ANNALES DE L'INSTITUT FOURIER

JOSEP GONZALEZ ROVIRA

Equations of hyperelliptic modular curves

Annales de l'institut Fourier, tome 41, n° 4 (1991), p. 779-795

<http://www.numdam.org/item?id=AIF_1991__41_4_779_0>

Ann. Inst. Fourier, Grenoble
41, 4 (1991), 779-795.

EQUATIONS OF HYPERELLIPTIC MODULAR CURVES

by Josep GONZÀLEZ ROVIRA

1. Introduction.

Let N be a positive integer and let $\Gamma_0(N)$ be the subgroup of the modular group $\Gamma = SL(2,\mathbb{Z})/(\pm 1)$ defined by the matrices $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, where N divides C. As usual, we denote by $X_0(N)$ the complet complex curve corresponding to the subgroup $\Gamma_0(N)$.

In [O1], Ogg determines all the modular hyperelliptic curves with genus $g \geqslant 2$. He shows that only in the case $N = 37$ the hyperelliptic involution w does not preserve the cusps, and that this is the only case in which w does not belong to the normalizer of $\Gamma_0(N)$ in $SL(2,\mathbb{R})/(\pm 1)$. In all the other cases he computes the hyperelliptic involution w. His results can be displayed as follows :

* $w = w_{N_1}$, with $1 < N_1 \mid N$ and $(N_1, N/N_1) = 1$ (Atkin-Lehner involution) for

N = 22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 41, 46, 47, 50, 59, 71,

$w = w_{11}, w_{23}, w_{26}, w_7, w_{29}, w_{15}, w_{31}, w_{11}, w_{35}, w_{39}, w_{41}, w_{23}, w_{47}, w_{50}, w_{59}, w_{71}$,

respectively.

Key-words : Modular curves - Hyperelliptic curves - Modular equations - eta functions.
A.M.S. Classification : 14G35 - 11F11 - 11G18.

* w is not an Atkin-Lehner involution for

$$N = 40,48 \quad \text{and} \quad w = \begin{pmatrix} -10 & 1 \\ -120 & 10 \end{pmatrix}, \quad \begin{pmatrix} -6 & 1 \\ -48 & 6 \end{pmatrix}, \text{ respectively.}$$

The modular curve $X_0(N)$ is elliptic for $N = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49$. In these cases, w_N is always a hyperelliptic involution.

Several equations for the modular curves $X_0(N)$ are known in the literature. They cover all values of N for which $X_0(N)$ is elliptic and some of the values of N for which $X_0(N)$ is hyperelliptic (cf. [F], [MS], [B]). Our goal is to give a procedure to compute, in a unified way, the equations of all hyperelliptic modular curves with $g > 0$.

Our method uses some results of Newman [N1]-[N2] and ideas appearing in Birch's computation of an equation for $X_0(50)$ (cf. [B]).

For the computation of the equations it has been essential a previous study of a multiplicative group of modular functions, that we call Newman group, obtained through Newman theorem 1 of [N2].

I would like to thank Pilar Bayer for the encouragement and useful discussions throughout this work.

1. General facts.

1.1. Cusps in $X_0(N)$.

The number of cusps in $X_0(N)$ is $\sum_{0<d|N} \varphi(d,N/d)$, where φ denotes the Euler function. In order to get a system of representatives of these cusps, we choose fractions a/d for each $0 < d \mid N$, where a runs over a system of representatives of $(\mathbb{Z}/f_d\mathbb{Z})^*$, $f_d = (d,N/d)$, with the condition $(a,d) = 1$. In this way $0 \equiv 1$, $i\infty \equiv 1/N$.

The ramification index of the cusp a/d under the covering map $\pi : X_0(N) \to X(1)$ is equal to $e_d = N/(df_d)$. If follows then that $\sum_{0<d|N} \varphi(f_d)e_d = \psi(N)$ where $\psi(N) := \prod_{p|N} (1+1/p)$.

1.2. The normalizer of $\Gamma_0(N)$ in $SL(2,\mathbb{R})/(\pm 1)$.

$SL(2,\mathbb{R})/(\pm 1)$ is the set of automorphisms of the upper half-plane, and, if we denote by $\Gamma_0^*(N)$ the normalizer of $\Gamma_0(N)$ in $SL(2,\mathbb{R})/(\pm 1)$, this group singles out a group of automorphisms of $X_0(N)$ through the quotient $B(N) = \Gamma_0^*(N)/\Gamma_0(N)$.

The group $B(N)$ has been described by Lehner and Newman [LeN], and revised by Atkin-Lehner in [ALe]. If we denote e_2, e_3 the greatest exponents such that $2^{e_2}3^{e_3}$ divide N and we write $\nu_2 = 2^{\min(3,[e_2/2])}$, $\nu_3 = 3^{\min(1,[e_3/2])}$, then the matrix $\begin{pmatrix} q & 1 \\ 0 & q \end{pmatrix}$ where $q = \nu_2$ or $q = \nu_3$ defines an automorphism S_q of $X_0(N)$. The group $B(N)$ is generated by the Atkin-Lehner involutions and the automorphisms S_q with $q = \nu_2, \nu_3$.

In the case $N = 37$, the hyperelliptic involution does not belong to $B(N)$.

1) If $N = N_1 \cdot N_2$ with $(N_1, N_2) = 1$ and $N_1 > 1$, the Atkin-Lehner involution w_{N1} is defined by the matrix $\begin{pmatrix} N_1 A & B \\ N\ C & N_1 D \end{pmatrix}$ with A, B, C, $D \in \mathbb{Z}$ and determinant equal to N_1. It is always true that $w_N = w_{N_1} w_{N_2}$.

