ACTA ARITHMETICA
XCVI.4 (2001)

Bounds for frequencies of class groups of real quadratic genus 1 function fields

by

Christian Friesen (Marion, OH)

1. Introduction. A long-standing conjecture of Gauss [11] is that there are infinitely many real quadratic number fields with ideal class number 1 and empirical evidence suggests the much stronger statement that about 3/4 of all primes p give rise to a field $\mathbb{Q}(\sqrt{p})$ with a class number of 1. This observation, and many others, have been given a wonderful heuristic explanation by Cohen and Lenstra [4]. Although computational data is abundant [2, 3, 14, 17, 20], proofs are conspicuously absent.

In the function field case, where similar conjectures have been introduced by Friedman and Washington [6] and refined by Yu [21], more is known. Let $\mathbb{F}_q$ be the finite field of q elements, let T be an indeterminate and let $M \in \mathbb{F}_q[T]$ be a squarefree monic polynomial of even degree d. Write the ideal class number of $\mathbb{F}_q(T, \sqrt{M(T)})$ as h_M. Although the expectations in this setting are frequently stated in terms requiring the degree to increase as q stays fixed we will be fixing the degree and letting q increase. Madan [15] showed that there are infinitely many q such that there is an $M \in \mathbb{F}_q[T]$ with $h_M = 1$ and $d = 4$ and Schmidt [19] proved that for sufficiently large primes q there exists an $M \in \mathbb{F}_q[T]$ with $d = 6$ and $h_M = 1$.

Suppose we are interested in arbitrary odd class numbers h. Ichimura [13] proved that there exist infinitely many primes q with quartics $M \in \mathbb{F}_q[T]$ such that $h_M = h$. In a joint paper with van Wamelen [10] it was shown that for all odd h and for all q (a power of a prime $p \geq 5$) that are sufficiently large there exist quartics $M \in \mathbb{F}_q[T]$ such that $h_M = h$. In the same article it was shown that there are at least $q^{7/2}/(10 \log\log q)$ monic irreducible quartics $M \in \mathbb{F}_q[T]$ that satisfy $h_M = 1$. This last result gives a lower bound of about $0.4q^{-1/2}(\log\log q)^{-1}$ for the probability that a randomly chosen irreducible monic quartic $M \in \mathbb{F}_q[T]$ has ideal class number 1.

2000 *Mathematics Subject Classification*: Primary 11R29; Secondary 11G20, 11R58.
Key words and phrases: class groups, Cohen–Lenstra conjecture, function fields.

This is somewhat unsatisfying as this lower bound vanishes when $q \to \infty$ whereas the empirical data [7] quite clearly indicates that we should expect proportions close to 3/4. As one of our main results we prove here that, when constrained to those monic quartics that have an irreducible cubic factor, the proportion of $M \in \mathbb{F}_q[T]$ with $h_M = 1$ is between 70% and 84%.

Further motivation for looking at ideal class groups in this context comes from the field of cryptography. Scheidler, Stein and Williams [18] have proposed a key-exchange cryptosystem based on the continued fraction expansion of an irrational quadratic in a real quadratic function field $\mathbb{F}_q(T, \sqrt{M(T)})$. The case where M has degree $d = 4$ was chosen as the one that performed best in terms of empirically-measured speed vs. hypothesized security. The security of this cryptosystem hinges on two main conjectures: that the discrete logarithm problem is usually difficult and that the continued fraction expansion of $\mathbb{F}_q(T, \sqrt{M(T)})$ is usually large (or, equivalently, that the ideal class number is small). Showing, as we will, that the class number is 1 more than 2/3 of the time means that the second assumption above will not be of concern as one could repeatedly iterate the coding process with enough different values of M to obtain arbitrarily small probability that none of them have class number of 1. This leaves us with a probability arbitrarily close to 1 that the code will not be broken due to a small continued fraction expansion.

The question as to how often we should expect the ideal class number to be divisible by a prime p is also of some interest. Restricting ourselves once more to the function field case we have a result of Yu [21] where for a fixed degree d the fraction of ideal class groups with a given p-Sylow group tends towards some limit as $q \to \infty$, subject to the condition that $p \nmid q - 1$. Yu further shows that the limit (as $d \to \infty$ with d even) of these limits exists and is equal to that predicted by the Cohen–Lenstra heuristics! The values of the individual limits, however, (say for $d = 4$, which is the case of interest for this paper) remain unspecified. We shall shed light on some of the behavior in the $d = 4$ case by determining upper and lower bounds for $P(h_M \equiv 0 \pmod p)$ and $P(h_M = p)$ for odd primes p. We shall also investigate how often the p-rank of the ideal class group is equal to 2.

2. Preliminaries. Let q be a prime, $\mathbb{F}_q$ be the finite field of q elements and T be an indeterminate. For any squarefree monic quartic $M \in \mathbb{F}_q[T]$ we write the ideal class group of $\mathbb{F}_q(T, \sqrt{M(T)})$ as $\mathcal{C}l_M$ and the cardinality of $\mathcal{C}l_M$, the ideal class number, as h_M. Readers interested in an introduction to quadratic function fields are directed to Emil Artin's thesis [1] or to more recent work of Hayes [12].

Define S_q to be the set of all monic quartics $M \in \mathbb{F}_q[T]$ that are divisible by an irreducible cubic in $\mathbb{F}_q[T]$. For the remainder of the paper we will

restrict our attention solely to polynomials belonging in this set—a restriction that is forced on us by the nature of some results that we pilfer from an earlier paper. At times it will be useful to consider the subset S_q', defined as those elements of S_q with a zero coefficient for the cubic term (i.e. those of the form $M(T) = T^4 + aT^2 + bT + c$ for some $a, b, c \in \mathbb{F}_q$). For any $N(T) \in S_q'$ consider the translates of N, those $M \in S_q$ of the form $M(T) = N(T + d)$ where $d \in \mathbb{F}_q$. Since $\mathbb{F}_q(T, \sqrt{N(T)})$ and $\mathbb{F}_q(T, \sqrt{M(T)})$ are isomorphic via $T \mapsto T + d$ and $\sqrt{N(T)} \mapsto \sqrt{M(T)}$ it follows that $\mathcal{C}l_M \cong \mathcal{C}l_N$ for any translate M of N. Therefore any result concerning the proportions of ideal class groups in S_q' will automatically be true also of the ideal class groups of S_q.

Suppose that $M(x)$ is a monic squarefree quartic for which the Jacobian of $y^2 = M(x)$ has odd cardinality. All points on this curve not of the form $(x, 0)$ can be paired up via $(x, y) \leftrightarrow (x, -y)$. This implies that there are an odd number of points on the curve precisely when there are an odd number of solutions to $M(x) = 0$. For a squarefree quartic this is equivalent to saying that M is the product of a linear polynomial and a cubic irreducible polynomial; in other words the Jacobian of $y^2 = M(x)$ has odd cardinality if and only if $M \in S_q$. This will, as a consequence later on, restrict our attention to those elliptic curves whose elliptic groups are also of odd cardinality.

