



Efficient DDH Distinguishers in Class Groups of Orders in $\mathbb{Q}(\sqrt{-3})$

Antonio Sanso

Ethereum Foundation, Switzerland

Abstract. We give an explicit algorithm to evaluate an efficiently computable *cubic genus* invariant on ideal class groups of non-maximal imaginary quadratic orders in $K = \mathbb{Q}(\sqrt{-3})$. Concretely, we consider the order $\mathcal{O}_\Delta$ of discriminant $\Delta = -3f^2$ with conductor $f > 1$. We assume that f is known as an integer, but its prime factorization is not; instead, we are given only a single nontrivial factor $a \mid f$ arising in Dedekind’s parametrization of these discriminants (so that the complementary factor needed in the cubic-residuosity test can be recovered as an integer from (f, a) , without factoring it).

Under these assumptions, our method computes a nontrivial *two-valued* genus invariant

$$\chi_H : \text{Cl}(\mathcal{O}_\Delta) \rightarrow \{\pm 1\},$$

whose $+1$ -fiber is a distinguished index-3 subgroup singled out by classical work of Dedekind; equivalently, $\chi_H([\tau]) = +1$ if and only if $[\tau]$ lies in that subgroup.

The construction is inspired by work of Dedekind and Shanks on index-3 subgroups of quadratic form class groups and their characterization via cubic residuosity of primes represented by form classes. We prove correctness and analyze the running time of the resulting evaluation procedure, and we validate the approach with a SageMath implementation. As an application, we obtain an explicit Decisional Diffie–Hellman (DDH) distinguisher in cyclic subgroups of $\text{Cl}(\Delta)$ generated by an element outside the distinguished index-3 subgroup, under the same partial-factorization assumption.

1 Introduction

The class groups of imaginary quadratic orders sit at a crossroads of explicit arithmetic, binary quadratic forms, and algorithmic questions about representing primes and navigating ideal classes. In this paper we revisit a classical theme going back to Dedekind and Gauss: for discriminants of the special shape $\Delta = -3f^2$, the set of proper classes of primitive positive definite binary quadratic forms admits a distinguished decomposition governed by cubic residuosity conditions on represented primes. Shanks [Sha71, §8] highlights concrete examples of this phenomenon and relates them to 3-Sylow structure in class groups.

Our aim is to make this structure *algorithmic* in a setting that is particularly natural from a computational perspective. We focus on non-maximal imaginary quadratic orders in $K = \mathbb{Q}(\sqrt{-3})$ of discriminant

$$\Delta = -3f^2,$$

where $f > 1$ is the conductor. We assume that f is known as an integer (equivalently, Δ is known), but that its prime factorization is not. We consider a partial-factorization regime: we assume knowledge of a single nontrivial factor $a \mid f$ (in the sense of Dedekind’s

E-mail: antonio.sanso@ethereum.org (Antonio Sanso)



parametrization), while the factorization of the complementary factor (and hence the class number $\# \text{Cl}(\Delta)$) may be unknown.

If the conductor f is fully factored, then one can typically recover substantial information about the size and structure of $\text{Cl}(\Delta)$ (for instance via standard formulas for the class number of an order). In particular, any known small prime divisor ℓ of $\# \text{Cl}(\Delta)$ yields an efficiently computable homomorphism $\text{Cl}(\Delta) \rightarrow C_\ell$, and therefore an immediate distinguisher for DDH distributions in $\text{Cl}(\Delta)$. Thus, DDH is not expected to be hard in these groups when the complete factorization of f is available.

By contrast, the focus of this paper is the partial-factorization regime: we show that for $\Delta = -3f^2$ one can still compute a nontrivial cubic-genus invariant—and hence obtain a DDH distinguisher as an application—assuming only knowledge of a *single* nontrivial factor of f , without the full factorization of f and without knowledge of $\# \text{Cl}(\Delta)$.

