MATHEMATICS OF COMPUTATION
Volume 69, Number 231, Pages 1213–1228
S 0025-5718(99)01154-0
Article electronically published on May 24, 1999

CLASS GROUP FREQUENCIES OF REAL QUADRATIC FUNCTION FIELDS: THE DEGREE 4 CASE

CHRISTIAN FRIESEN

ABSTRACT. The distribution of ideal class groups of $\mathbb{F}_q(T, \sqrt{M(T)})$ is examined for degree-four monic polynomials $M \in \mathbb{F}_q[T]$ when $\mathbb{F}_q$ is a finite field of characteristic greater than 3 with $q \in [20000, 100000]$ or $q \in [1020000, 1100000]$ and M is irreducible or has an irreducible cubic factor. Particular attention is paid to the distribution of the p-Sylow part of the class group, and these results agree with those predicted using the Cohen-Lenstra heuristics to within about 1 part in 10000. An alternative set of conjectures specific to the cases under investigation is in even sharper agreement.

1. INTRODUCTION

There is no dearth of data when it comes to ideal class numbers or ideal class groups of quadratic number fields; we may turn to papers of Buell, Kuroda, Saito and Wada or Tennenhouse and Williams [3], [4], [11], [12], [16]. If, however, we ask for ideal class numbers of quadratic function fields then we come away almost empty-handed, save for the rather small tables of Artin or Feng and Sun [2], [10]. There is, or so it would appear, a good reason for this. Namely, for any degree d and for any finite field $\mathbb{F}_q$ of q elements there are q^d monic polynomials $M(T)$ giving rise to (ostensibly different) quadratic fields $\mathbb{F}_q(T, \sqrt{M(T)})$. Determining the class group for each such quadratic field rapidly exhausts any available time resources for all but the smallest values of q and d.

In the case where M is a monic irreducible of degree 4 (which is one of the cases of interest for this paper) we can reduce the number of class group calculations needed above down from q^4 to about $q/2$. Even then, with q near 10000, the calculations become quite time-consuming. We can do better, though, and dispense with the calculation of the class group almost entirely by making use of results of Schoof [14], who built on previous work of Waterhouse [17] and Deuring [7]. Schoof provides formulae for counting the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$. Some results of Friesen [9], based on theorems of Stein [15] and Adams and Razar [1], relate class groups of some of these elliptic curves with the ideal class groups of certain $\mathbb{F}_q(T, \sqrt{M(T)})$ with M of degree 4. Using this connection, we are able to determine the distribution of these ideal class groups.

Received by the editor September 8, 1998.

1991 *Mathematics Subject Classification.* Primary 11R29, 11R58, 11R11.

Key words and phrases. Class groups, Cohen-Lenstra conjecture, function fields, class numbers.

Part of the interest in how these ideal class groups are distributed comes from testing the function field analogues of the Cohen-Lenstra conjectures [5] proposed by Friedman and Washington [8] and later modified slightly by Jiu-Kang Yu [18]. The original Cohen-Lenstra conjectures, for number fields, have plenty of empirical support. Such evidence is largely lacking in the function field setting, with Feng and Sun [10] providing some data for $q \leq 11$. In Yu's paper [18] he proves, subject to some conditions, that for a fixed degree the fraction of ideal class groups with a given p-Sylow group tends towards a limit as q increases. In section 4 of this paper we shall examine the distribution of the p-Sylow part of the ideal class groups in the degree 4 case.

Motivation for looking at the *sizes* of class groups comes from the field of cryptography. In a recent paper Scheidler, Stein and Williams [13] discuss a key-exchange cryptosystem based on the continued fraction expansion of an irrational quadratic in a real quadratic function field $\mathbb{F}_q(T, \sqrt{M(T)})$. They singled out the case where M is of degree 4 as the one that performed best (in terms of empirically-measured speed and hypothesized security). The security of this cryptosystem relies in part on the likelihood of the ideal class group of $\mathbb{F}_q(T, \sqrt{M(T)})$ being small. With this in mind we also examine, in section 5, some data regarding the distribution of small ideal class groups.

In this paper we shall concern ourselves with degree-four polynomials $M \in \mathbb{F}_q[T]$ that are irreducible or factor as a linear times an irreducible cubic. These are precisely the cases where the ideal class number is odd. We shall examine the distribution of small ideal class groups of $\mathbb{F}_q(T, \sqrt{M(T)})$ (and the p-Sylow parts of these groups) for q in the intervals $[20000, 100000]$ and $[1020000, 1100000]$. When we average our results in an appropriate manner we will find close agreement with the predictions obtained by applying the Cohen-Lenstra heuristics. An alternative set of predictions will also be considered.

2. Preliminaries

We let $\mathbb{F}_q$ be the finite field of characteristic greater than 3 and having q elements, and use $\mathbb{F}_q{}^*$ to denote the multiplicative group. Take M to be a degree 4 squarefree monic (leading coefficient $= 1$) in $\mathbb{F}_q[T]$, where T is an indeterminate. Adjoining $\sqrt{M(T)}$ to $\mathbb{F}_q(T)$ provides us with a quadratic extension whose ring of integers is $\mathcal{O}_M = \mathbb{F}_q[T, \sqrt{M(T)}]$. Two ideals $\mathcal{A}$ and $\mathcal{B}$ of $\mathcal{O}_M$ are equivalent 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 will denote by $Cl(\mathcal{O}_M)$, and whose order, h_M, is called the *ideal class number*. For the sake of convenience we shall define $I_q(n)$ as the set of monic irreducible polynomials of degree n in $\mathbb{F}_q[T]$. For the purposes of this paper we shall restrict our attention to the two sets of quartics described by $I_q(4)$ and $I_q(1)I_q(3)$.

If we fix a monic squarefree quartic M and choose any $a \in \mathbb{F}_q$, then we can create another monic squarefree quartic $N(T) = M(T + a)$, where $Cl(\mathcal{O}_M)$ is trivially isomorphic to $Cl(\mathcal{O}_N)$. Since the characteristic of $\mathbb{F}_q$ is odd, we may choose $a \in \mathbb{F}_q$ such that the polynomial $N(T)$ has no cubic term and, instead of considering all quartics, we can restrict our attention to those with no cubic term in our examination of the distribution of class groups.

From an earlier paper [9, Theorem 2.4] we quote the following theorem.

Theorem 2.1. *Let $\mathbb{F}_q$ be the finite field with q elements and characteristic $\neq 2, 3$. Then there is a 1-1 correspondence between irreducible monic quartics $M \in \mathbb{F}_q[t]$ with no cubic term and pairs $E, \mathcal{P}$ of non-singular elliptic curves $E : w^2 = v^3 + Av + B$ with a 2-rank of one and with $\mathcal{P}$ a point on E such that $\#E(\mathbb{F}_q)/\operatorname{ord}(\mathcal{P})$ is odd. Under this correspondence the ideal class group $Cl(\mathcal{O}_M)$ is isomorphic to the coset $E(\mathbb{F}_q)/\langle\mathcal{P}\rangle$.*

In particular, this reduces the problem from that of determining the distribution of the class groups associated to monic irreducible quartics to that of determining the distribution of certain elliptic curves with a 2-rank of one.

