Elliptic and modular curves over finite fields and related computational issues

Noam D. Elkies

March, 1997

Based on a talk given at the conference
COMPUTATIONAL PERSPECTIVES ON NUMBER THEORY
in honor of A.O.L. Atkin
held September, 1995 in Chicago

Introduction

The problem of calculating the trace of an elliptic curve over a finite field has attracted considerable interest in recent years. There are many good reasons for this. The question is intrinsically compelling, being the first nontrivial case of the natural problem of counting points on a complete projective variety over a finite field, and figures in a variety of contexts, from primality proving to arithmetic algebraic geometry to applications in secure communication. It is also a difficult but rewarding challenge, in that the most successful approaches draw on some surprisingly advanced number theory and suggest new conjectures and results apart from the immediate point-counting problem.

It is those number-theoretic considerations that this paper addresses, specifically Schoof's algorithm and a series of improvements using modular curves that have made it practical to compute the trace of a curve over finite fields whose size is measured in googols. Around this main plot develop several subplots: other, more elementary approaches better suited to small fields; possible generalizations to point-counting on varieties more complicated than elliptic curves; further applications of our formulas for modular curves and isogenies. We steer clear only of the question of how to adapt our methods, which work most readily for large prime fields, to elliptic curves over fields of small characteristic; see [Ler] for recent work in this direction.

Our present paper is organized in four sections. In the first section we describe elementary approaches to the problem of computing the trace, outline Schoof's original algorithm, and sketch several practical improvements, concentrating on the role played by isogenies and modular curves. The next section considers how these methods apply to curves of higher genus and to some algebraic varieties of higher degree. The third section explains what information we need about the modular curve $\mathrm{X}_0(l)$ to carry out the program outlined in §1 for curves over fields of characteristic $> l$, expanding on and streamlining the treatment of [El2].[1] In the fourth section we discuss how the explicit equations for and

[1] There are two main changes: we dispense with extraneous factors of π by working from the start with isogenies between Tate curves instead of lattices in $\mathbf{C}$; and we simplify the recursion (69) for the coefficients of the isogeny. We note that in the meantime Schoof has developed an alternative approach to computing an l-isogeny associated to a given point of

functions on $\mathrm{X}_0(l)$ needed for that and other applications can be obtained.

In addition to working out some specific examples in the course of the exposition, we also include an Appendix giving explicit coordinates and equations for modular curves of five levels with various applications. Besides illustrating a variety of approaches to and uses for such equations, the five segments of the Appendix might serve as prototypes for entries in an encyclopædia, atlas or hiker's guide to modular curves to be compiled at some future date.

It is particularly appropriate that this paper should appear in a volume dedicated to A.O.L. Atkin. Atkin's many contributions to the theory and computational practice of elliptic and modular curves have been particularly seminal in the development of Schoof's idea from a purely theoretical gem to a practical algorithm at the center of much recent research. Atkin's influence is not evident from the bibliography of this paper, because he has disseminated his results and insights in letters to his colleagues, as in the age of Fermat and his contemporaries, rather than by formal publication. Indeed Atkin has not to my knowledge published a single research article on these ideas.[2] But this article and the work it represents would scarcely have been possible without Atkin's contribution.

A few notational conventions must be noted here. By trafficking in a perfusion of elliptic curves and Eisenstein series we risk a confusion of E's. To forestall confusion we use E (or E_1, E', etc.) for an elliptic curve, and E (subscripted appropriately) for an Eisenstein series. In estimates of running times etc. we generally use ϵ in an exponent as an abbreviation for $o(1)$, and without the implication that all or any of these ϵ's are the same; in nearly all cases a factor x^ϵ is actually $(\log x)^{O(1)}$.

1. Counting points on elliptic curves: general remarks

Elementary methods: counting and BSGS. Let $k = \mathbf{F}_q$ be a finite field of q elements, and E an elliptic curve over k. A natural invariant of E is the number

$$N_1 = N_1(E) = \#E(k) = q + 1 - t \tag{1}$$

of k-rational points of E. By a fundamental theorem of Hasse (*Math. Z.* **31** (1930), 565–82; see [Sil], Thm. V.2.4 (p.136)) the <u>trace</u> t is bounded by $|t| \leqslant 2\sqrt{q}$, so $N_1 \leqslant (\sqrt{q}+1)^2$. It is easy to count, or even list, these points in time $q^{1+\epsilon}$, little more than the time $O(N_1 \log q)$ it takes to merely write down N_1 coordinate pairs.[3] But in general we do not need a roster of $E(k)$, only its size N_1, and a computation time of $q^{1+\epsilon}$ is far from satisfactory when q is at all large: it takes only $O(\log q)$ bits to specify k, E and N_1, so $q^{1+\epsilon}$ is exponential time, and

$\mathrm{X}_0(l)$, based on differentiating modular equations; see [Sc2, §7], especially Theorem 7.3.

[2] As a result some of his work appears here, explicitly credited to him, for the first time.

[3] Schoof observes that in the seminal paper [SD] even the fact that this can be done in time $q^{1+\epsilon}$ as opposed to $q^{2+\epsilon}$ was deemed worthy of note (specifically, of a footnote, on page 284)!

prohibitively large once q is much larger than say[4] 10^6. Still we mention this direct approach not only for comparison with more sophisticated methods but because we shall see that in more general contexts (e.g. counting points of a curve of genus $\geqslant 3$ over k) it may be the best method practically available.

A much faster method exploits the group structure of $E(k)$ and the fact that, by Hasse, N_1 is known to within $O(q^{1/2})$. To simplify the exposition assume that the group $E(k)$ is "nearly cyclic" in the sense that its exponent exceeds $4\sqrt{q}$ and so determines N_1. (For a randomly chosen curve this is usually the case; in particular if q is prime then either E or its quadratic twist E^{tw} always satisfies this condition once $q \geqslant 461$ [Co1, p.397], and since E^{tw} has trace $-t$ computing $N_1(E^{\text{tw}})$ will determine $N_1(E)$ as well. If q is not prime the condition may fail, most notably when q is a square and E is a supersingular curve whose Frobenius endomorphism is a square root of q. This requires a more involved algorithm, but still of the same complexity, since at worst we can adapt the algorithm for general abelian groups [Co1, p.236].) Choose a random point[5] P and calculate $Q := (q+1)P$. Note that by the usual doubling trick (see for instance [Co1, p.8]) this may be done in only $O(\log q)$ group operations in $E(k)$, each of which takes only a constant number of field operations in k. Then $Q = tP$, and since $|t| < 2\sqrt{q}$ we may find t by trying the $2\lfloor 2\sqrt{q}\rfloor$ small multiples of P to find those that match Q. The only hitch is that there may be more than one such multiple. However, in that case Q has order at most $4\sqrt{q}$. By our assumption on E, the order of Q will exceed $4\sqrt{q}$ with probability at least $q^{-\epsilon}$, and thus if we try more random P until a unique t emerges we will succeed in expected time $q^{1/2+\epsilon}$.

This may be reduced further to $q^{1/4+\epsilon}$ using Shanks' "Baby Step Giant Step" (BSGS) method, an observation attributed to Mestre in [Co1, p.397]. This is because the $O(q^{1/2})$ possible values of t fall in an arithmetic sequence. Let $Q_1 = Q + \lfloor 2\sqrt{q}\rfloor P$ and $t_1 = t + \lfloor 2\sqrt{q}\rfloor \in [0, 4\sqrt{q}]$. Let $S = \lceil (16q)^{1/4}\rceil$, so $t_1 = aS + b$ for some positive integers $a, b < S$. Then $Q = tP$ becomes

$$bP = Q_1 - (aS)P. \tag{2}$$

Compute and list the multiples bP (the "baby steps") and $aS \cdot P$ (the "giant steps"), and find matches between the two lists in $O(S \log S)$ steps, either by merging them and sorting the combined list or using hashing (see [Kn-3] for both approaches). This yields t_1, and thus also t, in only $q^{1/4+\epsilon}$ time. This

[4] Cohen suggests [Co1, p.396] that 10^4 is a reasonable limit, though that is in the context of computing L-functions of elliptic curves over $\mathbf{Q}$, where one needs the trace mod p for each prime p up to that limit and thus must compute N_1 many times.

[5] It is not known how to deterministically find in polynomial time any nonzero point on a general elliptic curve E/k. In practice, however, if E is given in Weierstrass form one need only choose the x-coordinate randomly from k and test whether x lifts to a pair of k-rational points, which will happen with probability $1/2 + O(q^{-1/2})$ by the Hasse bound, and thus almost certainly if we try say $\log q$ random values of x. To compute the y-coordinate we must also evaluate a square root; this, too, is easy in practice even though no deterministic algorithm has been proved to do it efficiently [Co1, 31–33]. In fact for our present purposes it is readily checked that the y coordinate, which only distinguishes P from $-P$, is not even needed.

improvement comes at the cost of taking also $O(q^{1/4})$ space, whereas our other algorithms thus far have required only enough space to store a constant number of field elements. However, if q is small enough for us to comfortably undertake a $q^{1/4+\epsilon}$-time computation, it is also small enough for us to afford $O(q^{1/4})$ space on present-day computers. For even larger q, if only $S < q^{1/4}$ space is available we can still partition the gamut of possible t into intervals of length S^2, apply BSGS to each interval, and thus obtain the answer in expected time $O(q^{1/2+\epsilon}/S)$. Alternatively, we may adapt Pollard's "kangaroo trap" method [Pol], a randomized algorithm requiring only $O(\log q)$ space whose heuristically expected running time is $q^{1/4+\epsilon}$, same as for the space-intensive BSGS approach.

Schoof's algorithm. Of course $q^{1/4+\epsilon}$ is much smaller than the $q^{1+\epsilon}$ for direct counting, but still grows exponentially. Remarkably, a much more complicated algorithm discovered by Schoof takes deterministically polynomial time $O(\log^M q)$, though the degree of the polynomial M is moderately large. An interesting tale hangs on the title of the paper [Sc1] introducing this algorithm. According to Schoof, he found the algorithm a few years earlier, but it was then refused publication on the grounds that the result was of little interest and no use! He then noticed that if q is prime and E is the reduction mod q of a curve with complex multiplication by a quadratic imaginary ring $O_D = \mathbf{Z}[\frac{1}{2}(D + \sqrt{-D})]$ of small discriminant $-D$, which is a square mod q — for instance if q is a prime $\equiv 1 \bmod 3$, and E is the CM curve $Y^2 = X^3 - 1$ with $D = -3$ — then the trace t of E yields a square root of $-D \bmod q$. Indeed the integer $4q - t^2$ is Db^2 for some $b \in \mathbf{Z}$, and then $(t/b)^2 \equiv -D \bmod q$. Thus Schoof's algorithm, together with an algorithm to compute the CM curve mod q given D, yielded the first unconditionally deterministic polynomial-time algorithm for extracting square roots of small integers mod q; with this application, the result was deemed publishable. Of course in practice one would never use this method to compute the square root, or even the representation $4q = t^2 + Db^2$, because the randomized algorithms of Tonelli-Shanks and Cornacchia [Co1, 32–36] are so much faster; indeed we shall see that to speed up Schoof's algorithm in practice we'll need to solve about $\log q$ quadratic equations over k, whose discriminants will not in general lift to small integers.

Schoof's algorithm exploits not only the group structure of E and the Hasse bound but also the interpretation of t as the linear coefficient of the characteristic polynomial χ_E satisfied by the Frobenius endomorphism $\phi : P \mapsto P^q$ of E:

$$\chi_E(\phi) = \phi^2 - t\phi + q = 0. \tag{3}$$

That is, if P is any point of E defined over some field containing k then

$$P^{q^2} - tP^q + qP = 0, \tag{4}$$

where P^q and P^{q^2} are the points obtained from P by replacing its coordinates by their q-th and q^2-th powers respectively. In particular, given some prime $l \neq \operatorname{char} k$, the identity (4) holds for all the l-torsion points $P \in E(\bar{k})$. But for such P the term tP^q in (4) depends only on the residue of $t \bmod l$, and conversely the identity (4) determines this residue uniquely. If we know $t \bmod l$ for small primes $l = 2, 3, 5, \ldots, l_i$ then, by the "Chinese Remainder Theorem" we know t modulo their product,

$$L_i := \prod_{j=1}^{i} l_j, \tag{5}$$

and once L_i exceeds $\lceil 4\sqrt{q}\,\rceil$ this together with $|t| \leqslant 2\sqrt{q}$ identifies t as an integer. But we can compute $t \bmod l$ in time polynomial in l and $\log q$ using (4). Indeed there are $l^2 - 1$ nonzero torsion points P, whose x-coordinates are roots of the division polynomials ψ_l of E; unless $l = \operatorname{char} k$, the ψ_l have degree $\frac{1}{2}(l^2 - 1)$ (except for $\deg \psi_2 = 3$) and coefficients in k, and are readily computed from the Weierstrass equation of E (see for instance [Co1, p.105, Ex. 3.7]), in $l^{O(1)}$ arithmetic operations in k. For each of the l possible values of $t \bmod l$, the identity (4) can be tested in $O(\log q)$ arithmetic operations mod ψ_l, using the repeated-squaring trick to handle the q-th and q^2-th powers, for a total of $l^{O(1)} \log q$ operations in k. By the Prime Number Theorem (actually the Čebyšev estimates on $\pi(x)$ suffice) L_i first exceeds $\lceil 4\sqrt{q}\,\rceil$ when $l_i \gg \log q$. Thus the total number of operations needed to compute each $t \bmod l_i$, and thence t, is bounded by a power of $\log q$ as claimed.[6]

How large a power of $\log q$ is needed? As we have outlined it, the algorithm is grossly inefficient; we should only compute $P^q, P^{q^2} \bmod \psi_l$ once, not l times, and can also use BSGS to find $t \bmod l$ instead of trying every integer mod l. The computational cost is then dominated by the $C \log q$ multiplications mod ψ_l needed to compute P^q, P^{q^2}. Done directly this requires on the order of $l^4 \log q$ arithmetic operations in k, which summed over the primes $l \ll \log q$ comes to $\log^{6-\epsilon} q$ operations; if each operation takes $O(\log^2 q)$ ticks, we obtain the upper bound $O(\log^8 q)$ of [Sc1] on the computation time. Using fast convolution techniques for the polynomial and finite-field arithmetic saves factors of $l^{2-\epsilon}$ and $\log^{1-\epsilon} q$, reducing the estimate to $\log^{5+\epsilon} q$, though with the ϵ tending to 0 very slowly as q increases.

While the fact that t can be computed in polynomial time is an important theoretical discovery (see e.g. [G-K]), it is not practical as it stands. This is because even its running time does not drop significantly below that $q^{1/4+\epsilon}$ of BSGS until q is so large that either approach would take unreasonably long. Nevertheless Schoof's algorithm is fundamental also to the practical computation of traces of elliptic curves over large finite fields. This is both because it can be used in tandem with BSGS to compute t faster than either method could by itself,

[6] We have been tacitly assuming that none of the small primes $l = l_j$ is the characteristic of k. If in fact k contains $\mathbf{Z}/l_j$, we could just skip that prime and substitute l_{i+1}, but in fact it is easier to compute $t \bmod l$. If ψ_l is a constant polynomial then E is supersingular and $l | t$ (and there are at most 5 possibilities for t so it can be computed almost instantaneously). More commonly, the curve is ordinary and ψ_l is the l-th power of a polynomial of degree $\frac{1}{2}(l-1)$ whose roots are the x-coordinates of the nonzero l-torsion points, and we can proceed to determine $t \bmod l$ as before but much more quickly because we work modulo a polynomial of much lower degree.

and more crucially because it is the basis for more recent improved algorithms which do substantially improve on BSGS. We address the former point first: even if we must stop computing $t \bmod l_j$ at some $i' < i$, before we know enough to determine t exactly, we do know an arithmetic progression mod $L_{i'}$ of length $O(q^{1/2}/L_{i'})$ in which t must lie, which reduces the BSGS work by a factor of $L_{i'}^{1/2}$. Even $i' = 2$ suffices to more than halve the computation time, and requires only arithmetic with polynomials of degree at most 4. (For instance, when q is odd, $2|\#E(k) \Leftrightarrow E$ has a k-rational 2-torsion point $\Leftrightarrow \psi_2$ has a root in $k \Leftrightarrow \gcd(\psi_2, x^q - x \bmod \psi_2)$ has positive degree.) Note, however, that this does not further improve the asymptotic behavior of Schoof's algorithm: for large q, a running time of $\log^{5+\epsilon} q$ limits the use of BSGS to arithmetic progressions of length $\log^{10+\epsilon} q$, and thus forces us to use Schoof for all but the last 10 primes l_j.

We next describe improvements that in practice drastically reduce the computational cost of finding $t \bmod l$ and thus of Schoof's algorithm. Our description will be conceptual, in terms of the action of $\phi \in \mathrm{Gal}(\bar{k}/k)$ on $E[l]$ or more generally $E[l^r]$; the translation of this description into polynomial arithmetic, necessary to carry out the computation, will be treated later. Schoof computes the trace of the image of ϕ in $\mathrm{GL}_2(\mathbf{Z}/l)$ via the action of ϕ on the $\frac{1}{2}(l^2-1)$ pairs of nonzero points of $E[l]$, represented by the polynomial ψ_l of degree $\frac{1}{2}(l^2-1)$. It is the need to compute modulo such a large polynomial that makes the algorithm so onerous. The key to the improvements is the possibility of extracting the same information from polynomials of considerably lower degree.

Beyond Schoof. Shortly after [Sc1] appeared, but before learning of that paper, I suggested the following approach to computing t: If, for some small prime l, the quadratic polynomial χ_E factors mod l, then ϕ acting on $E[l]$ has at least one eigenvalue $\lambda \bmod l$, and so at least one ϕ-stable subgroup $G \subset E[l]$ of size l on which ϕ acts by multiplication by λ. Now there are $l+1$ possible subgroups G, which are the kernels of the $l+1$ isogenies $E \to E_1$ of degree l, with the ϕ-stable ones corresponding to k-rational isogenies. To find rational isogenies, we would need to find roots in k of a polynomial of degree $l+1$ such as $\Phi_l(j(E), j') = 0$, where $j(E), j'$ are the j-invariants of E, E_1, and Φ_l is the l-th modular equation relating the j-invariants of l-isogenous curves. Given a ϕ-stable subgroup G, we could find the $\lambda \bmod l$ such that $(\phi - \lambda)|_G = 0$ as we did for $t \bmod l$ starting from (4), but with ψ_l replaced by the polynomial of degree $\frac{1}{2}(l-1)$ vanishing only on the x-coordinates of $G - \{0\}$. Thus for such l we could find λ, and thence $\lambda + p/\lambda \equiv t \bmod l$, by working modulo polynomials of degree at most $l+1$ and thus requiring only $l^{1+\epsilon} \log q$ field operations (or $l^2 \log q$ without fast polynomial arithmetic). For most E we expect that χ_E will factor mod l about half the time, so we will need to do this computation for about twice as many primes (L_i must exceed about $16q$ instead of $\lceil 4\sqrt{q})$ to accumulate enough information to determine t. Still these primes are each $\ll \log q$, so reasoning as before we expect to compute t in time $\log^{4+\epsilon} q$.

When I showed this to Barry Mazur, he consulted Michael Rabin, who quickly directed me to the paper [Sc1]. It appeared that Schoof had already accomplished what I had set out to do and more. Not only did he already have the idea of recovering t from its residues mod l and using the action of ϕ on $E[l]$ to find these residues, but he even succeeded in computing them and thus t in polynomial time without any hypotheses. By contrast, my approach, even if carried to completion (that is, if the coordinates of G could be efficiently computed from the j-invariant of $E_1 = E/G$), would fail if there were not enough small primes l at which χ_E factors. (Of course the analytic form of Dirichlet's theorem on primes in arithmetic progressions guarantees that asymptotically about half of the $(1 + o(1))x/\log x$ the primes $l < x$ will work, but it is not yet proved that there are any such $l \ll \log q$ or even $\ll \log^{O(1)} q$.) This last point seemed decisive, since at the time computing t seemed a purely theoretical problem, for which a deterministic polynomial-time algorithm trumps a heuristic one, however large the exponents of $\log q$ might be.

But once attention turned to the practical computation of t, the idea of using ϕ-eigenspaces G to find $t \bmod l$ promised to drastically reduce the actual computation time by computing modulo polynomials of degree $l + 1$ and $\frac{1}{2}(l - 1)$ instead of $\frac{1}{2}(l^2 - 1)$. This would save a factor of l (or l^2 without fast polynomial arithmetic), more than compensating for the few factors of 2 incurred because we only find $t \bmod l$ half the time. For instance, for $q \cong 10^{100}$ we find that L_i first exceeds $4q^{1/2}$ at $i = 32$ ($l_i = 131$), and $16q$ at $i = 55$ ($l_i = 257$), so we expect to compute t using polynomial arithmetic in degree < 300, as opposed to $\frac{1}{2}(131^2 - 1) = 8580$ for Schoof (or $\frac{1}{2}(79^2 - 1) = 3120$ if we relegate the last ten primes to BSGS). Realizing this considerable gain required actually finding a ϕ-stable group G when it exists; we shall turn to this problem in the next section, after a digression on counting points on varieties more complicated than elliptic curves.

At about the same time Atkin observed that the factorization of the polynomial $\Phi_l(j(E), j')$ in k already encodes information about $t \bmod l$, since it gives in effect the cycle structure of the action of $\phi|_{E[l]} \in \mathrm{PGL}_2(\mathbf{F}_l)$ on the $l + 1$ points of the projective line $(E[l] - \{\mathbf{0}\})/\mathbf{F}_l^*$. In general this cycle structure does not determine $t \bmod l$ completely but restricts it to a subset of $\mathbf{F}_l$, and it is not easy to reconstruct the integer t from this information for the various l; nevertheless Atkin succeeded in computing t for several curves E over finite fields $\mathbf{Z}/p$ with $p \cong 10^{65}$. The use of ϕ-stable subgroups to find $t \bmod l$ made it feasible to handle considerably larger p: Atkin announced the computation of t for a 100-digit prime p in late Feb.1992, and doubled the number of digits a few months later; by March 1994, he computed t for a "random" curve mod $p \cong 10^{275}$ [C-M, p.44]. In the years since, this has been increased to 500-digit primes $p \cong 10^{499}$ [Mor] thanks both to faster hardware and to improved algorithms. The latter include nice ways to further exploit the action of ϕ on torsion points. If l is split in $\mathbf{Z}[\phi] \otimes \mathbf{Q}$ then not only $E[l]$ but also $E[l^i]$ has a ϕ-stable line (cyclic subgroup of order l^i) for all i, which can be used in much the same way to determine $t \bmod l^i$ for small prime powers l^i; Couveignes and Morain [C-M] use such prime powers instead of larger primes l to compute t more efficiently. For any prime l, each factor of $\Phi_l(j(E), j')$ specifies a ϕ-stable set of l-isogenies from E, the nonzero points of whose kernels constituting ϕ-stable subsets of $E[l] - \{\mathbf{0}\}$. The corresponding factor of ψ_l can then be used in place of ψ_l. When $\Phi_l(J(E), j')$ has linear factors (i.e. roots $j' \in k$) this factor is just the polynomial giving the x-coordinates of a ϕ-stable group G. But even in the absence of such G, the irreducible factors of $\Phi_l(j(E), j')$ may have degree low enough compared with $l+1$ that the corresponding factors of ψ_l (whose degree is $(l-1)/2$ times larger) are much more tractable than ψ_l itself. Lercier and Morain, in an e-mail announcement dated Feb.95, attribute this observation to a preprint [Dew] of Dewaghe, and implemented it to set the 500-digit record noted above. Asymptotically these improvements contribute only a factor of $1+\epsilon$ to the computational efficiency, but the ϵ makes a big difference for $p < 10^{1000}$. Still, it is the primes l inert in the CM ring $\mathbf{Z}[\phi]$ that should offer the most scope for further improvement: a computation of $t \bmod l$ for such l in time comparable to what is now possible for split and ramified l would almost double the number of digits in p. The conjugacy class of the image of ϕ in $PGL_2(\mathbf{Z}/l)$ determines $t \bmod l$ up to sign, so one expects that at least $t^2 \bmod l$ should be accessible from the action of Frobenius on the roots of $\Phi_l(j(E), j')$. For now, though, this hope remains unrealized.

2. Point-counting beyond elliptic curves.

Higher genus. (See also [Poo], especially §§3–5.) Let C now be a curve of positive genus g over the finite field $k = \mathbf{F}_q$. Until we state otherwise, we will assume g is given and consider the situation as q increases. If $g = 1$, the problems of computing the characteristic polynomial of Frobenius

$$\chi_C(X) = X^{2g} + \sum_{i=1}^{2g} (-1)^i s_i X^{2g-i}, \tag{6}$$

the size of the Jacobian $\#J_C(k)$, and the number $N_1(C)$ of k-rational points are equivalent. But once $g \geqslant 2$, the characteristic polynomial contains more information: $N_1(C)$ may be recovered as $q + 1 - s_1$, and $\#J_C(k)$ as $\chi_C(1)$, but in general $N_1(C)$ and $\#J_C(k)$ do not determine χ_C. Generalizing $N_1(C)$ we could ask for each $i > 0$ for the number

$$N_i(C) = \#C(\mathbf{F}_{q^i}) \tag{7}$$

of points of C rational over the degree-i extension of k. The $N_i(C)$ are also determined by χ_C, and conversely the N_i for $1 \leqslant i \leqslant g$ together determine χ_C. Indeed, since $q^i + 1 - N_i$ is the trace of the i-th power of Frobenius, the first claim is immediate; the second follows because the traces of the first g powers, i.e. the first g power sums of the eigenvalues of Frobenius, determine their first g elementary symmetric functions $s_1, \ldots, s_g$, from which the remaining coefficients of χ_C are obtained via the functional equation: $s_{2g-i} = q^{g-i} s_i$.

