Canad. J. Math. Vol. **56** (1), 2004 pp. 55–70

$\mathbb{Z}[\sqrt{14}]$ is Euclidean

Malcolm Harper

Abstract. We provide the first unconditional proof that the ring $\mathbb{Z}[\sqrt{14}]$ is a Euclidean domain. The proof is generalized to other real quadratic fields and to cyclotomic extensions of $\mathbb{Q}$. It is proved that if K is a real quadratic field (modulo the existence of two special primes of K) or if K is a cyclotomic extension of $\mathbb{Q}$ then:

the ring of integers of K is a Euclidean domain if and only if it is a principal ideal domain.

The proof is a modification of the proof of a theorem of Clark and Murty giving a similar result when K is a totally real extension of degree at least three. The main changes are a new Motzkin-type lemma and the addition of the large sieve to the argument. These changes allow application of a powerful theorem due to Bombieri, Friedlander and Iwaniec in order to obtain the result in the real quadratic case. The modification also allows the completion of the classification of cyclotomic extensions in terms of the Euclidean property.

1 Introduction

Let K be an algebraic number field—a finite extension of $\mathbb{Q}$. $\mathcal{O}_K$ will denote the ring of integers of K. As is usual we will say K is Euclidean when we mean that $\mathcal{O}_K$ is a Euclidean domain. In this paper we continue an investigation into which number fields are Euclidean. Our initial target for investigation will be $\mathbb{Z}[\sqrt{14}]$. The number 14 was the least d for which the Euclidean status of $\mathbb{Q}(\sqrt{d})$ was unknown.

We will use a definition of Euclidean domain due to Samuel [18]. Essentially we require a well-ordered way of measuring the size of $\beta \neq 0$ so that if β does not evenly divide α we can nonetheless find a remainder whose size is less than the size of β.

Definition 1 Let ϕ be a map from the non-zero elements of $\mathcal{O}_K$ into a well-ordered set W. ϕ is a *Euclidean algorithm* for $\mathcal{O}_K$ if for all α and non-zero β in $\mathcal{O}_K$ there are γ and ρ in $\mathcal{O}_K$ with

$$\alpha = \gamma\beta + \rho \quad \text{and}$$
$$\text{either} \quad \rho = 0 \quad \text{or} \quad \phi(\rho) < \phi(\beta).$$

$\mathcal{O}_K$ is a *Euclidean domain* if and only if there is a Euclidean algorithm for $\mathcal{O}_K$.

The algorithm Euclid used in $\mathbb{Z}$ was the absolute norm map, $\phi(n) = |n|$. Another Euclidean algorithm for $\mathbb{Z}$ is $\phi(n) = [\log_2 |n|]$ where $[x]$ is the integral part of x.

Samuel showed that for $\mathcal{O}_K$ there is an algorithm ϕ into some well-ordered W if and only if there is an algorithm ϕ' into $\mathbb{N}_0$, the non-negative integers. We will consider only algorithms into $\mathbb{N}_0$.

Received by the editors April 19, 2002; revised August 15, 2002.
AMS subject classification: 11R04, 11R11.
©Canadian Mathematical Society 2004.

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

Originally the question of what K are Euclidean was posed as: For what fields K is the absolute norm map $\phi(\alpha) = \left|N_{K/\mathbb{Q}}\alpha\right|$ a Euclidean algorithm for $\mathcal{O}_K$? We will call such fields *norm-Euclidean*.

Weinberger [19] applied Hooley's primitive root techniques [11] to the Euclidean algorithm problem and showed the following proposition.

Proposition 1 *Let K be a number field of class number one. Suppose $\mathcal{O}_K$ has an infinite unit group. Assuming a generalized Riemann hypothesis, $\mathcal{O}_K$ is Euclidean.*

Not only should $\mathbb{Z}[\sqrt{14}]$ be a Euclidean domain, but assuming a GRH (generalized Riemann hypothesis), outside of the imaginary quadratic fields, every number field of class number one should be Euclidean.

In the 1980s Lenstra suggested that the unconditional (independent of the assumption of a GRH) primitive root techniques of Gupta and R. Murty [5] should be applied to the Euclidean problem. Gupta, R. Murty and K. Murty [6] found a result for S-integers of K. Let K be a number field and let S be a finite set of places of K including the infinite places S_∞. $\mathcal{O}_S$ is the ring of S-integers of K. Set $d = \gcd\{(N_{K/\mathbb{Q}}\mathfrak{p}) - 1 : \mathfrak{p} \in S \setminus S_\infty\}$.

Proposition 2 *If K is Galois over $\mathbb{Q}$, K has a real embedding or $\zeta_d \in K$, and $\#S \geq \max\{5, 2[K:\mathbb{Q}] - 3\}$ then $\mathcal{O}_S$ is a Euclidean domain.*

Gupta, Murty and Murty were thus able to provide the first examples of rings $\mathcal{O}_S$ that are Euclidean but not norm-Euclidean. Unfortunately the size of S required precludes the application of their theorem to $\mathcal{O}_K$. Results for $\mathcal{O}_K$ had to wait a few more years.

Clark and R. Murty [3] provided results for $K/\mathbb{Q}$ totally real and Galois in 1995. They replaced the above condition on the size of S by a condition requiring the existence of a suitably large set of admissible primes in $\mathcal{O}_K$. Admissible primes are defined explicitly in the next section.

Proposition 3 **([3])** *Let R be a* PID *whose quotient field K is a totally real Galois extension of $\mathbb{Q}$ of degree n. If there is a set of s admissible primes of R with $s \geq |n-4|+1$ then $\mathcal{O}_K$ is Euclidean.*

When $n = 2$, that is when K is a real quadratic field, the proposition requires $s \geq 3$. However for any real quadratic field s can be at most 2. The proposition cannot be applied to real quadratic fields. Clark and Murty point out that their theorem implies that $\mathbb{Z}[\sqrt{14}, 1/p]$ is Euclidean when $p = 1298852237$. Actually it is straightforward to combine the result of Clark and Murty with that of Gupta, Murty and Murty (Proposition 2) and show that $\mathbb{Z}[\sqrt{14}, 1/p]$ is Euclidean for any p [7].

Here we modify the approach of Clark and Murty to prove that $\mathbb{Z}[\sqrt{14}]$ is Euclidean. We then apply the modified proof to other real quadratic fields and to cyclotomic fields.

