BULLETIN DE LA S. M. F.

ANDREW P. OGG

Hyperelliptic modular curves

Bulletin de la S. M. F., tome 102 (1974), p. 449-462

<http://www.numdam.org/item?id=BSMF_1974__102__449_0>

Bull. Soc. math. France,
102, 1974, p. 449-462.

HYPERELLIPTIC MODULAR CURVES

BY

ANDREW P. OGG

[Université d'Orsay et Université de Berkeley]

SUMMARY. — Let $X_0(N)$ be the modular curve corresponding to the subgroup $\Gamma_0(N)$ of the modular group defined by matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with N dividing c. It is shown that $X_0(N)$ is hyperelliptic for exactly nineteen values of N, the largest being $N = 71$. The only case where the hyperelliptic involution is not defined by an element of $SL(2, \mathbf{R})$ is $N = 37$.

RÉSUMÉ. — Soit $X_0(N)$ la courbe modulaire correspondant au sous-groupe $\Gamma_0(N)$ du groupe modulaire défini par les matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec N divisant c. On démontre que $X_0(N)$ est hyperelliptique pour exactement dix-neuf valeurs de N, la plus grande étant $N = 71$. Le seul cas où l'involution hyperelliptique n'est pas définie par un élément de $SL(2, \mathbf{R})$ est $N = 37$.

Let N be a positive integer, and let $\Gamma_0(N)$ be the subgroup of the modular group $\Gamma = SL(2, \mathbf{Z})/(\pm 1)$ defined by matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with N dividing c. Let $Y_0(N)$ be the quotient of the upper half-plane $\mathfrak{H}$ by $\Gamma_0(N)$, and let $X_0(N)$ be the compactification of $Y_0(N)$ obtained by adding cusps. We give $Y_0(N)$ and $X_0(N)$ their standard structures of algebraic curves over $\mathbf{Q}$ (*cf.* [10] for a convenient description of the cusps, and their rationality); although the questions studied in this paper seem to have little to do with rationality, we shall be making more use than one might expect of the rational structure. Let $g = g(N)$ be the genus of $X_0(N)$. We assume that $g \geqq 2$, i. e. that N is not among the fifteen values $N =$ 1-10, 12, 13, 16, 18, 25 with $g = 0$, nor among the twelve values $N = 11, 14, 15, 17$, 19-21, 24, 27, 32, 36, 49 with $g = 1$.

The main objective of this paper is to prove that $X_0(N)$ is not hyperelliptic for $N \geqq 72$, as conjectured by NEWMAN. That $X_0(N)$ is not hyperelliptic for N sufficiently large was proved by LARCHER [4]. There are exactly nineteen values of N for which $X_0(N)$ is hyperelliptic; they are listed below in Theorems 1 and 2. The principal difficulty in the proof, and the motivation of this work, was the curious phenomenon of the " exceptional " hyperelliptic involution for $N = 37$, which was noticed in the following two situations.

In [5], LEHNER and NEWMAN determined the normalizer of $\Gamma_0(N)$ in $SL(2, \mathbf{R})/(\pm 1)$, i. e. they determined that subgroup B of the automorphism group A of $X_0(N)$ which is defined by automorphisms of $\mathfrak{H}$. If N is divisible neither by 4 nor by 9, then B is just the group W of involutions of Atkin-Lehner type : if $N = q_1^{e_1} \ldots q_r^{e_r}$ is the product of r distinct prime-powers, we have an involution w_M for each M dividing N with M relatively prime to N/M, and they form a group W which is the product of r groups of order 2. The involution w_N is defined by the matrix $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Furthermore, these involutions are all rational. If N is divisible by 4 or 9, then B is somewhat bigger than W, since for example $\Gamma_0(N)$ is normal in $\Gamma_0(N/2)$ if 4 divides N. As LEHNER and NEWMAN noted in a page of corrections attached to their reprints of [5], B is not necessarily equal to A when $\Gamma_0(N)$ has elliptic fixed points, i. e. when the mapping $\mathfrak{H} \to Y_0(N)$ is ramified; they gave the example of $X_0(37)$, which is hyperelliptic because of genus 2, but the hyperelliptic involution is not w_{37}. This is the only example of the phenomenon that I know. It would be of great interest to know the full automorphism group A of $X_0(N)$ in all cases. In this paper, we study only the question of when $X_0(N)$ is hyperelliptic, i. e. when $X_0(N)$ divided by a certain involution v has genus 0, and the hyperelliptic involution v is " exceptional ", i. e. not in B. Of course this is much easier than finding A, since the hyperelliptic involution has very special properties [not to mention that $X_0(N)$ is usually not hyperelliptic]. The main result is that 37 is unique.

