*Functiones et Approximatio*
*XXXV (2006), 249–259*

# PRIME NUMBERS IN CERTAIN ARITHMETIC PROGRESSIONS

M. Ram Murty[1] & Nithum Thain[2]

Dedicated to Professor Eduard Wirsing
on the occasion of his 75th birthday

**Abstract:** We discuss to what extent Euclid's elementary proof of the infinitude of primes can be modified so as to show infinitude of primes in arithmetic progressions (Dirichlet's theorem). Murty had shown earlier that such proofs can exist if and only if the residue class (mod $k$) has order 1 or 2. After reviewing this work, we consider generalizations of this question to algebraic number fields.
**Keywords:** Dirichlet's theorem, prime divisors of polynomials, Chebotarev density theorem.

## 1. Introduction

Around 300 B.C., Euclid proved that there are an infinite number of prime numbers. The proof is classical and we explain it to high school students. Suppose that there are only finitely many, $p_1, p_2, \ldots, p_k$ say, then the number $p_1 p_2 \cdots p_k + 1$ is not divisible by any of $p_1, p_2, \ldots, p_k$ and hence must either be prime or divisible by a prime not in our list. This contradiction forces an infinitude of prime numbers, provided there is at least one.

To what extent can this ancient proof be generalized? In 1837, Dirichlet succeeded in showing that for any $l$ and $k$ satisfying $(l, k) = 1$, there are infinitely many primes $p$ such that $p \equiv l \pmod{k}$. But his approach was by means of $L$-functions and analysis. Our question asks how far Euclid's proof can be pushed to yield Dirichlet's theorem. The existence of such a "Euclidean proof" (to be made precise later) for certain arithmetic progressions is well-known. For example, using properties of the cyclotomic polynomial, it is possible to give a "Euclidean proof" for the infinitude of primes $\equiv 1 \pmod{k}$, for any integer $k$. Such a proof exists for other progressions as well. The progressions $3 \pmod 4$ and $5 \pmod 6$ are treated in Hardy and Wright [5]. Bateman and Low [2] give such a proof for every coprime residue class $(\text{mod } 24)$. In order to characterize the arithmetic progressions for which such a proof exists, Murty proved in [7]:

---

**2001 Mathematics Subject Classification:** 11A41, 11C08, 11R04, 11R18.
[1] Research partially supported by NSERC grant.
[2] Research partially supported by NSERC Undergraduate Student Research Award.

**Theorem 1. (Murty)** *A "Euclidean proof" exists for the arithmetic progression $l \pmod k$ if and only if $l^2 \equiv 1 \pmod k$.*

In other words, it is impossible to prove Dirichlet's theorem for certain arithmetic progressions by Euclid's method.

However, the paper was published in the Journal of Madras University and is difficult to obtain. We present this paper in order to make these ideas more accessible and to present a recent generalization of these results to abelian number fields.

Our first goal is to give a precise definition of a Euclidean proof and then to give such a proof of the infinitude of primes in progressions $l \pmod k$ satisfying $l^2 \equiv 1 \pmod k$, provided at least one such prime exists. Such a proof already exists in an old paper of I. Schur [10] and we review it in Section 2. In Section 3, we deal with the converse problem. Generalizations to algebraic number fields are discussed in Section 4. The main tool will be the Chebotarev density theorem which will show that the class of polynomials we need for a Euclidean proof does not exist unless $l^2 \equiv 1 \pmod k$.

## 2. Euclidean proof

Consider the "Euclidean proof" for the arithmetic progression $\equiv 1 \pmod 4$. Suppose that there are only finitely many: $p_1, \ldots, p_k$ (say). Consider the polynomial $f(x) = 4x^2+1$ and form the number $f(p_1 \cdots p_k) = 4(p_1 \cdots p_k)^2+1$. If $q$ is a prime divisor of this number, then $-1$ is a quadratic residue mod $q$. Hence $q \equiv 1 \pmod 4$. Thus either $f(p_1 \cdots p_k)$ is a prime $\equiv 1 \pmod 4$ or is divisible by a prime $q \equiv 1 \pmod 4$ not in the list $p_1, \ldots, p_k$. This gives us an infinitude of such primes provided we have one. Since $5 \equiv 1 \pmod 4$, we have a proof for this progression.

