Compositio Mathematica **111:** 35–49, 1998.

The modularity of some $\mathbb{Q}$-curves

BOYD B. ROBERTS and LAWRENCE C. WASHINGTON*
Department of Mathematics, University of Maryland, College Park, MD 20742
**e-mail: lcw@math.umd.edu*

Received 13 May 1996; Accepted in final form 11 December 1996

Abstract. A $\mathbb{Q}$-curve is an elliptic curve, defined over a number field, that is isogenous to each of its Galois conjugates. Ribet showed that Serre's conjectures imply that such curves should be modular. Let E be an elliptic curve defined over a quadratic field such that E is 3-isogenous to its Galois conjugate. We give an algorithm for proving any such E is modular and give an explicit example involving a quotient of $J_0(169)$. As a by-product, we obtain a pair of 19-isogenous elliptic curves, and relate this to the existence of a rational point of order 19 on $J_1(13)$.

Mathematics Subject Classifications (1991). 11G05, 11G18.

Key words: elliptic curves, modular forms, $\mathbb{Q}$-curves.

Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$ and without complex multiplication. E is called a $\mathbb{Q}$-curve if it is isogenous to each of its Galois conjugates. We say that E is modular if for some N there is a non-constant morphism $J_1(N) \to E$, where $J_1(N)$ is the Jacobian of the modular curve $X_1(N)$. Ribet [12] showed that if E is modular, then E is a $\mathbb{Q}$-curve, and conversely, if Serre's conjecture 3.2.4$_?$ [18] holds, then all $\mathbb{Q}$-curves are modular. See also [18, Thm. 5]. When E is defined over $\mathbb{Q}$, then E is automatically a $\mathbb{Q}$-curve, and this reduces to the conjecture that all E over $\mathbb{Q}$ are modular (it can be shown that for E defined over $\mathbb{Q}$, the existence of a map $J_1(N) \to E$ implies the existence of a map $J_0(N') \to E$ for some N'). Wiles [27] has proved a general result, extended by Diamond [4], that implies, among other things, the modularity of all semistable elliptic curves over $\mathbb{Q}$, and also the modularity of several other $\mathbb{Q}$-curves. However the method runs into difficulties when the mod 3 representation is reducible. Over $\mathbb{Q}$, this was handled by the '3–5' switch [27], which relied on the fact that the elliptic curve $X_0(15)$ has finite Mordell-Weil group over $\mathbb{Q}$. This of course fails over many quadratic fields. Also, since we are working in the rather restrictive context of $\mathbb{Q}$-curves, it is not certain that the '3–5' switch can be applied.

In the following, we start with the family of 3-$\mathbb{Q}$-curves (i.e., the isogeny is of degree 3) defined over a quadratic field K. We consider those that are 3-isogenous over K to their Galois conjugates, hence have reducible $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-representations (which remain reducible when extended to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representations). Therefore the general results of Wiles and Diamond do not apply. We describe a general strategy for proving individual curves in the family are modular. In a sense, such calculations can be regarded as a check on a consequence of Serre's conjecture in

a case that does not already follow from earlier conjectures such as the Shimura–Taniyama–Weil conjecture.

We note that the absence in general of a point of order 2 on these curves makes it difficult, though perhaps not impossible, to apply the method of Faltings-Serre-Livné [7], which has often been used to prove individual curves modular.

As an example, we treat a particular curve that appears as a quotient of $J_0(169)$ and which was discussed briefly by Ribet [12]. As a by-product, we find another curve to which this curve is 19-isogenous and relate this phenomenon to the existence of a rational point of order 19 on $J_1(13)$. In fact, $J_1(13)$ is isogenous over $\mathbb{Q}(\zeta_{13})$ to the product of our curve and its Galois conjugate.

1. The family of 3-$\mathbb{Q}$-curves

THEOREM 1. *Suppose $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field and E is a non-CM $\mathbb{Q}$-curve defined over K that is 3-isogenous to its Galois conjugate. Then E has the form*

$$E_m\colon y^2 = x^3 - \left(\frac{15m^2}{4} - \frac{3m}{\sqrt{d}}\right) D^2 x - \left(\frac{11m^3}{4} - \frac{7m^2}{2\sqrt{d}} + \frac{m}{2d}\right) D^3$$

with $D \in K^\times$ and $m \in \mathbb{Q}^\times$.

This is proved in [17] by considering a twisted form of $X_0(3)$. Note that changing D gives twists of the curve and does not affect modularity. For simplicity, we have suppressed D from the notation for E_m.

Note that the conjugate of E is obtained by changing m to $-m$ and D to $-D^\sigma$, where σ is the non-trivial automorphism of K.

It is convenient to write $m = a/b$ with $(a, b) = 1$. Then

$$j(E_m) = \frac{2^4 3^3 a\sqrt{d}(5a\sqrt{d} - 4b)^3}{(a\sqrt{d} - b)(a\sqrt{d} + b)^3}. \qquad (*)$$

The isogeny μ from E_m to E_m^σ is defined over K if and only if $\mathrm{Norm}(D) = -3A^2$ for some $A \in K^\times$. If $A \in \sqrt{d}\mathbb{Q}^\times$, then $\mu^\sigma\mu = 3$, and if $A \in \mathbb{Q}^\times$, then $\mu^\sigma\mu = -3$.

From now on, we shall assume that the 3-isogeny is defined over K. For simplicity, we shall also assume that $\mu^\sigma\mu = +3$ and that K is real quadratic. Since $\mathbb{Q}(\sqrt{+3})$ is totally real, it follows from [12, Proposition 3.4; or 14, Sect. 1] that E_m should arise from the part of $J_1(N)$ with trivial character, hence from $J_0(N)$, for some N. In the cases where other parts of $J_1(N)$ are needed, the considerations are similar.

