

ON THE GENUS OF FIELDS OF ELLIPTIC MODULAR FUNCTIONS

BY
DONALD L. MCQUILLAN¹

1. Introduction

Let Γ be the 2×2 modular group, that is the group of transformations

$$\tau \rightarrow \frac{a\tau + b}{c\tau + d}$$

of the upper half plane to itself where a, b, c, d are integers and $ad - bc = 1$. The principal congruence subgroup $\Gamma(n)$ is defined by the conditions

$$a \equiv d \equiv 1 \pmod{n} \quad \text{and} \quad b \equiv c \equiv 0 \pmod{n}.$$

A subgroup G of Γ which contains $\Gamma(n)$ is called a congruence subgroup and is said to be of level n if n is the smallest such integer. Now G has a fundamental region in the upper half plane which can be compactified to a Riemann surface and the genus of this Riemann surface is referred to as the genus of G . It is the purpose of this paper to give a genus formula for congruence subgroups and to apply this formula to a conjecture of Rademacher (cf. [4]) which says that there is only a finite number of congruence subgroups which have genus zero. In [4] M. Knopp and M. Newman give a result in this direction; they prove that the genus of G is positive if G is free and the level of G is relatively prime to 2, 3, 5, 7, and 13. Our results improve somewhat on this (Theorem 3, Section 3). However the genus formula has intrinsic interest. If we combine it with the results of Gierster [1], [2] on the subgroup structure of $\Gamma/\Gamma(p^m)$ where p is an odd prime we can write down explicitly the genus of every congruence subgroup of prime-power level. The case of *prime* level is particularly simple and then the genera can be written down without any difficulty (cf. [3]).

The methods are algebraic and so will apply to Igusa's elliptic modular functions in the case that the characteristic is greater than 3. We shall denote by $K(n)$ the field of elliptic modular functions of level n , i.e., the field of meromorphic functions on the compact Riemann surface corresponding to $\Gamma(n)$. We recall that $K(n)$ is an algebraic function field of one variable and if j is the Weierstrass absolute invariant then $K(n)$ is a finite Galois extension of $C(j)$. The Galois group is $\Gamma/\Gamma(n)$ which is isomorphic to the linear fractional group $LF(2, n)$ consisting of the group of 2×2 matrices of determinant 1 over the ring of integers modulo n in which a matrix and its negative are identified. If $\Gamma \supset G \supset \Gamma(n)$ and H is the corresponding subgroup of $LF(2, n)$ then by Galois theory H corresponds to a subfield F of

Received April 30, 1965.

¹ Research supported by the National Science Foundation.

$K(n)$ and the genus of F is the genus of G . The elements

$$T = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad S = \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

of $LF(2, n)$ generate the group and we set

$$R = TS = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Now $K(n)$ is ramified over $C(j)$ at precisely $j = 0, 12^3$ and ∞ with ramification indices 3, 2 and n and inertia groups at these places are generated by R, T and S respectively.

2. Genus Formula

Let H be a subgroup of $LF(2, n)$ and let F be the corresponding field between $C(j)$ and $K(n)$. We shall use $g(H)$ for the genus of F . When H is the identity E , say, then of course $F = K(n)$ and it is well known that

$$g(E) = 1 + (1/24)(n - 6)\phi(n)\psi(n), \quad n > 2,$$

where $\phi(n)$ is the Euler function and

$$\begin{aligned} \psi(n) &= n \prod_{p|n} (1 + 1/p), \\ g(E) &= 0 \quad \text{when} \quad n = 1, 2. \end{aligned}$$

Indeed $g(E) = 0$ when $n \leq 5$ and so we shall assume in what follows that $n > 5$. We shall denote the order of H by h and define

$$\begin{aligned} \rho(n) &= n \prod_{p|n} \left(1 - \left(\frac{-3}{p} \right) / p \right) \\ \tau(n) &= n \prod_{p|n} \left(1 - \left(\frac{-4}{p} \right) / p \right). \end{aligned}$$

The following results follow at once from [5] when n is odd; the case of even n presents no new difficulty.

