VIGRE Number Theory Working Group "Mazur Seminar" Talk 1

UNIVERSAL FAMILIES AND RULING OUT SMALL PRIMES

Bryden Cais

September 16, 2003

1 Introduction

The purpose of this talk is to give the general flavor of the background (i.e. pre Mazur) material on the possibilities for torsion subgroups of elliptic curves over $\mathbb{Q}$. To that end, there are three sections: in the first, we show how to write down a one parameter family of elliptic curves defined over $\mathbb{Q}$ having a rational point of of order N for $3 \leq N \leq 10$ and $N = 12$. (The case $N = 2$ can also be treated but is somewhat different). We then give some motivation as to why it is these values of N that occur and why A Ogg. conjectured that these are the only possible values. In the second section, we will show that no elliptic curve over $\mathbb{Q}$ can have a rational point of order 11. We do this by showing that the modular curve $X_1(11)$, which classifies pairs (E, P) of elliptic curves E and points P of E having order 11, has no rational points other than cusps. In the third section, we tackle the same problem for points of order 35. This is substantially more subtle than the previous case as the genus of $X_1(35)$ is large.

2 Familes of elliptic curves

In this section, following [8], we construct a one-parameter family of elliptic curves over $\mathbb{Q}$ with a rational point of exact order 5. In the course of this construction, we will explicitly see that the modular curve $X_1(5)$ has genus 0. This construction can be done similarly for a point of exact order N when $3 \leq N \leq 10$ or $N = 12$.

Let E be an elliptic curve with a point P of order 5. Embed E in $\mathbb{P}^2$ with coordinates X, Y, Z in the usual way, with $x = X/Z$ and $y = Y/Z$. By performing a change of coordinates if necessary, we may suppose that $P = (0, 0, 1)$, $O = (0, 1, 0)$, and the tangent line to E at P is the line $y = 0$. This forces E to have Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

Observe that a_2 is a unit since otherwise P would be an inflection point, and hence have order 3. We therefore make the change of variables $x \mapsto \lambda^2 x$, $y \mapsto \lambda^3 y$ (which fixes fixing P, O) where $\lambda = a_3/a_2$ to bring the (affine) equation of E to the form

$$y^2 + \alpha xy + \beta y = x^3 + \beta x^2. \tag{1}$$

Observe that this form of the Weierstrass equation for E is *uniquely* determined by E. Indeed, the only coordinate changes preserving the Weirstrass form of the equation of E and fixing P, O are of the form $(x, y) \mapsto (u^2 x, u^3 y)$; but these do not preserve the form (1) unless $u = 1$.

Now, it is not difficult to determine that on the curve (1),

$$2P = (-\beta, \beta(\alpha - 1)) \qquad\qquad 3P = (1 - \alpha, \alpha - \beta - 1).$$

Moreover, P has order 5 if and only if $3P = -2P$, i.e. if and only if $\alpha = 1 + \beta$. Therefore, E has Weierstrass equation

$$E_\beta : y^2 + (1 + \beta)xy + \beta y = x^3 + \beta x^2. \tag{2}$$

The discriminant of E_β is

$$\Delta(\beta) = -\beta^5(\beta^2 + 11\beta - 1), \tag{3}$$

which is nonzero except for $\beta \in \{0, \frac{-11 \pm 5\sqrt{5}}{2}\}$ and the point at infinity on the projective line $\mathbb{P}^1$. Hence, for any field and any $\beta \in K - \{\beta : \Delta(\beta) = 0\}$ we obtain an elliptic curve E_β defined over K and unique up to isomorphism, with a point $P = (0, 0)$ of exact order 5. In particular, for $K = \mathbb{Q}$, we have obtained a one parameter family of elliptic curves defined over $\mathbb{Q}$ with a rational point of order 5.

We thus have the identification of $Y_1(5) \simeq \mathbb{P}^1 - \{\infty, \{\Delta = 0\}\}$ and hence $X_1(5) \simeq \mathbb{P}^1$ (which shows that $X_1(5)$ has genus 0).

