ON EUCLIDEAN IDEAL CLASSES IN CERTAIN ABELIAN EXTENSIONS

J.-M. DESHOUILLERS, S. GUN AND J. SIVARAMAN

ABSTRACT. In this article, we show that certain abelian extensions K with unit rank greater than or equal to 3 have cyclic class group if and only if it has a Euclidean ideal class. This result improves an earlier result of Murty and Graves. One can improve this result up to unit rank 2 if one assumes the Elliott and Halberstam conjecture (see Conjecture 1 in preliminaries). These results are known under generalized Riemann hypothesis by the work of Lenstra [17] (see also Weinberger [21]).

1. INTRODUCTION

Throughout the paper, let K be a number field with ring of integers $\mathcal{O}_K$ and an infinite unit group $\mathcal{O}_K^\times$. We shall call the rank of $\mathcal{O}_K^\times$, the unit rank of K. Also let E_K be the set of all fractional ideals of K containing $\mathcal{O}_K$. An ideal class $[\mathfrak{I}]$ of Cl_K is called a Euclidean ideal class if there exists a map $\psi : E_K \to \mathbb{N}$ such that for any ideal $\mathfrak{a} \in [\mathfrak{I}]$ and for all ideals $\mathfrak{b} \in E_K$ and for all $x \in \mathfrak{ab} \setminus \mathfrak{a}$, there exists $z \in x + \mathfrak{a}$ such that

$$\psi(z^{-1}\mathfrak{ab}) < \psi(\mathfrak{b}).$$

When $\mathcal{O}_K$ is a PID, the principal ideal class is Euclidean if and only if $\mathcal{O}_K$ is a Euclidean domain.

Lenstra [17] introduced the notion of Euclidean ideal classes in order to generalize the concept of Euclidean domains and also to capture cyclic class groups. In the same paper, Lenstra showed that class group Cl_K of K is cyclic if and only if it has a Euclidean ideal class, provided generalized Riemann hypothesis holds. When $\mathcal{O}_K$ is a PID, this result was already proved by Weinberger [21]. Prior to this work, Motzkin [18], while trying to answer a question of Zariski, showed that if the unit rank of K is zero and $\mathcal{O}_K$ is a PID then it does not necessarily mean that $\mathcal{O}_K$ is Euclidean. In the same paper, Motzkin also devised a criterion to determine when an integral domain is Euclidean. Using this criterion and its variant deduced by Clark and Murty [3], several authors [10, 12, 13, 16, 19] have tried to prove the result of Weinberger unconditionally.

In a recent work, Graves [7] generalized Clark and Murty's criterion in the set-up of Euclidean ideal classes. Using this criterion, Graves and Murty [8] tried to remove generalized

2010 *Mathematics Subject Classification.* 11A05, 13F07, 11R04, 11R27, 11R32, 11R37, 11R42, 11N36.

Key words and phrases. Euclidean ideal classes, Galois Theory, Hilbert class fields, Brun's Sieve, Bombieri-Vinogradov theorem, Linear Sieve.

Riemann hypothesis from the work of Lenstra for certain abelian extensions. More precisely, they showed that if the Hilbert class field $H(K)$ of K is abelian over $\mathbb{Q}$ and unit rank of K is greater than or equal to 4, then Cl_K is cyclic if and only if it has a Euclidean ideal class. In [8], the authors require a co-primality condition (section 5, page 2982) whose proof appears to be incomplete. In this article, we restrict ourselves to a finer family of number fields, but improve on the rank as our theorem works even when these number fields have unit rank 3.

More precisely, we prove the following theorem.

Theorem 1. *Suppose that K is a number field with unit rank greater than or equal to 3 and its Hilbert class field $H(K)$ is abelian over $\mathbb{Q}$. Also suppose that the conductor of K is f and $\mathbb{Q}(\zeta_f)$ over K is cyclic. Then Cl_K is cyclic if and only if it has a Euclidean ideal class.*

As an immediate corollary, we have

Corollary 2. *Let K be an abelian number field with conductor f and the unit rank of K be greater than or equal to 3. If $\mathbb{Q}(\zeta_f)$ over K is cyclic, then $\mathcal{O}_K$ is Euclidean if and only if it is a PID.*

Result similar to Corollary 2 was deduced in [13] but again some additional arguments are required (see section 4, page 75) to complete the proof as in the case of [8].

In a recent work, the third author [20] shows that if one were only to consider the finiteness of the unit rank, the statement can be shown using an application of Brun's sieve as mentioned in [1]. Now if we assume the conjecture of Elliott and Halberstam (see section 2 for the precise statement), we can derive a stronger result. In particular, we have

Theorem 3. *Let K be a number field such that the Hilbert class field $H(K)$ is abelian and the Galois group $Gal(\mathbb{Q}(\zeta_f)/K)$ is cyclic where f is the conductor of K. Now if the Elliott and Halberstam conjecture is true and the unit rank of K is strictly greater than one, then Cl_K is cyclic if and only if it has a Euclidean ideal class.*

As before, one deduces that

Corollary 4. *Let K be an abelian number field with conductor f and the unit rank of K is strictly greater than one. Suppose that the Elliott and Halberstam conjecture is true. If $\mathbb{Q}(\zeta_f)$ over K is cyclic, then $\mathcal{O}_K$ is Euclidean if and only if it is a PID.*

The article is organized as follows. In section 2, we list some preliminaries and in section 3, we derive some sieve theoretic lemmas required for our result. In section 4, we give proofs of Theorem 1 and Theorem 3 and finally in section 5, we show that our arguments used to prove Theorem 1 and Theorem 3 actually prove stronger results.

