Fields Institute Communications
Volume 00, 0000

Prime-power real cyclotomic class number heuristics

Joe Buhler
Reed College, Portland, OR, USA
jpb@reed.edu

Carl Pomerance
Bell Labs, Murray Hill, NJ, USA
carlp@research.bell-labs.com

Leanne Robertson
Smith College, Northampton, MA, USA
lroberts@math.smith.edu

Dedicated to Hugh Williams on the occasion of his sixtieth birthday

Abstract. Let $h^+(\ell^n)$ denote the class number of the maximal totally real subfield $\mathbb{Q}(\cos(2\pi/\ell^n))$ of the field of ℓ^n-th roots of unity. The goal of this paper is to show that (speculative extensions of) the Cohen-Lenstra heuristics on class groups provide support for the following conjecture: for all but finitely many pairs (ℓ, n), where ℓ is a prime and n is a positive integer, $h^+(\ell^{n+1}) = h^+(\ell^n)$. In particular, this predicts that for all but finitely many primes ℓ, $h^+(\ell^n) = h^+(\ell)$ for all positive integers n.

Extensive computations of René Schoof [9] enumerate all "small" components of the plus part of the class group of cyclotomic fields of prime conductor. Let ℓ be an odd prime, $K(\ell) := \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ be the maximal totally real subfield of ℓ-th roots of unity, and $G(\ell) := \mathrm{Gal}\,(K(\ell)/\mathbb{Q})$ be the Galois group of $K(\ell)$ over $\mathbb{Q}$, so that $G(\ell)$ is a cyclic group of order $(\ell-1)/2$. The class group $Cl^+(\ell)$ of $K(\ell)$ is a module over the group ring $\mathbb{Z}[G(\ell)]$. For all $\ell < 10000$, Schoof finds the largest subgroup of the class group whose simple factors (as $\mathbb{Z}[G(\ell)]$ modules) have size less than 80000. Let $h^+(\ell)$ denote the order of the class group of $K(\ell)$, and $\tilde{h}^+(\ell)$ denote the order of Schoof's subgroup. For all $\ell < 10000$ either $h^+(\ell) = \tilde{h}^+(\ell)$ or $h^+(\ell) > 80000\,\tilde{h}^+(\ell)$; it seems very likely that $h^+(\ell) = \tilde{h}^+(\ell)$ in every case. In fact, the largest simple factor found in the search has order 1451, there are 2 others over 500, and almost all of the others are below 100. The novelty and extent of these computations are indicated by the fact that $h^+(\ell)$ is known only for $\ell \le 67$ (or $\ell \le 163$ assuming the GRH); the exact computations of $h^+(\ell)$ rely on bounds on discriminants, and at the moment it seems difficult to extend them beyond these limits.

At the end of [9] the "probability" that $h^+(\ell) = \tilde{h}^+(\ell)$ for all $\ell < 10000$ is computed on the assumption that, as $\mathbb{Z}[G(\ell)]$ modules, the class groups of these fields behave probabilistically as the Cohen-Lenstra heuristics predict would be the case for a large sample of fields of the given signature and Galois group. This probability is found to be greater than 0.98, i.e., under this speculative extension of the heuristics, the tables in [9] are highly likely to give $h^+(\ell)$ exactly for all $\ell < 10000$.

Our goal is to analyze similar heuristics for the plus part of the class groups of prime-power conductor. Let $h^+(\ell^n)$ denote the class number of the field $K(\ell^n)$. We are led to make the following conjecture.

Conjecture 1 *For all but finitely many pairs (ℓ, n), where ℓ is a prime and n is a positive integer, the class number of $K(\ell^{n+1})$ is equal to the class number of $K(\ell^n)$, i.e.,*

$$h^+(\ell^{n+1}) = h^+(\ell^n). \tag{1}$$

The ℓ-Sylow subgroup of the class group $Cl^+(\ell^n)$ has been studied for many years, and several famous conjectures make predictions about the power of ℓ dividing $h^+(\ell^n)$. The Cohen-Lenstra heuristics, of the type that we will use for the prime-to-ℓ part of the class number, are not thought to apply to the power of ℓ dividing $h^+(\ell^n)$ for $n > 1$ since ℓ divides the degree of $K(\ell^n)$ over $\mathbb{Q}$. Our belief in the "ℓ-part" of the conjecture is based on several things.