The situation is almost identical for elliptic curves with a point of exact order N for $3 \leq N \leq 10$ and $N = 12$ ($N = 2$ must be treated differently). Indeed, these are *precisely* the cases when $X_1(N)$ has genus zero (see Table 1). Since $X_1(N)$ over $\mathbb{Q}$ always has a rational point (namely any cusp) this gives the identification $X_1(N)(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$ in the above cases; i.e. in each of these cases, we can obtain a one parameter family of elliptic curves defined over $\mathbb{Q}$ having an exact point of order N. That these are the *only* instances when $X_1(N)$ has genus 0 (together with calculations for other N that we shall give a flavor of below) lead A. Ogg to conjecture exactly what groups can occur as the torsion subgroup of an elliptic curve over $\mathbb{Q}$.

Table 1

N	Genus of $X_1(N)$	Genus of $X_0(N)$
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	1	1
12	0	0
13	2	0
14	1	1
15	1	1
16	2	0
17	5	1
18	2	0
20	3	1
21	5	1
24	5	1
25	12	0
27	13	1
35	25	3
49	69	1

3 Elliptic curves with a point of order 11

In this section we will show that no elliptic curve over $\mathbb{Q}$ can have a rational point of order 11. We will accomplish this by deriving a model for the modular curve $X_1(11)$ over $\mathbb{Q}$ and will subsequently show that $X_1(11)(\mathbb{Q})$ contains only cusps.

Let E be an elliptic curve with a rational point P of order 11. As usual, we shall suppose that $E \subset \mathbb{P}^2$ is a nonsingular cubic curve having the point at infinity $O = (0,1,0)$ as a flex and that the group structure on E is such that 3 points add up to 0 if and only if they are collinear. Since P has order 11, we see that no three of the points $O, P, 3P, 4P$ are collinear. It follows that we may choose our coordinate system in $\mathbb{P}^2$ so that

$$P = (0,0,1) \qquad 3P = (1,0,0)$$
$$4P = (1,1,1) \qquad 5P = (x_1, x_2, x_3)$$

with $x_1, x_2, x_3 \in \mathbb{Q}$. Observe that these requirements specify E *uniquely*: indeed, the four points $O, P, 3P, 4P$ are in "general" position, and there are no projective automorphisms fixing these four points other than the identity. This rigidifies our problem.

We now explicitly determine the points $-P, -3P, -4P, -5P$ in terms of x_1, x_2, x_3. By our description of the group law on E we see that $-5P, O, 5P$ are collinear, as are $-5P, P, 4P$. It follows that $-5P$ is the unique point of intersection of the lines L_1 joining $O, 5P$ and L_2 joining $P, 4P$. We easily determine the parameterizations

$$\begin{aligned} L_1 :& \alpha(x_1, x_2 - x_1, x_3) + (0, x_1, 0) \\ L_2 :& \beta(1, 1, 0) + (0, 0, 1), \end{aligned}$$

where we are using the fact that $x_1 \neq 0$ (since otherwise $5P, P, O$ would be collinear and $6P = 0$). We find that L_1, L_2 intersect at the point where $\beta = x_1/x_3$, that is, the point (x_1, x_1, x_3). It follows that $-5P = (x_1, x_1, x_3)$. In this manner, we produce the following table:

$$\begin{aligned} P &= (0,0,1) & -P &= (0, x_2, x_3 - x_1) \\ 3P &= (1,0,0) & -3P &= (x_3 - x_1, x_3 - x_2 - x_1, 0) \\ 4P &= (1,1,1) & -4P &= (1,0,1) \\ 5P &= (x_1, x_2, x_3) & -5P &= (x_1, x_1, x_3). \end{aligned}$$

Finally, since $2P$ is the point of intersection of the lines through $-5P, 3P$ and $p, -3P$, we determine that

$$2P = (x_1(x_3 - x_1), x_1(x_3 - x_2 - x_1), x_3(x_3 - x_2 - x_1)).$$

Now the condition that $11P = O$ is precisely the condition that $2P, 4P, 5P$ are collinear, i.e. that the determinant

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1(x_3 - x_1) & x_1(x_3 - x_2 - x_1) & x_3(x_3 - x_2 - x_1) \end{vmatrix} = x_3(x_2 - x_1)(x_3 - x_2 - x_1) + x_1^2(x_3 - x_1)$$

is zero. Since $x_1 \neq 0$, we let $x_2/x_1 = y$ and $x_3/x_1 = x$ and find that a rational point of order 11 on E gives a rational point on the affine curve $(x-1)^2 = xy(x-y)$.

