ACTA ARITHMETICA
LXXXI.1 (1997)

Class numbers of real quadratic function fields

by

Christian Friesen (Marion, Ohio)
and Paul van Wamelen (Baton Rouge, La.)

1. Introduction. Gauss [7] conjectured that there are infinitely many real quadratic fields with ideal class number 1. Empirical evidence suggests that about 3/4 of all primes p give rise to a field $\mathbb{Q}(\sqrt{p})$ with a class number of 1 and Cohen and Lenstra [3] have given very general heuristic arguments supporting this observation and many others. Given the many similarities between function fields and number fields it is reasonable to conjecture that the same is true of real quadratic function fields (see, for example, Friedman and Washington [5]). Those conjectures fix q and let the degree of M vary as they look at the ideal class number of $\mathbb{F}_q(t, \sqrt{M(t)})$. In this paper we shall fix the degree to be 4 and examine the behavior of ideal class numbers as q varies (excluding only powers of 2 or 3). In our first result we shall give a lower bound for the number of monic irreducible quartics $M \in \mathbb{F}_q[t]$ such that $\mathbb{F}_q(t, \sqrt{M(t)})$ has ideal class number of 1 and in the second theorem we shall see that, for any odd h and for all sufficiently large q, there exists an M as above giving rise to an ideal class number of h.

Readers interested in an introduction to quadratic function fields are directed to Emil Artin's thesis [1] or to more recent work of D. R. Hayes [8]. We turn briefly to a description of our notation.

Let $\mathbb{F}_q$ be the finite field of odd characteristic having q elements and use $\mathbb{F}_q^*$ to denote the multiplicative group. Fix M to be an even-degree squarefree monic in $\mathbb{F}_q[t]$ where t is an indeterminate. Adjoining $\sqrt{M}$ to $\mathbb{F}_q(t)$ provides us with a quadratic extension (analogous to a real quadratic extension) with $\mathcal{O}_M = \mathbb{F}_q[t, \sqrt{M(t)}]$ as its ring of integers.

For an irreducible even-degree monic M we have the *fundamental unit* of $\mathcal{O}_M$ defined as the element $T + U\sqrt{M}$ such that $T, U \in \mathbb{F}_q[t]$ are monic

1991 *Mathematics Subject Classification*: 11R58, 11R29, 11R11.
The second author was partially supported by grant LEQSF(1995-97)-RD-A-09 from the Louisiana Educational Quality Support Fund.

polynomials with T of minimal degree satisfying $T^2 - U^2M \in \mathbb{F}_q^*$. The *regulator* R_M of $\mathcal{O}_M$ is then the degree of T.

Two ideals $\mathcal{A}$ and $\mathcal{B}$ of $\mathcal{O}_M$ are *equivalent*, $\mathcal{A} \sim \mathcal{B}$, if $\mathcal{A} = c\mathcal{B}$ for some $c \in \mathbb{F}_q(t, \sqrt{M(t)})$. The set of ideal classes under this equivalence forms a finite abelian group called the *ideal class group* which we shall denote $\mathrm{Cl}(\mathcal{O}_M)$.

From this point onwards we shall restrict ourselves to M that are of degree 4 and if we let h_M denote the *ideal class number* of $\mathbb{F}_q(t, \sqrt{M(t)})$ then the number of points over $\mathbb{F}_q$ on the curve $y^2 = M(t)$ (including the infinite ones) is equal to $h_M R_M$.

Recently Thomas A. Schmidt [11] proved that for sufficiently large primes p there exists a degree six polynomial $M \in \mathbb{F}_p[t]$ such that the field $\mathbb{F}_p(t, \sqrt{M(t)})$ has ideal class number of 1. In the case of degree 4 polynomials we obtain a stronger result (Theorem 1.1) and a more general result (Theorem 1.2) which we describe below.