It is known that these involutions act on the cusps in the following way :

If $z = a/d$ is a cusp such that $(a,d) = 1$, $(a,f_d) = 1$ and $d \mid N$, then

$$w_{N_1}(a/d) = a'/d' \quad \text{where} \quad d' = N_1 d_2/d_1 \qquad \text{and} \qquad \begin{cases} a' \equiv -a \pmod{f_1} \\ a' \equiv a \pmod{f_2} \end{cases}$$

with $f_1, d_1 \mid N_1$; $f_2, d_2 \mid N_2$; $f_d = f_1 f_2$; $d = d_1 d_2$.

In particular w_{N_1} transforms all the cusps with the same denominator d in cusps with the same denominator $N_1 d/(N_1, d)^2$.

In this way w_{N_1} acts on the set of the positive divisors of N by : $w_{N_1}(d) = N_1 d/(N_1, d)^2$.

2) It is easy to see that S_2 transforms cusps with the same denominator into cusps with the same denominator, while S_4, S_8, S_3 do not verify this condition :

$$S_3(-1/3) = 1, \quad S_3(1/3) = 2/3 ; \quad S_4(-1/4) = 1, \quad S_4(1/4) = 1/2 ;$$
$$S_8(-1/8) = 1, \quad S_8(1/8) = 1/4.$$

We denote by $B'(N)$ the subgroup of $B(N)$ generated by the Atkin-Lehner involutions and S_2 if $4 \mid N$. The subgroup $B'(N)$ acts on the set of positive divisors of N, and for $N = 40$ or $N = 48$ the hyperelliptic involution w is in $B'(N)$ because $w = (w_8 S_2)^2 w_5$ or $w = (w_{16} S_2)^2 w_3$.

We denote by $\mathbb{C}(X_0(N))$ the function field of $X_0(N)$ and by $S_{2k}(\Gamma_0(N))$ the vector space of parabolic modular forms of weight $2k$, which is isomorphic to the space of holomorphic differentials $H^0(X_0(N),\Omega^k)$.

In general, if an automorphism u of $B(N)$ is defined by the matrix $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with determinant M, then u acts on the modular forms of weigth $2k$ by: $(f \mid u)(z) = f(\gamma(z))M^k/(Cz+D)^{2k}$.

2. Newman's group.

2.1. The matrix A_N.

Let $\Delta(z) = e^{2\pi iz} \prod_{n>0} (1-e^{2\pi inz})^{24}$ be the parabolic modular form of weight 12 for Γ. Given a natural $N > 1$, for each positive divisor $d \mid N$ we have that $\Delta(dz)$ belongs to $S_{12}(X_0(N))$. We provide the set of divisors $0 < d \mid N$ with an ordering. Let us denote by $A_N = (a_d^{d'})_{0<d,d' \mid N}$ the matrix indexed by these divisors such that $a_d^{d'}$ is the order of $\Delta(dz)$ at the cusps of denominator d'. If we want this definition to be meaningful, we have to show that if there exist different cusps with denominator d', $\Delta(dz)$ has the same order in all of them (cf. Proposition 1).

If $\{s_i\}$ denotes the set of cusps of $X_0(N)$ we have:

i) $a_d^N = d$; $a_1^{d'} = e_{d'} = \dfrac{N}{d'(d',N/d')}$, because $q = e^{2\pi iz}$ is a uniformizer of $i\infty$ and $\Delta(z)$ is a modular form on $X_0(1)$, with a simple zero at $i\infty$.

ii) $\sum_i \operatorname{ord}_{s_i} \Delta(dz) = \psi(N)$ if $0 < d \mid N$, because the degree of any modular form of weigth 12 on $X_0(N)$ is $\psi(N)$. In terms of the matrix A_N this condition yields $\sum_{0<d' \mid N} a_d^{d'} \varphi(d',N/d') = \psi(N)$.

iii) Given the projection $X_0(N) \to X_0(N/d)$, $\alpha \mapsto \beta$, and given a divisor $m \mid N/d$, we have that $\operatorname{ord}_\alpha \Delta(mz) = \operatorname{ord}_\beta \Delta(mz) e(\alpha/\beta)$, where $e(\alpha/\beta)$ denotes the ramification index of α over β. Thus $e(\alpha/\beta) = e_\alpha/e_\beta$, where e_α, e_β are the ramification indices of α, β under the projections over $X_0(1)$.

PROPOSITION 1. — i) *The matrix* A_N *is well defined and* $a_d^{d'} = \dfrac{N(d,d')^2}{dd'(d',N/d')}$.

ii) *If* $N = p^\alpha$, p *prime and* $\alpha > 0$, *then*

$$\det(A_N) = p^{[(3\alpha^2+1)/4]-\alpha}\varphi(N)^\alpha\psi(N)^\alpha.$$

iii) *If* $N = \Pi p_i^{\alpha_i}$ *is the decomposition of* N *in prime factors, then* $\det(A_N) = \Pi \det(A_{p_i})^{\sigma_0(N/p_i)}$ *where* $\sigma_0(m)$ *denotes the number of positive divisors of* m. *In particular* $\det(A_N) \neq 0$.

For *i*), see [Li].

The proof of *ii*) and *iii*) has no special difficulty and can be performed by induction over the number of divisors of N.

2.2. Newman's group.

The function $\eta(z) = q^{1/24}\prod_{n>0}(1-q^n)$ has neither poles nor zeros in the upper half-plane. For all $\tau = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ of Γ with $C > 0$, we have: $\eta(\tau z) = \xi(\tau)(-i(Cz+D))^{1/2}\eta(z)$, where we take the branch of the square-root function which is positive on the positive real axis. $\xi(\tau)$ denotes a 24-th root of unity defined by $\xi(\tau) = \exp\{\pi i \alpha_\tau\}$, where $\alpha_\tau = \dfrac{A+D}{12C} - s(A,C)$ and $s(h,k)$ is the Dedekind sum. We recall that:

1) If $h\bar{h} \equiv 1 \pmod{k}$ then $s(h,k) = s(\bar{h},k)$.

