Inventiones math. 22, 41 – 49 (1973)

Points of Order 13 on Elliptic Curves

B. Mazur (Cambridge, Mass.) and J. Tate (Cambridge, Mass.)

1. Introduction

The main object of this note is to show that an elliptic curve defined over $\mathbb{Q}$ cannot have a rational point of order 13. Equivalently, $X_1(13)$, the curve that classifies elliptic curves with a chosen point of order 13, has no non-cuspidal points rational over $\mathbb{Q}$. This has also been announced by Blass who uses a method somewhat different from ours [1][1].

Our approach consists in applying a descent argument to J, the jacobian of $X_1(13)$, proving that J has precisely 19 rational points over $\mathbb{Q}$[2].

The possibility that this could be done occurred to us when Ogg passed through our town and mentioned that he had discovered a point of order 19 on the 2-dimensional abelian variety J. It seemed (to us and to Swinnerton-Dyer) that if such an abelian variety J, which has bad reduction at only one prime, and has a sizeable number of endomorphisms, has a point of order 19, it is not entitled to have any other points.

We show this below by an argument that requires a minimum of calculation (by "pure thought") and which may have parallels in the study of $X_1(n)$ for a few other higher values of n (e.g. see the forthcoming work of D. Kubert). Our first goal is to determine the structure of the Galois module V of 19-division points on J. To do this we use the action on V of a certain group Δ of automorphisms of $X_1(13)$. This group exists for $X_1(n)$, any n, and we begin by describing it as an abstract group on which Galois acts, which we call the twisted dihedral group.

2. The Twisted Dihedral Group

Let $\bar{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and let $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Fix an integer n. Let K denote the cyclotomic extension of $\mathbb{Q}$ obtained by

---

[1] Blass has communicated to us that he works directly on a hyperelliptic model of $X_1(13)$ of the form $y^2 = g(x)$, where $g(x)$ is a certain sixth degree polynomial which factors in a field of class number 1—not the field $\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$ which occurs below, however.

[2] Ogg [4] has checked that the L-series of J is non-zero at $s = 1$ and thus the above result is in accord with the general conjecture of Birch and Swinnerton-Dyer.

adjoining all n-th roots of 1 in $\bar{\mathbb{Q}}$. There is a canonical identification,

$$\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\approx} (\mathbb{Z}/n)^*.$$

Let Γ denote the group $(\mathbb{Z}/n)^*/(\pm 1)$. If m is an integer relatively prime to n, let γ_m denote its image in Γ. Also, if α is in G, or in $\mathrm{Gal}(K/\mathbb{Q})$, let γ_α denote its image in Γ, making use of the canonical identification alluded to. Thus we have $\gamma_\alpha = \gamma_\beta$ if and only if α and β coincide on the maximal real subfield K^+ of K.

We shall now describe a specific group Δ, which is a dihedral extension of $\mathbb{Z}/2$ by Γ

$$0 \to \Gamma \to \Delta \to \mathbb{Z}/2 \to 0.$$

As ζ runs through all primitive n-th roots of 1, the symbols $\tau_\zeta = \tau_{\zeta^{-1}}$ will run through the elements of the non-trivial Γ-coset of Δ. Moreover, the following relations are imposed:

$$\gamma_m \tau_\zeta = \tau_{\zeta^m}$$
$$\tau_\zeta \gamma_m \tau_\zeta^{-1} = (\gamma_m)^{-1}$$
$$(\tau_\zeta)^2 = 1.$$

is a natural action of $\mathrm{Gal}(K^+/\mathbb{Q})$ on Δ, given by the rules

$$\gamma_m^\alpha = \gamma_m, \quad \text{and} \quad (\tau_\zeta)^\alpha = \tau_{\zeta^\alpha} = \gamma_\alpha \tau_\zeta.$$

This group Δ, with its G-action, is called the *twisted dihedral group.*

Let $n \geqq 4$. Let $X_1(n)$ denote the non-singular projective curve over $\mathbb{Q}$ associated to the moduli problem:

Classify injections x: $\mathbb{Z}/n\mathbb{Z} \hookrightarrow E$ up to isomorphism, where E is an elliptic curve.

