rank r, then* $\dim_{\mathbf{Q}_p} \mathbf{Q}_p \otimes_{\mathbf{Z}_p} X/I_{C_n}X - rp^{2n} = 0(p^n)$ *as a function of n.*

PROOF: The analogous theorem may be proved for any p-analytic group, in the sense of [1], by the techniques described there; the proof is essentially contained in the proof of Lemma 3.4.1 of [1].

Let χ be a character of $(\mathbf{Z}/p\mathbf{Z})^\times$, and, for any Λ_G-module X, let X^χ be the Λ_G-submodule on which $(\mathbf{Z}/p\mathbf{Z})^\times \subset Z$ acts via the character χ. Since $(\mathbf{Z}/p\mathbf{Z})^\times$ is of order prime to p, the functor $X \to X^\chi$ is exact, and $X \simeq \bigoplus_\chi X^\chi$.

PROPOSITION 1: *Let N be a non-zero Λ_G-submodule of M^χ, for any χ. Then N is of rank $p+1$ over Λ_{C_0}.*

PROOF: We first assume that the image PN of N in $PM^\chi \overset{\text{def}}{=} M^\chi/\Lambda_G I_{Z_0} M^\chi$ is non-trivial; recall that Z_0 is the subgroup of the center of G consisting of diagonal matrices congruent to the identity (mod p). The argument of [2, Proposition 1.6] shows immediately that PN is of rank $p+1$ over PC_0, where $PC_0 = C_0/Z_0$. In particular, PM^χ/PN, which is isomorphic to $(M^\chi/N)/\Lambda_G I_{Z_0}\ (M^\chi/N)$, is a torsion Λ_{PC_0}-module, which implies that M^χ/N is a torsion Λ_{C_0}-module; i.e., that N has rank $p+1$ over Λ_{C_0}.

Now assume N is contained in the kernel of the map $M^\chi \to PM^\chi$. If γ is a topological generator of Z_0, this kernel is equal to $(\gamma-1)M^\chi$. Let k be the smallest integer such that N is not contained in $(\gamma-1)^{k+1}M^\chi$. Since $(\gamma-1)\colon M^\chi \to M^\chi$ is an injection and a Λ_G-map, it makes sense to define $N' = (\gamma-1)^{-k}N \subset M^\chi$; N' is then Λ_G-isomorphic to N. The argument above may now be applied to N'; it follows that N', hence N, is of rank $p+1$ over Λ_{C_0}.

Let $M_n = M/I_{G_n}M$. The decomposition of Kubert-Lang: $G = CB^1$; $G_nB^1 = C_nB^1$ ([5, II]) implies that the maps

$$v_{n,m} : M_n \to M_m \qquad m \geq n$$

$$x(\mathrm{mod}\ I_{G_n}M) \mapsto \sum_{y \in C_m/C_n} yx(\mathrm{mod}\ I_{G_m}M);\ x \in M$$

are well-defined Λ_G-morphisms; further, it implies that M is a free rank-one Λ_C-module. Denote by $\check{M}$ the module $\varprojlim_{v_{n,m}} M_n$. Then

PROPOSITION 2: *As Λ_G-modules, $\check{M}$ is isomorphic to M'.*

PROOF: This is a special case of the proposition in the appendix to [2].

PROPOSITION 3: *Let X be a $\mathbf{Z}_p$-free Λ_G-quotient of $\check{M}$. Then, if $X^\chi \neq 0$, for some character χ of $(\mathbf{Z}/p\mathbf{Z})^\times$, we have*

$$\dim_{\mathbf{Q}_p} \mathbf{Q}_p \otimes_{\mathbf{Z}_p} (X^\chi)^{G_n} - (p+1)p^{2n} = O(p^n)$$

as a function of n.