LEMMA 1. *The orders of the normalizers of T and R , in $LF(2, n)$ are $\tau(n)$ and $\delta\rho(n)$ respectively, where $\delta = 1$ if $n \equiv 0 \pmod{3}$ and $\delta = \frac{1}{2}$ otherwise.*

LEMMA 2. *R and R^{-1} are conjugate in $LF(2, n)$ if and only if*

$$n \not\equiv 0 \pmod{3}.$$

We can now state the

THEOREM. *Let r, t and $s(d)$ be the number of distinct cyclic subgroups of H generated by a conjugate in $LF(2, n)$ of R, T and S^d respectively where d is a divisor of n . Then*

$$\begin{aligned} g(H) &= 1 + n\phi(n)\psi(n)/24h - r\rho(n)/3h - t\tau(n)/4h \\ &\quad - \phi(n)\psi(n) \sum_{d|n} \frac{\phi(d)}{\psi(d)} s\left(\frac{n}{d}\right) / 4h. \end{aligned}$$

Proof. Let \mathfrak{D} be the different of $K(n)$ over F . Then, by the relative genus formula,

$$2g(E) - 2 = (2g(H) - 2)h + \text{deg } \mathfrak{D}.$$

Let $D(a)$ be the contribution to $\text{deg } \mathfrak{D}$ of those places of $K(n)$ which lie above $j = a$. Now if I is the inertia group of a place of $K(n)$ over $j = a$ then I operates on the homogeneous space $\sum_{\sigma \in LF(2,n)} H\sigma$ and by Hilbert's Galois theory there is a one-to-one correspondence between the orbits and the places of F lying over $j = a$. Furthermore if P is the place corresponding to the orbit $\langle H\sigma \rangle$ then $\sigma I\sigma^{-1} \cap H$ is the inertia group of a place of $K(n)$ above P , and the number of points in the orbit is just the ramification index of P over $j = a$. Let $j = 0$ and $I = (R)$. Then $|\sigma I\sigma^{-1} \cap H| = 1$ or 3 and this order is 3 if and only if $\sigma R\sigma^{-1} \in H$. It follows from the lemmas that the number of σ 's with this property is precisely $r\rho(n)$; hence the number of cosets $H\sigma$ is $r\rho(n)/h$ and the number of places of F which ramify in $K(n)$ with index 3 is $r\rho(n)/h$. It follows that $D(0) = \frac{2}{3}r\rho(n)$. In a similar manner one sees that $D(12^3) = \frac{1}{2}t\rho(n)$. Finally let $j = \infty$ and $I = (S)$. Let d be a divisor of n , $f(d)$ the number of places of F which ramify in $K(n)$ with index n/d , and $C(d)$ the number of elements σ in $LF(2, n)$ such that $\sigma S^d\sigma^{-1} \in H$. Then $\sum_{e|d} ef(e) = (1/h)C(d)$ and so, by the Möbius inversion formula

$$df(d) = (1/h) \sum_{e|d} \mu(e)C(d/e).$$

Now

$$\begin{aligned} D(\infty) &= (h/n) \sum_{d|n} df(d)(n/d - 1) \\ &= h \sum_{d|n} f(d) - (h/n) \sum_{d|n} df(d) \\ &= \sum_{d|n} 1/d \sum_{e|d} \mu(e)C(d/e) - (1/n)C(n). \end{aligned}$$

From this it follows easily that

$$D(\infty) = (1/n) \sum_{d|n, d < n} \phi(n/d) C(d).$$

The normalizer of S^d consists of all elements

$$\pm \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

such that $\gamma \equiv 0 \pmod{n/d}$ and $\alpha^2 \equiv 1 \pmod{n/d}$. By considering the natural homomorphism from $LF(2, n)$ onto $LF(2, n/d)$ defined by reduction modulo n/d it can be seen that the order of this normalizer is

$$\frac{1}{2}n\phi(n)\psi(n)/\psi(n/d)A(d)$$

where $A(d)$ is the number of quadratic residues modulo n/d . Now S^{md} is conjugate in $LF(2, n)$ to S^d if and only if m is a quadratic residue modulo n/d and so

$$C(d) = \frac{1}{2}n\phi(n)\psi(n)s(d)/\psi(n/d).$$

It follows that

$$D(\infty) = \frac{1}{2} \phi(n)\psi(n) \sum_{d|n, d < n} \frac{\phi\left(\frac{n}{d}\right)}{\psi\left(\frac{n}{d}\right)} s(d)$$

and the proof of the theorem is complete.