The classical statements of Dedekind describe an index-3 subgroup of the class group for discriminants of the form $-3f^2$, characterized by which primes $p \equiv 1 \pmod{3}$ are represented by classes in that subgroup, and equivalently by whether a prescribed integer is a cubic residue modulo p . The first goal of this paper is to turn this into a *computable invariant* on ideal classes in $\text{Cl}(\Delta)$: given an ideal class (or a reduced binary quadratic form) and partial conductor information, we design an explicit procedure that evaluates a cubic-genus value efficiently.

Class groups of imaginary quadratic orders have been proposed and used in cryptography, notably due to their “unknown order” behavior in some representations; see [BW88, Lip12, Wes19, Pie19, BBF19] and many subsequent works. The cited constructions do not rely on DDH or CDH; instead, they rely on assumptions concerning the hardness of computing an ℓ -th root for a suitable ℓ . A standard and widely used principle is that any efficiently computable, nontrivial invariant mapping group elements into a small set can be leveraged as a distinguisher for decisional Diffie–Hellman (DDH) distributions. In our setting, once the cubic-genus invariant can be evaluated efficiently on class group elements, it yields such a distinguisher for DDH instances instantiated in $\text{Cl}(\Delta)$.

Our contribution We provide an explicit algorithm to evaluate a nontrivial cubic-genus *distinguisher*

$$\chi_H : \text{Cl}(\Delta) \rightarrow \{\pm 1\}$$

in the partial-factorization regime where f is composite and only a single nontrivial factor $a \mid f$ is known. The construction is inspired by the classical observations of Shanks [Sha71, §8] and the work of Dedekind [Ded00] relating index-3 subgroups of form class groups to cubic residuosity conditions on represented primes. We prove correctness of the evaluation procedure, discuss its complexity, and provide a SageMath implementation. As an application, we derive an efficient DDH distinguisher in these class groups under the same partial-factorization assumption.

Outline In Section 2 we recall background on imaginary quadratic orders, ideals, and binary quadratic forms. Section 3 presents our main algorithmic results: we restate Dedekind’s theorem in modern language, define the cubic-genus invariant, give an evaluation algorithm, and prove correctness and complexity bounds. In Section 4 we derive, as an application, an efficient distinguisher for decisional Diffie–Hellman (DDH) instances in these class groups. We conclude in Section 5.

2 Preliminaries

We recall standard facts and notation on imaginary quadratic orders; see [Cox89] for details.

We write $\text{Cl}(\Delta)$ for the proper form class group of discriminant Δ ; via the standard correspondence we identify $\text{Cl}(\Delta)$ with the ideal class group of proper invertible $\mathcal{O}_\Delta$ -ideals.

A *quadratic number field* is a degree-2 extension $K/\mathbb{Q}$. It can be written uniquely as $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is squarefree and $d \neq 0, 1$. We say that K is *imaginary quadratic* if $d < 0$.

The *fundamental discriminant* Δ_K of $K = \mathbb{Q}(\sqrt{d})$ is

$$\Delta_K = \begin{cases} d, & \text{if } d \equiv 1 \pmod{4}, \\ 4d, & \text{if } d \equiv 2, 3 \pmod{4}. \end{cases}$$

The ring of integers $\mathcal{O}_K$ (the *maximal order*) is

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{if } d \equiv 1 \pmod{4}, \\ \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \pmod{4}. \end{cases}$$

An *order* $\mathcal{O}$ in K is a subring of $\mathcal{O}_K$ containing 1 and free as a $\mathbb{Z}$ -module of rank 2. Every order has the form

$$\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$$

for a unique integer $f \geq 1$, called the *conductor* of $\mathcal{O}_f$, and its discriminant is

$$\text{disc}(\mathcal{O}_f) = f^2 \Delta_K.$$

In our setting $K = \mathbb{Q}(\sqrt{-3})$ and $\Delta = -3f^2$, so $\mathcal{O}_\Delta = \mathcal{O}_f$.

A proper (invertible) fractional ideal of $\mathcal{O}_\Delta$ can be written in the form

$$\mathfrak{a} = q\left(A\mathbb{Z} + \frac{-B + \sqrt{\Delta}}{2}\mathbb{Z}\right),$$

with $q \in \mathbb{Q}_{>0}$, $A \in \mathbb{N}$, and $B \in \mathbb{Z}$ satisfying $B^2 \equiv \Delta \pmod{4A}$. If $q = 1$ we call $\mathfrak{a}$ *integral*. If in addition $-A < B \leq A$, then the pair (A, B) determines the ideal uniquely, and we denote it by (A, B) .

