BULL. AUSTRAL. MATH. SOC.
VOL. 10 (1974), 197-218. 10D05

On the coefficients of transformation polynomials for the modular function

Kurt Mahler

In a previous paper (*Acta Arith.* 21 (1972), 89-97), I had proved that the sum of the absolute values of the coefficients of the mth transformation polynomial $F_m(u, v)$ of the Weber modular function $j(\omega)$ of level 1 is not greater than

$$2^{(36n+57)2^n}$$

when $m = 2^n$ is a power of 2. The aim of the present paper is to give an analogous bound for the case of general m. This upper bound is much less good and of the form

$$e^{cm^{3/2}},$$

where $c > 0$ is an absolute constant which can be determined effectively. It seems probable that also in the general case an upper bound of the form

$$e^{O(m \log m)}$$

should hold, but I have not so far succeeded in proving such a result.

1.

Let ω be a complex variable in the upper half-plane

$$U : I(\omega) > 0 .$$

Received 31 October 1973.

Thus the two exponential functions

$$x = e^{2\pi i\omega} \quad \text{and} \quad x' = e^{-2\pi i/\omega}$$

satisfy the inequalities

$$0 < |x| < 1 \quad \text{and} \quad 0 < |x'| < 1 .$$

The Weber modular function $j(\omega)$ of level 1 satisfies

$$j\left(\frac{\alpha\omega+\beta}{\gamma\omega+\delta}\right) = j(\omega)$$

for every set of four integers $\alpha, \beta, \gamma, \delta$ of determinant

$$\alpha\delta - \beta\gamma = 1 ,$$

so that in particular

$$j(-1/\omega) = j(\omega) .$$

It can be expressed as a Laurent series

$$j(\omega) = \sum_{h=0}^{\infty} a_h x^{h-1} ,$$

where the coefficients a_h are positive integers and where in particular

$$a_0 = 1 , \quad a_1 = 744 .$$

Hence, on putting

$$g(x) = \sum_{h=2}^{\infty} a_h x^{h-1} ,$$

$j(\omega)$ has the two representations

$$j(\omega) = \frac{1}{x} + 744 + g(x) = \frac{1}{x'} + 744 + g(x') .$$

2.

In the last formula, assume that ω is purely imaginary, say

$$\omega = si , \text{ where } s > 0 ,$$

so that

$$x = e^{-2\pi s} \quad \text{and} \quad x' = e^{-2\pi/s} .$$

Since its coefficients a_h are positive, $g(x)$ is positive, and it is an increasing function of x. Now

$$0 < x \le e^{-2\pi} \quad \text{if} \quad s \ge 1 ;$$

$$0 < x' \le e^{-2\pi} \quad \text{if} \quad 0 < s \le 1 ;$$

$$x = x' = e^{-2\pi} \quad \text{if} \quad s = 1 .$$

Therefore

$$0 < j(si) \le \begin{cases} \frac{1}{x} + 744 + g\left(e^{-2\pi}\right) & \text{if} \quad s \ge 1 , \\ \frac{1}{x'} + 744 + g\left(e^{-2\pi}\right) & \text{if} \quad 0 < s \le 1 . \end{cases}$$

Further

$$j(i) = 1728 = e^{2\pi} + 744 + g\left(e^{-2\pi}\right) , \quad e^{2\pi} > 535 ,$$

so that

$$744 + g\left(e^{-2\pi}\right) < 1199 .$$

It follows then that

$$(1) \qquad 0 < j(si) < \begin{cases} e^{2\pi s} + 1199 & \text{if} \quad s \ge 1 , \\ e^{2\pi/s} + 1199 & \text{if} \quad 0 < s \le 1 . \end{cases}$$

3.

Let k be any non-negative integer. Then $j(\omega)^k$ can again be written as a Laurent series

$$(2) \qquad j(\omega)^k = \sum_{h=0}^{\infty} a_h(k) x^{h-k}$$

with integral coefficients $a_h(k)$. Here evidently

$$a_0(k) = 1 ; \quad a_h(k) = 0 \quad \text{if} \quad h \ge 1 , \quad k = 0 ; \quad a_h(k) > 0 \quad \text{if} \quad k \ge 1 .$$

By means of the inequalities (1) we can easily obtain an upper estimate for these coefficients.

Assume for the moment that both h and k are positive, and put

$$s = (k/h)^{1/2}$$

in (1). The series (2) implies then that

$$0 \le a_h(k)e^{-2\pi(h-k)(k/h)^{\frac{1}{2}}} < \begin{cases} \left(e^{2\pi(k/h)^{\frac{1}{2}}}+1199\right)^k & \text{if } 1 \le h \le k , \\ \left(e^{2\pi(h/k)^{\frac{1}{2}}}+1199\right)^k & \text{if } 1 \le k \le h , \end{cases}$$

or equivalently,

$$0 \le a_h(k) < e^{2\pi(hk)^{\frac{1}{2}}}\left(1+1199e^{-2\pi(k/h)^{\frac{1}{2}}}\right)^k \quad \text{if } 1 \le h \le k ,$$

and

$$0 \le a_h(k) < e^{4\pi(hk)^{\frac{1}{2}}}\left(e^{-2\pi(k/h)^{\frac{1}{2}}}\left\{1+1199e^{-2\pi(h/k)^{\frac{1}{2}}}\right\}\right)^k \quad \text{if } 1 \le k \le h .$$