THEOREM 1. — *$N = 37$ is the only case where $X_0(N)$ is hyperelliptic, with an exceptional hyperelliptic involution v.*

This work is related to the problem of finding the rational points on $Y_0(N)$, on which MAZUR and I have been working for some time (*cf.* [6], [11]). Suppose that $X_0(N)$ admits a rational automorphism u which does not preserve the set of rational cusps. Then u must map a rational cusp onto a rational point of $Y_0(N)$; thus $Y_0(N)_{\mathbf{Q}}$ is not empty, i. e. some elliptic curve over $\mathbf{Q}$ admits a rational cyclic isogeny of degree N. This is the situation for $N = 37$ (*cf.* [7]), where the hyperelliptic involution v

carries the two cusps (which are rational) onto two rational points of $Y_0(37)$, as it happens the only two rational points of $Y_0(37)$. As MAZUR and I are inclining to the opinion that $Y_0(N)$ has no rational points except for a finite number of values of N, we are certainly interested in knowing when this sort of thing is going on, and in putting a stop to it if at all possible. Perhaps $N = 37$ is the only such case; at any rate, it is the only case of an exceptional hyperelliptic involution. The question of whether $X_0(N)$ is hyperelliptic or not is quite relevant to the problem of the rational points of $Y_0(N)$; the Atkin-Lehner involutions are one of the principal tools, and it is essential to know if a given involution w is a hyperelliptic involution or not.

Once we have Theorem 1, it is relatively easy to prove :

THEOREM 2. — *There are exactly eighteen values of N besides $N = 37$ for which $X_0(N)$ is hyperelliptic. For two of these values, namely $N = 40$, 48, the hyperelliptic involution v is not of Atkin-Lehner type. The remaining sixteen values are listed in the table below, together with their genera and hyperelliptic involutions v.*

N	q	v	N	q	v
22	2	w_{11}	35	3	w_{35}
23	2	w_{23}	39	3	w_{39}
26	2	w_{26}	41	3	w_{41}
28	2	w_7	46	5	w_{23}
29	2	w_{29}	47	4	w_{47}
30	3	w_{15}	50	2	w_{50}
31	2	w_{31}	59	5	w_{59}
33	3	w_{11}	71	6	w_{71}

It is a pleasure to acknowledge some helpful correspondence and conversations with Barry MAZUR and Morris NEWMAN.

1. Weierstrass points, hyperelliptic curves

We collect here some facts we need, which can be found in many places. Let X be a compact Riemann surface of genus $g \geqq 2$. (Most of the following holds for complete non-singular curves in any characteristic.)

A point P of X is a *Weierstrass point* if there exists a non-constant function f on X which has a pole of order $\leqq g$ at P and is regular elsewhere.

The number n of Weierstrass points is finite, and satisfies

$$2g+2 \leqq n \leqq g^3-g,$$

with $n = 2g+2$ if, and only if, X is hyperelliptic, i. e. admits a function of degree 2. In pratice, one finds Weierstrass points by the following theorem.

SCHOENEBERG'S THEOREM [12]. — *Let P be a fixed point of an automorphism w of X, of period $p > 1$; let $g^{(w)}$ be the genus of $X^{(w)} = X/(w)$, the space of orbits of X under the group of order p generated by w. If $g^{(w)} \neq [g/p]$, then P is a Weierstrass point of X.*

Now let X be hyperelliptic, i. e. X admits a mapping of degree 2 onto the projective line, i. e. X possesses an involution (automorphism of period 2) v such that $X^{(v)}$ is of genus 0. v is the only involution of X such that $X^{(v)}$ is of genus 0, and will be called the *hyperelliptic involution* of X. One way to characterize v is as follows. Let $P, Q \in X$. Then $Q = v(P)$ if, and only if, $(g-1)(P+Q)$ is a canonical divisor. From this, or otherwise, we note that v is in the center of the automorphism group of X, and if X is defined over a field K, then so is v. Finally, the Weierstrass points of X are exactly the $(2g+2)$ fixed points of v.

PROPOSITION 1. — *Let v be the hyperelliptic involution of X, and let w be another involution. Let $u = vw$ (also an involution). Then the fixed-point sets of u, v, and w are disjoint. If g is even, then w and u have two fixed points each. If g is odd, then w has four fixed points, and u has none, or vice versa.*

Proof. — The number $n(w)$ of fixed points of w is even, since by the Riemann-Hurwitz formula the genus of $X^{(w)}$ is

$$g^{(w)} = (g+1)/2 - n(w)/4.$$

Because v and w commute, they operate on each other's sets of fixed points, so if they have one common fixed point P, then they have another one Q. We can regard the divisors $2(P)$ and $2(Q)$ on X as points of $X^{(v)}$ or of $X^{(w)}$. Since $X^{(v)}$ is of genus 0, $2(P) - 2(Q)$ is the divisor of a function f. Then $f \circ w = \pm f$; the plus sign must hold since f has a zero of even order at P and Q. Then f defines a function of degree 1 on $X^{(w)}$, which is of genus > 0, a contradiction. Thus v and w have no common fixed point; the same is true for v and u, and u and w. Then the fixed points of w are not Weierstrass points, so by Schoeneberg's theorem, if $n(w) > 0$, then $g^{(w)} = [g/2]$, i. e. $n(w) = 2$ if g is even, and $n(w) = 4$ if g is odd. Finally, in the case where g is odd, let us apply the Riemann-Hurwitz formula to the mapping of degree 4 onto a curve of genus 0 obtained by dividing by the group of order 4 on our involutions. Since the fixed-point sets are disjoint, we get

$$2g-2 = 4(-2)+n(v)+n(w)+n(u) = -8+(2g+2)+n(w)+n(u),$$

and so $4 = n(w)+n(u)$. Since $n(w)$ and $n(u)$ are 0 or 4, one of them is 0 and the other one is 4.