2) If $\sigma = \begin{pmatrix} C & -D \\ A & -B \end{pmatrix}$ with A, $C > 0$ then $\alpha_\tau + \alpha_\sigma = 1/4$.

3) If k is odd then $12ks(h,k) \equiv k + 1 - 2\left(\dfrac{h}{k}\right) \pmod 8$, where (-) is the Jacobi symbol.

The function η allows the construction of modular functions, as it is shown in the following theorem.

THEOREM (Newman). — *Given the function* $F(z) = \prod_{0<d|N} \eta(dz)^{r_d}$ *with* $r_d \in \mathbb{Z}$, *if the following conditions are satisfied :*

i) $\sum_{0<d|N} r_d = 0$,

ii) $\prod_{0<d|N} d^{r_d}$ *is a square,*

iii) *the order of* F *at the cusps is an integer or, equivalently, the vector* $A_N \begin{pmatrix} r_1 \\ \vdots \\ r_N \end{pmatrix}$ *belongs to* $24 \prod_{0<d|N} \mathbb{Z}$,

then F *is a modular function on* $X_0(N)$.

The second condition is, essentially, a parity condition, since it is fulfilled if all the exponents are even.

The third condition can be replaced by a weaker one, demanding that the order of F at 0 and $i\infty$ be an integer. Under this formulation the theorem was proved by Newman in [N2]. Later Ligozat demonstrated in [Li] that the three conditions are necessary for F to be a modular function.

Let us notice that, given two vectors $r = (r_d)_{0<d|N}$, $n = (n_d)_{0<d|N}$ such that $A_N r = n$, if $\sum_d r_d = 0$ then $\sum_d n_d \varphi(d, N/d) = 0$ because $\sum_d a_{d'}^d \varphi(d, N/d) = \psi(N)$. The converse is true also due to $\det(A_N) \neq 0$.

Thus if n satisfies the conditions of the theorem, the order of F at any cusp denominator d is $n_d/24$ and so $\sum_{0<d|N} n_d \varphi(d, N/d) = 0$.

Let us denote by $\mathbb{G}_N$ the multiplicative group of the modular functions obtained by the above procedure. These functions have all their zeros and poles at the cusps, and have the same order at the cusps with the same denominator $d \mid N$.

The Fourier expansions of the functions $F \in \mathbb{G}_N$ have the shape $q^m + \sum_{n>m} a_n q^n$ with $a_n \in \mathbb{Z}$ for all $n > m$ (*).

PROPOSITION 2. — *For any modular function F without zeros or poles in the upper half-plane and such that it has the same order at all cusps with the same denominator $0 < d \mid N$, there exists a positive integer μ such that $F^\mu \in \mathbb{C} \otimes \mathbb{G}_N$. If moreover, F has the Fourier expansion as (*) then $\mu = 1$ and $F \in \mathbb{G}_N$.*

Indeed, if we denote by $n = (n_d)_{0<d\mid N}$ the vector of the orders of F at the cusps $0 < d \mid N$, it suffices to take μ as the smaller integer which renders $24\mu A_N^{-1} n = (r_d)_{0<d\mid N}$ integer and fulfills the parity condition, since the condition $\Sigma r_d = 0$ follows from $\Sigma n_d \varphi(d, N/d) = 0$.

Let F be a modular function such that $F^\mu = \Pi \eta(dz)^{r_d} \in \mathbb{G}_N$ for a certain natural $\mu > 1$, and such that F has the Fourier expansion of the shape $q^m + \sum_{n>m} a_n q^n$ with $a_n \in \mathbb{Z}$ for all $n > m$. Let a_i be the first a_n non zero.

We denote by $d_1, \ldots, d_k$ the positive divisors of N such that $d_1 < d_2 < \cdots < d_k$ and $r_{d_i} \neq 0$. We have $(F/q^m)^\mu = \prod_d \prod_{n>0} (1-q^{dn})^{r_d}$, thus $1 + \mu a_i q^{i-m} + \cdots = 1 - r_{d_1} q^{d_1} + \cdots$, and so $r_{d_1} \equiv 0 \pmod{\mu}$.

It is easy to see that if $r_{d_i} \in \mu\mathbb{Z}$ and $i < k$ then $r_{d_{i+1}} \in \mu\mathbb{Z}$. Thus, we have $F = \Pi \eta(dz)^{r_d/\mu}$ and $F \in \mathbb{G}_N$ because F is a modular function. □

PROPOSITION 3. — *Let $F = \prod_{0<d\mid N} \eta(d(z))^{r_d}$ be a function of $\mathbb{G}_N$.*

i) *If $w = w_{N_1}$ then $F \mid w = \varepsilon_{N_1}(F) \prod_{0<d\mid N} d_1^{-r_d/2} \eta(w(d)z)^{r_d}$, where $d_1 = (N_1, d)$ and $\varepsilon_{N_1}(F) = \pm 1$. If N_1 is odd then $\varepsilon_{N_1}(F) = (-1)^{\sum_d d_1 \left(1 - 2\left(\frac{N_2/d_2}{d_1}\right)\right) r_d/4}$, where $d_2 = d/d_1$, $N_2 = N/N_1$ and $(-)$ denote the symbol of Jacobi. Always $\varepsilon_{N_1}(F) = \varepsilon_{N_2}(F)$, in particular $\varepsilon_N(F) = 1$.*

ii) *If $w = S_2$ then $F \mid w = \varepsilon(F) \prod_{(d,2)=2} \eta(dz)^{r_d} \prod_{(d,2)=1} \left(\frac{\eta(2dz)^3}{\eta(dz)\eta(4dz)}\right)^{r_d}$ where $\varepsilon(F)$ is equal to $(-1)^{\mathrm{ord}_{i\infty} F}$.*

iii) *$\mathbb{Q} \otimes \mathbb{G}_N$ is stable under automorphisms of group $B'(N)$.*

i) Assume $w = w_{N_1}$. Given the matrix $\gamma = \begin{pmatrix} AN_1 & B \\ CN & DN_1 \end{pmatrix}$ with determinant N_1, and given a positive divisor d of N, we denote by γ_d the matrix $\begin{pmatrix} Ad_1 & Bd_2 \\ N_2 C/d_2 & DN_1/d_1 \end{pmatrix}$ of Γ. From the equality $d\gamma(z) = \gamma_d(w(d)z)$, it follows that $F \mid w = \varepsilon \prod_d \eta(w(d)z)^{r_d} d_1^{-r_d/2}$, where $\varepsilon = \prod_d \xi(\gamma_d)^{r_d}$.

