Explicit bounds for 2-torsion in class groups of number fields

University of Basel

Louis Mallet-Burgues

August 5, 2024

Contents

Présentation

J'ai effectué un stage de recherche de 4 mois au département de mathématiques de l'université de Bâle sous la supervision de Philipp Habegger, chercheur en théorie des nombres. L'objet de mon stage consistait à étudier un article de Bhargava, Shankar, Taniguchi, Thorne, Tsimerman et Zhao [3] sur la 2-torsion du groupe des classes d'un corps de nombres. Bien que l'essentiel du travail de lecture d'articles et d'apprentissage des cours nécéssaires à la compréhension de l'article se faisait en autonomie, j'avais aussi la possibilité d'échanger sur de nombreux sujets pendant mes rendez-vous hebdomadaires avec M. Habegger et avec les doctorants avec qui je partageais l'open space. Le début de mon stage a surtout consisté à me familiariser d'avantage avec la théorie algébrique des nombres, la théorie des réseaux et la cohomologie des groupes. J'ai ensuite décidé de reprendre la méthode de l'article [3] de façon plus explicite. Il restait cependant un point d'ombre dans l'article qui s'est révélé plus tard être une erreur de la part des auteurs, et après en avoir parlé à M. Habegger, nous avons contourné le problème en utilisant une méthode légèrement différente. J'ai ensuite construit un contre-exemple qui montre que ce point d'ombre était bien un énoncé faux, grâce à un article de Pagano et Koymans [11]. Lors de la fin du stage, j'ai essentiellement lu des ouvrages de géométrie algébrique et de courbes elliptiques pour étudier le paragraphe 5 de l'article [3], mais le temps ne m'a pas permis d'en venir à bout.
En parallèle de ce travail de recherche, j'ai assisté au cours de master de M. Habegger intitulé "heights and diophantine equations", ce qui m'a permis de découvrir la dynamique arithmétique et les problèmes d'intersections improbables. Il y avait aussi un séminaire organisé par les doctorants et post-doctorants de l'université de Bâle chaque semaine, et c'était l'occasion de discuter avec des jeunes chercheurs travaillant sur des sujets différents. Enfin, j'ai profité du temps qu'il me restait et des connaissances que j'ai apprises là bas pour terminer de rédiger des notes de cours en théorie algébrique des nombres que j'avais commencé à écrire avant le stage.

Je tiens à remercier chaleureusement mon encadrant, Philipp Habegger, pour l'expérience formidable que j'ai vécue pendant mon stage, pour toutes nos discussions fructueuses au tableau noir et pour ses cours passionnants sur les équations diophantiennes. De même, j'aimerais exprimer ma gratitude à l'université de Bâle, à ses enseignants et à ses doctorants et post-doctorants pour leur accueil et pour l'atmosphère agréable qui règne dans l'open space. Enfin, je tiens à remercier tout particulièrement mon tuteur, François Charles, pour m'avoir aidé à trouver ce stage et pour avoir contacté M. Habegger.

Introduction

Following the work of Bhargava, Shankar, Taniguchi, Thorne, Tsimerman and Zhao [3], we give explicit bounds on the size of the 2-torsion of the class group of a number field K in terms of its discriminant $\mathrm{Disc}(K)$.
One of the main motivations for the modern formulation of algebraic number theory initially phrased by Dirichlet is the acknowledgement that some number rings are not unique factorization domains (UFD) : the fundamental theorem of arithmetic no longer holds in these rings. In this report, a number field K is a finite extension of $\mathbb{Q}$ and to such a field we may attach its ring of algebraic integers $\mathcal{O}_K$ which contains those elements of K whose minimal polynomial above $\mathbb{Q}$ is monic with integral coefficients. Though the ring $\mathcal{O}_K$ is not a UFD in general, we may still factor its *ideals* into products of prime ideals in a unique way : one says $\mathcal{O}_K$ is a *Dedekind* ring. It is equivalent for a Dedekind ring A to be a UFD and to be a principal domain, hence one may measure the obstruction of A being a UFD with the *class group* of A : it is the quotient of the group of non-zero fractional ideals of A by the subgroup of principal non-zero fractional ideals.

Example 0.1. The quadratic number field $K = \mathbb{Q}(\sqrt{-5})$ has ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ which is not a unique factorization domain : its class group has order 2 and it is generated by the class of the prime ideal $(2, 1+\sqrt{-5})$.

It is a non-trivial theorem that the class group of the ring of integers of a number field is always a *finite (abelian) group*. The usual proof relies on geometry of numbers as developped by Minkowski : the ring of integers $\mathcal{O}_K$ forms a *lattice* of the real vector space $K \otimes_{\mathbb{Q}} \mathbb{R}$ whose covolume can be computed in terms of the discriminant of K, and finding small elements in this lattice allows one to show that any ideal is equivalent to an ideal of bounded norm. However, computing the size or the structure of this class group turns out to be difficult in general. Some explicit results for abelian number fields can be obtained using the analytic class number formula of Dirichlet, but there are few general results regarding the size of the class group of a general number field.
Given a number field K and a prime p, it is somewhat easier to ask about the size of the p-torsion part of the class group of K, especially the 2-torsion part. It is conjectured that, for any $\varepsilon > 0$ and any $n \geq 1$ one has $|\mathrm{Cl}(K)(p)| = O(|\mathrm{Disc}(K)|^{\varepsilon})$ for number fields of degree n. Using techniques of geometry of numbers, the authors of [3] manage to obtain a bound of the type $O(|\mathrm{Disc}(K)|^{1/2})$ for the 2-torsion of the class group of number fields with fixed degree n, which they refine to $O(|\mathrm{Disc}(K)|^{1/2-1/(2n)+\varepsilon})$ using the Bombieri-Pila determinant method [5] to count integral points on plane algebraic curves. In this report, we make their result explicit by keeping track of all constants appearing in the Bombieri-Pila theorem 3.1 and in their method. We also fix an issue in their proof (see section 4). This leads to the following result :

Theorem 0.2. *Let $n \geq 2$ be an integer. For a number field K of degree n, one has $|\mathrm{Disc}(K)| \geq 3$ and the following inequality holds :*

$$\boxed{|\mathrm{Cl}(K)(2)| \leq C_n \cdot |\mathrm{Disc}(K)|^{\frac{1}{2}-\frac{1}{2n}+11\frac{n\log n}{\log\log|\mathrm{Disc}(K)|}}}$$

with $C_n \leq n^{n^3 \log n + O(n^3)}$. In fact one can take :

$$C_n = \left(2^{16n^2} + 2^{\frac{n^2}{4}}\,\mathrm{SG}_n\right)^n$$

where SG_n is the number of subgroups of the symetric group $\mathfrak{S}_n$.

The result obtained in [3] seems to be the state of the art regarding this general question. More recent articles obtain bounds on average or bounds for certain infinite families of number fields, sometimes relying on the generalized Riemann Hypothesis (see [9] and [11] for instance).
In section 1, we obtain the first explicit bound of the type $O(|\mathrm{Disc(K)}|^{1/2})$ for the 2-torsion of the class group of a number field of fixed degree. Although this is not the final result, it is used later in section 2 to obtain the stronger theorem 0.2. This section uses an explicit form of the Bombieri-Pila determinant method which we cover in section 3.1 : it is used to estimate the number of integral points on a smooth plane curve in a box of given size. To make this report as self-contained as possible, we recall the basics of geometry of numbers in the appendix (section 5).

1 A first estimate on the 2-torsion of the class group of a number field

Let K be a number field of degree $n = r + 2s$ with r real embeddings and $2s$ non real embeddings. For convenience we assume $n \geq 2$.
The algebra $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$ is endowed with the p-norm for $p \geq 1$ defined by the formula :

$$|x|_p = \left(\sum_i |x_i|^p + 2 \sum_j \left|z_j\right|^p \right)^{1/p}$$

with $x = (x_1, \ldots, x_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s$. The limit case is the infinite-norm, given by :

$$|x|_\infty = \sup(\sup_i |x_i|, \sup_j \left|z_j\right|)$$

In these notes we shall only consider the norms $|\bullet|_2$ and $|\bullet|_\infty$. Note that $|\bullet|_2$ is a Euclidean norm induced by the trace :

$$|x|_2^2 = \mathrm{Tr}_{K_{\mathbb{R}}/\mathbb{R}}(x\overline{x})$$

with $\overline{x} = (x_1, \ldots, x_r, \overline{z_1}, \ldots, \overline{z_s})$. It is an easy exercise to check that this norm is sub-multiplicative.
The vector space $K_{\mathbb{R}}$ is endowed with the usual Lebesgue measure on $\mathbb{R}^n$, which comes from the following n-form :

$$dx_1 \wedge \ldots dx_r \wedge d\,\mathrm{Re}\, z_1 \wedge d\,\mathrm{Im}\, z_1 \wedge \cdots \wedge d\,\mathrm{Re}\, z_s \wedge d\,\mathrm{Im}\, z_s$$

The ring of integers $\mathcal{O}_K$ is a lattice of $K_{\mathbb{R}}$ whose covolume (see 5) is given by :

$$\mathrm{covol}(\mathcal{O}_K) = \frac{|\mathrm{Disc}\, K|^{1/2}}{2^s}$$

for that measure. More generally any fractional ideal I of K is a lattice with covolume :

$$\mathrm{covol}(I) = \mathrm{covol}(\mathcal{O}_K)\|I\|$$

where $\|I\|$ denotes the norm of the ideal I over $\mathbb{Q}$.
The field K has n infinite places taking multiplicity into account. If v is an infinite place, we write $|\bullet|_v$ for the absolute value on K that represents v and extends the usual absolute value on $\mathbb{Q}$.
The following theorem gives the first general estimate on the size of the 2-torsion of the class group.

Theorem 1.1. *Let $m \geq 2$ be an integer. For any $\omega \in \mathrm{Cl}(K)(m)$, one can find some $\beta \in \mathcal{O}_K \setminus \{0\}$ so that :*

$$[\beta\mathcal{O}_K] = \omega^m$$

and :

$$\left|\beta\right|_\infty \leq |\mathrm{Disc}(K)|^{\frac{m}{2n}}$$

In particular one has :

$$\boxed{|\mathrm{Cl}(K)(m)| \leq \left|\overline{B}_\infty\left(0, |\mathrm{Disc}(K)|^{\frac{m}{2n}}\right) \cap \mathcal{O}_K^{[m]}\right|}$$

where $\mathcal{O}_K^{[m]}$ denotes the set of $\beta \in \mathcal{O}_K$ such that $\left|N_{K/\mathbb{Q}}(\beta)\right|^{1/m} \in \mathbb{Z}$.

Proof. Pick some representative $I \subseteq \mathcal{O}_K$ for ω. Since $\omega^m = 1$, there is some $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that $I^m = \alpha\mathcal{O}_K$.
Now consider the compact convex symetric body :

$$A = \{x \in K_{\mathbb{R}} \mid \forall v \ |x|_v \leq C_v\}$$

where the C_v are some constants yet to be chosen for each v an infinite place. One has :

$$\mathrm{vol}(A) = 2^r \pi^s \prod_v C_v$$

where the product takes into account the multiplicity of places (i.e each complex place appears twice). By choosing $C_v = |\mathrm{Disc}\, K|^{1/(2n)} |\alpha|_v^{-1/m}$ one has :

$$2^n \,\mathrm{covol}(I^{-1}) = 2^{n-s} |\mathrm{Disc}(K)|^{1/2} \|I\|^{-1} = 2^{n-s} |\mathrm{Disc}(K)|^{1/2} \left|N_{K/\mathbb{Q}}(\alpha)\right|^{-1/m} \leq \mathrm{vol}(A)$$

since $2^r \pi^s \geq 2^{n-s}$. By Minkowski's first theorem 5.5, one can find $\kappa \in I^{-1} \cap A$ non zero. Now put :

$$\beta = \alpha \kappa^m \in O_K$$

which is an element of $\mathcal{O}_K$ since $\kappa \in I^{-1}$. Therefore :

$$(\kappa I)^m = \beta \mathcal{O}_K$$

and $[\kappa I] = \omega$. By construction :

$$\left|\beta\right|_\infty \leq |\mathrm{Disc}(K)|^{\frac{m}{2n}}.$$

Moreover one clearly has $\beta \in \mathcal{O}_K^{[m]}$. Hence the map :

$$\overline{B}_\infty \left(0, |\mathrm{Disc}(K)|^{\frac{m}{2n}}\right) \cap \mathcal{O}_K^{[m]} \setminus \{0\} \longrightarrow \mathrm{Cl}(K)(m)$$

sending β to the class of the m-th root of the ideal $\beta\mathcal{O}_K$ if it exists and to 1 otherwise is onto, which yields the desired inequality. □

Now observe that the first successive minimum of the lattice $\mathcal{O}_K$ for the 2-norm is $\sqrt{n}$ (achieved for instance at $x = 1$), in other words :

$$\inf_{x \in \mathcal{O}_K \setminus \{0\}} |x|_2 = \sqrt{n}.$$

This is becaue, for any $x \in \mathcal{O}_K \setminus \{0\}$ the inequality of arithmetic and geometric means gives :

$$N_{K_{\mathbb{R}}/\mathbb{R}}(x\overline{x})^{1/n} \leq \frac{1}{n} \mathrm{Tr}_{K_{\mathbb{R}}/\mathbb{R}}(x\overline{x}) = \frac{|x|_2^2}{n}$$

and $N_{K/\mathbb{Q}}(x) \in \mathbb{Z} \setminus \{0\}$.

Hence, using theorems 5.9 and 5.10 from appendix 1, there exists a sub-lattice Λ of $\mathcal{O}_K$ and a basis $(v_1, \ldots, v_n)$ of Λ (hence with $v_i \in \mathcal{O}_K$) such that :

$$\lambda_i^{(2)} = |v_i|_2$$

where $\lambda_i^{(2)}$ stands for the i-th successive minimum of $\mathcal{O}_K$ for the norm $|\bullet|_2$, and such that :

$$v_1 = 1.$$

Let $(v_1^*, \ldots, v_n^*)$ denote the dual basis of $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q})$ that corresponds to this basis. The following theorem shows that the lattice $\mathcal{O}_K$ is not too skew when it has no small non-trivial subfields.

Theorem 1.2. *Let $\kappa \in \{2, \ldots, n\}$ be an integer such that K has no non-trivial subfield of degree strictly lower than κ. Suppose*

$$n - \kappa = q(\kappa - 1) + r$$

with $0 \leq r < \kappa - 1$. Then one has the inequality :

$$\lambda_{n-\kappa+2}^{n-\kappa} \leq \left(\prod_{i=2}^{n-\kappa+1} \lambda_i\right) \cdot \left(\prod_{j=n+2-\kappa-q}^{n-\kappa+1} \lambda_j\right)^{\kappa-1} \cdot \lambda_{n+1-\kappa-q}^r$$

where the successive minima λ_i are given by the 2-norm.

