The Method of Graphs. Examples and Applications

J.-F. Mestre.
Tr. Andrei Jorza

February 18, 2004

1 Introduction

Let $S_k(N,\varepsilon)$ be the space of cusp forms of weight k, level N and character ε, where k and N are integers ≥ 1, and ε is a Dirichlet character N. There are several ways to construct a basis. For example one can use Selberg's trace formula. Denote by $\mathrm{Tr}(n)$ the trace of T_n, the n-th Hecke operator. The function

$$f = \sum_{n=1}^{\infty} \mathrm{Tr}(n) q^n$$

is in $S_k(N,\varepsilon)$. The set of $f_i = T_i f$ generate this space, and this theoretically allows us to construct a basis. For example, if N is prime, $\varepsilon = 1$ and $k = 2$, then the set of the f_i ($1 \leq i \leq g$ where g is the genus of $X_0(N)$) is a basis of $S_2(N,1)$.

But, even in that case, which is the most favorable, the computations become hard: on an average computer we can only hope to treat N of the size of 5000 (always with N prime, weight 2 and trivial character); actually, the computation of $\mathrm{Tr}(n)$ requires the knowledge of many class numbers of imaginary quadratic fields of discriminant of order at most n and to obtain a basis $f_1, f_2, \ldots, f_g$ one needs to compute $\mathrm{Tr}(n)$ for $n \leq g^2$.

In the following section we describe the "method of graphs", which relies on the results of Deuring and Eichler, and developed by J. Oestrlé and myself, which allows us to obtain a basis for $S_2(N,1)$ more quickly (at least when N is a prime).

In the second section, we indicate how this method allows us to prove that certain elliptic curves defined over $\mathbf{Q}$ are Weil curves[1] (which, by providing an adequate Weil curve, yields all the imaginary quadratic fields of class number at most 3, due to a result of Goldfeld and recent works of Gross and Zagier).

The third section is dedicated to the verification of a conjecture of Serre in certain particular cases; this is possible because of the method described in the first section. It is known that this conjecture, if it is true, has numerous consequences (e.g., the Shimura-Taniyama-Weil conjecture, and thus Fermat's Last Theorem).

[1] It is now a theorem that every elliptic curve is a Weil curve, i.e., the Shimura-Taniyama-Weil conjecture is true. – William Stein

2 The method of graphs

2.1 Definitions and notations

In the following p is a prime number and N_1 is a positive integer coprime to p. Set $N = pN_1$.

Let

$$M_N = \oplus_S \mathbf{Z}[S]$$

where S is taken over all supersingular points of $X_0(N_1)$ in characteristic p, i.e., over the set of isomorphism classes of pairs (E, C) consisting of an elliptic curve E defined over $\overline{\mathbb{F}}_p$ and a cyclic group C of E of order N_1. Two such pairs are identified if they are, in the obvious sense, $\overline{\mathbb{F}}_p$-isomorphic.

Let

$$\alpha_S = \frac{|\operatorname{Aut}(S)|}{2},$$

where $\operatorname{Aut}(S)$ is the group of $\overline{\mathbb{F}}_p$-automorphisms of S. We always have $\alpha_S \leq 12$, and if p does not divide 6 then $\alpha_S \leq 3$.

Therefore we can define a scalar product on M_N by $\langle S, S\rangle = \alpha_S$ and $\langle S, S'\rangle = 0$ if $S \neq S'$. Let $\mathrm{Eis} = \sum \alpha_S^{-1}[S]$ and let

$$M_N^0 = \left\{\sum x_S[S] : \sum x_S = 0\right\}$$

be the subspace orthogonal to Eis.

For all integers $n \geq 1$ coprime with p we define an operator T_n on M by

$$T_n(E, C) = \sum_{C_n} (E/C_n, (C + C_n)/C_n)$$

where C_n runs over all the cyclic subgroups of order n such that $C \cap C_n = 0$.

For all $q \mid N_1$ and coprime with $q' = N_1/q$, we define the same way the Atkin-Lehner involutions W_q by

$$W_q(E, C) = (E/q'C, (E_q + C)/q'C),$$

where E_q is the group of points of order dividing q of E.

Finally we define an involution W_p by $W_p = -\operatorname{Frob}_p$, where Frob_p is the endomorphism of M_N that transforms (E, C) to (E^p, C^p). (The fact that it is an involution reflects that the supersingular points are defined over $\mathbb{F}_{p^2}$.)

These operators have the following properties: the set of W_q and T_n (n coprime with N) generate an abelian semigroup of hermitian operators with respect to the scalar product $\langle \cdot, \cdot \rangle$. The T_n commute with each other for all n coprime to p. If $q = q_1 q_2$ (q_1, q_2 coprime) and if $n = n_1 n_2$ (n_1, n_2 coprime with each other and with p) then $W_q = W_{q_1} W_{q_2}$ and $T_n = T_{n_1} T_{n_2}$.

For all $d \mid N_1$ we have a homomorphism $\phi_d : M_N \longrightarrow M_{N/d}$ that transforms (E, C) to (E, dC). This homomorphism commutes with T_n (n coprime with N), and with W_q (for $q \mid N/d$). For $d \mid N_1$ and coprime with N_1/d we have

$$T_d \phi_d = \phi_d (T_d + W_d)$$

2.2 An isomorphism with $S_2(N)$

We consider here the space $S_2(N)$ of cusp forms of weight 2 over $\Gamma_0(N)$, with its natural structure of $\mathbf{T}$-module, where $\mathbf{T}$ is the Hecke algebra [?].

Theorem 2.1. *There exists an isomorphism compatible with the action of the Hecke operators, between $M_N^0 \otimes \mathbf{C}$ and the subspace of $S_2(N)$ generated by the newforms of level N and oldforms coming from the cusp forms of weight 2 and level pd, $d \mid N_1$.*

Remark 2.2. Assume N (or without loss N_1) is square-free. We can determine efficiently the subspace M_N^0 corresponding to newforms in $S_2(N)$; it is the subspace formed by all x so that for all divisors d of N_1 we have

$$\phi_d(x) = \phi_d(W_d(x)) = 0.$$

In particular if $N = pq$, q prime, it is the subspace of M_{pq} intersection of the kernel of ϕ_q and of $\phi_q W_q$.

