PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 64, Number 1, May 1977

CONGRUENCE FUNCTION FIELDS OF GENUS g AND CLASS NUMBER $g + 1$

JAMES R. C. LEITZEL

ABSTRACT. Congruence function fields of genus g and class number $g + 1$ are fully classified. As an application we determine explicitly the real quadratic function fields with this property and of odd characteristic for which the ring of integers is a unique factorization domain.

Introduction. In his dissertation Emil Artin [1] studied the arithmetic and analytic theory of quadratic extensions of $K(x)$ where K is a field of prime order. His approach to this subject was in complete analogy to the theory of algebraic number fields, and, for this reason, he separated these extensions into two classes, real and imaginary, depending upon the decomposition of the infinite prime of $K(x)$ in the extension. The field was called an *imaginary* extension if only one prime lies over the infinite prime of $K(x)$ and in the other case the field was called a *real* extension.

Since Artin's original work, the idea of a congruence function field has been broadened to include any finite field K as field of constants. Throughout this paper the term "function field" will mean a function field in one variable whose exact field of constants, K, is a finite field with q elements. For F/K, a function field, we denote by h_F the order of the finite group of divisor classes of degree zero. In the sense of Artin, the class number h_X of a quadratic function field is the class number of the Dedekind ring R which is the integral closure of $K[x]$ in F. In the context of real quadratic function fields, the connection between the two class numbers is given by $h_F = rh_X$ and is a consequence of F. K. Schmidt's relation [6, p. 32]. The number r is the "regulator" and can be computed as follows: Let p_1, p_2 denote the two primes of degree one lying above the infinite prime of $K[x]$. Then p_1/p_2 is a divisor of degree zero in F and $r = \operatorname{ord}(p_1/p_2)$ in $C_0(F)$, the group of divisor classes of degree zero for F. Alternatively $r = \pm v_{p_i}(\varepsilon_0)$ where ε_0 is a fundamental unit (in the sense of Artin) of the quadratic extension and v_{p_i} is the valuation associated with the corresponding extension of the infinite prime of $K[x]$.

In his recent doctoral thesis, D. J. Madden [5] has proved that if α is a primitive integral element in a geometric extension F of $K(x)$ of prime power degree l^n, where $l \neq \operatorname{char} K$, and containing $l^n - 1$ roots of unity there is a prime p_∞ lying over the infinite prime of $K(x)$ so that

Presented to the Society, January 27, 1977; received by the editors June 1, 1976.
AMS (MOS) subject classifications (1970). Primary 12A90; Secondary 14H05.
Key words and phrases. Class number, congruence function field, real quadratic function field.

$$v_{p_\infty}(\alpha) \leqslant \frac{e_\infty - 1}{l^n - 1} - \frac{2e_\infty}{l^n} - \frac{2g}{l^n(l^n - 1)} \tag{1}$$

where g is the genus of F and e_∞ is the ramification index of p_∞. Interpreting this result for real quadratic extensions of $K(x)$ we see that, in terms of the regulator,

$$r \geqslant g + 1. \tag{2}$$

Therefore if F/K is a real quadratic function field with $h_F = g + 1$, (2) and the relation between h_X and h_F noted earlier would imply $h_X = 1$. These fields then provide examples of function fields where the ring of integers is a unique factorization domain. The result of Madan [3] is also of interest for genus one fields.

In this paper we determine all congruence function fields F of genus g with class number $g + 1$ and, for those with char $F \neq 2$, we explicitly characterize the ones which are real quadratic fields. More specifically we prove the following theorems:

THEOREM 1. *Let F/K be a function field of genus g and with $|K| = q$. Then $h_F > g + 1$ for each of the following cases*: (a) $q > 5$; (b) $q = 5, g > 1$; (c) $q = 4, g > 2$; (d) $q = 3, g > 3$; (e) $q = 2, g > 8$.

THEOREM 2. *Let F/K be a real quadratic function field with $|K| = q$ and* char $K \neq 2$. *If g is the genus of F and $h_F = g + 1$, then either*

(a) $q = 5, g = 1$ *and* $N_1 = 2$, *or*

(b) $q = 3, g = 1$ *and* $N_1 = 2$, *or*

(c) $q = 3, g = 2$ *and* $N_1 = 2, N_2 = 3$.

