THE GENUS OF SUBFIELDS OF $K(n)$

JOSEPH B. DENNIN, JR.

ABSTRACT. In this paper we fix a genus $g$ and show that the number of fields of elliptic modular functions $F$ of genus $g$ is finite.

1. Introduction. Let $\Gamma$ be the group of linear fractional transformations $w \mapsto (aw + b)/(cw + d)$ of the upper half plane into itself with integer coefficients and determinant 1. $\Gamma$ is isomorphic to the group of $2 \times 2$ matrices with integer entries and determinant 1 in which a matrix is identified with its negative. $\Gamma(n)$, the principal congruence subgroup of level $n$, is the subgroup of $\Gamma$ consisting of those elements for which $a \equiv d \equiv 1 \pmod{n}$ and $b \equiv c \equiv 0 \pmod{n}$. $G$ is called a congruence subgroup of level $n$ if $G$ contains $\Gamma(n)$ and $n$ is the smallest such integer. $G$ has a fundamental domain in the upper half plane which can be compactified to a Riemann surface and then the genus of $G$ is defined to be the genus of the Riemann surface. We denote by $K(n)$ the field of elliptic modular functions of level $n$, i.e., the field of meromorphic functions on the Riemann surface corresponding to $\Gamma(n)$.

If $j$ is the absolute Weierstrass invariant, $K(n)$ is a finite Galois extension of $C(j)$ with $\Gamma/\Gamma(n)$ for Galois group. $SL(2, n)$ is the special linear group of degree two with coefficients in $\mathbb{Z}/n\mathbb{Z}$ and $LF(2, n) = SL(2, n)/\pm I$ where $I$ is the identity matrix. Then $\Gamma/\Gamma(n) \cong LF(2, n)$. If $\Gamma(n) \subseteq G \subseteq \Gamma$ and $H$ is the corresponding subgroup of $LF(2, n)$, then by Galois theory $H$ corresponds to a subfield $F$ of $K(n)$ and the genus of $F$, denoted by $g(F)$, equals the genus of $G$.

In this paper we fix a genus $g$ and show that the number of $F$ such that $C(j) \subseteq F \subseteq K(n)$ for some $n$ and such that $g(F) = g$ is finite. More precisely we prove that, for the fixed $g$, there are constants $r, t_1, \ldots, t_r$ such that any field of genus $g$ is a subfield of $K(p_1^{t_1} \cdots p_r^{t_r})$ where $p_1, \ldots, p_r$ are the first $r$ primes arranged in their natural order. A corollary to this result is a proof of a conjecture of H. Rademacher that the number of congruence subgroups of $\Gamma$ of genus 0 is finite. Some previous results on the Rademacher
conjecture have been obtained by Knopp and Newman [5], McQuillan [8] and the present author [1], [2]. The case of arbitrary genus \( g \) and \( n = p^m \), a prime power, has been considered in [3]. The proof of the theorem is in two steps. First we show that there is an \( r \) such that any field of genus \( g \) is a subfield of \( K(p_1^{x_1} \cdots p_r^{x_r}) \) for some \( x_i, 1 \leq i \leq r \). Then we find constants \( t_1, \ldots, t_r \) such that any field of genus \( g \) is a subfield of \( K(p_1^{t_1} \cdots p_r^{t_r}) \).

2. Preliminaries. The following notation will be standard. \( G(L/K) \) is the Galois group of \( L \) over \( K \). \( g(K) \) is the genus of \( K \). \( K \cdot K' \) is the composite of \( K \) and \( K' \) considered in some larger field containing both \( K \) and \( K' \). \( |A| \) denotes the order of the group \( A \). \( \langle c \rangle \) is the group generated by \( c \). With the primes considered in their natural order, \( p_i \) is the \( i \)th prime. \( p_r \) is the largest prime \( p \) such that, for some \( x \), \( K(p^x) \) contains a field of genus \( \leq g \) other than \( C(x) \). \( p_r \) exists by [3, Proposition 2.6] and is larger than 3.