Theorem A *$\mathbb{Z}[\sqrt{14}]$ is a Euclidean domain.*

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

Theorem B *Suppose $K/\mathbb{Q}$ is a real quadratic field. If $\mathcal{O}_K$ is a* PID *and contains a set of two admissible primes then $\mathcal{O}_K$ is a Euclidean domain. If the discriminant of K does not exceed* 500 *then $\mathcal{O}_K$ is Euclidean if and only if it is a* PID.

Theorem C *$\mathbb{Z}[\zeta_d]$ is a Euclidean domain if and only if it is a principal ideal domain.*

Contrasting the method here with the method of Clark and Murty suggests a means of attack on the Euclidean algorithm problem in general Galois extensions of $\mathbb{Q}$. M. Ram Murty and this author prove in a forthcoming paper that for $K/\mathbb{Q}$ Galois with unit rank exceeding 3, $\mathcal{O}_K$ is Euclidean $\iff$ it is a PID [9].

2 Motzkin's Lemma

Motzkin [16] provided a characterization of Euclidean domains. It was originally used to show that the rings of integers of the number fields $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$ are not Euclidean for any algorithm. Samuel [18] suggested that the characterization might be used to show that some rings are Euclidean. In his paper, Samuel singled out $\mathbb{Z}[\sqrt{14}]$ as the ring on which these methods should be tested. Based on heuristic reasoning inspired by an appropriate generalization of Artin's primitive root conjecture, he was led to speculate that $\mathbb{Z}[\sqrt{14}]$ is Euclidean. (It is easy to see that $\mathbb{Z}[\sqrt{14}]$ is not norm-Euclidean.)

Definition 2 **(Motzkin's Construction)** Let R be an integral domain. Define A_0 to be the unit group of R, that is $A_0 = R^\times$. For $n \geq 1$, successively define A_n as the set of all non-zero elements β in R such that every non-zero residue class modulo βR has a representative in A_{n-1}. That is:

$$A_n = \left\{ \beta \in R \setminus 0 : A_{n-1} \cup \{0\} \xrightarrow{\text{onto}} R/(\beta R) \right\};$$

$$\text{define } A = \bigcup_{n \geq 0} A_n.$$

Proposition 4 **(Motzkin's Lemma)** *R is Euclidean if and only if every non-zero element of R is in A.*

Proof Proofs appear in Motzkin [16] and Samuel [18] for example. ∎

In the case of a real quadratic field, Motzkin's set A_1 consists of irreducibles π such that some fundamental unit generates all of the non-zero residue classes (mod π). This is suggestive of Artin's primitive root conjecture which Hooley proved under the assumption of a generalized Riemann hypothesis. In the light of Hooley's conditional resolution of Artin's primitive root conjecture [11], one can ask when we can expect that the full ring of integers, $\mathcal{O}_K$, of an algebraic number field K is Euclidean. Surely a necessary condition is that the ring $\mathcal{O}_K$ be a principal ideal domain (PID). That this condition is sufficient (when K is not an imaginary quadratic field) is a remarkable prediction of the generalized Riemann hypothesis (GRH). This is Weinberger's theorem. More precisely, he proves unconditionally:

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

Proposition 5 *If $\mathcal{O}_K$ is a* PID *and all primes of $\mathcal{O}_K$ are in A_2 then $\mathcal{O}_K$ is Euclidean.*

Proof This is shown by applying Motzkin's lemma, Proposition 4 and an analog of Dirichlet's theorem on primes in arithmetic progressions for number fields. See Weinberger [19]. ∎

He then shows, assuming GRH, that if $\mathcal{O}_K$ has an infinite unit group then all primes are in A_2 (Proposition 1).

There have been several attempts to remove the dependence on a GRH from this proposition. The first was a paper by Gupta, R. Murty and K. Murty [6] in which they showed unconditionally that the ring of S-integers, $\mathcal{O}_{K,S}$, for a finite set S, is Euclidean whenever $\mathcal{O}_K$ is a PID and contains infinitely many units. In that paper, we find the first examples of rings of S-integers of number fields which are Euclidean, but not norm-Euclidean. In the particular case that K is a real quadratic field, they show that $\mathcal{O}_{K,S}$ is Euclidean whenever $\mathcal{O}_K$ is a PID and $\#S \geq 5$.

The second attempt is due to Clark and R. Murty. They observed that the previous argument can be modified by introducing what they call *Wieferich primes*. In the case of a quadratic field K, these primes can essentially be characterized as primes π satisfying:

(1) $\epsilon^{N(\pi)-1} \not\equiv 1 \pmod{\pi^2}$ where ϵ is the fundamental unit of K and
(2) the image of $\epsilon \pmod{\pi}$ generates the group $(\mathcal{O}_K/\pi)^\times$.

Their terminology is motivated by an old theorem of Wieferich, namely, if p is a prime such that $2^{p-1} \not\equiv 1 \pmod{p^2}$ then $x^p + y^p = z^p$ has no solutions with $(p, xyz) = 1$.

These Wieferich primes seem to play an important role in the study of Euclidean rings. In this paper, we will call them *admissible sets of primes*.

Definition 3 **(Admissible Sets of Primes)** Let $\pi_1, \ldots, \pi_s \in \mathcal{O}_K$ be distinct non-associate primes. $\{\pi_1, \ldots, \pi_s\}$ is an *admissible set of primes* if for all $\beta = \pi_1^{a_1} \cdots \pi_s^{a_s}$, with $a_i \in \mathbb{N}_0$, every coprime residue class $(\mathrm{mod}\ \beta)$ can be represented by a unit of $\mathcal{O}_K$.

If r is the rank of $\mathcal{O}_K^\times$ modulo torsion, then the number of elements in an admissible set of primes satisfies $s \leq r + 1$. To see this recall that by Dirichlet's unit theorem

$$\mathcal{O}_K^\times \simeq W_K \oplus \mathbb{Z}^r$$

where W_K is the finite group of roots of unity in K. Thus $\left(\mathcal{O}_K/(\pi_1^{a_1} \cdots \pi_s^{a_s})\right)^\times$ must be generated by $r + 1$ elements. Since

$$\left(\mathcal{O}_K/(\pi_1^{a_1} \cdots \pi_s^{a_s})\right)^\times \simeq \bigoplus_{1 \leq i \leq s} \left(\mathcal{O}_K/(\pi_i^{a_i})\right)^\times,$$

by the Chinese remainder theorem we must have $s \leq r + 1$. Heuristics suggest that $s = r + 1$ can always be attained.