Proof. Consider the $\mathbb{Q}$-vector space :

$$L = \mathrm{Vect}_{\mathbb{Q}}(v_1, v_2, \dots, v_{n-\kappa+1}).$$

Observe the following fact : let $r \in K$ be such that $rL \subseteq L$. Thus L is a $\mathbb{Q}(r)$-vector space and its $\mathbb{Q}$-codimension in K is divisible by $[\mathbb{Q}(r) : \mathbb{Q}]$:

$$[\mathbb{Q}(r) : \mathbb{Q}] \mid \kappa - 1$$

which contradicts the minimality of κ unless we have $r \in \mathbb{Q}$. Therefore for any irrational $r \in K \setminus \mathbb{Q}$, L is not stable by multiplication by r.
Let us turn this observation into a linear algebra problem by defining $V = \mathrm{Vect}_{\mathbb{Q}}(v_2, \dots, v_{n-\kappa+1})$ and by considering the map :

$$V \longrightarrow (K/L)^{n-\kappa}$$

sending r to $(\pi(rv_2), \dots, \pi(rv_{n-\kappa+1}))$ with $\pi : K \longrightarrow K/L$ the projection. By the previous observation and because $v_1 = 1$, this map is injective.
Therefore the matrix of this map in the natural bases has a maximal square sub-matrix with non zero determinant and the usual formula for determinant yields some injective map:

$$\sigma : \{2, \dots, n-\kappa+1\} \longrightarrow \{2, \dots, n-\kappa+1\} \times \{n-\kappa+2, \dots, n\}$$

which we can write $\sigma = (\alpha, \beta)$ such that for all i :

$$v^*_{\beta(i)}\left(v_i v_{\alpha(i)}\right) \neq 0$$

The family $\left(v_1, v_2, \dots, v_{n-\kappa+1}, \left(v_i v_{\alpha(i)}\right)\right)$ is then free, hence by definition of $\lambda_{n-\kappa+2}$ one has :

$$\left|v_i v_{\alpha(i)}\right|_2 \geq \lambda_{n-\kappa+2}.$$

By sub-multiplicativity of the 2-norm one has :

$$\lambda_{n-\kappa+2} \leq \lambda_i \lambda_{\alpha(i)}.$$

Using that σ is injective, the fibers of α have cardinality at most $\kappa - 1$. By multiplying these inequations with i ranging from 2 to $n - \kappa + 1$ one has :

$$\lambda_{n-\kappa+2}^{n-\kappa} \leq \left(\prod_{i=2}^{n-\kappa+1} \lambda_i\right) \cdot \left(\prod_{j=n+2-\kappa-q}^{n-\kappa+1} \lambda_j\right)^{\kappa-1} \cdot \lambda_{n+1-\kappa-q}^{r}$$

as desired. □

By applying the previous theorem with $\kappa = 2$ (hence $r = 0$ et $q = n - 2$), we obtain :

$$\lambda_n^{n-2} \leq \prod_{i=2}^{n-1} \lambda_i^2$$

Multiply by λ_n^2 to get the inequality :

$$\lambda_n^n \leq \prod_{i=2}^{n} \lambda_i^2 = \frac{1}{n} \prod_{i=1}^{n} \lambda_i^2$$

Now use Minkowski's second theorem 5.12 to obtain the following theorem.

Theorem 1.3. *One has the following estimate for the n-th successive minimum of the lattice $\mathcal{O}_K$ for the 2-norm :*

$$\boxed{\lambda_n^{(2)} \leq A_n |\mathrm{Disc}(K)|^{1/n}}$$

with a constant that depends only on n :

$$A_n = \frac{4}{\pi} \frac{\Gamma\left(\frac{n}{2} + 1\right)^{2/n}}{n^{1/n}} \sim \frac{2n}{\pi e}$$

as n goes to infinity.

Proof. By Minkowski's second theorem and since $|\bullet|_2$ is a Euclidean norm one has :

$$\prod_i \lambda_i \leq 2^n \frac{\mathrm{covol}(\mathcal{O}_K)}{\mathrm{vol}(B(0,1))}$$

where $B(0,1)$ is the unit ball of $K_{\mathbb{R}}$ for the 2-norm. The desired inequality follows immediately using the fact that $2r+3s \leq 2n$. Now one has :

$$\begin{aligned} A_n &= \frac{4}{\pi} \frac{\Gamma\left(\frac{n}{2}+1\right)^{2/n}}{n^{1/n}} \\ &= \frac{4}{\pi} \frac{\left(\left(\frac{n}{2e}\right)^{n/2} \sqrt{\pi n}\right)^{2/n} (1+o(1))^{2/n}}{n^{1/n}} \\ &= \frac{4}{\pi} \frac{n}{2e} \pi^{1/n} (1+o(1)) \\ &= \frac{2n}{\pi e}(1+o(1)) \end{aligned}$$

as desired. □

In the appendix, lemma 7.2 we show that for any integer $n \geq 1$, one has :

$$A_n \leq 3n$$

hence in the rest of these notes we shall remember the simpler bound :

$$\boxed{\lambda_n^{(2)} \leq 3n |\mathrm{Disc}(K)|^{1/n}}.$$

Note that this is also true for $n = 1$.
Combining theorems 1.1, 1.3 and 5.13 in the case $m = 2$, we obtain a first bound for the size of the 2-torsion of the class group.

Theorem 1.4. *Let K be a number field of degree $n \geq 1$. Then one has :*

$$\boxed{|\mathrm{Cl}(K)(2)| \leq (15n)^n 2^{n^2} |\mathrm{Disc}(K)|^{1/2}} \leq 2^{4n^2} |\mathrm{Disc}(K)|^{1/2}.$$

Note that the last inequality is really poor but it will suffice for theorem 0.2 because it will be in competition with much larger quantities.

Proof. We first suppose $n \geq 2$. We start using theorem 5.13 on the number of points in the intersection of a lattice with a set :

$$\begin{aligned} |\mathrm{Cl}(K)(2)| &\leq \left|\overline{B}_\infty\left(0, |\mathrm{Disc}(K)|^{\frac{1}{n}}\right) \cap \mathcal{O}_K\right| \\ &\leq \frac{\mathrm{vol}\left(\overline{B}_\infty\left(0, |\mathrm{Disc}(K)|^{\frac{1}{n}} + 2^n \lambda_n^{(\infty)}\right)\right)}{\mathrm{covol}(\Lambda)} \\ &\leq \frac{2^s 2^r \pi^s \left(|\mathrm{Disc}(K)|^{\frac{1}{n}} + 2^n \lambda_n^{(\infty)}\right)^n}{|\mathrm{Disc}\, K|^{1/2}} \end{aligned}$$

From theorem 1.3 we have :

$$\lambda_n^{(\infty)} \leq \lambda_n^{(2)} \leq 3n |\mathrm{Disc}(K)|^{1/n}$$

since $|\bullet|_\infty \leq |\bullet|_2$. Therefore :

$$\begin{aligned} |\mathrm{Cl}(K)(2)| &\leq 2^s 2^r \pi^s (1+2^n 3n)^n |\mathrm{Disc}(K)|^{1/2} \leq (2\sqrt{\pi})^n 2^{n^2} (4n)^n |\mathrm{Disc}(K)|^{1/2} \leq (8\sqrt{\pi}n)^n 2^{n^2} |\mathrm{Disc}(K)|^{1/2} \\ &\leq (15n)^n 2^{n^2} |\mathrm{Disc}(K)|^{1/2} \end{aligned}$$

as desired. Notice that it clearly holds for $n = 1$. Eventually we conclude by using some rough inequalities, provided that $n \geq 2$:

$$(15n)^n 2^{n^2} \leq 2^{4n+n\log_2 n+n^2} \leq 2^{4n+2n^2} \leq 2^{4n^2}.$$

□

2 Power saving

We now want to perform some power saving on the exponent 1/2 on the discriminant in theorem 1.4. Following [3] we shall prove theorem 0.2. For what follows it will be convenient to make the following observation which is an easy consequence of a theorem of Minkowski stating the inequality $|\mathrm{Disc}(K)| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^n$ (one can also use Stickelberger's criterion which says that the discriminant of a number field must be congruent to 0 or 1 modulo 4) :

Lemma 2.1. *If K is a number field of degree at least 2, then :*

$$|\mathrm{Disc}(K)| \geq 3.$$

In particular $\log|\mathrm{Disc}(K)| \geq 1$.

2.1 Case where K has no subfield of index 2

Let us suppose here that K has no subfield of index 2.
Thanks to theorem 1.1, we know that our goal is to get a more precise bound for how many $\beta \in O_K^{[2]}$ satisfy $\left|\beta\right|_\infty \leq |\mathrm{Disc}(K)|^{1/n}$.
To do this we make a dichotomy : we first count those β whose characteristic polynomial $\chi_\beta(X) = N_{K/\mathbb{Q}}(X-\beta)$ over $\mathbb{Q}$ is a square and then those for which χ_β is not a square.

Lemma 2.2. *Let $a \in K$ and let π_a denote the minimal polynomial of a. One has :*

$$\chi_a = \pi_a^{[K:\mathbb{Q}(a)]}$$

and the following are equivalent :

- *The polynomial χ_a is a square in $\mathbb{Q}[x]$.*
- *The index $[K:\mathbb{Q}(a)]$ is even.*

Proof. Let π_a denote the minimal polynomial of a. One has :

$$\chi_a = \pi_a^j$$

where $j = [K:\mathbb{Q}(a)]$ because for each conjugate b of a, there are exactly j many $\sigma \in \mathrm{Hom}_{\mathbb{Q}-\mathrm{alg}}(K,\mathbb{C})$ sending a to b (they correspond to the extensions to K of the only morphism $\mathbb{Q}(a) \longrightarrow \mathbb{C}$ that sends a to b). The equivalence then follows from the irreducibility of π_a. □

Theorem 2.3. *Suppose K has degree $n \geq 2$ and has no subfield of index 2. Then the number of $\beta \in \mathcal{O}_K$ such that χ_β is a square in $\mathbb{Q}(X)$ and such that $\left|\beta\right|_\infty \leq |\mathrm{Disc}(K)|^{1/n}$ is bounded above by :*

$$2^{\frac{n^2}{4}}\,\mathrm{SG}_n\,|\mathrm{Disc}(K)|^{1/4}$$

where the SG_n is the number of subgroups of the symetric group $\mathfrak{S}_n$.

Proof. Denote by ℓ this number we wish to estimate. From lemma 2.2, we have :

$$\ell \leq \sum_{\substack{F\subseteq K,\\ [K:F]\equiv 0\ [2]}} \left|\mathcal{O}_K \cap \overline{B}_\infty\left(0, |\mathrm{Disc}(K)|^{\frac{1}{n}}\right) \cap F\right| = \sum_{\substack{F\subseteq K,\\ [K:F]\equiv 0\ [2]}} \left|\mathcal{O}_F \cap \overline{B}_\infty\left(0, |\mathrm{Disc}(K)|^{\frac{1}{n}}\right)\right|$$

For such F we have $|\mathrm{Disc}(K)| = \left\|\mathcal{D}_{K/F}\right\|_{F/\mathbb{Q}} \cdot |\mathrm{Disc}(F)|^{[K:F]}$ with $\mathcal{D}_{K/F}$ the relative discriminant, hence :

$$|\mathrm{Disc}(F)| \leq |\mathrm{Disc}(K)|^{1/[K:F]}.$$

Now notice that the restriction of the infinite norm of K to F is exactly the infinite norm on F because any embedding of F can be extended to an embedding of K. Therefore for any such F of degree $d = r_F + 2s_F$ one has, using theorems 5.13 and 1.3 (with $R = |\mathrm{Disc}(K)|^{1/n}$) :

$$\begin{aligned}
\left|\mathcal{O}_F \cap \overline{B}_\infty(0,R)\right| &\leq \frac{2^{r_F+s_F}\pi^{s_F}\left(R + 2^d \lambda_d^{(\infty)}(\mathcal{O}_F)\right)^d}{|\mathrm{Disc}(F)|^{1/2}} \\
&\leq 2^{r_F+s_F}\pi^{s_F}\left(R + 2^d \lambda_d^{(2)}(\mathcal{O}_F)\right)^d \\
&\leq 2^{r_F+s_F}\pi^{s_F}\left(R + 2^d 3d\,|\mathrm{Disc}(F)|^{1/d}\right)^d \\
&\leq 2^{r_F+s_F}\pi^{s_F}\left(R + 2^d 3d\,|\mathrm{Disc}(K)|^{1/n}\right)^d \\
&\leq 2^{r_F+s_F}\pi^{s_F}\,|\mathrm{Disc}(K)|^{d/n}\left(1 + 2^d 3d\right)^d \\
&\leq 2^{r_F+s_F}\pi^{s_F}\,|\mathrm{Disc}(K)|^{1/4}\left(1 + 2^d 3d\right)^d \\
&\leq 2^{4d^2}\,|\mathrm{Disc}(K)|^{1/4} \leq 2^{4(n/4)^2}\,|\mathrm{Disc}(K)|^{1/4} \leq 2^{n^2/4}|\mathrm{Disc}(K)|^{1/4}
\end{aligned}$$

using the same inequality as in the proof of 1.4, and using the facts that $|\mathrm{Disc}(F)| \geq 1$ and $[K : F] \geq 4$ since by hypothesis $[K : F]$ is even and K has no subfield of index 2. Now the number of subfields of K is bounded by the number of subgroups of the symetric group $\mathfrak{S}_n$ by Galois theory, which concludes the proof. □

Now let us count those β for which χ_β is not a square. First we need the following lemma.

Lemma 2.4. *Suppose K has degree $n \geq 2$ and has no subfield of index 2. Consider the projection :*

$$K_{\mathbb{R}} \xrightarrow{\pi} K_{\mathbb{R}}/\mathbb{R}.$$

Then one has the following estimate :

$$\boxed{\left|\pi\left(\overline{B}_\infty\left(0, |\mathrm{Disc}(K)|^{\frac{1}{n}}\right) \cap \mathcal{O}_K\right)\right| \leq 2^{4n^2}\,|\mathrm{Disc}(K)|^{1/2-1/n}}.$$

Proof. Notice that $\mathbb{Z} \subseteq \mathcal{O}_K$ and $\pi(\mathcal{O}_K) = \mathcal{O}_K/\mathbb{Z}$. Put $R = |\mathrm{Disc}(K)|^{1/n}$. For each line $L \in \pi\left(\overline{B}_\infty(0,R) \cap \mathcal{O}_K\right)$, one has :

$$2R - 1 \leq \left|L \cap \overline{B}_\infty(0,2R) \cap \mathcal{O}_K\right|$$

for, if x is any element of $L \cap \mathcal{O}_K$ (thus $L = x + \mathbb{R}$), the points $x + k$ for $|k| \leq R$ all lie in $L \cap \overline{B}_\infty(0,2R) \cap \mathcal{O}_K$, and there are $2\lfloor R \rfloor + 1 \geq 2R - 1$ such points. Since these lines are disjoint from each other it follows that :

$$\left|\pi\left(\overline{B}_\infty(0,R) \cap \mathcal{O}_K\right)\right| \cdot (2R-1) \leq \left|\overline{B}_\infty(0,2R) \cap \mathcal{O}_K\right|.$$

Now we use the same method as in theorem 1.4 to bound the right hand side :

$$\left|\overline{B}_\infty(0,2R) \cap \mathcal{O}_K\right| \leq 2^{r+s}\pi^s(2 + 2^n 3n)^n\,|\mathrm{Disc}(K)|^{1/2} \leq 2^{r+s}\pi^s 2^{n^2}(4n)^n\,|\mathrm{Disc}(K)|^{1/2} \leq 2^{4n^2}\,|\mathrm{Disc}(K)|^{1/2}.$$

Now one concludes using the fact that $2R - 1 \geq R$ since $R \geq 1$. □

Theorem 2.5. *Suppose K has degree $n \geq 2$ and has no subfield of index 2, and suppose that the following holds :*

$$|\mathrm{Disc}(K)| \geq e^{6n^2}.$$

Then the number of $\beta \in \mathcal{O}_K^{[2]}$ such that χ_β is not a square in $\mathbb{Q}[X]$ and $\left|\beta\right|_\infty \leq |\mathrm{Disc}(K)|^{1/n}$ is bounded above by :

$$2^{16n^2}(\log|\mathrm{Disc}(K)|)^{2n+9/2}\,|\mathrm{Disc}(K)|^{\frac{1}{2}-\frac{1}{2n}}.$$