A similar proof exists for $3 \pmod 4$. In this case, we use the polynomial $g(x) = 4x-1$. If there are only finitely many such primes $\equiv 3 \pmod 4$, $p_1, \ldots, p_k$ say, then $g(p_1 \cdots p_k) = 4(p_1 \cdots p_k) - 1$ has prime factors $\equiv 1$ or $3 \pmod 4$ since it is odd. It cannot have all of its prime factors $\equiv 1 \pmod 4$ for otherwise the number would be $\equiv 1 \pmod 4$ which is not the case. Hence, it has at least one prime factor $\equiv 3 \pmod 4$ which is not in our list. This again proves an infinitude provided there is at least one.

A characteristic feature of both these proofs is the assertion of the existence of a polynomial whose values at integer arguments are divisible by primes in the required progression. In one case, namely $f(x) = 4x^2 + 1$, all values at integer arguments are only divisible by primes $\equiv 1 \pmod 4$. In the second case, $g(x) = 4x - 1$, each value at an integer argument is divisible by at least one prime $\equiv 3 \pmod 4$. In either case, a polynomial $\in \mathbb{Z}[x]$ exists such that in the set of prime divisors of the polynomial values at integer arguments, there are infinitely many primes in the desired arithmetic progression. Accordingly, we shall say that a prime $p$ is a **prime divisor** of polynomial $f \in \mathbb{Z}[x]$ if $p \mid f(n)$ for some $n \in \mathbb{Z}$. Thus the first requirement of a "Euclidean proof" for the arithmetic progression $l \pmod k$ is the existence of a polynomial with infinitely many prime divisors $\equiv l \pmod k$.

It is not at first clear that a polynomial has infinitely many prime divisors. This is not difficult to establish and was done by Schur ([10], p.41). Since the proof is in the spirit of Euclid, we give it.

**Theorem 2. (Schur)** *If $f \in \mathbb{Z}[x]$ is non-constant, then $f$ has infinitely many prime divisors.*

**Proof.** We may suppose $f(0) = c \neq 0$. Now, $f(x) = \pm 1$ has only finitely many solutions, so $f$ must have at least one prime divisor. Suppose $f$ only has a finite number of prime divisors $p_1, p_2, ..., p_k$. Let $Q = p_1 p_2 ... p_k$. Then $f(Qcx) = cg(x)$ for some polynomial $g \in \mathbb{Z}[x]$ of the form $1 + c_1 x + c_2 x^2 + ...$ with $Q \mid c_i$ for each $i$. Note that $g$ must have a prime divisor, $p$, by the argument above. Then $p \mid g$ implies that $p \mid f$. But $p \nmid Q$ (for otherwise, $p \mid 1$). This is a contradiction. So $f$ has infinitely many prime divisors. ∎

We shall denote by $P(f)$ the set of prime divisors of $f$. Thus, Schur's theorem says that $P(f)$ is infinite. On the other hand, if $f$ is irreducible and of degree at least 2, then there are infinitely many primes which are not divisors of $f$. This is a consequence of the Chebotarev density theorem which will be alluded to in Section 3.

The next constraint imposed on our hypothetical "Euclidean polynomial" arises from a theorem of Nagell [9]. We give a direct field theoretic proof. A longer, but more elementary proof, was given by Nagell [9].

**Theorem 3. (Nagell)** *If $f, g \in \mathbb{Z}[x]$ are non-constant, then $P(f) \cap P(g)$ is infinite.*

**Proof.** Suppose $\alpha$ is a root of $f$ and $\beta$ is a root of $g$. By Dedekind's theorem (see [8], p. 65), except for a finite number of exceptions, $p$ is a prime divisor of $f$ exactly when $p$ has a first degree prime ideal factor in the field $\mathbb{Q}(\alpha)$. A similar statement holds for $g$. Consider the field, $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$ for some $\theta \in \mathcal{O}_K$. If $h$ is the minimal polynomial of $\theta$ then Schur's Theorem assures us that there are infinitely many primes which have a first degree prime ideal factor in $\mathbb{Q}(\alpha, \beta)$. These primes thus have a first degree prime ideal factor in both $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$. Thus, except for a finite number of exceptions, these primes are in both $P(f)$ and $P(g)$. ∎

This theorem has a remarkable consequence. It is well known (see Theorem 4 and 5 below) that the prime divisors of the $k$-th cyclotomic polynomial consist of the prime divisors of $k$ and primes $p \equiv 1 \pmod{k}$. It follows from the theorem of Nagell that any polynomial has infinitely many prime divisors $\equiv 1 \pmod{k}$ for any integer $k$. This forces our "Euclidean polynomial" to have such prime divisors. Thus the most reasonable definition of a **Euclidean proof** for the arithmetic progression $l \pmod{k}$ is the existence of a polynomial $f \in \mathbb{Z}[x]$ such that all prime divisors of $f$ (apart from finitely many) are either $\equiv 1 \pmod{k}$ or $l \pmod{k}$. We may also suppose that this polynomial is irreducible.

