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 \( \text{mod } 7 \). 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 \( \bar{X} \) is the reduction of \( X \) \( \text{mod } p \), then \( \#X(\mathbb{Q}) \leq \#\bar{X}(\mathbb{F}_p) + 2g - 2 \). The proposition follows once we note that \( C \) has good reduction at \( p = 7 \), that \( \#C(\mathbb{F}_7) = 8 \), 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]1.) 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 \( E_2 \)
$E_2$ 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 $\tilde{C}$ denote the reduced curve. It is shown in [T] that if $N_\ell = \#\tilde{C}(\mathbb{F}_{11^\ell})$, then the $L$-function of $\tilde{C}$ over $\mathbb{F}_{11}$ is $L(\tilde{C}/\mathbb{F}_{11}, t) = 1 - at + bt^2 - 11at^3 + 121t^4$, where $a = 11 + 1 - N_1$ and $b = (1/2)(N_2 + N_2^2) - (1 + 11)N_1 + 11$. A calculation shows that $\#\tilde{C}(\mathbb{F}_{11}) = 16$ and $\#\tilde{C}(\mathbb{F}_{121}) = 118$, so $L(\tilde{C}/\mathbb{F}_{11}, t) = 1 + 4t + 6t^2 + 44t^3 + 121t^4$.

By the functional equation $L(\tilde{C}/\mathbb{F}_{11}, t) = 11^2t^4L(\tilde{C}/\mathbb{F}_{11}, 1/11^t)$, the $L$-function factors over its splitting field as $(1 - at)(1 - (11/\alpha)t)(1 - \beta t)(1 - (11/\beta)t)$, for some $\alpha$, $\beta$. So if we set $(1 - at)(1 - (11/\alpha)t) = 1 + ut + 11t^2$, $(1 - \beta t)(1 - (11/\beta)t) = 1 + vt + 11t^2$, 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

\begin{align*}
\alpha &= -2\zeta_5^2 - 2\zeta_5^3 \pm (\zeta_5 - \zeta_5^2 + \zeta_5^3 - \zeta_5^4), \\
\beta &= -2\zeta_5 - 2\zeta_5^4 \pm (\zeta_5 + \zeta_5^2 - \zeta_5^3 - \zeta_5^4).
\end{align*}

Let $\mathcal{P}$ be a prime of $K$ above 11, and suppose that the absolute norm of $\mathcal{P}$ is 11. 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 $J(\tilde{C})$ over $\mathbb{F}_{11^s}$ induces an endomorphism $F_{11^s}$ on the Tate module $T_s(J(\tilde{C}))$, and that $L(\tilde{C}/\mathbb{F}_{11^s}, t) = \det(1 - F_{11^s}tT_s(J(\tilde{C})))$. 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 $L(E_i/\mathbb{F}_{11^s}, t)$ for $i = 1, 2$, we have that

\begin{equation}
L(\tilde{C}/\mathbb{F}_{11^s}, t) = L(E_1/\mathbb{F}_{11^s}, t)L(E_2/\mathbb{F}_{11^s}, t)
= (1 - a_1t + 11ift^2)(1 - a_2t + 11ift^2),
\end{equation}

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

\begin{equation}
L(\tilde{C}/\mathbb{F}_{11^s}, t) = (1 - \alpha s)(1 - (11/\alpha)s)(1 - \beta s)(1 - (11/\beta)s).
\end{equation}

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

\begin{equation}(1 - \alpha s)(1 - (11/\alpha)s) = (1 - a_1t + 11ift^2),\end{equation}

which means that $[\mathbb{Q}(\alpha s) : \mathbb{Q}] = 1$ or 2. Since $\alpha \in \mathbb{Q}(\zeta_5)$, which has a unique quadratic subfield, we can assume $\alpha s \in \mathbb{Q}(\sqrt{5})$. If we let $\sigma$ denote complex conjugation, then $\alpha s = \sigma(\alpha s) = (\sigma(\alpha))s$; so $(\alpha s\sigma(\alpha))s = 1$. Therefore $(\alpha/\sigma(\alpha))$ 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


**Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395**

*E-mail address: grant@boulder.colorado.edu*