2.3 Relation to the quaternion algebra

The matrices of the operators T_n acting on M_N are the same as the classical Brandt matrices [?], constructed using quaternion algebras.

Let $B_{p,\infty}$ be the quaternion algebra over $\mathbf{Q}$ ramified exactly at p and infinity, and let $\mathcal{O}$ is an Eichler order of level N_1 (defined by Eichler [?] in the case when N_1 is square-free, and defined in general by Pizer [?]), and let $I_1, I_2, \ldots, I_h$ be representatives of the left ideal classes of $\mathcal{O}$.

Let $\mathcal{O}_i$ be the right order (i.e., right normalizers) of the ideals I_i, and e_i be the number of units of $\mathcal{O}_i$. The Brandt matrix $B(n) = (b_{i,j}^{(n)})$ has i, j entry

$$b_{i,j}^{(n)} = e_j^{-1} \cdot |\{\alpha : \alpha \in I_j^{-1} I_i,\ \mathrm{Nor}(\alpha)\,\mathrm{Nor}(I_j)/\,\mathrm{Nor}(I_i) = n\}|$$

where Nor is the norm over $B_{p,\infty}$ (the norm of an ideal being the gcd of the norms of its nonzero elements).

In the language of supersingular curves of characteristic p, we may give these matrices (actually their transposes) the following interpretation:

Let S be a supersingular point as in I.1, i.e., a supersingular elliptic curve E defined over $\overline{\mathbb{F}}_p$ together with a cyclic group C of order N_1. The ring of endomorphisms $\mathcal{O}_1$ of S is an Eichler order of level N_1. To all the other supersingular points $S' = (E', C')$ we associate the set $I_{S,S'}$ of homomorphisms from S to S', i.e. the set of all homomorphisms α from E to E' that send C to C'. This is obviously a left ideal over $\mathcal{O}_1$, and its inverse ideal is $I_{S',S}$. We can prove that all the right ideals of $\mathcal{O}_1$ are obtained in this way, and the whole Eichler order of level N_1 if the rign of endomorphisms of a supersingular point S. It is clear that the general term $B_{i,j}^{(n)}$ of the n-th Brandt matrix is the number of isogenies of S_i to S_j (the supersingular points being conveniently indexed,) two such isogenies being identified is different by an automorphism of S_j. We can retrieve the matrix of the operator T_n acting over M_n.

On the other hand if for all pairs of supersingular points (S, S') we associate the function

$$\theta_{S,S'}(q) = \sum_{\alpha} q^{\deg \alpha}$$

where α goes through all the homomorphisms of S to S', we retrieve the functions θ classically associated with the ideals of the orders of the quaternions, or, if one prefers, associated with the positive integer quadratic forms in 4 variables.

It is therefore easy to prove that if $\sum x_S[S]$ is an elements of $M_N \otimes \mathbf{C}$ eigenvector of all the Hecke operators and if $f(q)$ is the corresponding modular form, we have, for all S'

$$x_{S'} f(q) = \sum_{S} x_S \theta_{S,S'}$$

which allows, in theory, to find the coefficients a_n of f, using the x_S. In practice, unfortunately, the computation of a_n demands the knowledge of all the isogenies of degree n to S', and there doesn't seem to be a simple algorithm for that.

Nevertheless, in certain cases, there exists a different method to calculate the coefficients of f, which is easy as far as computation is concerned. Suppose that N is a prime (thus equal to p), or N is a product of primes pq and $X_0(q)$ is of genus 0 (thus $q = 2, 3, 5, 7$ or 13).

In the appendix, we give for each such case an equation of $X_0(q)$ of the form $xy = p^k$, thus the action of the Hecke operators T_2 and T_3 over $X_0(q)$, which is given by an equation much simpler than the equation of modular polynomials $\Phi_2(j, j'), \Phi_3(j, j')$ (which give the action of T_2, T_3 on $X_0(1)$, parametrized by the modular invariant j; cf. section 2.4).

Let $u = x$ if $N = pq$ and $u = j$ if $N = p$. The Fourier expansion of u at infinity is $1/q + \cdots$. Let $f(q) = \sum a_n q^n$ a normalized newform of level N and weight 2 corresponding to a vector $\sum x_S[S]$ of $M_N^0 \otimes K$, where K is the extension of $\mathbf{Q}$ generated by the a_n. Therefore there exists a prime ideal $\wp$ of K over p so that

$$\left(\sum x_S \cdot u(S)\right) f(q) \frac{dq}{q} \equiv \sum x_S \frac{du}{u - u(S)} \pmod{\wp}. \tag{1}$$

(it is about the congruence between Laurent series in q).

Suppose for example that f corresponds to a Weil curve of conductor N, so that a_n are in $\mathbf{Z}$. The x_S are in $\mathbf{Z}$ and one can prove that $\sum x_S u(S) \neq 0$. Thus we know $a_n \text{mod } p$ for all n. Hasse's inequality $|a_l| < 2\sqrt{l}$ for l prime proves that we know the a_n for $n < p^2/16$.

2.4 Explicit construction of the net M_N

In this section we suppose that N is odd. Suppose that given an explicit model of the curve $X_0(N_1)$, and so the action of the Hecke operator T_2 on that model (cf. Appedix).

First we need to find a supersingular points. Note that they are defined over $\mathbb{F}_{p^2}$. For example suppose that $N = p$. First we check to see if p is inert in one of the 9 imaginary quadratic fields of class number 1. If yes, then one can take for the initial value of j the modular invariant of the curve of complex multiplication by the ring of integers of corresponding fields. If not, one can know a list of minimal polynomials of modular invariants of elliptic curves of complex multiplication by imaginary quadratic fields of small class numbers, and apply the same method. One needs here to solve over $\mathbb{F}_{p^2}$ a polynomial equation, which can be done in $\log p$ operations – at least probabilistically. Finally suppose that all these attempts fail. There remains the possibility to enumerate all the values of $\mathbb{F}_p$ until finding a supersingular value. We know there must exist a supersingular j-invariant in $\mathbb{F}_p$, but unfortunately only a very small number—on the order of the size of the class group of $\mathbf{Q}(\sqrt{-p})$, or approximately $\sqrt{p}$.

