Advanced Studies in Pure Mathematics 12, 1987
Galois Representations and Arithmetic Algebraic Geometry
pp. 235–247

Torsion Points on Curves

Robert F. Coleman

§ 1.

Let C be a smooth complete curve defined over a field K. Let $\bar{K}$ denote the algebraic closure of K. We define an equivalence relation on $C(\bar{K})$ as follows. If $P, Q \in C(\bar{K})$, then we write $P \sim Q$ iff a positive integral multiple of the divisor $P-Q$ is principal. We call an equivalence class under this relation a *torsion packet*.

Suppose J is the Jacobian of C, $P \in C(\bar{K})$ and $i\colon (C, P) \to (J, 0)$ is an Albanese mapping. Then Abel's theorem implies $i^{-1}((i(C) \cap J_{\mathrm{Tor}})(\bar{K}))$ is the torsion packet containing P.

Examples. (i) $C = \boldsymbol{P}^1_K$ then $C(\bar{K})$ is the unique torsion packet on C.

(ii) C is an elliptic curve. Then the torsion packets are the sets $\{P+T\colon T \in C(\bar{K})_{\mathrm{Tor}}\}$ for $P \in C(\bar{K})$. Hence every torsion packet is infinite and if $\mathrm{char}\,(K)=0$ or K has positive transcendence degree, the number of non-trivial torsion packets is infinite.

(iii) K is a field of positive characteristic and transcendence degree 0. Then $C(\bar{K})$ is a torsion packet.

(iv) char $K=0$ and $g(C) \geq 2$, then Raynaud has proven that every torsion packet is finite [R-1] and if $g(C) \geq 3$ there are only finitely many non-trivial torsion packets [R-2].

(v) If $g(C)=2$ the morphism

$$\begin{aligned} C \times C &\longrightarrow J \\ (P, Q) &\longmapsto (P-Q) \end{aligned}$$

is surjective and since $\sharp J(\bar{K})_{\mathrm{Tor}} = \infty$, $\sharp\{(P, Q)\colon P \neq Q, P \sim Q\} = \infty$. This, together with the previous example, implies that if $\mathrm{char}\,(K)=0$ the number of non-trivial torsion packets on C is infinite.

(vi) Suppose $K=\boldsymbol{Q}$, m is a positive integer and F_m is the complete projective curve with homogeneous equation

$$X^m + Y^m + Z^m = 0.$$

Received May 27, 1986.

Let T_m = locus of $XYZ=0$ on F_m. Then we can show

(a) T_m is a torsion packet if $m=(p-1)/k$ with p a prime number and k an integer such that $1 \leq k \leq 8$ [C-2].

(b) If $m=p-1$, $m \geq 12$, then T_m is the only non-trivial torsion packet in $F_m(\bar{\boldsymbol{Q}})$.

(vii) If C is a modular curve then the cusps on C are contained in a torsion packet, but it is not known when the set of cusps is a torsion packet. (On $X_1(13)$ it is not. [C-1])

(viii) Suppose $f\colon C \to \boldsymbol{P}^1_K$ is a cyclic p-covering. Then the branch points of f on C are contained in a torsion packet.

There are still several interesting unsolved problems concerning torsion points on curves. We begin with the following generalization of the Manin-Mumford conjecture: Let X be a Zariski open in C. Suppose

$$\begin{array}{c} A \\ \big\downarrow{\scriptstyle \pi} \\ X \end{array}$$

is a family of Abelian varieties over X. Let Γ denote a group of sections of π. Suppose there is no non-constant $s \in \Gamma$ such that s factors through a section of a subfamily of one-dimensional group varieties (i.e., an extension of an elliptic family by a family of finite group schemes). For $P \in X(\bar{K})$ let A_P denote the fiber at P and

$$\Gamma_P = \{s(P) : s \in \Gamma\} \subseteq A_P(\bar{K}).$$

Conjecture 1. *Suppose* char $(K)=0$, *then*

$$\text{rank}\, \Gamma_P = \text{rank}\, \Gamma \tag{1}$$

for all but finitely many $P \in X(\bar{K})$.

Suppose $X=C$ and J is the Jacobian of C and $a\colon C \to J$ is an Albanese morphism. Let Γ be the group of sections of $C \times J \to C$ generated by (id, a). Then if $g(C) \geq 1$, rk $\Gamma = 1$ and if $g(C) \geq 2$ the above conjecture is just the Manin-Mumford conjecture. We also note that Mordell's conjecture is a consequence of this conjecture.

