

Rational points on $X(11)$ over $\mathbf{Q}(\mu_{11})$ via Galois equivariance of the Cassels-Tate pairing

Tom Fisher

April 11, 2001

Abstract

We show that the elliptic curves of conductor 11 have Mordell-Weil rank zero over the cyclotomic field $\mathbf{Q}(\mu_{11})$. Our method makes use of the Galois equivariance of the Cassels-Tate pairing, and does not require any computer calculations. As an application we find all rational points on the modular curve $X(11)$ over $\mathbf{Q}(\mu_{11})$. With a modest amount of computer calculation we extend our results to the field $\mathbf{Q}(\mu_5)\mathbf{Q}(\mu_{11})^+$.

1 The elliptic curves of conductor 11

The elliptic curves over \mathbf{Q} with conductor 11 are

$$\begin{array}{lll} A_0 = X_0(11) & y^2 + y = x^3 - x^2 - 10x - 20 & 11A1 \\ A_1 = X_1(11) & y^2 + y = x^3 - x^2 & 11A3 \\ A_2 & y^2 + y = x^3 - x^2 - 7820x - 263580 & 11A2 \end{array}$$

Here the labels 11A1-3 are those used in [Cr], whereas the labels A_0, A_1, A_2 are taken from [CS]. When there is no need to distinguish the three curves we shall simply write A to denote any one of them. From Cremona [Cr] we learn that there are isogenies of degree 5 defined over \mathbf{Q}

$$A_1 \rightleftarrows A_0 \rightleftarrows A_2 \tag{1}$$

with

$$\begin{aligned} \ker(A_1 \rightarrow A_0) &\simeq \mathbf{Z}/5\mathbf{Z} \\ \ker(A_0 \xrightarrow{\times 5} A_0) &\simeq \mu_5 \oplus \mathbf{Z}/5\mathbf{Z} \\ \ker(A_2 \rightarrow A_0) &\simeq \mu_5. \end{aligned}$$

The modular curve $A_1 = X_1(11)$ has 10 cusps. There are 5 cusps defined over \mathbf{Q} and 5 defined over $\mathbf{Q}(\mu_{11})^+ := \mathbf{Q}(\mu_{11}) \cap \mathbf{R}$. Naturally we take the point at infinity on A_1 to be one of the rational cusps. The irrational cusps generate a cyclic subgroup \mathcal{C} of order 25. We write $\rho : G_{\mathbf{Q}} \rightarrow (\mathbf{Z}/25\mathbf{Z})^*$ for the character defined by $\sigma(P) = \rho(\sigma)P$ for all $P \in \mathcal{C}$. In fact \mathcal{C} is the kernel of the isogeny $A_1 \rightarrow A_0 \rightarrow A_2$ of degree 25. We deduce that ρ takes values congruent to 1 mod 5.

2 Explicit descent via 5-isogeny

We aim to compute the rank of the elliptic curves A over certain number fields F . We begin by giving a description of the Selmer groups attached to the 5-isogenies (1). By definition they are subgroups of $H^1(F, \mu_5) = F^*/F^{*5}$ and $H^1(F, \mathbf{Z}/5\mathbf{Z}) = \text{Hom}(G_F, \mathbf{Z}/5\mathbf{Z})$.

Proposition 2.1 *Let F be a number field. Then*

$$\begin{aligned} S(A_0 \rightarrow A_1/F) &\simeq \left\{ \theta \in F^*/F^{*5} \mid \begin{array}{l} \text{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod{5} \text{ for all } \mathfrak{p} \\ \text{and } F(\sqrt[5]{\theta})/F \text{ split at } \mathfrak{p} \mid 11 \end{array} \right\} \\ S(A_1 \rightarrow A_0/F) &\simeq \left\{ \chi \in \text{Hom}(G_F, \mathbf{Z}/5\mathbf{Z}) \mid \chi \text{ unramified at all } \mathfrak{p} \nmid 11 \right\} \\ S(A_2 \rightarrow A_0/F) &\simeq \left\{ \theta \in F^*/F^{*5} \mid \text{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod{5} \text{ for all } \mathfrak{p} \nmid 11 \right\} \\ S(A_0 \rightarrow A_2/F) &\simeq \left\{ \chi \in \text{Hom}(G_F, \mathbf{Z}/5\mathbf{Z}) \mid \begin{array}{l} \chi \text{ unramified at all } \mathfrak{p} \\ \text{and } \chi \text{ split at } \mathfrak{p} \mid 11 \end{array} \right\} \end{aligned}$$

(Here χ split at \mathfrak{p} means \mathfrak{p} splits in the fixed field of the kernel of χ .)

Proof. More generally in [F1] we considered pairs of 5-isogenous elliptic curves C_λ and D_λ with $\ker(C_\lambda \rightarrow D_\lambda) \simeq \mu_5$ and $\ker(D_\lambda \rightarrow C_\lambda) \simeq \mathbf{Z}/5\mathbf{Z}$. For each prime \mathfrak{p} there is an exact sequence

$$C_\lambda(F_{\mathfrak{p}}) \longrightarrow D_\lambda(F_{\mathfrak{p}}) \xrightarrow{\delta_{\mathfrak{p}}} F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*5}.$$

We recall [F1, Propositions 2.15 and 2.16] that $\delta_{\mathfrak{p}}$ has image

$$\text{im } \delta_{\mathfrak{p}} = \begin{cases} F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*5} & \text{if } \text{ord}_{\mathfrak{p}}(\lambda) \neq 0 \\ \mathfrak{O}_{\mathfrak{p}}^*/\mathfrak{O}_{\mathfrak{p}}^{*5} & \text{if } \text{ord}_{\mathfrak{p}}(\lambda) = \text{ord}_{\mathfrak{p}}(\lambda^2 - 11\lambda - 1) = 0 \\ 1 & \text{if } \text{ord}_{\mathfrak{p}}(\lambda^2 - 11\lambda - 1) > 0 \text{ and } \mathfrak{p} \nmid 5. \end{cases} \quad (2)$$

