A NOTE ON THE LOW ORDER ASSUMPTION IN CLASS GROUPS OF IMAGINARY QUADRATIC NUMBER FIELDS

KARIM BELABAS, THORSTEN KLEINJUNG, ANTONIO SANSO,
AND BENJAMIN WESOLOWSKI

Abstract. In this short note we analyze the low order assumption in the imaginary quadratic number fields. We show how this assumption is broken for Mersenne primes. We also provide a description on how to possible attack this assumption for other class of prime numbers leveraging some new mathematical tool coming from higher (cubic) number fields.

1. Introduction

Cryptography based on class groups of imaginary quadratic orders (IQ cryptography, IQC) is a fascinating area pioneered by Buchmann and Williams in [1]. After a long hiatus where IQC did not find any obvious real life application Lipmaa had the idea to make use of IQ's techniques to build secure accumulators without trusted setup [2], leveraging the unknown order property of class groups of imaginary quadratic fields. In the last years we have seen this unknown order property used as a basis to build Verifiable Delay Functions (VDF) [3, 4], cryptographic accumulators and vector commitments for blockchain applications [5] and polynomial commitment used for zero knowledge [6]. The security of some of this primitives (VDF in the specific case pointed out in [7]) are bound to two complexity assumptions: the *low order assumption* [7, Definition 1] and the *adaptive root assumption* [7, Definition 2] with the *adaptive root assumption* implying the *low order assumption*. Breaking the low order assumption consists in finding an element $\mu \in G$ and an integer $d < 2^\lambda$ such that $\mu \neq 1_G$ and $\mu^d = 1_G$. In this paper we are going to analyze in more details the low order assumption in the class group of an imaginary quadratic number fields.

2. Low Order assumption in the RSA group

Given an odd integer N with unknown factorization the *low order assumption* is believed to hold for the group $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$. The low order assumption in RSA groups has been extensively analyzed in [8].

Univ. Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France
INRIA, IMB, UMR 5251, F-33400, Talence, France

Laboratory for Cryptologic Algorithms, School of Computer and Communication Sciences, EPFL, Switzerland

Adobe and Ruhr Universität Bochum

Univ. Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France
INRIA, IMB, UMR 5251, F-33400, Talence, France

3. Low Order assumption in the class group of an imaginary quadratic number field

For class group of the number field $\mathbb{Q}(\sqrt{-p})$, with $p \equiv 3 \pmod 4$ we know that the *class number* (the class group order) is odd and it is believed hard to compute when $|p|$ is large. The *low order assumption* in the class group of an imaginary quadratic field has not been studied much and is one of the goal for this work. While the Cohen-Lenstra heuristics [9] suggest that the class group often contains elements of small odd order it seems out of reach by current techniques to find such low order forms. In [10, §2] Shanks provides some interesting relations that can help to shade some light and one in particular caught our attention: if

$$\Delta = 2^p - 1$$

then

$$h(-\Delta) \equiv 0 \pmod{p-2}$$

and the associated low order element is of the form

$$(2, 1, 2^{p-3}).$$

This relation tells us that the low order assumption is violated for Mersenne primes. Other relations exist but require an even class number and are out of our scope. Shanks gives some other hint in [11]: for negative discriminants $\Delta = 8k - 1$ the class number h must satisfy $h \geq 1 + log_2\, k$. Furthermore if the class number respects $h(1 - 8k) = 6n \pm 1$ then

$$\Delta = \frac{2^{h+2} - (2u + v)^2}{v^2}$$

with odd v and $(2u + v)$ when h is prime and > 3. It is interesting to note that assigning $v = 1$ and $u = 0$ gives exactly the formula for Mersenne primes above.

4. Constructing malicious discriminants

For any discriminant $\Delta < 0$, the norm of the algebraic number $\alpha = x + y\sqrt{\Delta} \in \mathbb{Q}(\sqrt{\Delta})$ is $N(\alpha) = x^2 - \Delta y^2$. This element α generates a principal ideal (α) of the same norm, which, by construction, is principal. Now, if z is a prime number, and $N(\alpha) = z^3$, we can deduce that (α) factors as a product of 3 prime ideals of norm z. Indeed z cannot be inert in $\mathbb{Q}(\sqrt{\Delta})$, and either $(\alpha) = \mathfrak{z}^3$ or $(\alpha) = (z)\mathfrak{z}$ where $\mathfrak{z}$ is a prime ideal above z. The case $(\alpha) = (z)\mathfrak{z}$ is equivalent to z dividing x and y and $\mathfrak{z}$ is then principal. The case $(\alpha) = \mathfrak{z}^3$ implies that $\mathfrak{z}$ has order 1 or 3 in the class group.

