JP Jour. Algebra, Number Theory & Appl. **6**(1) (2006), 129-148

ARITHMETIC PROPERTIES OF CLASS NUMBERS OF IMAGINARY QUADRATIC FIELDS

SAFUAT HAMDY
College of Information Technology
United Arab Emirates University
Al-Ain, United Arab Emirates

FILIP SAIDAK
Department of Mathematics
University of Missouri
Columbia, MO 65211, *U. S. A.*
e-mail: filip@math.missouri.edu

Abstract

Under the assumption of the well-known heuristics of Cohen and Lenstra (and the new extensions we propose) we give proofs of several new properties of class numbers of imaginary quadratic number fields, including theorems on smoothness and normality of their divisors. Some applications in cryptography are also discussed.

www.pphmj.com

1. Introduction

The theory of class numbers $h(-\Delta)$ of imaginary quadratic fields $Q(\sqrt{-\Delta})$, aspects of which we would like to discuss in this paper, has a long history dating back to Gauß and his *Disquisitiones Arithmeticae* [13] of 1801. There he proved that the ring of integers of the imaginary quadratic number field $Q(\sqrt{-\Delta})$ is a principal ideal domain for the

2000 Mathematics Subject Classification: 11E16, 11E45.

Keywords and phrases: divisors of class numbers, Cohen-Lenstra heuristics, Erdös-Kac theorem.

Received April 22, 2005

© 2006 Pushpa Publishing House

following nine values of Δ: $\Delta = 3, 4, 7, 8, 11, 19, 43, 67, 163,$ and he conjectured that these were the only values of Δ for which the class number is 1. This is equivalent to the statement that binary quadratic forms $Ax^2 + Bxy + Cy^2$, with $\Delta = 4AC - B^2$, will always have more than one class if $\Delta > 163$. This tantalizing conjecture was proved by Heegner [14] in 1952. Today two main research problems in the theory of class numbers of imaginary quadratic fields deal with:

(A) General growth properties of class numbers.

(B) Divisibility properties of class numbers.

While these two aspects are related, the more difficult of the two - the group of questions labelled (B) - is something we would like to investigate in detail with the help of Dirichlet's class number formula, Siegel's theorem and the Cohen-Lenstra heuristics.

Let us begin by giving a brief explanation of the role of the two conjectures in the theory.

(A) Gauß himself conjectured that $h(-\Delta) \to \infty$ as $\Delta \to \infty$, a theorem that was proved by Heilbronn only in 1934. Following Dirichlet (see [25]), one defines $L(s, \chi_\Delta)$ as:

$$L(s, \chi_\Delta) := \sum_{n=1}^{\infty} \frac{\chi_\Delta(n)}{n^s} = \prod_p \left(1 - \frac{\chi_\Delta(p)}{p^s}\right)^{-1},$$

where χ_Δ is the Kronecker symbol $\chi_\Delta(n) = (-\Delta/n)$. His class number formula states

$$h(-\Delta) = \frac{\sqrt{\Delta}}{\pi} L(1, \chi_\Delta),$$

and this shows that many growth questions concerning $h(-\Delta)$ could be resolved if we had more information about the behavior of $L(s, \chi_\Delta)$ at the line $s = 1$.

It was Littlewood [17] who proved that

$$L(s, \chi_\Delta) \neq 0 \quad \text{for} \quad \Re(s) > 1/2 \Rightarrow h(-\Delta) >> \frac{\sqrt{|\Delta|}}{\log \log |\Delta|}, \tag{†}$$

www.pphmj.com

i.e., the Riemann Hypothesis (see [20]) can be used to give us a very good lower bound on $h(-\Delta)$. In 1935 Siegel [23] proved - this time unconditionally - that if χ is any real primitive Dirichlet character (mod p), and $\varepsilon > 0$, then we have

$$L(1, \chi) > \frac{C(\varepsilon)}{q^{\varepsilon}} \Rightarrow h(-\Delta) >> \Delta^{\frac{1}{2}-\varepsilon}, \tag{††}$$

as $\Delta \to \infty$. For our counting applications bounds of this type will be sufficient.