(N_1, N_2 *denote, respectively, the number of primes of degree one and degree two in* F.)

1. **Proof of Theorem 1.** Let F/K be a function field of genus g and with $|K| = q$. Let $\bar{F}/\bar{K}$ denote the constant extension of degree $2g - 1$. If $\bar{N}_1$ denotes the number of primes of degree one in the extension $\bar{F}$, we have, by the Riemann hypothesis,

$$\bar{N}_1 \geqslant q^{2g-1} + 1 - 2g \cdot q^{(2g-1)/2}.$$

Because of the decomposition behavior of primes in constant extensions of function fields, these $\bar{N}_1$ primes come from primes of F of degree dividing $2g - 1$. Thus F must have, at least, $(q^{2g-1} + 1 - 2gq^{(2g-1)/2})(2g - 1)^{-1}$ integral divisors of degree $2g - 1$. However the total number of integral divisors in F of degree $2g - 1$ is $h_F(q^g - 1)(q - 1)^{-1}$. Therefore $h_F > g + 1$ if

$$(q - 1)(q^{2g-1} + 1 - 2gq^{(2g-1)/2}) > (g + 1)(2g - 1)(q^g - 1).$$

Set

$$S(q, g) = (q - 1)(q^{2g-1} + 1 - 2gq^{(2g-1)/2}) - (g + 1)(2g - 1)(q^g - 1).$$

The argument now proceeds parallel to that given in [4].

We consider $S(q, g)$ as a function of g and compute

$$\partial S/\partial g = (q-1)\left[2q^{2g-1}\ln q - 2q^{(2g-1)/2} - 2gq^{(2g-1)/2}\ln q\right] - (g+1)(2g-1)q^g \ln q - (q^g-1)(4g+1).$$

After simplification we can write

$$\partial S/\partial g = 4g + 1 + 2(q-1)q^{(2g-1)/2}T(q, g)$$

where

$$T(q, g) = (q^{(2g-1)/2}\ln q - 1 - g\ln q) - \tfrac{1}{2}q^{1/2}(q-1)^{-1}\left[4g + 1 + (2g^2+g-1)\ln q\right].$$

Likewise we find

$$\partial T/\partial g = (\ln q)^2 q^{(2g-1)/2} - \ln q - \tfrac{1}{2}q^{1/2}(q-1)^{-1}\left[4 + (4g+1)\ln q\right].$$

Therefore as a function of g, $S(q, g)$ will be an increasing function whenever $S(q, g) > 0$, $T(q, g) > 0$ and $(\partial T/\partial g)(q, g) > 0$. It can be readily checked that these conditions are satisfied precisely for the values stated in the theorem.

2. **Proof of Theorem 2.** Let F/K be a real quadratic function field of genus g with $|K| = q \neq 2^v$ and $h_F = g + 1$. In the case $g = 1$ we know that $h_F = N_1$, the number of primes of degree one. Since F is a real quadratic function field the infinite prime of $K[x]$ must split so that in any case $N_1 \geqslant 2$. From Theorem 1 and the above remarks we conclude (a) and (b) of Theorem 2.

The remaining possibilities are $q = 3$ and $g = 2$ or $g = 3$.

Using the functional equation for the zeta function it is possible to develop an explicit formula for the class number in terms of the number of primes of degree less than or equal to g. For the details of this procedure see, for example, [4, pp. 426–427]. In the case of interest here, $q = 3$ and we have

$$\text{for } g = 2, \quad 2h_F = N_1^2 + N_1 + 2N_2 - 6, \tag{3}$$

$$\text{for } g = 3, \quad 6h_F = N_1^3 + 3N_1^2 - 16N_1 + 6N_1N_2 + 6N_3. \tag{4}$$

Now for a real quadratic function field of genus 2 with $|K| = 3$ we get from (3), since $h_F = 3$,

$$N_1^2 + N_1 + 2N_2 = 12. \tag{5}$$

Furthermore $N_1 \geqslant 2$ so (5) gives two possibilities:

(i) $N_1 = 2$, $N_2 = 3$, or

(ii) $N_1 = 3$, $N_2 = 0$.