THEOREM 1.1. *Let $\mathbb{F}_q$ be the finite field of q elements with characteristic greater than 3. Then there exist at least $q^{7/2}/(10 \log\log q)$ monic irreducible quartics $M \in \mathbb{F}_q[t]$ such that the field $\mathbb{F}_q(t, \sqrt{M(t)})$ has ideal class number $h_M = 1$.*

THEOREM 1.2. *For any odd positive integer h there exists a bound N such that if $\mathbb{F}_q$ is the finite field of $q > N$ elements with characteristic greater than 3 then there exists an irreducible monic $M(t) \in \mathbb{F}_q[t]$ of degree 4 such that the field $\mathbb{F}_q(t, \sqrt{M(t)})$ has ideal class number of $h_M = h$.*

The idea of the proof of these theorems is the following. One of the authors recently proved the following theorem [6] which we quote here without proof.

THEOREM 1.3. *Let $\mathbb{F}_q$ be the finite field with q elements and with odd prime characteristic. If $M \in \mathbb{F}_q[t]$ is a monic quartic irreducible with $h_M R_M = 2^s mn$ where m, n are odd and where m is squarefree then there exist at least $2^{s-3} q(q-1)\phi(m)$ monic quartic irreducibles, $N \in \mathbb{F}_q[t]$, such that $\mathbb{F}_q[t, \sqrt{N(t)}]$ has ideal class number $h_N = n$ and regulator $R_N = 2^s m$.*

This reduces the task of finding quartics which give function fields with prescribed class numbers to finding quartics $M(t)$ such that the number of points on the elliptic curve $y^2 = M(t)$ has a certain squarefree part. In Section 3 we show that there exist "enough" integers L in the interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$ with the needed properties. In Section 2 we show that for such an L there exists a quartic $M(t)$ such that $y^2 = M(t)$ has L points.

2. Quartics $M(t)$ where $y^2 = M(t)$ has L solutions. Throughout this section we will assume that $\mathrm{char}(\mathbb{F}_q)$ is not equal to 2 or 3.

In this section we will show that given an even number L in the allowed range for the number of points on an elliptic curve, we can find a monic irreducible quartic M such that $y^2 = M(x)$ has L rational points over $\mathbb{F}_q$. We start by finding an explicit elliptic curve in Weierstrass form isomorphic to a given $y^2 = M(x)$.

PROPOSITION 2.1. *For any separable*

$$M(u) = u^4 + b_3u^3 + 3b_2u^2 + b_1u + b_0$$

in $\mathbb{F}_q[u]$ *the hyperelliptic curve defined by*

$$C_1 : \quad v^2 = M(u)$$

is isomorphic over $\mathbb{F}_q$ *to*

$$C_2 : \quad y^2 = x^3 + (-3b_2^2 + b_3b_1 - 4b_0)x + 2b_2^3 - b_2b_3b_1 + b_1^2 - 8b_2b_0 + b_3^2b_0.$$

Proof. By C_1 defining a hyperelliptic curve we mean C_1 is the affine part and the points at infinity are added by gluing on the chart

$$v'^2 = 1 + b_3u' + 3b_2u'^2 + b_1u'^3 + b_0u'^4$$

using the isomorphism

$$u' = \frac{1}{u}, \qquad v' = \frac{v}{u^2}.$$

In this way C_1 becomes a smooth projective variety (see [9, Section IIIa §1]).

It is easy to check that the map taking (u, v) to

$$(x, y) = (b_2 + b_3u + 2u^2 + 2v, b_1 + 6b_2u + 3b_3u^2 + 4u^3 + b_3v + 4uv)$$

is a rational map from C_1 to C_2 (see [2, pp. 35–36] for a method for obtaining this map). Also, if we set

$$\begin{aligned} v(x, y) = {} & -32b_2^3 + 3b_2^2b_3^2 + 12b_2b_3b_1 - b_3^3b_1 - 4b_1^2 + 24b_2x^2 - 3b_3^2x^2 \\ & + 8x^3 - 12b_2b_3y + b_3^3y + 8b_1y - 4y^2 \end{aligned}$$

then the map taking (x, y) to

$$(u, v) = \left(\frac{b_2b_3 - 2b_1 - b_3x + 2y}{8b_2 - b_3^2 + 4x}, \frac{v(x, y)}{(8b_2 - b_3^2 + 4x)^2} \right)$$

is a rational map from C_2 to C_1. It is also straightforward to verify that these two maps are inverses of each other. This shows that the two curves C_1 and C_2 are birationally equivalent. Since the discriminants of the quartic and cubic are equal and $M(x)$ is separable, the cubic must also be separable and therefore C_2 is smooth. So it only remains to recall that two birationally equivalent smooth curves are in fact isomorphic. ∎

It can be shown that for an irreducible M the cubic we find in this proposition has one and only one root in $\mathbb{F}_q$. We therefore need to show that for any L there exists an elliptic curve with L rational points and this additional property. We do this next.

