CONJECTURES ON THE DISTRIBUTION BEHAVIOR OF THE CLASS NUMBERS OF CERTAIN REAL QUADRATIC NUMBER FIELDS

JINWEN XU

Abstract. Given a random real quadratic field from \(\{Q(\sqrt{p}) \mid p \text{ primes}\}\), the conjectural probability \(P(h = q)\) that it has class number \(q\) is given for all positive odd integers \(q\). Some related conjectures in [4], known as the Cohen-Lenstra heuristic, are given here as corollaries. These results suggest that the set of real quadratic number fields may have some natural hierarchical structures.

In this article, we shall study the distribution behavior of the class numbers of real quadratic number fields in the set \(\mathbb{P} := \{Q(\sqrt{p}) \mid p \text{ primes}\}\). These class numbers are all odd integers according to [1, Sec.3.8 (Theorem 8)]. Let \(P(h = q)\) stand for the probability that a randomly chosen member from \(\mathbb{P}\) has class number \(q\), where \(q\) is any positive odd integer. In section 1, the conjectural value of \(P(h = q)/P(h = 1)\) is given in conjecture 1.1. Then in section 2, \(P(h = 1)\) is calculated based on conjecture 1.1, alongside with some corollaries. Finally, the current status of this conjecture and some ideas for future work, including some similar observations to the set \(\mathbb{A} := \{Q(\sqrt{d}) \mid d > 0 \text{ square free}\}\), are given in the last section.

1. The main conjecture

First we define \(P(h = q)\) precisely, and make an important assumption.

Definition 1.1. Denote the \(i\)-th prime number as \(p_i\). Define

\[
P(h = q) := \lim_{x \to \infty} \frac{\# \{i \mid h(Q(\sqrt{p_i})) = q, i \leq x\}}{x}.
\]

Assumption. \(P(h = q)\) exists for all positive odd integers \(q\).

For convenience, denote \(P(h = 1)\) by \(P_0\), and write

\[
P(h = q) = \lambda_q P_0,
\]

where \(\lambda_q\) is a constant depending on \(q\). In this setting, one has \(\lambda_1 = 1\).

Now we can state the main conjecture, which gives the conjectural value of \(\lambda_q\):

Conjecture 1.1. (1) For any odd prime number \(p\), one has:

\[
\lambda_p = \frac{1}{p(p-1)}
\]

\[
\lambda_{p^n} = \lambda_{p^{n-1}}(p^{\lfloor n/2 \rfloor} - 1)^{-1}, \quad n \geq 2.
\]

(2) For \(q = p_1^{r_1} \cdots p_t^{r_t}\), one has:

\[
\lambda_q = \lambda_{p_1^{r_1}} \cdots \lambda_{p_t^{r_t}}.
\]

Remark 1. \(\lambda\) is an arithmetic function in \(q\). Part (2) of conjecture 1.1 says that \(\lambda\) is multiplicative.

Remark 2. Part (2) of conjecture 1.1 is actually a result of the assumption combined with part (1):

\[
P(h = q) = \left( \prod_{m=1}^{t} P\left(\{p_m^r \mid h\} \cap \{p_m^{r+1} \mid h\}\right) \right) P(p \mid h \text{ for all other } p)
\]

\[
= \left( \prod_{m=1}^{t} \frac{P(h = p_m^r)}{P(p_m \neq p^{r+1} \mid h)} \right) P(p \mid h \text{ for all other } p)
\]

\[
= \left( \prod_{m=1}^{t} \frac{\lambda_{p_m^r}}{P(p_m \neq p^{r+1} \mid h)} \right) P(p \mid h \text{ for all other } p)
\]

\[
= \left( \prod_{m=1}^{t} \lambda_{p_m^r} P(p_m \mid h) \right) P(p \mid h \text{ for all other } p) = \left( \prod_{m=1}^{t} \lambda_{p_m^r} \right) P_0.
\]
Thus, and thus finally which is precisely

\[ \sum_{k=0}^{\infty} \frac{1}{(2k+1)^2} = \frac{\pi^2}{8} - 1. \]