We shall be somewhat relaxed with our terminology and write, for instance,

$$P(h \equiv 0 \pmod p) \quad \text{to mean} \quad \frac{\#\{M \in S_q : h_M \equiv 0 \pmod p\}}{\#S_q}.$$

The number of monic irreducible cubics in $\mathbb{F}_q[T]$ is given by $(q^3 - q)/3$ and there are q linear polynomials so $\#S_q = (q^4 - q^2)/3$. Define $N_q(A, B)$ as the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with $E(\mathbb{F}_q) \cong C_A \times C_B$.

Before submerging ourselves in the proof details it would, perhaps, be appropriate to outline our approach. Suppose, for instance, that we wish to bound $P(h \equiv 0 \pmod 3)$. We would begin with the bounds for the $N_q(A, B)$ that were obtained in a prior paper [8] and sum over all $A \equiv 0 \pmod 3$ to obtain the number of desired isomorphism classes. Next we would determine the number of elliptic curves of the form $E : y^2 = x^3 + Rx + S$ in each isomorphism class. Then, for each such curve E, we would count the number of $\mathbb{F}_q$-rational points $\mathcal{P}$ such that the subgroup $E(\mathbb{F}_q)/\langle \mathcal{P} \rangle$ satisfies the criteria for our ideal class groups (in this particular example we would require that the subgroup has cardinality divisible by 3). We would then see a 1-1 correspondence between such $E, \mathcal{P}$ pairs and $M \in S_q'$ under which $\mathcal{C}l_M \cong E(\mathbb{F}_q)/\langle \mathcal{P} \rangle$. It is precisely at this step that our decision to

examine the set S_q' forces us to consider only those elliptic groups where $\#E(\mathbb{F}_q) = AB$ is odd. We then multiply our count by q, accounting for translations, to obtain the number of desired $M \in S_q$ and finally divide by the total number of $M \in S_q$ to arrive at the proportion of M with the desired class group structure.

Without further ado we introduce some necessary notation. We write $m \mid n$ to mean that m divides n and $m \parallel n$ to mean that $m \mid n$ and $(m, n/m) = 1$. Also useful to us will be $\lfloor x \rfloor$ which denotes the greatest integer less than or equal to x. C_n shall be the cyclic group of order n and, for any set S, we use $\#S$ for the cardinality of S. Let $\mathrm{ord}_p(v)$ be the highest power of p dividing v. For $q \geq 3$ a prime and v and w odd positive integers with $w \mid q-1$ we define

$$\sigma(v) = \prod_{\substack{p^2 \mid v \\ p \mid (q-1)/w}} p^{\lfloor \mathrm{ord}_p(v)/2 \rfloor}.$$

From a previous paper [8] we have the following:

THEOREM. *Let $q > e^{100}$ be an odd prime. Let v and w be positive odd integers such that $w \mid q-1$. Define $\tau(x)$ as the number of positive squarefree divisors of x and let $\phi()$ denote Euler's totient function. Define $\sigma(v)$ as above. For any odd positive integers A and B with $B \mid A$ define $N_q(A,B)$ as the number of isomorphism classes of elliptic curves, E, over $\mathbb{F}_q$ with $E(\mathbb{F}_q) \cong C_A \times C_B$ where C_n is the cyclic group of order n. Then*

$$\sum_{\substack{B \equiv 0 \pmod w \\ AB \equiv 0 \pmod{vw^2} \\ AB \text{ odd}}} N_q(A,B) < \frac{0.74q}{\phi(v)w^3} \Bigg(\prod_{\substack{p \parallel v \\ p \mid (q-1)/w}} \frac{p}{p+1} \Bigg) \Bigg(1 + \frac{132 w^{1.25} \tau(v) v \sigma(v)}{q^{0.125}} \Bigg). \tag{2.1}$$

When, in addition, $vw < q^{0.07}$ we also have

$$\sum_{\substack{B \equiv 0 \pmod w \\ AB \equiv 0 \pmod{vw^2} \\ AB \text{ odd}}} N_q(A,B) > \frac{0.58q}{\phi(v)w^3} \Bigg(\prod_{\substack{p \mid v \\ p \mid (q-1)/w}} \frac{p}{p+1} \Bigg) \Bigg(1 - \frac{132 w^{1.25} \tau(v) v}{q^{0.125}} \Bigg). \tag{2.2}$$

REMARK. If $w \nmid q-1$ then

$$\sum_{\substack{B \equiv 0 \pmod{w} \\ AB \equiv 0 \pmod{vw^2} \\ AB \text{ odd}}} N_q(A,B) = 0.$$

This is equivalent to the statement that if we have an elliptic curve with $E(\mathbb{F}_q) \cong C_A \times C_B$ and $B \mid A$ then we must also have $B \mid q-1$.

We now wish to determine the number of elliptic curves of the form $E : y^2 = x^3 + Rx + S$ in each of these isomorphism classes. From earlier comments we are only interested in non-singular elliptic curves with groups of odd cardinality. Since the only points that are not paired up via $(x,y) \leftrightarrow (x,-y)$ are those with $y = 0$ or the point at infinity it follows that we must have an even number of solutions to $0 = x^3 + Rx + S$. This, in turn, means that $x^3 + Rx + S$ is an irreducible cubic and as a consequence we must have $S \neq 0$. If $q \not\equiv 1 \pmod 3$ then R must be non-zero if $x^3 + Rx + S$ is irreducible. Two elliptic curves, E_1 and E_2, of the form $E_i : y^2 = x^3 + R_i x + S_i$ are isomorphic if and only if $R_2 = a^4 R_1$ and $S_2 = a^6 S_1$ for some $a \in \mathbb{F}_q^*$. With the exception of at most 4 isomorphism classes (characterized by $R = 0$ when $q \equiv 1 \pmod 3$) we have exactly $(q-1)/2$ elliptic curves of the desired form in each isomorphism class. The exceptional classes, when they occur, have exactly $(q-1)/6$ elliptic curves of the desired form.

It follows that, for any odd A and B, the number of elliptic curves of the form $E : y^2 = x^3 + Rx + S$ with $E(\mathbb{F}_q) \cong C_A \times C_B$ is at least

$$(N_q(A,B) - 4)\frac{q-1}{2} + 4\frac{q-1}{6} > (N_q(A,B) - 3)\frac{q-1}{2}$$

and at most

$$N_q(A,B)\frac{q-1}{2}.$$

We paraphrase without proof an earlier result [9], Theorem 2.5, to obtain the following theorem.