Suppose \( G \) is a subgroup of \( G_1 \times G_2 \). Let \( N_i = \) the projection of \( G \) onto \( G_i \), \( ft_1 = \{g_1|g_1 \in G_1, (g_1, 1) \in G\} \), \( ft_2 = \{g_2|g_2 \in G_2, (1, g_2) \in G\} \). \( ft_i \) is called the \( i \)th foot of \( G \). We will use extensively the following proposition on subgroups of the direct product of two finite groups which can be found in [7].

Proposition 1. Suppose \( G \subseteq G_1 \times G_2 \) with \( G_1, G_2 \) finite. Then \( ft_i \) is a normal subgroup of \( N_i, i = 1, 2 \), and \( N_1/ft_1 \cong N_2/ft_2 \).

We now collect some basic facts about the groups \( LF(2, m) \) which we will need. \( |LF(2, m)| = \frac{m}{\phi(m)} \phi(m) \) where \( \phi(m) \) is the Euler \( \phi \) function and \( \phi(m) = m \Pi_p\phi(m)|1 + 1/p \). Suppose \( p \) is a prime and consider the natural homomorphism \( f^n: LF(2, p^n) \rightarrow LF(2, p) \) defined by reduction modulo \( p \), \( 1 \leq r < n \). The kernel of \( f^n = K' \) and \( |K'| = p^3(n-r) \) if \( p \neq 2, r \neq 1; |K'| = 2^{3n-4} \) for \( p = 2 \). For \( p > 3 \), the only nontrivial normal subgroups of \( LF(2, p^n) \) are \( K^n, 1 \leq r < n \) [7]. The following lemma is proven in [4] for \( p > 2 \) and in [2] for \( p = 2 \).

Lemma 1. If \( |H \cap K^n_{n-1}| \leq p^2 \), then \( |H \cap K^n_t| \leq p^{2n-2t}, 1 \leq t \leq n-1 \).

As an easy corollary to this we have

Corollary 1. If \( H \) is a subgroup of \( K^n_t \) and \( |H| \geq 2n - 2t + r \) for some \( r, 1 \leq r \leq n-t \), then \( K^n_{n-r} \subseteq H \).

The following is a collection of facts about fields and Galois groups which we will use. The proofs are straightforward and most can be found in a standard text such as Lang [6]. Suppose \( K \) and \( K' \) are subfields of \( L \) and \( K \cap K' = k \).
(1) \( G(L/K \cdot K') = G(L/K) \cap G(L/K') \).
(2) \( G(L/k) = G(L/K) \cdot G(L/K') \) if \( K \) or \( K' \) is normal over \( k \).
(3) \( G(K \cdot K'/k) \cong G(K/k) \times G(K'/k) \) with the isomorphism given by projecting \( \sigma \) in \( G(K \cdot K'/k) \) onto both factors.
(4) \( G(K \cdot K'/K) \cong G(K'/k) \) with the isomorphism given by restricting \( \sigma \) in \( G(K \cdot K'/k) \) to \( K' \).
(5) If \( k \subseteq M \subseteq L \) and \( k \subseteq F \subseteq K \) are fields with \( L \cap K = k \), then in \( K \cdot L, (F \cdot L) \cap (K \cdot M) = F \cdot M \).

3. Main results. Let \( n = mp^s \) with \( (p, m) = 1 \) and \( p \) the largest prime dividing \( n \). Consider the following diagram of fields and Galois groups.

\[ \begin{array}{c}
K(n) \\
| \quad | \\
G(m) \\
| \quad | \\
\langle c \rangle \\
| \quad | \\
G(p^s) \\
| \\
K(m) \\
| \\
K(p^s) \\
| \\
LF(2,m) \\
| \\
C(j) \\
\end{array} \]

\( G \cong LF(2, m) \times LF(2, p^s) \). \( G(m) \) is the kernel of the natural homomorphism from \( LF(2, n) \) to \( LF(2, m) \) and equals \( \{ \pm(a/b) | a \equiv d \equiv 1, b \equiv c \equiv 0 \pmod{m} \} \). \( \langle c \rangle \) has order 2 and is the kernel of the homomorphism from \( LF(2, n) \) to \( G \). By the Chinese remainder theorem, \( c = \pm(a/0, b) \) with \( a \equiv 1 \pmod{m} \) and \( a \equiv -1 \pmod{p^s} \). Hence \( \langle c \rangle \) is contained in the center of \( LF(2, n) \).