First, the Kummer-Vandiver conjecture that $h^+(\ell)$ is not divisible by ℓ implies that $h^+(\ell^n)$ is prime to ℓ for all n [10, Corollary 10.5]. The Kummer-Vandiver conjecture is true for all ℓ less than 12 million [1], and thus $h^+(\ell^n)$ is prime to ℓ for all $\ell < 12000000$. Moreover, results in K-theory by Soulé, Snaith, and others [8] provide some support for the idea that the conjecture is true for all primes.

Second, Greenberg's conjecture on Iwasawa invariants of totally real number fields implies that for every ℓ there is an n_0 such that for all $n \geq n_0$ the ℓ-Sylow subgroup of $Cl^+(\ell^n)$ is equal to the ℓ-Sylow subgroup of $Cl^+(\ell^{n_0})$. Although we know of no proposed heuristic probability distribution on n_0, it seems plausible to guess that $n_0 = 1$ for all but finitely many ℓ.

From now on, we study the p-Sylow subgroups of $Cl^+(\ell^n)$ for $p \neq \ell$. Our primary theorem is that an expression that represents the "expected" number of counterexamples to (1), under suitable heuristics, is finite.

To explain this more carefully, we begin by introducing notation for the relevant finite Galois modules. Let ℓ be a prime, and n a positive integer; to avoid trivialities we assume that $\ell^n > 2$ throughout. Let $K(\ell^n)$ denote the maximal totally real subfield of the field of ℓ^n-th roots of unity; $K(\ell^n)$ is a Galois extension of $\mathbb{Q}$ with group $G = \mathrm{Gal}(K(\ell^n)/\mathbb{Q}) = G(\ell^n)$ that is cyclic of order

$$|G| \;=\; \phi(\ell^n)/2 \;=\; \ell^{n-1}(\ell-1)/2,$$

where ϕ is Euler's function. Any finite $\mathbb{Z}[G]$ module has a composition series, and each simple module M is a quotient of $\mathbb{Z}[G]$ by a maximal ideal. The order of a finite $\mathbb{Z}[G]$ module is the product, counting multiplicities, of the orders of the simple modules M that arise in the composition series.

A simple module M has order $q = p^f$ where p is a prime, and can be described as follows (see [9]). Choose a divisor D of $|G| = \phi(\ell^n)/2$ that is not divisible by p. Choose a prime ideal P of $\mathbb{Z}[\zeta_D]$ of norm $q = p^f$, where f is the multiplicative order

of p mod D. Let $\overline{P}$ be the inverse image of P in $\mathbb{Z}[G]$ under the surjective ring homomorphism

$$\mathbb{Z}[G] \to \mathbb{Z}[\zeta_D]$$

that takes a generator of G to ζ_D. Then let $M = \mathbb{Z}[G]/\overline{P}$. We say that M has "level n" if the divisor D of $\phi(\ell^n)/2$ does not divide $\phi(\ell^{n-1})/2$.

The Cohen-Lenstra heuristics [2, 3] predict, roughly, that in a large sample totally real Galois extensions F of $\mathbb{Q}$, with fixed Galois group G, the class group of F behaves as a random

finite $\mathbb{Z}[G]$ module modulo a random cyclic module. They carefully analyze [3, Example 5.10, p. 47] a natural notion

of randomness when G is abelian, and prove that the probability that a given simple module M, with order relatively prime to the order of G, does not occur in the Jordan-Hölder composition series of a random module modulo a random cyclic submodule is

$$p_M := \prod_{k=2}^{\infty} \left(1 - |M|^{-k}\right) \tag{2}$$

where $|M|$ denotes the order of M. In addition, these probabilities should be independent for different M.

We would like to apply this to class groups $Cl^+(\ell^n)$, but this is hard to formalize in the usual frequentist language of probability since there is no underlying probability space. Indeed, the original Cohen-Lenstra heuristics apply to a large collection of fields of a given degree, and we are applying them to a large collection of fields whose degrees are unbounded. Instead we adopt a subjective Bayesian view, where probability arises from ignorance. Thus we use the Cohen-Lenstra heuristics as the basis for the assignment of subjective probabilities, on the grounds that they are a plausible first guess. One justification for this way of thinking is that the heuristics actually make predictions which can be tested empirically. For example, in [9] it is noted that similar heuristics imply that the proportion of $\ell < 10000$ with $h^+(\ell) = 1$ should be about 71%, which is only slightly smaller than the 75% of the ℓ in

the sample that were observed to have $\tilde{h}^+(\ell) = 1$. Similarly, heuristic predictions about $h^+(\ell^n)$ can be explored empirically by searching for M-isotypic components for "small" ℓ, n, and M, comparing the observed frequencies with the predictions implicit in the analysis below; we hope to carry out this empirical investigation in future work.