For each legitimate isogeny class (keeping in mind that we require a 2-rank of one) we need to determine the number of elliptic curves of the form $E : w^2 = v^3 + Av + B$. We will modify results of Schoof [14] to count the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves with the elliptic group isomorphic to a fixed one. From this we easily determine the number of elliptic curves of the form $E : w^2 = v^3 + Av + B$ with a 2-rank of one by calculating the number of such curves in any isomorphism class. To finish our computations we find all odd subgroups $E(\mathbb{F}_q)/\langle\mathcal{P}\rangle$ as $\mathcal{P}$ varies among points on E such that $\#E(\mathbb{F}_q)/\operatorname{ord}(\mathcal{P})$ is odd.

We define C_m to be the cyclic group of order m and modify the results of Schoof to obtain the following theorem.

Theorem 2.2. *Let $p > 3$ be the characteristic of the finite field $\mathbb{F}_q$, where $q = p^d$. Let $b|a$ be positive integers and define $N_q(a, b)$ as be the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with $E(\mathbb{F}_q) \cong C_a \times C_b$. Let $t = q + 1 - ab$, and let $\mu()$ and $H()$ denote the Möbius function and Kronecker class number, respectively. Then*

$$N_q(a,b) = \begin{cases} \displaystyle\sum_{\substack{b|n \\ n|q-1 \\ n^2|ab}} \mu\left(\frac{n}{b}\right) H\left(\frac{t^2-4q}{n^2}\right) & \text{if } t^2 < 4q;\ p \nmid t, \\ H(-4p) & \text{if } t = 0;\ d \text{ odd};\ b = 1;\ q \equiv 1 \pmod 4, \\ H(-4p) - H(-p) & \text{if } t = 0;\ d \text{ odd};\ b = 1;\ q \equiv 3 \pmod 4, \\ H(-p) & \text{if } t = 0;\ d \text{ odd};\ b = 2;\ q \equiv 3 \pmod 4, \\ \frac{p}{12} + \frac{1}{2} - \frac{1}{3}\left(\frac{-3}{p}\right) - \frac{1}{4}\left(\frac{-4}{p}\right) & \text{if } t^2 = 4q;\ a = b, \\ 2 & \text{if } t^2 = q;\ b = 1;\ p \equiv 2 \pmod 3, \\ 2 & \text{if } t = 0;\ d \text{ even};\ b = 1;\ p \equiv 3 \pmod 4, \\ 0 & \text{in all other cases.} \end{cases}$$

Proof. The proof follows from Theorems (4.6), (4.8) and (4.9) in Schoof's paper [14]. There are only two points which may benefit from further explanation. First, even though Schoof does not deal with the situation where n is even in Theorem (4.9), that case follows from his other theorems as well. The second issue to address is that of the sum involving the Möbius function above. In [14, Theorem (4.9)] we see that $H\left((t^2 - 4q)/n^2\right)$ counts the number of isomorphism classes of elliptic curves E with $E(\mathbb{F}_q)[n] \cong C_n \times C_n$ when $n|q-1$ and $n^2|q+1-t$. To obtain all elliptic curves with $E(\mathbb{F}_q) \cong C_a \times C_b$ we count the number of curves with $E(\mathbb{F}_q)[b] \cong C_b \times C_b$ and subtract an amount for all curves satisfying $E(\mathbb{F}_q)[n] \cong C_n \times C_n$ for all non-trivial positive integer multiples n of b. We must, of course, be wary of counting some curves more than once, and the necessary inclusion-exclusion results in our use of the Möbius function above. □

Our next step is to determine the number of elliptic curves of the form $E : w^2 = v^3 + Av + B$ in each of our isomorphism classes. We begin by noting that, since the characteristic of $\mathbb{F}_q$ is neither 2 nor 3, every isomorphism class contains a curve of the form $E : w^2 = v^3 + Av + B$. All other such curves in that isomorphism class are related to this curve via

$$w' = a^3 w, \qquad v' = a^2 v, \qquad A' = a^4 A, \qquad B' = a^6 B$$

for some $a \in \mathbb{F}_q{}^*$. If A and B are both non-zero then we obtain exactly $(q-1)/2$ distinct pairs (A', B') as $a \in \mathbb{F}_q{}^*$ varies, and hence the isomorphism class contains exactly $(q-1)/2$ curves in this instance. Since we require non-singular elliptic curves, it is not possible for both A and B to be 0. If $A = 0$, then for our curve to have a 2-rank of one it must follow that $v^3 + B$ has exactly one linear factor. This is the case if and only if $q \equiv 2 \pmod 3$, which in turn implies that $a^6 B$ gives us $(q-1)/2$ distinct values as $a \in \mathbb{F}_q{}^*$ varies. If $B = 0$ then there are either $(q-1)/4$ or $(q-1)/2$ distinct values of $a^4 A$ as $a \in \mathbb{F}_q{}^*$ varies, depending on whether $q \equiv 1$ or $3 \pmod 4$. We conclude that each isomorphism class has $(q-1)/2$ elliptic curves of the desired form, with the exception (occurring when $q \equiv 1 \pmod 4$) of the two isomorphism classes that contain an elliptic curve of the form $E : w^2 = v^3 + Av$.

Now that we have the number of elliptic curves satisfying our conditions, we can apply Theorem 2.1. It will be necessary to determine, for a given group G, the distribution of the subgroups of the form $G/\langle\sigma\rangle$ as σ varies. This is immediately obvious if G is cyclic. We state without proof a lemma that encompasses the case where G is of rank 2.

Lemma 2.3. *Let p be a prime. Fix integers $r \geq s \geq 0$ and let $G \cong C_{p^r} \times C_{p^s}$ with generators α and β of orders p^r and p^s, respectively. Fix integers $u \geq v \geq 0$ and define $R_p(r, s, u, v)$ as the number of $\sigma \in G$ such that $G/\langle\sigma\rangle$ is isomorphic to $C_{p^u} \times C_{p^v}$. Let $k = r + s - u - v$. If $k \leq 0$, then $R_p(r, s, u, v) = 0$ except when $r = u$ and $s = v$, in which case $R_p(r, s, u, v) = 1$. For the following situations where $k \geq 1$ we have*

$$R_p(r,s,u,v) = \begin{cases} \phi(p^k)\phi(p^{s-v}) & \text{if } r > u > s \geq v, \\ \phi(p^k)p^{s-v} & \text{if } r > u = s > v, \\ \phi(p^k)(p^k + p^{k-1}) & \text{if } r = u = s > v, \\ \phi(p^k)p^k & \text{if } r = u > s \geq v, \\ 0 & \text{in all other cases,} \end{cases}$$

where $\phi()$ denotes the Euler totient function.