We further recall that our co-ordinate λ on $X_1(5)$ was chosen such that D_λ has Weierstrass equation

$$y^2 + (1 - \lambda)xy - \lambda y = x^3 - \lambda x^2. \quad (3)$$

We see that $A_1 = D_1$ and $A_0 = D_{11}$. The descriptions of $S(A_0 \rightarrow A_1/F)$ and $S(A_2 \rightarrow A_0/F)$ now follow from (2) on taking $\lambda = 1$, respectively $\lambda = 11$. Tate local duality tells us that the images of the local connecting maps attached to an isogeny and its dual are exact annihilators with respect to the Tate pairing. The descriptions of $S(A_1 \rightarrow A_0/F)$ and $S(A_0 \rightarrow A_2/F)$ follow. \square

Suppose F is number field for which we have a working knowledge of the unit group and the class group. It is now a straightforward exercise in Kummer theory to compute the Selmer groups $S(A_0 \rightarrow A_1/F)$ and $S(A_2 \rightarrow A_0/F)$. If $\mu_5 \subset F$, then the Selmer groups attached to the dual isogenies may be treated similarly. However there is a better way.

Proposition 2.2 *Let F be a number field with r_1 (resp. r_2), real (resp. pairs complex conjugate) embeddings and m primes above 11. Then*

$$\frac{\#S(A_0 \rightarrow A_1/F)}{\#S(A_1 \rightarrow A_0/F)} = \#\mu_5(F) \times 5^{r_1+r_2-1} \times 5^{-m}$$

$$\frac{\#S(A_2 \rightarrow A_0/F)}{\#S(A_0 \rightarrow A_2/F)} = \#\mu_5(F) \times 5^{r_1+r_2-1} \times 5^m.$$

Proof. This is an application of Cassels' formula [Ca2, Theorem 1.1]. Let us note that for $\mathfrak{p}|11$, inspection of the j -invariants shows that the Tamagawa factors are $c_{\mathfrak{p}}(A_0) = 5 \operatorname{ord}_{\mathfrak{p}}(11)$ and $c_{\mathfrak{p}}(A_1) = c_{\mathfrak{p}}(A_2) = \operatorname{ord}_{\mathfrak{p}}(11)$. At each infinite place, it follows by Vélú's formulae [V1] that the periods Ω_i are related via $\Omega_1/\Omega_0 = \Omega_0/\Omega_2 = 5$. \square

Remark 2.3 In simple cases, for example if F has class number 1, it is a tolerable exercise in class field theory to deduce Proposition 2.2 directly from Proposition 2.1. The beauty of Cassels' formula is that the class number of F does not appear.

We shall also require a description of the Selmer group attached to the cyclic isogeny $A_2 \rightarrow A_1$ of degree 25.

Proposition 2.4 *Let F be a number field containing $\mathbf{Q}(\mu_{11})^+$. Then*

$$S(A_2 \rightarrow A_1/F) \simeq \left\{ \theta \in F^*/F^{*25} \mid \begin{array}{l} \text{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod{25} \text{ for all } \mathfrak{p} \nmid 11 \\ \text{and } \theta \in F_{\mathfrak{p}}^{*5} \text{ for all } \mathfrak{p} \mid 11 \end{array} \right\}$$

Proof. Since F contains $\mathbf{Q}(\mu_{11})^+$ we have

$$\begin{aligned} \ker(A_1 \rightarrow A_2) &\simeq \mathbf{Z}/25\mathbf{Z} \\ \ker(A_2 \rightarrow A_1) &\simeq \mu_{25}. \end{aligned}$$

Thus $S(A_2 \rightarrow A_1/F) \subset H^1(G_F, \mu_{25}) = F^*/F^{*25}$. Our description of this Selmer group is no more than one would expect upon generalising [F1, Theorem 1] from curves parametrised by $X_1(5)$ to curves parametrised by $X_1(25)$. In the interests of brevity we take a rather more *ad hoc* approach. For each prime \mathfrak{p} we consider the diagram

$$\begin{array}{ccccc} A_2(F_{\mathfrak{p}}) & \longrightarrow & A_0(F_{\mathfrak{p}}) & \xrightarrow{\delta_{20}} & F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*5} \\ \parallel & & \downarrow & & \downarrow \\ A_2(F_{\mathfrak{p}}) & \longrightarrow & A_1(F_{\mathfrak{p}}) & \xrightarrow{\delta_{21}} & F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*25} \\ \downarrow & & \parallel & & \downarrow \\ A_0(F_{\mathfrak{p}}) & \longrightarrow & A_1(F_{\mathfrak{p}}) & \xrightarrow{\delta_{01}} & F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*5} \end{array}$$

and claim that

$$\text{im } \delta_{21} = \begin{cases} F_{\mathfrak{p}}^{*5}/F_{\mathfrak{p}}^{*25} & \text{if } \mathfrak{p} \mid 11 \\ \mathfrak{O}_{\mathfrak{p}}^*/\mathfrak{O}_{\mathfrak{p}}^{*25} & \text{if } \mathfrak{p} \nmid 11. \end{cases} \quad (4)$$

Indeed if $\mathfrak{p} \mid 11$ we saw in the proof of Proposition 2.1 that $\text{im } \delta_{20} = F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*5}$ whereas $\text{im } \delta_{01} = 1$. A straightforward diagram chase now gives $\text{im } \delta_{21} = F_{\mathfrak{p}}^{*5}/F_{\mathfrak{p}}^{*25}$ as required. Now suppose $\mathfrak{p} \nmid 11$. The proof of Proposition 2.1 gives $\text{im } \delta_{20} = \text{im } \delta_{01} = \mathfrak{O}_{\mathfrak{p}}^*/\mathfrak{O}_{\mathfrak{p}}^{*5}$. A diagram chase convinces us it is enough to show $\text{im } \delta_{21} \supset \mathfrak{O}_{\mathfrak{p}}^*/\mathfrak{O}_{\mathfrak{p}}^{*25}$. By Tate local duality this is equivalent to showing $\text{im } \delta_{12}$ consists of unramified cocycles. But the latter follows by a standard argument [S, Theorem 4.2], since $\ker(A_1 \rightarrow A_2) \simeq \mathbf{Z}/25\mathbf{Z}$ has trivial intersection with the formal group mod \mathfrak{p} . Indeed A_1 has minimal Weierstrass equation $y^2 + y = x^3 - x^2$ and $\ker(A_1 \rightarrow A_0) \simeq \mathbf{Z}/5\mathbf{Z}$ is generated by $(x, y) = (0, 0)$. This completes the proof of (4) and the proposition follows. \square