In theory the fastest way to compute χ_C, and thus also $\#J_C(k)$ and $N_i(C)$, is Pila's generalization [Pil] of Schoof's algorithm, which computes χ_C, or even

χ_A for a principally polarized abelian variety[7] (ppav) A of dimension g, in polynomial time $\log^{C_g+o_g(1)} q$. We noted already that χ_C is determined by the coefficients $s_1, \ldots, s_g$ which are the elementary symmetric functions of degree $\leqslant g$ in the roots of χ_C. Since these roots all have norm $q^{1/2}$, we have $s_i \ll q^{g/2}$ for $i \leqslant g$, so these coefficients can be computed from their residues mod l for the primes $l \ll g \log q$. These residues are the coefficients of χ_C mod l, which is the characteristic polynomial of the action of ϕ on $J_C[l]$. Suppose we can represent J_C explicitly enough to write the group law algebraically and represent the nonzero l-torsion points by roots of a polynomial Ψ_l of degree $l^{2g}-1$ over k, as we have done in the case $g = 1$ of an elliptic curve $E = J_E$. If χ_C mod l has no repeated factors, we can determine it as before, by finding the unique s_i mod l $(1 \leqslant i \leqslant g)$ such that

$$P^{q^{2g}} + q^g P + \sum_{i=1}^{g-1} (-1)^i s_i (P^{q^i} + P^{q^{2g-i}}) + (-1)^g s_g P^{q^g} = 0 \tag{8}$$

for all $P \in J_C[l]$. To handle the general case we would first find the minimal polynomial

$$\mu_{C,l}(X) = X^h + \sum_{i=1}^{h} (-1)^i m_i X^{2g-i} \tag{9}$$

of $\phi|_{J_C[l]}$ by testing, for each $h \leqslant 2g$ and each possible h-tuple $(m_1, \ldots, m_h)$ satisfying a functional equation $\mu_{C,l}(q/x) = \pm q^{h/2} x^{-g} \mu_{C,l}(x)$, whether

$$P^{q^h} + \sum_{i=1}^{h} (-1)^i m_i P^{q^{h-i}} = 0 \tag{10}$$

holds for all $P \in J_C[l]$. For the smallest h for which some such $(m_1, \ldots, m_h)$ exists, it is unique, and yields the minimal polynomial $\mu_{C,l}$. Let $\mu_{C,l} = \prod_i f_i^{\alpha_i}$ be the factorization of $\mu_{C,l}$ into irreducibles over $\mathbf{Z}/l$. Compute for each i the size of the subgroup $G_i \subseteq J_C[l]$ killed by $f_i(\phi)^{a_i}$, which will be 1 more than the degree of the polynomial obtained by solving mod Ψ_l an equation corresponding to $(f_i(\phi)^{a_i})(P) = 0$. Necessarily $\#G_i = l^{\beta_i \deg f_i}$ for some integer $\beta_i \geqslant \alpha_i$. The characteristic polynomial χ_C is then $\prod_i f_i^{\beta_i}$.

How long should this computation take? Once we have obtained the polynomial Ψ_l, the most time-consuming steps are raising $2g$ polynomials mod Ψ_l to the power q, and finding the coefficients of $\mu_{C,l}$. Using fast polynomial arithmetic the first step requires $l^{2g+\epsilon} \log q$ field operations. The second step involves finding $l^{\lfloor h/2 \rfloor}$ coefficients of the minimal polynomial $\mu_{C,l}$ of degree $h \leqslant 2g$ (and usually $= 2g$), which we do using BSGS in $O_g(l^{\frac{1}{2}\lfloor h/2 \rfloor})$ operations mod Ψ_l, or a total of $l^{5g/2+\epsilon}$ field operations. Summing this over $l \ll \log q$, we find that the coefficient matching takes time comparable with the q-th powers for $g = 2$,

[7] Or even an abelian variety with a polarization of bounded degree, in which case the bound on the degree enters at least into the $o(1)$ of the $\log^{C_g+o(1)} q$ complexity estimate.

and dominates the computation time once $g \geqslant 3$; the final estimate on the computational complexity is $l^{5g/2+2+\epsilon}$ for $g \geqslant 2$.

But all this begs the question of how to find the polynomial Ψ_l in the first place. For elliptic curves ($g = 1$) this is well known and turns out to be an asymptotically negligible part of the computation. One expects that the same should be true for any given $g \geqslant 2$ as well; but so far carrying out this program seems utterly beyond practical implementation and represents a formidable challenge even in theory. Already for $g = 2$ it took a substantial effort to prove that there exists any finite constant C_2 such that χ_C can be computed in time $\log^{C_2+\epsilon} q$ for any curve $C/\mathbf{F}_q$ of genus 2 [AH]. For general g, it took even more heroic efforts by Pila (whose paper [Pil] represents a doctoral dissertation), supplemented by work of Huang and Ierardi [H-I], to get a bound $\log^{\Delta} q$ with Δ depending only (but exponentially) on g. The situation for hyperelliptic curves, including of course all curves with $g = 2$, is somewhat more promising thanks to Cantor's explicit formulas [Can].

As with Schoof's algorithm, these generalizations have striking consequences for the theoretical complexity of number-theoretic computation, similar to those of Schoof: primality certification [AH] and solving polynomial equations with small coefficients mod p [Pil]. But, even more so than Schoof's algorithm, they are ill suited to practical implementation, even allowing for potential improvements analogous to those available for $g = 1$. Nevertheless, we may want to repeatedly compute χ_C or $N_1(C)$ for curves C of small genus $g > 1$ over moderately large finite fields k, for instance to investigate the arithmetic of a curve over $\mathbf{Q}$ [Poo, §5] or to count points on a variety of higher dimension (see below). It turns out that, even ruling out Schoof-like methods, we can often compute these invariants of C in time which, though still exponential, is much less than might be expected.

We assume that C is given explicitly as a curve in some projective space of low dimension, or as a low-degree cover of $\mathbf{P}^1$, so that we can count points over $\mathbf{F}_{q^i}$ in time $q^{i+\epsilon}$, and in particular find some point $P_0 \in C(k)$ in time q^ϵ. (By the Weil estimates such a point must exist once $q > 4g^2$, which we may assume since we are concerned with fixed g and large q.) We then use P_0 to embed C in J_C, and identify J_C with linear equivalence classes of effective divisors of degree g on C. Given two such divisors, we can check whether they are equivalent, or find a divisor corresponding to their sum in J_C, in $O_g(1)$ field operations by using Riemann-Roch to reduce these problems to linear algebra with matrices of bounded size. (See for instance [Vol].) While this picture of J_C may not solve the problem of efficiently computing l-division polynomials Ψ_l, it is enough for our purposes.

For instance, since $\#J_C(k) \in [(\sqrt{q} - 1)^{2g}, (\sqrt{q} + 1)^{2g}]$ and this interval has length $\ll q^{g-1/2}$ we may use BSGS to find $\#J_C(k)$ in time $q^{g/2-1/4+\epsilon}$, as we did for $g = 1$. But in fact we can do better once $g \geqslant 3$. For instance, once we spend $q^{1+\epsilon}$ time counting k-rational points, we know the coefficient s_1 of χ_C, which restricts $\#J_C(k)$ to an interval of length $\ll q^{g-1}$ and thus reduces to

BSGS computation to $q^{(g-1)/2+\epsilon}$. When g increases further, it pays to first spend even more time counting points over small-degree extensions of k to find more coefficients of χ_C. Balancing the counting and BSGS costs we find that we should begin by calculating $N_i(C)$ for each $i \leqslant \lfloor 2g/5 \rfloor$ in time $q^{\lfloor 2g/5 \rfloor+\epsilon}$, which determines s_i for $i \leqslant \lfloor 2g/5 \rfloor$ and restricts $\#J_C(k)$ to an interval of length $\ll q^{(g-\lfloor 2g/5 \rfloor-1)/2}$. Comparing the square root of this with $q^{\lfloor 2g/5 \rfloor+\epsilon}$ we find that $\#J_C(k)$ *can be computed in expected time* $q^{\frac{1}{4}\lfloor 8g/5 \rfloor+o_g(1)}$ *for every* g*.*

We remark that it is no accident that the improvement ratio in the exponent from $g/2 - 1/4$ to $2g/5 - O(1)$ is the same for large g as that realized by Shanks' $D^{1/5+\epsilon}$ algorithm [Co1, 235 ff.] for finding the class number $h_D = h(\mathbf{Q}(\sqrt{-D}))$ over the $D^{1/4+\epsilon}$ it takes using only BSGS. Shanks' method assumes the Generalized Riemann Hypothesis (GRH) for the L-function of that quadratic field to approximate its value at 1, and thus h_D, to within $D^{2/5+\epsilon} = h^{4/5+\epsilon}$ by the product of the first $D^{1/5} \cong h^{2/5}$ Euler factors. For J_C the "Riemann Hypothesis" is a theorem and the initial computation of $N_1, N_2, \ldots, N_{\lfloor 2g/5 \rfloor}$ to find $s_1, \ldots, s_{\lfloor 2g/5 \rfloor}$ amounts to approximating $\chi_C(1)$ by the first $q^{\lfloor 2g/5 \rfloor} \cong \#J^{2/5}$ Euler factors of the L-function of C. Note that this improvement applies to Jacobians, which can be interpreted as class groups, but not to general ppav's.

[Further remark occasioned by correspondence from Andreas Stein: Shanks' algorithm for the class number of a real quadratic field hinges not (directly) on the structure of its class group, but on what Shanks calls the "infrastructure" of the field ([Sha], see [Co1, p.274 ff.]), which makes the algorithm deterministic, whereas using BSGS to determine the size of a group requires random choices of group elements. In their manuscript [S-W] Stein and Williams adapted this approach to "real quadratic function fields", i.e. hyperelliptic curves with a non-Weierstrass rational point P_0, to obtain a deterministic algorithm with the same $q^{(2/5+o(1))g}$ run time. The point P_0 and its hyperelliptic image are used as the two infinite places of the function field. This extra datum is but a minor hurdle in our setting of fixed g and large q, when such P_0 always exist and are easily found in expected time q^ϵ. In [S-W] q must be odd, but the algorithm probably has an even-characteristic analogue. Can analogous methods make deterministic the computation of $\#J_C(k)$ for non-hyperelliptic curves C, or of $\#A(k)$ for the twists A of J_C that we use below?]

A further refinement lets us compute, in the same expected time $q^{\frac{1}{4}\lfloor 8g/5 \rfloor+o_g(1)}$, the special value $\chi_C(-1)$ (as opposed to $\#J_C(k) = \chi_C(+1)$). This is because $\chi_C(-1)$ is the number of k-rational points of the quadratic twist J_C^{tw}. If C is hyperelliptic then J_C^{tw} is the Jacobian of its quadratic twist C^{tw} so we already know how to count its k-rational points in time $q^{\lfloor 2g/5 \rfloor}$, though of course we need not compute $N_i(C^{\mathrm{tw}})$ once we know $N_i(C)$. Even when C is not hyperelliptic, we can interpret $\chi_C(-1)$ as the size of the groups

$$J_C(\mathbf{F}_{q^2})/J_C(\mathbf{F}_q) \cong J_C[\phi+1] = \{P \in J_C(\mathbf{F}_{q^2}) : \phi P = -P\} \tag{11}$$

(the isomorphism being given by $\phi-1$). We can compute in such a group almost as easily (i.e. slower only by a constant factor) as in J_C; using the known $N_i(C)$

we approximate its size to within $O(q^{(g-\lfloor 2g/5\rfloor -1)/2})$ as before, and thus compute it in expected time $q^{\frac{1}{4}\lfloor 8g/5\rfloor + o_g(1)}$.

For $g=2,3$ the numbers $N_1(C), N_2(C), \ldots, N_{\lfloor 2g/5\rfloor}$ together with $\chi_C(\pm 1)$ give enough linear equations on the coefficients s_i of χ_C to determine these coefficients exactly. By doing some more work, but no more than the $q^{\frac{1}{4}\lfloor 8g/5\rfloor + o_g(1)}$ already expended, we can find χ_C also for $g=4,5$ and, with some subterfuge, even for $6 \leqslant g \leqslant 9$. We consider each case in turn:[8]

Genus 2. Without precomputing any $N_i(C)$ we find $\chi_C(1)$ and $\chi_C(-1)$ in expected time $q^{3/4+\epsilon}$, from which we recover

$$s_1 = \frac{\chi_C(-1)-\chi_C(1)}{2(q+1)}, \quad s_2 = \frac{\chi_C(1)+\chi_C(-1)}{2} - (q^2+1) \tag{12}$$

(and the fact that $s_1 \in \mathbf{Z}$ provides a check on the computation). In particular *we can find the trace of a genus-2 curve in expected time* $q^{3/4+\epsilon}$, less than the $q^{1+\epsilon}$ time it takes to count points directly. In fact the BSGS computation of $\chi_C(-1)$ is almost superfluous once $\chi_C(+1)$ is known, because $\chi_C(1) = q^2+1-(q+1)s_1+s_2$ together with the inequalities $s_1 \ll \sqrt{q}$, $s_2 \ll q$ (more precisely

$$|s_1| \leqslant 4\sqrt{q}, \quad 6q - 2\sqrt{q}\,|s_1| \leqslant s_2 \leqslant 2q + \frac{1}{4}s_1^2) \tag{13}$$

leaves at most $O(1)$ choices for (s_1, s_2) (once q is large enough, at most 7 pairs can satisfy (13), usually less), and thus only $O(1)$ possibilities for $\chi_C(-1) = \#J_C^{\mathrm{tw}}$, which we can distinguish in expected time q^ϵ.

Genus 3. In time $q^{1+\epsilon}$ we compute $N_1(C)$, thus restricting $\#J_C(k)$ to an interval of length $O(q^2)$ and letting us compute it also in expected time $q^{1+\epsilon}$. At this point we know $s_1 = q+1-N_1(C)$ and $(q+1)s_2 - s_3 = \#J_C(k) - (q^3+1) + (q^2+1)s_1$. Since $s_2 \ll q$ and $s_3 \ll q^{3/2}$ this leaves $O(q^{1/2})$ possibilities for (s_2, s_3) which we expect to distinguish in time $q^{1/2+\epsilon}$ (whereas a second BSGS computation starting only from s_1 to determine $\#J_C^{\mathrm{tw}}$ would take $q^{1+\epsilon}$); indeed since the possible values of $\#J_C^{\mathrm{tw}}$ lie in an arithmetic progression we expect to find the correct one in time only $q^{1/4+\epsilon}$. However we handle this last step, *we can find χ_C for a genus-3 curve C in expected time* $q^{1+\epsilon}$, essentially the same time that it takes just to find $N_1(C)$ by counting points.

Genus 4. We take $q^{1+\epsilon}$ time to compute $N_1(C)$ and $q^{3/2+\epsilon}$ to find $\chi_C(1)$ and $\chi_C(-1)$. At this point we know s_1, s_3, and $(q^2+1)s_2 + s_4$. Since $s_4 \ll q^2$ there are only $O(1)$ possibilities for χ_C. To distinguish these we need a new ingredient, and find it in the groups

$$J_C(\mathbf{F}_{q^4})/J_C(\mathbf{F}_{q^2}) \cong J_C[\phi^2+1] = \{P \in J_C(\mathbf{F}_{q^4}) : \phi^2 P = -P\}, \tag{14}$$

the last being the group of $\mathbf{F}_{q^2}$-rational points on the quadratic twist of $J_C/\mathbf{F}_{q^2}$. (We could similarly use the subgroups $J_C[\phi^2 \pm \phi + 1]$ of $J_C(\mathbf{F}_{q^3})$ and $J_C(\mathbf{F}_{q^6})$.

[8] The reader more interested in the "big picture" or specifically in matters related to Schoof's algorithm may skip or skim the next few pages concerning the details of the cases $2 \leqslant g \leqslant 9$, which are not needed in the sequel.

The group (14) has size $\chi_C(i)\chi_C(-i)$; more precisely, its order ideal as a $\mathbf{Z}[i]$ module[9] (with ϕ acting as $i=\sqrt{-1}$) is $(\chi_C(i))$. Each of the $O(1)$ possible χ_C yields a different $(\chi_C(i))$ once q is large enough, so we expect to pick out the correct one in time q^ϵ. (Note that it is usually easy to tell that such a group does *not* have order ideal I for some $I \subset \mathbf{Z}[i]$ of norm $\cong q^{2g}$.) Thus for $g=4$ we still expect to compute χ_C in little more than the time $q^{3/2+\epsilon}$ that it took to find its special values $\chi_C(\pm 1)$.

Genus 5. In $q^{2+\epsilon}$ time we compute $N_1(C)$ and $N_2(C)$, limiting $\chi_C(\pm1)$ to intervals of length $O(q^{7/2})$, and letting us compute them in time $q^{7/4+\epsilon}$. (We could also count points only over k to find $\chi_C(\pm1)$ in time $q^{2+\epsilon}$, but since we want to get at χ_C itself we may as well begin by computing s_2 as well which reduces the BSGS work.) We then know s_1, s_2, s_4, and $(q^2+1)s_3+s_5$. Since $s_5 \ll q^{5/2}$ this leaves $O(\sqrt{q})$ possibilities, which we again expect to distinguish with much less work than the $q^{2+\epsilon}$ we have done so far. In fact, since the possible values of $\chi_C(i)$ fall in an arithmetic sequence in $\mathbf{Z}[i]$, we can generalize the BSGS or Pollard method to do this final step in time $q^{1/4+\epsilon}$. Note that this improvement, which will be crucial for $g=7,8$, requires the $\mathbf{Z}[i]$-module structure of $J_C[\phi^2+1]$, because the possible orders of $J_C[\phi^2+1]$ as $\mathbf{Z}$-modules (=abelian groups) constitute a quadratic sequence, not a linear one, for which no comparable BSGS or Pollard shortcut is evident.

Genus 6. Here we spend $q^{2+\epsilon}$ time computing s_1 and s_2, and $q^{9/4+\epsilon}$ finding $\chi_C(1)$ and $\chi_C(-1)$ which gives us $(q^2-q+1)s_3+s_5$ and $(q^2+1)s_4+s_6$. Since $s_5 \ll q^{5/2}$ and $s_6 \ll q^3$, this leaves $O(\sqrt{q})$ possibilities for (s_3,s_5) and $O(q)$ for (s_4,s_6), so we expect to determine χ_C by doing $q^{3/2+\epsilon}$ additional work, still negligible compared to the $q^{5/2+\epsilon}$ used to find $\chi_C(\pm1)$. Again we can further shorten this last step by adapting BSGS, to $q^{3/4+\epsilon}$. This is because, while the set of possible values of $\chi_C(i)$ no longer constitutes an arithmetic progression, it is the convolution of two arithmetic progressions. It can thus be expressed as a convolution $\{s+t : s\in S, t\in T\}$ of two sets $S,T \in \mathbf{Z}[i]$ of about equal size, which is all BSGS requires: S and T will index the baby and giant steps respectively. (Can one adapt Pollard's kangaroo-hunting paradigm to such convolutions and thus keep the square-root time gain of BSGS without paying its square-root space cost?)

Genus 7. In time $q^{11/4+\epsilon}$ we compute s_1, s_2, and $\chi_C(\pm1)$, which give us

$$(q^4+1)s_3+(q^2+1)s_5+s_7, \quad \text{and} \quad (q^2-q+1)s_4+s_6.$$

The Weil bounds $s_i \ll q^{i/2}$ $(i=5,6,7)$ restrict s_3, s_4 to intervals of length $O(q^{1/2}), O(q)$, and then s_5 to within $O(q^{3/2})$. The resulting $O(q^3)$ possibilities can no longer be distinguished exhaustively, but the BSGS trick still applies, in expected time $q^{3/2} \ll q^{11/4+\epsilon}$.

Genus 8. The $q^{3+\epsilon}$-computation of $\chi_C(\pm1)$ yields s_1, s_2, s_3,

$$(q^4+1)s_4+(q^2+1)s_6+s_8, \quad \text{and} \quad (q^2-q+1)s_5+s_7.$$

[9] That is, the product of ideals I_j such that the module is isomorphic with $\prod_j(\mathbf{Z}[i]/I_j)$.

Here the ranges of s_4, s_5, s_6 are $O(q), O(q^{3/2}), O(q^2)$ so BSGS will take time $q^{9/4+\epsilon} \ll q^{3+\epsilon}$ to find $\chi_C(\pm i)$. A new wrinkle here is that this may still fail to determine all the coefficients: instead of s_4, s_8 we only find $(q^4+1)s_4 + s_8$. This does not quite suffice since we only know $s_8 \ll q^4$. But the $O(1)$ possibilities remaining can be distinguished by the values of χ_C at cube roots of unity, i.e. by working in

$$J_C(\mathbf{F}_{q^3})/J_C(\mathbf{F}_q) \cong J_C[\phi^2+\phi+1] \tag{15}$$

(the latter being the subgroup $\{P : \phi^2 P + \phi P + P = 0\}$ of $J_C(\mathbf{F}_{q^3})$). Thus we still find χ_C in expected time $q^{3+\epsilon}$.

Genus 9. This is the last case where our methods find χ_C in essentially the same time $q^{\frac{1}{4}\lfloor 8g/5 \rfloor + o_g(1)}$ it takes to just compute $\chi_C(1) = \#J_C(k)$. Here $\frac{1}{4}\lfloor 8g/5 \rfloor = 7/2$, and in time $q^{7/2+\epsilon}$ we find s_1, s_2, s_3 as well as

$$(q^4 - q^3 + q^2 - q + 1)s_4 + (q^2 - q + 1)s_6 + s_8$$

and

$$(q^4+1)s_5 + (q^2+1)s_7 + s_9.$$

By the Weil bounds there are $O(q)$ choices for s_4 and $O(q^{3/2})$ for s_5 consistent with given values of these linear combinations of the s_i. For each of the $O(q^{5/2})$ possible (s_4, s_5) there are ranges of lengths $O(q^2), O(q^{5/2})$ for s_6, s_7 which make $\chi_C(i)$ vary in the convolution of two arithmetic progressions with common difference $(2q-2)(q^2+1)$ and $2i(q^2+1)$ in $\mathbf{Z}[i]$. Thus the set of possible $\chi_C(i)$, which now has size $O(q^7)$, is still contained in the convolution of some $S, T \subset \mathbf{Z}[i]$ with each of S, T no larger than a constant multiple of the square root of that size. For instance we may replace each $O(q^2)$-length progression with common difference $(2q-2)(q^2+1)$ with $q+1$ progressions ϖ of common difference $2q^4 - 2$, then index S by triples (s_4, s_5, ϖ), and let T be $\{2m(q^4-1) + 2ni(q^2+1) \mid (m,n) \ll (q, q^{5/2})\}$. Then, provided we can afford $O(q^{7/2})$ space, we can use BSGS to determine $\chi_C(i)$ in expected time $q^{7/2+\epsilon}$, the same that it took to compute $\chi_C(1)$. We then know s_6, s_7 and the linear combinations $(q^4+q^3+q^2+q+1)s_4 + s_8$ and $(q^4+1)s_5 + s_9$. and as in the $g = 8$ case quickly distinguish the remaining $O(\sqrt{q})$ possibilities by using the groups (15) to test the corresponding values of χ_C at cube roots of unity.

Past genus 9 it no longer seems possible to use these methods to find χ_C so quickly. When $g = 10$ the $q^{4+\epsilon}$ computation yields s_1, s_2, s_3, s_4 and two linear forms in $s_5, \ldots, s_{10}$, and it takes at least $q^{9/2+\epsilon}$ further work to distinguish the remaining $O(q^9)$ possibilities. For even larger g it seems that in computing χ_C we can save no more than a fixed power of q over the direct approach of counting $N_i(g)$ for $i \leqslant g$. This is to be expected because already for the five coefficients s_{g-4} through s_g there are about $q^{5g/2-3}$ possibilities, so we can hardly hope to distinguish them in time less than q^g with a square-root method such as BSGS.

Higher dimension? The mod-l step of Schoof's algorithm in effect approximates the action of ϕ on the l-adic first cohomology group $H^1_l(E)$. More generally, the mod-l^i computation of [C-M] approximates this action more closely, and the Adleman-Huang and Pila generalizations involve $H^1_l(C) = H^1_l(J_C)$. Now let V be a smooth projective variety of dimension $d > 1$ over $k = \mathbf{F}_q$. Then the zeta function Z_V, and so in particular $\#V(k)$, can again be described in terms of the action of Frobenius on $H^i_l(V)$, this time with $1 \leqslant d \leqslant d$. If for some algebraic family $\mathcal{V}$ of varieties V we could exhibit $H^i_l(V) \bmod l$ explicitly in time polynomial in $l, \log q$ then we would have a polynomial-time algorithm for computing Z_V for $V \in \mathcal{V}$.

In a few cases this approach can succeed nontrivially. We noted already the example of abelian varieties V. If V is a cubic surface then the only problem is to determine the action of ϕ on the Neron-Severi group; there are only finitely many possibilities, indexed by conjugacy classes in the Weyl group of E_6, and we find the right one by factoring a polynomial of degree 27 corresponding to the lines on V [Wei, p.558]. If V is a quartic surface, or more generally a K3 surface, of Neron-Severi rank >16, then V is isogenous to the Kummer quotient of an abelian surface $\tilde{V}$, and the zeta function of $\tilde{V}$ determines that of V. Of course this becomes even easier when $\tilde{V}$ is itself isogenous to the product of two elliptic curves, as happens surprisingly often for "naturally arising" K3 surfaces with many symmetries, see for instance [PTV]. For a final example, if V is a Fano threefold, such as a cubic or quartic hypersurface in $\mathbf{P}^4$, then Z_V is determined by the L-function of the intermediate Jacobian of V, which is at least in principle accessible by Schoof-Pila.