2. Modular $\mathbb{Q}$-curves

We start with $E = E_m$ for some m, defined over the quadratic field $K = \mathbb{Q}(\sqrt{d})$ of discriminant d, as in Section 1, with the isogeny μ defined over K. Our goal

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

is to show E is modular. The abelian variety $A = E \times E^\sigma$ can be defined over $\mathbb{Q}$ (it is the restriction of scalars from K to $\mathbb{Q}$ of E) and there is an injection $\mathbb{Q}(\sqrt{3}) \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ (if $\mu^\sigma \mu = -3$, then we would have an injection of the field $\mathbb{Q}(\sqrt{-3})$ instead).

Such a situation also arises with abelian varieties attached to modular forms. Let $f = q + a_2 q^2 + a_3 q^3 + \cdots$ be a normalized Hecke eigenform of weight 2 for $\Gamma_0(N)$ and let $L = \mathbb{Q}(a_2, a_3, \ldots)$. By [21, Thm. 7.14], there is a $\mathbb{Q}$-simple abelian variety A_f of dimension $[L\colon \mathbb{Q}]$ with $L \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$. In fact, A_f is a quotient of $J_0(N)$ and the Hecke operator T_p acts as the endomorphism corresponding to $a_p \in L$. We could also take A_f to be a quotient of $J_1(N)$; this would give us an abelian variety isogenous to A_f and would not affect the following (since the map η below is defined in both situations).

Suppose now that

$$L = \mathbb{Q}(a_2, a_3, \ldots) = \mathbb{Q}(\sqrt{3})$$

and let $f' = q + a_2' q^2 + a_3' q^3 + \ldots$, where a_n' is the $\mathrm{Gal}(L/\mathbb{Q})$-conjugate of a_n. Then f' is also a Hecke eigenform for $\Gamma_0(N)$. Suppose that $f' = f \otimes \chi = \sum \chi(n) a_n q^n$, where χ is the quadratic character associated to the quadratic field $K = \mathbb{Q}(\sqrt{d})$. Then f is a modular form with 'extra twist' in the sense of Shimura [22] and Ribet [13]. We assume in addition that f has no CM. This means that there is no non-trivial Dirichlet character ϕ such that $a_p = \phi(p) a_p$ for almost all p. In particular, this implies that the $\overline{\mathbb{Q}}$-factors of A_f do not have CM [24, Prop. 1.6; 14, Cor. 3.5]. As in Shimura [22], there is a K-endomorphism η of A_f such that

(1) $\eta^2 = d$
(2) $\eta T_p = \chi(p) T_p \eta$ for all Hecke operators T_p, where $p \nmid N$ is prime
(3) $\eta f = \sqrt{d} f'$ and $\eta f' = \sqrt{d} f$
(4) $\eta^\sigma = -\eta$, where σ is the non-trivial automorphism of K.

In fact, η is constructed as follows.

In our case, since f and $f \otimes \chi$ have level N, we have $d^2 | N$. For $1 \leqslant u \leqslant d-1$, let $\alpha_u = \begin{pmatrix} 1 & u/d \\ 0 & 1 \end{pmatrix}$. Then $\alpha_u \Gamma_1(N) \alpha_u^{-1} = \Gamma_1(N)$, so the map $z \mapsto \alpha_u(z)$ is an automorphism of $X_1(N)$ and induces a corresponding automorphism of the Jacobian $J_1(N)$. The maps $\alpha_1, \ldots, \alpha_{d-1}$ yield a map

$$J_1(N) \to J_1(N) \times \cdots \times J_1(N).$$

There is also a map

$$J_1(N) \times \cdots \times J_1(N) \to J_1(N)$$

defined by $(z_1, \ldots, z_{d-1}) \mapsto \sum \chi(j) z_j$. The composite of these two maps gives

$$\eta\colon J_1(N) \to J_1(N).$$

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

An easy calculation shows that η maps a modular form $\sum b_n q^n$ to $g(\chi)\sum \chi(n) b_n q^n$, where $g(\chi) = \sum \chi(j)\, e^{2\pi i j/d} = \sqrt{d}$ is the Gauss sum attached to χ. Since $f \otimes \chi = f', \eta$ maps the $\mathbb{C}$-span of f, f' to itself and satisfies (1), (2), and (3) on this space. By [1, Lem. 29]), η gives an endomorphism of the space of weight two cusp forms for $\Gamma_0(N)$, so η acts on $J_0(N)$. It follows that η gives an endomorphism of A_f satisfying these three properties.

Property (4) can be verified as in [22], but instead we use an argument inspired by one in [15]. Since all endomorphisms of A_f are defined over $\overline{\mathbb{Q}}$, this holds for η. As we shall see below, the existence of η satisfying (1), (2), (3) implies that A_f is isogenous over $\overline{\mathbb{Q}}$ to the product of two elliptic curves E_1 and E_2 that are isogenous to each other. Therefore, since we are not dealing with CM curves, $\mathrm{End}(A_f) \otimes \mathbb{Q} \simeq M_2(\mathbb{Q})$. Let g be a Galois automorphism of the field of definition of End (A_f). Then g induces an automorphism of $M_2(\mathbb{Q})$. By the Noether-Skolem theorem, this is an inner automorphism, so there exists $e \in GL_2(\mathbb{Q})$ such that g induces the map $m \mapsto eme^{-1}$. The field $L = \mathbb{Q}(\sqrt{3})$ injects into $\mathrm{End}_{/\mathbb{Q}}(A_f) \otimes \mathbb{Q}$ via the Hecke operators, so g, hence e, commutes with the action of L. Since L is its own commutator in $M_2(\mathbb{Q})$, we have $e \in L$. Since g is of finite order, e^k is in the center of $M_2(\mathbb{Q})$, namely $\mathbb{Q}$, for some $k \geqslant 1$. Since L is totally real, it follows easily (for example, use [6, Chap. VIII, Sect. 9]) that $e \in \mathbb{Q}^\times$ or $e \in \sqrt{3}\mathbb{Q}^\times$. Since $\mathbb{Q}^\times$ acts trivially, there are two choices for g. Therefore all endomorphisms of A_f, in particular η, are defined over a quadratic field K_1.