For an elliptic curve E defined over $\mathbb{F}_q$, let $\#E(\mathbb{F}_q)$ denote the number of rational points (including the points at infinity) on E and $E(\mathbb{F}_q)[n]$ the rational n-torsion points. Let $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$.

PROPOSITION 2.2. *Let $\mathbb{F}_q$ be the finite field with q elements and with odd characteristic p and let $t \in [-2\sqrt{q}, 2\sqrt{q}]$ be an even integer. If $p \nmid t$ or $q = p$ then there exists an elliptic curve E defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q+1-t$ and $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. In [12] Schoof computes the number of elliptic curves with a given number of rational points. He also computes the number of such elliptic curves with the n torsion points all being rational. Although he does this explicitly only for n odd, a reading of the proof shows that it contains a proof of our theorem. For the sake of completeness we outline the proof.

As negation on an elliptic curve is defined over $\mathbb{F}_q$ the rational points occur in pairs. This implies that the number of non-2-division points is a multiple of 2. Therefore, if the curve has an even number of rational points, there must be a non-zero rational 2-division point.

First, assume $p \nmid t$. The canonical map

$$\mathrm{End}_{\mathbb{F}_q}(E)/2\,\mathrm{End}_{\mathbb{F}_q}(E) \hookrightarrow \mathrm{End}(E(\overline{\mathbb{F}}_q)[2])$$

is injective (see [13]). If ϕ is the Frobenius endomorphism then it is clear that $(\phi - 1)P = 0$ if and only if P is rational. The above injection then implies that if $E(\overline{\mathbb{F}}_q)[2] \subset E(\mathbb{F}_q)$ then

$$\frac{\phi - 1}{2} \in \mathrm{End}_{\mathbb{F}_q}(E).$$

Using the fact that ϕ satisfies the equation $\phi^2 - t\phi + q = 0$ it is easy to verify that $(\phi - 1)/2$ satisfies

$$\left(\frac{\phi-1}{2}\right)^2 - \left(\frac{t-2}{2}\right)\left(\frac{\phi-1}{2}\right) + \frac{q+1-t}{4} = 0.$$

This quadratic has discriminant $(t^2-4q)/4$. It is non-zero because we assume $p \nmid t$.

By [15, Theorem 4.1] and [15, Theorem 4.2] (or see [12]) there exists an elliptic curve E with $\#E = q + 1 - t$ such that its $\mathbb{F}_q$ endomorphism ring is given by the complex quadratic order of discriminant $t^2 - 4q$. This ring does not contain the root of a quadratic with discriminant $(t^2 - 4q)/4$. So this elliptic curve cannot have all of $E(\overline{\mathbb{F}}_q)[2]$ rational. As $E(\overline{\mathbb{F}}_q)[2] \cong$

$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and we have already seen that there is one rational 2-torsion point we must have

$$E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}.$$

By [12, Lemma 4.8] and [15, Theorem 4.1] there is always an elliptic curve with $\#E(\mathbb{F}_p) = p+1$ and $E(\mathbb{F}_p)$ cyclic. This implies that $E(\mathbb{F}_p)[2] \ncong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and so the case $q = p$ and $t = 0$ is also taken care of. ∎

Finally we need to show that there exists an M mapping to each elliptic curve found in the above proposition. The following lemma is the crucial ingredient for doing so.

LEMMA 2.3. *Let σ be a generator of the Galois group of $\mathbb{F}_{q^4}/\mathbb{F}_q$. The map from $\mathbb{F}_{q^4} - \mathbb{F}_{q^2}$ to $\mathbb{F}_{q^2}$ given by*

$$H(r) = -2r\sigma(r) + r\sigma^2(r) + \sigma(r)\sigma^2(r) + r\sigma^3(r) + \sigma(r)\sigma^3(r) - 2\sigma^2(r)\sigma^3(r)$$

is onto $\mathbb{F}_{q^2} - \mathbb{F}_q$.