But in all these cases we succeed only by reducing $H^i(V)$ for $i > 1$ to H^0 and H^1 of auxiliary varieties. Can anything be done when this is not possible — when, as the adherents of "motives" would say, the weight-i motive $H^i(V)$ ($i \geqslant 2$) cannot be expressed in terms of motives of weight 0 or 1? if V is an arbitrary quartic surface, is it even in principle possible to compute in $l^{O(1)}$ field operations a polynomial Ψ_l of degree l^{20} whose roots represent the part of $H^2_l(V) \bmod l$ orthogonal to the (hyper)plane section, and thus to compute Z_V and enumerate $V(k)$ in time polynomial in $\log q$?[10]

Coming back to earth from these speculative heights, we find that even without a Schoof-type algorithm the problem of computing of $\#V(k)$ is an attractive problem that should reward geometrically-inspired algorithmic finesse. The direct way, generalizing the $q^{1+\epsilon}$ approach for curves, uses a low-degree cover $f : V \to \mathbf{P}^d$ and takes time $q^{d+\epsilon}$. With $O(q^{d-1})$ points of $\mathbf{P}^d$ excepted, the preimages of each point under f correspond to roots of a polynomial of fixed degree and so can be enumerated in time q^ϵ for a total of $q^{d+\epsilon}$; the exceptional points, where f is not finite-to-one, come from a subvariety of V of dimension at

[10] Added at the last moment: the Kuga-Satake construction, used in [Del] to prove the Weil conjectures for K3 surfaces, probably answers this question affirmatively by associating to V a ppav whose H^1_l is the spin representation of the orthogonal group defined by $H^2_l(V)$ (with the intersection pairing). This may even extend to any "weight-2 motive". The construction is transcendental, but once it is known it can be given by algebraic equations, though exhibiting and analyzing an algorithm to carry it out for the general quartic surface is a most daunting prospect. No such construction seems to be known for motives of weight $\geqslant 3$, though, so we may ask instead: is there a polynomial-time algorithm for counting points on a general (say) quintic threefold over a large finite field?

most $d-1$, so by induction on d we enumerate $V(k)$ in the time claimed. But, as for curves of genus $\geqslant 2$, we can improve on this for certain V. For instance if there is a map from V to $\mathbf{P}^{d-1}$ (or, more rarely, to some other variety of dimension $d-1$) whose generic fiber is a curve of genus 2 or 1 then we can save a factor of $q^{1/4}$ or $q^{3/4}$ respectively since we can count points on curves of that genus in time $q^{3/4+\epsilon}$ or $q^{1/4+\epsilon}$ instead of $q^{1+\epsilon}$.

In fact for the case of genus 1 we can save a full factor of q even without invoking Schoof if we are willing to dedicate $O(q \log q)$ space to the computation. For instance, we can count points on a quartic surface with a rational line in time $q^{1+\epsilon}$. (Projection from the line gives a map to $\mathbf{P}^1$ whose generic fiber is a plane cubic.) This is because the $q^{1/4+\epsilon}$ time to compute the trace of one elliptic curve E_0 can be amortized over many curves isogenous with E_0 and thus of the same trace. We begin by tabulating the $2q + O(1)$ isomorphism classes of elliptic curves over k. Each genus-1 curve E in our fibration we look up in the table, and if it is there already we add $\#E(k)$ to the tally of rational points. If it is not there yet, we first do the BSGS computation of the trace of E, and also list small primes l split in the quadratic ring $\mathbf{Z}[\phi]$ (any prime l will do if $\phi \in \mathbf{Z}$, which can only happen if q is a square and E is supersingular). For each such l we shall see in the next section that we can compute in time $q^{\epsilon} l^{O(1)}$ a curve E_1/k that is l-isogenous to E_0. We enter E_1 and its trace into our table. We repeat this process until we find no new curves in the isogeny class of E_0. The curves thus obtained correspond to ideal classes of $\mathbf{Z}[\phi]$ generated by the prime ideals above our l. The running time of our algorithm thus depends on the sizes of subgroups of ideal class groups generated by small primes, which seem difficult to analyze rigorously. However the Cohen-Lenstra heuristics [C-L] suggest that even if we use just the smallest available l we will on average catch a positive proportion of the isogeny class. Moreover the smallest l will almost always be small enough that we can comfortably absorb the factor $l^{O(1)}$ into q^{ϵ}. (While this $l^{O(1)}$ reflects part of the computation we would use to implement Schoof's algorithm, it is much more palatable than fully applying Schoof to every curve, because we need only the smallest good l, not the first $C \log q$ of them.) there are only $O(q^{1/2})$ such classes, we thus expect to fill the table of traces in time $q^{1+\epsilon}$ and thus count points in time $q^{d-1+\epsilon}$ as claimed.

If $d > 2$ we do not even need the isogeny trick since we can afford to take $q^{2+\epsilon}$ time to compile the table. Likewise if V is birational to a family of curves of genus $g \geqslant 2$, and $d = \dim V$ is large enough ($d > 3g-2 = \dim \mathcal{M}_g + 1$) then we can compute $\#V(d)$ in time $q^{d-1+\epsilon}$ instead of $q^{d+\epsilon}$ if we are willing to dedicate $O(q^{3g-3} \log q)$ space to a table of the genus-g curves over k. An improvement ratio larger than q may occasionally be possible if we can usefully write V as a family of surfaces or higher-dimensional varieties; for instance if V is one of the 4-dimensional family of singular quintic threefolds $\alpha \wedge \beta = 0$ in $\mathbf{P}^4$ with α, β sections of the Horrocks-Mumford bundle [H-M], then V is birational to a pencil of abelian surfaces $a\alpha + b\beta = 0$ ($(a:b) \in \mathbf{P}^1$), each of which can be counted in time $q^{3/4+\epsilon}$ using BSGS, so $\#V(k)$ may be computed in total time $q^{7/4+\epsilon}$.

3. Modular curves parametrizing isogenies

The curve $\mathrm{X}_0(l)$**.** It is well-known that l-isogenies between elliptic curves E, E_1 are parametrized by the modular curve $\mathrm{X}_0(l)$ and that the function field of this modular curve is generated by $j = j(E), j' = j(E_1)$ satisfying the polynomial equation $\Phi_l(j, j') = 0$, where Φ_l is an irreducible polynomial of the form

$$\Phi_l(X, Y) = X^{l+1} + Y^{l+1} + \sum_{a=0}^{l}\sum_{b=0}^{l} f_{ab} X^a Y^b \tag{16}$$

with $f_{ab} \in \mathbf{Z}$. Since the dual of an l-isogeny from E to E_1 is an l-isogeny from E_1 to E, the polynomial Φ_l is symmetric under the involution $(X, Y) \leftrightarrow (Y, X)$ (the *Fricke* or *Atkin-Lehner involution* $w = w_l$), i.e. its coefficients satisfy $f_{ab} = f_{ba}$. Since the Tate curves[11] $\mathbf{G}_m/q^{\mathbf{Z}}$ and $\mathbf{G}_m/q^{l\mathbf{Z}}$ are l-isogenous, their j-invariants

$$\begin{aligned} j = j(\mathbf{G}_m/q^{\mathbf{Z}}) &= \frac{1}{q} + 744 + 196884q + \ldots [= j(q)], \\ j' = j(\mathbf{G}_m/q^{l\mathbf{Z}}) &= \frac{1}{q^l} + 744 + 196884q^l + \ldots [= j(q^l)] \end{aligned} \tag{17}$$

satisfy the equation $\Phi_l(j, j') = 0$. By comparing q-expansions we can thus recursively find all the coefficients of Φ_l. This direct approach requires at least $C \cdot l^4$ arithmetic operations, but we can reduce that to $l^{3+\epsilon}$ because we know not only $j' = j(q^l)$ but also the other l roots of $\Phi_l(j(q), x) = 0$: they are $j(q_1)$ where $q_1^l = q$. Using fast convolution techniques we compute the first $2l^2 + O(l)$ coefficients of the q-expansion of $j = E_4^3/\eta^{24}$ and its powers $j^2, j^3, \ldots, j^l$ in a total of $q^{3+\epsilon}$ arithmetic operations. Extracting from the expansion of lj^i $(i \leqslant l)$ the powers of q^l and substituting q for this q^l, we obtain $2l + O(1)$ initial terms of the q-expansion of each of the power sums $p_i = \sum_{q_1^l = q} j^i(q_1)$. In $l^{3+\epsilon}$ further arithmetic operations[12] we then find the elementary symmetric functions to the same precision using Newton's identities, or equivalently using the formula

$$\prod_{q_1^l = q} \bigl(1 - j(q_1)t\bigr) = \exp\left[-\sum_{i=1}^{\infty} p_i \frac{t^i}{i}\right] = \prod_{i=1}^{\infty} \exp(-p_i t^i/i) \tag{18}$$

and ignoring terms in t^{l+1} and beyond. Multiplying this generating polynomial $\prod_{q_1^l=q}\bigl(1 - j(q_1)t\bigr)$ by $(1 - j(q^l)t)$ in yet another $l^{2+\epsilon}$ steps yields $\Phi_l(j(q), Y)$ with

[11] The traditional use of q both for $\#k$ and for the parameter of the Tate curve is unfortunate, but will fortunately cause no confusion here.

[12] In fact fewer operations — only $l^{5/2+\epsilon}$, perhaps as little as $l^{2+\epsilon}$ — suffice to carry out the rest of the calculation, using more efficient ways to compose power series as described in [Kn-2, pp.656–7]; but this cannot improve the asymptotics of computing Φ_l as long as we do not know how to compute the power sums (or directly the elementary symmetric functions) in the $j(q_1)$ in less than $l^{3+\epsilon}$ operations, so for now we content ourselves with establishing the same $l^{3+\epsilon}$ bound for the entire computation.

each coefficient computed as a power series up to and including the constant term. Since we already have the q-expansions of $j^a(q)$ for $q \leqslant l$, we can for each $b = 0, 1, 2, \ldots, l$ express the Y^b coefficient as a polynomial $\sum_{a=0}^{l} f_{ab} j^a(q)$ in $j(q)$ in $O(l^2)$ steps, completing the computation of $\Phi_l(X, Y)$ in the claimed $l^{3+\epsilon}$ time. Note that for the Schoof application this computation need only be done once for each l; having computed and stored the coefficients $f_{ab} \in \mathbf{Z}$ we can use them for any elliptic curve in any characteristic.

Obstacles. But there are problems with this familiar picture. The lesser problem is that the coefficients f_{ab} are notoriously huge; already for $l = 2, 3$ we have

$$\begin{aligned}\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488(XY^2 + X^2Y) \\ -162000(X^2+Y^2) + 40773375XY + 8748000000(X+Y) - 2^{12}3^9 5^9,\end{aligned} \tag{19}$$

$$\begin{aligned}\Phi_3(X,Y) \quad = \quad & X^4 + Y^4 - X^3Y^3 + 2232(X^2Y^3 + X^3Y^2) \\ & -1069956(XY^3 + X^3Y) + 36864000(X^3+Y^3) + 2587918086X^2Y^2 \\ & +8900222976000(X^2Y + XY^2) - 2^{31}5^6 22973XY + 2^{45}3^3 5^9(X+Y).\end{aligned} \tag{20}$$

Since the coefficients grow as $\exp(l \log^{O(1)} l)$,[13] our "$l^{3+\epsilon}$ arithmetic operations" actually take time $l^{4+\epsilon}$ to carry out, and the result requires $l^{3+\epsilon}$ space to store. Thus our $\log^{4+\epsilon} q$ computation of the trace of an elliptic curve over $\mathbf{F}_q$ would also require $\log^{4+\epsilon} q$ space for permanent storage. It might seem that we can reduce this to $\log^{3+\epsilon} q$ temporary storage by computing Φ_l over k from scratch each time it is needed rather than over $\mathbf{Z}$ once and for all; unfortunately this would nullify our gains on Schoof's algorithm because doing $l^{3+\epsilon}$ field operations to compute Φ_l for each l would bring us back to a $\log^{5+\epsilon}$-time algorithm. Still the size of the f_{ab} is only a mild annoyance; computing a hundred or so Φ_l once and for all and storing the results on tape or CD-ROM would be an awkward and ugly project but not an impossible one.[14] Atkin observes that in practice one does better by a constant but considerable factor by working not with j but with its cube root

$$j^{1/3} = q^{-1/3}(1 + 248q + 4124q^2 + 34752q^3 + 213126q^4 + \cdots). \tag{21}$$

Except for $l = 3$, the modular functions $j(q)^{1/3}, j(lq)^{1/3}$ also satisfy a symmetric polynomial of degree $l + 1$, say $\Phi_l^{(3)}(j^{1/3}, j'^{1/3}) = 0$; for instance

$$\Phi_2^{(3)}(X,Y) = X^3 + Y^3 - (XY)^2 + 495XY - 54000. \tag{22}$$

[13] The precise logarithmic growth order has been obtained by P. Cohen [Co2]; taking m prime in her formula we find that the largest coefficient of Φ_l is $\exp 6l(\log l + O(1))$.

[14] The size of the coefficients of Φ_l has occasioned some wild overestimates of the difficulty of computing these polynomials. It has been suggested that even for $l = 11$ the computation is out of reach except possibly by heroic means — this when Atkin had already computed Φ_{11} and even Φ_{13} in a few seconds... Indeed by 1993 Jiu-Kang Yu had computed Φ_l for all $l \leqslant 41$ using nothing more than matching coefficients on MATHEMATICA [Yu].

These polynomials $\Phi_l^{(3)}$ have smaller coefficients $f_l^{(3)}$, which even vanish unless $a + lb \equiv l + 1 \bmod 3$. The approach outlined above for finding Φ_l works also for $\Phi^{(3)}$, or indeed to find a polynomial relation between any pair of modular functions with known q-expansion (a fact we make good use of later), but takes less time because the "arithmetic operations" involve much smaller numbers. From $\Phi_l^{(3)}$ we readily recover Φ_l itself using the identity

$$\Phi_l(X^3, Y^3) = \Phi_l^{(3)}(X,Y)\Phi_l^{(3)}(X, e^{2\pi i/3}Y)\Phi_l^{(3)}(X, e^{4\pi i/3}Y). \tag{23}$$

But there is a more fundamental problem: while $\mathrm{X}_0(l)$ parametrizes l-isogenies, one cannot easily read off an l-isogeny from the a solution of $\Phi_l(j, j') = 0$, and we can only carry out our proposed improvement of Schoof's algorithm once we have the kernel of the isogeny explicitly. Now it is well-known that the model $\Phi_l(X,Y) = 0$ of $\mathrm{X}_0(l)$ has singularities — only regular double points (nodes) over $\mathbf{C}$, often worse in small characteristics — at points (j, j') where j, j' are the invariants of a pair of CM (complex multiplication) curves with more than one l-isogeny, so the coordinates (j, j') cannot determine the isogeny. But even away from those singularities it is not at all clear how to recover the isogeny from the values of j, j', a problem made prominent by the application to Schoof's algorithm though it might well have been noticed earlier. Consider for instance the case of the exotic 37-isogeny.[15] In [M-SD] Mazur and Swinnerton-Dyer give an explicit equation for the modular curve $\mathrm{X}_0(37)$ of genus 2, and find on it a pair of $\mathbf{Q}$-rational points which are neither cusps nor CM points. By writing the rational functions j, j' on $\mathrm{X}_0(37)$ in terms of the coordinates of that equation (we shall say much more about this process later) we find that these points parametrize a 37-isogeny between curves of j-invariant $-9317 = -7 \cdot 11^3$ and $-7 \cdot 137^3\, 2083^3$. Let E, then, be the curve

$$Y^2 + XY + Y = X^3 + X^2 - 8X + 6 \tag{24}$$

of j-invariant $-7 \cdot 11^3$ and minimal conductor 35^2 (ascribed to Vélu in the "remarks on isogenies" preceding the tables of [B-K]). There is then a rational 37-element subgroup $G \subset E(\overline{\mathbf{Q}})$, and the quotient curve $E_1 = E/G$ has j-invariant $j' = -7 \cdot 137^3\, 2083^3$. But knowing j' does not fully determine the curve $E_1/\mathbf{Q}$, let alone the coordinates of the points of G (i.e. the degree-18 factor of the division polynomial ψ_{37} of E). The first question can be answered by local considerations: E_1 must have the same conductor 35^2 as E, which turns out to be possible only for 4 quadratic twists, and the correct one

$$Y^2 + XY + Y = X^3 + X^2 - 208083X - 36621194 \tag{25}$$

can be deduced by counting points modulo small primes. Both questions can be answered by transcendental methods such as computing to high precision generators of the period lattice of E, and the Weierstrass $\wp$-function at points of G to

[15] The same could be said for the exotic isogenies of degrees 17 and 11, though the 11-isogeny happens to involve curves of conductor as low as 121 so it can already be found in Tingley's "Antwerp" tables [B-K], while the other two requires conductors beyond even the range of Cremona's tables [Cre].

obtain its X-coordinates as high-precision real numbers, from which their symmetric functions may be recognized as integers, while the integer coefficients of a Weierstrass equation for E_1 may be computed from its period lattice generated by G and the periods of E. This is Cremona's approach in [Cre, pp.79–80]. But neither of these methods would apply if j, j' were solutions of Φ_{37} over a finite field; even in characteristic zero they are not geometrically satisfactory since they yield only specific isogenies, not a generic l-isogeny parametrized by $\mathrm{X}_0(l)$.

Preview: $\mathrm{X}_0(l)$ and $\mathrm{X}_0^+(l)$ as smooth curves. Now the singular model $\Phi_l(j, j') = 0$ of $\mathrm{X}_0(l)$ is not suitable for such geometrical investigations, so we should start by resolving those singularities and adding the two cusps $(j : j' : 1) = (0 : 1 : 0)$ and $(1 : 0 : 0)$ to obtain a smooth projective model for $\mathrm{X}_0(l)$. In fact we do not actually compute this model starting from Φ_l since it is more efficient to derive such a model directly from modular forms and functions on $\mathrm{X}_0(l)$, and write j, j' in terms of the coordinates of the model. Resolving the singularities also considerably simplifies the formulas for finding j'. For instance, when $l = 3$, the curve $\mathrm{X}_0(l)$ has genus 0 and is parametrized by the "Hauptmodul"

$$h = (\eta_1/\eta_3)^{12} = q^{-1} - 12 + 54q - 76q^2 - 243q^3 \cdots, \tag{26}$$

in terms of which

$$j = \frac{(h + 3^3)(h + 3^5)^3}{h^3}, \qquad j' = \frac{(h_1 + 3^3)(h_1 + 3^5)^3}{h_1^3} \tag{27}$$

where $hh_1 = 3^6$. Thus to find j' we solve not the imposing equation $\Phi_3(j, j') = 0$ but the simpler $(h + 3^3)(h + 3^5)^3 = h^3 j$, and from any solution compute $h_1 = 3^6/h$ and recover j' from (27). [The coefficients become even smaller if we use $H := h/27$, $H_1 := h_1/27$, when $j = 27(H+1)(H+9)^3/H^3$ and j' is the same with h replaced by $H_1 = 1/H$.] We shall later say much more about how we actually find such nice models of $\mathrm{X}_0(l)$ and exhibit j, j' as rational functions on them. For the time being we collect a few familiar facts about the Atkin-Lehner involution $w : j \leftrightarrow j'$ as an automorphism of $\mathrm{X}_0(l)$: over $\mathbf{C}$, if $\mathrm{X}_0(l)$ is represented as the quotient of the extended upper half-plane $\{\tau \in \mathbf{C} : \operatorname{Im} \tau > 0\} \cup \mathbf{P}^1(\mathbf{Q})$ by $\Gamma_0(l)$ then w is $\tau \leftrightarrow -1/l\tau$, which in particular exchanges the two cusps $\tau = i\infty$ (corresponding to $q = 0$, $(j : j' : 1) = (0 : 1 : 0)$) and $\tau = 0$ (with $(j : j' : 1) = (1 : 0 : 0)$). For instance on $\mathrm{X}_0(3)$ we have $w(h) = h_1 = 3^6/h$, with $h = \infty, 0$ at the infinite and zero cusp. The quotient curve

$$\mathrm{X}_0^+(l) := \mathrm{X}_0(l)/\{1, w\} \tag{28}$$

has genus at most half that of $\mathrm{X}_0(l)$ (because w has at least one fixed point $\tau = -i/\sqrt{l}$), and only one cusp. A rational function, modular function,[16] or modular form on $\mathrm{X}_0^+(l)$ is the same as such a function or form on $\mathrm{X}_0(l)$ that is invariant under w; in odd or zero characteristic, if v is an *anti*-invariant function

[16] i.e. rational function with no poles except possibly at cusp(s).

(i.e. $v \circ w = -v$) then the function field of $\mathrm{X}_0(l)$ is obtained from that of $\mathrm{X}_0^+(l)$ by adjoining a square root of the w-invariant function v^2. For instance the curve $\mathrm{X}_0^+(3)$ has genus 0, with Hauptmodul

$$u = \frac{(h+27)^2}{h} = q^{-1} + 42 + 783q + 8672q^2 + 65367q^3 + \cdots, \tag{29}$$

and the function field of $\mathrm{X}_0(3)$ is obtained from the function field $\mathbf{C}(u)$ of $\mathrm{X}_0^+(3)$ by adjoining $v = \sqrt{u^2 - 108u}$.

Quadratic twists. The next difficulty is that knowing $\mathrm{X}_0(l)$ as an algebraic curve and j, j' as rational functions on it does not completely determine a generic pair E, E_1 of l-isogenous curves: E, E_1 are known only up to quadratic twist. All we know is that, for some nonzero λ, the curve E has Weierstrass form

$$Y^2 = X^3 + a_4 X + a_6 \tag{30}$$

where, in terms of the coordinate q_z on $\mathbf{G}_m/q^{\mathbf{Z}}$, the functions X, Y are

$$\begin{aligned} X &= \lambda\left[\frac{1}{12} - 2\sum_{n=1}^{\infty}\frac{q^n}{(1-q^n)^2} + \sum_{n=-\infty}^{\infty}\frac{q^n q_z}{(1-q^n q_z)^2}\right], \\ Y &= \frac{1}{2}\lambda^{1/2} q_z \frac{d}{dq_z} X = \frac{1}{2}\lambda^{3/2}\sum_{n=-\infty}^{\infty}\frac{(q^n q_z)^2 + q^n q_z}{(1-q^n q_z)^3} \end{aligned} \tag{31}$$

invariant under $q_z \mapsto q q_z$, and the coefficients a_4, a_6 are proportional to the well-known Eisenstein series $\mathsf{E}_4, \mathsf{E}_6$:

$$\begin{aligned} a_4 &= -\frac{\lambda^2}{48}\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n) q^n\right) = -\frac{\lambda^2}{48}\mathsf{E}_4(q), \\ a_6 &= \frac{\lambda^3}{864}\left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n) q^n\right) = \frac{\lambda^3}{864}\mathsf{E}_6(q) \end{aligned} \tag{32}$$

(with $\sigma_k(n) = \sum_{d|n} d^k$ as usual). We can obtain these formulas in two ways: either start with the familiar double sums for the Weierstrass function $\wp(z)$ and its derivative for the lattice $\mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau)$ and express them in terms of $q = e^{2\pi i \tau}$ and $q_z = e^{2\pi i z}$, absorbing powers of 2π into λ; or work directly on $\mathbf{G}_m/q^{\mathbf{Z}}$, mimicking the Weierstrass approach by exhibiting the functions X, Y of degree 2 and 3 with poles only at the origin $q_z = 1$, and matching singular parts to find the cubic equation they satisfy. Either way, we see that to specify an elliptic curve up to isomorphism, we need not only q but also λ mod squares. Moreover, to give a generic l-isogeny over $\mathrm{X}_0(l)$ we must choose λ so the a_4, a_6 of (32) are rational functions on $\mathrm{X}_0(l)$; since $\mathsf{E}_4, \mathsf{E}_6$ are modular forms of weights $4, 6$ this means λ must be a nonzero meromorphic modular form of weight -2. Once we choose such a form λ_0, a given l-isogeny $E \to E_1$ may not be the specialization of our generic l-isogeny over $\mathrm{X}_0(l)$ at the point $(j(E), j(E_1))$. It will, however, be isomorphic to a quadratic twist of that isogeny. Thus we will be able to handle any l-isogeny once we explicitly describe the generic isogeny specified by some meromorphic modular form λ_0.

The isogenous curve. Once the Weierstrass model (30) of an elliptic curve E and a finite subgroup $G \subset E$ are given, the isogenous quotient curve $E_1 = E/G$ is determined up to isomorphism, but there are many different Weierstrass equations $Y_1^2 = X_1^3 + a_4' X_1 + a_6'$ giving the same E_1, since the coordinates X_1, Y_1 could be multiplied by λ^2, λ^3 for any nonzero λ. This isomorphism multiplies the invariant differential $\omega_1 = dX_1/2Y_1$ by $1/\lambda$. Thus the choice of Weierstrass equation is equivalent to the choice of a a nonzero invariant differential on E_1. Once the choice is made, we describe E_1 more precisely as an ordered pair (E_1, ω_1), and likewise $E = (E, dX/2Y) = (E, \omega)$. We say that an isogeny $\alpha : (E, \omega) \to (E_1, \omega_1)$ between such elliptic curves is *normalized* if $\omega = \alpha^* \omega_1$. We thus associate, to each finite subgroup G of a curve (E, ω) (equivalently, an elliptic curve with a given Weierstrass equation), a specific Weierstrass equation for the quotient curve E_1 by requiring that the quotient map $(E, \omega) \to (E_1, \omega_1)$ be a normalized isogeny. We shall next do this for the l-isogenies parametrized by $\mathrm{X}_0(l)$. Note that the composite of two isogenies is normalized, but if we follow α by the normalized form of the dual isogeny $\bar{\alpha} : E_1 \to E$ the resulting Weierstrass model of E is not the one we started with but the isomorphic one with a_4, a_6 replaced by $l^4 a_4, l^6 a_6$. This is because $\bar{\alpha}\alpha = l$ and the normalized form of the multiplication-by-l isogeny is $(E, \omega) \to (E, \omega/l)$.