Then, as in [4], one has the following classical description of the complex-analytic Riemann surface of complex points of $X_1(n)$:

Consider the subgroup $\Gamma_1(n)$ of the full modular group $\mathbf{PSL}(2, \mathbb{Z}) = \mathbf{SL}(2, \mathbb{Z})/(\pm 1)$ consisting in those γ which can be represented by matrices satisfying the following congruence modulo n:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod n.$$

Let $Y_1(n)$ denote the quotient of the upper half-plane under the action of $\Gamma_1(n)$. Then $Y_1(n)$ is an open Riemann surface whose compactification is $X_1(n)$, and:

$$X_1(n) = Y_1(n) \cup \text{cusps}.$$

The dihedral group Δ acts in a natural way as a group of automorphisms on $X=X_1(n)$. This action has the following modular description:

If

$$x\colon\ \mathbb{Z}/n\mathbb{Z} \overset{\beta}{\hookrightarrow} E$$

is a "point" of $X_1(n)$, let $\gamma_m x$ denote the "point":

$$\gamma_m x\colon\ \mathbb{Z}/n\mathbb{Z} \overset{m\beta}{\hookrightarrow} E.$$

Let $\tau_\zeta x$ denote the "point":

$$\tau_\zeta x\colon\ \mathbb{Z}/n\mathbb{Z} \underset{\approx}{\overset{i_\zeta}{\to}} \mu_n \overset{\bar\beta}{\hookrightarrow} \bar E$$

where $\bar E = E/\mathrm{image}(\beta)$, μ_n is the galois module of n-th roots of 1, and $\bar\beta$ is the inclusion given to us by self-duality of E [3], and finally i_ζ is the map sending 1 to ζ. The verification that this defines an action of Δ is left to the reader.

This action is "defined ever $\mathbb{Q}$" in the sense that it enjoys the following galois-compatibility:

$$(\delta\cdot x)^\alpha = \delta^\alpha \cdot x^\alpha$$

for $\delta\in\Delta$, and x a point of X, rational over $\bar{\mathbb{Q}}$.

3. The Structure $X_1(13)$

From here on, fix $n=13$. Then Γ is cyclic of order 6, with γ_2 as generator. The reader is referred to [4] for the following description of $X_1(13)=X$:

X is of genus 2, and its jacobian $\mathrm{Pic}^0 X = J$ is an abelian variety of dimension 2 over $\mathbb{Q}$ with bad reduction only at the prime 13. The curve X has precisely 12 cusps, 6 of which are rational (over $\mathbb{Q}$) and the remaining 6 are rational over the maximal totally real subfield in $\mathbb{Q}(\zeta_{13})$. The group Γ operates cyclically on each of the sets of 6 cusps and Δ acts freely on the set of all cusps. If we imbed X in J by one of the 6 rational cusps to $0\in J$, then these 6 rational cusps generate a subgroup $T\subset J$ of order 19. The group T is the entire torsion subgroup of the Mordell-Weil group of J, and $X\cap T$ consists in precisely the 6 rational cusps.

The abelian variety J is simple over $\mathbb{Q}$. Here is the easy way of seeing this: If not, there would be an exact sequence of abelian varieties over $\mathbb{Q}$

$$0\to J_1\to J\to J_2\to 0$$

[3] The eternal problem concerning which convention to take for the sign of the self-duality, (one may adopt the choice of alternating form (,) defined by Weil [6] for example) and whether one wants image β to appear in the first or second entry of (,) forces us to confess that there are *two* natural choices for $\bar\beta$ which differ by sign. Luckily this ambiguity will not plague us insofar as the two natural choices are isomorphic to each other (by multiplication by -1) and therefore they give rise to the same point on $X_1(n)$.

where J_i $(i=1,2)$ are elliptic curves over $\mathbb{Q}$ with bad reduction only at 13. One of the J_i's has a rational point of order 19 because J does. This is impossible, for the reduction of this elliptic curve at $p=2$ can have by the Riemann hypothesis at most 5 rational points over the field of two elements, and a point of order 19 cannot reduce to zero under reduction in characteristic two.