2. PRELIMINARIES

Throughout the paper, we will assume that f is the smallest even integer such that $K \subseteq \mathbb{Q}(\zeta_f)$. We shall assume a variant of Motzkin's criterion proved by Graves [7] in the Euclidean ideal class set-up. In order to describe this criterion, let us consider the set

$$\tilde{E}_K := \{\mathfrak{p}^{-1} \in E_K \ : \ \mathfrak{p} \text{ is a prime ideal in } \mathcal{O}_K\} \cup \{\mathcal{O}_K\}$$

and its subsets defined as follows;

$$B_{0,\mathfrak{a}} := \mathcal{O}_K, \quad B_{i,\mathfrak{a}} := B_{i-1,\mathfrak{a}} \cup \Big\{\mathfrak{p}^{-1} \in \tilde{E}_K \ : \ \text{for all } x \in \mathfrak{p}^{-1}\mathfrak{a} \setminus \mathfrak{a}, \text{there exists } y \in \mathfrak{a} \text{ such that } (x-y)^{-1}\mathfrak{p}^{-1}\mathfrak{a} \in B_{i-1,\mathfrak{a}}\Big\}.$$

Lemma 5. [Variant of Motzkin's criterion (Graves [7])] *Let K be a number field and $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. If*

$$\tilde{E}_K = \cup_{i=0}^{\infty} B_{i,\mathfrak{a}}\,, \tag{1}$$

then $[\mathfrak{a}]$ is a Euclidean ideal class.

In the same article, Graves showed that to prove (1), it is sufficient to show the following lemma which can be thought of as a generalization of Harper's criterion (see pages 61-62 of [12]).

Lemma 6 (Graves [7])**.** *Let K be a number field with infinitely many units and cyclic class group Cl_K. If $[\mathfrak{a}]$ generates Cl_K and*

$$|\{\mathfrak{p} \ : \ \mathfrak{N}(\mathfrak{p}) \leq x, \ [\mathfrak{p}] = [\mathfrak{a}], \ \mathcal{O}_K^{\times} \to (\mathcal{O}_K/\mathfrak{p})^{\times} \text{ is surjective}\}| \gg \frac{x}{\log^2 x},$$

then $[\mathfrak{a}]$ is a Euclidean ideal class. Here $\mathfrak{N}(\mathfrak{p})$ denotes the norm of an ideal $\mathfrak{p}$.

Another important ingredient required for our proofs is the following result of Gupta and Murty as given in the paper of Harper and Murty [13].

Lemma 7 (Gupta and Murty [9])**.** *Let K be a number field and r be the rank of $\mathcal{O}_K^{\times}$. Also let P_K be the set of prime ideals in $\mathcal{O}_K$. For $\mathfrak{p} \in P_K$, if $f_{\mathfrak{p}}$ denotes the cardinality of the set $\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_K^{\times}\}$, then*

$$|\{\mathfrak{p} \in P_K \ : \ f_{\mathfrak{p}} \leq Y\}| \ll Y^{1+\frac{1}{r}}.$$

Other important ingredients required to prove our results come from the lower bound sieve of Friedlander and Iwaniec [6] and also the result of Bombieri, Friedlander and Iwaniec [2]. To describe these results, we need to introduce few more notations. Let $P_{\mathbb{Q}}$ be the set of rational primes, $\mathcal{P}$ be a subset of $P_{\mathbb{Q}}$, z be a real number and

$$\mathcal{P}(z) := \prod_{\substack{p \in \mathcal{P}, \\ p \leq z}} p. \tag{2}$$

Given a subset of non negative integers $\mathcal{A}$, let $\mathcal{A}_q := \{a \in \mathcal{A} \ : \ q|a\}$, where q is a natural number. Suppose that ω is a multiplicative function and q is a square free natural number with all its prime divisors in $\mathcal{P}$ such that

$$|\mathcal{A}_q| \ = \ \frac{\omega(q)}{q}|\mathcal{A}| \ + \ r_q, \tag{3}$$

for some r_q. Set

$$V(z) = \prod_{\substack{p<z,\\ p\in\mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right) \tag{4}$$

and

$$S(\mathcal{A}, \mathcal{P}, z) = \{a \in \mathcal{A} \ : \ (a, \mathcal{P}(z)) = 1\}, \tag{5}$$

where $(a, \mathcal{P}(z))$ denotes the gcd of a and $\mathcal{P}(z)$. We now introduce the notion of a well factorable function as defined by Iwaniec [15] (see also page 255 of [6]).

Definition 1. *Let D be a real number greater than or equal to one and $\lambda(q)$ be an arithmetic function with support $[1, D]$. We say that λ is a well factorable function of level D if for any real numbers $M, N \geq 1$ with $MN = D$, one can write*

$$\lambda(q) := \sum_{\substack{mn=q,\\ m\leq M,\\ n\leq N}} \alpha(m)\beta(n), \qquad \textit{where} \quad 1 \leq q \leq MN.$$

Here α and β are arithmetic functions which depend on M, N and $|\alpha(m)|, |\beta(n)| \leq 1$.

In this set-up, one has the following lower bound Sieve.