(B) Questions concerning distribution and divisibility properties of class numbers are even more difficult. In fact, in many situations it is very hard, if not impossible, then to even conjecture anything plausible about a given class number phenomenon. The remarkable heuristics due to Cohen and Lenstra (see [4, 5] and [2, 3]), which are notoriously unprovable right now, but describe very accurately the most fundamental property of class numbers - the prime divisibility - are an exception to this rule. For class numbers of imaginary quadratic fields we restate a special case of these heuristics, together with our extensions, in the form:

Conjecture 1.1. Let $p > 2$ denote a prime number. Then, in the above notation, we have

(a) (Divisibility) The probability $\mho(p)$ that p divides $h(-\Delta)$ is equal to

$$\Pr[h(-\Delta) \equiv 0 (\bmod p)] := \mho(p) = 1 - \prod_{n=1}^{\infty}\left(1 - \frac{1}{p^n}\right) = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^5} - \frac{1}{p^7} + \cdots. \tag{1}$$

(b) (Uniformity) The property (a) can be refined as follows: As $x \to \infty$,

$$\#\{\Delta \le x : h(-\Delta) \equiv 0 (\bmod p)\} \sim x\mho(p),$$

where p is fixed, or - more generally - a prime that satisfies $p = o(x^{\alpha})$, for all $\alpha > 0$.

(c) (Independence) If p and q are fixed odd primes, and $\mho(pq)$ denotes the probability that both p and q divide $h(-\Delta)$, i.e., $h(-\Delta) \equiv 0 (\bmod pq)$, then $\mho(pq) = \mho(p)\mho(q)$. More generally, the density statement remains true as $x \to \infty$, as long as $p, q = o(x^{\alpha})$, for all $\alpha > 0$.

www.pphmj.com

(d) (Equidistribution) For a given prime p and an integer $0 \leq a < p$, define $\mho_a(p)$ to be the probability that $h(-\Delta) \equiv a (\bmod p)$. Then all moduli $a \neq 0$ are equidistributed, i.e.,

$$\mho_a(p) = \frac{1}{p-1}\left[\frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^5} - \frac{1}{p^7} + L\right]. \tag{2}$$

Remark. The parts (a), (b) and (c) of Conjecture 1.1 implicitly follow from ideas behind the Cohen-Lenstra heuristics, and will be the starting points of most of our investigations. The part (d) is our new addition, which abundant numerical evidence seems to support, see Appendix.

2. Lemmas

Let $\mathbb{N}$ denote the set of all natural numbers and S denote the set of all square-free integers < 0, and let $S(x)$ be the number of $n \in S$, such that $|n| \leq x$. Due to the congruence conditions on fundamental discriminants Δ, we will consider two cases. The set S_1 will be the set of all $\Delta < 0$, such that $\Delta \equiv 1 (\bmod 4)$ and $\Delta \in S$, the set S_2 will be the set of all negative Δ with $\Delta \equiv 0 (\bmod 4)$, $\Delta/4 \equiv 2, 3 (\bmod 4)$ and $\Delta/4 \in S$. Also, we will let $S^* = S_1 \cup S_2$ and $S^*(x)$ be the number of elements $s \in S^*$, with $|s| \leq x$. The symbol $[x]$ will denote the integer part of x, and as usual, we define $\{x\} = x - [x]$ to be the fractional part of x.

The following elementary lemmas will be applied:

Lemma 2.1 (Euler [10, 11])**.**

$$A := \sum_p \frac{1}{p^2} < \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} = 1.64493\ldots$$

and

$$\sum_{y \leq p \leq x} \frac{1}{p^2} < \sum_{y \leq n \leq x} \frac{1}{n^2} < \frac{1}{y}, \tag{3}$$

where the sums are extended over primes, A is an absolute constant and $2 \leq y \leq x$.

www.nphmj.com

Lemma 2.2 (Mertens [18]).

$$\sum_{y \le p \le x} \frac{1}{p} = \log\log x - \log\log y + O(1), \tag{3*}$$

for $3 \le y \le x$, *where the absolute value of the O-constant is smaller than* 1.

Lemma 2.3 (Landau [15]). *If* $3 < y \le x$, *then for a product of* k *distinct primes we have*

$$\sum_{y \le p_1 \cdots p_k \le x} \frac{1}{p_1 \cdots p_k} = (\log\log x)^k - (\log\log y)^k + O_k((\log\log x)^{k-1}), \tag{4}$$

where the absolute value of the constant O_k *is smaller than* k.