When $K \subseteq \bar{\boldsymbol{Q}}$, Silverman [S] has proven, with the above hypothesis on Γ replaced by the hypothesis that no non-zero element of Γ is "constant", that (1) holds for $P \in C(\bar{\boldsymbol{Q}})$ of sufficiently large height. (Note: this is stronger than the result stated in [S] but the proof is the same.) On the other hand, Szpiro [Sz, Note 4] has shown there are finitely many points in $C(\bar{\boldsymbol{Q}})$ of "small" height (where "small" is not yet completely understood).

When char $(K)>0$ not much is known; as explained in example (iv), the analogue of the Manin-Mumford conjecture for curves over finite fields is false. Does it hold for curves which do not come by extension of scalars from a curve over a finite field? This would be a consequence of the function field analogue of the above mentioned result of Szpiro. Even over finite fields there are some interesting questions. Does the analogue of Bogomolov's theorem [B] hold? I.e., let C be a curve over a finite field K. Let m be a positive integer, and let $a\colon C\to J$ be an Albanese morphism from C into its Jacobian. Suppose $g(C)\geq 2$.

Problem 2. *Is* $\#((a(C)\cap J[m^\infty])(\bar{K}))<\infty$?

We can prove: Let S be a set of rational primes. Let $S(N)$ denote the set of positive integers divisible only by primes in S. Suppose S is finite.

Theorem 3.

$$\lim_{\substack{m\to\infty\\ m\in S(N)}} \frac{\#(a(C)\cap J[m](\bar{K}))}{m^2}=0.$$

The proof of this when char $(K)\notin S$ will be given in Sections 2–4.

On the other hand, Anderson and Indik [A-I] have proven the following result. Let $\Pi_m\colon J[\bar{F}_p]\to J[m^\infty]$ denote the natural projection.

$$(J(\bar{F}_p)=\prod_{l\text{ prime}} J[l^\infty](\bar{F}_p)).$$

Then the composition

$$\Pi_m\circ a\colon C(\bar{F}_p)\longrightarrow J[m^\infty]$$

is a surjection.

Now let us return to curves defined over number fields. We formulate yet another conjecture.

Let $\mathfrak{P}$ be a prime of K.

(i) at which $K/\boldsymbol{Q}$ is unramified,

(ii) at which C has good reduction,

(iii) which does not divide 6.

Let T be a torsion packet in $C(\bar{K})$ which is stable under $G((\bar{K}/K))$. Suppose $g(C)\geq 2$.

Conjecture 4. *$K(T)/K$ is unramified above $\mathfrak{P}$.*

We can prove the following [C-3]: Let $\mathfrak{P}$ be a prime of K which satisfies, in addition to (i)–(iii) above, one of the following conditions:

(a) C has ordinary reduction at $\mathfrak{P}$, or
(b) C has superspecial reduction at $\mathfrak{P}$, or
(c) char $\mathfrak{P}>2g$.

Then if $g(C)\geq 2$, $K(T)/K$ is unramified at $\mathfrak{P}$. (Note: Ordinary means the Hasse-Witt matrix is invertible and superspecial means it is zero.) This, combined with results of Bogomolov [B], can be used to give a new proof of the Manin-Mumford conjecture.

We can also prove Conjecture 4 for the cuspidal torsion packet on abelian covers of $\boldsymbol{P}^1_K$ unramified outside $\{0, 1, \infty\}$ [C-4]. (This is the torsion packet which contains the inverse image of $\{0, 1, \infty\}$.)

In view of example (viii) one could attempt to make counter-examples to Conjecture 4 by constructing cyclic p-covers of $\boldsymbol{P}^1_{\boldsymbol{Q}}$ with good reduction over $\boldsymbol{Q}_p$. However, one can prove

Proposition 5. *Suppose K is an unramified extension of $\boldsymbol{Q}_p$. Suppose C is a curve with good reduction over K and α is an automorphism of C of order p. Then if $p>3$, α has no fixed points.*

This will be proved in Section 5.

Finally we would like to state one last conjecture. Let g be an integer $g\geq 4$.