PROOF: Let $X = M/Y$, for some submodule Y of M. Consider the following diagram:

$$\begin{array}{ccccc} (Y^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)^{G_n} & \to & (Y^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p)^{G_n} & & \\ \downarrow & & \downarrow & & \\ (M^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)^{G_n} & \to & (M^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p)^{G_n} & \to & 0 \\ \downarrow & & \downarrow & & \\ (X^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)^{G_n} & \to & (X^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p)^{G_n} & & \end{array} \tag{1}$$

The columns are evidently exact; that the middle row is exact follows directly from Proposition 2 and the definition of M' as a function space. Let * denote Pontryagin dual. Proposition 2 implies that $(M \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p)^*$ is isomorphic to M^χ. Assume $X^\chi \neq 0$; by freeness, $X^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p \neq 0$. Thus $(X^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p)^* \stackrel{\text{def}}{=} \tilde{X}^\chi$ is a non-zero Λ_G-submodule of M. It now follows from Proposition 1 that $\tilde{X}^\chi$ is a rank $p+1$ Λ_{C_0}-module, and that $\tilde{Y}^\chi \stackrel{\text{def}}{=} (Y^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p)^*$ is a rank zero Λ_{C_0}-module; i.e., a torsion Λ_{C_0}-module. From Lemma 1 and duality it follows that $\dim_{\mathbf{Q}_p}(Y^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)^{G_n} \leq \dim_{\mathbf{Q}_p} (\tilde{Y}^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)^{C_n} = O(p^n)$, whereas $\dim_{\mathbf{Q}_p}(X^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)^{G_n} \leq \dim_{\mathbf{Q}_p}(X^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)^{C_n} = (p+1)p^{2n} + O(p^n)$; moreover, $\dim_{\mathbf{Q}_p}(M^\chi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)^{G_n} = (p+1)p^{2n}$. Combining these observations with diagram (1) yields the proposition.

2. Kubert-Lang Units

Let E be an elliptic curve over the number field K, and let p be a prime number. If $E[p^n]$ is the subgroup of p^n-division points in E, let $K_n = K(E[p^{n+1}])$, $n = 0, 1, 2, \ldots$; let $L = \bigcup_n K_n$. We assume E has no complex multiplication. Then $\mathrm{Gal}(L/K)$ is, by a theorem of Serre ([10]), isomorphic to an open subgroup of $G = \mathrm{GL}(2, \mathbf{Z}_p)$; the imbedding is given by the action of $\mathrm{Gal}(L/K)$ on the Tate module $T_p(E) = \varprojlim_n E[p^n]$. Henceforward we assume $\mathrm{Gal}(L/K)$ is isomorphic to $GL(2, \mathbf{Z}_p)$. Let S denote the set of places of L consisting of (a) all archimedean places; (b) all places dividing p; and (c) all places at which the j-invariant of E is not an integer. For any subfield $L' \subset L$, we let S also denote the set of restrictions of places in S to L'.

Let $\mathscr{E}$ be the group of S-units of L; i.e., the direct limit of the

groups $\mathscr{E}_n$ of S-units of the integer rings of K_n. Then $\mathscr{E} \supset \boldsymbol{\mu}$, the group of p^nth roots of unity for all n. Let $\mathscr{E}' = \mathscr{E}/\boldsymbol{\mu}'$, where $\boldsymbol{\mu}'$ is the group of of roots of unity in $\mathscr{E}$.

LEMMA 2: *The group $\mathscr{E}'$ is a free abelian group.*

PROOF: By Lemma 3.4.2.1 of [2], it is enough to show that $(\mathscr{E}')^{G_n}$ is free and finitely generated over Z for all n. We have an exact cohomology sequence

$$\mathscr{E}_n = \mathscr{E}^{G_n} \to (\mathscr{E}')^{G_n} \to H^1(G_n, \mu').$$

It is enough to show that $H^1(G_n, \boldsymbol{\mu}')$ is finite for each n.

Now $\boldsymbol{\mu}$ is of finite index in $\boldsymbol{\mu}$, since the maximal abelian extension of $\mathbf{Q}$ in L is finite over the field obtained by adjoining $\boldsymbol{\mu}$ to $\mathbf{Q}$. Thus we may as well show that $H^1(G_n, \boldsymbol{\mu})$ is finite for all n. But G_n acts on $\boldsymbol{\mu}$ via the determinant character: $g(\zeta) = \zeta^{\det g}$, $g \in G_n$, $\zeta \in \boldsymbol{\mu}$. By the Hochschild-Serre spectral sequence, it is enough to show that $H^1(Z_n, \boldsymbol{\mu})$ and $H^0(Z_n, \boldsymbol{\mu})$ are finite; since Z_n acts non-trivially on $\boldsymbol{\mu}$, this is clear.