3 Initial estimates for the rank over $\mathbf{Q}(\mu_{11})$

Let $F = \mathbf{Q}(\mu_{11})$ and let τ in $\text{Gal}(F/\mathbf{Q})$ be an element of order 5. It is well known that F has class number 1, and that the only units in F are cyclotomic units. Explicitly, writing $e_0 = \zeta_{11} - \zeta_{11}^{-1}$ and $e_i = \tau^i(e_0)$, a set of fundamental units is $e_0/e_1, e_1/e_2, e_2/e_3, e_3/e_4$. We also note that e_0 generates the unique prime above 11. It is an easy exercise to deduce from Propositions 2.1 and 2.2 that

$$\begin{aligned} S(A_0 \rightarrow A_1/F) &\simeq (\mathbf{Z}/5\mathbf{Z})^3 \\ S(A_1 \rightarrow A_0/F) &= 0 \end{aligned} \tag{5}$$

and

$$\begin{aligned} S(A_2 \rightarrow A_0/F) &\simeq (\mathbf{Z}/5\mathbf{Z})^5 \\ S(A_0 \rightarrow A_2/F) &= 0. \end{aligned} \tag{6}$$

We know A_1 has a cyclic subgroup of order 25 defined over F . Reducing modulo a couple of primes, say 23 and 67, the Hasse bounds are sufficient to prove

$$A_1(F)_{\text{tors}} \simeq \mathbf{Z}/25\mathbf{Z}.$$

Since $\mathbf{Q}(A_2[5]) = \mathbf{Q}(\mu_5, \sqrt[5]{11})$ is linearly disjoint from F it follows

$$A_0(F)_{\text{tors}} \simeq \mathbf{Z}/5\mathbf{Z} \quad \text{and} \quad A_2(F)_{\text{tors}} = 0.$$

Taking these torsion contributions into account, the estimates for rank $A(F)$ given by (5) and (6) are 2 and 4 respectively. We shall improve on these estimates by making use of the Cassels-Tate pairing.

4 Preliminaries on the Cassels-Tate pairing

Let E and E' be elliptic curves defined over a number field F . Let $\psi : E \rightarrow E'$ be an isogeny of degree m , with dual isogeny $\widehat{\psi} : E' \rightarrow E$. There is an exact sequence of G_F -modules

$$0 \longrightarrow E'[\widehat{\psi}] \longrightarrow E'[m] \xrightarrow{\widehat{\psi}} E[\psi] \longrightarrow 0.$$

Taking Galois cohomology and restricting to Selmer groups we obtain an exact sequence

$$E[\psi](F) \longrightarrow S(E' \rightarrow E/F) \longrightarrow S(E' \xrightarrow{\times m} E'/F) \longrightarrow S(E \rightarrow E'/F).$$

Proposition 4.1 (Cassels-Tate pairing) *Let $E \rightarrow E'$ be as above.*

(i) *There is an alternating pairing \langle , \rangle on $S(E \rightarrow E'/F)$ taking values in \mathbf{Q}/\mathbf{Z} whose kernel is the image of $S(E' \xrightarrow{\times m} E'/F)$.*

(ii) *If we have isogenies $E \rightarrow E' \rightarrow E''$ then the pairings on $S(E \rightarrow E'/F)$ and $S(E \rightarrow E''/F)$ are compatible.*

(iii) *Suppose E, E', ψ are defined over $F_0 \subset F$. If F is a normal extension of F_0 then the pairing \langle , \rangle on $S(E \rightarrow E'/F)$ is $\text{Gal}(F/F_0)$ -equivariant. It is to be understood that the Galois action on \mathbf{Q}/\mathbf{Z} is trivial.*

Proof. See Cassels [Ca1] or Milne [Mi]. □

This theorem has an even better known corollary.

Corollary 4.2 *Let F be a number field and E/F an elliptic curve. There is an alternating pairing \langle , \rangle on $\text{III}(E/F)$ taking values in \mathbf{Q}/\mathbf{Z} whose kernel is the divisible subgroup of $\text{III}(E/F)$.*

For our calculations we also require

Proposition 4.3 *Let $\psi : E_1 \rightarrow E_2$ be an isogeny of elliptic curves over a number field F . Then ψ and $\widehat{\psi}$ are adjoints with respect to the Cassels-Tate pairing, i.e. $\langle \psi x, y \rangle_2 = \langle x, \widehat{\psi} y \rangle_1$ for all $x \in \text{III}(E_1/F)$ and $y \in \text{III}(E_2/F)$.*

Proof. See Cassels [Ca2, Theorem 1.2]. □

5 An application of Galois equivariance

Again we take $F = \mathbf{Q}(\mu_{11})$ and τ in $\text{Gal}(F/\mathbf{Q})$ an element of order 5.