2. **Atkin-Lehner involutions of** $X_0(N)$

Let $N = N'N''$, where $(N', N'') = 1$. As Atkin and Lehner showed [2], the involution $w = w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ of $X_0(N)$ factors as $w = w'w''$ ($w' = w_{N'}$, $w'' = w_{N''}$); in terms of matrices, w' is defined by any integral matrix of determinant N' of the form

$$w' = \begin{pmatrix} 1 & 0 \\ 0 & N' \end{pmatrix}\begin{pmatrix} N'a & b \\ N''c & d \end{pmatrix} = \begin{pmatrix} a & b \\ N''c & N'd \end{pmatrix}\begin{pmatrix} N' & 0 \\ 0 & 1 \end{pmatrix}$$
$$\in \begin{pmatrix} 1 & 0 \\ 0 & N' \end{pmatrix}.\Gamma_0(N'') \cap \Gamma_0(N'').\begin{pmatrix} N' & 0 \\ 0 & 1 \end{pmatrix}.$$

Let us first examine the action of w' on the cusps. Following the notation of [10], let $P = \begin{pmatrix} x \\ d \end{pmatrix}$ be a cusp of $X_0(N)$, where $d \mid N$, $d > 0$, $(x, d) = 1$. We can reduce x modulo $t = (d, N/d)$, and there are $\varphi(t)$ conjugate cusps associated to d. The factorization $N = N'N''$ defines correspondingly $d = d'd''$, $t = t't''$.

PROPOSITION 2. — *Let* $\bar{P} = w'(P) = \begin{pmatrix} \bar{x} \\ \bar{d} \end{pmatrix}$. *Then* $\bar{d} = (N'/d')\,d''$, $t = \bar{t}$, *and* $\bar{x} \equiv -x \pmod{t'}$, $\bar{x} \equiv x \pmod{t''}$.

The proof, an easy computation, is left to the reader.

Suppose P is fixed by w'. Then $N' = d'^2$, $t' = d'$, and $2x \equiv 0 \pmod{d'}$, or $2 \equiv 0 \pmod{d'}$. Assuming $N' \neq 1$, we have $N' = 4$. Conversely, such cusps are fixed :

PROPOSITION 3. — *w' has no fixed points at cusps (given $N' > 1$), except for the case $N' = 4$, where the cusps with $d' = 2$ are fixed.*

Turning now to non-cusps, it is easier to describe the fixed points in terms of elliptic curves. (*Cf.* NEWMAN [9] for a non-elliptic treatment; he assumes that $(N, 6) = 1$, but that restriction is easily removed.) Let (E, C) represent a point of $Y_0(N)$: E is an elliptic curve, and C a cyclic subgroup of order N; if (ω_1, ω_2) is a basis for the lattice of periods of E, with ω_2/N generating C, and $\tau = \omega_1/\omega_2 \in \mathfrak{H}$, then the orbit of τ under $\Gamma_0(N)$ is the point of $Y_0(N)$ represented. Then $C = C' + C''$, uniquely, where C' (resp. C'') is of order N' (resp. N''). Then w' sends the isomorphism class of (E, C) to that of $(\bar{E}, \bar{C})$, where $\bar{E} = E/C'$ and $\bar{C} = (E_{N'} + C'')/C'$. (Here $E_{N'}$ is the set of points on E with $N'.P = 0$.)

Now suppose that (E, C) represents a fixed point of w'. Then (E, C) and $(\bar{E}, \bar{C})$ are isomorphic, i. e. there is an isomorphism of $\bar{E}$ onto E carrying $\bar{C}$ onto C, so E admits a complex multiplication λ of kernel C',

$$0 \to C' \to E \xrightarrow{\lambda} E \to 0,$$

such that $\lambda(E_{N'}) = C'$, i. e. $\lambda^2 = N'.\varphi$, where φ is an automorphism of E, and $\lambda(C'') = C''$. Considering at first only the first condition, and supposing $N' > 3$, we have $\lambda = \sqrt{-N}$, and there are

$$\nu(N') = \begin{cases} h(-N') + h(-4N') & [N' \equiv 3 \pmod 4], \\ h(-4N)' & \text{(otherwise)} \end{cases}$$