THEOREM 2.3. *Let $\mathbb{F}_q$ be the finite field with q elements and characteristic $\neq 2, 3$. There is a 1-1 correspondence between $M \in S_q'$ and pairs $E, \mathcal{P}$ of non-singular elliptic curves $E : w^2 = v^3 + Av + B$ with $\#E(\mathbb{F}_q)$ odd and with $\mathcal{P}$ a finite $\mathbb{F}_q$-rational point on E. Under this correspondence the ideal class group of $\mathbb{F}_q(T, \sqrt{M(T)})$ is isomorphic to the coset $E(\mathbb{F}_q)/\langle \mathcal{P} \rangle$ where $\langle \mathcal{P} \rangle$ denotes the subgroup generated by $\mathcal{P}$.*

The above theorem is a consequence of a birational equivalence between an elliptic curve, E, and a plane quartic model, $y = M(x)$, for it. Under such a correspondence the Jacobian of the quartic may be canonically identified with the group $E(\mathbb{F}_q)$ and it is this correspondence that leads to the stated result.

REMARK. Suppose that $E(\mathbb{F}_q) \cong C_A \times C_B$ with an odd prime $p \mid A$ and $p \nmid B$. Then there exist AB/p elements g of $C_A \times C_B$ with $p \mid (AB/\#\langle g\rangle)$. Since one of these elements g is the identity, corresponding to the point at infinity of $E(\mathbb{F}_q)$, there are exactly $AB/p - 1$ finite $\mathbb{F}_q$-rational points $\mathcal{P}$ on E that will have associated quartics in S'_q with ideal class group divisible by p.

The Weil bound gives $\#E(\mathbb{F}_q) \in [(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$ (this standard result can be found, for instance, in Eichler [5]) so the number of finite $\mathbb{F}_q$-rational points $\mathcal{P}$ for each curve E is in $[q - 2\sqrt{q}, q + 2\sqrt{q}]$.

3. Bounds on ideal class group frequencies. The author has some conjectures [7] for the degree 4 case which are in close, but not perfect, agreement with those obtained by averaging the Cohen–Lenstra heuristics. As a consequence, it is conjectured that for $q \not\equiv 1 \pmod p$ we should see that

$$\lim_{q\to\infty} P(h_M \equiv 0 \pmod p) = \frac{1}{p(p-1)}$$

with slightly different limits if we restrict our q to those satisfying $q \equiv 1 \pmod p$. In the following theorem we prove upper and lower bounds that differ from the above prediction by less than 20% (in relative terms).

THEOREM 3.1. *Let $q > e^{100}$ be prime. Let p be an odd prime. Define S_q to be the set of all monic quartics $M \in \mathbb{F}_q[T]$ that are divisible by an irreducible cubic in $\mathbb{F}_q[T]$. Let h_M be the ideal class number of $\mathbb{F}_q(T, \sqrt{M(T)})$ and write $P(p|h)$ as shorthand for $\#\{M \in S_q : h_M \equiv 0 \pmod p\}/\#S_q$. Then*

$$P(p|h) < \frac{1.12}{p(p-1)} + \frac{295}{q^{0.125}p} + \frac{232}{q^{0.125}p^{1.75}}.$$

If, in addition to the above hypotheses, we require that $p < q^{0.03}$, then we obtain the lower bounds

$$P(p|h) > \frac{0.867}{p(p-1)} - \frac{234}{q^{0.125}p} > \frac{0.84}{p(p-1)} \qquad \text{if } p \nmid q-1,$$

$$P(p|h) > \frac{0.867(p+1)}{p^3} - \frac{234}{q^{0.125}p} - \frac{150}{q^{0.125}p^{1.75}} > \frac{0.84(p+1)}{p^3} \qquad \text{if } p \mid q-1.$$

Proof. If we wish the ideal class group of the quartic to be divisible by p then p must divide the order of group of the associated elliptic curve. This is only possible if $p \mid A$ where $E(\mathbb{F}_q) \cong C_A \times C_B$. We begin by considering the case where $p \nmid q-1$. Recalling formula (2.1) and setting $v = p$ and $w = 1$ we obtain

$$\sum_{\substack{A \equiv 0 \pmod p \\ A \text{ odd}}} N_q(A,B) = \sum_{\substack{AB \equiv 0 \pmod p \\ AB \text{ odd}}} N_q(A,B) < q\left(\frac{0.74}{p-1} + \frac{196p}{q^{0.125}(p-1)}\right).$$

Now, each isomorphism class contains at most $(q-1)/2$ elliptic curves of the desired form and each such curve has a group of order less than $q+2\sqrt{q}+1$. Since $p\nmid q-1$ it follows from the remark immediately after (2.2) that $p\nmid B$. The remark following Theorem 2.3 implies that, for each such elliptic curve, just less than 1 in p of its $\mathbb{F}_q$-rational points $\mathcal{P}$ will result in a quartic with an ideal class number divisible by p. Therefore the number of monic quartics $M\in S_q'$ that give rise to ideal class numbers of $\mathbb{F}_q(T,\sqrt{M(T)})$ that are divisible by p is bounded from above by

$$q\biggl(\frac{0.74}{p-1}+\frac{196p}{q^{0.125}(p-1)}\biggr)\frac{q-1}{2}\cdot\frac{q+2\sqrt{q}+1}{p}<q^3\biggl(\frac{0.37}{p^2-p}+\frac{98}{q^{0.125}p}\biggr).$$

Let us now consider the other case, where $p\,|\,q-1$. Again referring to (2.1) with $v=p$ and $w=1$ we obtain the following bound for the number of desired isomorphism classes:

$$\sum_{\substack{A\equiv 0\,(\mathrm{mod}\,p)\\ A\,\mathrm{odd}}}N_q(A,B)<q\biggl(\frac{0.74p}{p^2-1}+\frac{196p^2}{q^{0.125}(p^2-1)}\biggr).$$

Some of isomorphism classes above will have a p-rank of 2. We determine an upper bound for these via (2.1) once again, this time with $v=1$ and $w=p$. The number of isomorphism classes with a p-rank of 2 is then bounded from above by

$$\sum_{\substack{A\equiv 0\,(\mathrm{mod}\,p)\\ B\equiv 0\,(\mathrm{mod}\,p)\\ AB\,\mathrm{odd}}}N_q(A,B)=\sum_{\substack{B\equiv 0\,(\mathrm{mod}\,p)\\ AB\equiv 0\,(\mathrm{mod}\,p^2)\\ AB\,\mathrm{odd}}}N_q(A,B)<q\biggl(\frac{0.74}{p^3}+\frac{98}{q^{0.125}p^{1.75}}\biggr).$$

If an elliptic curve E has a p-rank of 2 then $p\,|\,\#(E(\mathbb{F}_q)/\langle\mathcal{P}\rangle)$ for all $\mathcal{P}$. It follows that every $\mathbb{F}_q$-rational point $\mathcal{P}$ of E gives rise to a quartic M with $p\,|\,h_M$. So, we shall count, with weight $1/p$, all the elliptic curves with p-rank at least 1 and then count, with weight $1-1/p$, those with p-rank of 2 and thus avoid doubly counting the same contribution. We obtain the following upper bound for the number of monic quartics $M\in S_q'$ that give rise to an ideal class group divisible by p:

$$\begin{aligned}&q^3\biggl(\frac{0.37}{p^2-1}+\frac{98p}{q^{0.125}(p^2-1)}+\biggl(1-\frac{1}{p}\biggr)\biggl(\frac{0.37}{p^3}+\frac{49}{q^{0.125}p^{1.75}}\biggr)\biggr)\\&\qquad<q^3\biggl(0.37\biggl(\frac{1}{p^2-1}+\frac{p-1}{p^4}\biggr)+\frac{98p}{q^{0.125}(p^2-1)}+\frac{49(p-1)}{q^{0.125}p^{2.75}}\biggr)\\&\qquad<q^3\biggl(\frac{0.37}{p(p-1)}+\frac{98}{q^{0.125}p}+\frac{77}{q^{0.125}p^{1.75}}\biggr).\end{aligned}$$

