Canad. Math. Bull.Vol. **35** (3), 1992 pp. 361–370

CLASS NUMBER DIVISIBILITY IN REAL QUADRATIC FUNCTION FIELDS

CHRISTIAN FRIESEN

ABSTRACT. Let q be a positive power of an odd prime p, and let $\mathbb{F}_q(t)$ be the function field with coefficients in the finite field of q elements. Let $h(\mathbb{F}_q(t,\sqrt{M}))$ denote the ideal class number of the real quadratic function field obtained by adjoining the square root of an even-degree monic $M \in \mathbb{F}_q[t]$. The following theorem is proved: Let $n \geqq 1$ be an integer not divisible by p. Then there exist infinitely many monic, squarefree polynomials, $M \in \mathbb{F}_q[t]$ such that n divides the class number, $h(\mathbb{F}_q(t,\sqrt{M}))$. The proof constructs an element of order n in the ideal class group.

Introduction. Class numbers, especially those of quadratic number fields, have long been objects of interest but many easily-stated conjectures remain unproved. It is therefore pleasing whenever a simple result shows up. It is just such a result that Hong Wen Lu proved in 1985 [5] and which we reproduce below.

THEOREM. *Let $D = 4m^{2n} + 1$ be squarefree, where m and n are integers satisfying $n > 0$ and $m \geqq 2$. Then n divides $h(\mathbb{Q}(\sqrt{D}))$, the ideal class number of $\mathbb{Q}(\sqrt{D})$.*

The analog of this result in the function field case is the topic of this paper and it is surprising how little mathematical machinery is needed to provide a proof. Much of it, in fact, is quite elementary. We state here the two main results proved in this paper:

MAIN THEOREM. *Let q be a positive power of an odd prime p, $\mathbb{F}_q$ the field of q elements and let n be a positive integer. Let $X \in \mathbb{F}_q[t]\backslash\mathbb{F}_q$ and let $a \in \mathbb{F}_q^*$. We let $M = X^{2n} + a^2$. If M is monic and squarefree then n divides h_M, the ideal class number of $\mathbb{F}_q(t,\sqrt{M})$.*

COROLLARY. *Let q be a positive power of an odd prime p, $\mathbb{F}_q$ the field of q elements and let n be a positive integer not divisible by p. Then there exist infinitely many squarefree, even-degree monics, $M \in \mathbb{F}_q[t]$, such that $n|h_M$, the ideal class number of $\mathbb{F}_q(t,\sqrt{M})$.*

The proofs will be deferred to Sections 4 and 5.

The serious study of quadratic function fields can be said to have started with the doctoral thesis of E. Artin [1]. Several decades later L. Carlitz [2] continued the investigation into these fields which have now seen a resurgence of interest. One can, for example, point to recent work of D. R. Hayes [4].

The author would like to acknowledge the support of a Toronto University grant and an NSERC Canada research grant. This paper is a reworking of a chapter of the author's doctoral thesis.

Received by the editors July 17, 1991.

AMS subject classification: 11A55, 11R29.

Key words and phrases: Continued Fractions, Function Fields, Class Numbers

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press

We begin by defining $\mathbb{F}_q$ to be the finite field with q elements and characteristic $p \neq 2$. Let $K = \mathbb{F}_q(t)$ be the field obtained by adjoining a transcendental element, t. Denote by K_∞ the completion of K at ∞. We may write any element $\alpha \in K_\infty^*$ in the form

$$\alpha = \sum_{i=-\infty}^{d} a_i t^i \quad \text{with} \quad a_i \in \mathbb{F}_q \quad \text{and} \quad a_d \neq 0.$$

We define

$$\deg(\alpha) \stackrel{\text{def}}{=} d \quad \text{and} \quad \|\alpha\| \stackrel{\text{def}}{=} q^d \quad \text{and} \quad \operatorname{sgn}(\alpha) \stackrel{\text{def}}{=} a_d$$

It will be convenient to extend the definition of $\|\alpha\|$ to all of K_∞ by setting $\|0\| \stackrel{\text{def}}{=} 0$.

