Class Numbers of Imaginary Quadratic Orders in the Polynomial Hierarchy

Frank Vega

Information Physics Institute, 840 W 67th St, Hialeah, FL 33012, USA

Abstract

For $d \geq 3$ with $-d \equiv 0, 1 \pmod 4$, let $h(-d)$ be the number of classes of primitive positive definite binary quadratic forms of discriminant $-d$. We prove that $d \mapsto h(-d)$ is computable in deterministic polynomial time with an oracle for a language in the second level Σ_2^{P} of the polynomial hierarchy. The proof uses only reduction theory of binary quadratic forms, Lagrange's theorem and Hermite normal forms; it does not assume the generalized Riemann hypothesis, does not take a generating set of the class group as input, and uses no randomness. A Σ_2^{P} oracle finds a generating set of $O(\log d)$ forms, and an NP oracle then determines the lattice of relations, whose index is $h(-d)$. Consequently, if P = NP, class numbers of imaginary quadratic fields are computable in polynomial time. As an application, the number D_n of representations of n by the ternary form $8x^2 + 2y^2 + 16z^2$ in Tunnell's congruent number criterion equals $2h(-4n)$ for square-free $n \equiv 2 \pmod 8$ and vanishes for square-free $n \equiv 6 \pmod 8$; hence D_n lies in $\mathrm{FP}^{\Sigma_2^{\mathrm{P}}}$ on even square-free n, and an exact counting reduction from #SAT to D_n would collapse the polynomial hierarchy to Δ_3^{P}.

Keywords: class numbers, binary quadratic forms, polynomial hierarchy, counting complexity, Tunnell's theorem, congruent numbers, Hermite normal form, black-box groups
2020 MSC: 11Y40, 11R29, 68Q15, 11E16, 11E20

1. Introduction

For an integer $d \geq 3$ with $-d \equiv 0, 1 \pmod 4$, let $h(-d)$ be the number of $\mathrm{SL}_2(\mathbb{Z})$-classes of primitive positive definite binary quadratic forms of discriminant $-d$; when $-d$ is a fundamental discriminant, $h(-d)$ is the class number of $\mathbb{Q}(\sqrt{-d})$. Computing $h(-d)$ from the binary encoding of d is a classical problem of computational number theory. Shanks's baby-step giant-step method and its refinements compute it in time exponential in $\log d$ [1]; under the generalized Riemann hypothesis (GRH), Hafner and McCurley gave a subexponential algorithm [2]; and under GRH the class group is generated by forms of norm $O(\log^2 d)$ [3], so that Watrous's quantum algorithm for the order of a solvable black-box group [4] computes $h(-d)$ in quantum polynomial time.

The form class group $\mathrm{Cl}(-d)$ is an abelian group whose elements have unique polynomial-size encodings, the reduced forms, and whose operation is computable in polynomial time. For black-box groups given by a list of generators, Babai and Szemerédi [5] proved that membership lies in NP, and Babai [6] proved that order verification lies in $\mathrm{AM} \cap \mathrm{coAM}$. These results take a generating set as part of the input. No small generating set of $\mathrm{Cl}(-d)$ is known to be computable without GRH.

In this paper we prove that $d \mapsto h(-d)$ is computable in deterministic polynomial time with an oracle for a language in Σ_2^{P} (Theorem 3.1). The proof is elementary: it uses only reduction theory of binary quadratic forms, Lagrange's theorem, and Hermite normal forms of integer matrices. It does not assume GRH, does not take a generating set as input, and uses no interactive proofs or randomness. Its consequences are the following.

1. If P = NP, then class numbers of imaginary quadratic orders are computable in deterministic polynomial time (Corollary 3.2).