Proof. Fix an element δ_0 in $\mathbb{F}_{q^4}$ but not in $\mathbb{F}_{q^2}$. Set $\delta = \delta_0 - \sigma^2(\delta_0)$. Then $\sigma^2(\delta) = -\delta$. It is clear that we can write any element of $\mathbb{F}_{q^4}$ as $r_1\delta + r_2$ for some $r_1, r_2 \in \mathbb{F}_{q^2}$. We then have

$$H(r_1\delta + r_2) = -6r_1\sigma(r_1)\delta\sigma(\delta) + (r_2 - \sigma(r_2))^2 - r_1^2\delta^2 - \sigma(r_1^2\delta^2).$$

Note that, as $\sigma(\delta\sigma(\delta)) = -\delta\sigma(\delta)$, we can write any element of $\mathbb{F}_{q^2}$ as $t_1\delta\sigma(\delta) + t_2$ for some $t_1, t_2 \in \mathbb{F}_q$. So to show that the map H is onto we need to demonstrate that for any t_1 in $\mathbb{F}_q^*$ and t_2 in $\mathbb{F}_q$ we can find r_1 in $\mathbb{F}_{q^2}^*$ and r_2 in $\mathbb{F}_{q^2}$ such that

$$-6r_1\sigma(r_1) = t_1,$$
$$(r_2 - \sigma(r_2))^2 - r_1^2\delta^2 - \sigma(r_1^2\delta^2) = t_2.$$

It is well known that the norm map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ is onto and so it is clear that we can find r_1 such that $-6r_1\sigma(r_1) = t_1$. Note that if now $t_2 + r_1^2\delta^2 + \sigma(r_1^2\delta^2)$ is zero we are done, but if it is a non-zero square in $\mathbb{F}_q$ then there is no r_2 such that $(r_2 - \sigma(r_2))^2$ equals it. So we need to show that we can pick r_1 such that $t_2 + r_1^2\delta^2 + \sigma(r_1^2\delta^2)$ is not a square in $\mathbb{F}_q$.

For s any one of the $q+1$ values $1, g^{q-1}, g^{2(q-1)}, \ldots, g^{q(q-1)}$, where g is a generator of $\mathbb{F}_{q^2}^*$, we see $\sigma(s) = 1/s$ and $-6(sr_1)\sigma(sr_1)$ also equals t_1. If

$$r_1^2\delta^2 + \sigma(r_1^2\delta^2) = s^2r_1^2\delta^2 + \sigma(s^2r_1^2\delta^2)$$

then

$$s^2\left(\frac{1}{s^2} - 1\right)r_1^2\delta^2 = \left(\frac{1}{s^2} - 1\right)\sigma(r_1^2\delta^2),$$

so $s^2 = 1$ or $s = \pm\sigma(r_1\delta)/(r_1\delta)$. If we apply σ to this last equality and then take reciprocals we find $-s = \pm\sigma(r_1\delta)/(r_1\delta)$. This is a contradiction and so $s = \pm 1$. So we see that there are $(q+1)/2$ values of $t_2 + r_1^2\delta^2 + \sigma(r_1^2\delta^2)$ such that $-6r_1\sigma(r_1) = t_1$. As there are only $(q-1)/2$ non-zero squares in $\mathbb{F}_q$ we

can pick r_1 such that $-6r_1\sigma(r_1) = t_1$ and $t_2 + r_1^2\delta^2 + \sigma(r_1^2\delta^2)$ is zero or a non-square. Finally, it is clear that we can then choose

$$r_2 = \tfrac{1}{2}\sqrt{t_2 + r_1^2\delta^2 + \sigma(r_1^2\delta^2)}$$

for either of the two possible square roots. ∎

We are now able to prove the main theorem of this section.