The matrix $\gamma' = \begin{pmatrix} DN_1 & B \\ CN & AN_1 \end{pmatrix}$ also defines w, and we have: $F = (F|w)\,|\,w = \varepsilon\varepsilon' F$ where $\varepsilon' = \prod_d \xi(\gamma'_{w(d)})^{r_d}$. Due to the fact that $Ad_1DN_1/d_1 \equiv 1 \pmod{N_2C/d_2}$, it follows that $\xi(\gamma_d) = \xi(\gamma'_{w(d)})$, thus $\varepsilon^2 = 1$, so $\Sigma\alpha_{\gamma_d} r_d$ belongs to $\mathbb{Z}$ and $\varepsilon = (-1)^{\Sigma\alpha_{\gamma_d} r_d}$.

We can take $A = C = 1$, and so $\gamma = \begin{pmatrix} N_1 & B \\ N & DN_1 \end{pmatrix}$. We have $\alpha_{\gamma_d} + \alpha_{\sigma_d} = 1/4$, where $\sigma_d = \begin{pmatrix} N_2/d_2 & -DN_1/d_1 \\ d_1 & -Bd_2 \end{pmatrix}$, thus $e = \Sigma\alpha_{\gamma_d} r_d = -\Sigma\alpha_{\sigma_d} r_d$.

If N_1 is odd then we have:

$$e \equiv \Sigma\left(d_1 + 1 - 2\left(\frac{N_2/d_2}{d_1}\right) + Bd_2 - \frac{N_2}{d_2}\right) r_d/12d_1$$

$$\equiv \Sigma d_1\left(1 - 2\left(\frac{N_2/d_2}{d_1}\right)\right) r_d/4 \pmod 2$$

because $\Sigma(N_2 d_1/d_2) r_d = 24\,\mathrm{ord}_{1/N_1} F$, and $\Sigma d_1 d_2 r_d = 24\,\mathrm{ord}_{i\infty} F$. If $N_1 = N$ then $\varepsilon = 1$ since $\eta(-1/z) = (-iz)^{1/2}\eta(z)$. Always $\varepsilon_{N_1}(F) = \varepsilon_{N_2}(F)$, because $\varepsilon_{N_1}(F)\varepsilon_{N_2}(F) = \varepsilon_N(F) = 1$.

ii) $w = S_2$. For all odd natural d we have:

$$\prod_{n \geq 1} (1-q^{2dn})^3/(1-q^{dn})(1-q^{4dn}) = \prod_{(n,2)=1} (1+q^{dn}) \prod_{(n,2)=2} (1-q^{dn}).$$

It follows that

$$\eta(dw(z)) = \eta(dz + d/2)$$

$$= \exp\{\pi i d/24\} \cdot \begin{cases} \eta(dz) & \text{if } (d,2) = 2 \\ \eta(2dz)^3/\eta(dz)\eta(4dz) & \text{if } (d,2) = 1. \end{cases}$$

This proves *ii)*, since $\varepsilon = \exp\left\{\pi i \sum_d r_d d/24\right\} = \exp\{\pi i\,\mathrm{ord}_{i\infty} F\}$.

iii) It is sufficient to prove the statement for $w = w_{N_1}, S_2$. Due to the fact that the three conditions of the theorem of Newman are necessary, we have $F|w \in \mathbb{C} \otimes \mathbb{G}_N$.

If $w = w_{N_1}$ then $F|w \in \mathbb{Q} \otimes \mathbb{G}_N$ since $\prod_d (d_1)^{-r_d/2} \in \mathbb{Q}$, because $\prod_d d^{r_d}$ is a square. In the case $w = S_2$ the proposition is obvious.

3. Hyperelliptic modular curves.

Recall that a compact Riemann surface X of genus g is hyperelliptic if it satisfies one of the following equivalent conditions:

i) there exists a covering $F: X \to \mathbb{P}^1(\mathbb{C})$ of degree 2,

ii) there exists an involution $w: X \to X$ with $2g+2$ fixed points

iii) there exists an involution $w: X \to X$ such that X/w has genus zero.

If we denote by $z_1, \ldots, z_{2g+2}$ the images by F of the ramification points, then X is the curve defined by the equation $Y^2 = \prod_{i=1}^{2g+2} (F - z_i)$ or $Y^2 = \prod_{i=1}^{2g+1} (F - z_i)$, depending on whether $z_i \neq \infty$ for all $i = 1, \ldots, 2g+2$ or $z_{2g+2} = \infty$, or, equivalently, on whether F has two simples poles at non ramification points or a double pole at a ramification point.

Conversely the equation $Y^2 = \prod_{i=1}^{n} (Z - z_i)$ with $z_i \neq z_j$ if $i = j$, defines a hyperelliptic curve of genus $g = [(n-1)/2]$.

If the genus $g > 1$ then X has exactly $2g+2$ Weierstrass points, which are the ramifications points of the covering F and, at the same time, the fixed points of w. In this case w is the only hyperelliptic involution, and w is in the center of the automorphism group of X.

In the following, $X_0(N)$ is a hyperelliptic modular curve of non zero genus. We denote by w the only hyperelliptic involution if the genus is greater that one or the Atkin involution if the genus is one (that is always hyperelliptic), and X_w denote the quotient curve $X_w = X_0(N)/w$.