**Lemma 2.** \( G(m) \cong SL(2, p^s) \).

**Proof.** Consider \( \theta : SL(2, p^s) \times \{ \begin{pmatrix} 1 \\ 0 \\ \end{pmatrix} \} \to LF(2, m) \) given by:

\[
SL(2, p^s) \times \begin{pmatrix} 1 \\ 0 \\ \end{pmatrix} \xrightarrow{\ i \ } SL(2, p^s) \times SL(2, m) \\
\xrightarrow{\ f \ } SL(2, n) \xrightarrow{\ g \ } LF(2, n) \xrightarrow{\ h \ } LF(2, m)
\]

where \( i \) is the injection, \( f \) is the isomorphism given by the Chinese remainder theorem, \( g \) is reduction mod \( \pm I \) and \( h \) is the natural homomorphism.

Then \( G(m) \) equals the kernel of \( h \) and \( g \circ f \circ i \) is 1-1 into \( G(m) \) since the
THE GENUS OF SUBFIELDS OF $K(n)$

intersection of the kernel of $g$ and the image of $f \circ i = 1$. But $|G(m)| = p^s \phi(p^s) = |\text{SL}(2, p^s)|$ so that the map is onto. Hence $\text{SL}(2, p^s) \cong G(m)$.

**Proposition 2.** Suppose $F \subseteq K(m)K(p^s)$ with $(m, p) = 1$, $p$ the largest prime dividing $n$ and $p > p_r$. If $g(F) \leq g$, then $F \subseteq K(m)$.

**Proof.** Let $H = G(K(n)/F)$ so that $H \subseteq \text{LF}(2, m) \times \text{LF}(2, p^s)$.

$N_2$, the projection of $H$ onto $\text{LF}(2, p^s)$, is $G(K(p^s)/F \cap K(p^s))$. But $g(F \cap K(p^s)) \leq g(F)$ and so by the assumption on $p$, $F \cap K(p^s) = C(j)$. Therefore $N_2 = \text{LF}(2, p^s)$. $f_{t_2}$ is normal in $N_2$ and, since $p > 3$, $f_{t_2} = K_{t_2}$ for some $t$. Therefore $N_2/f_{t_2} \cong \text{LF}(2, p^4)$ and so $p$ divides $|N_2/f_{t_2}|$. But $N_2/f_{t_2} \cong N_1/f_{t_1}$ so that $p$ divides $|N_1|$. But $N_1 \subseteq \text{LF}(2, m)$ and $p \nmid |\text{LF}(2, m)|$. So $N_2 = f_{t_2}$ and $N_1 = f_{t_1}$. So $H = N_1 \times \text{LF}(2, p^s)$ and by Galois theory, $F \subseteq K(m)$.

**Proposition 3.** Suppose $F \subseteq K(mp^s)$ with $(m, p) = 1$, $p$ the largest prime dividing $n$ and $p > p_r$. If $g(F) = g$, then $F \subseteq K(m)K(p^s)$.

**Proof.** Let $H = G(K(n)/F)$. If $c \in H$, we are done. So suppose $H \cap (c) = 1$. $H \cdot (c) = G(K(n)/F \cap K(m)K(p^s))$. By Proposition 2, $F \cap K(m)K(p^s) \subseteq K(m)$ since $g(F \cap K(m)K(p^s)) \leq g(F)$. So $G(m) \subseteq H \cdot (c)$. So $G(m) = G(m) \cap (H \cup cH) = (G(m) \cap H) \cup c \cdot (G(m) \cap H)$ since $c \in G(m)$. Therefore $G(m) \cap H$ is a normal subgroup of index 2 in $G(m)$. But by Lemma 2, $G(m) \cong \text{SL}(2, p^s)$ which has no subgroups of index 2 for $p > 3$ [7]. So $H \cap (c) \neq 1$.