Given Δ, finding an element α whose norm is a third power of a prime seems computationally hard. However, one can hope to find elements of order 3 in a class group by generating Δ *a posteriori*. First fix a prime number z, then choose any integers x and y such that y^2 divides $z^3 - x^2$, and define

$$\Delta = \frac{x^2 - z^3}{y^2}.$$

To obtain a b-bit negative discriminant, one could simply choose a $b/3$-bit prime number z, a $b/2$-bit integer x larger than $z^{3/2}$, and $y = 1$. The prime ideals above z in $\mathbb{Q}(\sqrt{\Delta})$ are either principal or of order 3 in the class group. The value $y = 1$ is chosen for simplicity, but more generally, one could choose any $b/4$-bit integer y

whose prime factors satisfy $(z/p) = 1$ (z is a quadratic residue modulo p), then a $b/2$-bit integer solution x to $x^2 \equiv z^3 \mod y^2$.

4.1. **Discriminants with prescribed bits.** The above strategy allows to find 'random looking' discriminants together with a class of order 3 in the corresponding class group. It does not allow to fix the discriminant *a priori*. However, we now show that it is possible to fix half the bits of the discriminant. Let δ a $b/2$-bit integer. We are looking for a discriminant $\Delta = -(\delta + 2^{b/2}\delta')$, with δ' another $b/2$-bit integer.

Choose a $b/3$-bit prime number z so that the quadratic equation $x^2 \equiv \delta + z^3 \mod 2^{b/2}$ has a solution, and choose x a $b/2$-bit long solution. Now, let $\Delta = z^3 - x^2$. As above, the prime ideals above z in $\mathbb{Q}(\sqrt{\Delta})$ are either principal or of order 3 in the class group, and now the $b/2$ least significant bits of Δ are given by δ.

5. Binary cubic forms and their relationship to the binary quadratic forms

It is well known that there is a close relationship between binary cubic forms of discriminant $\Delta = -27D$ and ideal class group of the quadratic field $\mathcal{L} = \mathbb{Q} = (\sqrt{D})$. This section summarizes parts of [12, Chapter 3]. Given a primitive integral binary cubic form in the form

$$C(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3 \ .$$

where $a, b, c, d \in \mathbb{Z}$. Let Q be the Hessian of C. Then we have

$$Q = 9q, \quad \text{where} \quad q = (b^2 - ac, bc - ad, c^2 - bd) \ .$$

The discriminant of the binary quadratic form q is equal to

$$D = -3b^2c^2 + 4ac^3 + 4b^3d - 6abcd + a^2d^2 \ .$$

Now there is a well defined map between the $SL_2(\mathbb{Z})$-class of C and the $SL_2(\mathbb{Z})$-class of the Hessian Q. Let $Cl^+(bcf(\Delta))$ be the set of $SL_2(\mathbb{Z})$-class of binary cubic forms of discriminant $\Delta = -27D$, let $Cl^+_{\mathcal{L}}[3]$ be the 3-torsion subgroup of the narrow ideal class group of the quadratic field $\mathcal{L} = \mathbb{Q} = (\sqrt{D})$ and let $Cl^+(bqf(D))[3]$ be the $SL_2(\mathbb{Z})$-classes of binary quadratic forms isomorphic to $Cl^+_{\mathcal{L}}[3]$, than the map is given by:

$$\varphi : Cl^+(bcf(\Delta)) \longrightarrow Cl^+(bqf(D))[3]$$
$$\varphi : [(a, 3b, 3c, d)] \longrightarrow [(b^2 - ac, bc - ad, c^2 - bd)]$$

This allows to exhibit elements of order 3 in class groups of quadratic fields without even computing the class number. Unfortunately, the corresponding algorithms are more expensive that class group computations, see details in the Appendix.

6. Diophantine equations and class numbers

We have seen above that the *low order assumption* is broken for a really narrow set of primes namely Mersenne primes. Mersenne primes are number of the form

$$\Delta = 2^p - 1$$

So far about 50 Mersenne primes have been discovered making the set of Mersenne primes ultra sparse. In this section we focus on searching for other classes of possible *weak primes* with regard to the *low order assumption* in the class group of

an imaginary quadratic number field. We can slightly generalize a bit the Mersenne case with the following Theorem:

Theorem 6.1. *If $D = 4u^3 - 1$ with $u \in \mathbb{Z}_{>0}$, then the low order assumption is violated for the group of classes of primitive binary quadratic forms with discriminant $-D$.*