Suppose that n is a prime power, say $n = p^m$. When $p > 2$ an element of $LF(2, p^m)$ has order 2 if and only if its trace is zero, and consequently every element of order 2 is conjugate to T [2]. When $p > 3$ an element has order 3 if and only if its trace is ± 1 and therefore every element of order 3 is conjugate to R [2]. If we also remark that in this case

$$\phi(d)/\psi(d) = (p - 1)/(p + 1)$$

when $d > 1$ we can state the

COROLLARY. *Let H be a subgroup of $LF(2, p^m)$ where p is prime and greater than 3. Let r and t be the number of elements of order 3 and 2 respectively in H . Then*

$$g(H) = 1 + \frac{p^m - 6}{24h} p^{2m-2}(p^2 - 1) - \frac{r}{3h} p^{m-1} \left(p - \left(\frac{-3}{p} \right) \right) - \frac{t}{4h} p^{m-1} \left(p - \left(\frac{-1}{p} \right) \right) - \frac{1}{4h} p^{2m-2}(p - 1)^2 W$$

where

$$W = \sum_{r=0}^{m-1} s(p^r).$$

Now all subgroups of $LF(2, p)$ are known [1] (we may assume $p > 5$). A subgroup of $LF(2, p)$ is

- (i) a cyclic group C_m of order m where $m = p$, $m |(p - 1)/2$ or $m |(p + 1)/2$,
- (ii) a dihedral group D_{2n} of order $2n$ where $n | p - 1$ or $n | p + 1$,
- (iii) a metacyclic group M_{pu} of order pu where $u |(p - 1)/2$,
- (iv) a tetrahedral group \mathfrak{S} , octahedral group \mathfrak{O} , or icosahedral group \mathfrak{I} .

If u is an integer we set $u_2 = 1$ or 0 according as $u \equiv 0 \pmod{2}$ or $u \not\equiv 0 \pmod{2}$, and we set $u_3 = 1$ or 0 according as $u \equiv 0 \pmod{3}$ or $u \not\equiv 0 \pmod{3}$.

When $H = C_p$ then $r = t = 0$ and $W = 1$ so that

$$g(C_p) = (p - 5)(p - 7)/24.$$

When $H = C_m$ where $m |(p + \varepsilon)/2$ and $\varepsilon = \pm 1$, then $r = m_3$, $t = m_2$ and $W = 0$. Furthermore if $m_2 = 1$ then

$$\left(\frac{-1}{p} \right) = -\varepsilon,$$

and if $m_3 = 1$ then

$$\left(\frac{-3}{p}\right) = -\varepsilon.$$

We get

$$g(C_m) = 1 + \frac{(p-6)(p^2-1)}{24m} - \frac{p+\varepsilon}{2m} \left[\frac{1}{2} m_2 + \frac{2}{3} m_3\right].$$

When $H = D_{2n}$ where $n \mid p + \varepsilon$ then $r = n_3, t = n + n_2, W = 0$ and so

$$g(D_{2n}) = 1 + \frac{(p-6)(p^2-1)}{48n} - \frac{n_3}{6n}(p+\varepsilon) - \frac{(n+n_2)}{8n} \left(p - \left(\frac{-1}{p}\right)\right).$$

When $H = M_{pu}$ where $u \mid (p-1)/2$ then

$$t = \frac{1}{2} p \left(1 + \left(\frac{-1}{p}\right)\right) u_2, \quad r = p \left(1 + \left(\frac{-3}{p}\right)\right) u_3, \quad W = 1$$

and so

$$g(M_{pu}) = 1 + \frac{p-1}{2u} \left\{ \frac{p-11}{12} - \frac{u_2}{4} \left(1 + \left(\frac{-1}{p}\right)\right) - \frac{u_3}{3} \left(1 + \left(\frac{-3}{p}\right)\right) \right\}.$$