Email address: vega.frank@gmail.com (Frank Vega)

2. Let D_n be the number of representations of n by the ternary form $8x^2 + 2y^2 + 16z^2$ that appears in Tunnell's congruent number criterion [7]. For square-free $n \equiv 2 \pmod 8$ one has $D_n = 2h(-4n)$ (Proposition 4.2), and $D_n = 0$ for square-free $n \equiv 6 \pmod 8$ (Lemma 4.1). Hence $n \mapsto D_n$ on even square-free n lies in $\mathrm{FP}^{\Sigma_2^{\mathrm{P}}}$ (Corollary 4.3).
3. An exact counting reduction from #SAT to D_n, computable in polynomial time with an NP oracle, would imply $\#\mathrm{P} \subseteq \mathrm{FP}^{\Sigma_2^{\mathrm{P}}}$ and, by Toda's theorem [8], the collapse of the polynomial hierarchy to Δ_3^{P} (Theorem 4.4). Thus, unless the polynomial hierarchy collapses, Tunnell's count D_n cannot carry #P-hardness, although it is a #P function of n.

Section 2 fixes notation. Section 3 proves the main theorem and its first consequences. Section 4 applies it to Tunnell's count. Section 5 relates the results to prior work, and Section 6 concludes.

2. Preliminaries

For an integer m we write $|m|$ for its bit length. $\Sigma_2^{\mathrm{P}} = \mathrm{NP}^{\mathrm{NP}}$ and $\Delta_3^{\mathrm{P}} = \mathrm{P}^{\Sigma_2^{\mathrm{P}}}$ are levels of the polynomial hierarchy PH; for a class C of languages, FP^C is the class of functions computable in deterministic polynomial time with an oracle for a language in C. If P = NP, then PH = P, so $\mathrm{FP}^{\mathrm{NP}} = \mathrm{FP}^{\Sigma_2^{\mathrm{P}}} = \mathrm{FP}$. A function $f : \{0,1\}^* \to \mathbb{N}$ is in #P if $f(x)$ is the number of strings y of length $p(|x|)$ accepted by a polynomial-time verifier $V(x, y)$, for some polynomial p [9, 10]; #SAT, the number of satisfying assignments $\#\varphi$ of a Boolean formula φ, is #P-complete under parsimonious reductions [11].

$H(d)$ denotes the Hurwitz class number, which counts all, not necessarily primitive, classes of positive definite binary forms of discriminant $-d$, weighted by $1/2$ and $1/3$ for classes of forms equivalent to multiples of $x^2 + y^2$ and $x^2 + xy + y^2$ respectively, and which is zero unless $-d \equiv 0, 1 \pmod 4$ [12]. For a fundamental discriminant $-d < -4$ one has $H(d) = h(-d)$.

3. Class Numbers in the Polynomial Hierarchy

We use the standard facts [1, Section 5.4] that every class of primitive positive definite forms of discriminant $-d$ contains exactly one reduced form (a, b, c), with $|b| \le a \le c$, $b \ge 0$ if $|b| = a$ or $a = c$, and $a \le \sqrt{d/3}$; that reduced forms have encoding length $O(\log d)$; and that composition followed by reduction, the group operation of the form class group $\mathrm{Cl}(-d)$, is computable in time polynomial in $\log d$. Consequently $\prod_i f_i^{v_i}$ can be computed by repeated squaring in time polynomial in $\log d$ and in the bit lengths of the exponents. We also use the crude bound

$$h(-d) \;\le\; \#\{(a,b) : 1 \le a \le \sqrt{d/3},\ |b| \le a\} \;\le\; \tfrac{d}{3} + 2\sqrt{d/3} \;\le\; d \qquad (d \ge 3), \tag{1}$$

and the polynomial-time computability of Hermite normal forms of integer matrices [13].

Theorem 3.1 (Class numbers in $\mathrm{FP}^{\Sigma_2^{\mathrm{P}}}$)**.** *The function $d \mapsto h(-d)$, defined for $d \ge 3$ with $-d \equiv 0, 1 \pmod 4$, lies in $\mathrm{FP}^{\Sigma_2^{P}}$. In particular, if P = NP, then $d \mapsto h(-d)$ is computable in deterministic polynomial time.*

Proof. Let $G = \mathrm{Cl}(-d)$, write 1_G for the class of the principal form, and put $h = |G| \le d$ by (1). If $h = 1$ the procedure below terminates immediately with the empty generating set and outputs 1.