So assume we know a supersingular point S_1. Knowing the action of T_2 on the model given by $X_0(N)$ allows us to obtain the three supersingular points S_2, S_3, S_4 (not necessarily distinct) related to S_1 by a 2-isogeny. It comes down to solving a degree 3 polynomial over $\mathbb{F}_{p^2}$, which needs extracting cubic and square roots, operations that need $O(\log p)$ operations. Sometimes we may as well exlude this computation. Suppose that $n = p$ and that we have, say $p \equiv 2(\text{mod } 3)$. Thus p is inert in $\mathbf{Q}(\sqrt{-3})$, so $j = 0$ is a supersingular value, and we know that the three isogenies of degree 2 send the curve of the invariant to the curve of complex multiplication by $\mathbf{Z}[\sqrt{-3}]$, for which the invariant is $j = 54000$.

In any case, we have at most one time when we need to solve a 3rd degree equation: once S_2 is known, we search from S_i $(i \geq 2)$ the three supersingular points which are related, but we already know one, so we only need to solve a second degree equation, which comes down to square roots over $\mathbb{F}_{p^2}$ which is fast (probabilistic methods require $O(\log p)$ operations using an algorithm that is very simple to implement).

To prove that we can find, step by step, all the supersingular points of M_N it is enough to prove that the graph of T_2 (and more generally of T_n) is connected. But, as Serre remarked, the eigenvalue $a_2 = 3$ of T_2 over M_N has multiplicity equal to the number of connected components of the graph of T_2. But in M_N, the space M_N^0 corresponding to the cusp forms of codimension 1, so 3 is a simple eigenvalue in M_N (because for a cusp form we have $|a_2| < 2\sqrt{2}$), so the graph of T_2 is connected.

In conclusion, an algorithm in $O(N \log N)$ operations gives all the supersingular points and the Brandt matrix B_2 associated to them. One of the advantages of this matrix is that it is very sparse; on each line and column there are at most 3 nonzero terms, which are integers whose sum is 3. This allows, given an eigenvalue, to find very quickly, if N is large, the corresponding eigenvectors.

2.5 Examples

1. Take for example $N = p = 37$. Since 37 is inert in $\mathbf{Q}(\sqrt{-2})$, one can take as the first vertex of our graph the curve E_1 of complex multiplications by $\mathbf{Z}[\sqrt{-2}]$, for which the modular invariant is $j_1 = 8000 \equiv 8 \text{mod } 37$. We need to find now all the invariants of curves 2-isogenous to this, i.e., to solve the equation $\Phi_2(x, 8000) \equiv 0(\text{mod } 37)$. But $\sqrt{-2}$ is an endomorphism of degree 2 of E_1, so j_1 is a root (over $\mathbf{Q}$) of the polynomial $\Phi_2(x, 8000)$. Dividing this polynomial by $x - 8000$ we get a second degree polynomials with roots j_2, j_3, the invariants of the other two curves, E_2, E_3 related to E_1 by a degree 2 isogeny. Let $\omega \in \mathbb{F}_{p^2}$ so that $\omega^2 = -2$. One gets that then $j_2 = 3 + 14\omega, j_3 = 3 - 14\omega$.

   Another method to find j_2, j_3 consists in remarking that 37 is equally inert in the field

$K = \mathbf{Q}(\sqrt{-15})$, for which the class number is 2. The second degree polynomial giving the values of the modular invariants of 2 curves of complex multiplication by the ring of integers of K is $x^2 + 191025x - 121287375$, whose roots generate $\mathbf{Q}(\sqrt{5})$, so modulo 37 are conjugate in $\mathbb{F}_{37^2}$. We can thus find j_2, j_3.

For N prime congruent to 1 mod 12, the number of supersingular curves mod N is $(N-1)/12$. For $N = 37$ we get 3 supersingular curves. It remains to show that the action of T_2 on E_2 (by conjugations we get the action on E_3). It is not possible to have 2 isogenies of E_2 on E_1, because then we would have 5 isogenies of degree 2 starting in E_1. Therefore there is one 2-isogeny of E_2 over E_2.

Actually, if there is a 2-isogeny of an elliptic curve of invariant j on itself, this invariant is the root of the equation $\Phi_2(x, x) = 0$, a fourth degree equation that can be written as

$$(x - 1728)(x - 8000)(x + 3375)^2$$

. (To see this, one can make the computation of the equation of $\Phi_2(j, j')$ above. One can also search which are the curves of complex multiplication that admit a degree 2 endomorphism, i.e., which are the imaginary quadratic fields that contains an element of norm 2. One finds, by multiplication by the units of the ("corps pres?") the elements $1 + i, \sqrt{-2}, \frac{1+\sqrt{-7}}{2}$ and $\frac{1-\sqrt{-7}}{2}$ that are the endomorphisms of degree 2 of the curves of invariant $j = 1728, j = 8000$ and for the last two, $j = -3375$.)

By order, mod p, the graph of T_2 cannot contain a loop of a supersingular curve on itself – although this curve is defined over $\mathbb{F}_p$ (and, more precisely, it is one of 3 curves described above). Therefore, there are 2 isogenies relating E_2 to E_3 and the graph of T_2 acting on M_{37} is completely determined.

To compute the corresponding eigenvectors, one can evidently diagonalize the matrix $(3, 3)$ of T_2 but there is a simpler method:

the involution $W_{37} = -\operatorname{Frob}_{37}$ separates M_{37} in an obvious way into two orthogonal proper subspaces, one generated by $u_1 = [E_2] - [E_3]$, associated with the eigenvalue 1, and the other associated with the eigenvalue -1, generates by $\text{Eis} = [E_1] + [E_2] + [E_3]$ and the vector product of u_1 and Eis, let it be $u_2 = 2[E_1] - [E_2] - [E_3]$. One can deduce, without recourse to T_2, that there exist 2 newforms for which the q-expansion has rational coefficient, and thus that $J_0(37)$, the jacobian of $X_0(37)$ is isogenous to the product of 2 elliptic curves (which is well-known, see for example [?]). Formula (1) above allows us to obtain the first 83 terms of their function L.

2. $p - 37, N = 2 \cdot 37$.

