involve
a journal of mathematics

Divisibility of class numbers of imaginary quadratic function fields

Adam Merberg

mathematical sciences publishers

2008 Vol. 1, No. 1

Divisibility of class numbers of imaginary quadratic function fields

Adam Merberg

(Communicated by Ken Ono)

We consider applications to function fields of methods previously used to study divisibility of class numbers of quadratic number fields. Let K be a quadratic extension of $\mathbb{F}_q(x)$, where q is an odd prime power. We first present a function field analog to a Diophantine method of Soundararajan for finding quadratic imaginary function fields whose class groups have elements of a given order. We also show that this method does not miss many such fields. We then use a method similar to Hartung to show that there are infinitely many imaginary K whose class numbers are indivisible by any odd prime distinct from the characteristic.

1. Introduction and statement of results

The study of the structure of class groups of imaginary quadratic number fields dates back to Gauss, who posed the problem of finding all positive square-free d such that the class group of $\mathbb{Q}(\sqrt{-d})$, which we denote by $\mathrm{Cl}(-d)$, has some fixed order h. Heegner [1952], Baker [1967] and Stark [1967] solved Gauss's problem in the case $h = 1$, showing that there are only nine imaginary quadratic fields of class number 1. Baker [1971] and Stark [1975] later presented solutions to the case $h = 2$. A famous theorem of Siegel says that for $\epsilon > 0$, there exist positive constants $c_1(\epsilon)$ and $c_2(\epsilon)$ such that for each square-free d we have

$$c_1(\epsilon)d^{\frac{1}{2}-\epsilon} < h(-d) < c_2(\epsilon)d^{\frac{1}{2}+\epsilon}.$$

But this bound was ineffective. Goldfeld [1976] and Gross and Zagier [1983] showed that Gauss's problem is effectively computable for any h.

Of interest in the study of the structure of the class groups of the imaginary quadratic fields is the presence or absence of c-torsion for positive integers c. For $c = 2$, the answer to this question follows from Gauss's genus theory. For odd

MSC2000: primary 11R29; secondary 11R11.
Keywords: number theory, quadratic function fields, class numbers, class groups, divisibility.

primes c, a conjecture of Cohen and Lenstra [1984] states that the "probability" that $\mathrm{Cl}(-d)$ has an element of order c is

$$1-\prod_{1\le k<\infty}(1-c^{-k}).$$

With a few exceptions, little is known about divisibility of class numbers of imaginary quadratic number fields. A theorem of Davenport and Heilbronn [1971] shows that for $c=3$, the proportion of d for which the order of $\mathrm{Cl}(-d)$ is prime to 3 is at least $1/2$. Other results do not even give positive proportions. Soundararajan [2000] used a Diophantine construction to show that the number of $d<X$ such that $\mathrm{Cl}(-d)$ has an element of even order c is

$$\gg\begin{cases} X^{1/2+2/c-\epsilon}, & \text{if } c\equiv 0 \pmod 4,\\ X^{1/2+3/(c+2)-\epsilon}, & \text{if } c\equiv 2 \pmod 4.\end{cases} \tag{1}$$

This can also be used to give a bound for c odd since if $\mathrm{Cl}(-d)$ has an element of order $2c$, then it also has an element of order c. On the question of indivisibility of class numbers, Kohnen and Ono [1999] showed that for odd primes c, the number of $d<X$ such that $\mathrm{Cl}(-d)$ has no $c-$torsion is at least

$$\left(\frac{2(c-2)}{\sqrt{3}(c-1)}-\epsilon\right)\frac{\sqrt{X}}{\log X},$$

for any $\epsilon>0$.

In the setting of function fields, Friedman and Washington [1989] conjectured an analog of the Cohen–Lenstra heuristics. Achter [2006] used methods of algebraic geometry to prove this conjecture in a recent paper.

In this paper, we consider divisibility of class numbers of imaginary quadratic function fields. We use several styles of arguments applied to imaginary quadratic number fields prior to the work of Achter. We let q be a power of an odd prime, and define $k:=\mathbb{F}_q(x)$ and $A:=\mathbb{F}_q[x]$, the rational function field and polynomial ring over the finite field with q elements. Denote by $\mathrm{Cl}(f)$ the (divisor) class group of the function field $k(\sqrt{f})$ for f square-free and let $h(f)=\#\mathrm{Cl}(f)$. We look in particular at the case when $\deg f$ is odd. This is an analog of the case of an imaginary quadratic number field in which the prime at infinity ramifies and the unit group has rank 0. This case also has the property that the class number of the function field $k(\sqrt{f})$ is the same as the class number of its maximal order [Rosen 2002, Chapter 14]. Soundararajan [2000, Proposition 1] used solutions to the Diophantine equation $t^2d=m^c-n^2$ to find d such that $\mathrm{Cl}(-d)$ has an element of order c. The following is our analogous result for function fields.