Proof. Let $D = 4u^3 - 1$ for some $u > 0$, let $\omega_D = (1 + \sqrt{-D})/2$ and consider the ideal $I = (u, \omega_D)$ in the ring $\mathbb{Z}[\omega_D]$ with norm u. Then $I^3 = (u^3, \omega_D^3)$ is contained in the principal ideal (ω_D) and since both have norm u^3, they are equal. Also, for $u > 1$, I is not principal since for $a, b \in \mathbb{Z}$ we have

$$N(a + b\omega_D) = (a + b/2)^2 + b^2 D/4 \geq D/4 > u$$

so the class of I has order 3. □

Replacing u with 2 and 3 with $p - 2$, i.e., $D = 2^p - 1$, proves the Mersenne case (although one has to argue slightly more, namely that the smaller powers of I are not principal because the smallest norm of a principal ideal is 2^p except for principal ideals arising from integers).

One interesting set of primes are the one of the form

$$\Delta = k2^n - 1$$

This class of primes can leverage on some of the fastest primality tests so far discovered [13] and can be potentially used by implementers due its attractive performance [1]. Note that if k is a perfect cube and $n - 2 \equiv 0 \pmod 3$ then we are in the exact situation of Theorem 6.1.

This theorem can be generalized to construct elements of arbitrary order. For instance, restricting to fundamental discriminants for simplicity:

Theorem 6.2 (Mollin [14])**.** *Let D be a squarefree number and let $\sigma = 2$ when $D \equiv 3 \pmod 4$ and $\sigma = 1$ otherwise. Assume further that $D = \sigma^2 m^t - b^2$ where $t > 1$, $m > 1$ and $b > 0$ are integers such that $b \neq 2m^{t/2} - 1$ if t is even and $b \neq \lfloor \sigma m^{t/2} \rfloor$ if t is odd. Then the ideal $(m, (b + \sqrt{-D})/\sigma)$ has order t in the ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$.*

Corollary 6.3. *Let $D = 4m^t - b^2$ be a prime number, where b and t are odd positive integers such that $b \neq \lfloor 2m^{t/2} \rfloor$. Then the ideal $(m, (b + \sqrt{-D})/2)$ has order t in the ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$.*

Let us show an example

Example 1. Let us use as discriminant
$D = -4040759726892480388249547825493979292744722294820044 7$ this corresponds to the entry $k = 27$ and $n = 170$ in [13, Table 2]. This meets the requirements of Theorem 6.1. We can easily compute $c = \sqrt[3]{k2^{n-2}} = 216172782113783808$ and obtain the primitive integral binary cubic form

$$C(x, y) = ax^3 - 3cxy^2 + dy^3.$$

computing the Hessian of C gives

$$q = (216172782113783808, -1, 467306717268134486567744669629808 64)$$

that an the element of order 3 as expected.

[1] Chia Network blockchain showed a mild interest on using this class of prime numbers, which eventually waned.

Example 2. For fixed t, the following straightforward GP script (see [15]) produces pairs (m, b) satisfying the hypotheses of Corollary 6.3 by sampling random B-bit integers. We thus obtain negative prime discriminants $b^2 - 4m^t$ with $tB + 2$ bits together with a binary quadratic form (m, b, m^{t-1}) of low order t in the corresponding classgroup.

```
loword(B, t) =
{
  while(1,
    my(b = random(2^B), m = random(2^B), mt = m^t);
    D = 4*mt - b^2;
    if (D <= 0 || b == sqrtint(4*mt) || !isprime(D), next);
    q = qfbred(Qfb(m, b, mt / m));
    q0 = q^0; /* trivial class */
    if (q == q0 || q^t != q0, error()); /* paranoia */
    return([t, m, b]));
}
```

Trying it for $B = 16$ for consecutive primes t, we obtain in about 3 seconds:

t	form $(m, b, *)$ of order t
3	$(22182, 21373, *)$
5	$(30680, 36619, *)$
7	$(22862, 59303, *)$
11	$(23366, 26165, *)$
13	$(29532, 28003, *)$
17	$(29454, 9733, *)$
19	$(10874, 3913, *)$
23	$(13310, 20463, *)$
29	$(31418, 64623, *)$
31	$(11885, 61429, *)$
37	$(45748, 24609, *)$
41	$(61340, 50381, *)$
43	$(245, 30283, *)$
47	$(3962, 53951, *)$
53	$(36034, 58875, *)$
59	$(32910, 64843, *)$

These examples show how easy it is to construct discriminants together with a low order element in their class group without computing the class number. The likelihood that such a discriminant is chosen at random is negligible, though. On the other hand, given D, it seems hard to prove that a given number is *not* of the form specified by Corollary 6.3 in general, even for a fixed order $t \geq 3$: it amounts to proving that the given hyperelliptic curve has no integer points.

