SURJECTIVITY OF MOD $2^n$ REPRESENTATIONS OF ELLIPTIC CURVES

TIM AND VLADIMIR DOKCHITSER

Associated to an elliptic curve $E/\mathbb{Q}$ and a prime $l$ are representations

$$\bar{\rho}_l : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut} \frac{E[l^n]}{l^n} \cong \text{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$$

and their inverse limit, the $l$-adic representation

$$\rho_l : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut} \frac{T_lE}{l^n} \cong \text{GL}_2(\mathbb{Z}_l).$$

As explained by Serre ([2] IV, 3.4), for $l \geq 5$ the group $\text{SL}_2(\mathbb{Z}_l)$ has no proper closed subgroups that surject onto $\text{SL}_2(\mathbb{F}_l)$, so

$$\bar{\rho}_l \text{ surjective } \implies \rho_l \text{ surjective for } l \geq 5.$$ 

The condition $l \geq 5$ is necessary, and

$$\bar{\rho}_l \text{ surjective } \nRightarrow \bar{\rho}_{ln+1} \text{ surjective for } l^n = 2, 3, 4.$$ 

Elliptic curves with surjective mod 3 but not mod 9 representation have been classified by Elkies [1], and the purpose of this note is to do this in the ‘2 not 4’ and ‘4 not 8’ cases as well:

**Theorem.** Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$ with discriminant $\Delta = -16(4a^3 + 27b^2)$ and $j$-invariant $j = -1728(4a)^3/\Delta$. Then

1. $\bar{\rho}_2$ is surjective $\Leftrightarrow$ $x^3 + ax + b$ is irreducible and $\Delta \notin \mathbb{Q}^\times 2$.
2. $\bar{\rho}_4$ is surjective $\Leftrightarrow$ $\bar{\rho}_2$ is surjective, $\Delta \notin -1 \cdot \mathbb{Q}^\times 2$ and $j \neq -4t^3(t + 8)$ for any $t \in \mathbb{Q}$.
3. $\bar{\rho}_8$ is surjective $\Leftrightarrow$ $\bar{\rho}_4$ is surjective and $\Delta \notin \pm 2 \cdot \mathbb{Q}^\times 2$.

**Proof.** The $x$-coordinates of the three non-trivial 2-torsion points are the roots of $x^3 + ax + b$ and their $y$-coordinates are 0. So $\bar{\rho}_2$ surjects onto $\text{GL}_2(\mathbb{F}_2) \cong S_3$ if and only if this cubic is irreducible and its discriminant $\Delta/16$ is not a square. Note that this proves (1) and that $\mathbb{Q}(E[2])$ contains $\mathbb{Q}(\sqrt{\Delta})$.

Now recall that by the properties of the Weil pairing, $\mathbb{Q}(E[n]) \supset \mathbb{Q}(\zeta_n)$ and the corresponding map $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is simply the determinant. In particular,

$$\mathbb{Q}(E[4]) \supset \mathbb{Q}(\sqrt{\Delta}, \sqrt{-1}) \text{ and } \mathbb{Q}(E[8]) \supset \mathbb{Q}(\sqrt{\Delta}, \sqrt{-1}, \sqrt{2}).$$

Incidentally, as there are elliptic curves whose 2-torsion defines an $S_3$-extension of $\mathbb{Q}$ which is disjoint from $\mathbb{Q}(\zeta_8)$, e.g. $y^2 = x^3 - 2$, this shows that the canonical maps (mod 2, det)

$$\text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow S_3 \times (\mathbb{Z}/4\mathbb{Z})^\times \text{ and } \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) \longrightarrow S_3 \times (\mathbb{Z}/8\mathbb{Z})^\times$$

*Date: April 25, 2011.*
are surjective (being already surjective on the subgroups \(\text{Im} \tilde{\rho}_4\) and \(\text{Im} \tilde{\rho}_8\) for this elliptic curve). Hence, if an elliptic curve \(E/\mathbb{Q}\) has surjective \(\tilde{\rho}_4\), then \(\mathbb{Q}(E[2], \zeta_4)\) has degree 12, so \(\mathbb{Q}(\sqrt{\Delta}, \sqrt{-1})\) has degree 4. Similarly, if \(\tilde{\rho}_8\) is surjective, then \(\mathbb{Q}(\sqrt{\Delta}, \sqrt{-1}, \sqrt{2})\) has degree 8.

