$\mathbb{Q}$-curves and Galois representations

Jordan S. Ellenberg *
Princeton University
ellenber@math.princeton.edu

30 Jan 2003

Introduction and definitions

Let K be a number field, Galois over $\mathbb{Q}$. A $\mathbb{Q}$-*curve* over K is an elliptic curve over K which is isogenous to all its Galois conjugates. The current interest in $\mathbb{Q}$-curves, it is fair to say, began with Ribet's observation [27] that an elliptic curve over $\bar{\mathbb{Q}}$ admitting a dominant morphism from $X_1(N)$ must be a $\mathbb{Q}$-curve. It is then natural to conjecture that, in fact, all $\mathbb{Q}$-curves are covered by modular curves. More generally, one might ask: from our rich storehouse of theorems about elliptic curves over $\mathbb{Q}$, which ones generalize to $\mathbb{Q}$-curves?

In this paper, we discuss recent progress towards several problems of this type, and some Diophantine applications. We will also state several open problems which seem both interesting and accessible to existing methods.

Remark 1. Elliptic curves with complex multiplication supply a natural population of $\mathbb{Q}$-curves. Indeed, the original use of the term "$\mathbb{Q}$-curve", by Gross [13], referred to CM curves exclusively. The arithmetic of CM curves is much more fully understood than that of curves without extra endomorphisms. For that reason, we will assume hereafter that our $\mathbb{Q}$-curves are *not* CM.

One might think of the class of $\mathbb{Q}$-curves as the "mildest possible generalization" of the class of elliptic curves over $\mathbb{Q}$. For many structures on elliptic curves over $\mathbb{Q}$ are invariant under isogeny. And since a $\mathbb{Q}$-curve E/K has an isogeny class which is fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we should expect that any isogeny-invariant structure of elliptic curves over $\mathbb{Q}$ can be defined for $\mathbb{Q}$-curves as well.

The structure we have chiefly in mind is the ℓ-adic Galois representation

$$\rho_{C,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{End}(T_\ell C)$$

attached to any elliptic curve C over $\mathbb{Q}$. The isomorphism class of $\rho_{E,\ell}$ depends only on the isogeny class of C, and so one expects to find ℓ-adic representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ attached to $\mathbb{Q}$-curves as well. Indeed, given a $\mathbb{Q}$-curve E/K, there exists a representation

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{Q}}_\ell^* \,\mathrm{GL}_2(\mathbb{Q}_\ell)$$

such that the restriction $\rho_{E,\ell}|K$ agrees, up to multiplication by scalars, with the action of $\mathrm{Gal}(\bar{K}/K)$ on $T_\ell E$. We define $\rho_{E,\ell}$ as follows. For each $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, let $\mu_\sigma : E^\sigma \to E$ be an isogeny. Then we can define

$$\tilde{\rho}_{E,\ell}(\sigma) \in \mathrm{GL}(T_\ell E)$$

*Partially supported by NSA Young Investigator Grant MDA905-02-1-0097.

by the rule

$$\tilde{\rho}_{E,\ell}(\sigma)(P) = \mu_\sigma(P^\sigma).$$

Now $\tilde{\rho}_{E,\ell}$ is not a homomorphism from $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{GL}(T_\ell E)$. However, it is easily checked that

$$\tilde{\rho}_{E,\ell}(\sigma)\tilde{\rho}_{E,\ell}(\tau)\tilde{\rho}_{E,\ell}(\sigma\tau)^{-1}$$

acts on $T_\ell E$ in the same way as does

$$c_E(\sigma,\tau) = (1/\deg \mu_{\sigma\tau})\mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^\vee \in (\mathrm{Hom}(E,E) \otimes_{\mathbb{Z}} \mathbb{Q})^* = \mathbb{Q}^*.$$

In particular, the projectivizations of the $\tilde{\rho}_{E,\ell}(\sigma)$ fit together into a projective Galois representation

$$\mathbb{P}\rho_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Q}_\ell).$$

It is easy to check that c_E is a cocycle in $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mathbb{Q}^*)$. A theorem of Tate shows that c_E is trivial when the coefficients are extended from $\mathbb{Q}$ to $\bar{\mathbb{Q}}$, and this gives the existence of $\rho_{E,\ell}$. One point of view is that $\rho_{E,\ell}$ is the ℓ-adic Galois representation attached to an abelian variety of GL_2-type, which admits E as a factor over $\bar{\mathbb{Q}}$ [27, §6].