Now the birational transformations

$$\begin{aligned} v &= 1 - x + xy & x &= \frac{(v-1)^2}{u - v + 1} \\ u &= xy(y-1) & y &= \frac{u}{v-1} \end{aligned}$$

transform the curve $(x-1)^2 = xy(x-y)$ into the elliptic curve M

$$u^2 + u = v^3 - v^2,$$

which gives a minimal model for $X_1(11)$.

We have thus seen that any elliptic curve $E/\mathbb{Q}$ with a rational point of order 11 gives rise to a rational point of $u^2+u=v^3-v^2$. We now show that this elliptic curve has rank 0, and that the points of finite order correspond to degenerate cases above.

Using the Nagell-Lutz method for finding torsion points, we compute that

$$M_{\mathrm{tors}}(\mathbb{Q}) = \{O, (0,0), (0,1), (-1,0), (-1,1)\} \simeq \mathbb{Z}/5.$$

These 5 points correspond to

$$(x_1, x_2, x_3) \in \{(0,1,0), (0,1,1), (0,0,1), (1,1,1), (1,0,1)\}.$$

But in each of these cases, one sees that the point $5P = (x_1, x_2, x_3)$ on our original elliptic curve is equal to one of $O, P, -P, 4P, -4P$ and hence does not have order 11. It therefore remains to show that $M(\mathbb{Q})$ has rank 0.

Using the program **PARI**, we can compute that

$$L_M(1) = 0.253841860855910684337758923 7\ldots,$$

where L_M is the L function attached to the elliptic curve M. From work of Kolyvagin and Gross-Zagier, we know that if L_M is nonvanishing at $s=1$ (i.e. has analytic rank 0) than $M(\mathbb{Q})$ has rank 0. We shall actually prove that $M(\mathbb{Q})$ has rank 0 without appealing to such machinery, but it's at least good to know in advance that our work will not be in vain.

We first make the change of variables $u+1/2 = s/2^3$ and $v = t/2^2$ so that M is put in the form

$$M : s^2 = t^3 - 4t^2 + 16 := f(t).$$

Now suppose that M has a rational point. It is easy to see that this point has the form $(m/e^2, n/e^3)$ for integers m, n, e with $e > 0$ and $(m, e) = 1$. We first claim that we can take m, n to be *odd*. Indeed, let $M(\mathbb{F}_2)$ denote the reduction of M modulo 2. It is easy to see that $\#M(\mathbb{F}_2) = 3$. It follows that the image of $[3]M(\mathbb{Q})$ in $M(\mathbb{F}_2)$ is zero (since reduction modulo 2 is a group homomorphism) and hence that $[3]M(\mathbb{Q})$ lies in the kernel of the reduction map; i.e. the set of all points in $M(\mathbb{Q})$ with the form $(m/e^2, n/e^3)$ and e even, m, n odd. Since $M_{\mathrm{tors}}(\mathbb{Q})$ is a group of order 5, we have the claim.

We now show that multiplication by 2 on $M(\mathbb{Q})$ is a group isomorphism (i.e. we perform a "2-descent").