**Theorem 1.** If $F$ has genus $g$, then $F \subseteq K(p_1^{x_1} \cdots p_r^{x_r})$ for some $x_i, 1 \leq i \leq r$.

**Proof.** Suppose $F \subseteq K(n)$ and $p$ is the largest prime not in $\{p_1, \ldots, p_r\}$ which divides $n$. Write $n = mp^s$ with $(m, p) = 1$. Then by Proposition 3, $F \subseteq K(m)K(p^s)$ and then by Proposition 2, $F \subseteq K(m)$. Repeating the argument, one has, after a finite number of steps, $F \subseteq K(m)$ with $p_1, \ldots, p_r$ the only primes dividing $m$.

For $1 \leq i \leq r$, let $e_i$ be the smallest power of $p_i$ such that any field $\nsubseteq C(j)$ of genus $\leq g$ which is contained in $K(p_i^{x_i})$ for some $x_i$ is actually contained in $K(p_i^{x_i})$ [3]. Suppose $p_i^{d_i} | \Pi_{j=i+1}^r (p_j^2 - 1)$. Since $K(p_i^{x_i}) \subseteq K(p_i^{x_i+1})$, we may assume in the following that, for all $i, x_i > e_i + d_i$.

**Proposition 4.** Suppose $F \subseteq \Pi_{i=1}^r K(p_i^{x_i})$ with $x_i > e_i + d_i$ and $g(F) \leq g$. Then

$$F \subseteq K(p_1^{e_1+d_1}) \cdot K(p_2^{e_2+d_2+1}) \cdot \cdots \cdot K(p_r^{e_r+d_r})$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Proof. The proof is by induction on the number of primes. Suppose

\[ F \subseteq K(p_r^{x_r-1}) \cdot K(p_r^{x_r}) \quad \text{and} \quad H = G(K(p_r^{x_r-1}) \cdot K(p_r^{x_r})/F) \]

so that \( H \subseteq LF(2, p_r^{x_r-1}) \times LF(2, p_r^{x_r}) \). Then, since

\[ N_2 = G(K(p_r^{x_r})/F \cap K(p_r^{x_r})) \quad \text{and} \quad (F \cap K(p_r^{x_r})) \subseteq K(p_r^{x_r}) \]

\( N_2 \supseteq K^{x_r} \). There is an \( H' \subseteq H \) such that \( N_2 = K^{x_r} \). Then \( |N_2'/t_2'| \) divides \( p_r^{y} \) but \( p_r \nmid |N_2'| \) since \( N_1' \subseteq LF(2, p_r^{x-r-1}) \). So \( N_2' = f_{t_2}' = K^{x_r} \). But \( f_{t_2} \supseteq f_{t_2}' \) so that \( I \times K_r^{x_r} \subseteq H \) and \( F \subseteq K(p_r^{x_r-1}) \cdot K(p_r^{x_r}) = L_1 \). Similarly

\[ N_1 = G(K(p_r^{x_r-1})/F \cap K(p_r^{x_r-1})) \quad \text{and} \quad K^{x_r-1} \subseteq N_1. \]

There is an \( H' \subseteq H \) such that \( N_1 = K^{x_r-1} \). \( |N_1'/f_{t_1}'| = p_r^{y} \) and \( N_1'/f_{t_1}' \approx N_2'/f_{t_2}' \). So \( p_r^{y} \mid p_r^{2} - 1 \) and \( y \leq d_{r-1} \). Let \( f_{t_1}' = p_r^{y} \). Then \( (3x_{r-1} - 3e_{r-1}) - z = y < d_{r-1} \), i.e.

\[ z > (3x_{r-1} - 3e_{r-1}) - d_{r-1} = (2x_{r-1} - 2e_{r-1}) + ((x_{r-1} - e_{r-1}) - d_{r-1}) \]

and so, by the corollary to Lemma 1, \( f_{t_1}' \supseteq K^{x_r-1}+d_{r-1} \). So

\[ K^{x_r-1}+d_{r-1} \times I \subseteq H \quad \text{and} \quad F \subseteq K(p_r^{x_r-1}+d_{r-1}) \cdot K(p_r^{x_r}) = L_2. \]

Then \( F \subseteq L_1 \cap L_2 \) which by fact (5) equals \( K(p_r^{x_r-1}+d_{r-1}) \cdot K(p_r^{x_r}) \).

