A CURVE FOR WHICH COLEMAN'S EFFECTIVE CHABAUTY BOUND IS SHARP

DAVID GRANT

(Communicated by William Adams)

Abstract. We show that Coleman's effective Chabauty bound is sharp for the curve \( C : y^2 = x(x-1)(x-2)(x-5)(x-6) \) defined over \( \mathbb{Q} \), by considering its reduction mod 7. We also show that the Jacobian of \( C \) is absolutely simple.

Let \( C \) be the curve
\[
y^2 = x(x-1)(x-2)(x-5)(x-6)
\]
defined over \( \mathbb{Q} \) and \( J(C) \) its Jacobian. Recently Gordon and the author computed that \( J(C)(\mathbb{Q}) \cong \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^4 \) [GG].

Proposition 1. Let \( P_\infty \) denote the point at infinity on \( C \). Then
\[
C(\mathbb{Q}) = \{ P_\infty, (0, 0), (1, 0), (2, 0), (5, 0), (6, 0), (3, 6), (3, -6), (10, 120), (10, -120) \}.
\]

Proof. The genus of \( C \) is 2, which is greater than the Mordell-Weil rank of \( J(C)(\mathbb{Q}) \), so Chabauty's Theorem [Ch] shows that \( #C(\mathbb{Q}) \) is finite (of course so does Faltings's Theorem [F]). For any \( q \) a power of a prime, we let \( \mathbb{F}_q \) be the field with \( q \) elements. The proof of Corollary 4.6 of [Co] shows that if \( X \) is a curve of genus \( g \geq 2 \) over \( \mathbb{Q} \), if the Mordell-Weil rank of the Jacobian of \( X \) over \( \mathbb{Q} \) is less than \( g \), if \( p > 2g \) is a prime of good reduction for \( X \), and if \( \tilde{X} \) is the reduction of \( X \) mod \( p \), then \( #X(\mathbb{Q}) \leq #\tilde{X}(\mathbb{F}_p) + 2g - 2 \). The proposition follows once we note that \( C \) has good reduction at \( p = 7 \), that \( #\tilde{C}(\mathbb{F}_7) = 8 \), and that the stated points lie on the curve.

So far as I know, \( C \) is the first example of a curve (whose Jacobian has Mordell-Weil rank > 0) whose rational points were determined by Coleman's bound. (See also [M].) Of course if \( C \) covered an elliptic curve over \( \mathbb{Q} \) of rank 0, then \( C(\mathbb{Q}) \) could also be determined via the cover. We now show that \( C \) covers no elliptic curves.

Proposition 2. \( J(C) \) is absolutely simple.

Proof. The following argument was worked out jointly with Jaap Top. If \( J(C) \) were not absolutely simple, then there would be a pair of elliptic curves \( E_1 \) and \( E_2 \) with...
$E_2$ and an isogeny $\phi: J(C) \to E_1 \times E_2$, where $E_1$, $E_2$, and $\phi$ are all defined over some number field $K$. We will derive a contradiction by comparing the $L$-function of $C$ with those of $E_1$ and $E_2$.

Note that by (1), $C$ has good reduction at the prime $p = 11$. Let $\hat{C}$ denote the reduced curve. It is shown in [T] that if $N_2 = \#\hat{C}(\mathbb{F}_{11})$, then the $L$-function of $\hat{C}$ over $\mathbb{F}_{11}$ is $L(\hat{C}/\mathbb{F}_{11}, t) = 1 - at + bt^2 - 11at^3 + 121t^4$, where $a = 11 + 1 - N_1$ and $b = (1/2)(N_2 + N_1^2) - (1 + 11)N_1 + 11$. A calculation shows that $\#\hat{C}(\mathbb{F}_{11}) = 16$ and $\#\hat{C}(\mathbb{F}_{121}) = 118$, so $L(\hat{C}/\mathbb{F}_{11}, t) = 1 + 4t + 6t^2 + 44t^3 + 121t^4$.