Proposition 5.1 *Let $F = \mathbf{Q}(\mu_{11})$.*

(i) *The Cassels-Tate pairing on $S(A_2 \rightarrow A_0/F) \simeq (\mathbf{Z}/5\mathbf{Z})^5$ has rank 2.*

(ii) *The Cassels-Tate pairing on $S(A_0 \rightarrow A_1/F) \simeq (\mathbf{Z}/5\mathbf{Z})^3$ has rank 2.*

Proof. (i) We consider the exact sequences

$$0 \longrightarrow S(A_0 \rightarrow A_1/F) \longrightarrow S(A_0 \xrightarrow{\times 5} A_0/F) \longrightarrow S(A_1 \rightarrow A_0/F) \quad (7)$$

$$0 \longrightarrow S(A_0 \rightarrow A_2/F) \longrightarrow S(A_0 \xrightarrow{\times 5} A_0/F) \longrightarrow S(A_2 \rightarrow A_0/F) \quad (8)$$

From (7) we learn that $S(A_0 \xrightarrow{\times 5} A_0/F) \simeq (\mathbf{Z}/5\mathbf{Z})^3$. Then (8) and Proposition 4.1(i) tell us the Cassels-Tate pairing on $S(A_2 \rightarrow A_0/F)$ has rank 2.

(ii) We shall use the Galois equivariance of the Cassels-Tate pairing to deduce this from (i). Let us note that it is sufficient to show that the pairing on $S(A_0 \rightarrow A_1/F)$ is non-zero. We consider the exact sequence

$$0 \longrightarrow S(A_2 \rightarrow A_0/F) \longrightarrow S(A_2 \rightarrow A_1/F) \longrightarrow S(A_0 \rightarrow A_1/F). \quad (9)$$

By Propositions 2.1 and 2.4 we have

$$\begin{aligned} S(A_2 \rightarrow A_0/F) &= \langle e_0, e_1, e_2, e_3, e_4 \rangle && \subset F^*/F^{*5} \\ S(A_2 \rightarrow A_1/F) &= \langle e_0e_1^{-2}e_2, e_1e_2^{-2}e_3, e_2e_3^{-2}e_4, e_3^5, e_4^5 \rangle && \subset F^*/F^{*25} \\ S(A_0 \rightarrow A_1/F) &= \langle e_0e_1^{-2}e_2, e_1e_2^{-2}e_3, e_2e_3^{-2}e_4 \rangle && \subset F^*/F^{*5}. \end{aligned}$$

In particular (9) is exact on the right. Let

$$R := \mathbf{Z}_5[\tau] = \mathbf{Z}_5[X]/(X^5 - 1).$$

Then the group

$$\widehat{F} := F^* \otimes \mathbf{Z}_5 = \varprojlim F^*/F^{*5^n}$$

which we write additively, has a natural structure of R -module. Let $M \subset \widehat{F}$ be the R -module generated by $e_0 = \zeta_{11} - \zeta_{11}^{-1}$ and let $N = (\tau - 1)^2M$. Then (9) yields an exact sequence of R -modules

$$0 \longrightarrow M/5M \xrightarrow{\times 5} (N + 5M)/25M \longrightarrow (N + 5M)/5M \longrightarrow 0. \quad (10)$$

These groups admit alternating pairings $\langle \cdot, \cdot \rangle_{20}$, $\langle \cdot, \cdot \rangle_{21}$ and $\langle \cdot, \cdot \rangle_{01}$.

Lemma 5.2 *The pairings $\langle \cdot, \cdot \rangle_{**}$ are related via*

(i) $\langle x, y \rangle_{20} = \langle 5x, 5y \rangle_{21}$ for all $x, y \in M$.

(ii) $\langle x, y \rangle_{01} = \langle x, 5y \rangle_{21}$ for all $x, y \in N + 5M$.

Proof. (i) This is immediate by Proposition 4.1(ii).

(ii) Let ψ be the 5-isogeny $A_2 \rightarrow A_0$. By Proposition 4.3, $\langle \psi x, z \rangle_0 = \langle x, \widehat{\psi} z \rangle_2$. Writing $z = \psi y$ and noting that our identification of the exact sequences (9) and (10) suppresses the map ψ , we conclude $\langle x, y \rangle_{01} = \langle x, 5y \rangle_{21}$ as required. \square

Lemma 5.3 *There is a unit $u \in R$ such that $\tau - 1$ and $u(\tau - 1)$ are adjoints with respect to the pairings $\langle \cdot, \cdot \rangle_{20}$ and $\langle \cdot, \cdot \rangle_{01}$. For the pairing $\langle \cdot, \cdot \rangle_{21}$ we again have*

$$\langle (\tau - 1)x, y \rangle_{21} = \langle x, u(\tau - 1)y \rangle_{21}$$

provided y belongs to $(\tau - 1)\widehat{F}$.

Proof. For \langle, \rangle_{20} and \langle, \rangle_{01} this is immediate by Proposition 4.1(iii). Indeed $\tau-1$ and $\tau^{-1}-1$ are adjoints, and τ is a unit. For \langle, \rangle_{21} we should take slightly more care, since the identification of (9) and (10) does not respect the natural Galois module structures. In fact there is a twist by the character ρ defined in §1. Since ρ takes values congruent to 1 mod 5 and $5(\tau-1)R = (\tau-1)^5R$, the lemma follows as before. \square

Now $M/(\tau-1)M \simeq \mathbf{Z}_5$ and the pairing \langle, \rangle_{20} is alternating, so

$$\langle, \rangle_{20} \text{ is non-zero} \iff \langle(\tau-1)M, M\rangle_{20} \neq 0. \quad (11)$$

Similarly $N/(\tau-1)N \simeq \mathbf{Z}_5$ and $N = (\tau-1)^2M$ give

$$\langle, \rangle_{01} \text{ is non-zero} \iff \langle(\tau-1)^3M, (\tau-1)^2M\rangle_{01} \neq 0. \quad (12)$$

With these preliminaries we compute

$$\begin{aligned} & \langle(\tau-1)^2M, (\tau-1)^3M\rangle_{01} &= 0 \\ \iff & \langle(\tau-1)^2M, 5(\tau-1)^3M\rangle_{21} &= 0 && \text{by Lemma 5.2(ii)} \\ \iff & \langle(\tau-1)^5M, 5M\rangle_{21} &= 0 && \text{by Lemma 5.3} \\ \iff & \langle 5(\tau-1)M, 5M\rangle_{21} &= 0 && \text{since } 5(\tau-1)R = (\tau-1)^5R \\ \iff & \langle(\tau-1)M, M\rangle_{20} &= 0 && \text{by Lemma 5.2(i)} \end{aligned}$$