In these estimates, firstly

$$e^{-2\pi(k/h)^{\frac{1}{2}}} < 1 .$$

Secondly, the derivative with respect to k of

$$\left(1+1199e^{-2\pi(k/h)^{\frac{1}{2}}}\right)^k$$

is negative. This function of k is therefore decreasing, and it follows that

$$\left(1+1199e^{-2\pi(k/h)^{\frac{1}{2}}}\right)^k \le \left(1+1199e^{-2\pi h^{-\frac{1}{2}}}\right)^1 < 1200 .$$

Thirdly, if $1 \le k \le h$,

$$\left(1+1199e^{-2\pi(h/k)^{\frac{1}{2}}}\right)^k \le \left(1+1199e^{-2\pi(h/k)^{\frac{1}{2}}}\right)^h ,$$

whence, by the preceding inequality applied with h and k interchanged,

$$\left(1+1199e^{-2\pi(h/k)^{\frac{1}{2}}}\right)^k < 1200 .$$

We find therefore in both cases $1 \le h \le k$ and $1 \le k \le h$ that

$$(3) \qquad 0 \le a_h(k) \le 1200.e^{4\pi(hk)^{\frac{1}{2}}} .$$

It is easily verified that this estimate remains still valid when one or both of h and k are equal to zero.

4.

From now on let $m \ge 2$ be a fixed integer. Put

$$M = \psi(m) = m \prod_{p|m} \left(1 + \frac{1}{p}\right)$$

where in the product p runs over all the distinct prime factors of m. Denote by T the set of all triplets $\{A, B, D\}$ of integers A, B, D satisfying

$$1 \le A \le m, \quad 0 \le B \le D-1, \quad 1 \le D \le m, \quad AD = m, \quad (A, B, D) = 1 .$$

Let further $T(A, D)$ be the subset of those triplets in T for which A and D are fixed. The set T has exactly M elements, and there are $d(m)$ different sets $T(A, D)$ where $d(m)$ denotes the number of divisors of m.

With each triplet $\{A, B, D\}$ in T, we associate the modular function

$$j\left(\frac{A\omega+B}{D}\right), = j(\omega \mid A, B, D) \quad \text{say,}$$

which is of level m; there are M such functions. Each of these functions can be derived from every other one by a suitable modular transformation

$$\omega \to \frac{\alpha\omega+\beta}{\gamma\omega+\delta} ,$$

where $\alpha, \beta, \gamma, \delta$ are again integers of determinant 1.

By the theory of the modular function $j(\omega)$, there exists a unique primitive irreducible symmetric polynomial $F_m(u, v) \not\equiv 0$ in two variables u and v with integral coefficients such that

$$F_m\big(j(\omega \mid A, B, D), j(\omega)\big) = 0$$

identically in ω *for all triplets* $\{A, B, D\}$ *in* T.

This polynomial is of degree M in both u and v, and its terms of highest degree in these two variables are exactly u^M and v^M, respectively. In explicit form,

$$F_m\big(u,\ j(\omega)\big) = \prod_T \big(u - j(\omega \mid A,\ B,\ D)\big)\ ,$$

where the product extends over all the triplets in T.

We can write $F_m(u, v)$ as

$$F_m(u,\ v) = \sum_{k=0}^{M} \sum_{l=0}^{M} f_{kl} u^{M-k} v^{M-l}\ ,$$

where all the coefficients f_{kl} are integers. Put

$$L_m = \sum_{k=0}^{M} \sum_{l=0}^{M} |f_{kl}|\ .$$

It is known that with increasing m this number L_m quickly becomes very large. Our aim will be to find an upper estimate for L_m.

For this purpose we shall construct a second polynomial $G(u, v) \not\equiv 0$ with integral coefficients which is divisible by $F_m(u, v)$. This new polynomial will be of higher degree than M in u and v, but it has the advantage that it is easier to find an upper estimate for the sum of the absolute values of its coefficients. As a first step to the construction of $G(u, v)$ we shall construct the Laurent series in fractional powers of x of the function

(4) $$J_{kl}(\omega \mid A,\ B,\ D) = j(\omega \mid A,\ B,\ D)^k j(\omega)^l\ , \quad (k,\ l = 0,\ 1,\ 2,\ \ldots)\ .$$

5.