We say that α is *monic* if $\operatorname{sgn}(\alpha) = 1$. If α is a monic of even degree d then there exists a unique monic element $y \in K_\infty$, of degree $d/2$, such that $y^2 = \alpha$ (see Artin [1, Section 3]). We may write $y = \sqrt{\alpha}$.

The "polynomial part" function is defined as follows: if $\alpha = \sum_{i=-\infty}^{d} a_i t^i$ then

$$[\alpha] \stackrel{\text{def}}{=} \begin{cases} \sum_{i=0}^{d} a_i t^i & \text{if } d \geqq 0, \\ 0 & \text{if } d < 0. \end{cases}$$

We now define the continued fraction algorithm. Given an element $\alpha \in K_\infty^*$ we can define $F_0(\alpha) \stackrel{\text{def}}{=} \alpha$ and, if $F_i(\alpha) \neq [F_i(\alpha)]$,

$$F_{i+1}(\alpha) \stackrel{\text{def}}{=} (F_i(\alpha) - [F_i(\alpha)])^{-1}.$$

It is easy to see that this sequence of elements terminates if and only if α is a rational element. We shall call $F_n(\alpha)$ the n^{th} *iterate* of α.

For convenience we shall write $(a_0; a_1, a_2, \ldots, a_{n-1}, a_n)$ for the continued fraction expansion

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

where $a_i \in K_\infty^*$ and where $\deg(a_i) > 0$ for $1 \leqq i \leqq n$.

For an $\alpha \in K_\infty$ we define $a_n(\alpha) \stackrel{\text{def}}{=} [F_n(\alpha)]$ as the polynomial part of the n^{th} iterate of α. We call $a_n(\alpha)$ the n^{th} *partial quotient*. Two other sequences are very important in the study of continued fraction expansions. We define

$$Q_{-1}(\alpha) \stackrel{\text{def}}{=} 0, \; Q_0(\alpha) \stackrel{\text{def}}{=} 1,$$

$$Q_n(\alpha) \stackrel{\text{def}}{=} a_n(\alpha) Q_{n-1}(\alpha) + Q_{n-2}(\alpha) \quad \text{for} \quad 1 \leq n,$$

$$P_{-1}(\alpha) \stackrel{\text{def}}{=} 1, \; P_0(\alpha) \stackrel{\text{def}}{=} a_0(\alpha) \quad \text{and}$$

$$P_n(\alpha) \stackrel{\text{def}}{=} a_n(\alpha) P_{n-1}(\alpha) + P_{n-2}(\alpha) \quad \text{for} \quad 1 \leq n.$$

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press

In general we will drop the dependence on α in the above notation for ease of reading and will reinstate it only when it seems necessary.

1. **Continued fraction identities.**

LEMMA 1.0. *Assume $\alpha \in K_\infty^*$ is irrational and let a_n be the n^{th} partial quotient in the continued fraction expansion of α. Then we have the following results, for all $n \geqq 1$, where the P_i, Q_i and F_i are understood to be functions of α.*

$$\alpha = \frac{P_{n-1}F_n + P_{n-2}}{Q_{n-1}F_n + Q_{n-2}}, \tag{1.1}$$

$$\|Q_n\| = \|a_1 a_2 \ldots a_n\|, \tag{1.2}$$

$$(-1)^n = Q_n P_{n-1} - P_n Q_{n-1}, \tag{1.3}$$

$$\|\alpha - P_n / Q_n\| = \frac{1}{\|Q_n Q_{n+1}\|} \textit{ and} \tag{1.4}$$

$$\|P_{n+1} - Q_{n+1}\alpha\| < \|P_n - Q_n\alpha\|. \tag{1.5}$$

PROOF. All of these proofs will proceed by induction. From the definition we have $F_1 = 1 / (\alpha - a_0)$ and substituting this into equation (1.1) shows that the desired equality holds for $n = 1$. We then assume equation (1.1) holds for n and, using the definitions of F_{n+1} and a_n, substitute $(a_n F_{n+1} + 1) / F_{n+1}$ for F_n to arrive at