Corollary 2.4. *Let* M *be the set of all the integers* m, *fixed factorization of which has exactly* s *primes in the first power*, t *primes in the second power, etc. Then for* $3 \le y \le x$ *we have*

$$\sum_{\substack{m \in M \\ y \le m \le x}} \frac{1}{m} = (\log\log x)^s - (\log\log y)^s + O_A((\log\log x)^{s-1}). \tag{5}$$

Lemma 2.5 (Dirichlet [6]). *The number of square-free numbers below* x *can be estimated as*:

$$S(x) := \sum_{\substack{|n| \le x \\ n \in S}} 1 = \sum_{|n| \le x} \mu(n)^2 = \frac{6}{\pi^2} x + O(\sqrt{x}). \tag{6}$$

Corollary 2.6. *In the above notation*,

$$S_1(x) \sim \frac{1}{3} \cdot \frac{6}{\pi^2} x = \frac{2}{\pi^2} x,\ S_2(x) \sim \frac{2}{3} \cdot \frac{6}{\pi^2} \cdot \frac{x}{4} = \frac{1}{\pi^2} x \Rightarrow S^*(x) = \frac{3}{\pi^2} x + O(\sqrt{x}). \tag{7}$$

The estimate (8) will be used extensively in Section 4.

3. Smoothness of Class Numbers

In this section we show that the difference in the smoothness probability of class numbers of imaginary quadratic number fields and that of ordinary integers is negligible. Some new notation is needed. An integer n is said to be *B-smooth*, if all its prime factors are $\le B$. Let D be a positive integer and H be an upper bound for the class numbers of fundamental discriminants Δ such that $|\Delta| \le D$. Then we prove

www.pphmj.com

Theorem 3.1. *Let $u > 1$ be a fixed real number and let $B = H^{1/u}$ be a smoothness-bound. Let Δ be a randomly chosen fundamental discriminant such that $|\Delta| \leq D$, and let x be a randomly chosen integer such that $1 \leq x \leq H$. Then under the assumption of Conjecture* 1.1, *we have*

$$\lim_{D \to \infty} \frac{\Pr[h(-\Delta) \text{ is } B\text{-smooth}]}{\Pr[x \text{ is } B\text{-smooth}]} = 1. \tag{8}$$

Remark. For the smoothness probability of integers, we have

$$\Pr[x \text{ is } B\text{-smooth}] = 1 - \Pr[x \text{ is not } B\text{-smooth}], \tag{9}$$

where

$$\Pr[x \text{ is not } B\text{-smooth}] = \sum_{i > 0} (-1)^{i-1} S_i, \tag{10}$$

with

$$\lim_{D \to \infty} S_i = \sum_{p_1, \, \ldots, \, p_i} \prod_{p_j} \frac{1}{p_j} \tag{11}$$

such that each product of primes appears only once. Accordingly,

$$\sum_{p_1, \, \ldots, \, p_i} \text{ is a shorthand for } \sum_{\substack{B < p_1 \leq \cdots \leq p_i \\ p_1 \cdots p_i \leq H}},$$

where each S_i is the sum of products that involves exactly i primes. Clearly, we have $S_i = 0$ for all $i > u$.

Expressions similar to (10) and (11) can be found for class numbers if one replaces $1/p$ by $\mho(p)$ in (11), as claimed by the Cohen-Lenstra heuristics, so that

$$\Pr[h(-\Delta) \text{ is not } B\text{-smooth}] = \sum_{i > 0} (-1)^{i-1} T_i, \tag{12}$$

with

$$\lim_{D \to \infty} T_i = \sum_{p_1, \, \ldots, \, p_i} \prod_{p_j} \mho(p_j). \tag{13}$$

www.pphmj.com

Again, $T_i = 0$ for all $i > u$. Let $E_i = T_i - S_i$. Then we prove that $\lim_{D\to\infty} T_i/S_i = 1$ or $\lim_{D\to\infty} E_i/S_i = 0$ for all $i \le u$. This is equivalent to the main result of Theorem 3.1.

Theorem 3.2. *Let* $1 \le i \le u$ *and let* $E_i = T_i - S_i$, *with* T_i *and* S_i *be defined as in equations* (13) *and* (11). *Then* $\lim_{D\to\infty} E_i/S_i = 0$.