As this bound is larger (with the presence of the third term) than the bound in the case where $p \nmid q-1$ we conclude that, no matter what the congruence of q is modulo p, we have an upper bound for the number of monic quartics $M \in S'_q$ having an ideal class number of $\mathbb{F}_q(T, \sqrt{M(T)})$ divisible by p of

$$q^3\left(\frac{1.12}{p(p-1)} + \frac{295}{q^{0.125}p} + \frac{232}{q^{0.125}p^{1.75}}\right).$$

From our previous remark concerning S_q and S'_q we may multiply these results for S'_q by q to obtain the desired upper bounds for the set S_q.

We begin our proof of the lower bounds by first treating the case $p \nmid q-1$. From (2.2), with $v = p$ and $w = 1$ we have

$$\sum_{\substack{A \equiv 0 \,(\mathrm{mod}\, p)\\ A \text{ odd}}} N_q(A,B) = \sum_{\substack{AB \equiv 0 \,(\mathrm{mod}\, p)\\ AB \text{ odd}}} N_q(A,B) > q\left(\frac{0.58}{p-1} - \frac{154w^{1.25}p}{q^{0.125}(p-1)}\right).$$

We see that there are at least

$$q\left(\frac{0.58}{p-1} - \frac{154w^{1.25}p}{q^{0.125}(p-1)} - \frac{3}{q}\right)\frac{q-1}{2}$$

elliptic curves of the desired form with $p \,|\, A$ each of which has at least $q - 2\sqrt{q} + 1$ points $\mathcal{P}$ on it. Since $p \nmid q-1$ the p-Sylow subgroup is cyclic and therefore there are $\#E/p - 1$ points $\mathcal{P}$ on the curve that are associated with a quartic M such that $h_M \equiv 0 \,(\mathrm{mod}\, p)$. It follows that the number of $M \in S'_q$ with $p \,|\, h_M$ must be at least

$$q^3\left(\frac{0.289}{p(p-1)} - \frac{78}{q^{0.125}p}\right)$$

from which we can easily obtain the stated lower bounds for the case where $p \nmid q-1$.

The case $p \,|\, q-1$ is more complicated. If the p-rank of the elliptic group is 1 then we proceed as before. If $E(\mathbb{F}_q) \cong C_A \times C_B$ with $p \,|\, B$ then every associated monic will have an ideal class group divisible by p.

From (2.2), with $v = p$ and $w = 1$ we have

$$\sum_{\substack{A \equiv 0 \,(\mathrm{mod}\, p)\\ A \text{ odd}}} N_q(A,B) > q\left(\frac{0.58p}{p^2-1} - \frac{154p^2}{q^{0.125}(p^2-1)}\right).$$

If all of the elliptic curves in the isomorphism classes counted above had a p-rank of 1 then we would proceed as before, with the comment that the number of M in S'_q related to each such curve must be $\#E(\mathbb{F}_q)/p - 1$. However, since we are in the case where $p \,|\, q-1$, some of the isomorphism classes will have elliptic curves with a p-rank of 2 and for these curves every one of the associated $M \in S'_q$ will satisfy $h_M \equiv 0 \,(\mathrm{mod}\, p)$. To determine the

additional contribution from these we find a lower bound for the number of isomorphism classes with a p-rank of 2 by setting $v = 1$ and $w = p$ in (2.2) to obtain

$$\sum_{\substack{B\equiv 0 \,(\mathrm{mod}\, p)\\ AB\equiv 0 \,(\mathrm{mod}\, p^2)\\ AB \text{ odd}}} N_q(A,B) > q\bigg(\frac{0.58}{p^3} - \frac{77p^{1.25}}{q^{0.125}p^3}\bigg).$$

Combining the contributions from the elliptic curves of p-rank 1 with those of p-rank 2, being careful not to count the same curves twice, gives us the following lower bound for the number of $M \in S_q'$ with $p \,|\, h_M$:

$$\begin{aligned}
&\#\{M \in S_q' : h_M \equiv 0 \ (\mathrm{mod}\, p)\}\\
&\qquad > \frac{q(q-1)}{2}\bigg(\frac{0.58p}{p^2-1} - \frac{154p^2}{q^{0.125}(p^2-1)}\bigg)\frac{q-2\sqrt{q}+1-p}{p}\\
&\qquad\quad + \frac{q(q-1)}{2}\bigg(\frac{0.58(p-1)}{p^4} - \frac{77p^{1.25}(p-1)}{q^{0.125}p^4}\bigg)(q-2\sqrt{q})\\
&\qquad > q^3\bigg(\frac{0.289(p+1)}{p^3} - \frac{78}{q^{0.125}p} - \frac{50}{q^{0.125}p^{1.75}}\bigg).
\end{aligned}$$

Multiplying the above result by q converts it to the number of $M \in S_q$ with $p \,|\, h_M$. Finally, since $\#S_q < q^4/3$, if we further divide by $q^4/3$ we will immediately obtain the lower bound for $P(h \equiv 0 \ (\mathrm{mod}\, p))$ in the case where $p \,|\, q-1$, concluding our proof. ∎

Lemma 3.2. *Let $q > e^{100}$ be prime. Let p and r be distinct odd primes. Define S_q to be the set of all monic quartics $M \in \mathbb{F}_q[T]$ that are divisible by an irreducible cubic in $\mathbb{F}_q[T]$. Let h_M be the ideal class number of $\mathbb{F}_q(T, \sqrt{M(T)})$ and write $P(pr|h)$ as shorthand for $\#\{M \in S_q : h_M \equiv 0 \ (\mathrm{mod}\, pr)\}/\#S_q$. Then, for $M \in S_q$,*

$$P(pr|h) < \frac{1.12}{(p^2-p)(r^2-r)} + \frac{597}{q^{0.125}(p-1)(r-1)}.$$

Proof. If we wish the ideal class group of the quartic to be divisible by pr then pr must divide the order of the group of the associated elliptic curve. We treat separately the 4 cases depending on the value of $\gcd(pr, q-1)$ and begin by considering the case where $\gcd(pr, q-1) = 1$. Recalling the result of (2.1) and setting $v = pr$ and $w = 1$ we obtain

$$\sum_{\substack{AB\equiv 0 \,(\mathrm{mod}\, pr)\\ AB \text{ odd}}} N_q(A,B) < \frac{0.74q}{(p-1)(r-1)}\bigg(1 + \frac{528pr}{q^{0.125}}\bigg).$$