(3) If \(\tilde{\rho}_8\) is surjective, then so is \(\tilde{\rho}_4\), and as \(\mathbb{Q}(\sqrt{\Delta}) \neq \mathbb{Q}(\sqrt{\pm 2})\), it follows that \(\Delta \notin \pm 2 \cdot \mathbb{Q}^\times\). Conversely, if \(\tilde{\rho}_4\) is surjective and \(\Delta \notin \pm 2 \cdot \mathbb{Q}^\times\), then \(\mathbb{Q}(\sqrt{\Delta}, \sqrt{-1}, \sqrt{2})\) is a \(C_2 \times C_2 \times C_2\)-extension of \(\mathbb{Q}\). So \(\text{Im} \tilde{\rho}_8\) surjects onto \(\text{GL}_2(\mathbb{Z}/4\mathbb{Z})\) and onto \((\mathbb{Z}/8\mathbb{Z})^\times\), and possesses a \(C_2 \times C_2 \times C_2\)-quotient. A computation shows that the only such subgroup of \(\text{GL}_2(\mathbb{Z}/8\mathbb{Z})\) is the full group itself.

(2) The argument is the same as for (3), except that in this case \(\text{GL}_2(\mathbb{Z}/4\mathbb{Z})\) does have a (unique up to conjugacy) proper subgroup which surjects onto \(\text{GL}_2(\mathbb{Z}/2\mathbb{Z})\) and onto \((\mathbb{Z}/4\mathbb{Z})^\times\), and has a \(C_2 \times C_2\)-quotient. This group has index 4, and is conjugate to \(H_{24} = \langle (\frac{0}{1}, \frac{1}{0}), (\frac{0}{1}, \frac{1}{1}) \rangle \cong C_3 \rtimes D_8\). The following lemma completes the proof. \(\square\)

**Lemma.** Let \(E/\mathbb{Q}\) be the elliptic curve \(y^2 = x^3 + ax + b\) with \(b \neq 0\). The following conditions are equivalent:

1. \(\text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})\) is conjugate to a subgroup of \(H_{24}\).
2. The polynomial \(f(x) = x^4 - 4ax^3 + 6a^2x^2 + 4(7a^3 + 54b^2)x + (17a^4 + 108ab^2)\) has a rational root.
3. \(j(E) = -4t^3(t + 8)\) for some \(t \in \mathbb{Q}\).

**Proof.** (1)\(\iff\) (2). Regard \(a\) and \(b\) as indeterminants and \(E\) as a curve over \(K = \mathbb{Q}(a, b)\). Consider the 4-torsion polynomial (cf. \(\psi_4\) in [3] Exc. III.3.7)

\[
\psi(x) = x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - (a^3 + 8b^2).
\]

Its roots \(x_1, \ldots, x_6 \in \bar{K}\) are the \(x\)-coordinates of the primitive 4-torsion points of \(E\). Pick a basis \(P = (x_1, y_1), Q = (x_2, y_2)\) for the 4-torsion, and for each of the four left cosets \(C\) of \(H_{24}\) in \(\text{GL}_2(\mathbb{Z}/4\mathbb{Z})\) define

\[
\theta_C = \sum_{g \in C} x(gP)x(gQ),
\]

where \(x(\cdot)\) is the \(x\)-coordinate. The \(\theta_C\) are distinct, which can be checked by specialising e.g. \(a \mapsto 0, b \mapsto 1\), where the numbers are \(0, -6, 3 \pm 3\sqrt{-3}\).