Proof. Since $B < p_j$ for all primes p_j and $\mho(p_j) < \frac{1}{p_j}\left(1 + \frac{1}{p_j}\right)$, we have

$$E_i = \sum_{p_1, \dots, p_i}\left(\prod_{p_j}\mho(p_j) - \prod_{p_j}\frac{1}{p_j}\right) = \sum_{p_1, \dots, p_i}\prod_{p_j}\frac{1}{p_j}\left(\prod_{p_j} p_j \cdot \mho(p_j) - 1\right)$$

$$< \sum_{p_1, \dots, p_i}\prod_{p_j}\frac{1}{p_j}\left(\prod_{p_j}\left(1 + \frac{1}{p_j}\right) - 1\right) < \sum_{p_1, \dots, p_i}\prod_{p_j}\frac{1}{p_j}\left(\left(1 + \frac{1}{B}\right)^i - 1\right)$$

$$= S_i\left(\frac{i}{B} + \frac{i(i-1)}{2B^2} + \cdots\right) < S_i \cdot \frac{i+1}{B}.$$

The last inequality holds for sufficiently large B, e.g., $B > i^2$, which is a modest requirement. Therefore, $E_i/S_i < (i+1)/B$ and since $i \le u$ with u fixed, and $B \to \infty$, this proves the result.

Since u is fixed and $i \le u$, $\Pr[h(-\Delta)$ is B-smooth$]$ differs from $\Pr[x$ is B-smooth$]$ only by finitely many vanishing terms. This proves Theorem 3.1.

Remark. Using a similar argument, one might even let u grow modestly.

Remark. Buchmann and Williams demonstrated in [1] how to exploit class groups of imaginary quadratic number fields for cryptography. Since class groups are finite abelian groups, they can be, in principle, used for cryptographic public-key primitives of Diffie-Hellman type. However, no efficient algorithm is known for computing the class number or non-trivial

www.pphmj.com

divisors thereof. Thus, it cannot be efficiently checked whether the class number is smooth or whether it is divisible by a large prime; moreover, it cannot be efficiently checked whether a randomly chosen element of the class group generates the class group or a large subgroup thereof. The only thing one can do is to resort to a probabilistic argument. Specifically, another conjecture of Cohen-Lenstra claims that the class group is cyclic or, with high probability, contains a large cyclic class group. Therefore, a randomly chosen element will most likely generate a large subgroup of the class group. But for cryptographic purposes, this is not sufficient. Instead, it is necessary that the class number is divisible by a large prime. Hence, *upper bounds* for the smoothness probability of class numbers are required.

4. Number of Divisors of Class Numbers

For any positive integer n and any real number y, with $2 \leq y \leq x$, let us define

$$\omega_y(n) = \sum_{\substack{p \mid n \\ p \leq y}} 1 \quad \text{and} \quad \Omega_y(n) = \sum_{\substack{p^a \| n \\ p^a \leq y}} a. \tag{14}$$

www.pphmj.com

For $y = x$ this reduces to the well-known functions $\omega(n)$ and $\Omega(n)$, both of which will be subjects of our investigations. In general, an arithmetic function $f(n)$ is said to have a *normal order* $F(n)$, if for any $\varepsilon > 0$, for almost all $n \leq x$, $(1-\varepsilon)F(n) < f(n) < (1+\varepsilon)F(n)$.

Lemma 4.1 (Turán [26]).

For all $x > 0$,

$$\sum_{n \leq x} (\omega(n) - \log\log x)^2 \ll x \log\log x. \tag{15}$$

Remark. It follows that the normal order of $\omega(n)$ is $\log\log n$ (the same is true for $\Omega(n)$).

Here we prove a Turán-type theorem for class numbers of imaginary quadratic fields. The estimation of the first two moments of $\omega(h(-\Delta))$ is required.

Theorem 4.2. *Let us assume the truth of our Conjecture* 1.1. *Then, for all* $x > 0$,

$$\sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^*}} (\omega(h(-\Delta)) - \log\log x)^2 \ll x \log\log x. \tag{16}$$

Proof. For the first moment, interchanging the order of summation, and by applying (1), Lemma 2.1 and Lemma 2.2, we obtain

$$\begin{aligned}
\mathfrak{M}_y^1(x) := \sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^*}} \omega_y(h(-\Delta)) &= \sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^*}} \sum_{\substack{p|h(-\Delta) \\ p\le y}} 1 = \sum_{p\le y} \sum_{\substack{p|h(-\Delta) \\ 0<|\Delta|\le x}} 1 \\
&= \sum_{p\le y} [S^*(x)\mho(p)] = \sum_{p\le y} S^*(x)\mho(p) - \sum_{p\le y} \{S^*(x)\mho(p)\} \\
&= \sum_{p\le y} S^*(x)\mho(p) + O(\pi(x)) \\
&= \sum_{3\le p\le y} S^*(x)\left(1 - \prod_{n=1}^{\infty}\left(1 - \frac{1}{p^n}\right)\right) + O(x) \\
&= \sum_{3\le p\le y} \left(\frac{S^*(x)}{p} + O\left(\frac{S^*(x)}{p^2}\right)\right) + O(x) \\
&= S^*(x)\log\log y + O(x).
\end{aligned}$$