In real life deployments, in order to meet the *quantum annoyance* property defined in [16], the Chia blockchain[2] picks a new random discriminant every 10 minutes. A different situation might arise though if a special prime is chosen to meet specific optimization requirements.

[2] `https://chia.net/`.

7. Conclusions

The low order assumption is an important assumption that is at the core of some cryptographic primitives: Verifiable Delay Functions, accumulators, polynomial commitments. In this work we were able to break the low order assumption in the class group of an imaginary quadratic number field for some really special class of prime numbers and we have shown how it is possible to construct malicious discriminants having prescribed properties. ICQ leverages on some well known topic in number theory but many of the assumptions are new in the field of cryptography. We hope that this work provides some incentive for researchers to think about this new problems.

Acknowledgments. We would like to thank Dan Boneh, Bram Cohen, Luca de Feo, Florian Luca, Simon Masson, István András Seres, Renate Scheidler for fruitful discussions.

References

[1] Johannes Buchmann and Hugh C. Williams. A key-exchange system based on imaginary quadratic fields. *J. Cryptology*, 1:107–118, 1988.

[2] 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.

[3] Benjamin Wesolowski. Efficient verifiable delay functions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 379–407, Cham, 2019. Springer International Publishing.

[4] K. Pietrzak. Simple verifiable delay functions. *Cryptology ePrint Archive, Report 2018/627*, 2018.

[5] 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.

[6] Benedikt Bünz, Ben Fisch, and Alan Szepieniec. Transparent snarks from dark compilers. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 677–706, Cham, 2020. Springer International Publishing.

[7] D. Boneh, B. Bünz and B. Fisch. A survey of two verifiable delay functions. *Cryptology ePrint Archive, Report 2018/712*, 2018.

[8] Istvn Andrs Seres and Pter Burcsi. A note on low order assumptions in rsa groups. Cryptology ePrint Archive, Report 2020/402, 2020. `https://eprint.iacr.org/2020/402`.

[9] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[10] D. Shanks. Class number, a theory of factorization, and genera. In *Proceedings of Symposia in Pure Mathematics*, 1971.

[11] Daniel Shanks. On Gauss's class number problems. *Math. Comp.*, 23:151–163, 1969.

[12] Samuel A. Hambleton and Hugh C. Williams. *Cubic fields with geometry*. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer, Cham, 2018.

[13] Hans Riesel. Lucasian criteria for the primality of $N = h \cdot 2^n - 1$. *Math. Comp.*, 23:869–875, 1969.

[14] R. A. Mollin. Solutions of Diophantine equations and divisibility of class numbers of complex quadratic fields. *Glasgow Math. J.*, 38(2):195–197, 1996.

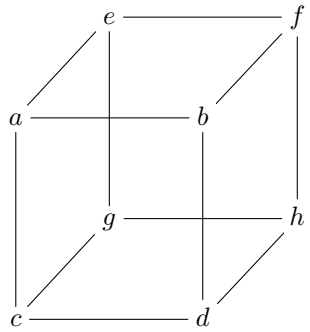
[15] The PARI Group, Bordeaux. *PARI/GP, version* `2.13.0`, 2020. `http://pari.math.u-bordeaux.fr/`.

[16] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. In Steven D. Galbraith and Shiho Moriai,

editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 248–277, Cham, 2019. Springer International Publishing.
[17] Manjul Bhargava. Higher composition laws I: A new view on Gauss composition, and quadratic generalizations. *Annals of Mathematics*, 159(1):217–250, jan 2004.
[18] Manjul Bhargava. Gauss composition and generalizations. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory - 5th International Symposium, ANTS-V Sydney, Australia, July 7-12, 2002 Proceedings*, Lecture Notes in Computer Science, pages 1–8, Germany, jan 2002. Springer Verlag. 5th International Algorithmic Number Theory Symposium, ANTS 2002 ; Conference date: 07-07-2002 Through 12-07-2002.
[19] Karim Belabas. A fast algorithm to compute cubic fields. *Math. Comp*, 66:1213–1237, 1997.
[20] Karim Belabas. On quadratic fields with large 3-rank. *Math. Comp.*, 73(248):2061–2074, 2004.
[21] J. E. Cremona. Reduction of binary cubic and quartic forms. *LMS Journal of Computation and Mathematics*, 2:6292, 1999.
[22] Daniel C. Shanks. Determining all cubic fields having a given fundamental discriminant. Unpublished manuscript, 1987.
[23] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

