Canad. J. Math. Vol. **56** (1), 2004 pp. 71–76

Euclidean Rings of Algebraic Integers

Malcolm Harper and M. Ram Murty

Abstract. Let K be a finite Galois extension of the field of rational numbers with unit rank greater than 3. We prove that the ring of integers of K is a Euclidean domain if and only if it is a principal ideal domain. This was previously known under the assumption of the generalized Riemann hypothesis for Dedekind zeta functions. We now prove this unconditionally.

1 Introduction

An integral domain R is said to be Euclidean if there exists a map $\phi\colon R \setminus \{0\} \to \mathbb{N}$ such that given any $a, b \in R$, there exist q and r such that $a = bq + r$ with either $r = 0$ or $\phi(r) < \phi(b)$. Any such ring is a principal ideal domain (PID).

If R is the ring of integers of an algebraic number field, then clearly a necessary condition for R to be Euclidean is that R be a PID. That this condition is also sufficient whenever the quotient field of R is not an imaginary quadratic field is a remarkable prediction of the generalized Riemann hypothesis (GRH) and is a beautiful theorem of Weinberger [W]. Such a result, together with its connection to a number field version of the Artin primitive root conjecture was first signaled in a paper of Samuel [S]. In that paper, Samuel discusses the situation with quadratic extensions of $\mathbb{Q}$. After reviewing a general criterion of Motzkin [M] for a ring to be Euclidean, he applies it to the context of quadratic fields.

This criterion is easily described. Let $A_0 = \{0\}$ and define inductively A_n to be the set of elements r of R having the property that every residue class modulo r has a representative in A_j for some $j < n$. Thus, A_1 consists of the unit group of R. Motzkin's criterion is that R is Euclidean if and only if $R = \bigcup_{n=0}^{\infty} A_n$.

Motzkin used his criterion to prove that of the nine imaginary quadratic fields of class number one, only five of them are Euclidean and for these fields, the norm map serves as the function ϕ. In contrast, Samuel's work [S] made the exciting prediction that any ring of integers of a real quadratic field of class number one is Euclidean, but not necessarily for the absolute value of the norm map serving as ϕ. In particular, Samuel conjectured that $\mathbb{Z}[\sqrt{14}]$ is Euclidean this being the quadratic field of smallest discriminant whose nature was unresolved.

We refer the reader to Lenstra's paper [L] for both the historical developments and applications of these ideas in the more general context of function fields over finite fields where the GRH is known and the analog of Weinberger's theorem can be proved unconditionally.

In an earlier paper [H], the first author proved that $\mathbb{Z}[\sqrt{14}]$ is Euclidean without the use of the generalized Riemann hypothesis. More generally, he proved that if K is

Received by the editors April 19, 2002; revised August 15, 2002.
The second author's research was partially supported by an NSERC grant.
AMS subject classification: 11R04, 11R27, 11R32, 11R42, 11N36.

a real quadratic field and O_K its ring of integers whose discriminant is less than 500, then O_K is Euclidean if and only if O_K has class number one. In the same paper, he also determined all the cyclotomic fields whose ring of integers is a Euclidean domain.

In this paper, we generalize the work of Harper [H] to a larger context that includes the abelian case. Our methods originate in the papers of Gupta, K. Murty and R. Murty [GMM] where the first attempt was made to make Weinberger's results unconditional using the earlier work [GM] on Artin's primitive root conjecture. Their work studied the ring $O_{K,S}$ of S-integers where S was a finite set of places that included the infinite places and required $|S| \geq \max(5, 2[K:\mathbb{Q}]-3)$ to be applicable in the Euclidean context. A novel idea was injected into the method by Clark and Murty [CM] in 1995. This idea allowed one to discover new Euclidean rings of integers of totally real Galois extensions K over $\mathbb{Q}$ with $[K:\mathbb{Q}] \geq 4$. Thus, at that time, the case of $\mathbb{Z}[\sqrt{14}]$ was still elusive.

In [H], a variant of the Motzkin criterion was discovered, which when combined with the lower bound sieve results of previous works on the problem, along with a clever use of the large sieve inequality, finally led to the applicability of the method to the quadratic field context.

The goal of this paper is to prove:

Theorem 1 *Let $K/\mathbb{Q}$ be a finite Galois extension with unit rank $r > 3$. Then O_K is Euclidean if and only if O_K is a* PID.

As a corollary, we deduce:

Corollary *Let $K/\mathbb{Q}$ be a finite Galois extension of degree > 8. Then O_K is Euclidean if and only if O_K is a* PID.

Indeed, if r_1 and r_2 denotes the number of real and complex embeddings of K respectively, we have $r > (r_1 + 2r_2 - 2)/2 = (n-2)/2$ so that $r > 3$ whenever $n > 8$ and $r_1 > 0$. If $r_1 = 0$, then $r = r_2 - 1 > 3$ whenever $n > 8$.