For the second moment, interchanging the order of summation gives us

$$\begin{aligned}
\mathfrak{M}_y^2(x) := \sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^*}} \omega_y^2(h(-\Delta)) &= \sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^*}} \left(\sum_{\substack{p|h(-\Delta) \\ p\le y}} 1 \right)^2 \\
&= \sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^*}} \sum_{\substack{p|h(-\Delta) \\ p\le y}} \sum_{\substack{q|h(-\Delta) \\ q\le y}} 1 = \sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^*}} \sum_{\substack{p\ne q \\ p,q\le y \\ pq|h(-\Delta)}} 1 + \sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^*}} \sum_{\substack{p|h(-\Delta) \\ p\le y}} 1 \\
&= \sum_{\substack{p\ne q \\ p,q\le y \\ pq\le x}} \sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^* \\ pq|h(-\Delta)}} 1 + \sum_{\substack{0<|\Delta|\le x \\ \Delta\in S^*}} \omega_y(h(-\Delta)).
\end{aligned}$$

www.pphmj.com

And therefore, using Lemma 2.1 and Corollary 2.4, we obtain

$$\mathfrak{M}_y^2(x) = \sum_{\substack{3 \le p < q \le y \\ pq \le h(-\Delta)}} \left[S^*(x)\left(1 - \prod_{n=1}^{\infty}\left(1 - \frac{1}{p^n}\right)\right)\left(1 - \prod_{n=1}^{\infty}\left(1 - \frac{1}{q^n}\right)\right)\right] + O(x \log\log y)$$

$$= \sum_{\substack{3 \le p < q \le y \\ pq \le h(-\Delta)}} S^*(x)\left(1 - \prod_{n=1}^{\infty}\left(1 - \frac{1}{p^n}\right)\right)\left(1 - \prod_{n=1}^{\infty}\left(1 - \frac{1}{q^n}\right)\right) + O(x \log\log y)$$

$$= \sum_{\substack{3 \le p < q \le y \\ pq \le x}} \frac{S^*(x)}{pq} + O\left(\sum_{3 \le p < q \le y} \frac{S^*(x)}{pq^2}\right)$$

$$+ O\left(\sum_{3 \le p < q \le y} \frac{S^*(x)}{p^2 q}\right) + O(x \log\log y)$$

$$= S^*(x)(\log\log y)^2 + O(x \log\log y).$$

From unconditional lower and upper bounds similar to (††) it follows that choosing, in estimates for $\mathfrak{M}_y^1(x)$ and $\mathfrak{M}_y^2(x)$, the parameter y as $y = x^{\delta}$, for a constant $\delta < \frac{1}{2} - \varepsilon$, will give

$$\mathfrak{T}(x) := \sum_{\substack{0 < |\Delta| \le x \\ \Delta \in S^*}} (\omega(h(-\Delta)) - \log\log x)^2$$

$$= \sum_{\substack{0 < |\Delta| \le x \\ \Delta \in S^*}} \omega^2(h(-\Delta)) - 2\log\log x \sum_{\substack{0 < |\Delta| \le x \\ \Delta \in S^*}} \omega(h(-\Delta)) + (\log\log x)^2 \sum_{\substack{0 < |\Delta| \le x \\ \Delta \in S^*}} 1$$

$$= 2S^*(x)(\log\log x)^2 + O(x \log\log x) - 2\log\log x(S^*(x)\log\log x + O(x))$$

$$= O(x \log\log x).$$

This proves Theorem 4.2.

Remark. From the first moment estimate alone it is easy to deduce that the average number of prime factors of $h(-\Delta)$, for $0 < |\Delta| \le x$, is

www.pphmj.com

simply

$$\frac{1}{S^*(x)} \sum_{\substack{0<|\Delta|\le x \\ \Delta \in S^*}} \omega(h(-\Delta)) \to \log\log x, \text{ as } x \to \infty. \tag{17}$$

Estimating the higher moments can be done by using methods analogous to those employed in the proof of our Theorem 4.2. And with the help of the powerful Fréchet-Shohat theorem (see [12]) this in fact yields a more general result:

Theorem 4.3. *Assuming the Conjecture* 1.1, *as* $x \to \infty$, *we have*

$$\#\left\{0 < |\Delta| \le x : \Delta \in S^*,\ A \le \frac{\omega(h(-\Delta)) - \log\log x}{\sqrt{\log\log x}} \le B\right\}$$

$$\sim \frac{3x}{\sqrt{2}\pi^{5/2}} \int_A^B e^{-t^2/2} dt. \tag{18}$$

Not unlike most results discussed in [19] and [21], this is another example of a non-abelian extension of the fundamental Erdös-Kac theorem [9].