Via the usual correspondence, the integral ideal (A, B) corresponds to the primitive positive definite binary quadratic form

$$[A, B, C] : Ax^2 + Bxy + Cy^2, \quad \text{with} \quad B^2 - 4AC = \Delta,$$

where $C = (B^2 - \Delta)/(4A) \in \mathbb{N}$. A form $Ax^2 + Bxy + Cy^2$ is *primitive* if $\gcd(A, B, C) = 1$.

An integer m is *represented* by a binary quadratic form $F(x, y)$ if the equation

$$m = F(x, y)$$

has an integer solution $(x, y) \in \mathbb{Z}^2$. If moreover $\gcd(x, y) = 1$, we say that m is *properly represented* by $F(x, y)$.

3 The algorithm

3.1 Historical motivation

Our approach is motivated by classical observations of Dedekind [Ded00], as highlighted by Shanks [Sha71, §8], connecting index-3 subgroups of class groups of binary quadratic forms to cubic residuosity conditions on primes represented by those forms.

For example, cf. Dedekind [Ded00], the discriminant $-4 \cdot 243$ has class number $h(-4 \cdot 243) = 9$, with class group $C(3) \times C(3)$. There are four subgroups of order 3, not merely one as would be the case if the group were cyclic. One of these four, comprising $I = (1, 0, 243)$ and the forms $(9, \pm 6, 28)$, represents all primes having 2 as a cubic residue. Another: I and $(4, \pm 2, 61)$ has 3 as a cubic residue; the third: I and $(7, \pm 6, 36)$ has 6; and the last: I and $(13, \pm 4, 19)$ has both $12 = 4 \cdot 3$ and $18 = 2 \cdot 9$ as cubic residues. The discriminant $-4 \cdot 675$, with a group $C(3) \times C(6)$, may be used similarly for $a = 2, 5, 10, 20$, and 50.

We will use the following theorem of Dedekind, as presented in [Ded00]. (Dedekind writes D for the discriminant; we write Δ .)

Theorem 1. *Let a, b be two natural numbers. Suppose at least one of a, b is greater than 1, and ab is not divisible by the square of any natural prime number. Further, let $k = 3ab$ or ab , depending on whether $(a^2 - b^2)$ is indivisible or divisible by 9. Then the number of all non-equivalent, positive, primitive binary quadratic forms $(A, \frac{1}{2}B, C)$ of the discriminant $B^2 - 4AC = D = -3k^2$ is always a multiple of 3 ($3k''$), and one-third of the form classes represented by these forms constitute a composition group $\mathfrak{K}$, characterized by the following property: Let p be any natural prime number congruent to 1 (mod 3) and not dividing D . Then, through the k'' forms of the group $\mathfrak{K}$, all and only those prime numbers p can be represented for which ab^2 , and hence a^2b , is a cubic residue, while through the forms of the remaining $2k''$ classes, all and only those prime numbers p can be represented for which ab^2 is a cubic non-residue.*

In the paper [Ded00], Dedekind makes reference to an unpublished note by Gauss. This note contains the same example that we previously cited from Shanks [Sha71, §8]:

A very elegant observation made by induction.

2 is a cubic residue or non-residue of the prime number p in the form $3n + 1$, depending on whether p is representable by the form

$$x^2 + 27y^2$$

$$\text{or } 4x^2 + 2xy + 7y^2$$

3 is a residue or non-residue, depending on whether p is representable by $x^2 + 243y^2$ or

$$4x^2 + 2xy + 61y^2$$

$$7x^2 + 6xy + 36y^2 \text{ or } 9x^2 + 6xy + 28y^2$$

...

.