Theorem 8. [Friedlander and Iwaniec (see page 256 of [6], see also Iwaniec [15])] *Let $D \geq 1$, $s \geq 2$ be real numbers and $z = D^{1/s}$. Also let $\mathcal{A}$ be a subset of non-negative integers satisfying*

$$\prod_{\substack{w\leq p<z,\\ p\in\mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \leq T \ \left(\frac{\log z}{\log w}\right),$$

where $w \geq 2$ is an integer and $T > 0$ is an absolute constant. Then for sufficiently large D and for any real number $\varepsilon > 0$, we have

$$S(\mathcal{A}, \mathcal{P}, z) \ \geq \ XV(z)\{g(s) - \varepsilon\} + \sum_{d|\mathcal{P}(z)} \lambda(d) \ r_d.$$

Here $|\mathcal{A}| \sim X$, $\mathcal{P}(z), V(z)$ be as in (2) and (4), λ is some well factorable function of level D and g is a continuous function on $[2, \infty)$ satisfying

$$g(s) \ = \ 2e^{\gamma} \log(s-1)/s,$$

for $s \in [2, 4]$. Here γ is the Euler and Mascheroni constant.

To complete the proof of Theorem 1, we estimate the error term by using the following theorem.

Theorem 9. [Bombieri, Friedlander and Iwaniec (see [2], see also [5, 14])] *Let a, k be positive natural numbers with $(a, k) = 1$. For any positive natural number q with $(q, k) = 1$, let*

$$u_q \equiv a \bmod k \qquad \text{and} \qquad u_q \equiv 1 \bmod q.$$

Fix a positive integer $A > 0$ and a real number $\theta < 4/7$. For every well factorable function λ of level x^θ, one has

$$\sum_{\substack{q \le x^\theta \\ (q,k)=1}} \lambda(q) \left(\pi(x, qk, u_q) - \frac{\mathrm{li}(x)}{\varphi(qk)} \right) \ll \frac{x}{\log^A x}.$$

The constant in $\ll$ depends on a, A, k and θ.

As we mentioned in the introduction, one can improve Theorem 1, if one uses the following conjecture along with an elementary version of the linear sieve.

Conjecture 1. [Elliott and Halberstam conjecture [4]] *For every real number $\theta < 1$ and for every positive integer $A > 0$, one has*

$$\sum_{q \le x^\theta} \max_{y \le x} \max_{(a,q)=1} \left| \pi(y, q, a) - \frac{\mathrm{li}(y)}{\varphi(q)} \right| \ll \frac{x}{\log^A x}$$

for all real numbers $x > 2$.

We now state the elementary version of the linear sieve required for our proof. Notations are as before.

Theorem 10. [Halberstam and Richert (see page 236 of [11])] *Let $\mathcal{P}$ be a subset of $P_{\mathbb{Q}}$, z be a real number and $\mathcal{P}(z), \omega, r_q, V(z)$ and $S(\mathcal{A}, \mathcal{P}, z)$ be as in* (2), (3), (4) *and* (5). *Suppose that*

(1) *there exists a constant $A_1 \ge 1$ such that*

$$0 \le \frac{\omega(p)}{p} \le 1 - \frac{1}{A_1}$$

for all $p \in \mathcal{P}$;

(2) *there exist constants L and A_2, independent of z and integer g_1 with $2 \le g_1 \le z$ such that*

$$-L \le \sum_{\substack{g_1 \le p \le z \\ p \in \mathcal{P}}} \frac{\omega(p) \log p}{p} - \log \left(\frac{z}{g_1} \right) \le A_2 \, ;$$

(3) *there exists a real number α with $0 < \alpha \le 1$ such that*

$$\sum_{\substack{q | P(z), \\ q < \frac{X^\alpha}{\log^F X}}} \mu^2(q) \, 3^{\nu(q)} | \, r_q | \le \frac{G_1 X}{\log^2 X}$$

for some positive constants F and G_1. Here μ is the Möbius function and $\nu(q)$ denotes the number of distinct prime divisors of q.

Then for $X \geq z$, one has

$$S(\mathcal{A}, \mathcal{P}, z) \geq XV(z)\left\{g\left(\alpha\frac{\log X}{\log z}\right) - \frac{B}{\log^{1/14} X}\right\},$$

where B is an absolute constant, g and X are as in Theorem 8.

3. Applications of Sieve methods

In this section, using Theorem 8 and Theorem 9, we deduce the following sieve theoretic result which plays a key role in the proof of Theorem 1.

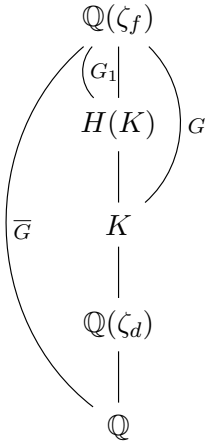
Theorem 11. *Let K be a number field and its Hilbert class field $H(K)$ be abelian over $\mathbb{Q}$. Also let f be the conductor of $H(K)$ and $\mathbb{Q}(\zeta_f)$ over K be cyclic. Set $d := \max\{n \,:\, \mathbb{Q}(\zeta_n) \subseteq K\}$ and*

$$\mathcal{A} := \left\{\frac{\ell - 1}{d} \,:\, \ell \in \mathbb{Q} \text{ is prime, } \ell \leq x, \text{ and } \ell \equiv b \bmod f\right\},$$

where $b \bmod f$ is a generator of $\mathbb{Q}(\zeta_f)$ over K. Let $\mathcal{P} := \{p \in \mathbb{Q} \,:\, p \text{ prime}\}$. Then for any real number $\eta < 16/63$, one has

$$S(\mathcal{A}, \mathcal{P}, x^\eta) \gg \frac{x}{\log^2 x}.$$

Proof. Let $\overline{G}$ be the Galois group of $\mathbb{Q}(\zeta_f)/\mathbb{Q}$, G be the Galois group of $\mathbb{Q}(\zeta_f)$ over K and G_1 be the Galois group of $\mathbb{Q}(\zeta_f)$ over $H(K)$. Consider the diagram