We now introduce the Kubert-Lang units. Let $g^N_{r,s,N}$ be the modular function denoted $g_{r,s}$ in [5, II], i.e., the one with q-expansion at infinity

$$\zeta^{6rs} q^{N+6r^2/N-6r}(1-\zeta^s q^{r/N})^{12N} \prod_{n=1} [(1-\zeta^s q^{n+r/N})(1-\zeta^s q^{n-r/N})]^{12N};$$

here $\zeta = e^{2\pi i/N}$. Then $g^N_{r,s,N}$ is a modular function of level N, for every pair of integers (r, s), depending only on the residue classes of r and s modulo N. In particular, when $N = p^{n+1}$, a choice of basis for the Tate module $T_p(E)$ allows us to specialize $g^N_{r,s,N}$ at E and obtain an S-unit in the field K_n.

However, $g^N_{r,s,N}$ is the Nth power of the function denoted $\mathfrak{f}^{12}_{r,s}\Delta$ in [5, II]; we call this function $g_{r,s,N}$, and remark that it is modular of level N^2, as shown in [5, II]. In particular, it too specializes at E to give rise to an S-unit in L, when $N = p^{n+1}$; furthermore, its image in $\mathscr{E}'$ is evidently in $(\mathscr{E}')^{G_n}$. Finally, when $(r, s) = (1, 0)$, $g_{r,s,N}$ is invariant under the group B^1 (in the convention of [5 II], $g_{r,s,N}$ is invariant under the group $\begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix}$, which is conjugate to B^1 by an outer automorphism).

Let U_n be the subgroup of the multiplicative group of the modular function field (of level p^{2n+2}) generated by the Siegel functions $g_{r,s,p^{n+1}}$, modulo its subgroup of roots of unity. Let M_n be as in §1, and let M_n^+

be the submodule of M_n fixed by $\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \in Z$. Since U_n is generated over Λ_G by $g_{1,0,p^{n+1}}$, by [5, II], it follows from the independence results of Kubert and Lang (cf. [5, II] and also [5, V]) that, as a Λ_G-module,

$$U_n \otimes_{\mathbf{Z}} \mathbf{Z}_p \simeq M_n^+.$$

Now the *distribution relations* of Robert and Kubert-Lang ([5, III], Theorem 3.1) immediately imply

LEMMA 3: *Under the isomorphism described above, the following diagram is commutative*:

$$\begin{array}{ccc} U_n \otimes_{\mathbf{Z}} \mathbf{Z}_p & \xrightarrow{\sim} & M_n^+ \\ \downarrow & & \downarrow v_{n,m}^+ \qquad m \geq n \\ U_m \otimes_{\mathbf{Z}} \mathbf{Z}_p & \xrightarrow{\sim} & M_m^+ \end{array}$$

Here the inclusion on the left is provided by the distribution relations, and $v_{n,m}^+$ is the restriction of $v_{n,m}$ to M_n^+.

COROLLARY: *If* $U = \cup_n U_n \otimes_{\mathbf{Z}} \mathbf{Z}_p$ (the union being taken in the modular function field), then U is isomorphic to $\check{M}^+ = \varinjlim_{v_{n,m}^+} M_n^+$ as a Λ_G-module.

THEOREM 1: *Let* $(K - L)$ *be the subgroup of* $\mathscr{E}$ *generated by specializations of* $g_{r,s,p^{n+1}}$ *at the elliptic curve* E, *for all integers* r, s, n. *Let* $(K\text{–}L)_n = (K\text{–}L) \cap \mathscr{E}_n$; *let* d_n *be the rank of* $(K\text{–}L)_n$ *as a* $\mathbf{Z}$*-module. Then*

$$d_n - \lambda(p+1)p^{2n} = O(p^n),$$

where λ *is the number of characters* χ *of* $(\mathbf{Z}/p\mathbf{Z})^\times \subset Z$ *such that* $((K - L) \otimes_{\mathbf{Z}} \mathbf{Q}_p)^\chi \neq 0$.