Suppose $K_1 \neq K$. Choose $p \nmid N$ such that p splits in K_1 but is inert in K. Choose a prime $\mathfrak{p}$ of $\overline{\mathbb{Q}}$ over p and let F be the Frobenius for $\mathfrak{p}$ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then F is trivial on K_1, so it commutes with η. Let $\tilde{A}_f$ be the reduction of A_f modulo $\mathfrak{p}$. In $\mathrm{End}(\tilde{A}_f)$ we have the relation $F^2 - T_p F + p = 0$. Therefore,

$$0 = (F^2 - T_p F + p)\eta = \eta(F^2 + T_p F + p).$$

Multiplying by η and using the fact that $\mathrm{End}(\tilde{A}_f)$ has no $\mathbb{Z}$-torsion, we obtain $F^2 + T_p F + p = 0$. Since it is possible to choose p such that $T_p \neq 0$ on A_f (the set of p with $a_p = 0$ has density 0 [19]), we have a contradiction. Therefore $K_1 = K$.

Now apply a similar argument with $K_1 = K$ and choose p such that its Frobenius F equals σ on K and such that $T_p \neq 0$ on A_f. Then σ^2 is trivial on K, hence commutes with η. The above argument yields $0 = \eta F^2 + \eta^\sigma T_p F + \eta p$. Multiplying by η and comparing with the original equation multiplied by d yields $\eta\eta^\sigma T_p = -dT_p$. Since $T_p^2 \in \mathbb{Z}$ for all p, we may multiply on the right by T_p and remove the integer to obtain $\eta\eta^\sigma = -d = \eta^2$. Multiplying by η and dividing by d yields $\eta^\sigma = -\eta$, in $\mathrm{End}(\tilde{A}_f)$. Since the map $\mathrm{End}(A_f) \to \mathrm{End}(\tilde{A}_f)$ is injective, we obtain (4).

The existence of η allows us to decompose A_f over K as isogenous to a product of two elliptic curves:

$$A_f \sim E^1 \times E^2.$$

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

Since we need to do calculations with these curves, we show how to give E^1 and E^2 explicitly, at least when there is a Hecke operator satisfying $T_p^2 = 3$ on A_f.

If $p \nmid N$ and $a_p \notin \mathbb{Q}$, then $a_p' = \chi(p)a_p = -a_p$, so $a_p = r\sqrt{3}$ with $r \in \mathbb{Q}$. Assume that there exists p with $r = \pm 1$, so $a_p^2 = 3$. By assumption, $\mathrm{Norm}(D) = -3dA_1^2$ for some $A_1 \in \mathbb{Q}^\times$. This may be rewritten to yield that 3 is a norm from $\mathbb{Q}(\sqrt{d})$; in other words, there exist $x, y \in \mathbb{Q}$ such that $3 = x^2 - dy^2$. Let z be a common denominator for x and y and let

$$e = z(T_p + y\eta + x) \in \mathrm{End}(A_f).$$

Then $e^2 = 2zxe$. We have $e^\sigma = e - 2zy\eta$ since T_p is defined over $\mathbb{Q}$. Let

$$E^1 = A_f/eA_f, \qquad E^2 = A_f/e^\sigma A_f.$$

Then E^2 is the Galois conjugate of E^1. Since $T_p e = e^\sigma T_p$ and $T_p e^\sigma = eT_p$, the Hecke operator T_p induces maps

$$\tau : E^1 \to E^2 \quad \text{and} \quad \tau^\sigma : E^2 \to E^1$$

with $\tau^\sigma \tau = 3 \in \mathrm{End}(E^1)$. Since the cardinalities of the kernels of τ and τ^σ are equal, τ and τ^σ must be 3-isogenies. Therefore E^1 is a 3-$\mathbb{Q}$-curve, so it is given by Theorem 1.

We claim that the natural map

$$\psi : A_f \to E^1 \times E^2$$

is an isogeny. Suppose Q is in the kernel of ψ. Then $Q \in eA_f$, so $(2zx - e)Q = 0$. Similarly, $Q \in e^\sigma A_f$, so $(2zx - e + 2yz\eta)Q = 0$. Therefore $2yz\eta Q = 0$ and hence $2yzdQ = 0$. It follows that the kernel is finite. Since $e^\sigma \eta P_1 + e\eta P_2$ maps to $(e^\sigma \eta P_1, e\eta P_2) = 2zyd(-P_1, P_2)$, the surjectivity of ψ follows from the divisibility of A_f. Therefore ψ is an isogeny.

In order to show that the original elliptic curve E is modular, it is necessary to

(1) find the correct modular form f, and
(2) show that the corresponding E^1, or its conjugate E^2, is isogenous to E.

We start with (1). Let ℓ be any prime. Attached to f is an irreducible λ-adic Galois representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{Q}}_\ell)$$

such that

$$\mathrm{Tr}(\rho_f(\mathrm{Frob}_p)) = a_p \quad \text{and} \quad \det(\rho_f(\mathrm{Frob}_p)) = p$$

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

for all primes $p \nmid \ell N$ (where Frob_p denotes any choice of Frobenius element). The restriction of ρ_f to $\text{Gal}(\overline{\mathbb{Q}}/K)$ is equivalent to the representation ρ_{E^1} on the ℓ-adic Tate module of E^1 (which is equivalent to that for E^2 since E^1 and E^2 are isogenous over K).

For the lemma below, we need the commuting algebra of $\rho_f(\text{Gal}(\overline{\mathbb{Q}}/K))$ to be the scalar matrices. This can be shown using the results of [14]. Alternatively, by [16, Thm. 3.1], we may assume that ℓ is such that $\rho_f(\text{Gal}(\overline{\mathbb{Q}}/K)) \supseteq \text{GL}_2(\mathbb{Z}_\ell)$, and hence ρ_f gives an absolutely irreducible representation of $\text{Gal}(\overline{\mathbb{Q}}/K)$.