$$\begin{aligned}\alpha &= \frac{P_{n-1}F_n + P_{n-2}}{Q_{n-1}F_n + Q_{n-2}} \\ &= \frac{P_{n-1}\frac{a_n F_{n+1}+1}{F_{n+1}} + P_{n-2}}{Q_{n-1}\frac{a_n F_{n+1}+1}{F_{n+1}} + Q_{n-2}} \\ &= \frac{P_{n-1} + P_{n-1}a_n F_{n+1} + P_{n-2}F_{n+1}}{Q_{n-1} + Q_{n-1}a_n F_{n+1} + Q_{n-2}F_{n+1}} \\ &= \frac{P_{n-1} + P_n F_{n+1}}{Q_{n-1} + Q_n F_{n+1}}\end{aligned}$$

which completes the induction. It is easy to see that the second equation holds for $n = 1$ and the fact that the a_i have positive degree leads to the conclusion that $\|Q_n\| > \|Q_{n-1}\|$ and, therefore, that $\|Q_{n+1}\| = \|a_{n+1}Q_n + Q_{n-1}\| = \|a_{n+1}Q_n\|$ from where an induction argument finishes off the proof of this part. The third equation is true for $n = 0$ and we use the definitions of P_i and Q_i to see that

$$Q_{n+1}P_n - P_{n+1}Q_n = -(Q_n P_{n-1} - P_n Q_{n-1})$$

which gives us the required step to complete this induction. For the fourth formula we use identity (1.1) to see that

$$\alpha - \frac{P_n}{Q_n} = \frac{P_n F_{n+1} + P_{n-1}}{Q_n F_{n+1} + Q_{n-1}} - \frac{P_n}{Q_n} = \frac{Q_n P_{n-1} - P_n Q_{n-1}}{Q_n (Q_n F_{n+1} + Q_{n-1})}.$$

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press

Now the numerator on the right is just $(-1)^n$ by equation (1.3) and

$$||Q_nF_{n+1} + Q_{n-1}|| = ||Q_nF_{n+1}|| = ||Q_na_{n+1}|| = ||Q_{n+1}||$$

gives us (1.4). We arrive at the final result by using (1.4) to show that the left-hand-side of (1.5) equals $1/||Q_{n+2}||$ and that the right-hand-side equals $1/||Q_{n+1}||$ which is strictly larger. This completes the proof of the lemma. ■

LEMMA 1.6. *Let α be an monic irrational in K_∞ and let P_n, Q_n arise out of the continued fraction expansion for α. If $A, B \in \mathbb{F}_q[t]$ and if $n \geqq 0$ such that*

$$||\alpha B - A|| < ||\alpha Q_n - P_n||$$

then $||B|| \geqq ||Q_{n+1}||$.

PROOF. We see that equation (1.3), $Q_{n+1}P_n - P_{n+1}Q_n = (-1)^{n+1}$, implies that there exist $X, Y \in \mathbb{F}_q[t]$ such that

$$XQ_n + YQ_{n+1} = B \text{ and}$$
$$XP_n + YP_{n+1} = A.$$

If $||XQ_n|| \neq ||YQ_{n+1}||$ then $||B|| = \max\big(||XQ_n||, ||YQ_{n+1}||\big) \geqq ||Q_{n+1}||$ and we are done. Else we have $||XQ_n|| = ||YQ_{n+1}||$ implies $||X|| > ||Y||$. We now write

$$||\alpha B - A|| = ||X(\alpha Q_n - P_n) + Y(\alpha Q_{n+1} - P_{n+1})||.$$

Using equation (1.5) together with $||X|| > ||Y||$ we obtain the contradiction

$$||\alpha B - A|| = ||X(\alpha Q_n - P_n)|| \geqq ||\alpha Q_n - P_n||$$

which concludes the proof. ■

LEMMA 1.7. *Let α be an monic irrational in K_∞. If A, B are coprime elements of $\mathbb{F}_q[t]$ satisfying*

$$||\alpha - A/B|| < \frac{1}{||B^2||}$$

then $A = aP_n$ and $B = aQ_n$ for some $n \geqq 0$ and some $a \in \mathbb{F}_q^*$ and where P_n, Q_n arise out of the continued fraction expansion for α.

