Can. J. Math., Vol. XXIII, No. 6, 1971, pp. 960–968

WEIERSTRASS POINTS AT THE CUSPS OF $\Gamma_0(16p)$ AND HYPERELLIPTICITY OF $\Gamma_0(n)$.

H. LARCHER

For a fixed positive integer n we consider the subgroup $\Gamma_0(n)$ of the modular group $\Gamma(1)$. $\Gamma_0(n)$ consists of all linear fractional transformations $L: z \to (az + b)/(cz + d)$ with rational integers a, b, c, d, determinant $ad - bc = 1$, and $c \equiv 0 (\mathrm{mod}\, n)$. If $\mathscr{H} = \{z | z = x + iy,\ x \text{ and } y \text{ real and } y > 0\}$ is the upper half of the z-plane then $S_0 = S_0(n) = \mathscr{H}/\Gamma_0(n)$, properly compactified, is a compact Riemann surface whose genus we denote by $g(n)$. A point P of a Riemann surface S of genus g is called a Weierstrass point if there exists a function on S that has a pole of order $\alpha \leqq g$ at P and is regular everywhere else on S.

Lehner and Newman started the search for Weierstrass points of S_0 (or, loosely, of $\Gamma_0(n)$). In [**5**], they gave sufficient conditions for the cusps 0 and $i\infty$ to be Weierstrass points of $\Gamma_0(n)$ provided that $n \equiv 0 \pmod 4$ or $n \equiv 0 \pmod 9$. In [**1**], Atkin obtained a much more general result. We may loosely describe his result by the statement that "almost all" n which are not quadratfrei have the cusps 0 and $i\infty$ as Weierstrass points of $\Gamma_0(n)$. To qualify "almost all", we mention that his proof does not apply for relatively few, but still infinitely many n which are not quadratfrei. Among these are found the integers of the form $n = 16p$, where the prime $p \geqq 3$, and which are the objects of the first part of our investigation.

The papers [**5**] and [**1**] used the following result which is essentially due to Schoenberg (see [**8**]). Let S_1 and S_2 be compact Riemann surfaces of respective genera g_1 and g_2 ($g_2 \geqq 2$), and let $\Pi: S_2 \to S_1$ be an analytic branched covering such that all points on S_2 lying over the same point P of S_1 have the same branch order. If $n \geqq 2$ is the number of sheets in S_2 over S_1, and if S_2 has either (i) more than four branch points of order $n - 1$, or (ii) only one branch point of order $n - 1$ and the total branch order B of S_2 over S_1 satisfies $B \leqq 2(n - 2)$, then these branch points are Weierstrass points of S_2. The result is obtained by lifting suitable functions on S_1 to functions on S_2 and making use of the Riemann-Hurwitz relation $2(g_2 - 1) = 2n(g_1 - 1) + B$. If the relation is written in the form $n(g_1 + 1) = g_2 - (B - 4n + 2)/2$, we readily deduce that the points of branch order $n - 1$ are Weierstrass points provided that $B \geqq 4n - 2$ or $B \leqq 2n - 4$.

This paper consists of two parts whose results are contained in the following two theorems.

Received November 18, 1970 and in revised form, July 9, 1971.

https://doi.org/10.4153/CJM-1971-103-6 Published online by Cambridge University Press

THEOREM 1. *If the prime $p \geqq 3$, then all cusps of $\Gamma_0(16p)$ are Weierstrass points.*

THEOREM 2. *For all sufficiently large positive integers n, $\Gamma_0(n)$ is not hyperelliptic.*