Before making the "probabilities" precise, we comment on technical aspects of our assumptions. First, the absolute norm of any ideal is principal, so that the class group is actually a module over the quotient $\mathbb{Z}[G(\ell^n)]/\langle Nrm\rangle$ of the group ring by the module generated by the norm element $Nrm := \sum \sigma$; one checks that this just means that any M that occurs as a simple factor in a class group has $D > 1$. In our case, we are interested in modules of level at least two, so this is automatic since D will always be divisible by ℓ.

Second, we note that primes dividing the degree are usually excluded when considering Cohen-Lenstra heuristics. In our case the degree of $K(\ell^n)$ is $\ell^{n-1}(\ell - 1)/2$. Let p be the unique prime dividing the order of a simple galois module M. As discussed above, we rely on other ideas to support the conjecture in the case $p = \ell$. It might also seem prudent to exclude the primes p dividing $(\ell - 1)/2$. However,

[10, Theorem 10.4(a)] implies that the question of whether or not p divides the class number of $K(\ell^n)$ is equivalent to the question of whether or not p divides the class number of the field L that is the largest subfield of $K(\ell^n)$ whose degree over $\mathbb{Q}$ is prime to p. Similarly, the heuristics used here are equivalent to Cohen-Lenstra heuristics for $L/\mathbb{Q}$, so that they arise in a situation in which p in fact does not divide the degree.

If a counterexample to (1) exists then there is a simple M of level $n+1$ that occurs in a composition series of $Cl^+(\ell^{n+1})$. According to the (extended) heuristics, the "probability" that such a simple module M occurs is $1-p_M$, where p_M is defined in (2). Thus the expected number of counterexamples to (1), over all ℓ and n, is

$$E := \sum_{\ell} \sum_{n=1}^{\infty} \left(1 - \prod p_M\right) \tag{3}$$

where the product is over all simple modules of level $n+1$. Our main result is that this sum converges.

We remark that if $pr_1, pr_2, \cdots$ are the probabilities of various events then $Ex := \sum pr_i$ is the expected number that occur. Further, if the events are independent, then $Pr := \prod(1-pr_i)$ is the probability that none occur. Using $x < -\log(1-x)$ we see that $Ex < -\log Pr$ so that if the expectation is finite it follows that Pr is positive.

In any event, applying $1 - x < -\log x$ together with (2) gives

$$E < \sum_{\ell \text{ prime}} \sum_{n\ge 1} \sum_{M} -\log\left(\prod_{k\ge 2}(1-|M|^{-k})\right)$$

where the innermost sum is over all simple modules M of level $n+1$.

Now recall that if $p \neq \ell$ is a prime not dividing D then p splits in $\mathbb{Z}[\zeta_D]$ into $\phi(D)/f$ ideals of norm p^f, where f is the multiplicative order of $p \bmod D$. Thus the product over M of level $n+1$ can be replaced by a product over pairs (D,p) where: p is a prime not equal to ℓ, and if ℓ is odd then $D = \ell^n d$, where d is a divisor of $(\ell-1)/2$ not divisible by p, and if $\ell = 2$ then $D = 2^{n-1}$

(and we fix $d = 1$). Substituting all of this into the formula for E, and using the power series for the logarithm, gives

$$E < \sum_{\ell} \sum_{n\ge 1} \sum_{d} \sum_{p\nmid \ell d} \sum_{k\ge 2} \sum_{m\ge 1} \frac{\phi(D)}{f m p^{kfm}}, \tag{4}$$

where $f = f(\ell, n, d, p)$ is the multiplicative order of p modulo D. Here the sum over d is the sum over divisors d of $(\ell-1)/2$ if ℓ is odd, and is the singleton sum with $d = 1$ if $\ell = 2$. Our goal is to show that this 6-fold sum is finite.

Note that for $A \ge 2$,

$$\sum_{k\ge 2} \frac{1}{A^k} = \frac{1}{A(A-1)} \le \frac{2}{A^2}. \tag{5}$$

Thus it suffices to fix $k = 2$ in (4). Further, for $A \ge 4$,

$$\sum_{m\ge 1} \frac{1}{mA^m} = -\log\left(1 - A^{-1}\right) < 1.16A^{-1}, \tag{6}$$

so that we may also fix $m = 1$. Thus it suffices to show that the 4-fold sum

$$\sum_{\ell} \sum_{n \geq 1} \sum_{d} \sum_{p \nmid \ell d} \frac{\phi(D)}{f p^{2f}} \tag{7}$$

is finite.