Proof. The proof is left to the reader. □

Suppose we have finite abelian groups G and H. To determine the number of $\sigma \in G$ such that $G/\langle\sigma\rangle \cong H$ we apply the above lemma for all primes p dividing the order of G and then multiply together all the values of R_p.

From Theorem 2.2 we obtain the number of isomorphism classes of elliptic curves of given form. We have seen that almost all of these classes contain $(q-1)/2$ elliptic curves. Applying Theorem 2.1 together with Lemma 2.3, we obtain a count for $M \in I_q(4)$ giving rise to an ideal class group of specified form.

If, instead of quartic irreducibles, we consider $M \in I_q(1)I_q(3)$ (that is to say, precisely those that will give rise to a Jacobian with an odd number of points), then there are the following differences. The elliptic curves of interest are the irreducible ones (to give us a 2-rank of zero). An argument similar to the one above shows that almost all isomorphism classes here contain $(q-1)/2$ elliptic curves of the form $E : w^2 = v^3 + Av + B$. The 4 exceptions are the classes containing elliptic curves with $A = 0$, and these occur when $q \equiv 1 \pmod 3$. Those exceptional classes contain $(q-1)/6$ elliptic curves of the desired form. We are obliged to use a slightly different version of Theorem 2.1 (to be found in [9, Theorem 2.5]). We may then apply Theorem 2.2 and Lemma 2.3 to count all $M \in I_q(1)I_q(3)$ giving rise to an ideal class group of the specified form.

3. Algorithm

As noted in the previous section, to obtain exact values for the distribution of the ideal class groups we would need to determine the ideal class groups for two exceptional cases whenever $q \equiv 1 \pmod 4$ (if $M \in I_q(4)$) or $q \equiv 1 \pmod 3$ (if $M \in I_q(1)I_q(3)$). Rather than perform these computations, which are increasingly time-consuming as q grows, we will content ourselves with the small degree of inaccuracy that ignoring these exceptions creates. This error, bounded in size by $1/q$ when $M \in I_q(4)$, makes it convenient to focus only on $q > 20000$, ensuring an accuracy to within 5×10^{-5} for the smaller q and an error of less than 10^{-6} for $q \in [1020000, 1100000]$.

The first step in an efficient determination of the distribution of the ideal class groups is the creation of a table of the Kronecker class numbers necessary for the formulae of Theorem 2.2. To find $H(\Delta)$ for some negative discriminant Δ we count integer triplets (a, b, c) satisfying

$$a > 0, \qquad b^2 - 4ac = \Delta, \qquad |b| \le a \le c, \qquad b \ge 0 \text{ whenever } a = |b| \text{ or } a = c.$$

Rather than performing this count for every discriminant Δ, it is more practical to iterate over possible values of b, a and c and increment the item corresponding to $b^2 - 4ac$ in an array (whose elements represent $H(\Delta)$ for a range of Δ). This quick (15 minute) computation was performed once to determine all $H(\Delta)$ for $\Delta \in [-4400000, 0]$, and the resulting 4MB of data was then loaded into memory as needed, sufficing for all calculations with $q < 1100000$. We note that if we are examining the frequency of occurrence of an ideal class group (or p-Sylow subgroup) of rank 2, say $C_a \times C_b$ with $a|b$, then from Theorem 2.2 we see that the largest discriminant we use is bounded by $-4q/b^2$ This means that we may extend our range for q up to $1100000b^2$, and we shall do so later on to obtain greater accuracy for rank 2 observations.

The next step is, for every q and every group (or p-Sylow subgroup, as desired), to cycle through all possible integral values of $t \in [-2\sqrt{q}, 2\sqrt{q}]$ that could result in an ideal class group (or p-Sylow subgroup, respectively) of the desired form. For $M \in I_q(4)$ this means t is even; for $M \in I_q(1)I_q(3)$ this means t is odd. In either case $q + 1 - t$ needs to be divisible by the order of the desired group (or p-Sylow subgroup). Write $q + 1 - t$ as $2^m n$ with n odd. Then, for all combinations of positive integers a, b with $b|a$ and $ab = n$ we determine $N_q(2^m a, b)$ from Theorem 2.2. Finally we use Lemma 2.3 to determine the number of $\sigma \in C_a \times C_b$ such that $(C_a \times C_b)/\langle\sigma\rangle$ is of the desired form.

In the $I_q(4)$ case the total count is divided by the number of quartics in $I_q(4)$ and then, if $q \equiv 1 \pmod 4$, is multiplied by an additional factor of $q/(q+1)$ to correct for our overcount of the exceptional cases. In the $I_q(1)I_q(3)$ case the total is divided by the number of quartics in $I_q(1)I_q(3)$ and then, if $q \equiv 1 \pmod 3$, is multiplied by an additional factor of $(q+1)/(q+5)$.

4. Distribution of p-Sylow subgroups of ideal class groups

It may be naïve to expect that the p-Sylow subgroups of ideal class groups, for the very limited case where we are dealing with irreducible quartics (or those quartics with exactly one linear factor), should have a distribution governed by the Cohen-Lenstra heuristics. At first glance, in fact, we note that we must treat separately the case where $p|q-1$ in order to obtain any kind of limit at all (see Figure 4.1 for a graph of the frequency of C_3 as a 3-Sylow subgroup), and even then neither limit agrees with the heuristic prediction. However, on *averaging* the cases where $p|q-1$ and $p \nmid q-1$ (weighted appropriately, of course) we see an agreement with the heuristics to a very high degree of precision (Table 4.2). With few exceptions, to be discussed later, the differences between the observed and predicted averages (for $q \sim 10^6$) are on the order of 10^{-6}. The need to average results to obtain heuristically predicted values is not new to this situation – Cohen and Martinet [6] noted that for pure cubic number fields one obtains the predicted value (to within a few parts per thousand) for the probability that the class number is 1 only if one appropriately averages the rather different 'limits' arrived at for $q \equiv -1 \pmod 9$ with those for $q \equiv 2, 5 \pmod 9$.

It should be noted that the p-rank of our class groups is at most 2 (Theorem 2.2), and this requires that we modify the numbers of the Cohen-Lenstra heuristics