Conjecture 6. *There are only finitely many curves over $\boldsymbol{C}$ of genus g whose Jacobians admit the structure of a CM Abelian variety.*

This is an analogue of the Manin-Mumford conjecture because the CM points on the moduli space of principally polarized Abelian varieties of genus g are analogous to torsion points. In fact the CM liftings to $\bar{\boldsymbol{Q}}_p$ of an ordinary Abelian variety over $\bar{\boldsymbol{F}}_p$ are the torsion points in the moduli space of all liftings (see [K]). Dwork and Ogus have obtained a partial result in this direction, see [D-O].

§ 2. Torsion points on curves over finite fields

In this section we will begin a proof of Theorem 3. Let K be a finite field of characteristic p and C a curve of genus ≥ 2 over K. Suppose S is a finite set of rational primes. Let J be the Jacobian of C. We will suppose C is embedded in J. Let $\phi: J\to J$ denote the Frobenius endomorphism of J over K. Then $\phi: J[m](\bar{K})\overset{\sim}{\to} J[m](\bar{K})$ for all integers m. In particular if $\beta\in \mathrm{End}_K(J)$ such that $(\phi^n-\beta)J[m]=(0)$, then

$$(C\cap J[m])(\bar{K})\subseteq(C\cap \beta C)(\bar{K}). \tag{2}$$

Let $W_k=$the image of C^k in J under the map

$$(Q_1, \cdots, Q_k) \longmapsto Q_1 + \cdots + Q_k.$$

Lemma 7. *If $\beta \in \mathrm{End}_K(J)$ and $\beta C \neq C$ then $\#(C \cap \beta C)(\bar{K}) \leq W_{g-1} \cdot \beta C$ where "$\cdot$" denotes the intersection pairing.*

Proof. All we need show is that there exists an $x \in W_{g-2}$ such that $\beta C \not\subseteq -x + W_{g-1}$. Otherwise $\beta C + W_{g-2} \subseteq W_{g-1}$. Since $\beta C \neq C$ this contradicts Lemma 5.4 of [C-1].

Lemma 8. *There exists a constant M_r depending only on r such that if $\beta = \sum_{i=0}^{r-1} n_i \phi^i$, $\beta C \neq C$ and $\beta \in \mathrm{End}_K(J)$. Then*

$$\#(C \cap \beta C) \leq \max_{i,j}\{|n_i n_j|\} M_r.$$

Proof. $\#(C \cap \beta C) \leq W_{g-1} \cdot \beta C$. By Theorem 5, IV Section 3, of [L],

$$W_{g-1} \cdot \beta C = (\beta^{-1} W_{g-1}) \cdot C.$$

By Proposition 2 of IV, Section 1 of [L], we have

$$2\beta^{-1}(W_{g-1}) = \sum_{i,j} n_i n_j D_{ij},$$

where $D_{ij} = ((\phi^i + \phi^j)^{-1} - (\phi^{-i} + \phi^{-j})) W_{g-1}$. Hence

$$W_{g-1} \cdot \beta C = \frac{1}{2} \sum_{i,j} n_i n_j (D_{ij} \cdot C).$$

If we take $M_r = (r^2/2) \max |D_{ij} \cdot C|$ we obtain the result.

Let $\boldsymbol{Z}[\phi]$ denote the subring of $\mathrm{End}_K(J)$ generated by ϕ. Let $r = \mathrm{rk}\, \boldsymbol{Z}[\phi]$. Let $\varepsilon > 0$. Suppose we could show that for each sufficiently large $m \in S(N)$ there exists a $\beta = \sum_{i=0}^{r-1} n_i \phi^i \in \boldsymbol{Z}[\phi]$ and an $n \in N$ such that

(i) $(\beta - \phi^n) J[m] = (0)$
(ii) $|n_i| < \varepsilon m$ for all i, and
(iii) $\beta C \neq C$.

Then it would follow from Lemma 8 and equation (2) that

$$\#(C \cap J[m])(\bar{K}) \leq \varepsilon^2 m^2 M_r$$

for sufficiently large $m \in S(N)$. This would imply Theorem 2.

When $p \notin S$ we will establish the existence of such β and n for large $m \in S(N)$. This additional hypothesis simplifies the argument. For then (i) translates into

(i′) $\beta = \phi^n \bmod m\boldsymbol{Z}[\phi]$.

In any case, (iii) is equivalent to

(iii′) $\beta \neq \phi^k \phi$

for any $k \in N$, $\rho \in \operatorname{Aut}(J)$ such that ρ preserves C, since the genus of C is strictly greater than one.