Let $\lambda_1, \lambda_2, \lambda_3$ denote the three roots of $f(t)$ is some (henceforth fixed) algebraic closure K, with λ_1 real. Set $L = \mathbb{Q}(\lambda_1)$. We state the following (easily verified) facts about L:

1. L has discriminant $D_L = -2^2 \cdot 11$.

2. The polynomial f has discrminant $D_f = -2^8 \cdot 11$

3. L has class number 1.

4. An integral basis for the ring of integers $\mathcal{O}$ of L is $\{1, \pi, \pi^2\}$, where $\pi = \lambda_1/2$.

5. The index I of $\mathbb{Z}[\lambda_1]$ in $\mathcal{O}$ is 8. This follows from items 1 and 2, and the formula $I^2 = D_f/D_L$.

6. The unit group of L has rank 1, generated by the fundamental unit $\pi - 1$

7. The prime $2 = P_2^3$ is totally ramified in L, with $P_2 \subset \mathcal{O}$ the unique prime above 2.

8. The prime 11 factors as $P_{11}Q_{11}^2$ in L for prime ideals $P_{11}, Q_{11} \subset \mathcal{O}$.

Now, in K we have the factorization

$$n^2 = (m - \lambda_1 e^2)(m - \lambda_2 e^2)(m - \lambda_3 e^2),$$

and we set $\gamma = (m - \lambda_2 e^2)(m - \lambda_3 e^2)$. Observe that $\gamma \in \mathcal{O} \subset L$. If P is a prime ideal of $\mathcal{O}$, and A is any $\mathcal{O}$ ideal, we let $v_P(A)$ denote the order of A at P. Suppose that $v_P(m - \lambda_1 e^2)$ is odd. Then it is clear that $v_P(\gamma) > 0$. We certainly have $v_P(e) = 0$ (since otherwise $v_P(m) > 0$ and $(e, m) \neq 1$). Writing

$$f(x) = (x - \lambda_1)f'(\lambda_1) + O((x - \lambda_1)^2)$$

we have

$$(m - \lambda_1 e^2)\gamma = (m - \lambda_1 e^2)f'(\lambda_1) + O((m - \lambda_1 e^2)^2),$$

from which it follows that $v_P(f'(\lambda_1)) \geq \min\{v_P(m - \lambda_1 e^2), v_P(\gamma)\}$. We conclude that the ideal $(\gamma, m - \lambda_1 e^2)$ divides $N_{L/\mathbb{Q}}(f'(\lambda_1)) = -D_f$.

We therefore have $(m - \lambda_1 e^2) = AB^2$ for ideals $A, B \subset \mathcal{O}$ with A squarefree and A dividing D_f. From our list above, we see that A is divisible only by primes above 11 or 2. We show that in fact, neither of these possibilities can occur. Indeed, since $n^2 = N_{L/\mathbb{Q}}(m - \lambda_1 e^2) = N_{L/\mathbb{Q}}(A)N_{L/\mathbb{Q}}(B)^2$ we see that $N_{L/\mathbb{Q}}(A)$ is a square. It follows that if 11 divides $N_{L/\mathbb{Q}}(A)$ then $P_{11}Q_{11}$ divides A and hence $(m - \lambda_1 e^2)$; therefore $P_{11}^2 Q_{11}^2$ divides $(m - \lambda_1 e^2)^2$ so that $11 | (m - \lambda_1 e^2)^2$. Letting $\alpha = (m - \lambda_1 e^2)^2/11$ we have $\alpha \in \mathcal{O}$ and $11\alpha \in \mathbb{Z}[\lambda_1]$. Since 11 does not divide e, we have $\alpha \notin \mathbb{Z}[\lambda_1]$. It follows that 11 divides the index I of $\mathbb{Z}[\lambda_1]$ in $\mathcal{O}$. But this is clearly false as the index is 8.

Since $2 = P_2^3$ is totally ramified in L, if $2 | N_{L/\mathbb{Q}}(A)$ then we must have $v_{P_2}(A) = 1$ (since A is squarefree). But then we see that $N_{L/\mathbb{Q}}(A)$ is *exactly* divisible by 2 and is hence not a square.