3.2 Dedekind's theorem in modern form

Theorem 1 is stated in the classical language of composition of binary quadratic forms and “form classes” representing primes. For our purposes it is convenient to isolate the group-theoretic content for the discriminants we actually use, namely

$$\Delta = -3f^2,$$

where $f > 1$ is the conductor. We therefore formulate Dedekind's theorem directly for Δ and use the standard identification between the proper form class group of discriminant Δ and the ideal class group of $\mathcal{O}_\Delta$.

Theorem 2 (Dedekind, modern restatement for $\Delta = -3f^2$). *Let $f > 1$ be an integer. Assume there exist integers $a, b > 1$ with ab squarefree such that*

$$f = \begin{cases} ab, & \text{if } 9 \mid (a^2 - b^2), \\ 3ab, & \text{if } 9 \nmid (a^2 - b^2). \end{cases}$$

Set $\Delta := -3f^2$, and let $\text{Cl}(\Delta)$ denote the proper class group of primitive positive definite binary quadratic forms of discriminant Δ (equivalently, the ideal class group of $\mathcal{O}_\Delta$).

Then $\#\text{Cl}(\Delta)$ is divisible by 3, and there exists a subgroup

$$H \leq \text{Cl}(\Delta), \quad [\text{Cl}(\Delta) : H] = 3,$$

with the following property.

For every prime $p \equiv 1 \pmod{3}$ with $p \nmid \Delta$, the prime p is properly represented by a form class in H if and only if ab^2 is a cubic residue modulo p ; equivalently,

$$p \text{ is represented by some class in } H \iff \left(\frac{ab^2}{p}\right)_3 = 1 \iff \left(\frac{a^2b}{p}\right)_3 = 1,$$

where $\left(\frac{\cdot}{p}\right)_3$ is the cubic residue symbol in $\mathbb{F}_p^\times$ (which is defined since $p \equiv 1 \pmod{3}$).

Moreover, the remaining two cosets of H in $\text{Cl}(\Delta)$ represent exactly those primes $p \equiv 1 \pmod{3}$, $p \nmid \Delta$, for which ab^2 is a cubic non-residue modulo p .

Remark 1. Theorem 2 applies to those conductors f that admit a decomposition as above with $a, b > 1$ and ab squarefree. In particular, this imposes arithmetic restrictions on f ; we do not claim that every conductor f yields an index-3 subgroup characterized by cubic residuosity.

Table 1: Number of conductors $2 \leq f \leq B$ admitting parameters $a, b > 1$ satisfying the hypotheses of Theorem 2.

Bound B	Count	Percentage
10^3	244	24.42%
10^4	3,039	30.39%
10^5	34,551	34.55%
10^6	377,352	37.74%

We enumerated conductors $2 \leq f \leq B$ satisfying the hypotheses of Theorem 2. As shown in Table 1, approximately 37.74% of conductors up to 10^6 admit such parameters. Thus, the applicable family is substantial, but does not include arbitrary conductors.

Lemma 1 (Recovering the Dedekind factor c from f). *Assume the hypotheses of Theorem 2. Then $3 \nmid f$ holds in the case $f = ab$ and $3 \mid f$ holds in the case $f = 3ab$. Equivalently, defining*

$$c := \begin{cases} 1, & 3 \nmid f, \\ 3, & 3 \mid f, \end{cases}$$

one has $f = cab$ with the same parameters a, b as in Theorem 2.

Proof. If $f = 3ab$ then clearly $3 \mid f$. Conversely, suppose $f = ab$ and ab is squarefree with $9 \mid (a^2 - b^2)$. If $3 \mid a$ then $a^2 \equiv 0 \pmod{9}$ and, since ab is squarefree, $3 \nmid b$, so $b^2 \not\equiv 0 \pmod{9}$; hence $a^2 - b^2 \not\equiv 0 \pmod{9}$, a contradiction. Similarly $3 \nmid b$. Therefore $3 \nmid ab = f$ in the $f = ab$ case. $\square$

We now specialize to the partial-factorization model considered in this paper. Fix $\Delta = -3f^2$ with $f > 1$ known as an integer, and assume we are given a nontrivial factor $a \mid f$ which is the parameter a appearing in Theorem 2. Define $c \in \{1, 3\}$ from f as in Lemma 1, and then set

$$b := \frac{f}{ca}.$$

Note that b is a known integer (but not assumed factored). Our goal is to make the index-3 decomposition of Theorem 2 algorithmic by giving an efficient procedure that, on input $[\mathfrak{r}] \in \text{Cl}(\Delta)$, determines *membership in* the distinguished subgroup H using only (f, a) .