Below is a table illustrating conjecture 1.1:

| \( q \) | \( \mathbb{P}(h = q) / \mathbb{P}_0 \) | \( \mathbb{P}(h = q) / \mathbb{P}_0 \) | \( \mathbb{P}(h = q) / \mathbb{P}_0 \) | \( \mathbb{P}(h = q) / \mathbb{P}_0 \) | \( \mathbb{P}(h = q) / \mathbb{P}_0 \) |
|---|---|---|---|---|---|
| 1 | 1 | 11 | 1/110 | 21 | 1/252 | 31 | 1/930 | 41 | 1/1640 |
| 3 | 1/6 | 13 | 1/156 | 23 | 1/506 | 33 | 1/660 | 43 | 1/1806 |
| 5 | 1/20 | 15 | 1/120 | 25 | 1/480 | 35 | 1/840 | 45 | 1/960 |
| 7 | 1/42 | 17 | 1/272 | 27 | 1/384 | 37 | 1/1332 | 47 | 1/2162 |
| 9 | 1/48 | 19 | 1/342 | 29 | 1/812 | 39 | 1/936 | 49 | 1/2016 |

In the next section, we shall calculate \( \mathbb{P}_0 \) based on this conjecture.

2. Calculation of \( \mathbb{P}_0 \) and some corollaries

Since \( \mathbb{P}_0 = \prod_{p \geq 3} \mathbb{P}(p \nmid h) \), where \( p \) runs over all odd prime numbers, we only need to know \( \mathbb{P}(p \nmid h) \).

Fix a prime number \( p \). One clearly has

\[ \mathbb{P}(h \in \{p^k\}) = \mathbb{P}(p \mid h) \mathbb{P}(p \neq p' \mid h). \]

On the other hand, according to conjecture 1.1,

\[ \mathbb{P}(h \in \{p^k\}) = \sum_k \lambda_{p^k} \mathbb{P}_0 = \sum_k \lambda_{p^k} \mathbb{P}(p \nmid h) \mathbb{P}(p \neq p' \nmid h). \]

Thus,

\[ \sum_k \lambda_{p^k} = \frac{\mathbb{P}(p \mid h)}{\mathbb{P}(p \nmid h)} = \frac{1 - \mathbb{P}(p \nmid h)}{\mathbb{P}(p \nmid h)} \]

Now we write \( \sum_k \lambda_{p^k} \) in another way. Beginning with the equality\(^1\)

\[ \prod_{k \geq 1} (1 - p^{-k})^{-1} = 1 + \frac{1}{p-1} \left( 1 + \frac{1}{p-1} \left( 1 + \frac{1}{p^2-1} \left( 1 + \frac{1}{p^2-1} \left( 1 + \frac{1}{p^3-1} \left( 1 + \frac{1}{p^3-1} \left( 1 + \cdots \right) \right) \right) \right) \right) \]

one has:

\[ \prod_{k \geq 1} (1 - p^{-k})^{-1} - \frac{p}{p-1} = \left( \frac{1}{p-1} \right)^2 \left( 1 + \frac{1}{p^2-1} \left( 1 + \frac{1}{p^2-1} \left( 1 + \frac{1}{p^3-1} \left( 1 + \frac{1}{p^3-1} \left( 1 + \cdots \right) \right) \right) \right) \]

\[ \iff \prod_{k \geq 2} (1 - p^{-k})^{-1} - 1 = \frac{1}{p(p-1)} \left( 1 + \frac{1}{p^2-1} \left( 1 + \frac{1}{p^2-1} \left( 1 + \frac{1}{p^3-1} \left( 1 + \frac{1}{p^3-1} \left( 1 + \cdots \right) \right) \right) \right) \]

which is precisely

\[ \frac{1 - \prod_{k \geq 2} (1 - p^{-k})}{\prod_{k \geq 2} (1 - p^{-k})} = \sum_k \lambda_{p^k}. \]

Compare eqs. (2.1) and (2.2), one gets

**Corollary 2.1.** The conjectural probability that an odd prime number \( p_0 \) does not divide the class number of \( \mathbb{Q}(\sqrt{\mathfrak{p}}) \) is

\[ \mathbb{P}(p_0 \nmid h) = \prod_{k \geq 2} (1 - p_0^{-k}). \]

And thus finally

**Corollary 2.2.** The conjectural probability of \( \mathbb{Q}(\sqrt{\mathfrak{p}}) \) has class number one is

\[ \mathbb{P}_0 = \prod_{p \geq 3} \prod_{k \geq 2} (1 - p^{-k}) \]

\[ = \prod_{k \geq 2} \left( 1 - 2^{-k} \zeta(k) \right)^{-1} \approx 0.75446. \]

Corollaries 2.1 and 2.2 coincide with conjectures (C7) and (C11) in [4]. Here we arrived at those results from a different starting point.