§ 3. S-adic uniform distribution

Let S be a set of rational primes. By Z_S we mean $\varprojlim Z/mZ$ where m ranges over $S(N)$. If S is the set of all primes, then we set $\hat{Z}=Z_S$.

For $x \in (R/Z)^n$ we let $\langle x\rangle$ denote its unique representative in $[0, 1)^n$. There is a natural embedding $(Q\otimes Z_S)/Z_S \to Q/Z$ and so of

$$(Q\otimes Z_S)^r/Z_S^r \to (Q/Z)^r.$$

For $x \in Q\otimes Z_S^r$ we let $\langle x\rangle = \langle (x+Z_S^r)/Z_S^r\rangle$.

Now suppose M is a free Z_S module of finite rank r and $g\colon N\to M$ is a function which extends continuously to a function $g\colon \hat{Z}\to M$. It follows that for each $m \in S(N)$ there exists a $\pi_m \in N$, $\pi_m>0$ such that $g(x+\pi_m)\equiv g(x) \bmod m$ for all $x \in N$. We say g is *uniformly distributed* if for each isomorphism $L\colon M\cong Z_S^r$ and each open subset U of $[0, 1)^r$,

$$\lim_{\substack{m\to\infty\\ m\in S(N)}} \frac{\#\left\{\{0\le k<\pi_m\colon \left\langle \frac{g(k)}{m}\right\rangle \in U\right\}}{\pi_m} = \operatorname{Vol}(U)$$

Note that the term in this limit corresponding to m is independent of the choice of π_m. We have the following Weyl-type criterion for uniform distribution.

Theorem 9. *g is uniformly distributed iff for each non-zero Z_S-linear map $L\colon M\to Z_S$,*

$$\lim_{\substack{m\to\infty\\ m\in S(N)}} \frac{1}{\pi_m}\sum_{a=0}^{\pi_m-1} e\left(\frac{L\circ g(a)}{m}\right)=0$$

where $e(x)=\exp(2\pi i\langle x\rangle)$.

We call the m^{th} term in this limit $\sum_m(g)$. It is independent of the choice of π_m.

Example. Suppose $g\colon N\to\hat{Z}$ is given by $g(n)=f(n) \in Z\subseteq\hat{Z}$ for some non-constant polynomial $f(x) \in Z[x]$. Then the estimates on exponential sums due to Deligne [D] and Igusa [I] show that g is uniformly distributed.

Suppose now $M=Z_S$. For $l \in S$, let g_l be the composition of g with the projection from Z_S onto Z_l. We say g is *nowhere constant* if g

does not vanish on any non-empty open subset of $\boldsymbol{Z}$, locally analytic if for each $l \in S$ and each $a \in \boldsymbol{N}$ there exists a neighborhood U of a in $\hat{\boldsymbol{Z}}$ of the form $U' \times D$ where $U' = \prod_{r \neq l} \boldsymbol{Z}_r$ and $D \subseteq \boldsymbol{Z}_l$ is of the form $\{x \in \boldsymbol{Z}_l : |x - a_l| \leq |l^k|\}$ for some k in $\boldsymbol{N}$ and there exists a restricted power series

$$h(T) \in \boldsymbol{Q}_l\langle\langle T \rangle\rangle$$

such that for $x \in U$, $\hat{g}(x) = h(x_l - a_l/l^k)$.

Proposition 10. *Suppose S is finite and $g: \boldsymbol{N} \to \boldsymbol{Z}_S$ is nowhere constant and locally analytic. Then g is uniformly distributed.*

Proof. It suffices to show that under these assumptions,

$$\lim_{\substack{m \to \infty \\ m \in S(\boldsymbol{N})}} \sum_M (g) = 0 \tag{3}$$

because bg satisfies the same hypotheses as g for each $b \in \boldsymbol{Z}_S$, $b_l \neq 0$, $l \in S$.

Suppose $\mathscr{C}$ is a finite open covering of $\hat{\boldsymbol{Z}}$. It suffices to prove

$$\lim_{\substack{m \to \infty \\ m \in S(\boldsymbol{N})}} \frac{1}{\pi_m} \sum_{\substack{a=0 \\ a \in U}}^{\pi_m - 1} e\left(\frac{g(a)}{m}\right) = 0$$

for each $U \in \mathscr{C}$. Hence after passing to a suitable covering and a change of variables using the fact that g_l is locally analytic, we may suppose

$$g_l(x) = h_l(x_l)$$

for some $h_l(T) \in \boldsymbol{Q}_l\langle\langle T \rangle\rangle$. After passing to a finer covering, using the fact that g is nowhere constant, takes values in $\boldsymbol{Z}$ and perhaps applying another change of variables we may suppose $h_l(T) \in \boldsymbol{Z}_l\langle\langle T \rangle\rangle$ and $h_l'(a) = 0$ for all $a \in \boldsymbol{Z}_l$, $a \neq 0$.