Theorem 1.1. *Let $c\ge 3$ be a positive odd integer. Let $f\in A$ be a square-free polynomial of odd degree. If there exist nonzero $m,n,t\in A$ such that $m^c=n^2-t^2f$*

with $(m, n) = 1$ *and* $c \deg m < p \deg f$, *where* p *is the smallest prime dividing* c, *then* $\mathrm{Cl}(f)$ *has an element of order* c.

Remark 1. Cardon and Ram Murty [2001] used a similar Diophantine method to give a bound similar to Equation (1) in the function field case.

In the number field case, Soundararajan showed that any d such that $\mathrm{Cl}(-d)$ has an element of order c satisfies a Diophantine condition similar to that in his construction. The following is a function field analog of his result. In the theorem, the Diophantine condition from Theorem 1.1 corresponds to the case $l = 1$. Like Soundararajan's result, this is proven only in the case of c prime, but we expect a similar result to hold if c is composite.

Theorem 1.2. *Let* $c \geq 3$ *be prime and let* $f \in A$ *be a square-free polynomial of odd degree. Denote by* $h_c(f)$ *the number of elements of order* c *in* $\mathrm{Cl}(f)$. *Let* $C_+ = 2$ *and* $C_- = 1$. *If for each choice of* ϵ *in* $\{+, -\}$, D_ϵ *is the number of solutions in polynomials* l, m, n *and* t *with* l, m, n *monic to*

$$lm^c = n^2 l^2 - t^2 f, \quad \text{where } l \mid f,\ (m, fn) = 1 \text{ and } \deg lm < \frac{C_\epsilon}{2} \deg f, \tag{2}$$

then $D_- \leq h_c(f) \leq D_+$.

We also consider indivisibility of class numbers of quadratic function fields. Hartung [1974] used a famous class number relation to show that there are infinitely many imaginary quadratic number fields whose class numbers are not divisible by 3, and his method extends to any odd prime. We prove the following analog for function fields.

Theorem 1.3. *If* $c = 4$ *or* c *is an odd prime not dividing* q, *then there exist infinitely many quadratic imaginary function fields* K *over* k *with class number not divisible by* c.

Theorem 1.1 will be proven in Section 2, and Theorem 1.2 will be proven in Section 3. In Section 4, we prove Theorem 1.3. In Section 5, we conclude with some numerical examples.

2. Proof of Theorem 1.1

Some additional definitions and comments will be useful in proving these theorems. Given a quadratic extension K of the rational function field k, we can define a norm map $N : K \to k$ taking x to the product of its Galois conjugates (or $N(x) = x^2$ for $x \in k$). Furthermore, if B is the integral closure of A in K, then we can define the norm of an ideal $\mathfrak{I} \subset B$ as the ideal in A generated by elements of the set $\{N(b) : b \in \mathfrak{I}\}$. The ring B is a Dedekind domain and thus has unique factorization of ideals [Rosen 2002, Chapter 7]. In the special case that $\mathfrak{I} \subset B$ is principal, say

$\mathfrak{I} = (b)$, it is clear that $N(\mathfrak{I}) = (N(b))$. We also note that since A is a principal ideal domain, $N(\mathfrak{I})$ is principal even if $\mathfrak{I}$ is not. We also note that if $K = k(\sqrt{f})$, then $B = A[\sqrt{f}]$. This follows immediately from the formula for the roots of a quadratic equation. In the case of quadratic number fields, we have multiple cases depending on the parity of the discriminant, but in the function field case multiple cases do not arise since 2 is a unit of A so that an element of the form $(a+b\sqrt{f})/2$ (as would be given by the quadratic formula) can always be rewritten as $a'+b'\sqrt{f}$ with $a, b \in A$.

Proof of Theorem 1.1. Let $K = k(\sqrt{f})$ and consider the factorization of ideals $(m)^c = (n + t\sqrt{f})(n - t\sqrt{f})$ in the integral closure B of A in K. We claim that the ideals on the right side are relatively prime. If $\mathfrak{h}$ is a common prime divisor, then $(n + t\sqrt{f}) + (n - t\sqrt{f}) = 2n \in \mathfrak{h}$. However, we also have $m^c \in \mathfrak{h}$, which implies that $m \in \mathfrak{h}$ since $\mathfrak{h}$ is prime. Then $\mathfrak{h} | ((m, n))$, but this is a contradiction since $(m, n) = 1$.