PROOF: By Lemma 2, the image $(K\text{–}L)'$ of $(K\text{–}L)$ in $\mathscr{E}'$ is a free abelian group. Thus, by the corollary to Lemma 3, $(K\text{–}L)' \otimes_{\mathbf{Z}} \mathbf{Z}_p$ is a free quotient of $\check{M}^+$. It follows from Proposition 3 that

$$\dim_{\mathbf{Q}_p}((K\text{–}L)' \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)^{G_n} - \lambda(p+1)p^{2n} = O(p^n).$$

We will be done once we show that $(K\text{–}L)'^{G_n}$ and $(K\text{–}L)_n$ have the

same **Z**-rank. But this follows immediately from the finiteness of $H^1(G_n, \mu)$ proved in the course of the proof of Lemma 2.

REMARK: As noted on page 263 of [6], the Siegel functions generate the modular function field. Thus the field generated over K by the elements of $(K-L)$ is of index two in L, and in particular is not contained in any cyclotomic extension of K. It follows that $(K-L)$ contains elements of infinite order; i.e., that $\lambda > 0$.

3. An application of p-adic L-functions

We retain the notation of §2, and assume further that E has *good ordinary reduction* at some place v of K dividing p; we extend v to a place of K_∞, also denoted v. Without loss of generality, we may assume that the decomposition group D_v of v is contained in B; it has finite index in B by [11], A.2.4. Let $\{v'\}$ be the (finite) set of places of K_∞ dividing v and such that $D_{v'} \subset B$; let $F_\infty = \prod_{\{v'\}} K_{\infty,v'}$. Then B acts on F, and we may think of B as the "Galois group" of F_∞/K_v. Let F_n be the subalgebra of F fixed by B_n; it is the product of completions of K_n at the finite set of primes $\{v_n\}$, which consists of the set of restrictions of elements of $\{v'\}$ to K_n. We write $F_n = \prod_{\{v_n\}} K_{n,v_n}$.

Now we may consider the specializations of the Kubert-Lang units $g_{0,s,p^{n+1}}^{p^{n+1}}$, $s \in \mathbf{Z}$, as elements of the algebra F_n. Let $\mathcal{O}_n \subset F_n$ be the product of the integer rings $\mathcal{O}_{v_n}$ of K_{n,v_n}; let $\mathcal{P}_n$ be the product of the maximal ideals $\mathcal{P}_{v_n}$ of $\mathcal{P}_{v_n}$. If $\zeta = e^{2\pi i/p^{n+1}}$, then $g_{0,s,p^{n+1}}^{p^{n+1}}$ is the modular function denoted H_{ζ^s} by Katz in [4], and specializes to an element $h(\zeta^s)$ of F_n. As remarked by Katz ([4], 10.1.5), $(h(\zeta^s)/h(\zeta^{s'}))^{p-1} \equiv 1 \pmod{\mathcal{P}_n}$, if s and s' are two integers relatively prime to p; we may thus define the p-adic logarithm

$$\log_p(h(\zeta^s)/h(\zeta^{s'})) \overset{\text{def.}}{=} \frac{1}{p-1}\log_p((h(\zeta^s)/h(\zeta^{s'}))^{p-1});$$

the $\log_p$ on the right-hand side is defined by the usual convergent power series.

Now $Z \subset B$ acts on the set of $h(\zeta^s)$: if we write $z(a)$ for the diagonal matrix $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, then

$$z(a)h(\zeta^s) = h(\zeta^{as}).$$

Let $(\widetilde{K-L})$ be the subgroup of $(K-L)$ consisting of elements which

have absolute value one at the places v'; we note that $(K-L)/(\widetilde{K-L})$ is a free $\mathbf{Z}$-module of finite rank. By the above remarks, we see that $h(\zeta^s)/h(\zeta^{s'}) \in (\widetilde{K-L}) \cap (K-L)_n$ for any integers s, s' relatively prime to p. Now the map from $(K-L)$ to F_∞ extends to a homomorphism $\varphi : (\widetilde{K-L}) \otimes_{\mathbf{Z}} \mathbf{Z}_p \to F_\infty^\times$, whose image is contained in the subgroup of elements of absolute value one. Our object in this paragraph is to determine conditions under which the image of $((\widetilde{K-L}) \otimes_{\mathbf{Z}} \mathbf{Z}_p)^\chi$ in $F_\infty^\times$ is non-trivial, for a given character χ of $\Delta \overset{\text{def.}}{=} (\mathbf{Z}/p\mathbf{Z})^\times \subset Z$. When this image is non-trivial, $((K-L) \otimes_{\mathbf{Z}} \mathbf{Z}_p)^\chi$ is *a fortiori* non-trivial, and the conclusion of Theorem 1 can be strengthened.