Suppose now $m \in S(\boldsymbol{N})$, $m = \prod_{l \in S} l^{n_l}$. We may write

$$\frac{1}{m} = \sum_{l \in S} \frac{b_l(m)}{l^{n_l}}$$

where $b_l(m) \in \boldsymbol{Z}$, $(b_l(m), l) = 1$. One checks easily that

$$\sum\nolimits_m (g) = \prod_{l \in S} \frac{1}{l^{n_l}} \sum_{a=0}^{l^{n_l}-1} e\left(\frac{g_l(a) b_l(m)}{l^{n_l}}\right)$$

Hence it suffices to prove

Lemma 11. *Let $h \in \boldsymbol{Z}_l\langle\langle T \rangle\rangle$ such that $h'(a) \neq 0$ for all $a \in \boldsymbol{Z}_l$, $a \neq 0$. Then if*

$$\Sigma_n(bh)=\frac{1}{l^n}\sum_{a=0}^{l^n-1} e\left(\frac{bh(a)}{l^n}\right),$$

$\Sigma_n(bh)$ converges to zero uniformly with respect to $b \in Z_l^*$.

Proof. Let k be any natural number. We first observe that if $a \in Z_l$ and $\mathrm{ord}_l\, h'(a)<k$ then $\mathrm{ord}_l\, h'(a+il^k)<k$, using the Taylor expansion for $h'(T)$. Second, let $a_1, \cdots, a_t$ be representatives mod l^{n-k} for these $a \in Z_l$ such that $\mathrm{ord}_l\, h'(a)<k$. Then if $n\geq 2k$ we have

$$\sum_{\substack{a=0\\ \mathrm{ord}_l\, q<k}}^{l^r-1} e\left(\frac{bh(a)}{l^n}\right)=\sum_{i=1}^{t}\sum_{j=0}^{l^k-1} e\left(\frac{bh(a_i+jl^{n-k})}{l^n}\right)$$

As $\mathrm{ord}_l\, h'(a_i)=\mathrm{ord}_l\, h'(a)<k$, $h(a_i+jl^{n-k})\equiv h(a_i)+h'(a_i)jl^{n-k} \bmod l^{2(n-k)}$ and $2(n-k)\geq n$, the above sum equals

$$\sum_{i=1}^{t} e\left(\frac{bh(a_i)}{l^n}\right)\sum_{j=0}^{l^k-1} e\left(\frac{jbh'(a_i)}{l^k}\right)$$

Since $(bh'(a_i)/l^k)\notin Z_l$, this sum is zero. Hence if $n\leq 2k$

$$|\Sigma_n(bh)|=\left|\frac{1}{l^n}\sum_{\substack{a=0\\ \mathrm{ord}_l\, h(a)\geq k}}^{l^n-1} e\left(\frac{bh(a)}{l^n}\right)\right|\leq\frac{1}{l^n}N_{n,k} \tag{4}$$

where $N_{n,k}=\#\{0\leq a\leq l^n-1\colon \mathrm{ord}_l\, h_l'(a)\geq k\}$. Now let $r=\mathrm{ord}_{T=0}\, h'(T)$ and

$$s=\max_{\substack{a\in Z_l\\ a\neq 0}} \mathrm{ord}_l\left(\frac{h'(a)}{a^r}\right).$$

Then $r, s<\infty$ and are independent of b. Moreover, if t_1 is any natural number and $\mathrm{ord}_l\, h'(a)\geq s+rk$ it follows that $\mathrm{ord}_l\, a\geq t$ unless $r=0$. If $r=0$, then $N_{n,s+1}=0$ so it follows from (4) that $\Sigma_n(bh)=0$ for $n>2(s+1)$. Hence we may suppose $r>0$. It follows that if $n\geq 2(s+rt)$ then

$$N_{n,s+rt}\leq l^{n-t}.$$

Hence $\Sigma_n(bh)\leq l^{-t}$ for $n\geq 2(s+rt)$. This proves the lemma and so the proposition.