We now begin to give a Euclidean proof for every progression $l \pmod{k}$ satisfying $l^2 \equiv 1 \pmod{k}$.

Let $\zeta$ be a primitive $k$-th root of unity. The field $K := \mathbb{Q}(\zeta)$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to the group of coprime residue classes modulo $k$, which we denote by $(\mathbb{Z}/k\mathbb{Z})^*$.

**Theorem 4. (Schur)** *Let $H$ be a subgroup of $(\mathbb{Z}/k\mathbb{Z})^*$. Then there is an irreducible polynomial $f$ so that all of the prime divisors of $f$, with a finite number of exceptions, belong to the residue classes of $H$.*

**Proof.** Let $\mathbb{Q}(\eta)$ be the fixed field of $H$, where $\eta = h(\zeta)$ for some $h \in \mathbb{Z}[x]$. Let $m_1, ..., m_s$ be coset representatives of $H$ in $(\mathbb{Z}/k\mathbb{Z})^*$.
Set $\eta_i = h(\zeta^{m_i})$, $1 \leqslant i \leqslant s$. Suppose these are not distinct. Let $\sigma_i$ denote the automorphism of $\mathbb{Q}(\zeta)/\mathbb{Q}$ sending $\zeta$ to $\zeta^i$. Then $\sigma_{m_i}(\eta) = \sigma_{m_j}(\eta)$ for some distinct coset representatives $m_i, m_j$ of $H$. But then $\sigma_{m_i m_j^{-1}}(\eta) = \eta$, so $\sigma_{m_i m_j^{-1}}$ fixes $\mathbb{Q}(\eta)$ which implies that $m_i$ and $m_j$ are in the same coset of $H$. A contradiction. Thus $\eta_i = h(\zeta^{m_i})$, $1 \leqslant i \leqslant s$ are the distinct conjugates of $\eta$.
Now, we define

$$f(x) := \prod_{i=1}^{s}(x - \eta_i).$$

By the above, $f(x)$ is an irreducible polynomial in $\mathbb{Q}(x)$. We will show that $f$ satisfies the condition in the theorem. Let $p$ be a prime divisor of $f$ so that $p \nmid k$ and so that $p \nmid D(f)$ (where $D(f)$ is the discriminant of $f$). Note that we have only excluded finitely many primes. Now, since $p$ is a prime divisor of $f$, there exists a rational integer $a$ so that

$$f(a) = \prod_{i=1}^{s}(a - \eta_i) \equiv 0 \pmod{p}.$$

Let $\mathfrak{p}$ be any prime ideal dividing $(p)$. Then $\mathfrak{p} \mid (a - \eta_i)$ for some $i$. Now, $a^p \equiv a \pmod{p}$ so $a^p \equiv a \pmod{\mathfrak{p}}$. Also, $h(x)^p \equiv h(x^p) \pmod{\mathfrak{p}}$ for the same reason. Thus, we get the following congruence:

$$h(\zeta^{m_i}) \equiv \eta_i \equiv a \equiv a^p \equiv \eta_i^p \equiv h(\zeta^{m_i})^p \equiv h(\zeta^{pm_i}) \pmod{\mathfrak{p}}.$$

In particular, we see that $\mathfrak{p} \mid (h(\zeta^{m_i}) - h(\zeta^{pm_i}))$. Now, since $p \nmid k$, we have that $pm_i$ is coprime to $k$, so $h(\zeta^{pm_i})$ is one of $\eta_1, \ldots, \eta_s$. Suppose $h(\zeta^{pm_i}) \neq h(\zeta^{m_i})$. Then $\mathfrak{p} \mid D(f)$ and since $D(f)$ is a rational integer, $p \mid D(f)$. But this contradicts our choice of $p$.
Thus, $h(\zeta^{pm_i}) = h(\zeta^{m_i})$ and so $\eta_i$ is fixed by the automorphism $\sigma_p$. So $\mathbb{Q}(\eta_i)$ is fixed by $\sigma_p$. But, by the above remarks $\mathbb{Q}(\eta_i)$ is a Galois extension, and consequently $\mathbb{Q}(\eta_i) = \mathbb{Q}(\eta)$. Thus $\sigma_p$ fixes $\mathbb{Q}(\eta)$ and so $p$ belongs to a residue class of $H$. ■

The following is a converse of Theorem 4.