Now, each isomorphism class contains at most $(q-1)/2$ elliptic curves of the desired form and each such curve has a group of order less than

$q+2\sqrt{q}+1$. Since $p\nmid q-1$ and $r\nmid q-1$ it follows that $p\nmid B$ and $r\nmid B$ and we have $\#E(\mathbb{F}_q)/(pr)-1$ points $\mathcal{P}$ such that the quartic M associated with $(E,\mathcal{P})$ satisfies $h_M \equiv 0 \pmod{pr}$. Therefore the number of monic quartics $M \in S'_q$ with $pr \mid h_M$ is bounded from above by

$$q\frac{0.74}{(p-1)(r-1)}\left(1+\frac{528pr}{q^{0.125}}\right)\frac{q-1}{2}\cdot\frac{q+2\sqrt{q}+1}{pr} < q^3\frac{0.37}{pr(p-1)(r-1)}\left(1+\frac{528pr}{q^{0.125}}\right).$$

Dividing this by $\#S'_q$ gives, for the case where $\gcd(pr,q-1)=1$,

$$P(pr|h) < \frac{1.12}{(p^2-p)(r^2-r)}+\frac{587}{q^{0.125}(p-1)(r-1)}.$$

The next cases to be considered are when exactly one of p and r divides $q-1$. We shall treat the case where $\gcd(pr,q-1)=p$ and use the symmetry of the situation to obtain the other result as well. We shall see that there are two main differences between this case and the situation where $\gcd(pr,q-1)=1$. They are the presence of the factor $p/(p+1)$ that shows up in the determination of the number of isomorphism classes and the fact that some of the elliptic curves will now have a p-rank of 2.

Referring to (2.1) once again we obtain the bound below for the number of isomorphism classes of desired form:

$$\sum_{\substack{AB\equiv 0 \pmod{pr}\\ AB \text{ odd}}} N_q(A,B) < \frac{0.74qp}{(p^2-1)(r-1)}\left(1+\frac{528pr}{q^{0.125}}\right).$$

Some of the isomorphism classes above will have a p-rank of 2. We determine an upper bound for these via (2.1) once again, this time with $v=r$ and $w=p$. The number of isomorphism classes with a p-rank of 2 and divisible by r is bounded from above by

$$\sum_{\substack{B\equiv 0 \pmod{p}\\ AB\equiv 0 \pmod{p^2r}\\ AB \text{ odd}}} N_q(A,B) < \frac{0.74q}{(r-1)p^3}\left(1+\frac{264p^{1.25}r}{q^{0.125}}\right).$$

All of the $\mathbb{F}_q$-rational points $\mathcal{P}$ on the elliptic curves E with p-rank of 2 give rise to quartics with associated ideal class number divisible by p and fewer than $\#E(\mathbb{F}_q)/r$ of these give class numbers that are also divisible by r. To avoid counting the same curve twice we add to the amount from the curves with p-rank ≥ 1 a correction equal to $(p-1)/p$ of the total we obtain from the p-rank 2 curves. We obtain the following upper bound, when $\gcd(pr,q-1)=p$, for the number of monic quartics $M \in S'_q$ such that h_M

is divisible by pr:

$$\begin{aligned} q^3\bigg(\frac{0.37}{(p^2-1)(r^2-r)}\bigg(1+\frac{528pr}{q^{0.125}}\bigg)+\frac{0.37(p-1)}{(r^2-r)p^4}\bigg(1+\frac{264p^{1.25}r}{q^{0.125}}\bigg)\bigg) \\ < q^3\bigg(0.37\bigg(\frac{p^4+p^3-p^2-p+1}{p^4(p^2-1)(r^2-r)}\bigg) \\ + \frac{196pr}{q^{0.125}(p^2-1)(r^2-r)}+\frac{98(p-1)p^{1.25}r}{q^{0.125}(r^2-r)p^4}\bigg) \\ < q^3\bigg(\frac{0.37}{(p^2-p)(r^2-r)}+\frac{198}{q^{0.125}(p-1)(r-1)}\bigg) \end{aligned}$$

where we have used basic calculus to see that

$$\frac{196p}{p^2-1}+\frac{98(p-1)}{p^{2.75}}<\frac{198}{p-1}.$$

Since the bound we have obtained above is symmetric with respect to p and r it follows that the same upper bound (for the number of monic quartics $M\in S_q'$ such that h_M is divisible by pr) holds for the case where $p\nmid q-1$ and $r\mid q-1$.

The final case remaining is the case where $\gcd(pr,q-1)=pr$. We begin by determining an upper bound for the number of isomorphism classes whose groups are divisible by pr and obtain

$$\sum_{\substack{AB\equiv 0\,(\mathrm{mod}\,pr)\\ AB\,\mathrm{odd}}} N_q(A,B)<\frac{0.74qpr}{(p^2-1)(r^2-1)}\bigg(1+\frac{528pr}{q^{0.125}}\bigg).$$

We now need to determine the maximum number of isomorphism classes where the p-rank is 2, where the r-rank is 2 and where they are both equal to 2 and sum their contributions making particular note of the fact that if both p- and r-ranks of an elliptic curve are 2 then all associated values of $M\in S_q'$ have $pr\mid h$. We obtain, for the number of monic quartics $M\in S_q'$ such that h_M is divisible by pr, the following upper bound:

$$\begin{aligned} &\frac{0.37q^3}{(p^2-1)(r^2-1)}\bigg(1+\frac{528pr}{q^{0.125}}\bigg)+\frac{p-1}{pr}\cdot\frac{0.37q^3}{(r-1)p^3}\cdot\frac{r}{r+1}\bigg(1+\frac{264p^{1.25}r}{q^{0.125}}\bigg) \\ &\quad+\frac{r-1}{pr}\cdot\frac{0.37q^3}{(p-1)r^3}\cdot\frac{p}{p+1}\bigg(1+\frac{264r^{1.25}p}{q^{0.125}}\bigg)+\frac{0.37q^3}{p^3r^3}\bigg(1+\frac{132p^{1.25}r^{1.25}}{q^{0.125}}\bigg) \\ &<0.37q^3\bigg(\frac{1}{(p^2-1)(r^2-1)}+\frac{p-1}{(r^2-1)p^4}+\frac{r-1}{(p^2-1)r^4}+\frac{1}{p^3r^3}\bigg) \\ &\quad+\frac{49q^3}{q^{0.125}}\bigg(\frac{4pr}{(p^2-1)(r^2-1)}+\frac{2p^{1.25}r(p-1)}{(r^2-1)p^4}\end{aligned}$$

$$+\frac{2r^{1.25}p(r-1)}{(p^2-1)r^4}+\frac{p^{1.25}r^{1.25}}{p^3r^3}\Bigg)$$
$$<q^3\Bigg(\frac{0.37}{(p^2-p)(r^2-r)}+\frac{199}{q^{0.125}(p-1)(r-1)}\Bigg).$$