Step 1: a small generating set. For a list $S = (s_1, \dots, s_t)$ of reduced forms, every element of $\langle S \rangle$ has the form $\prod_i s_i^{v_i}$ with $0 \le v_i < h \le d$. Hence the language

$$L_1 = \{(d, S, w) : \exists f \text{ reduced, with prefix } w,\ \forall v \in \{0, \dots, d\}^t : \textstyle\prod_i s_i^{v_i} \ne f\}$$

is in Σ_2^{P}, because t never exceeds $\log_2 d + 1$ and all quantified objects have polynomial length. Starting from $S = ()$, we use L_1 with prefix search to find a reduced form $f \notin \langle S \rangle$, append it to S, and repeat until no such f exists. Each step at least doubles $|\langle S \rangle|$ by Lagrange's theorem, so the loop stops after $t \le \log_2 h \le \log_2 d$ steps with $\langle S \rangle = G$.

Step 2: the relation lattice. Let $\varphi : \mathbb{Z}^t \to G$, $\varphi(v) = \prod_i s_i^{v_i}$, and $\Lambda = \ker \varphi$. Since φ is surjective, $[\mathbb{Z}^t : \Lambda] = h$, and $h\mathbb{Z}^t \subseteq \Lambda$. The Hermite normal form basis of Λ is triangular with positive diagonal entries whose product is h and with off-diagonal entries bounded by the diagonal ones; hence all its entries lie in $[0, h] \subseteq [0, d]$.

Step 3: lattice completion. For a finite list B of integer vectors, membership in the lattice $\mathcal{L}(B)$ spanned by B is decidable in polynomial time via Hermite normal forms [13]. Hence

$$L_2 = \{(d, S, B, w) : \exists v \in [-d, d]^t \text{ with prefix } w,\ \varphi(v) = 1_G,\ v \notin \mathcal{L}(B)\}$$

is in NP. Starting from $B = ()$, we use L_2 with prefix search to find such v, append it to B, and repeat until none exists. Each appended vector strictly enlarges $\mathcal{L}(B) \subseteq \Lambda$. At most t additions increase the rank. Between two rank increases, while $\mathcal{L}(B)$ has rank r and spans the rational subspace V, the index $[\Lambda \cap V : \mathcal{L}(B)]$ is a positive integer bounded by the determinant of $\mathcal{L}(B)$, which is at most $(d\sqrt{t})^r$ by Hadamard's inequality applied to r independent vectors of B; each addition that does not increase the rank replaces this index by a proper divisor. Hence the loop stops after at most $t + t^2 \log_2(d\sqrt{t}) = O(\log^3 d)$ additions. Full rank is reached because the vectors $he_i \in \Lambda \cap [-d, d]^t$ are available to the search. When the loop stops, every vector of $\Lambda \cap [-d, d]^t$, in particular every vector of the Hermite normal form basis of Λ, lies in $\mathcal{L}(B)$, so $\mathcal{L}(B) = \Lambda$. We output $|\det H|$, where H is the Hermite normal form basis of $\mathcal{L}(B)$; this equals $[\mathbb{Z}^t : \Lambda] = h$.

All steps run in time polynomial in $\log d$ with queries to $L_1 \in \Sigma_2^{\mathrm{P}}$ and $L_2 \in \mathrm{NP} \subseteq \Sigma_2^{\mathrm{P}}$. Under P = NP both languages are in P. □

Corollary 3.2 (Class numbers under P = NP)**.** *If P = NP, then $d \mapsto h(-d)$ is computable in deterministic polynomial time; in particular, the class number of every imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ is computable in time polynomial in* $\log d$.

Proof. Under P = NP, $\Sigma_2^{\mathrm{P}} = \mathrm{P}$, and Theorem 3.1 applies. □

Remark 3.3 (The oracle queries)**.** Step 1 of the proof makes $O(\log^2 d)$ queries to the Σ_2^{P} language L_1, and Step 3 makes $O(\log^5 d)$ queries to the NP language L_2, since each of its $O(\log^3 d)$ prefix searches determines a vector of $O(\log^2 d)$ bits. The only Σ_2^{P} queries are those that certify that a list of reduced forms generates $\mathrm{Cl}(-d)$. Given a generating set of $O(\log d)$ forms, for instance the one provided under GRH by [3], Steps 2 and 3 alone compute $h(-d)$ in $\mathrm{FP}^{\mathrm{NP}}$.