Finally, when

$$H = 5 \quad \text{then} \quad t = 3, \quad r = 4, \quad W = 0;$$

$$H = \emptyset \quad \text{then} \quad t = 9, \quad r = 4, \quad W = 0;$$

$$H = \mathcal{G} \quad \text{then} \quad t = 15, \quad r = 10, \quad W = 0;$$

we can therefore write

$$g(5) = 1 + \frac{(p-6)(p^2-1)}{288} - \left(p - \left(\frac{-3}{p}\right)\right) / 9 - \left(p - \left(\frac{-1}{p}\right)\right) / 16$$

$$g(\emptyset) = 1 + \frac{(p-6)(p^2-1)}{576} - \left(p - \left(\frac{-3}{p}\right)\right) / 18 - 3 \left(p - \left(\frac{-1}{p}\right)\right) / 32$$

$$g(\mathcal{G}) = 1 + \frac{(p-6)(p^2-1)}{1440} - \left(p - \left(\frac{-3}{p}\right)\right) / 18 - \left(p - \left(\frac{-1}{p}\right)\right) / 16.$$

3. Fields with genus zero

From the last results of the previous section we have, by an easy computation, the following

THEOREM 1. *Let H be a non-trivial subgroup of $LF(2, p)$, $p > 5$, and let $g(H)$ be the genus of the corresponding field of modular functions. Then $g(H)$ is positive except in the following cases*

$$H = C_p, \quad p = 7$$

$$H = M_{pu}, \quad p = 7 \text{ and } 13$$

$$H = 5, \emptyset, \quad p = 7$$

$$H = \mathcal{G}, \quad p = 11.$$

COROLLARY. *The number of prime level modular function fields of genus zero is finite.*

DEFINITION. We shall denote by $p(n)$ the smallest prime which divides the natural number n .

THEOREM 2. *Let $C(j) \subset F \subset K(n)$ where $p(n) > 13$ and the genus of F is zero. Then $F = C(j)$.*

Proof. Suppose first that $n = p^m$ where p is prime; when $m = 1$ our result is true by Theorem 1, so we proceed by induction on m . Let H be the subgroup of $LF(2, p^m)$ corresponding to F and denote by $K_r^m, m \geq r$, the kernel of the homomorphism from $LF(2, p^m)$ to $LF(2, p^r)$ defined by reduction modulo p^r . Then

$$F \cap K(p^{m-1}) = C(j)$$

by the induction hypothesis so that $H \pmod{p^{m-1}} = LF(2, p^{m-1})$. From [2] it follows that $H \supset K_{m-1}^m$ so that $F \subset K(p^{m-1})$ and therefore $F = C(j)$ by the induction hypothesis. To prove the theorem for composite n we set $p =$ the largest prime divisor of n and write $n = p^m r$ where $r > 1$ and $(r, p) = 1$. We use induction on the number of distinct prime divisors of n . Let H be the subgroup of $LF(2, n)$ corresponding to F and suppose that $H \neq LF(2, n)$, i.e., $F \neq C(j)$. Let C be the subgroup of $LF(2, n)$ corresponding to $K(p^m) \cdot K(r)$; C has order 2 and belongs to the centre of $LF(2, n)$. Now the subgroup of $LF(2, n)$ corresponding to $F_1 = F \cap K(p^m) \cdot K(r)$ is $H \cdot C$. If $C \subset H$ then $F_1 = F \neq C(j)$; otherwise $C \cap H =$ identity and consequently if $F_1 = C(j)$ we have $LF(2, n) = C \cdot H$ so that H is a normal subgroup of $LF(2, n)$ of index 2. This is a contradiction [6]. Therefore F_1 is a non-trivial subfield of $K(p^m) \cdot K(r)$ of genus zero. We denote by G the Galois group of $K(p^m) \cdot K(r)/C(j)$ and by $G(r)$ and $G(p^m)$ the subgroups of G which correspond to $K(p^m)$ and $K(r)$ respectively. Let H_1 correspond to F_1 . We note that $G(r) = LF(2, r)$ and $G(p^m) = LF(2, p^m)$ and that $G = G(p^m) \times G(r)$. Now by the first part of the proof and by the induction hypothesis we have

$$F_1 \cap K(p^m) = F_1 \cap K(r) = C(j)$$

and therefore $H_1 \cdot G(r) = H_1 \cdot G(p^m) = G$. It follows that H_1 is a subgroup of $G(p^m) \times G(r)$ which projects onto the two factors and so there are normal subgroups L and M of $G(p^m)$ and $G(r)$ respectively such that

$$G(p^m)/L = G(r)/M.$$

By [6] this is impossible unless

$$L = G(p^m), \quad M = G(r) \quad \text{and} \quad H_1 = G(p^m) \times G(r).$$

Therefore $F_1 = C(j)$ which gives a contradiction.