The latter result may be compared with a conjecture by Lehner and Newman that for $n \geqq 72$, $\Gamma_0(n)$ is not hyperelliptic. The proof of Theorem 1 is based on the following result by Lewittes which is found in [**6**]. If H is a group of automorphisms of order k of a Riemann surface S of genus g (i.e., conformal homeomorphisms of S onto itself), D the vector space of abelian differentials of the first kind on S, and if h is an element of H, then h can be used to define a linear transformation on D. Thus we obtain a representation of H by a group of matrices H^*. If h generates H, $h(P) = P$ for a point P on S, and h rotates at P by ϵ, where ϵ is a primitive k-th root of unity, then with respect to a suitable basis in D, h has a representation by the diagonal matrix

$$\operatorname{diag}(\epsilon^{\gamma_1}, \epsilon^{\gamma_2}, \ldots, \epsilon^{\gamma_g}),$$

where $\gamma_1, \gamma_2, \ldots, \gamma_g$ are the gaps at P. Denoting the number of diagonal elements of the form $e^{2\pi i l/k}$ by $m(l)$ $(l = 0, 1, \ldots, k-1)$, it is clear that knowledge of the $m(l)$ might yield sufficient information to conclude that P is a Weierstrass point.

Proof of Theorem 1. First we compute the number of cusps of $S_0(16p)$ and the number of double triangles which meet at each cusp. These triangles derive from the standard triangulation of a fundamental domain of $\Gamma_0(16p)$. Since some of the results obtained here are of interest beyond the scope of this paper, we again let n by any positive integer. With regard to the following derivation, see also [**10**].

We consider the subgroup of $\Gamma(1)$ defined by

$$\Gamma_n = \sum_{k=1}^{n} \Gamma(n) U^k,$$

where $\Gamma(n)$ is the principal congruence subgroup of level n of $\Gamma(1)$ and $U: z \rightarrow z + 1$. If A is an element in Γ_n then

$$\bar{A} \equiv \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \pmod{n},$$

where the integer r satisfies $0 \leqq r \leqq n - 1$. Now it is readily verified that Γ_n is a normal subgroup of $\Gamma_0(n)$. From this, the determinant condition $ad \equiv 1 \pmod{n}$ for the elements of $\Gamma_0(n)$, and the observation that the pairs (a, d) and $(-a, -d)$ lead to the same substitution, follow that the factor group $\mathscr{V} = \Gamma_0(n)/\Gamma_n$ is a group of automorphisms of order $\frac{1}{2}\varphi(n)$ of $S(\Gamma_n)$, the compact Riemann surface associated with Γ_n, where $\varphi(n)$ is the Euler φ function. From now on, $S(G)$ denotes the Riemann surface associated with G, where G is a subgroup of $\Gamma(1)$. $\mathscr{V}$ may contain elliptic and parabolic elements and hence have elliptic and parabolic fixed points on $S(\Gamma_n)$. The number of elliptic elements depends on the number of incongruent solutions of the congruences $x^2 + 1 \equiv 0$ and $x^2 - x + 1 \equiv 0 \pmod n$. The number of parabolic substitutions in $\mathscr{V}$ is equal to the number of incongruent solutions of $x^2 \equiv 0 \pmod n$ with $x \not\equiv 0$. The last congruence has solutions provided only that n is not quadratfrei. If $n = d^2m$, where m is quadratfrei and $d > 1$, then the incongruent solutions are $x = kdm$ with $1 \leqq k \leqq d - 1$. Putting

$$\bar{A} = \begin{bmatrix} 1 + dm & -m \\ n & 1 - dm \end{bmatrix},$$

we see that

$$\bar{A}^k = \begin{bmatrix} 1 + kdm & -km \\ kn & 1 - kdm \end{bmatrix};$$

i.e., the parabolic substitutions in $\mathscr{V}$ form a cyclic subgroup $\mathscr{U}$ of order d.

To compute the fixed points of the group of automorphisms $\mathscr{U}$ on $S(\Gamma_n)$ we define

$$\mathscr{A} = \mathscr{A}(n) = \sum_{k=1}^{d} \Gamma_n A^k$$

and observe that $\mathscr{A}$ does not contain any elliptic transformations. For a positive divisor e of d and $e \neq d$ we denote by $h(e)$ the number of cusps on $S(\Gamma_n)$ which are fixed points of the parabolic substitutions B in $\mathscr{A}$ such that $B^{d/e}$ is in Γ_n and having the properties: (i) d/e is the smallest such integer, and (ii) there is no parabolic substitution B_1 in $\mathscr{A}$ such that $B_1{}^r = B$ for some $r > 1$. Now $h(e)$ is simply the number of modulo Γ_n inequivalent fixed points of the parabolic substitutions B whose matrices are of the form