A two-valued cubic genus invariant

Let $\Delta = -3f^2$ be as in Theorem 2, and let $H \leq \text{Cl}(\Delta)$ be the distinguished index-3 subgroup. We will refer to H as the *principal cubic genus*. For algorithmic purposes, we consider the associated *membership indicator*

$$\chi_H : \text{Cl}(\Delta) \longrightarrow \{\pm 1\}, \quad \chi_H([\mathfrak{r}]) = \begin{cases} +1, & [\mathfrak{r}] \in H, \\ -1, & [\mathfrak{r}] \notin H. \end{cases}$$

Thus, χ_H is a two-valued membership invariant for H , not a cubic character on the full ideal class group.

Dedekind's theorem characterizes H by a cubic residuosity condition on primes represented by form classes. This yields an efficient evaluation procedure for χ_H that only requires the integer arithmetic $f = c \cdot a \cdot b$ with $c \in \{1, 3\}$ and $b = f/(ca)$, but does not require factoring b .

3.3 Evaluating the invariant

In this subsection we give an explicit procedure to evaluate χ_H on an input class $[\mathfrak{r}] \in \text{Cl}(\Delta)$, with $\Delta = -3f^2$ as above, using only Dedekind's characterization of membership in H .

Input. A class $[\mathfrak{r}] \in \text{Cl}(\Delta)$, represented by a reduced primitive positive definite binary quadratic form $[A, B, C]$ of discriminant Δ (equivalently, by an ideal (A, B)), and an integer $a > 1$ satisfying the hypotheses of Theorem 2.

Output. The value $\chi_H([\mathfrak{r}]) \in \{\pm 1\}$.

Algorithm (informal).

Let $F(x, y) = Ax^2 + Bxy + Cy^2$ be the reduced form representing $[\mathfrak{r}]$. We search for a prime p properly represented by F satisfying $p \equiv 1 \pmod{3}$ and $p \nmid \Delta$, and then test whether a^2b is a cubic residue modulo p , where $b = f/(ca)$ and $c \in \{1, 3\}$ is determined from f as in Lemma 1.

Algorithm 1 (evaluation of χ_H).

1. Repeat:

- (a) Choose integers $(x, y) \in \mathbb{Z}^2$ uniformly at random subject to $\gcd(x, y) = 1$ and $|x|, |y| \leq |\Delta|$.
- (b) Set $p \leftarrow F(x, y)$.

until p is prime, $p \equiv 1 \pmod{3}$, and $p \nmid \Delta$.

2. Determine $c \in \{1, 3\}$ by

$$c := \begin{cases} 1, & 3 \nmid f, \\ 3, & 3 \mid f, \end{cases}$$

set $b \leftarrow f/(ca)$, and compute

$$t := (a^2b)^{(p-1)/3} \bmod p \in \mathbb{F}_p^\times.$$

3. Output

$$\chi_H([\mathfrak{r}]) := \begin{cases} +1, & t \equiv 1 \pmod{p}, \\ -1, & t \not\equiv 1 \pmod{p}. \end{cases}$$

Theorem 3 (Well-definedness and correctness). *Assume $\Delta = -3f^2$ and that a (together with the associated parameters in Theorem 2) satisfies the hypotheses of Theorem 2. Let $c \in \{1, 3\}$ be defined from f as in Lemma 1, and set $b := f/(ca)$. Let $[\mathfrak{r}] \in \text{Cl}(\Delta)$ and let $p \equiv 1 \pmod{3}$, $p \nmid \Delta$, be any prime properly represented by the class $[\mathfrak{r}]$. Define*

$$\chi_H([\mathfrak{r}]) := \begin{cases} +1, & (a^2b)^{(p-1)/3} \equiv 1 \pmod{p}, \\ -1, & (a^2b)^{(p-1)/3} \not\equiv 1 \pmod{p}. \end{cases}$$

Then $\chi_H([\mathfrak{r}])$ is independent of the choice of such a prime p represented by $[\mathfrak{r}]$. In particular, Algorithm 1 computes a well-defined invariant of the class $[\mathfrak{r}]$. Moreover, $\chi_H([\mathfrak{r}]) = +1$ if and only if $[\mathfrak{r}] \in H$, where $H \leq \text{Cl}(\Delta)$ is the index-3 subgroup singled out by Theorem 2.