To study $X_0(74)$ one uses the homomorphism ϕ_2 of M_{74} to M_{37} defined previously. The fibres of reach of the three supersingular points $[E_1], [E_2]$ and $[E_3]$ of $X_0(1)$mod 37 are formed by three distinct supersingular points of $X_0(2)$mod 2. In a general way, write that if $S_1, S_2, \ldots, S_k$ are the supersingular points of $X_0(qM)$mod p above a supersingular point S of $X_0(M)$mod p (p, q coprime and coprime with M), one has the formula

$$\frac{q+1}{\mathrm{Aut}\,S}=\sum_{1}^{k}\frac{1}{\mathrm{Aut}\,S_i}.$$

The equation of $X_0(2)$ used here is that described in the appendix: $uv = 2^{12}$, the involution W_2 switching u and v. Recall that $W_{37} = -\,\mathrm{Frob}_{37}$ and that $j = (u+16)^3/u$ (where j is the invariant of the curve E, image of the point (E, C) of $X_0(2)$ via the homomorphism "oubli – oblivion?" of $X_0(2)$ on $X_0(1)$.) From the equation $j = j_1 = 8$ one gets the values of the three supersingular points of E_1, of coordinates $u_1 = (-1+\omega)/2, u_2 = (-1-\omega)/2 = W_2(u_1)$ and $u_3 = 27 = W_2(u_2)$. (Here again, it is possible to guess the value of u_3, because it is clear by the action of $T(2)$ on $X_0(1)$mod 37 done previously that one of the above E_1 must be invariant relative to W_2; or the two solutions of $u^2 = 2^{12}$ are $u_1, -u_1$. Replacing them in the equation that gives j one can see that it is about u_1. To get u_2, u_3 it is enough to solve a second degree equation.)

One can compute that $u_4 = W_2(u_1) = 2^{12}/u_1 = -5-5\omega$, and one finds that the corresponding invariant $j(u_4)$ is $j_2 = 3+14\omega$. One solves the second degree equation given 2 other points above by j_2 and so $u_5 = 15+17\omega, u_6 = 16-12\omega$. Note that $u_7 = W_2(u_2) = \bar{u}_4, u_8 = W_2(u_5) = \bar{u}_5$ and $u_9 = W_2(u_6) = \bar{u}_6$ the x-coordinates of three supersingular points over E_3 ($x \longrightarrow \bar{x}$ being the nontrivial automorphism of $\mathbb{F}_{p^2}$.) We get the list of all supersingular points of $X_0(2)$mod 37.

As said above, the space M_{74}^{new} corresponding to the newforms is the intersection of the kernel of ϕ_2 and the kernel of $\phi_2 W_2$. If we write $[u_i]$, $i = 1, \ldots, 9)$ the generators of M_{74} corresponding to the supersingular points of x-coordinate u_i, an examination of the action of W_{37} and W_2 prove that M_{74}^{new} is the direct sum of two 2-dimensional subspaces, one G_1, generated by $e_1 = [u_1]-[u_2]-[u_4]+[u_7]-[u_9]$ and $e_2 = [u_5]-[u_6]-[u_8]+[u_9]$, on which $W_{37} = -W_2 = 1$ and the other, G_2, generated by $e_3 = [u_1]+[u_2]-2[u_3]+[u_4]-[u_6]+[u_7]-[u_9]$, on which $W_2 = -W_{37} = 1$.

Using the equation of T_3 acting on $X_0(2)$ (cf. appendix), one can prove that the matrix of T_3 acting on G_1 (respectively G_2) in the basis (e_1, e_2) (respectively (e_3, e_4)) is $\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$, of characteristic polynomial x^2+x-1 (respectively $\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}$, of characteristic polynomial x^2-3x-1).

One deduces that $J_0^{new}(74)$ is isogenous to the product of two abelian simple varieties, A_1 (resp. A_2), of real multiplication by the ring of integers of $\mathbf{Q}(\sqrt{5})$, (respectively $\mathbf{Q}(\sqrt{13})$.)

If $\lambda = \frac{-1+\sqrt{5}}{2}, \mu = \frac{3+\sqrt{13}}{2}$, then the vectors $v_1 = e_1 + (\lambda+1)e_2, v_2 = e_1 - \lambda e_2, v_3 = \mu e_3 + e_4, v_4 = (3-\mu)e_3 + e_4$ corresponding to the 4 newforms f_1, f_2, f_3, f_4 of weights 2 and level 74. Using (1) one gets the first 83 values of the coefficients of these newforms. For example for f_1 the list of the first values of a_l is

l	2	3	5	7	11	13
a_l	1	$\frac{-1+\sqrt{5}}{2}$	$\frac{1-3\sqrt{5}}{2}$	$-1+\sqrt{5}$	$\frac{-5-\sqrt{5}}{2}$	$\frac{1+3\sqrt{5}}{2}$

and for f_3 one gets

l	2	3	5	7	11	13
a_l	-1	$\frac{3+\sqrt{13}}{2}$	$-1-\sqrt{13}$	$\frac{1-\sqrt{13}}{2}$	$\frac{-1-\sqrt{13}}{2}$	$\frac{-1+\sqrt{13}}{2}$

3 Application to the study of Weil curves

Let $f = \sum a_n q^n$ be a newform of weight 2 and level N with integer coefficients. They correspond to a strong Weil curve $\mathcal{E}$ of conductor N. Unfortunately the coefficients a_n don't give too much information on $\mathcal{E}$ and do not allow us to obtain a simple equation for $\mathcal{E}$. (In [**?**] there is a method due to Serre that sometimes allows us to get such an equation, but that method is not systematic.) Here we give a method that at least when $N = p$ is a prime, one can solve the problem.

From now on let N be a prime. According to the last section, for a newform f there is associated a vector $v_f = \sum x_S[S]$, $x_S \in \mathbf{Z}$, an eigenvector of the Hecke operators defined in 2.1. Theorem 1 doesn't describe the isomorphism (which is not canonical) between $S_2(N)$ and $M_N^0 \otimes \mathbf{C}$. But suppose known the terms a_n of f (a_2 is sufficient in general). The construction of section 2.4 gives us both the supersingular values mod N and the graph of T_2 acting on M_N. We can determine the eigenspace V_2 associated with the eigenvalue a_2. If it is of dimension 1, we also have v_f, or at least the space it generates. Otherwise, we apply T_3 to V_2 (which is of tentatively small dimension—for conductors < 80000, $\dim V_2$ doesn't goes beyond 6), until finding a 1-dimensional space, corresponding to the same eigenvalues of the operators T_l as f. Choose in this space a vector $r_f = \sum x_E[E]$ with integer x_E coprime in pairs[2]; then r_f is determined up to sign.