We have thus shown that $(m - \lambda_1 e^2)$ is the square of some ideal $B \subset \mathcal{O}$. Using the fact that $\mathcal{O}$ has trivial ideal class group, we may write $(m - \lambda_1 e^2) = \pm\epsilon^r \eta^2$ for some $\eta \in \mathcal{O}$ and $r \in \{0, 1\}$, where $\epsilon = \pi - 1$ is the fundamental unit of L. Now since $\pi = \lambda_1/2$ satisfies $x^3 - 2x^2 + 2$, we see that $N_{L/\mathbb{Q}}(\pi) = 2$, i.e. $\pi = P_2$ (up to a unit). Since $\lambda_1 = 2\pi$ we see that $2, \lambda$ are congruent to 0 modulo π^2. Since we have put ourselves in the situation where m is odd, we have $m - \lambda_1 e^2 \equiv 1 \mod \pi^2$. There are exactly four residue classes modulo π^2 (namely $0, 1, \pi, 1 + \pi$), so for any $\eta \in \mathcal{O}$ we have $\eta^2 \equiv 1$ or 0 modulo π^2. Hence, $\pm\epsilon\eta^2$ is congruent to $(\pi - 1)$ or 0 modulo π^2. Since $m - \lambda_1 e^2 \equiv 1$

mod π^2 it follows that $m - \lambda_1 e^2 = \pm\eta^2$ for some $\eta \in \mathcal{O}$. However, since complex conjugation interchanges the roots λ_2, λ_3 and fixes λ_1, we see that

$$(m - e^2\lambda_2)(m - e^2\lambda_3) = |(m - e^2\lambda_2)|^2$$

where $|\cdot|$ is the usual absolute value on $\mathbb{C}$. Hence $(m - e^2\lambda_2)(m - e^2\lambda_3) \in \mathbb{R}$ is *positive*. Since $n^2 = (m - e^2\lambda_1)(m - e^2\lambda_2)(m - e^2\lambda_3)$ is also positive, we have $m - e^2\lambda_1 > 0$ so that $m - e^2\lambda_1 = \eta^2$ for some $\eta \in L$. Let $L = L_1$ and let L_2, L_3 denote the galois conjugates of L_1 in K. We thus see that $(m - \lambda_i e^2) \in L_i$ is a square. for each i.

But now the homomorphism $\phi_i : M(\mathbb{Q}) \longrightarrow L_i^\times / L_i^{\times 2}$ given by $(m/e^2, n/e^3) \mapsto (m/e^2 - \lambda_i) L_i^{\times 2}$ has trivial image. It follows that the standard "Mordell Weil" homomorphism $M(\mathbb{Q}) \longrightarrow L_1^\times / L_1^{\times 2} \times L_2^\times / L_2^{\times 2} \times L_3^\times / L_3^{\times 2}$ has trivial image. Since the kernel is precisely $2M(\mathbb{Q})$, we have shown that $M(\mathbb{Q}) = 2M(\mathbb{Q})$ and hence that M has rank 0. It follows that there are no elliptic curves $E/\mathbb{Q}$ with a rational point of order 11.

4 Elliptic curves with a point of order 35

.

When the curve $X_1(N)$ has large genus it is unreasonable to expect to be able to show that $X_1(N)$ has no rational points other than cusps by a direct argument. The strategy for curves of high genus like this is to show that they admit a rational map to some other curve, of lower genus, which has no rational points (other than the "expected" ones coming from the cusps of $X_1(N)$). An obvious candidate is $X_0(N)$. In terms of moduli spaces, the natural map $X_1(N) \longrightarrow X_0(N)$ takes a pair $(E, P) \in X_1(N)$ and sends it to the pair $(E, \langle P \rangle) \in X_0(N)$, where $\langle P \rangle$ is the subgroup generated by P. On the complex analytic side, the natural inclusion of groups $\Gamma_1(N) \hookrightarrow \Gamma_0(N)$ induces a holomorphic map of Riemann Surfaces $\Gamma_1(N)/\mathfrak{H}^* \longrightarrow \Gamma_0(N)/\mathfrak{H}^*$. This is a Galois covering with galois group $\Gamma_0(N)/\pm\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$.