4. Application to Tunnell's Count

For a positive integer n let

$$C_n = \#\{(x, y, z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 64z^2\}, \qquad D_n = \#\{(x, y, z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 16z^2\}.$$

Tunnell [7] proved that if an even square-free n is congruent, then $2C_n = D_n$, and that the converse holds if the Birch–Swinnerton-Dyer conjecture holds for the curve $y^2 = x^3 - n^2 x$. Both counts are #P functions of n: a witness is a triple (x, y, z) of bit length $O(|n|)$, checked in polynomial time. Let $\mathcal{N} = \{n \in \mathbb{N} : n \text{ square-free},\ n \equiv 2 \pmod 8\}$.

Lemma 4.1 (Local vanishing)**.** *Let n be an even square-free positive integer. If $n \equiv 6 \pmod 8$, then $C_n = D_n = 0$; in particular Tunnell's identity $2C_n = D_n$ holds trivially.*

Proof. Write $n = 2m$ with m odd; $n \equiv 6 \pmod 8$ means $m \equiv 3 \pmod 4$. A representation $n = 8x^2 + 2y^2 + 16z^2$ gives $m = 4x^2 + y^2 + 8z^2 \equiv y^2 \pmod 4$, while $y^2 \equiv 0$ or $1 \pmod 4$, a contradiction. The same argument applies to $m = 4x^2 + y^2 + 32z^2$. □

Proposition 4.2 (Class-number formula)**.** *For every $n \in \mathcal{N}$,*

$$D_n = 2h(-4n),$$

where $h(-4n)$ is the class number of $\mathbb{Q}(\sqrt{-n})$. Consequently $D_n > 0$, $D_n = O(\sqrt{n} \log n)$, and for $n \in \mathcal{N}$ Tunnell's identity $2C_n = D_n$ is equivalent to $C_n = h(-4n)$.

Proof. Write $n = 2m$, so $m \equiv 1 \pmod 4$ is odd and square-free. Dividing $n = 8x^2 + 2y^2 + 16z^2$ by 2 shows that $D_n = r_{(1,4,8)}(m)$, the number of representations of m by $Q(y, x, z) = y^2 + 4x^2 + 8z^2$. The form $X^2 + 4Y^2 + 8Z^2$ has class number one (its genus consists of a single class), and for such forms the Siegel–Weil average collapses to the representation number itself; on this basis Bringmann and Kane proved [12, Lemma 4.2] that, for every $m \geq 1$,

$$r_{(1,4,8)}(m) = c_{(1,4,8)}(m)(H(8m) - 2H(2m)),$$

with the constant $c_{(1,4,8)}(m)$ tabulated in [12, Appendix B]: it equals 2 for $m \equiv 1 \pmod 4$, 4 for $m \equiv 4 \pmod 8$, 12 for $m \equiv 0 \pmod 8$, and 0 in the remaining classes. The proof in [12] is unconditional: both sides are modular forms of weight $3/2$ on an explicit congruence subgroup, and the identity is verified on the number of coefficients prescribed by the valence formula. For our $m \equiv 1 \pmod 4$ we obtain $r_{(1,4,8)}(m) = 2(H(8m) - 2H(2m))$. Since m is odd, $-2m \equiv 2 \pmod 4$ is not a discriminant, so $H(2m) = 0$. Since m is odd and square-free, $-8m = -4n$ is a fundamental discriminant, and it is smaller than -4, so $H(8m) = h(-4n)$. Hence $D_n = 2h(-4n)$. Dirichlet's class number formula $h(-4n) = \pi^{-1}\sqrt{4n}\,L(1, \chi_{-4n})$ and the elementary bound $L(1, \chi_{-4n}) = O(\log n)$ give $D_n = O(\sqrt{n}\log n)$, and $h(-4n) \geq 1$ gives $D_n > 0$. The last assertion is immediate. □

Corollary 4.3 (Complexity of Tunnell's count)**.** *The function $n \mapsto D_n$ on even square-free n lies in $FP^{\Sigma_2^P}$. If $P = NP$, it is computable in deterministic polynomial time.*