Note that, in all 4 cases, the number of desired monics $M \in S'_q$ is less than

$$q^3\Bigg(\frac{0.37}{(p^2-p)(r^2-r)}+\frac{199}{q^{0.125}(p-1)(r-1)}\Bigg)$$

and that, once we divide this by $(q^3-q)/3$ we can obtain the desired upper bound for the proportion of $M \in S'_q$ such that $pr \mid h$. This proportion is necessarily the same when we consider $M \in S_q$ as well. ∎

THEOREM 3.3. *Let $q > e^{100}$ be prime. Let $p < q^{0.03}$ be an odd prime. Define S_q to be the set of all monic quartics $M \in \mathbb{F}_q[T]$ that are divisible by an irreducible cubic in $\mathbb{F}_q[T]$. Let h_M be the ideal class number of $\mathbb{F}_q(T, \sqrt{M(T)})$ and write $P(h = p)$ as shorthand for $\#\{M \in S_q : h_M = p\}/\#S_q$. Then, if $p \nmid q-1$,*

$$\frac{1}{p^2-p}\Bigg(0.56-\frac{0.236p}{q^{0.03}}+\frac{1.12}{p^2(p-1)}\Bigg) < P(h=p) < \frac{1.121}{p(p-1)}$$

and, if $p \mid q-1$,

$$\frac{1}{p^2-p}\Bigg(0.559-\frac{0.263p}{q^{0.03}}-\frac{0.867}{p^2}+\frac{1.12}{p^3(p-1)}\Bigg) < P(h=p) < \frac{1.121}{p(p-1)}.$$

Proof. The trivial inequality $P(h = p) \le P(h \equiv 0 \pmod p)$ together with Theorem 3.1 and the remark that

$$\frac{295}{q^{0.125}p}+\frac{232}{q^{0.125}p^{1.75}} < 0.0005$$

serves to prove the upper bounds. The lower bounds, however, will require some effort. Let us begin with the case $p \nmid q-1$. It is clear that

$$P(h=p) \ge P(h \equiv 0 \pmod p) - P(h \equiv 0 \pmod{p^2}) - \sum_{\text{odd prime } r \ne p} P(pr|h).$$

The first term on the right has a lower bound of $\frac{0.867}{p(p-1)} - \frac{234}{q^{0.125}p}$ given by Theorem 3.1. The final summation can be bounded using Lemma 3.2 as follows:

$$\sum_{\substack{\text{odd prime } r<q \\ r \ne p}} P(pr|h) < \frac{1.12}{p^2-p}\sum_{r<q}\frac{1}{r^2-r}+\frac{597}{q^{0.125}(p-1)}\sum_{r<q}\Bigg(\frac{1}{r}+\frac{1}{r^2-r}\Bigg)$$

where the summation is understood to be over all odd primes $r < q$ with the exception of $r = p$. It is a straightforward matter, by summing a

finite number of terms and then using integrals to bound the remainder, to arrive at

$$\sum_{\text{odd prime } r} \frac{1}{r^2 - r} < 0.2733.$$

In addition we may use a result from a paper of Rosser and Schoenfeld [16], (3.20), to see that

$$\sum_{\text{odd prime } r}^{N} \frac{1}{r} < \log\log N.$$

These inequalities permit the following simplification:

$$\sum_{\substack{\text{odd prime } r<q \\ r\neq p}} P(pr|h) < \frac{0.307}{p^2-p} - \frac{1.12}{p^2(p-1)^2} + \frac{164 + 597\log\log q}{q^{0.125}(p-1)} - \frac{597}{q^{0.125}(p-1)^2}.$$

Next we wish to determine an upper bound for $P(p^2|h)$. Since $p \nmid q-1$ it follows that $\sigma(p^2) = 1$. Making use of this in (2.1) with $v = p^2$ and $w = 1$ gives us

$$\sum_{\substack{A \equiv 0 \,(\mathrm{mod}\, p^2) \\ A \text{ odd}}} N_q(A,B) < \frac{0.74q}{p^2-p}\left(1 + \frac{264p^2}{q^{0.125}}\right).$$

Since $p \nmid q-1$ all of the elliptic curves in the isomorphism classes above have cyclic p-Sylow groups and it follows that for each such curve fewer than $\#E(\mathbb{F}_q)/p^2$ of the points on the curve will be associated with an $M \in S'_q$ with $h_M \equiv 0 \,(\mathrm{mod}\, p^2)$. We conclude that

$$P(p^2|h) < \frac{1.12}{p^4-p^3} + \frac{294}{q^{0.125}(p^2-p)}.$$

Combining our pieces shows that

$$P(h=p) > \frac{0.867}{p^2-p} - \frac{234}{q^{0.125}p} - \frac{1.12}{p^4-p^3} - \frac{294}{q^{0.125}(p^2-p)} - \frac{0.307}{p^2-p} + \frac{1.12}{p^2(p-1)^2} - \frac{164 + 597\log\log q}{q^{0.125}(p-1)} + \frac{597}{q^{0.125}(p-1)^2}, \tag{3.4}$$

which we simplify to get

$$P(h=p) > \frac{1}{p^2-p}\left(0.56 - \frac{p(597\log\log q + 398)}{q^{0.125}} + \frac{1.12}{p^2(p-1)}\right).$$

Since $(597\log\log q + 398)/q^{0.095} < 0.236$ for $q > e^{100}$ we see that we may

replace the above bound with

$$\frac{1}{p^2-p}\left(0.56-\frac{0.236p}{q^{0.03}}+\frac{1.12}{p^2(p-1)}\right)$$

as was required.

We next treat the case $p \mid q-1$. Referring to Theorem 3.1 we see that

$$P(h \equiv 0 \pmod p) > \frac{0.867(p+1)}{p^3}-\frac{234}{q^{0.125}p}-\frac{150}{q^{0.125}p^{1.75}}.$$

All that remains is the determination of $P(p^2|h)$. It is in this calculation where the complication due to a p-rank of 2 rears its ugly head. As before, we subtract off an amount due to the case where the elliptic curve has a p-Sylow group that is cyclic and of order at least p^2. But we also need to discuss the situation where the p-Sylow group has a p-rank of 2.