To check if $\{\pi_1, \ldots, \pi_s\}$ is admissible it will usually suffice to check whether every coprime residue class of $\beta = \pi_1^2 \cdots \pi_s^2$ can be represented by a unit. This is a proposition on page 160 of the paper of Clark and Murty [3].

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

Proposition 6 *Let $\pi_1, \ldots, \pi_s \in \mathcal{O}_K$ be distinct non-associate primes. Further suppose that each π_i is unramified and of odd prime norm. If every coprime residue class modulo $\pi_1^2 \cdots \pi_s^2$ contains a unit then $\{\pi_1, \ldots, \pi_s\}$ is an admissible set of s primes in $\mathcal{O}_K$.*

Clark and Murty combine Proposition 6 with the following proposition to show certain totally real Galois extensions are Euclidean but not norm-Euclidean. They give examples of quartic and cubic extensions to which their theorem applies. In his thesis [2] in 1992, Clark gave examples of totally real, quartic, Galois extensions that were Euclidean, but not norm-Euclidean. These were the first examples of number fields K that are Euclidean, but not norm-Euclidean.

The Motzkin variant used by Clark and Murty is:

Proposition 7 *Let A_0 be the monoid generated by the unit group and an admissible set of primes. Complete the construction of the A_n as in Motzkin's construction, Definition 2, above. If every prime of $\mathcal{O}_K$ lies in A_2 then $\mathcal{O}_K$ is Euclidean.*

In essence, Clark and Murty are boosting the size of the starting set in the construction by identifying certain special primes that act enough like units that a variant of Motzkin's lemma goes through. With more degrees of freedom in A_0 it is possible for them to show that all of the primes of $\mathcal{O}_K$ are in A_2 for certain fields where this was not possible before.

3 A Variation of Motzkin's Lemma

Notice that while the constructions of A_n used by Weinberger and by Clark and Murty use arbitrary elements of $\mathcal{O}_K$, the hypotheses of Propositions 5 and 7 consider only the primes of $\mathcal{O}_K$. Some gain can be made by considering only the primes during the construction. This motivates:

Definition 4 **(The Construction of** B**)** Let B_0 be the monoid generated by the unit group and an admissible set of primes. For $n \geq 1$, successively define B_n as the set of all *primes* π of $\mathcal{O}_K$ such that every non-zero residue class modulo (π) has a representative in $B_{n-1} \cup B_0$. That is:

$$B_n = \{\text{primes } \pi \in \mathcal{O}_K : B_{n-1} \cup B_0 \xrightarrow{\text{onto}} (\mathcal{O}_K/\pi)^\times\}.$$

Now let $B = \bigcup_{n \geq 0} B_n$.

Our main result here is:

Lemma 1 *Let $\mathcal{O}_K$ be a principal ideal domain. If all primes of $\mathcal{O}_K$ are in B then $\mathcal{O}_K$ is Euclidean.*

Proof We shall use Proposition 4, Motzkin's lemma. To show that a non-zero β is in A, it suffices to show that every non-zero residue class (mod β) has a representative in A. We can draw this conclusion since $\mathcal{O}_K$ has finite norms.

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

We will proceed by induction. Let $\Omega_0(\beta)$ count those prime divisors of β that are in B_0 according to their multiplicity and let $\Omega_1(\beta)$ count those prime divisors that are not in B_0. Define λ on the prime elements of $\mathcal{O}_K$ by

$$\lambda(\pi) = \begin{cases} 0, & \text{if } \pi \in B_0; \\ n, & \text{if } \pi \in B_n \setminus B_{n-1}. \end{cases}$$

Extend λ to all non-zero $\beta \in \mathcal{O}_K$ by complete additivity. For example, if $\beta = \pi_1^{a_1} \cdots \pi_s^{a_s}$ then

$$\lambda(\beta) = \sum_i a_i \lambda(\pi_i), \quad \Omega_0(\beta) = \sum_{\pi_i \in B_0} a_i, \quad \text{and} \quad \Omega_1(\beta) = \sum_{\pi_i \notin B_0} a_i.$$

Ω_0, Ω_1 and λ are all well-defined since each B_n is closed under the taking of associates; since the B_n, $n \geq 1$, form an increasing sequence of sets; since all of the primes of $\mathcal{O}_K$ are in B by hypothesis; and by unique factorization in $\mathcal{O}_K$.

Now induct on $\big(\Omega_1(\beta), \Omega_0(\beta), \lambda(\beta)\big)$ ordered lexicographically. If $\beta \in \mathcal{O}_K^\times$ then $\big(\Omega_1(\beta), \Omega_0(\beta), \lambda(\beta)\big) = (0,0,0)$ and $\beta \in A$ by definition. Suppose $\beta \in \mathcal{O}_K$ is neither zero nor a unit. Let $\alpha \pmod{\beta}$ be a non-zero residue class $(\bmod \beta)$. We will exhibit an $\alpha' \equiv \alpha \pmod{\beta}$ that precedes β in the ordering. By the induction hypothesis if α' precedes β then $\alpha' \in A$ so $\alpha \pmod{\beta}$ has a representative in A.

Assume first that α and β are coprime. There are various cases:

$\beta \in B_0$; that is $\Omega_1(\beta) = 0$ and $\Omega_0(\beta) \geq 1$:
By the definition of B_0, we can represent $\alpha \pmod{\beta}$ by a unit α' so that $\Omega_1(\alpha') = 0$ and $\Omega_0(\alpha') = 0$.

β is a prime not in B_0; that is $\Omega_1(\beta) = 1$ and $\Omega_0(\beta) = 0$:
$\alpha \pmod{\beta}$ can be represented by an element of B_0 so that $\Omega_1(\alpha') = 0$ or by a prime preceding β in which case $\Omega_1(\alpha') = 1$, $\Omega_0(\alpha') = 0$ and $\lambda(\alpha') < \lambda(\beta)$.

Otherwise $\Omega_1(\beta) = 1$ and $\Omega_0(\beta) \geq 1$ or else $\Omega_1(\beta) \geq 2$:
We use an analog of Dirichlet's theorem on primes in arithmetic progression for number fields to find a prime α' representing $\alpha \pmod{\beta}$. Either $\Omega_1(\alpha') = 1$ and $\Omega_0(\alpha') = 0$ (when $\alpha' \notin B_0$) or $\Omega_1(\alpha') = 0$ and $\Omega_0(\alpha') = 1$ (when $\alpha' \in B_0$).

