EXISTENCE OF EUCLIDEAN IDEAL CLASSES BEYOND CERTAIN RANK

ABSTRACT. In his seminal paper on Euclidean ideal classes, Lenstra showed that under generalised Riemann hypothesis, a number field K has a Euclidean ideal class if and only if the class group is cyclic. In [3], the authors show that under certain conditions on the Hilbert class field of the number field K, for unit rank greater than or equal to 3, K has a Euclidean ideal class if and only if the class group is cyclic. The main objective of this article is to give a short alternate proof of the fact that, under similar conditions, there exists an integer $r \geq 1$ such that all fields with unit rank greater than or equal to r have a Euclidean ideal class if and only if the class group is cyclic. The main novelty of this proof is that we use Brun's sieve as opposed to the linear sieve as seen traditionally in the context of this problem.

1. INTRODUCTION

Throughout this paper K will denote a number field and $\mathcal{O}_K$, its ring of integers. Given K, $\mathcal{O}_K$ is said to be a Euclidean domain if there exists a map $\phi : \mathcal{O}_K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ such that for any $a, b \neq 0$ in $\mathcal{O}_K$, there exist q, r in $\mathcal{O}_K$ such that

$$a = bq + r$$

with $r = 0$ or $\phi(r) < \phi(b)$. In 1973, Weinberger [12] proved that under generalised Riemann hypothesis, if $\mathcal{O}_K$ has infinitely many units, $\mathcal{O}_K$ is a principal ideal domain if and only if it is a Euclidean domain. This marked the beginning of a lot of activity, the main objective of which was to make this result unconditional. Some of the most notable results along these lines were [2], [5] ,[8], [9] , [10] and [11]. In the mean time, Lenstra [7] generalised the definition of Euclidean domains to domains with Euclidean ideal classes in order to capture cyclic class groups as opposed to principal ideal domains. Before going any further, we define Euclidean ideal classes.

Definition 1. *Let E be the set of all fractional ideals of K containing $\mathcal{O}_K$. Suppose that $[\mathfrak{I}]$ is an ideal class and $\mathfrak{a} \in [\mathfrak{I}]$. If there exists a map $\psi : E \to \mathbb{N} \cup \{0\}$ such that for all ideals $\mathfrak{b} \in E$ and for all $x \in \mathfrak{ab} \setminus \mathfrak{a}$, there exists $z \in x + \mathfrak{a}$ such that*

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

then we say that $\mathfrak{a}$ is a Euclidean ideal and that $[\mathfrak{I}]$ is a Euclidean ideal class.

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

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

Lenstra proved that under generalised Riemann hypothesis K has a Euclidean ideal class if and only if the class group is cyclic. In 2013 Graves and Murty [4] were able to make this unconditional for a family of number fields with abelian Hilbert class field and unit rank (rank of the free part of $\mathcal{O}_K^*$ as a finitely generated $\mathbb{Z}$ module) greater than or equal to 4 using the linear sieve. In [3], the authors, Deshouillers, Gun and Sivaraman, prove the same for a finer family of fields with abelian Hilbert class fields and unit rank greater than or equal to three, again by an application of the linear sieve but this time with the use of well factorable weights due to which they can achieve rank 3. In this article we give a short proof of the fact that there exists a finite natural number r such that a family of number fields with unit rank greater than or equal to r have a Euclidean ideal class using Brun's sieve. More precisely, we prove the following.

Theorem 1. *Let K be a number field and $H(K)$ its Hilbert class field. Suppose that the Hilbert class field is abelian over $\mathbb{Q}$. Let f be the smallest even positive integer such that $\mathbb{Q}(\zeta_f)$ contains $H(K)$. Further, suppose that the Galois group of $\mathbb{Q}(\zeta_f)$ over K is cyclic, then there exists a finite natural number r such that if K has unit rank greater than or equal to r, it has a Euclidean ideal class.*

Once we prove this theorem, we can deduce the following corollary.

Corollary 2. *Let K be an abelian number field with class number 1. Let f be the smallest even positive integer such that $\mathbb{Q}(\zeta_f)$ contains $H(K)$. If $\mathbb{Q}(\zeta_f)$ over K is cyclic, then there exists a finite natural number r such that if unit rank of K is greater than or equal to r, $\mathcal{O}_K$ is a Euclidean domain.*

Note that the above corollary was proved by Harper and Murty [8] using the linear sieve. In the next section we state some preliminaries and finally in the last section, we provide the proof of Theorem 1.

2. Preliminaries

The main theorem we will be using is Brun's sieve as stated in [1]. We begin with a few definitions. Let Σ be a finite set of rational primes. Let

$$P_\Sigma(z) := \prod_{\substack{p<z \\ p\notin\Sigma}} p.$$

When $\Sigma = \phi$, the empty set, we denote the product by $P(z)$. Consider the linear forms $L_i(n) = a_i n + b_i$ where a_i and b_i belong to $\mathbb{N}$ and $1 \leq i \leq k$. Let

$$\Omega^{(*)}(x,z) := \{n \leq x : \gcd(L_1(n)\cdots L_{k-1}(n), P_\Sigma(z)) = 1, L_k(n) \text{ prime }\}.$$

Further we assume that all the prime divisors of

$$(2k)!\prod_{i=1}^{k} a_i \prod_{1\leq i<j\leq k}(a_i b_j - a_j b_i) \tag{1}$$

belong to Σ.