If $E(\mathbb{F}_q) \cong C_{p^n}$ with $n \geq 2$ or if $E(\mathbb{F}_q) \cong C_p \times C_p$ then fewer than $\#E/p^2$ of the points $\mathcal{P}$ on E will be associated with an $M \in S$ such that $p^2 \mid h_M$. If $E(\mathbb{F}_q) \cong C_{p^m} \times C_p$ with $m \geq 2$ then less than $\#E/p$ of the points $\mathcal{P}$ on E will be associated with an $M \in S$ such that $p^2 \mid h_M$. If $E(\mathbb{F}_q) \cong C_{p^m} \times C_{p^n}$ with $m \geq n \geq 2$ then all of the finite points $\mathcal{P}$ on E will be associated with an $M \in S$ such that $p^2 \mid h_M$. We shall use (2.1) three times, once each with $(v,w) = (p^2,1)$, (p,p) and $(1,p^2)$. Both of the latter two cases are subsets of the preceding cases and we shall correct our results against overcounting. We obtain

$$\begin{aligned} P(p^2|h) &< \frac{1.12}{p^4-p^3}\left(1+\frac{264p^3}{q^{0.125}}\right)+\frac{1.12}{p^5}\left(1+\frac{264p^{1.25}p}{q^{0.125}}\right) \\ &\quad +\frac{1.12(p-1)}{p^7}\left(1+\frac{132p^{2.5}}{q^{0.125}}\right) \\ &< \frac{1}{p^2-p}\left(\frac{1.12(p+1)}{p^3}+\frac{296p}{q^{0.125}}+0.0006\right), \end{aligned}$$

since

$$\frac{296p^{0.25}}{q^{0.125}p}+\frac{148p^{0.5}}{q^{0.125}p^2} < 0.0006.$$

Combining our many pieces for the $p \mid q-1$ case, noting that the bound for $P(pr|h)$ is the same as we used previously, shows that

$$\begin{aligned} P(h=p) &> \frac{1}{p^2-p}\left(\frac{0.867(p^2-1)}{p^2}-\frac{234(p-1)}{q^{0.125}}-\frac{150(p-1)}{q^{0.125}p^{0.75}}\right) \\ &\quad -\frac{1}{p^2-p}\left(0.307-\frac{1.12}{p(p-1)}\right. \end{aligned} \tag{3.5}$$

$$+\frac{(164+597\log\log q)p}{q^{0.125}}-\frac{597p}{q^{0.125}(p-1)}\Bigg)$$
$$-\frac{1}{p^2-p}\Bigg(\frac{1.12(p+1)}{p^3}+\frac{296p}{q^{0.125}}+0.0006\Bigg),$$

which gives us

$$P(h=p)>\frac{1}{p^2-p}\Bigg(0.559-\frac{0.263p}{q^{0.03}}-\frac{0.867}{p^2}+\frac{1.12}{p^3(p-1)}\Bigg)$$

as

$$\frac{597\log\log q+694+150p^{-0.75}}{q^{0.095}}<0.263.$$

This concludes our proof. ∎

COROLLARY 3.6. *Let $q>e^{100}$ be prime. Let S be the set of all monic quartics $M=T^4+aT^2+bT+c\in\mathbb{F}_q[T]$ (for some $a,b,c\in\mathbb{F}_q$) that are divisible by some irreducible cubic in $\mathbb{F}_q[T]$ and that have no cubic term. Let h_M be the ideal class number of $\mathbb{F}_q(T,\sqrt{M(T)})$ and write $P(h=p)$ as shorthand for $\#\{M\in S_q : h_M=p\}/\#S_q$. Then*

$$\begin{aligned}
&9.78\%<P(h=3)<18.7\% && \text{if } 3\nmid q-1,\\
&2.56\%<P(h=5)<5.61\% && \text{if } 5\nmid q-1,\\
&1.14\%<P(h=7)<2.67\% && \text{if } 7\nmid q-1,\\
&0.39\%<P(h=11)<1.02\% && \text{if } 11\nmid q-1,\\
&8.09\%<P(h=3)<18.7\% && \text{if } 3\mid q-1,\\
&2.48\%<P(h=5)<5.61\% && \text{if } 5\mid q-1,\\
&1.07\%<P(h=7)<2.67\% && \text{if } 7\mid q-1,\\
&0.37\%<P(h=11)<1.02\% && \text{if } 11\mid q-1.
\end{aligned}$$

Proof. These statements follow immediately from (3.4) and (3.5). ∎

In the number field situation one expects (see the heuristics of Cohen and Lenstra [4]) that the ideal class number of $\mathbb{Q}(\sqrt{p})$ is 1 for about 75.4% of all primes p. The function field case in which we find ourselves is somewhat different and it is worth mentioning that computational results [7] suggest very strongly that there is no limit for $P(h=1)$ as $q\to\infty$. Rather, what is observed is that the probability depends crucially on the primes dividing $q-1$. What we do expect, however, is that, no matter what the divisibility of $q-1$, if q is sufficiently large ($q>10000$ should suffice) then $74.5\%<P(h=1)<76.5\%$. In the following theorem we prove bounds that are considerably looser.

THEOREM 3.7. *Let $q>e^{100}$ be prime. Define S_q to be the set of all monic quartics $M\in\mathbb{F}_q[T]$ that are divisible by an irreducible cubic in $\mathbb{F}_q[T]$. Let*

h_M be the ideal class number of $\mathbb{F}_q(T, \sqrt{M(T)})$ and write $P(h = 1)$ as shorthand for $\#\{M \in S_q : h_M = 1\}/\#S_q$. Then

$$70\% < P(h = 1) < 84\%.$$

P r o o f. From Theorem 3.1 the number of monic quartics $M \in S_q$ that have the ideal class number of $\mathbb{F}_q(T, \sqrt{M(T)})$ divisible by some p is bounded from above by

$$\sum_{p \text{ odd prime}} q^4 \left(\frac{0.371}{p(p-1)} + \frac{99}{q^{0.125}p} + \frac{78}{q^{0.125}p^{1.75}} \right).$$

We recall from the proof of Theorem 3.3 that

$$\sum_{p \text{ odd prime}} \frac{1}{p^2 - p} < 0.2733 \quad \text{and} \quad \sum_{p \text{ odd prime}}^{N} \frac{1}{p} < \log\log N$$

and easily obtain, as well,

$$\sum_{p \text{ odd prime}} \frac{1}{p^{1.75}} < 0.31.$$

Combining these results, for $q > e^{100}$, gives the number of quartics $M \in S_q$ that have some prime dividing the ideal class number as being bounded from above by $0.1032q^4$. But this quantity counts M more than once whenever h_M is divisible by more than one prime. We shall attempt a small correction of this by subtracting out the number of M with h_M divisible by pr. To do this we will require lower bounds for $P(pr|h)$ where p and r are distinct odd primes. From (2.2) we have, when $pr < q^{0.07}$,

$$\sum_{\substack{AB \equiv 0 \,(\mathrm{mod}\, pr) \\ AB \text{ odd}}} N_q(A, B) > \frac{0.58qpr}{(p^2-1)(r^2-1)} \left(1 - \frac{528pr}{q^{0.125}} \right).$$

Since every elliptic group in the isomorphism classes above has at least $\#E(\mathbb{F}_q)/(pr) - 1$ values of associated $M \in S_q'$ with $h_M \equiv 0 \,(\mathrm{mod}\, pr)$ we can obtain the following lower bound:

$$\frac{0.289q^3}{(p^2-1)(r^2-1)} - \frac{154prq^3}{q^{0.125}(p^2-1)(r^2-1)}$$

for the number of $M \in S_q'$ with $h_M \equiv 0 \,(\mathrm{mod}\, pr)$. A short computation, summing over all products $pr < 500$ of distinct odd primes p and r, gives us a lower bound of $0.0037q^4$ for the number of $M \in S_q$ whose class numbers are divisible by at least 2 distinct primes. Subtracting this from our earlier result shows that there are at most $0.0995q^4$ values of $M \in S_q$ whose ideal class number is divisible by some prime. Since $\#S_q = (q^4 - q^2)/3$ it follows that at least 70% of the $M \in S_q$ must satisfy $h_M = 1$.