To go further, we need a geometric interpretation of the x_E. Let $\Delta = \pm N^\delta$, the discriminant of the minimal Weierstrass model of $\mathcal{E}$, let $\phi : X_0(N) \longrightarrow \mathcal{E}$ be a minimal cover of $\mathcal{E}$ of degree $n = \deg \phi$.

According to Deligne-Rapoport [**?**], there exists a model $X_0(N)_{/\mathbf{Z}}$ of $X_0(N)$ defined over $\mathbf{Z}$ for which reduction mod N is the union of two projective lines, one C_∞ classifying the elliptic curves of characteristic N provided with the group scheme kernel of the Frobenius (this corresponding to inseparable isogenies), the other one, C_0, classifying the curves provided with Verschiebung. These two lines intersect at supersingular points. As far as the curve $\mathcal{E}$ is concerned, reduction mod N of its Neron model has identity component $\mathcal{E}^0_{/\mathbb{F}_N}$ isomorphic to $\mathbb{F}_{N^2}$ of the multiplicative group G_m. One can prove that the cover extends to $X_0(N)_{/\mathbf{Z}} - \S$ where $\S$ is the set of all supersingular points of characteristic N, and define by restriction a regular "application ?" of C_∞ on $\mathcal{E}^0_{/\overline{\mathbb{F}}_N}$, of a rational function ϕ over C_∞, for which the poles and zeros are in $\mathcal{E}$. The divisor $\sum \lambda_E[E]$ of ϕ, E going through all the supersingular curves mod N, and thus an element of M_N^0, defined up to sign (depending on the choice of isomorphism of $\mathcal{E}^0_{/\mathbb{F}_N}$ over G_m.)

Proposition 3.1. *In the above notation the divisor* $(\Phi) = \sum \lambda_E[E]$ *is equal to* $\pm r_f$.

[2] That seems to strong to me; do we just mean that the gcd of coefficients is 1?

It is not difficult to see that (Φ) is proportional to r_f. By contradiction, the fact that the l_E are coprime with one another is obtained from the result of Ribet which says that if l is a prime different from 2, 3 then all cusp forms mod l of weight 2 and level Np (where Np is square-free) for which the associated representation mod l is irreducible and not ramified at p, comes from a cusp form mod l of weight 2 and level N (this result was conjectured by Serre in 1985. This also shows that the Taniyama-Weil conjecture implies the Fermat theorem.)

To prove the previous theorem, one proves first that δ is related to λ_E by $\delta = \gcd(\lambda_E\omega_E - \lambda_F\omega_F)$ where ω_E is the number of automorphisms of E. Suppose that a prime number l divides the gcd is λ_E. It also divides δ, and one deduces from here that p is not ramified in the field of points of order l or $\mathcal{E}$. If l is coprime with 6 Ribet's [3] theorem shows that the modular form f associated to $\mathcal{E}$ is congruent mod l to a modular form of weight 2 and level 1, which cannot be but the Eisenstein series. The curve $\mathcal{E}$ is semi-stable, which implies ([**?**], p.306) that $\mathcal{E}$ or a curve $\mathbf{Q}$-isogenous to it has a point of finite order l. If $l = 2, 3$ we get the same result due to [**?**], Appendix. Now, we know explicitly the curves of prime conductor with torsion [**?**] namely the curves 11A and 11B of [**?**], which have a point of order 5, curves 17A,17B,17C (point of order 4), 17D (point of order 2), 19A and 19B (point of order 3), 37B, 37C (point of order 3) and the curves of Setzer-Neumann [**?**], which have a point of order 2. In each of these cases, we know δ, which is equal to the number of finite points rational over $\mathbf{Q}$ of the considered curves, and one can verify that the λ_E are coprime with one another. This proves the proposition. Note that along the proof we showed that Ribet's theorem implies the following

Theorem 3.2. *Let E be a strong Weil curve of prime conductor N. The valuation of its discriminant in N is equal to the number of torsion points of $E(\mathbf{Q})$.*

We state without proof the theorem that allows us to get an explicit equation for $\mathcal{E}$ once we know the λ_E.

Theorem 3.3. *Let $\mathcal{E}$ be a strong Weil curve of prime conductor N, and $\sum \lambda_E[E]$ the element of M_N^0 associated to $\mathcal{E}$ via the constructions above. There exists an equation of $\mathcal{E}$*

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$$

with $c_4, c_6 \in \mathbf{Z}$ so that, if $H = \max(\sqrt{|c_4|}, \sqrt[3]{|c_6|})$ we have:

1. *$H \le \frac{8n}{\sqrt{N}-2}(\log(H^6/1728) + b)$, where $b = (\Gamma(1/3)/\Gamma(2/3))^3 = 7.74316962\ldots$.*

2. *Let $\Delta' = (c_4^3 - c_6^2)/1728$. Then $\Delta' = \Delta$ if $\mathcal{E}$ is supersingular in characteristic 2, and $\Delta' = \Delta$ or $2^{12}\Delta$ otherwise.*

3. *$c_4 \equiv (\sum \lambda_E j_E)^4 mod\ N$.*

4. *$c_6 \equiv -(\sum \lambda_E j_E)^6 mod\ N$.*

[3] K.Ribet, *Lectures on Serre's conjectures*, MSRI, Fall 1986

5. $n\delta = \lambda_E^2 \omega_E$.

If the λ_E are known then 5 allows us to get n and 1 allows us to find a bound on H, thus on c_4, c_6. By 2 we have $c_4^3 - c_6^2 = 1728\Delta'$, which allows us to find c_4, c_6. The congruences 3 and 4 allow us to reduce the number of computations significantly. Thus we have found an equation of a strong Weil curve corresponding to the initial newform f.

This method also allows us to prove that an elliptic curve of small prime conductor is a Weil curve. Suppose that we are given such a curve by its equation. Then we may compute the number of its points N_l mod l for $l = 2, 3, \ldots$. Next we search, by the method of graphs, whether $a_2 = 3 - N_2$ is the eigenvalue of T_2 acting on M_N. If not then the Taniyama-Weil conjecture is false. If yes, then continue with T_3 acting on the found eigenspace, if it is not of dimension 1, until we get an eigenspace of dimension 1 for the Hecke operators, with integers eigenvalues. If there is no such thing, then we get a counterexample to the Taniyama-Weil conjecture. If there is one, we compute the equation of a corresponding Weil curve. If this curve is isogenous to the initial curve, we are done. Otherwise, the initial curve is not a Weil curve.