such elliptic curves (admitting an endomorphism λ with $\lambda^2 = -N'$, and with cyclic kernel). Here $h(-d)$ is the class number of primitive quadratic forms of discriminant $-d$. For $N' = 2$ (resp. 3), we have in addition λ associate to $(1+i)$ [resp. $(3+\sqrt{-3})/2$]. For $N'' = 1$, this is a familiar formula of FRICKE. For $N'' > 1$, we must add in the second condition $\lambda(C'') = C''$, i. e. we ask if $\lambda - x$ contains cyclic groups of order N'' in its kernel, for an integer x. If N'' is odd, and $N' > 3$, the number of fixed points of w is thus

$$\nu(N').\Pi_{p \mid N''}\left(1 + \left(\frac{-4N'}{P}\right)\right).$$

where $\left(\dfrac{-d}{p}\right)$ is the Legendre symbol; a similar formula holds in the other cases.

It is now an easy exercise to check that the hyperelliptic involution v is as claimed, in the sixteen cases in Theorem 2 where v is of the form $w_{N'}$. [Recall that the genus g is

$$g = 1+\psi/12-\alpha/4-\beta/3-\sigma/2,$$

where $\psi = N.\Pi_{p\mid N}(1+1/p)$ is the index, σ is the number of cusps, and α (resp. β) is the number of solutions (mod N) of $x^2+1 \equiv 0 \pmod N$ (resp. $x^2+x+1 \equiv 0 \pmod N$).] For example, let us compute the number of fixed points of w_7 on $X_0(28)$, which has $g = 2$. There are two elliptic curves E and E' involved, with endomorphism rings $\mathbf{Z}[(1+\sqrt{-7})/2]$ and $\mathbf{Z}[\sqrt{-7}]$. [Only two curves since $h(-7) = 1 = h(-28)$.] On E, $\ker(\sqrt{-7} \pm 1) = C_2 \times C_4$, where C_n is the cyclic group of order n, which contains two subgroups which are cyclic of order 4. This contributes 4 fixed points of w_7, two each for $\sqrt{-7}+1$ and $\sqrt{-7}-1$. On E', $\ker(\sqrt{-7} \pm 1) = C_8$, contributing two fixed points. Thus w_7 has six fixed points, and so $g^{(7)} = 3/2 - 6/4 = 0$; w_7 is the hyperelliptic involution of $X_0(28)$.

As an application, let us prove that $X_0(34)$ is not hyperelliptic. Here $g = 3$, and each of w_2, w_{17}, and w_{34} has four fixed points; if we assume that there is a hyperelliptic involution v, it is none of these. Now w_2 has two sets of two conjugate fixed points, corresponding to $\lambda = 1+i$ (resp. $\sqrt{-2}$), hence rational over $\mathbf{Q}(i)$ [resp. $\mathbf{Q}(\sqrt{-2})$] exactly. The involution v, being rational, must preserve the set of two points over $\mathbf{Q}(i)$, and hence interchanges them, by Proposition 1, as does w_{34}. But then $u = vw_{34}$ has fixed points, contrary to Proposition 1.

3. The main result for odd N

The following simple theorem reduces our problem to manageable proportions (essentially $N < 100$) :

THEOREM 3. — *Suppose $X_0(N)$ is hyperelliptic. Let r be the number of distinct prime factors of N, and let $\psi = N\prod_{p\mid N}(1+1/p)$ be the index of $\Gamma_0(N)$ in Γ. Then :*

(i) $2^r+\psi/12 \leqq 10$, *if N is odd.*

(ii) $2^r+\psi/6 \leqq 20$, *if $3 \nmid N$,*

(iii) $2^r+\psi/3 \leqq 52$, *if $5 \nmid N$.*

Proof. — Suppose N is odd. Then $X_0(N)$ reduces well modulo the prime 2, and the reduced curve is still hyperelliptic. Now a hyperelliptic curve over a finite field has at most $2(1+q)$ points rational in the field of q elements, since it is a double covering of a curve of genus 0, which has $1+q$ points in the field of q elements. Taking $q = 4$, we have at least 2^r cusps rational in $\mathbf{F}_4$, so if we can find at least $\psi/12$ other points, we will have proved (i).

Consider the elliptic curve E, in characteristic 2, with $j = 0$. E is the only supersingular curve in characteristic 2, and has an automorphism group of order 24. We can take as defining equation $E : y^2+y = x^3$. Since E has exactly 3 points in $\mathbf{F}_2$, its Frobenius endomorphism is $\pi_2 = \sqrt{-2}$. Over $\mathbf{F}_4$, then, the Frobenius is -2, an integer; hence all of the ψ cyclic subgroups C of E, of order N, are rational over $\mathbf{F}_4$. If φ is an automorphism of E, then (E, C) and $(E, \varphi C)$ give the same point of $X_0(N)$, and conversely; since there are 24 automorphisms, and ± 1 fixes C, the number of points on $X_0(N)$ over $j = 0$, rational over $\mathbf{F}_4$, is then $\geqq \psi/12$. Thus (i); the proof is the same for (ii), (iii); the number of automorphisms in characteristic 3 (resp. 5) of the supersingular elliptic curve ($j = 0$) is 12 (resp. 6.). [Of course, we have a similiar statement for any $p \nmid N$, but it is less useful for larger values of p. Note also that the statement can be strengthened for a particular value of N, if we can find more points in the finite field involved].