Given two points P, Q of $X_0(N)$ such that $w(P) \neq Q$, due to the fact that X_w has genus zero, there exists a function F on X_w such that $\mathrm{div}_{X_w} F$ is $(Q) - (P)$. If we consider this function F on $X_0(N)$, it is invariant under w, and has $D = (w(Q)) + (Q) - (w(P)) - (P)$ as a divisor. On the other hand, the function field over X_w are the rational functions in F.

The next proposition shows several elementary facts which will be essential to construct the required equations.

PROPOSITION 4. – i) *Let F, G be functions over $X_0(N)$ such that $G|w \neq G, F|w = F$ and such that F viewed as a function over Y has a simple pole. Then $\mathbb{C}(X_0(N)) = \mathbb{C}(F,G)$.*

ii) *For all $f \in S_2(\Gamma_0(N))$ then $f|w = -w$.*

iii) *The cusp $i\infty$ is not a ramification point over $X_0(N)/w$.*

i) and *ii)* are obvious because the degree of the extension $\mathbb{C}(X_0(N))/\mathbb{C}(F)$ is equal to 2 and $H^0(X_0(N)/w, \Omega^1)$ is equal to $\{0\}$.

ii) If w is an Atkin-Lehner involution, it is clear that $w(i\infty) \neq i\infty$.

In the case $N = 40$, 48 the proposition can be easily checked. Finally, as it has been shown by Ogg, $i\infty$ is not a Weierstrass point when N is prime and so $i\infty$ is not a ramification point of $X_0(37)$. □

We must look for functions F, G of $X_0(N)$ such that:

*) $F|w = F$; F, considered as a function over X_w, has a simple pole at $i\infty$ and its Fourier expansion is normalized. Furthermore, if $N = 37$ we require, moreover, that F has a simple zero at 0.

*) $G|w \neq G$, $G \in \mathbb{G}_N$ and $H = G + G|w$, considered as a function over X_w, has the only pole at $i\infty$.

Because *iii)* of the proposition 4, the equation that we will find for $X_0(N)$ will be of the form $Y^2 = \prod_{i=1}^{2g+2} (X - x_i)$.

4. Modular equations.

4.1. The search for a function F.

PROPOSITION 5 ($X_0(N)$ *elliptic*). – *Let $X_0(N)$ be elliptic and let be G a modular function with poles and zeros only at $0, i\infty$. If we denote by ω the Néron differential, then $F = \dfrac{q.dG/dq}{G\omega}$ is a modular function invariant under w_N, and with a simple pole at $i\infty$, 0.*

There always exists a function G as described, and due to the fact that it has zeros and poles only at $0, i\infty$ it satisfies $G\left(\frac{-1}{Nz}\right) = a/G(z)$ for $a \in \mathbb{C}^*$. Taking the derivative with respect to z, we get :

$$\frac{G'(-1/Nz)}{G(-1/Nz)} \cdot 1/Nz^2 = -\frac{G'(z)}{G(z)}, \qquad \text{that is} \qquad \frac{dG/dz}{G}\Big| w_N = -\frac{dG/dz}{G}.$$

Thus, the logarithmic derivative of G has two simple poles at 0, $i\infty$, and is an eigenvector of w_N with eigenvalue -1. Since $\omega | w_N = -\omega$, and ω does not have any zeros, it follows that the quotient between the logarithmic derivative and the Néron differential is a function F as the one described in the proposition. Furthemore, $\frac{qdG/dq}{G}$ is equal to the logarithmic differential $\frac{dG/dz}{G}$ up to a multiplicative constant. □

PROPOSITION 6 ($X_0(N)$ *hyperelliptic non elliptic*). — *If* $X_0(N)$ *has genus* $g > 1$ *then there exist two parabolic forms of weigth two* f_g, f_{g-1} *with Fourier expansions of the form* $f_i = q^i + \sum_{n>i} a_n q^n$ $i = g-1, g$. *The modular function* $F = f_{g-1}/f_g$ *is invariant under* w, *has poles only at* $i\infty$, $w(i\infty)$ *which are simples, and* F *is normalized.*

In $S_2(\Gamma_0(N))$, there always exists a basis of parabolic forms h_1, $i = 1, \ldots g$ such that $h_i \equiv q^i \bmod q^{g+1}$, because $i\infty$ is not a Weierstrass point. Thus, the existence of parabolic forms of the type f_g, f_{g-1} is ensured. Any parabolic form is an eigenvector of w with eigenvalue -1, and so, $i\infty$, $w(i\infty)$ are zeros of the same order.

Thus, if we think of f_g, f_{g-1} as holomorphic differentials, their divisors are :

$$\begin{aligned} \operatorname{div} f_g &= (g-1)[(i\infty)+(w(i\infty))], \\ \operatorname{div} f_{g-1} &= (P) + (w(P)) + (g-2)[(i\infty).(w(i\infty))] \end{aligned}$$

with P, $w(P) \neq i\infty$. It is obvious that f_{g-1}/f_g satisfy the required conditions. □

PROPOSITION 7 ($N=37$). — *Let* f, g *be the parabolic normalized forms of weigth two, such that* $f|w_{37} = f$ and $g|w_{37} = -g$, *then the modular function* $F = (f+g)/(f-g)$ *is invariant under* w *and* $\operatorname{div} F = (0) + (w(0)) - (i\infty) - (w(i\infty))$.

If we look upon $h = f - g$, $h' = f + g$ as holomorphic differentials, their divisors are:

$\operatorname{div} h = (i\infty) + (w(i\infty))$ because h has a simple zero at $i\infty$ and $h|w = -h$.
$\operatorname{div} h' = (0) + (w(0))$ because $w_N w = w w_N$ and $h|w_N = h'$.