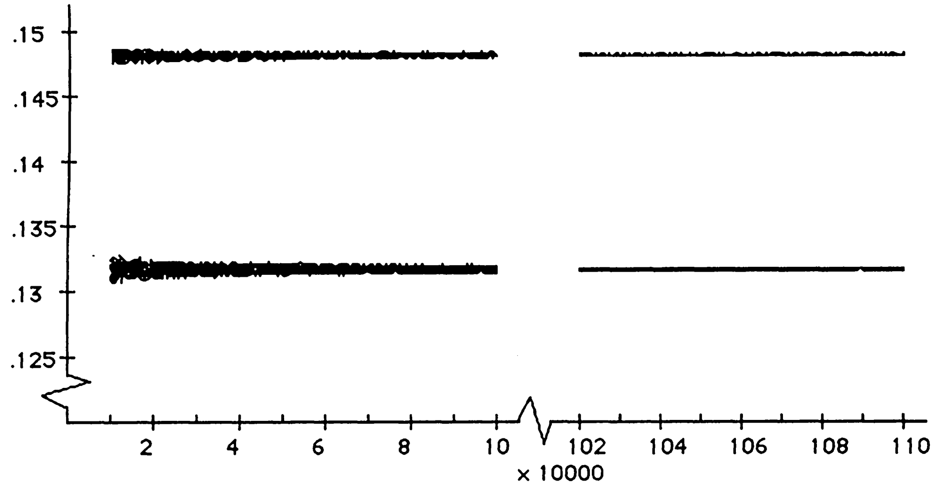

Figure 4.1. A point $(q, f(q))$ represents a value of q in $[10000, 100000]$ or $[1020000, 1100000]$ together with the observed proportion, $f(q)$, of $M \in I_q(4)$ whose 3-Sylow subgroup of $Cl(\mathcal{O}_M)$ is isomorphic to C_3. The upper and lower 'lines' correspond to $q \not\equiv 1 \pmod 3$ and $q \equiv 1 \pmod 3$, respectively.

TABLE 4.2. Columns 2 through 5 represent the average over all $q \in [20000, 100000]$ (unless starred*, in which case $q \in [1020000, 1100000]$) of the observed proportion of $M \in I_q(4)$ and $M \in I_q(1)I_q(3)$ whose p-Sylow subgroup of $Cl(\mathcal{O}_M)$ is isomorphic to G_p. $CL(G_p)$ refers to the prediction via Cohen-Lenstra heuristics, and $P(G_p)$ is the prediction using CONJ 1 and CONJ 2 via the appropriately averaged values of $P(G_p, k)$ as below: $P(G_p = C_{p^m}) := \frac{(p-2)P(G_p,0)+P(G_p,1)}{p-1}$ and $P(G_p = C_{p^m} \times C_p) := \frac{(p-1)P(G_p,1)+P(G_p,2)}{p(p-1)}$

G_p	$I_q(4)$	$I_q(1)I_q(3)$	$I_q(4)^*$	$I_q(1)I_q(3)^*$	$CL(G_p)$	$P(G_p)$
C_3	.139916	.139920	.139918	.139918	.140032	.139918
$C_3 \times C_3$	.001981	.001982	.001981	.001982	.001945	.001981
C_5	.047520	.047516	.047520	.047520	.047521	.047520
$C_5 \times C_5$	.000079	.000079	.000079	.000079	.000079	.000079
C_7	.023243	.023243	.023244	.023245	.023244	.023244
$C_7 \times C_7$	.000010	.000010	.000010	.000010	.000010	.000010
C_9	.015546	.015545	.015546	.015547	.015559	.015546
$C_9 \times C_3$	.000294	.000294	.000294	.000294	.000288	.000294
C_{11}	.009008	.009007	.009008	.009008	.009008	.009008
C_{13}	.006369	.006368	.006369	.006369	.006369	.006369
C_{17}	.003663	.003662	.003663	.003663	.003663	.003663
C_{19}	.002915	.002915	.002915	.002915	.002915	.002915
C_{23}	.001972	.001972	.001972	.001972	.001972	.001972
C_{25}	.001901	.001900	.001901	.001901	.001901	.001901
C_{27}	.001727	.001727	.001727	.001727	.001729	.001727
C_{29}	.001230	.001229	.001230	.001230	.001230	.001230
C_{31}	.001074	.001073	.001074	.001074	.001074	.001074
C_{37}	.000750	.000750	.000750	.000750	.000750	.000750
C_{41}	.000609	.000609	.000609	.000609	.000609	.000609
C_{43}	.000553	.000553	.000553	.000553	.000553	.000553
C_{47}	.000462	.000462	.000462	.000462	.000462	.000462
C_{49}	.000475	.000474	.000475	.000474	.000474	.000474

even as we accept a key premise, namely that a p-Sylow subgroup G (in the real quadratic case) occurs with a frequency inversely proportional to $\#G\#\operatorname{Aut}(G)$.

Let us define

$$W_p = \sum_{G_p} \frac{1}{\#G_p\#\operatorname{Aut}(G_p)},$$

where the sum is over all finite p-Sylow groups G_p (including the trivial one) that have p-rank at most 2. A straightforward calculation determines that

$$W_p = \frac{p^8 - p^7 - p^6 + p^5 + p^4 - p^2 + 1}{(p+1)^2(p-1)^4(p^2+p+1)}.$$

The expected fraction of ideal class groups with a p-Sylow subgroup isomorphic to a given one, G_p, is $\frac{1}{W_p\#G_p\#\operatorname{Aut}(G_p)}$, and these quantities are displayed in the tables as CL (Cohen-Lenstra) predictions. In the function field case these expectations are frequently couched in terms requiring the degree to increase as q stays fixed. We, however, will be fixing the degree (equal to 4) and letting q increase.

When Yu [18] discusses the distribution of p-Sylow subgroups of class groups he requires that $q \not\equiv 1 \pmod{p}$ and under that condition proves a general theorem that guarantees, as a particular case, that there is a limit as $q \to \infty$ of the frequency of occurence of any fixed p-Sylow subgroup arising from the ideal class groups of quartics in $\mathbb{F}_q[T]$. In our computations we must restrict ourselves to the limited set of those squarefree quartics that have odd class numbers, but we should not, in light of Yu's theorem, find it too surprising that even with our restriction we still observe a limit on the frequencies of the p-Sylow subgroups in this case. We observe limits for cyclic p-Sylow subgroups, albeit different ones for $p|q-1$ and $p \nmid q-1$. When $G_p = C_{p^m} \times C_{p^n}$ with $m \geq n \geq 1$, we can see a further refinement in the averages depending on whether $p^n || q-1$ or $p^{n+1}|q-1$. All of these empirically observed 'limits' seem quite sharp (see Figure 4.1 and Tables 4.2 and 4.3).

We determine the average for cyclic p-Sylow subgroups *not* by averaging over all q but rather via the formula $\dfrac{D_1 + (p-2)D_0}{p-1}$, where D_1 and D_0 are the frequencies observed when $p|q-1$ and $p \nmid q-1$, respectively. This minimizes difficulties that can arise from a choice of interval in which the ratio of q with $p|q-1$ to those with $p \nmid q-1$ is different from the theoretical $1 : p-2$. A similar calculation is invoked for the rank 2 p-Sylow subgroups.

The empirically observed values are in close agreement (when averaged over all values of q and not just those satisfying $q \not\equiv 1 \pmod{p}$) to the values predicted by using the Cohen-Lenstra heuristics. The one feature of the data that suggests that this may not be, in fact, exactly correct is that the computational results are consistently lower than predicted when 3 divides the order of the group. As an example we can look at the frequency of occurrence of the 3-Sylow subgroup C_3, which averages to $1.39918 \cdot 10^{-1}$ for large q versus the expected value of $1.40032 \cdot 10^{-1}$ (see Table 4.2). This is, admittedly, a small difference. Further computations might bring the results closer to expectations (although the sharpness of the limits and the decreasing relative standard deviations shown in Table 4.5 undermine that possibility). It should be noted, however, that the CL (Cohen-Lenstra) predictions are most out of line with the computations precisely when $3|\#G$, and this suggests that there may be another factor at work here that diminishes quickly as p increases. With this in mind, and with only the empirical evidence to justify the formulae appearing below, let us consider the following model.