Then

$$\overline{G} := \{\sigma_a \,:\, 1 \leq a \leq n,\ (a, f) = 1\},$$

where $\sigma_a : \mathbb{Q}(\zeta_f) \to \mathbb{Q}(\zeta_f) \in \overline{G}$ is such that $\sigma_a(\zeta_f) = \zeta_f^a$ and

$$G \subset \left\{\sigma_a \in \overline{G} \,:\, a \equiv 1 \bmod d\right\}.$$

By assumption, G is cyclic and $\mathbb{Q}(\zeta_d)$ is the maximal cyclotomic field inside K. Since f is assumed to be even, $d|f$. We claim that

$$G \cap \left\{ \sigma_a \in \overline{G} \ : \ a \equiv 1 \bmod d, \ \left(\frac{a-1}{d}, \ \frac{f}{d} \right) = 1 \right\} \neq \phi.$$

Suppose not. Now if G is generated by σ_b, where $((b-1)/d, \ f/d) = h \neq 1$, then every element of G is of the form

$$\underbrace{\sigma_b \circ \cdots \circ \sigma_b}_{r \text{ times}} \ = \ \sigma_{b^r}.$$

Using Binomial theorem, we then have

$$G \subset \left\{ \sigma_a \in \overline{G} \ : \ a \equiv 1 \bmod dh \right\}.$$

This implies that

$$\mathbb{Q}(\zeta_{dh}) \ \subset \ K,$$

a contradiction to the maximality of d. Let $m = (b-1)/d$. Now choose n_0 such that

$$m + n_0 f/d \in P_{\mathbb{Q}} \quad \text{and} \quad (m + n_0 f/d, f) = 1.$$

For any real number $x > 0$, suppose that

$$\mathcal{A}' := \{ \ell - 1 \leq x \ : \ \ell \in \mathbb{Q} \text{ is prime and } \ell \equiv 1 + dm + n_0 f \bmod df \}.$$

Then we have

$$|\mathcal{A}'| \sim \frac{\mathrm{li}(x)}{\varphi(df)}$$

as $x \to \infty$. Set $\mathcal{P}_1 := \{p : p \nmid f\}$. Then for any $p \in \mathcal{P}_1$, we have

$$|\mathcal{A}'_p| = |\{u \in \mathcal{A}' : p|u\}| \sim \frac{\mathrm{li}(x)}{\varphi(pdf)}$$

as $x \to \infty$. Therefore for any square-free number q with prime divisors in $\mathcal{P}_1$, we have

$$|\mathcal{A}'_q| \ = \ \frac{\omega(q)}{q} |\mathcal{A}'| \ + \ r_q.$$

Here

$$\frac{\omega(q)}{q} = \frac{1}{\varphi(q)} \quad \text{and} \quad r_q = \left(\pi(x, qdf, u_q) - \frac{\mathrm{li}(x)}{\varphi(qdf)} \right),$$

where u_q satisfies

$$u_q \ \equiv \ 1 \bmod q \quad \text{and} \quad u_q \ \equiv \ 1 + dm + n_0 f \bmod df.$$

Since $2|f$, for any integer $w \geq 2$, one has

$$\begin{aligned}\prod_{\substack{w\leq p<z\\ p\in\mathcal{P}_1}}\left(1-\frac{\omega(p)}{p}\right)^{-1} &= \exp\left(-\sum_{\substack{w\leq p<z\\ p\in\mathcal{P}_1}}\log(1-\frac{1}{p-1})\right)\\ &= \exp\left(\sum_{\substack{w\leq p<z\\ p\in\mathcal{P}_1}}(\frac{1}{p-1}+\frac{1}{2(p-1)^2}+\cdots)\right)\\ &\leq \exp\left(\sum_{\substack{w\leq p<z\\ p\in\mathcal{P}_1}}\frac{1/(p-1)}{1-1/(p-1)}\right)\\ &\leq \exp\left(\sum_{\substack{w\leq p<z\\ p\in\mathcal{P}_1}}\frac{1}{p}+\frac{2}{p(p-2)}\right) \ll \frac{\log z}{\log w}.\end{aligned}$$

Therefore using Merten's theorem and Theorem 8, there exists an absolute constant $C_1 > 0$ such that

$$S(\mathcal{A},\mathcal{P}_1,D^{1/s}) \geq \frac{C_1 x}{\log^2 x}+\sum_{(q,df)=1}\lambda_n(q)\,r_q, \tag{6}$$

for some well factorable function λ_n of level $D \geq 1$ and for any $s \geq 2$. Now let $D = x^{4/7-\varepsilon}$ where $0 < \varepsilon < 4/7$ is a real number. Then applying Theorem 9 with $k = df$, we have

$$\sum_{\substack{q\leq D,\\ (q,df)=1}}\lambda_n(q)\,r_q \ll \frac{x}{\log^A x} \tag{7}$$

for any positive integer A. Finally by choosing $s = 9/4$ and using equations (6), (7), we get that

$$S(\mathcal{A}',\mathcal{P}_1,x^{\frac{4-7\varepsilon}{15.75}}) \gg \frac{x}{\log^2 x}.$$