In particular, this allows us to prove that the elliptic equation

$$y^2 + y = x^3 - 7x + 6$$

of conductor 5077, is a Weil curve.

This curve seems to be the smallest curve (ordering the curves by their conductors) having a Mordell-Weil rank ≥ 3 [?]. The interest in it is the following:

Let $f(z) = \sum a_n q^n$ $(q = e^{2\pi i z})$, a newform of weight 2 and conductor N, and let $L(s) = \sum a_n n^{-s}$, the associated L function. If the order of L in 1 is ≥ 3 then Goldfeld proved that there exists a computable constant C_f so that

$$\log p < C_f h(-p),$$

where $p \equiv 3(\text{mod } 4)$ is a prime number coprime with N and $h(-p)$ is the number of classes of imaginary quadratic fields of discriminant $-p$. We have other formulas, but more complicated, in the case of imaginary quadratic fields of non-prime discriminant (see [?] for example).

If the Birch and Swinnerton-Dyer conjecture is true, all the Weil curves for which the Mordell-Weil group over $\mathbf{Q}$ is of rank ≥ 3 have to be given by such modular forms, but until the work of Gross and Zagier [?], there was no way to verify that the derivative at 1 of the L function of a Weil curve is indeed 0. The results of Gross and Zagier allow to write $L'(1)$ as the product of a non-zero factor easily computable and the Néron-Tate height of a Heegner point (cf. [?] for more details.) It is therefore possible, by decreasing the height of rational points on the curve and increasing $L'(1)$ by a careful computation, to prove that L is of order ≥ 3 at $s = 1$. (In all the previous, we considered odd Weil curves, i.e., for which the L function has an odd order at 1 – or if one prefers for which the sign of the functional equation is -1.)

One has several method to construct Weil curves for which the Mordell-Weil group is of rank ≥ 3 (and which are good candidates for the preceding question: by the method of

Gross-Zagier, one may compute $L'(1)$. If it is zero, one has an L function which allows to obtain an increase of the absolute value of the discriminant of imaginary quadratic fields of given class numbers; if it is non-zero, the conjecture of Birch and Swinnerton-Dyer is false.) One can, for example, search for curves of complex multiplication of rank 3 (we know that they are Weil curves), but the constant C_f is very large. One can deform[4] a Weil curve (for example the curve 37C of [?] until getting a rank 3 curve (for the curve 37C, one can deform by $\mathbf{Q}(\sqrt{-139})$, as shown by Gross and Zagier [?].) This leads to a constant C_f of order of 7000

One may choose some elliptic curve defined over $\mathbf{Q}$, or rank 3, and try to prove that it is a Weil curve. This was done in [?] for the mentioned curve of conductor 5077, using the trace formula. But the computation is very long. The method of graphs allows us to do it in about 5 seconds an a computer that needed 5 hours with the mentioned method.

For this curve, one has $C_f < 50$: all imaginary quadratic curves of discriminant d with $|d| > e^{150}$ therefore has a class number ≥ 4. On the other hand, there is no imaginary quadratic field of discriminant d and class number 3 for $907 < |d| < 10^{2500}$ [?]. Therefore (after an examination of a table of class numbers of the first quadratic fields):

Theorem 3.4. *The imaginary quadratic fields of class number 3 are the 16 fields of discriminant:* $-23, -31, -59.-83, -107, -139, -211, -283, -307, -331, -379, -499, -547, -643, -883, -907$.

4 Application to a conjecture of Serre

Let ρ be a continuous representation of $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ in $GL_2(V)$ where V is a dimension 2 vector space over a finite field $\mathbb{F}_q$ of characteristic p. Assume this is an odd representation, i.e., that $\rho(c)$ the image of the complex conjugation, seen as an element of $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ has eigenvalues 1 and -1. In that case put $G = Im\rho$.

In [?] Serre defines the level, the character and the weight of such a representation:

1. The level.

   Let l be a prime number different from p. Write G_i $(i = 0, \ldots)$ the groups of ramifications of ρ at l. Let
   $$n(l) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \text{codim} V^{G_i},$$
   where $g_i = |G_i|$.

   The conductor of the representation ρ is defined as
   $$N = \prod_{l \neq p} l^{n(l)}.$$

2. The character.

[4] Twist?

The determinant of ρ yields a character of $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ in $\mathbb{F}_q^*$, for which the conductor divides pN. Therefore, one can write

$$\det \rho = \varepsilon \chi^{k-1},$$

where χ is the cyclotomic character of conductor p and ε is the character $(\mathbf{Z}/N\mathbf{Z})^* \longrightarrow \mathbb{F}_q^*$. The integer k is defined mod $(p-1)$, and the fact that the representation is odd implies that $\varepsilon(-1) = (-1)^k$.

By definition, ε is the character of the representation ρ.

3. The weight.

   The integer k above is defined mod $(p-1)$. Read Serre's article for the definition of the weight $k \in \mathbf{Z}$ of the representation ρ. As the conductor N depends only on the behavior of ρ ar places coprime with p, the definition of weight only uses the local properties at p of the representation ρ.

Then Serre's conjecture is:

Conjecture 4.1. *Let ρ be a representation as above, of weight k, level N and character ε. Assume this representation is irreducible. Then it comes from a cusp form mod p of weight k, level N and character ε.*

This conjectures, if true, has numerous consequences: it implies the Taniyama-Weil conjecture and Fermat's theorem.

Many such representations ρ are modular, either by construction, or because they are part of classical conjectures (Langlands, Artin, ...) that carry on the conjecture (but sometimes in a weak form, i.e., with a weight or conductor bigger than those defined in [**?**].)

In order to verify (or contradict) Serre's conjecture, we need to find the extensions $K/\mathbf{Q}$ of Galois group subgroup of $GL_2(\mathbb{F}_q)$ of odd determinant and $p \neq 2$. It is in general not difficult to calculate, for l prime and not too large, the trace a_l of Frob_l in $GL_2(\mathbb{F}_q)$: if $P(x)$ is a polynomial whose roots generate K the decomposition of Pmod l usually will suffice.