When $p = \mathfrak{p}\mathfrak{p}'$ splits in K, $\text{Frob}_p \in \text{Gal}(\overline{\mathbb{Q}}/K)$. Moreover, $a_p = a'_p$, so $a_p \in \mathbb{Z}$. In addition,

$$\text{Tr}(\rho_{E^1}(\text{Frob}_p)) = p + 1 - \#(E^1 \bmod \mathfrak{p}),$$

and similarly for our original curve E.

By counting points on $E \bmod \mathfrak{p}$ for various split p, we can find several coefficients of the desired modular form f. It is worth pointing out that this procedure can only give us a_p^2 for the inert p. This corresponds to the fact that $a_p = -a'_p$ for these p, and ρ_f and $\rho_{f'}$ are equivalent on $\text{Gal}(\overline{\mathbb{Q}}/K)$, so we cannot expect to remove the ambiguity in sign.

Using modular symbols, one can find the Hecke eigenforms for $\Gamma_0(N)$. Among these, there should be two with the appropriate values of a_p, namely f and f'. In fact, there cannot be any eigenform other than f and f' with the same values of a_p for all split p, so sufficient computation will eventually single out f and f'. Namely, the Frobenius elements for the split primes are dense in $\text{Gal}(\overline{\mathbb{Q}}/K)$, so any representation of $\text{Gal}(\overline{\mathbb{Q}}/K)$ is determined up to equivalence by these a_p. The uniqueness of the pair (f, f') now follows from the following.

LEMMA. *Let $\rho\colon Gal(\overline{\mathbb{Q}}/K) \to GL_n(F)$ be an absolutely irreducible representation, where F is a field. Then ρ has at most two extensions to a representation of* $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Proof. Let $\tilde{\rho}$ be an extension of ρ and let σ denote any extension of the non-trivial element $\sigma \in \text{Gal}(K/\mathbb{Q})$ to an element of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We have $\sigma g \sigma^{-1} \in \text{Gal}(\overline{\mathbb{Q}}/K)$ for all $g \in \text{Gal}(\overline{\mathbb{Q}}/K)$, and $\rho(\sigma g \sigma^{-1}) = \tilde{\rho}(\sigma)\rho(g)\tilde{\rho}(\sigma)^{-1}$. Therefore the matrix $\tilde{\rho}(\sigma)$ intertwines two absolutely irreducible representations and hence is determined up to a scalar. Since $\tilde{\rho}(\sigma)^2 = \rho(\sigma^2)$, this scalar is determined up to sign. Since $\tilde{\rho}$ is determined by $\tilde{\rho}(\sigma)$, there are at most two choices for $\tilde{\rho}$. □

Since the coefficients of the modular form are determined by the Galois representation (use 'multiplicity one' to include the bad primes), the two possible extensions of the Galois representation correspond to f and f', if they actually exist, and so it is possible to determine uniquely the pair (f, f'). Moreover, $f \otimes \chi$ will have the same values of a_p for split p and in the cases we need will also be a newform for $\Gamma_0(N)$. Since $f \otimes \chi \neq f$ (since we are not in a CM situation; moreover, the CM

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

case can be handled by other methods; see [14]), we must have $f \otimes \chi = f'$, as desired.

We are now in the following situation. We have a modular form f and a corresponding elliptic curve E^1, which we know to be modular. We know f explicitly, but we do not have an exact equation for E^1, though a numerical approximation can be calculated. For our original elliptic curve E, we of course have an exact equation, but we do not have a modular form, though we know many coefficients of the supposed modular form. We want to match up the two situations by showing that E and E^1 are isogenous.

Since E^1 is a 3-$\mathbb{Q}$-curve, it is on the list in Theorem 1. The idea is to exhibit the finitely many j-invariants that allow the appropriate reduction properties, and hence obtain a finite list of possible values of $j(E^1)$. Since $j(E^1)$ can be computed numerically very accurately, we can determine the exact value from this list. If it agrees with $j(E)$, we are done since then E and E^1 are $\overline{\mathbb{Q}}$-isomorphic. If not, we need to look for an isogeny. Since we now know $j(E^1)$ exactly, this task is much easier.

3. The general case

E^1 is given by Theorem 1, so $E^1 = E_m$ for some $m = a/b$ and a suitable choice of D. The curve E^1 is a quotient over K of $J_1(N)$ and hence has good reduction outside the set of primes dividing N. Therefore the norm of the denominator of $j(E^1)$ divides a power of N. A standard calculation shows that the only common factors of the numerator and denominator of the expression $(*)$ for the j-invariant are composed of primes dividing $6\sqrt{d}$, so we find that $(da^2 - b^2)^4$ divides a power of $6dN$. Let S be the set of rational primes dividing $6dN$. Then

$$da^2 - b^2 = \pm \prod_{p \in S} p^{g_p}$$

for some exponents $g_p \geqslant 0$.

Let $p \notin S$ and let $\mathfrak{p}$ be a prime of K above p. Suppose $p|a$. Since E^1 has good reduction at $\mathfrak{p}$, there is a Weierstrass model for E^1 with good reduction at $\mathfrak{p}$. In particular, there is a choice of D in Theorem 1 such that the equation is integral at $\mathfrak{p}$, so

$$0 \leqslant v_{\mathfrak{p}}\left(\left(\frac{15m^2}{4} - \frac{3m}{\sqrt{d}}\right) D^2\right) = v_{\mathfrak{p}}(a) + 2v_{\mathfrak{p}}(D)$$

and

$$0 \leqslant v_{\mathfrak{p}}\left(\left(\frac{11m^3}{4} - \frac{7m^2}{2\sqrt{d}} + \frac{m}{2d}\right) D^3\right) = v_{\mathfrak{p}}(a) + 3v_{\mathfrak{p}}(D).$$

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

Since at least one of the coefficients of the Weierstrass model must be prime to $\mathfrak{p}$, we have $v_{\mathfrak{p}}(D) \leqslant 0$ and $v_{\mathfrak{p}}(a) = -3v_{\mathfrak{p}}(D)$. Since $v_{\mathfrak{p}}(a)$ is a multiple of 3 for all such $\mathfrak{p}$, it follows that

$$a = ce^3 \text{ with } c|(6dN)^2, \quad c, e \in \mathbb{Z}.$$

Note that there are only finitely many possible values of c.