Over $\mathbf{C}$, the point of $\mathrm{X}_0(l)$ represented by the $\Gamma_0(l)$ orbit of τ parametrizes the isogeny $\mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau) \to \mathbf{C}/(\mathbf{Z} + \mathbf{Z}l\tau)$ taking z to lz. The corresponding isogeny $\alpha : E \to E_1$ between Tate curves is

$$\mathbf{G}_m/q^{\mathbf{Z}} \to \mathbf{G}_m/q^{l\mathbf{Z}}, \qquad q_z \mapsto q_z^l. \tag{33}$$

Replacing q by q^l in (31,32) yields coordinates and a Weierstrass equation for E_1. But these are not normalized, because they yield an invariant differential on E_1 that pulls back to $\lambda^{-1/2} d(q_z^l)/q_z^l = \lambda^{-1/2} l \, dq_z/q_z = l\omega_E$. Thus to normalize the isogeny we multiply the coordinates on E_1 by l^2, l^3, and the coefficients of its Weierstrass equation by l^4, l^6, to obtain

$$\begin{aligned} X_1 &= \lambda l^2 \left[\frac{1}{12} - 2 \sum_{n=1}^{\infty} \frac{q^{ln}}{(1-q^{ln})^2} + \sum_{n=-\infty}^{\infty} \frac{q^{ln} q_z}{(1-q^{ln}q_z)^2} \right], \\ Y &= \frac{1}{2} \lambda^{3/2} l^3 \sum_{n=-\infty}^{\infty} \frac{(q^{ln}q_z)^2 + q^{ln}q_z}{(1-q^{ln}q_z)^3}; \end{aligned} \tag{34}$$

$$a_4 = -\frac{\lambda^2}{48} l^2 \mathsf{E}_4(q^l), \qquad a_6 = \frac{\lambda^3}{864} l^3 \mathsf{E}_6(q^l). \tag{35}$$

Thus we can find a Weierstrass equation of a curve l-isogenous to a given elliptic curve E once we know, in addition to j, j', four further modular functions on $\mathrm{X}_0(l)$, namely

$$A_4 := \lambda_0^2 \mathsf{E}_4(q) \qquad A_6 := \lambda_0^3 \mathsf{E}_6(q), \tag{36}$$

$$A'_4 := \lambda_0^2 \mathsf{E}_4(q^l), \quad \text{and} \quad A'_6 := \lambda_0^3 \mathsf{E}_6(q^l), \tag{37}$$

for some nonzero meromorphic weight-2 modular form λ_0. To do this, we find a point P on $\mathrm{X}_0(l)$ at which j is the j-invariant of E, and compute A_4, A_6, A'_4, A'_6 at this point. Then E is a quadratic twist of the curve $y^2 = x^3 - (A_4(P)/48)x + (A_6(P)/864)$ which is the specialization to P of one of the curves involved in our generic l-isogeny; that is,

$$-48a_4(E) = \gamma^2 A_4(P), \quad 864a_6(E) = \gamma^3 A_6(P), \tag{38}$$

for some nonzero γ, namely $\gamma = -18a_6(E)A_4(P)/a_4(E)A_6(P)$. The isogenous curve is then

$$E_1 : y'^2 = x'^3 - \frac{\gamma^2}{48} A'_4(P)x' + \frac{\gamma^3}{864} A'_6(P). \tag{39}$$

(We have suppressed the factors l^4, l^6 that normalize the isogeny but do not change the isomorphism class of E_1; without them the dual isogeny $E_1 \to E$ is normalized instead.)

Of course once we know the functions (36,37), the formulas for j, j' are redundant since these are $(12A_4)^3/(A_4^3 - A_6^2)$ and $(12A'_4)^3/(A_4'^3 - f_6'^2)$. Moreover, $\mathsf{E}_4(q^l), \mathsf{E}_6(q^l)$ are respectively $l^2 w^* \mathsf{E}_4(q)$ and $-l^3 w^* \mathsf{E}_6$, so if λ_0 is invariant or anti-invariant under w then the formulas for A_4 and A_6 determine A'_4 and A'_6 via the involution w. Usually we will take λ_0 anti-invariant (we shall see later why this is more convenient than an invariant form), and obtain the formulas for A_4, A'_4, A_6, A'_6 on $\mathrm{X}_0(l)$ by writing

$$A_4 + l^2 A'_4, \quad \frac{1}{v}(A_4 - l^2 A'_4), \quad A_6 + l^3 A'_6, \quad \frac{1}{v}(A_6 - l^3 A'_6) \tag{40}$$

(where v is our anti-invariant modular function) as rational functions on $\mathrm{X}_0^+(l)$; once $\mathrm{X}_0(l)$ has positive genus it is easier to recognize rational functions on the lower-genus curve $\mathrm{X}_0^+(l)$.

We illustrate this by verifying algebraically one of the "exotic" isogenies described in [B-K]: a non-CM isogeny of degree $l = 11$. We begin by finding equations for $\mathrm{X}_0(11)$, $\mathrm{X}_0^+(11)$. The curve $\mathrm{X}_0(11)$ has genus 1, with holomorphic differential (= weight-2 cusp form)

$$\omega = (\eta\eta_{11})^2 = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 \cdots. \tag{41}$$

Since ω is anti-invariant, $\mathrm{X}_0^+(11)$ has no holomorphic differentials, and is thus a rational curve. Thus it has a Hauptmodul, i.e. a degree-1 rational function u taking the cusp to ∞, with q-expansion $q^{-1} + O(1)$. Then $\varepsilon = u\omega$ is another anti-invariant weight-2 modular form on $\mathrm{X}_0(11)$ (but not a cusp form); since ω has no zeros in the upper half-plane, any modular form ε of weight 2 with $w^*\varepsilon = -\varepsilon$ and $\varepsilon(i\infty) = 1$ will yield a suitable $u = \varepsilon/\omega$. We obtain such ε from the Eisenstein series of weight 2, an anti-invariant form on $\mathrm{X}_0(l)$ defined for any l by

$$\mathsf{E}_2^{(l)}(q) = q\frac{d}{dq}\log\frac{\eta(q^l)}{\eta(q)} = \frac{l-1}{24} + \sum_{n=1}^{\infty}\sigma_1(n)(q^n - lq^{ln}). \tag{42}$$

Taking[17]

$$\varepsilon = \frac{3}{5}\big(4\mathsf{E}_2^{(11)} + \omega\big) = 1 + 3q + 6q^2 + 9q^3 + 18q^4 + 15q^5 + \cdots \tag{43}$$

we get our Hauptmodul

$$u = \frac{\varepsilon}{\omega} = q^{-1} + 5 + 17q + 46q^2 + 116q^3 + 252q^4 + 533q^5 + \cdots. \tag{44}$$

An anti-invariant function is then

$$v = \frac{1}{\omega}q\frac{du}{dq} = -q^{-2} - 2q^{-1} + 12 + 116q + 597q^2 + 2298q^3 + \cdots. \tag{45}$$

Since u, v have poles only at the cusps, and $\mathrm{X}_0^+(11)$ has only one cusp, we can recognize v^2 as a polynomial in u by comparing q-expansions there; we find

$$v^2 = u^4 - 16u^3 + 2u^2 + 12u - 7 = (u-1)(u^3 - 17u^2 + 19u - 7). \tag{46}$$

We take $\lambda_0 = 1/\omega$; since this, too, has poles only at the cusps, our functions (40) must be polynomials in u and so again readily recognizable from their q-expansions. We find:

$$\begin{gathered} A_4 = 61u^2 - 246u + 45 + 60v, \qquad A_4' = (61u^2 - 246u + 45 - 60v)/11^2, \\ A_6 = -665u^3 + 5733u^2 - 1323u - 945 - (666u - 918)v, \\ A_6' = \big[665u^3 - 5733u^2 + 1323u + 945 - (666u + 918)v\big]/11^3. \end{gathered} \tag{47}$$

We thus find also $j = (12A_4)^3/(A_4^3 - A_6^2)$ as a polynomial in u, v, and use (46) to eliminate v and find the polynomial relation between j and u:

$$j^2 - P(u)j + (u^4 + 228u^3 + 486u^2 - 540u + 225)^3 = 0, \tag{48}$$

where $P(u)$ is the polynomial

$$\begin{aligned} u^{11} - 55u^{10} + 1188u^9 - 12716u^8 + 69630u^7 - 177408u^6 + 133056u^5 \\ +132066u^4 - 187407u^3 + 40095u^2 + 24300u - 6750. \end{aligned} \tag{49}$$

[17] It is of course no accident that $E_1^{(11)} \equiv \omega \bmod 5$ and thus that ε and $u = \varepsilon/\omega$ have integer coefficients. This could have been expected on general principles in several ways; alternatively we could obtain ε directly as an integral modular form with constant coefficient 1 by subtracting ω from the square of the theta series $\sum\sum_{m,n\in\mathbf{Z}} q^{m^2+mn+3n^2}$.

Now let $E/\mathbf{Q}$ be the curve numbered 121F in [B-K] and 121-C1 in [Cre]:

$$Y^2 + XY = X^3 + X^2 - 2X - 7. \tag{50}$$

This is not in reduced Weierstrass form, but we can put it in that form by the affine-linear change of coordinates

$$(x, y) = (4X + \frac{5}{3}, 8Y + 4X), \qquad (X, Y) = \big(\frac{x}{4} - \frac{5}{12}, \frac{y-x}{8} + \frac{5}{24}\big). \tag{51}$$

This yields

$$y^2 = x^3 - \frac{121}{3}x - \frac{10406}{27} \qquad (j = -121). \tag{52}$$

Substituting $j = -121$ into (48) we obtain a polynomial in u of degree 12 whose only rational root is $u = -2$; taking $u = -2$ in our formula for j as a polynomial in u, v yields $-(1124040v + 12364561)$, which equals -121 at $v = -11$. We thus find that there is a unique 11-isogeny over $\mathbf{Q}$ from E to some other curve E_1, parametrized by the point $(u, v) = (-2, -11)$ on $\mathrm{X}_0(11)$. Moreover the dual isogeny $E_1 \to E$ is parametrized by the image $(2, -11)$ of that point under w, so in particular $j(E_1)$ is the value at $(-2, 11)$ of $j(u, v)$, i.e. $-(1124040 \cdot 11 + 12364561) = -11 \cdot 131^3$. At $(u, v) = (-2, -11)$ we have $A_4 = 121$, $A_6 = 5203$; thus to solve (38) with $a_4(E) = -121/3$ and $a_6 = -10406/27$ we take $\gamma = -4$. Using this γ, and restoring the normalizing factors l^4 and l^6, we find

$$\begin{aligned} a_4(E_1) &= -\frac{(11\gamma)^2}{48} A_4(-2, 11) = -\frac{174361}{3}, \\ a_6(E_1) &= -\frac{(11\gamma)^3}{864} A_6(-2, 11) = \frac{145619386}{27}. \end{aligned} \tag{53}$$

We recover the Néron model

$$Y^2 + XY = X^3 + X^2 - 3632X + 82757 \tag{54}$$

of the isogenous curve E_1 by applying the change of variable (51) in reverse, and thus confirm that E_1 is indeed the curve numbered 121G in [B-K] and 121-C2 in [Cre], with the isogeny $E \to E_1$ normalized.

The kernel of the isogeny. But finding the isogenous curve E_1 is still not the same as finding the isogeny $\alpha : E \to E_1$. For the application to Schoof it is enough to find $G = \ker \alpha$, but that is equivalent to finding α which is just the quotient map $E \to E/G \cong E_1$. As observed in [Vél], this can be done explicitly by finding functions x', y' of degrees 2, 3 on E/G with double and triple poles at the origin and comparing singular parts to find that they satisfy a Weierstrass equation with coefficients

$$a_4' = a_4 - 5 \sum (3x^2(g) + a_4), \quad a_6' = a_6 - 7 \sum (5x^3(g) + 3a_4 x(g) + 2a_6). \tag{55}$$

Specifically, if $\alpha : E \to E_1$ is a normalized isogeny between elliptic curves $E : y^2 = x^3 + a_4 x + a_6$ and $E_1 : y'^2 = x'^3 + a_4 x' + a_6$ then

$$x'(\alpha(P)) = x(P) + \sum_{\substack{g \in G \\ g \neq 0}} [x(P+g) - x(g)], \quad y'(\alpha(P)) = \sum_{g \in G} y(P+g), \tag{56}$$

where $G = \ker \alpha$ as before. Indeed these are functions of the desired degrees and poles which transform correctly under $P \leftrightarrow -P$. Moreover, near $P = 0$ we have $x' = x + O(1/x)$ (this is why we subtracted $\sum_{g \neq 0} x(g)$ from $\sum_{g \in G} x(P+g)$) and $y' = y(1 + O(1/x^2))$, so x', y' satisfy a reduced Weierstrass equation. It then remains only to check that the isogeny is normalized, i.e. that $dx'/y' = dx/y$; but this readily follows from the fact that dx/y is translation invariant:

$$\frac{d}{dx(P)} x(P+g) = \frac{1}{y(P)} y(P+g), \tag{57}$$

which summed over $g \in G$ yields $dx'/dx = y'/y$ as desired. Now $x(\alpha(P))$ is actually a rational function of $x(P)$, and $y(\alpha(P))$ is y times such a function; to find these functions we average the g and $-g$ terms in (56):

$$\begin{aligned} x'(\alpha(P)) &= x + \sum_{\substack{g \in G \\ g \neq 0}} \left[\frac{x(P+g) + X(P-g)}{2} - X(g) \right] \\ &= x + \sum_{\substack{g \in G \\ g \neq 0}} \left[\frac{3x^2(g) + a_4}{x - x(g)} + 2 \frac{x^3(g) + a_4 x(g) + a_6}{(x - x(g))^2} \right], \end{aligned} \tag{58}$$

$$\begin{aligned} y'(\alpha(P)) &= y + \sum_{\substack{g \in G \\ g \neq 0}} \frac{y(P+g) + y(P-g)}{2} \\ &= y - y \sum_{\substack{g \in G \\ g \neq 0}} \left[\frac{3x^2(g) + a_4}{(x - x(g))^2} + 4 \frac{x^3(g) + a_4 x(g) + a_6}{(x - x(g))^3} \right]. \end{aligned} \tag{59}$$

Expanding in inverse powers of x yields (with all sums over nonzero $g \in G$):

$$x'(\alpha(P)) = x + \frac{\sum (3x^2(g) + a_4)}{x} + \frac{\sum (5x^3(g) + 3a_4 x(g) + 2a_6)}{x^2} + \cdots, \tag{60}$$

$$y'(\alpha(P)) = y \left[1 - \frac{\sum (3x^2(g) + a_4)}{x^2} - \frac{\sum (10x^3(g) + 6a_4 x(g) + 4a_6)}{x^3} - \cdots \right], \tag{61}$$

from which the formula (55) for the Weierstrass coefficients of E_1 follows.

We give these formulas in such detail because they almost let us go in reverse, determining G from the known parameters a_4, a_6, a_4', a_6' of the isogeny. We assume for simplicity that l is odd, the case $l = 2$ being different but easy and well-known (see e.g. [Sil, p.74, Ex. 4.5]). Then G consists of $\mathbf{0}$ and $d := (l-1)/2$ pairs of nonzero points with the same x-coordinates, and we want the monic polynomial of degree d whose roots are these x-coordinates, or equivalently the elementary symmetric functions s_i of these roots. As before, it is enough to find their first d power sums p_i and use the Newton identities (18) to recover the elementary symmetric functions. Now for the isogeny (33) between Tate curves the kernel is $\boldsymbol{\mu}_l = \{\zeta : \zeta^l = 1\}$, so the x-coordinates in question are

$$x(\zeta) = \lambda_0 \left[\frac{1}{12} - 2 \sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} + \sum_{n=-\infty}^{\infty} \frac{q^n \zeta}{(1-q^n\zeta)^2} \right], \tag{62}$$

with ζ a nontrivial l-th root of unity (and $x(\zeta) = x(\zeta^{-1})$). Thus we could complete the description of a generic l-isogeny by working out the q-expansions of the power sums $p_1, p_2, \ldots, p_d$ in these $x(\zeta)$ and writing them or the resulting elementary symmetric functions s_i as rational functions on $\mathrm{X}_0(l)$. But in fact only the first power sum is needed $p_1 = s_1$. The formula (55) expresses p_2 in terms of a_4, a_4', and a linear combination of p_1, p_3 in terms of a_6, a_6'. (Warning: the sums $\sum_g x(g)^i$ occurring in (55) are not p_i but $2p_i$ because each root is counted twice, as both $x(g)$ and $x(-g)$.) Expanding both sides of the Weierstrass equation for E_1 in inverse powers of x and comparing x^{-r} coefficients then yields the p_{r+3} power sum in terms of the previous ones.[18] One nice form of this recursion is obtained by differentiating that Weierstrass equation

$$y'(\alpha(P))^2 = x'(\alpha(P))^3 + a_4' x'(\alpha(P)) + a_6' \tag{63}$$

with respect to x. We have seen already that $y' = y\,dx'/dx$. Thus applying $y\,d/dx$ to both sides of (63) and dividing by y' yields

$$3x'^2 + a_4' = 2y\frac{dy'}{dx} = 2y\frac{d}{dx}\left(y\frac{dx'}{dx}\right) = 2y\frac{dy}{dx}\frac{dx'}{dx} + 2y^2\frac{d^2x'}{dx^2}; \tag{64}$$

since $2y\,dy/dx = d(y^2)/dx = 3x^2 + a_4$ we finally obtain

$$3x'^2 + a_4' = (3x^2 + a_4)\frac{dx'}{dx} + 2(x^3 + a_4x + a_6)\frac{d^2x'}{dx^2}. \tag{65}$$

Write the expansion (60) as $x'(P) = x + \sum_{n=1}^{\infty} c_n/x^n$ where

$$c_n = (4n+2)p_{n+1} + (4n-2)a_4p_{n-1} + (4n-4)a_6p_{n-2} \tag{66}$$

(of course $p_0 = d$). Then for $r > 0$ the LHS and RHS of (65) have x^{-r} coefficients

$$6c_{r+1} + 3\sum_{n=1}^{r-1} c_n c_{r-n}, \tag{67}$$

$$(2r+1)(r+1)c_{r+1} + (2r-1)(r-1)a_4c_{r-1} + (2r-2)(r-2)a_6c_{r-2} \tag{68}$$

[18] This is where we simplify the recursion in [El2], by expanding in powers of $1/x$ rather than $z = \int_0^P dx/2y$. Schoof [Sc2, §8] finds an alternative simplification, using expansions in powers of z but managing the algebra more cleverly than we did in [El2].

respectively (with $c_n = 0$ for $n \leqslant 0$). Equating these we find

$$(r-1)(2r+5)c_{r+1} = 3\sum_{n=1}^{r-1} c_n c_{r-n} - (2r-1)(r-1)a_4 c_{r-1} - (2r-2)(r-2)a_6 c_{r-2}. \tag{69}$$

This holds identically for $r = 1$, and for $r \geqslant 2$ gives c_{r+1} as a quadratic polynomial in $c_1, c_2, \ldots, c_{r-1}$ provided $r-1$ and $2r+5$ are invertible. We already know c_1 and c_2 from (55,66) and can thus recursively compute $c_3, c_4, \ldots, c_{d-1}$ in $O(l^2)$ arithmetic operations in any field of characteristic either zero or $> 2(d-2)+5 = l$.[19]

By (66) we can thus also inductively calculate $p_2, \ldots, p_d$ in such a field once we know p_1. We cannot express p_1 directly in terms of a_4, a_6, a_4', a_6'; but we can write p_1 for our generic l-isogeny as a modular function on $\mathrm{X}_0(l)$. We can then evaluate that first power sum at the point parametrizing a given normalized isogeny $\alpha : E \to E_1$ and multiply by γ to obtain p_1 for α. We reproduce the computation of [El2, Prop. 1]. By (62) the generic sum is

$$\frac{1}{2}\lambda_0 \sum_{\substack{\zeta^l=1\\ \zeta\neq 1}} \left[\frac{1}{12} - 2\sum_{n=1}^{\infty}\frac{q^n}{(1-q^n)^2} + \sum_{n=-\infty}^{\infty}\frac{q^n\zeta}{(1-q^n\zeta)^2}\right], \tag{70}$$

the initial factor $1/2$ accounting for the double occurrence of each summand in $\sum_\zeta$. By the identity

$$\sum_{\zeta^l=1}\frac{\zeta t}{(1-\zeta t)^2} = \frac{l^2 t^l}{(1-t^l)^2} \tag{71}$$

(perhaps most easily proved by comparing Taylor expansions about $t = 0$), the sum (70) simplifies to

$$\lambda_0\left[\frac{l-1}{24} - l\sum_{n=1}^{\infty}\frac{q^n}{(1-q^n)^2} + l^2\sum_{n=1}^{\infty}\frac{q^{ln}}{(1-q^{ln})^2} + \frac{1-l^2}{24}\right], \tag{72}$$

the last term arising as

$$\frac{1}{2}\sum_{\substack{\zeta^l=1\\ \zeta\neq 1}}\frac{\zeta}{(1-\zeta)^2} = \frac{1}{2}\lim_{t\to 1}\left(\frac{l^2t^l}{(1-t^l)^2} - \frac{t}{(1-t)^2}\right). \tag{73}$$

It remains only to combine the terms $(l-1)/24$, $(1-l^2)/24$ and expand the sums in Taylor series to recognize (72) as the multiple

$$-l\lambda_0 \mathsf{E}_2^{(l)}(q) \tag{74}$$

[19] This is where our approach fails most critically for fields of small characteristic, though even the Newton recursion breaks down once the characteristic falls below $l/2$.

of the Eisenstein series (42)! Thus, having already identified A_4, A_6, A'_4, A'_6 as rational functions on $\mathrm{X}_0(l)$ we need only write the modular function $\lambda_0 \mathsf{E}_2^{(l)}$ as well in terms of our coordinates on $\mathrm{X}_0(l)$ (or $\mathrm{X}_0^+(l)$ if λ_0 is anti-invariant) to complete our description of a generic l-isogeny over $\mathrm{X}_0(l)$.

We can now conclude the computation of the 11-isogeny from the curve (50) to (54). From the known a_4, a_6, a'_4, a'_6 we initialize our recursion (69) with $c_1 = 11616$, $c_2 = -775208$ and compute

$$c_3 = \frac{135399968}{3}, \quad c_4 = -\frac{22089105632}{9}, \quad c_5 = \frac{3434826856736}{27}. \tag{75}$$

By (43,44) we already know that on $\mathrm{X}_0(11)$

$$\lambda_0 \mathsf{E}_2^{(11)} = \frac{\mathsf{E}_2^{(11)}}{\omega} = \frac{5}{12}u - \frac{1}{4} \tag{76}$$

Thus $p_1 = -143/3$ by (74), since $u = -2$ and $\gamma = -4$ for our isogeny. Also $p_0 = (l-1)/2 = 5$, so from (66) and the known c_n we obtain

$$p_2 = \frac{18029}{9}, \quad p_3 = -\frac{2090759}{27}, \quad p_4 = \frac{264952853}{81}, \quad p_5 = -\frac{33598876223}{243}. \tag{77}$$

By (18) we then find the polynomial whose roots are the x-coordinates of $\ker \alpha$:

$$(3x)^5 + 143(3x)^4 + 1210(3x)^3 - 104786(3x)^2 - 693451(3x) + 6091987. \tag{78}$$

Thus at these torsion points $X = (x/4) - (5/12)$ is a root of the quintic

$$X^5 + 14X^4 + 30X^3 - 37X^2 - 76X + 1 \tag{79}$$

of discriminant 11^{12}. Note that this quintic has cyclic Galois group, so its roots necessarily lie in the cyclotomic extension of $\mathbf{Q}$ generated by $\xi = 2\cos(2\pi/11)$; indeed, these roots are the conjugates of $-\xi^4 + 2\xi^2 + 2\xi - 1$.

In concluding this section, we remark that while we are most interested in normalized isogenies of odd prime degree, our formulas work in greater generality: the c_n recursion holds for any normalized isogeny, and the formulas for p_1 as well as earlier parts of the recipe involving A_4, A_6, A'_4, A'_6 hold provided the normalized isogeny has cyclic kernel (so is parametrized by $X_0(N)$ for some N), with p_1 modified slightly in the case of even degree to handle the 2-torsion points. In practice it may help to carry out the following "sanity check" on these convoluted computations: extend the c_n recursion a few further terms than necessary to compute a few power sums past p_d, and confirm that the symmetric functions $s_{d+1}, s_{d+2}, \ldots$ obtained by Newton's identities vanish as they must.

4. Equations and coordinates for modular curves

We have so far largely ignored the question of how to find the equations for $\mathrm{X}_0(l)$ and the formulas for j, $\mathsf{E}_2^{(l)}$, etc. that we use in the isogeny computation. This problem, together the intimately related problems of finding modular forms of low weight and the ring of modular functions on these curves, are of considerable interest even if we put aside the specific application to computing traces of elliptic curves: they are intrinsically compelling, and as we show in the Appendix explicit equations, functions and modular forms on $\mathrm{X}_0(l)$ (and also on modular curves of composite level) can be put to a variety of good uses. Moreover the computational methods and results suggest new conjectures and open problems that may deepen our understanding of these modular curves.

The rational case. When $\mathrm{X}_0(l)$ has genus 0 these equations are well-known. There are five such l, namely the primes $l = 2, 3, 5, 7, 13$ for which $l - 1|12$. In each case, a Hauptmodul for $\mathrm{X}_0(l)$ is $h = (\eta(q)/\eta(q^l))^{24/(l-1)}$, with $hw(h) = l^{12/(l-1)}$. (We have seen this already for $l = 3$ (26); that this and other η products and quotients appearing herein are in fact modular forms and functions on the appropriate curves can be verified by Ligozat's test [Lig].) Since h has a simple pole at the cusp $q = 0$ and a simple zero at the other cusp $\tau = 0$ of $\mathrm{X}_0(l)$ we can recognize other modular functions on $\mathrm{X}_0(l)$ as rational functions of h by manipulating q-expansions. For instance $j(q)$ has poles of orders $1, l$ at the cusps and no other poles, so $h^l j(q)$ is a polynomial of degree $l + 1$ in h, which we recover by comparing its q-expansion with that of h, finding:

$$\begin{aligned}
l = 2: &\quad j = h^{-2}(h + 256)^3, \\
l = 3: &\quad j = h^{-3}(h + 27)(h + 243)^3, \\
l = 5: &\quad j = h^{-5}(h^2 + 250h + 5^5)^3, \\
l = 7: &\quad j = h^{-7}(h^2 + 13h + 49)(h^2 + 245h + 7^4)^3, \\
l = 13: &\quad j = h^{-13}(h^2 + 5h + 13)(h^4 + 247h^3 + 3380h^2 + 15379h + 13^4)^3.
\end{aligned} \tag{80}$$

[As in the case of $l = 3$ we can reduce the coefficients by multiplying h by a power of l.]