Now suppose N is prime, and $X_0(N)$ is hyperelliptic. Then

$$N+1 = \psi \leqq 12.8 = 96,$$

so $N \leqq 89$. Now $X_0(N)$ is hyperelliptic, with $v = w_N$, for $N = 23$, 29, 31, 41, 47, 59, 71, and $N = 37$ is an admitted exception; assume then that N is none of these. By Proposition 1, we are concerned only with the cases for which w_N has 2 or 4 fixed points; after computing $h(-4N)$ for the remaining N, we find that only $N = 43$, 67, 73 remain to be tested. For $N = 43$ or 67, $h(-N) = 1$ and $h(-4N) = 3$. By the theory of complex multiplication, the corresponding j-invariants have degree 1 (resp. 3) over $\mathbf{Q}$. Hence w_N has one rational fixed point, and 3 conjugate fixed points. The hyperelliptic involution v, being rational, must fix the rational fixed point of w_N, contrary to Proposition 1. Thus $N \neq 43$, 67. Finally, suppose $N = 73$. From WADA's tables [14] of characteristic polynomials of Hecke operators, we find that $X_0(73)$ has 26 points in the field of 9 elements, and so is not hyperelliptic. [*Remark* : It may appear that the proof at this point requires a computer. However, one can easily give a recipe for the number of points on $X_0(N)$ rational over any finite field, involving only class numbers and Legendre symbols. I intend to publish this sometime, but it would carry us too far afield to go into this question here.]

Thus, for N prime, the hyperelliptic curves $X_0(N)$ are as claimed in Theorems 1 and 2.

Now suppose that $X_0(N)$ is hyperelliptic, where N is odd and composite; suppose also that $N \neq 33, 35, 39$, the only three such values on our list of known cases. By Theorem 3, $4+\psi/12 \leqq 10$, so $\psi \leqq 72$. The only possibilities are $N = 45, 51, 55$, which have $\psi = 72$. For $N = 51$ or 55, w_N has 8 fixed points, so $X_0(N)$ is not hyperelliptic. Finally, for $N = 45$, all 8 cusps are rational over $\mathbf{F}_4$, giving at least $8+6 = 14$ points over $\mathbf{F}_4$. Thus $X_0(45)$ is not hyperelliptic.

Thus Theorems 1 and 2 are proved for odd N. It will be convenient to postpone to section 5 the mopping-up operation, for even N.

4. Some applications of Dedekind's function

Let $\eta(\tau) = z^{1/24}\prod_{n=1}^{\infty}(1 - z^n)$ be Dedekind's function ($z = \exp 2\pi i \tau$), and let $\Delta = \eta^{24}$ be the discriminant function. We write $\eta_M(\tau) = \eta(M\tau)$, $\Delta_M(\tau) = \Delta(M\tau)$. If N' divides N, then $\Delta_{N'}$ is a modular form of weight 12 for $\Gamma_0(N)$, having no zeroes except at cusps, and with a zero at a cusp $\begin{pmatrix} x \\ d \end{pmatrix}$ of order $(N d'^2)/N' dt$, where $d' = (d, N')$, $t = (d, N/d)$ (*cf.* [10]). If p is a prime > 3, then η^p/η_p is a modular form of weight $(p - 1)/2$ and multiplier $\left(\frac{d}{p}\right)$ for $\Gamma_0(p)$ (HECKE [3], n° 42); hence η_M^p/η_{pM} has the same property for $\Gamma_0(pM)$. For $p = 3$, the same if true for η^9/η_3^3, and η^{16}/η_2^8 is a form for $\Gamma_0(2)$.

The next theorem is due to NEWMAN [8], at least if $(N, 6) = 1$; his proof, using Dedekind's transformation formulas for $\eta(\tau)$, is entirely different. [The assumption that $X_0(N)$ have $g \geqq 2$ is for the moment not relevant.]

THEOREM 4. — *Let $N = p.q$ be the product of two distinct primes.*
(i) *Let $h = ((p+1)(q - 1), 24)$. Then $f = (\eta.\eta_p/\eta_q.\eta_{pq})^{24/h}$ is a function on $X_0(pq)$, and $f^{1/n}$ is not a function on $X_0(pq)$, for $n > 1$.*

(ii) *Let* $k = ((p-1)(q-1), 24)$. *Then* $F = (\eta . \eta_{pq}/\eta_p \eta_q)^{24/k}$ *is a function on* $X_0(pq)$, *and* $F^{1/n}$ *is not a function on* $X_0(pq)$, *for* $n > 1$.