Since we observe no significant distinction between the probabilities for the cases $I_q(4)$ and $I_q(1)I_q(3)$, we will state our assumptions for the irreducibles, $I_q(4)$, but expect no difference if we were to include the other set of quartics as well. We beg the reader's indulgence in our use of $C_m \times C_1$ to denote the group C_m – it simplifies the presentation of the following conjectures and is used in several ensuing formulae.

Conjectured model. *For any odd prime p, any finite abelian p-Sylow group G_p with rank at most 2, and any integer $k \geq 0$ we define*

$$P(G_p, k) = \lim_{\substack{q \to \infty \\ p^k || q-1}} \frac{\#\{M \in I_q(4) : Cl(\mathbb{F}_q(T, \sqrt{M(T)})) \otimes \mathbb{Z}_p \cong G_p\}}{\#I_q(4)}.$$

TABLE 4.3. Columns 2,3,5 and 6 represent the observed average, over all $q \in [1020000, 1100000]$ separated according to whether $p|q-1$ or not, of the proportion of $M \in I_q(4)$ (or $M \in I_q(1)I_q(3)$ if starred*) whose p-Sylow subgroup of $Cl(\mathcal{O}_M)$ is isomorphic to G_p. Columns 4 and 7 represent predictions as per CONJ 1.

G_p	$p\nmid q-1$	$p\nmid q-1^*$	$P(G_p,0)$	$p\mid q-1$	$p\mid q-1^*$	$P(G_p,1)$
C_3	.148148	.148148	.148148	.131688	.131687	.131687
C_5	.048000	.048000	.048000	.046080	.046080	.046080
C_7	.023323	.023324	.023324	.022848	.022848	.022848
C_9	.016461	.016461	.016461	.014632	.014632	.014632
C_{11}	.009016	.009015	.009016	.008941	.008941	.008941
C_{13}	.006372	.006372	.006372	.006336	.006334	.006335
C_{17}	.003664	.003664	.003664	.003652	.003651	.003651
C_{19}	.002916	.002916	.002916	.002909	.002907	.002908
C_{23}	.001973	.001972	.001973	.001968	.001969	.001969
C_{25}	.001920	.001920	.001920	.001843	.001843	.001843
C_{27}	.001829	.001829	.001829	.001626	.001626	.001626
C_{29}	.001230	.001230	.001230	.001230	.001228	.001229
C_{31}	.001074	.001074	.001074	.001073	.001073	.001073
C_{37}	.000750	.000750	.000750	.000750	.000750	.000750
C_{41}	.000609	.000609	.000609	.000608	.000610	.000609
C_{43}	.000554	.000553	.000553	.000553	.000553	.000553
C_{47}	.000462	.000462	.000462	.000462	.000464	.000462
C_{49}	.000476	.000476	.000476	.000466	.000466	.000466

We know, from reading Theorem 2.2, that for any $m \geq n \geq 1$, $P(C_{p^m} \times C_{p^n}, k) = 0$ if $k < n$. The data suggest that the limits above exist and that, for all $m > n \geq 0$ and $k \geq n$, they satisfy the following conjectured formulae:

$$\text{(CONJ 1)} \qquad P(C_{p^m} \times C_{p^n}, k) = \frac{(p+1)(p^2-\delta_{kn})}{p^{2m+3n+3}},$$

$$\text{(CONJ 2)} \qquad P(C_{p^m} \times C_{p^m}, k) = \frac{p^4-p^2-p+\delta_{km}}{p^{5m+2}(p^2-1)},$$

where $\delta_{xy} = 1$ if $x > y$ and 0 otherwise.

Using these two conjectures, one may show that, for fixed k and for q satisfying $p^k || q-1$, the expected probability that p divides the class number is conjecturally

$$\frac{p^2+p-\delta_{k0}}{p^4-p^2}.$$

Except for the unexpected cancellation, when $k > 0$, of various terms depending on k, the straightforward derivation of the above formula is of little interest and will be omitted.

These two conjectures (exhibited under the P columns in Tables 4.2–4.4) correspond quite well with the empirical observations found by averaging the frequencies of all p-Sylow subgroups of order less than 50 for all $M \in I_4(q)$ for all q (q a power of a prime greater than 3) in the ranges $[20000, 100000]$ and $[1020000, 1100000]$. With the larger range for q we observe a difference of at most 10^{-6}, and that only rarely, in Tables 4.2 and 4.3 between the empirical results and the predictions based

TABLE 4.4. Columns 2 and 4 represent the observed average, over all $q \in [8000000, 8000000+100000p^n]$ satisfying $p^n|q-1$, separated according to whether $p^{n+1}|q-1$ or not, of the proportion of $M \in I_q(4)$ whose p-Sylow subgroup of $Cl(\mathcal{O}_M)$ is isomorphic to $C_{p^m} \times C_{p^n}$. Columns 3 and 5 represent predictions as per CONJ 1 and CONJ 2.

$C_{p^m} \times C_{p^n}$	$p^n\|\|q-1$	$P(G_p, n)$	$p^{n+1}\|q-1$	$P(G_p, n+1)$
$C_3 \times C_3$	.0039437	.0039438	.0040009	.0040009
$C_5 \times C_5$	.0003173	.0003173	.0003179	.0003179
$C_7 \times C_7$	.0000593	.0000593	.0000593	.0000594
$C_9 \times C_3$	.0006097	.0006097	.0005419	.0005419
$C_9 \times C_9$	.0000162	.0000162	.0000165	.0000165
$C_{11} \times C_{11}$	.0000062	.0000062	.0000062	.0000062
$C_{13} \times C_{13}$	.0000027	.0000027	.0000027	.0000027
$C_{17} \times C_{17}$	.0000007	.0000007	.0000007	.0000007
$C_{19} \times C_{19}$	.0000004	.0000004	.0000004	.0000004
$C_{25} \times C_5$	.0000154	.0000154	.0000147	.0000148
$C_{27} \times C_3$	.0000677	.0000677	.0000602	.0000602
$C_{27} \times C_9$	.0000025	.0000025	.0000022	.0000022
$C_{49} \times C_7$	.0000014	.0000014	.0000014	.0000014
$C_{81} \times C_3$	.0000075	.0000075	.0000067	.0000067

on CONJ 1 and CONJ 2. In Table 4.4, where we examine the rank 2 p-Sylow subgroups, our values for q are close to 10^7 and we see that the discrepancy between our predictions and the data are only occasionally as large as 10^{-7}. In these tables CONJ 1 and CONJ 2 match the data to within the computational error discussed in Section 3. The great weakness of these conjectured formulae is that, whereas the Cohen-Lenstra predictions are backed by some very sensible heuristics, the above conjectures lack any kind of compelling theoretical reason to accept them. We shall, however, give them a second look when discussing the distribution of the ideal class groups (not just p-Sylow parts) in the next section.