Set

$$\mathcal{A}'' := \left\{\frac{\ell-1}{d} \ : \ \text{for all } \ell-1\in\mathcal{A}'\right\}.$$

Clearly $S(\mathcal{A}'',\mathcal{P}_1,x^\eta) \gg x/\log^2 x$ for any real number $\eta < 16/63$. Since every element of $\mathcal{A}''$ is co-prime to f and $\mathcal{A}'' \subset \mathcal{A}$, we have

$$S(\mathcal{A},\mathcal{P},x^\eta) \geq S(\mathcal{A}'',\mathcal{P},x^\eta) \gg \frac{x}{\log^2 x}.$$

□

Now if we assume the conjecture of Elliott and Halberstam (see Conjecture 1), we can prove the following statement using Theorem 10.

Theorem 12. *Suppose that the Elliott and Halberstam conjecture is true. Let K be a number field and its Hilbert class field $H(K)$ be abelian over $\mathbb{Q}$. Also let f be the conductor of $H(K)$ and $\mathbb{Q}(\zeta_f)$ over K be cyclic. Set $d := \max\{n \ : \ \mathbb{Q}(\zeta_n) \subseteq K\}$ and*

$$\mathcal{A} := \left\{ \frac{\ell - 1}{d} \ : \ \ell \in \mathbb{Q} \text{ is prime and } \ell \equiv b \bmod f \right\},$$

where $b \bmod f$ is a generator of $\mathbb{Q}(\zeta_f)$ over K. Let $\mathcal{P} := \{p \ : \ p \leq x\}$. Then for any positive real number $\eta < 1/2$, one has

$$S(\mathcal{A}, \mathcal{P}, x^{\eta}) \gg \frac{x}{\log^2 x}$$

where the constant implied in the symbol $\gg$ depends on η.

Proof. As in the proof of Theorem 11, we can show that there exists a $b \bmod f$ which generates $\mathbb{Q}(\zeta_f)$ over K such that $b = 1 + dm$ with $(m, f/d) = 1$. As before, choose an n_0 such that $m + n_0 f/d$ is a prime co-prime to f. Now let

$$\mathcal{A}' := \{\ell - 1 \leq x \ : \ \ell \in \mathbb{Q} \text{ is prime and } \ell \equiv 1 + dm + n_0 f \bmod df\}$$

and $\mathcal{P}_1 = \{p \ : \ p \nmid f\}$ be as in the proof of Theorem 11. Using Theorem 10, we would like to estimate $S(\mathcal{A}', \mathcal{P}_1, x^{1/2-\delta})$ for any $\delta > 0$. In order to apply Theorem 10, we need $\mathcal{A}'$ and $\mathcal{P}_1$ to satisfy the conditions of Theorem 10. Note that for all $p \in \mathcal{P}_1$, one has $\omega(p)/p = 1/\varphi(p)$ and

$$|r_q| \ \leq \ \max_{y \leq x} \max_{(a,q)=1} \left| \pi(y, qdf, a) - \frac{\mathrm{li}(y)}{\varphi(qdf)} \right|,$$

where q is any square-free number with primes divisors in $\mathcal{P}_1$. Since the conductor f of K is always even, condition 1 of Theorem 10 will be trivially satisfied by choosing $A_1 = 2$. To check condition 2, we consider

$$\sum_{\substack{g_1 \leq p \leq z \\ p \in \mathcal{P}_1}} \frac{\omega(p) \log p}{p} \ = \ \sum_{g_1 \leq p \leq z} \frac{\frac{p}{p-1} \log p}{p} \ - \ \sum_{\substack{g_1 \leq p \leq z, \\ p \mid df}} \frac{\frac{p}{p-1} \log p}{p}.$$

Since the second term in the above equality is bounded by a constant, we have

$$\begin{aligned} \sum_{\substack{g_1 \leq p \leq z \\ p \in \mathcal{P}_1}} \frac{\omega(p) \log p}{p} - \log(z/g) \ &= \ \sum_{g_1 \leq p \leq z} \frac{\log p}{p} \ + \ \sum_{g_1 \leq p \leq z} \frac{\log p}{p(p-1)} \ - \ \log(z/g_1) \ + \ O(1) \\ &= \ O(1). \end{aligned}$$