Appendix A. Bhargava cubes and order 3 ideal classes

A great way to visualize the correspondence defined in section 5 is using the work by Manjul Bhargava. In his cornerstone paper [17] Bhargava introduced a new composition law for binary quadratic fields (about 200 years after Gauss) and 13 new composition laws for higher degree number fields using what is now known as the *Bhargava cube*. He noticed that when putting numbers on the corners of a cube (representing a $2 \times 2 \times 2$ matrix) as below



the cube can be sliced into pairs of 2×2 matrices in three different ways

$$M_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \; N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

$$M_2 = \begin{bmatrix} a & c \\ e & g \end{bmatrix} \; N_2 = \begin{bmatrix} b & d \\ f & h \end{bmatrix}$$

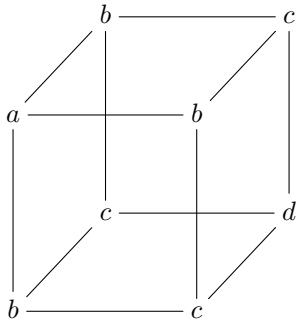
$$M_3 = \begin{bmatrix} a & e \\ b & f \end{bmatrix} \; N_3 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}$$

From these slicings, it is now possible to construct three quadratic forms having the same discriminant:

$$Q_1(x, y) = -\det(M_1 x - N_1 y)$$

$$Q_2(x,y) = -\det(M_2 x - N_2 y)$$
$$Q_3(x,y) = -\det(M_3 x - N_3 y)$$

Bhargava observed that the product of these three quadratic forms is the identity for the classic Gauss composition, and that any three quadratic forms with trivial product arrises from such a cube. Next step is to impose some symmetry to the cube (in this case forming a triply symmetric cube):

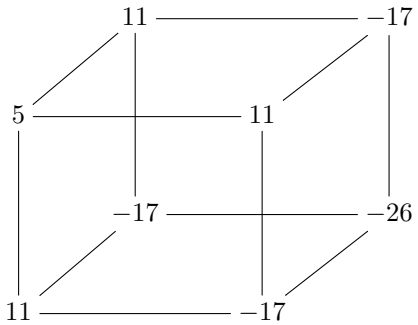


Just as symmetric square matrix defines a quadratic form, a triply symmetric cube defines a cubic form: the above cube induces the cubic form

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3.$$

We also know from the discussion above that this cube defines three binary quadratic forms whose product is the identity. So this triply symmetric cube also parametrizes an order in a quadratic fields together with three ideal classes of trivial product. The symmetries in the cube imply that all three quadratic forms are actually the same, therefore it is a quadratic form of order 1 or 3. Next step has been suggested by Bhargava in [18] where he points out that the method described by Belabas in [19] could be used to enumerate order 3 ideal classes in quadratic orders. Let us run through an example.

Example 3. Assume we want to find an element of order 3 for the binary quadratic form with discriminant $\Delta = -470551$. $-\Delta$ is a prime number equal to 7 (mod 8). Now using the algorithm in [19] we can generate the reduced defining polynomial for the binary cubic form having discriminant $3^3\Delta = 12704877$. This outputs the binary cubic form $5x^3 + (3 \cdot 11)x^2y - (3 \cdot 17)xy^2 - 26y^3$ that is equivalent to the following Bhargava cube:



This triple symmetric cube is formed by composing twice the following binary quadratic form of order 3: $206x^2 + 57xy + 575y$

Some comment about the example above: we were able to find an element of order 3 without computing the class number of the binary quadratic form. All using a combination of Belabas algorithm and Bhargava cube. Unfortunately, the algorithm listing fields with $|disc|$ in the range $[X-Y, X]$ has complexity $O(X^{3/4}+Y)$ (see [20]); in our example $Y = 0$ so we can find an element of order 3 in time about $O(X^{3/4})$. This is more expensive than computing the full class group *per se*. The variant introduced by Cremona in [21, Algorithm 2] also runs in time $O(X^{3/4})$.

Finally, Daniel Shanks's CUFFQI algorithm [22] constructs all cubic fields of a fixed fundamental discriminant X in time polynomial in $\log |X|$ (see Renate Scheidler's paper in [12, Chapter 4]) but it requires as input the 3-part of the class group of the quadratic field with that discriminant (that is actually what we are looking for!). More generally, *given* the class group and units of a number field K, the same techniques using class field theory and virtual units allow to visualize elements of arbitrary order t in the class group by exhibiting unramified extensions of degree t of K, given by a list of irreducible polynomials, see [23]. The complexity is again dominated by the time needed to compute the class number and class group structure.