We note that these formulas can in fact be obtained from the ramification behavior of the cover $\mathrm{X}_0(l)/\mathrm{X}(1)$ without invoking q-expansions (and indeed we once did obtain them in this way). For instance, for $l = 5$ we must have $j = P(h)/h^5$ where P is a monic polynomial of degree 6 such that $j = 0$ and $j = 12^3$ have respectively two triple and two double roots (the two simple roots of $j = 12^3$ corresponding to the self-isogenies $2 \pm i$ of a curve with that j-invariant). Thus

$$\begin{aligned}
P(h) &= \alpha(1 + Ah + A'h^2)^3, \\
P(h) - 12^3 h^5 &= \alpha(1 + Bh + B'h^2)(1 + Ch + C'h^2)^2
\end{aligned} \tag{81}$$

for some $\alpha, A, A', B, B', C, C'$. Equating coefficients, we find first (from the h, h^2 terms)

$$B = 3A - 2C, \qquad B' = 3(A - C)^2 + 3A' - 2C', \tag{82}$$

then (from h^3, h^4)

$$A' = -\frac{20C^2 - 40AC + 11A^2}{36}, \quad C' = -\frac{4C^2 + 10AC - 5A^2}{36}, \tag{83}$$

The condition $A'^3 = \alpha^{-1}B'C'^2$ then becomes $(C-A)^5(5C-2A) = 0$; but we cannot have $C = A$ because under (82,83) the h^5 coefficient of $(1+Ah+A'h^2)^3 - (1+Bh+B'h^2)(1+Ch+C'h^2)^2$ is $-2(C-A)^5/9$. Thus $A = 5C/2$, and the final condition $-2(C-A)^5/9 = 12^3/\alpha$ yields $C = 4/125$, so we have found our solution

$$(A, A', B, B', C, C') = \left(\frac{2}{5^2}, \frac{1}{5^5}, \frac{22}{5^3}, \frac{1}{5^3}, \frac{4}{5^3}, -\frac{1}{5^6}\right) \tag{84}$$

of (81), which is equivalent to the $l = 5$ formula of (80). That w_5 takes h to $5^3/h$ can then be deduced from the fact that this involution switches the points $h = 0, \infty$ where $j = \infty$, as well as the simple roots $h = -11 \pm 2i$ of $j = 12^3$.

We chose this case $l = 5$ to illustrate the method because the identity

$$(t^2 + 10t + 5)^3 - (t^2 + 22t + 125)(t^2 + 4t - 1)^2 = 12^3 t \tag{85}$$

obtained from (81,84) by substituting $h = 1/t$ also plays a key role in Hall's conjecture. That conjecture asserts that if x, y are integers with $x^3 \neq y^2$ then

$$|x^3 - y^2| \gg |x|^{1/2-\epsilon} \tag{86}$$

([Hal]; see also [Lan], [Sil, p.268]). The exponent $1/2 - \epsilon$ is what one would expect either on probabilistic grounds or from the ABC conjecture, but the only known proof that $0 < |x^3 - y^2| \ll x^{1/2}$ holds infinitely often is to multiply both sides of (85) by c^3 for some small integer c such that the Fermat-Pell equation $t^2 + 22t + 125 = cu^2$ has infinitely many integer solutions (t, u) (for instance $c = 2$ with $t = 3$, 71, 467, etc.) and set $x = c(t^2 + 10t + 5)$, $y = c^2u(t^2 - 4t + 1)$. This trick has been known for some time, and is attributed in [Sil] to [Dan] (see Exercise 9.10 and p.371), but the connection with $\mathrm{X}_0(5)$ had not apparently been noticed despite the presence of the suggestive factor of 12^3. Noting that Hall's conjecture says in effect that the discriminant of the elliptic curve $Y^2 = X^3 - 3xX + 2y$ is at most $|x|^\epsilon$ times smaller than $\sqrt{|x|}$, this connection means that in every known infinite family of curves with discriminants $\ll \sqrt{|x|}$ each curve admits a rational 5-isogeny!

The general case. Now the methods of [Mat] show that the ramification behavior of the cover $\mathrm{X}_0(l)/\mathrm{X}(1)$ specifies it uniquely for every l: there are three ramification points whose associated monodromy elements are an involution, a 3-cycle and a transvection in $\mathrm{PSL}_2(\mathbf{F}_l)$, and these three conjugacy classes form a rigid triple, i.e. there is up to conjugation in that group a unique way to write a transvection as the product of an involution and a 3-cycle.[20] But once $\mathrm{X}_0(l)$ has positive genus it quickly becomes impractical to actually compute the

[20] This is not quite true, because there are two $\mathrm{PSL}_2(\mathbf{F}_l)$ conjugacy classes of transvections which become conjugate in $\mathrm{PGL}_2(\mathbf{F}_l)$. Each of these is uniquely a product of a 2- and a 3-cycle up to $\mathrm{PSL}_2(\mathbf{F}_l)$ conjugation, so yields a unique cover of $\mathbf{P}^1(\mathbf{C})$, and the two covers are isomorphic because they come from triples equivalent under $\mathrm{Aut}(\mathrm{PSL}_2(\mathbf{F}_l))$. Thus the cover $\mathrm{X}(l)/\mathrm{X}(1)$ is indeed uniquely determined by the ramification data, and so can be defined over $\mathbf{Q}$ (which we know already because it is the Galois closure of $\mathrm{X}_0(l)/X(1)$), but the action of $\mathrm{PSL}_2(\mathbf{F}_l)$ on it cannot — a distinction we shall meet again in the Appendix (see Level 161).

cover from its ramification data. Fortunately we can do it with q-expansions, though it takes more work. Suppose for instance that l is one of the ten primes 11, 17, 19, 23, 29, 31, 41, 47, 59, 71 for which $\mathrm{X}_0(l)$ has genus $g > 0$ but $\mathrm{X}_0^+(l)$ is rational. Then the g-dimensional space of weight-2 cuspforms on $\mathrm{X}_0(l)$ consists entirely of anti-invariant forms. Since we may identify a cusp form f with the holomorphic differential $f\,dq/q$ on that (hyper)elliptic curve, we can obtain equations and coordinates for $\mathrm{X}_0(l)$ from the q-expansions of cusp forms as we did in (44,45,46) for the smallest case $l = 11$. That is, a Hauptmodul for $\mathrm{X}_0^+(l)$ is $u = f_1/f_0$ where f_0 is the unique cuspform of the form $q^g + O(q^{g+1})$ and f_1 is a modular form of weight 2 with leading term q^{g-1} at $q = 0$; if $g = 1$ then f_1 is not a cuspform but we may use $f_1 = \frac{24}{l-1}\mathsf{E}_2^{(l)} + cf_0$ as in (43,44). Then $q\,du/dq = -q^{-1} + O(1)$ is an anti-invariant meromorphic cuspform of weight 2 with no poles other than the cusps, so

$$v := \frac{1}{f_0}\,q\frac{du}{dq} = -q^{-(g+1)} + O(q^{-g}) \tag{87}$$

is an anti-invariant function regular away from the cusps, whence $v^2 = Q(u)$ for some monic polynomial Q of degree $2g+2$ readily obtained from the initial $2g+3$ terms of the q-expansions of u, v. Then Q has distinct roots and $v^2 = Q(u)$ is an equation for the (hyper)elliptic curve $\mathrm{X}_0(l)$. The ring of modular functions is generated by u, v; knowing the q-expansions of a modular function f as well as its image under w (as we do for $j(q)$), we identify the polynomials A, B such that $f = A(u) + vB(u)$ from the q-expansions of $(f + w^*f)/2 = A(u)$, $(f - w^*f)/2v = B(u)$ as we did for $v^2 = Q(u)$. From $j = A(u) + vB(u)$ we get our polynomial relation

$$j^2 = 2A(u) + (A^2 - QB^2)(u) \tag{88}$$

between j and u. Given j, u we readily solve for $v = (j - A(u))/B(u)$, unless $B(u) = 0$ — but then $j = j'$, which can only occur for curves having CM with discriminant $\geqslant -4l$.[21] In the context of computing the trace mod l we may safely assume that j is not one of these CM values, and then find a rational point (u, v) with a given j-invariant by solving the degree-$(l+1)$ polynomial (88) in u. To find the kernel of the resulting l-isogeny we also need the five functions (36,37,74) for some λ_0, and it is convenient to choose the anti-invariant

$$\lambda_0 = f_0^{m-1}/(\eta(q)\eta(q^l))^2 m \tag{89}$$

where $m = 12/\gcd(12, l+1)$ is the smallest choice making (89) a meromorphic form on $\mathrm{X}_0(l)$. The functions (40,74) are then polynomials in u, which we again recognize from their q-expansions as we did for $l = 11$ (47,76).

We have not yet explained how we obtained our cuspforms such as f_0 and f_1. In general we might ask how to compute a basis for the weight-2 cuspforms

[21] Note that it follows that B has on the order of $\sqrt{l}$ factors, corresponding to the various possible discriminants; for instance, in the case $l = 11$, for which we gave u, v in (44,45), we have $(j(q^{11}) - j(q))/v = u(u-1)(u-3)(u-6)(u-15)(u^2-10u+5)(u^2-12u-9)$.

on $\mathrm{X}_0(l)$. There are many ways to do this. If nothing else, one can use the theta functions θ_L of even lattices L of rank 4 with discriminant l^2 and level l (i.e. $lL^* \subset L$). In [Gro, p.143] a family of such L is described and their theta functions are shown to span the weight-2 modular forms (including those not vanishing at the cusps) over $\mathbf{Q}$; the size of this family grows as l^2, but only $g(\mathrm{X}_0(l)) + O(1)$ of them chosen at random will almost certainly suffice to generate all the forms. Moreover by Poisson inversion $w^*\theta_L = -\theta_{l^{1/2}L^*}$ so we can decompose the space of forms into w-eigenspaces. This approach may be awkward but it works for all l; for instance we use it in the Appendix (following [M-SD]) to deal with the recalcitrant case $l = 37$. Two other general approaches, which I have not tried to implement, are the method of [Cre] using an explicit basis for $H_1(\mathrm{X}_0(l), \mathbf{Z})$ and the related method of using trace formulas. But when $l \equiv 3 \bmod 4$ we prefer to generate weight-1 forms from theta functions of even lattices L of rank 2 and discriminant l, and write weight-2 forms as quadratic polynomials in these forms and/or (if $l \equiv 11 \bmod 12$) in the weight-1 form $\eta(q)\eta(q^l)$. Since a rank-2 L is always homothetic to its own dual, this method will only generate anti-invariant forms, but those usually suffice to give equations for $\mathrm{X}_0^+(l)$ which yield the w-invariant cuspforms as the holomorphic differentials. Modifying the theta functions also lets us treat many $l \equiv +1 \bmod 4$; for instance a $\mathrm{X}_0^+(17)$ Hauptmodul is

$$(\theta/\omega)^2 = q^{-1} + 2 + 7q + 14q^2 + 29q^3 + 50q^4 + \cdots \tag{90}$$

where $\omega = \eta(q)\eta(q^{17})$ and θ is a modified theta function

$$\frac{1}{2}\sum_{m,n\in\mathbf{Z}}\sum\left(q^{(m+\frac{1}{2})^2+17n^2} - q^{m^2+17(n+\frac{1}{2})^2}\right) = q^{1/4} + q^{9/4} - q^{17/4} - 2q^{21/4} + q^{25/4}\cdots \tag{91}$$

associated to the quadratic form $(1, 0, 17)$ of discriminant $-4l$.[22] Then θ^2 is a weight-2 cuspform for $\Gamma_0(17)$ with nontrivial character, but ω^2 has the same character so the quotient is a genuine modular function on $\mathrm{X}_0(17)$. The Hecke operators provide yet another way to obtain modular forms once a single one is known; for instance (90) is also $[T_3(\omega^2)/\omega^2] - 2$. We use Hecke operators in this way in the level-161 part of the Appendix. The disadvantage of this approach is that it takes nr coefficients of the q-expansion of a modular form f to get only r coefficients of $T_n f$.

It might seem that we have relied so heavily on the $\mathrm{X}_0^+(l)$ Hauptmodul u that our approach works only for those l for which the genus $g^+(l)$ of $\mathrm{X}_0^+(l)$ is 0. But in fact all that we need is the ring of modular functions on $\mathrm{X}_0^+(l)$; when $g^+(l) > 0$, this is no longer a polynomial ring, but it is still finitely generated and we can find generators and relations. By Riemann-Roch there is a modular function on $\mathrm{X}_0^+(l)$ of degree[23] exactly d for all integers $d \geqslant 0$ with exactly $g^+(l)$

[22] NB The discriminant of a positive-definite quadratic form of rank 2 is *minus* the discriminant of the associated lattice...

[23] Note that the degree of a modular function on $\mathrm{X}_0^+(l)$ is the order of its pole at the cusp, as no other pole is allowed.

exceptions, with all exceptional d's less than $2g^+(l)$. It follows that the ring of modular functions is generated by functions of degree $\leqslant 2g^+(l)+1$. This is because any larger d can be written in at least one way as d_1+d_2 with neither of d_1, d_2 exceptional, so any degree-d function differs from the product of functions of degree d_1, d_2 by a function of degree $< d$; thus by induction on d any degree-d function is a polynomial in functions of degree $\leqslant 2g^+(l)+1$. These functions in turn are linearly spanned by 1 and $g^+(l)+1$ functions of distinct positive degrees. Moreover, by comparing monomials in these generators with degree (as $\mathrm{X}_0^+(l)$ functions) at most $4g^+(l)+2$ we get enough relations between them to generate the ideal of relations between our $g^+(l)+1$ basic functions. We can then eliminate all but the two lowest-degree functions to get a singular model of $\mathrm{X}_0^+(l)$ as a plane curve and express each of the remaining $g^+(l)-1$ functions as a rational function of the first two. Note that we never required more than the first $O(l)$ coefficients of the q-expansions of any of the functions involved. It is then straightforward to express any modular function on $\mathrm{X}_0^+(l)$, such as $j+j'$ and jj', as a polynomial in the $g^+(l)+1$ basic functions, and thus as a rational function in the first two, using only the q-expansion of the target function up to and including the constant term. We can then deduce the polynomial relating j with a given function of small positive degree on $\mathrm{X}_0^+(l)$, as we found (48) in the case $l=11$, to find an explicit polynomial of degree $l+1$ whose roots give the points on $\mathrm{X}_0(l)$ parametrizing l-isogenies involving a curve with given j-invariant.

To get the modular functions on $\mathrm{X}_0(l)$ from those on $\mathrm{X}_0^+(l)$, it may no longer suffice to adjoin a single anti-invariant nonzero function v,[24] but it is at least true that given such v we can write any modular function f on $\mathrm{X}_0(l)$ uniquely as $A+B/v$ for some $\mathrm{X}_0^+(l)$ modular functions A, B which we can compute from the q-expansions of f, w^*f and v.

Moreover, we readily adapt our genus-0 methods to find the modular functions of degree $\leqslant 2g^+(l)+1$ on $\mathrm{X}_0^+(l)$ and an anti-invariant function v. The simplest general approach is probably to take linear combinations of the images of the weight-m form $(\eta(q)\eta(q^l))^m$ under the first few Hecke operators and divide by $(\eta(q)\eta(q^l))^m$, with m chosen large enough that $m(l+1)/24 > 2g^+(l)+1$ so all the desired modular functions yield cusp forms when multiplied by $(\eta(q)\eta(q^l))^m$. We likewise obtain v by dividing a form of weight m, transforming appropriately under w, by $(\eta(q)\eta(q^l))^m$. Using a form of weight $m-2$ instead of m we obtain a λ_0 for use in (40,74). We then have all the information we need to complete our program of efficiently computing the trace mod l of an elliptic curve over a finite field that has an l-isogeny rational over that field. As in the case $g^+(l)=0$,

[24] A single v suffices if and only if the ramification divisor of the double cover $\mathrm{X}_0(l)/\mathrm{X}_0^+(l)$ is linearly equivalent to a multiple of the pole of $\mathrm{X}_0^+(l)$. This is of course always the case when $g^+(l)=0$, but I found only two instances with $g^+(l)>0$, namely the two cases $l=83$, $l=131$ of $g^+(l)=1$ and $l\equiv -1 \bmod 12$. For those l we readily see that if v is chosen so that $(\eta(q)\eta(q^l))^2 v$ is the normalized invariant differential on the elliptic curve $\mathrm{X}_0^+(l)$ then every anti-invariant modular function on $\mathrm{X}_0(l)$ is a multiple of v. These may well be the only two cases where this happens once $g^+(l)>0$.

this general recipe can often be simplified for specific l; we illustrate some useful shortcuts in the Appendix.

We have said nothing about the computational complexity of finding these formulas. In fact it is not at all easy to estimate the computational cost accurately. Since the genus of our curves grows linearly with l it appears that we still do no better than $l^{3+\epsilon}$ arithmetic operations, though with much smaller implied constants. Thus to efficiently carry out our proposed improvement on Schoof's algorithm we still want to compute, and preferably store, the formulas for each l in characteristic zero. Once more we face the question of how expensive each "arithmetic operation" is, i.e. how large the coefficients in our formulas get. This is where the cost estimate becomes difficult. However, the numerical evidence is encouraging, especially compared with the forbiddingly large coefficients encountered in Φ_l; and it suggests that theoretical investigation of the size of the equations needed to describe $\mathrm{X}_0(l)$ may be worthwhile in its own right.

We have explicitly computed several dozen modular curves, and always found their equations and the formulas for j, j' and the other five functions (40,74) manageable, quite unlike the unwieldy model $\Phi_l(j, j') = 0$ of $\mathrm{X}_0(l)$. In particular, when $g^+(l)$ is small enough that $\mathrm{X}_0^+(l)$ is a (hyper)elliptic curve or a complete intersection in $\mathbf{P}^{g-1}$, we always obtained remarkably simple equations for $\mathrm{X}_0^+(l)$, with single-digit coefficients. (See for instance (112, 121) in the Appendix for $l = 191$, 239; also (99) (for $l = 37$) and the other curves $\mathrm{X}_0^+(l)$ of genus 1, i.e. with $l = 43$, 53, 61, 79, 83, 89, 101, 131, which can be found in the tables of modular elliptic curves.) One might have expected that resolving the singularities of $\Phi_l(j, j') = 0$ and forming the quotient by w would yield equations with coefficients smaller than those of Φ_l, but a reduction this drastic demands a specific explanation. In effect we observe that all the curves $\mathrm{X}_0^+(l)$ we have computed have small naïve height, so their canonical (Faltings) heights should be small as well. It would be very interesting to see if good bounds can be obtained on these heights for all l; more generally, for the modular curves of possibly composite level $\mathrm{X}_0(N)$ and their quotients by their groups of Atkin-Lehner involutions (see for instance (137, 150) in the Appendix), to determine how the height behaves as a function of N.

Atkin's idea: lifting $\mathrm{X}_0(l)$ from characteristic l. In February of 1991 Atkin announced the remarkable idea of obtaining the first few modular functions on $\mathrm{X}_0^+(l)$ by lifting w-invariant functions from the reduction of $\mathrm{X}_0(l)$ mod l. Now while $\mathrm{X}_0(l)$ is known to have good reduction at any prime other than l, it also has very bad reduction at l: it is birational to a union of two projective lines. Indeed if $\alpha : E \to E_1$ is an l-isogeny in characteristic l then $\alpha\bar{\alpha} = l$ is inseparable, so either α or $\bar{\alpha}$ is inseparable. In the former case α factors through the Frobenius isogeny $E \to E^l$ so we have an isomorphism $E^l \cong E_1$ and in particular $j(E_1) = j(E^l) = (j(E))^l$; in the latter case $j(E) = (j(E_1))^l$ for the same reason. This explains Kronecker's congruence

$$\Phi_l(j, j') \equiv (j' - j^l)(j'^l - j) \bmod l, \tag{92}$$

and the fact that the reduction mod l of $\mathrm{X}_0(l)$ is birational to the union of the lines $j' = j^l$, $j = j'^l$, switched by w. Note that these lines meet at the l^2 points where j, j' are conjugate elements of $\mathbf{F}_{l^2}$, and that these l^2 intersections are transverse. But $\Phi_l(j, j') = 0$ is not a smooth model of $\mathrm{X}_0(l)$ even in characteristic 0, so we expect to resolve some of these l^2 double points. In fact if E is defined over $\mathbf{F}_{l^2}$ we can still distinguish the inseparable Frobenius isogeny $E \to E^l$ from its dual, unless E is supersingular when the dual isogeny is also inseparable. Thus for $j \in \mathbf{F}_{l^2}$ we expect the point (j, j^l) on $\Phi_l(j, j') = 0$ to yield two distinct points on $\mathrm{X}_0(l)$ mod l, unless E is supersingular in which case j, j' should be a point of transverse self-intersection of $\mathrm{X}_0(l)$ mod l (transverse because resolving some singularities $\Phi_l(j, j') = 0$ should not make other singularities worse). A precise version of this is proved in [DR], where parts (i), (ii) of Thm.6.9 (p.286) identify $\mathrm{X}_0(l)$ mod l with the union of the j- and j'-lines, attached transversely at (j, j^l) with j contained in the set S_l of j-invariants of supersingular curves in characteristic l. We recall for later use that the number $\#S_l$ of supersingular j-invariants is 1 more than the genus of $\mathrm{X}_0(l)$, which is $l/12 + O(1)$.

The ring of "modular functions on $\mathrm{X}_0(l) \bmod l$" then comprises those pairs $(P(j), P'(j'))$ of polynomials for which $P'(j) = P(j^l)$ for each $j \in S_l$. The involution w switches P and P'; a "modular function on $\mathrm{X}_0^+(l) \bmod l$" is a w-invariant function on $\mathrm{X}_0(l)$ mod l, i.e. a polynomial $P(j) = P'(j)$ such that

$$P(j) = P(j^l) \qquad \text{for all } j \in S_l. \tag{93}$$

Note that this is no condition at all if $j \in \mathbf{F}_l$, and otherwise j and j^l give the same condition. (In effect this means that $\mathrm{X}_0^+(l)$ mod l is the j-line glued transversely to itself at conjugate pairs $\{j, j^l\}$ of supersingular j-invariants not in $\mathbf{F}_l$.) In particular this ring consists of all polynomials in j if and only if $S_l \subset \mathbf{F}_l$, which by the usual formulas for the genus of $\mathrm{X}_0(l)$ and $\mathrm{X}_0^+(l)$ is the case precisely when l is one of the fifteen primes 2, 3, 5, . . . , 31, 41, 47, 59, 71 for which $\mathrm{X}_0^+(l)$ is rational. Indeed in each case we confirm that the Hauptmodul is congruent to j mod l up to an additive constant; for instance the $\mathrm{X}_0^+(11)$ Hauptmodul (44) is $\equiv j - 2$ mod 11. Likewise for $l > 2$ anti-invariant "modular functions on $\mathrm{X}_0(l)$" are $P(j) = -P'(j)$ such that $P(j) = -P(j^l)$ for all $j \in S_l$, which in particular implies that P vanishes on $S_l \cap \mathbf{F}_l$.

How do we compute the ring of polynomials satisfying (93)? First we must determine S_l, but this is easy. For $l \leqslant 307$ this set was already exhibited in the table [B-K, 143–144], which gives the polynomial $\prod_{j_1 \in S_l}(j - j_1)$ in factored form. For any l this polynomial may be obtained as a finite hypergeometric series — there are several such results, some due to Atkin, see [Mor, Thm.2.2] and more extensively [K-Z] — but these results, though elegant, are not convenient for computation since one must then factor a polynomial of degree $l/12$ over $\mathbf{F}_l$. It is probably simplest to start from one $j_1 \in S_l \cap \mathbf{F}_l$ and find the others by repeated 2-isogenies. The initial j_1 can certainly be found in time at most $l^{1+\epsilon}$ (and expected time $l^{1/2+\epsilon}$) by testing whether a curve of j-invariant 0,1,2,. . . mod l is supersingular, but all but one in 512 l's is ramified or inert in one of the nine imaginary quadratic fields of class number 1, in which case we can simply reduce mod l the j-invariant of a corresponding CM curve over $\mathbf{Q}$. (In particular this works for all $l < 15073$, which at least for the Schoof application is more than enough for the foreseeable future.) Finding the three 2-isogenous invariants amounts to solving a cubic equation $\Phi_2(j, j_1) = 0$, or better $(h + 256)^3 = h^2 j_1$ (see (19,80); indeed only the first 2-isogeny requires a cubic equation since afterwards one root is known beforehand and the other two are determined by a quadratic equation. This will reach all of S_l because the bimodule of isogenies between two given supersingular elliptic curves is a lattice of discriminant l^2 which contains elements of norm $N \not\equiv 0 \bmod l$, and in particular $N = 2^n$ for all sufficiently large N. [This follows for instance from standard estimates for coefficients of the theta function of this lattice, which is a modular form of weight 2 on $\mathrm{X}_0(l)$; but in fact the result is completely elementary given that S_l is a finite set closed under the Φ_2 correspondence, as we shall expound elsewhere.] The number of quadratics to be solved is thus $\ll \# S_l \ll l$ so we succeed in listing S_l in time $l^{1+\epsilon}$, little more than the time it takes to write it down. Solving (93) is a lengthier but conceptually simpler computation: as in the characteristic-zero case the ring of polynomials satisfying that condition is generated by polynomials of degree $\leqslant 2g^+(l) + 1$, and (93) gives $g^+(l)$ linear conditions on the $\leqslant 2g^+(l) + 2$ coefficients. We readily compute these linear conditions in time $l^{2+\epsilon}$, and use (say) Gaussian elimination to solve them in time $l^{3+\epsilon}$, obtaining a basis of solutions consisting of monic polynomials of distinct degrees. It may be possible to exploit the special form of these linear equations to drive the computing time even lower, but the straightforward $l^{3+\epsilon}$ is already easily manageable because the implied constants are so favorable: g^+ is only $1/24$ the size of l. For instance, even for $l = 997$, when $g^+ = 38$ (both larger than anything needed thus far for computing the trace of elliptic curves over large fields), we are only dealing with a 38×78 linear system over $\mathbf{F}_l$. Similar techniques yield the reduction mod l of spaces of modular forms on $\mathrm{X}_0(l)$ and $\mathrm{X}_0^+(l)$; for instance the weight-2 w-invariant cuspforms mod l are generated by $dj/(j - j_0)(j - j_0^l)$ where $j_0 \in S_l \backslash \mathbf{F}_l$.