Proof. Let again $R = |\mathrm{Disc}(K)|^{1/n}$, and denote by g the number of such β we wish to count.
First observe that if $\beta \in \mathcal{O}_K$, whether χ_β is a square or not only depends on the class of β modulo $\mathbb{Z}$.
Therefore :

$$g = \sum_{c \in \pi\left(\overline{B}_\infty(0,R) \cap \mathcal{O}_K\right)} g_c$$

where g_c is the number of β in the class c such that $g_c \in \mathcal{O}_K^{[2]} \cap \overline{B}(0,R)$.
Fix a class $c = \pi(\beta)$ and let us bound g_c. The elements we wish to count are the $\beta - k \in \overline{B}(0,R)$ with $k \in \mathbb{Z}$ and $\left|N_{K/\mathbb{Q}}(\beta - k)\right| = \left|\chi_\beta(k)\right|$ is a square. This imposes to have $|k| \leq 2R$ by triangular inequality (since $|k|_\infty = |k|$). Since $\chi_\beta = \pi_\beta^q$ where $q = [K : \mathbb{Q}(\beta)]$ is odd, it is equivalent for $\left|\chi_\beta(k)\right|$ to be a square and for $\left|\pi_\beta(k)\right|$ to be a square, where π_β denotes the minimal polynomial of β.
Therefore :

$$g_c \leq \left|\left\{k \in [-2R, 2R] \cap \mathbb{Z} \mid \pi_\beta(k) \text{ is a square}\right\}\right| + \left|\left\{k \in [-2R, 2R] \cap \mathbb{Z} \mid -\pi_\beta(k) \text{ is a square}\right\}\right|.$$

Let us eliminate the case where β is rational (i.e. $\beta \in \mathbb{Z}$ because β is an algebraic integer). There is only one class, namely $\pi(0)$ for which this happens, and in this case we can use the rough bound :

$$g_{\pi(0)} \leq 5R.$$

Now suppose β is irrational, hence $d = \deg \pi_\beta \geq 2$. Consider the $\mathbb{C}$-irreducible curves of degree d : $C : y^2 = \pi_\beta(x)$ and $C' : y^2 = -\pi_\beta(x)$ over $\mathbb{Q}$.
Notice that for all $k \in [-2R, 2R] \cap \mathbb{Z}$ one has :

$$\left|\pi_\beta(k)\right| = \prod_{\sigma : K \longrightarrow \mathbb{C}} \left|k - \sigma(\beta)\right|^{1/q} \leq (3R)^{n/q} = (3R)^d$$

Hence if $y^2 = \pm\pi_\beta(k)$ one has $\left|y\right| \leq (3R)^{d/2}$.
Therefore g_c is bounded above by the number of integral points (x, y) (i.e. points with coordinates in $\mathbb{Z}$) on C and C' with $|x| \leq 2R$ and $\left|y\right| \leq (3R)^{d/2}$.
Put $t = 2(3R)^{d/2}$ so that, since $4R \leq t$, the points we need to count are contained in some square of side t. By assumption on the discriminant, one has :

$$t \geq 2\left(3 \cdot \left(e^{6n^2}\right)^{1/n}\right)^{d/2} \geq e^{3dn} \geq e^{3d^2}$$

which is the assumption we need to use the Bombieri-Pila theorem 3.1. With $N_d = 40 \cdot (5e)^{4d} d^{2d}$ as introduced in theorem 3.1 and $\Delta = |\mathrm{Disc}(K)| \geq 3$, one obtains :

$$\begin{aligned}
g_c &\leq 2N_d \cdot (\log t)^{2d+9/2} t^{1/d} \leq 2N_n \cdot \left(\log 2 + \frac{n}{2}\log 3 + \frac{d}{2n}\log\Delta\right)^{2n+9/2} \sqrt{6} \cdot \Delta^{\frac{1}{2n}} \\
&\leq 2\sqrt{6}N_n \cdot \left(\frac{d}{2n}\log\Delta\left(1 + \frac{2n\log 2}{6dn^2} + \frac{n^2\log 3}{6dn^2}\right)\right)^{2n+9/2} \cdot \Delta^{\frac{1}{2n}} \\
&\leq 2\sqrt{6}N_n \cdot \left(\frac{d}{2n}\log\Delta\left(1 + \frac{\log 2}{12} + \frac{\log 3}{12}\right)\right)^{2n+9/2} \cdot \Delta^{\frac{1}{2n}} \\
&\leq 2\sqrt{6}N_n \cdot (\log\Delta)^{2n+9/2} \cdot \Delta^{\frac{1}{2n}}
\end{aligned}$$

using $n \geq d \geq 2$, $\Delta \geq e^{6n^2}$ and $1 + \log(6)/12 \leq 2$. Now we sum over all $c \in \pi\left(\overline{B}_\infty(0,R) \cap \mathcal{O}_K\right)$ using lemma 2.4 (as well as $g_{\pi(0)}$) to get :

$$\begin{aligned}
g &\leq 2\sqrt{6}N_n \cdot (\log\Delta)^{2n+9/2} \cdot \Delta^{\frac{1}{2n}} \times 2^{4n^2}\Delta^{1/2-1/n} + 5\Delta^{1/n} \\
&\leq 2\sqrt{6} \cdot 2^{4n^2} N_n (\log\Delta)^{2n+9/2} \Delta^{\frac{1}{2}-\frac{1}{2n}} + 5\Delta^{\frac{1}{2}-\frac{1}{2n}} \\
&\leq 6 \cdot 2^{4n^2} N_n (\log\Delta)^{2n+9/2} \Delta^{\frac{1}{2}-\frac{1}{2n}}
\end{aligned}$$

and then we use easy inequalities :

$$\log_2(6 \cdot 2^{4n^2} N_n) = 4n^2 + 2n\log_2(n) + 4n\log_2(5e) + \log_2(240) \leq 6n^2 + 4n\log_2(5e) + \log_2(240) \leq 16n^2$$

since $n \geq 2$. This concludes the proof. □

Corollary 2.6. *Let K be a number field of degree $n \geq 1$ that has no subfield of index 2. Then the following inequality holds :*

$$\boxed{|\mathrm{Cl}(K)(2)| \leq B_n \cdot \left(\log_{\geq 1} |\mathrm{Disc}(K)|\right)^{2n+9/2} |\mathrm{Disc}(K)|^{\frac{1}{2}-\frac{1}{2n}}}$$

with $B_n = 2^{16n^2} + 2^{\frac{n^2}{4}}\,\mathrm{SG}_n \leq n^{n^2 \log n + O(n^2)}$, *and* $\log_{\geq 1}(x) = \max(\log(x), 1)$.

Proof. Under the assumption $|\mathrm{Disc}(K)| \geq e^{6n^2}$ (which implies $n \geq 2$), it is straightforward by adding the bounds of theorems 2.3 and 2.5 together and using theorem 1.1.
Now if $|\mathrm{Disc}(K)| \leq e^{6n^2}$ then theorem 1.4 gives :

$$|\mathrm{Cl}(K)(2)| \leq 2^{4n^2} e^{3n^2} \leq 2^{16n^2} \leq B_n$$

as one can easily check by taking the logarithm, so the inequality still holds in this case using $\log_{\geq 1}$ instead of log. □

2.2 General case

Now we deal with the general case in order to prove theorem 0.2 using relative genus theory results coming from [10]. For convenience, let us first state the few elementary results that we will need.

Lemma 2.7.

- *For any integer $n \geq 1$, denote by $\omega(n)$ the number of divisors of n. Using [12], theorem 11, we have for $n \geq 3$:*

$$\omega(n) \leq 1.4 \frac{\log n}{\log\log n}.$$

- *The quantity B_n defined in 2.6 increases with n. This is because $\mathfrak{S}_n$ embeds in $\mathfrak{S}_{n+1}$ for all n.*
- *For all $x \geq 3$ one has :*

$$(\log\log x)^2 \leq \log x.$$

Suppose that K has degree at least 2. In particular from lemma 2.1 the absolute value of the discriminant of K, which we will denote by Δ for convenience, is at least 3 :

$$\Delta \geq 3.$$

By induction we can find $F \subseteq K$ a subfield of index 2^r which has no subfield of index 2, for some $r \geq 0$. We denote by $\mathrm{r}_2(K)$ the dimension of the $\mathbb{F}_2$-vector space $\mathrm{Cl}(K)(2)$, in other words :

$$\mathrm{r}_2(K) = \log_2(|\mathrm{Cl}(K)(2)|).$$

Using [10], theorem 2.7 which is obtained by inductively applying relative genus theory for quadratic extensions, we have :

$$\mathrm{r}_2(K) \leq 2^r\,\mathrm{r}_2(F) + nr \cdot \omega\left(\left\|\mathcal{D}_{K/F}\right\|_{F/\mathbb{Q}}\right)$$

where $n = [K : \mathbb{Q}]$ and $\mathcal{D}_{K/F}$ denotes the relative discriminant of the extension K/F. Recall we have the following formula for relative discriminants :

$$\Delta = |\mathrm{Disc}(K)| = \left\|\mathcal{D}_{K/F}\right\|_{F/\mathbb{Q}} \cdot |\mathrm{Disc}(F)|^{[K:F]}$$

from which we deduce that $\left\|\mathcal{D}_{K/F}\right\|_{F/\mathbb{Q}} \mid \Delta$ hence $\omega\left(\left\|\mathcal{D}_{K/F}\right\|_{F/\mathbb{Q}}\right) \leq \omega(\Delta)$ and $|\mathrm{Disc}(F)| \leq \Delta^{2^{-r}}$. Now applying theorem 2.6 to F we obtain, using that B_n is increasing with n :

$$\begin{aligned}
\mathrm{r}_2(K) &\leq 2^r \log_2(B_{2^{-r}n}) + 2^r\left(2\frac{n}{2^r} + \frac{9}{2}\right)\log_2\left(\log_{\geq 1}|\mathrm{Disc}(F)|\right) + 2^r\left(\frac{1}{2} - \frac{2^{r-1}}{n}\right)\log_2|\mathrm{Disc}(F)| + nr\omega(\Delta) \\
&\leq n\log_2(B_n) + \left(2n + 9\cdot 2^{r-1}\right)\log_2\left(\log_{\geq 1}\Delta\right) + \left(\frac{1}{2} - \frac{2^{r-1}}{n}\right)\log_2\Delta + n\log_2(n)\omega(\Delta) \\
&\leq n\log_2(B_n) + \left(2n + \frac{9}{2}n\right)\log_2(\log\Delta) + \left(\frac{1}{2} - \frac{1}{2n}\right)\log_2\Delta + 1.4n\log_2(n)\frac{\log\Delta}{\log\log\Delta} \\
&\leq n\log_2(B_n) + \log_2\Delta\left(\frac{13}{2}n\frac{\log\log\Delta}{\log\Delta} + \frac{1}{2} - \frac{1}{2n} + 1.4\frac{n\log n}{\log\log\Delta}\right)
\end{aligned}$$

Now notice that :

$$\frac{\log\log\Delta}{\log\Delta} \leq \frac{1}{\log\log\Delta}$$

because $\Delta \geq 3$ and using the last part of lemma 2.7. Using this bound we obtain :

$$\begin{aligned} r_2(K) &\leq n\log_2(B_n) + \log_2\Delta\left(\frac{1}{2} - \frac{1}{2n} + \frac{1.4n\log n + 6.5n}{\log\log\Delta}\right) \\ &\leq n\log_2(B_n) + \log_2\Delta\left(\frac{1}{2} - \frac{1}{2n} + \frac{1.4n\log n + \frac{6.5}{\log 2}n\log n}{\log\log\Delta}\right) \\ &\leq n\log_2(B_n) + \log_2\Delta\left(\frac{1}{2} - \frac{1}{2n} + 11\frac{n\log n}{\log\log\Delta}\right) \end{aligned}$$

And by taking the exponential in base 2 we prove theorem 0.2 :

$$|\mathrm{Cl}(K)(2)| \leq C_n \cdot |\mathrm{Disc}(K)|^{\frac{1}{2} - \frac{1}{2n} + 11\frac{n\log n}{\log\log|\mathrm{Disc}(K)|}}$$

with $C_n = B_n^n \leq n^{n^3\log n + O(n^3)}$.

3 The Bombieri-Pila determinant method

The goal of this section is to give a complete proof of a theorem of Bombieri and Pila [5] that aims to give an upper bound to the number of points with bounded integer coordinates on some real curve that is irreducible over the complex numbers (we say it is absolutely irreducible).
We obtain a slightly better bound by using a more recent paper [4] and by making all estimations explicit.

Theorem 3.1. *Let $F \in \mathbb{R}[X,Y]$ be a $\mathbb{C}$-irreducible polynomial of degree $d \geq 2$. Denote by $V(F)$ the set of real points of F. Let I and J be bounded intervals of length t and suppose that $t \geq \exp(3d^2)$.*
Then the number of points in $V(F) \cap I \times J \cap \mathbb{Z}^2$ is bounded above in the following way :

$$\boxed{\left|V(F) \cap (I \times J) \cap \mathbb{Z}^2\right| \leq N_d \cdot (\log(t))^{2d+9/2}\, t^{1/d}}$$

with :

$$N_d = 40 \cdot (5e)^{4d}\, d^{2d}.$$

The idea of the proof is as follows : after removing all singularities from the curve $V(F)$, cover what remains with graphs of smooth functions f with small first derivative in either one of the forms $y = f(x)$ or $x = f(y)$. The integer-coordinates points of such a graph can then be covered by some other algebraic curves that share no common irreducible component with $V(F)$ and whose degree is a parameter we choose at the very end.
By Bézout's theorem (at least a weak version of it that gives only an inequality, see [7], exercise 10 for a proof), there can not be too many points on $V(F)$ that are also on other algebraic curves. This gives the conclusion.

If I is an interval of $\mathbb{R}$ and f is any bounded function on I, we define :

$$\|f\|_I = \sup_{x \in I} |f(x)|$$

i.e. the infinity-norm of f on I. Also define $\lambda(I)$ to be the length of the interval I.

3.1 Covering the graph with curves

Definition 3.2. *Let $\mathcal{M} \subseteq \mathbb{N}^2$ be a finite of D many pairs (a,b) (that correspond to monomials $X^aY^b \in \mathbb{R}[X,Y]$).*
Denote by $\langle\mathcal{M}\rangle$ the D-dimensional vector space of polynomials in $\mathbb{R}[X,Y]$ whose monomials X^aY^b are such that $(a,b) \in \mathcal{M}$.
A $\mathcal{M}$-curve is the zero-locus in $\mathbb{R}^2$ of any non-zero polynomial in $\langle\mathcal{M}\rangle$.

Theorem 3.3. *Let $\mathcal{M} \subseteq \mathbb{N}^2$ be a finite set of $D \geq 2$ many pairs (a,b). Let I be a non trivial compact interval and write $A = \sup_{x\in I} |x|$. Let f be a $\mathcal{C}^{D-1}$ function on I. Suppose that C and δ are positive constants such that :*

$$\frac{\left\|f^{(k)}\right\|}{k!} \leq C \cdot \delta^k$$

for $0 \leq k \leq D-1$. Suppose also that :

$$\lambda(I) > \frac{1}{4}\left((2A)^p (CD)^q\right)^{-\frac{1}{\binom{D}{2}}} \delta^{-1}$$

where $p = \sum_{(a,b)\in\mathcal{M}} a$ and $q = \sum_{(a,b)\in\mathcal{M}} b$.

Then the set S defined by the intersection of the graph of f with the lattice $\mathbb{Z}^2$:

$$S = \{(x, f(x)) \mid x \in I\} \cap \mathbb{Z}^2$$

is contained in some $\mathcal{M}$-curve.