Thus, the factorization of ideals shows that each of $(n \pm t\sqrt{f})$ is a cth power. Since $\{1, \sqrt{f}\}$ is a basis for B over A, let $\mathfrak{b}^c = (n+t\sqrt{f})$. We show that $\mathfrak{b}$ has order exactly c in $\mathrm{Cl}(f)$. Otherwise, $\mathfrak{b}$ has order $r < c$. Then $\mathfrak{b}^r = (u + v\sqrt{f})$ for some $u, v \in A$. We now consider the norms of each side of the equation $(n+t\sqrt{f}) = \mathfrak{b}^c$. On the left side, we have

$$N(n+t\sqrt{f}) \;=\; (n^2 - t^2 f) \;=\; (m)^c.$$

On the right side,

$$N(\mathfrak{b}^c) \;=\; N(\mathfrak{b}^r)^{c/r} \;=\; (u^2 - v^2 f)^{c/r}.$$

Comparing degrees now gives $c \deg m = c/r \cdot \deg(u^2 - v^2 f)$. Since the prime at infinity ramifies in $k(\sqrt{f})$, the unit group of the integral closure of A in $k(\sqrt{f})$ has rank 0, thus it follows that $n+t\sqrt{f} = [\alpha(u+v\sqrt{f})]^{c/r}$ for some $\alpha \in \mathbb{F}_q^\times$. Since $t \neq 0$, it is immediate that $v \neq 0$. Thus $v^2 f \neq 0$ has odd degree, and since u^2 has even degree, $\deg(u^2 - v^2 f) \geq \deg f$. Then $c \deg m \geq c/r \cdot \deg f$. But $c/r \geq p$, and $c \deg m < p \deg f$ by hypothesis, so it must be that $\mathfrak{b}$ has order exactly c in $\mathrm{Cl}(f)$. □

Remark 2. Soundararajan's Proposition 1 in [Soundararajan 2000] also holds if c is even. Indeed, in the function field case, the proof goes through without the explicit assumption that c is odd, but the conditions $m^c = n^2 - t^2 f$ and $c \deg m < p \deg f$ are never simultaneously satisfied for c even.

3. Proof of Theorem 1.2

Proof of Theorem 1.2. We first prove the lower bound. Suppose that we have a solution in l, m, n to t to Equation (2). We will show that the pair of solutions

(l, m, n, t) and $(l, m, n, -t)$ uniquely determines a pair of two ideals $\mathfrak{a}$ and $\bar{\mathfrak{a}}$ of order c in $\mathrm{Cl}(f)$ such that $N(\mathfrak{a}) = N(\bar{\mathfrak{a}})$ has degree less than $\frac{1}{2}\deg f$.

Let $K = k(\sqrt{f})$ and, as before, denote by B the integral closure of A in K. Consider the factorization of ideals in B:

$$(l)(m)^c = (lm^c) = (nl + t\sqrt{f})(nl - t\sqrt{f}). \tag{3}$$

Since $l|f$, l is a product of primes in K which are ramified over k, whence $(l) = \mathfrak{l}^2$ for some ideal $\mathfrak{l}$ of B. Letting $\mathfrak{h} = (nl + t\sqrt{f}, nl - t\sqrt{f})$, it follows from Equation (3) that $\mathfrak{l}^2|\mathfrak{h}^2$ so $\mathfrak{l}|\mathfrak{h}$. Furthermore, $\mathfrak{h}^2$ contains both lm^c and $(nl)^2 = n^2l^2$. Since $ln|fn$ and $(m, fn) = 1$, it follows that $(m^c, nl) = (m^c, n^2l) = 1$. Thus $(lm^c, n^2l) = l$, so $l \in \mathfrak{h}^2$. This shows that $\mathfrak{h}^2$ divides $(l) = \mathfrak{l}^2$, thus $\mathfrak{h} = \mathfrak{l}$.

We can now write $(nl + t\sqrt{f}) = \mathfrak{b}\mathfrak{l}$ and $(nl - t\sqrt{f}) = \bar{\mathfrak{b}}\mathfrak{l}$ where $\mathfrak{b}$ and $\bar{\mathfrak{b}}$ are relatively prime. Since $\mathfrak{l}^2 = (l)$, we have that $\bar{\mathfrak{b}}\mathfrak{b} = (m)^c$, so $\mathfrak{b}$ and $\bar{\mathfrak{b}}$ must both be cth powers, say $\mathfrak{b} = \beta^c$ and $\bar{\mathfrak{b}} = \bar{\beta}^c$ where β is an ideal of norm m. Define $\mathfrak{a} = \beta\mathfrak{l}$. Clearly $\mathfrak{a} \neq \bar{\mathfrak{a}}$ since otherwise we would have $\mathfrak{b} = \bar{\mathfrak{b}}$, from which it would follow that $t = 0$.