Note that the description above defines $\rho_{E,\ell}$ only up to twisting by scalars. In some cases there may be a "best" choice among the twists of $\rho_{E,\ell}$, but in this paper we will always take the projectivization $\mathbb{P}\rho_{E,\ell}$ as our real object of interest. This projective Galois representation is an invariant of the *geometric* isogeny class of E.

What kinds of $\mathbb{Q}$-curves are there?

A priori, a $\mathbb{Q}$-curve can be defined over an arbitrarily complicated number field. Of course, a $\mathbb{Q}$-curve defined over a large number field L might be geometrically isogenous to a curve over a smaller number field K. In fact, if we are considering $\mathbb{Q}$-curves only up to isogeny, we may assume that K is a compositum of quadratic extensions of $\mathbb{Q}$. (Of course, this would be false if we allowed our $\mathbb{Q}$-curves to have CM!)

Theorem 2 (Elkies,[6]). *Let E be a $\mathbb{Q}$-curve (without complex multiplication) over a number field L. Then E is geometrically isogenous to a $\mathbb{Q}$-curve E'/K, where K is a Galois extension of $\mathbb{Q}$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^r$.*

See [28] for a slightly more general version of this theorem with a different proof.

One naturally wishes to place $\mathbb{Q}$-curves in a moduli space. The presence of discrete invariants (for instance, the minimal degree of an isogeny between E and its Galois conjugate) ensures that no single connected moduli space will parametrize all $\mathbb{Q}$-curves. However, if all discrete invariants are held constant, the category of $\mathbb{Q}$-curves is indeed parametrized by a modular curve.

To fix ideas, consider the class of $\mathbb{Q}$-curves E which are defined over quadratic fields K, and which admit cyclic isogenies of degree d, defined over K, to their Galois conjugates. We call such an E a *$\mathbb{Q}$-curve of degree d*. Let E^σ/K be the Galois conjugate of E. Then the isogeny $\phi : E \to E^\sigma$ is represented by a point of $X_0(d)(K)$. Moreover, the Galois conjugate P^σ represents an isogeny $\phi^\sigma : E^\sigma \to E$. Since E does not have CM, ϕ^σ can only be $\pm\hat{\phi}$. In other words, P^σ is the image of P under the Atkin-Lehner involution w_d. It follows that the image of P in the quotient curve $X_0(d)/w_d$ is defined over $\mathbb{Q}$.

Let N be a squarefree positive integer, and let $X^*(N)$ be the quotient of $X_0(N)$ by the group generated by all Atkin-Lehner involutions $w_p, p|N$. If x is a point of $X^*(N)(\mathbb{Q})$ lying under a point

y of $X_0(N)(K)$ for some number field K, and if E/K is an elliptic curve parametrized by y; then the Galois conjugates of E lie in the orbit of E under the Atkin-Lehner involutions. In particular, the Galois conjugates of E are all isogenous to E, and E is a $\mathbb{Q}$-curve.

What Elkies in fact proves in [6] is that every non-CM $\mathbb{Q}$-curve is isogenous to one parametrized, as above, by a rational point of $X^*(N)$. So the title question of this section can be rephrased as follows: what are the rational points on $X^*(N)$? More precisely: what are the rational points on $X^*(N)$ which are neither cusps nor CM points?

We first observe that, as with the modular curves $X_0(N)$, the curves $X^*(N)$ have genus greater than 2 when N is sufficiently large. Gonzalez and Lario [12] give a complete list of the N for which $X^*(N)$ has genus 0 or 1; there are 43 values of N for which $X^*(N)$ is rational and 38 values such that $X^*(N)$ has genus 1. In many of the cases where $X^*(N)$ is rational, explicit equations for the corresponding family of $\mathbb{Q}$-curves have been worked out: see [12], [14],[16],[17], [24].

Since $X^*(N)$ has finitely many points for N sufficiently large, it is natural to make the following conjecture, which was first formulated (in somewhat greater generality) by Elkies. We call a point on $X^*(N)$ which is neither cuspidal nor CM an *exceptional point.*

Conjecture 3. There are only finitely many positive squarefree integers N such that $X^*(N)(\mathbb{Q})$ contains an exceptional point.