THEOREM 2.4. *Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p not 2 or 3. Let L be any even integer with $|L - q - 1| \le 2\sqrt{q}$. Set $t = L - q - 1$. If $p \nmid t$ or $q = p$ then there exists at least one monic irreducible quartic $M \in \mathbb{F}_q[x]$ such that the number of points defined over $\mathbb{F}_q$ (including the two points at infinity) on the hyperelliptic curve $y^2 = M(x)$ is L.*

Proof. Proposition 2.2 says that for L satisfying the hypothesis we can find an elliptic curve defined over E with $\#E(\mathbb{F}_q) = L$ and $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$. As the characteristic is not 2 or 3 any such elliptic curve can be written in the form

$$y^2 = (x - (-b - \sigma(b)))(x - b)(x - \sigma(b))$$

for some $b \in \mathbb{F}_{q^2} - \mathbb{F}_q$ and σ a generator for the Galois group of $\mathbb{F}_{q^4}/\mathbb{F}_q$.

Using Proposition 2.1 it is easy to show that if

$$M(x) = (x - r)(x - \sigma(r))(x - \sigma^2(r))(x - \sigma^3(r))$$

for some $r \in \mathbb{F}_{q^4}$ then the hyperelliptic curve $y^2 = M(x)$ is isomorphic to the elliptic curve given by $y^2 = (x - (-b - \sigma(b)))(x - b)(x - \sigma(b))$ where

$$b = \tfrac{1}{3}(-2r\sigma(r) + r\sigma^2(r) + \sigma(r)\sigma^2(r) + r\sigma^3(r) + \sigma(r)\sigma^3(r) - 2\sigma^2(r)\sigma^3(r)).$$

Lemma 2.3 says that there is an $r \in \mathbb{F}_{q^4} - \mathbb{F}_{q^2}$ mapping onto any $b \in \mathbb{F}_{q^2} - \mathbb{F}_q$. As r is not in $\mathbb{F}_{q^2}$, $M(x)$ is irreducible and as the two curves are isomorphic over $\mathbb{F}_q$ they have the same number of points. This completes the proof. ∎

3. Odd-part-squarefree integers. In this section we shall determine lower bounds for the number of even integers n in an interval that have odd part squarefree (that is, $p^2 \nmid n$ for odd primes p).

LEMMA 3.1. *Fix an odd prime p and positive integers b, r, t. The number of integers x in the interval $[r, r+t]$ satisfying $x \not\equiv b \pmod p$ and that have an odd part that is squarefree is bounded from below by*

$$(t+1)\left(1 - \frac{1}{p} - \sum_{v \le \sqrt{r+t}} \frac{1}{v^2}\right) - \pi(\sqrt{r+t})$$

where the sum is over all odd primes v less than or equal to $\sqrt{r+t}$ and where $\pi(x)$ represents the number of primes less than or equal to x.

P r o o f. Consider an odd prime v. Asymptotically we have $(t+1)/v^2$ elements in the interval $[r, r+t]$ that are divisible by v^2. The absolute error in this estimate is at most $1 - v^{-2}$. If we now sum over all odd primes $v \le \sqrt{r+t}$ we arrive at an upper bound for the number of elements in the interval that do not have odd part squarefree as

$$\sum_{v \le \sqrt{r+t}} \left(\frac{t+1}{v^2} + 1 \right) < \pi(\sqrt{r+t}) - 1 + \sum_{v \le \sqrt{r+t}} \frac{t+1}{v^2}$$

where the sum is over all odd primes v less than or equal to $\sqrt{r+t}$. Now, the number of integers in this interval that are congruent to b modulo p is bounded from above by $(t+1)/p + (p-1)/p$ so the number of odd-part-squarefree integers $x \not\equiv b \pmod{p}$ is at least

$$t + 1 - \left(\frac{t+1}{p} + 1 \right) - \sum_{v \le \sqrt{r+t}} \frac{t+1}{v^2} - (\pi(\sqrt{r+t}) - 1),$$

which finishes the proof of this lemma. ∎

For the results that are to follow we will wish to obtain approximate values for the two terms above. We note that

$$\sum_{v \le \sqrt{r+t}} \frac{1}{v^2} < \sum_{v} \frac{1}{v^2} < 0.21$$

where the second sum, over all odd primes, is arrived at by summing all primes less than 1000 and using the integral $\int_{1000}^{\infty} x^{-2}\,dx$ to bound the error.