We now show that $\mathfrak{a}$ has order exactly c. Since

$$\mathfrak{a}^c = \beta^c\mathfrak{l}^c = \mathfrak{b}\mathfrak{l}(l)^{(c-1)/2} = (nl + t\sqrt{f})(l)^{(c-1)/2}$$

is principal, $\mathfrak{a}$ has order dividing c. Suppose $\mathfrak{a}$ is principal and write $\mathfrak{a} = (a + b\sqrt{f})$ with $a, b \in A$ and b nonzero (if b is 0 it follows from $\mathfrak{a}^c = (nl + t\sqrt{f})(l)^{(c-1)/2}$ that $t = 0$). Then $N(\mathfrak{a}) = N((a + b\sqrt{f})) = (a^2 - b^2f)$. Since a^2 has even degree and b^2f has odd degree, the degree of this must be at least $\deg f$. However, this implies that $\frac{1}{2}\deg f > \deg lm = \deg N(\mathfrak{a}) \geq \deg f$, a contradiction. Thus $\mathfrak{a}$ is not principal and must have order c.

We now consider the degree of a generating element of $N(\mathfrak{a})$. We have

$$N(\mathfrak{a})^c = (nl + t\sqrt{f})(l)^{(c-1)/2} \cdot (nl - t\sqrt{f})(l)^{(c-1)/2} = (lm^c)(l)^{c-1} = ((lm)^c).$$

Thus $N(\mathfrak{a})^c$ is generated by $(lm)^c$ whence $N(\mathfrak{a}) = (lm)$ which has degree $\deg lm < \frac{1}{2}\deg f$.

We now show that different solutions to Equation (2) with $C_\epsilon = 1$ correspond to distinct pairs of ideals of order c in $\mathrm{Cl}(f)$. Consider two distinct solutions (l_1, m_1, n_1, t_1) and (l_2, m_2, n_2, t_2) with $\deg l_im_i < \frac{1}{2}\deg f$. Let $\mathfrak{a}_i$ denote the corresponding ideals having order c in $\mathrm{Cl}(f)$. Suppose that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are in the same class in $\mathrm{Cl}(f)$. Then $\mathfrak{a}_1\bar{\mathfrak{a}}_2$ is principal, so let $\mathfrak{a}_1\bar{\mathfrak{a}}_2 = (a + b\sqrt{f})$. Then

$$(a^2 - b^2f) = N(\mathfrak{a}_1\bar{\mathfrak{a}}_2) = (l_1m_1l_2m_2).$$

Considering degrees in this equality, we see that

$$\deg(a^2 - b^2f) = \deg l_1m_1 + \deg l_2m_2 < \deg f,$$

so $b=0$ and $\mathfrak{a}_1\bar{\mathfrak{a}}_2=(a)$. Thus

$$(a)^c \;=\; \mathfrak{a}_1^c\bar{\mathfrak{a}}_2^c \;=\; (n_1l_1+t_1\sqrt{f})(n_2l_2-t_2\sqrt{f})(l_1l_2)^{(c-1)/2}.$$

Since the $\sqrt{f}$ term on the right side must be zero, we have $n_1l_1t_2=n_2l_2t_1$. From the equation in Equation (2), it is clear that $(n_il_i,t_i)^2|l_im_i^c$. Since l_i is square-free, this implies that $(n_il_i,t_i)|m_i^c$. Since also $(n_il_i,t_i)|fn_i$ and $(m_i^c,fn_i)=(m_i,fn_i)=1$, it follows that $(n_il_i,t_i)=1$. Using the fact that l_i and n_i are monic, we have that $t_1=t_2$ and $n_1l_1=n_2l_2$. Substituting into the Equation (2) gives $l_1m_1^c=l_2m_2^c$. Since l_i divides f and m_i is prime to f, it follows that $m_1=m_2$ and $l_1=l_2$, so the solutions are not distinct. A similar argument shows that $\mathfrak{a}_1$ and $\bar{\mathfrak{a}}_2$ are in different classes unless $(l_2,m_2,n_2,t_2)=(l_1,m_1,n_1,-t_1)$. Thus each pair of solutions of the form (l_1,m_1,n_1,t_1), $(l_1,m_1,n_1,-t_1)$ yields a unique pair of elements of order c. This completes the proof of the lower bound $D_-\le h_c(f)$.

It remains to show the upper bound. Define $s=h_c(f)/2$ for simplicity of notation. We note that s is an integer since if $\mathscr{C}\in \mathrm{Cl}(f)$ has order c, then so does $\mathscr{C}^{-1}$ (note also that since $c>2$ these elements must be distinct). Let $\mathscr{C}_1,\bar{\mathscr{C}}_1,\dots,\mathscr{C}_s,\bar{\mathscr{C}}_s$ be the classes of order c in $\mathrm{Cl}(f)$. By Theorem 4.4 in [Hayes 1999], we can choose integral ideals $\mathfrak{a}_i\in\mathscr{C}_i$ and $\bar{\mathfrak{a}}_i\in\bar{\mathscr{C}}_i$ of minimal degree less than $(\deg f-1)/2$. Furthermore, it is clear that ideals $\mathfrak{a}_i$ and $\bar{\mathfrak{a}}_i$ chosen to be minimal in this way are not divisible by any principal ideals.