As we shall mention later on, J is not absolutely irreducible. Consider the characteristic polynomial of the generator $\gamma_2 \in \Gamma$ acting on J. Since J is simple over $\mathbb{Q}$, this polynomial is a power of an irreducible polynomial. Since the action of γ_2 on J is *precisely* of order 6 (that is, not of order 1, 2, 3) as can be seen by its action on the 6 rational cusps, the characteristic polynomial of γ_2 has no choice but to be:

$$(1-x+x^2)^2$$

and consequently the action of Δ induces an action of the quotient ring

$$D=\mathbb{Z}[\Delta]/(1-\gamma_2+\gamma_2^2)$$

on J. Since D is an order in a simple algebra, this action is faithful. In the ring D, γ_2 generates a ring isomorphic to $\mathbb{Z}[\sqrt[3]{1}]$, with $\gamma_2=-\sqrt[3]{1}$.[4]

Let V denote the galois module of 19-division points of J. Then V is a vector space of dimension 4 over the field with 19 elements. In the discussion to follow, all vector spaces will be over this field.

The vector space V is canonically a G-module, and possesses a G-compatible action of Δ. Denote by $V(1) \subset V$ the subspace of dimension 1 given by the cyclic group $T \subset J$ of 19 rational points. Then G acts trivially on $V(1)$.

Let $19=\pi\bar{\pi}$ denote a decomposition of 19 as a product of prime elements in the ring $\mathbb{Z}[\gamma_2] \approx \mathbb{Z}[\sqrt[3]{1}]$. Since π and $\bar{\pi}$ are relatively prime the space V decomposes accordingly into the direct sum of the kernels of π and $\bar{\pi}$:

$$V=V_\pi \oplus V_{\bar{\pi}}.$$

The subspaces V_π and $V_{\bar{\pi}}$ are easily seen to be stable under the actions of G and of Γ, but they are interchanged under any τ_ζ. Indeed, the map $\xi \to \tau_\zeta \xi \tau_\zeta$ is a non-trivial automorphism of $\mathbb{Z}[\gamma_2]$ and consequently $\tau_\zeta \pi = \bar{\pi} \tau_\zeta$.

The subspace $V(1)$ is contained in one of the two subspaces V_π and $V_{\bar{\pi}}$ because it is stable under γ_2. Interchanging π and $\bar{\pi}$ if necessary, we can assume

$$V(1) \subset V_{\bar{\pi}}.$$

[4] As Serre remarked, $D \otimes \mathbb{Q} \simeq \mathbf{M}_2(\mathbb{Q})$, the algebra of 2×2 matrices over $\mathbb{Q}$. Consequently J is not irreducible over any field over which the action of Δ is rational.

We now define a subspace $V(\gamma)\subset V$ which is stable under the action of G and of Γ.

$$V(\gamma)=\{v\in V \mid v^{\alpha}=\gamma_{\alpha}v, \text{ for all } \alpha\in G\}.$$

Claim 1. *For any ζ, τ_ζ interchanges the subspaces $V(1)$ and $V(\gamma)$.*

One proves the above claim, in one direction, by the calculation

$$(\tau_\zeta v)^{\alpha}=(\tau_\zeta)^{\alpha}v^{\alpha}=\gamma_{\alpha}\tau_\zeta v^{\alpha}=\gamma_{\alpha}(\tau_\zeta v)$$

if $v\in V(1)$, and in the other direction similarly.