Now (11) and (12), together with this last calculation, show that Proposition 5.1(ii) follows from Proposition 5.1(i). \square

6 Conclusions over $\mathbf{Q}(\mu_{11})$

Let $F = \mathbf{Q}(\mu_{11})$. We now have enough information to compute the groups $A(F)$ and $\text{III}(A/F)(5)$. First we consider the exact sequence

$$0 = S(A_1 \rightarrow A_0/F) \longrightarrow S(A_1 \xrightarrow{\times 5} A_1/F) \longrightarrow S(A_0 \rightarrow A_1/F).$$

By Propositions 4.1(i) and 5.1(ii) we have $S(A_1 \xrightarrow{\times 5} A_1/F) \simeq \mathbf{Z}/5\mathbf{Z}$. We deduce $\text{rank } A(F) = 0$ and $\text{III}(A_1/F)(5) = 0$. The exact sequence (7) gives $S(A_0 \xrightarrow{\times 5} A_0/F) \simeq (\mathbf{Z}/5\mathbf{Z})^3$. By Propositions 4.1(ii) and 5.1(ii) the Cassels-Tate pairing on this Selmer group has rank 2. Thus $\text{III}(A_2/F)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^2$. Finally the exact sequence

$$0 \longrightarrow \mathbf{Z}/5\mathbf{Z} \longrightarrow S(A_2 \rightarrow A_0/F) \longrightarrow S(A_2 \xrightarrow{\times 5} A_2/F) \longrightarrow S(A_0 \rightarrow A_2/F)$$

tells us that $S(A_2 \xrightarrow{\times 5} A_2/F) \simeq (\mathbf{Z}/5\mathbf{Z})^4$ but that the Cassels-Tate pairing on this Selmer group only has rank 2. Since the multiplication by 25 map on A_2 factors through A_1 , and we have already shown $\text{III}(A_1/F)(5) = 0$, we deduce that $\text{III}(A_2/F)(5)$ has exponent 25. We summarise our results

Theorem 1 *Let $F = \mathbf{Q}(\mu_{11})$ or $\mathbf{Q}(\mu_{11})^+$. Then*

$$\begin{aligned} A_0(F) &\simeq \mathbf{Z}/5\mathbf{Z} & \text{III}(A_0/F)(5) &\simeq (\mathbf{Z}/5\mathbf{Z})^2 \\ A_1(F) &\simeq \mathbf{Z}/25\mathbf{Z} & \text{III}(A_1/F)(5) &= 0 \\ A_2(F) &= 0 & \text{III}(A_2/F)(5) &\simeq (\mathbf{Z}/5\mathbf{Z})^2 \oplus (\mathbf{Z}/25\mathbf{Z})^2. \end{aligned}$$

We have treated the case $F = \mathbf{Q}(\mu_{11})$, but all our proofs, with trivial modifications, carry over to the case $F = \mathbf{Q}(\mu_{11})^+$.

7 Rational points on $X(11)$ over $\mathbf{Q}(\mu_{11})$

The modular curve $X(11)$ was described by Klein [K] as the singular locus of the Hessian of the cubic threefold

$$C := x_0^2x_1 + x_1^2x_2 + x_2^2x_3 + x_3^2x_4 + x_4^2x_0 = 0.$$

Here x_0, \dots, x_4 are co-ordinates on \mathbf{P}^4 . Equivalently $X(11)$ is defined by the 4×4 minors of the matrix $(\partial^2 C / \partial x_i \partial x_j)$. We refer to Adler [AR] for details. In fact $X(11)$ has degree 20 and genus 26, and so lies on 15 quartics. These are

$$\begin{aligned} x_0x_1x_3^2 + x_2^2x_3x_4 - x_0^2x_1x_4 &= 0 \\ x_0^3x_3 + x_0x_1^3 + x_2^3x_4 &= 0 \\ x_0^2x_2^2 + x_0x_3^3 - x_0^2x_3x_4 + x_1x_2x_3x_4 &= 0 \end{aligned}$$

and their cyclic permutes. The action of $\text{PSL}_2(\mathbf{Z}/11\mathbf{Z})$ on $X(11)$, given by relabelling torsion, lifts to an action on \mathbf{P}^4 . As special cases, the diagonal matrices give an action of $\mathbf{Z}/5\mathbf{Z}$

$$(x_0 : x_1 : x_2 : x_3 : x_4) \mapsto (x_4 : x_0 : x_1 : x_2 : x_3)$$

whereas the matrices $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ give an action of μ_{11}

$$(x_0 : x_1 : x_2 : x_3 : x_4) \mapsto (x_0 : \zeta^4x_1 : \zeta^7x_2 : \zeta x_3 : \zeta^2x_4).$$

$X(11)$ has 5 cusps of the form $(1 : 0 : 0 : 0 : 0)$ and 55 cusps of the form

$$(\zeta - \zeta^{10} : \zeta^3 - \zeta^8 : \zeta^9 - \zeta^2 : \zeta^5 - \zeta^6 : \zeta^4 - \zeta^7). \quad (13)$$

Quotienting out by the action of μ_{11} gives a morphism $X(11) \rightarrow X_1(11)$ of degree 11. This leads to alternative (affine) equations for $X(11)$

$$\left\{ \begin{array}{l} y^2 + y = x^3 - x^2 \\ xy^2(x-1)(x-y-1)^3 = t^{11} \end{array} \right\} \subset \mathbf{A}^2 \times \mathbf{G}_m$$

the relationship being

$$\begin{array}{lll} x & = & -x_0x_1x_3/x_2^2x_4 & x-1 & = & -x_0^2x_1/x_2^2x_3 \\ y & = & x_0x_1^3/x_2^3x_4 & y+1 & = & -x_0^3x_3/x_2^3x_4 \\ t & = & -x_0x_1/x_2^2 & x-y-1 & = & -x_0^2x_1x_4/x_2^4. \end{array}$$