We begin with the series for $j(\omega \mid A, B, D)^k$ where $\{A, B, D\}$ is any triplet in T, while as before $k \geq 0$. Put

$$\varepsilon = e^{2\pi i/D}\ ,$$

so that by (2),

$$j(\omega \mid A, B, D)^k = \sum_{h=0}^{\infty} a_h(k)\left(\varepsilon^B x^{A/D}\right)^{h-k} .$$

Here h can be written as

$$h = rD + \rho \text{ , where } r = 0, 1, 2, \ldots \text{ , and } \rho = 0, 1, \ldots, D-1 .$$

Since

$$\varepsilon^D = 1 \text{ , } \left(\varepsilon^B x^{A/D}\right)^D = x^A = x^{m/D} ,$$

it follows that

$$j(\omega \mid A, B, D)^k = \sum_{\rho=0}^{D-1} \varepsilon^{B(\rho-k)} \sum_{r=0}^{\infty} a_{rD+\rho}(k) x^{\{mr+A(\rho-k)\}/D} .$$

Since also

$$j(\omega) = \sum_{s=0}^{\infty} a_s(l) x^{s-l} ,$$

the functions (4) have then the Laurent series

$$J_{kl}(\omega \mid A, B, D) = \sum_{\rho=0}^{D-1} \varepsilon^{B(\rho-k)} \sum_{r=0}^{\infty} a_{rD+\rho}(k) x^{\{mr+A(\rho-k)\}/D} \sum_{s=0}^{\infty} a_s(l) x^{s-l} ,$$

or say,

$$(5) \quad J_{kl}(\omega \mid A, B, D) = \sum_{\rho=0}^{D-1} \varepsilon^{B(\rho-k)} \sum_{h=0}^{\infty} a_{h,\rho}(k, l \mid A, D) x^{\{h-Ak-Dl\}/D} .$$

Here the new coefficients $a_{h,\rho}$ are non-negative integers which depend on A and D , but not on B . They have the explicit form

$$a_{h,\rho}(k, l \mid A, D) = \sum_{r,s} a_{rD+\rho}(k) a_s(l) ,$$

where the summation extends over all pairs of non-negative integers r, s for which

$$\{mr+A(\rho-k)\} + D(s-l) = h - Ak - Dl ,$$

that is,

$$mr + Ds = h - A\rho .$$

Since $AD = m$, this condition is equivalent to

$$Ar + s = \frac{h-A\rho}{D} .$$

Since r and s are non-negative, it can then only be satisfied if simultaneously

$$h \equiv A\rho \pmod{D} \quad \text{and} \quad h \ge A\rho .$$

Put therefore

$$\sigma = \frac{h-A\rho}{D} \quad \text{and} \quad H = \left[\frac{\sigma}{A}\right] = \left[\frac{h-A\rho}{m}\right] .$$

Then σ and H are non-negative integers such that

$$h = A\rho + D\sigma \quad \text{and} \quad 0 \le H \le \frac{h-A\rho}{m} \le \frac{h}{m} .$$

In this new notation, the formula for $a_{h,\rho}$ can be written as

(6) $$a_{h,\rho}(k,\ l \mid A,\ D) = \sum_{r=0}^{H} a_{Dr+\rho}(k) a_{\sigma-Ar}(l) .$$

Here the sum on the right-hand side contains

$$H + 1 \le \frac{h}{m} + 1$$

terms.

6.

An upper bound for the coefficients $a_{h,\rho}$ can be obtained as follows. Denote by t a real variable, and put

$$\Theta(t) = \{(Dt+\rho)k\}^{\frac{1}{2}} + \{(\sigma-At)l\}^{\frac{1}{2}} .$$

Then, by (3), the products on the right-hand side of (6) satisfy the inequality

$$0 \le a_{Dr+\rho}(k) a_{\sigma-Ar}(l) \le 1200^2 \exp\left(4\pi\Theta(r)\right) .$$

Therefore

$$0 \le a_{h,\rho}(k,\ l \mid A,\ D) \le 1200^2 \left(\frac{h}{m} + 1\right) \exp\left(4\pi\Theta(\bar{r})\right) ,$$

where $\bar{r}$ has been chosen so as to make $\Theta(r)$ a maximum.

The integer $\bar{r}$ lies in the interval $0 \le \bar{r} \le \frac{\sigma}{A}$ because the suffix $\sigma - Ar$ cannot be negative. Let t be a real variable in the same interval $0 \le t \le \frac{\sigma}{A}$, and put

$$x = \{(Dt+\rho)k\}^{\frac{1}{2}} \quad \text{and} \quad y = \{(\sigma-At)l\}^{\frac{1}{2}} .$$

Then, identically in t, the expressions

$$\gamma(x, y) = x + y \quad \text{and} \quad \Gamma(x, y) = Alx^2 + Dky^2 - hkl$$

satisfy the equations

$$\Theta(t) = \gamma(x, y) \quad \text{and} \quad \Gamma(x, y) = 0 .$$

The maximum of $\Theta(t)$ can then be obtained by applying Lagrange's method to the function

$$\gamma(x, y) + \Lambda\Gamma(x, y) ,$$

where Λ is Lagrange's parameter. This maximum is easily found to be

$$\left(\frac{(Al+Dk)h}{AD}\right)^{\frac{1}{2}} \quad \text{where} \quad AD = m ,$$

and naturally $\Theta(\bar{r})$ cannot be larger. Hence we find that

(7) $$0 \le a_{h,\rho}(k, l \mid A, D) \le 1200^2\left(\frac{h}{m} + 1\right)\exp\left(4\pi\left(\frac{(Al+Dk)h}{m}\right)^{\frac{1}{2}}\right)$$
if $h \equiv A\rho \pmod{D}$, $h \ge A\rho$,

but that

(8) $$a_{h,\rho}(k, l \mid A, D) = 0 \quad \text{otherwise.}$$

It is interesting to note that the upper bound in (7) does not depend on ρ.