Proof. An even square-free n satisfies $n \equiv 2$ or $6 \pmod 8$, and square-freeness and n mod 8 are decidable in $\mathrm{FP}^{\mathrm{NP}}$, since integer factorization is: the predicate "m has a divisor in $[2, k]$" is in NP ∩ coNP, and prime factors are found by binary search. If $n \equiv 6 \pmod 8$ output 0 (Lemma 4.1); if $n \equiv 2 \pmod 8$ output $2h(-4n)$ (Proposition 4.2), computed by Theorem 3.1. □

Theorem 4.4 (No exact counting reduction to D_n)**.** *Suppose there are functions R, α, β, computable in polynomial time with an NP oracle, such that for every Boolean formula φ, $R(\varphi)$ is an even square-free integer, $\alpha(\varphi) \geq 1$ and $\beta(\varphi)$ are integers, and $D_{R(\varphi)} = \alpha(\varphi)\,\#\varphi + \beta(\varphi)$. Then $\#P \subseteq FP^{\Sigma_2^P}$ and $PH = \Delta_3^P$.*

Proof. On input φ, compute $n = R(\varphi)$, $\alpha(\varphi)$ and $\beta(\varphi)$ with the NP oracle, compute D_n by Corollary 4.3, and output $(D_n - \beta(\varphi))/\alpha(\varphi) = \#\varphi$. Every oracle used is in Σ_2^{P}, so $\#\mathrm{SAT} \in \mathrm{FP}^{\Sigma_2^{\mathrm{P}}}$. Every $f \in \#\mathrm{P}$ reduces parsimoniously to #SAT, so $\#\mathrm{P} \subseteq \mathrm{FP}^{\Sigma_2^{\mathrm{P}}}$, and hence $\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{P}^{\Sigma_2^{\mathrm{P}}} = \Delta_3^{\mathrm{P}}$. By Toda's theorem [8], $\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}} \subseteq \Delta_3^{\mathrm{P}} \subseteq \mathrm{PH}$. □

Corollary 4.5 (Quantum computation of Tunnell's count)**.** *Assume GRH. Then $n \mapsto D_n$ on even square-free n is computable with bounded error in quantum polynomial time.*

Proof. Under GRH, $\mathrm{Cl}(-d)$ is generated by the classes of prime forms of norm less than $6\log^2 d$ [3], which can be listed in polynomial time. Reduced forms give a unique encoding of group elements and the group operation is polynomial-time, so Watrous's quantum algorithm for the order of a solvable black-box group [4] computes $h(-d)$ with bounded error in polynomial time. Square-freeness and n mod 8 are decided with Shor's factoring algorithm [14], and Lemma 4.1 and Proposition 4.2 give D_n. □

The identity of Proposition 4.2 has also been confirmed by exhaustive computation for all $n \in \mathcal{N}$ with $n \leq 3 \cdot 10^4$ and for 1500 random $n \in \mathcal{N}$ with $n \leq 2 \cdot 10^5$, in exact integer arithmetic by enumeration of representations and of reduced binary quadratic forms; for every square-free $n \equiv 6 \pmod 8$ with $n \leq 2 \cdot 10^5$ (20267 integers), $D_n = 0$.

5. Relationship to Prior Work

The theory of black-box groups gives complexity bounds for problems on finite groups whose elements have unique encodings and whose operations are computable in polynomial time, when a generating set is part of the input: membership is in NP [5], and order verification is in AM ∩ coAM [6]. Theorem 3.1 concerns the class group of a single discriminant, given only d; Step 1 of its proof finds a generating set of $O(\log d)$ forms with a Σ_2^{P} oracle, and Steps 2 and 3 compute the order of the group they generate with an NP oracle, deterministically. Under GRH, a generating set of polynomial size is available directly [3], and the order can be computed in subexponential classical time [2] or in quantum polynomial time [4]. Tunnell's criterion has been studied computationally on a large scale [15]. The class-number formula for D_n is an instance of the theory of ternary forms with one class in their genus [12].