Atkin cautions that it might not be possible to lift a modular form or function over $\mathbf{F}_l$ to one in characteristic zero with the same order pole or zero at each cusp. For such a lift to exist, the $\mathbf{Q}$-vector spaces of modular forms of low weights and the $\mathbf{Q}$-algebra of modular functions must have generators $q^\alpha(1 + O(q))$ with distinct α's and l-integral coefficients (i.e. coefficients with denominators prime to l). For small l we readily find such generators even with all the q-coefficients in $\mathbf{Z}$, and we expect at least l-integral coefficients for all l, but we do not know a proof that this is always the case. In the sequel we *assume* that the monic generators do in fact have l-integral coefficients, and thus that the lifts to characteristic zero preserve the order of poles and zeros at the cusps.

Given this assumption, we can make some use of these functions and forms on $\mathrm{X}_0(l), \mathrm{X}_0^+(l)$ even without finding their characteristic-zero lifts. For instance, Atkin determined for $l \leqslant 883$ whether the cusp of $\mathrm{X}_0^+(l)$ is a Weierstrass point and if so obtained its Weierstrass gap sequence. Surprisingly he found that the cusp is indeed a Weierstrass point for some l as small as 109, and all l larger than 389, and indeed its multiplicity as a Weierstrass point appears to grow slowly with l. This new and intriguing phenomenon has not yet been proved and quantified, though Atkin has announced that he can at least show the multiplicity is positive for a set of primes of positive density. Another application would be finding the prime conductors of modular forms of weight 1 of type $2A_4$ and $2A_5$, by searching for l for which the dimension of the space of cusp forms of weight 1 mod l exceeds that of the subspace generated by differences between theta functions. Note that while this computation also relies on the l-integrality assumption, its results (unlike the list of Weierstrass gaps) would be unconditional: if there are no $2A_4$ and $2A_5$ forms in characteristic 0 then there are none mod l either; if there is such a form, and we lift it from its reduction mod l, we can then recover the corresponding extension of $\mathbf{Q}$ and use it to check directly that our form gives the correct Galois representation.

Still, to obtain explicit equations for and modular forms on $\mathrm{X}_0(l)$ we need to actually lift the mod-l expansions to characteristic zero. This seems at first a difficult problem because we cannot simply lift each coefficient to the corresponding integer in $(-l/2, +l/2)$. The coefficients of the equations relating j with the modular functions of least degree, and the q-expansions of these functions, may be much smaller than those of j and Φ_l, but usually still not small enough to guess from their reduction mod l. For instance the *logarithm* of the q^m coefficient of a given nonconstant modular function f grows as $C_f\sqrt{m}$. But here the second part of Atkin's idea enters: if $\deg f$ is small enough, specifically $< (l+1)/24$, then $\eta(q)\eta(q^l)f$ is a cusp form of weight 1 (with nontrivial character) on $\Gamma_0(l)$, so its coefficients grow very slowly, the m-th coefficient being $\ll m^\epsilon$. So we might expect that a long enough initial stretch of these coefficients will fall in $(-l/2, +l/2)$ that we may lift the expansion of $\eta(q)\eta(q^l)f$ as far as we need it from characteristic l, where we know it as $\eta(q)\eta(q^l)$ times a polynomial in $j(q)$, and then divide by $\eta(q)\eta(q^l)$ to recover the expansion of f itself.

An obvious problem with this is that we have ignored the constants implied in "$\ll m^\epsilon$": our cusp form's coefficients must grow slowly, but they may start out already too large to be of any use. But remarkably it turns out that in practice the coefficients are very small indeed if we choose a reasonable basis of modular functions f on $\mathrm{X}_0^+(l)$ of degree $< (l+1)/24$, or equivalently for the forms $\eta(q)\eta(q^l)f$. One natural approach is to choose a basis inductively as follows: let the first form be $\eta(q)\eta(q^l)$ itself (with $f = 1$); and let the r-th form vanish to maximal order, say order n_r, at the cusp $q = 0$ subject to the condition that it is not in the span of the first $r-1$ forms, and normalized to have q^{n_r} coefficient 1 and q^{n_s} coefficient 0 for each $s < r$. (This is tantamount to one of the "echelon forms" of basic linear algebra.) Then Atkin observes experimentally that not only are the coefficients of these forms always integers (as noted in the discussion of the l-integrality assumption), but these integers are very small, and thus that we can lift as many coefficients as needed to $\mathbf{Z}$ from their reductions mod l. A typical case is $l = 31$, when the basis consists of $\eta(q)\eta(q^{31})$ (whose coefficients we knew to be small) and the reduction mod 31 of $\eta(q)\eta(q^{31})(j(q)+1)$, whose q-expansion begins

$$q^{1/3}(1+q^2-q^3+q^5-q^6-2q^9-q^{10}-q^{13}+2q^{16}-q^{21}-2q^{22}+q^{23}\cdots), \quad (94)$$

and of the first 200 coefficients, the majority vanish, a few dozen are ± 1 or ± 2, and only two are as large as ± 3. As with the the equations for $\mathrm{X}_0^+(l)$, the remarkably small coefficients here are a new phenomenon that begs for theoretical explanation and quantification. Indeed it seems plausible that a single explanation underlies both phenomena.

Do we actually get enough modular functions in this way? It might happen that $\mathrm{X}_0^+(l)$ carries no nonconstant modular functions at all of degree $< (l+1)/24$. For instance that is the case for $l=11$ and $l=37$. But there is always a function of degree at most $g^+(l)+1$, which is smaller than $(l+1)/24$ for all but finitely many l of which the largest, not surprisingly, is 163. Once we find a single such function f we can compute the polynomial relation between it and $j(q)$ as we did in §1 with Φ_l, by writing the power sums in $f(q)$ and the $f(q_1)$ ($q_1^l = q$) as polynomials in j.

This, however, is not enough to compute l-isogenies using the approach of §3, because it is hardly ever the case that $2g^+(l)+1 < (l+1)/24$, so we cannot get the full ring of modular functions this way. Thus, given j we may find an l-isogenous j' (this is easy once we have at least two nonconstant functions of degree $< (l+1)/24$ on $\mathrm{X}_0^+(l)$ but not the kernel of the l-isogeny. Indeed, Atkin, Morain and others who have actually carried out record trace computations have obtained the kernel in other ways. But I believe that the approach of §3 can be combined with Atkin's idea as long as there is at least one nonconstant modular function of degree $< (l+1)/24$ on $\mathrm{X}_0^+(l)$. The reason is that while $2g^+(l)+1$ is usually not as small as $(l+1)/24$, it is always bounded by $(l+1)/12$. Thus the ring of modular functions on $\mathrm{X}_0^+(l)$ is generated by functions f such that $(\eta(q)\eta(q^l))^2 f$ is a cuspform of weight 2 on $\Gamma_0(l)$, possibly with nontrivial character (depending on l mod 12). Thus its q^m coefficient is $\ll m^{1/2+\epsilon}$, and again the implied constants are in practice favorable enough for an echelon basis that the first few fall well inside $(-l/2, +l/2)$ and so can be lifted from the reductions mod l. (Again a theoretical understanding of this observation would be most welcome.) This may not be enough to get at j, j' and the other modular functions directly, but it does (for those l we have tried) give enough of the q-expansion to find the relations among the generators of the ring. These yield a polynomial equation between each generator and the one of least degree. Since that first generator is known to as many q-coefficients as we need (once $l > 163$), those equations let us recover the expansions of the remaining generators to the length we need. It remains only to find the form λ_0 of weight -2; but this too can be done Atkin-style, starting from a form on $\mathrm{X}_0^+(l)$ mod l with a pole of minimal order at infinity, multiplying by $(\eta(q)\eta(q^l))^3$ to get a form of weight 1, lifting that form to a form $(\eta(q)\eta(q^l))^3\lambda_0$ with (we hope) small integer coefficients, and dividing by $(\eta(q)\eta(q^l))^3$ to recover the power series for λ_0.

Appendix: Further explicit examples

For the five cases $N = 37,\ 191,\ 239,\ 161 (= 7 \cdot 23),\ 75$ we give explicit equations for the curve $\mathrm{X}_0(N)/W$ for one or more subgroups W of the group of Atkin-Lehner involutions of $\mathrm{X}_0(N)$. Rather than use the same method in each case we choose to show a variety of techniques even though some of them do not apply to every modular curve. In each case, except for $N = 239$ which we chose only to illustrate the computation of a genus-3 curve $\mathrm{X}_0^+(l)$ and the small naïve height of such a curve, we give a specific mathematical application of the formulas obtained. These applications are: the investigation of the exotic 37-isogeny between elliptic curves over $\mathbf{Q}$ first noticed in [M-SD]; computation of a pair of non-CM elliptic curves over a quadratic extension of $\mathbf{Q}$ related by a cyclic isogeny of degree 191 (possibly the largest degree possible); finding explicit equations for the non-constant cover of $\mathbf{P}^1(\mathbf{Q})$ with Galois group $\mathrm{PSL}_2(\mathbf{F}_{23})$, constructed abstractly by Shih [Sh1]; and assisting in the proof of the generalization of Wiles' modularity theorem to curves of arithmetic conductor $\not\equiv 0 \bmod 27$ [CDT]. This list is not exhaustive; for instance explicit modular equations play a role in the determination of the full automorphism group of a modular curve, and in certain computations with Heegner points, see for instance [El1, El4].

Level 37: The modular curve $\mathrm{X}_0(37)$ and the exotic 37-isogeny

We begin with an ad-hoc construction of the modular curves $\mathrm{X}_0(37), \mathrm{X}_0^+(37)$ adapted from [M-SD] and simplified somewhat. By the usual formulas these curves have genus 2,1 respectively.

Let θ_A, θ_B, and θ_C be the theta-functions associated to the type-II positive-definite quadratic forms with matrices

$$A = \begin{pmatrix} 4 & 0 & 2 & 1 \\ 0 & 2 & 1 & 1 \\ 2 & 1 & 20 & 1 \\ 1 & 1 & 1 & 10 \end{pmatrix},\ B = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 8 & 1 & -3 \\ 0 & 1 & 10 & 2 \\ 1 & -3 & 2 & 12 \end{pmatrix},\ C = \begin{pmatrix} 4 & 1 & 2 & 1 \\ 1 & 4 & 1 & 0 \\ 2 & 1 & 6 & -2 \\ 1 & 0 & -2 & 20 \end{pmatrix}.$$

These have discriminant 37^2 and level 37; also A is self-dual (i.e. describes a lattice similar to its own dual lattice), and B, C are each other's duals. Thus we obtain an anti-invariant cusp form ϕ_- of weight two:

$$\phi_- = \frac{1}{4}(3\theta_A - 2\mathcal{E}_2) = q + q^3 - 2q^4 - q^7 - 2q^9 \ldots, \tag{95}$$

and an invariant cusp-form ϕ_+ of weight two:

$$\phi_+ = \frac{1}{2}(\theta_B - \theta_C) = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 \ldots \tag{96}$$

which is a holomorphic differential on the elliptic curve $\mathrm{X}_0^+(37)$.

We obtain modular functions on $\mathrm{X}_0^+(37)$ thus: $z = (\theta_A/\phi_-) - 1$ is a degree-2 function one of whose poles it at the cusp; since $(q\,dz/dq)/\phi_+ = -z^2 + O(1)$ at the cusp, we can by symmetry eliminate the other pole of z to construct the degree-2 modular function

$$x = \frac{1}{2}\left(z^2 + 1 - \frac{q\,dz/dq}{\phi_+}\right) = q^{-2} + 2q^{-1} + 5 + 9q + 18q^2 + \ldots \tag{97}$$

on $\mathrm{X}_0^+(37)$. The $\mathbf{C}$-algebra of modular functions on $\mathrm{X}_0^+(37)$ is then generated by x and a degree-3 function y. We can exhibit a suitable y in two ways. Since we already know the invariant differential $\phi_+(dq/q)$, we can use it to obtain a degree-3 function $(q\,dx/dq)/\phi_+$, and then choose

$$y = q^{-3} + 3q^{-2} + 9q^{-1} + 20 + 46q + 92q^2 + \ldots \tag{98}$$

so that $\phi_+(dq/q) = -dx/(2y+1)$. Alternatively, we could start use η-ratios to find the degree-3 function $(\eta/\eta_{37})^2 + 37(\eta_{37}/\eta)^2$, compare q-expansions to find the cubic equation satisfied by that function and x, and determine the linear combination

$$y = \left(\frac{\eta}{\eta_{37}}\right)^2 + 37\left(\frac{\eta_{37}}{\eta}\right)^2 + 5x - 7$$

that puts that equation in minimal (Néron) form. Either way, we find that our x, y are related by the familiar equation

$$y^2 + y = x^3 - x \tag{99}$$

numbered 37A in [B-K] and 37-A1 in [Cre].

We then compute that $z = (y+1)/(x+1)$ and $(\phi_-/\phi_+)^2 = 1 + 4(x-6)/(y - 6x + 22)$, to obtain the anti-invariant modular function

$$s = \frac{x^2 - 6x - 11 - 4y}{x+1} \cdot \frac{\phi_-}{\phi_+} = q^{-2} - 2 - 5q - 14q^2 - 19q^3 - \ldots, \tag{100}$$

with

$$s^2 = x^2 - 6x - 11 - 4y. \tag{101}$$

To write a generic 37-isogeny over $\mathrm{X}_0(37)$ we choose $\lambda_0 = \phi_-^{-1})$. We find

$$\begin{aligned}
\lambda_0 \mathsf{E}_2^{(37)}{}_2 &= \frac{3y - x + 2}{2(x+1)}, \\
\frac{1}{2}(A_4 + 37^2 A_4') &= 5\,\frac{137x^2y - 250x^3 - 356xy + 189x^2 + 57y - 23x}{(x+1)y}, \\
\frac{1}{2}(A_4 - 37^2 A_4') &= 12s\left[\frac{10xy + 100x^2 - 13y - 18x - 85}{(x+1)^2(x-1)} - 57\right], \qquad (102) \\
\frac{1}{2}(A_6 - 37^3 A_6') &= \frac{s}{(x+1)^3(x-1)}\Big[25327x^3y - 25579x^4 - 33643x^2y
\end{aligned}$$

$$+ 31252x^3 - 19640xy - 1549x^2 + 18227y - 26005x + 12152\Big],$$

$$\frac{1}{2}(A_6 - 37^3 A_6') \;=\; -\frac{126}{(x+1)^2 y}\Big[201x^5 - 601x^3y - 742x^4 + 414x^2y$$
$$- 703x^3 + 346xy + 919x^2 - 3y + 85x\Big].$$

[Note the denominators, which arise because the cusps are not the only poles of λ_0; but since the other poles are known, we can cancel out the poles of $\lambda_0 \mathsf{E}_2^{(37)}$ etc. by multiplying them by suitable powers of $x \pm 1$, and recognize the resulting modular functions as polynomials in x, y from their q-expansions as usual.]

It is known that the elliptic curve $\mathrm{X}_0^+(37)$ has trivial torsion and rank one (and indeed is the modular elliptic curve of least conductor with positive rank); that its group of rational points is generated by $P : (x, y) = (0, 0)$ (by a 2-descent, [Sil, pp.320–1, Ex. 10.9 and p.275, Ex. 9.13a,b]); and that the only integral points are the multiples $\pm 3P, \pm P, \pm 2P, \pm 4P, \pm 6P$ with x-coordinates $-1, 1, 0, 2, 6$ [Sil, p.275, Ex. 9.13c]. Using our equations above to compute j, j' at these ten points, we find that nine of them are Heegner points, with

$$3P, 2P, -P, P, -2P, -3P, -4P, 4P, 6P \tag{103}$$

parametrizing 37-isogenies between CM elliptic curves of discriminants

$$-3, -4, -7, -11, -12, -16, -27, -28, -67 \tag{104}$$

respectively; and the tenth point, $-6P : (x, y) = (6, -15)$, lifts to a pair of rational points on $\mathrm{X}_0(37)$ that determine the unique pair of rational j-invariants of 37-isogenous elliptic curves [M-SD]. The "remarks on isogenies" preceding the Antwerp tables exhibit a minimal model for a curve of least conductor, namely $1225 = 35^2$, for one of these j-invariants; no derivation is given there beyond the attribution to Vélu. We use our explicit modular functions on $\mathrm{X}_0(37)$ to confirm the equation for that curve, give a minimal model for the isogenous curve, and determine the kernel of the isogeny.

To match Vélu's curve we choose the quadratic twist $\gamma = 140/37$. We then obtain, at the two rational points $(x, y, s) = (6, -15, 7)$ and $(6, -15, -7)$ on $\mathrm{X}_0(37)$, the elliptic curves

$$\begin{aligned} E_1 :\ Y_1^2 &= X_1^3 - \frac{385}{3}X_1 + \frac{16450}{27} \qquad (j = -7 \cdot 11^3) \\ E_2 :\ Y_1^2 &= X_1^3 - \frac{9987985}{3}X_1 - \frac{63131603150}{27} \qquad (j = -7 \cdot 137^3 2083^3); \end{aligned} \tag{105}$$

the transformation $(X_1, Y_1) = (4X + (5/3), 8Y + 4X + 4)$ then provides the minimal models:

$$Y^2 + XY + Y = X^3 + X^2 - 8X + 6 \tag{106}$$

for E_1 (this was the equation attributed to Vélu), and

$$Y^2 + XY + Y = X^3 + X^2 - 208083X - 36621194 \tag{107}$$

for E_2. Next we compute the kernel G of the 37-isogeny from E_1 to E_2. We find that each of the points of G is defined over the degree-12 real subfield F of the cyclotomic field $\mathbf{Q}(e^{2\pi i/35})$, and the X-coordinates are defined over its quadratic subfield, which is the totally real sextic number field of least discriminant $300125 = 5^3 7^4$ [Poh], obtained by composing the real quadratic and cubic fields of least discriminant: $\mathbf{Q}(\sqrt{5})$ and $\mathbf{Q}(\cos 2\pi/7)$. Indeed, G is generated by a 37-torsion point with X-coordinate

$$X = \sqrt{5}\bigl(2\cos\frac{2\pi}{7} + \frac{1}{2}(3+\sqrt{5})\bigr). \tag{108}$$

The Galois group of F is canonically isomorphic to the 12-element cyclic group $(\mathbf{Z}/35\mathbf{Z})^*/\{\pm 1\}$, generated by ± 2; the corresponding automorphism of F induces multiplication by 8 on G. This allows the determination mod 37 of the trace of Frobenius of E_1 mod l for any prime l of good reduction (i.e. $l \neq 5, 7$): let β mod 12 be such that $p \equiv \pm 2^\beta$ mod 35; then the trace mod 37 is $8^\beta + p \cdot 14^\beta$. For instance, the trace is divisible by 37 for $p = 11$, 47, 137, 223, 1543, 1777, 1951, 2971 and no other $p < 3000$; of these, all are supersingular with the exception of 1951, which has trace -74.

We remark that while [Cre] lists only modular elliptic curves of conductor < 1000, Cremona has extended his computations up to conductor 5077, and so in particular has verified that these curves (106,107) are modular; they are numbered 1225-H1 and 1225-H2 in his lists publicly available (though not yet formally published) on `ftp://euclid.exeter.ac.uk/pub/cremona/data/` .

Level 191:
The curve $\mathrm{X}_0^+(191)$ and a pair of non-CM 191-isogenous Q-curves

For any prime l, a non-cusp point P on $\mathrm{X}_0^+(l)$ defined over some field K (not of characteristic l) parametrizes a pair of l-isogenous curves E_1, E_2 up to quadratic twist. If the two curves are isomorphic, we have a pair of degree-l endomorphisms of the same elliptic curve; thus the curve has complex multiplication and l is split in the CM field (or ramified, in which case P comes from a point of $\mathrm{X}_0(l)$ fixed by w). Otherwise, if the points above P in $\mathrm{X}_0(l)$ are both rational we have two l-isogenous curves over K, but in the more usual case that P does not lift to a rational point of $\mathrm{X}_0(l)$ the l-isogenous curves E_1, E_2 are conjugate over some quadratic extension $K(\sqrt{\delta})$ of K (namely the field of definition of the preimages of P on $\mathrm{X}_0(l)$), in which case they are a pair of "K-curves" [Rib, El3]. Note that we do not claim that the isogeny is defined over $K(\sqrt{\delta})$. From our formulas (32,35) for isogenies over $\mathrm{X}_0(l)$ we see that by choosing a w-invariant λ_0 we find E_1 such that E_1/G is isomorphic with the $\sqrt{l}$-twist of E_2. Thus E_1 has a quadratic twist E_1^{tw} isogenous *over* $K(\sqrt{\delta})$ with the Galois conjugate of E_1^{tw} only when l or $-l$ is a norm $\gamma\bar{\gamma}$ for some $\gamma \in K(\sqrt{\delta})$, in which case we can take E_1^{tw} to be the twist by $\sqrt{\gamma}$ or $\sqrt{\delta^{1/2}\gamma}$ of E_1.

Taking now $K = \mathbf{Q}$, we have 13 j-invariants of CM curves, each of which yields a rational point on $\mathrm{X}_0^+(l)$ for 50% of the primes l. One might expect that, once l is large enough that the genus $g^+(l)$ of $\mathrm{X}_0^+(l)$ exceeds 1, these are the only rational points on $\mathrm{X}_0^+(l)$. (In each of the nine cases $l = 37$, 43, 53, 61, 79, 83, 89, 101, 131 where $\mathrm{X}_0^+(l)$ has genus 1 it is an elliptic curve of rank 1 — indeed it is clear *a priori* that the analytic rank is odd — and thus infinitely many rational points; for instance there are infinitely many pairs of 131-isogenous $\mathbf{Q}$-curves.) In fact once $g^+(l) \geqslant 3$ this seems a reasonable conjecture, a conjecture we in fact advanced in [El3].[25] But for $g^+(l) = 2$ the hyperelliptic involution of $\mathrm{X}_0^+(l)$ may take a cusp or CM point to a new rational point, producing a sporadic pair of l-isogenous $\mathbf{Q}$-curves. It was such a construction on $\mathrm{X}_0(37)$ that produced the exotic 37-isogeny described in the Appendix, and much the same thing happens for some of the hyperelliptic $\mathrm{X}_0^+(l)$, including the last case $l = 191$ of genus 2.[26] In this part of the Appendix we give an explicit equation for $\mathrm{X}_0^+(191)$ and locate the cusp and the four rational CM points, of discriminants -7, -11, -19, and -28. We find that four of these pair up under the hyperelliptic involution, but the fifth is sent to a new rational point (which together with the other five presumably exhausts the rational points on the curve); we then describe the sporadic pair of 191-isogenous $\mathbf{Q}$-curves associated to this sixth point. The prime 191 would be the largest for which such a sporadic pair exists if the conjecture concerning rational points of $\mathrm{X}_0^+(l)$ for $g^+(l) \geqslant 3$ is correct.

Let φ be the weight-1 form $(q) = \eta(q)\eta(q^{191})$, and let $\vartheta_4, \vartheta_5, \vartheta_6$ be the theta series of the quadratic forms $(4, 1, 12)$, $(5, 3, 10)$, $(6, 1, 8)$ of discriminant -191. Then

$$\begin{aligned} z_3 &:= \frac{\vartheta_5 - \vartheta_6}{2\varphi} = q^{-3} + q^{-1} + q + q^2 + 2q^3 + 2q^4 + 3q^5 + 3q^6 + \cdots, \\ z_4 &:= \frac{\vartheta_4 - \vartheta_5}{2\varphi} = q^{-4} + q^{-2} + q^{-1} + 2 + 2q + 3q^2 + 3q^3 + 5q^4 + \cdots \end{aligned} \tag{109}$$

are modular functions of degree 3, 4 on $\mathrm{X}_0^+(191)$. By comparing q-expansions we find that they map $\mathrm{X}_0^+(191)$ to the singular plane quartic

$$z_3^4 + 3z_3^3 + (-z_4 + 4)z_3^2 + z_3 + (-z_4^3 + 2z_4^2 - 1) = 0 \tag{110}$$

with a node at $(z_3, z_4) = (-1, 1)$. Thus

$$u := \frac{z_4 - 1}{z_3 + 1} = q^{-1} + q^4 + q^5 + q^9 + q^{10} + q^{11} + \cdots \tag{111}$$

[25] At any rate it should be true that $\mathrm{X}_0^+(l)$ has no $\mathbf{Q}$-rational points other than cusps and CM points once l is large enough; this is part of the natural extension to arithmetic subgroups of $\mathrm{PGL}_2^+(\mathbf{Q})$ of Serre's conjecture for arithmetic subgroups of $\mathbf{Z}$ from his paper "Répresentations l-adiques" [Se2, #112], see 6.6 on page 395 and the correction on p.712.