A great deal of calculation is required to improve on this result and we shall

limit ourselves to the case $p(n) > 5$. The proof of the following lemma will be sketched at the end of the paper.

LEMMA. *If $C(j) \subset F \subset K(7^a \cdot 11^b \cdot 13^c)$ and the genus of F is zero then F is contained in $K(7)$, $K(11)$ or $K(13)$.*

With the aid of this lemma we can prove

THEOREM 3. *If $C(j) \subset F \subset K(n)$ where $p(n) > 5$ and if the genus of F is zero then F is contained in $K(7)$, $K(11)$, or $K(13)$.*

Proof. If $p(n) > 13$ then we are finished by Theorem 2. If not let $n = r \cdot m$ where $r = 7^a \cdot 11^b \cdot 13^c$ and $p(m) > 13$. We show first that F is contained in the compositum $K(r) \cdot K(m)$. Let C be the subgroup of $LF(2, n)$ which corresponds by Galois theory to this compositum and let H be the subgroup which corresponds to F . If $F \not\subset K(r) \cdot K(m)$ then $H \cap C = \text{identity}$, the subgroup HC corresponds to

$$F_0 = F \cap K(r) \cdot K(m) \quad \text{and} \quad K(n) = F \cdot K(r) \cdot K(m).$$

Now the number of places of F_0 which ramify in $K(n)$ with index 2 is $t \cdot \tau(n)/h$. On the other hand by considering the tower $F_1 \subset F \subset K(rm)$ it is clear that this number is also $2 + t\tau(n)/2h$. It follows that $4h = t\tau(n)$. The Galois group of $K(r) \cdot K(m)/C(j)$ is $LF(2, r) \times LF(2, m)$ and if H_0 is the subgroup of this corresponding to F_0 then $H \cong H_0$, in fact $H \pmod{C} = H_0$. Since $F_0 \cap K(m) = C(j)$ by Theorem 1, it follows that the projection of H_0 into $LF(2, m)$ is all of $LF(2, m)$ and so (cf. [6]) $H_0 = H_1 \times LF(2, m)$ where H_1 is the subgroup of $LF(2, r)$ which corresponds to $F_1 = F_0 \cap K(r)$. Since $\tau(n)$ is multiplicative we see that $4h_1 = t_1\tau(r)$. By the previous lemma F_1 is contained in $K(p)$ where $p = 7, 11$ or 13 , and if H_2 is the subgroup of $LF(2, p)$ which corresponds to F_1 then an easy computation shows that $4h_2 = t_2\tau(p)$. The possibilities for H_2 are listed in Theorem 1 and for these groups it is quickly seen that $4h_2 \neq t_2\tau(p)$. We have a contradiction and therefore

$$F \subset K(r) \cdot K(m).$$

The argument just used for F_0 shows that $F \subset K(r)$ and so, by the lemma, $F \subset K(p)$ where $p = 7, 11$ or 13 .

Proof of the lemma. Suppose first that $F \subset K(p^m)$, $m > 1$, where $p = 7, 11$, or 13 . If $F \cap K(p) = C(j)$ then an argument already used in Theorem 2 shows that $F = C(j)$. In any case the genus formula shows that p^{m-1} divides h and so $H \cap K_1^m$ is not trivial; it follows (cf. [2, pp. 353-360]) that if $F_1 = F \cap K(p)$ corresponds to a tetrahedral, octahedral, or icosahedral subgroup of $LF(2, p)$ then $H \supset K_1^m$ and $F = F_1 \subset K(p)$. Now if H_1 is the subgroup of $LF(2, p)$ which corresponds to F_1 then by Theorem 1 there remains only the possibilities $H_1 = M_{pu}$ ($p = 7$ or 13) and $H_1 = C_p$ ($p = 7$). In the first case H_1 is conjugate [1] in $LF(2, p)$ to a subgroup of the group of triangu-