In each case there is an $\alpha' \equiv \alpha \pmod{\beta}$ with α' preceding β under our ordering.

If $\gcd(\alpha, \beta) = \delta \neq 1$, we can find an α'/δ representing $\alpha/\delta \pmod{\beta/\delta}$ with α'/δ preceding β/δ as above. But then α' represents $\alpha \pmod{\beta}$ while α' precedes β since each of Ω_1, Ω_0 and λ is completely additive. The only possible exception is when β/δ is a unit, but then $\alpha \pmod{\beta}$ is the zero class which we need not consider.

This completes the proof. ∎

4 Application of the Large Sieve

Lemma 1 shows that we only need to prove that all primes are in B in order to show that $\mathcal{O}_K$ is Euclidean. We next derive a numerical criterion to prove this. Our main

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

tools are the large sieve method in number fields as derived by Wilson [20] and an estimate due to Gupta and Murty [5].

For the remainder of this paper we will always take $\mathcal{O}_K$ to be a PID. If $S \subseteq \mathcal{O}_K$ then $\mathcal{S}$ will denote the set of ideals generated by elements of S, $\mathcal{S} = \{\alpha\mathcal{O}_K : \alpha \in S\}$. For $\mathcal{S}$ a set of ideals, $\mathcal{S}(x)$ is the set of those ideals in $\mathcal{S}$ whose norm does not exceed x, that is $\mathcal{S}(x) = \{\mathfrak{a} \in \mathcal{S} : N\mathfrak{a} \leq x\}$. For example, $\mathcal{B}_1(x) = \{(\beta) : \beta \in B_1 \text{ and } |N\beta| \leq x\}$. Our next result is:

Lemma 2 *If* $\#\mathcal{B}_1(x) \gg x/\log^2 x$ *then* $\mathcal{O}_K$ *is Euclidean.*

Before we prove this lemma, we review the result of Gupta and Murty and the large sieve inequality for number fields.

4.1 The Gupta-Murty Lemma

If $\mathfrak{M}$ is a monoid in $\mathcal{O}_K$ whose elements are coprime to an ideal $\mathfrak{a}$ then under reduction mod $\mathfrak{a}$, the image of $\mathfrak{M}$ forms a subgroup of $(\mathcal{O}_K/\mathfrak{a})^\times$. $f_{\mathfrak{M}}(\mathfrak{a})$ will denote the order of this subgroup. If $\mathfrak{M}$ is generated by a single element, $\mathfrak{M} = \langle\alpha\rangle$, then $f_\alpha(\mathfrak{a})$ denotes the order while if $\mathfrak{M} = \mathcal{O}_K^\times$ we write $f(\mathfrak{a})$ for the order. In their work on Artin's primitive root conjecture Gupta and Murty provided a bound on the number of prime ideals $\mathfrak{p}$ with $f_{\mathfrak{M}}(\mathfrak{p})$ small in terms of the size of $\mathfrak{M}$. The number of *multiplicatively independent* elements of $\mathfrak{M}$ measures its size.

Definition 5 $\alpha_1, \ldots, \alpha_t \in K$ are *multiplicatively independent* if, for $a_i \in \mathbb{Z}$, $\alpha_1^{a_1} \cdots \alpha_t^{a_t} = 1$ implies that all a_i are 0.

The Gupta-Murty bound is:

Proposition 8 *Let* $\mathfrak{M}$ *be a monoid in* $\mathcal{O}_K$. *If* $\mathfrak{M}$ *contains a set of* t *multiplicatively independent elements then*

$$\#\{\mathfrak{p} : f_{\mathfrak{M}}(\mathfrak{p}) \leq Y\} \ll Y^{\frac{t+1}{t}}.$$

The implied constant depends only on K *and* $\mathfrak{M}$.

Proof See Lemma 6 of Clark and Murty [3] for a proof in the number field case. ∎

4.2 The Large Sieve Inequality

Let $\mathcal{A}$ be any finite set of non-associated elements of $\mathcal{O}_K$ and let $\mathcal{P}$ be any finite set of non-ramifying prime ideals of K. Denote the cardinality of $\mathcal{A}$ by Z and the cardinality of $\{\beta \in \mathcal{A} : \beta \equiv \alpha \pmod{\mathfrak{p}}\}$ by $Z(\alpha, \mathfrak{p})$. X and Q are bounds on the norms of all the elements of $\mathcal{A}$ and $\mathcal{P}$ respectively.

$$\text{That is} \quad X \geq \max_{\beta\in\mathcal{A}} |N\beta| \quad \text{and} \quad Q \geq \max_{\mathfrak{p}\in\mathcal{P}} N\mathfrak{p}.$$

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

Proposition 9 **(The Large Sieve in Number Fields)**

$$\sum_{\mathfrak{p}\in\mathcal{P}}\left(N\mathfrak{p}\sum_{\alpha(\mathrm{mod}\ \mathfrak{p})}\left(Z(\alpha,\mathfrak{p})-\frac{Z}{N\mathfrak{p}}\right)^2\right)\ll(Q^2+X)Z$$

where the implied constant depends only on K.

Proof This is Wilson's Theorem 1 [20]. ∎

$\omega(\mathfrak{p})$ will denote the number of residue classes $\alpha \pmod{\mathfrak{p}}$ for which $Z(\alpha,\mathfrak{p})=0$. Then

$$\sum_{\alpha(\mathrm{mod}\ \mathfrak{p})}\left(Z(\alpha,\mathfrak{p})-\frac{Z}{N\mathfrak{p}}\right)^2\geq\frac{Z^2\omega(\mathfrak{p})}{N\mathfrak{p}^2}$$

and we deduce:

Corollary 9.1

$$\sum_{\mathfrak{p}\in\mathcal{P}}\frac{\omega(\mathfrak{p})}{N\mathfrak{p}}\ll\frac{Q^2+X}{Z}.$$

4.3 The Proof of Lemma 2

We will show that $\#\mathcal{B}_2(x)\sim x/\log x$. This implies that all primes must be in B_3, for if not, say $\pi\notin B_3$. Then there is a residue class $(\mathrm{mod}\ \pi)$ which has no representative from B_2. This would contradict Dirichlet's theorem. Hence by Lemma 1, $\#\mathcal{B}_2(x)\sim x/\log x$ suffices to show that $\mathcal{O}_K$ is Euclidean. Proving that $\#\mathcal{B}_2(x)\sim x/\log x$ is equivalent to showing that $\mathcal{B}_2^c$, the complement of $\mathcal{B}_2$ in the set of prime ideals of $\mathcal{O}_K$, satisfies

$$\#\mathcal{B}_2^c(x)=\underline{o}(x/\log x).$$

This is what we show using the large sieve method.