To obtain the upper bound we use Theorem 3.1 and Corollary 3.6 to see that

$$P(h=1) < 1 - P(h \equiv 0 \pmod 3) - P(h=5) - P(h=7),$$
$$P(h=1) < 1 - 0.128 - 0.0248 - 0.0107 < 0.84,$$

as required. ∎

Previously mentioned conjectures [7] lead to the prediction that we should expect

$$\lim_{\substack{q\to\infty \\ q\equiv 1 \pmod p}} P(p\text{-rank} = 2) = \frac{1}{p^3(p^2-1)}.$$

Our final theorem proves bounds which create an interval approximately centered on the expected result.

THEOREM 3.8. *Let $q > e^{100}$ be prime. Let $p < q^{0.03}$ be an odd prime. Define S_q to be the set of all monic quartics $M \in \mathbb{F}_q[T]$ that are divisible by an irreducible cubic in $\mathbb{F}_q[T]$. Let $r_p(M)$ be the p-rank of the ideal class group of $\mathbb{F}_q(T, \sqrt{M(T)})$ and write $P(r_p = 2)$ as shorthand for $\#\{M \in S_q : r_p(M) = 2\}/\#S_q$. Then $P(r_p = 2) = 0$ if $p \nmid q-1$ and if $p \mid q-1$ we have*

$$0.85/p^5 < P(r_p = 2) < 1.14/p^5.$$

Proof. If $p \nmid q-1$ then we will refer to the remark following (2.2) together with Theorem 2.3 to conclude that a p-rank of 2 is impossible here. Substituting $w = p$ and $v = 1$ into (2.1) and (2.2) gives us the following bounds:

$$\sum_{\substack{B\equiv 0 \pmod p \\ AB\equiv 0 \pmod{p^2} \\ AB \text{ odd}}} N_q(A,B) < \frac{0.74q}{p^3} + \frac{98p^{1.25}}{q^{0.125}p^3} < \frac{0.74q}{p^3} + \frac{98}{q^{0.0875}p^3} < \frac{0.756q}{p^3}$$

and

$$\sum_{\substack{B\equiv 0 \pmod p \\ AB\equiv 0 \pmod{p^2} \\ AB \text{ odd}}} N_q(A,B) > \frac{0.58q}{p^3} - \frac{77p^{1.25}}{q^{0.125}p^3} > \frac{0.567q}{p^3}.$$

To translate the above bounds into the quartic case we will use Theorem 2.3 and we must determine, for an arbitrary abelian group G of p-rank 2, how many elements $g \in G$ are such that the $G/\langle g\rangle$ is non-cyclic. If we write $G = \{a^i b^j : i, j \in \mathbb{Z}\}$ where a and b are independent and generate G, then it is easy to see that $G/\langle g\rangle$ is non-cyclic precisely when $g = a^{px}b^{py}$ for some integers x and y. It then follows immediately from Theorem 2.3 and previous

comments that

$$\#\{M \in S_q : r_p(M) = 2\} < q\frac{0.756q}{p^3} \cdot \frac{q-1}{2}\left(\frac{q+2\sqrt{q}+1}{p^2} - 1\right) < \frac{0.378q^4}{p^5},$$

$$\begin{aligned}\#\{M \in S_q : r_p(M) = 2\} &> q\left(\frac{0.557q}{p^3} - 3\right)\frac{q-1}{2}\left(\frac{q-2\sqrt{q}+1}{p^2} - 1\right)\\ &> \frac{0.2834q^4}{p^5}\end{aligned}$$

from which we also obtain

$$0.85q/p^5 < P(r_p = 2) < 1.14q/p^5.$$

It is worth noting that when p is very small in comparison to q the above results can be sharpened slightly. For example, when $p = 3$ and $q > e^{100}$ with $3 \mid q-1$ then we can show that the probability that the 3-rank is 2 (for the ideal class group of $\mathbb{F}_q(T, \sqrt{M(T)})$ with $M \in S_q$) is between $0.86/3^5$ and $1.12/3^5$. ∎

References

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

[2] D. A. Buell, *Class groups of quadratic fields II*, Math. Comp. 48 (1987), 85–93.

[3] —, *The expectation of success using a Monte Carlo factoring method—some statistics on quadratic class numbers*, ibid. 43 (1984), 313–327.

[4] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, in: Number Theory (Noordwijkerhout, 1983), H. Jager (ed.), Lecture Notes in Math. 1068, Springer, Berlin, 1984, 33–62.

[5] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*, Academic Press, New York, 1966.

[6] 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.

[7] C. Friesen, *Class group frequencies of real quadratic function fields*: *The degree 4 case*, Math. Comp. 69 (2000), 1213–1228.

[8] —, *Bounds for the number of certain elliptic curves over finite fields*, preprint, 1999.

[9] —, *A special case of Cohen–Lenstra heuristics in function fields*, in: Fifth Conference of the Canadian Number Theory Association, K. S. Williams and R. Gupta (eds.), CRM Proc. Lecture Notes 19, Amer. Math. Soc., Providence, RI, 1999, 99–105.

[10] C. Friesen and P. van Wamelen, *Class numbers of real quadratic function fields*, Acta Arith. 81 (1997), 45–55.

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

[12] D. R. Hayes, *Real quadratic function fields*, in: Canad. Math. Soc. Proc. 7, 1985, 203–236.

[13] H. Ichimura, *Class numbers of real quadratic function fields of genus one*, Finite Fields Appl. 3 (1997), 181–185.
[14] S. Kuroda, *Table of class number $h(p) > 1$ for quadratic fields $Q(\sqrt{p})$, $p \leq 2776817$*, Math. Comp. 29 (1975), 335–336.
[15] M. Madan, *Note on a problem of S. Chowla*, J. Number Theory 2 (1970), 279–281.
[16] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.
[17] M. Saito and H. Wada, *Tables of ideal class groups of real quadratic fields*, Proc. Japan Acad. Ser. A Math. Sci. 64 (1988), 347–349.
[18] R. Scheidler, A. Stein and H. C. Williams, *Key-exchange in real quadratic congruence function fields*, Des. Codes Cryptogr. 7 (1996), 153–174.
[19] T. A. Schmidt, *Infinitely many real quadratic fields of class number one*, J. Number Theory 54 (1995), 203–205.
[20] M. Tennenhouse and H. C. Williams, *A note on class-number one in certain real quadratic and pure cubic fields*, Math. Comp. 46 (1986), 333–336.
[21] J.-K. Yu, *Toward a proof of the Cohen–Lenstra conjecture in the function field case*, preprint, 1996.

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

Received on 19.8.1999
and in revised form 4.5.2000 (3673)