lar elements

$$\pm \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod p,$$

and so we can assume that H is a subgroup of the group of elements

$$\pm \begin{pmatrix} a & b \\ cp & d \end{pmatrix} \pmod{p^m}.$$

We may also assume that H does not contain K_{m-1}^m since otherwise $F \subset K(p^{m-1})$ and we are finished by an easy induction. But then [2, pp. 353–360] H is a subgroup of the group of elements

$$\pm \begin{pmatrix} a & b \\ cp^2 & d \end{pmatrix} \pmod{p^m}$$

and so $F \cap K(p^2)$ corresponds to the group of elements

$$\pm \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod{p^2}$$

in $LF(2, p^2)$. This field has positive genus when $p = 7$ or 13 and so we have a contradiction. Suppose finally that $H_1 = C_p$ ($p = 7$); we show by induction on m that $F = F_1$. When $m \geq 2$ then, by the induction hypothesis $F_1 = F \cap K(p^{m-1})$ and so the subgroup of $LF(2, p^{m-1})$ corresponding to F_1 has order p^{3m-5} since $|K_1^m| = p^{3m-6}$. It follows that h , the order of H , is p^{3m-5+r} where $r = 1, 2$, or 3 . From the genus formula we get

$$2 \cdot 7^m + 7^{m-3+r} \equiv 3 \pmod 9$$

and therefore $a = 3$, $h = p^{3m-2}$ and $F = F_1$.

Suppose now that $F \subset K(7^a) \cdot K(13^c)$. If $F_1 = F \cap K(7^a) = C(j)$ then one argues as before to show $F \subset K(13^c)$ and so $F \subset K(13)$ by the first part of the proof. Similarly if $F_2 = F \cap K(13^c) = C(j)$ then $F \subset K(7)$. In any case $F_1 \subset K(7)$ and $F_2 \subset K(13)$, by the first part of the proof, and if H_1, H_2 are the corresponding subgroups of $LF(2, 7)$ and $LF(2, 13)$ respectively then $H_1 \times H_2$ is the subgroup of $LF(2, 7) \times LF(2, 13)$ corresponding to $F_1 F_2$ in $K(7) \cdot K(13)$. Now by Theorem 1 the only possibilities are $H_1 = \mathfrak{J}, \mathfrak{O}, C_p, M_{pu}$ where $p = 7$ and $H_2 = M_{pu}$ where $p = 13$. One checks easily that the genus of $F_1 F_2$ is positive and since $F \supset F_1 F_2$ this is a contradiction. Therefore $F \subset K(7)$ or $K(13)$. Suppose now that $F \subset K(7^a \cdot 13^c)$; then the argument already used in the proof of the theorem shows that $F \subset K(7^a) \cdot K(13^c)$ so that $F \subset K(7)$ or $K(13)$. In exactly the same way the case $F \subset K(7^a \cdot 11^b \cdot 13^c)$ can be treated.

BIBLIOGRAPHY

1. J. GIERSTER, *Die Untergruppen der Galois'schen Gruppe der Modular-Gleichungen für den Fall eines primzahlen Transformation-grades*, Math. Ann., vol. 18 (1881), pp. 319–365.

2. ———, *Über die Galois'sche Gruppe der Modulargleichungen wenn der Transformationsgrad die Potenz einer Primzahl > 2 ist*, Math. Ann., vol. 26(1886), pp. 309–368.
3. E. GROSSWALD, *On the genus of the fundamental region of some subgroups of the modular group*, Amer. J. Math., vol. 74(1952), pp. 86–88.
4. M. I. KNOPP AND M. NEWMAN, *Congruence subgroups of positive genus of the modular group*, Illinois J. Math., vol. 9(1965), pp. 577–583.
5. D. L. MCQUILLAN, *Some results on the linear fractional group*, Illinois J. Math., vol. 10(1966), pp. 24–38.
6. ———, *Classification of normal congruence subgroups of the modular groups*, Amer. J. Math., vol. 87 (1965), pp. 285–296.

UNIVERSITY OF WISCONSIN
MADISON, WISCONSIN