We shall bound the function $\pi(x)$ with the assistance of the result due to Rosser and Schoenfeld [10, formula 3.2]

$$\pi(x) < \frac{x}{\log x} \left(1 + \frac{3}{2 \log x} \right).$$

Corollary 3.2. *For any odd positive integer n there exists a positive integer N such that if $q = p^m > N$ for some odd prime $p \ge 5$ and some positive integer m then there exists an integer x in the interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$ satisfying $x \equiv 0 \pmod{2n}$, $x \not\equiv 1 \pmod{p}$ and such that x/n has odd part squarefree.*

P r o o f. We begin our task by rewriting the problem. If we consider only those integers in the interval that are divisible by $2n$ and then divide by the same we obtain the equivalent statement that there exists an integer x in the interval $\left[\frac{q+1-2\sqrt{q}}{2n}, \frac{q+1+2\sqrt{q}}{2n}\right]$ such that $2xn \not\equiv 1 \pmod{p}$ and x has odd part squarefree. Let r be the first integer in our interval. Then the integers in our interval are those in $[r, r+t]$ where $t > 2\sqrt{q}/n - 2$. If $p \mid n$ then the condition $2xn \not\equiv 1 \pmod{p}$ is superfluous, otherwise we may rewrite it as $x \not\equiv (2n)^{-1} \pmod{p}$. To show the existence of at least one integer

with the desired properties we need to demonstrate that the lower bound of Lemma 3.1 is positive. In other words, we will wish to prove that

$$1 - \frac{1}{p} > \frac{\pi(\sqrt{r+t})}{t+1} + \sum_v \frac{1}{v^2}.$$

Using 0.21 as an upper bound for the summation and using $p = 5$ as a worst case for the left reduces the problem to showing that

$$0.59 > \frac{\pi(\sqrt{r+t})}{t+1}.$$

In the asymptotic sense, as q approaches infinity we have $r+t \approxeq q/(2n)$ and $t+1 \approxeq 2\sqrt{q}/n$. Since we have $\pi(x) \approxeq x/\log x$ we can write

$$\frac{\pi(\sqrt{r+t})}{t+1} \approxeq \frac{\sqrt{\frac{q}{2n}}}{\log\left(\sqrt{\frac{q}{2n}}\right)} \cdot \frac{1}{\frac{2\sqrt{q}}{n}} = \frac{\sqrt{n}}{\sqrt{2}(\log q - \log(2n))}$$

and it is clear that we can choose q so that the quantity in question is smaller than 0.59 from which the existence of the desired integer may be concluded. The arguments that follow serve to put a value to the bound N of the corollary.

We have $(q+1+2\sqrt{q})/(2n) \geq r+t$, which implies that

$$\begin{aligned}
\frac{\pi(\sqrt{r+t})}{t+1} &\leq \frac{\pi\left(\sqrt{\frac{q+1+2\sqrt{q}}{2n}}\right)}{\frac{2\sqrt{q}}{n} - 1} \\
&= \frac{1}{1 - \frac{n}{2\sqrt{q}}} \cdot \frac{\pi\left(\frac{\sqrt{q}+1}{\sqrt{2n}}\right)}{\frac{2\sqrt{q}}{n}} \\
&< \frac{1}{1 - \frac{n}{2\sqrt{q}}} \cdot \frac{n}{2\sqrt{q}} \left(1 + \frac{3}{2\log\left(\frac{\sqrt{q}+1}{\sqrt{2n}}\right)}\right) \frac{\frac{\sqrt{q}+1}{\sqrt{2n}}}{\log\left(\frac{\sqrt{q}+1}{\sqrt{2n}}\right)} \\
&= \frac{1 + q^{-1/2}}{1 - \frac{n}{2\sqrt{q}}} \left(1 + \frac{3}{2\log\left(\frac{\sqrt{q}+1}{\sqrt{2n}}\right)}\right) \frac{\sqrt{n}}{2\sqrt{2}\log\left(\frac{\sqrt{q}+1}{\sqrt{2n}}\right)} \\
&< \frac{1 + q^{-1/2}}{1 - \frac{n}{2\sqrt{q}}} \left(1 + \frac{3}{\log\left(\frac{q}{2n}\right)}\right) \frac{\sqrt{n}}{\sqrt{2}\log\left(\frac{q}{2n}\right)}.
\end{aligned}$$