PROOF. Let A, B be coprime elements of $\mathbb{F}_q[t]$ satisfying the above inequality. Fix n so that $||Q_n|| \leqq ||B|| < ||Q_{n+1}||$. Then the contrapositive of Lemma 1.6 requires that

$$||\alpha B - A|| \geqq ||\alpha Q_n - P_n||.$$

From the original hypothesis we have

$$||\alpha B - A|| < \frac{1}{||B||}$$

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press

and combining the above two equations and dividing by Q_n results in the inequality:

$$||\alpha - P_n/Q_n|| < \frac{1}{||BQ_n||}.$$

At this stage we shall assume that the conclusion of the lemma does not hold. Then, since equation (1.3) forces P_n and Q_n to be relatively prime, it follows that $BP_n - AQ_n$ is nonzero and we have

$$\begin{aligned}\frac{1}{||BQ_n||} &\leqq \frac{||BP_n - AQ_n||}{||BQ_n||}\\ &= ||P_n/Q_n - A/B||\\ &\leqq \max\left(||\alpha - P_n/Q_n||, ||\alpha - A/B||\right)\\ &< \max\left(\frac{1}{||BQ_n||}, \frac{1}{||B^2||}\right)\\ &\Rightarrow ||B|| < ||Q_n||\end{aligned}$$

and this contradiction finishes the proof of the lemma. ■

2. **More continued fraction theory.**

LEMMA 2.0. *Let $M = X^2 + b$ with $X \in \mathbb{F}_q[t] \backslash \mathbb{F}_q$ and $b \in \mathbb{F}_q^*$. Then all values of the iterates, $F_n(\sqrt{M})$, for $n > 0$, are given by*

$$F_n = \begin{cases} \sqrt{M} + X & \text{if } n \text{ is even} \\ \frac{\sqrt{M}+X}{b} & \text{if } n \text{ is odd.} \end{cases}$$

PROOF. We begin by noting that $[\sqrt{M}]$ is X. It follows that $a_0 = X$ and that

$$F_1 = \frac{1}{\sqrt{M} - X} = \frac{\sqrt{M} + X}{b}.$$

Now a_1 is the polynomial part of $(\sqrt{M} + X)/b$ which is just $2X/b$ and from this we see that

$$F_2 = \frac{1}{\frac{\sqrt{M}+X}{b} - \frac{2X}{b}} = \frac{b}{\sqrt{M} - X} = \sqrt{M} + X.$$

We perform the iteration one more time to arrive at the conclusion that $F_3 = (\sqrt{M}+X)/b$ which is the same value that we obtained for F_1. The definition of the algorithm makes it clear that this continued fraction expansion will be periodic, with the iterates alternating between $(\sqrt{M} + X)/b$ and $\sqrt{M} + X$. This concludes the proof of this lemma. ■

LEMMA 2.1. *Let $M \in \mathbb{F}_q[t] \backslash \mathbb{F}_q$ be monic, squarefree and of even degree. Then the continued fraction expansion of $\sqrt{M}$ is periodic and, for all $n \geqq 0$, the iterates F_n have the form $F_n = (\sqrt{M} + p_n)/q_n$ for polynomials $p_n, q_n \in \mathbb{F}_q[t]$ that depend upon M.*

PROOF. Since the main theorem of this paper deals only with M of the form $X^2 + b$ and since we have seen, in the previous lemma, that this fact holds for polynomials of

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press

that form we will not need to prove this statement in general. It is not difficult to do so but it would take us out of our way and we include the lemma here only to allow for greater generality in some of the intermediate lemmas. Readers are referred to Artin [1, Section 13] or Friesen [3, Chapter 1] for details of the function field case or even to Niven and Zuckerman [6, Chapter 7] for the very similar number field analog. ■

We remark that the periodicity of the continued fraction of $\sqrt{M}$ shows that the set $\{q_i\}_{i\geqq 1}$ must be finite for any M of the above form.