7.

Next denote by N a positive integer and by

$$c_{kl} \quad (k, l = 0, 1, \ldots, N)$$

a set of $(N+1)^2$ indeterminates; both N and the indeterminates will be fixed later.

In the polynomial

$$G(u, v) = \sum_{k=0}^{N} \sum_{l=0}^{N} c_{kl} u^{N-k} v^{N-l}$$

replace u and v by

$$u = j(\omega \mid A, B, D) \quad \text{and} \quad v = j(\omega) \ .$$

Then $G(u, v)$ becomes a modular function $G(\omega \mid A, B, D)$ of level m,

$$G(\omega \mid A, B, D) = G\big(j(\omega \mid A, B, D), j(\omega)\big) =$$
$$= \sum_{k=0}^{N} \sum_{l=0}^{N} c_{kl} J_{N-k, N-l}(\omega \mid A, B, D) \ .$$

This function can again be written as a Laurent series

$$G(\omega \mid A, B, D) = \sum_{j=0}^{\infty} G_j(A, B, D) x^{\{j-(A+D)N\}/D} \ , \tag{9}$$

where, by (5), the new coefficients $G_j(A, B, D)$ have the form

$$G_j(A, B, D) = \sum_k \sum_l \sum_\rho \sum_h c_{kl} \varepsilon^{B(\rho-N+k)} a_{h,\rho}(N-k, N-l \mid A, D) \ . \tag{10}$$

Here the summation extends over all sets of integers k, l, ρ, h satisfying

$$0 \le k \le N \ , \quad 0 \le l \le N \ , \quad 0 \le \rho \le D-1 \ , \quad h + Ak + Dl = j \ .$$

To these conditions we may add the congruence $h \equiv A\rho \pmod{D}$ and hence also

$$j \equiv A(\rho+k) \pmod{D} \ . \tag{11}$$

For if either of these congruences does not hold, then $a_{h,\rho} = 0$ by (8), so that the corresponding term in (10) makes no contribution to the multiple sum.

8.

In order to learn more about the coefficients G_j, we apply the previous assumptions

$$(A, B, D) = 1 \quad \text{and} \quad AD = m \ .$$

It follows that, on putting

$$(A,\ D) = \Delta\ ,\quad A = a\Delta\ ,\quad D = d\Delta\ ,$$

we have

$$\Delta^2 | m\ ,\quad (a,\ d) = 1\ ,\quad (\Delta,\ B) = 1\ .$$

The congruence (11) now takes the form

(12) $$j \equiv a\Delta(\rho+k) \pmod{d\Delta}$$

and implies that

$$\Delta | j\ .$$

There is then an integer $J \geq 0$ such that

$$j = J\Delta\ .$$

Since $(a,\ d) = 1$, there further exists an integer $\bar{a}$ satisfying

$$a\bar{a} \equiv 1 \pmod{d}\ .$$

The congruence (12) is now equivalent to

$$J \equiv a(\rho+k) \pmod{d}\ ,$$

hence implies that

$$\rho + k \equiv \bar{a}J \pmod{d}\ .$$

Therefore, if $a_{h,\rho}$ does not vanish, then $\rho + k$ necessarily lies in one of the Δ residue classes

(13) $$\rho + k \equiv \bar{a}J + \nu d \pmod{D}\ ,\ \text{where}\quad \nu = 0,\ 1,\ \ldots,\ \Delta-1\ .$$

By $D = d\Delta$,

$$\varepsilon = e^{2\pi i/D} = e^{2\pi i/(d\Delta)}\ .$$

It follows that

$$\varepsilon^{B(\rho-N+k)} = \varepsilon^{B(\bar{a}J-N)}\eta^{B\nu}\ ,\ \text{where}\quad \eta = e^{2\pi i/\Delta}\quad \text{and}\quad \nu = 0,\ 1,\ \ldots,\ \Delta-1\ .$$

Here η is a primitive Δth. root of unity, B is relatively prime to Δ , and so $\eta^{B\nu}$ assume exactly the distinct values

$$1,\ \eta,\ \eta^2,\ \ldots,\ \eta^{\Delta-1}\ .$$

9.