It follows that the function $F = h'/h$ is invariant under w, and has simple zero at 0, $w(0)$ and simple pole at $i\infty$, $x(i\infty)$. □

PROPOSITION 8 (*N composed $\neq 49, 27$*). — *Let N be a non prime number different from 27 and 49. For every cusp s with denominator d satisfying $(d, N/d) = 1$, and such that both s, $w(s)$ are different from $i\infty$, there exists a function $F \in \mathbb{G}_N$ invariant under w such that* $\operatorname{div} F = (s) + (w(s)) - (i\infty) - (w(i\infty))$.

The proof is performed by checking that in every $X_0(N)$ and for every cusp $s = 1/d$ the following system

$$A_N \begin{pmatrix} r_1 \\ \vdots \\ r_N \end{pmatrix} = 24 \begin{pmatrix} 0 \\ 1 \\ 1 \\ \cdots \\ -1 \\ -1 \end{pmatrix} \begin{matrix} \\ \leftarrow s \\ \leftarrow w(s) \\ \\ \leftarrow w(i\infty) \\ \leftarrow i\infty \end{matrix}$$

has as integer solution which satisfies the parity condition. The results are summarized in the table. Let us notice that the conditions imposed on the cusps s are necessary and sufficient for F to belong to $\mathbb{G}_N$. Moreover, in view of the previous results, we already know that, for a suitable number μ, $F^\mu \in \mathbb{G}_n$, so proposition 2 affirms that $\mu = 1$.

4.2. The search for a function G.

Let F be a modular function of $X_0(N)$ non constant, such that $\operatorname{div} F = (P) + (w(P)) - (i\infty) - (w(i\infty))$.

a) Assume $N \neq 37$. In this case $w(i\infty)$ is a cusp. We are looking for a function $G \in \mathbb{G}_N$ with poles only at $i\infty$ and zeros only at $w(i\infty)$. According to what we have said, this function does exist and it is not invariant under w. It only remains to compute the smaller natural α

such that the vector

$$\alpha.24.A_N^{-1}\begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}\begin{matrix} \leftarrow w(i\infty) \\ \\ \leftarrow i\ \infty \end{matrix} = \begin{pmatrix} r_1 \\ \vdots \\ \vdots \\ r_N \end{pmatrix}$$

is integer and satisfies the parity conditions.

Since $\operatorname{div} G = \alpha(w(i\infty)) - \alpha(i\infty)$, $\operatorname{div} G|w = -\operatorname{div} G$ we have $G|w = b/G$ for a certain $b \in \mathbb{Q}^*$. For instance if $N = p$ prime, $G(z) = \left[\dfrac{\eta(z)}{\eta(pz)}\right]^{24/d}$ with $d = (12, p-1)$. In this case $G|w_N = p^{12/d}/G$.

b) Assume N is composed and $N \neq 27, 49$, or N is equal to 37. In this case we take F such that P is a cusp. We are looking for a function $G \in \mathbb{G}_N$ with $\operatorname{div} G = \beta(P) - \beta(i\infty)$. We will have

$$\operatorname{div} G|w = \beta(w(P)) - \beta(w(i\infty)) = \operatorname{div}(F^\beta/G),$$

and thus there exists a certain $b \in \mathbb{C}^*$ such that $G|w = bF^\beta/G$. For instance if $N = 37$, $G(z) = \eta(z)^2/\eta(37z)^2$ and $G|w = bF^3/G$.

4.3. The equations.

No matter which of the above mentioned possibilities we try, we will have $H = G + G|w = G + bF^n|G$ with a pole of multiplicity m at $i\infty$, $w(i\infty)$ ($n = 0$ $m = \alpha$ or $n = \beta$ $m = \beta$ depending on the chosen possibility).

Thus, in any case we have $H = P(F)$, where P is a polynomial of degree m. Expanding G, F in Fourier series in q, $P(F)$ and b are easily evaluated, because if H and $P(F)$ have the same polar part, then $H - P(F)$ has no poles and is a constant.

With the change $U = 2G - P(F)$, the equality $G + bF^n/G = P(F)$ yields the equation $U^2 = P(F)^2 - 4bF^n$. Let us write $Q(x) = R(x)T(x)^2$, where $Q(x)$ is the polynomial $Q(x) = P(x)^2 - 4bx^n$ and $R(x)$ has no double roots. The change $Y = U/T(F)$ yields the equation $Y^2 = R(F)$, where $R(x)$ is a polynomial of degree $2g + 2$, because the genus of the equation must be equal to g.

TABLE N COMPOSED ($\neq 27, 29$)