Let $\tilde{\chi}$ be a character of Z of exact conductor p^{n+1}; i.e., a homomorphism $\tilde{\chi} : Z \to \mathbf{Q}_p(\boldsymbol{\mu}_{p^n})^\times$ whose kernel is Z_n. Let $\chi = \tilde{\chi} \mid \Delta$; we call χ the *tame* part of $\tilde{\chi}$. I claim that, if, for some non-trivial $\tilde{\chi}$ with tame part χ, we have

$$h(\tilde{\chi}) = \sum_{a \in (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times} \tilde{\chi}^{-1}(z(a)) \log_p(h(\zeta^{as})/h(\zeta^{s'})) \neq 0,$$

for some pair of integers s, s' relatively prime to p, then $\varphi((K-L) \otimes_{\mathbf{Z}} \mathbf{Z}_p)^\chi \neq 0$. (Here we have written $\tilde{\chi}^{-1}(z(a))$ by abuse of notation when $a \in (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times$; evidently this is a well defined function.) In fact, since $\tilde{\chi}$ is non-trivial, $h(\tilde{\chi})$ is just the image in F_n of the element

$$\sum_{a \in (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times} \tilde{\chi}^{-1}(z(a)) h(\zeta^{as}) = \left(\sum_{Z/Z_n} \tilde{\chi}^{-1}(z) z \right) h(\zeta^s) \in \mathcal{O}_n^\times \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$$

(multiplication is here written additively), under the natural extension of the p-adic logarithm. But

$$e(\tilde{\chi}) = (1/(p-1)p^n) \sum_{Z/Z_n} \tilde{\chi}^{-1}(z) z$$

is the orthogonal idempotent in $\mathbf{Q}_p(\boldsymbol{\mu}_{p^n})[Z/Z_n]$ corresponding to the character $\tilde{\chi}$. Our claim follows immediately, since $e(\tilde{\chi})$ is a non-zero multiple of the orthogonal idempotent corresponding to the character χ in $\mathbf{Q}_p[\Delta] \subset \mathbf{Q}_p(\zeta_{p^n})[Z/Z_n]$.

Let $a \neq 1$ be a p-adic unit; we may regard it as an element of Z. Katz has proved:

THEOREM (Katz, [4], 10.2.12 and [3]): *There is a $\bar{K}_v$-valued measure $\mu_E^{(a)}$ on the p-adic group Z with the property that its associated p-adic L-function*

$$L_E^{(a)}(f) = \int_Z f d\mu_E^{(a)} \qquad f \in C(Z, \bar{K}_v)$$

satisfies, for any character $\tilde{\chi}$ of exact conductor p^{n+1},

$$L_E^{(a)}(\tilde{x}) = -\frac{1}{12p^{2n+2}} G(\tilde{\chi})h(\tilde{\chi})(1-\tilde{\chi}(a))$$

here $G(\tilde{\chi})$ is the Gauss sum $\Sigma_{a\in(\mathbf{Z}/p^{n+1}\mathbf{Z})^\times} \tilde{\chi}(a)\zeta^{-as}$, where s is as in the definition of $h(\chi)$.

For notions associated with p-adic measures and p-adic L-functions, see [3], §3, and [7], §7. We need only to make use of the following lemma:

LEMMA ([7], §7): *The function $L^{(a)}(f)$ is determined by the set of functions $L_\chi^{(a)}(f_0) = L^{(a)}(\chi, f_0)$, where χ is a character of Δ and where $f_0 \in C(Z_0, \bar{K}_v)$; here $\chi \cdot f_0(z) = \chi(d) f_0(z_0)$ if $z = d \cdot z_0$ for $d \in \Delta$ and $z_0 \in Z_0$. Furthermore, if $L_\chi^{(a)}(f_0)$ is not zero for all f_0, for some fixed χ, then $L_\chi^{(a)}(\chi')$ is zero for at most finitely many continuous characters $\chi' : Z_0 \to \bar{K}_v^\times$.*