LEMMA 2.2. *Let $M \in \mathbb{F}_q[t]\backslash\mathbb{F}_q$ be monic, squarefree and of even degree. Write the iterates $F_n(\sqrt{M}) = (\sqrt{M}+p_n)/q_n$ as in Lemma 2.1. Then the following identity holds for all $n \geqq 1$:*

$$P_{n-1}^2 - MQ_{n-1}^2 = (-1)^n q_n.$$

PROOF. We substitute $\alpha = \sqrt{M}$ and $F_n = (\sqrt{M}+p_n)/q_n$ into equation (1.1) to obtain

$$\sqrt{M} = \frac{P_{n-1}(\sqrt{M}+p_n)+P_{n-2}q_n}{Q_{n-1}(\sqrt{M}+p_n)+Q_{n-2}q_n}.$$

We cross-multiply to get

$$MQ_{n-1} + Q_{n-1}p_n\sqrt{M} + Q_{n-2}q_n\sqrt{M} = P_{n-1}(\sqrt{M}+p_n) + P_{n-2}q_n.$$

We separately equate the rational and the irrational parts to obtain the pair of equations:

$$MQ_{n-1} = P_{n-1}p_n + P_{n-2}q_n \text{ and} \tag{2.3}$$

$$P_{n-1} = Q_{n-1}p_n + Q_{n-2}q_n. \tag{2.4}$$

Now we multiply equation (2.3) by Q_{n-1} and equation (2.4) by P_{n-1} before subtracting the former from the latter to arrive at

$$P_{n-1}^2 - MQ_{n-1}^2 = q_n(P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}).$$

We finish the proof of the lemma by using equation (1.3) to see that the right-hand-side is equal to $q_n(-1)^n$. ■

LEMMA 2.5. *Let $M \in \mathbb{F}_q[t]\backslash\mathbb{F}_q$ be monic, squarefree and of even degree. Write the iterates $F_n(\sqrt{M}) = (\sqrt{M}+p_n)/q_n$ as in Lemma 2.1. Let $N \in \mathbb{F}_q[t]$ satisfy $\|N\| < \|\sqrt{M}\|$. If the equation*

$$A^2 - MB^2 = N$$

has a solution in coprime $A, B \in \mathbb{F}_q[t]$ then

$$N = a^2(-1)^n q_n$$

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press

for some $a \in \mathbb{F}_q^*$ and some $n \geqq 1$.

PROOF. Let $A, B \in \mathbb{F}_q[t]$ satisfy $A^2 - MB^2 = N$. Taking norms leads to the equality

$$\|\sqrt{M} - A/B\| \, \|\sqrt{M} + A/B\| = \frac{\|N\|}{\|B^2\|}.$$

At least one of the two norms on the left-hand-side of the equation must be $\geqq \|\sqrt{M}\|$ (since their sum has norm equal to $\|\sqrt{M}\|$) and by adjusting the sign of A we may assume without loss of generality that $\|\sqrt{M} + A/B\| \geqq \|\sqrt{M}\|$ and hence

$$\|\sqrt{M} - A/B\| \leqq \frac{\|N\|}{\|B^2\|} \frac{1}{\|\sqrt{M}\|} < \frac{1}{\|B^2\|}.$$

Now we apply Lemma 1.7, with $\alpha = \sqrt{M}$, to see that $A = \pm aP_{n-1}$ and $B = aQ_{n-1}$ for some choice of $n \geqq 1$ and $a \in \mathbb{F}_q^*$, where the ± arises out of the possible adjustment to the sign of A earlier on. We may apply Lemma 2.2 to see that $A^2 - MB^2 = a^2(-1)^n q_n$ as required. ∎

This completes the continued fraction part of the preparation. Before continuing we shall need to take a quick look at ideal theory.