5. Open Problems

(1) The most natural extension of Conjecture 1.1 seems to be the one concerning arbitrary composite divisors. Using the special case of d being a square-free integer as a guide, the independence of probabilities of each of its prime factors dividing a class number translates into: $\mho(d) = \prod_{p|d} \mho(p)$. In cases when $p^\alpha \| d$, for some $\alpha \ge 2$, the assumption of the change of variable $p \to p^\alpha$ in the formula for $\mho(p)$ seems the most logical one. This would give us:

Conjecture 5.1. For any $d \in \mathbb{N}$, we have

$$\Pr[d \mid h(-\Delta)] := \mho(d) = \prod_{p^\alpha \| d} \left[1 - \prod_{n=1}^{\infty}\left(1 - \frac{1}{(p^\alpha)^n}\right)\right]. \tag{19}$$

www.pphmj.com

In other words, if $d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then

$$\begin{aligned}
\mho(d) &= \left(\frac{1}{p_1^{\alpha_1}} + \frac{1}{p_1^{2\alpha_1}} - \frac{1}{p_1^{5\alpha_1}} + \cdots \right) \\
&\quad \cdot \left(\frac{1}{p_2^{\alpha_2}} + \frac{1}{p_2^{2\alpha_2}} - \frac{1}{p_2^{5\alpha_2}} + \cdots \right) \cdots \left(\frac{1}{p_k^{\alpha_k}} + \frac{1}{p_k^{2\alpha_k}} + \cdots \right) \\
&= \frac{1}{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} + \frac{1}{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} \left(\sum_{1 \le i \le k} \frac{1}{p_i^{\alpha_i}} \right) \\
&\quad + \frac{1}{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} \left(\sum_{1 \le i, j \le k} \frac{1}{p_i^{\alpha_i} p_j^{\alpha_j}} \right) + \cdots \\
&= \frac{1}{d} + \frac{1}{d} \left(\sum_{p^{\alpha} \| d} \frac{1}{p^{\alpha}} \right) + \frac{1}{d} \left(\sum_{\substack{p^{\alpha} \| d \\ q^{\beta} \| d}} \frac{1}{p^{\alpha} q^{\beta}} \right) + \cdots = \frac{1}{d} + O\left(\frac{1}{d^{\kappa}} \right),
\end{aligned}$$

where one should expect $\kappa \ge 1 + \omega(d)^{-1}$. Now, since for most d we have $\omega(d) < \log d / \log\log d$, it follows that $\log\log d < \omega(d)^{-1} \log d$, and so $\log d < d^{\omega(d)^{-1}}$. This implies

$$\left| \mho(d) - \frac{1}{d} \right| < \frac{1}{d \log d}. \tag{20}$$

(2) However, on average better error terms should be expected. Precise information concerning these error terms could then lead to estimates such as:

$$\mathfrak{M}^1(x, \sigma) := \sum_{\substack{0 < |\Delta| \le x \\ \Delta \in S^*}} \sigma(h(-\Delta)) = \sum_{\substack{0 < |\Delta| \le x \\ \Delta \in S^*}} \sum_{d | h(-\Delta)} d \sim Ax^2, \text{ and}$$

$$\mathfrak{M}^1(x, \phi) := \sum_{\substack{0 < |\Delta| \le x \\ \Delta \in S^*}} \phi(h(-\Delta)) = \sum_{\substack{0 < |\Delta| \le x \\ \Delta \in S^*}} \sum_{d | h(-\Delta)} \mu(d) \frac{h(-\Delta)}{d} \sim Bx^2.$$

www.pphmj.com

(3) Another fundamental arithmetical property of integers one should investigate is primality. Although it is unlikely that minor modifications of the above methods would be sufficient to resolve this question, the following conjecture seems plausible:

Conjecture 5.2. Let $\pi^*(x)$ be the number of fundamental discriminants Δ, with $0 < |\Delta| \le x$, for which $h(-\Delta)$ is a prime number. Then there exists a constant Θ, such that

$$\pi^*(x) \sim \mathrm{li}(S^*(x)) \sim \Theta \frac{x}{\log x} \text{ as } x \to \infty. \tag{21}$$

Acknowledgements

We would like to thank the referee for helpful comments and Hugh Williams (University of Calgary) for his continuing support.