Claim 2. *The self-duality of V induces a (Cartier) duality between the Galois modules V_π and $V_{\bar\pi}$.*

Since each of these spaces is of dimension 2 and their sum is V, it suffices to show that they are self orthogonal under the canonical pairing of V with itself to the Galois module of 19-th roots of unity (the "e_{19}-pairing" of Weil). We denote this pairing simply by $(\ ,\ )$. We have

$$(\gamma_2 u, \gamma_2 v)=(u, v)$$

because γ_2 must induce the identity on the 2-dimensional cohomology of our curve X. On the other hand, V_π and $V_{\bar\pi}$ are eigenspaces for γ_2, with eigenvalues the two primitive 6-th roots of unity in the field $\mathbb{Z}/19$. Since the square of a primitive sixth root of unity is not 1, our claim follows.

Corollary. *Let $V(\chi)$ denote the Galois module of* 19-th *roots of unity. There is a short exact sequence of G-modules as follows:*

$$0\to V(\gamma)\to V_\pi \xrightarrow{b} V(\chi)\to 0.$$

Take the map b to be the Cartier dual of the inclusion $V(1)\hookrightarrow V_{\bar\pi}$. By Claim 1 we know that $V(\gamma)$ is a one-dimensional subspace of V_π. Hence our corollary will be proven if we can show that $V(\gamma)$ is in the kernel of b. For this it suffices to show that $V(\gamma)$ and $V(\chi)$ are not isomorphic. But they certainly are not, since $\mathrm{Gal}(\mathbb{Q}(\sqrt[13]{1})^{+}/\mathbb{Q})$ acts faithfully on $V(\gamma)$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt[9]{1})/\mathbb{Q})$ acts faithfully on $V(\chi)$.

4. The Descent

We shall now use our analysis of the Galois structure of the 19-division points of J to prove

Theorem. *There are precisely* 19 *rational points on J. There are no rational points on X other than its six rational cusps.*

Corollary. *There is no elliptic curve defined over $\mathbb{Q}$ possessing a rational point of order* 13.[5]

[5] It is, however, extremely easy to find *isogenies* of order 13 of elliptic curves defined over $\mathbb{Q}$: they form a parametrizable family since $X_0(13)$ is of genus zero.

The theorem is proved by a π-descent (cf. [3]). Let $S=(\operatorname{Spec}\mathbb{Z})-(13)$ be the open subscheme of $\operatorname{Spec}\mathbb{Z}$ obtained by removing the closed point 13. Let A be the abelian scheme over S with generic fiber J. We have a short exact sequence of group schemes over S

$$0\to F\to A\xrightarrow{\pi}A\to 0$$

where $F=A_\pi$ is a finite flat group scheme of order 19^2 whose generic fiber corresponds to the Galois module $V=J_\pi$.

Proposition. *The map π induces a surjection on $A(S)$.*

The theorem follows from the proposition. Indeed, the group $A(S)\approx J(\mathbb{Q})$ is finitely generated ("Mordell-Weil Theorem") and a finitely generated $\mathbb{Z}[\sqrt[3]{1}]$-module on which π acts surjectively is finite. Thus the proposition implies $J(\mathbb{Q})$ is finite, hence of order 19 by the result quoted above. The assertion about X also follows from a result of Ogg mentioned above, namely, that $X\cap T$ consists of precisely the six rational cusps.

Let $P=\operatorname{Spec}\mathbb{Q}_{13}$. Then P is an S-scheme, and we have a commutative diagram with exact rows

$$\begin{array}{ccccc}
A(S) & \xrightarrow{\pi} & A(S) & \longrightarrow & H^1(S,F)\\
\downarrow & & \downarrow & & \downarrow{\scriptstyle\rho}\\
A(P) & \xrightarrow{\pi} & A(P) & \longrightarrow & H^1(P,F)
\end{array}$$

where cohomology means f.p.p.f. cohomology. From this diagram it is clear that to prove the proposition it suffices to prove two things:

(i) π acts surjectively on $A(P)$.

(ii) ρ is injective.