$$\bar{B} = \begin{bmatrix} 1 + \lambda\mu edm & -\lambda^2\delta \\ \mu^2e^2mn/\delta & 1 - \lambda\mu edm \end{bmatrix},$$

where $(\mu, \lambda) = 1$, $(\mu, d/e) = 1$, $(\lambda, d/e) = 1$, $\delta | e^2m$, and $(\delta, e^2m/\delta) = 1$. The last three restrictions are necessary in order for B to satisfy the properties (i) and (ii), required in the definition of $h(e)$, while the restriction $(\mu, \lambda) = 1$ becomes obvious after writing down the fixed points of the substitutions B. It is well known that two pairs of integers $\{a, b\}$ and $\{a', b'\}$, where $(a, b, n) = 1$ and $(a', b', n) = 1$, are equivalent modulo $\bar{\Gamma}_n$, the homogeneous group associated with Γ_n, if and only if $b' \equiv b \pmod n$ and $a' \equiv a \pmod{(b, n)}$. Applying this to the fixed points of the substitutions B we obtain

$$h(e) = \tfrac{1}{2} \sum_{\delta | e^2m}^{*} \varphi(d\delta/e)\varphi(ne/d\delta).$$

This may be written in the form

$$h(e) = \tfrac{1}{2} \frac{e}{d} \varphi(n)\varphi(d/e) \sum_{\delta | e^2m}^{*} 1, \tag{1}$$

https://doi.org/10.4153/CJM-1971-103-6 Published online by Cambridge University Press

$n = d^2m$ and m quadratfrei. Here we use the symbol $\sum^*$ to indicate that summation is extended only over those divisors δ of e^2m for which $(\delta, e^2m/\delta) = 1$.

We derive one more formula which we need later on. If $e|n$ we denote by $\mathscr{C}_e$ the set of cusps on $S(\Gamma_n)$ at which e double triangles meet. If C is a parabolic substitution in Γ_n whose fixed point lies in $\mathscr{C}_e$, then for suitable λ and μ

$$\bar{C} = \begin{bmatrix} 1 + \lambda\mu n & -\lambda^2 e \\ \mu^2 \frac{n}{e} n & 1 - \lambda\mu n \end{bmatrix},$$

where $(\lambda, n/e) = 1$ and $(\mu, e) = 1$. Since the matrix of the transform of C under R: $z \to -1/nz$ is of the form

$$\begin{bmatrix} 1 - \lambda\mu n & -\mu^2 \frac{n}{e} \\ \lambda^2 en & 1 + \lambda\mu n \end{bmatrix},$$

we deduce

(2) $$R\,\mathscr{C}_e R^{-1} = \mathscr{C}_{n/e}.$$

To compute the number of cusps and the number of double triangles which meet at each cusp of $S(\Gamma_n)$, we make use of the formula

(3) $$f(e) = \tfrac{1}{2} e\varphi(e)\varphi(n/e),$$

where $e|n$ and $e \neq n$, which is due to Lewittes [7]. Here, $f(e)$ has the same meaning on $S(\Gamma(n))$ as $h(e)$ has on $S(\Gamma_n)$. If in (3) we replace e by n, we get the number of cusps on $\Gamma(n)$ which are not fixed points under any automorphism belonging to the group $\Gamma_n/\Gamma(n)$. This is an immediate consequence of formula (2). Now it is readily seen that for any e which is a divisor of n there are $f(e)/e$ cusps on $S(\Gamma_n)$ at which e double triangles meet. It is advantageous to introduce an expression from which this can be read off quickly. Making an unorthodox use of the set notation we define for Γ_n the "cusp schema"

(4) $$\mathscr{C}(\Gamma_n) = \{\tfrac{1}{2}\varphi(e)\varphi(n/e)C_e |\ e|n \text{ and } e > 0\},$$

where kC_j means that there are k cusps at which j double triangles meet.