Before proving this, we make a back-of-the-envelope calculation that suggests that this is plausible. We expect that the dominant terms in the sum will be those with $\ell > 2$, $n = 1$, and $f = 1$; in fact we expect that the sum converges if and only if the sum of those terms converges (as it happens, this expectation is verified in the proof of Theorem 1 below).

The condition that $f = 1$ merely means that we restrict to primes p that are congruent to 1 modulo D. Since $\ell > 2$ and $n = 1$, we have $D = \ell d$, where d divides $(\ell - 1)/2$. To show that the sum

$$\sum_{\ell} \sum_{d} \phi(\ell d) \sum_{p \equiv 1 \bmod \ell d} \frac{1}{p^2} \tag{8}$$

is finite, we use the heuristic approximation

$$\sum_{p \equiv 1 \bmod \ell d} g(p) \approx \frac{1}{\phi(\ell d)} \int_{\ell d + 1}^{\infty} g(x) \frac{dx}{\log x} \, .$$

For $g(x) = x^{-2}$ this gives

$$\sum_{p \equiv 1 \bmod \ell d} \frac{1}{p^2} \approx \frac{1}{\phi(\ell d)} \frac{1}{\ell d \log(\ell d)}.$$

(Note that if $\ell d + 1$ is prime, then this sum is at least $1/(\ell d + 1)^2$, and the approximate formula definitely does *not* hold. However, it may be reasonable to assume that it holds *on average*.) Thus (8) plausibly converges if the sum

$$\sum_{\ell} \sum_{d | (\ell - 1)/2} \frac{1}{\ell d \log(\ell d)}$$

converges. Interchanging the sums gives

$$\sum_{d=1}^{\infty} \sum_{\ell \equiv 1 \bmod 2d} \frac{1}{d\ell \log(\ell d)} \; < \; \sum_{d=1}^{\infty} \frac{1}{d} \sum_{\ell \equiv 1 \bmod 2d} \frac{1}{\ell \log(\ell)}.$$

Employing the same heuristic as above, we find that the inner sum should be of the order of $1/\phi(2d)\log(2d)$. (In fact, the Brun–Titchmarsh inequality can rigorously show that the inner sum is $O(\log\log(3d)/\phi(d)\log(2d))$, which is sufficient for convergence.) Since

$$\begin{aligned} \sum_{d=1}^{\infty} \frac{1}{d\phi(2d)\log(2d)} \; &< \; \sum_{d=1}^{\infty} \frac{1}{d\phi(d)} = \prod_{p} \left(1 + \frac{1}{p\phi(p)} + \frac{1}{p^2 \phi(p^2)} + \cdots \right) \\ &= \; \prod_{p} \left(1 + \frac{p}{(p-1)(p^2-1)} \right) \; < \; \infty \end{aligned}$$

we find, modulo our plausible assumptions, that the sum is finite, and thus the expected number of counterexamples to (1) is finite.

Although this reasoning is heuristic, we can rigorously prove the following result.

Theorem 1 *The sum for E in (3) converges.*

Proof By the earlier remarks, it suffices to show that the sum in (7) is finite. For notational simplicity, we consider the contributions to the sum from $\ell = 2$ and odd ℓ separately.

First consider the contribution to (7) from $\ell = 2$. We need to show that

$$\sum_{n\ge 1}\sum_{p>2}\frac{2^{n-2}}{fp^{2f}}$$

is finite, where p ranges over odd primes and f is the order of p modulo 2^{n-1}. Noting that $p^f = 1 + 2^{n-1}t$ for some integer t, we see that the sum is finite since it is less than

$$\sum_{n\ge 1}\sum_{t\ge 1}\frac{2^{n-2}}{(1+2^{n-1}t)^2} < \sum_{n\ge 1}\sum_{t\ge 1}\frac{1}{2^n t^2} = \frac{\pi^2}{6}.$$

To prove the theorem it remains to show that the contribution to the sum in (7) from odd primes ℓ is finite. By the definition of f, and interchanging the order of the inner summations, we see that it suffices to show that

$$\sum_{f\ge 1}\sum_{p}\sum_{\substack{\ell^n d\mid p^f-1\\ d\mid(\ell-1)/2}}\frac{\phi(\ell^n d)}{fp^{2f}} \;<\; \infty. \tag{9}$$