Letting $x = e^2, y = b, k = \pm \prod p^{g_p}$ yields

$$(y + \sqrt{-k})(y - \sqrt{-k}) = dc^2x^3.$$

Standard techniques (see, for example, [26]) reduce this to a finite set of equations of the form

$$F(X, Y) = \prod_{p \in S} p^{f_p},$$

where $X, Y \in \mathbb{Z}$ and $f_p \in \mathbb{Z}_{\geqslant 0}$ are allowed to vary, and where F is a cubic form.

For example, one such equation is obtained as follows. Write $-k = s^2\ell$ with ℓ squarefree. Suppose $\ell > 0$ and let $u + v\sqrt{\ell}$ be the fundamental unit of $\mathbb{Q}(\sqrt{\ell})$. Assume for simplicity that dc^2 is a cube. Then one equation that arises is

$$y + s\sqrt{\ell} = y + \sqrt{-k} = (X + Y\sqrt{\ell})^3(u + v\sqrt{\ell}),$$

hence

$$s = (X^3 + 3XY^2\ell)v + (3X^2Y + Y^3\ell)u \stackrel{\text{def}}{=} F(X, Y).$$

Other equations are obtaining by varying the power of the fundamental unit and by introducing contributions from suitable representatives of the ideal class group. Note that the prime factors of s divide k, hence are in S. Since there are only finitely many possibilities for ℓ, and the class number of each $\mathbb{Q}(\sqrt{\ell})$ is finite, there are only finitely many such F's, and they can be given explicitly.

Each such equation can be solved explicitly by the techniques of [25]. Therefore it is possible to make a finite list of possible values of $m = a/b$.

Note that the list of m obtained by the above method gives a set of curves E_m defined over K, and this set contains the set of curves that are quotients of the given $J_1(N)$.

4. A more restricted case

If all the prime factors of N ramify or are inert in K, then the following result shows that the j-invariant is an algebraic integer. If we calculate $j(E^1)$ and its conjugate $j(E^2)$ sufficiently accurately, we can therefore determine the minimal polynomial of $j(E^1)$ exactly in $\mathbb{Z}[X]$ and therefore evaluate $j(E^1)$ exactly.

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

PROPOSITION. *Let E be a 3-$\mathbb{Q}$-curve defined over a quadratic field K. Let p be a prime that is inert or ramified in K. Then the j-invariant of E is integral at p.*

Proof. $j(E)$ has the form $(*)$ for suitable relatively prime integers a, b. Let $\mathfrak{p}$ be the prime of K above p and suppose $v_{\mathfrak{p}}(a\sqrt{d}-b) > 0$ (equivalently, $v_{\mathfrak{p}}(a\sqrt{d}+b) > 0$, since p doesn't split).

If $p \neq 2$ ramifies, then $p|d$, so $p|b$. Since $(a,b) = 1$, we have $p \nmid a$, so $v_{\mathfrak{p}}(a\sqrt{d} - b) = 1$. Similarly, $v_{\mathfrak{p}}(a\sqrt{d} + b) = 1$. Therefore the power of $\mathfrak{p}$ from $\sqrt{d}$ and $(5a\sqrt{d} - 4b)^3$ in the numerator cancels the $\mathfrak{p}^4$ in the denominator, so j is $\mathfrak{p}$-integral.

If $p \neq 2$ is inert, then $v_{\mathfrak{p}}(a\sqrt{d} - b) > 0$ implies p divides both a and b, which is impossible.

A similar argument handles the case $p = 2$. □

The above proof is clearly the 'wrong' one, and the proposition cries out for generalization. Bjorn Poonen remedied these matters by supplying us with the following. In particular, it gives a much more intrinsic proof of the above proposition.

PROPOSITION. *Let E be an elliptic curve defined over a normal number field K. Let p be a rational prime and let $\mathfrak{p}$ be a prime of K above p. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and assume $\sigma(\mathfrak{p}) = \mathfrak{p}$. Suppose E^σ is ℓ-isogenous to E for some non-square ℓ. Then $j(E)$ is integral at $\mathfrak{p}$.*

Proof. Complete K at $\mathfrak{p}$. If $j(E)$ is not integral at $\mathfrak{p}$, then E over $\overline{\mathbb{Q}}_p$ is analytically isomorphic to $\overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$ for some q. The assumptions imply that σ induces an automorphism of the completion of K, and E^σ over $\overline{\mathbb{Q}}_p$ is analytically isomorphic to $\overline{\mathbb{Q}}_p^\times/\sigma(q)^{\mathbb{Z}}$. The fact that E and E^σ are isogenous implies that $q^m = \sigma(q)^n$ for some integers m, n [20, IV-34]; moreover, mn/ℓ is a rational square. Since q and $\sigma(q)$ have the same valuation, $m = n$, which is impossible. □

5. An example, Part I

We illustrate the above with the case $m = 1/11, d = 13, D = 143 - 55\sqrt{13}$ in Theorem 1, so we start with

$$E = E_{1/11}\colon y^2 = x^3 + \frac{-12285 + 3483\sqrt{13}}{2}x - 270270 + 74844\sqrt{13}.$$

Tate's algorithm shows that the conductor over K of E is the ideal (13). By [9, Prop. 1], the conductor over $\mathbb{Q}$ of the abelian variety $E \times E^\sigma$ is 169, so we expect E to be a quotient of $J_1(169)$. Since $\mathbb{Q}(\sqrt{3})$ is totally real, E should be a quotient of $J_0(169)$ [12, Prop. 3.4; 14, Sect. 1]. A calculation with modular symbols shows that there is a modular form

$$f = q + \sqrt{3}q^2 + 2q^3 + q^4 - \sqrt{3}q^5 + \cdots$$

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

and that f and f' are the only eigenforms with the correct coefficients. Moreover, $f' = f \otimes \chi$, where χ is the quadratic character mod 13. From the above, we obtain an elliptic curve E^1 (the existence of E^1 in this case was proved by Ribet [12]). Below, we calculate

$$j(E^1) \simeq -62947.470268\ldots \quad \text{and} \quad j(E^2) \simeq 1184.470268\ldots\ .$$