Proof. — That the functions f and F are on $X_0(pq)$ follows from the results of Hecke stated above, with a little manupilation. For example, we can write :

$$f = (\eta_p \eta_q^p/\eta^p \eta_{pq})^{24/h} (\eta^q/\eta_q)^{(p+1)24/h} \Delta^{-(p+1)(q-1)/h}$$
$$= (\eta^q \eta_p^q/\eta_q \eta_{pq})^{24/h} (\eta^p/\eta_p)^{(q-1)24/h} \Delta^{-(p+1)(q-1)/h}.$$

If $p > 3$, the first expression shows that f is on $X_0(pq)$, by checking the cases $q > 3$, $q = 3$, $q = 2$, where the exponent $(p+1)24/h$ is divisible by 2, 6, 8, respectively, as required. Similarly, if $q > 3$, the second expression shows that f is on $X_0(pq)$, again by cases : $p > 3$, $p = 3$, $p = 2$. Only $N = 6$ remains, which is uninteresting, since $g = 0$. The proof for F is easier, since it is symmetric in p and q; taking $p > q$, we have

$$F = (\eta^p \eta_{pq}/\eta_p \eta_q^p)^{24/k} (\eta_q/\eta^q)^{(p-1)24/k} \Delta^{(p-1)(q-1)/k}.$$

and we see that F is on $X_0(pq)$, say by considering $q > 3$, $q = 3$, $q = 2$ in order.

Now suppose that $f^{1/n}$ or $F^{1/n}$ is still on $X_0(pq)$, where n is an integer $\geqq 1$. Note that $f^{1/n}$ and $F^{1/n}$ are power series in $z = \exp 2\pi i \tau$ with rational coefficients. Multiplying $f^{1/n}$ or $F^{1/n}$ by $\Delta_q \Delta_{pq}$ or $\Delta_p \Delta_q$, we get a cusp form of weight 24 for $\Gamma_0(pq)$ with rational Fourier coefficients. These Fourier coefficients have bounded denominators (Shimura [13], Theorem 3.52, p. 85); the same is then true for $f^{1/n}$ or $F^{1/n}$ by dividing the Δ-factor back out. That $n = 1$, hence Theorem 4, follows from :

LEMMA. — *Let* $f(z) = (1-z^{n_1})^\alpha . (1-z^{n_2})^\alpha \ldots$, *where* $\alpha \in \mathbf{Q}$, $\alpha \notin \mathbf{Z}$, $n_i \in \mathbf{Z}$, $0 < n_1 \leqq n_2 \leqq n_3 \leqq \ldots$. *Then* $f(z) = \sum_{m=0}^{\infty} a_m z^m$, *where the* a_m *have unbounded denominators.*

Proof. — Expanding $f(z)$ as a product of binomial series, we see that the coefficient of z^m, where $m = n_1 m_0$ is a multiple of n_1, is

$$\pm \binom{\alpha}{m_0} + \sum \pm \binom{\alpha}{m_1} \cdots \binom{\alpha}{m_r},$$

where the summation is over $m = n_1 m_1 + \ldots + n_r m_r$, with $m_i \geqq 0$, and $m_1 < m_0$. Let l be some prime in the denominator of α. Then the first term dominates, in the l-adic absolute value, and tends to ∞ as $m_0 \to \infty$.

Using the rules stated above for the order of $\Delta_{N'}$ at cusps, we find the divisors

$$(f) = n(P_1 + P_p - P_q - P_{pq}),$$
$$(F) = m(P_1 - P_p - P_q + P_{pq}),$$

where P_j is the cusp $\begin{pmatrix} 1 \\ j \end{pmatrix}$,

$$n = \mathrm{num}((p+1)(q-1)/24) = (p+1)(q-1)/h$$

is the numerator of $(p+1)(q-1)/24$, and

$$m = \mathrm{num}((p-1)(q-1)/24) = (p-1)(q-1)/k.$$

Thus we have :

COROLLARY 1 :

(i) $P_1 + P_p - P_q - P_{pq}$ *defines a divisor class on* $X_0(pq)$ *of order exactly* $n = \mathrm{num}\ ((p+1)(q-1)/24)$.

(ii) $P_1 - P_p - P_q + P_{pq}$ *defines a divisor class on* $X_0(pq)$ *of order exactly* $m = \mathrm{num}\ ((p-1)(q-1)/24)$.

COROLLARY 2 :

(i) $X_0(pq)$ *is hyperelliptic, with hyperelliptic involution* w_p, *if and only if* $p.q = 11.2,\ 11.3,\ 23.2$ (in that order).

(ii) $X_0(pq)$ *is hyperelliptic, with hyperelliptic involution* w_{pq}, *if and only if* $pq = 26,\ 35,\ 39$.

Proof. — These are simply the only values of p and q for which n (resp. m) is 1.

Note that this gives a different proof from the one in section 2, that these values correspond to hyperelliptic curves, as stated in Theorem 2. Of course, this general method is not limited to a product of two primes, but we shall not seek any more general results in this direction. (Note, however, how much better the method works for the product of two primes than for a single prime, since we have more cusps, and η' *s*, to work with.) We close this section by showing explicitly that the remaining curves listed in Theorem 2 are indeed hyperelliptic.