3. **Some ideal theory.** Let $M \in \mathbb{F}_q[t]\backslash\mathbb{F}_q$ be a square-free monic of even degree and let E be the quadratic extension $\mathbb{F}_q(t, \sqrt{M})$. Let $O_E = \mathbb{F}_q[t] + \mathbb{F}_q[t]\sqrt{M}$ be the ring of integers of E. Then we speak of equivalence between two ideals $\mathcal{A}$ and $\mathcal{B}$ of O_E as follows:

$$\mathcal{A} \overset{\text{def}}{\sim} \mathcal{B} \text{ if there exists a } \rho \in E^* \text{ such that } \mathcal{A} = \rho\mathcal{B}.$$

These ideal classes form a finite group under multiplication and the number of these ideal classes will be denoted

$$h_M \overset{\text{def}}{=} \text{class number of } \mathbb{F}_q(t, \sqrt{M}).$$

Every ideal $\mathcal{A} \subset O_E$ can be written in the form $\mathcal{A} = \omega_1\mathbb{F}_q[t] + \omega_2\mathbb{F}_q[t]$ for some $\omega_1, \omega_2 \in O_E$ and we define the norm of the ideal $\mathcal{A}$ as:

$$\mathcal{N}(\mathcal{A}) \overset{\text{def}}{=} \frac{\omega_1\overline{\omega_2} - \omega_2\overline{\omega_1}}{b\sqrt{M}}$$

where $b \in \mathbb{F}_q^*$ is chosen equal to the sgn of the numerator, thus ensuring that the norm is monic. We refer the reader to Artin [1, Section 5] for the straightforward proofs that $\mathcal{N}(\mathcal{A})$ is well-defined and that $\mathcal{N}(\mathcal{A}\mathcal{B}) = \mathcal{N}(\mathcal{A})\mathcal{N}(\mathcal{B})$ for any ideals $\mathcal{A}, \mathcal{B} \subset O_E$.

Any ideal equivalent to O_E is called a principal ideal and it is not hard to see that any principal ideal may be written in the form $(P + Q\sqrt{M})O_E$ for some $P, Q \in \mathbb{F}_q[t]$. We may choose $\omega_1 = P + Q\sqrt{M}$ and $\omega_2 = P\sqrt{M} + QM$ as an $\mathbb{F}_q[t]$-base of the above ideal and from this we see that the norm of such an ideal is $(P^2 - MQ^2)/b$ for some constant $b \in \mathbb{F}_q^*$.

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press

LEMMA 3.0. *Let $M \in \mathbb{F}_q[t]\backslash\mathbb{F}_q$ be monic, squarefree and of even degree. Write the iterates $F_n(\sqrt{M}) = (\sqrt{M}+p_n)/q_n$ as in Lemma 2.1. Let $E = \mathbb{F}_q(t,\sqrt{M})$ and let O_E be the integers of E. Let $\mathcal{A}$ be an ideal of O_E, without factors in $\mathbb{F}_q[t]\backslash\mathbb{F}_q$, satisfying*

$$\|\mathcal{N}(\mathcal{A})\| < \|\sqrt{M}\|.$$

If $\mathcal{A}$ is a principal ideal then $\mathcal{N}(\mathcal{A}) = aq_i$ for some $a \in \mathbb{F}_q^*$ and for some $i \geqq 1$.

PROOF. $\mathcal{A}$ being principal means that $\mathcal{A} = (P+Q\sqrt{M})O_E$ for some $P, Q \in \mathbb{F}_q[t]$. Then $\mathcal{N}(\mathcal{A}) = (P^2 - MQ^2)/b$ for some $b \in \mathbb{F}_q^*$. From $\|\mathcal{N}(\mathcal{A})\| < \|\sqrt{M}\|$ we see that $\|P^2 - MQ^2\| < \|\sqrt{M}\|$ and all that remains in order to apply Lemma 2.5 (with $A = P$ and $B = Q$) is to verify that P and Q are coprime. Assume that $D \in \mathbb{F}_q[t]$ divides both P and Q. Then it would also divide $P + Q\sqrt{M}$. But $\mathcal{A}$ was without factors in $\mathbb{F}_q[t]\backslash\mathbb{F}_q$ so D cannot be anything but an element of $\mathbb{F}_q^*$. It follows that P and Q are coprime and Lemma 2.5 declares that

$$P^2 - MQ^2 = c^2(-1)^i q_i$$

for some $i \geqq 1$ and some $c \in \mathbb{F}_q^*$. This implies that $\mathcal{N}(\mathcal{A}) = aq_i$ for some $i \geqq 1$ and some constant $a = c^2(-1)^i/b \in \mathbb{F}_q^*$ as required. ■

This is a very basic application of continued fraction theory to ideal theory (a more general approach would take us out of our way) but already we see that a good understanding of the q_i in the continued fraction expansion of $\sqrt{M}$ provides us with much information.