§ 4. End of proof of Theorem 3

Suppose $\mathcal{O}$ is a flat finite integral extension of Z and $\mathcal{O}=Z[\alpha]$ where α^n-1 is not a zero-divisor and $r=\mathrm{rk}\,\mathcal{O}=\mathrm{rk}\,Z[\alpha^n]$ for all $n\in N$, $n>0$. Suppose S is a finite set of primes of Z such that α is a unit in $\mathcal{O}_S=\mathcal{O}\otimes Z_S$. Let $g\colon N\rightarrow\mathcal{O}_S$ be the map $n\mapsto\alpha^n$.

Proposition 12. *g is uniformly distributed.*

Proof. First it is clear that g extends to a continuous function from N onto $\mathcal{O}_S$ since α is a unit in $\mathcal{O}_S$. Let L: $\mathcal{O}_S \to Z_S$ be a non-zero Z_S-linear map. It is also clear that $L \circ g$ is locally analytic. After Section 3, all we need show is that $L \circ g$ is nowhere constant. If $L \circ g$ is constant on a non-empty open subset of $\hat{Z}$, it follows that there exists a $c \in Z_S$ and integers $a \geq 0$, $b > 0$ such that $L(\alpha^{a+nb}) = c$ for all $n \in N$. So if $c = 0$ then it follows that $\alpha^a, \alpha^{a+b}, \cdots, \alpha^{a+(n-1)b}$ are dependent over Z_S. Since α is a unit it follows that $1, \alpha^b, \cdots, \alpha^{(r-1)b}$ are dependent. So

$$Z_S[\alpha^b] = Z_S \otimes Z[\alpha^b]$$

is not free of rank r, which contradicts our hypotheses. Now suppose $c \neq 0$. Let $f(x)$ be the minimal monic polynomial over Z satisfied by α^b. Then

$$0 = L(\alpha^a f(\alpha^b)) = CL(1)$$

and so since $f(1) \in Z$ and $C \neq 0$, $f(1) = 0$. It follows that $\alpha^b - 1$ is a zero divisor in $\mathcal{O}$, a contradiction.

In contrast to the results of [K-S], we have

Corollary 12.1. *Let F_n denote the n^{th} Fibonacci number. Let S denote a finite subset of the rational primes not containing* 5. *Then the function*

$$n \longmapsto F_n \in Z \subseteq Z_S$$

is uniformly distributed.

Proof. Let T: $Q(\sqrt{5}) \to Q$ denote the trace. As is well known,

$$F_n = T\left(\frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n\right).$$

Since $(1+\sqrt{5})/2$ is the fundamental unit in $Q(\sqrt{5})$, the corollary is an immediate consequence of the proposition.

We now are ready to apply these results on uniform distribution to estimate $\#(C \cap J[m])(\bar{K})$, $m \in S(N)$, $p \notin S$. We may suppose

$$r = \operatorname{rk} Z[\phi] = \operatorname{rk} Z[\phi^n]$$

for all $n \in Z$, $n > 0$ by replacing K by a finite extension. Then the ring $Z[\phi] \subseteq \operatorname{End}(J)$ and ϕ satisfy the hypotheses of the previous proposition since ϕ has no root of unity eigenvalues, and ϕ is a unit outside p. Hence for each $\varepsilon>0$, $0<c<1$ and for $m \in S(N)$ sufficiently large

$$\#\left\{\beta=\sum_{i=0}^{r-1} n_i\phi^i : |n_i|<\varepsilon m,\ \beta\equiv\phi^n \bmod m\boldsymbol{Z}[\phi] \text{ for some } n \in \boldsymbol{N}\right\}$$
$$\geq(\varepsilon m)^r c.$$

This certainly supplies us with β satisfying (i) and (i′) of Section 2. It remains to check that (iii′) can be fulfilled also. Let $\sigma\colon \boldsymbol{Z}[\phi]\to\boldsymbol{C}$ be a ring homomorphism. Suppose $\beta \in \boldsymbol{Z}[\phi]$,

$$\beta=\phi^k\rho \tag{5}$$

$\rho \in \mathrm{Aut}\,(J)$ fixing C, and some $k \in \boldsymbol{N}$. Since ρ is necessarily of finite order,