Starting with a minimal pair of ideals $\mathfrak{a}_i$ and $\bar{\mathfrak{a}}_i$ we construct a solution to Equation (2) with $C_\epsilon=2$. Write $\mathfrak{a}_i=\mathfrak{b}_i\mathfrak{l}_i$ where $\mathfrak{l}_i$ is either the unit ideal or has order 2 in $\mathrm{Cl}(f)$ and $\mathfrak{b}_i$ is not divisible by any ideals of order 2. Similarly, write $\bar{\mathfrak{a}}_i=\bar{\mathfrak{b}}_i\bar{\mathfrak{l}}_i$ (in fact, $\mathfrak{l}_i=\bar{\mathfrak{l}}_i$). Then denote the unique monic generator of $N(\mathfrak{l}_i)$ by l_i. Note that each prime dividing l_i also divides f since any prime dividing $\mathfrak{l}_i$ is ramified over k. Since $\mathfrak{l}_i$ is not divisible by any principal ideal, l_i is not divisible by the square of any prime, so in particular $l_i|f$. Define m_i to be the monic generator for $N(\mathfrak{b}_i)$. Then

$$\deg l_im_i \;=\; 2\deg \mathfrak{b}_i\mathfrak{l}_i \;=\; 2\deg\mathfrak{a}_i \;\le\; \deg f-1 \;<\; \frac{C_+}{2}\deg f.$$

Since $\mathfrak{a}_i$ has order c, we can write $\mathfrak{a}_i^c=(a_i+b_i\sqrt{f})$ for some polynomials a_i and b_i, and we can assume that a_i is monic. Then $(l_i)^{(c-1)/2}=\mathfrak{l}_i^{c-1}$ divides $\mathfrak{a}_i^c$, so $l_i^{(c-1)/2}$ divides both a_i and b_i, so we may write $a_i=w_il_i^{(c-1)/2}$ and $b_i=t_il_i^{(c-1)/2}$. Since also $\bar{\mathfrak{a}}_i^c=(a_i-b_i\sqrt{f})$, we have that $(l_im_i)^c=l_i^{c-1}w_i^2-l_i^{c-1}t_i^2f$, and so $l_im_i^c=w_i^2-t_i^2f$. From the assumption that $l_i|f$ it follows that $l_i|w_i^2$, and since l_i is square-free this implies that $l_i|w_i$. Write $w_i=n_il_i$. Since $a_i=w_il_i^{(c-1)/2}$ and l_i are both monic, n_i is also monic. Thus, we have a solution to $l_im_i^c=n_i^2l_i^2-t_i^2f$ with $l_i|f$ and $\deg l_im_i<\frac{C_+}{2}\deg f$. Since t_i is not restricted to being monic, we note that substituting $-t$ for t gives another solution.

We now show that for the solutions constructed, $(m_i, n_i f) = 1$. Since $\mathfrak{b}$ and $\bar{\mathfrak{b}}$ are not divisible by any ideals of order 2, it follows that m_i, the monic generator for $N(\mathfrak{b}_i)$, is coprime to f. Since $(m_i, n_i)^2$ divides m_i^c and n_i^2 it also divides $t_i^2 f$, but since n_i is coprime to f, it follows that $(m_i, n_i)^2 | t_i^2$, so $(m_i, n_i) | t_i$. Since $n_i | a_i$, it follows that $(m_i, n_i) | (a_i + b_i \sqrt{f}) = \mathfrak{a}_i^c$. In particular, this means that each prime of A dividing (m_i, n_i) also divides $\mathfrak{a}_i$. However A is a principal ideal domain, but $\mathfrak{a}_i$ was taken not to be divisible by any principal ideal, so $(m_i, n_i) = 1$ and since also $(m_i, f) = 1$, we have $(m_i, n_i f) = 1$ as desired.

Finally, we must show that different pairs of ideals $\mathfrak{a}_i, \bar{\mathfrak{a}}_i$ and $\mathfrak{a}_j, \bar{\mathfrak{a}}_j$ give rise to distinct pairs of solutions as constructed above. If not, then it would follow that $a_i = a_j$ and $b_i = \pm b_j$. Then $\mathfrak{a}_i^c = \mathfrak{a}_j^c$, so $\mathfrak{a}_i = \mathfrak{a}_j$. Thus, we have shown that a pair of inverse elements of $\mathrm{Cl}(f)$ having order c gives a unique pair of solutions to Equation (2), concluding the proof of the upper bound $h_c(f) \le D_+$. □

4. Proof of Theorem 1.3

4.1. ***Background.*** We will use a class number relation over function fields proven by Yu. Before stating the proposition, we introduce some additional notation. If $m \in A$ is of odd degree but is not necessarily square-free, we define $h(m)$ to be the class number of the order $A[\sqrt{m}]$. This notation is consistent with our previous definition of $h(n)$ for n square-free because the class number of the maximal order $A[\sqrt{m}]$ is equal to the class number of the field $k(\sqrt{m})$ when m has odd degree and is square-free [Rosen 2002, Chapter 14]. We define $w(m) := \#A[\sqrt{m}]^\times/(q-1)$ and $h'(m) := h(m)/w(m)$. This allows us define the Hurwitz class number

$$H(m) := \sum_{n^2 | m} h'(m/n^2).$$

We now have defined all of the notation that we will need for the following class number relation, Proposition 7 of Yu [1995].