After these preliminary results, we are ready to compute the "cusp schema" for $\Gamma_0(16p)$. From (4), it follows that

$$\mathscr{C}(\Gamma_{16p}) = \{\tfrac{1}{2}\varphi(e)\varphi(16p/e)C_e |\ e|16p \text{ and } e > 0\}.$$

By our theory, since $n = 4^2p$, $S(\Gamma_{16p})$ has a group of automorphisms of order 4. According to formula (1), there are $h(1) = 4\varphi(p)$ and $h(2) = 8\varphi(p)$ parabolic fixed points of order four and two, respectively. To decide which cusps on $S(\Gamma_{16p})$ are fixed under these automorphisms, we use (2) together with $R\mathscr{A}R^{-1} = \mathscr{A}$, which is readily verified. From $\mathscr{C}(\Gamma_{16p})$, one deduces that the fixed points of order four are the cusps of $\mathscr{C}_4$ and $\mathscr{C}_{4p}$ and that those of order two are the cusps of $\mathscr{C}_2$ and $\mathscr{C}_{8p}$. Hence, the "cusp schema" of $\mathscr{A}(16p)$ is

$$\mathscr{C}(\mathscr{A}) = \{4\varphi(p)C_1, 4\varphi(p)C_p, \varphi(p)C_4, \varphi(p)C_{4p}, \varphi(p)C_{16}, \varphi(p)C_{16p}\}.$$

Since $S(\mathscr{A})$ has a group of automorphisms of order $\varphi(p)$ without parabolic fixed points, we finally have

$$\mathscr{C}(\Gamma_0(16p)) = \{4C_1, 4C_p, C_4, C_{4p}, C_{16}, C_{16p}\}. \tag{5}$$

Now $\Gamma_0(16p)$ is a normal subgroup of index four of $\Gamma_0(4p)$. To show this we observe that if A is in $\Gamma_0(16p)$ and B is in $\Gamma_0(4p)$, where

$$\bar{A} = \begin{bmatrix} a & b \\ 16pc & d \end{bmatrix},$$

then BAB^{-1} is in $\Gamma_0(16p)$ provided that $a - d \equiv 0 \pmod 4$. Writing the determinant as the congruence $ad \equiv 1 \pmod 8$, we deduce that $a^2 + d^2 \equiv 2 \pmod 8$. The two congruences imply that $(a - d)^2 \equiv 0 \pmod 8$, and hence that $a - d \equiv 0 \pmod 4$. Thus the factor group $\Gamma_0(4p)/\Gamma_0(16p)$ is a group of automorphisms of order four of $S_0(16p)$. From the "cusp schema" (5), we see that it has four parabolic fixed points of order four, one of which is the cusp 0. To obtain a formula for $m(l)$ $(l = 1, 2, 3)$ at 0, we need the rotations $e^{2\pi i r_j/4}$, where $(r_j, 4) = 1$, produced by a generator of the group of automorphisms at all the fixed points P_j $(j = 1, 2, 3, 4)$. Here the r_j's are quadratic residues mod 4, and hence $r_j = 1$ $(j = 1, 2, 3, 4)$. To see the latter, one can simply write down the parabolic substitutions for the four fixed points and thus obtain the rotations. We do it in more generality, since it throws light on why and how the quadratic residues appear in the rotations.

Let G_1 be a normal subgroup of index k of G_2 and let A be a parabolic substitution such that $G_2 = \sum_{i=1}^{k} G_1 A^i$, where $\Gamma(n) \subset G_1 \subset G_2 \subset \Gamma(1)$. (We remark that in all the cases we run into here, the groups G_1 and G_2 can be characterized by arithmetic properties of the coefficients of their respective elements.) Then G_2/G_1 is a cyclic group of automorphisms of order k of $S(G_1)$. If the cusp P of $S(G_1)$ is a fixed point of A, then there is a parabolic substitution B in G_2 such that

$$\bar{B} = \begin{bmatrix} 1 + \lambda\mu a & -\lambda^2 b \\ \mu^2 c & 1 - \lambda\mu a \end{bmatrix},$$