Proof. For each $\underline{m} = (a,b) \in \mathcal{M}$, put :

$$f_{\underline{m}}(x) = x^a f(x)^b$$

so that $f_{\underline{m}}$ is a $\mathcal{C}^{D-1}$ function on I. Let us first obtain some rough estimate on $f_{\underline{m}}^{(k)}$ for all $k \leq D-1$:

$$\begin{aligned} f_{\underline{m}}^{(k)}(x) &= \sum_{i_0+\cdots+i_b=k} \frac{k!}{i_0!\dots i_b!} \frac{\mathrm{d}^{i_0} x^a}{\mathrm{d}\, x^{i_0}} \cdot \frac{\mathrm{d}^{i_1} f(x)}{\mathrm{d}\, x^{i_1}} \cdots \frac{\mathrm{d}^{i_b} f(x)}{\mathrm{d}\, x^{i_b}} \\ &= \sum_{i_0+\cdots+i_b=k} \frac{k!}{i_0!\dots i_b!} a(a-1)\dots(a-i_0+1)x^{a-i_0} \cdot \frac{\mathrm{d}^{i_1} f(x)}{\mathrm{d}\, x^{i_1}} \cdots \frac{\mathrm{d}^{i_b} f(x)}{\mathrm{d}\, x^{i_b}} \end{aligned}$$

Using the hypotheses on f one has :

$$\begin{aligned} \left\|f_{\underline{m}}^{(k)}\right\|_I &\leq \sum_{i_0+\cdots+i_b=k} k! A^{a-i_0} \binom{a}{i_0} \cdot C^b \prod_{j=1}^{b} \delta^{i_j} \\ &\leq \sum_{i_0+\cdots+i_b=k} k! A^a \binom{a}{i_0} C^b \delta^k \\ &\leq \sum_{i_0=0}^{k} \binom{a}{i_0} k! A^a C^b \delta^k \left(\sum_{i_1+\cdots+i_b=k-i_0} 1 \right) \\ &\leq \sum_{i_0=0}^{k} \binom{a}{i_0} k! A^a C^b \delta^k (k-i_0+1)^b \\ &\leq 2^a k^k A^a C^b \delta^k (k+1)^b \\ &\leq k! (2A)^a \delta^k (C(k+1))^b \end{aligned}$$

Therefore :

$$\boxed{\frac{\left\|f_{\underline{m}}^{(k)}\right\|_I}{k!} \leq (2A)^a \delta^k (C(k+1))^b}$$

Now suppose that S is not contained in any $\mathcal{M}$-curve. Consider the linear map :

$$\langle \mathcal{M} \rangle \longrightarrow \mathbb{R}^S$$

that sends some polynomial $P \in \langle \mathcal{M} \rangle$ to the family $(P(x,y))_{(x,y)\in S}$. This map is injective since S is not contained in any $\mathcal{M}$-curve.
Hence there is some subset $T \subseteq S$ with $|T| = D$ such that the restricted map :

$$\varphi : \langle \mathcal{M} \rangle \longrightarrow \mathbb{R}^T$$

is an isomorphism. Denote by $(x_1, f(x_1)),\dots,(x_D, f(x_D))$ the elements of T, with $x_1 < x_2 < \cdots < x_D$. The matrix of φ in the (unordered) bases given by $\mathcal{M}$ and T is precisely :

$$\left(f_{\underline{m}}(x_i)\right)_{\underline{m}\in\mathcal{M}, 1\le i\le D}$$

and its entries are integers because $T \subseteq \mathbb{Z}^2$. Since this matrix is non-degenerate, its determinant is a non-zero integer, hence it is at least 1 in absolute value :

$$\boxed{\left|\det\left(f_{\underline{m}}(x_i)\right)_{\underline{m}\in\mathcal{M}, 1\le i\le D}\right| \ge 1}$$

Now we want to estimate this determinant using the bounds we have found for the $\left\|f_{\underline{m}}^{(i)}\right\|_I$.
For any $\underline{m} \in \mathcal{M}$ and any $1 \le k \le D$, by Lagrange interpolation, the polynomial $P_{\underline{m},k}$ defined by :

$$P_{\underline{m},k} = \sum_{i=1}^{k} f_{\underline{m}}(x_i) \prod_{j\ne i, j\le k} \frac{X - x_j}{x_i - x_j}$$

coincides with $f_{\underline{m}}$ at the k distinct points $x_1,\dots,x_k$.
By Rolle's theorem applied $k-1$ times, $f_{\underline{m}}^{(k-1)}$ and $P_{\underline{m},k}^{(k-1)}$ (which is a constant polynomial) have the same value at some $t_{\underline{m},k} \in I$:

$$f_{\underline{m}}^{(k-1)}(t_{\underline{m},k}) = (k-1)! \sum_{i=1}^{k} \frac{f_{\underline{m}}(x_i)}{\prod_{j\ne i, j\le k}(x_i - x_j)}$$

This triangular system of equations between the $\left(f_{\underline{m}}^{(k-1)}(t_{\underline{m},k})\right)_{\underline{m},k}$ and the $\left(f_{\underline{m}}(x_i)\right)_{\underline{m},i}$ yields :

$$\left|\det\left(\frac{f_{\underline{m}}^{(k-1)}(t_{\underline{m},k})}{(k-1)!}\right)_{\underline{m},k}\right| = \left|\det\left(f_{\underline{m}}(x_i)\right)_{\underline{m},i}\right| \cdot \prod_{i=1}^{D}\prod_{j=1}^{i-1}\left|x_i - x_j\right|^{-1}$$

One then has :

$$\begin{aligned}
1 &\le \left|\det\left(f_{\underline{m}}(x_i)\right)_{\underline{m}\in\mathcal{M}, 1\le i\le D}\right| \\
&\le \left|\det\left(\frac{f_{\underline{m}}^{(k-1)}(t_{\underline{m},k})}{(k-1)!}\right)_{\underline{m},k}\right| \prod_{j<i}\left|x_i - x_j\right| \\
&\le \sum_{\sigma}\prod_{k=1}^{D} \frac{\left\|f_{\sigma(k)}^{(k-1)}\right\|_I}{(k-1)!} \cdot \prod_{j<i}\left|x_i - x_j\right| \\
&\le \sum_{\sigma=(a,b)}\prod_{k=1}^{D} (2A)^{a(k)}\delta^{k-1}(Ck)^{b(k)} \cdot \lambda(I)^{\binom{D}{2}} \\
&\le \sum_{\sigma=(a,b)} (2A)^{p}(CD)^{q} \cdot (\delta\lambda(I))^{\binom{D}{2}} \\
&\le D! \cdot (2A)^{p}(CD)^{q} \cdot (\delta\lambda(I))^{\binom{D}{2}} \\
&\le D^{D} \cdot (2A)^{p}(CD)^{q} \cdot (\delta\lambda(I))^{\binom{D}{2}}
\end{aligned}$$

where σ ranges over all bijections $\{1,\dots,D\} \longrightarrow \mathcal{M}$, writing $\sigma = (a,b)$ to say that $\sigma(k) = (a(k), b(k))$. Therefore :

$$\begin{aligned}
\lambda(I) &\ge D^{-\frac{2}{D-1}} \left((2A)^{p}(CD)^{q}\right)^{-\frac{1}{\binom{D}{2}}} \delta^{-1} \\
&\ge \frac{1}{4}\left((2A)^{p}(CD)^{q}\right)^{-\frac{1}{\binom{D}{2}}} \delta^{-1}
\end{aligned}$$

for $D \ge 2$, as desired. □

Corollary 3.4. *Let $\mathcal{M} \subseteq \mathbb{N}^2$ be a finite set of $D \geq 2$ many pairs (a,b), and keep the same notation for p and q. Let I be a non trivial compact interval with $A = \sup_{x\in I} |x|$ and let f be a $\mathcal{C}^{D-1}$ function on I that satisfies the same estimates :*

$$\frac{\left\|f^{(k)}\right\|}{k!} \leq C \cdot \delta^k$$

for $0 \leq k \leq D-1$.
Then the set S previously defined is contained in the union of :

$$\left\lfloor 1 + 4\delta\lambda(I)\left((2A)^p(CD)^q\right)^{\frac{1}{\binom{D}{2}}} \right\rfloor$$

many $\mathcal{M}$-curves.

Proof. Denote by $(x_1, f(x_1)),\dots,(x_s, f(x_s))$ the elements of S, with $x_1 < x_2 < \cdots < x_s$.
Put $n_0 = 1$. Suppose n_k has been defined. If the set $\{(x_{n_k}, f(x_{n_k})),\dots,(x_s, f(x_{n_s}))\}$ is contained in some $\mathcal{M}$-curve then stop the induction and put $S_{k+1} = \{(x_{n_k}, f(x_{n_k})),\dots,(x_s, f(x_{n_s})\}$.
Otherwise pick n_{k+1} maximal so that $n_k < n_{k+1} \leq s$ and so that the set :

$$S_{k+1} = \{(x_{n_k}, f(x_{n_k})),\dots,(x_{n_{k+1}-1}, f(x_{n_{k+1}-1}))\}$$

is contained in some $\mathcal{M}$-curve. Note that it is possible because one point Q is always contained in some $\mathcal{M}$-curve because the map $\langle\mathcal{M}\rangle \longrightarrow \mathbb{R}$ that evaluates a polynomial at Q is not injective since $D \geq 2$.
This process will stop, and we get a partition of S :

$$S = \bigsqcup_{k=1}^{N} S_k$$

with S_k contained in some $\mathcal{M}$-curve, and for all $1 \leq k < N$, the set $S_k \sqcup \{(x_{n_k}, f(x_{n_k}))\}$ not contained in any $\mathcal{M}$-curve.
By the previous theorem one has for all $0 \leq k \leq N-2$:

$$\lambda([x_{n_k}, x_{n_{k+1}}]) \geq \frac{1}{4}\left((2A)^p(CD)^q\right)^{-\frac{1}{\binom{D}{2}}} \delta^{-1}$$

by maximality of n_{k+1}. Summing over k yields :

$$\lambda(I) \geq (N-1)\cdot\frac{1}{4}\left((2A)^p(CD)^q\right)^{-\frac{1}{\binom{D}{2}}} \delta^{-1}$$

and since S is contained in the union of N many $\mathcal{M}$-curves, we get the desired result. □

Using this and Bézout's theorem, one has the following theorem.

Theorem 3.5. *Let $F \in \mathbb{R}[X,Y]$ be a $\mathbb{C}$-irreducible polynomial of degree $d \geq 2$ and let $\ell \geq d$ by an integer. Put :*

$$D = d(\ell - d + 1) \geq 2.$$

Let I be a non trivial compact interval contained in $[0,A]$ for some $A > 0$ and let f be a $\mathcal{C}^{D-1}$ function on I that satisfies the estimates :

$$\frac{\left\|f^{(k)}\right\|}{k!} \leq A \cdot \delta^k$$

for $0 \leq k \leq D-1$, and such that $F(x, f(x)) = 0$.
Then one has the following bound for the size of previously defined set S :

$$\boxed{|S| \leq \kappa d\ell}$$

where

$$\kappa = 1 + 4\delta\lambda(I)(2AD)^{\frac{d+\ell}{D-1}}.$$

Proof. Consider $t \geq 0$ maximal so that the monomial $X^{d-t}Y^t$ appears in F. Now define the following set of pairs :

$$\mathcal{M} = \left\{(a,b) \mid d \leq a+b \leq \ell \text{ and } X^{d-t}Y^t \nmid X^aY^b\right\}$$

For all $d \leq i \leq \ell$ there are exactly d many elements $(a,b) \in \mathcal{M}$ that satisfy $a+b=i$, so :

$$|\mathcal{M}| = (\ell - d + 1)d = D$$

which motivates the definition of D. Also define p and q like before : $p = \sum_{(a,b)\in\mathcal{M}} a$ and $q = \sum_{(a,b)\in\mathcal{M}} b$. Notice that :

$$p+q = \sum_{(a,b)\in\mathcal{M}} (a+b) = \sum_{i=d}^{\ell} di = d\frac{d+\ell}{2}(\ell - d + 1) = \frac{D(d+\ell)}{2}.$$

Now use corollary 3.4 to obtain that S in contained in a union of at most :

$$\left\lfloor 1 + 4\delta\lambda(I)((2A)^p(AD)^q)^{\frac{1}{\binom{D}{2}}} \right\rfloor$$

many curves. Observe since $p \leq p+q$ and $q \leq p+q$ and $p+q = \frac{D(d+\ell)}{2}$, this number is less than κ defined as :

$$\kappa = 1 + 4\delta\lambda(I)(2AD)^{\frac{d+\ell}{D-1}}.$$

Now observe that for each $G \in \langle\mathcal{M}\rangle \setminus \{0\}$, the polynomial G is not divisible by F by construction of the set S : if $G = HF$, write $F = F_d + \cdots + F_0$ and $H = H_s + \cdots + H_0$ with F_i and H_i homogenous of degree i, $F_d \neq 0$ and $H_s \neq 0$. One has :

$$G = H_sF_d + \text{lower degree terms}$$

which implies that H_sF_d is also in $\langle\mathcal{M}\rangle$.
Now by definition of t one has $F_d = \alpha_0X^d + \alpha_1X^{d-1}Y + \cdots + \alpha_tX^{d-t}Y^t$ with $\alpha_t \neq 0$. Write also $H_s = \beta_0X^s + \beta_1X^{s-1}Y + \cdots + \beta_sY^s$ so that :

$$H_sF_d = \sum_{i,j} \alpha_i\beta_jX^{d+s-i-j}Y^{i+j} \in \langle\mathcal{M}\rangle$$

and therefore we can sum only on those (i,j) that satisfy $d \leq i+j \leq \ell$, $0 \leq i \leq t$, $0 \leq j \leq s$ and $X^{d-t}Y^t \nmid X^{d+s-i-j}Y^{i+j}$. It is easy to see that there are no such pairs, which is absurd.
Hence by Bézout's theorem, since F is irreducible in $\mathbb{C}[X,Y]$ and does not divide G, for each $G \in \langle\mathcal{M}\rangle \setminus \{0\}$, one has :

$$|V(G) \cap V(F)| \leq d\ell$$

where $V(F)$ denotes the zero locus in $\mathbb{R}^2$. Therefore :

$$|S| \leq \kappa d\ell$$

as desired. □

3.2 Some elementary results

In order to continue the program announced before (3), one needs a few elementary lemmas that we list and prove here.

Lemma 3.6. *Let $a < b$ be real numbers, $k \geq 1$ and $C, \delta > 0$. Let f be a C^k function on $[a,b]$. Suppose that for all $x \in [a,b]$:*

$$\frac{\left|f^{(i)}(x)\right|}{i!} \leq C\delta^i$$

for $i < k$ and :

$$\frac{\left|f^{(k)}(x)\right|}{k!} \geq C\delta^k.$$

Then one has :

$$\boxed{b - a \leq \frac{2}{\delta}}.$$

Proof. Using Taylor's formula, there is some $t \in]a,b[$ such that :

$$f(b) - \sum_{i=0}^{k-1} \frac{f^{(i)(a)}}{i!}(b-a)^i = \frac{f^{(k)}(t)}{k!}(b-a)^k$$

and then :

$$C\left(\delta(b-a)\right)^k \leq \left|\frac{f^{(k)}(t)}{k!}(b-a)^k\right| \leq C + \sum_{i=0}^{k-1} C\left(\delta(b-a)\right)^i$$

now put $x = \delta(b-a) > 0$. One has :

$$x^k \leq 1 + \sum_{i=0}^{k-1} x^i.$$

We need to show that $x \leq 2$. Suppose not : then $x \neq 1$ so $x^k \leq 1 + \frac{x^k - 1}{x-1}$, hence $x^k(x-2) \leq -1$ which is absurd. □

Lemma 3.7. *Let K be a field, $F \in K[X,Y]$ be a degree $d \geq 0$ polynomial and $f \in K[X]$ be such that :*

$$F(X, f(X)) = 0.$$

Then $\deg(f) \leq d$.