Since we shall treat the special case $n = 1$ in the following corollary we may assume here that $n \geq 3$. If we assume, in addition, that $q > 2500n^2$ then we obtain

$$\frac{\pi(\sqrt{r+t})}{t+1} < \frac{1 + \frac{1}{150}}{1 - \frac{1}{100}} \left(1 + \frac{3}{\log 3750}\right) \frac{\sqrt{n}}{\sqrt{2}\log\left(\frac{q}{2n}\right)} < \frac{\sqrt{n}}{\log\left(\frac{q}{2n}\right)}.$$

When $q > 2n\exp(\sqrt{n}/0.59)$ the above expression will be less than 0.59 as required to demonstrate the existence of our desired integer. So, we may take N to be the maximum of $2500n^2$ and $2n\exp(\sqrt{n}/0.59)$. Looking at our asymptotic formula we see that the best we could hope for, in order to require $0.59 > \pi(\sqrt{r+t})/(t+1)$, is to get $N > 2n\exp(\sqrt{n}/(0.59\sqrt{2}))$. Even this is not, we should point out, the sharpest obtainable result—in the interest of brevity we have used an estimate for the number of squarefree integers that is not the best possible and readers interested in attempting improvements are referred to papers by Filaseta and Trifonov [4] and by Warlimont [14]. ∎

COROLLARY 3.3. *For all $q = p^m$ for some positive integer m and some prime $p \geq 5$ at least $1/2$ of all even integers x in the interval $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ have odd part squarefree and satisfy $x \not\equiv 1 \pmod{p}$.*

P r o o f. Our argument consists of a computer check to verify the result for all $q < 10^5$ and a proof, which follows, that the statement is also true for $q \geq 10^5$.

Following the argument of the previous lemma we see that we need to bound $\pi(\sqrt{r+t})/(t+1)$ by 0.09 in order to be certain of having $1/2$ of the integers satisfying our requirements. From above we have

$$\frac{\pi(\sqrt{r+t})}{t+1} < \frac{1+q^{-1/2}}{1-\frac{1}{2\sqrt{q}}}\left(1+\frac{3}{\log\left(\frac{q}{2}\right)}\right)\frac{1}{\sqrt{2}\log\left(\frac{q}{2}\right)}$$

where the right-hand side is a decreasing function of q. Substituting $q = 10^5$ gives a result on the right that is less than 0.09 and it follows that for $q \geq 10^5$ we have at least $1/2$ of the even integers in the interval $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ with odd part squarefree and satisfying $x \not\equiv 1 \pmod{p}$. We conclude our proof with the remark that a computer program verified the statement for all $q < 10^5$. ∎

4. Conclusion. We are now in a position to prove

THEOREM 1.1. *Let $\mathbb{F}_q$ be the finite field of q elements with characteristic greater than 3. Then there exist at least $q^{7/2}/(10\log\log q)$ monic irreducible quartics $M \in \mathbb{F}_q[t]$ such that the field $\mathbb{F}_q(t, \sqrt{M(t)})$ has ideal class number $h_M = 1$.*

P r o o f. Using Theorem 2.4 together with Corollary 3.3 gives us more than $2[\sqrt{q}]$ distinct even values of $L = 2^s m$ with odd part m squarefree such that there is at least one irreducible monic M with L points on the curve $y^2 = M(t)$. Now Theorem 1.3 says that for every such M we get at least $2^{s-3}q(q-1)\phi(m)$ monic quartic irreducibles N such that $h_N = 1$. It is evident that the curves $y^2 = M(t)$ and $y^2 = N(t)$ have the same number of

points (since $h_M R_M = h_N R_N$) and thus there will be no overlap as we take different values of L. To continue from here we shall need to find a lower bound for $2^{s-3}\phi(m) = \frac{1}{4}\phi(2^s m)$ for even integers $2^s m \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ with m odd. We will use a result of Rosser and Schoenfeld [10, formula 3.42]

$$\phi(n) > \frac{n}{e^\gamma \log\log n + 2.50637/(\log\log n)}$$

where γ is Euler's constant. The bound on the right is an increasing function of n and it follows that

$$\phi(2^s m) > \frac{q+1-2\sqrt{q}}{e^\gamma \log\log(q+1-2\sqrt{q}) + 2.50637/(\log\log(q+1-2\sqrt{q}))}$$

for $2^s m$ in the chosen interval.