where $bc = a^2$, $P = \lambda a/\mu c$, and k is the smallest positive integer such that B^k is in G_1. Putting $(\lambda, \mu) = \epsilon$, we observe that for any ϵ with $(\epsilon, k) = 1$, the parabolic substitution $B(\epsilon)$ with

$$\bar{B}(\epsilon) = \begin{bmatrix} 1 + \epsilon^2\lambda\mu a & -\epsilon^2\lambda^2 b \\ \epsilon^2\mu^2 e & 1 - \epsilon^2\lambda\mu a \end{bmatrix}$$

and $(\lambda, \mu) = 1$, is in G_2 and has the same properties as $\bar{B}$ above. In the usual triangulation of $S(G_1)$, a neighbourhood of P consists of a certain number of

https://doi.org/10.4153/CJM-1971-103-6 Published online by Cambridge University Press

double triangles. The two boundary arcs of this neighbourhood which meet at P are identified under $B^k(1)$. Putting $e(\alpha) = e^{2\pi i \alpha}$, we see that

$$t = e(1/\mu^2 ck(z - P)) \tag{6}$$

is a local parameter at P on $S(G_1)$. To find the rotation of A at P, we have to find that $B(\epsilon)$ for which there exists an element C in G_1 satisfying $CA = B(\epsilon)$. This determines a unique ϵ mod k, and hence the rotation of A at P is given by

$$\frac{1}{z - P} \rightarrow \frac{1}{z - P} + \epsilon^2 \mu^2 c.$$

Introducing this in (6) yields $t' = e(\epsilon^2/k)t$; i.e., A rotates at P by $e(\epsilon^2/k)$.

Now $m(0) = \hat{g}$, the genus of $S_0(4p)$, since this is the number of linearly independent differentials in D which are invariant under $\Gamma_0(4p)/\Gamma_0(16p)$. We obtain a formula for $m(l)$ $(l = 1, 2, 3)$ by either an application of the Riemann-Roch Theorem, or the use of a formula by Chevalley and Weil [**3**]. We use the latter and obtain

$$m(l) = \hat{g} - 1 + \sum_{i=1}^{4} (1 - l/4), \quad l = 1, 2, 3. \tag{7}$$

In particular, we have: $m(0) = \hat{g}$, $m(1) = \hat{g} + 2$, $m(2) = \hat{g} + 1$, and $m(3) = \hat{g}$.

If g is the genus of $S_0(16p)$ and if $\gamma_1 < \gamma_2 < \ldots < \gamma_g$ are the gaps at a point P on S_0 which is not a Weierstrass point, then $\gamma_i = i$ for $i = 1, 2, \ldots, g$. This implies that if P is not a Weierstrass point, then for any two non negative integers l_1 and l_2 less than k, $|m(l_1) - m(l_2)| \leqq 1$. However, P is a Weierstrass point if for two integers l_1 and l_2, $|m(l_1) - m(l_2)| \geqq 2$. In our case we have $m(1) - m(3) = 2$, and hence the cusp 0 is a Weierstrass point of $S_0(16p)$. Evidently, the same holds for all the cusps which are fixed points of $\Gamma_0(4p)/\Gamma_0(16p)$.

Finally, it is easy to see that all the cusps of $S_0(16p)$ are Weierstrass points. Let A be an automorphism of the Riemann surface S and let $f(P)$ be a function on S. Then $f(A^{-1}P)$ is a function on S and has the same behaviour at AP as $f(P)$ has at P. In particular, P and AP are both Weierstrass points, or not. Now R: $z \rightarrow -1/16pz$ is an automorphism of $S_0(16p)$ and maps (i) 0 onto $i\infty$, which is one of the cusps of $\mathscr{C}_1$, and (ii) C_{16} onto one of the cusps of $\mathscr{C}_p$. Under $\Gamma_0(4p)/\Gamma_0(16p)$, the four cusps of $\mathscr{C}_1$ and $\mathscr{C}_p$ are mapped onto themselves. This completes the proof of Theorem 1.