We apply the large sieve as follows: Let $\mathcal{A}$ be a set of representatives of $\mathcal{B}_1(x^2)$. Let $Z=\#\mathcal{A}=\#\mathcal{B}_1(x^2)$, and set $X=x^2$. Let $\mathcal{P}=\mathcal{B}_2^c(x)$ so $Q=x$. By Corollary 9.1 and the hypothesis on $\mathcal{B}_1(x)$, we have

$$\sum_{\mathfrak{p}\in\mathcal{B}_2^c(x)}\frac{\omega(\mathfrak{p})}{N\mathfrak{p}}\ll\frac{x^2}{\#\mathcal{B}_1(x^2)}\ll\log^2 x. \tag{1}$$

Now we need a lower bound on $\omega(\mathfrak{p})$ for $\mathfrak{p}\in\mathcal{B}_2^c$ so that we can use (1) to estimate $\#\mathcal{B}_2^c(x)$. Recall that when reduced modulo $\mathfrak{p}$, the unit group forms a subgroup of $(\mathcal{O}_K/\mathfrak{p})^\times$ and that $f(\mathfrak{p})$ denotes the size of this subgroup. Note that $\mathfrak{p}\in\mathcal{B}_2^c$ means some non-zero residue class mod $\mathfrak{p}$ fails to have a representative in B_1. Since B_1 is closed under the taking of associates, if one non-zero residue class mod $\mathfrak{p}$ is not represented then at least $f(\mathfrak{p})$ non-zero residue classes mod $\mathfrak{p}$ are not represented by elements of B_1. Thus for $\mathfrak{p}\in\mathcal{B}_2^c$, $\omega(\mathfrak{p})\geq f(\mathfrak{p})$.

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

By the Gupta-Murty bound (Proposition 8),

$$\#\{\mathfrak{p} : f(\mathfrak{p}) \leq Y\} \ll Y^2$$

provided $\mathcal{O}_K$ has a unit of infinite order. Thus,

$$\#\{\mathfrak{p} : N\mathfrak{p} \leq x \text{ and } f(\mathfrak{p}) \leq N\mathfrak{p}^{\frac{1}{2}-\varepsilon}\} \ll x^{1-2\varepsilon}$$

and so

$$\#\{\mathfrak{p} : N\mathfrak{p} \leq x \text{ and } f(\mathfrak{p}) \leq N\mathfrak{p}^{\frac{1}{2}-\varepsilon}\} = \underline{o}(x/\log x). \tag{2}$$

On the other hand using equation (1)

$$\begin{aligned}
\log^2 x &\gg \sum_{\substack{\mathfrak{p}\in\mathcal{B}_2^c(x)\\ f(\mathfrak{p})>N\mathfrak{p}^{\frac{1}{2}-\varepsilon}}} \frac{\omega(\mathfrak{p})}{N\mathfrak{p}} \\
&\geq \sum_{\substack{\mathfrak{p}\in\mathcal{B}_2^c(x)\\ f(\mathfrak{p})>N\mathfrak{p}^{\frac{1}{2}-\varepsilon}}} \frac{f(\mathfrak{p})}{N\mathfrak{p}} \\
&> \sum_{\substack{\mathfrak{p}\in\mathcal{B}_2^c(x)\\ f(\mathfrak{p})>N\mathfrak{p}^{\frac{1}{2}-\varepsilon}}} \frac{1}{N\mathfrak{p}^{\frac{1}{2}+\varepsilon}} \\
&> \frac{\#\{\mathfrak{p}\in\mathcal{B}_2^c(x) : f(\mathfrak{p}) > N\mathfrak{p}^{\frac{1}{2}-\varepsilon}\}}{x^{\frac{1}{2}+\varepsilon}}.
\end{aligned}$$

Thus

$$\#\{\mathfrak{p}\in\mathcal{B}_2^c(x) : f(\mathfrak{p}) > N\mathfrak{p}^{\frac{1}{2}-\varepsilon}\} = \underline{o}(x/\log x). \tag{3}$$

Equations (2) and (3) together give

$$\#\mathcal{B}_2^c(x) = \underline{o}(x/\log x) \quad \text{and so} \quad \#\mathcal{B}_2(x) \sim x/\log x.$$

B_3 contains all primes and so by Lemma 1, $\mathcal{O}_K$ is Euclidean. This completes the proof of Lemma 2. ∎

5 The Proof of Theorem A

We can now apply Lemma 2 to show that $\mathbb{Z}[\sqrt{14}]$ is Euclidean. We first exhibit an admissible set of two primes for $\mathbb{Z}[\sqrt{14}]$. Thus we will have three multiplicatively independent elements in B_0. The lower bound sieve then shows that $\#\mathcal{B}_1(x) \gg x/\log^2 x$ and hence that $\mathbb{Z}[\sqrt{14}]$ is Euclidean.

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

We will apply the lower bound sieve using the techniques pioneered by Gupta and Murty [5] in their work on Artin's primitive root conjecture. These techniques were first applied to the Euclidean algorithm problem by Gupta, Murty and Murty [6] and then by Clark [2] and by Clark and Murty [3].

The key ingredients here are the Rosser–Iwaniec lower bound sieve with bilinear form for the remainder terms; a Bombieri–Vinogradov type theorem of Bombieri, Friedlander and Iwaniec to control the remainder terms in the sieve and allow sieving past $x^{\frac{1}{4}}$; and the Gupta–Murty estimate on the number of $\mathfrak{p}$ with $f_{B_0}(\mathfrak{p})$ bounded, our Proposition 8.

5.1 Admissible Primes in $\mathbb{Z}[\sqrt{14}]$

$\epsilon = 15 + 4\sqrt{14}$ is the fundamental unit of $\mathbb{Z}[\sqrt{14}]$. $\mathbb{Z}[\sqrt{14}]^{\times}$ is generated by -1 and ϵ. Set $\pi_1 = 5 - \sqrt{14}$ and $\pi_2 = 3 - 2\sqrt{14}$.