It is however, much harder to find modular forms mod p, if they exist, that correspond to the representation ρ given by the field K: the discriminant of K is usually large, thus so is the conductor of ρ, which is related to it, so it is not easy to make the computations.

4.1 The case $SL_2(\mathbb{F}_4)$

A troubling case is that of $p = 2$, because, since $-1 \equiv 1 (\mathrm{mod}\ 2)$ all representations are odd.

The representations of $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ in $GL_2(\mathbb{F}_2) = S_3$ (although altogether real, cf. [**?**]) come from weight 1 modular forms; the group S_3 can be realized as a subgroup of $GL_2(\mathbf{C})$. One can hope that by multiplication with convenient Eisenstein series, one can obtain a modular form of weight and level predicted by the Serre conjecture (cf. [**?**] for examples.)

In order to obtain the most interesting case for characteristic 2, one considers the representations with values in $GL_2(\mathbb{F}_4)$. The isomorphism $A_5 \simeq SL_2(\mathbb{F}_4)$ allows us to obtain several examples. Let K be an extension of $\mathbf{Q}$ of Galois group A_5. Since A_5 "immerses ?"

into $PGL_2(\mathbf{C})$, if the field is not completely real, the associated representation ρ comes from a weight 1 modular form (module Artin's conjecture, cf. [**?**]). Suppose now that K is real. None of the classical conjectures allow us to suspect that ρ comes from a modular form, even if of higher weight or level. It is this case that we will study in what follows. The method of graphs here is indispensable, the modular forms that we look at having a conductor too large to be studied with the Eichler-Selberg trace formula.

Let $P(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ be a rational polynomial of discriminant D. In order that the field of roots of P be A_5 it is sufficient and necessary that P be irreducible, that D be square-free, and that there exist a prime number l not dividing D so that Pmod l having exactly two roots in $\mathbb{F}_l$ (this last condition assuring that the group is all of A_5).

It is clear that $\varepsilon = 1$. If $p \mid D$, p coprime with 30, $n(p) = 1$ if it "seulment si l'inertie en p ==?" is of order 2, and thus the polynomial P has at most double roots mod p. As far as the weight k is concerned, it is either 2 or 4 according to the ramification of K at 2. To simplify the computation, we have limited to searching examples among the representations of prime level and weight 2.

On the other hand, since it is about representations in $SL_2(\mathbb{F}_4)$m the coefficient a_2 of the sought modular form, if it exists, cannot be in $\mathbb{F}_4$, but in $\mathbb{F}_{16}$. This comes from the fact that the coefficient a_l of a modular form mod l is equal to an eigenvalue of Frob_l, and not to its trace. Now, if a matrix in $SL_2(\mathbb{F}_4)$ is of order 5, its eigenvalues are in $\mathbb{F}_{16}$ not in $\mathbb{F}_4$.

The examples treated above were obtained by making a systematic search on a computer of convenient polynomials (totally real, of type A_5, for which the conductor of the associated representation is a prime N, and for which the weight is 2).

Thereafter, for each such polynomial P, one computes the corresponding eigenvalue a_2 (in $\mathbb{F}_{16}$), and one tries to find whether there exists a modular form mod 2 of level N and weight 2 so that T_2 has a_2 as an eigenvalue. In all the cases considered, we have thereafter found an eigenspace of dimension 1 or 2. Using the operators T_3, T_5, one calculates the coefficients a_3, a_5, and verifies that they correspond to the values predicted by the decomposition of P in 3 and 5.

Clearly, this doesn't really prove that the representation ρ associated to P is modular: we have only exhibited a modular form mod 2 of proper level and weight for which the terms a_2, a_3, a_5 are convenient. But there is a good indication of the truthfulness of the conjecture of Serre in the considered cases: an exhaustive search over numerous primes N of the coefficients a_2 of modular forms of weight 2 and level N proves that it is rare that there are fields of small degree. (Actually, is seems that 2, and in general the small primes, are the most "inert" possible in the fields that appear in the Hecke algebra of modular forms, fields which themselves in general appear to have the largest degree possible, taking into account constraints such as the Atkin-Lehner involutions, primes of Eisenstein, etc. One gets that one has small factors, – corresponding for example to elliptic curves with prime conductor – but this is apparently rare.)

4.2 A few examples

1. $P(x) = x^5 - 10x^3 + 2x^2 + 19x - 6.$

The discriminant is $(2^3 887)^2$. This polynomial is irreducible mod 5, thus irreducible over $\mathbf{Q}$. Its roots are all real (apply Sturm's algorithm). One has that

$$P(x) \equiv x(x-1)(x^3+x^2-1) \text{mod } 3,$$

which gives a cycle of order 3; the Galois group of K, the field of roots of P, is thus A_5.

From $P(x) \equiv (x-462)(x-755)^2(x-788)^2 \text{mod } 887$ one gets that the conductor N of the associated representation is $N = 887$. One can also prove that 2 is "little ramified" in the sense of [**?**], thus ρ has weight 2. Examining the reduction mod 2 of P proves that the coefficients a_2, a_3, a_5 of the modular form mod 2 of level 887 (which must correspond to ρ via the Serre conjecture) are 1, 1, j (where $j \in \mathbb{F}_4$ has the property that $j^2+j+1=0$).

One therefore applies the method of graphs: the space of modular forms mod 2 of weight 2 and level 887 has dimension 73, and computation shows that the eigenspace G_1 of T_2 corresponding to the eigenvalue 1 has dimension 2; T_3 acts as the identity on G_1, and j, j^2 are the eigenvalues of T_5 acting on G_1, from where get a basis of G_1 formed by $f_1 = q+q^2+q^3+q^4+jq^5+\cdots$ and $f_2 = q+q^2+q^3+q^4+j^2q^5+\cdots$, eigenvectors of Hecke operators. These corroborate the conjecture.

2. $P(x) = x^5 - 23x^3 + 55x^2 - 33x - 1$.

   Then $D = 13613^2, P(x) \equiv (x-6308)(x-2211)^2(x-8248)^2 \text{mod } 13613$, $N = 13613$; P being irreducible mod 2, Frob_2 is a cycle of order 5, and $a_2 = \zeta_5$ is a fifth root of unity, viewed as an element of $\mathbb{F}_{16}$. Computation also shows that in the space of modular forms mod 2 of level 13613 and weight 2, which has dimension 1134, ζ_5 is a simple eigenvalue of T_2. The coefficients a_3, a_5 are respectively equal to $1+\zeta_5^2+\zeta_5^3 = j$ and $\zeta_5^2+\zeta_5^3 = j^2$, which are the traces of $\text{Frob}_3, \text{Frob}_5$ in $SL_2(\mathbb{F}_4)$.