Within the accuracy of our calculations, these equal $j(E^\sigma)$ and $j(E)$, respectively, which are roots of the polynomial

$$X^2 + 61763X - 74559407.$$

Both E^1 and E^2 are defined over $K = \mathbb{Q}(\sqrt{13})$, so $j(E^1)$ and $j(E^2)$ are conjugate algebraic numbers in this field. They are algebraic integers by the proposition of Section 4. Therefore, $j(E^1) + j(E^2)$ and $j(E^1)j(E^2)$, which are numerically approximated by -61763 and -74559407, respectively, are actually equal to these numbers. Therefore $j(E^2) = j(E)$. This proves $E = E_{1/11}$ is modular.

The calculation of the j-invariants can be done as follows. Consider, for example $E^1 = A_f/eA_f$, where $e = T_2 + \eta + 4$. The cotangent space of A_f can be identified with $\mathbb{C}f + \mathbb{C}f'$, and the tangent space $\mathcal{T}$ consists of the linear functionals on this space. Let (g, y) denote the pairing between the span of f, f' and $\mathcal{T}$. There is a map $\phi\colon \Gamma_0(169) \to \mathcal{T}$ with $\phi(\gamma)(g) = \int_z^{\gamma z} g\,\mathrm{d}z$, for any fixed z in the upper half plane, and $\mathcal{T}/\phi(\Gamma_0(169)) \simeq A_f$. Let

$$h = \sqrt{13}f - (4 - \sqrt{3})f'.$$

Then $eh = 0$ (this determines h up to a scalar multiple), so $(h, e\mathcal{T}) = 0$. Consider the map $\psi\colon \mathcal{T} \to \mathbb{C}$ given by $y \mapsto (h, y)$, and let $L = \psi(\phi(\Gamma_0(169)))$. Then L is a lattice in $\mathbb{C}$ and $\mathbb{C}/L \simeq E$.

Modular symbols, as in [2, 3], can be used to find a $\mathbb{Z}$-basis of $\phi(\Gamma_0(169))$, and of $\psi(\phi(\Gamma_0(169)))$. This gives us the periods of E^1. It is then straightforward to calculate the j-invariant (see for example [2]).

6. An example, Part II

We now turn to the technique of Section 3, applied to the same example. As mentioned at the end of that section, we will actually obtain all E_m over $\mathbb{Q}(\sqrt{13})$ that are quotients of $J_1(169)$. In this case there are exactly two pairs of curves. They are isogenous, so E^1 is automatically isogenous to each of these. We therefore identify E^1 up to isogeny without ever calculating its periods, etc. This of course happens because $J_0(169)$ has exactly one 2-dimensional $\mathbb{Q}$-simple factor.

First we need to be a little more explicit in the argument of Section 3. Let E_m be a 3-$\mathbb{Q}$-curve over $\mathbb{Q}(\sqrt{13})$ arising as a quotient of $J_0(169)$. Consider $j(E_m)$, which is given by $(*)$. An easy calculation shows that $\gcd(5\sqrt{13}a - 4b, \sqrt{13}a + b)$

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

divides $9\sqrt{13}$ and that $\gcd(5\sqrt{13}a - 4b, \sqrt{13}a - b)$ divides $\sqrt{13}$. Write $3 = (4+\sqrt{13})(4-\sqrt{13}) = \pi\overline{\pi}$. Since $(a, b) = 1$, at most one of $\pi, \overline{\pi}$ divides $a\sqrt{13}-b$, and since the denominator of $j(E_m)$ cannot contain π or $\overline{\pi}$, it follows that $a\sqrt{13}-b$ contains at most π^3 or $\overline{\pi}^3$. If a, b are of opposite parity, then 2 does not divide $a\sqrt{13} \pm b$. If they have the same parity, they must be odd, so $(a\sqrt{13} \pm b)/2$ is integral, and must be prime to 2 in order to keep 2 out of the denominator of $j(E_m)$. Finally, $v_{\sqrt{13}}(a\sqrt{13} - b) = 1$ or 0, depending on whether 13 does or does not divide b.

Putting everything together, we have

$$13a^2 - b^2 = \pm 2^\alpha 3^\beta 13^\gamma$$

with $\alpha = 0, 2; 0 \leqslant \beta \leqslant 3$, and $\gamma = 0, 1$. From the above, $a = ce^3$ with $e \in \mathbb{Z}$, so we may rewrite this as $13c^2e^6 - b^2 = \pm 2^\alpha 3^\beta 13^\gamma$. It seems best at this point to let $x_1 = e^2$ and obtain $13c^2x_1^3 - b^2 = \pm 2^\alpha 3^\beta 13^\gamma$. Note that we have the auxiliary conditions that $(b, cx_1) = 1$ and $c|(2\cdot 3\cdot 13)^2$. Multiply by c_1^2, where c_1 is an integer chosen so that $13c_1^2c^2$ is a cube. A straightforward calculation yields the equation

$$x^3 - y^2 = \pm 2^{\alpha'} 3^{\beta'} 13^{\gamma'},$$

where $\alpha' = 0, 2, 4, \beta' = 0, 1, 2, 3, 4, \gamma' = 0, 2, 3, 4$. For example, if $\alpha = 0$ then $\alpha' = 0, 2, 4$, while if $\alpha = 2$ then c is odd, hence c' is odd, so $\alpha' = 2$.

Of course, x and y are to be integers. We also have $13|x$. In fact, $x = 13\cdot$square, and

$$m = \pm\frac{\sqrt{x^3/13}}{y}.$$

Using the method of Gebel–Pethő–Zimmer [5], Josef Gebel computed the integer points on these curves $Y^2 = X^3 + k$ for the 120 possible values of k. In the table below, we list all solutions with both $X \geqslant 500$ and $|Y| \geqslant 10000$ (the smaller solutions are easily found by computer; those with $X < 0$ correspond to k with the opposite sign).