[26] One might object that conceivably $\mathrm{X}_0^+(l)$ could be hyperelliptic even when $g^+(l) \geqslant 3$. It turns out that this never happens, though. If $\mathrm{X}_0^+(l)$ is hyperelliptic then $\mathrm{X}_0(l)$ admits a rational map of degree 4. Following [Ogg, p.456], we reduce this map mod 2 and count points over $\mathbf{F}_4$: there are at most $4(4+1) = 20$ points, of which two are cusps. But there are also $(l+1)/24$ supersingular points, so $l \leqslant 24 \cdot 18 - 1 = 431$. It is now straightforward to check for each $l \leqslant 431$ with $g^+(l) > 2$ that the w-invariant cusp forms of weight 2 on $\mathrm{X}_0(l)$ cannot be the holomorphic differentials of a hyperelliptic curve.

is a rational function of degree 2 on that curve, and we obtain a hyperelliptic equation for $\mathrm{X}_0^+(191)$ by substituting (111) into (110):

$$z_3^2 - (u^3 + u - 1)z_3 - (u^3 + u^2 - u) = 0. \tag{112}$$

Thus the w-invariant cusp forms of weight 2 are the holomorphic differentials

$$\begin{gathered} g_2 = -\frac{q\,du/dq}{2z_3 - u^3 - u + 1} = q - q^3 - q^4 - q^5 - q^7 - q^8 - 2q^9 - q^{10} + q^{12} \ldots, \\ g_1 = ug_2 = q^2 - q^4 - q^5 - q^6 - q^7 - 2q^8 + q^{11} \cdots. \end{gathered} \tag{113}$$

Under the Hecke operator T_2, the form g_1 maps to g_2, which maps to $g_1 - g_2$; thus T_2 has characteristic equation $T_2^2 + T_2 = 1$, and the eigenforms are $g_1 + tg_2$ where $t^2 + t = 1$.

The ring of modular functions on $\mathrm{X}_0^+(191)$ is generated by z_3, z_4, and

$$z_5 := uz_4 - 1 = q^{-5} + q^{-3} + q^{-2} + 2q^{-1} + 2 + 4q + 4q^2 + 7q^3 + \cdots. \tag{114}$$

These must all be integers at a rational CM point. To find the (u, z_3, z_4, z_5) coordinates at the CM points of discriminant -7, -11, -19, -28 it is probably easiest to use transcendental methods,[27] evaluating the q-expansions at appropriate quadratic irrationalities such as $\tau = (39 + \sqrt{-7})/382$, $(107 + \sqrt{-11})/382$, $(73 + \sqrt{-19})/382$, and $(39 + \sqrt{-7})/191$ to sufficient precision to recognize them as integers. We find that the coordinates are respectively $(0, -1, 1, -1)$, $(0, 0, 1, -1)$, $(\infty, -1, 0, 1)$ and $(2, -1, 1, 1)$. Thus the hyperelliptic involution $(u, z) \leftrightarrow (u, u^3 + u - 1 - z)$ switches the first two of these, takes the CM-19 point to the cusp $(\infty, \infty^3, \infty^4, \infty^5)$, and takes the last point to a non-CM integral point, namely

$$(u, z_3, z_4, z_5) = (2, 10, 23, 45). \tag{115}$$

Using the methods described in this paper, with $\lambda_0 = \varphi^{-2}$, we have computed the Weierstrass coefficients of a pair of 191-isogenous curves parametrized by the generic point on $\mathrm{X}_0^+(191)$; sparing the reader these formulas, we content ourselves with exhibiting their specialization to the rational point (115). Both curves are defined over $\mathbf{Q}(r)$ where $r^2 = 2036079533 = 61 \cdot 229 \cdot 145757$; their j-invariants are

$$\begin{gathered} 28912495115622316689557642664280631020825709568000000 \\ \pm 6407493927137554671415525409106656684013158400 0r. \end{gathered} \tag{116}$$

(The coefficient of r, proportional to $j' - j$, is remarkably smooth: it factors as

$$2^{16}\ 3^7\ 5^3\ 7^2\ 11\ 13\ 17\ 19\ 29\ 31\ 41\ 59\ 83\ 103\ 139\ 181\ 191\ 499\ 1151\ 3769\ 8171.) \tag{117}$$

[27] If this seems distasteful one can use the q-expansions to write $j + j'$ and jj' as polynomials in z_3, z_4, z_5 and thus in u, z, and for each CM invariant j_0 solve $j + j' = 2j_0$, $jj' = j_0^2$. But this is considerably more work, and does not even avoid transcendental methods unless the singular moduli j_0 were found algebraically — which to be sure can be done, for instance using the product formulas of [G-Z], but is not the usual approach.

We may take

$$a_4, a_4' = -77257886474370 \mp 959424380r, \tag{118}$$

$$a_6, a_6' = -\frac{1171277779175840439425}{4} \mp \frac{9601637469265219}{2}r, \tag{119}$$

when these curves have extended Weierstrass form $y^2 + y = x^3 + a_4 x + (a_6 - \frac{1}{4})$, $y^2 + y = x^3 + a_4' x + (a_6' - \frac{1}{4})$ with algebraic integer coefficients. Each curve then has discriminant of norm 191^6, and indeed the coefficients are contained in the second and third powers of the prime ideal $(191, r \pm 54)$. Since this ideal is not principal (it is not even in the trivial genus since 191 is not a square mod 61 or 229), there is no quadratic twist of these curves with good reduction everywhere, even though for each prime of $\mathbf{Q}(r)$ there is a twist with good reduction at that prime. The fact that 191 is not the norm of any element of $\mathbf{Q}(r)$ also means, as we noted above, that we cannot find a conjugate pair of elliptic curves over $\mathbf{Q}(r)$ with j-invariant (116) such that the 191-isogeny between them is defined over $\mathbf{Q}(r)$.

Level 239: The modular curve $\mathrm{X}_0^+(239)$ of genus 3

The w-invariant cusp forms of weight two on $\mathrm{X}_0(239)$ are generated by the forms g_1, g_2, g_3 uniquely determined by the q-expansions

$$\begin{aligned} g_1 &= q - q^2 - q^5 - q^7 + q^8 - 2q^9 - q^{12} \ldots, \\ g_2 &= q^2 - q^3 - q^6 - 2q^8 + q^9 - q^{10} + q^{12} \ldots, \\ g_3 &= -q^3 + q^4 + q^5 - q^8 - q^{10} + q^{11} + q^{12} \ldots; \end{aligned} \tag{120}$$

Then $(g_1 : g_3 : g_2)$ maps $\mathrm{X}_0^+(239)$ to the smooth quartic curve in $\mathbf{P}^2$ with affine equation

$$s^3 - (r^2 - r + 2)s^2 + (r^3 + r^2 - r + 3)s + (r^2 + r - 1) = 0, \tag{121}$$

where

$$\begin{aligned} r = \frac{g_1}{g_2} &= q^{-1} + q^5 + q^6 + q^{11} \ldots, \\ s = \frac{g_3}{g_2} &= -q + q^3 + q^4 - q^6 - 2q^7 - q^8 + q^9 + 2q^{10} + 2q^{11} \ldots . \end{aligned} \tag{122}$$

The ring of modular functions on $\mathrm{X}_0^+(239)$ is generated by the functions

$$\begin{aligned} F_4 &= r^4 + (1-s)r^3 + sr^2 + (s^2 - 2s + 2)r - s + 1 \\ &= q^{-4} + q^{-3} + q^{-2} + q^{-1} + 2 + 2q + 3q^2 + 3q^3 \ldots, \\ F_5 &= r^5 - sr^4 + 2sr^3 + (s^2 - 4s + 3)r^2 - (s^2 - 2s + 1)r + s^2 - s + 2 \\ &= q^{-5} + q^{-3} + q^{-2} + 2q^{-1} + 2 + 3q + 3q^2 + 5q^3 \ldots, \\ F_6 &= r^6 - sr^5 + (2s - 1)r^4 + (s^2 - 3s + 2)r^3 - (s^2 - s + 1)r^2 + sr + s - 1 \\ &= q^{-6} + q^{-2} + q^{-1} + 2 + 2q + 3q^2 + 4q^3 \ldots, \end{aligned} \tag{123}$$

$$\begin{aligned}F_7 \;&=\; r^7 - sr^6 + (2s-1)r^5 + (s^2-3s+2)r^4 - (s^2-s+2)r^3 \\ &\qquad +(2s-1)r^2 - 2r - s^2 + 2s - 4 \\ &=\; q^{-7} + q^{-1} + 2q + 3q^2 + 5q^3 \ldots\;.\end{aligned}$$

In fact, these four modular functions were found first, in the same way we arrived at the functions z_3, z_4 on $\mathrm{X}_0^+(191)$ (see (109)): they are

$$\begin{gathered}F_4 = \frac{\vartheta_6 - \vartheta_8}{2\varphi}, \qquad F_5 = \frac{\vartheta_5 - \vartheta_6}{2\varphi} + 1, \\ F_6 = \frac{\vartheta_4 - \vartheta_5}{2\varphi} - F_4, \qquad F_7 = \frac{\vartheta_3 - \vartheta_4}{2\varphi} - F_4 - F_5,\end{gathered} \tag{124}$$

where $\varphi = \eta(q)\eta(q^{239})$ and $\vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_8$ are the theta series of the quadratic forms $(3,1,20)$, $(4,1,15)$, $(5,1,12)$, $(6,1,10)$, $(8,7,9)$ of discriminant -239. We then found quadratic relations between these q-expansions and eliminated F_6, F_7 to obtain a relation between F_4 and F_5 in the form of an irreducible plane quintic with three nodes at $(F_4, F_5) = (-1, 4)$ and $(-\rho, \rho)$ with ρ one of the two primitive cube roots of unity. The nonsingular quartic form of the curve was then obtained by a quadratic transformation relative to these three points, taking

$$s = \frac{F_5 - (F_4-1)^2}{(F_4+F_5)(F_4+1)}, \qquad r = \frac{F_5 - 4}{F_4 + 1} + s + 1. \tag{125}$$

The invariant forms g_1, g_2, g_3 were then recovered from

$$g_2 \frac{dq}{q} = \frac{-dr}{r^3 + (1-2s)r^2 + (2s-1)r + 3s^2 - 4s + 3}, \tag{126}$$

$g_1 = rg_2$, $g_3 = sg_2$. The Hecke algebra on the g_i is isomorphic with $\mathbf{Z}[\cos(2\pi/7)]$.

There are five "obvious" rational points on $\mathrm{X}_0^+(239)$: the cusp, the CM points of discriminants -7, -19, -28, and -43. From the q-expansions it is clear that at the cusp F_j $(4 \leqslant j \leqslant 7)$ has a pole of order j while r, s have a simple pole and zero respectively. At the four rational CM points we compute the following coordinates:

	F_4	F_5	F_6	F_7	$(r:s:1)$
CM-7	0	0	1	1	$(1:1:0)$
CM-19	-1	0	2	2	$(0:1:0)$
CM-28	0	2	-1	-1	$(-1:1:2)$
CM-43	1	-2	1	0	$(-1:1:1)$

(127)

These five are probably the only rational points on $\mathrm{X}_0^+(239)$.

Level 161:
The modular curve $\mathrm{X}_0^{++}(161)$ and Shih's $\mathrm{PSL}_2(\mathbf{F}_{23})$ cover of $\mathbf{Q}(T)$

E. Noether asked whether every finite group G arises as a Galois group over $\mathbf{Q}$, and if so whether $G = \mathrm{Gal}(K/\mathbf{Q})$ for infinitely many number fields K. The problem is still open, but much interesting mathematics has been developed to give partial solutions; see [Se1] for a good sample. A natural approach is to look for a family of fields K parametrized by T, i.e. for a normal extension $L/\mathbf{Q}(T)$ with Galois group G not of the form $K(T)$ for some number field K as above. From such L we can find infinitely many G-extensions of $\mathbf{Q}$ by specializing T. This approach has been quite successful for many specific groups or families of groups G; for instance it is known that even the Fischer-Griess "Monster" arises in this way [Mat], though it seems hopeless to exhibit equations for that extension. Now for prime l the group $\mathrm{PSL}_2(\mathbf{F}_l)$ is the geometric Galois group of the cover of the rational curve $\mathrm{X}(1)$ by the modular curve $\mathrm{X}(l)$, from which one might expect to obtain $\mathrm{PSL}_2(\mathbf{F}_l)$ as a Galois group over $\mathbf{Q}(T)$ and thus over $\mathbf{Q}$. Since the cover $\mathrm{X}(l)/\mathrm{X}(1)$ is the Galois closure of $\mathrm{X}_0(l)/\mathrm{X}(1)$, that putative $\mathrm{PSL}_2(\mathbf{F}_l)$ cover would be the splitting field of $\Phi_l(T, j')$, or more nicely of the polynomial relating j with some lower-degree function on $\mathrm{X}_0(l)$. Unfortunately this fails because the $\mathrm{PSL}_2(\mathbf{F}_l)$ action on $\mathrm{X}(l)$ cannot be defined over $\mathbf{Q}$ once $l > 2$. Nevertheless Shih ([Sh1], see also [Se1, Ch.5]) was able to modify that cover to produce a $\mathrm{PSL}_2(\mathbf{F}_l)$ extension of $\mathbf{Q}(T)$ whenever 2, 3, or 7 is a quadratic nonresidue of the odd prime l. In the first two cases the covers are ramified only above three points $T \in \mathbf{P}^1$ and can be obtained as special cases of the "rigidity" methods of [Mat]; in [Sh2, §5] Shih obtained for $l = 11, 13$ explicit polynomials of degree $l + 1$ over $\mathbf{Q}(T)$ whose splitting fields are those $\mathrm{PSL}_2(\mathbf{F}_l)$ covers. But in the third case the cover of $\mathbf{P}^1$ has four ramification points and cannot be obtained from rigidity considerations. The smallest l for which $(2/l) = (3/l) = +1$ but $(7/l) = -1$ is $l = 23$. There is thus a polynomial of degree 24 over $\mathbf{Q}(T)$ whose splitting field has Galois group $\mathrm{PSL}_2(\mathbf{F}_{23})$ and constant field $\mathbf{Q}$, and thus yields infinitely many $\mathrm{PSL}_2(\mathbf{F}_{23})$ extensions of $\mathbf{Q}$. We show how to obtain such a polynomial explicitly from equations for the modular curve

$$\mathrm{X}_0^{++}(161) = \mathrm{X}_0(7 \cdot 23)/\langle w_7, w_{23}\rangle. \tag{128}$$

Shih's construction starts from $\mathrm{X}_0(l_0)$ where l_0 is the auxiliary prime 2, 3, or 7. This is a rational curve with an involution $w_0 = w_{l_0}$. Let $\mathrm{X}_0^{\mathrm{tw}}(l_0)$ be the quadratic twist of this by $\mathbf{Q}(\sqrt{l^*})$, where $l^* = \pm l$ with the sign chosen so $l^* \equiv 1 \bmod 4$, i.e. so the quadratic extension $\mathbf{Q}(\sqrt{l^*})$ of $\mathbf{Q}$ is ramified only at l. Then $\mathrm{X}_0^{\mathrm{tw}}(l_0)$ parametrizes l_0-isogenous pairs (E_1, E_2) of elliptic curves whose j-invariants are quadratic conjugates in $\mathbf{Q}(\sqrt{l^*})$. (As usual these elliptic curves defined only up to quadratic twist, here and later.) This curve $\mathrm{X}_0^{\mathrm{tw}}(l_0)$ has genus 0, and for our three l_0 the fixed points of w_0 are rational so $\mathrm{X}_0^{\mathrm{tw}}$ has rational points and is thus isomorphic with $\mathbf{P}^1$ over $\mathbf{Q}$ [Se1, Prop. 5.3.1]. The curve $\mathrm{X}_0(l_0 l)$ covers $\mathrm{X}_0(l)$ with geometric Galois group $\mathrm{PSL}_2(\mathbf{F}_l)$ and has an Atkin-Lehner involution w lifting w_0. Thus we may twist $(\mathrm{X}_0(l_0 l), w)$ by $\mathbf{Q}(\sqrt{l^*})$ to obtain a curve $\mathrm{X}_0^{\mathrm{tw}}(l_0 l)$ covering $\mathrm{X}_0^{\mathrm{tw}}(l)$. A (non-cusp) point on $\mathrm{X}_0^{\mathrm{tw}}(l_0 l)$ is then equivalent to two points P, P' on $\mathrm{X}_0^{\mathrm{tw}}(l)$ parametrizing two pairs (E_1, E_2), (E_1', E_2') as above together with l-isogenies between E_i and E_i'; the cover $\mathrm{X}_0^{\mathrm{tw}}(l_0 l) \to \mathrm{X}_0^{\mathrm{tw}}(l_0)$ takes (P, P') to P; and a point on the Galois closure of the cover above P is equivalent to a choice of l-torsion structures on E_1, E_2 up to $\mathbf{F}_l^*$ scaling, compatible with the l_0-isogeny. Thus the geometric

Galois group is again $\mathrm{PSL}_2(\mathbf{F}_l)$, but this time the $\mathrm{PSL}_2(\mathbf{F}_l)$ action can actually be defined over $\mathbf{Q}$ when $(l_0/l) = -1$ ([Sh1], [Se1, Cor. 5.2.2]).

To get explicit equations for this cover, then, we need a degree-1 function T for $\mathrm{X}_0^{\mathrm{tw}}(l_0)$, a rational function R on $\mathrm{X}_0^{\mathrm{tw}}(l_0 l)$ not in $\mathbf{Q}(T)$, and the monic polynomial of degree $l+1$ over $\mathbf{Q}(T)$ satisfied by R. The splitting field of this polynomial will then be the desired $\mathrm{PSL}_2(\mathbf{F}_l)$ extension. In our case $l_0 = 7$ and $l = 23$. We know already that $\mathrm{X}_0(7)$ has Hauptmodul $h(q) = (\eta(q)/\eta(q^7))^4$ with $w_0(h) = 49/h$, so $\mathrm{X}_0^+(7)$ has Hauptmodul

$$u = \frac{(h+7)^2}{h} = q^{-1} + 10 + 51q + 204q^2 + 681q^3 + 1956q^4 + \cdots \tag{129}$$

and, as we found (26,29) for $l_0 = 3$, the double cover $\mathrm{X}_0(7)/\mathrm{X}_0^+(7)$ is obtained by adjoining $h - 49/h = \sqrt{u^2 - 28u}$. Thus we can write the twist $\mathrm{X}_0^{\mathrm{tw}}(7)$ as the conic

$$v^2 = -23(u^2 - 28u). \tag{130}$$

with a rational point $(u, v) = (0, 0)$. Projecting from this known point we identify the conic (130) with $\mathbf{P}^1$: let $T = 23u/v$; then

$$u = \frac{28T^2}{T^2+23}, \qquad v = \frac{23 \cdot 28\, T}{T^2 + 23}. \tag{131}$$

We will obtain R as a rational function on the curve $\mathrm{X}_0^{++}(161)$; since as a function on $\mathrm{X}_0(161)$ such a function is invariant under w_7 it will automatically be a rational function on $\mathrm{X}_0^{\mathrm{tw}}(161)$ as well.

Now $\mathrm{X}_0^{++}(161)$ is a curve of genus 2, so it admits a rational function of degree 2, and a unique such function of the form $q^{-1} + O(q)$. We find this function in much the same way that we did for $\mathrm{X}_0^+(191)$, and choose that function for our R. We begin with a modular form on $\mathrm{X}_0(161)$ which is a product of η-functions and thus vanishes only at the cusps:

$$f(q) = \prod_{d|161} \eta(q^d) = q^8 - q^9 - q^{10} + q^{13} + q^{16} + q^{17} - 2q^{20} \cdots. \tag{132}$$

This is in an eigenspace of the involutions w_7, w_{23} (as it happens $w_7^* f = -f$, $w_{23}^* f = +f$); we will obtain modular functions on $\mathrm{X}_0^{++}(161)$ from other weight-2 forms in the same eigenspace by dividing them by f. Since $161 \equiv 1 \bmod 4$ we cannot readily obtain such forms from theta series as we could for $\mathrm{X}_0^+(191)$. We can, however, use linear combinations of the images of f under various Hecke operators T_n (a somewhat less convenient approach because it requires more coefficients of f, but it is easy to generate these coefficients from the η-product). We find that the ring of modular functions is generated by

$$\begin{aligned}
u_1 &= \frac{T_6 f - T_2 f}{3f} - 3 \;=\; q^{-3} + q^{-1} + q + q^2 + 3q^3 + \cdots, \\
u_2 &= \frac{T_2 f}{f} - 3 \;=\; q^{-4} + q^{-2} + q^{-1} + 3q + 4q^2 + \cdots, \\
u_3 &= -\frac{T_3 f}{f} - u_2 - 2u_1 - 6 \;=\; q^{-5} + 2q^{-2} + q^{-1} + 3q + 4q + \cdots,
\end{aligned} \tag{133}$$

satisfying the cubic and quadratic relations

$$u_1 u_3 = u_2^2 - u_1^2 + 4u_2 - 5u_1, \qquad u_2 u_3 = u_1^3 - 2u_1u_2 + 3u_1^2 - 2u_2 + u_1. \tag{134}$$

Eliminating u_3 (which appears linearly in both equations) we find an equation for $\mathrm{X}_0^{++}(161)$ as the singular plane quartic

$$u_1^4 + 3u_1^3 + u_1^2 = u_2^3 + 4u_2^2 + (u_1^2 - 3u_1)u_2; \tag{135}$$

Thus

$$R := \frac{u_2}{u_1} = q^{-1} + q^2 - q^3 + q^4 + 2q^5 \cdots \tag{136}$$

is a rational function of degree 2 on $\mathrm{X}_0^{++}(161)$, and we obtain a hyperelliptic model

$$u_1^2 + (3 - R - R^3)u_1 = 4R^2 - 3R - 1 \tag{137}$$

of our curve. Thus the w-invariant cusp forms of weight 2 are the holomorphic differentials

$$\begin{aligned} g_2 = -\frac{q\,dR/dq}{2u_1 - R^3 - R + 3} &= q^2 - q^4 - 2q^5 - q^6 - 2q^8 + 4q^11\ldots, \\ g_1 = Rg_2 &= q - q^3 - q^4 - 2q^5 - q^7 - q^8 - 2q^9 - 2q^{10}\ldots, \end{aligned} \tag{138}$$

with $T_2 g_1 = g_2$ and $T_2 g_2 = f_1 - f_2$ as with the $\mathrm{X}_0^+(191)$ forms (138) and thus again with Hecke eigenforms $g_1 + tg_2$ where $t^2 + t = 1$.

To obtain our explicit polynomial over $\mathbf{Q}(T)$ with Galois group $\mathrm{PSL}_2(\mathbf{F}_{23})$ we now proceeded as follows. Our $\mathrm{X}_0^+(7)$ Hauptmodul $u(q)$ is a rational function on $\mathrm{X}_0(161)/\langle w_7\rangle$; its image under w_{23} is $u(q^{23})$. Thus $u(q) + u(q^{23})$ and $u(q)u(q^{23})$ are rational functions on $\mathrm{X}_0^{++}(161)$. Moreover these functions of degree 23, 24 have no poles other than the cusp. They are thus in the ring of modular functions on $\mathrm{X}_0^{++}(161)$, and by comparing q-expansions we wrote them as polynomials in u_1, u_2, u_3 and thus in u_1, R. This yields the quadratic equation over $\mathbf{Z}[R, u_1]$ satisfied by u. We eliminated u_1 by multiplying this equation by its conjugate under the hyperelliptic involution $u_1 \leftrightarrow R^3 + R - 3 - u_1$, obtaining a polynomial relation between R and u of degree 24 in R and 4 in u. Substituting this into (131) and clearing the powers of $T^2 + 23$ in the denominator we found our desired polynomial of degree 24 giving Shih's cover $\mathrm{X}_0^{\mathrm{tw}}(161)/\mathrm{X}_0^{\mathrm{tw}}(7)$. We refrain from exhibiting this polynomial term by term, since the following display of the smaller polynomial equation relating R, u may already suffice to try the reader's patience:

$$\begin{gathered} (u^2 + 28u + 196)R^{24} + (-u^3 - 32u^2 - 326u - 1036)R^{23} \\ +(69u^2 + 1472u + 7613)R^{22} + (460u^2 + 10741u + 61272)R^{21} \\ +(23u^3 - 667u^2 - 27140u - 184529)R^{20} \\ +(-23u^3 + 2392u^2 + 69759u + 442566)R^{19} \end{gathered}$$

$$
\begin{aligned}
&+(23u^3+11914u^2+397187u+3274303)R^{18}\\
&+(-161u^3-25438u^2-777262u-6220166)R^{17}\\
&+(368u^3-6440u^2+523894u+9544655)R^{16}\\
&+(-529u^3+248676u^2+5396053u+25743072)R^{15}\\
&+(575u^3-628015u^2-13487798u-64815863)R^{14}\\
&+(-1610u^3+484334u^2+4711159u-34084068)R^{13}\\
&+(3036u^3+728341u^2+32792549u+333459911)R^{12}\\
&+(-2668u^3-2210346u^2-72707186u-618029274)R^{11}\\
&+(2300u^3+2772006u^2+75088698u+587040017)R^{10}\\
&+(-3542u^3-1548820u^2-45456257u-486831570)R^{9}\\
&+(5428u^3-644920u^2+17414726u+604311568)R^{8}\\
&+(-2599u^3+1455854u^2-3915704u-630498632)R^{7}\\
&+(-1748u^3-677304u^2-3213077u+372098876)R^{6}\\
&+(1265u^3-85744u^2+6552355u-99826532)R^{5}\\
&+(345u^3+239269u^2-4106857u+2861959)R^{4}\\
&+(-113436u^2+1074744u+1754532)R^{3}\\
&+(-598u^3+10442u^2-250010u+378166)R^{2}\\
&+(252u^3+3924u^2+59796u-171972)R+(u^2+18u+281)^2=0.
\end{aligned}
\tag{139}
$$

Substituting $u = 28t^2/(t^2+23)$ yields a $\mathrm{PSL}_2(\mathbf{F}_{23})$ extension of $\mathbf{Q}$ for almost all t (see [Se1, Ch.3] for the precise meaning of this "almost all"); more generally, for $c \in \mathbf{Q}^*$ taking $u = 28t^2/(t^2+23c)$ yields a polynomial whose splitting field is almost always a $\mathrm{PGL}_2(\mathbf{F}_{23})$ extension containing $\mathbf{Q}(\sqrt{c})$ as the subfield fixed by $\mathrm{PSL}_2(\mathbf{F}_{23})$.