Proposition 4.1. *If $m \in A$ is monic, then*

$$\sum_{\substack{t \in A \\ \mu \in \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}}} H(t^2 - \mu m) = \sum_{d | m} \max(|d|, |m/d|) - \sum_{\substack{d | m \\ \deg d = 1/2 \deg m}} |m|^{-1/2} \frac{|m| - |m - d^2|}{q-1}, \quad (4)$$

where the sums on the right are over monic divisors and the sum on the left is over pairs (t, μ) such that $t^2 - \mu m$ is an imaginary discriminant. This is equivalent to the condition that either $t^2 - \mu m$ has odd degree or $t^2 - \mu m$ has a leading coefficient that is not a square in $\mathbb{F}_q$ [Rosen 2002, Chapter14].

We need one additional lemma regarding class numbers. Define the Kronecker symbol χ_f on the monic irreducible elements of A by

$$\chi_f(P) = \begin{cases} 1 & \text{if } P \text{ splits in } k(\sqrt{f}), \\ 0 & \text{if } P \text{ ramifies in } k(\sqrt{f}), \\ -1 & \text{otherwise,} \end{cases}$$

and extend χ_f to all monic polynomials in A by $\chi_f\left(\prod P_i^{e_i}\right) = \prod \chi_f(P_i)^{e_i}$. The following is Lemma 3 in [Yu 1995].

Lemma 1. For any square-free $f \in A$ and any $b \in A$,

$$\frac{h'(fb^2)}{h'(f)} = |f| \prod_{P|f} \left(1 - \frac{\chi_f(P)}{|P|}\right).$$

Corollary 1. Under the hypotheses of the lemma, $h'(fb^2)|h'(f)$.

We also prove a general proposition about polynomials.

Proposition 4.2. *Let $f_1, \dots, f_n \in A$ be monic polynomials of odd degree. There exists a monic irreducible polynomial $m \in A$ of odd degree such that each f_i for $1 \le i \le n$ is a quadratic nonresidue modulo m.*

Proof. Let $p_1, \dots, p_r$ be the monic irreducible polynomials of odd degree dividing any of the f_i, and let $l_1, \dots, l_s$ be the monic irreducibles of even degree dividing any of the f_i. By the multiplicativity of the Legendre symbol, it suffices to find a monic polynomial m such that $(p_u/m) = -1$ for each u and $(l_v/m) = 1$ for each v.

For each u with $1 \le u \le r$, let π_u be an irreducible polynomial such that $(\pi_u/p_u) = (-1)^{(q+1)/2}$. For $1 \le v \le s$, choose ν_v to be a monic irreducible such that $(\nu_v/l_v) = 1$. Such π_u and ν_v exist by Dirichlet's theorem on primes in arithmetic progressions. Applying this theorem again, choose m to be a monic irreducible of odd degree such that $m \equiv \pi_u \pmod{p_u}$ and $m \equiv \nu_v \pmod{l_v}$ for each choice of u and v.

We show that m satisfies the conclusion of the proposition. Applying quadratic reciprocity for function fields [Rosen 2002, Chapter 3], for each p_u we have

$$\left(\frac{p_u}{m}\right) = (-1)^{\frac{q-1}{2}\cdot\deg m\cdot\deg p_u}\cdot\left(\frac{m}{p_u}\right) = (-1)^{\frac{q-1}{2}}\cdot\left(\frac{\pi_u}{p_u}\right) = (-1)^{\frac{q-1}{2}}\cdot(-1)^{\frac{q+1}{2}} = -1.$$

Similarly, for the l_v, we have

$$\left(\frac{l_v}{m}\right) = (-1)^{\frac{q-1}{2}\cdot\deg m\cdot\deg l_v}\cdot\left(\frac{m}{l_v}\right) = 1\cdot\left(\frac{\nu_v}{l_v}\right) = 1.$$

Thus, m satisfies the conditions stated at the beginning of the proof and thus also the conclusion of the proposition. □

4.2. ***Proof of Theorem 1.3.*** Suppose that S is any finite set (possibly empty) of monic polynomials $f \in A$ of odd degree such that $c \nmid h(f)$. By Proposition 4.2, take m to be an irreducible monic polynomial of odd degree such that each $f \in S$ is a quadratic nonresidue modulo m (if $S = \varnothing$, take m to be any monic irreducible of odd degree). The class number relation Equation (4) gives us

$$\sum_{\substack{t \in A \\ \mu \in \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}}} H(t^2 - \mu m) \;=\; \sum_{d \mid m} \max(|d|, |m/d|) \;=\; 2q^{\deg m}.$$