$$|\sigma(\beta)|=|\sigma(\phi)|^k=(\sqrt{q}\,)^k$$

where $q=\#K$, by the Riemann hypothesis. On the other hand, if

$$\beta=\sum_{i=0}^{r-1} n_i\phi^i, \qquad |n_i|<\varepsilon m \tag{6}$$

then $|\sigma(\beta)|\leq\varepsilon m(\sqrt{q}\,)^r$. So if β satisfies (5) and (6),

$$k\leq(\log_{\sqrt{q}}(\varepsilon m))+r.$$

Let $w=$the number of automorphisms of J which preserve C. This number is finite since $\mathrm{Aut}\,(C)$ is finite. It follows that the number of β satisfying (5) and (6) is at most

$$w(\log_{\sqrt{q}}(\varepsilon m)+r+1)$$

which for m sufficiently large is less than $(\varepsilon m)^r c$ since $r\geq 1$. This insures the existence of a β satisfying (i), (ii) and (iii) for m sufficiently large in $S(\boldsymbol{N})$ and hence completes the proof of Theorem 2 when $p \notin S$. When $p \in S$, the same ideas can be made to work but the required definition of uniform convergence becomes more complicated as the rank over $\boldsymbol{Z}_p$ of the closure of the image of $\boldsymbol{Z}[\phi]$ in End $T_p(J)$ is smaller than the rank of $\boldsymbol{Z}[\phi]$ over $\boldsymbol{Z}$.

§ 5. Cyclic p-extensions of curves over $\boldsymbol{Q}_p$

Let K denote the maximal unramified extension of $\boldsymbol{Q}_p$. Suppose $p>3$. Let $\mathcal{O}$ denote the ring of integers in K. We will now begin the proof of Proposition 5. Suppose Y is a curve over K with good reduction and α is an automorphism of Y of order p with fixed points. Since the proposition is easy when $Y=\boldsymbol{P}^1_K$ we may suppose that the genus of Y is positive. Then Y has a canonical model over the integers $\mathcal{O}$ of K with good reduction and α extends to this model. We claim there is an open disk in Y, isomorphic to the open unit disk over K, fixed by α. We may take any residue class containing a fixed point of α as our disk.

Proposition 5 will now follow from

Proposition 13. *There are no non-trivial analytic automorphisms of order p of the open unit disk over K.*

Lemma 14. *Let k be an integer. Suppose R is any ring in which k is not a zero divisor. Let $g(x) \in R[[x]]$ such that*

$$g(x) \equiv x \bmod x^2 \quad \text{and} \quad \underbrace{g \circ g \circ \cdots \circ g}_{k \text{ times}}(x) = x.$$

Then $g(x) = x$.

Proof. Suppose $g(x) \neq x$. Let n be such that $g(x) \equiv x + cx^n \bmod x^{n+1}$ with $c \neq 0$. Then

$$\underbrace{g \circ g \circ \cdots \circ g}_{k \text{ times}}(x) \equiv x + kcx^n \bmod x^{n+1}.$$

Hence $kc = 0$ and so $c = 0$, a contradiction.

Lemma 15. *Consider thə series*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$$

over $\boldsymbol{Z}[[a_0, a_1, \cdots, a_n, \cdots]]$. Then

$$\underbrace{f \circ f \circ \cdots \circ f}_{k \text{ times}}(x) \equiv a_0(1 + a_1 + \cdots + a_1^{k-1}) + a_1^k x$$
$$\text{modulo} \quad (a_0^2a_2,\ a_0^3,\ a_0^2x,\ a_0a_2x,\ a_0x^2,\ a_2x^2,\ x^3).$$

Proof. This follows easily by induction on k.

Lemma 16. *There are no solutions of*

$$1 + x + x^2 + \cdots + x^{p-1} \equiv 0 \bmod p^2$$

in $\mathcal{O}$.

Proof. Suppose x were a solution. Then it is easy to see that $x = 1 + a$ for some $a \in (p)$. Then

$$1+x+\cdots+x^{p-1}\equiv p+\frac{p(p-1)}{2}a \bmod p^2$$
$$\equiv p \bmod p^2 \text{ since } p>2.$$

Proof of Proposition 13. Let f be an analytic isomorphism of the open unit disk over K. Then f may be expressed as a series

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n+\cdots$$

with $a_n \in \mathcal{O}$, $a_0 \in p\mathcal{O}$, $a_1 \in \mathcal{O}^*$. Suppose f has order p. Then after Lemma 15 we have

$$a_0(1+a_1+\cdots+a_1^{p-1})\equiv 0 \bmod a_0^2(a_0, a_2)$$
$$a_1^p\equiv 1 \bmod a_0(a_0, a_2).$$

It follows that either

(i) $a_0=0$, $a_1^p=1$

or

(ii) $1+a_1+\cdots+a_1^{p-1}\equiv 0 \bmod a_0(a_0, a_2)$.