3. We write the other found polynomials; in each case there exists a modular form of weight 2 and appropriate level, for which the first terms a_n correspond to those values predicted by the Serre conjecture.

$$P(x) = x^5+x^4-16x^3-7x^2+57x-35, N = 8311, \sqrt{D} = N$$

$$P(x) = x^5+2x^4-43x^3+29x^2+2x-3, N = 8447, \sqrt{D} = 2^2N$$

$$P(x) = x^5+x^4-13x^3-14x^2+18x+14, N = 15233, \sqrt{D} = 2N$$

$$P(x) = x^5+x^4-37x^3+67x^2+21x+1, N = 24077, \sqrt{D} = 2^2N$$

5 Appendix: The curves $X_0(p)$ of genus 0

In [**?**], it is proven that if p is a prime number then the curve $X_0(p)$ over $\mathbf{Z}_p$ is formally isomorphic to the curve of equation $xy = p^k$, in the neighborhood of each point reducing mod p to a supersingular point S, k being one half the number of automorphisms of S.

If $X_0(p)$ has genus 0 (i.e., $p = 2, 3, 5, 7, 13$) one has such a model over $\mathbf{Z}$, given by the function

$$x = \left(\frac{\eta(z)}{\eta(pz)}\right)^{\frac{24}{p-1}}, \qquad (2)$$

where $\eta(z) = q^{1/24} \prod_{i=1}^{\infty}(1 - q^n)$ and $q = e^{2\pi iz}$.

This results from Fricke [**?**], who gives for each of the above p's an expression of the “oubli ?” homomorphism $j : X_0(p) \longrightarrow X_0(1)$, which associates to each point (E, C) of $X_0(p)$ the point (E) of $X_0(1)$, parametrized by the modular invariant j.

In the following we recall these equations and give the expressions of the correspondences T_2, T_3 over these curves. The variable x is the one given by equation (2), the involution W_p switches x and y and the divisor of x is $(0) - (\infty)$, where 0 and ∞ are two points of $X_0(p)$.

1. $p = 2$ The equations given by Fricke (modified to give the model of $X_0(2)$ over $\mathbf{Z}$) are:

   $$xy = 2^{12}$$

   $$j = \frac{(x+16)^3}{x}$$

   T_2 is given by

   $$y^2 - y(x^2 + 2^4 3x) - 2^{12}x = 0$$

   (to each point x is associated by T_2 the formal sum of points of coordinate y that are roots of this polynomial.)

   T_3 is given by

   $$x^4+y^4-x^3y^3-2^3 3^2 x^2y^2(x+y)-2^2 3^2 5^2 xy(x^2+y^2)+2\cdot 3^2 1579x^2y^2-2^{15} 3^2 xy(x+y)-2^{24}xy = 0$$

2. $p = 3$.

   $$xy = 3^6$$

   $$j = \frac{(x+27)(x+3)^3}{x}$$

   $$T_2 : x^3 + y^3 - 2^3 3xy(x+y) - x^2y^2 - 3^6 xy = 0$$

   $$T_3 : y^3 - y^2(x^3 + 2^2 3^2 x^2 + 2 \cdot 3^2 5y) - 3^6 yx(x + 2^2 3^2) - 3^{12}x = 0$$

3. $p = 5$.

   $$xy = 5^3$$

   $$j = \frac{(x^2+10x+5)^3}{x}$$

   $$T_2 : x^3 + y^3 - x^2y^2 - 2^3 xy(x+y) - 7^2 xy = 0$$

   $$T_3 : x^4+y^4-x^3y^3-2\cdot 3^2 x^2y^2(x+y)-3^4 xy(x^2+y^2)-2\cdot 3^2 23x^2y^2-2250xy(x+y)-5^6 xy = 0$$

4. $p = 7$.

$$xy = 7^2$$

$$j = \frac{(x^2+13x+49)(x^2+5x+1)^3}{x}$$

$$T_2 : x^3+y^3-x^2y^2-2^3xy(x+y)-7^2xy = 0$$

$$T_3 : x^4{+}y^4{-}x^3y^3{-}2^23x^2y^2(x{+}y){-}2{\cdot}3{\cdot}7xy(x^2{+}y^2){-}3{\cdot}53x^2y^2{-}2^23{\cdot}7^2xy(x{+}y){-}7^4xy = 0$$

5. $p = 13$.

$$xy = 13$$

$$j = \frac{(x^2+5x+13)(x^4+7x^3+20x^2+19x+1)^3}{x}$$

$$T_2 : x^3+y^3-x^2y^2-2^2xy(x+y)-13xy = 0$$

$$T_3 : x^4{+}y^4{-}x^3y^3{-}2{\cdot}3x^2y^2(x{+}y){-}3{\cdot}5xy(x^2{+}y^2){-}3{\cdot}11x^2y^2{-}2{\cdot}3{\cdot}13xy(x{+}y){-}13^2xy = 0$$

The polynomials above that give T_2, T_3 are of simpler form than the classical modular equations $\Phi_2(j,j')$ and $\Phi_3(j,j')$ (that correspond to the action of T_2 and T_3 on $X_0(1)$). For comparison, we recall their expressions:

$$\begin{aligned}\Phi_2(j,j') &= j^3+j'^3-j^2j'^2+2^43\cdot 31jj'(j+j')-2^43^45^3(j^2+j'^2)\\ &\quad +3^45^34027jj'+2^83^75^6(j+j')-2^{12}3^95^9\end{aligned}$$

$$\begin{aligned}\Phi_3(j,j') &= j^4+j'^4-j^3j'^3-2^23^39907jj'(j^2+j'^2)+2^33^231j^2j'^2(j+j')\\ &\quad -2^{16}5^33^517\cdot 263jj'(j+j')+2^{15}3^25^3(j^3+j'^3)+2\cdot 3^413\cdot 193\cdot 6367j^2j'^2\\ &\quad -2^{31}5^622973jj'+2^{30}3^35^6(j^2+j'^2)+2^{45}3^35^9(j+j')\end{aligned}$$