6. Conclusion

The class number $h(-d)$ of every imaginary quadratic order is computable in $\mathrm{FP}^{\Sigma_2^{\mathrm{P}}}$, without GRH and without a given generating set, and hence in polynomial time if P = NP. For square-free $n \equiv 2 \pmod 8$, Tunnell's count D_n equals $2h(-4n)$, so it lies in $\mathrm{FP}^{\Sigma_2^{\mathrm{P}}}$ on all even square-free n, and an exact counting reduction from #SAT to D_n would collapse the polynomial hierarchy to Δ_3^{P}. Two questions remain open: whether $h(-d)$ is computable in $\mathrm{FP}^{\mathrm{NP}}$ without GRH, which by Remark 3.3 reduces to certifying a generating set of $\mathrm{Cl}(-d)$ with an NP oracle; and whether the other Tunnell count C_n, which differs from $h(-4n)$ by a coefficient of a weight-3/2 cusp form, lies in the polynomial hierarchy.

Acknowledgements

The author would like to thank Iris, Marilin, Sonia, Yoselin, and Arelis for their support.

Statements and Declarations

Declaration of interests

The author declares no competing interests.

Funding sources

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of generative AI in scientific writing

The author designed the results of this article, and used Claude Opus 5.5 to improve the readability of this manuscript; the author ran all the computations. After using this tool, the author reviewed and edited the content as needed and takes full responsibility for the content of the publication.

Data availability

All numerical data used in this article are reported in Section 4.

References

[1] H. Cohen, A Course in Computational Algebraic Number Theory, Vol. 138 of Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1993. doi:10.1007/978-3-662-02945-9.

[2] J. L. Hafner, K. S. McCurley, A rigorous subexponential algorithm for computation of class groups, Journal of the American Mathematical Society 2 (4) (1989) 837–850. doi:10.1090/S0894-0347-1989-1002631-0.

[3] E. Bach, Explicit bounds for primality testing and related problems, Mathematics of Computation 55 (191) (1990) 355–380. doi:10.1090/S0025-5718-1990-1023756-8.

[4] J. Watrous, Quantum algorithms for solvable groups, in: Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, ACM, New York, NY, USA, 2001, pp. 60–67. doi:10.1145/380752.380759.

[5] L. Babai, E. Szemerédi, On the complexity of matrix group problems I, in: 25th Annual Symposium on Foundations of Computer Science, IEEE, 1984, pp. 229–240. doi:10.1109/SFCS.1984.715919.

[6] L. Babai, Bounded round interactive proofs in finite groups, SIAM Journal on Discrete Mathematics 5 (1) (1992) 88–111. doi:10.1137/0405008.

[7] J. B. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, Inventiones Mathematicae 72 (2) (1983) 323–334. doi:10.1007/BF01389327.

[8] S. Toda, PP is as hard as the polynomial-time hierarchy, SIAM Journal on Computing 20 (5) (1991) 865–877. doi:10.1137/0220053.

[9] L. G. Valiant, The complexity of computing the permanent, Theoretical Computer Science 8 (2) (1979) 189–201. doi:10.1016/0304-3975(79)90044-6.

[10] L. G. Valiant, The complexity of enumeration and reliability problems, SIAM Journal on Computing 8 (3) (1979) 410–421. doi:10.1137/0208032.

[11] S. Arora, B. Barak, Computational Complexity: A Modern Approach, Cambridge University Press, Cambridge, UK, 2009. doi:10.1017/CBO9780511804090.

[12] K. Bringmann, B. Kane, Class numbers and representations by ternary quadratic forms with congruence conditions, Mathematics of Computation 91 (333) (2022) 295–329. doi:10.1090/mcom/3648.
[13] R. Kannan, A. Bachem, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix, SIAM Journal on Computing 8 (4) (1979) 499–507. doi:10.1137/0208040.
[14] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing 26 (5) (1997) 1484–1509. doi:10.1137/S0097539795293172.
[15] W. B. Hart, G. Tornaría, M. Watkins, Congruent number theta coefficients to 10^{12}, in: Algorithmic Number Theory (ANTS-IX), Vol. 6197 of Lecture Notes in Computer Science, Springer, Berlin, 2010, pp. 186–200. doi:10.1007/978-3-642-14518-6_17.