Only $k = 18252$ yields any values of m that yield suitable values of $j(E_m)$, and rather surprisingly it yields two pairs:

$$m = \pm 1/11 \quad \text{and} \quad m = \pm 1331/4799,$$

which come from the point (13, 143) and from the point listed in the table. The values $m = 1/11$ and $-1/11$ correspond to our original elliptic curve E and its conjugate (and their twists). The other values yield values of $j(E_m)$ that are numerically different from $j(E^1)$ and $j(E^2)$. This gives another verification that E is modular and is isomorphic to E^2. But what if we had started with E corresponding to the second value of m? All the calculations would be the same as above and

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

Table I.

k	X	$\pm Y$
−676	901	27045
−26364	832	23998
−3084588	3549	211419
−711828	637	16055
−12338352	2028	91260
1028196	660	16986
18252	1573	62387
54756	39672	7901802
316368	897	26871
219024	585	14157
37015056	279864	148054140

we would obtain $E^1 = E_{1/11}$. If $E_{1331/4799}$ is a modular elliptic curve, it must be isogenous to $E_{1/11}$.

A calculation yields $j(\tau_1) = j(E_{1/11})$ with

$$\tau_1 = \tfrac{1}{2} + i0.58684446\ldots,$$

and $j(\tau_2) = j(E_{-1331/4799})$ with

$$\tau_2 = \tfrac{1}{2} + i8.09413792\ldots$$

Suppose $j(\tau_1)$ and $j(\tau_2)$ and j-invariants of n-isogenous elliptic curves. Then there is a matrix $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ of determinant n such that

$$\frac{x\tau_1 + y}{z\tau_1 + w} = \tau_2.$$

Writing $\tau_j = \frac{1}{2} + it_j$ and looking at real and imaginary parts, we obtain

$$-2x - 4y + z + 2w = 4zt_1t_2 \quad \text{and} \quad (2x - z)t_1 = (z + 2w)t_2.$$

If $z \neq 0$ then t_1t_2 is rational. If $2x - z \neq 0$, then t_1/t_2 rational. If both of these happen, then τ_1 and τ_2 are imaginary quadratic. Since the elliptic curves we are considering do not have CM, this is ruled out. Therefore either $z = 0$ or $2x = z$.

In our case, $t_1t_2 \simeq 4.75000$, which we suspect equals 19/4, so we should have $2x = z$, and hence $z + 2w = 0$. Substituting into the first of the above equations yields $-z - 4y = 19z$. If we take $z = 2$, then $x = 1$, $y = -10$, and $w = -1$. The resulting matrix has determinant 19, and it maps τ_1 to τ_2, within the accuracy of our

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

computations. Therefore we suspect that $E_{1/11}$ and $E_{-1331/4799}$ are 19-isogenous. F. Morain was able to show that this is indeed the case, using the formulas for isogenies that he developed for primality testing [10].

7. The 19-isogeny

The reader might recall that $J_1(13)$ has a rational point of order 19 [11]. Moreover, Mazur and Tate [8] showed that a twisted form of $J_1(13)$ decomposes into the product of two elliptic curves over $\mathbb{Q}(\sqrt{13})$. It is reasonable to guess therefore that $J_1(13)$ is $\overline{\mathbb{Q}}$-isogenous to our abelian variety A_f. In fact, this is the case.

Let ψ be the character mod 13 such that $\psi(2) = \zeta_{12}$. There is a modular form

$$g = q + (-1 - \zeta_6)q^2 + (-2 + 2\zeta_6)q^3 + \cdots = \sum b_n q^n$$

of level 13 and character ψ^8. The numbers $\psi(n)^2 b_n$ are the coefficients of a modular form of level 169 with character ψ^6, which is the quadratic character mod 13. This modular form corresponds to a 2-dimensional abelian variety that splits into two elliptic curves over $\mathbb{Q}(\sqrt{13})$. However, the coefficients of the modular form lie in $\mathbb{Q}(\sqrt{-3})$, and we have a modular form with character; so we need to twist again, either by ψ^3 or by ψ^9 to get rid of the quadratic character. It turns out that ψ^9 gives the correct choice of signs (the other choice gives the conjugate form f'), and we find that

$$\psi(n)^5 b_n = a_n.$$

Therefore, for any suitable prime ℓ, the ℓ-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_{13}))$ on the Tate modules of $J_1(13)$ and A_f are equivalent, so the abelian varieties are isogenous over $\mathbb{Q}(\zeta_{13})$. The rational point of order 19 on $J_1(13)$ should correspond (unless it is in the kernel of the isogeny) to a point of order 19 on A_f on which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via the character ψ^5. This point should yield corresponding points on the elliptic curves E^1 and E^2.

Let $P = (x, y)$, where

$$\begin{aligned} x &= -120 - 45(\zeta_{13} + \zeta_{13}^{-1}) - 72(\zeta_{13}^2 + \zeta_{13}^{-2}) \\ &\quad -9(\zeta_{13}^3 + \zeta_{13}^{-3}) - 9(\zeta_{13}^4 + \zeta_{13}^{-4}) \\ y &= 108(4(\zeta_{13} - \zeta_{13}^{-1}) + 5(\zeta_{13}^2 - \zeta_{13}^{-2}) + 8(\zeta_{13}^3 - \zeta_{13}^{-3}) \\ &\quad +4(\zeta_{13}^4 - \zeta_{13}^{-4}) + 6(\zeta_{13}^5 - \zeta_{13}^{-5}) - (\zeta_{13}^6 - \zeta_{13}^{-6})). \end{aligned}$$

Let $\sigma_4 : \zeta_{13} \mapsto \zeta_{13}^4$ be a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q}(\sqrt{13}))$. Then $19P = 0$ on E^1 and $\sigma_4(P) = 8P$ (note that 8 mod 19 has multiplicative order 6). Of course σ_2, which generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q})$, maps P to a point of order 19 on the conjugate curve E^2.

https://doi.org/10.1023/A:1000210813088 Published online by Cambridge University Press

The point P was found using PARI as follows. Because complex conjugation should act via an odd character, the y-coordinate of P should be imaginary. Therefore P should correspond to 1/19 of an imaginary period of E^1. Also, the $\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q}(\sqrt{13}))$-conjugates of P are $8P, 8^2P = 7P, 18P, 11P$, and $12P$, and the remaining $\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q})$-conjugates lie among similarly computed points on E^2. Trying the various possibilities (does $\sigma_4(P) = 8P$ or $\sigma_4^{-1}(P) = 8P$; which point on E^2 is $\sigma_2(P)$?), and solving for the coefficients of $\zeta_{13}^j \pm \zeta_{13}^{-j}$, eventually yields the above value for P.