The relations (9) and (10) can now be simplified. The formula (9) immediately becomes

$$(14) \qquad G(\omega \mid A,\, B,\, D) = \sum_{J=0}^{\infty} G_{J\Delta}(A,\, B,\, D)x^{\{J-(a+d)N\}/d} ,$$

with coefficients $G_{J\Delta}$ which can be written in the form

$$(15) \qquad G_{J\Delta}(A,\, B,\, D) = \varepsilon^{B(\bar{a}J-N)} \sum_{\nu=0}^{\Delta-1} \eta^{B\nu} L_{J,\nu}(A,\, D) .$$

Here $L_{J,\nu}$ is independent of B and is defined by the multiple sum

$$(16) \qquad L_{J,\nu}(A,\, D) = \sum_{k} \sum_{l} \sum_{h} C_{kl} a_{h,\rho}(N-k,\, N-l \mid A,\, D) ,$$

where the summations are extended over all sets of integers $k,\, l,\, h$ satisfying

$$0 \le k \le N , \quad 0 \le l \le N , \quad h + Ak + Dl = J\Delta ,$$

and where ρ denotes the unique integer which satisfies the two conditions

$$\rho + k \equiv \bar{a}J + \nu d \pmod{D} , \quad 0 \le \rho \le D-1 .$$

Actually, the summation over h is trivial since h can only have the single value

$$h = \Delta(J-ak-dl) .$$

This formula shows that also h is divisible by Δ .

The expressions $L_{J,\nu}$ are linear forms in the $(N+1)^2$ indeterminates C_{kl} with non-negative integral coefficients $a_{h,\rho}$. If all these coefficients of $L_{J,\nu}$ are zero, define a quantity $\Lambda_{J,\nu}(A,\, D)$ by

$$\Lambda_{J,\nu}(A,\, D) = 1 .$$

Otherwise denote by $\Lambda_{J,\nu}(A,\, D)$ the sum of the coefficients of $L_{J,\nu}$,

$$(17) \qquad \Lambda_{J,\nu}(A,\, D) = \sum_{k} \sum_{l} a_{h,\rho}(N-k,\, N-l \mid A,\, D) .$$

Here ρ and the summations are just as (16), but the trivial summation over h has now not been indicated. We see that for all values of J, ν, A, and D

$$\Lambda_{J,\nu}(A, D) \geq 1$$

is a positive integer.

An upper estimate for $\Lambda_{J,\nu}(A, D)$ can be obtained as follows.

The sum (17) for $\Lambda_{J,\nu}$ consists of $(N+1)^2$ terms $a_{h,\rho}(N-k, N-l \mid A, D)$ where by (7) each of these terms satisfies an inequality

$$0 \leq a_{h,\rho}(N-k, N-l \mid A, D) \leq 1200^2\left(\frac{h}{m} + 1\right)\exp\left(4\pi\left(\frac{\{A(N-l)+D(N-k)\}h}{m}\right)^{\frac{1}{2}}\right) ,$$

and where

$$A = a\Delta , \quad D = d\Delta , \quad h = \Delta(J-ak-dl) \leq \Delta J .$$

Since k and l are non-negative, it follows that

$$0 \leq a_{h,\rho}(N-k, N-l \mid A, D) \leq 1200^2\left(\frac{\Delta J}{m} + 1\right)\exp\left(4\pi\Delta\left(\frac{(a+d)NJ}{m}\right)^{\frac{1}{2}}\right) .$$

This estimate is uniform in k and l and hence implies that

$$(18) \qquad 1 \leq \Lambda_{J,\nu}(A, D) \leq 1200^2(N+1)^2\left(\frac{\Delta J}{m} + 1\right)\exp\left(4\pi\Delta\left(\frac{(a+d)NJ}{m}\right)^{\frac{1}{2}}\right)$$

for all suffices J and ν and for all triplets $\{A, B, D\}$ in T.

10.

The terms in the Laurent series (14) for $G(\omega \mid A, D)$ contain non-positive powers of x as long as

$$0 \leq J \leq (a+d)N .$$

There are thus

$$(a+d)N + 1$$

such terms, with the coefficients

$$G_{J\Delta}(A, B, D) , \quad (J = 0, 1, \ldots, (a+d)N) .$$

We associate now with the triplet $\{A, B, D\}$ in T the system of $(a+d)N+1$ equations

$$G_{J\Delta}(A, B, D) = 0 , \quad \big(J = 0, 1, \ldots, (a+d)N\big) .$$

From the representation (15) it is obvious that this system of equations is satisfied if the following second system of equations

$$E(A, D): \quad L_{J,\nu}(A, D) = 0 , \quad \begin{pmatrix} J = 0, 1, \ldots, (a+d)N \\ \nu = 0, 1, \ldots, \Delta-1 \end{pmatrix}$$

holds. This system no longer depends on B, but is the same for all triplets in the set $T(A, D)$.

Finally denote by E the union of all the several systems $E(A, D)$,

$$E: \quad L_{J,\nu}(A, D) = 0 , \quad \begin{pmatrix} J = 0, 1, \ldots, (a+d)N \\ \nu = 0, 1, \ldots, \Delta-1 \\ A \geq 1,\ D \geq 1,\ AD = m \end{pmatrix} .$$

Each system $E(A, D)$ consists of

$$\Delta\big((a+d)N+1\big) = (A+D)N + \Delta = (A+D)N + (A, D) \leq (A+D)(N+1)$$

equations since trivially $(A, D) \leq A + D$. The number of equations of E is therefore at most

$$2\sigma(m)(N+1), = U \text{ say,}$$

where as usual $\sigma(m)$ denotes the sum of the positive divisors of m; for both A and D run exactly over these divisors.