The proof of this theorem involves many important ideas. In addition to the Motzkin criterion described above, the generalization of the Bombieri-Vinogradov theorem to algebraic number fields as developed by K. Murty and R. Murty [MM] plays a vital role. Their generalization has two versions, one which is unconditional and another which assumes the Artin holomorphy conjecture for the Artin L-functions that intervene. Undoubtedly, we feel that there is great scope for further improvements. In particular, it should be possible to sharpen the theorem to allow $r = 3$. This is possible in the abelian case thanks to a theorem of Bombieri, Friedlander and Iwaniec [BFI] extending the range of applicability of the Bombieri-Vinogradov theorem beyond the usual limit of $x^{1/2}$ in the lower bound sieve method. Such a result is not available in the non-abelian context and so our result stands with the strict inequality at present. Still, by injecting ideas utilised in Theorem 2 (below), especially the notion of admissible primes, one can hope to make further improvements. This we hope to develop in future research.

As is well-known, the Euclidean algorithm plays an important role in the study of bounded generation of arithmetic groups. We state that one can apply our theorem to this study, and refer the reader to the exposition of K. Murty [KM].

https://doi.org/10.4153/CJM-2004-004-5 Published online by Cambridge University Press

2 Variation of Motzkin's Criterion

In [H], Harper discovered a variation of Motzkin's criterion applicable to rings of integers of algebraic number fields. This can be described as follows.

First we define the notion of admissible sets of primes as described by Clark and Murty [CM]. Let K be an algebraic number field, O_K its ring of integers. We suppose that O_K is a PID. Let $\pi_1, \dots, \pi_s \in \mathrm{O}_K$ be distinct non-associate primes. We say $\{\pi_1, \dots, \pi_s\}$ is an admissible set of primes if for all $\beta = \pi_1^{a_1} \cdots \pi_s^{a_s}$ with a_i non-negative integers, every coprime residue class (mod β) can be represented by a unit of O_K. As noted in [CM], to check if $\{\pi_1, \dots, \pi_s\}$ is admissible, it suffices to check that every coprime residue class (mod $\pi_1^2 \cdots \pi_s^2$) can be represented by a unit of O_K.

Now let B_0 be the monoid generated by the unit group and an admissible set of primes (which could be empty). For $n \geq 1$, inductively define B_n as the set of all primes π of O_K such that every non-zero residue class modulo (π) has a representative in $B_{n-1} \cup B_0$. Thus, B_1 is the set of primes π such that every residue class mod π is represented by an element of B_0. The fundamental result in [H] is:

Proposition 1 *Suppose* O_K *is a* PID. *If all the primes of* O_K *lie in* $\bigcup_{n=0}^{\infty} B_n$, *then* O_K *is Euclidean.*

A key innovation in the argument of Harper [H] was the following application of the large sieve inequality.

Proposition 2 *Suppose that* O_K *is a* PID. *Let* $B_n(x)$ *denote the cardinality of the set of elements in* B_n *whose norm is less than or equal to* x. *If*

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

then O_K *is Euclidean.*

It is this last proposition that simplfies the earlier approaches to the study of Euclidean rings of algebraic integers. Indeed, in the proofs below we apply the lower bound sieve to establish Proposition 2.

3 Preliminaries

We record in this section various theorems from the literature which will be needed in the proofs.

Proposition 3 **([MM])** *Let* $K/\mathbb{Q}$ *be a finite Galois extension with group* G. *Let* C *be a conjugacy class of* G, *and* a, q *be positive integers with* $1 \leq a < q$, $(a, q) = 1$. *Denote by* $\pi_C(x, q, a)$ *the number of primes* $p \leq x$ *such that* $p \equiv a \pmod{q}$ *with Artin symbol* $(p, K/\mathbb{Q}) \in C$. *There exist numbers* $\delta(C, q, a) \geq 0$ *such that for any* $\epsilon > 0$ *and* $A > 0$, *we have*

$$\sum_{q \leq Q} \max_{(a,q)=1} \max_{y \leq x} |\pi_C(y, q, a) - \delta(C, q, a)\pi(y)| \ll \frac{x}{(\log x)^A},$$

with $Q = x^{\alpha - \epsilon}$ *where* $\alpha \leq \min(2/|G|, 1/2)$ *and the summation is over* q *such that* $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$. *(Here,* $\pi(y)$ *denotes the number of primes* $p \leq y$.*)*

https://doi.org/10.4153/CJM-2004-004-5 Published online by Cambridge University Press

This is the basic result of [MM]. However, as remarked in Section 7 of that paper, some improvements can be made (see, in particular Theorem 7.3 and Section 7.4).