Proposition 10 *$\{\pi_1, \pi_2\}$ is an admissible set of primes in $\mathbb{Z}[\sqrt{14}]$.*

Proof $N\pi_1 = 11$ and $N\pi_2 = -47$ so π_1, π_2 are split primes in $\mathbb{Z}[\sqrt{14}]$. The order of $\epsilon \pmod{\pi_1^2}$ is $(10)(11) = 110$ and its order $(\bmod \pi_2^2)$ is $(46)(47)/2 = 1081$. Thus ϵ is a generator of $\left(\mathbb{Z}[\sqrt{14}]/(\pi_1)^2\right)^{\times}$ and $-\epsilon$ is a generator $(\bmod \pi_2^2)$. Since $\gcd(110, 1081) = 1$, ϵ^{1081} is a generator $(\bmod \pi_1^2)$ that is congruent to $1 \pmod{\pi_2^2}$. If ϵ^{1081a} is the inverse of $-\epsilon \pmod{\pi_1^2}$ then $-\epsilon^{1081a+1}$ is congruent to $1 \pmod{\pi_1^2}$ but generates $\left(\mathbb{Z}[\sqrt{14}]/(\pi_2^2)\right)^{\times}$. Thus by the Chinese remainder theorem, every coprime residue class modulo $(\pi_1^2\pi_2^2)$ can be represented by a unit. By Proposition 6, $\{\pi_1, \pi_2\}$ is admissible. ∎

5.2 The Lower Bound Sieve

To apply the lower bound sieve method, we will need the following results:

Definition 6 **(Well-factorable)** Let λ be an arithmetic function defined for $1 \leq q \leq Q$. If for all $Q_1, Q_2 \geq 1$ with $Q_1Q_2 = Q$ there are arithmetic functions λ_i defined for $1 \leq q \leq Q_i$ with $|\lambda_i(q)| \leq 1$ and

$$\lambda(q) = \sum_{\substack{q_1q_2=q \\ q_i \leq Q_i}} \lambda_1(q_1)\lambda_2(q_2)$$

then λ is said to be *well-factorable of level Q*.

Let $\mathcal{P}$ be a set of primes and let $\mathcal{A}$ be a set of positive integers all of which are less than or equal to x. For each $\ell \in \mathcal{P}$ distinguish $\omega(\ell)$ residue classes $(\bmod \ell)$. These are the residue classes which will be sifted out of $\mathcal{A}$. $S(\mathcal{A}, \mathcal{P}, z)$ counts the number of elements of $\mathcal{A}$ that do not lie in any of the distinguished residue classes for any $\ell \in \mathcal{P}$ with $\ell < z$. It is the number of elements of $\mathcal{A}$ remaining after sifting.

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

Let $\mathcal{A}_\ell$ denote the set of those elements of $\mathcal{A}$ that belong to one of the distinguished classes (mod ℓ) and let $\mathcal{A}_q$ denote those elements that lie in some distinguished class for all $\ell|q$. X is an approximation to the size of $\mathcal{A}$ so that

$$X\prod_{\ell|q}\frac{\omega(\ell)}{\ell} \quad \text{approximates} \quad \#\mathcal{A}_q.$$

Call the error in the approximation r_q, that is:

$$r_q = \#\mathcal{A}_q - X\prod_{\ell|q}\frac{\omega(\ell)}{\ell}.$$

If we choose X so that the remainder terms, r_q can be controlled, Iwaniec's bilinear form of the remainder [12] gives:

Proposition 11 **(The Lower Bound Sieve)** *For each $\varepsilon, \varepsilon' > 0$ there is an N depending on ε' and ε such that*

$$S(\mathcal{A},\mathcal{P},x^\theta) \geq X\prod_{\substack{\ell\in\mathcal{P}\\ \ell<x^\theta}}\Big(1-\frac{\omega(\ell)}{\ell}\Big)\Big\{f\Big(\frac{2\theta+\varepsilon}{\theta}\Big)-\varepsilon'\Big\} - R_0 - \sum_{n=1}^{N} R_n$$

for all x sufficiently large.

Here f is a well-known function, $f(u) = \frac{2e^\gamma}{u}\log(u-1)$ if $2 < u \leq 4$, so $f(u)$ is positive in this range.

$$R_0 = \sum_{q<x^{\frac{1}{4}}}\big|r_q\big| \quad \text{and} \quad R_n = \sum_q \lambda_n(q) r_q$$

for some well-factorable functions λ_n of level $x^{2\theta+\varepsilon}$.

Proof See Iwaniec [12, Theorem 4]. ∎

The usual form of the Bombieri-Vinogradov theorem shows that $R_0 \ll x/\log^3 x$. To control the R_n remainder terms we will need the following theorem of Bombieri, Friedlander and Iwaniec [1]:

Proposition 12 *Suppose $a \neq 0$, $\varepsilon > 0$ and $Q = x^{4/7-\varepsilon}$. For any well-factorable function $\lambda(q)$ of level Q and any $A > 0$,*

$$\sum_{(q,a)=1}\lambda(q)\Big(\psi(x;q,a)-\frac{x}{\phi(q)}\Big) \ll x/\log^A x.$$

Proof See Bombieri, Friedlander and Iwaniec [1, Theorem 10]. ∎

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

Proposition 12 needs to be modified slightly in order to apply it here. Fouvry [4, pp. 388 and 389] has sketched the process and Heath-Brown [10] has provided details.

Proposition 13 *Let* $\gcd(a,k)=1$. *For any* q *with* $\gcd(q,k)=1$ *let* u_q *be a solution of*

$$u_q \equiv a \pmod{k} \quad \textit{and}$$
$$u_q \equiv 1 \pmod{q}.$$

Fix $A>0$ *and* $\theta<\frac{4}{7}$. *For every well-factorable function of level* x^θ

$$\sum_{\gcd(q,k)=1} \lambda(q)\Big(\pi(x;qk,u_q)-\frac{\operatorname{li} x}{\phi(qk)}\Big) \ll \frac{x}{\log^A x}.$$

The implied constant depends on a, k, θ *and A.*

Proof This is Lemma 2 in Heath-Brown [10]. ∎

Applying Proposition 13 in Proposition 11, see Heath-Brown [10] for example, we obtain:

Lemma 3 *Suppose a and k are coprime integers. Set* $d=\gcd(a-1,k)$ *and suppose* $\gcd\big((a-1)/d,d\big)=1$. *The number of primes* $p\le x$ *such that*

$$p \equiv a \pmod{k} \quad \textit{and}$$
$$\frac{p-1}{d} \textit{ is divisible only by primes } \ell \textit{ exceeding } x^{\frac{2}{7}-\varepsilon}$$

is $\gg x/\log^2 x$.