Several examples of exceptional points are known: [6] exhibits an exceptional point on $X^*(191)$, and Galbraith ([9],[10]) gives several more examples of exceptional points on $X^*(N)$, with N as large as 311.

We should emphasize that the method used by Mazur in [21] to control rational points on $X_0(N)$ is not directly applicable to Conjecture 3. Mazur's argument bounds the rational points on a curve X by means of a morphism

$$X \to A$$

where A is an abelian variety with $|A(\mathbb{Q})| < \infty$. But each simple factor A of the Jacobian of $X^*(N)$ is associated to a newform of weight 2 and level N whose functional equation has sign -1. Under the Birch-Swinnerton-Dyer conjecture, every such A has infinite Mordell-Weil group, so Mazur's argument does not apply. Note that this is the same difficulty that arises in the older problem of showing that the modular curve $X_{non-split}(p)$ does not have rational points for p large enough.

On the other hand, Mazur's method may apply if we specify the field of definition K of the $\mathbb{Q}$-curve. For example, Mazur shows in [21, §8] that, if K is a quadratic imaginary field, and N is a sufficiently large prime which is inert in K, then $X_0(N)(K)$ is empty. In particular, there are no $\mathbb{Q}$-curves over K of degree N. More generally, let K be a quadratic field, χ the corresponding quadratic Dirichlet character, and σ a generator for $\mathrm{Gal}(K/\mathbb{Q})$. Let N be a prime. We denote by $X_0^\chi(N)/\mathbb{Q}$ the modular curve admitting an isomorphism

$$\phi : X_0^\chi(N) \times_{\mathbb{Q}} K \to X_0(N) \times_{\mathbb{Q}} K$$

satisfying $\phi^\sigma = w_N \circ \phi$. Note that ϕ induces a bijection between $X_0^\chi(N)(\mathbb{Q})$ and the points P of $X_0(N)(K)$ satisfying $P^\sigma = w_N P$. In particular, every $\mathbb{Q}$-curve of degree N over K is parametrized by a point of $X_0^\chi(N)(\mathbb{Q})$.

The cuspidal points of $X_0^\chi(N)$ are no longer defined over $\mathbb{Q}$, so it is not immediately clear that $X_0^\chi(N)$ has any rational points at all, even locally.

Problem A: For which χ and N does $X_0^\chi(N)$ have rational points over every completion of $\mathbb{Q}$?

Noam Elkies pointed out to me that the answer to Problem A is certainly not "all χ and N"; for instance, the genus-0 curve $X_0^\chi(5)$ is a Brauer-Severi curve which is rational if and only if 5 is a norm from K.

Even if $X_0^\chi(N)$ has local points, one should be able to use Mazur's argument to obtain reduction information about the corresponding $\mathbb{Q}$-curves.

Problem B: Suppose K is a real quadratic field, and let N be a prime which splits in K. Suppose E is a $\mathbb{Q}$-curve over K of degree N. Show that E has potentially good reduction at all primes greater than 3.

The conditions on N and K imply that the Jacobian of $X_0^\chi(N)(\mathbb{Q})$ has quotients of the form A_f, where f is a cusp form whose functional equation has sign $+1$. By the results of Kolyvagin and Logachev, in order to show A_f has rank 0, it suffices to show that the special value of the L-function $L(f,s)$ at $s=1$ is nonzero. This should be achievable by an averaging argument as in [8]. One then applies Corollary 4.3 of [21] to obtain the desired result. Can the arguments of [21, §5,6,7] be modified to show that under some circumstances there are no rational points on $X_0^\chi(N)$?

We have seen already that $\mathbb{Q}$-curves yield rational points on $X^*(N)$; the problem of describing a $\mathbb{Q}$-curve attached to a point of $X^*(N)(\mathbb{Q})$ is more subtle, due to the fact that $X^*(N)$ is not a fine moduli space. In particular, it is a delicate matter to determine a number field K over which all Galois conjugates of E and the isogenies between them can be defined. We will not treat this problem here, simply referring the reader to [24], [25], [11].