Proof of (i). Let $\mathscr{A}$ denote the Néron model of J over $\mathbb{Z}_{13}$, and let N be the kernel of the reduction map $\mathscr{A}(\mathbb{Z}_{13})\to\mathscr{A}(\mathbb{Z}/13)$. Then N is a pro-13-group on which 19, and hence π, must act bijectively. Since N is of finite index in $\mathscr{A}(\mathbb{Z}_{13})=A(P)$, and since an endomorphism of a finite group is surjective if and only if it is injective, we are reduced to showing that π acts injectively on $A(P)=J(\mathbb{Q}_{13})$, i.e. that $(V_\pi)^D=0$, where D is a 13-decomposition subgroup of G. By the corollary in § 3 it suffices to note that both $V(\chi)^D=0$ and $V(\gamma)^D=0$, i.e. that 13 does not split completely either in the field $\mathbb{Q}(\sqrt[9]{1})$ (because $13\not\equiv 1 \pmod{19}$) or in the maximal real subfield of $\mathbb{Q}(\sqrt[13]{1})$ (because 13 ramifies).

Proof of (ii). Let $T=\operatorname{Spec}\mathbb{Z}[\sqrt[13]{1}, 13^{-1}]$ be the normalization of S in $\mathbb{Q}(\sqrt[13]{1})$. Note that $T\to S$ is étale.

Lemma. *There is a short exact sequence of S-group schemes*

$$0 \to E \to F \to \mu_{19} \to 0$$

where E is a finite étale group scheme over S whose restriction to T is isomorphic to $\mathbb{Z}/19$.

Let E be the Zariski closure in A of $V(\gamma)$, regarded as a finite subgroup of J. Then E is a finite flat closed subgroup of F, and the quotient F/E has generic fiber corresponding to the Galois module $V(\chi)$. Thus F/E and μ_{19} have isomorphic generic fibers, and so do $E|T$ and $\mathbb{Z}/19$. The lemma now follows from the fact that a finite flat group scheme of prime order p over U is determined by its generic fiber, if U is an open subset of the spectrum of the ring of integers in a number field such that each point of U above p has absolute ramification index $<p-1$. This fact is a corollary of Theorem 3 of [5]; the key point is already the purely local theorem of [5], which shows that with the ramification so limited, there is only one group scheme over each local ring which is compatible with a given group scheme over its field of fractions.

Now consider the exact commutative diagram

$$\begin{array}{ccccc} H^1(S,E) & \longrightarrow & H^1(S,F) & \longrightarrow & H^1(S,\mu_{19}) \\ & & \Big\downarrow \rho & & \Big\downarrow \rho' \\ & & H^1(P,F) & \longrightarrow & H^1(P,\mu_{19}). \end{array}$$

It shows that to prove (ii), i.e. ρ injective, it suffices to prove two things:

(ii a) ρ' is injective.

(ii b) $H^1(S,E)=0$.

To prove (ii a) we use the exact sequence

$$0 \longrightarrow \mu_{19} \longrightarrow \mathbb{G}_m \xrightarrow{19} \mathbb{G}_m \longrightarrow 0.$$

Since $H^1(S,\mathbb{G}_m)=\operatorname{Pic} S=0$ and similarly $H^1(P,\mathbb{G}_m)=0$, we are reduced to showing

$$\mathbb{G}_m(S)/19\,\mathbb{G}_m(S) \to \mathbb{G}_m(\mathbb{Q}_{13})/19\,\mathbb{G}_m(\mathbb{Q}_{13})$$

is injective. This is true, because $\mathbb{G}_m(S)=(\pm 13^n)_{n\in\mathbb{Z}}$, and 13 is not a 19-th power in $\mathbb{Q}_{13}$.

To prove (ii b) we note that

$$H^1(S,E)=H^1(T,E)^{\mathrm{Gal}(T/S)}$$

because T/S is Galois of degree 12 prime to 19. Hence it suffices to show $H^1(T,E)=H^1(T,\mathbb{Z}/19)=0$. This amounts to the fact that T has no connected étale Galois covering of degree 19, i.e. that the field $K=\mathbb{Q}(\sqrt[13]{1})$ has no abelian extension of degree 19 unramified outside the prime λ above 13. This is true by class field theory, because the class number of K is prime to 19 (in fact it is 1; cf. [2]), and the group of λ-adic units is divisible by 19 (because it has a subgroup of index $13-1=12$ which is a pro-13-group).