A field of genus 2 is necessarily hyperelliptic. For $q = 3$, $K[x]$ has four primes of degree one. If $N_1 = 3$ then at least two of these primes remain inert in F, i.e. $N_2 \geqslant 2$. So we are left with possibility (i), which is (c) of the theorem.

To complete the proof we must show that there is no such field of genus 3. If $g = 3$, then $h_F = 4$ and from (4) we get

$$N_1^3 + 3N_1^2 - 16N_1 + 6N_1N_2 + 6N_3 = 24. \tag{6}$$

As before $N_1 \geqslant 2$ in our situation and since N_1, N_2, N_3 are nonnegative, (6) clearly requires $N_1 < 4$. For $N_1 = 2, 3$, respectively, we find the conditions $2N_2 + N_3 = 6$ and $3N_2 + N_3 = 3$. Because F is a quadratic extension of $K(x)$ we further have that if $N_1 = 2$ then $N_2 \geqslant 3$ and if $N_1 = 3$ then $N_2 \geqslant 2$. These requirements rule out all possibilities except

$$N_1 = 2, \quad N_2 = 3, \quad N_3 = 0. \tag{7}$$

Corresponding to this possibility we compute the polynomial numerator of the zeta function to be

$$L(u) = 1 - 2u + u^2 - 8u^3 + 3u^4 - 18u^5 + 27u^6. \tag{8}$$

As in Eichler [2], we compute the logarithmic derivative of the zeta function expressed as a power series in u. In this series expansion the coefficient of $u^j, j = 0, 1, 2, \ldots$, gives the number of primes of degree one in the constant extension of degree $j + 1$. Carrying out this computation we get the series

$$2 + 8u + 2u^2 + 28u^3 + 62u^4 + 344u^5 + \ldots. \tag{9}$$

Of particular interest is the coefficient of u^5, giving the number of primes of degree one in a constant extension of degree six. On the other hand for a constant extension of degree six, the Riemann hypothesis gives the following lower bound on the number $\overline{N}_{1,6}$ of primes of degree one,

$$\overline{N}_{1,6} \geqslant q^6 + 1 - 2g\sqrt{q^6}\,.$$

In our case $q = 3$ and $g = 3$, so that

$$\overline{N}_{1,6} \geqslant 568. \tag{10}$$

This is a contradiction and so there is no function field which satisfies the conditions (7).

3 **Remarks and examples.** The possibilities listed in Theorem 2 are actually realized.

(a) For $|K| = 5$, $F = K(x, y)$ where $y^2 = x^4 + 2$ is an example where $g(F) = 1$ and $h_F = 2$.

(b) For $|K| = 3$, $F = K(x, y)$ where $y^2 = x^4 + 2x^2 + 2$ is an example where $g(F) = 1$ and $h_F = 2$.

(c) For $|K| = 3$, $F = K(x, y)$ where $y^2 = x^6 + x^4 + 2x^3 + x^2 + x + 2$ is an example where $g(F) = 2$ and $h_F = 3$.

As a further remark let me note that to achieve real quadratic fields F in which the ring of integers is a unique factorization domain one must have that the group $C_0(F)$ of divisor classes of degree zero, is a cyclic group. Madan [3] does this for genus one fields by requiring the order of $C_0(F)$ to be prime. The examples cited above also have prime class number. This need not

always occur. The field $F = K(x, y), y^2 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $|K| = 3$, provides an example of a field with genus 2 and composite class number, $h_F = 35$. Here the group $C_0(F)$ is cyclic and by computing the fundamental unit one can check that the regulator $r = 35$ so that $h_X = 1$.

BIBLIOGRAPHY

1. E. Artin, *Quadratische Körper in Gebiete der hoheren Kongruenzen*. I, II, Math. Z. **19** (1924), 153–246.

2. M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, New York, 1966. MR **35** #160.

3. M. L. Madan, *Note on a problem of S. Chowla*, J. Number Theory **2** (1970), 279–281. MR **42** #3056.

4. M. L. Madan and C. S. Queen, *Algebraic function fields of class number one*, Acta Arith. **20** (1972), 423–432. MR **46** #5287.

5. M. L. Madan and D. J. Madden, *The exponent of class group in congruence function fields*, Acta Arith. **32** (1976).

6. F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Characteristik p*, Math. Z. **33** (1931), 1–32.

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210