Now suppose

\[ F \subseteq K(p_t^{x_t}) \cdot \prod_{i=t+1}^{r} K(p_i^{x_i}) \quad \text{and} \quad F \cap \prod_{i=t+1}^{r} K(p_i^{x_i}) \subseteq \prod_{i=t+1}^{r} K(p_i^{x_i+d}) \]

and

\[ H = G\left( \prod_{i=t}^{r} K(p_i^{x_i})/F \right). \]

Then \( N_2 \supseteq \prod_{i=t+1}^{r} K^{x_i+d_i} \) and so there is an \( H' \subseteq H \) such that \( N_2' = \prod_{i=t+1}^{r} K^{x_i+d_i} \). Then \( N_2'/f_{t_2}' \approx N_1'/f_{t_1}' \), \( |N_2'/f_{t_2}'| \) divides \( \prod_{i=t+1}^{r} p_r^{y_i} \) and, if \( p_{t+1} \neq 3 \), no \( p_i \) divides \( |N_1'| \). So

\[ N_2' = f_{t_2}' \quad \text{and} \quad f_{t_2} \supseteq f_{t_2}' = \prod_{i=t+1}^{r} K^{x_i+d_i}. \]

So

\[ F \subseteq K(p_t^{x_t}) \cdot \left( \prod_{i=t+1}^{r} K(p_i^{x_i+d_i}) \right) = L_1. \]

If \( p_{t+1} = 3 \), then it is possible that \( p_{t+1} \parallel |N_1'| \) in which case, arguing as
in the 2nd part of the first step of the induction, one gets
\[ F \subseteq K(p^x_t)^t \cdot K(p^{x_t+1+d+x_t+1}) \cdot \prod_{i=t+2}^r K(p_i^{e_i+d_i}) = L_1. \]

Similarly \( K_{i=1}^t \subseteq N_1 \) and so there is an \( H' \subseteq H \) such that \( N_1' = K_{i=1}^t \). Let \( |N'_1|/|t_1'| = p^{y_1}_t \) and \( |t_1'| = p^{x_1}_t \). Then, as before, \( z > (2x_t - 2e_t) + (x_t - e_t) - d_t \) and so \( t_1' \geq K_{i=1}^t \). Therefore
\[ F \subseteq K(p^x_t)^t \cdot \left( \prod_{i=t+1}^r K(p_i^{x_i}) \right) = L_2. \]

Again \( F \subseteq L_1 \cap L_2 \) which equals \( \prod_{i=t+1}^r K(p_i^{e_i+d_i}) \) unless \( p_{t+1} = 3 \) in which case \( e_{t+1} + d_{t+1} \) has to be replaced by \( e_{t+1} + d_{t+1} + 1 \).

Let \( n = \prod_{i=1}^r p_i^{x_i}, L = \prod_{i=1}^r K(p_i^{x_i}) \) and \( A = G(K(\mathfrak{n})) / K(p_1^{x_1} p_2^{t_2} \cdots p_r^{t_r}) \)
where \( t_2 = e_2 + d_2 + 1 \) and \( t_i = e_i + d_i, i \neq 2 \).

**Proposition 5.** If \( F \subseteq K(n) \) and \( g(F) = g \), then \( F \subseteq K(p_1^{x_1} p_2^{t_2} \cdots p_r^{t_r}). \)

**Proof.** Let
\[ c_i = \pm \left( \begin{array}{cc} a_i & 0 \\ 0 & a_i \end{array} \right), \quad a_i \equiv 1 \pmod{\prod_{j=1; j \neq i}^r p_j^{x_j}}, \quad a_i \equiv -1 \pmod{p_i^{x_i}}, \]
be the nontrivial element in the kernel of the homomorphism from \( LF(2, n) \) to \( LF(2, p_i^{x_i}) \times LF(2, \prod_{j=1; j \neq i}^r p_j^{x_j}) \). Then \( C \), the group generated by the \( c_i \), \( 1 \leq i \leq r \), equals \( G(K(\mathfrak{n}))/L) \), is contained in the center of \( LF(2, n) \) and has order \( 2^{r-1} \). \( G(K(\mathfrak{n}))/F \cap L) = C \cdot H \) and \( [CH: H] = 2^s, 0 \leq s \leq r - 1 \). By Proposition 4, \( F \cap L \subseteq K(p_1^{x_1}) \cdot \prod_{i=2}^r K(p_i^{x_i}) \) and so
\[ F \cap L \subseteq F \cap K(p_1^{x_1} p_2^{t_2} \cdots p_r^{t_r}). \]