Modularity

We say a $\mathbb{Q}$-curve E is *modular* if $\rho_{E,\ell}$ is the ℓ-adic Galois representation attached to a cusp form on $\Gamma_1(N)$ for some N. Equivalently, E is a quotient of $J_1(N)_{\bar{\mathbb{Q}}}$. Note that this definition depends only on $\mathbb{P}\rho_{E,\ell}$.

Ribet showed in [27] that every elliptic curve over $\bar{\mathbb{Q}}$ which admitted a non-constant morphism from $J_1(N)$ for any N is a $\mathbb{Q}$-curve. He also conjected the converse:

Conjecture 4 (Ribet). All $\mathbb{Q}$-curves are modular.

Naturally, progress towards this conjecture followed very closely upon the work of Wiles on modular deformations. Since this technique involves passing between ℓ-adic and mod-ℓ representations, we now introduce the mod ℓ representation

$$\bar{\rho}_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^* \,\mathrm{GL}_2(\mathbb{F}_\ell)$$

associated to a $\mathbb{Q}$-curve E. Defining this representation is subtle only when ℓ divides the degree μ_σ for some σ [7, Def. 2.14].

The first advance towards Conjecture 4 was made by Hasegawa, Hashimoto, and Momose [15]. Their idea was to consider a prime $\ell \geq 5$ such that one of the isogenies

$$\mu_\sigma : E^\sigma \to E$$

has squarefree degree which is a multiple of ℓ. Then the curve E/K admits a rational ℓ-isogeny, which means the image of G_K under $\bar{\rho}_{E,\ell}$ lies in a Borel subgroup. In fact, under certain circumstances the authors show that the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ under $\bar{\rho}_{E,\ell}$ is a dihedral group. But dihedral Galois representations are known classically to be modular, so one can use the theorems of Wiles, Taylor-Wiles, and Diamond to conclude that the deformation $\rho_{E,\ell}$ of $\bar{\rho}_{E,\ell}$ is modular as well. Hida, working independently, proved a similar result using a similar method in [18], as did Momose and Shimura [23]. A typical result is the following:

Theorem 5 (Hida,[18]). *Let E be a quadratic $\mathbb{Q}$-curve of degree $p \geq 5$ over a quadratic field unramified at p. Then E is modular.*

This approach generalizes quite nicely to Hilbert-Blumenthal abelian varieties over $\bar{\mathbb{Q}}$ which are isogenous to all their Galois conjugates, or $\mathbb{Q}$-HBAV's: see [19, Cor. 3.3].

The results of [15],[18], and [23] yield modularity for many classes of $\mathbb{Q}$-curves. However, these theorems do not apply to $\mathbb{Q}$-curves of degree 2, a case which has particularly nice Diophantine applications described below. The author and Chris Skinner took a different approach to proving modularity of $\mathbb{Q}$-curves in [7]. Instead of exploiting the isogenies between conjugates, [7] uses the mod 3 representation attached to E, which has solvable projective image and is therefore modular by the Langlands-Tunnell theorem. The lifting theorems of Wiles, as refined by Conrad, Diamond, and Taylor, then yield a modularity result for $\mathbb{Q}$-curves, under certain local conditions at 3. For instance, one has the following theorem.

Theorem 6 (Ellenberg-Skinner,[7]). *Let E/K be a $\mathbb{Q}$-curve with semistable reduction at all primes of K dividing 3, and suppose that $K/\mathbb{Q}$ is unramified at 3. Then E is modular.*

There are infinitely many $\mathbb{Q}$-curves whose modularity has not yet been proven. One example is the curve

$$\begin{aligned} E : y^2 \quad = \quad & x^3 + (-994708512\sqrt{5257}\sqrt{73} - 414461880\sqrt{5257} - 4973542560\sqrt{73} - 1089620282520)x \\ & +366019575465 60\sqrt{5257}\sqrt{73} + 5349307626327168\sqrt{5257} \\ & +55021459817878848\sqrt{73} + 32065347994985088. \end{aligned}$$

This curve is parametrized by a point of $X^*(6)$; we obtained the equation by specializing the explicit description of the universal $\mathbb{Q}$-curve over $X^*(6)$ given by Quer in [24, §6] to the point $a = 2^2 \cdot 3^2 \cdot 73$.