4. **The main theorem.**

MAIN THEOREM. *Let q be a positive power of an odd prime p, $\mathbb{F}_q$ the field of q elements and let n be a positive integer. Let $X \in \mathbb{F}_q[t]\backslash\mathbb{F}_q$ and let $a \in \mathbb{F}_q^*$. We let $M = X^{2n} + a^2$. If M is monic and squarefree then n divides h_M, the ideal class number of $\mathbb{F}_q(t,\sqrt{M})$.*

PROOF.

STEP 1. There exists an ideal $\mathcal{A}$ such that $\mathcal{A}^{2n} = (\sqrt{M}-a)O_E$.

We shall use the notation $\mathcal{P}^k \| \mathcal{A}$ for prime ideal $\mathcal{P}$ and ideal $\mathcal{A}$ to mean that $\mathcal{P}^k$ divides $\mathcal{A}$ and that $\mathcal{P}^{k+1}$ does not divide $\mathcal{A}$. Let $X = c\prod_i P_i^{e_i}$ be the factorization of X into distinct monic irreducibles $P_i \in \mathbb{F}_q[t]\backslash\mathbb{F}_q$ with $c \in \mathbb{F}_q^*$. For each such P_i the ideal P_iO_E factors in O_E as the product of the two ideals $\mathcal{P}_i\overline{\mathcal{P}_i}$, where $\overline{\mathcal{P}_i}$ denotes the conjugate of $\mathcal{P}_i$ in E. Then $\mathcal{P}_i^{2ne_i}\|X^{2n}O_E$. Since P_i does not divide $(\sqrt{M}+a)$ it follows that not both $\mathcal{P}_i$ and its conjugate can divide $(\sqrt{M}+a)O_E$. Let us relabel $\mathcal{P}_i$ and its conjugate so that $\mathcal{P}_i$ is the one that does not divide $(\sqrt{M}+a)O_E$. But $X^{2n}O_E = (\sqrt{M}+a)(\sqrt{M}-a)O_E$ which means that $\mathcal{P}_i^{2ne_i}\|(\sqrt{M}-a)O_E$. Since all prime ideal factors of $(\sqrt{M}-a)O_E$ arise out of irreducible factors of X in the above fashion we conclude that

$$(\sqrt{M}-a)O_E = \prod_i \mathcal{P}_i^{2ne_i}.$$

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press

Let $\mathcal{A} = \prod_i \mathcal{P}_i^{e_i}$. This ideal satisfies $\mathcal{A}^{2n} = (\sqrt{M} - a)O_E$. It follows from

$$\big(\mathcal{N}(\mathcal{A})\big)^{2n} = \mathcal{N}(\mathcal{A}^{2n}) = \mathcal{N}((\sqrt{M} - a)O_E) = M - a^2 = X^{2n}$$

that $\mathcal{N}(\mathcal{A}) = dX$ for some $d \in \mathbb{F}_q^*$. Since $\mathcal{A}^{2n}$ is a principal ideal we see that the order of $\mathcal{A}$ in the ideal class group must divide $2n$.

STEP 2. The order of $\mathcal{A}$ is $\geqq n$.

We prove the above assertion by contradiction. Let δ be the order of $\mathcal{A}$. If $\delta < n$ then we would have a principal ideal $\mathcal{A}^\delta$ with

$$\|\mathcal{N}(\mathcal{A}^\delta)\| = \|\mathcal{N}(\mathcal{A})\|^\delta = \|dX\|^\delta = \|X\|^\delta < \|X^n\| = \|\sqrt{M}\|$$

and from Lemma 3.0 it would follow that

$$\mathcal{N}(\mathcal{A}^\delta) = bq_i$$

for some $b \in \mathbb{F}_q^*$ and some $i \geqq 1$. We recall that q_i equals 1 or a^2 in this case and therefore it follows that $\mathcal{N}(\mathcal{A}) \in \mathbb{F}_q$ which contradicts $\mathcal{N}(\mathcal{A}) = dX$. We conclude that $\delta \geqq n$.