Of course, this strategy may fail miserably: Indeed, it can happen (as in the cases $N = 13, 16, 18, 25$) that $X_1(N)$ has no non-cuspidal rational points, while $X_0(N)$ has infinitely many rational points. In the cases listed above, the genus of $X_0(N)$ is *zero*, and since $X_0(N)$ always has a rational point (namely, any cusp) we have the identification $X_0(N)(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$. In moduli theoretic terms, there are (one parameter) families of elliptic curves with a "rational" subgroup of order N for $N = 13, 16, 18, 25$. Here, a rational subgroup of order N is a subgroup of $E[N](\bar{\mathbb{Q}})$ which is fixed (as a group but not necessarily point-wise) by the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. thus, in these cases, one needs different methods to show that $X_1(N)$ has no non-cuspidal rational points.

This strategy can also be rather complicated to implement. For $N = 17, 20, 21, 24, 27$ the curve $X_0(N)$ has genus 1, and we can hope to "get lucky" and be able to show by a direct argument that $X_0(N)$ has no rational points other than the ones coming from the cusps of $X_1(N)$. This works, for example, in the case $N = 17$ [7]. However, for $N = 35$, the curves $X_1(N)$ and $X_0(N)$ have genus 25 and 3 respectively. Thus, even if we are "lucky" and $X_0(35)$ has no non-cuspidal rational points, it may in practice be very hard to show this by directly working with a set of equations for $X_0(35)$ in some projective space.

In this section, we will construct a quotient curve of $X_0(35)$ having genus 1, and show directly that this quotient has no rational points other than those coming from the cusps of $X_0(35)$ (which in turn must come from the cusps of $X_1(35)$). It will follow that there are no elliptic curves over $\mathbb{Q}$ possessing a rational subgroup of order 35, and hence, no elliptic curves having a rational point of order 35.

We will now proceed to determine a model for $X_0(35)$ and the above mentioned quotient curve. For any $n|N$ we let W_n be the Atkin-Lehner involution as defined in [4]. Let $\Omega^1(X)$ denote, as usual, the space of holomorphic differentials on X. Recall [4, pg. 9] that we have the natural identification

$$\Omega^1(X_0(N)/W_n) \simeq \{f \in S_2(N) : f|_{W_n} = f\}, \tag{4}$$

where a weight 2 cusp form f, invariant under W_n is mapped to the differential ω given locally by $f(z)dz$. Moreover, we know that the genus g of a curve X is given by the dimension (as a complex vector space) of $\Omega^1(X)$. Consulting Table 5 of [1], we see that $S_2(35)$ has dimension 3, and that we can find a basis of $S_2(35)$ consisting of eigenforms for the W_n with $n|35$. One sees that $S_2(35)$ splits into a one dimensional space of cusp forms with eigenvalue $+1$ with respect to W_5 and eigenvalue -1 for W_7, and a two dimensional space of cusp forms having eigenvalue -1 for W_5 and $+1$ for W_7. Since $W_{35} = W_5W_7$, it follows that no cusp form on $\Gamma_0(35)$ has eigenvalue 1 for W_{35}. From the identification (4), we see that the dimension (over $\mathbb{C}$) of $\Omega^1(X_0(35)/W_{35})$ is zero, hence we have an isomorphism $X_0(35)/W_{35} \simeq \mathbb{P}^1$. Since W_{35} is an involution, this shows that $X_0(35)$ admits a degree 2 map to $\mathbb{P}^1$ and is hence a hyperelliptic curve of genus 3. It follows that we have en embedding $X_0(35) \to \mathbb{P}^2$. If we give $\mathbb{P}^2$ homogenous coordinates (X, Y, Z), then we can realize the image of $X_0(35) \cap \{Z \neq 0\}$ under this embedding as the locus $y^2 = p(x)$, where p is a polynomial of degree $2g + 2 = 8$ and $x = X/Z,\ y = Y/Z$. Moreover, we also see that the dimension of $\Omega^1(X_0(35)/W_5)$ is one, and hence that $X_0(35)/W_5$ is an elliptic curve. It is this quotient that we will determine has no "unexpected" rational points. It is worth pointing out that one can explicitly determine the action of W_5 on $X_0(35)$ in terms of pairs (E, C) of elliptic curves and rational subgroups C of order 35: indeed, we know that C contains a subgroup of order 5, call it D, and a subgroup or order 7, say F. Let $\phi : E \to E/D$ be the quotient map and let F' denote the image of F under ϕ. Finally, let D' be the kernel of the dual map $\tilde{\phi}$ and let C' be the composition of D' and F'. Then C' has order 35 and in the quotient, $X_0(35)/W_5$, the pair (E, C) is mapped to the pair $(E/D, C')$ [5].