Proof The proof is identical to that of Heath-Brown's Lemma 1 [10]. ∎

5.3 Completion of the proof

Now we can prove Theorem A:

Theorem A $\mathbb{Z}[\sqrt{14}]$ *is a Euclidean domain.*

Proof We apply Lemma 2 to the ring $R=\mathbb{Z}[\sqrt{14}]$ with B_0 equal to the monoid generated by the admissible primes π_1 and π_2 of Proposition 10 and the units of $\mathbb{Z}[\sqrt{14}]$. By Lemma 2, it suffices to show that $\#\mathcal{B}_1(x)\gg x/\log^2 x$. We deduce this from Lemma 3. Indeed, setting $a=11$ and $k=56$ in Lemma 3 we have that the set of $p\le x$ with $p\equiv 11 \pmod{56}$ and $\ell|(p-1)/2$ implies $\ell>x^{\frac{2}{7}-\varepsilon}$ has cardinality $\gg x/\log^2 x$. Since each $p\equiv 11 \pmod{56}$ splits in $\mathbb{Z}[\sqrt{14}]$, there are $\gg x/\log^2 x$ primes

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

$\mathfrak{p}$ of $\mathbb{Z}[\sqrt{14}]$ such that $N\mathfrak{p} \le x$ and $\ell | (N\mathfrak{p}-1)/2$ implies $\ell > x^{\frac{2}{7}-\varepsilon}$. $f_{B_0}(\mathfrak{p})$ denotes the order of the subgroup of $(\mathbb{Z}[\sqrt{14}]/\mathfrak{p})^{\times}$ formed by reducing B_0 mod $\mathfrak{p}$. $\mathfrak{p} \in \mathcal{B}_1$ if and only if $f_{B_0}(\mathfrak{p}) = N\mathfrak{p} - 1$. By the choice of a and k, $N\mathfrak{p} = p \equiv 3 \pmod 4$. Since $-1 \in B_0$, without loss of generality $2 | f_{B_0}(\mathfrak{p})$ and so $2 \nmid (N\mathfrak{p}-1)/f_{B_0}(\mathfrak{p})$. $(N\mathfrak{p}-1)/f_{B_0}(\mathfrak{p})$ equals one or exceeds $x^{\frac{2}{7}-\varepsilon}$. In the latter case $f_{B_0}(\mathfrak{p}) \le x^{\frac{5}{7}+\varepsilon}$. By the Gupta-Murty estimate, Proposition 8,

$$\#\{\mathfrak{p} : f_{B_0}(\mathfrak{p}) \le x^{\frac{5}{7}+\varepsilon}\} \ll x^{(\frac{5}{7}+\varepsilon)\frac{4}{3}},$$

since B_0 has three multiplicatively independent elements. Choosing $\varepsilon < 1/28$ gives the bound $\underline{o}(x/\log^2 x)$ for the number of $\mathfrak{p}$ with $f_{B_0}(\mathfrak{p}) \le x^{\frac{5}{7}+\varepsilon}$. Thus there are $\gg x/\log^2 x$ primes $\mathfrak{p}$ with $N\mathfrak{p} \le x$ and $f_{B_0}(\mathfrak{p}) = N\mathfrak{p} - 1$. $\#\mathcal{B}_1(x) \gg x/\log^2 x$ and so by Lemma 2, $\mathbb{Z}[\sqrt{14}]$ is Euclidean. ■

6 Real Quadratic Fields

We can generalize the result for $\mathbb{Z}[\sqrt{14}]$ to other real quadratic fields.

Theorem B *Suppose $K/\mathbb{Q}$ is a real quadratic field. If $\mathcal{O}_K$ is a* PID *and contains a set of two admissible primes then $\mathcal{O}_K$ is a Euclidean domain. If the discriminant of K does not exceed* 500 *then $\mathcal{O}_K$ is Euclidean if and only if it is a* PID.

We will first prove a lemma, also useful for extending Theorem A to cyclotomic fields.

Lemma 4 *Suppose $\mathcal{O}_K$ is a* PID *and contains a set of s admissible primes. Let r be the rank of $\mathcal{O}_K^{\times}$ modulo torsion and define $d = \max\{d' : \zeta_{d'} \in K\}$. If $r + s \ge 3$ and if there are a and $k \in \mathbb{Z}$ satisfying:*

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

then $\mathcal{O}_K$ is a Euclidean domain.

Proof We begin by noting that the conditions on a, k, d imply that $\gcd\big((a-1)/d, d\big) = 1$. To see this, let us observe that if a and k satisfy the conditions of the lemma, then for any integer n, the number $a' = a + nk$ will also satisfy the condition $\gcd\big((a'-1)/d, d\big) = 1$ provided n is suitably chosen. Indeed, the second condition implies that $a = 1 + dh$ for some h satisfying $\gcd(h, k/d) = 1$. Then $(a'-1)/d = h + nk/d$ can be taken to be a large prime by Dirichlet's theorem for an appropriate choice of n.

Our Motzkin variant, Lemma 1, holds for any K with class number one. Wilson's large sieve, Proposition 9, and the Gupta-Murty estimate, Proposition 8, hold for arbitrary K so Lemma 2 also holds if $\mathcal{O}_K$ is a PID.

If we examine the proof of Theorem A we see that the only places we used the fact that $\mathcal{O}_K = \mathbb{Z}[\sqrt{14}]$ were:

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

d	Norm Euclidean	d	Norm Euclidean
3	Yes	24	Yes
4	Yes	25	
5	Yes	27	
7	Yes	28	
8	Yes	32	No
9	Yes	33	
11	Yes	35	
12	Yes	36	
13		40	
15	Yes	44	
16	Yes	45	
17		48	
19		60	
20	Yes	84	
21			

Table 1: Cyclotomic extensions of $\mathbb{Q}$ with class number one.

(1) the assumption that $\mathcal{O}_K$ is a PID;
(2) the demonstration of the two admissible primes that allowed the construction of B_0 with three multiplicatively independent elements; and
(3) the choice of $a = 11$ and $k = 56$ above.