It only remains to remark that, since δ must divide $2n$ and is no smaller than n it must be equal to n or $2n$. So we have exhibited an ideal, $\mathcal{A}$, in the ideal class group, with order, δ, divisible by n. It follows that h_M, the order of the group, is divisible by n and the proof is complete. ■

5. **An application.** For the above theorem it is of relevance to determine families of X such that $M = X^{2n} + a^2$ is monic and squarefree. We may satisfy the monic condition by requiring that $(\mathrm{sgn}(X))^{2n} = 1$ and could, for example, just let X itself be monic. The squarefree condition is the more troublesome one to deal with. We display two families of X, such that $X^{2n} + a^2$ is monic and squarefree, in the following lemma.

LEMMA 5.0. *Let q be a positive power of an odd prime p. Fix a positive integer n, not divisible by p, and an element $a \in \mathbb{F}_q^*$. Let $X \in \mathbb{F}_q[t] \backslash \mathbb{F}_q$ be such that* $(\mathrm{sgn}(X))^{2n} = 1$. *Then $X^{2n} + a^2$ is monic and squarefree whenever X has one of the two forms:*

$$(5.1) \qquad X(t) = G(t^p) + bt^m \qquad p \not| m, \quad G(t) \in \mathbb{F}_q[t]$$
$$b \in \mathbb{F}_q^*, \quad G(0)^{2n} \neq -a^2$$

or

$$(5.2) \qquad X(t) = G(t^p) + bt \qquad G(t) \in \mathbb{F}_q[t], \quad b \in \mathbb{F}_q^*.$$

PROOF. It is clear that $X^{2n} + a^2$ is monic. We need only show that it is squarefree. $X^{2n} + a^2$ is squarefree if and only if it shares no factors with its derivative $2nX^{2n-1}X'$. Since $a \neq 0$ and $p \not| 2n$ we have $X^{2n} + a^2$ is squarefree if and only if $X^{2n} + a^2$ and X' are coprime. For the first form we note that $X'(t) = bmt^{m-1}$ can have zeros only at $t = 0$. But

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press

the condition $G(0)^{2n} \neq -a^2$ prevents $t = 0$ from being a root of $X^{2n} + a^2$ and so $X^{2n} + a^2$ must be squarefree. The second example is even simpler. We just note that $X' = b \neq 0$ has no roots. This finishes off the proof of the lemma. ■

COROLLARY. *Let q be a positive power of an odd prime p, $\mathbb{F}_q$ the field of q elements and let n be a positive integer not divisible by p. Then there exist infinitely many squarefree, even-degree monics, $M \in \mathbb{F}_q[t]$, such that $n | h_M$, the ideal class number of $\mathbb{F}_q(t, \sqrt{M})$.*

PROOF. We use Lemma 5.0 to demonstrate the existence of infinitely many monics, M, that are squarefree and of the form required for the main theorem to hold. It follows that there are infinitely many monics such that n divides the class number in question. ■

REFERENCES

1. E. Artin, *Quadratische Körper im Gebiet der höheren Kongruenzen I, II,* Math. Zeitschrift **19**(1924) 153–246.

2. L. Carlitz, *A class of polynomials,* Trans. Amer. Math. Soc. **43**(1938) 168–182.

3. C. Friesen, Continueu Fractions and Real Quadratic Function Fields Doctoral Thesis, Brown University 1989.

4. D. R. Hayes, *Real Quadratic Function Fields,* Canadian Mathematical Society Conference Proceedings **7**(1985) 203–236.

5. Hong Wen Lu, *Divisibility of the Class Number of some real quadratic fields,* Acta Math. Sinica **28**(1985) 756–762.

6. I. Niven and H. S. Zuckerman, An introduction to the Theory of Numbers, edition 4 John Wiley & Sons New York 1980.

7. O. Perron , Die Lehre von den Kettenbrüchen Chelsea Publishing New York 1950.

Mathematics Department
University of Toronto
Toronto, Ontario
Canada

https://doi.org/10.4153/CMB-1992-048-5 Published online by Cambridge University Press