In case (i) we have $a_1=1$ since $p>2$, hence $f(x)=x$ after Lemma 14. In case (ii) we have $a_0(a_0, a_2)=p\mathcal{O}$ after Lemma 16 and so $a_0 \in p\mathcal{O}^*$, $a_1\equiv 1 \bmod p\mathcal{O}$ and $a_2 \in \mathcal{O}^*$. From this we see that f has exactly two fixed points which are defined over a quadratic extension of K. Let α be one of these fixed points. Set

$$g(x)=f(x+\alpha)-\alpha.$$

Then

$$g(x)\equiv cx \bmod x^2, \qquad \text{with } c \in K(\alpha)$$

and $\overbrace{g\circ g\circ\cdots\circ g}^{p \text{ times}}(x)=x$. It follows from Lemma 15 that $c^p=1$. But since $p>3$ there are no non-trivial p^{th} roots of unity in a quadratic extension of K. Hence $c=1$ and applying Lemma 14 again we have

$$x=g(x)=f(x)$$

as required.

Remarks. 1. If $p=2$ or 3, the statement of the theorem fails to be true. E.g., $\boldsymbol{P}^1_{\boldsymbol{Z}_p}$ has the automorphisms $x\mapsto 1/x$ and $x\mapsto 1/1-x$, which have order 2 and 3 respectively. By pulling back one can make examples of higher genus.

2. The proof of Proposition 5 may be adapted to prove that the same conclusion holds of the ramification index e of K over $\boldsymbol{Q}_p$ is strictly less then $(p-1)/2$ or if $p=3$ and the order of α is 9 or if $p=2$, $g>0$, and the order of α is 4. This raises the question, what are ȷhe general conditions on the order of α and e that insure the conclusion of Proposition 5?

3. As a corollary, one deduces that if $p>3$ and $f\colon X\rightarrow \boldsymbol{P}_K^1$ is a Galois covering of smooth curves over K and the ramification index with respect to f of some point of X is divisible by p, then X has bad reduction.

References

[A-I] Anderson, G. and R. Indik, On primes of degree one in function fields, Proceedings AMS, **94**, no. 1 (1985), 31–32.

[B] Bogomolov, F., Sur l'algebricite des representations γ-adiques, C. R. Acad. Sci., **290** (1980), 701–704.

[C-1] Coleman, R., Torsion points on curves and p-adic abelian integrals, Ann. of Math., **121** (1985), 111–168.

[C-2] ——, Torsion points on Fermat curves, Compositio Math., **58** (1986), 191–208.

[C-3] ——, Ramified torsion points on curves, to appear.

[C-4] ——, Torsion points on abelian coverings of $\boldsymbol{P}^1\{0, 1, \infty\}$, to appear.

[D] Deligne, P., Cohomologie étale, Seminaire de Geometrie algebrique du Bourbaki SGA 4, Springer Lecture Notes, **569** (Berlin, 1977).

[D-O] Dwork, B. and A. Ogus, Canonical liftings of abelian varieties, to appear in Compositio.

[I] Igusa, J., Complex powers and asymptotic expansions, I, I. Reine Angew. Math., **268–269** (1974), 110–130.

[K] Katz, N., Serre Tate local moduli, Springer Lecture Notes, **868**, 138–202.

[K-S] Kuiper, L. and J. S. Shiue, A distribution property of the sequence of Fibonacci numbers, Fibonacci Quarterly, **10**, no. 4 (1972), 375–376.

[L] Lang, S., Abelian varieties, Interscience Pub. (1959).

[R-1] Raynaud, M., Courbes sur une variété abélienne et points de torsion, Invent. Math., **71** (1983), 207–233.

[R-2] ——, Sous-variété d'une variétés abélienne et points de torsion.

[S] Silverman, J., Heights and the specialization map for families of abelian varieties, J. Reine Angew. Math., **342** (1983), 197–211.

[Sz] Szpiro, L., Presentation de la thèorie d'Arakélov, to appear in the Proceedings of the Arcata Conference.

Department of Mathematics
University of California
Berkeley, California 94720
U.S.A.