Proposition 4 **([MM, p. 269])** *With the same setting as in Proposition 3, let A be any abelian subgroup of G with $A \cap C \neq \phi$. Let $d = [G : A]$. Then, we may take $Q = x^{1/\eta - \epsilon}$ in Proposition 3 with*

$$\eta = \begin{cases} d-2 & \text{if } d \geq 4 \\ 2 & \text{if } d \leq 4. \end{cases}$$

Moreover, we may replace d above by d^* where

$$d^* = \min_H \max_\omega [G : H]\omega(1)$$

where the minimum is taken over all subgroups H satisfying the two conditions

- *$H \cap C \neq \phi$ and*
- *for every irreducible character ω of H and any non-trivial Dirichlet character χ, the Artin L-series $L(s, \omega \otimes \chi)$ is entire.*

The maximum above is over all irreducible characters of H. In particular, if Artin's holomorphy conjecture is true for $K/\mathbb{Q}$, then we may take $d^* = \max_\chi \chi(1)$ where the maximum is over all irreducible characters of G.

Proposition 5 **(Application of the Lower Bound Sieve)** *Let $K/\mathbb{Q}$ be a finite Galois extension and set*

$$t = \max_m \{m : K \supseteq \mathbb{Q}(\zeta_m)\}.$$

Let η be as in Proposition 4 with $C = 1$. Then, the number of primes $p \leq x$ such that p splits completely in K and such that for every prime ℓ with $\ell | (p-1)/t$ we have $\ell > x^{1/2\eta - \epsilon}$, is

$$\gg \frac{x}{\log^2 x}.$$

Proposition 6 **(Gupta-Murty [GM])** *Let K be an algebraic number field. Let M be a monoid in O_K and for $\mathfrak{p}$ coprime to the elements of M, denote by $f_M(\mathfrak{p})$ the order of M mod $\mathfrak{p}$. If M contains r multiplicatively independent elements, then*

$$\#\{\mathfrak{p} : f_M(\mathfrak{p}) \leq Y\} \ll Y^{(r+1)/r}.$$

4 The Abelian Case

We begin with Lemma 4 of [H].

Proposition 7 *Suppose O_K is a* PID *and contains a set of s admissible primes. Let r be the rank of $\mathrm{O}_K^\times$ modulo torsion and define $t = \max\{d' : \zeta_{d'} \in K\}$. If $r + s \geq 3$ and if there are a and $k \in \mathbb{Z}$ satisfying*

(1) $\gcd(a, k) = 1$;
(2) $\gcd(a - 1, k) = t$; *and*
(3) $p \equiv a \pmod{k}$ *implies there is a prime $\mathfrak{p}$ of K with norm p,*

then O_K is Euclidean.

https://doi.org/10.4153/CJM-2004-004-5 Published online by Cambridge University Press

We will use this proposition to establish the following:

Theorem 2 *Let $K/\mathbb{Q}$ be abelian of degree n with O_K a* PID *that contains s admissible primes. Let r be the rank of the unit group. If $r + s \geq 3$, then O_K is Euclidean.*

Proof Let t be as in Proposition 7. We count the number of primes $p \leq x$ such that p splits completely in K and p does not split completely in $\mathbb{Q}(\zeta_{\ell t})$ for $\ell | t$. Let k be the conductor of K. Since $K/\mathbb{Q}$ is abelian, this means that there is a set S of residue classes mod k such that p splits completely in K if and only if $p \equiv a (\mathrm{mod}\, k)$ with $a \in S$. Since $\mathbb{Q}(\zeta_t)$ is contained in K, we have $a \equiv 1 (\mathrm{mod}\, t)$. We want to show that there is an a in S satisfying the conditions of Proposition 7, namely $\gcd(a-1, k) = t$. To do this, it suffices to show that there is a positive density of primes p which split competely in K but not in $\mathbb{Q}(\zeta_{\ell t})$ for $\ell | t$ for these primes will satisfy $\gcd(p-1, k) = t$. If we let $K_{\ell t} = K\mathbb{Q}(\zeta_{\ell t})$, then the number of primes in our count is

$$\sum_{\delta | t} \mu(\delta) \pi(K_{t\delta}, x)$$

where $\pi(L, x)$ is the number of primes $p \leq x$ splitting completely in L. Since the degree of $K_{t\delta}$ over $\mathbb{Q}$ is $n\delta$ as is easily checked, we have by the Chebotarev density theorem, that the quantity in question is

$$\sim \sum_{\delta | t} \mu(\delta) \frac{\pi(x)}{n\delta} = \frac{\pi(x)}{n} \frac{\phi(t)}{t},$$

which is a positive proportion. This completes the proof.