Since $c \nmid 2q^{\deg m}$, at least one of the terms on the left side of the equation is not divisible by c, we can take μ and t so that $H(t^2 - \mu m)$ is not divisible by c. From the definition of the Hurwitz class number,

$$H(t^2 - \mu m) \;=\; \sum_{n^2 \mid m} h'\left(\frac{t^2 - \mu m}{n^2}\right).$$

Since the left side of the equation is indivisible by c, we can choose n such that $h'\left(\frac{t^2 - \mu m}{n^2}\right)$ is indivisible by c. We now write

$$\frac{t^2 - \mu m}{n^2} \;=\; f b^2,$$

where f is square-free. From Corollary 1, we have that $h'(f) | h'(fb^2)$. In particular, $c \nmid h'(f)$. Furthermore, we have $h'(f) = h(f)/w(f)$. Since the prime at infinity is totally ramified in $k(\sqrt{f})$, the group of units of $A[\sqrt{f}]$ has rank 0 and thus is just $\mathbb{F}_q^\times$. This means that

$$w(f) \;=\; \frac{\# A[\sqrt{f}]^\times}{q - 1} \;=\; 1.$$

So $h(f) = w(f)h'(f) = h'(f)$, whence $c \nmid h(f)$. This gives us an element $f \in A$ such that $h(f)$ is indivisible by c.

We show that $f \notin S$. We have that $f \cdot (bn)^2 = t^2 - \mu m$. Reducing modulo m, we have $f \equiv (t/bn)^2 \pmod{m}$, so f is a quadratic residue modulo m. In particular, $f \notin S$. Thus, there are infinitely many quadratic imaginary discriminants f of odd degree such that c does not divide the class number of $K = k(\sqrt{f})$.

5. Examples

We consider first an example constructed by Theorem 1.1. Let $q = 3$ and $c = 17$, so that we aim to construct a quadratic imaginary discriminant $f \in \mathbb{F}_3[x]$ such that

$h(f)$ is divisible by 17. Take

$$\begin{aligned} f &= 2x^5+2x^4+1,\\ n &= x^7+2x^6+x^5+2x^4+x^3+2,\\ t &= x^6+x^5+2x^3+1,\\ m &= x. \end{aligned}$$

Our choice of f is square-free (and, in fact, irreducible). The condition $c \deg m < p \deg f$ is clearly satisfied (note that since c is prime, we have $c = p$). We also have $(m, n) = 1$ and $m^{17} = n^2 - t^2 f$, so Theorem 1.1 says that $\mathrm{Cl}(f)$ has an element of order 17. Indeed, $h(f) = 17$. In fact, computation of a finite number of class numbers shows that there is no choice of f of smaller degree such that $17|h(f)$.

We now provide an example of the method of the proof of Theorem 1.3. Let $q = 3$, and define $k = \mathbb{F}_q(x)$. Begin with the polynomials

$$f_1 = x+2 \quad \text{and} \quad f_2 = x^3+x^2+2x = x(x^2+x+2).$$

It can be computed that $h(f_1) = 1$ and $h(f_2) = 6$. We will use the method of the proof of Theorem 1.3 to find a third quadratic imaginary discriminant f_3 such that $h(f_3)$ is relatively prime to $c = 5$. Using the same notation as the proof of Proposition 4.2, we have $p_1 = x$ and $l_1 = x^2+x+2$. The method of the proof now calls for us to find irreducible polynomials π_1 and ν_1 such that

$$\left(\frac{\pi_1}{p_1}\right) = (-1)^{\frac{q+1}{2}} = 1 \quad \text{and} \quad \left(\frac{\nu_1}{l_1}\right) = 1.$$

It will thus suffice to take $\pi_1 \equiv 1 \pmod{p_1}$, and $\nu_1 \equiv 1 \pmod{l_1}$. Because the next step in the proof is to apply the Chinese Remainder Theorem, it is unnecessary (although a trivial exercise) to actually compute irreducible polynomials π_1 and ν_1. In the proof we use the existence of irreducible polynomials to apply quadratic reciprocity, but for the purpose of construction we need only find appropriate residue classes to apply the Chinese Remainder Theorem. We now need a monic irreducible polynomial m of odd degree such that

$$m \equiv \begin{cases} 1 & \pmod{p_1},\\ 1 & \pmod{l_1}. \end{cases}$$

One such polynomial is $m = p_1 \cdot l_1 + 1 = x^3+x^2+2x+1$. By the class number relation Equation (4), we have

$$\sum_{\substack{t\in A\\ \mu\in\mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}}} H(t^2-\mu m) = \sum_{d|m} \max(|d|, |m/d|) = 54,$$

where the sum on the left is over all (μ, t) such that μ is either 1 or 2 and t has degree 0 or 1. Expanding the sum, we have

$$\begin{multline*}H(-m)+H(-2m)+2H(1-m)+2H(1-2m)+2H(x^2-m)\\ +2H(x^2-2m)+2H((x+1)^2-m)+2H((x+1)^2-2m)\\ +2H((x+2)^2-m)+2H((x+2)^2-2m)=54.\end{multline*}$$