We close this part by giving two examples for $\Gamma_0(n)$, where the only Weierstrass points are the cusps. For $\Gamma_0(48)$ and $\Gamma_0(64)$, the genus $g = 3$ and the gaps at the twelve respective cusps are 1, 2, 5. Since $(g - 1)g(g + 1) = 24$, there are no other Weierstrass points. For $\Gamma_0(48)$, it follows from our derivation by putting $p = 3$. In the case of $\Gamma_0(64)$, one has to carry out the parallel steps to the above derivation and one obtains the stated result.

Proof of Theorem 2. Henceforth, we call an automorphism of order two of a Riemann surface an involution. A hyperelliptic Riemann surface S of genus g has a unique involution J with $2g + 2$ fixed points which are precisely the Weierstrass points of S. The possible orders which groups of automorphisms of a hyperelliptic surface may have are rather few. Thus a look at them is often sufficient to conclude that a Riemann surface is not hyperelliptic. This will not work here, since in general we only know one involution of $S_0(n)$. In the proof of Theorem 2 we make use of the following

LEMMA. *An involution $H \neq J$ of a hyperelliptic surface S has either* 0, 2, *or* 4 *fixed points which are not Weierstrass points of S.*

Although it does not contain any new result we prove the lemma here. It may be considered trivially true if H has no fixed points. Let P be a Weierstrass point of S and let us assume that $H(P) = P$. Then there exists an H-invariant function f on S which has a pole of order two at P and is regular everywhere else on S. We can lower f to a function $\hat{f}$ on $\hat{S}$, the orbit space of S under H, and $\hat{f}$ is regular everywhere on $\hat{S}$ except for a simple pole at one point. But $H \neq J$ implies that the genus $\hat{g}$ of $\hat{S}$ is at least one, which is a contradiction. Next we note that the set of Weierstrass points is invariant under an automorphism. If $\Pi: S \rightarrow \hat{S}$ is the branched analytic covering defined by H and if P is a Weierstrass point of S, then $\hat{P} = \Pi(P)$ is a Weierstrass point $\hat{S}$, provided $\hat{g} \geqq 2$. In particular, S is again hyperelliptic. From the Riemann-Hurwitz relation we deduce

$$(8) \qquad 2\hat{g} + 2 = 3 + g - t/2 \geqq g + 1 = \tfrac{1}{2}(2g + 2),$$

where t is the number of fixed points of H and g is the genus of S. This implies that $t \leqq 4$ and that t is even for $\hat{g} \geqq 2$. (8) still holds for $\hat{g} = 1$, since $2(\hat{g} + 1) \geqq g + 1$ simply reflects the fact that a fixed point under H is not a Weierstrass point.

An immediate consequence of the Lemma is the

COROLLARY. *If an involution H of a hyperelliptic surface has more than four fixed points then $H = J$.*

The idea in the proof of Theorem 2 is as follows. The substitution $R: z \rightarrow -1/nz$ defines an involution on $S_0(n)$ with t fixed points all of which are elliptic for $n \geqq 5$. For those n for which we can establish the inequality $4 < t < 2g + 2$, Theorem 2 follows from the Corollary.

We divide the proof into several parts.

(i) n is not quadratfrei and, if p, q, and r denote distinct primes, is not of the form:

(9)
- (1) $n = 8p$.
- (2) $n = p^2q$ and not both p and q are congruent 1 mod 12.
- (3) $n = p^2qr$ and neither $x^2 + 1 \equiv 0$ nor $x^2 - x + 1 \equiv 0 \pmod{pqr}$ is soluble.
- (4) $n = 81$.

https://doi.org/10.4153/CJM-1971-103-6 Published online by Cambridge University Press

The exceptions (9) cover those n for which we do not know whether the cusp $i\infty$ is a Weierstrass point or not (see [**1**]).