Theorem 3 (Bilu, Deshouillers, Gun and Luca [1]). *Under the above notation and assumption* (1) *, we have for* $2 \leq z \leq x$

$$|\Omega^{(*)}(x,z)| = \frac{\mathrm{li}(|a_k|x)}{\varphi(|a_k|)} W_{k-1}^{(*)}(z)(1+O(E^{(*)}(x,z)))$$

where φ *denotes the Euler totient function,*

$$E^{(*)}(x,z) \quad = \quad exp(-(u/3)(\log u - \log\log u - \log(k-1) - 3)) + \frac{1}{\log z},$$

$$u = \frac{\log x}{\log z} \quad \text{and} \quad W_\ell^{(*)}(z) = \prod_{p|P_\Sigma(z)} \left(1 - \frac{\ell}{p-1}\right).$$

The above sieve will enable us to show that a certain set is "large". This will be followed by an application of the following lemma of Graves in order to show the existence of a Euclidean ideal class.

Lemma 4 (Graves [6]). *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 proof is the following result of Gupta and Murty as given in the paper of Harper and Murty [8].

Lemma 5 (Harper and Murty [8]). *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*

$$f_\mathfrak{p} = |\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_K^\times\}|,$$

then

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

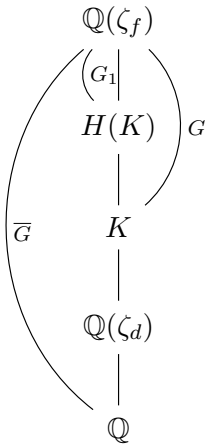
3. Proof of the main theorem

We begin with the following proposition.

Proposition 6. *Let* K *be a number field. Suppose that the Hilbert class field* $H(K)$ *of* K *is abelian over* $\mathbb{Q}$ *and let* f *be the smallest even integer such that* $H(K)$ *is contained in* $\mathbb{Q}(\zeta_f)$*. Now suppose that* $\mathbb{Q}(\zeta_f)$ *over* K *is cyclic and generated by* $\zeta_f \to \zeta_f^b$*. Further, let* $d = max(n : \mathbb{Q}(\zeta_n) \subseteq K)$*. Then, there exists* $\eta > 0$ *such that*

$$\left|\mathcal{A}(\eta)(x) := \left\{\frac{\ell-1}{d} \ : \ \ell \in P_\mathbb{Q}, \ \ell \leq x \ , \ell \equiv b \bmod f \text{ and } \left(\frac{\ell-1}{d}, P(x^\eta)\right) = 1\right\}\right| \gg \frac{x}{\log^2 x}.$$

Proof. Let $\Sigma_1 = \{p \in \mathbb{Q} \ : \ p \text{ prime and } p \mid 3f\}$. 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 that our claim is not true i.e., we have $((b-1)/d, f/d) = h \neq 1$, where G is generated by σ_b. 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 $m = (b-1)/d$.

Let $n_0 \in \mathbb{N}$ be such that $m + n_0 f/d$ is a prime co-prime to $3f$ and let

$$\mathcal{A}'(x, z) := \{y \leq x : 1 + dm + n_0 f + 3ydf \text{ is prime and } (m + n_0(f/d) + 3yf, P_{\Sigma_1}(z)) = 1\}.$$

Then by Theorem 3

$$|\mathcal{A}'(x, z)| = \frac{\mathrm{li}(dfx)}{\phi(df)} \prod_{p | P_{\Sigma_1}(z)} (1 - \frac{1}{p-1})(1 + O(E^{(*)}(x, z))) \tag{2}$$

where

$$E^{(*)}(x,z) = exp(-(u/3)(\log u - \log\log u - 3)) + \frac{1}{\log z}$$

$\Sigma_1 = \{p \in P_{\mathbb{Q}} \ : \ p \mid 3f\}$ and $u = \frac{\log x}{\log z}$. Since the O constant is absolute, if we put $u = 1/\eta$ for small η and large x we get,

$$\begin{aligned}
|\mathcal{A}'(x,x^\eta)| &\gg \frac{x}{\log x}\prod_{\substack{p<x^\eta \\ p\notin\Sigma_1}}(1-\frac{1}{p-1}) \\
&\gg \frac{x}{(\log x)(\exp(\sum_{\substack{p<x^\eta, \\ p\neq 2}}(\frac{1}{p-1}+\frac{1}{2(p-1)^2}\cdots)))} \\
&\gg \frac{x}{(\log x)(\exp(\sum_{\substack{p<x^\eta \\ p\neq 2}}(\frac{1/(p-1)}{1-1/(p-1)})))} \\
&\gg \frac{x}{(\log x)(\exp(\sum_{\substack{p<x^\eta, \\ p\neq 2}}(\frac{1}{p}+\frac{2}{p(p-2)})))} \\
&\gg \frac{x}{\log^2 x}.
\end{aligned}$$