If we look at the expected average of the frequency of occurrence of C_{p^n} according to CONJ 1, we arrive at

$$\frac{(p+1)(p^3-p^2-1)}{p^4}\frac{1}{\#G_p\#\operatorname{Aut}(G_p)},$$

whereas CL would predict

$$\frac{(p+1)^2(p-1)^4(p^2+p+1)}{p^8-p^7-p^6+p^5+p^4-p^2+1}\frac{1}{\#G_p\#\operatorname{Aut}(G_p)}.$$

These two predictions differ by a factor of about $1+p^{-7}$, an amount that, as p grows, quickly becomes insignificant. Only when $p=3$, in fact, is the difference large enough (see Table 4.2) to exceed the computational error remarked on in section 3.

The same holds true for rank 2 p-Sylow subgroups, where, using the conjectures above, we arrive at an average value of

$$\frac{(p^2-1)(p^3-1)}{p^5}\frac{1}{\#G_p\#\operatorname{Aut}(G_p)},$$

TABLE 4.5. Relative standard deviations, as q varies among the cases listed below, for the observed proportions of $M \in I_q(4)$ whose p-Sylow subgroup of $Cl(\mathcal{O}_M)$ is isomorphic to G_p.
(*1) $q \in [20000, 30000]$ with $\mathrm{ord}_p(q-1) = n$
(*2) $q \in [20000, 30000]$ with $\mathrm{ord}_p(q-1) > n$
(*3) $q \in [90000, 100000]$ with $\mathrm{ord}_p(q-1) = n$
(*4) $q \in [90000, 100000]$ with $\mathrm{ord}_p(q-1) > n$
(*5) $q \in [1020000, 1030000]$ with $\mathrm{ord}_p(q-1) = n$
(*6) $q \in [1020000, 1030000]$ with $\mathrm{ord}_p(q-1) > n$.
Note: If $G_p = C_{p^m}$ then we take n to be 0.

$C_{p^m} \times C_{p^n}$	(*1)	(*2)	(*3)	(*4)	(*5)	(*6)
C_3	.001	.002	.0006	.001	.0002	.0004
$C_3 \times C_3$	.009	.01	.004	.005	.001	.002
C_5	.007	.005	.003	.002	.001	.0007
$C_5 \times C_5$	.04	.04	.02	.02	.005	.005
C_7	.008	.01	.004	.006	.001	.002
$C_7 \times C_7$	.07	.06	.04	.04	.01	.01
C_9	.01	.01	.005	.005	.002	.001
$C_9 \times C_3$	.03	.04	.02	.02	.005	.006
C_{11}	.02	.02	.008	.009	.002	.003
C_{13}	.02	.03	.009	.01	.003	.004
C_{17}	.03	.03	.01	.02	.004	.005
C_{19}	.03	.04	.02	.02	.004	.005
C_{23}	.04	.06	.02	.02	.006	.006
C_{25}	.04	.04	.02	.02	.006	.006
C_{27}	.04	.04	.02	.02	.006	.006
C_{29}	.05	.07	.02	.03	.007	.008
C_{31}	.05	.08	.03	.04	.008	.009
C_{37}	.06	.06	.03	.05	.01	.01
C_{41}	.07	.09	.03	.04	.01	.01
C_{43}	.07	.09	.04	.05	.01	.02
C_{47}	.08	.1	.04	.05	.01	.02
C_{49}	.08	.1	.04	.05	.01	.01

which differs from the prediction via CL by a factor of about $1 + p^{-4}$. Here the difference is more pronounced, but since rank 2 groups are significantly less frequent it is, once again, only for $p = 3$ that we are able to see clearly the difference (Table 4.2) between these two predictions.

5. DISTRIBUTION OF IDEAL CLASS GROUPS

Another point of comparision between the Cohen-Lenstra heuristics and our model is in the prediction of the frequency of class groups (and not just their p-Sylow subgroups), in particular the frequency of $h_M = 1$. Both the data and our conjectures bear out the need to average over lots of values of q, as we expect a higher proportion of class number 1 groups occurring when $q - 1$ is divisible by small primes. In Figure 5.1, for example, we initially see an upper and a lower bar, corresponding to $q \equiv 1 \pmod 3$ and $q \not\equiv 1 \pmod 3$, respectively. Each of these

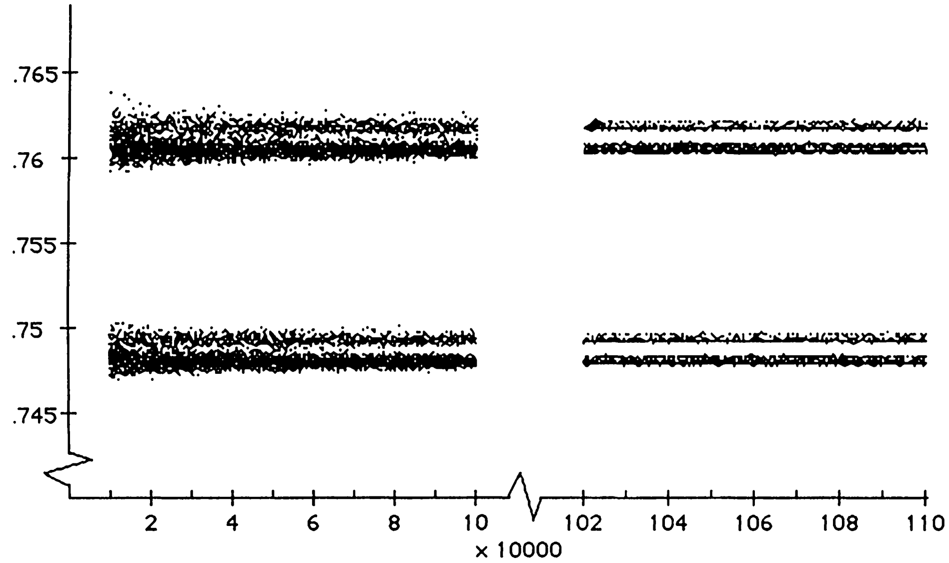

FIGURE 5.1. A point $(q, f(q))$ represents a value of q in $[10000, 100000]$ or $[1020000, 1100000]$ together with the observed proportion, $f(q)$, of $M \in I_q(4)$ with $h_M = 1$. The upper and lower 'halves' correspond to $q \equiv 1 \pmod 3$ and $q \not\equiv 1 \pmod 3$, respectively, with further splitting depending on whether 5 divides $q-1$, whether 7 divides $q-1$, and so forth.

then splits into two bars, corresponding to $q \equiv 1 \pmod 5$ and $q \not\equiv 1 \pmod 5$. With q sufficiently large we would expect to observe differences modulo 7 and 11 and so forth.