Proof sketch. By Theorem 2, a prime $p \equiv 1 \pmod{3}$ with $p \nmid \Delta$ is properly represented by a class in H if and only if a^2b (equivalently ab^2) is a cubic residue modulo p , i.e. if and only if $(a^2b)^{(p-1)/3} \equiv 1 \pmod{p}$. If $[\mathfrak{r}] \in H$ and p is properly represented by $[\mathfrak{r}]$, then p is represented by a class in H (namely $[\mathfrak{r}]$), hence the residue test holds. If $[\mathfrak{r}] \notin H$, then $[\mathfrak{r}]$ lies in one of the other two cosets; by the “Moreover” clause of Theorem 2, primes represented by those cosets are exactly the primes for which ab^2 is a cubic non-residue, hence the residue test fails. Therefore the predicate is constant on the class $[\mathfrak{r}]$, so χ_H is well-defined and equals $+1$ precisely on H . $\square$

Complexity.

The modular exponentiation in Step (2) runs in time polynomial in $\log p$. Primality testing can also be performed in time polynomial in $\log p$. The bound $|x|, |y| \leq |\Delta|$ ensures that the bit length of $p = F(x, y)$ is polynomial in $\log |\Delta|$, so each trial in Step (1) can be performed in polynomial time. The dominant cost is Step (1), i.e. finding a suitable prime p represented by the input form F . Under standard heuristic assumptions on the density of primes represented by a fixed primitive positive definite form together with the congruence conditions $p \equiv 1 \pmod{3}$ and $p \nmid \Delta$, the expected number of trials in Step (1) is polynomial in $\log |\Delta|$, so Algorithm 1 runs in expected time polynomial in $\log |\Delta|$.

4 Application to decisional Diffie–Hellman

4.1 Cryptographic context

Class groups of imaginary quadratic orders have been used in cryptography since the work of Buchmann and Williams [BW88]. More recently, the “unknown order” aspect of these

groups has been used in constructions such as accumulators and verifiable delay functions (VDFs) [Lip12, Wes19, Pie19], and related commitment primitives in blockchain-oriented applications [BBF19]. While many proposals work with the maximal order, there is also an active line of work using and analyzing schemes instantiated in non-maximal orders [CL15, CLT18].

Relevance to this paper. Our results show that for certain non-maximal orders of discriminant $\Delta = -3f^2$ satisfying Dedekind’s hypotheses, *partial* information about the conductor already suffices to compute a nontrivial two-valued genus invariant on $\text{Cl}(\Delta)$, yielding an explicit and efficiently computable DDH distinguisher in that parameter regime.

Scope and impact. We are not aware of deployed or proposed protocols instantiated in the specific discriminant family and partial-factorization model considered here; we view our result primarily as a cautionary parameter-family distinguisher. The DDH distinguisher established here does not by itself yield an algorithm for the computational Diffie–Hellman problem, nor does it directly imply a break of CDH-based constructions. The DDH distinguisher established here does not lead to any attack on the root assumptions used in the applications of groups of unknown order.

4.2 A DDH distinguisher from χ_H

We explain how the efficiently computable membership predicate χ_H can be leveraged as a DDH distinguisher in cyclic subgroups of $\text{Cl}(\Delta)$ generated by an element outside the principal cubic genus H .