In order to check condition 3, we observe by Cauchy Schwarz inequality that

$$\sum\nolimits' \mu^2(q) \, 3^{\nu(q)} \, |r_q| \ \leq \ \sqrt{\sum\nolimits' \ 9^{\nu(q)} \, |r_q|} \, \sqrt{\sum\nolimits' \ |r_q|}$$

where the sum $\sum'$ is over the integers q which are less than $X^\alpha/\log^F X$ and divide $\mathcal{P}_1(z)$ Here $\mathcal{P}_1(z)$ is as defined in (2). Note that for any $q|\mathcal{P}_1(z)$, we have

$$\begin{aligned} |r_q| &\leq |\mathcal{A}'_q| + \left|\frac{\mathrm{li}(x)}{\varphi(qdf)}\right| \leq \frac{2x}{\varphi(q)} \\ \text{and} \quad \sum{}' \frac{9^{\nu(q)}}{\varphi(q)} &\leq \sum_{\substack{q<\frac{X^\alpha}{(\log X)^F},\\ q \text{ square free}}} \frac{9^{\nu(q)}}{\varphi(q)} \\ &\leq \prod_{p<\frac{X^\alpha}{(\log X)^F}} \left(1+\frac{1}{p-1}\right)^9 \\ &\leq \prod_{p<\frac{X^\alpha}{(\log X)^F}} \left(1-\frac{1}{p}\right)^{-9} \ll \log^9 x\,, \end{aligned}$$

where in the last step, we have used Merten's theorem. Hence

$$\sum{}' \; 9^{\nu(q)} \; |r_q| \; \ll \; x \log^9 x.$$

We now use Elliott and Halberstam conjecture to see that

$$\sum_{\substack{q|\mathcal{P}_1(z),\\ q\leq \frac{x^{1-\varepsilon}}{\log^B x}}} |r_q| \; \leq \sum_{q\leq \frac{(dfx)^{1-\varepsilon}}{\log^B(dfx)}} \max_{y\leq x} \max_{(a,q)=1} \left|\pi(y,q,a) - \frac{\mathrm{li}(y)}{\varphi(q)}\right| \ll \frac{x}{\log^3 x}$$

for any $\epsilon > 0$. Therefore by applying Theorem 10 and choosing $z = x^{1/2-\varepsilon}$ with $\varepsilon \leq 1/2$, we have

$$S(\mathcal{A}', \mathcal{P}_1, x^{1/2-\varepsilon}) \; \geq \; \frac{\mathrm{li}(x)}{\varphi(df)} V(x^{1/2-\varepsilon}) \left\{ g\left(\frac{(1-\varepsilon_1)\log X}{(\frac{1}{2}-\varepsilon)\log x}\right) \; - \; \frac{B}{\log^{14} X}\right\}.$$

Choose $\max(0, 4\varepsilon - 1) < \varepsilon_1 < 2\varepsilon$. Then we get

$$\frac{(1-\varepsilon_1)\log X}{(\frac{1}{2}-\varepsilon)\log x} \; = \; \frac{(2-2\varepsilon_1)(\log x - \log\log x + \log(1/\varphi(df)))}{(1-2\varepsilon)\log x} \; \leq \; \frac{2-2\varepsilon_1}{1-2\varepsilon} \; \leq \; 4.$$

Similarly, for $\varepsilon' > 0$ such that

$$\varepsilon' < \frac{2\varepsilon - \varepsilon_1}{1-\varepsilon_1},$$

and sufficiently large x, we get

$$\frac{(1-\varepsilon_1)\log X}{(\frac{1}{2}-\varepsilon)\log x} = \frac{(2-2\varepsilon_1)(\log x - \log\log x + \log(1/\varphi(df)))}{(1-2\varepsilon)\log x} \geq \frac{(2-2\varepsilon_1)(1-\varepsilon')}{1-2\varepsilon} > 2.$$

Thus there exists a constant $Z > 0$ such that for any real number $\eta < 1/2$ and x sufficiently large, we have

$$S(\mathcal{A}', \mathcal{P}_1, x^\eta) \; \geq \; \frac{Zx}{\log^2 x}. \tag{8}$$

Using arguments similar to the proof of Theorem 11, we now have

$$S(\mathcal{A}, \mathcal{P}, x^\eta) \gg \frac{x}{\log^2 x},$$

where

$$\mathcal{A} := \left\{ \frac{\ell - 1}{d} \ : \ \ell \in \mathbb{Q} \text{ is prime }, \ \ell \leq x \text{ and } \ell \equiv b \bmod f \right\},$$

and $\mathcal{P} = \{p \in \mathbb{Q} \ : \ p \text{ prime}\}$. □

4. Proof of Theorem 1 and Theorem 3

In this section, we give proofs of our theorems. We start by proving Theorem 1.

Proof. Let P_K be the set of prime ideals in $\mathcal{O}_K$ and $[\mathfrak{a}]$ be a generator of the class group Cl_K of K. Then for any real number $x > 0$, set

$$B_1(x) := \{\mathfrak{p} \in P_K \ : \ \mathfrak{N}(\mathfrak{p}) \leq x, \ [\mathfrak{p}] = [\mathfrak{a}], \ \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{p})^\times \text{ is surjective}\}. \tag{9}$$

In order to complete the proof of Theorem 1, by Lemma 6, it suffices to show that

$$|B_1(x)| \gg \frac{x}{\log^2 x}.$$

Applying Theorem 11 to

$$\mathcal{A} = \left\{ \frac{p - 1}{d} \ : \ p \leq x, \ p \in P_{\mathbb{Q}}, \ p \equiv b \bmod f \right\},$$

where $b \bmod f$ is a generator of the Galois group $G := \mathrm{Gal}(\mathbb{Q}(\zeta_f)/K)$, we get

$$S(\mathcal{A}, \mathcal{P}, x^\eta) = |\{ \ u \in \mathcal{A} \ : \ \ell | u, \ \ell \in P_{\mathbb{Q}} \implies \ell > x^\eta\}| \gg \frac{x}{\log^2 x}$$

for any positive real number $\eta < 16/63$. Set

$$\begin{aligned} \mathcal{B} &:= \{ \ u \in \mathcal{A} \ : \ \ell | u, \ \ell \in P_{\mathbb{Q}} \implies \ell > x^\eta\} \\ \text{and} \quad \mathcal{C} &:= \{p \in \mathbb{Q} \ : \ p \in P_{\mathbb{Q}}, \ \frac{p-1}{d} \in \mathcal{B}\}. \end{aligned}$$