N	s	F	G	$G\|w$
		elliptic		
14	1/7	$\dfrac{\eta(2z)^4\eta(7z)^4}{\eta(z)^4\eta(14z)^4}$	$\dfrac{\eta(2z)\eta(7z)^7}{\eta(z)\eta(14z)^7}$	$8F^2/G$
15	1/5	$\dfrac{\eta(3z)^3\eta(5z)^3}{\eta(z)^3\eta(15z)^3}$	$\dfrac{\eta(3z)\eta(5z)^5}{\eta(z)\eta(15z)^5}$	$9F^2/G$
20	1/4	$\dfrac{\eta(4z)^2\eta(5z)^2}{\eta(z)^2\eta(20z)^2}$	$\dfrac{\eta(4z)^4\eta(10z)^2}{\eta(2z)^2\eta(20z)^4}$	$5F^2/G$
	1/2	$\dfrac{\eta(2z)^4\eta(10z)^4}{\eta(z)^3\eta(4z)\eta(5z)\eta(20z)^3}$		
21	1/3	$\dfrac{\eta(3z)^2\eta(7z)^2}{\eta(z)^2\eta(21z)^2}$	$\dfrac{\eta(3z)^3\eta(7z)^7}{\eta(z)\eta(21z)^3}$	$7F^2/G$
24	1/8	$\dfrac{\eta(2z)\eta(3z)^2\eta(8z)^2\eta(12z)}{\eta(z)^2\eta(4z)\eta(6z)\eta(24z)^2}$	$\dfrac{\eta(8z)^4\eta(12z)^4}{\eta(4z)^2\eta(24z)^4}$	$3F^2/G$
	1/2	$\dfrac{\eta(2z)^5\eta(3z)\eta(8z)\eta(12z)^5}{\eta(z)^3\eta(4z)^3\eta(6z)^3\eta(24z)^3}$		
	1/4	$\dfrac{\eta(4z)^4\eta(6z)^4}{\eta(z)\eta(2z)^2\eta(3z)\eta(8z)\eta(12z)^2\eta(24z)}$		
32	1/2	$\dfrac{\eta(2z)^3\eta(16z)^3}{\eta(z)^2\eta(4z)\eta(8z)\eta(32z)^2}$	$\dfrac{\eta(16z)^6}{\eta(8z)^2\eta(32z)^4}$	$2F^2/G$
36	1/4	$\dfrac{\eta(4z)\eta(9z)}{\eta(z)\eta(36z)}$	$\dfrac{\eta(4z)^2\eta(18z)}{\eta(2z)\eta(36z)^2}$	$3F^2/G$
		non elliptic		
22	1/11	$\dfrac{\eta(z)^2\eta(11z)^2}{\eta(2z)^2\eta(22z)^2}$	$\dfrac{\eta(2z)\eta(11z)^{11}}{\eta(z)\eta(22z)^{11}}$	$-F^5/G$
26	1/2	$\dfrac{\eta(2z)^2\eta(13z)^2}{\eta(z)^2\eta(26z)^2}$	$\dfrac{\eta(2z)^4\eta(13z)^2}{\eta(z)^2\eta(26z)^4}$	$13F^3/G$
28	1	$\dfrac{\eta(z)\eta(7z)}{\eta(4z)\eta(28z)}$	$\dfrac{\eta(14z)^2\eta(4z)^4}{\eta(2z)^2\eta(28z)^4}$	$-7/G$
	1/2	$\dfrac{\eta(2z)^3\eta(14z)^3}{\eta(z)\eta(7z)\eta(4z)^2\eta(28z)^2}$		
30	1/6	$\dfrac{\eta(z)\eta(6z)^2\eta(10z)^2\eta(15z)}{\eta(2z)^2\eta(3z)\eta(5z)\eta(30z)^2}$	$\dfrac{\eta(z)\eta(6z)^6\eta(10z)^2\eta(15z)^3}{\eta(2z)^2\eta(3z)^3\eta(5z)\eta(30z)^6}$	$5F^4/G$

N	s	F	G	$G\|w$
	1	$\frac{\eta(z)^2\eta(6z)\eta(10z)\eta(15z)^2}{\eta(2z)^2\eta(3z)\eta(5z)\eta(30z)^2}$		
	1/3	$\frac{\eta(3z)\eta(5z)}{\eta(2z)\eta(30z)}$		
33	1/11	$\frac{\eta(z)\eta(11z)}{\eta(3z)\eta(33z)}$	$\frac{\eta(3z)\eta(11z)^{11}}{\eta(z)\eta(33z)^{11}}$	F^{10}/G
35	1/5	$\frac{\eta(5z)\eta(7z)}{\eta(z)\eta(35z)}$	$\frac{\eta(5z)^5\eta(7z)}{\eta(z)\eta(35z)^5}$	$49F^6/G$
39	1/3	$\frac{\eta(3z)\eta(13z)}{\eta(z)\eta(39z)}$	$\frac{\eta(3z)^3\eta(13z)}{\eta(z)\eta(39z)^3}$	$13F^4/G$
40	1/8	$\frac{\eta(2z)\eta(8z)^2\eta(20z)^3}{\eta(4z)^3\eta(10z)\eta(40z)^2}$	$\frac{\eta(8z)^4\eta(20z)^2}{\eta(4z)^2\eta(40z)^4}$	$5F^4/G$
	1	$\frac{\eta(z)\eta(8z)\eta(10z)^2}{\eta(4z)^2\eta(5z)\eta(40z)}$		
	1/2	$\frac{\eta(2z)^3\eta(8z)\eta(5z)\eta(20z)}{\eta(z)\eta(4z)^3\eta(10z)\eta(40z)}$		
46	1	$\frac{\eta(z)\eta(23z)}{\eta(2z)\eta(46z)}$	$\frac{\eta(2z)^8\eta(23z)^4}{\eta(z)^4\eta(46z)^8}$	$23^2/G$
48	1/16	$\frac{\eta(4z)\eta(16z)^2\eta(24z)^3}{\eta(8z)^3\eta(12z)\eta(48z)^2}$	$\frac{\eta(16z)^4\eta(24z)^2}{\eta(8z)^2\eta(48z)^4}$	$-3F^4/G$
	1	$\frac{\eta(z)\eta(4z)\eta(16z)\eta(6z)^2\eta(24z)}{\eta(2z)\eta(8z)^2\eta(3z)\eta(12z)\eta(48z)}$		
	1/2	$\frac{\eta(2z)^2\eta(16z)\eta(3z)\eta(24z)}{\eta(z)\eta(8z)^2\eta(6z)\eta(48z)}$		
50	1/2	$\frac{\eta(2z)\eta(25z)}{\eta(z)\eta(50z)}$	$\frac{\eta(2z)^2\eta(25z)}{\eta(z)\eta(50z)^2}$	$5F^3/G$

In order to compute the equations that follow, we have used the functions F which appear with functions G beside them.

