

DENSITIES FOR RANKS OF CERTAIN PARTS OF p -CLASS GROUPS

FRANK GERTH III

ABSTRACT. Let K be a Galois extension of the field of rational numbers of prime degree p , and let C_K be the p -class group of K . In this paper densities for the ranks of certain parts of such C_K are calculated, and these densities suggest a way to extend conjectures of Cohen and Lenstra.

1. Introduction. Let p be a prime number, and let \mathbf{Q} denote the field of rational numbers. Let K be a Galois extension of \mathbf{Q} such that $\text{Gal}(K/\mathbf{Q})$ is a cyclic group of order p . Let C_K denote the p -class group of K ; i.e., the Sylow p -subgroup of the ideal class group of K . (For $p = 2$, we shall be using the Sylow 2-subgroup of the narrow ideal class group of K .) Let σ be a generator of $\text{Gal}(K/\mathbf{Q})$, and let $C_K^{(1-\sigma)^i} = \{a^{(1-\sigma)^i} : a \in C_K\}$ for $i = 0, 1, 2, \dots$. Suppose exactly t primes ramify in K/\mathbf{Q} . It is a classical result that $C_K/C_K^{1-\sigma}$ is an elementary abelian p -group with rank equal to $t - 1$. Furthermore, $C_K^{(1-\sigma)^i}/C_K^{(1-\sigma)^{i+1}}$ is an elementary abelian p -group of each i , and

$$\text{rank } C_K = \text{rank}(C_K/C_K^p) = \sum_{i=1}^{p-1} \text{rank}(C_K^{(1-\sigma)^{i-1}}/C_K^{(1-\sigma)^i}),$$

where $C_K^p = \{a^p : a \in C_K\}$ (cf. [9, Proposition 4.2 and 11, Satz 6]). Since we know that $\text{rank } C_K/C_K^{1-\sigma} = t - 1$, we shall focus our attention on $C_K^{1-\sigma}/C_K^{(1-\sigma)^2}$. If we let $R_K = \text{rank}(C_K^{1-\sigma}/C_K^{(1-\sigma)^2})$, then $0 \leq R_K \leq t - 1$. In this paper we shall consider the following question: how likely is $R_K = 0$, $R_K = 1$, $R_K = 2$, etc., as $t \rightarrow \infty$.

2. Statement of main results. Let notation be the same as in §1. For each positive integer t , each nonnegative integer r , and each positive real number x , we define

$$A_t = \{\text{cyclic extensions } K \text{ of } \mathbf{Q} \text{ of degree } p \text{ with exactly } t \text{ ramified primes}\}$$

(when $p = 2$, we shall consider separately the imaginary and real quadratic fields)

$$A_{t,x} = \{K \in A_t : \text{the conductor of } K \text{ is } \leq x\},$$

$$A_{t,r,x} = \{K \in A_{t,x} : R_K = r\}.$$

Then we define the density $d_{t,r}$ by

$$(1) \quad d_{t,r} = \lim_{x \rightarrow \infty} \frac{|A_{t,r,x}|}{|A_{t,x}|}$$

Received by the editors March 25, 1985 and, in revised form, November 25, 1985.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 11R20, 11R29, 11R45.

©1987 American Mathematical Society
 0002-9939/87 \$1.00 + \$.25 per page

where $|S|$ denotes the cardinality of a set S . We then define the limit density $d_{\infty,r}$ by

$$(2) \quad d_{\infty,r} = \lim_{t \rightarrow \infty} d_{t,r}.$$

Our theorems will show that these limits exist and will provide the values for these limits. For $p = 2$, we have obtained the following result in [6, Theorems 4.3 and 5.11].

THEOREM 1. *For imaginary quadratic fields,*

$$d_{\infty,r} = \frac{2^{-r^2} \prod_{k=1}^{\infty} (1 - 2^{-k})}{\prod_{k=1}^r (1 - 2^{-k})^2} \quad \text{for } r = 0, 1, 2, \dots$$

For real quadratic fields,

$$d_{\infty,r} = \frac{2^{-r(r+1)} \prod_{k=1}^{\infty} (1 - 2^{-k})}{\prod_{k=1}^r (1 - 2^{-k}) \prod_{k=1}^{r+1} (1 - 2^{-k})} \quad \text{for } r = 0, 1, 2, \dots$$

REMARK. When $p = 2$,

$$R_K = \text{rank}(C_K^{1-\sigma}/C_K^{(1-\sigma)^2}) = \text{rank}(C_K^2/C_K^4) = 4\text{-class rank of } C_K.$$

So Theorem 1 gives limit densities for the 4-class ranks of imaginary and real quadratic fields.