\(^1\)The author was not able to find a reference for this, but it can be proved simply by checking that the ratio of L.H.S and R.H.S tends to 1.
3. Status of the conjecture and some remarks for further work

3.1. Current status. Conjecture 1.1 says that over 75% of real quadratic fields in \( \{ \mathbb{Q}(\sqrt{d}) \mid d \text{ prime} \} \) have class number one, thus implies Gauss’s class number conjecture for real quadratic fields, which states that there are infinitely many such fields with class number one. We are far from proving this yet. Numerical calculations dating back to late 1980s have showed that the actual ratio tends to \( P_0 \) very slowly, see [5, Figure 4.1].

One related known result is that the number of real quadratic fields with absolute discriminant \( \leq X \) and class number divisible by \( q \) is \( \gg X^{(1/q) - \varepsilon} \) for all \( \varepsilon > 0 \) (Yu, [6]); better estimation for small class number cases can be found in [2, 3].

3.2. On the set \( A \) of all real quadratic fields. In this subsection, we briefly discuss some observations on the class numbers of members in \( A = \{ \mathbb{Q}(\sqrt{d}) \mid d > 0 \text{ square free} \} \). Similarly to the previous discussion, define \( P_i \) to be the probability that a randomly chosen member from \( A \) has class number \( i \), and assume that \( P_i \) exists for all \( i \geq 1 \). Then numerical result suggests that:

**Conjecture 3.1.** For positive odd integers \( q \), \( P_q/P_1 = \lambda_q \).

**Conjecture 3.2.** For any even number \( n > 0 \), write \( n = 2^r q \), where \( q \) is an odd number. Then \( P_n = \lambda_q P_{2^r} \).

With the conjectures above, one can deduce that:

**Corollary 3.3.** \( P_0 = \sum_{k=0}^\infty P_{2^k} \).

*Proof*. \[
1 - (P_1 + P_2 + P_4 + P_8 + P_{16} + \cdots) = (\lambda_3 + \lambda_5 + \lambda_7 + \lambda_9 + \cdots)(P_1 + P_2 + P_4 + P_8 + P_{16} + \cdots) \quad \text{(by conjecture 3.1 and 3.2)}
\]
\[
= (1/P_0 - 1)(P_1 + P_2 + P_4 + P_8 + P_{16} + \cdots) \quad \text{(by conjecture 1.1)}
\]
Thus \( (1/P_0)(P_1 + P_2 + P_4 + P_8 + P_{16} + \cdots) = 1 \), hence \( P_0 = \sum_{k=0}^\infty P_{2^k} \). \( \square \)

Despite the (conjectural) summation formula above, the relationship among \( P_1, P_2, P_4, P_8, \) etc. is currently unknown. However, from the numerical calculation, it seems that \( P_2 > P_1 \), which suggests that properties of the even part of class groups might be different from those of the odd part.

3.3. A heuristic assertion. According to conjecture 1.1, for any odd integers \( q_1, q_2 \) with \( q_1 \mid q_2 \), the ratio \( \lambda_{p_1}/\lambda_{p_2} \) is an integer. This suggests that the set \( P = \{ \mathbb{Q}(\sqrt{d}) \mid d \text{ prime} \} \) may have some natural hierarchical structures.

3.3.1. An illustration. Consider \( \lambda_1/\lambda_3 = 6 \), it is reasonable to think of this as if for any member in \( P \) with class number three, there are six members of class number one “growing” out of it, as illustrated below:

Here \( K_3 \) represents some real quadratic field in \( P \) with class number three, and \( K_i \) represents those with class number one that is related to \( K_3 \) in this hypothetical hierarchical structure.