On the other hand, each of the equations of E is a homogeneous linear equation for the

$$(N+1)^2, = V \text{ say,}$$

indeterminates C_{kl}, with integral coefficients ≥ 0 the sum of which is estimated in (18).

11.

So far the indeterminates C_{kl} were not yet fixed; let us now take for them rational integers not all zero such that the equations of E are satisfied.

For this purpose we shall apply the following lemma which goes back at least to the paper Baker [1].

LEMMA 1. *Let*

$$(g_{ij}) \ , \quad \begin{pmatrix} i = 1, 2, \ldots, u \\ j = 1, 2, \ldots, v \end{pmatrix} ,$$

where $u < v$ *, be a matrix with integral elements and let*

$$g_i = \max\left(1, \sum_{j=1}^{v} |g_{ij}|\right) , \quad (i = 1, 2, \ldots, u) .$$

Then there exist integers $x_1, x_2, \ldots, x_v$ *not all zero such that*

$$\sum_{j=1}^{v} g_{ij}x_j = 0 \quad \textit{for} \quad i = 1, 2, \ldots, u \ ;$$

$$\max(|x_1|, \ldots, |x_v|) \le (g_i \ldots g_u)^{\frac{1}{v-u}} .$$

For the application soon to be made, we note that this estimate for the x's remains valid if $u, g_1, \ldots, g_v$ in the upper estimate are replaced by larger numbers provided only that u remains less than v .

We found that the total number of linear equations E for the $V = (N+1)^2$ indeterminates C_{kl} was not greater than $U = 2\sigma(m)(N+1)$. The lemma may therefore be applied with $u = U$ and $v = V$ provided that $U < V$, that is,

(19) $$N \ge 2\sigma(m) .$$

Let this condition for N *from now on be satisfied.*

First consider the set of equations $E(A, D)$ that belong to any given pair A, D of complementary divisors of m . The maxima g_i in Lemma 1 can in this case be identified with the integers $\Lambda_{J,\nu}(A, D)$, and their product for $E(A, D)$ becomes

$$\prod_J \prod_\nu \Lambda_{J,\nu}(A, D), = P(A, D) \quad \text{say;}$$

here J runs over the values $0, 1, \ldots, (a+d)N$, and ν over the values

$0, 1, \ldots, \Delta-1$. For the union E of all the sets of equations $E(A, D)$ the product of the corresponding maxima g_i becomes therefore

$$\prod_{A,D} P(A, D) = \prod_{A,D} \prod_{J} \prod_{\nu} \Lambda_{J,\nu}(A, D), = P \quad \text{say.}$$

Here the new product $\prod_{A,D}$ extends over all pairs A, D of complementary divisors of m .

12.

An upper estimate for the product P can be found as follows.

The formula (18) gave an upper bound for $\Lambda_{J,\nu}(A, D)$ which did not depend on ν . Here ν has the Δ possible values $0, 1, 2, \ldots, \Delta-1$, and J assumes the $(a+d)N + 1$ values $0, 1, 2, \ldots, (a+d)N$. The formula (18) leads therefore to the estimate

$$1 \le P(A, D) \le \left(1200^2(N+1)^2\right)^{\Delta\{(a+d)N+1\}} \prod_{J=0}^{(a+d)N} \left(\frac{\Delta J}{m} + 1\right)^{\Delta} \cdot$$
$$\cdot \exp\left(4\pi\Delta^2\left(\frac{(a+d)N}{m}\right)^{\frac{1}{2}} \sum_{J=0}^{(a+d)N} J^{\frac{1}{2}}\right) .$$

This formula can be slightly simplified, as follows.

It is obvious that

$$(a+d)N \ge 2 \text{ , and that therefore } 2\Delta\{(a+d)N+1\} \le 3\Delta(a+d)N .$$

Further, by hypothesis, $m \ge 2$ and $\Delta^2 | m$, hence

$$\frac{\Delta}{m} \le \frac{1}{2} \text{ , so that } \frac{\Delta J}{m} + 1 \le J \quad \text{if} \quad J \ge 2 .$$

Also it is easily proved that

$$n! \le \frac{2}{3} n^n \quad \text{if} \quad n \ge 2 .$$

It follows that

$$\prod_{J=0}^{(a+d)N} \left(\frac{\Delta J}{m} + 1\right) \le \frac{3}{2} \prod_{J=1}^{(a+d)N} J = \frac{3}{2}\left((a+d)N\right)! \le \left((a+d)N\right)^{(a+d)N} ,$$

hence that

$$\left(1200^2(N+1)^2\right)^{\Delta\{(a+d)N+1\}} \prod_{j=0}^{(a+d)N} \left(\frac{\Delta J}{m} + 1\right) \le \left(1200^3(N+1)^4(a+d)\right)^{\Delta(a+d)N} .$$

Next, trivially,

$$\sum_{j=0}^{(a+d)N} J^{\frac{1}{2}} \le (a+d)N \cdot \left((a+d)N\right)^{\frac{1}{2}} = \left((a+d)N\right)^{3/2} .$$