Our goal in this paper is to prove the following theorem.

THEOREM 2. *Suppose $p \geq 3$. Then*

$$d_{\infty,r} = \frac{p^{-r(r+1)} \prod_{k=1}^{\infty} (1 - p^{-k})}{\prod_{k=1}^r (1 - p^{-k}) \prod_{k=1}^{r+1} (1 - p^{-k})} \quad \text{for } r = 0, 1, 2, \dots$$

Values for $d_{\infty,r}$ for small p and r appear in the Appendix.

3. Proof of Theorem 2. We let notation be the same as in §§1 and 2, and we assume $p \geq 3$. First we note that the fields K in $A_{t,x}$ have conductor $f_K = p^2 p_1 \cdots p_{t-1}$ or $f_K = p_1 \cdots p_t$, where p_1, \dots, p_t are distinct rational primes with each $p_i \equiv 1 \pmod{p}$. We can ignore the fields K with $f_K = p^2 p_1 \cdots p_{t-1} \leq x$ when calculating $d_{t,r}$ since the number of such fields is

$$O\left(\frac{x(\log \log x)^{t-2}}{\log x}\right), \quad \text{while } |A_{t,x}| \gg \frac{x(\log \log x)^{t-1}}{\log x}$$

(cf. [10, Theorem 437 and 4, p. 201]). For each field K with $f_K = p_1 \cdots p_t$, we introduce a $t \times t$ matrix M_K whose entries m_{ij} are defined in terms of Hilbert symbols by

$$\omega^{m_{ij}} = \left(\frac{p_j \mu_K}{\wp_i} \right) \quad \text{for } 1 \leq i \leq t, 1 \leq j \leq t,$$

where ω is a primitive p th root of unity, \wp_i is a prime of $F = \mathbf{Q}(\omega)$ above p_i , and μ_K is an element of F satisfying $KF = F(\mu_K^{1/p})$. (See [3, p. 197] for more details.) We view M_K as a matrix over \mathbf{F}_p , the finite field with p elements. It is known that $R_K = t - 1 - \text{rank } M_K$ (cf. [9, Proposition 4.6, Proposition 4.7, and IV B 4, p. 45]).

Using this fact, we have in effect determined $d_{t,r}$ in [5]. To be more precise, $d_{t,r}$ in (1) corresponds to $B_{t,e}$ in [5, Equation 2.2]. So

$$(3) \quad d_{t,r} = \left[\prod_{j=1}^{t-1-r} \left(1 - \frac{1}{p^{t+1-j}} \right) \right] \cdot \frac{1}{p^{tr}} \cdot \sum_{\substack{i_1 + \dots + i_{t-1-r} \leq r \\ \text{each } i_s \geq 0}} \left(\prod_{s=1}^{t-1-r} p^{si_s} \right).$$

(When $r = t - 1$, $d_{t,t-1} = p^{-t(t-1)}$.) The main ideas used in proving (3) can be explained as follows. Let J be any $t \times t$ matrix with coefficients in \mathbb{F}_p and with the sum of the entries in each column of J equal to 0. Let

$$N_J(x) = |\{ K : M_K = J \text{ and } f_K \leq x \}|.$$

Then $N_J(x) = h(x) + o(h(x))$, where $h(x)$ is a function that is independent of J . (This corresponds to equidistribution of the Hilbert symbols. See [3, p. 196 and pp. 200–206] for more details.) It follows that

$$\frac{|A_{t,r;x}|}{|A_{t;x}|} = \frac{\sum_J^{(r)} N_J(x)}{\sum_J N_J(x)} = \frac{\sum_J^{(r)} 1 + o(1)}{\sum_J 1 + o(1)}$$

where $\sum_J^{(r)}$ denotes a sum over those J with rank $J = t - 1 - r$. Hence

$$d_{t,r} = \left(\sum_J^{(r)} 1 \right) / \left(\sum_J 1 \right).$$

This rational number is calculated in [5] and is given by (3).