Since for any $l = 1 + dm + n_0 f + 3ydf$ for $y \in \mathcal{A}'(x,x^\eta)$, $\frac{l-1}{d}$ is coprime to $3f$, there exists $\eta > 0$ such that

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

□

Proof of Theorem 1. 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

$$B_1(x) := \{\mathfrak{p} \in P_K \ : \ \mathfrak{N}(\mathfrak{p}) \le x, \ [\mathfrak{p}] = [\mathfrak{a}], \ \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{p})^\times \text{ is surjective}\}. \tag{3}$$

In order to complete the proof of Theorem 1, by Lemma 4, it suffices to show that

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

Let $\zeta_f \to \zeta_f^b$ be a generator of $\mathbb{Q}(\zeta_f)$ over K. By Theorem 2, we have

$$\left|\mathcal{A}(\gamma)(x) = \left\{\frac{\ell-1}{d} \ : \ \ell \in \mathbb{Q} \text{ is prime }, \ \ell \le x \ , \ell \equiv b \bmod f \text{ and } \left(\frac{\ell-1}{d}, P(x^\gamma)\right) = 1\right\}\right| \gg \frac{x}{\log^2 x}$$

for all real $\gamma < \eta$. Let

$$\begin{aligned}
\mathcal{B}(\gamma)(x) &:= \left\{l : \frac{l-1}{d} \in \mathcal{A}(\gamma)(x)\right\}, \\
f_{\mathfrak{p}} &:= |\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_K^\times\}|, \quad S_{\mathfrak{p}} := (\mathfrak{N}(\mathfrak{p})-1)/f_{\mathfrak{p}}, \\
J_1(x) &:= \{\mathfrak{p} \in P_K \ : \ \mathfrak{N}(\mathfrak{p}) \in \mathcal{B}(\gamma)(x), \ S_{\mathfrak{p}} = 1\} \quad \text{and} \\
J_2(x) &:= \{\mathfrak{p} \in P_K \ : \ \mathfrak{N}(\mathfrak{p}) \in \mathcal{B}(\gamma)(x), \ S_{\mathfrak{p}} > 1\}.
\end{aligned}$$

Consider the following diagram.

$$\begin{array}{c} \mathbb{Q}(\zeta_f) \\ | \\ H(K) \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$$

Let $p \in \mathcal{A}$ and let $\mathfrak{P}$ be a prime above it in $\mathbb{Q}(\zeta_f)$. Suppose that $\mathfrak{p} = \mathfrak{P} \cap K$. From the properties of the frobenius, we observe that

$$\left[\frac{\mathbb{Q}(\zeta_f)/\mathbb{Q}}{p}\right] = \left[\frac{\mathbb{Q}(\zeta_f)/K}{\mathfrak{p}}\right]$$

and that

$$\left[\frac{\mathbb{Q}(\zeta_f)/K}{\mathfrak{p}}\right]\Bigg|_{H(K)} = \left[\frac{H(K)/K}{\mathfrak{p}}\right]$$

This allows us to conclude that $J_1(x) \subseteq B_1(x)$. So, it suffices to show that

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

Note that $\mathfrak{N}(\mathfrak{p}) \in \mathcal{B}(\gamma)(x)$ 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

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

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

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

where r is the unit rank of K. Now we choose $\gamma = 1/r$, then

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

This implies that

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

and hence

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

whenever $r > 1/\eta$. This completes the proof of Theorem 1. □

Acknowledgements: I would like to thank Sanoli Gun for all the encouragement and useful discussions.

REFERENCES

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

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

[3] J-M. Deshouillers, S. Gun and J. Sivaraman, *On Euclidean Ideal classes in certain Abelian extensions*, submitted.

[4] 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.

[5] 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.

[6] H. Graves, *Growth results and Euclidean ideals*, J. Number Theory **133** (2013), no. 8, 2756–2769.

[7] H.W. Lenstra, Jr., *Euclidean ideal classes*, Astérisque **61** (1979), 121–131.

[8] M. Harper and M.R. Murty, *Euclidean rings of algebraic integers*, Canad. J. Math. **56** (2004), no. 1, 71–76.

[9] M. Harper, $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*, Canad. J. Math. **56** (2004), no. 1, 55–70.

[10] M. R. Murty and K. L. Petersen, *The Euclidean algorithm for number fields and primitive roots*, Proc. Amer. Math. Soc. **141** (2013),181–190.

[11] W. Narkiewicz, *Euclidean algorithm in small abelian fields*, Funct. Approx. Comment. Math. **37** (2007), no 2, 337–340.

[12] P. J. Weinberger, *On Euclidean rings of algebraic integers*, Proc. Symposia Pure Math. **24** (1972), 321–332.

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

E-mail address: jyothsnaa@imsc.res.in