For $N = 30$, $\eta^2 \eta_{15}^2 \eta_6 \eta_{10}/\eta_3 \eta_5 \eta_2^2 \eta_{30}^2$ is a function on $X_0(30)$ with divisor $P_1+P_{15}-P_2-P_{30}$, proving again that $X_0(30)$ is hyperelliptic, with $v = w_{15}$. For $N = 28$, $\eta\eta_7/\eta_4 \eta_{28}$ is on $X_0(28)$, with divisor $P_1+P_7-P_4-P_{28}$, proving again that $X_0(28)$ is hyperelliptic, with $v = w_7$.

Finally, we have the slightly exceptional cases $N = 40, 48$. For $N = 40$, let us note first that $\eta_2^{12}/\eta_4^4 \eta^8$ is on $X_0(8)$; since the genus is 0, this is just a question of verifying that the function is of integral order at each cusp. It follows that

$$\begin{aligned} f &= \eta^2 \eta_4 \eta_{10}^3/\eta_5^2 \eta_2^3 \eta_{20} \\ &= (\eta_4^5/\eta_{20})(\eta_{10}^3/\eta_2^{15})(\eta^{10}/\eta_5^2)(\eta_2^{12}/\eta_4^4 \eta^8) \end{aligned}$$

is on $X_0(40)$, and we find the divisor $(f) = P_1+P_{10}-P_2-P_5$. This shows that $X_0(40)$ is hyperelliptic. Also, $v = \begin{pmatrix} -10 & 1 \\ -120 & 10 \end{pmatrix}$ defines an involution on $X_0(40)$, by [5], or by direct calculation; it is the hyperelliptic involution since it has the correct effect on P_1, P_{10}, P_2, P_5. Finally, $\eta^2 \eta_6^3 \eta_4/\eta_3^2 \eta_2^3 \eta_{12}$ is a function on $X_0(48)$, with divisor $P_1+P_6-P_2-P_3$, so $X_0(48)$ is hyperelliptic; $v = \begin{pmatrix} -6 & 1 \\ -48 & 6 \end{pmatrix}$ is the hyperelliptic involution,

5. The main result for even N

Besides the methods already used, we will use the following observation of Newman [9]. If $X_0(N)$ is " subhyperelliptic ", i. e. is hyperelliptic, or of genus $\leqq 1$, i. e. admits a non-constant function of degree $\leqq 2$, and if M divides N, then $X_0(M)$ is again subhyperelliptic.

Now let $X_0(N)$ be hyperelliptic, where N is even, and not one of our known values, i. e. $N \neq 22, 26, 28, 30, 40, 46, 48, 50$. Also, $N \neq 34$ (end of section 2), so $N \geqq 38$.

Suppose N is not divisible by 4, say $N = 2M$, where M is odd and $\geqq 19$. If $3 \nmid M$, then by the 3-test of Theorem 3, we have $4+\psi(N)/6 \leqq 20$, or $3\psi(M) = \psi(N) \leqq 96$, $\psi(M) \leqq 32$. Hence $M = 19, 29, 31$. If $M \equiv -1 \pmod 4$, then $X_0(N)$ has no elliptic fixed points, and so the hyperelliptic involution is forced to be of Atkin-Lehner type. $M = 19$, 31 are then eliminated by Corollary 2 to Theorem 4. For $N = 58$, w_{29}

has 6 fixed points, which eliminates $M = 29$. Thus N must be divisible by 3; we now write $N = 6M$, where M is odd and $\geqq 7$. If $5 \nmid M$, then by the 5-test of Theorem 3 we have $3\psi(3M) = \psi(N) \leqq 3.48$, or $\psi(3M) \leqq 48$. Then $M = 7, 9, 11$. But for $N = 42, 54, 66$, we have $g = 5, 4, 9$, respectively, and $X_0(N)$ is not hyperelliptic since w_{14} has 8 fixed points resp. w_{54} has 6 fixed points resp. w_{66} has 8 fixed points. Thus N must be divisible by 5; we now write $N = 30M$, where M is odd and $\geqq 3$. Then M is not divisible by 7, since we just showed that $X_0(42)$ is not hyperelliptic, and hence by the unstated 7-test of Theorem 3, $8+\psi(N)/2 \leqq 2(1+49) = 100$. Then $\psi(15M) \leqq 61$, which is not possible.

Thus we must have 4 dividing N, and $N \geqq 44$. Note that $X_0(N)$ has no elliptic fixed points, so Theorem 1 is proved, and that w_N is not the hyperelliptic involution v, since it does not commute with $\begin{pmatrix} 1 & 0 \\ N/2 & 1 \end{pmatrix}$.