We must show that $\lim_{t \rightarrow \infty} d_{t,r}$ has the value given by Theorem 2. We let $k = t + 1 - j$ and $w = t - 1 - r$. Then

$$\begin{aligned} d_{t,r} &= \left[\prod_{k=r+2}^t \left(1 - \frac{1}{p^k} \right) \right] \cdot \frac{1}{p^{r(r+1)} p^{wr}} \cdot \sum_{\substack{i_1 + \dots + i_w \leq r \\ \text{each } i_s \geq 0}} p^{1i_1 + 2i_2 + \dots + wi_w} \\ &= \left[\frac{\prod_{k=1}^t (1 - p^{-k})}{\prod_{k=1}^{r+1} (1 - p^{-k})} \right] \cdot p^{-r(r+1)} \cdot \left[\frac{1}{p^{wr}} \sum_{\substack{i_1 + \dots + i_w \leq r \\ \text{each } i_s \geq 0}} p^{1i_1 + 2i_2 + \dots + wi_w} \right], \end{aligned}$$

and then

$$(4) \quad d_{\infty,r} = \left[\frac{p^{-r(r+1)} \prod_{k=1}^{\infty} (1 - p^{-k})}{\prod_{k=1}^{r+1} (1 - p^{-k})} \right] \cdot \left[\lim_{w \rightarrow \infty} \frac{1}{p^{wr}} \sum_{\substack{i_1 + \dots + i_w \leq r \\ \text{each } i_s \geq 0}} p^{1i_1 + 2i_2 + \dots + wi_w} \right].$$

If $r = 0$, then $d_{\infty,0}$ in (4) is the same as $d_{\infty,0}$ in the statement of Theorem 2. So we may assume $r \geq 1$. To evaluate the limit in (4), we shall use the following lemma.

LEMMA. *Let w and m be positive integers, and let*

$$F_{w,m} = \frac{1}{p^{wm}} \sum_{\substack{i_1 + \dots + i_w = m \\ \text{each } i_s \geq 0}} p^{1i_1 + 2i_2 + \dots + wi_w}.$$

Then

$$\lim_{w \rightarrow \infty} F_{w,m} = \prod_{k=1}^m (1 - p^{-k})^{-1}.$$

PROOF. First we note that

$$F_{w,m} = \sum_{\substack{i_1 + \cdots + i_w = m \\ \text{each } i_s \geq 0}} p^{(1-w)i_1 + (2-w)i_2 + \cdots + (-1)i_{w-1} + 0i_w}$$

since $1/p^{wm} = p^{-w(i_1 + \cdots + i_w)}$. Also we note that $F_{w,m}$ appears in $F_{w+1,m}$ exactly as those terms having $i_1 = 0$. Then

$$\lim_{w \rightarrow \infty} F_{w,m} = \sum_{l=0}^{\infty} b_{l,m} p^{-l},$$

where $b_{l,m}$ is the number of times that

$$l = (w-1)i_1 + (w-2)i_2 + \cdots + 1i_{w-1} + 0i_w \quad \text{for some } w.$$

Since $i_1 + \cdots + i_{w-1} \leq m$, such an expression can be associated to a partition of l into at most m parts. Conversely, given such a partition, we can let $w-1$ be the largest integer appearing in it and let i_s be the number of times $w-s$ appears, $1 \leq s \leq w-1$. So $b_{l,m}$ is the number of partitions of l into at most m parts. Next we observe that

$$\begin{aligned} \prod_{k=1}^m (1 - p^{-k})^{-1} &= \prod_{k=1}^m (1 + p^{-k} + p^{-2k} + \cdots) \\ &= \sum_{j_1, j_2, \dots, j_m \geq 0} p^{-1j_1 - 2j_2 - \cdots - mj_m} = \sum_{l=0}^{\infty} c_{l,m} p^{-l}, \end{aligned}$$

where $c_{l,m}$ is the number of times that $l = 1j_1 + 2j_2 + \cdots + mj_m$. But then $c_{l,m}$ is the number of partitions of l into parts with each part at most m . From [10, Theorem 343], $b_{l,m} = c_{l,m}$ for all l and m , and hence the lemma is proved.