Now for \(h \in \text{Gal}(K(E[4])/K) \subset \text{GL}_2(\mathbb{Z}/4\mathbb{Z})\) we have \(h(\theta_C) = \theta_{hC}\), and hence the polynomial

\[
\tilde{f}(x) = \prod_{C}(x - \theta_C) = \sum_{i=0}^{4} \lambda_i x^i
\]

has coefficients in \(K\). The roots \(x_i \in \bar{K}\) of \(\psi\) are integral over \(R = \mathbb{Z}[a, b]\), and therefore so are the \(\theta_C\). Because \(R\) is integrally closed in its field of fractions \(K\) and the \(\lambda_i\) are both in \(K\) and are integral over \(R\), they lie in \(R\). Moreover, if we rescale \(a \mapsto s^2a, b \mapsto s^3b\), then the roots of \(\psi(x)\) change to
\(x_i \mapsto sx_i\), and therefore \(\theta_C \mapsto s^2\theta_C\). So \(\lambda_i\) must have weight \(2i\), in the sense that

\[
\lambda_1 \in \mathbb{Z}a, \quad \lambda_2 \in \mathbb{Z}a^2, \quad \lambda_3 \in \mathbb{Z}a^3 + \mathbb{Z}b^2 \quad \text{and} \quad \lambda_4 \in \mathbb{Z}a^4 + \mathbb{Z}ab^2.
\]

Now we can compute \(\tilde{f}\) numerically for a few specialisations \(a, b \in \mathbb{Z}\) (using complex uniformisation of torsion points and rounding the coefficients) to deduce the exact formulae for the \(\lambda_i\), and we find that \(\tilde{f}(x) = f(4x)\).

Let us return to \(a, b \in \mathbb{Q}\), constructing \(\psi, \theta_C\) and \(\tilde{f}\) in the same way. Note that the discriminant of \(f\) is \(3^6b^2\Delta_E\), so it has no repeated roots and the \(\theta_C\) are distinct. Now \(h: \theta_C \mapsto \theta_{hC}\) defines a transitive action of \(\text{GL}_2(\mathbb{Z}/4\mathbb{Z})\) on these, and for \(h \in \text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})\) it coincides with the Galois action \(\theta_C \mapsto h(\theta_C)\). Because all four \(\theta_C\) are distinct, the stabiliser of \(\theta_{H_{24}}\) is precisely \(H_{24}\), and the stabilisers of the others are the conjugates of \(H_{24}\). So \(\text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})\) is conjugate to a subgroup of \(H_{24}\) if and only if one of the \(\theta_C\) is rational, equivalently if \(f\) has a rational root.

\((2) \iff (3)\). First note that if \(a = 0\), equivalently \(j = 0\), then both conditions are satisfied (\(f(0) = 0\) and \(j = 0\)). Suppose \(a \neq 0\) and that \(f(x)\) has a rational root \(r\). Then \(u = r/a\) satisfies

\[
\frac{b^2}{a^3} + 6u^2 + 4(7 + 54\frac{b^2}{a^3})u + (17 + 108\frac{b^2}{a^3}) = 0.
\]

Rewriting \(\frac{b^2}{a^3}\) in terms of \(j = \frac{1728(4a)^3}{10(4a^2 + 27b^2)}\) (namely \(\frac{b^2}{a^3} = -\frac{4(j-1728)}{27j}\)), we find that \(j = -27648\frac{2n+1}{(u-1)^2}\). Replacing \(u\) by \(\frac{12}{12} + 1\) we get \(j = -4t^3(t+8)\), as claimed. Reversing the argument gives the other implication as well. \(\square\)

**Remark.** The elliptic curve

\[
y^2 = x^3 - \frac{3t^2 + 24t}{t^2 - 4t + 12}x - \frac{2t^2 + 28t + 96}{t^2 - 4t + 12} (t \neq -8)
\]

has \(j\)-invariant \(-4t^3(t+8)\). So for every curve of this form the polynomial \(f(x)\) has a rational root and, conversely, every elliptic curve over \(\mathbb{Q}\) for which \(f(x)\) has a rational root is a twist of a curve in the family.

**Acknowledgements.** We would like to thank Matt Greenberg and Gagan Sekhon for asking the questions that led to this work. The first author is supported by a Royal Society University Research Fellowship.

**References**

[1] N. Elkies, Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9, preprint, 2006.

[2] J.-P. Serre, Abelian \(l\)-adic Representations and Elliptic Curves, Addison-Wesley 1989.

[3] J. H. Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag 1986.