Therefore, by $A = a\Delta$, $D = d\Delta$, and $\Delta \ge 1$,

$$(20) \qquad 1 \le P(A, D) \le \left(1200^3(N+1)^4(a+d)\right)^{(A+D)N} \cdot \exp\left(4\pi \frac{(A+D)^2N^2}{m^{\frac{1}{2}}}\right) .$$

This estimate finally leads also to one for P . We know that $A \ge 1$ and $D \ge 1$ run over all pairs of complementary divisors of m . Denote then, as usual, by $d(m)$ the number of positive divisors of m , by $\sigma(m)$ again the sum of these divisors; and by $\sigma_2(m)$ the sum of their squares. It is immediately clear that

$$\sum_{A,D} (A+D) = 2\sigma(m) , \quad \sum_{A,D} (A+D)^2 = 2\sigma_2(m) + 2md(m) .$$

Further, trivially, $A + D \le m + 1$, whence

$$\sum_{A,D} (A+D)\log(A+D) \le 2\sigma(m)\log(m+1) ,$$

and the same upper estimate holds also for

$$\sum_{A,D} (A+D)\log(a+d) .$$

Therefore by (20) and by the definition of P ,

$$(21) \qquad 1 \le P \le \left(1200^3(N+1)^4(m+1)\right)^{2\sigma(m)N}\exp\left(8\pi \frac{\sigma_2(m)+md(m)}{m^{\frac{1}{2}}} N^2\right) .$$

13.

Lemma 1 can now be applied to the system E which consists of at most

$$U = 2\sigma(m)(N+1)$$

homogeneous linear equations for the

$$V = (N+1)^2$$

indeterminates C_{kl}. We choose for N the odd integer

$$N = 4\sigma(m) - 1 > 2\sigma(m) ,$$

so that

$$(N+1)^2 = 16\sigma(m) , \quad U = 8\sigma(m)^2 , \quad V = 16\sigma(m)^2 , \quad V - U = 8\sigma(m)^2 .$$

By Lemma 1, *there exist integers*

$$C_{kl} \quad (k,\ l = 0,\ 1,\ \ldots,\ N)$$

not all zero such that

$$1 \le \max_{k,l} |C_{kl}| \le P^{1/(V-U)}$$

and that all the equations of E *are satisfied.*

Substitute here for P its upper estimate (21). The exponent of the first factor on the right-hand side of (21) divided by $V - U$ is equal to

$$\frac{2\sigma(m)}{V-U} = \frac{4\sigma(m)N}{V} < \frac{4\sigma(m)}{N+1} = 1 .$$

In the second factor,

$$\frac{N^2}{V-U} = \frac{2N^2}{V} = \frac{2N^2}{(N+1)^2} < 2 ,$$

so that this factor raised to the power $1/(V-U)$ gives the contribution

$$\exp\left(16\pi \frac{\sigma_2(m)+md(m)}{m^{\frac{1}{2}}}\right) .$$

Hence the estimate for $\max|C_{kl}|$ takes the explicit form

$$1 \le \max_{k,l} |C_{kl}| \le 1200^3\left(4\sigma(m)\right)^4(m+1)\exp\left(16\pi \frac{\sigma_2(m)+md(m)}{m^{\frac{1}{2}}}\right) .$$

From this we finally deduce that

$$(22) \qquad 1 \le \sum_{k=0}^{N} \sum_{l=0}^{N} |C_{kl}| \le 1200^3\left(4\sigma(m)\right)^6(m+1)\exp\left(16\pi \frac{\sigma_2(m)+md(m)}{m^{\frac{1}{2}}}\right) .$$

14.

The expression

$$G(\omega) = G(\omega \mid m, 0, 1) = G\big(j(m\omega), j(\omega)\big)$$

is again a modular function of level m. In the fundamental region

$$|R(\omega)| \le \frac{1}{2}, \quad |\omega| \ge 1$$

of $j(\omega)$, $G(\omega)$ has its only possible pole at the point at infinity, that is, at $x = 0$. If any modular substitution

$$\omega \to \frac{\alpha\omega+\beta}{\gamma\omega+\delta}, \text{ where } \alpha, \beta, \gamma, \delta \text{ are integers and } \alpha\delta - \beta\gamma = 1,$$

is applied to the variable ω, then $G(\omega)$ is changed into one of the functions

$$G(\omega \mid A, B, D) = G\left(j\left(\frac{A\omega+B}{D}\right), j(\omega)\right), \text{ where } \{A, B, D\} \text{ is a triplet in } T.$$

A possible pole of any one of these functions either lies again at the point at infinity, that is, at $x = 0$; or it lies at a rational point on the real axis. In the latter case a suitable modular transformation changes this point into the point at infinity, and so some function $G(\omega \mid A', B', D')$, where also $\{A', B', D'\} \in T$, would have at pole at $x = 0$.