Now applying the Lemma to the sum in (4), we get

$$\begin{aligned} \lim_{w \rightarrow \infty} \frac{1}{p^{wr}} \sum_{\substack{i_1 + \cdots + i_w \leq r \\ \text{each } i_s \geq 0}} p^{1i_1 + 2i_2 + \cdots + wi_w} &= \lim_{w \rightarrow \infty} \left[\frac{1}{p^{wr}} + \sum_{m=1}^r \frac{1}{p^{w(r-m)}} F_{w,m} \right] \\ &= \lim_{w \rightarrow \infty} F_{w,r} = \prod_{k=1}^r (1 - p^{-k})^{-1}, \end{aligned}$$

which completes the proof of Theorem 2.

4. Cohen-Lenstra Conjectures. We let notation be the same as in previous sections. In [1] Cohen and Lenstra have made various conjectures that apply to the prime to p part of the class groups for Galois extensions of \mathbf{Q} of degree p . Since our results apply to the p part of the class groups, our results do not prove or disprove any of the Cohen-Lenstra Conjectures. However, our results do have an interesting relationship with the Cohen-Lenstra Conjectures. To describe this relationship, we first let S_K be the narrow ideal class group of K , and we let $H_K = S_K^{1-\sigma}$, which is the narrow principal genus of K for the fields K we are considering. Then our Theorems 1 and 2 appear to be what would be predicated if we assumed that Fundamental Assumptions 8.1 and Theorem 6.3 in [1] apply to H_K . Actually the appropriate Cohen-Lenstra

probability is defined in a different way than our density $d_{\infty,r}$. More precisely, let

$$d_r = \lim_{x \rightarrow \infty} \left(\frac{\sum_{\substack{K \\ |D_K| \leq x \\ R_K = r}} 1}{\sum_{\substack{K \\ |D_K| \leq x}} 1} \right)$$

where K ranges over the Galois extensions of \mathbf{Q} of degree p , D_K is the discriminant of K , and R_K is defined in §1. (When $p = 2$, the real and imaginary quadratic fields are handled separately.) This Cohen-Lenstra probability d_r omits all reference to the number t of ramified primes and deals with the discriminant D_K instead of the conductor f_K . Since $|D_K| = f_K^{p-1}$, there is no difficulty in passing from the conductor to the discriminant. So we see that

$$(5) \quad d_r = \lim_{x \rightarrow \infty} \left(\frac{\sum_{s=1}^{\infty} |A_{s,r;x}|}{\sum_{s=1}^{\infty} |A_{s;x}|} \right).$$

(Note that for each x the above sums are finite.) However,

$$d_{\infty,r} = \lim_{t \rightarrow \infty} d_{t,r} = \lim_{t \rightarrow \infty} \left(\lim_{x \rightarrow \infty} \frac{|A_{t,r;x}|}{|A_{t;x}|} \right).$$

Since for fixed t and $s < t$, $|A_{s,r;x}| = o(|A_{t,r;x}|)$ and $|A_{s;x}| = o(|A_{t;x}|)$ as $x \rightarrow \infty$ (cf. [5, Propositions 3.3 and 3.4 and 6, Propositions 2.1 and 5.1]), then

$$(6) \quad d_{\infty,r} = \lim_{t \rightarrow \infty} \left(\lim_{x \rightarrow \infty} \frac{\sum_{s=1}^t |A_{s,r;x}|}{\sum_{s=1}^t |A_{s;x}|} \right).$$

From (5) and (6), it seems plausible that $d_r = d_{\infty,r}$, although a proof would involve more detailed estimates with explicit dependence on t carefully analyzed.

Now assuming $d_r = d_{\infty,r}$, our results suggest that the Cohen-Lenstra Conjectures should be extended to include all of the narrow principal genus for Galois extensions of \mathbf{Q} of prime degree p . In particular, the conjectures in §9 of [1] could be extended to all of the narrow principal genus. As an example we mention how conjecture (C14) in [1] could be extended.