By the functional equation $L(\hat{C}/\mathbb{F}_{11}, t) = 11^2t^4L(\hat{C}/\mathbb{F}_{11}, 1/11t)$, the $L$-function factors over its splitting field as $(1 - \alpha t)(1 - ((1/11)\alpha) t)(1 - \beta t) \times (1 - (11/\beta)t)$, for some $\alpha$, $\beta$. So if we set $(1 - \alpha t)(1 - ((1/11)\alpha) t) = 1 + ut + 11t^2$, $(1 - \beta t)(1 - (11/\beta)t) = 1 + vt + 11t^2$, we can take $u = 2 + 2\sqrt{5}$, $v = 2 - 2\sqrt{5}$. Therefore if $\zeta_5 = e^{2\pi i/5}$, then $\zeta_5 + \zeta_5^{-1} = (\sqrt{5} - 1)/2$, and solving the quadratics we get

$$
\alpha = -2\zeta^2_5 - 2\zeta^3_5 \pm (\zeta_5 - \zeta^2_5 + \zeta^3_5 - \zeta^4_5), \\
\beta = -2\zeta_5 - 2\zeta^4_5 \pm (\zeta_5 + \zeta^2_5 - \zeta^3_5 - \zeta^4_5).
$$

Let $\mathcal{P}$ be a prime of $K$ above 11, and suppose that the absolute norm of $\mathcal{P}$ is $11^f$. Then $\mathcal{P}$ is a prime of good reduction for $C$, and so also for $J$ and $E_1$ and $E_2$.

Let $\ell$ be a prime not dividing 11. Recall that for any $s$, the Frobenius $F_{11}^s$ on $J(\hat{C})$ over $\mathbb{F}_{11^s}$ induces an endomorphism $F_{11}^s$ on the Tate module $T_s(J(\hat{C}))$, and that $L(\hat{C}/\mathbb{F}_{11^s}, t) = \det(1 - F_{11^s}^s T_s(J(\hat{C})))$. For any prime $\ell$ not dividing the degree of $\phi$, we get an isomorphism $T_\ell(J(C)) \cong T_\ell(E_1) \times T_\ell(E_2)$ over $K$, and so using the functional equations of $L(E_i/\mathbb{F}_{11^f}, t)$ for $i = 1, 2$, we have that

$$
L(\hat{C}/\mathbb{F}_{11^f}, t) = L(\hat{E}_1/\mathbb{F}_{11^f}, t)L(\hat{E}_2/\mathbb{F}_{11^f}, t) = (1 - a_1 t + 11^f t^2)(1 - a_2 t + 11^f t^2),
$$

for some integers $a_1$ and $a_2$. But the Frobenius on $J(C)$ over $\mathbb{F}_{11^f}$ is $(F_{11})^f$, so

$$
L(\hat{C}/\mathbb{F}_{11^f}, t) = (1 - \alpha^f t)(1 - (11/\alpha)^f t)(1 - \beta^f t)(1 - (11/\beta)^f t).
$$

Renumbering $E_1$ and $E_2$ if necessary, from (3) and (4) we can set

$$
(1 - \alpha^f t)(1 - (11/\alpha)^f t) = (1 - a_1 t + 11^f t^2),
$$

which means that $[\mathbb{Q}(\alpha^f) : \mathbb{Q}] = 1$ or 2. Since $\alpha \in \mathbb{Q}(\zeta_5)$, which has a unique quadratic subfield, we can assume $\alpha^f \in \mathbb{Q}(\sqrt{5})$. If we let $\sigma$ denote complex conjugation, then $\alpha^f = \sigma(\alpha^f) = (\sigma(\alpha))^f$; so $\alpha/\sigma(\alpha))^f = 1$. Therefore $(\alpha/\sigma(\alpha))^f$ is a root of unity in $\mathbb{Q}(\zeta_5)$, and hence a $10^{th}$-root of unity. Therefore $\alpha^{10} \in \mathbb{Q}(\sqrt{5})$. But a calculation with (2) shows this is not the case, so $J(C)$ is absolutely simple.

References


A CURVE FOR WHICH COLEMAN'S EFFECTIVE CHABAUTY BOUND IS SHARP


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO AT BOULDER, BOULDER, COLORADO 80309-0395
E-mail address: grant@boulder.colorado.edu