5 Proof of the Main Theorem

We want to use Proposition 2 to show that O_K is Euclidean. Let $B_1(x)$ count the number of primes π with norm less than x for which we have $O_K^\times (\mathrm{mod}\, \pi) = (O_K/\pi)^\times$. It suffices to show that

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

By Proposition 5, the number of primes π which split completely in K with $p = N_{K/\mathbb{Q}}(\pi) \leq x$ having the property that any prime ℓ dividing $p - 1$ is either greater than $x^{1/2\eta - \epsilon}$ or a divisor of t, (where t, η are defined in Proposition 5) is

$$\gg \frac{x}{\log^2 x}.$$

For p sufficiently large, we already know that t divides the order of the image of $O_K^\times$ mod π since the group of roots of unity injects into $(O_K/\pi)^\times$. By virtue of the constraint on p guaranteed by Proposition 5, no prime dividing t can divide the index of the image. Thus, the only possible prime divisors of the index are greater

https://doi.org/10.4153/CJM-2004-004-5 Published online by Cambridge University Press

than $x^{1/2\eta-\epsilon}$ which means that if the index is not 1, then the size of the image is less than $x^{1-1/2\eta+\epsilon}$. By Proposition 6, the number of such primes is

$$O(x^{(1-1/2\eta+\epsilon)(1+1/r)}) = o(x/\log^2 x)$$

whenever $\eta < (r+1)/2$. We apply Proposition 5. We determine η of Proposition 4 as follows. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and let A be an abelian subgroup of G. Set $d = [G : A]$. If $d \leq 4$, we can take $\eta = 2$ so we need $r > 3$. If $d \geq 4$, we can take $\eta = d - 2$, and we need $d - 2 < (r+1)/2$ which means we need to ensure $r > 2d - 5$. This is the case if G has an abelian subgroup of order $e \geq 4$, since

$$r = r_1 + r_2 - 1 \geq \frac{r_1 + 2r_2 - 2}{2} = \frac{n-2}{2} > \frac{2n}{e} - 5 = 2d - 5.$$

Thus, we may assume every prime divisor of $|G| = n$ is ≤ 3. Hence, $n = 2^a 3^b$. If $b \geq 2$, G has a subgroup of order 9 and again by the above argument we are done. If $a \geq 2$, we are also done. The only case left is if n divides 6. As the abelian case was dealt with in the previous section, the only case to treat is the non-abelian case of $n = 6$. But in this case, we have Artin's conjecture on the holomorphy of non-abelian L-series, so that we may take $\eta = 2$ in Proposition 4. Thus, $r > 3$ is allowed and the proof is complete.

Acknowledgments The authors would like to thank the referee for helpful comments and suggestions.

References

[BFI] E. Bombieri, J. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli.* Acta Math. **156**(1986), 203–251.
[CM] D. Clark and M. Ram Murty, *The Euclidean algorithm for Galois extensions of* $\mathbb{Q}$. J. Reine Angew. Math. **459**(1995), 151–162.
[GM] R. Gupta and M. Ram Murty, *A remark on Artin's conjecture.* Invent. Math. **78**(1984), 127–130.
[GMM] R. Gupta, M. Ram Murty and V. Kumar Murty, *The Euclidean algorithm for S-integers.* In: Number Theory (eds. H. Kisilevsky and J. Labute), CMS Conf. Proc. **7**(1987), 189–201.
[H] M. Harper, $\mathbb{Z}[\sqrt{14}]$ *is Euclidean.* Canad. J. Math. **56**(2004), 55–70.
[L] H. Lenstra, *Euclidean number fields, I.* Math. Intelligencer **2**(1979), 6–15.
[M] Th. Motzkin, *The Euclidean algorithm.* Bull. Amer. Math. Soc. **55**(1949), 1142–1146.
[KM] V. Kumar Murty, *Bounded and Finite Generation of Arithmetic Groups.* In: Number Theory (ed. K. Dilcher), CMS Conf. Proc. **15**(1995), 249–261.
[MM] M. Ram Murty and V. Kumar Murty, *A variant of the Bombieri-Vinogradov theorem.* In: Number Theory (eds. H. Kisilevsky and J. Labute), CMS Conf. Proc. **7**(1987), 243–272.
[S] P. Samuel, *About Euclidean Rings.* J. Algebra **19**(1971), 282–301.
[W] P. Weinberger, *On Euclidean rings of algebraic integers.* In: Analytic Number Theory (St. Louis, 1972), Proc. Sympos. Pure Math. **24**(1973), 321–332.

Champlain College
Montreal
Canada
email: malcolmharper@sympatico.ca

Department of Mathematics
Queen's University
Kingston, Ontario
K7L 3N6
email: murty@mast.queensu.ca