Proof. Denote by ℓ the degree of f.
Reducing $F(X, f(X)) = 0$ modulo the ideal $(Y - f(X))$ yields :

$$F(X,Y) \equiv 0 \left[Y - f(X)\right]$$

hence $Y - f(X)$ divides F in $K[X,Y]$, but $Y - f(X)$ has degree ℓ in the variable X, so $\ell \leq d$. □

Lemma 3.8. *Let f be a smooth function defined on some non trivial interval I, which satisfies :*

$$F(x, f(x)) = 0$$

with $F \in \mathbb{R}[X,Y]$ of degree $d \geq 2$ irreducible on $\mathbb{C}$. Suppose also that f is not a polynomial.
Then for any $k \geq 1$ and any $c \in \mathbb{R}$:

$$\boxed{\left|\{f^{(k)} = c\}\right| \leq d(d-1)(2k-1)}$$

Proof. From $F(x, f(x)) = 0$, one has by differentiating :

$$\partial_x F + \partial_y F \cdot f' = 0 \quad (*)$$

where we implicitly evaluate everything at $(x, f(x))$. Let us show by induction on $k \geq 1$ that there exist some $H_k \in \mathbb{R}[X,Y]$ with degree less than $(2d-3)k + 2 - d \geq 0$ such that :

$$H_k + \left(\partial_y F\right)^{2k-1} f^{(k)} = 0.$$

The case $k = 1$ comes from $(*)$. Then suppose we have case k. By differentiating one obtains :

$$\partial_x H_k + \partial_y H_k \cdot f' + (2k-1)(\partial_y F)^{2k-2}(\partial_{xy} F + \partial_{yy} F \cdot f')f^{(k)} + (\partial_y F)^{2k-1} f^{(2k+1)} = 0$$

and by multiplying by $(\partial_y F)^2$, using $(*)$ and the equation at rank k :

$$H_{k+1} + \left(\partial_y F\right)^{2k+1} f^{(k+1)} = 0$$

with :

$$H_{k+1} = \partial_y F\left(\partial_y F \partial_x H_k - \partial_x F \partial_y H_k\right) + (2k-1)H_k(\partial_x F \partial_{yy} F - \partial_y F \partial_{xy} F)$$

which implies :

$$\deg H_{k+1} \leq 2d - 3 + \deg H_k \leq (2d-3)(k+1) + 2 - d$$

as announced.
Now let $c \in \mathbb{R}$ and put $Q_k = H_k + (\partial_y F)^{2k-1} c$.
Now we show that the polynomials F and Q_k are relatively prime in $\mathbb{C}[X,Y]$. Otherwise one would have $F \mid Q_k$ by irreducibility of F in $\mathbb{C}[X,Y]$ and then for all $x \in I$ one would have $Q_k(x, f(x)) = 0$ meaning that :

$$(\partial_y F)^{2k-1}(x, f(x)) \cdot c = (\partial_y F)^{2k-1}(x, f(x)) \cdot f^{(k)}(x)$$

for all $x \in I$. Now $\partial_y F$ is not the zero polynomial otherwise from $F(x, f(x)) = 0$, I would be trivial or F would be zero. Hence $\partial_y F$ and F are relatively prime in $\mathbb{C}[X,Y]$ and by Bézout's theorem $V(\partial_y F) \cap V(F)$ is finite.
Therefore $(\partial_y F)^{2k-1}(x, f(x))$ can have only finitely many zeros on I. Hence the set $\{f^{(k)}(x) = c\}$ is dense in I and by continuity f is a polynomial, and this case we excluded.
Therefore F and Q_k are relatively prime and by Bézout's theorem one has :

$$|V(F) \cap V(Q_k)| \leq d \cdot \deg Q_k \leq d(d-1)(2k-1)$$

Now if $f^{(k)}(x) = c$ then $(x, f(x)) \in V(F) \cap V(Q_k)$, hence by injectivity of $x \mapsto (x, f(x))$:

$$\left|\{f^{(k)} = c\}\right| \leq d(d-1)(2k-1)$$

as desired. □

Lemma 3.9. *Let f be a smooth function defined on some non trivial interval I, which satisfies :*

$$F(x, f(x)) = 0$$

with $F \in \mathbb{R}[X,Y]$ of degree $d \geq 2$ irreducible on $\mathbb{C}$. Let $k \geq 1$.
Let $A_1, \ldots, A_k \geq 0$. Then there exists a partition of I in at most $2d^2k^2$ intervals I_j so that for all j and all $\ell \in \{1, \ldots, k\}$, either :

$$\sup_{I_j} \left|f^{(\ell)}\right| \leq A_\ell$$

or :

$$\inf_{I_j} \left|f^{(\ell)}\right| \geq A_\ell.$$

Proof. There are two cases regarding whether f is a polynomial or not.
If f is not a polynomial, then subdivide I at each point where $f^{\ell}(x) = \pm A_\ell$ for any $\ell \in \{1, \ldots, k\}$. Using lemma 3.8, there are at most :

$$\sum_{\ell=1}^{k} 2d(d-1)(2\ell-1) = 2d(d-1)\ell^2$$

such points, which makes at most :

$$1 + 2d(d-1)\ell^2 \leq 2d^2\ell^2$$

intervals. By the intermediate value theorem, one clearly has the desired result.
Now suppose f is a polynomial. By lemma 3.7, f has degree at most d. Now subdivide I at each point where $f^{(l)}(x) = \pm A_\ell$ for any $1 \leq \ell \leq \min(k, \deg(f) - 1)$ (note that $f \neq 0$ because $\deg F \geq 2$ and F is irreducible).
This time we have at most :

$$\sum_{\ell=1}^{\min(k,\deg(f)-1)} 2(\deg(f) - \ell) \leq \sum_{\ell=1}^{d-1} 2(d-\ell) = d(d-1) \leq 2d^2k^2$$

such points because $f^{(l)}$ has degree $\deg(f) - \ell$. By the intermediate value theorem and the fact that for $\ell \geq \deg(f) - 1$, $f^{(\ell)}$ is a constant so it obviously satisfies one of the two inequalities, we obtain again the desired result. □

3.3 A proof of the Bombieri-Pila theorem

In this part we prove 3.1. As announced in 3, we first deal with graphs of smooth curves contained in $V(F)$.

Theorem 3.10. *Let f be a C^∞ function on some bounded non trivial interval I of length t. Let $F \in \mathbb{R}[X,Y]$ be a $\mathbb{C}$-irreducible polynomial of degree $d \geq 2$ such that $F(x, f(x)) = 0$. Suppose that :*

$$\left\|f'\right\|_I \leq 1$$

and consider the set S given by the intersection of the graph of f with the lattice $\mathbb{Z}^2$. Then one has :

$$\boxed{|S| \leq M_d \cdot (\log(t))^{2d+9/2}\, t^{1/d}}$$

provided $t \geq \exp(3d^2)$, with :

$$M_d = 40 \cdot (5e)^{3d}\, d^{2d}.$$

Proof. First, upon translating the graph of f by elements of $\mathbb{Z}^2$ and without changing any hypothesis, we may suppose it is contained in $[0, \lambda(I)+1]^2$ with $\lambda(I)$ the length of I as usual (using the fact that $\|f'\|_I \leq 1$).
We make the assumption that $\lambda(I) \geq 1$ for now.
Now fix $\delta > 0$ to be chosen later. Fix $\ell \geq 2d$ to be chosen later too. Keep the notation as in theorem 3.5 :

$$D = d(\ell - d + 1) \geq 2$$

as well as

$$\kappa = 1 + 4\delta\lambda(I)(2AD)^{\frac{d+\ell}{D-1}}$$

with $A = \sup_{x\in I}|x| \leq \lambda(I)+1$. Taking into account $\ell \geq 2d$ one has :

$$\frac{d+\ell}{D-1} = \frac{d+\ell}{d\ell - d^2 + d - 1} \leq \frac{d+\ell}{d\ell - d^2} \leq \frac{1}{d}\frac{\ell - d + 2d}{\ell - d} \leq \frac{1}{d} + \frac{2}{\ell - d} \leq \frac{1}{d} + \frac{4}{\ell}.$$

Note also that $D \leq d\ell$. Now define the exponent α to be :

$$\alpha = \frac{1}{d} + \frac{4}{\ell} > 0$$

so that :

$$\kappa \leq 1 + 4\delta\lambda(I)(4\lambda(I)D)^\alpha \leq 1 + 4\delta\lambda(I)(4\lambda(I)d\ell)^\alpha$$

since $4\lambda(I)D \geq 1$ and $\lambda(I)+1 \leq 2\lambda(I)$. We now put :

$$K(t) = 1 + 4\delta t(4td\ell)^\alpha$$

which does not depend on F, so that $\kappa \leq K(\lambda(I))$.
Using lemma 3.9, subdivide I into at most $2d^2D^2$ intervals I_j such that for all $i \in \{1,\dots,D-1\}$ and all j one has either :

$$\sup_{I_j} \frac{\left|f^{(i)}\right|}{i!} \leq (\lambda(I)+1)\delta^i$$

or :

$$\inf_{I_j} \frac{\left|f^{(i)}\right|}{i!} \geq (\lambda(I)+1)\delta^i.$$

Now fix some j and let us count the elements of the graph in $I_j \times \mathbb{R} \cap \mathbb{Z}^2$. There are two possibilities :
Either $\sup_{I_j} \frac{\left|f^{(i)}\right|}{i!} \leq (\lambda(I)+1)\delta^i$ is true for all $i \in \{0,\dots,D-1\}$ (it is always true for $i=0$ because the graph is contained in $[0,\lambda(I)+1]^2$) or there is some $1 \leq k \leq D-1$ such that one has $\sup_{I_j} \frac{\left|f^{(i)}\right|}{i!} \leq (\lambda(I)+1)\delta^i$ for all $i < k$ and $\inf_{I_j} \frac{\left|f^{(k)}\right|}{k!} \geq (\lambda(I)+1)\delta^k$.
In the first case, using theorem 3.5, one has :

$$\left|S \cap I_j \times \mathbb{R}\right| \leq K(\lambda(I))d\ell$$

because I_j is shorter than I.
In the second case, using lemma 3.6 :

$$\lambda(I_j) \leq \frac{2}{\delta}.$$

Now for all $t \geq 1$, define $B(t)$ to be the supremum over all non trivial intervals J of length less than t, over all C^∞ functions g on J with $\|g'\|_J \leq 1$ satisfying $G(x, g(x)) = 0$ for some $G \in \mathbb{R}[X, Y]$ irreducible in $\mathbb{C}[X, Y]$ of degree d, of the number of points on the graph of f in the lattice $\mathbb{Z}^2$. Note that $B(t) < \infty$ because it is bounded above by $(t+2)^2$. Note also that B is an increasing function in t.
By summing all the bounds on the number of points on each I_j one gets :

$$B(t) \leq K(t) d\ell \cdot 2(dD)^2 + B\left(\frac{2}{\delta}\right) \cdot 2(dD)^2$$

for all $t \geq 1$. We still need to choose parameters $\delta > 0$ and $\ell \geq 2d$ (note that $K(t)$ depends on those parameters). Instead of choosing δ, it is equivalent and easier to choose $\mu > 0$ so that :

$$\frac{2}{\delta} = \mu t.$$

We will even choose $\mu < 1$ in order to make an induction to bound $B(t)$. One has (using again $D \leq d\ell$) :

$$\begin{aligned}
B(t) &\leq K(t) d\ell \cdot 2(dd\ell)^2 + B(\mu t) \cdot 2(dd\ell)^2 \\
&= 2d^5\ell^3 (1 + 4\delta t (4td\ell)^\alpha) + 2d^4\ell^2 B(\mu t) \\
&= 2d^5\ell^3 \left(1 + \frac{8}{\mu}(4td\ell)^\alpha\right) + 2d^4\ell^2 B(\mu t) \\
&\leq 2d^5\ell^3 \left(\frac{9}{\mu}(4td\ell)^\alpha\right) + 2d^4\ell^2 B(\mu t) \\
&= Ut^\alpha + VB(\mu t) \quad (*)
\end{aligned}$$

because $(4td\ell)^\alpha / \mu \geq 1$ since $\mu < 1$, and letting :

$$U = \frac{18d^5\ell^3}{\mu}(4d\ell)^\alpha$$

and

$$V = 2d^4\ell^2.$$

By induction on the formula $(*)$ we see that :

$$B(t) \leq V^n B(\mu^n t) + t^\alpha U \left(1 + (V\mu^\alpha) + (V\mu^\alpha)^2 + \cdots + (V\mu^\alpha)^{n-1}\right)$$

for all $n \geq 0$ such that $\mu^{n-1} t \geq 1$ (in order to keep the hypothesis $t \geq 1$ that was required to get formula $(*)$).
Now we choose parameter μ so that :

$$V\mu^\alpha = \frac{1}{2}$$

which is compatible with the condition $\mu < 1$. Also we choose the best n as possible, that is n such that $\mu^n t < 1 \leq \mu^{n-1} t$ which is possible since $\mu < 1$. So far the only parameter yet to choose is ℓ.
One has now :

$$B(t) \leq V^n B(\mu^n t) + \frac{t^\alpha U(1 - (1/2)^n)}{1 - 1/2} \leq V^n + 2t^\alpha U$$

because $\mu^n t < 1$ and, in a square (aligned with the axes) of side strictly less than 1, there is at most one point of $\mathbb{Z}^2$.
Since $\mu^{n-1} t \geq 1$, we have $\mu^n t \geq \mu$ thus $V^n \leq \frac{V}{2^{n-1}} t^\alpha \leq 2Vt^\alpha$. One therefore has :

$$B(t) \leq 2(U + V)t^\alpha$$

and we still have to estimate $U + V$ and choose ℓ. Observe that :

$$U + V = \frac{18d^5\ell^3}{\mu}(4d\ell)^\alpha + 2d^4\ell^2 = 18d^5\ell^3(2V)^{1/\alpha}(4d\ell)^\alpha + 2d^4\ell^2 \leq d^5\ell^3(4d^4\ell^2)^{1/\alpha}(4d\ell)^\alpha \left(18 + \frac{1}{4}\right) \leq \frac{73}{4} d^5\ell^3(4d^4\ell^2)^{1/\alpha}(4d\ell)^\alpha$$

because $2d^4\ell^2 \leq \frac{1}{4}d^5\ell^3$. Hence :

$$\begin{aligned} B(t) &\leq \frac{73}{2}d^5\ell^3(4d^4\ell^2)^{1/\alpha}(4d\ell)^\alpha t^\alpha \\ &\leq \frac{73}{2}d^5\ell^3(4d^4\ell^2)^d(4d\ell)^{3/2}t^{4/\ell}t^{1/d} \\ &\leq 292\cdot 4^d d^{13/2}d^{4d}\exp\left(\frac{4}{\ell}\log(t)+\left(2d+\frac{9}{2}\right)\log(\ell)\right)t^{1/d} \end{aligned}$$

and the term in the exponential is minimal when :

$$\ell = \frac{4\log(t)}{2d+\frac{9}{2}}$$

Since ℓ has to be an integer, we rather take :

$$\ell = \left\lceil \frac{4\log(t)}{2d+\frac{9}{2}} \right\rceil$$

Also we want $\ell \geq 2d$ so we require :

$$t \geq \exp\left(d^2+\frac{9}{4}d\right)$$

or more simply $t \geq \exp(3d^2)$. In this case, one has :

$$\begin{aligned} B(t) &\leq 292\cdot 4^d d^{13/2}d^{4d}\cdot\left(\frac{10e}{4d+9}\right)^{2d+9/2}\cdot(\log(t))^{2d+9/2}\,t^{1/d} \\ &\leq 292\cdot 4^d d^{13/2}d^{4d}\cdot\left(\frac{10e}{4d}\right)^{2d+9/2}\cdot(\log(t))^{2d+9/2}\,t^{1/d} \\ &\leq 292\frac{6^9}{512}\cdot 4^d d^{2d+2}\left(\frac{10e}{4}\right)^{2d}\cdot(\log(t))^{2d+9/2}\,t^{1/d} \\ &\leq 40\cdot d^{2d}(5e)^d\,(5e)^{2d}\cdot(\log(t))^{2d+9/2}\,t^{1/d} \\ &\leq 40\cdot(5e)^{3d}\,d^{2d}\cdot(\log(t))^{2d+9/2}\,t^{1/d} \end{aligned}$$

because $10e \leq 6^2$ and $d^2 \leq (5e)^d$. □

Eventually we prove theorem 3.1 :