Let $G = \langle g \rangle \leq \text{Cl}(\Delta)$ be cyclic. If $g \in H$, then $\chi_H(g^e) = +1$ for all e and χ_H carries no distinguishing information on G . We therefore assume $g \notin H$, so the image of g in the quotient $\text{Cl}(\Delta)/H \cong C_3$ has order 3. In this case,

$$\chi_H(g^e) = +1 \iff g^e \in H \iff 3 \mid e.$$

Given a quadruple (g, g^x, g^y, g^z) , define

$$u := \chi_H(g^x), \quad v := \chi_H(g^y), \quad w := \chi_H(g^z).$$

Consider the test

$$\text{Test}(g, g^x, g^y, g^z) = \begin{cases} \text{DH}, & \text{if } (w = +1) \iff (u = +1 \text{ or } v = +1), \\ \text{Random}, & \text{otherwise.} \end{cases}$$

Equivalently, the test accepts “DH” exactly when $w = -1$ forces $u = v = -1$ and $w = +1$ forces at least one of u, v to be $+1$.

Correctness on DH samples. If the input is a genuine Diffie–Hellman tuple, so $z = xy$, then

$$w = +1 \iff 3 \mid xy \iff (3 \mid x) \text{ or } (3 \mid y) \iff (u = +1) \text{ or } (v = +1),$$

so **Test** outputs DH with probability 1 on DH samples.

Behavior on random samples. In the standard DDH experiment, the “random” distribution has x, y, z independent and uniformly random (modulo the group order). In particular, modulo 3 we may treat x, y, z as independent uniform elements of $\mathbb{Z}/3\mathbb{Z}$, so each of u, v, w equals $+1$ with probability $1/3$ and -1 with probability $2/3$, independently.

Let A be the event “ $u = +1$ or $v = +1$ ” (equivalently $3 \mid x$ or $3 \mid y$). Then

$$\Pr[A] = 1 - \Pr[u = -1 \text{ and } v = -1] = 1 - \left(\frac{2}{3}\right)^2 = \frac{5}{9}.$$

Let B be the event “ $w = +1$ ” (equivalently $3 \mid z$), with $\Pr[B] = 1/3$ independent of A . The acceptance condition of **Test** on random samples is exactly $B \Leftrightarrow A$, so

$$\Pr[\text{Test outputs DH} \mid \text{Random}] = \Pr[A \cap B] + \Pr[A^c \cap B^c] = \frac{5}{9} \cdot \frac{1}{3} + \frac{4}{9} \cdot \frac{2}{3} = \frac{13}{27}.$$

Thus the distinguishing advantage (difference in acceptance probabilities) is

$$\text{Adv} = 1 - \frac{13}{27} = \frac{14}{27}.$$

Remark. The distinguisher above uses only the two-valued test χ_H evaluated on (g^x, g^y, g^z) . A C_3 -valued character on $\text{Cl}(\Delta)/H$ would also yield a homomorphic DDH distinguisher of the usual character form, but it is not necessary for obtaining a concrete advantage in the standard DDH experiment as soon as one can evaluate membership in H and the subgroup generator satisfies $g \notin H$.

4.3 Implementation

We implemented the evaluation procedure in SageMath to demonstrate correctness and feasibility. The source code is freely available on GitHub at the following URL: <https://github.com/asanso/DDH-cic>.

4.4 Countermeasures

A direct countermeasure against the two-valued test χ_H is to restrict to the subgroup H (the principal cubic genus), since χ_H is then identically $+1$ and yields no distinguishing information. Enforcing membership in H may be nontrivial depending on the representation and sampling procedure.

A generic method is to work inside $\text{Cl}(\Delta)^3$, since $\text{Cl}(\Delta)^3 \subseteq H$ for any index-3 quotient: indeed, the quotient map $\pi : \text{Cl}(\Delta) \twoheadrightarrow \text{Cl}(\Delta)/H \cong C_3$ satisfies $\pi(x^3) = \pi(x)^3 = 1$ for all x . If one also applies the standard countermeasure of working with squares (principal genus), then one operates in $\text{Cl}(\Delta)^6$. In a key-exchange setting, this can be enforced by cubing all exchanged group elements.