The final proof of the Shimura-Taniyama conjecture for elliptic curves rests crucially on the use of the "$3 - 5$ switch." The ideas is as follows: suppose we wish to show an elliptic curve $C/\mathbb{Q}$ is modular, but the local behavior of C at 3 is so unpleasant that the 3-adic Tate module of C cannot be proved modular. Then one uses the rationality of the curve $X(5)$ to find a curve C' with an isomorphism of Galois modules

$$C[5] \cong C'[5]$$

and which has a "better" mod 3 representation. One then uses the 3-adic representation to show modularity of C', and the coincidence of mod 5 representations suffices to show that modularity of C' implies modularity of C.

This approach is unlikely to work for $\mathbb{Q}$-curves. For instance, let E be a $\mathbb{Q}$-curve of degree 2. Then the set of pairs (E', ϕ), where E' is a quadratic $\mathbb{Q}$-curve of degree 2 and ϕ is an isomorphism $\bar{\rho}_{E,5} \cong \bar{\rho}_{E',5}$, is parametrized by the rational points of a modular curve X, which is geometrically isomorphic to $X_0(2) \times_{X(1)} X(5)$. In order to execute the desired switch, one wants X to have many rational points. But in fact, X has genus 4. So one expects (though it's not clear how to prove!) that, for most E, there will be no other $\mathbb{Q}$-curve with the same mod 5 representation. In other words, no "switch" is available, and we are stuck with the 3-adic behavior of E, no matter how disagreeable. The proof of Ribet's conjecture in full, therefore, will require results on modular deformations on Galois representations which go beyond those currently available.

Problem C. New results on Artin's conjecture for icosahedral Galois representations have recently appeared ([1], [29].) Note especially that the result of [1] does not stipulate local conditions at 3. Can these theorems be used in place of the Langlands-Tunnell theorem to show modularity for some $\mathbb{Q}$-curves whose behavior over $\mathbb{Q}_3$ is very bad, but which, say, have good ordinary reduction at primes over 5?

Surjectivity of mod-p representations

The resolution of the Fermat problem rests on two crucial theorems concerning the Galois representations attached to elliptic curves over $\mathbb{Q}$. One, the modularity theorem of Wiles and Taylor-Wiles, we have already discussed. The other is the theorem of Mazur:

Theorem 7 (Mazur, [21]). *Let $C/\mathbb{Q}$ be an elliptic curve, and $p > 163$ a prime. Then $\bar{\rho}_{C,p}$ is irreducible.*

To what extent are theorems of this kind true for $\mathbb{Q}$-curves? The nice fact is that, in some sense, the situation for $\mathbb{Q}$-curves is *better* than that for elliptic curves over $\mathbb{Q}$.

Theorem 8 ([8]). *Let K be an imaginary quadratic field, and d a squarefree integer. There exists a constant $M_{K,d}$ such that, for all quadratic $\mathbb{Q}$-curves E/K of degree d, and all primes $p > M_{K,d}$, either*

- *$\mathbb{P}\bar{\rho}_{E,p}$ is surjective;*
- *E has potentially good reduction at all primes greater than 3.*

The natural conjecture here is that, for p large enough, $\bar{\rho}_{E,p}$ is surjective whenever E is not CM. In this theorem one should think of "has potentially good reduction everywhere" as a proxy for "is CM". (Compare with [22].)

The idea of the proof is as follows. Let G be a maximal proper subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$. As in Mazur's original argument, we are trying to control points on a certain modular curve X, whose rational points parametrize $\mathbb{Q}$-curves E over K such that $\bar{\rho}_{E,p}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) \subset G$. In [21], G is a Borel subgroup, $K = \mathbb{Q}$, and $X = X_0(p)$; in [23], G is the normalizer of a split Cartan subgroup.

Now the main arithmetic step is to show the existence of a quotient

$$J(X) \to A$$

with $|A(\mathbb{Q})| < \infty$.

The proper maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$ are the Borel subgroups, the normalizers of Cartan subgroups, and the exceptional subgroups isomorphic to A_4, S_4, or A_5. If G is anything other than the normalizer of a non-split Cartan subgroup, it is not hard to show the existence of an A as above by imitating existing results. So from now on let X be the modular curve parametrizing quadratic $\mathbb{Q}$-curves over K of degree d, whose mod p Galois representation takes image in the normalizer of a non-split Cartan subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$. If $J(X)$ has a quotient with Mordell-Weil rank 0, Theorem 8 follows after applying a formal immersion theorem of Darmon and Merel [3].