We can use this to give another proof that $E_{1/11}$ and $E_{-1331/4799}$ are 19-isogenous. Since the subgroup of $E_{1/11}$ generated by P is rational over $\mathbb{Q}(\sqrt{13})$, we see that $E_{1/11}$ has a $\mathbb{Q}(\sqrt{13})$-isogeny of degree 19, the only question being what curve is it isogenous to. If $E_{1/11}$ is 19-isogenous to itself or to its conjugate, then it has an endomorphism of degree 19 or 57, which is impossible since $E_{1/11}$ does not have CM. The 19-isogenous curve still has a 3-isogeny with its conjugate, and has the same reduction properties as E^1, so it must be on our list. Therefore, we find that $E_{1/11}$ must be 19-isogenous to $E_{-1331/4799}$ or its conjugate. The method used above to predict that $E_{-1/11}$ and $E_{1331/4799}$ are 19-isogenous can be used to show that $E_{1/11}$ and the conjugate of $E_{-1331/4799}$ are not 19-isogenous; namely, the method yields only finitely many possibilities for the matrix of determinant ± 19, and none of these maps one τ to the other. Therefore $E_{1/11}$ and $E_{-1331/4799}$ must be 19-isogenous, as desired.

Acknowledgements

The authors wish to thank Horst Zimmer, Josef Gebel, François Morain, John Cremona, and Bjorn Poonen for their valuable assistance, some of which was initiated during an Oberwolfach Conference in 1995. The second author was supported by an NSA grant; he also thanks the Institute of Advanced Study for its hospitality during the final preparation of this paper.

References

1. Atkin, A. O. L. and Lehner, J.: Hecke operators for $\Gamma_0(m)$, *Math. Ann.* 185 (1970) 134–160.
2. Cremona, J. E.: *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.
3. Cremona, J. E.: Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction, *Math. Proc. Cambridge Phil. Soc.* 111 (1992) 199–218.
4. Diamond, F.: On deformation rings and Hecke rings, *Annals of Math.* 144 (1996) 137–166.
5. Gebel, J., Pethő, A. and Zimmer, H.: Computing integral points on elliptic curves, *Acta Arith.* 68 (1994) 171–192.
6. Lang, S.: *Algebra*, Addison-Wesley, 1965.
7. Livné, R.: Cubic exponential sums and Galois representations, *Current Trends in Arithmetical Algebraic Geometry (Arcata, 1985)*, 247–261, Contemp. Math., 67, Amer. Math. Soc., 1987.
8. Mazur, B. and Tate, J.: Points of order 13 on elliptic curves, *Invent. Math.* 22 (1973) 41–49.
9. Milne, J.: On the arithmetic of abelian varieties, *Invent. Math.* 17 (1972) 177–190.
10. Morain, F.: Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques, *J. Théor. Nombres Bordeaux* 7 (1995), 255–282.

11. Ogg, A.: Rational points on certain modular curves, *Analytic Number Theory*, Proc. Sympos. Pure Math., XXIV, 221–231, Amer. Math. Soc., 1973.
12. Ribet, K.: Abelian varieties over $\mathbb{Q}$ and modular forms, *Algebra and Topology 1992 (Taejŏn)*, 53–79 (1992), Korea Adv. Inst. Sci. Tech., Taejŏn.
13. Ribet, K.: Twists of modular forms and endomorphisms of abelian varieties, *Math. Ann.* 253 (1980) 43–62.
14. Ribet, K.: Galois representations attached to eigenforms with Nebentypus, *Modular Forms of One Variable, V*, 17–51, Lecture Notes in Math. 601, Springer-Verlag, Berlin, 1977.
15. Ribet, K.: Endomorphisms of semi-stable abelian varieties over number fields, *Ann. Math.* 101 (1975) 555–562.
16. Ribet, K.: On ℓ-adic representations attached to modular forms II, *Glasgow Math. J.* 27 (1985) 185–194.
17. Roberts, B.: $\mathbb{Q}$*-curves over Quadratic Fields*, Ph.D. thesis, University of Maryland, August 1995.
18. Serre, J-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* 54 (1987) 179–230.
19. Serre, J-P.: Quelques applications du théorème de densité de Chebotarev, *Publ. Math. IHES* 54 (1981) 323–401.
20. Serre, J-P.: *Abelian ℓ-adic Representations and Elliptic Curves*, W. A. Benjamin, Inc., New York-Amsterdam, 1968.
21. Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.
22. Shimura, G.: On the factors of the Jacobian variety of a modular function field, *J. Math. Soc. Japan* 25 (1973) 523–544.
23. Shimura, G.: On elliptic curves with complex multiplication as factors of the jacobians of modular function fields, *Nagoya Math. J.* 43 (1971) 199–208.
24. Shimura, G.: Class fields over real quadratic fields and Hecke operators, *Ann. Math.* 95 (1972) 130–190.
25. Tzanakis, N. and de Weger, B.: How to explicitly solve a Thue-Mahler equation, *Compositio Math.* 84 (1992) 223–288; 89 (1993) 241–242.
26. de Weger, B.: *Algorithms for Diophantine Equations*, CWI Tract, 65, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.
27. Wiles, A.: Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.* 141 (1995) 443–551.