5 Conclusions

We presented an explicit procedure to evaluate a nontrivial cubic-genus membership invariant on the class group $\text{Cl}(\Delta)$ for non-maximal orders in $K = \mathbb{Q}(\sqrt{-3})$ of discriminant $\Delta = -3f^2$. The distinguishing feature of our setting is a *partial-factorization* regime: the conductor f is assumed known as an integer, but only a single nontrivial factor $a \mid f$ (in Dedekind’s sense) is given, while the complementary factor $b = f/(ca)$ is not factored (with $c \in \{1, 3\}$ determined from f).

Using Dedekind’s index-3 decomposition of $\text{Cl}(\Delta)$ and its characterization via cubic residuosity of represented primes, we turned this classical structure into an efficient, computable membership test for the principal cubic genus. As an application, we showed that efficient evaluation of χ_H gives a concrete DDH distinguisher in cyclic subgroups generated by an element outside H .

This work is primarily algorithmic in nature. The construction relies on special features of the discriminants $\Delta = -3f^2$ (equivalently, the arithmetic of $\mathbb{Q}(\sqrt{-3})$ and cubic residuosity), and it is not immediate how to extend it to other fundamental discriminants or to more general non-maximal orders. Clarifying the precise scope of such genus-based invariants, and whether analogous efficiently computable characters exist beyond the -3 setting, is an interesting direction for future work.

Acknowledgments. We would like to thank Karim Belabas, Guilhem Castagnos, Péter Kutas, Simon-Philipp Merz and Benjamin Wesolowski for fruitful discussions and Luca De Feo for providing detailed and insightful comments that enhanced the quality and clarity of the paper.

References

- [BBF19] Dan Boneh, Benedikt Bünz, and Ben Fisch. Batching techniques for accumulators with applications to iops and stateless blockchains. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 561–586, Cham, 2019. Springer International Publishing. doi:10.1007/978-3-030-26948-7_20.
- [BW88] Johannes Buchmann and Hugh C. Williams. A key-exchange system based on imaginary quadratic fields. *J. Cryptology*, 1:107–118, 1988. doi:10.1007/BF02351719.
- [CL15] Guilhem Castagnos and Fabien Laguillaumie. Linearly homomorphic encryption from ddh. In Kaisa Nyberg, editor, *Topics in Cryptology – CT-RSA 2015*, pages 487–505, Cham, 2015. Springer International Publishing. doi:10.1007/978-3-319-16715-2_26.
- [CLT18] Guilhem Castagnos, Fabien Laguillaumie, and Ida Tucker. Practical fully secure unrestricted inner product functional encryption modulo p . In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 733–764, Cham, 2018. Springer International Publishing. doi:10.1007/978-3-030-03329-3_25.
- [Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$* . A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication. doi:10.1002/9781118400722.
- [Ded00] R. Dedekind. Ueber die anzahl der idealklassen in reinen kubischen zahlkörpern. *Journal für die reine und angewandte Mathematik*, 121:40–123, 1900. URL: <http://eudml.org/doc/149072>, doi:10.1515/crll.1900.121.40.
- [Lip12] Helger Lipmaa. Secure accumulators from euclidean rings without trusted setup. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *Applied Cryptography and Network Security - 10th International Conference, ACNS 2012, Singapore, June 26-29, 2012. Proceedings*, volume 7341 of *Lecture Notes in Computer Science*, pages 224–240. Springer, 2012. doi:10.1007/978-3-642-31284-7_14.
- [Pie19] Krzysztof Pietrzak. Simple Verifiable Delay Functions. In Avrim Blum, editor, *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, volume 124 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 60:1–60:15, Dagstuhl, Germany, 2019. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2019.60>, doi:10.4230/LIPIcs.ITCS.2019.60.
- [Sha71] D. Shanks. Class number, a theory of factorization, and genera. In *Proceedings of Symposia in Pure Mathematics*, 1971. doi:10.1090/pspum/020/0316385.
- [Wes19] Benjamin Wesolowski. Efficient verifiable delay functions. In *Advances in Cryptology – EUROCRYPT 2019*, volume 11478 of *Lecture Notes in Computer Science*, pages 379–407, Cham, 2019. Springer. doi:10.1007/978-3-030-17659-4_13.