Let

$$F(m) \;=\; \sum_{\substack{\ell^n d\mid m\\ d\mid(\ell-1)/2}}\phi(\ell^n d)$$

and let $\Omega_1(m)$ denote the number of odd prime factors of m, counted with multiplicity. Then

$$F(m) \;\le\; \sum_{\ell^n\mid m}\ell^n\sum_{d\mid m/\ell^n}\phi(d) \;=\; \sum_{\ell^n\mid m}\ell^n\cdot\frac{m}{\ell^n} \;=\; m\Omega_1(m). \tag{10}$$

Since $\Omega_1(m)\le \log_3 m \le \log m$, we have that the contribution to (9) from the terms with $f\ge 2$ is

$$\sum_{f\ge 2}\sum_{p}\frac{F(p^f-1)}{fp^{2f}} \;<\; \sum_{f\ge 2}\sum_{p}\frac{\log(p^f-1)}{fp^f} \;<\; \sum_{f\ge 2}\sum_{p}\frac{\log p}{p^f} \;<\; 2\sum_{p}\frac{\log p}{p^2},$$

which is finite. Hence, to prove the theorem it suffices to show that

$$S := \sum_{p}\frac{F(p-1)}{p^2} \;<\; \infty. \tag{11}$$

Let $F_0(m)$ be the same sum as with $F(m)$ but with the extra condition that $\ell^n \le m/\log^5 m$. We have $S \le S_1+S_2+S_3+S_4$, where

$$\begin{aligned}
&\text{in } S_1,\ \Omega_1(p-1) > 8\log\log p,\\
&\text{in } S_2,\ \Omega_1(p-1) \le 8\log\log p \text{ and } F_0(p-1) < F(p-1),\\
&\text{in } S_3,\ F_0(p-1) > p/\log p,\\
&\text{in } S_4,\ F_0(p-1) = F(p-1) \le p/\log p.
\end{aligned}$$

By Theorem 04 in [5] we have

$$\sum_{m\le x}(5/3)^{\Omega_1(m)} \;=\; O(x\log^{2/3}x),$$

so that the number of integers $m\le x$ with $\Omega_1(m)>8\log\log m$ is $O(x/\log^3 x)$ (using $8\log(5/3)-2/3>3$). Since (10) implies that $F(p-1)/p^2<(\log p)/p$, it follows by partial summation that

$$\begin{aligned} S_1 \;&<\; \sum_{\Omega_1(p-1)>8\log\log p}\frac{\log p}{p} \;=\; \int_2^\infty \frac{\log x-1}{x^2}\sum_{\substack{p\le x\\ \Omega_1(p-1)>8\log\log p}} 1\,dx \\ &=\; O\left(\int_2^\infty \frac{dx}{x\log^2 x}\right) \;=\; O(1). \end{aligned}$$

For S_2 we shall prove that the number of primes $p\le x$ with $F_0(p-1)<F(p-1)$ is $O(x\log\log x/\log^2 x)$. Since $F(p-1)/p^2\le(8\log\log p)/p$ for the primes considered in S_2, we would then have

$$\begin{aligned} S_2 \;&\le\; \sum_{F_0(p-1)<F(p-1)}\frac{8\log\log p}{p} \;=\; \int_2^\infty \frac{d}{dx}\left(\frac{-8\log\log x}{x}\right)\sum_{\substack{p\le x\\ F_0(p-1)<F(p-1)}} 1\,dx \\ &=\; O\left(\int_2^\infty \frac{(\log\log x)^2}{x\log^2 x}\,dx\right) \;=\; O(1). \end{aligned}$$

To see the assertion, let a be a positive integer with $a\le\log^5 x$. By Brun's sieve method (Theorem 2.2 in [4]) the number of primes $\ell\le x/a$ with $a\ell+1$ prime is $O(x/\phi(a)\log^2 x)$.

Thus, the number of primes $p\le x$ with some prime $\ell|p-1$ and $\ell>p/\log^5 p$ is

$$O\left(\frac{x}{\log^2 x}\sum_{a\le\log^5 x}\frac{1}{\phi(a)}\right) \;=\; O\left(\frac{x\log\log x}{\log^2 x}\right).$$

Further, the number of primes $p\le x$ with some $\ell^n|p-1$ where $\ell^n>p/\log^5 p$ and $n\ge 2$ is trivially at most

$$\pi(x^{1/2})+x\sum_{n\ge 2}\sum_{\ell^n>x^{1/2}/\log^5(x^{1/2})}\frac{1}{\ell^n} \;=\; O\left(x^{3/4}\log^{5/2}x\right).$$

Thus, our proof that $S_2<\infty$ is complete.