The *p-adic L-function* $L_E(\chi)$ is defined by Katz by the formula

$$L_E(\chi) = \frac{1}{1-\chi(a)} L_E^{(a)}(\chi); \quad \chi \neq 1$$

Katz has shown ([3], 3.7) that this expression is independent of the choice of a. As a consequence of the preceding remarks, we have

THEOREM 2: *Let χ be a character of Δ, and let $L_\chi(\chi')$ be the function associated to $L_E(\chi')$ as in the lemma. If $L_\chi(\chi') \neq 0$ for some non-trivial continuous character χ', then $((K-L)\otimes_{\mathbf{Z}} \mathbf{Z}_p))^\chi \neq 0$.*

PROOF: We have only to choose an a such that $\chi\chi'(a) \neq 1$, and apply the preceding argument.

REMARKS: 1. Katz's construction of p-adic measures depends upon a choice of trivialization of the formal group of $E/\bar{K}_v$; whether or not the p-adic L-function vanishes is, however, independent of the trivialization.

2. The Lemma illustrates the principle, already exploited in §2, that the non-triviality of $((K-L)\otimes_{\mathbf{Z}} \mathbf{Z}_p))^\chi$ implies that $((K-L)\otimes_{\mathbf{Z}} \mathbf{Z}_p))^\chi$ has infinite $\mathbf{Z}_p$-rank. (Actually we need to know that its image in $F_\infty^\times$ is non-trivial in order to draw this conclusion.)

3. Fix an even character χ of Δ; i.e., $\chi(-1) = 1$. The function $L_E(\chi)$, as a function of *ordinary elliptic curves* E over p-adic rings, is a p-adic generalized modular function of weight zero and nebentypus

χ which, moreover, is not identically zero (as can be verified by a computation of its q-expansion and application of the q-expansion principle; cf. [3]). It is not hard to see that, for any finite extension D of $\mathbf{Z}_p$, it is a *rigid analytic function* on the (rigid analytic) subset of the moduli space of ordinary elliptic curves over D with level p structure. This presumably means that $L_E(\chi) = 0$ for at most finitely many E over D. In particular, for all but finitely many E over K which are ordinary at some prime of K dividing p, the number λ in Theorem 1 may be replaced by $(p-1)/2$.

4. The conclusion of Theorem 2 may be strengthened to assert p-adic multiplicative independence of Kubert-Lang units, as opposed to mere multiplicative independence.

REFERENCES

[1] M. HARRIS: P-adic Representations Arising from Descent on Abelian Varieties, *Compositio Math., 39* (1979) 177–245.
[2] M. HARRIS, "Systematic Growth of Mordell-Weil Groups of Abelian Varieties in Towers of Number Fields," *Inv. Math., 51* (1979) 123–141.
[3] N. KATZ: The Eisenstein Measure and p-Adic Interpolation. *Am. J. Math., 99* (1977) 238–311.
[4] N. KATZ, "p-adic interpolation of real analytic Eisenstein series," *Ann. of Math., 104,* pp. 459–571 (1976).
[5] D. KUBERT and S. LANG, "Units in the Modular Function Field," II. *Math. Ann.*, 218, pp. 175–189 (1975); III. *Math. Ann.*, 218, pp. 273–285 (1975); V. *Math. Ann.*, 237, pp. 97–104. (1978).
[6] S. LANG, *Elliptic Functions*, Reading, Mass.: Addison-Wesley (1973).
[7] B. MAZUR and P. SWINNERTON-DYER, "Arithmetic of Weil Curves," *Inv. Math. 25,* pp. 1–61 (1974).
[8] K. RAMACHANDRA, "Some Applications of Kronecker's Limit Formula," *Ann. of Math., 80,* pp. 104–108 (1964).
[9] G. ROBERT, "Unités Elliptiques," *Memoire N° 36, Bull. Soc. Math. France* (1973).
[10] J.-P. SERRE, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques," *Inv. Math. 15,* pp. 259–331 (1972).
[11] J-P. SERRE, *Abelian l-adic Representations and Elliptic Curves*, New York: W. A. BENJAMIN, Inc. (1968).

(Oblatum 28-III-1979 & 13-VI-1979)

Department of Mathematics
Brandeis University
Waltham, Ma. 02154
USA