If one regards class number as a measurement of the distance from the ring of integers in this number field to an UFD, then one may interpret the meaning of this hierarchical structure as: the obstacles for the integer factorization in \( K_3 \) are contributed by those \( K_i \), which are all closer to an UFD related to it. More specifically, this means that the fundamental information about factorization contained in the inner structures of \( K_i \) are somehow kept and embedded in that of \( K_3 \). Thus, for example, one may expect the classical notion of ideals to be part of this new hypothetical structure.

The example above demonstrates only a small piece in the hierarchical structure. The global picture would be like patching together infinitely many such pieces with 1 and 3 replaced by \( q_1 \mid q_2 \). In this process, as composite numbers such as 27 (of form \( p^3 \)), 35 (of form \( pq \)) and the others coming into the picture, an intriguing global structure emerges, for which conjecture 1.1 only describes the general graph-theoretic information.

3.3.2. The “eigenvalue”. On the other hand, thinking along this direction, the equality, or at least some quantities in the equality:

\[
\left( 1 + \frac{1}{p-1} \right) \left( 1 + \frac{1}{p-1} \right) \left( 1 + \frac{1}{p^2-1} \right) \cdots
\]
\[
= 1 + \frac{1}{p-1} \left( 1 + \frac{1}{p-1} \right) \left( 1 + \frac{1}{p^2-1} \right) \left( 1 + \frac{1}{p^2-1} \right) \left( 1 + \frac{1}{p^3-1} \right) \cdots
\]
may be seen as the “signature” or “eigenvalue” of this particular hierarchical structure corresponding to \( \mathfrak{P} \),
encoding its degree information. Previously we have only considered the set \( \mathfrak{P} \), but one can reasonably speculate
that this kind of hierarchical structure exists in many other context, and each corresponds to a beautiful equality
of its own. This suggests, from another point of view, that the study of it might be fruitful.

3.3.3. On the construction. To really construct such a structure, [4, (C11)] suggests that the order at each vertex
may have something to do with the order of the corresponding automorphism groups, which offers a clue to
get started. Currently we do not know much about the arrangement of the vertices or when shall two of them
connected, and the above heuristic assertion on the hierarchical structure may still be a little over-simplified.
However, once this hierarchical structure is successfully constructed and its properties established, conjecture 1.1
follows immediately (although the proof itself would appear to be non-constructive).

It should be pointed out, however, that the set of complex quadratic fields does not seem to share a similar
hierarchical structure, since the class number \( h \to \infty \) as the discriminant tends to infinity. The author believes
that it is due to the presence of \( \sqrt{-1} \) that somehow causes the corresponding hierarchical structure “collapse”.

3.4. Final remarks. All these conjectures are obtained by merely observing several small class number tables of
size \( \sim 10^6 \). Thus it is possible that the conjectural value \( \lambda_{p^k} \) for large \( k \) is wrong (the exponent \( \lfloor n/2 + 1 \rfloor \) seems
to be somewhat mysterious). However, the author believes that even if there are some flaws in the conjectures,
the heuristic assertion above should still make some sense.

References

[1] Z. I. Borond & I. R. Shafarevich, Number Theory, Pure and Applied Mathematics, vol. 20, Academic Press Inc, 1966.
[2] D. Byeon & E. Koh, Real quadratic fields with class number divisible by 3, Manuscripta Mathematica 111, 2003, pp. 261–263.
[3] D. Byeon, Real quadratic fields with class number divisible by 5 or 7, Manuscripta Mathematica 120, 2006, pp. 211-215.
[4] H. Cohen & H. W. Lenstra, Jr., ‘Heuristics on class groups of number fields’, Number Theory (Noordwijkerhout, 1983), Lecture Notes in
Mathematics, vol. 1068, Springer-Verlag, Berlin and New York, 1984, pp. 33-62.
[5] A. J. Stephens & H. C. Williams, Computation of real quadratic fields with class number one. Math. Comp. 51, 1988, pp. 809-824.
[6] G. Yu, A note on the divisibility of class numbers of real quadratic fields. J. Number Theory 97, 2002, pp. 35-44.