The argument to show that $S_3<\infty$ will follow as with the argument for S_1 if we show that the number of primes $p\le x$ with $F_0(p-1)>p/\log p$ is $O(x/\log^3 x)$. We show this by an averaging argument. Note that by Theorem 318 in [6] for the

average order of the number-of-divisors function $\tau(u)$ we have that

$$\begin{aligned}\sum_{m\le x} F_0(m) &\le \sum_{\substack{\ell^n d\le x\\ d\mid(\ell-1)/2\\ \ell^n\le x/\log^5 x}} \phi(\ell^n d)\sum_{\substack{m\le x\\ \ell^n d\mid m}} 1 \le x\sum_{\substack{\ell^n d\le x\\ d\mid(\ell-1)/2\\ \ell^n\le x/\log^5 x}} 1\\ &\le x\sum_{\ell^n\le x/\log^5 x}\ \sum_{d\mid \ell-1} 1 \le x\sum_{n<\log x}\ \sum_{u<(x/\log^5 x)^{1/n}} \tau(u)\\ &= O\left(x\sum_{n<\log x}(x/\log^5 x)^{1/n}\log(x^{1/n})\right) = O(x^2/\log^4 x).\end{aligned}$$

Hence the number of integers $m\le x$ with $F_0(m) > m/\log m$ is $O(x/\log^3 x)$, which completes our estimation of S_3.

Finally, in S_4 we have $F(p-1) = F_0(p-1) \le p/\log p$, so that $S_4 \le \sum_{p \text{ prime}} \frac{1}{p\log p} < \infty$, where the sum is over all primes. Thus, we have that each of S_1, S_2, S_3, S_4 is finite, which shows that (11) holds, finishing the proof of the theorem.

□

Long ago, Weber conjectured that $h^+(2^n) = 1$ for all n. The argument at the beginning of the proof can be sharpened to provide strong support for this conjecture. First, it is known that $h^+(2^7) = 1$ from [7]. Thus we can take $n \ge 7$ in our estimates. The prime powers p^f that occur are congruent to 1 modulo 2^6, and the constants in (5) and (6) can be sharpened by using $A \ge 65$. We wrote a short computer program that calculated the sum, over $7 \le n \le 12$ and $p^f < 10^5$, of $2^{n-2}/fp^{2f}$, where p is an odd prime and f is the order of p modulo 2^{n-1}. The terms with $n > 12$ or $p^f > 10^5$ can be bounded by the elementary estimates given in the proof above, and the upshot is that we find that the expected number E of simple modules that occur in the class group of $K(2^n)$ for any n satisfies $E < .007$. Thus, reverting to a Bayesian probabilistic view of the (extended) Cohen-Lenstra heuristics, we might say that the probability that Weber's Conjecture is true is at least 99.6%.

Acknowledgments. We would like to thank René Schoof and Hendrik Lenstra, Jr., for several conversations, and for helpful comments on an earlier draft of this paper.

The authors would also like to thank Hugh Williams for his computational spirit, his cheerful personality, and also for having friends and colleagues who put on a marvelous conference in a scenic location that allowed us to develop the ideas discussed here.

References

[1] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and A. Shokrollahi, Irregular primes and cyclotomic invariants to twelve million, *J. Symb. Comp.*, **31**, 2001, 89–96.

[2] H. Cohen, and H.W. Lenstra, Jr., Heuristics on class groups, in *Number Theory*, 26–36, Lecture Notes in Math. **1052**, Springer, Berlin, 1984.

[3] H. Cohen, and H.W. Lenstra, Jr., Heuristics on class groups of number fields, in *Number Theory, Noordwijkerhout 1983*, 33–62, Lecture Notes in Math. **1068**, Springer-Verlag, Berlin 1984.

[4] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London, 1974.

[5] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics **90**, Cambridge University Press, Cambridge, 1988.

[6] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Fifth edition, The Clarendon Press, Oxford University Press, New York, 1979.
[7] F.J. van der Linden, Class number computations of real abelian number fields, *Math. Comp.* **39** (1982), 693–707. (See also *Math Reviews* **84e:12005**.)
[8] Victor Snaith, Equivariant motivic phenomena, University of Southampton preprint, May 2003.
[9] René Schoof, Class numbers of real cyclotomic fields of prime conductor, *Math. Comp.* **72** (2003), 913–937.
[10] Lawrence Washington, *Introduction to cyclotomic fields*, Second edition, Springer-Verlag, New York, 1997.