Suppose N is not divisible by 8, so $N = 4M$, where M is odd and $\geqq 11$. Since $X_0(2M)$ is subhyperelliptic, $M = 11, 13, 15, 23, 25$; the 3-test of Theorem 2 eliminates the last two, so actually $M = 11, 13, 15$. But $X_0(44)$ is not hyperelliptic because w_{44} has 6 fixed points; $X_0(60)$ is not hyperelliptic because w_{15} has 12 fixed points, $g^{(15)} = 1$. Finally, for $N = 52$, $g = 5$, and so $u = vw_{52}$ has no fixed point by Proposition 1. But u must fix the set consisting of the two fixed cusps P_2 and P_{26} of w_4, so u interchanges these two cusps, as does w_{52}. Hence v fixes these two fixed cusps of w_4, so $v = w_4$, by Proposition 1. Since w_4 has only four fixed points, this is not the case. Hence N is divisible by 8, $N \geqq 56$.

Suppose N is not divisible by 16, so $N = 8M$, where M is odd and $\geqq 7$. Since $X_0(4M)$ is subhyperelliptic, $M = 7$ or 9. But $X_0(56)$ is not hyperelliptic ($g^{(56)} = 1$), nor is $X_0(72)$, by the 5-test (at least 16 cusps, and 48 points over $j = 0$, in $\mathbf{F}_{25}$). Hence N is divisible by 16, $N \geqq 64$.

If N is not divisible by 32, then $N = 16M$, where M is odd and $\geqq 5$. Since $X_0(8M)$ is subhyperelliptic, we have $M = 5$, $N = 80$, but $X_0(80)$ is not hyperelliptic by the 3-test. Hence N is divisible by 32, $N \geqq 64$.

If N is not divisible by 64, then $N = 32M$, where M is odd and $\geqq 3$. Then $M = 3$, since $X_0(16M)$ is subhyperelliptic, but $X_0(96)$ is not hyperelliptic by the 5-test.

Thus we must have N divisible by 64, and it remains only to show that $X_0(64)$ is not hyperelliptic. Over $\mathbf{F}_9$, we have at least 8 rational cusps and 16 points over $j = 0$, so it is not hyperelliptic by the 3-test. Alternatively, the cusp $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is a Weierstrass point ([1], Theorem 2), and fixed by $\begin{pmatrix} 1 & 0 \\ 32 & 1 \end{pmatrix}$, which is not a hyperelliptic involution, which gives another proof. This completes the proof of Theorem 2.

REFERENCES

[1] ATKIN (A. O. L.). — Weierstrass points at cusps of $\Gamma_0(n)$, *Annals of Math.*, t. 85, 1967, p. 42-45.

[2] ATKIN (A. O. L.) and LEHNER (J.). — Hecke operators on $\Gamma_0(m)$, *Math. Annalen*, t. 185, 1970, p. 134-160.

[3] HECKE (E.). — *Mathematische Werke*. — Göttingen, Vandenhoeck und Ruprecht, 1959.

[4] LARCHER (H.). — Weierstrass points at the cups of $\Gamma_0(16p)$ and hyperellipticity of $\Gamma_0(n)$, *Canadian J. Math.*, t. 23, 1971, p. 960-968.

[5] LEHNER (J.) and NEWMAN (M.). — Weierstrass points of $\Gamma_0(n)$, *Annals of Math.*, t. 79, 1964, p. 360-368.

[6] MAZUR (B.). — *Modular curves and the Eisenstein ideal* (In preparation).

[7] MAZUR (B.) and SWINNERTON-DYER (P.). — Arithmetic of Weil curves, *Invent. Math.*, t. 25, 1974, p. 1-61.

[8] NEWMAN (M.). — Construction and applications of a class of modular functions, *Proc. London math. Soc.*, t. 7, 1957, p. 334-350.

[9] NEWMAN (M.). — Conjugacy, genus, and class numbers, *Math. Annalen*, t. 196, 1972, p. 198-217.

[10] OGG (A.). — Rational points on certain elliptic modular curves; " *Analytic number theory* ", p. 221-231. — Providence, American mathematical Society, 1973 (*Proceedings of Symposia in pure Mathematics*, 24).

[11] OGG (A.). — *Diophantine equations and modular forms*, Talk at the November 1973 meeting of the AMS in Tucson, to appear in the Bulletin AMS.

[12] SCHOENEBERG (B.). — Über die Weierstrasspunkte in den Körpern der elliptischen Modulfunktionen, *Abh. Math. Sem. Hamburg*, t. 17, 1951, p. 104-111.

[13] SHIMURA (G.). — *Introduction to the arithmetic theory of automorphic functions*. — Tokyo and Princeton, Shoten, 1971.

[14] WADA (H.). — A table of Hecke operators, *Proc. Japan Acad.*, t. 49, 1973, p. 380-384.

(Texte reçu le 1er juillet 1974.)

Andrew P. OGG,
Mathématiques, Bâtiment 425,
Université de Paris-Sud, Centre d'Orsay,
91405 Orsay (France)
[et University of California, Berkeley].