References

[1] J. Buchmann and H. C. Williams, A key-exchange system based on imaginary quadratic fields, J. Cryptology 1(3) (1988), 107-118.

[2] H. Cohen, A course in computational algebraic number theory, Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993.

[3] H. Cohen, Advanced topics in computational number theory, Graduate Texts in Mathematics, 193, Springer-Verlag, New York, 2000.

[4] H. Cohen and H. W. Lenstra, Heuristics on class groups, Number Theory, Springer-Verlag, New York, 1982, pp. 26-36.

[5] H. Cohen and H. W. Lenstra, Heuristics on class groups of number fields, Number Theory, Noordwijkerhout, 1983, pp. 33-62.

[6] P. G. L. Dirichlet, Abhand. Ak. Wiss., Berlin, 1849, pp. 69-83.

[7] W. Duke, Extreme values of Artin L-functions and class numbers, Compositio Math. 135 (2003), 103-115.

[8] P. Erdös, On the normal order of prime factors of $p-1$ and some related problems concerning Euler's φ-function, Quarterly J. Math. 6 (1935), 205-213.

[9] P. Erdös and M. Kac, The Gaussian law of errors in the theory of additive number-theoretic functions, Amer. J. Math. 62 (1940), 738-742.

[10] L. Euler, Variae observationes circa series infinitas, Comm. Acad. Sci. Petrop. 9 (1737), 222-236.

www.pphmj.com

[11] L. Euler, Introductio in Analysin Infinitorum, Chapter 15, Lausanne, 1748.

[12] M. Fréchet and J. Shohat, A proof of the generalized second-limit theorem in the theory of probability, Trans. Amer. Math. Soc. 33(2) (1931), 533-543.

[13] C. F. Gauß, Disquisitiones Arithmeticae, G. Fleischer, Leipzig, 1801.

[14] K. Heegner, Diophantische analysis und modulfunktionen, Math. Z. 56 (1952), 227-253.

[15] E. Landau, Sur quelques problèmes relatifs à la distribution des nombres premiers, Bull. Soc. Math. France 28 (1900), 25-38.

[16] J. E. Littlewood, Sur la distribution des nombres premiers, C. R. Acad. Sci. Paris 158 (1914), 1869-1872.

[17] J. E. Littlewood, On the class number of the corpus $P(\sqrt{-k})$, Collected Papers, Vol. 1, Clarendon Press, Oxford, 1982.

[18] F. Mertens, Ein Beitrag zur analytischen Zahlentheorie, J. für Reine Angew. Math. 78 (1874), 46-62.

[19] R. Murty and F. Saidak, Non-abelian generalizations of the Erdös-Kac theorem, Canad. J. Math. 56(2) (2004), 356-372.

[20] B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Grösse, 1859, Collected Works, Teubner, Leipzig, 1892, p. 145.

[21] F. Saidak, New Erdös-Kac type theorems, Arch. Math. (Basel) 85 (2005), 345-361.

[22] C. P. Schnorr and H. W. Lenstra, A Monte Carlo factoring algorithm with linear storage, Math. Comp. 43(167) (1984), 289-311.

[23] C. L. Siegel, Über die Classenzahl quadratischer Zahlkörper, Acta Arith. 1 (1935), 83-86.

[24] H. J. J. te Riele and H. C. Williams, New computations concerning the Cohen-Lenstra heuristics, preprint.

[25] E. Titchmarsh, The Theory of the Riemann Zeta-function, 2nd ed., Revised by D. R. Heath-Brown, Oxford Univ. Press, Oxford, 1986.

[26] P. Turán, On a theorem of Hardy and Ramanujan, J. London Math. Soc. 9 (1934), 274-276.

[27] L. C. Washington, Some remarks on Cohen-Lenstra heuristics, Math. Comp. 47(176) (1986), 741-747.

www.ppmj.com

Appendix

Class numbers distributed over residue classes modulo primes p, with $2 < p < 30$ and $0 < -\Delta \leq 2^{28}$. (The number of fundamental discriminants Δ for $0 < -\Delta \leq 2^{28}$ is 81 594 634.)