Putting the pieces together we have a number of monic quartic irreducibles N with $h_N = 1$ in excess of

$$2[\sqrt{q}\,]q(q-1)\frac{1}{4} \cdot \frac{(q^{1/2}-1)^2}{e^\gamma \log\log(q+1-2\sqrt{q}) + 2.50637/(\log\log(q+1-2\sqrt{q}))} > \frac{q^{7/2}}{10\log\log q} B(q)$$

where

$$B(q) = \frac{5(1-q^{-1/2})^3(1-q^{-1})\log\log q}{e^\gamma \log\log(q+1-2\sqrt{q}) + 2.50637/(\log\log(q+1-2\sqrt{q}))} > \frac{5(1-q^{-1/2})^3(1-q^{-1})}{e^\gamma + 2.50637/((\log\log q)(\log\log(q+1-2\sqrt{q})))}.$$

To prove the theorem we will show that $B(q) > 1$. Since the last line describes an increasing function with a value greater than 1 when $q > 1000$ it follows that our theorem holds for $q > 1000$. Let $p = \mathrm{char}(\mathbb{F}_q)$. For the values of q less than 1000 a computer program verified that

$$\sum 2^{s-3} q(q-1)\phi(m) > \frac{q^{7/2}}{10\log\log q}$$

where the first sum is over all even $2^s m \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ with m odd and squarefree and with $2^s m \not\equiv 1 \pmod{p}$ if $p \neq q$. In fact, we could have replaced the coefficient $1/10$ in our theorem with $(13\log\log 5)/5^{5/2} \approxeq 0.1107$, this minimum occurs at $q = 5$. ∎

In similar fashion to the above we may combine Theorem 2.4 with Corollary 3.2 and reference the result from [6] to obtain

THEOREM 1.2. *For any odd positive integer h there exists a bound N such that if $\mathbb{F}_q$ is the finite field of $q > N$ elements with characteristic*

greater than 3 *then there exists an irreducible monic* $M(t) \in \mathbb{F}_q[t]$ *of degree* 4 *such that the field* $\mathbb{F}_q(t, \sqrt{M(t)})$ *has ideal class number* $h_M = h$.

We may take N to be the maximum of $2500h^2$ and $2h\exp(\sqrt{h}/0.59)$.

References

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

[2] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Student Texts 24, Cambridge University Press, 1991.

[3] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, in: Number Theory Noordwijkerhout, H. Jager (ed.), Lecture Notes in Math. 1068, Springer, Berlin, 1984, 33–62.

[4] M. Filaseta and O. Trifonov, *On gaps between squarefree numbers. II*, J. London Math. Soc. (2) 45 (1992), 215–221.

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

[6] C. Friesen, *Randomness of class groups of some real quadratic function fields*, in preparation.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*, Yale University Press; A. A. Clarke, New Haven, Conn., 1966.

[8] D. R. Hayes, *Real quadratic function fields*, in: CMS Conf. Proc. 7, 1985, 203–236.

[9] D. Mumford, *Tata Lectures on Theta II*, Progr. Math. 43, Birkhäuser, 1984.

[10] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[11] T. A. Schmidt, *Infinitely many real quadratic fields of class number one*, J. Number Theory 54 (1995), 203–205.

[12] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A 46 (1987), 183–211.

[13] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 134–144.

[14] R. Warlimont, *Squarefree numbers in arithmetic progressions*, J. London Math. Soc. (2) 22 (1980), 21–24.

[15] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) 2 (1969), 521–560.

Ohio State University at Marion
1465 Mt. Vernon Avenue
Marion, Ohio 43302
U.S.A.
E-mail: friesen.4@osu.edu

Department of Mathematics
Louisiana State University
Baton Rogue, Louisiana 70803-4918
U.S.A.

Received on 17.5.1996
and in revised form on 1.10.1996 (2989)