Remarks. 1. It is of interest to list the main ingredients (apart from our analysis of 19-division points) which make the argument work:

(a) 13 and 19 are distinct primes.

(b) $13 \not\equiv 1 \bmod 19$.

(c) the class number of $\mathbb{Q}(\zeta_{13})$ is prime to 19.

2. We performed our descent over the base $S=\operatorname{Spec}\mathbb{Z}-(13)$ in order to deal solely with *finite* flat group schemes. We might have worked directly over $\operatorname{Spec}\mathbb{Z}$, in which case we would have been dealing with *quasi*-finite group schemes, but we could have avoided any special appeal to $\mathbb{Q}_{13}$. Such an argument yields easily the following extra bit of information: multiplication by π induces an injection on the Shafarevitch group of J over $\mathbb{Q}$.

5. An Afterthought

When you study $X_1(n)$, you find yourself quite naturally led to certain twisted forms of the curve $X_1(n)$, which become isomorphic to $X_1(n)$ over K^+. These can easily be defined explicitly, or by the following succinct modular description:

Let η be any integer mod $\varphi(n)/2$. Set $X^\eta = X_1^\eta(n)$ to be the complete curve over $\mathbb{Q}$ which is obtained from considering the following moduli problem.

Classify pairs

$$x\colon\ \mu_n^{\otimes\eta} \overset{\beta}{\hookrightarrow} E \qquad \text{where } \mu_n^{\otimes\eta} = \mu_n \otimes \overset{\eta \text{ times}}{\cdots} \otimes \mu_n.$$

We then have operators: $\tau\colon X^\eta \to X^{1-\eta}$, by setting τx to be

$$\tau x\colon\ \mu_n^{\otimes(1-\eta)} \overset{\bar{\beta}}{\hookrightarrow} \bar{E}$$

where $\bar{E}=E/\text{image}(\beta)$, as before.

Now specialize again to the case $n=13$. Over the field $\mathbb{Q}(\sqrt{13})$, the isomorphism class of X^η depends only on η mod 3 and so specializing to $\eta=2$ we have an involution:

$$\omega = \text{“}\tau\text{”}\colon\ X^2 \to X^2$$

defined over $\mathbb{Q}(\sqrt{13})$. This involution determines an involution of the Jacobian $\omega\colon J^2 \to J^2$. It is not too hard to see that the $+1$ and -1 eigenspaces of this involution ω are elliptic curves in J^2 which are conjugate over $\mathbb{Q}$, and isogenous. This indicates that our abelian variety of dimension 2 is actually, up to isogeny, a product of two elliptic curves over K^+.

References

1. Blass, J.: Points of order 13 on elliptic curves. (A. M. S. Announcement)
2. Masley, J.: On the class number of abelian number fields. Ph. D. dissertation. Princeton University, 1972
3. Mazur, B.: Rational points on abelian varieties with values in towers of number fields. Inventiones math. **18**, 183–266 (1972)
4. Ogg, A.: Rational points on certain elliptic modular curves. Talk given at AMS Symposium on Analytic Number Theory and Related Parts of Analysis. St. Louis, 1972. Mimeographed notes, Berkeley
5. Oort, F., Tate, J.: Group schemes of prime order. Annales Scient. de l'Ecole Norm. Sup., 4^e serie T.3, fasc. 1, 1–21 (1970)
6. Weil, A.: Variétés abéliennes et courbes algébriques, Publications de l'Institut de Mathématique de l'Université de Strasbourg (1948). Paris: Hermann Cie

Barry Mazur
John Tate
Department of Mathematics
Harvard University
1 Oxford Street
Cambridge, MA 02138, USA

(Received May 14, 1973)