The inverse map is

$$(x, y, t) \mapsto (xy(x-1) : \frac{-yt^4}{(x-y-1)} : \frac{-t^7}{(x-y-1)^2} : xy t : yt^2).$$

We write $P \in X_1(11)$ for the image of the cusp (13). Then P generates a subgroup of order 25. By Theorem 1 these are the only $\mathbf{Q}(\mu_{11})$ -rational points on $X_1(11)$. To find all $\mathbf{Q}(\mu_{11})$ -rational points on $X(11)$ we tabulate the points mP and look to see when $xy^2(x-1)(x-y-1)^3$ is an 11th power. We write $e_0 = \zeta - \zeta^{-1}$, $e_1 = \zeta^3 - \zeta^{-3}$, \dots so that (13) is the point $(e_0 : e_1 : e_2 : e_3 : e_4)$. Incidentally our table also allows us to identify the character ρ defined in §1. Indeed if $\tau : e_0 \mapsto e_1$ then $\rho(\tau) = 16$.

We find that the only $\mathbf{Q}(\mu_{11})$ -rational points on $X(11)$ lie above the points mP for $m \equiv 0, 1 \pmod{5}$. Since the latter are the cusps on $X_1(11)$, we deduce that the only $\mathbf{Q}(\mu_{11})$ -rational points on $X(11)$ are the 60 cusps. We have thus proved

Corollary 7.1 *There are no elliptic curves E over $F = \mathbf{Q}(\mu_{11})$ with $E[11](F) \simeq (\mathbf{Z}/11\mathbf{Z})^2$.*

Remark 7.2 This is a special case of a theorem of Merel [Me]. In fact Merel and Stein [MS] have shown that the corresponding statement holds for all primes p with $7 \leq p < 1000$ and $p \neq 13$.

Rational points on $X_1(11) : y^2 + y = x^3 - x^2$ over $\mathbf{Q}(\mu_{11})$

	x	y	$xy^2(x-1)(x-y-1)^3$
P	$-e_0e_1e_3/e_2^2e_4$	$e_0e_1^3/e_2^3e_4$	$-e_0^{11}e_1^{11}/e_2^{22}$
$2P$	$-e_0e_1/e_2e_3$	$e_0e_1e_4/e_2^2e_3$	$-e_0^6e_1^7e_4^2/e_2^{12}e_3^3$
$3P$	$-e_0e_4/e_1e_2$	$e_0^2e_4/e_1e_2e_3$	$-e_0^{12}e_4^3/e_1^7e_2^6e_3^2$
$4P$	$-e_1e_3e_4/e_0^2e_2$	$e_1e_3^3/e_0^3e_2$	$-e_3^{18}e_4^8/e_0^{16}e_1e_2^9$
$5P$	1	-1	{1}
$6P$	$-e_0e_2e_3/e_1e_4^2$	$e_2e_3^3/e_1e_4^3$	$-e_2^{11}e_3^{11}/e_4^{22}$
$7P$	$-e_1e_2/e_3e_4$	$e_0e_1e_2/e_3^2e_4$	$-e_0^2e_1^6e_2^7/e_3^{12}e_4^3$
$8P$	$-e_3e_4/e_0e_1$	$e_3e_4^2/e_0e_1e_2$	$-e_3^3e_4^{12}/e_0^7e_1^6e_2^2$
$9P$	$-e_1e_2e_4/e_0e_3^2$	$e_1^3e_4/e_0e_3^3$	$-e_1^{18}e_2^8/e_0^9e_3^{16}e_4$
$10P$	0	-1	{4}
$11P$	$-e_0e_2e_4/e_1^2e_3$	$e_0^3e_4/e_1^3e_3$	$-e_0^{11}e_4^{11}/e_1^{22}$
$12P$	$-e_2e_3/e_0e_4$	$e_1e_2e_3/e_0e_4^2$	$-e_1^2e_2^6e_3^7/e_0^3e_4^{12}$
$13P$	$-e_2e_3/e_0e_4$	$e_2e_3^2/e_0e_1e_4$	$-e_2^3e_3^{12}/e_0^6e_1^2e_4^7$
$14P$	$-e_0e_2e_4/e_1^2e_3$	$e_2e_4^3/e_1^3e_3$	$-e_0^8e_4^{18}/e_1^{16}e_2e_3^9$
$15P$	0	0	{5}
$16P$	$-e_1e_2e_4/e_0e_3^2$	$e_1e_2^3/e_0e_3^3$	$-e_1^{11}e_2^{11}/e_3^{22}$
$17P$	$-e_3e_4/e_0e_1$	$e_2e_3e_4/e_0^2e_1$	$-e_2^2e_3^6e_4^7/e_0^{12}e_1^3$
$18P$	$-e_1e_2/e_3e_4$	$e_1e_2^2/e_0e_3e_4$	$-e_1^3e_2^{12}/e_0^2e_3^7e_4^6$
$19P$	$-e_0e_2e_3/e_1e_4^2$	$e_0e_2^3/e_1e_4^3$	$-e_2^{18}e_3^8/e_0e_1^9e_4^{16}$
$20P$	1	0	{9}
$21P$	$-e_1e_3e_4/e_0^2e_2$	$e_3e_4^3/e_0^3e_2$	$-e_3^{11}e_4^{11}/e_0^{22}$
$22P$	$-e_0e_4/e_1e_2$	$e_0e_3e_4/e_1^2e_2$	$-e_0^7e_3^2e_4^6/e_1^{12}e_2^3$
$23P$	$-e_0e_1/e_2e_3$	$e_0e_1^2/e_2e_3e_4$	$-e_0^3e_1^{12}/e_2^7e_3^6e_4^2$
$24P$	$-e_0e_1e_3/e_2^2e_4$	$e_0^3e_3/e_2^3e_4$	$-e_0^{18}e_1^8/e_2^{16}e_3e_4^9$

Here $\{n\}$ in the right hand column denotes a zero of multiplicity n .