Also let

$$\begin{aligned} f_{\mathfrak{p}} &:= |\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_K^\times\}|, \quad S_{\mathfrak{p}} := (\mathfrak{N}(\mathfrak{p}) - 1)/f_{\mathfrak{p}}, \\ J_1 &:= \{\mathfrak{p} \in P_K \ : \ \mathfrak{N}(\mathfrak{p}) \in \mathcal{C}, \ S_{\mathfrak{p}} = 1\} \quad \text{and} \quad J_2 := \{\mathfrak{p} \in P_K \ : \ \mathfrak{N}(\mathfrak{p}) \in \mathcal{C}, \ S_{\mathfrak{p}} > 1\}. \end{aligned}$$

Since every prime which is equivalent to $b \bmod f$ splits completely in K, it suffices to show that

$$|J_2| = o\left(\frac{x}{\log^2 x}\right).$$

Note that $\mathfrak{N}(\mathfrak{p}) \in \mathcal{C}$ implies that $(\mathfrak{N}(\mathfrak{p}), d) = 1$. Since $d = \prod_{i=1}^{d-1}(1-\zeta_d^i)$, where ζ_d is a primitive d-th root of unity, the elements ζ_d^i for $1 \leq i \leq d-1$ are distinct modulo $\mathfrak{p}$ and hence they are distinct in $(\mathcal{O}_K/\mathfrak{p})^\times$. Thus

$$S_{\mathfrak{p}} \Big| \frac{\mathfrak{N}(\mathfrak{p})-1}{d} \implies S_{\mathfrak{p}} = 1 \text{ or } S_{\mathfrak{p}} > x^\eta.$$

Now if $\mathfrak{p} \in J_2$, then $S_{\mathfrak{p}} > x^\eta$. Using the Gupta and Murty Lemma, we then have

$$|\{\mathfrak{p} \in P_K \ : \ f_{\mathfrak{p}} \leq x^{1-\eta}\}| \ll x^{(1-\eta)(1+\frac{1}{r})},$$

where r is the unit rank of K. If the unit rank r of K is greater than or equal to 3 and $\eta = 251/1000$, then

$$(1-\eta)(1+\frac{1}{r}) < 1 \implies |\{\mathfrak{p} \in P_K \ : \ f_{\mathfrak{p}} \leq x^{1-\eta}\}| = o\left(\frac{x}{\log^2 x}\right).$$

This implies that

$$|J_2| \ \leq \ |\{\mathfrak{p} \in P_K \ : \ f_{\mathfrak{p}} \leq x^{1-\eta}\}| = o\left(\frac{x}{\log^2 x}\right).$$

and hence

$$B_1(x) \gg \frac{x}{\log^2 x}.$$

This completes the proof of Theorem 1. □

4.1. **Proof of Theorem 3.** Suppose that the Elliott and Halberstam conjecture is true. Then by Theorem 12, we have

$$S(\mathcal{A}, \mathcal{P}, x^\eta) \ \gg \ \frac{x}{\log^2 x} \tag{10}$$

for any real $\eta < 1/2$. Let

$$\begin{aligned}
\mathcal{B} \ &:= \ \{ u \in \mathcal{A} \ : \ \ell | u, \ \ell \in P_{\mathbb{Q}} \implies \ell > x^\eta\}, \quad \mathcal{C} \ := \ \{p \in \mathbb{Q} \ : \ p \in P_{\mathbb{Q}}, \ \frac{p-1}{d} \in \mathcal{B}\} \\
f_{\mathfrak{p}} \ &:= \ |\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_K^\times\}|, \quad S_{\mathfrak{p}} \ := \ (\mathfrak{N}(\mathfrak{p})-1)/f_{\mathfrak{p}}, \\
J_1 \ &:= \ \{\mathfrak{p} \in P_K \ : \ \mathfrak{N}(\mathfrak{p}) \in \mathcal{C}, \ S_{\mathfrak{p}} = 1\} \quad \text{and} \quad J_2 \ := \ \{\mathfrak{p} \in P_K \ : \ \mathfrak{N}(\mathfrak{p}) \in \mathcal{C}, \ S_{\mathfrak{p}} > 1\}.
\end{aligned}$$

Then proceeding as in the proof of Theorem 1, we have

$$|\{\mathfrak{p} \in P_K \ : \ f_{\mathfrak{p}} \leq x^{1-\eta}\}| \ \ll \ x^{(1-\eta)(1+\frac{1}{r})},$$

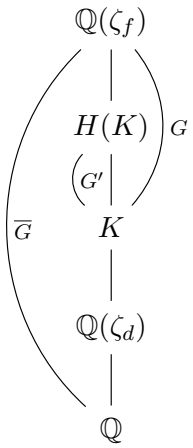
where r is the unit rank of K and $\eta := 1/2 - \varepsilon$. If the unit rank r of K is greater than or equal to 2 and $\eta = 5/14$, then

$$(1-\eta)(1+\frac{1}{r}) < 1 \implies |J_2| = o\left(\frac{x}{\log^2 x}\right) \implies B_1(x) \gg \frac{x}{\log^2 x},$$

where $B_1(x)$ is as defined in (9). This completes the proof of Theorem 3 when the unit rank of K is strictly greater than 1.