To determine the polynomial $p(x)$ we follow [4]. We know that the map

$$X_0(35) \longrightarrow X_0(35)/W_{35} \simeq P^1$$

is given (on affine pieces) by $(x, y) \mapsto x$ (equivalently, the involution W_{35} is the unique "hyperelliptic" involution of $X_0(35)$ given by $y \mapsto -y$). Thus, $x \in \mathbb{C}(X_0(35))$ has exactly 2 distinct poles (distinctness follows from the fact that the map is ramified only over the roots of p, which cannot include ∞). Observe that the divisor of poles of y is $g+1=4$ times the divisor of poles of x. Hence the differentials

$$\frac{dx}{y} \qquad \frac{xdx}{y} \qquad \frac{x^2dx}{y}$$

are holomorphic and have distinct divisors. It follows that they span $\Omega^1(X_0(35))$. Moreover, we can require that x have a simple pole at ∞ so that the orders of vanishing of $\frac{dx}{y}$, $\frac{xdx}{y}$, $\frac{x^2dx}{y}$ at ∞ are, respectively, 3,2,1. Now $S_2(35)$ has basis f_1, f_2, f_3, where the order of vanishing of f_j at ∞ is j. Equivalently, letting q be a local parameter at ∞ in the Riemann surface $X_0(35)(\mathbb{C})$, we may write $f_j = q^j + O(q^{j+1})$. It follows from the identification (4) that we have (at least up to scalar multiplication)

$$\frac{dx}{y} = f_3 \quad \text{and} \quad \frac{xdx}{y} = f_2.$$

From this, we easily obtain

$$x = \frac{f_2}{f_3} \quad \text{and} \quad y = \frac{dx}{f_3},$$

with x determined up to a constant. Using Stein's tables [9], we find

$$\begin{aligned} f_2 &= q^2 - 3q^4 - q^5 + 2q^6 + q^7 + O(q^8) \\ f_3 &= q^3 - 2q^4 - q^5 + 2q^6 + q^7 + O(q^8), \end{aligned}$$

and hence, using the fact that up to a factor of $2\pi i$ we have $dx = q\frac{dx}{dq}dt$ (for a local parameter t),

$$\begin{aligned} x &= q^{-1} + 2 + 2q + 3q^2 + 5q^3 + 6q^4 + 10q^5 + 12q^6 + 18q^7 + O(q^8) \\ y &= -q^{-4} - 2q^{-3} - 3q^{-2} + 17 + 68q + 208q^2 + 524q^3 + 1221q^4 + 2626q^5 + 5385q^6 + O(q^7). \end{aligned}$$

Using these q expansions and elementary linear algebra, we find that

$$y^2 - x^8 + 12x^7 - 50x^6 + 108x^5 - 131x^4 + 76x^3 + 10x^2 - 44x + 19$$

is a function on $X_0(35)$ with a zero of order at least 20 at the cusp ∞. It follows from general principles that this function is identically zero. Replacing x by $x+1$ gives the equation

$$\begin{aligned} y^2 &= x^8 - 4x^7 - 6x^6 - 4x^5 - 9x^4 + 4x^3 - 6x^2 + 4x + 1 && (5) \\ &= (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1), && (6) \end{aligned}$$

which is the affine piece of $X_0(35)$.