CONJECTURE (C14'). *For totally real Galois extensions of \mathbf{Q} of prime degree p (including $p = 2$), the probability $Z(p)$ that the narrow principal genus is trivial is given by*

$$Z(p) = \prod_{k=2}^{\infty} \left(\zeta_{\mathbf{Q}(\sqrt[p]{1})}(k) \right)^{-1}$$

where $\zeta_{\mathbf{Q}(\sqrt[p]{1})}(s)$ is the Dedekind zeta function of the cyclotomic field $\mathbf{Q}(\sqrt[p]{1})$.

Some numerical values of $Z(p)$ are as follows: $Z(2) = 0.436$, $Z(3) = 0.714$, $Z(5) = 0.903$, and $Z(7) = 0.929$. Also $\lim_{p \rightarrow \infty} Z(p) = 1$ (cf. [1, p. 58]). So for large p , one should expect the narrow principal genus to be trivial.

REMARK. The Cohen-Lenstra Conjectures should also apply to the usual principal genus, not just the narrow principal genus (cf. [6, p. 491]).

5. Estimate of a character sum. Our proof of Theorem 2 depends on results from [3 and 5]. In the proof of Lemma 3 in [3], we used a certain character sum estimate (see bottom of p. 202 in [3]) that was derived in a preliminary version of [7], but this particular character sum estimate was not included in the final version of [7]. So for the sake of completeness, we sketch a proof of that character sum estimate.

The basic reference for the techniques for this character sum estimate is [2]. We suppose that λ is a nonprincipal Dirichlet character with exponent l and conductor $p_1 \cdots p_s$, where l is a prime and p_1, \dots, p_s are distinct primes. We let x be a large real number, $q = p_1 \cdots p_s$, $y = x/q$, and

$$z = \exp[(\log x)/(b \log \log x)],$$

where b is a constant to be specified later. We assume $q \leq z$. We want to show

$$(7) \quad \sum_{p \leq y} \lambda(p) = O(y/(\log qy)^2)$$

where the sum ranges over all primes $p \leq y$. Note that we need only estimate $\sum_{(qy)^{1/2} < p \leq y} \lambda(p)$ since $q \leq z$ and $y = x/q$ imply $(qy)^{1/2} = O(y/(\log qy)^2)$. Now

$$\begin{aligned} \sum_{(qy)^{1/2} < p \leq y} \lambda(p) &= \sum_{\substack{(qy)^{1/2} < p^m \leq y \\ m \geq 1}} \frac{\lambda(p^m) \log p}{\log(p^m)} - \sum_{\substack{(qy)^{1/2} < p^m \leq y \\ m \geq 2}} \frac{\lambda(p^m) \log p}{\log(p^m)} \\ &= \sum_{(qy)^{1/2} < n \leq y} \frac{\lambda(n) \Lambda(n)}{\log n} + O(y^{1/2}) \end{aligned}$$

where

$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a power of a prime } p, \\ 0 & \text{otherwise.} \end{cases}$$

Using partial summation (cf. [10, Theorem 421]), we see that (7) will be proved if we can show that

$$(8) \quad \sum_{n \leq y} \lambda(n) \Lambda(n) = O(y/(\log qy)).$$

From [2, p. 126], we have

$$(9) \quad \sum_{n \leq y} \lambda(n) \Lambda(n) = -y^\beta/\beta + R(y, T)$$

where

$$(10) \quad |R(y, T)| \ll y(\log qy)^2 \exp[-c(\log y)/(\log qT)] \\ + yT^{-1}(\log qy)^2 + y^{1/4}(\log y).$$

In formulas (9) and (10), T is a parameter we are free to choose; q is the conductor of λ ; and c is a positive absolute constant. The term with y^β in (9) can occur only if λ is an “exceptional” real character (and hence $l = 2$). If λ is an exceptional character, then (8) may not be valid. However, we do know that

$$\beta < 1 - c_1/q^{1/2}(\log q)^2$$

for some positive absolute constant c_1 (see [2, p. 99]). Then one can show that $y^\beta = O(x/(\log x)^{1+\gamma})$ for some $\gamma > 0$. When sums are subsequently taken over the conductors $q = p_1 \cdots p_s$, fortunately the exceptional conductors are rather sparse. If these exceptional conductors are $q_0 < q_1 < q_2 < \cdots$, then $q_{j+1} > q_j^2$ for each j (see [2, p. 98]), and so $q_j > \exp(2^j)$ for each j . Since $q_j \leq \exp(\log x/(b \log \log x))$, then $j = O(\log \log x)$, and hence the total contribution of all y^β/β can be incorporated into the final error term $o(x(\log \log x)^s/(\log x))$ (cf. Lemma 3 of [3]).