5. Concluding remarks

As in the previous sections, let K be a number field with the unit rank of K be greater than or equal to 3 and its Hilbert class field $H(K)$ be abelian over $\mathbb{Q}$. Consider the diagram



Let $\overline{G}$ be the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbb{Q}$. Then

$$\overline{G} := \{\sigma_a \ : \ 1 \leq a \leq n, \ (a, f) = 1\},$$

where $\sigma_a : \mathbb{Q}(\zeta_f) \to \mathbb{Q}(\zeta_f) \in \overline{G}$ is such that $\sigma_a(\zeta_f) = \zeta_f^a$. If G is the Galois group of $\mathbb{Q}(\zeta_f)$ over K, Cl_K is cyclic and

$$\left\{\sigma_a \in G \ : \ G' = \langle \sigma_a|_{H(K)} \rangle\right\} \cap \left\{\sigma_a \in \overline{G} \ : \ a \equiv 1 \bmod d, \ \left(\frac{a-1}{d}, \ \frac{f}{d}\right) = 1\right\} \neq \phi,$$

then it has a Euclidean ideal class. Here the notation $G' = \langle \sigma_a|_{H(K)} \rangle$ denotes that $\sigma_a|_{H(K)}$ generates G'. Now if we assume the Elliott and Halberstam conjecture, then one can improve the unit rank up to 2. These results are stronger than Theorem 1 and Theorem 3 as they also include number fields

$$K \subset \ \mathbb{Q}(\zeta_{2^k}), \ \text{for all } k \geq 1$$

whose ring of integers $\mathcal{O}_K$ is a PID. Here ζ_{2^k} is the 2^k-th primitive root of unity.

References

[1] Y. F. Bilu, J-M. Deshouillers, S. Gun and F. Luca, *Random orderings in modulus of consecutive Hecke eigenvalues of primitive forms*, submitted.

[2] E. Bombieri, J. B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. **156** (1986), no. 3-4, 203–251.

[3] D. A. Clark and M. R. Murty, *The Euclidean algorithm for Galois extensions of* $\mathbb{Q}$, J. Reine Angew. Math. **459** (1995), 151–162.

[4] P. D. T. A. Elliott and H. Halberstam, *A conjecture in prime number theory*, Symposia Mathematica Vol. IV (INDAM, Rome, 1968/69) 59–72, Academic Press, London, 1970.

[5] É. Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat*, Invent. Math. **79** (1985), 383–407.
[6] J. B. Friedlander and H. Iwaniec, *Opera de Cribro*, Colloquium Publications - American Mathematical Society, (2010).
[7] H. Graves, *Growth results and Euclidean ideals*, J. Number Theory **133** (2013), no. 8, 2756–2769.
[8] H. Graves and M. R. Murty, *A family of number fields with unit rank at least 4 that has Euclidean ideals*, Proc. Amer. Math. Soc. **141** (2013), 2979–2990.
[9] R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), no. 1, 127–130.
[10] R. Gupta, M. R. Murty and V. K. Murty, *The Euclidean algorithm for S-integers*, Number Theory (Montreal 1985), CMS Conf. Proc. 7, American Mathematical Society, Providence (1987), 189–201.
[11] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press (London, 1974).
[12] M. Harper, $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*, Canad. J. Math. **56** (2004), no. 1, 55–70.
[13] M. Harper and M.R. Murty, *Euclidean rings of algebraic integers*, Canad. J. Math. **56** (2004), no. 1, 71–76.
[14] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38.
[15] H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith. **37** (1980), 307–320.
[16] H. W. Lenstra, Jr., *Euclid's algorithm in cyclotomic fields*, J. London Math. Soc. (2) **10** (1975), 457–465.
[17] H.W. Lenstra, Jr., *Euclidean ideal classes*, Astérisque **61** (1979), 121–131.
[18] T. Motzkin, *The Euclidean algorithm.*, Bull. Amer. Math. Soc. **55** (1949), 1142–1146.
[19] M. R. Murty and K. L. Petersen, *The Euclidean algorithm for number fields and primitive roots*, Proc. Amer. Math. Soc. **141** (2013),181–190.
[20] J. Sivaraman, *Euclidean ideal classes in number fields of finite rank*, preprint.
[21] P. J. Weinberger, *On Euclidean rings of algebraic integers*, Proc. Symposia Pure Math. **24** (1972), 321–332.

(J.-M. Deshouillers) INSTITUT DE MATHÉMATIQUES DE BORDEAUX UMR 5251 UNIVERSITÉ DE BORDEAUX 351, COURS DE LA LIBÉRATION - F 33 405 TALENCE, FRANCE.

(S. Gun and J. Sivaraman) INSTITUTE OF MATHEMATICAL SCIENCES, HBNI, C.I.T CAMPUS, TARAMANI, CHENNAI 600 113, INDIA.

Email address: jean-marc.deshouillers@math.u-bordeaux.fr
Email address: sanoli@imsc.res.in
Email address: jyothsnaa@imsc.res.in