Level 75:
Rational points on the modular curve $\mathrm{X}_0(75)/\langle w_5 \rangle$

In [Wil, T-W] it is shown that every semistable elliptic curve $E/\mathbf{Q}$ has a modular parametrization. A deep and difficult analysis of the representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on the 3^i- and 5^i-torsion points of E yields the result except when both $E[3]$ and $E[5]$ contain Galois-invariant proper subgroups, i.e. except for E admitting both a 3- and a 5-isogeny over $\mathbf{Q}$. But such a curve yields a rational point on the modular curve $\mathrm{X}_0(15)$. Fortunately it was already known that the curve $\mathrm{X}_0(15)$ is elliptic of rank zero, and of its eight torsion points four are cusps and the other four parametrize curves which were already known (as in the "remarks on isogenies" preceding the tables in [B-K]) to be modular — they are quadratic twists of the curves of conductor 50 — and at any rate not semistable.

While this result sufficed to prove Fermat's "Last Theorem" it is not fully satisfactory, since we would like to know that every $E/\mathbf{Q}$, semistable or not, has a modular parametrization. The hypothesis of semistability has not yet been removed entirely, but has been considerably weakened. At each step, as in the original Wiles-Taylor result, the representation theory was refined to deal with all E satisfying the hypothesis with the possible exception of curves with a special torsion structure. Such curves are parametrized by a modular curve, and one must compute that curve explicitly enough to determine all its rational points and the corresponding elliptic curves. Most recently, it was shown in [CDT] that E is modular provided its arithmetic conductor is not a multiple of 27 (this generalizes Wiles-Taylor because a semistable curve is one whose arithmetic conductor is squarefree). Here the exceptional curves were those E which admit a rational 3-isogeny as well as a rational pair of 5-isogenies. We shall see that these curves are parametrized by the modular curve $\mathrm{X}_0(75)/\langle w_5\rangle$, and compute equations for that curve from which we show that the only non-cuspidal point parametrizes 3-isogenies between curves both of which have j-invariant 0. Since these curves have complex multiplication, they are modular; this completes the proof of the result of [CDT].

Let E' be the curve 3-isogenous to E, and E_1, E_2 the pair of 5-isogenous curves. The images in E' of $\ker(E \to E_i)$ are a rational pair of 5-element subgroups, yielding a rational pair E'_1, E'_2 of curves 5-isogenous to E'. Then E_1, E'_2 are related by a cyclic 75-isogeny, as are E'_1, E_2; these isogenies yield a rational pair of points on $\mathrm{X}_0(75)$ permuted by the involution w_5. Thus the curve E yields a rational non-cusp point on the quotient curve $\mathrm{X}_0(75)/\langle w_5\rangle$. We readily find (or look up in the tables of [B-K]) that this curve has genus 3, and thus only finitely many rational points by Mordell-Faltings. In general we do not know how to provably list all the rational points of a given curve of genus > 1; but for our curve the Jacobian fortunately decomposes up to isogeny as the product of three elliptic curves each of which has rank 0. Thus we can find all the rational points among the preimages of the finitely many rational points on one of these curves under a nonconstant rational map from $\mathrm{X}_0(75)/\langle w_5\rangle$. We shall use the quotient map to $\mathrm{X}_0^{++}(75) = \mathrm{X}_0(75)/\langle w_3, w_5\rangle$. To carry out this computation we must first find explicit equations for $\mathrm{X}_0(75)/\langle w_5\rangle$ and the action of w_3 on this curve.

We begin by finding a basis for the holomorphic differentials on this curve, i.e. the weight-2 cusp forms on $\mathrm{X}_0(75)$ invariant under w_5. Since the level 75 is no longer squarefree we face new difficulties, since there are several kinds of cusps and we must ensure that our forms vanish on all of them. (Warning: the cusps not in the $\langle w_3, w_5\rangle$ orbit of the cusp at infinity are not rational over $\mathbf{Q}$.) However we also have a new tool: the quadratic twist Q_5, taking a cusp form $f(q) = \sum_{n=1}^{\infty} c_n q^n$ to the cusp form

$$Q_5 f(q) = \frac{1}{\sqrt{5}} \sum_{j=1}^{4} \chi_5(j) f(e^{2\pi i j/5} q) = \sum_{n=1}^{\infty} \chi_5(n) c_n q^n, \tag{140}$$

where χ_5 is the Dirichlet character $(\cdot/5)$. We have $Q_5 w_3^* = -w_3^* Q_5$, so Q_5 takes w_3-invariant forms to anti-invariant ones and vice versa. We can also use the weight-2 cusp form

$$\phi_{15}(q) = \eta(q)\eta(q^3)\eta(q^5)\eta(q^{15}) = q - q^2 - q^3 - q^4 + q^5 + q^6 + 3q^8 \cdots \tag{141}$$

on $\mathrm{X}_0(15)$, anti-invariant under w_5, to obtain the w_5-invariant "old" cuspform

$$f_1(q) = \phi_{15}(q) - 5\phi_{15}(q^5) = q - q^2 - q^3 - q^4 - 4q^5 + q^6 + 3q^8 \cdots . \tag{142}$$

Since ϕ_{15} is w_3-invariant, so is f_1, which thus generates the one-dimensional space of cuspforms on the elliptic curve $\mathrm{X}_0^{++}(75)$. By twisting f_1 we obtain the modular form

$$f_2(q) = Q_5 f_1(q) = q + q^2 + q^3 - q^4 + q^6 - 3q^8 \cdots \tag{143}$$

associated to the elliptic curves in the isogeny class numbered 75-B in [Cre] such as the $\mathbf{Q}(\sqrt{5})$-twists of the elliptic curve $\mathrm{X}_0(15)$. This is anti-invariant under w_3, but turns out to still be w_5-invariant and thus a cusp form on $\mathrm{X}_0(75)/\langle w_5 \rangle$. The third eigenform

$$f_3(q) = q - 2q^2 + q^3 + 2q^4 - 2q^6 + 3q^7 + q^9 + 2q^11 \cdots , \tag{144}$$

associated to the isogeny class 75-C, is somewhat trickier to obtain. Of course we could read it off the tables, or recover it from the reductions mod l of the 75-C curves, but the former method implicitly relies on modular symbol or trace formula computations, and the latter requires an explicit Weierstrass equation for one of these curves, which until we exhibit equations for $\mathrm{X}_0(75)/\langle w_5 \rangle$ must be found by the intricate methods described in [Cre]. Instead we obtain f_3 from the theta series

$$\begin{aligned} \vartheta(q) &= 1 + 2q + 2q^4 + 2q^9 + 2q^{16} + 4q^{19} + 4q^{21} + 6q^{25} + 4q^{31} + 2q^{36} + \cdots , \\ \vartheta'(q) &= 1 + 2q^3 + 4q^7 + 2q^{12} + 4q^{13} + 6q^{25} + 2q^{27} + 4q^{28} + 4q^{37} + \cdots \end{aligned} \tag{145}$$

of the quadratic forms $(1,1,19)$, $(3,3,7)$ of discriminant -75. We cannot blithely take the difference between them as we did in level 191, because these forms are of different genera and thus take equal but opposite values at some cusps, so $\vartheta - \vartheta'$ is not a cusp form. However, the weight-2 form $\vartheta^2 - \vartheta'^2$ does vanish at all cusps, and we find

$$f_3 = \frac{1}{2}\left[\frac{3}{4} Q_5 (\vartheta^2 - \vartheta'^2) - f_2\right]. \tag{146}$$

The forms f_2, f_3 are a basis for the space of cuspforms on $\mathrm{X}_0(75)/\langle w_5 \rangle$ anti-invariant under w_3.

We readily check that f_1, f_2, f_3 do not satisfy a quadratic relation. Since the genus-3 curve $\mathrm{X}_0(75)/\langle w_5 \rangle$ is thus not hyperelliptic, it is a nonsingular quartic in $\mathbf{P}^2$, with projective coordinates $(f_1 : f_2 : f_3)$; moreover, the curve, and thus also the homogeneous quartic satisfied by f_1, f_2, f_3, is symmetrical under the involution $f_1 \leftrightarrow -f_1$ coming from w_3. We could determine this quartic directly by matching q-expansion coefficients, but it is more convenient to exploit the w_3 symmetry. Thus

$$z = \frac{3f_2}{f_2 - f_3} = q^{-1} + 1 + 2q + q^3 + q^4 + q^5 + q^6 + 3q^7 + \cdots \tag{147}$$

is a rational function of degree 4 on $\mathrm{X}_0(75)/\langle w_5\rangle$ invariant under w_3, and thus of degree 2 on the quotient curve $\mathrm{X}_0^{++}(75)$, with one pole at the infinite cusp. As we did for $\mathrm{X}_0^{+}(37)$, we use z and f_1 to obtain the functions

$$x = \frac{1}{2}\left(z^2 - z - \frac{q\,dz/dq}{f_1}\right) - 1 = q^{-2} + q^{-1} + 1 + 2q + 5q^2 + 4q^3 + 6q^4 + \cdots, \tag{148}$$

$$y = -\frac{1}{2}\left(x + 1 + \frac{q\,dx/dq}{f_1}\right) = q^{-3} + q^{-2} + 2q^{-1} + 3 + 6q + 10q^2 + 18q^3 + \cdots \tag{149}$$

of degrees 2, 3 with double and triple pole at the cusp, and find a Weierstrass equation

$$y^2 + xy + y = x^3 + x^2 - 5x + 2 \tag{150}$$

for $\mathrm{X}_0^{++}(75)$, which we recognize as elliptic curve #15-A3 (15-B). [An equation with even smaller coefficients $Y^2 + XY = X^3 + 4X^2 + X$ is satisfied by $(X, Y) = (x - 1, y + 1)$.] In these coordinates we have $z = (x + y)/(x - 1)$. The function field of $\mathrm{X}_0(75)/\langle w_5\rangle$ is then obtained from that of $\mathrm{X}_0^{++}(75)$ by adjoining the function

$$v = \frac{3f_1}{f_2 - f_3} = q^{-1} - 1 - 2q^2 - 5q^3 + q^4 - 5q^5 + 5q^6 - q^7 + 3q^8 \cdots \tag{151}$$

anti-invariant under w_3. To relate v to x, y we note that v^2 is a rational function of x, y with poles only at the poles of z, so we may compare q-expansions to find

$$v^2 = \frac{x^2 - 3y - x - 14}{x - 1}. \tag{152}$$

Now the elliptic curve (150) has eight rational points, generated by the 2-torsion point $(x, y) = (-3, 1)$ and the 4-torsion point $(0, 1)$. It remains only to find which of these lifts to a rational point on $\mathrm{X}_0(75)/\langle w_5\rangle$. The origin $(x : y : 1) = (0 : 1 : 0)$ lifts to a pair of rational points, but these are cusps. The 2-torsion point $(1, -1)$ is a double pole of v^2 at which $((2y + x + 1)v)^2$ takes the value -44; thus it lies under two irrational points of $\mathrm{X}_0(75)/\langle w_5\rangle$. The 4-torsion point $(2, -4)$ is a simple zero of v^2 and thus lies under a rational point of $\mathrm{X}_0(75)/\langle w_5\rangle$ fixed under w_3, at which we compute $j(E) = j(E') = 0$. At the remaining five points

$$(0,1), \quad (0,-2), \quad (2,1), \quad (-3,1), \quad (3/4, -7/8), \tag{153}$$

we have $v^2 = 17, 8, -15, 5/4, 185/4$ respectively, none of which is a square. Thus as claimed the CM point above $(2, -4)$ is the only finite rational point of $\mathrm{X}_0(75)/\langle w_5 \rangle$.

We remark that of the seven finite rational points of $\mathrm{X}_0(75)/\langle w_5 \rangle$, all but the non-integral $(3/4, -7/8)$ are CM points. We saw this already for $(2, -4)$. At the point $(1, -1)$, the six curves E, E_i, E', E_i' all have j-invariant -2^{15}: these are CM curves with endomorphism ring $\mathbf{Z}[(1+\sqrt{-11})/2]$, and the isogenies of degree $3, 5$ are $\pm(1 \pm \sqrt{-11})/2$, $\pm(3 \pm \sqrt{-11})/2$. Each of these is only defined over $\mathbf{Q}(\sqrt{-11})$, but the six-curve configuration modulo $\langle w_3, w_5 \rangle$ is rational. At the points $(0, -2)$ and $(0, 1)$ the CM rings have discriminant -24, -51 respectively. Each of these rings has class number 2 with the nontrivial class represented by the ideal above the ramified prime 3. There are thus two CM j-invariants, with the corresponding curves E, E' related by a 3-isogeny. Since in both cases the prime 5 is split we also have a pair of 5-isogenies between E, E', so may take $E_i = E'$ and $E_i' = E$ to obtain a rational point of $\mathrm{X}_0^{++}(75)$.

Finally the points $(2, 1)$ and $(-3, 1)$ again yield $j(E) = j(E') = 0$. The existence of three rational points on $\mathrm{X}_0^{++}(75)$ with the same $j(E), j(E')$ may appear surprising; we explain it as follows. Given E, E', we specify E_1, E_2 by choosing a pair of distinct 5-element subgroups G_1, G_2 of E, up to the $\boldsymbol{\mu}_3$ automorphisms of E. Note that E has six 5-element subgroups, constituting a principal homogeneous space (PHS) for $\mathbf{F}_{25}^*/\mathbf{F}_5^* \cong \mathbf{Z}/6\mathbf{Z}$; $\boldsymbol{\mu}_3$ and multiplication by $\sqrt{-3}$ act by translation by $2\mathbf{Z}/6\mathbf{Z}$ and $(3 \bmod 6)$ respectively. Now a pair $\{G_1, G_2\}$ in that PHS may differ by 1, 2, or 3, canonically characterized as 6-, 3- and 2-torsion elements of $\mathbf{Z}/6\mathbf{Z}$. (The difference between a *non-ordered* pair of PHS elements is only defined up to sign.) We noted already that pairs related by $\boldsymbol{\mu}_3$, i.e. by translation by even integers, yield the same point on $\mathrm{X}_0(75)/\langle w_5 \rangle$. Since the 3-isogeny $E \to E' (\cong E)$ is multiplication by $\sqrt{-3}$, the involution w_3 acts on these points by translation by 3. Thus a rational point on $\mathrm{X}_0^{++}(75)$ with $j(E) = j(E') = 0$ is tantamount to an orbit of pairs $\{G_1, G_2\}$ under $\mathbf{Z}/6\mathbf{Z}$ translation. But this in turn is equivalent to the distance between G_1, G_2, which is a nonzero element of $\mathbf{Z}/6\mathbf{Z}$ up to sign, and noted already that there are three of these, each characterized in terms of the abstract group structure of $\mathbf{Z}/6\mathbf{Z}$. Thus there are three such points on $\mathrm{X}_0^{++}(75)$, and all are rational as claimed. But on $\mathrm{X}_0(75)/\langle w_5 \rangle$ a point with $j(E) = j(E') = 0$ is an orbit of pairs under translations only by $2\mathbf{Z}/6\mathbf{Z}$, and of the five such orbits only one is canonically characterized: the orbit of pairs related by translation by 3 mod 6, which is actually stable under w_3. This explains why only one of the three $j(E) = j(E') = 0$ points on $\mathrm{X}_0^{++}(75)$ lifts to a rational point on $\mathrm{X}_0(75)/\langle w_5 \rangle$ and that one is a fixed point of w_3.

[All these CM points on the elliptic curve $\mathrm{X}_0^{++}(75)$ were located by transcendental methods, though not the same ones we used for $\mathrm{X}_0^{+}(191)$ and $\mathrm{X}_0^{+}(239)$: for variety's sake, we instead integrated the oldform $dx/(2y + x + 1) = -f_1 dq/q$ (see (142)) termwise from $i\infty$ to each CM point to obtain its $\mathbf{C}/\Lambda$ coordinate, and evaluated the $\wp$ function and its derivative there to recover (x, y); since this was already known to lie in the finite list of eight rational points we did not then need to resort to methods such as described in [El4] to recognize x, y as rational numbers. For instance $\tau = 1/10 + \sqrt{-3}/30$, $\tau = 3/10 + \sqrt{-3}/30$, and $\tau = 1/2 + \sqrt{-3}/30$ yield the points $(2, 1)$, $(-3, 1)$, $(2, -4)$ respectively.]

Acknowledgements

The great debt this paper owes to Atkin has already been noted in the Introduction. In addition I am grateful to H. Cohen, B.H. Gross, J. Harris, B. Mazur, F. Morain, V. Miller, B. Poonen, R. Schoof, A. Stein, and J. Teitelbaum for helpful discussions and/or pointers to relevant literature. Symbolic, numerical and elliptic-curve computations were greatly assisted by the GP/PARI and MACSYMA packages.

The research reported herein was done intermittently over a period of roughly ten years during which I was variously supported by grants and fellowships from the National Science Foundation, the Putnam family, the Harvard Society of Fellows, and the Packard Foundation.

References

[AH] Adleman, L.M., Huang, M.-D.: *Primality Testing and Abelian Varieties over Finite Fields.* Berlin: Springer, 1992 (LNM 1512).

[B-K] Birch, B.J., Kuyk, W., ed.: *Modular Functions of One Variable IV.* Lect. Notes in Math. **476**, 1975.

[Can] Cantor, D.G.: On the analogue of the division polynomials for hyperelliptic curves, *J. reine angew. Math.* **447** (1994), 91–145.

[CDT] Conrad, B., Diamond, F., Taylor, R.: Modularity of certain potentially crystalline Galois representations. Preprint, 1997.

[C-M] Couveignes, J.-M., Morain, F.: Schoof's algorithm and isogeny cycles. Pages 43–58 in *Algorithmic Number Theory* (Proceedings of ANTS-I; L.M. Adleman, M.-D. Huang, eds.; Berlin: Springer, 1994; Lecture Notes in Computer Science 877).

[Co1] Cohen, H.: *A Course in Computational Algebraic Number Theory.* Berlin: Springer, 1993 (GTM 138).

[C-L] Cohen, H., Lenstra, H.W.: Heuristics on class groups of number fields. Pages 33–62 of *Number Theory* (Proceedings of Journées Arithmétiques 1983, Noordwijkerhout; H. Jager, ed.; Berlin: Springer, 1984 (LNM 1068)).

[Co2] Cohen, P.: On the coefficients of the transformation polynomials for the elliptic modular function, *Math. Proc. Cambridge Philos. Soc.* **95** (1984), 389–402.

[Cre] Cremona, J.E.: *Algorithms for modular elliptic curves.* Cambridge University Press, 1992.

[Dan] Danilov, L.V.: The Diophantine equation $x^3 - y^2 = k$ and Hall's conjecture, *Math. Notes Acad. Sci. USSR* **32** (1982), 617–618.

[Del] Deligne, P.: La conjecture de Weil pour les surfaces $K3$, *Inv. Math.* **15**, 206–226 (1972).

[DR] Deligne, P., Rapoport, M.: Les schémas de modules de courbes elliptiques. Pages 143–316 of *Modular Functions of One Variable II* (P. Deligne, W. Kuyk, eds.), Lect. Notes in Math. **349**, 1972.

[Dew] Dewaghe, L.: Remarques sur l'algorithme SEA. *Math. of Computation*, to appear.

[El1] Elkies, N.D.: The automorphism group of the modular curve $\mathrm{X}_0(63)$, *Compositio Math.* **74** (1990), 203–208.

[El2] Elkies, N.D.: Explicit isogenies. Manuscript, 1992.

[El3] Elkies, N.D.: Remarks on elliptic K-curves. Manuscript, 1994.

[El4] Elkies, N.D.: Heegner point computations. Pages 122–133 in *Algorithmic Number Theory* (Proceedings of ANTS-I; L.M. Adleman, M.-D. Huang, eds.; Berlin: Springer, 1994; Lecture Notes in Computer Science 877).

[G-K] Goldwasser, S., Kilian, J.: Almost all primes can be quickly certified. Pages 316–329 of *Proceedings of the 18th Annual Symposium on Theory of Computing* (New York: Association for Computing Machinery, 1986).

[Gro] Gross, B.H.: Heights and the Special Values of L-series. Pages 115–187 in *Number Theory* (Proceedings of 1985 Montreal conference; H. Kisilevsky, J.Labute, eds.; Canadian Math. Society, 1987).

[G-Z] Gross, B.H., Zagier, D.: On singular moduli, *J. reine angew. Math.* **335**, 191–220 (1985).

[Hal] Hall, M.: The Diophantine equation $x^3 - y^2 = k$. In *Computers in Number Theory* (A. Atkin, B. Birch, eds.; Academic Press, 1971).

[H-M] Horrocks, G., Mumford, D.: A rank 2 vector bundle on $\mathbf{P}^4$ with 15,000 symmetries, *Topology* **12** (1973), 63–81.

[H-I] Huang, M.-D., Ierardi, D.: Counting rational points on curves over finite fields, *IEEE Symposium on the Foundations of Computer Science*, Palo Alto, CA, November 1993.

[K-Z] Kaneko, M., Zagier, D.: Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials. Pages ??–?? in Atkin conference proceedings

[Kn-2] Knuth, D.E.: *The Art of Computer Programming, Vol. 2: Seminumerical algorithms*, 2nd ed. Reading (Mass.): Addison-Wesley, 1981.

[Kn-3] Knuth, D.E.: *The Art of Computer Programming, Vol. 3: Sorting and Searching*. Reading (Mass.): Addison-Wesley, 1973.

[Lan] Lang, S.: Old and new conjectured diophantine inequalities, *Bull. Amer. Math. Soc.* **23** (1990), 37–75.

[Ler] Lercier, R.: Computing isogenies in $F(2^n)$. Pages 197–212 in *Algorithmic Number Theory: Second International Symposium* (Proceedings of ANTS-II; H. Cohen, ed.; Berlin: Springer, 1996; Lecture Notes in Computer Science 1122).

[Lig] Ligozat, E.: Courbes Modulaires de Genre 1, *Mém. Soc. Math. de France* **43** (1975).

[Mat] Matzat, B.H.: *Konstruktive Galoistheorie.* Lect. Notes Math. **1284**, 1987.

[M-SD] Mazur, B., Swinnerton-Dyer, H.P.F.: Arithmetic of Weil Curves, *Inv. Math.* **25**, 1–61 (1974).

[Mor] Morain, F.: Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques, *J. Th. des Nombres de Bordeaux* **7** (1995), 255–282.

[Ogg] Ogg, A.P.: Hyperelliptic modular curves, *Bull. Soc. Math. France* **102** (1974), 449–462.

[PTV] Peters, C., Top, J., van der Vlugt, M.: The Hasse zeta function of a K3 surface related to the number of words of weight 5 in the Melas codes, *J. reine angew. Math.* **432**, 151–176 (1992).

[Pil] Pila, J.: Frobenius maps of abelian varieties and finding roots of unity in finite fields, *Math. of Comp.* **55**, 745–763 (1990).

[Poh] Pohst, M.: Berechnung kleiner Diskriminanten total reeller algebraischen Zahlkörper, *J. reine angew. Math.* **278/279** (1975), 278–300.

[Pol] Pollard, J.M.: Monte Carlo Methods for Index Computation (mod p), *Math. of Comp.* **32**, 918–924 (1978).

[Poo] Poonen, B.: Computational aspects of curves of genus at least 2. Pages 283–306 in *Algorithmic Number Theory: Second International Symposium* (Proceedings of ANTS-II; H. Cohen, ed.; Berlin: Springer, 1996; Lecture Notes in Computer Science 1122).

[Rib] Ribet, K.A.: Abelian varieties over **Q** and modular forms. CPAM preprint, Berkeley 9/92. Also in 1992 Proceedings of KAIST Mathematics Workshop (Taejon: Korea Advanced Institute of Science and Technology), 53–79.

[Sc1] Schoof, R.: Elliptic curves over finite fields and the computation of square roots mod p, *Math. of Comp.* **44**, 483–494 (1985).

[Sc2] Schoof, R.: Counting points on elliptic curves over finite fields, *J. Th. des Nombres de Bordeaux* **7** (1995), 219–254.

[Se1] Serre, J.-P.: *Topics in Galois Theory.* Boston: Jones and Bartlett, 1992.

[Se2] Serre, J.-P.: *Oeuvres III.* Springer: Berlin 1986.

[Sha] Shanks, D.: The Infrastructure of a real quadratic field and its applications, *Proc. 1972 number theory conference, Boulder*, 217–224.

[Sh1] Shih, K-y.: On the construction of Galois extensions of function fields and number fields, *Math. Ann.* **207** (1974), 99–120.

[Sh2] Shih, K-y.: p-division points on certain elliptic curves, *Compositio Math.* **36** (1978), 113–129.

[Sil] Silverman, J.: *The Arithmetic of Elliptic Curves.* New York: Springer, 1985 (GTM 106).

[S-W] Stein, A., Williams, H.C.: Baby Step Giant Step in Real Quadratic Function Fields, *Math. of Computation*, to appear.

[SD] Swinnerton-Dyer, H.P.F.: An Application of Computing to Class Field Theory. Chapter XII (pages 280–291) in *Algebraic number theory* (J.W.S. Cassels, A. Frohlich, eds.; London: Academic Press, 1967).

[T-W] Taylor, R., Wiles, A.: Ring-theoretic properties of certain Hecke algebras, *Ann. of Math. (2)* **141** (1995), #3, 553–572.

[Vél] Vélu, Isogénies entre courbes elliptiques, *Comptes Rendus Acad. Sci. Paris* A **273** (July 1971), 238–241.

[Vol] Volcheck, E.: Computing in the Jacobian of a plane algebraic curve. Pages 221–233 in *Algorithmic Number Theory* (Proceedings of ANTS-I; L.M. Adleman, M.-D. Huang, eds.; Berlin: Springer, 1994; Lecture Notes in Computer Science 877).

[Wei] Weil, A.: Abstract versus classical algebraic geometry. Pages 550–558 of *Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, Vol. III.*

[Wil] Wiles, A.: Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)* **141** (1995), #3, 443–551.

[Yu] Yu, J.-K.: On some congruences of modular polynomials. Preprint, 1997.