8 A further example

As explained in [CH] and [CS], there is some interest in computing rank $A(F)$ for number fields $F \subset \mathbf{Q}(A[5^\infty])$. In this section we explain how, with a modest amount of computer calculation (the author uses pari), we may prove rank $A(F) = 0$ for the field $F = \mathbf{Q}(\mu_5)\mathbf{Q}(\mu_{11})^+$.

Again let τ in $\text{Gal}(F/\mathbf{Q})$ be an element of order 5. We find that F has class number 5, and the Hilbert class field is the composite with $\mathbf{Q}(A_1[5])$. The primes above 11 are inert in this extension, and so generate the class group. The unit group \mathfrak{D}_F^* is generated by norms of cyclotomic units from $\mathbf{Q}(\mu_{55})$ together with $\pm\phi$ where $\phi = 1 + \zeta_5 + \zeta_5^4$. Writing $\bar{\phi} = 1 + \zeta_5^2 + \zeta_5^3$,

$$u_0 = 1 - (\zeta_{11} + \zeta_{11}^{-1})\phi, \quad v_0 = 1 - (\zeta_{11} + \zeta_{11}^{-1})\bar{\phi},$$

$u_i = \tau^i(u_0)$ and $v_i = \tau^i(v_0)$, a set of fundamental units is

$$\phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4.$$

We note $\prod_i u_i = \phi^5$ and $\prod_i v_i = \bar{\phi}^5$. The subgroup of F^*/F^{*5} with trivial valuation at all primes is generated by the units, together with the “virtual unit” $2 + \zeta_5$. Thus by Propositions 2.1 and 2.2 we find

$$\begin{aligned} S(A_0 \rightarrow A_1/F) &\simeq (\mathbf{Z}/5\mathbf{Z})^7 \\ S(A_1 \rightarrow A_0/F) &\simeq \mathbf{Z}/5\mathbf{Z} \end{aligned} \tag{14}$$

and

$$\begin{aligned} S(A_2 \rightarrow A_0/F) &\simeq (\mathbf{Z}/5\mathbf{Z})^{14} \\ S(A_0 \rightarrow A_2/F) &= 0. \end{aligned} \tag{15}$$

Since $\#A(\mathbf{F}_{220}) = 5^4 \cdot 41^2$ and $\#A(\mathbf{F}_{55}) = 5^2 \cdot 11^2$ we know $A(F)_{\text{tors}}$ is a 5-group. Let $\rho_5 : G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{Z}_5)$ be the Galois representation defined by the 5-power division points of A_0 . From the description of ρ_5 given by Lang and Trotter [LT, Part I, Theorem 8.1] we deduce

$$A_0(F)_{\text{tors}} \simeq (\mathbf{Z}/5\mathbf{Z})^2, \quad A_1(F)_{\text{tors}} \simeq \mathbf{Z}/25\mathbf{Z}, \quad A_2(F)_{\text{tors}} \simeq \mathbf{Z}/5\mathbf{Z}.$$

Taking these torsion contributions into account, the estimates for rank $A(F)$ given by (14) and (15) are 6 and 12 respectively. As in §5 we compute $S(A_0 \xrightarrow{\times 5} A_0/F)$ in two different ways and learn that the Cassels-Tate pairing on $S(A_2 \rightarrow A_0/F)$ has rank 6. We shall show that the pairing on $S(A_0 \rightarrow A_1/F)$ also has rank 6.

The Selmer group $S(A_2 \rightarrow A_0/F) \subset F^*/F^{*5}$ has basis

$$\zeta_5, \phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4, 2 + \zeta_5, u_0 - \phi, v_0 - \bar{\phi}, \gamma$$

where γ^5 in $\mathbf{Q}(\mu_5)$ is a Kummer generator for F over $\mathbf{Q}(\mu_5)$. For M a $\mathbf{Z}_5[\text{Gal}(F/\mathbf{Q})]$ -module we write

$$M^{[i]} = \{ m \in M \mid \sigma(m) = \omega^i(\sigma)m \text{ for all } \sigma \in \text{Gal}(F/\mathbf{Q}) \}$$

where $\omega : G_{\mathbf{Q}} \rightarrow \mathbf{Z}_5^*$ is the cyclotomic character. By Proposition 5.1(ii) we already know that the Cassels-Tate pairing on $S(A_0 \rightarrow A_1/F)^{[0]}$ has rank 2.

Proposition 8.1 *Let $F = \mathbf{Q}(\mu_5)\mathbf{Q}(\mu_{11})^+$.*

- (i) *The Cassels-Tate pairing on $S(A_2 \rightarrow A_0/F)^{[2]} \simeq (\mathbf{Z}/5\mathbf{Z})^6$ has rank 2.*
- (ii) *The Cassels-Tate pairing on $S(A_0 \rightarrow A_1/F)^{[2]} \simeq (\mathbf{Z}/5\mathbf{Z})^4$ has rank 4.*

Proof. (i) This is given by comparing the exact sequences (7) and (8).
(ii) We shall use the Galois equivariance of the Cassels-Tate pairing to deduce this from (i). We consider the exact sequence

$$0 \longrightarrow S(A_2 \rightarrow A_0/F)^{[2]} \longrightarrow S(A_2 \rightarrow A_1/F)^{[2]} \longrightarrow S(A_0 \rightarrow A_1/F)^{[2]}. \quad (16)$$

Let $w_i = u_i/v_i$ and $z = (u_0 - \phi)/(v_0 - \bar{\phi})$. Taking $\tau : \zeta_{11} + \zeta_{11}^{-1} \mapsto \zeta_{11}^3 + \zeta_{11}^{-3}$ a brute force calculation gives

$$\tau(z) = -\phi^{-2}w_2z. \quad (17)$$

We describe the Selmer groups in (16).