When we average the data we once again arrive at a result in close parallel with CL. In particular, if we determine the proportion of trivial class groups via CL we arrive at the product

$$\prod_{\text{odd } p} \frac{1}{W_p} \approx .754462,$$

compared to the empirically observed value of $\approx .754542$. Note that our CL-predicted value of .754462 is slightly higher than the one usually quoted (at about .754458), due to the absence of groups with p-rank greater than 2.

In addition to the two conjectures of the previous section we need one more in order to make predictions regarding ideal class groups (and not just their p-Sylow subgroups). It is the same as the assumption built into the Cohen-Lenstra heuristics regarding the independence of the p-Sylow subgroup occurrences, but more awkward to state in our case because the probabilities depend on the factorization of $q-1$. We define, for any group G and any q a power of a prime greater than 3,

$$P_q(G) = \prod_{\text{odd primes } p} P(G \otimes \mathbb{Z}_p, \operatorname{ord}_p(q-1)),$$

TABLE 5.2. Columns 2 through 5 represent the average over all $q \in [20000, 100000]$ (unless starred*, in which case $q \in [1020000, 1100000]$) of the observed proportion of $M \in I_q(4)$ and $M \in I_q(1)I_q(3)$ with $Cl(\mathcal{O}_M)$ isomorphic to G. When G is itself a p-Sylow group, then the values in columns 2–5 were obtained by taking $((p-2) * D_0 + D_1)/(p-1)$, where D_0 and D_1 are the observed averages over $p \nmid q-1$ and $p \mid q-1$ respectively.

G	$I_q(4)$	$I_q(1)I_q(3)$	$I_q(4)^*$	$I_q(1)I_q(3)^*$	$CL(G)$	$P(G)$
C_1	.754564	.754570	.754541	.754542	.754462	.754540
C_3	.125641	.125648	.125641	.125642	.125744	.125641
$C_3 \times C_3$	.001779	.001780	.001779	.001779	.001746	.001779
C_5	.037728	.037728	.037726	.037726	.037723	.037726
$C_5 \times C_5$	.000063	.000063	.000063	.000063	.000063	.000063
C_7	.017966	.017966	.017965	.017965	.017963	.017965
$C_7 \times C_7$	.000008	.000008	.000008	.000008	.000008	.000008
C_9	.013960	.013960	.013960	.013960	.013972	.013960
$C_9 \times C_3$	.000264	.000264	.000264	.000264	.000259	.000264
C_{11}	.006859	.006860	.006860	.006859	.006859	.006860
C_{13}	.004837	.004837	.004837	.004837	.004836	.004837
C_{15}	.006281	.006281	.006282	.006282	.006287	.006282
$C_{15} \times C_3$	.000089	.000089	.000089	.000089	.000087	.000089
C_{17}	.002774	.002774	.002774	.002774	.002774	.002774
C_{19}	.002207	.002207	.002206	.002206	.002206	.002206
C_{21}	.002991	.002991	.002991	.002991	.002994	.002992
C_{23}	.001491	.001491	.001491	.001491	.001491	.001491
C_{25}	.001509	.001509	.001509	.001509	.001509	.001509
C_{27}	.001551	.001551	.001551	.001551	.001552	.001551
C_{29}	.000930	.000929	.000929	.000929	.000929	.000929
C_{31}	.000812	.000811	.000811	.000811	.000811	.000811
C_{33}	.001142	.001142	.001142	.001142	.001143	.001142
C_{35}	.000898	.000898	.000898	.000898	.000898	.000898
C_{37}	.000567	.000567	.000567	.000566	.000566	.000567
C_{39}	.000805	.000805	.000805	.000805	.000806	.000805
C_{41}	.000460	.000460	.000460	.000460	.000460	.000460
C_{43}	.000418	.000418	.000418	.000418	.000418	.000418
C_{45}	.000698	.000698	.000698	.000698	.000699	.000698
C_{47}	.000349	.000349	.000349	.000349	.000349	.000349
C_{49}	.000367	.000367	.000367	.000367	.000367	.000367

and state our final conjecture:

$$\text{(CONJ 3)} \qquad \lim_{q\to\infty}\left(P_q(G) - \frac{\#\{M \in I_4(q) : Cl(\mathbb{F}_{\hat{q}}(T, \sqrt{M(T)})) \cong G\}}{\#I_4(q)}\right) = 0.$$

We should indicate at the outset that, for individual values of q, the differences observed in the limit above are large enough to raise serious doubts as to the validity of our conjecture(s). On the other hand, if we average over q in a congruence class

TABLE 5.3. Observed frequencies and prediction errors for $\mathcal{C}l(\mathcal{O}_M) = G$ for $M \in I_q(4)$ with $q \in [1020000, 1100000]$ as averaged over the stated congruence classes. $\epsilon_G(p|q-1)$ is the difference between the predicted value (using CONJ 1,2,3) and the observed value of the average over all $q \in [1020000, 1100000]$ satisfying $q \equiv 1 \pmod{p}$ of the proportion of $M \in I_q(4)$ with $\mathcal{C}l(\mathcal{O}_M) = G$. $\epsilon_G(p \nmid q-1)$ is defined similarly.

G	$3\|q-1$	$\epsilon_G(3\|q-1)$	$3\nmid q-1$	$\epsilon_G(3\nmid q-1)$	$5\|q-1$	$\epsilon_G(5\|q-1)$	$5\nmid q-1$	$\epsilon_G(5\nmid q-1)$
C_1	.760775	.000001	.748306	-.000002	.755510	.000023	.754216	-.000006
C_3	.118251	0	.133032	0	.125833	-.000026	.125577	.000009
C_5	.038037	.000001	.037412	.000003	.036582	.000001	.038108	0
C_7	.018112	.000001	.017815	.000002	.017987	.000002	.017956	.000001
C_9	.013139	0	.014781	0	.013981	-.000003	.013953	.000001
C_{11}	.006917	-.000001	.006803	0	.006869	0	.006857	0
C_{13}	.004877	0	.004797	0	.004843	0	.004835	0
C_{15}	.005913	-.000001	.006651	0	.006093	-.000002	.006345	0
C_{17}	.002797	0	.002751	0	.002778	0	.002773	0
C_{19}	.002224	0	.002188	0	.002209	0	.002205	0
C_{21}	.002815	0	.003167	0	.002996	0	.002990	0
C_{23}	.001504	0	.001479	0	.001493	0	.001491	0
C_{25}	.001522	0	.001497	0	.001463	0	.001524	0
C_{27}	.001460	0	.001642	0	.001553	0	.001550	0
C_{29}	.000937	0	.000922	0	.000930	0	.000929	0
C_{31}	.000818	0	.000805	0	.000812	0	.000811	0
C_{33}	.001075	0	.001209	0	.001144	0	.001142	0
C_{35}	.000906	0	.000891	0	.000871	0	.000907	0
C_{37}	.000571	0	.000562	0	.000567	0	.000566	0
C_{39}	.000758	0	.000853	0	.000806	0	.000805	0
C_{41}	.000464	0	.000456	0	.000461	0	.000460	0
C_{43}	.000421	0	.000414	0	.000418	0	.000418	0
C_{45}	.000657	0	.000739	0	.000677	0	.000705	0
C_{47}	.000352	0	.000346	0	.000350	0	.000349	0
C_{49}	.000370	0	.000364	0	.000367	0	.000367	0

we will see the same kind of strong correlation with experimental data (Tables 5.2 and 5.3) that characterized the p-Sylow predictions of the previous section.