A result of Chen and Edixhoven ([2],[4]) shows that $J(X)$ is a quadratic twist of $J_0^{p-new}(dp^2)/w_p$. In particular, if f is a weight 2 cusp form of level dp^2 which does not come from level dp, and which satisfies $w_p f = f$, then $J(X)$ has a quotient which is isomorphic over K to the modular abelian variety A_f. Thanks to work of Kolyvagin and Logachev, in order to show that a quotient A has Mordell-Weil rank 0, we need only show non-vanishing of the special value of the L-function attached to A at the center of the functional equation. Precisely: for us, it will suffice to prove the following lemma.

Lemma 9. *Let χ be the quadratic Dirichlet character associated to $K/\mathbb{Q}$. For all sufficiently large p, there exists a weight 2 newform f of level p^2 such that $w_p f = f$ and $L(f \otimes \chi, 1) \neq 0$.*

In fact, more is true: as Duke observed in [5], one can use the Petersson formula to approximate the *average* value of $L(f \otimes \chi, 1)$ as f ranges over newforms satisfying the criteria in Lemma 9. In order to prove that $L(f \otimes \chi, 1)$ is nonzero for *some* such f, it suffices to prove that the average is nonzero for p large enough, which is immediate from the analytic estimate.

Problem D: Optimize the dependence of $M_{K,d}$ on K and d in Theorem 8.

Problem E: Extend Theorem 8 to $\mathbb{Q}$-curves over polyquadratic fields.

Diophantine problems

A solution to the Fermat equation $A^p + B^p + C^p = 0$ gives rise, via the Frey-Hellegouarch construction, to an elliptic curve over $\mathbb{Q}$ whose associated mod p Galois representation is unramified away from a small set of primes defined independently of A, B, C. Analogously, certain "twisted" versions of the Fermat equation give rise to $\mathbb{Q}$-curves whose mod p Galois representations satify similar non-ramification conditions.

Proposition 10. *Let d be a positive integer and let $\alpha \in \mathbb{Q}(\sqrt{d})$ be an algebraic integer of norm ± 2. Let A, B be integers. Then*

$$E = E_{A,B} : y^2 = x^3 + 4\alpha\sqrt{d}Ax^2 + 2\alpha^2(dA^2 - d^{-1/2}B)x$$

is a $\mathbb{Q}$-curve over $\mathbb{Q}(\sqrt{d})$ of degree 2. The isogeny $\mu : E \to E^\sigma$ has equation

$$(x, y) \mapsto (\alpha^{-2}(y^2/x^2), \alpha^{-3}yx^{-2}(2\alpha^2(dA^2 - d^{-1/2}B) - x^2))$$

and the automorphism $\mu^\sigma\mu$ of E is multiplication by the norm of α. The invariants of the given Weierstrass model of E are

$$E_4 = 32\alpha^2(5dA^2 + 3d^{-1/2}B)$$

and

$$\Delta = 512\alpha^6(dA^2 + d^{-1/2}B)(dA^2 - d^{-1/2}B)^2.$$

Note that the odd primes dividing Δ are precisely those dividing $(dA)^4 - dB^2$. Suppose (A, B, C) is an integral solution in coprime integers to

$$(dA)^4 - dB^2 = 2^n C^p.$$

Then it follows from the theory of the Tate curve that the mod p representation $E_{A,B}[p]$ is unramified away from 2 and primes dividing d. Moreover, if $3 \not| d$, the representation $E_{A,B}[p]$ is modular, by [7]. Finally, in many cases we can show that $E_{A,B}[p]$ is surjective, by the argument of the previous section. By combining all these facts we can obtain Diophantine theorems. For instance, taking $d = -1$ and $\alpha = 1 + i$, we find ([8]) that the generalized Fermat equation $A^4 + B^2 = C^p$ has no solutions in coprime integers for $p \geq 211$.