Theorem 3.11. *Let $F \in \mathbb{R}[X,Y]$ be a $\mathbb{C}$-irreducible polynomial of degree $d \geq 2$. Denote by $V(F)$ the set of real points of F. Let I be a bounded interval of length t and J be a bounded interval of length t.*
Suppose that $t \geq \exp(3d^2)$.
Then the number of points in $V(F)\cap I\times J\cap\mathbb{Z}^2$ is bounded above in the following way :

$$\boxed{\left|V(F)\cap(I\times J)\cap\mathbb{Z}^2\right| \leq N_d\cdot(\log(t))^{2d+9/2}\,t^{1/d}}$$

with :

$$N_d = 40\cdot(5e)^{4d}\,d^{2d}.$$

Proof. Without changing the length of I and J we may suppose they are compact.
We first deal with the degenerate case where $\partial_X F = \pm\partial_Y F$. In this case the derivative of F in the direction $(1,\pm1)$ is always zero which implies that F is affine (i.e. $\deg F \leq 1$). This case is excluded.
We denote by Γ the set $V(F)\cap I\times J$. It is a compact subset of the plane.
A point p of Γ is said to be *special* if it is on the boundary of $I\times J$ or if it satisfies :

$$\partial_X F(p) = \pm\partial_Y F(p)$$

i.e. if the slope of the tangent line to the curve $V(F)$ passing by p is ±1. Let $S\subset\Gamma$ denote the set of special points. Using Bézout's theorem, the irreducibility of F and the fact that $\deg F \geq 2$, one sees that the curve $V(F)$ intersects the

square border $\partial(I \times J)$ in at most $4d$ points.
By Bézout's theorem again and since we have excluded the degenerate cases, there are at most $2d(d-1)$ points with $\partial_X F(p) = \pm \partial_Y F(p)$ hence :

$$|S| \leq 2d(d+1).$$

Now consider the set $X = \Gamma \setminus S$. Notice X can be obtained from the curve $V(F)$ by removing finitely many points, including its singularities, and then intersecting with the open set given by the interior of $I \times J$. Hence it is a C^∞ submanifold of $\mathbb{R}^2$ of dimension 1.
Therefore the connected components of X are open in X and if C is such a connected component, one has either :

$$|\partial_X F| < |\partial_Y F| \quad (a)$$

or

$$|\partial_Y F| < |\partial_X F| \quad (b)$$

on C by connectedness and because we have removed points with equality of these quantities.
We claim that C is the graph of some C^∞ function f with $|f'| \leq 1$ in the form $y = f(x)$ or $x = f(y)$ whether we are in case (a) or (b).
Without loss of generality let us suppose we are in case (a). The claim is true locally on C by the implicit function theorem, and to show that it is true globally we only need to prove that the x-coordinate form dx is injective on C. Suppose it is not : hence there are two points $p = (x, y_1)$ and $q = (x, y_2)$ with $y_1 < y_2$ on C. Since C is a 1 dimensional connected smooth manifold, it is either diffeomorphic to $\mathbb{R}$ or to a circle, hence there is some C^∞ arc $\gamma : [0,1] \longrightarrow C$ such that $\gamma(0) = p$ and $\gamma(1) = q$. Now applying Rolle's theorem to the smooth function $dx \circ \gamma$, there is some $s \in]0,1[$ with :

$$dx \circ \dot{\gamma}(s) = 0$$

Bot one also has $F \circ \gamma = 0$ so $\partial_Y F(\gamma(s)) = 0$, which is not possible on C in case (a). Notice this whole argument becomes much clearer with a drawing : we are just arguing that if two points on C have the same x-coordinate then C has a vertical tangent line.
Now that the claim is proved and since both $F(X,Y)$ and $F(Y,X)$ are $\mathbb{C}$-irreducible of degree $d \geq 2$, we may use theorem 3.10 to state that :

$$\left|C \cap \mathbb{Z}^2\right| \leq M_d \cdot (\log(t))^{2d+9/2}\, t^{1/d}.$$

The only thing left to do is to count the connected components of X.

Notice each connected component C of X contains a *special* point in its closure (the closure of C in Γ or in $\mathbb{R}^2$ is the same since Γ is closed in $\mathbb{R}^2$) : otherwise C would be closed in Γ (because its closure is still connected) hence it would be compact and we could then find a point in C with maximal x or y coordinate, yielding some vertical or horizontal tangent line whether we are in case (a) or (b).
Therefore :

$$\sum_C 1 \leq \sum_{p \in S} \sum_{\overline{C} \ni p} 1$$

where the sum runs over all connected components of X.
Eventually we claim that for each special point p there are at most d connected components of X containing p in their closure.
Consider a special point p and $C_1, \ldots, C_\ell$ some distinct connected components of X containing p in their closure. We aim to prove that $\ell \leq d$.
Now for each i, the projection $dx(C_i)$ is an interval (by connectedness) which contains $dx(p)$ and which is non trivial (otherwise the polynomial $F(dx(p), Y)$ would have infinitely many roots hence $F(dx(p), Y) = 0$ and $X - dx(p) \mid F$ which is impossible because F is $\mathbb{C}$-irreducible of degree at least 2). Therefore the set :

$$\bigcap_{i=1}^{\ell} dx(C_i)$$

is also a neighborhood of $dx(p)$. There exists some a in this neighborhood with $a \neq p$. The line $X = a$ intersects $V(F)$ in at most d points by Bézout's theorem and $\mathbb{C}$-irreducibility of F. Since $a \in \bigcap_{i=1}^{\ell} dx(C_i)$, it also intersects each C_i, yielding ℓ distinct points in $V(F) \cap V(X - a)$ because the C_i are disjoint. Hence $\ell \leq d$ as desired.
Therefore :

$$\sum_C 1 \leq |S| \cdot d \leq 2d^2(d+1) \leq 3d^3.$$

Putting all together we obtain :

$$\begin{aligned}\left|V(F)\cap(I\times J)\cap\mathbb{Z}^2\right| &\leq \left|X\cap\mathbb{Z}^2\right| + |S| \leq 3d^3M_d\cdot(\log(t))^{2d+9/2}\,t^{1/d} + 2d(d+1)\\ &\leq 4d^3M_d\cdot(\log(t))^{2d+9/2}\,t^{1/d}\\ &\leq N_d\cdot(\log(t))^{2d+9/2}\,t^{1/d}\end{aligned}$$

with $N_d = 40\cdot(5e)^{4d}\,d^{2d}$ since $4d^3 \leq (5e)^d$. □

Remark 3.12. *In the original paper from Bombieri and Pila [5] as well as in the notes [4], the number of connected component of the set X introduced in the previous proof is bounded by $O(d^2)$ instead of $O(d^3)$ without much explanation.*
It seems that it could be achieved using a theorem of Harnack and Coolidge on real algebraic curves ([6]). However it does not affect the bound too much because of all the rough estimations made before.

4 A counter example to a question in genus theory

In the article [3], paragraph 4, the authors use the following fact, supposedly known from genus theory, in order to deal with the case where the number field K has a subfield of index 2.

Claim 4.1. *(To disprove) Let $n \geq 1$ be an integer. There exists a constant $C = C(n) > 0$ such that for all quadratic extensions K/F of number fields with $[K:\mathbb{Q}] = n$, one has :*

$$r_2(K) \leq r_2(F) + 2t + C$$

where $r_2(K)$ (resp. $r_2(F)$) is the dimension over $\mathbb{F}_2$ of the 2-torsion of the class group of K (resp. of F) and t is the number of ramified primes in the extension K/F.

This result would be surprising because the best result known in this direction ([10], theorem 2.1) only gives a bound of the type :

$$r_2(K) \leq 2r_2(F) + 2t.$$

In fact the argument of Bhargava and co. to deal with the case where K has a subfield of index 2 doesn't work any more with this weaker inequality : their argument consisted in applying the first estimate 1.4 to F and then using the claim 4.1, which does not provide the right exponent on the discriminant if we use instead the weaker inequality.
In these notes we got around this issue by applying theorem 2.6 to a certain subfield of K that has no subfield of index 2 instead of the first estimate 1.4 (see paragraph 2.1).

The aim of this section is to give a proof that the claim 4.1 is false using the following theorem of Pagano and Koymans ([11], theorems 1.1 and 1.3).
In what follows, $\omega(n)$ denotes the number of prime divisors of n. If K is a number field, let K^+ be the subgroup of $K^\times$ consisting of *totally positive* elements, i.e. those elements whose image by anyn real embedding of K is positive. Define the *narrow* class group of K, $\mathrm{Cl}^+(K)$, to be the quotient of the group of non-zero fractional ideals of K by the subgroup of principal ideals generated by an element of K^+. Write $r_2^+(K)$ for the dimension over $\mathbb{F}_2$ of $\mathrm{Cl}^+(K)(2)$, the 2-torsion of the narrow class group.

Theorem 4.2. *(Pagano, Koymans, 2020) Let $n \geq 1$. A vector $(a_1,\dots,a_n)$ of integers is said to be acceptable if each a_i is squarefree, satisfies $a_i \geq 2$, has only prime factors equivalent to 1 modulo 4 and if the a_i are pairwise coprime.*
For such a vector, one has :

$$r_2^+(\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_n})) \leq 2^{n-1}\omega(a_1\cdot\dots\cdot a_n) - 2^n + 1$$

Also, for any integers $k_1,k_2,k_3 \geq 1$, there are infinitely many acceptable vectors (a_1,a_2,a_3) such that $\omega(a_i) = k_i$ that satisfy the following equality :

$$r_2^+(\mathbb{Q}(\sqrt{a_1},\sqrt{a_2},\sqrt{a_3})) = 4\omega(a_1\cdot\dots\cdot a_n) - 7.$$

Before we can use this result we need to relate the numbers $r_2^+(K)$ and $r_2(K)$.

Lemma 4.3. *Let K be any number field. One has :*

$$\boxed{0 \leq r_2^+(K) - r_2(K) \leq r}$$

where r is the number of real embeddings of K.

Proof. Let $\mathcal{P}(K)$ be the group of non-zero principal fractional ideals of K and $\mathcal{P}^+(K)$ be the subgroups of those generated by an element of K^+. One has an exact sequence :

$$1 \longrightarrow \frac{\mathcal{P}(K)}{\mathcal{P}^+(K)} \longrightarrow \mathrm{Cl}^+(K) \longrightarrow \mathrm{Cl}(K) \longrightarrow 1$$

By applying the left-exact 2-torsion functor and the right-exact $\bullet \otimes_{\mathbb{Z}} \mathbb{F}_2$ functor we have exact sequences of $\mathbb{F}_2$-vector spaces :

$$1 \longrightarrow \frac{\mathcal{P}(K)}{\mathcal{P}^+(K)}(2) \longrightarrow \mathrm{Cl}^+(K)(2) \longrightarrow \mathrm{Cl}(K)(2)$$

and :

$$\mathrm{Cl}^+(K) \otimes \mathbb{F}_2 \longrightarrow \mathrm{Cl}(K)(2) \otimes \mathbb{F}_2 \longrightarrow 1.$$

Now for any finite abelian group G, the vector spaces $G \otimes \mathbb{F}_2$ and $G(2)$ are (non-canonically) isomorphic (this can be seen by decomposing G into a product of cyclic groups or using duality : the dual of $G \otimes \mathbb{F}_2$ is the 2-torsion of the dual of G). Hence the second exact sequence yields :

$$r_2^+(K) \geq r_2(K)$$

Now observe that :

$$\frac{\mathcal{P}(K)}{\mathcal{P}^+(K)} = \frac{K^\times/\mathcal{O}_K^\times}{K^+/(\mathcal{O}_K^\times \cap K^+)} = \frac{K^\times}{K^+\mathcal{O}_K^\times}.$$

This is a quotient of $K^\times/K^+$ which embeds in $\{\pm 1\}^r$ via the sign of the real embeddings. Hence $\frac{\mathcal{P}(K)}{\mathcal{P}^+(K)}$ is a $\mathbb{F}_2$-vector space of dimension $d \leq r$. In particular, taking the 2-torsion doesn't affect this group, and the first exact sequence implies that :

$$\ell - r_2^+(K) + r_2(K) = \dim_{\mathbb{F}_2}\Big(\mathrm{Coker}\Big(\mathrm{Cl}^+(K)(2) \to \mathrm{Cl}(K)(2)\Big)\Big) \geq 0$$

hence :

$$r_2^+(K) - r_2(K) \leq \ell \leq r$$

which concludes the proof. □

Now we can disprove claim 4.1. Assume that it is true. Let $k_1, k_2, k_3 \geq 1$ be integers and choose any acceptable vector (a_1, a_2, a_3) with $\omega(a_i) = k_i$ that satisfy the equality of theorem 4.2. Consider $K = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})$ and $F = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2})$. According to 4.1 one has :

$$r_2(K) \leq r_2(F) + 2t + C$$

where t is the number of ramified primes in the quadratic extension K/F (it is quadratic because the vector (a_1, a_2, a_3) is acceptable) and $C = C(8)$ does not depend on K and F. Using lemma 4.3 this gives :

$$r_2^+(K) - r \leq r_2^+(F) + 2t + C$$

where r is the number of real embeddings of K, i.e. $r = 8$. Applying both results of 4.2 with the fact that (a_1, a_2) is also acceptable gives :

$$4\omega(a_1a_2a_3) - 7 - 8 \leq 2\omega(a_1a_2) - 3 + 2t + C.$$

It remains to estimate t. Notice that $K = F[\sqrt{a_3}]$ and the minimal polynomial of $\sqrt{a_3}$ over F is $\pi = X^2 - a_3$. This polynomial is separable modulo every prime p except 2 and the prime divisors of a_3, so any prime $\mathfrak{p}$ of F above p with $p \nmid 2a_3$ is unramified in K (because π is separable in $\mathcal{O}_F/\mathfrak{p} \supseteq \mathbb{F}_p$). Hence t is at most the number of primes of F above prime divisors of $2a_3$:

$$t \leq \omega(2a_3) \times [F : \mathbb{Q}] \leq 4(1 + k_3)$$

because $2 \nmid a_3$ by hypothesis. Putting all together and using the fact that the a_i are pairwise coprime, we obtain :

$$4(k_1 + k_2 + k_3) \leq 12 + C + 2(k_1 + k_2) + 8(1 + k_3)$$

hence :

$$2(k_1 + k_2) - 4k_3 \leq 20 + C.$$

This holds for all $k_1, k_2, k_3 \geq 1$, which is absurd. This disproves claim 4.1.

5 Appendix 1 : Lattices and Minkowski's theorems

In this appendix we recall the basic definitions and properties of lattices of a finite dimensional real vector space and we give proofs for the 2 Minkowski's theorems.