For example, if we combine the three conjectures to predict the average proportion of trivial class groups (with no restrictions on q), we come up with

$$\prod_{\text{odd } p} \frac{p^5 - p^4 - 2p^3 + p^2 + p + 1}{p^5 - p^4 - p^3 + p^2} \approx .754540,$$

which agrees almost exactly with the empirical result. In Table 5.2, where we average over all $q \in [1020000, 1100000]$, the greatest difference between the data and the predictions via CONJ 1,2,3 is $2 \cdot 10^{-6}$, whereas the greatest difference between the data and the CL predictions is about 50 times as great. It is not overly difficult to take the three conjectures and arrive at formulae for the expected frequency of various groups as q ranges over some congruence classes with respect to some modulus. As an example we provide, without further comment, the two cases below: Let

$$W = \prod_{\text{odd } p} \frac{p^5 - p^4 - 2p^3 + p^2 + p + 1}{p^5 - p^4 - p^3 + p^2}.$$

Then, if CONJ 1, CONJ 2 and CONJ 3 are true we have, for distinct odd primes p and r,

$$P(h = 1 : q \equiv 1 \pmod{p}) = \frac{p^5 - p^4 - 2p^3 + p^2 + 2p - 1}{p^5 - p^4 - 2p^3 + p^2 + p + 1} W,$$

$$P(h = r : q \not\equiv 1 \pmod{p})$$
$$= \frac{p^5 - p^4 - 2p^3 + p^2 + p}{p^5 - p^4 - 2p^3 + p^2 + p + 1} \cdot \frac{r^6 - 2r^4 - r^3 + r + 1}{r^8 - r^7 - 2r^6 + r^5 + r^4 + r^3} W,$$

where the above probabilities are understood to be averages over all allowable q. Table 5.3, which shows the details when we average over q belonging to various congruence classes, shows the efficacy of our conjectures in predicting these results. The greatest discrepancy here is about $3 \cdot 10^{-5}$, and the difference is typically very much smaller.

It should be remarked that the range of the larger q values was chosen to be $[1020000, 1100000]$ in part because that interval had an equal number of $q \equiv 1 \pmod 3$ and $q \not\equiv 1 \pmod 3$. The averages of ideal class group frequencies are less in need of correction as a result. If we had chosen a range such as, for example, $[950000, 1000000]$ (this was, in fact, the author's first choice) then there would have been about 2.5% more $q \equiv 1 \pmod 3$ than $q \not\equiv 1 \pmod 3$. This would have reduced the average frequency of all class groups divisible by 3 and would have led to an artificially increased value for the average of all class groups not divisible by 3. Although it would be possible to compensate for this effect, it was deemed simpler to remove the problem – at least as far as the most influential prime was concerned – with a more 'balanced' choice of interval.

6. Conclusion

The data, once suitably averaged, are in very close agreement with the values predicted by naïvely applying the Cohen-Lenstra heuristics, and match those heuristic predictions, to the best of the author's knowledge, to a higher degree of precision than any data previously published. In spite of this correlation, the slight differences that arise when 3 divides the class group suggest that the Cohen-Lenstra heuristics will not provide us with the exact values of the limits in the case under study here. An alternative set of conjectures suggested by the data, but without any heuristic underpinnings, comes startlingly close to recreating the experimental observations and allows us to estimate not only the averages (to a higher degree of precision than CL) but also the finer detail (when $p^k || q - 1$) that we witness in the computed results.

References

1. William W. Adams and Michael J. Razar, *Multiples of points on elliptic curves and continued fractions*, Proc. London Math. Soc. **41** (1980), 481–498. MR **82c:**14031
2. Emil Artin, *Quadratische Körper im Gebiet der höheren Kongruenzen I, II*, Math. Zeitschrift **19** (1924), 153–246.
3. Duncan A. Buell, *Class groups of quadratic fields II*, Math. Comp. **48** (1987), 85–93. MR **87m:**11109

4. Duncan A. Buell, *The expectation of success using a Monte Carlo factoring method – some statistics on quadratic class numbers*, Math. Comp. **43** (1984), 313–327. MR **85k:**11068
5. H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number Theory Noordwijkerhout (H. Jager, ed.), Lecture Notes in Math. vol. 1068, Springer-Verlag, Berlin and New York, 1984, pp. 33–62. MR **85j:**11144
6. H. Cohen and J. Martinet, *Class groups of finite fields: Numerical heuristics*, Math. Comp **48** (1987), 123–137. MR **88e:**11112
7. M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272. MR **3:**104f
8. Eduardo Friedman and Lawrence C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227–239. MR **91c:**11138
9. Christian Friesen, *A special case of Cohen-Lenstra heuristics in function fields*, Fifth Conference of the Canadian Number Theory Association (Kenneth S. Williams and Rajiv Gupta, ed.), CRM Proceedings and Lecture Notes, vol. 19, American Mathematical Society, Providence, RI, 1999, pp. 99–105.
10. KeQin Feng and Shu Ling Sun, *On class number of quadratic function fields*, Algebraic structures and number theory (Hong Kong 1988), World Sci. Publishing, Teaneck, NJ, 1990, pp. 88–113. MR **91m:**11098
11. S. Kuroda, *Table of class numbers, $h(p) > 1$, for quadratic fields $Q(\sqrt{p})$, $p \equiv 1 \pmod 4) \leq$* 2776817, Table, Univ. of Maryland, 1965, deposited in the UMT file; reviewed in Math. Comp. **29** (1975), 335-336.
12. Michiyo Saito and Hideo Wada, *Tables of ideal class groups of real quadratic fields*, Proc. Japan Acad. Ser. A Math. Sci. **64** (1988), 347–349. MR **90a:**11122
13. R. Scheidler, A. Stein, H. C. Williams, *Key-Exchange in Real Quadratic Congruence Function Fields*, Des. Codes Cryptogr. **7** (1996), 153–174. MR **97d:**94009
14. René Schoof, *Nonsingular Plane Cubic Curves over Finite Fields*, Journal of Combinatorial Theory, Series A **46** (1987), 183–211. MR **88k:**14013
15. Andreas Stein, *Equivalences between elliptic curves and real quadratic congruence function fields*, J. Théor. Nombres Bordeaux **9** (1997), no. 1, 75–95. MR **98d:**11144
16. 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. MR **87b:**11127
17. E. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup. (4) **2** (1969), 521–560. MR **42:**279
18. Jiu-Kang 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, Ohio 43302
E-mail address: friesen.4@osu.edu