$$\begin{aligned} S(A_2 \rightarrow A_0/F)^{[2]} &= \langle w_1, w_2, w_3, w_4, \phi, z \rangle \subset F^*/F^{*5} \\ S(A_2 \rightarrow A_1/F)^{[2]} &= \langle w_1, w_2, w_3, w_4, \phi^5, z^5 \rangle \subset F^*/F^{*25} \\ S(A_0 \rightarrow A_1/F)^{[2]} &= \langle w_1, w_2, w_3, w_4 \rangle \subset F^*/F^{*5} \end{aligned}$$

As before we write $R = \mathbf{Z}_5[\tau]$ and $\widehat{F} = F^* \otimes \mathbf{Z}_5$. We define $M \subset \widehat{F}$ to be the R -module generated by z and ϕ , and $N \subset \widehat{F}$ to be the R -module generated by w_0 . The exact sequence (16) becomes

$$0 \longrightarrow M/5M \xrightarrow{\times 5} (N + 5M)/25M \longrightarrow (N + 5M)/5M \longrightarrow 0 \quad (18)$$

Again we write $\langle \cdot, \cdot \rangle_{20}$, $\langle \cdot, \cdot \rangle_{21}$ and $\langle \cdot, \cdot \rangle_{01}$ for the alternating pairings. Lemmas 5.2 and 5.3 go through as before. Since

$$\langle M, N \rangle_{20} = \langle 5M, 5N \rangle_{21} = \langle 5M, N \rangle_{01} = 0$$

and $M/((\tau - 1)M + N) \simeq \mathbf{Z}_5$ we deduce

$$\langle , \rangle_{20} \text{ has rank } 2 \iff \langle (\tau - 1)M, M \rangle_{20} \neq 0. \quad (19)$$

By (17) we have $(\tau - 1)N = (\tau - 1)^2M$ and so $(\tau - 1)^4N \subset 5M$. Thus

$$\begin{aligned} \langle , \rangle_{01} \text{ has rank } 4 &\iff \langle (\tau - 1)^3N, N \rangle_{01} \neq 0 \\ &\iff \langle (\tau - 1)^2N, (\tau - 1)N \rangle_{01} \neq 0 \\ &\iff \langle (\tau - 1)^3M, (\tau - 1)^2M \rangle_{01} \neq 0 \end{aligned} \quad (20)$$

Now (19) and (20), together with the calculation at the end of §5, show that statements (i) and (ii) are equivalent. This completes the proof of the proposition. \square

Propositions 5.1(ii) and 8.1(ii) show that the Cassels-Tate pairing on $S(A_0 \rightarrow A_1/F) \simeq (\mathbf{Z}/5\mathbf{Z})^7$ has rank 6. As in §6 we now have sufficient information to compute $A(F)$ and $\text{III}(A/F)(5)$. We summarise our results.

Theorem 2 *Let $F = \mathbf{Q}(\mu_5)\mathbf{Q}(\mu_{11})^+$. Then*

$$\begin{aligned} A_0(F) &\simeq (\mathbf{Z}/5\mathbf{Z})^2 & \text{III}(A_0/F)(5) &\simeq (\mathbf{Z}/5\mathbf{Z})^6 \\ A_1(F) &\simeq \mathbf{Z}/25\mathbf{Z} & \text{III}(A_1/F)(5) &= 0 \\ A_2(F) &\simeq \mathbf{Z}/5\mathbf{Z} & \text{III}(A_2/F)(5) &\simeq (\mathbf{Z}/5\mathbf{Z})^6 \oplus (\mathbf{Z}/25\mathbf{Z})^6. \end{aligned}$$

References

- [AR] A. Adler and S. Ramanan, *Moduli of abelian varieties*, Lect. Notes in Math. **1644** Springer (1996)
- [BBBCO] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *pari/gp*, a computer algebra package, <http://www.parigp-home.de>
- [Ca1] J.W.S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung, *J. Reine Angew. Math.* **211** (1962) 95-112
- [Ca2] J.W.S. Cassels, Arithmetic on curves of genus 1, VIII. On conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.* **217** (1965) 180-199
- [CH] J. Coates and S. Howson, Euler characteristics and elliptic curves II, *J. Math Soc. Japan* **53** (2001) 175-235

- [CS] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, TIFR Lect. on Math. **88** Narosa (2000)
- [Cr] J.E. Cremona, *Algorithms for modular elliptic curves (second edition)*, Cambridge (1997)
- [F0] T.A. Fisher, *On 5 and 7 descents for elliptic curves*, Cambridge PhD Thesis (2000)
- [F1] T.A. Fisher, Some examples of 5 and 7 descent for elliptic curves over \mathbf{Q} , *J. Eur. Math. Soc.*, published online 15th February 2001
- [K] F. Klein, Über die Transformationen elfter Ordnung der elliptischen Funktionen, *Math. Ann.* **14** (1879) 428-471
- [LT] S. Lang and H. Trotter, *Frobenius distributions in GL_2 -extensions*, Lect. Notes in Math. **504** Springer (1976)
- [Me] L. Merel, Sur la nature non cyclotomic des points d'ordre fini des courbes elliptiques, to appear in *Duke Math. J.*
- [MS] L. Merel and W.A. Stein, *The field generated by the points of small prime order on an elliptic curve*, to appear in IMRN
- [Mi] J.S. Milne, *Arithmetic duality theorems*, Persp. in Math. **1** Academic Press (1986)
- [S] J.H. Silverman, *The arithmetic of elliptic curves*, GTM **106** Springer (1986)
- [V1] J. Vélú, Isogénies entre courbes elliptiques, *C. R. Acad. Sc. Paris* **273** (1971) 238-241
- [V2] J. Vélú, Courbes elliptique munies d'un sous-groupe $\mathbf{Z}/n\mathbf{Z} \times \mu_n$, *Bull. Math. Soc. math. France*, Mémoire **57** (1978)
- [W] L.C. Washington, *Introduction to cyclotomic fields (second edition)*, GTM **83** Springer (1997)