It remains to show that $|R(y, T)| \ll y/(\log qy)$. By choosing $T = (\log qy)^3$, we see that the second and third terms on the right side of (10) are $\ll y/(\log qy)$. Now

$$\frac{y(\log qy)^2}{\exp\left[\frac{c(\log y)}{\log qT}\right]} \ll \frac{y(\log qy)^2}{\exp\left[\frac{c \log((qy)^{1-\delta})}{(\log qy)/(b(\log \log qy)) + 3(\log \log qy)}\right]}$$

for any $0 < \delta < 1$. We let ϵ satisfy $0 < \epsilon < (1/3)c(1 - \delta)$. We choose y large enough so that

$$3(\log \log qy) < \epsilon(\log qy)/(\log \log qy),$$

and we choose $b > 0$ so that $c(1 - \delta) \geq 3((1/b) + \epsilon)$. Then

$$y(\log qy)^2 \exp[-c(\log y)/(\log qT)] \ll y/(\log qy),$$

and hence $|R(y, T)| \ll y/(\log qy)$.

In [3], where $l \geq 3$, (7) is needed for the slightly more general case of Hecke characters over $\mathbf{Q}(\exp(2\pi i/l))$ instead of Dirichlet characters. However, the methods are essentially the same as those used for Dirichlet characters (e.g., compare the methods in Chapter 14 of [8] with the methods in [2]). Furthermore there are no exceptional characters when $l \geq 3$.

ACKNOWLEDGMENT. The author thanks the referee for several helpful suggestions.

APPENDIX. Some values for $d_{\infty,r}$ in Theorems 1 and 2 are given below.

p	r	0	1	2	3	4
2 (imag. case)		0.288788	0.577576	0.128350	0.005239	4.7×10^{-5}
2 (real case)		0.577576	0.385051	0.036672	0.000699	3.0×10^{-6}
3		0.840189	0.157535	0.002272	3.3×10^{-6}	5.1×10^{-10}
5		0.950416	0.049501	8.3×10^{-5}	5.4×10^{-9}	1.4×10^{-14}
7		0.976261	0.023729	1.0×10^{-5}	8.6×10^{-11}	1.5×10^{-17}

REFERENCES

1. H. Cohen and H. Lenstra, Jr., *Heuristics on class groups of number fields*, Lecture Notes in Math., vol. 1068, Springer-Verlag, Berlin and New York, 1984, pp. 33–62.
2. H. Davenport, *Multiplicative number theory*, Markham, Chicago, Ill., 1967.
3. F. Gerth, *Counting certain number fields with prescribed l -class numbers*, J. Riene Angew., Math. 337 (1982), 195–207.
4. ———, *Asymptotic behavior of number fields with prescribed l -class numbers*, J. Number Theory 17 (1983), 191–203.

5. _____, *An application of matrices over finite fields to algebraic number theory*, Math. Comp. **41** (1983), 229–234.
6. _____, *The 4-class ranks of quadratic fields*, Invent. Math. **77** (1984), 489–515.
7. F. Gerth and S. Graham, *Application of a character sum estimate to a 2-class number density*, J. Number Theory **19** (1984), 239–247.
8. L. Goldstein, *Analytic number theory*, Prentice-Hall, Englewood Cliffs, N. J., 1971.
9. G. Gras, *Sur les l -classes d'idéaux dans les extensions cycliques relatives de degré premier l* , Ann. Inst. Fourier (Grenoble) **23** (1973), 1–48; **23** (1973), 1–44.
10. G. Hardy and E. Wright, *An introduction to the theory of numbers* (4th ed.), Oxford Univ. Press, London, 1965.
11. E. Inaba, *Über die Struktur der l -Klassengruppe zyklischer Zahlkörper von Primzahlgrad l* , J. Fac. Sci. Imp. Univ. Tokyo, Sect. I **4** (1940), 61–115.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS, AUSTIN, TEXAS 78712