Now, since W_5 is an involution, we know that the map $X_0(35) \longrightarrow X_0(35)/W_5$ has degree 2. Moreover, we have seen that the genus of $X_0(35)/W_5$ is 1 while the genus of $X_0(35)$ is 3. By Hurwitz's formula, we find that $X_0(35) \longrightarrow X_0(35)/W_5$ is ramified at four points. On physically examining the possible involutions of (6), we see that W_5 *must* correspond to the involution $x \mapsto -1/x,\ y \mapsto y/x^4$ since this is the only involution of (6) that ramifies at exactly four points (those corresponding to $x = \pm i$). It follows that the function field of $X_0(35)/W_5$ is generated by the functions $u = x - 1/x$ and $v = y(1 + 1/x^4)$. Straightforward calculations with (6) now show that $X_0(35)/W_5$ is given (at least in affine coordinates) by

$$v^2 = (u+1)(u^2+2)^2(u^3 - 5u^2 + 3u - 19.)$$

We know that this is an elliptic curve, and hence can put it in standard Weierstrass form by an appropriate birational transformation. We find [5, pg. 221] that the transformation

$$\begin{aligned} z &= \frac{7v}{2(u^2+2)(u+1)^2} - \frac{1}{2} \\ w &= \frac{u-6}{u+1} \end{aligned}$$

leads to

$$z^2 + z = w^3 + w^2 + 9w + 1, \tag{7}$$

or equivalently,

$$t^2 = s^3 + 4s^2 + 16 \cdot 9s + 16 \cdot 5. \tag{8}$$

We can use the method of Nagell-Lutz to determine the torsion group of (7). We find that the full torsion group is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and is given explicitly by the points $\{(1,3), (1,-4), O\}$. these points correspond to the values $w = 1, \infty$, which in turn correspond to $u = \infty, -1$. Since $u = x - 1/x$, we observe that $u = \infty$ comes from $x = 0, \infty$ and $u = -1$ does not come from a rational value of x. Since $x = 0, \infty$ are cusps of $X_0(35)$, we see that none of the torsion points of $X_0(35)/W_5$ come from non-cuspidal rational points of $X_0(35)$.

We can again appeal to **PARI** to compute that

$$L_{X_0(35)/W_5}(1) = 0.70291123913490551515799588 67\ldots,$$

so that (by BSD for modular elliptic curves of analytic rank 0) the rank of $X_0(35)/W_5(\mathbb{Q})$ is zero.

Of course, It can also be shown by the methods of the preceeding section that the elliptic curve (8) has rank 0. We will not carry this out here.

At any rate, we see that $X_0(35)$ has no rational points other than cusps. Thus, there are no elliptic curves E defined over $\mathbb{Q}$ with a rational point of order 35.

References

[1] Birch, B.J. and W. Kyuk, eds. *Modular Functions of One Variable IV*, Springer-Verlag LNM 476 (1975).

[2] Billing, G., and K. Mahler. On exceptional points on cubic curves. J. London Math. Soc. **15**, 32–43 (1940).

[3] Connell, I. Points of order 11 on Elliptic Curves. Nieuw Archief voor Wisk. 13, **3**, 257–288 (1995).

[4] Galbraith, S. Equations for Modular Curves. http://www.isg.rhul.ac.uk/~sdg/thesis.html (1996).

[5] Kubert, D. Universal Bounds on the Torsion of Elliptic Curves. Proc. London Math. Soc. (3) **33**, 193–237 (1976).

[6] Mazur, B., and J. Tate. Points of Order 13 on Elliptic Curves. Inventiones math. **22**, 41–49 (1973).

[7] Ogg, A. Rational Points of Finite Order on Elliptic Curves. Inventiones math. **12**, 105–111 (1971).

[8] Silverberg, A. Open Questions in Arithmetic Algebraic Geometry. In "Arithmetic Algebraic Geometry," (B. Conrad and K. Rubin, eds). American Math. Soc. IAS/Park City, Vol. 9 (2001).

[9] Stein, W. The Modular Forms Database: Tables. http://modular.fas.harvard.edu/Tables/basis_cuspforms/basis_gamma0.html.