However, our construction of $G(u, v)$ was such that the series (9) of each one of the functions $G(\omega \mid A, B, D)$ contained only *positive* (possibly fractional) powers of x. Therefore, when $G(\omega)$ is considered in the whole upper half-plane, it has no poles at all, but it has zeros at $x = 0$ for its different branches. This has the immediate consequence that

$$G\big(j(m\omega), j(\omega)\big) \equiv 0 \text{ \textit{identically in} } \omega.$$

On the other hand, also the mth transformation polynomial $F_m(u, v)$ has the property that

$$F_m\big(j(m\omega), j(\omega)\big) \equiv 0 \text{ identically in } \omega.$$

Further the polynomial $F_m\big(u, j(\omega)\big)$ is known to be irreducible over the transcendental extension $C\big(j(\omega)\big)$ of the complex number field C. It follows then that the polynomial $G\big(u, j(\omega)\big)$ is divisible by the polynomial $F_m(u, j(\omega))$, and hence also *the polynomial* $G(u, v)$ *by the polymonial* $F_m(u, v)$.

Both polynomials $F_m(u, v)$ and $G(u, v)$ have integral coefficients, and the sum of the absolute values of the coefficients of $G(u, v)$ allows the estimate (22).

The quotient polynomial $H(u, v)$ defined by

$$G(u, v) = F_m(u, v)H(u, v)$$

has again integral coefficients because $F_m(u, v)$ is primitive. Hence the sum of the absolute values of the coefficients of $H(u, v)$ is not less than 1.

Further $G(u, v)$ has in both u and v at most the degree N, and

$$2^{N+N} < 2^{8\sigma(m)} .$$

The general inequality (I) of my paper [3] leads therefore immediately to the following result.

THEOREM 1. *The sum of the absolute values of the coefficients of the mth transformation polynomial* $F_m(u, v)$ *does not exceed*

$$1200^3\left(4\sigma(m)\right)^6(m+1) \cdot 2^{8\sigma(m)} \cdot \exp\left(16\pi \frac{\sigma_2(m)+md(m)}{m^{\frac{1}{2}}}\right) .$$

We see that there exists a positive absolute constant c (which can be found effectively) such that the sum of the absolute values of the coefficients of $F_m(u, v)$ is at most

$$e^{cm^{3/2}} .$$

It seems very probable that this upper bound can be improved.

15.

As an application, consider an arbitrary primitive irreducible quadratic equation with integral coefficients

(23) $$a_0\Omega^2 + a_1\Omega + a_2 = 0 \text{ , where } a_0 > 0 \text{ , } 4a_0a_2 - a_1^2 > 0 .$$

This equation has just one complex root with *positive* imaginary part, ω say, and this root generates an imaginary quadratic field

$$K = Q(\omega)$$

over the rational field Q.

Denote by h the class number of K. It is proved in the theory of complex multiplication (see for example, Fueter [2]) that the singular value

$$S = j(\omega)$$

of the modular function is algebraic of the exact degree $2h$ over Q. Denote by

$$A_0x^{2h} + A_1x^{2h-1} + \ldots + A_{2h} = 0$$

the primitive irreducible algebraic equation with integral coefficients for S; here in fact A_0 may be taken equal to 1.

Put now

$$A = |A_0| + |A_1| + \ldots + |A_{2h}| .$$

By means of Theorem 1 we can establish an upper bound for A which depends only on the coefficients of the equation (23) for ω.

For this purpose write the equation (23) in the equivalent form

$$\Omega = \frac{-a_2}{a_0\Omega+a_1} .$$

In the usual terminology of the theory of complex multiplication, this is a substitution of order $m = a_0a_2$ and it implies that S satisfies the algebraic equation

$$F_m(u, u) = 0 .$$

Here $F_m(u, v)$ as before is the mth transformation polynomial. If in this polynomial u and v are identified, $F_m(u, u)$ becomes a polynomial not identically zero with integral coefficients, and it is obvious that the sum of the absolute values of the coefficients of $F_m(u, u)$ is not larger than the analogous sum for $F_m(u, v)$. It is further clear that the polynomial

$$A_0u^{2h} + A_1u^{2h-1} + \dots + A_{2h}$$

is a divisor of $F_m(u, u)$. Further $F_m(u, u)$ has at most the degree $2N$. Hence, on applying once more the theorem of my paper [3], it follows that

$$A \le 1200^3\left(4\sigma(m)\right)^6(m+1) \cdot 2^{16\sigma(m)} \cdot \exp\left(16\pi \frac{\sigma_2(m)+md(m)}{m^{\frac{1}{2}}}\right) .$$

Thus there exists a positive absolute constant C such that for all quadratic equations (23) the sum of the absolute values of the primitive irreducible equation for the singular module S does not exceed the value

$$e^{C\left(a_0a_2\right)^{3/2}} .$$

References

[1] A. Baker, "On some diophantine inequalities involving the exponential function", *Canad. J. Math.* **17** (1965), 616-626.

[2] R. Fueter, *Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen*, Erster Teil (Teubners Sammlung von Lehrbüchern auf dem Gebiete der mathematischen Wissenschaften, Band **41**. Verlag und Druck von B.G. Teubner, Leipzig, Berlin, 1924).

[3] K. Mahler, "On some inequalities for polynomials in several variables", *J. London Math. Soc.* **37** (1962), 341-344.

[4] Kurt Mahler, "On the coefficients of the 2^n-th transformation polynomial for $j(\omega)$ ", *Acta Arith.* **21** (1972), 89-97.

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, ACT.