We consider only those n for which $g \geqq 3$ and we assume $\Gamma_0(n)$ to be hyperelliptic. For all these n, the cusp $i\infty$ is a Weierstrass point of $\Gamma_0(n)$. The involution R has $t = \delta_n h(-4n)$ fixed points, where $h(d)$ is the class number of the quadratic number field of discriminant d and δ_n is 2, 4/3, or 1 according as $n \equiv 7 \pmod 8$, $n \equiv 3 \pmod 8$, or $n \not\equiv 3 \pmod 4$ (see [**4**]). For all n for which $t > 4$ we have by the corollary that $R = J$ and that $t = 2g + 2$, which are all the Weierstrass points of $\Gamma_0(n)$. But $i\infty$ is a Weierstrass point and not a fixed point of R, which is a contradiction. As for the existence of n's for which $t > 4$, we state the result: $\log h(-4n) \sim \log \sqrt{4n}$, which is due to Siegel [**9**].

(ii) n is quadratfrei. Let $n = \Pi_{i=1}^r p_i$, and let $\Gamma_0(n)$ be hyperelliptic. The genus of $\Gamma_0(n)$ is given by the formula

$$g = 1 + \frac{1}{12} \prod_{i=1}^{r} (p_i + 1) - \frac{a(n)}{4} - \frac{b(n)}{3} - 2^{r-1},$$

where $a(n)$ and $b(n)$ are the numbers of incongruent solutions of $x^2 + 1 \equiv 0$ and $x^2 - x + 1 \equiv 0 \pmod n$, respectively. If $\sigma(n)$ and $d(n)$ denote the sum and the number of divisors of n, then

$$g = [\sigma(n) - 3a(n) - 4b(n) - 6d(n) + 12]/12.$$

Observing that $d(n) = 2^r$ is an upper bound for $a(n)$ and $b(n)$, we obtain for all sufficiently large n

$$2g + 2 \geqq \tfrac{1}{6}[\sigma(n) - 13d(n) + 12] > \frac{4\sqrt{n}}{\pi} \log(4n) \geqq t > 4.$$

Here we make use of the result of Siegel and of the inequality:

$$h(-4d) \leqq [2\sqrt{d} \log(4d)]/\pi,$$

which holds for any positive integer d and is due to Bateman [**2**]. The inequality contradicts the hyperellipticity of $\Gamma_0(n)$.

(iii) There remain the first three cases listed in (9). Their proofs are analogous to case (ii) and are not repeated here. This completes the proof of Theorem 2.

We close with the remark (suggested by the referee) that Theorem 2 could be proved without Atkin's result, since the idea used in (ii) and (iii) would also work in part (i). However, the details in the proof of (i) would get more involved.

References

1. A. O. L. Atkin, *Weierstrass points at cusps of* $\Gamma_0(n)$, Ann. of Math. *85* (1967), 42–45.
2. P. Bateman, *On the representations of a number as the sum of three squares*, Trans. Amer. Math. Soc. *71* (1951), 70–101.

https://doi.org/10.4153/CJM-1971-103-6 Published online by Cambridge University Press

3. C. Chevalley and A. Weil, *Über das Verhalten der Integrale* 1. *Gattung bei Automorphismen des Funktionenkörpers*, Abh. Math. Sem. Univ. Hamburg *10* (1934), 358–361.
4. R. Fricke, *Lehrbuch der Algebra*, Band 3 (Braunschweig, 1928).
5. J. Lehner and M. Newman, *Weierstrass points of* $\Gamma_0(n)$, Ann. of Math. *79* (1964), 360–368.
6. J. Lewittes, *Automorphisms of compact Riemann surfaces*, Amer. J. Math. *85* (1963), 734–752.
7. ——— *Gaps at Weierstrass points for the modular group*, Bull. Amer. Math. Soc. *69* (1963), 578–582.
8. B. Schoenberg, *Uber die Weierstrass-Punkte in den Körpern der elliptischen Modulfunktionen*, Abh. Math. Sem. Univ. Hamburg *17* (1951), 104–111.
9. C. L. Siegel, *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arith. *1* (1936), 83–86.
10. J. R. Smart, *On Weierstrass points in the theory of elliptic modular forms*, Math. Z. *94* (1966), 207–218.

University of Maryland, Munich Campus,
Munich, Germany