Identifying the properties of this choice of a and k that were used in the proof immediately yields the result. ■

The Proof of Theorem B Apply Lemma 4. $r = 1$ so $r + s = 3$. By quadratic reciprocity there are a and k in $\mathbb{Z}$ such that $(a, k) = 1$, $(a - 1, k) = 2$, and all $p \equiv a \pmod{k}$ split in K.

For the second assertion we need only verify the existence of the admissible primes for all K with discriminant less than 500. This has been done by the author [8]. ■

7 Cyclotomic Fields

We now apply Lemma 4 when $K = \mathbb{Q}(\zeta_d)$, a cyclotomic extension.

Theorem C *$\mathbb{Z}[\zeta_d]$ is a Euclidean domain if and only if it is a principal ideal domain.*

Proof When $K = \mathbb{Q}(\zeta_d)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_d]$. p splits completely in K if and only if $p \equiv 1 \pmod{d}$. To simplify the definition of k we can without loss of generality take d to be even. Let $k = d\prod_{\ell|d} \ell$ and choose $a \pmod{k}$ so that if $\ell^t \| d$ then $a \equiv 1 + \ell^t \pmod{\ell^{t+1}}$. The hypotheses of Lemma 4 are satisfied provided that $r \geq 3$. $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \phi(d)$ so if $\phi(d) \geq 8$, we can conclude that $\mathbb{Z}[\zeta_d]$ is Euclidean if and

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

only if it is a PID. The remaining K, $\mathbb{Q}(\zeta_d)$ with $\phi(d) < 8$, have been completely characterized in terms of the Euclidean property. Lenstra [13] has shown that if $\phi(d) \leq 10$ and $d \neq 16, 24$ then $\mathbb{Z}[\zeta_d]$ is norm-Euclidean. Ojala [17] showed that $\mathbb{Z}[\zeta_{16}]$ is norm-Euclidean in 1977 and Lenstra [14] showed the same for $\mathbb{Z}[\zeta_{24}]$ the following year. ■

In fact, there are only 29 cyclotomic extensions of $\mathbb{Q}$ with class number one. 12 are known to be norm-Euclidean. Theorem C completes the classification of these fields in terms of the Euclidean property. In Table 1, *Yes* indicates that the field is norm-Euclidean, *No* indicates that it is not norm-Euclidean [15]. Notice that we now have an example of a cyclotomic field ($\mathbb{Q}(\zeta_{32})$) that is Euclidean, but is not norm-Euclidean.

8 Acknowledgements

This paper is a summary of my doctoral research. I would like to gratefully acknowledge the support of NSERC, the J. W. McConnell Foundation, CICMA, and the CRM during this period. I would like to thank M. Ram Murty for his extraordinary encouragement, guidance and support. I would also like to thank the referee for helpful comments and suggestions.

References

[1] E. Bombieri, J. B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large modulii.* Acta Math. **156**(1986), 203–251, MR 88b:11058.
[2] David A. Clark, *The Euclidean algorithm for Galois extensions of the rational numbers.* Ph.D. thesis, McGill University, Montreal, 1992.
[3] David A. Clark and M. Ram Murty, *The Euclidean algorithm for Galois extensions of* $\mathbb{Q}$. J. Reine Angew. Math. **459**(1995), 151–162, MR 96h:11104.
[4] Étienne Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat.* Invent. Math. **79**(1985), 383–407, MR 86g:11052.
[5] Rajiv Gupta and M. Ram Murty, *A remark on Artin's conjecture.* Invent. Math. **78**(1984), 127–130, MR 86d:11003.
[6] Rajiv Gupta, M. Ram Murty and V. Kumar Murty, *The Euclidean algorithm for S-integers.* In: Number Theory (Montreal, June 1985), CMS Conf. Proc. **7**, Amer. Math. Soc., 1987, 189–201, MR 88h:11088.
[7] Malcolm Harper, *A family of Euclidean rings containing* $\mathbb{Z}[\sqrt{14}]$. CMS talk, December 1998.
[8] ———, *A proof that* $\mathbb{Z}[\sqrt{14}]$ *is Euclidean.* Ph.D. thesis, McGill University, Montreal, 2000.
[9] Malcolm Harper and M. Ram Murty, *Euclidean rings of algebraic integers.* Canad. J. Math. **56**(2004), 71–76.
[10] D. R. Heath-Brown, *Artin's conjecture for primitive roots.* Quart. J. Math. Oxford Ser. (2) **37**(1986), 27–38, MR 88a:11004.
[11] Christopher Hooley, *On Artin's conjecture.* J. Reine Angew. Math. **225**(1967), 209–220, MR 34 #7445.
[12] Henryk Iwaniec, *A new form of the error term in the linear sieve.* Acta Arith. **37**(1980), 307–320, MR 82d:10069.
[13] Hendrik W. Lenstra, Jr., *Euclid's algorithm in cyclotomic fields.* J. London Math. Soc. (2) **10**(1975), 457–465, MR 52 #8100.
[14] ———, *Quelques exemples d'anneaux euclidiens*. C. R. Acad. Sci. Paris Sér. D **286**(1978), 683–685.
[15] ———, *Euclidean number fields I.* Math. Intelligencer **2**(1979), 6–15, MR 81b:12002.
[16] Th. Motzkin, *The Euclidean algorithm.* Bull. Amer. Math. Soc. **55**(1949), 1142–1146.
[17] T. Ojala, *Euclid's algorithm in the cyclotomic field* $\mathbb{Q}(\zeta_{16})$. Math. Comp. **31**(1977), 268–273, MR 54 #10194.

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press

[18] Pierre Samuel, *About Euclidean rings.* J. Algebra **19**(1971), 282–301, MR 43 #6190.
[19] Peter J. Weinberger, *On Euclidean rings of algebraic integers.* In: Analytic Number Theory (St. Louis, 1972), Proc. Sympos. Pure Math. **XXIV**, Amer. Math. Soc., 1973, 321–332, MR 49 #2671.
[20] Robin J. Wilson, *The large sieve in algebraic number fields.* Mathematika **16**(1969), 189–204, MR 41 #8374.

Champlain College
St. Lambert, Québec
J4P 3P2
email: malcolmharper@sympatico.ca

https://doi.org/10.4153/CJM-2004-003-9 Published online by Cambridge University Press