Therefore
\[ G(K(\mathfrak{n}))/K(p_1^{x_1} p_2^{t_2} \cdots p_r^{t_r}) \cap F) = A \cdot H \subseteq C \cdot H. \]

So we have \( H \subseteq A \cdot H \subseteq C \cdot H \) and \( H \) is normal in \( C \cdot H \) since \( C \) is in the center of \( LF(2, n) \). So \( H \) is normal in \( AH \) and \( AH/H \cong A/H \cap A \). So \( H \cap A \) is a normal subgroup of \( A \) of index \( 2^t, 0 \leq t \leq s \). But \( |A| = \prod_{i=1}^{r-2} p_i^{3(x_i-t_i)} \) which is odd. So \( A \cap H = A \) or \( A \subseteq H \). Therefore \( F \subseteq K(p_1^{x_1} p_2^{t_2} \cdots p_r^{t_r}). \)

**Proposition 6.** Suppose \( F \subseteq K(n) \) with \( n = 2^x m, (2, m) = 1 \) and \( g(F) = g \). Then \( F \subseteq K(2^{t+1} m) \) where \( t = e_1 + d_1 \).

**Proof.** As before.
C = G(K(n)/K(2^x) \cdot K(m)) \quad \text{and} \quad A = G(K(n)/K(2^t m)).

|C| = 2. F \cap K(2^x)K(m) \subseteq K(2^t K(m)) \text{ and so } F \cap K(2^x) \cdot K(m) \subseteq F \cap K(2^t m). \text{ Therefore } H \subseteq A H \subseteq C H. \text{ Since } [C H : H] \leq 2, \text{ there are 2 possibilities. If } H = C \cdot H, \text{ then } H = A \cdot H, A \subseteq H \text{ and so } F \subseteq K(2^t m). \text{ If } [C H : H] = 2 \text{ and } H = A H, \text{ again } A \subseteq H \text{ and we are done. So assume } [A H : H] = 2. \text{ Then since } A H / H \cong A / H \cap A, H \cap A \text{ is a normal subgroup of index 2 in } A. \text{ Let }

A' = G(K(2^x) \cdot K(m)/K(2^t K(m))

and let } \phi: A \to A' \text{ be the homomorphism obtained by restricting an automorphism } \sigma \text{ to } K(2^x) \cdot K(m). \phi \text{ is an isomorphism and so } \phi(H \cap A) \text{ has index 2 in } A'. \text{ But } A' = K^x \text{ and so }

\phi(H \cap A) \supseteq K^x_{t+1} = G(K(2^x) \cdot K(m)/K(2^t+1) \cdot K(m)).

Therefore

G(K(n)/K(2^{t+1} m)) \subseteq H \cap A \subseteq H \text{ and } F \subseteq K(2^{t+1} m).

Theorem 2. If } F \subseteq K(p_1^{x_1} \cdots p_r^{x_r}) \text{ has } g(F) = g, \text{ then
\begin{equation}
F \subseteq K(p_1^{e_1+d_1+1} \cdot p_2^{e_2+d_2+1} \cdot p_3^{e_3+d_3} \cdots p_r^{e_r+d_r}).
\end{equation}

Proof. Apply Propositions 5 and 6.

Combining Theorems 1 and 2, we obtain

Theorem 3. Suppose } F \subseteq K(n) \text{ for some } n \text{ and } g(F) = g. \text{ Then (\star) holds.

BIBLIOGRAPHY


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CONNECTICUT, STORRS, CONNECTICUT 06268