Another interesting case arises from the elliptic curve

$$y^2 + 1 = 2x^4 \tag{1}$$

whose integral points are related to the problem of expressing π as a sum of rational arctangents [26, §A.12] In particular, the point $(13, 239)$ corresponds to Machin's formula

$$\pi/4 = 4\arctan(1/5) - \arctan(1/239).$$

The problem of determining all integral solutions to (1) was first solved by Ljunggren [20]. Using the material in this section, one can reprove Ljunggren's result with a bonus: we can, in a sense, explain *why* there is an integral point on (1) with large height.

Setting $A = x, B = 2y$, we have

$$(2A)^4 - 2B^2 = 8;$$

setting $d = 2$ and $\alpha = \sqrt{2}$, we have a $\mathbb{Q}$-curve $E_{A,B}$ over $\mathbb{Q}(\sqrt{2})$ which has good reduction away from 2. By Tate's algorithm one finds that $E_{A,B}$ has conductor at most 2^{10}, and by [7] we know $E_{A,B}$ is modular. To find the possibilities for $E_{A,B}$, it thus suffices to find the $\mathbb{Q}$-curves among the modular abelian varieties of conductor dividing 2^{10}. The only difficulty is that there might be multiple $\mathbb{Q}$-curves $E_{A,B}$ lying in the same isogeny class. In fact, this is precisely what happens. There is an weight 2 newform f of level 1024 with $a_3(f) = \sqrt{2}, a_5(f) = -\sqrt{2}, a_7(f) = -2 \ldots$ It turns out that the mod 5 Galois representation associated to this representation is reducible; that is, there are two $\mathbb{Q}$-curves, connected by a 5-isogeny, attached to the same modular form. One of these curves is $E_{1,2}$ and the other is $E_{13,-478}$. In other words, the existence of a large-height solution to Ljunggren's equation is "explained" by the presence of a rational 5-isogeny on one of the modular abelian varieties of conductor 2^{10}.

In general, the method outlined here should give information about integral solutions to equations of the form

$$A^4 - mB^2 \in \mathbb{Z}[1/N]^* \tag{2}$$

and

$$A^4 - mB^2 = C^p \tag{3}$$

where m is a squarefree integer prime to 3.

If (A, B) is a solution to (2), the $\mathbb{Q}$-curve $E_{A,B}$ has good reduction away from primes $2mN$, and its conductor can thus be bounded by some constant M: if M is not too large, one can then look up in tables the weight 2 cusp forms of conductor dividing M whose associated abelian varieties are $\mathbb{Q}$-curves. Finally, one bounds the degree of an isogeny between $\mathbb{Q}$-curves of conductor dividing M as in [21, §5,6,7], thus classifying all $\mathbb{Q}$-curves associated to the modular abelian varieties under consideration.

Finding the solutions to (3) is more subtle; one still has that $E_{A,B}$ is modular, but all one can conclude is that $E_{A,B}[p]$ is a modular Galois representation with conductor less than some fixed M. If there exist surjective mod p modular representations V of that conductor, it may be quite difficult to control the set of $\mathbb{Q}$-curves E such that $E[p] \cong V$. On the other hand, one may be lucky enough to find, as in [8], that the computation of the conductor forces Galois to act non-surjectively on $E_{A,B}[p]$; in this case, one can hope to use Theorem 8 to get a Diophantine result.

Problem F. What Diophantine problems are associated to quadratic $\mathbb{Q}$-curves of small degree higher than 2? A natural approach is to work out a set of generators for the ring of modular forms on $X^*(d)$ for small d; if this ring has the form

$$\mathbb{C}[A, B, C]/f(A, B, C)$$

and C generates the ideal of cuspforms, then one should be able to classify triples of coprime integers (A, B, C) such that C is a pth power and $f(A, B, C) = 0$. The prototypical example is the case $d = 1$, in which case the ring of modular forms is given by

$$\mathbb{C}[E_4, E_6, \Delta]/(E_4^3 - E_6^2 = 1728\Delta)$$

and the Diophantine equation of interest is

$$x^3 - y^2 = z^p.$$

References

[1] K. Buzzard, M. Dickinson, N. Shepherd-Barron, and R. Taylor. On icosahedral Artin representations. *Duke Math. J.* 109 (2001), no. 2, 283–318.

[2] I. Chen. On relations between Jacobians of certain modular curves. *J. Algebra*, 231(1):414–448, 2000.