Definition 5.1. *Let V be a finite dimensional real vector space. A lattice of V is a subgroup Λ that is discrete (in the sense of the euclidean topology on V) and that spans V as a real vector space.*
It is equivalent to say that Λ is a finitely generated subgroup of V of rank $\dim V$ that spans V as a real vector space.
A subgroup of a lattice Λ is a lattice if and only if it has finite index in Λ. In this case it is called a sublattice of Λ.

In what follows, V is a finite dimensional real vector space endowed with some Lebesgue measure μ and Λ is a lattice of V.

Definition 5.2. *A measurable subset $D \subseteq V$ is said to be a free domain for Λ if the sets $x+D$ for $x \in \Lambda$ are pairwise disjoint. It is a generating domain for Λ if $V = \bigcup_{x\in\Lambda}(x+D)$, and it is a fundamental domain for Λ if it is both a free domain and a genetating domain.*
According to the next lemma, all fundamental domains D of Λ have the same measure, which we denote :

$$\mathrm{covol}(\Lambda) = \mu(D).$$

It is called the covolume of Λ. Notice it depends on μ.

Lemma 5.3. *Let F be a free domain for Λ and G be a generating domain for Λ. Then one has :*

$$\mu(F) \leq \mu(G).$$

In particular two fundamental domains have the same measure.

Proof. Since F is free one has :

$$G \supseteq \bigsqcup_{\lambda\in\Lambda}(G \cap (F+\lambda))$$

Hence, since Λ is coutable :

$$\mu(G) \geq \sum_{\lambda\in\Lambda}\mu(G\cap(F+\lambda)) = \sum_{\lambda\in\Lambda}\mu((G-\lambda)\cap F) = \sum_{\lambda\in\Lambda}\mu((G+\lambda)\cap F) \geq \mu\left(\bigcup_{\lambda\in\Lambda}(G+\lambda)\cap F\right) = \mu(F)$$

since G is a generating domain. □

Notice the covolume is always strictly positive because it is the determinant of a basis of the lattice with respect to some fixed basis of V that spans a cube of volume 1.
From this it follows that if $g \in \mathrm{GL}(V)$, one has :

$$\mathrm{covol}(g\Lambda) = |\det(g)|\mathrm{covol}(\Lambda)$$

and if $\Lambda' \subseteq \Lambda$ is a sublattice, one has :

$$\frac{\mathrm{covol}(\Lambda')}{\mathrm{covol}(\Lambda)} = [\Lambda : \Lambda'].$$

The following theorem is a rather direct consequence of lemma 5.3.

Theorem 5.4. *(Blichfeldt)*
Let A be a measurable subset of V such that $\mu(A) > \mathrm{covol}(\Lambda)$. Then there exist $x, y \in A$ such that $x - y \in \Lambda \setminus \{0\}$.
Moreover if A is compact, the conclusion still holds if we only have $\mu(A) \geq \mathrm{covol}(\Lambda)$.

Proof. The first statement is just the contrapositive of lemma 5.3, for if A does not satisfy the conclusion then it is a free domain.
Now if A is compact and has $\mu(A) \geq \mathrm{covol}(\Lambda)$, then for any $n \geq 1$ the measurable set $(1+1/n)A$ satisfies the hypothesis of the first statement so their exist $x_n, y_n \in (1+1/n)A$ such that $x_n - y_n \in \Lambda \setminus \{0\}$. Let us write $x_n = (1+1/n)a_n$ and $y_n = (1+1/n)b_n$. The sequences (a_n) and (b_n) live in the compact set A so they have subsequences that converge to some a and b in A, which are also limits of subsequences of (x_n) and (y_n), and since $\Lambda\setminus\{0\}$ is closed, one has $a-b \in \Lambda\setminus\{0\}$. □

Next we prove Minkowski's first theorem that allows one to find small non-zero vectors in a lattice.

Theorem 5.5. *(Minkowski) Let $A \subseteq V$ be a measurable, convex (or closed under taking the average of two vectors) and symetric with respect to 0. If $\mu(A) > 2^d \operatorname{covol}(\Lambda)$, then A contains a non-zero element of Λ.*
If A is also compact, the conclusion still holds with only $\mu(A) \geq 2^d \operatorname{covol}(\Lambda)$.
In particular, if V is endowed with some norm $|\bullet|$, then Λ contains an element $\lambda \neq 0$ such that :

$$|\lambda| \leq 2\left(\frac{\operatorname{covol}(\Lambda)}{\mu(B)}\right)^{1/d}$$

where B is the open unit ball of V and $d = \dim V$.

Proof. Define the measurable set $C = \frac{1}{2}A$. One has $\mu(C) > \operatorname{covol}(\Lambda)$ (or only $\mu(C) \geq \operatorname{covol}(\Lambda)$ in the second case).By Blichfeldt's theorem 5.4, there exist $x, y \in C$ such that $x - y \in \Lambda \setminus \{0\}$. Note that $x - y \in A$ because A is symetric with respect to 0 and closed under taking averages of two vectors, which yields the desired result.
Now let $R > 0$, and consider the closed ball centered at 0 with radius R, $R\overline{B}$. It is convex, compact and symetric with respect to 0. Also it has measure $R^d\mu(B)$, hence if $R^d\mu(B) \geq 2^d \operatorname{covol}(\Lambda)$, then $R\overline{B}$ contains a non-zero element of the lattice. It then suffices to let $R = 2\left(\frac{\operatorname{covol}(\Lambda)}{\mu(B)}\right)^{1/d}$ to conclude. □

The second Minkowski's theorem is about successive minima in a lattice. In what follows V is endowed with a norm $|\bullet|$ (which we will later suppose to be euclidean). B denotes the open unit ball of V and $\overline{B}$ is the closed unit ball. The following lemma is useful to define the notion of successive minima.

Lemma 5.6. *Let A be a discrete closed subset of V. Then the set $N = \{|a| \mid a \in A\}$ is a closed and discrete subset of $\mathbb{R}_+$. This holds in particular when A is a lattice of V.*

Proof. Let (a_n) be a sequence of points in A such that $|a_n| \longrightarrow \ell$. The aim is to show that $|a_n| = \ell$ for n large (this will show that N is closed and discrete at the same time). The sequence (a_n) is bounded and V has finite dimension, and A is closed and discrete, therefore (a_n) takes finitely many values, hence the same is true for $(|a_n|)$. However this sequence converges so it has to be constant for large n. □

Definition 5.7. *(Successive minima) Let $1 \leq k \leq d$ be an integer. One defines the k-th successive minimum of Λ for the norm $|\bullet|$ to be :*

$$\lambda_k = \inf\left\{r > 0 \mid \operatorname{Rk}\left(r\overline{B} \cap \Lambda\right) \geq k\right\}$$

where $\operatorname{Rk}(S)$ stands for the linear rank of a subset S of V, i.e. the dimension of the $\mathbb{R}$-linear span of S.

Lemma 5.8. *In the previous definition the infimum is also a minimum. In other words, for $r < \lambda_k$, the set $\Lambda \cap r\overline{B}$ has rank at most $k-1$, whereas for $r \geq \lambda_k$, it as rank at least k.*

Proof. The set $N = \{|x| \mid x \in \Lambda\}$ is discrete and closed in $\mathbb{R}_+$, so their exist $u > \lambda_k$ such that :

$$]\lambda_k, u] \cap N = \emptyset.$$

It follows that for every $r \in [\lambda_k, u]$ one has :

$$r\overline{B} \cap \Lambda = \lambda_k\overline{B} \cap \Lambda$$

which implies that the ranks of $\lambda_k\overline{B}$ and $u\overline{B}$ are the same and are at least k. □

Notice one has :

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_d$$

but in general the inequalities are not strict. The first successive minimum λ_1 is the smallest norm of a non-zero element of Λ. By Minkowski's first theorem 5.5 one has :

$$\lambda_1 \leq 2\left(\frac{\operatorname{covol}(\Lambda)}{\mu(B)}\right)^{1/d}$$

pour μ une mesure de Lebesgue quelconque sur V.

Theorem 5.9. *(Existence of a Minkowski basis) There exist some linearly independent vectors $v_1, \ldots, v_d \in \Lambda$ such that for all k :*

$$|v_k| = \lambda_k$$

and in particular :

$$\operatorname{Vect}_{\mathbb{R}}\left(\Lambda \cap \lambda_k\overline{B}\right) = \operatorname{Vect}_{\mathbb{R}}(v_1, \ldots, v_k).$$

Proof. Suppose $v_1,\dots,v_{k-1}$ are defined and satisfy $|v_i| = \lambda_i$ for $i < k$. By lemma 5.8, the set $\lambda_k \overline{B} \cap \Lambda$ has rank k and contains $v_1,\dots,v_{k-1}$ so there exist $v_k \in \Lambda$ outside of the $\mathbb{R}$-span of the v_i for $i < k$ such that $|v_k| \leq \lambda_k$. Necessarily $|v_k| \geq \lambda_k$ (by definition of λ_k), which implies that :

$$|v_k| = \lambda_k$$

The second statement comes from the fact that these two spaces have the same dimension and clearly $v_i \in \Lambda \cap \lambda_k \overline{B}$ for $i \leq k$. □

In general we can't find such v_i that generate Λ : they will only generate a sublattice of Λ. However we may find a basis of Λ consisting of small enough vectors :

Corollary 5.10. *There exist $(w_1,\dots,w_d)$ a $\mathbb{Z}$-basis of Λ such that :*

$$|w_k| \leq 2^{k-1}\lambda_k$$

and

$$\Lambda \cap \lambda_k B \subseteq \mathrm{Vect}_{\mathbb{Z}}(w_1,\dots,w_{k-1})$$

for all $1 \leq k \leq d$.

Proof. Pick a basis (v_i) as given by 5.9. Consider the sublattice $\mathrm{Vect}_{\mathbb{Z}}(v_1,\dots,v_k)$ of Λ. By the second part of the lemma below 5.11 one can find a basis $(w_1,\dots,w_d)$ of Λ and integers a_{ij} such that :

$$v_i = a_{i1}w_1 + \cdots + a_{ii}w_i$$

for all i, with $0 \leq a_{ij} < a_{ii}$. By induction we show that :

$$|w_j| \leq 2^{j-1}\lambda_j$$

for all j. Let $j \geq 1$, and suppose the inequality is true for all $k < j$. One has :

$$|w_j| = \frac{|v_j - a_{j1}w_1 - \cdots - a_{j,j-1}w_{j-1}|}{a_{jj}} \leq \sum_{k=1}^{j-1}|w_k| + \lambda_j \leq \sum_{k=1}^{j-1} 2^{k-1}\lambda_k + \lambda_j \leq 2^{j-1}\lambda_j.$$

as desired.
It follows from the properties of basis $(v_1,\dots,v_d)$ that for all k :

$$\Lambda \cap \lambda_k B \subseteq \Lambda \cap \mathrm{Vect}_{\mathbb{R}}(v_1,\dots,v_{k-1}) \subseteq \Lambda \cap \mathrm{Vect}_{\mathbb{R}}(w_1,\dots,w_{k-1})$$

because the base change is triangular. Note that $\Lambda \cap \mathrm{Vect}_{\mathbb{R}}(w_1,\dots,w_{k-1}) = \mathrm{Vect}_{\mathbb{Z}}(w_1,\dots,w_{k-1})$ because $\underline{w}$ is a basis of Λ, which concludes the proof. □

We used the following technical lemma that allows one to create a basis of Λ from a basis of some sublattice or conversely create a basis of a sublattice starting from a basis of Λ.

Lemma 5.11. *(Adapted basis lemma) Let $L \subseteq M$ be two lattices of V, and d denote the dimension of V.*
For any basis $(m_1,\dots,m_d)$ of M there exist a basis $(\ell_1,\dots,\ell_d)$ of L with triangular base change matrix $P = (p_{ij})$ with :

$$\ell_i = \sum_j p_{ij}m_j$$

or more visually :

$$\begin{aligned}
\ell_1 &= p_{11}m_1 \\
\ell_2 &= p_{21}m_1 + p_{22}m_2 \\
\ell_3 &= p_{31}m_1 + p_{32}m_2 + p_{33}m_3 \\
&\vdots
\end{aligned}$$

with $p_{ij} \in \mathbb{N}$, and $p_{ij} = 0$ for $j > i$, as well as $p_{ij} < p_{jj}$ for $j < i$.
Conversely, for any basis $(\ell_1,\dots,\ell_d)$ of L there exist a basis $(m_1,\dots,m_d)$ of M such that one has the same conditions as above except the last one which becomes : $p_{ij} < p_{ii}$ for $j < i$.

Proof. Let $(m_1,\dots,m_d)$ be a basis of M. Since M and L are free abelian group of the same rank, the group M/L is finite (because finitely generated of rank 0) which implies that for all i the set :

$$L \cap \{p_{i1}m_1 + \cdots + p_{ii}m_i \mid p_{ij} \in \mathbb{N},\ p_{ii} > 0\}$$

is non empty. Take $\ell_i = p_{i1}m_1 + \cdots + p_{ii}m_i$ in this set with p_{ii} minimal.
Now let us see why $(\ell_1,\dots,\ell_d)$ is a basis of L. It is free because the matrix P is non-singular. It generates L : let $x \in L \setminus \{0\}$ not generated by these vectors. One can write :

$$x = x_1m_1 + \cdots + x_km_k$$

with $k \leq d$, $x_k \neq 0$ and k minimal. Now write :

$$x_k = qp_{kk} + r$$

with $r < p_{kk}$. This yields :

$$x = q\ell_k + (x_1 - p_{k1})m_1 + \cdots + (x_{k-1} - p_{k,k-1})m_{k-1} + rm_k$$

hence $(x_1 - p_{k1})m_1 + \cdots + (x_{k-1} - p_{k,k-1})m_{k-1} + rm_k$ is an element of L, and by minimality of p_{ii}, we have :

$$r = 0$$

and then $(x_1 - p_{k1})m_1 + \cdots + (x_{k-1} - p_{k,k-1})m_{k-1}$ is also in L which implies, by minimality of k that it is generated by the ℓ_i, which means the same is true for x : it is a contradiction.
Hence $\underline{\ell}$ is a basis for L. Now we change this triangular system to obtain the inequalities that we want. Consider the elements :

$$\ell'_i = t_{i1}\ell_1 + \cdots + t_{ii}\ell_i$$

with t_{ij} in $\mathbb{Z}$ to be chosen later and $t_{ii} = 1$. The matrix $T = (t_{ij})$ is in $\mathrm{GL}_d(\mathbb{Z})$ because it has determinant 1, which means $\underline{\ell'}$ is still a basis for L.
Now define the matrix $P' = TP$, still triangular, with $p'_{ii} = p_{ii}$, so that :

$$\ell'_i = p'_{i1}m_1 + \cdots + p'_{ii}m_i$$

and it remains to show that we can choose t_{ij} in order to have for all $j < i$:

$$0 \leq p'_{ij} < p'_{jj} = p_{jj}$$

We fix i and choose $t_{i,i-1}$ then $t_{i,i-2}$, etc. until $t_{i,1}$. The first row of the system gives :

$$p'_{i,i-1} = t_{i,i-1}p_{i-1,i-1} + p_{i,i-1}$$

which allows, by changing $t_{i,i-1}$, to choose $p'_{i,i-1}$ to be any integer congruent to $p_{i,i-1}$ modulo $p_{i-1,i-1}$, and there is one satisfying :

$$0 \leq p'_{i,i-1} < p_{i-1,i-1}$$

and we do the same with the other rows of the system.