Class numbers modulo 3

r	$\lvert\{h_\Delta : h_\Delta \equiv r\}\rvert$	ratio
0	34689718	0.425147
1	23453706	0.287442
2	23451210	0.287411

Class numbers modulo 5

r	$\lvert\{h_\Delta : h_\Delta \equiv r\}\rvert$	ratio
0	19378805	0.237501
1	15549859	0.190575
2	15551471	0.190594
3	15556711	0.190659
4	15557788	0.190672

Class numbers modulo 7

r	$\lvert\{h_\Delta : h_\Delta \equiv r\}\rvert$	ratio
0	13239196	0.162256
1	11394295	0.139645
2	11387680	0.139564
3	11394471	0.139647
4	11390686	0.139601
5	11394647	0.139649
6	11393659	0.139637

www.pphmj.com

Class numbers modulo 11

r	$\lvert\{h_\Delta : h_\Delta \equiv r\}\rvert$	ratio
0	8034025	0.098463
1	7356266	0.090156
2	7354544	0.090135
3	7357121	0.090167
4	7354471	0.090134
5	7357417	0.090170
6	7361052	0.090215
7	7355405	0.090146
8	7357165	0.090167
9	7354244	0.090131
10	7352924	0.090115

Class numbers modulo 13

r	$\lvert\{h_\Delta : h_\Delta \equiv r\}\rvert$	ratio
0	6701937	0.082137
1	6240173	0.076478
2	6240889	0.076487
3	6246710	0.076558
4	6239184	0.076466
5	6239812	0.076473
6	6238677	0.076459
7	6241920	0.076499

www.pphmj.com

8	6241192	0.076490
9	6239307	0.076467
10	6244486	0.076531
11	6239754	0.076473
12	6240593	0.076483

Class numbers modulo 17

r	$\|\{h_\Delta : h_\Delta \equiv r\}\|$	ratio
0	5035875	0.061718
1	4788327	0.058684
2	4783983	0.058631
3	4783129	0.058621
4	4785807	0.058653
5	4780801	0.058592
6	4784558	0.058638
7	4783602	0.058626
8	4783894	0.058630
9	4789743	0.058702
10	4783779	0.058629
11	4785142	0.058645
12	4785824	0.058654
13	4785692	0.058652
14	4782903	0.058618
15	4786811	0.058666
16	4784764	0.058641

www.pphmj.com

Class numbers modulo 29

r	$\lvert \{h_\Delta : h_\Delta \equiv r\} \rvert$	ratio
0	2864412	0.035105
1	2812552	0.034470
2	2808860	0.034425
3	2813833	0.034486
4	2809880	0.034437
5	2813562	0.034482
6	2811339	0.034455
7	2812631	0.034471
8	2815450	0.034505
9	2815420	0.034505
10	2811288	0.034454
11	2811522	0.034457
12	2816226	0.034515
13	2814790	0.034497
14	2810376	0.034443
15	2810169	0.034441
16	2808037	0.034414
17	2811677	0.034459
18	2807920	0.034413
19	2809479	0.034432
20	2815502	0.034506
21	2809836	0.034437
22	2812796	0.034473
23	2811959	0.034463

www.pphmj.com

24	2808975	0.034426
25	2810773	0.034448
26	2811934	0.034462
27	2813283	0.034479
28	2810153	0.034440

Class numbers modulo 19

r	$\vert\{h_\Delta : h_\Delta \equiv r\}\vert$	ratio
0	4467172	0.054748
1	4285531	0.052522
2	4286500	0.052534
3	4284351	0.052508
4	4282174	0.052481
5	4288423	0.052558
6	4284006	0.052504
7	4284048	0.052504
8	4285689	0.052524
9	4288849	0.052563
10	4283502	0.052497
11	4284986	0.052516
12	4282311	0.052483
13	4281232	0.052470
14	4283882	0.052502
15	4286770	0.052537
16	4284237	0.052506
17	4286552	0.052535
18	4284419	0.052509

www.pphmj.com

Class numbers modulo 23

r	$\lvert\{h_\Delta : h_\Delta \equiv r\}\rvert$	ratio
0	3656305	0.044811
1	3544348	0.043438
2	3540027	0.043386
3	3544626	0.043442
4	3544497	0.043440
5	3545250	0.043450
6	3541255	0.043401
7	3542184	0.043412
8	3543479	0.043428
9	3541454	0.043403
10	3544149	0.043436
11	3543545	0.043429
12	3542744	0.043419
13	3540607	0.043393
14	3544661	0.043442
15	3547696	0.043480
16	3542390	0.043414
17	3540010	0.043385
18	3541053	0.043398
19	3538114	0.043362
20	3542505	0.043416
21	3542606	0.043417
22	3541129	0.043399

■

www.pphmj.com