[3] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[4] B. DeSmit and B. Edixhoven. Sur un résultat d'Imin Chen. *Math. Res. Lett.*, 7(2–3):147–153, 2000.

[5] W. Duke. The critical order of vanishing of automorphic L-functions with large level. *Invent. Math.*, 119(1):165–174, 1995.

[6] N. Elkies. Remarks on elliptic K-curves. Preprint, 1993.

[7] J. Ellenberg and C. Skinner. On the modularity of $\mathbf{Q}$-curves. *Duke Math. J.*, 109(1):97–122, 2001.

[8] J. Ellenberg. Galois representations attached to $\mathbf{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. Preprint, 2002.

[9] S. Galbraith. Rational points on $X_0^+(p)$ *Experiment. Math. 8* (1999), no. 4, 311–318.

[10] S. D. Galbraith. Rational points on $X_0^+(N)$ and quadratic $\mathbf{Q}$-curves. *J. Théor. Nombres Bordeaux* 14 (2002), no. 1, 205–219.

[11] J. González. Isogenies of polyquadratic $\mathbf{Q}$-curves to their Galois conjugates. *Arch. Math. (Basel)* 77 (2001), no. 5, 383–390.

[12] J. González and J.-C. Lario. Rational and elliptic parametrizations of $\mathbf{Q}$-curves. *J. Number Theory 72* (1998), no. 1, 13–31.

[13] B. Gross. *Arithmetic of elliptic curves with complex multiplication.* (LNM 776) Berling: Springer, 1980.

[14] Y. Hasegawa. $\mathbf{Q}$-curves over quadratic fields. *Manuscripta Math.* 94 (1997), no. 3, 347–364.

[15] Y. Hasegawa, K.-i. Hashimoto, and F. Momose. Modular conjecture for $\mathbf{Q}$-curves and QM-curves. *Internat. J. Math.* 10 (1999), no. 8, 1011–1036.

[16] T. Hibino and A. Umegaki. Families of elliptic $\mathbf{Q}$-curves defined over number fields with large degrees. *Proc. Japan Acad. Ser. A Math. Sci.* 74 (1998), no. 1, 20–24.

[17] T. Hibino and A. Umegaki. A family of elliptic $\mathbf{Q}$-curves defined over biquadratic fields and their modularity. *Acta Arith.* 88 (1999), no. 2.

[18] H. Hida. Modular Galois representations of "Neben" type. Preprint, 2000.

[19] H. Hida. Modularity problems of $\mathbf{Q}$-motives and base-change. Preprint, 2000.

[20] W. Ljunggren. Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. *Avh. Norske Vid. Akad. Oslo. I.* 1942, (1942). no. 5, 27 pp.

[21] B. Mazur. Rational isogenies of prime degree. *Invent. Math.* 44(2):129–162, 1978.

[22] F. Momose. Rational points on the modular curves $X_{split}(p)$. *Compositio Math.*, 52(1):115–137, 1984.

[23] F. Momose and M. Shimura. Moduli and modularity of (Q, F)-abelian varieties of GL_2-type. Algebraic number theory and related topics (Japanese) (Kyoto, 1998). *Surikaisekikenkyusho Kokyuroku* No. 1097 (1999), 151–160.

[24] J. Quer. $\mathbf{Q}$-curves and abelian varieties of GL_2-type. *Proc. London Math. Soc.* (3) 81 (2000), no. 2, 285–317.

[25] J. Quer. Fields of definition of $\mathbf{Q}$-curves. 21st Journes Arithmtiques (Rome, 2001). *J. Thor. Nombres Bordeaux 13* (2001), no. 1, 275–285.

[26] P. Ribenboim. *Catalan's conjecture*. Academic Press, Boston, 1994.

[27] K. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Algebra and Topology 1992*, pages 53–79. Korea Adv. Inst. Sci. Tech., 1992.

[28] K. Ribet. Fields of definition of abelian varieties with real multiplication. In *Arithmetic geometry (Tempe, AZ, 1993)*, 107–118, Contemp. Math., 174, Amer. Math. Soc., Providence, RI, 1994.

[29] R. Taylor. On icosahedral Artin representations II. To appear, *Amer. J. Math.*