Equations N composed ($\neq 27,49$)

14	$Y^2 = F^4 - 14F^3 + 19F^2 - 14F + 1$
15	$Y^2 = F^4 - 10F^3 - 13F^2 + 10F + 1$
20	$Y^2 = F^4 - 8F^3 - 2F^2 - 8F + 1$
21	$Y^2 = F^4 - 6F^3 - 17F^2 - 6F + 1$

22 $$Y^2 = F^6 + 12F^5 + 56F^4 + 148F^3 + 224F^2 + 192F + 64$$

24 $$Y^2 = F^4 - 8F^3 + 2F^2 + 8F + 1$$

26 $$Y^2 = F^6 - 8F^5 + 8F^4 - 18F^3 + 8F^2 - 8F + 1$$

28 $$Y^2 = F^6 + 6F^5 + 25F^4 + 60F^3 + 100F^2 + 96F + 64$$

30 $$Y^2 = F^8 + 6F^7 + 9F^6 + 6F^5 - 4F^4 - 6F^3 + 9F^2 - 6F + 1$$

32 $$Y^2 = F^4 - 8F^3 + 12F^2 - 16F + 4$$

33 $$Y^2 = F^8 + 8F^7 + 38F^6 + 108F^5 + 227F^4 + 324F^3 + 342F^2 + 216F + 81$$

35 $$Y^2 = F^8 - 4F^7 - 6F^6 - 4F^5 - 9F^4 + 4F^3 - 6F^2 + 4F + 1$$

36 $$Y^2 = F^4 - 4F^3 - 6F^2 - 4F + 1$$

39 $$Y^2 = F^8 - 6F^7 + 3F^6 + 12F^5 - 23F^4 + 12F^3 + 3F^2 - 6F + 1$$

40 $$Y^2 = F^8 + 8F^6 - 2F^4 + 8F^2 + 1$$

46 $$Y^2 = F^{12} + 10F^{11} + 49F^{10} + 166F^9 + 418F^8 + 824F^7 + 1\,301F^6 + 1\,648F^5 + 1\,672F^4 + 1\,328F^3 + 784F^2 + 320F + 64$$

48 $$Y^2 = F^8 + 14F^4 + 1$$

50 $$Y^2 = F^6 - 4F^5 - 10F^3 - 4F + 1$$

Equations N prime or N = 27, 49 :

11 $$Y^2 = F^4 + 4F^3 - 88F^2 - 668F - 1\,272$$

17 $$Y^2 = F^4 + 2F^3 - 39F^2 - 176F - 212$$

19 $$Y^2 = F^4 - 32F^2 - 76F - 48$$

23 $$Y^2 = F^6 + 4F^5 - 18F^4 - 142F^3 - 351F^2 - 394F - 175$$

27 $$Y^2 = F^4 - 18F^2 - 36F - 27$$

29 $$Y^2 = F^6 + 2F^5 - 17F^4 - 66F^3 - 83F^2 - 32F - 4$$

31 $$Y^2 = F^6 - 4F^5 - 14F^4 - 94F^3 - 159F^2 - 98F - 27$$

37 $$Y^2 = F^6 - 4F^5 - 40F^4 + 348F^3 - 1\,072F^2 + 1\,532F - 860$$

41 $$Y^2 = F^8 + 4F^7 - 8F^6 - 66F^5 - 120F^4 - 56F^3 + 53F^2 + 36F - 16$$

47 $$Y^2 = F^{10} + 4F^9 + 2F^8 - 32F^7 - 135F^6 - 294F^5 - 424F^4 - 410F^3 - 268F^2 - 100F - 19$$

49 $$Y^2 = F^4 - 2F^3 - 9F^2 + 10F - 3$$

59 $$Y^2 = F^{12} + 4F^{11} - 28F^9 - 84F^8 - 152F^7 - 202F^6 - 212F^5 - 176F^4 - 120F^3 - 68F^2 - 24F - 11$$

71 $$Y^2 = F^{14} + 4F^{13} - 2F^{12} - 38F^{11} - 77F^{10} - 26F^9 + 111F^8 + 148F^7 + F^6 - 122F^5 - 70F^4 + 30F^3 + 40F^2 + 4F - 11$$

In this case, F denotes the function which has a simple pole at $i\infty$ in the quotient curve and such that its Fourier coefficients are $a_{-1} = 1$, $a_0 = 0$.

BIBLIOGRAPHY

[ALe] A. O. Atkin, J. Lehner, Hecke Operators on $\Gamma_0(m)$, Math. Ann., 185 (1970), 134-160.

[B] B. J. Birch, Some calculations of modulars relations, in « Modular Functions of One Variable I », Springer Lecture Notes, 320, 175-186.

[F] R. Fricke, « Die elliptischen Funktionen und ihre Anwendungen, II », Teubner (1922).

[K] P. G. Kluit, On the Normalizer of $\Gamma_0(N)$, in « Modular Functions of One Variable V ». Springer Lecture Notes 601.

[LeN] J. Lehner, M. Newman, Weierstrass points of $\Gamma_0(N)$, Ann. of Math., 79 (1964), 360-368.

[Li] G. Ligozat, Courbes modulaires de genre 1, Bull. Soc. Math. France, Mémoire, 43 (1975).

[MS] B. Mazur, Swinnerton-Dyer, P: Arithmetic of Weil Curves, Inventiones Math., 25 (1974), 1-61.

[N1] M. Newman, Construction and application of a class of modular functions, Proceed. of London Math. Soc., (1957), 334-350.

[N2] M. Newman, Construction and application of a class of modular functions (II), Proceed. of London Math. Soc., (1959), 373-387.

[O1] A. P. Ogg, Hyperelliptic Modular Curves, Bull. Soc. Math. France, 102 (1974), 449-462.

[O2] A. P. Ogg, On the Weierstarss points of $X_0(N)$, Illinois J. of Math., Vol. 22 (1978), 31-35.

[R] E. Reyssat, Quelques Aspects des Surfaces de Riemann, Birkhäusser, 1989.

Manuscrit reçu le 13 mai 1991.

Josep Gonzàlez Rovira,
Escola Universitaria Politècnica de Vilanova i la Geltrú
Departament de Matemàtica Aplicada i Telemàtica
Av. Victor Balaguer, s/n
08800 Vilanova i La Geltrú (Spain).