Since $5 \nmid 54$, at least one of the Hurwitz class numbers on the left side of this equation is indivisible by 5. Although the first term, $H(-m)$ is 5, we find that the second term, $H(-2m)=H(m)$ is 3. Furthermore, since m is irreducible, we have by the definition of the Hurwitz class number that

$$H(-2m) \;=\; H(m) \;=\; \sum_{n^2|m} h'(m/n^2) \;=\; h'(m).$$

As discussed in the proof of Theorem 1.3, we have that $h(m)=h'(m)$, so $h(m)=3$. Thus choosing $f_3=m=x^3+x^2+2x+1$ gives a third polynomial f_3 with $5\nmid h(f_3)$.

References

[Achter 2006] J. D. Achter, "The distribution of class groups of function fields", *J. Pure Appl. Algebra* **204**:2 (2006), 316–333. MR 2006h:11132

[Baker 1967] A. Baker, "Linear forms in the logarithms of algebraic numbers. I, II, III", *Mathematika 13* (1966)*, 204-216; ibid. 14* (1967)*, 102-107; ibid.* **14** (1967), 220–228. MR 36 #3732

[Baker 1971] A. Baker, "Imaginary quadratic fields with class number 2", *Ann. of Math.* (2) **94** (1971), 139–152. MR 45 #8631

[Cardon and Ram Murty 2001] D. A. Cardon and M. Ram Murty, "Exponents of class groups of quadratic function fields over finite fields", *Canad. Math. Bull.* **44**:4 (2001), 398–407. MR 2002g:11164

[Cohen and Lenstra 1984] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups of number fields", pp. 33–62 in *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, Lecture Notes in Math. **1068**, Springer, Berlin, 1984. MR 85j:11144

[Davenport and Heilbronn 1971] H. Davenport and H. Heilbronn, "On the density of discriminants of cubic fields. II", *Proc. Roy. Soc. London Ser. A* **322**:1551 (1971), 405–420. MR 58 #10816

[Friedman and Washington 1989] E. Friedman and L. C. Washington, "On the distribution of divisor class groups of curves over a finite field", pp. 227–239 in *Théorie des nombres (Quebec, PQ, 1987)*, de Gruyter, Berlin, 1989. MR 91e:11138

[Goldfeld 1976] D. M. Goldfeld, "The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer", *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **3**:4 (1976), 624–663. MR 56 #8529

[Gross and Zagier 1983] B. Gross and D. Zagier, "Points de Heegner et dérivées de fonctions *L*", *C. R. Acad. Sci. Paris Sér. I Math.* **297**:2 (1983), 85–87. MR 85d:11062

[Hartung 1974] P. Hartung, "Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3", *J. Number Theory* **6** (1974), 276–278. MR 50 #4528

[Hayes 1999] D. R. Hayes, “Distribution of minimal ideals in imaginary quadratic function fields”, pp. 25–30 in *Applications of curves over finite fields (Seattle, WA, 1997)*, Contemp. Math. **245**, Amer. Math. Soc., Providence, RI, 1999. MR 2001a:11188

[Heegner 1952] K. Heegner, “Diophantische Analysis und Modulfunktionen”, *Math. Z.* **56** (1952), 227–253. MR 14,725j

[Kohnen and Ono 1999] W. Kohnen and K. Ono, “Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication”, *Invent. Math.* **135**:2 (1999), 387–398. MR 2000c:11087

[Rosen 2002] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **210**, Springer, New York, 2002. MR 2003d:11171

[Soundararajan 2000] K. Soundararajan, “Divisibility of class numbers of imaginary quadratic fields”, *J. London Math. Soc.* (2) **61**:3 (2000), 681–690. MR 2001i:11128

[Stark 1967] H. M. Stark, “A complete determination of the complex quadratic fields of class-number one”, *Michigan Math. J.* **14** (1967), 1–27. MR 36 #5102

[Stark 1975] H. M. Stark, “On complex quadratic fields wth class-number two”, *Math. Comp.* **29** (1975), 289–302. Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday. MR 51 #5548

[Yu 1995] J.-K. Yu, “A class number relation over function fields”, *J. Number Theory* **54**:2 (1995), 318–340. MR 96i:11128

Received: 2007-08-03 Revised: 2007-10-28 Accepted: 2007-10-28

Adam_Merberg@brown.edu *Department of Mathematics, Brown University,*
151 Thayer Street, Providence, RI 02912, United States