Now let us deal with the second part of the lemma. Let $\underline{\ell}$ be a basis for L. Since M/L is finite, there is some $D > 0$ such that :

$$DM \subseteq L.$$

Now we may apply the first statement of the lemma to the sublattice DM of L : there is a basis $(Dm_1,\dots,Dm_d)$ of DM such that :

$$\begin{aligned} Dm_1 &= q_{11}\ell_1 \\ Dm_2 &= q_{21}\ell_1 + q_{22}\ell_2 \\ Dm_3 &= q_{31}\ell_1 + q_{32}\ell_2 + q_{33}\ell_3 \\ &\vdots \end{aligned}$$

with $q_{ij} \geq 0$ et $q_{ii} > 0$. By inverting the system we obtain :

$$\begin{aligned}
\ell_1 &= u_{11} Dm_1 \\
\ell_2 &= u_{21} Dm_1 + u_{22} Dm_2 \\
\ell_3 &= u_{31} Dm_1 + u_{32} Dm_2 + u_{33} Dm_3 \\
&\vdots
\end{aligned}$$

with $U = Q^{-1} \in M_d(\mathbb{Q})$. Since $\underline{m}$ is a basis for M, the $u_{ij} D$ are integers. Now if we let $p_{ij} = Du_{ij} \in \mathbb{Z}$ and perform the same trick as in the first part we can get the desired inequalities. □

Now we prove the second Minkowski's theorem which gives an estimate of :

$$\prod_{k=1}^{d} \lambda_k$$

that generalizes the inequality given by the first Minkowski's theorem :

$$\lambda_1 \leq 2 \left(\frac{\operatorname{covol}(\Lambda)}{\mu(B)} \right)^{1/d}.$$

Several versions of this theorem exist, we only need the following one where the norm on V is *euclidean*.

Theorem 5.12. *(Minkowski's second theorem) Suppose the norm $|\bullet|$ comes from a euclidean inner product $\langle \bullet, \bullet \rangle$ on V. Then one has the following bounds :*

$$\beta_d \frac{\operatorname{covol}(\Lambda)}{\mu(B)} \leq \prod_{k=1}^{d} \lambda_k \leq 2^d \frac{\operatorname{covol}(\Lambda)}{\mu(B)}$$

with :

$$\beta_d = \frac{\pi^{d/2}}{\Gamma(\frac{d}{2}+1)} = \frac{1}{\sqrt{\pi d}} \left(\frac{2\pi e}{d} \right)^{d/2} (1 + o(1))$$

the volume of the unit ball of $\mathbb{R}^d$ and $d = \dim V$.

Proof. The formula we wish to prove is independent on the Lebesgue measure μ so we can assume it is compatible with the euclidean structure in the sense that any d-dimensional cube spanned by some orthonormal basis of V has volume 1.
Consider bases $(v_1, \ldots, v_d)$ and $(w_1, \ldots, w_d)$ given by the theorems 5.9 and 5.10 :
they are families of linearly independent vectors of Λ, with $|v_i| = \lambda_i$, $\underline{w}$ is a basis of Λ and :

$$\Lambda \cap \lambda_k B \subseteq \operatorname{Vect}_{\mathbb{Z}}(w_1, \ldots, w_{k-1})$$

for all k. We put $\Lambda' = \operatorname{Vect}_{\mathbb{Z}}(v_1, \ldots, v_d)$, the sublattice of Λ spanned by the (v_i).
The notation $[x_1, \ldots, x_d]$ stands for the determinant of $\underline{x}$ in some orthonormal basis of V (defined up to sign).
Hadamard's inequality yields :

$$|[v_1, \ldots, v_d]| \leq \prod_{k=1}^{d} |v_k| = \prod_{k=1}^{d} \lambda_k$$

and we also have :

$$|[v_1, \ldots, v_d]| = \operatorname{covol}(\Lambda') = \operatorname{covol}(\Lambda) \cdot [\Lambda : \Lambda'] \geq \operatorname{covol}(\Lambda).$$

Therefore :

$$\prod_{k=1}^{d} \lambda_k \geq \operatorname{covol}(\Lambda) = \beta_d \frac{\operatorname{covol}(\Lambda)}{\mu(B)}$$

as desired.
Now let us show that the upper bound stands. Using Schmidt's orthonormalization, there exist an orthonormal basis $(e_1, \ldots, e_d)$ of V and some real numbers t_{ij} such that :

$$w_i = \sum_{j \leq i} t_{ij} e_j$$

with $t_{ii} > 0$. We can then consider the vectors :

$$w_i' = \sum_{j \leq i} \frac{t_{ij}}{\lambda_j} e_j$$

which define a basis for V. They generate another lattice L of V with covolume :

$$\mathrm{covol}(L) = \left| \det\left(\frac{t_{ij}}{\lambda_j}\right)_{i,j} \right| = \prod_i \frac{t_{ii}}{\lambda_i} = \frac{\mathrm{covol}(\Lambda)}{\prod_i \lambda_i}$$

Next we show that the first successive minimum of L is at least 1 :

$$\lambda_1(L) \geq 1.$$

Let $x \in L$ be non-zero. We write :

$$x = \sum_{i=1}^{p} x_i w_i' = \sum_{i=1}^{p} \sum_{j=1}^{i} \frac{t_{ij} x_i}{\lambda_j} e_j = \sum_{j=1}^{p} \left(\sum_{i=j}^{p} \frac{t_{ij} x_i}{\lambda_j} \right) e_j$$

with $x_i \in \mathbb{Z}$ and $x_p \neq 0$ so that :

$$\begin{aligned} |x|^2 &= \sum_{j=1}^{p} \left(\sum_{i=j}^{p} \frac{t_{ij} x_i}{\lambda_j} \right)^2 = \sum_{j=1}^{p} \frac{1}{\lambda_j^2} \left(\sum_{i=j}^{p} t_{ij} x_i \right)^2 \geq \frac{1}{\lambda_p^2} \sum_{j=1}^{p} \left(\sum_{i=j}^{p} t_{ij} x_i \right)^2 \\ &= \frac{1}{\lambda_p^2} \left| \sum_{i=1}^{p} x_i w_i \right|^2 \geq 1 \end{aligned}$$

as desired, because $\sum_{i=1}^{p} x_i w_i \in \Lambda \setminus \mathrm{Vect}_{\mathbb{Z}}(w_1, \ldots, w_{p-1}) \subseteq V \setminus \lambda_p B$. By Minkowski's first theorem we obtain :

$$1 \leq \lambda_1(L) \leq 2 \left(\frac{\mathrm{covol}(L)}{\mu(B)} \right)^{1/d}$$

hence :

$$\prod_i \lambda_i \leq 2^d \frac{\mathrm{covol}(\Lambda)}{\mu(B)}$$

which concludes the proof. □

Eventually we prove the following theorem which is used to count elements in the intersection of a lattice with some sufficiently large set. In this theorem we do not assume that the norm is euclidean.

Theorem 5.13. *Let A be a measurable subset of V and F be a measurable fundamental domain for Λ. One has :*

$$|\Lambda \cap A| \leq \frac{\mu(A + F)}{\mathrm{covol}(\Lambda)}$$

Also there exist a measurable fundamental domain F contained in the closed ball centered at 0 with radius $2^d \lambda_d$:

$$F \subseteq \overline{B}(0, 2^d \lambda_d)$$

In particular one has :

$$|\Lambda \cap A| \leq \frac{\mu(A + \overline{B}(0, 2^d \lambda_d))}{\mathrm{covol}(\Lambda)}.$$

Proof. The first statement comes from the fact that :

$$\bigsqcup_{x \in \Lambda \cap A} (x + F) \subseteq A + F$$

which yields $\mu(F)\times|\Lambda\cap A|\leq\mu(A+F)$. For the second one, we pick a basis (w_i) of Λ as given by theorem 5.10 with :

$$|w_k|\leq 2^{k-1}\lambda_k$$

for all k. Consider the fundamental domain F defined by :

$$F=\left\{\sum_i t_i w_i \mid (t_i)\in[0,1[^d\right\}.$$

The triangular inequality gives :

$$F\subseteq\overline{B}(0,2^d\lambda_d).$$

because $\sum_{k=1}^d 2^{k-1}\lambda_k\leq\sum_{k=1}^d 2^{k-1}\lambda_d\leq 2^d\lambda_d$. □

6 Appendix 2 : A bound on the number of subgroups of a finite group

According to [1], we prove :

Theorem 6.1. *Let G be a finite group of order n. Then the number of subgroups of G is bounded above by :*

$$n^{\log_2 n}(\log n)^{O(\log n)}.$$

For this we need the following lemma.

Lemma 6.2. *A group G of order n can be generated by at most $\log_2(n)$ elements.*

Proof. By induction one can find a set of elements $g_1,\dots,g_k\in G$ with, for all i, (where $H_{i-1}=\langle g_1,\dots,g_{i-1}\rangle$) : $g_i\notin H_{i-1}$ and $G=H_k$ (and $H_0=1$). Notice that $[H_i:H_{i-1}]\geq 2$, hence :

$$n=[H_k:H_0]=\prod_{i=1}^k[H_i:H_{i-1}]\geq 2^k$$

so $k\leq\log_2(n)$: we have proved that G has a set of at most $\log_2(n)$ generators. □

We now prove the theorem.

Proof. According to lemma 6.2, any subgroup of G can be generated with at most $\log_2(n)$ elements of G. Hence the number of subgroups of G is bounded below by the number of subsets of G with at most $\log_2(n)$ elements, that is :

$$\sum_{k=0}^{\lfloor\log_2(n)\rfloor}\binom{n}{k}\leq(1+\log_2 n)\binom{n}{\log_2 n}$$

for large enough n. Using Stirling's approximation one has :

$$\binom{n}{\log_2 n}=n^{\log_2 n}(\log n)^{O(\log(n))}$$

which yields the desired result since multiplying by $\log_2 n+1$ doesn't affect the $O(\log(n))$ in the exponent. □

Corollary 6.3. *The symetric group $\mathfrak{S}_n$ has at most :*

$$n^{n^2\log n+O(n^2)}$$

many subgroups.

Proof. Using theorem 6.1 with $|\mathfrak{S}_n|=n!$ the group $\mathfrak{S}_n$ has at most :

$$\begin{aligned}(n!)^{\log_2(n!)}(\log(n!))^{O(\log(n!))}&=\exp\left(\frac{\log(n!)^2}{\log 2}\right)(n\log n+O(n))^{O(n\log n)}\\&=\exp\left(\frac{(n\log n)^2+O(n^2\log n)}{\log 2}+O(n\log n\log(n\log n+O(n)))\right)\\&=\exp\left(\frac{(n\log n)^2+O(n^2\log n)}{\log 2}\right)=n^{n^2\log_2 n+O(n^2)}=n^{n^2\log n+O(n^2)}\end{aligned}$$

many subgroups. □

7 Appendix 3 : An inequality on the Gamma function

Using [2], lemma 1.7, we prove the following inequality, where Γ is the usual Gamma function.

Proposition 7.1. *For all $x \geq 0$ one has :*

$$\Gamma(1+x) \leq x^x e^{-x} \sqrt{2\pi(1+x)}.$$

Proof. As usual denote by ψ the logarithmic derivative of Γ :

$$\psi(x) = \frac{\Gamma'(x)}{\Gamma(x)}$$

which is well defined and smooth for $x > 0$. According to [2], lemma 1.7, one has :

$$\psi(1+x) \geq \log\left(x + \frac{1}{2}\right)$$

for all $x \geq 0$. Now define :

$$f(x) = \log\Gamma(1+x) - \log\left(x^x e^{-x}\sqrt{2\pi(1+x)}\right) = \log\Gamma(1+x) - x\log x + x - \frac{1}{2}\log(2\pi(1+x))$$

so that :

$$f'(x) = \psi(1+x) - \log(x) - \frac{1}{2+2x} \geq \log\left(x+\frac{1}{2}\right) - \log(x) - \frac{1}{2+2x} \geq \log\left(1+\frac{1}{2x}\right) - \frac{1}{2+2x}.$$

Assuming we have proved that this last quantity is always positive for $x > 0$, we obtain that f is an increasing function. According to Stirling's approximation we have, when x goes to infinity :

$$f(x) = x\log x - x + \frac{1}{2}\log(2\pi x) + o(1) - x\log x + x - \frac{1}{2}\log(2\pi(1+x)) \longrightarrow 0$$

so f is a negative function, which is what we wanted.
It remains to show that :

$$\log\left(1+\frac{1}{2x}\right) \geq \frac{1}{2+2x}$$

for $x > 0$. Differentiating the difference gives :

$$\frac{d}{dx}\left(\log\left(1+\frac{1}{2x}\right) - \frac{1}{2+2x}\right) = \frac{-1}{2x^2+x} + \frac{1}{2(x+1)^2} \leq 0$$

hence the difference is a decreasing function but its limit at ∞ is 0 so it is a positive function. □

This result is used for the following lemma that we need in theorem 1.3.

Lemma 7.2. *Recall the definition of A_n from theorem 1.3 :*

$$A_n = \frac{4}{\pi}\frac{\Gamma\left(\frac{n}{2}+1\right)^{2/n}}{n^{1/n}}.$$

Then for all $n \geq 1$, one has :

$$A_n \leq \frac{6}{e}n \leq 3n.$$

Proof. Using 7.1, we have :

$$\begin{aligned} A_n &\leq \frac{4}{\pi}\frac{\left(\left(\frac{n}{2e}\right)^{n/2}\sqrt{2\pi(1+n/2)}\right)^{2/n}}{n^{1/n}} \leq \frac{4}{\pi}\frac{n}{2e}\left(2\pi\left(\frac{1}{n}+\frac{1}{2}\right)\right)^{1/n} \\ &\leq \frac{2n}{\pi e}\left(2\pi\left(\frac{3}{2}\right)\right) \leq \frac{6}{e}n \leq 3n. \end{aligned}$$

□

References

[1] General bound for the number of subgroups of a finite group, 2013. URL: https://mathoverflow.net/questions/132675/general-bound-for-the-number-of-subgroups-of-a-finite-group.

[2] Necdet Batir. Bounds for the gamma function, 2017. arXiv:1705.06167.

[3] Manjul Bhargava, Arul Shankar, Takashi Taniguchi, Frank Thorne, Jacob Tsimerman, and Yongqiang Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves, 2017. arXiv:1701.02458.

[4] Thomas F. Bloom and Jared Duker Lichtman. The bombieri-pila determinant method, 2023. arXiv:2312.12890.

[5] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Mathematical Journal*, 59(2):337 – 357, 1989. doi:10.1215/S0012-7094-89-05915-2.

[6] Arthur B. Coble. *The American Mathematical Monthly*, 39(5):293–295, 1932. URL: http://www.jstor.org/stable/2300863.

[7] Jean-François Dat. Td 1, 2023. URL: https://webusers.imj-prg.fr/~jean-francois.dat/enseignement/VA/TD1.pdf.

[8] Matthew Emerton. Genus theory. URL: https://math.uchicago.edu/~emerton/number-theory/genus.pdf.

[9] Christopher Frei and Martin Widmer. Averages and higher moments for the ℓ-torsion in class groups, 2020. URL: https://arxiv.org/abs/1810.04732, arXiv:1810.04732.

[10] Jürgen Klüners and Jiuya Wang. ℓ-torsion bounds for the class group of number fields with an ℓ-group as galois group, 2020. arXiv:2003.12161.

[11] Peter Koymans and Carlo Pagano. A sharp upper bound for the 2-torsion of class groups of multiquadratic fields, 2020. arXiv:2009.08399.

[12] Guy Robin. Estimation de la fonction de tchebychef theta sur le k-ième nombre premier et grandes valeurs de la fonction nombre de diviseurs premiers de n. *Acta Arithmetica*, 42(4):367–389, 1983. URL: http://eudml.org/doc/205883.