**Theorem 5. (Schur)** *If $f$ is as in Theorem 4, then any prime belonging to any residue class of $H$ divides $f$.*

**Proof.** Let $p$ be a prime belonging to some residue class of $H$. Since $p \in H$, $\sigma_p$ leaves $\mathbb{Q}(\eta)$ fixed. In particular,

$$\eta^p \equiv h(\zeta)^p \equiv h(\zeta^p) \equiv h(\zeta) \equiv \eta \pmod{p}.$$

So for any prime ideal $\mathfrak{p}$ dividing $p$, we have $\eta^p \equiv \eta \pmod{\mathfrak{p}}$. Since, $\mathcal{O}_K$ is a Dedekind domain, $\mathcal{O}_K/\mathfrak{p}$ is a field and so there are at most $p$ solutions to $x^p - x$ in this field. From this it follows that $\eta \equiv a \pmod{\mathfrak{p}}$ for some rational integer $a$. Thus, $\mathfrak{p} \mid f(a)$ and since $f(a)$ is a rational integer it follows that $p \mid f(a)$, as desired. ■

**Corollary 1.** *If $\phi_k$ is the $k$-th cyclotomic polynomial, then all of the prime divisors of $\phi_k$ are $\equiv 1$ (mod $k$) or divide $k$.*

**Proof.** This result follows from setting $H = \{1\}$ in the above theorem. We use the basic fact, from algebraic number theory, that the only primes which divide the discriminant of $\phi_k$ are those primes which divide $k$ (see [8], p.52). ■

Note that there are only finitely many primes which divide $k$. So all of the prime divisors of $\phi_k$ with the exception of finitely many are $\equiv 1 \pmod{k}$. This, in conjunction with Theorem 1 tell us that there are infinitely many primes $\equiv 1 \pmod{k}$ for any positive integer $k$.

**Theorem 6.** *If $l^2 \equiv 1$ (mod $k$) then there are infinitely many prime $\equiv l$ (mod $k$), provided there is at least one.*

**Proof.** The case $l \equiv 1 \pmod{k}$ is dealt with in the discussion following Corollary 1. Thus, we may suppose that $l$ is not congruent to 1 $\pmod{k}$.
We can thus apply the above theorems to the subgroup $H = \{1, l\}$ of $(\mathbb{Z}/k\mathbb{Z})^*$. Suppose $L$ is the fixed field of $H$. Now, set $h(\zeta) = (u - \zeta)(u - \zeta^l)$ for some rational integer $u$, to be chosen later. First note that if $m_1, \ldots, m_s$ denote the coset representatives of $H$ in $(\mathbb{Z}/k\mathbb{Z})^*$, and if we pick $u$ so that the $h(\zeta^{m_i})$ are distinct for $i = 1, \ldots, s$ then $L = \mathbb{Q}(h(\zeta))$. Note that we have only excluded a finite set of values for $u$. Applying Theorem 3 to $H$ with $\eta = h(\zeta)$ gives us a polynomial $f(x)$ all of whose prime divisors (apart from finitely many) are $\equiv 1$ or $l \pmod{k}$. We may write down $f$ explicitly:

$$f(x)^2 = \prod_{(a,k)=1} (x - (u - \zeta^a)(u - \zeta^{la})).$$

Now, note that $f(0) = \phi_k(u)$ where $\phi_k$ is the $k$-th cyclotomic polynomial. We now choose $u$ to be a non-zero multiple of $k$ so that $f(0) = \phi_k(u) \equiv 1 \pmod{k}$.

By Corollary 1, every prime divisor of $\phi_k$ either divides $k$ or is $\equiv 1 \pmod{k}$. Thus, every prime divisor of $\phi_k(u) = f(0)$ is $\equiv 1 \pmod{k}$.

Now pick some prime $p \equiv l \pmod{k}$ so that $p$ does not divide the discriminant of $f$. By Theorem 4, we may find some $b$ so that $p \mid f(b)$. In fact, we can choose $b$ so that $p^2 \nmid f(b)$. Note that if $p^2 \mid f(b)$, then $f(b+p) = f(b) + pf'(b) \equiv pf'(b) \pmod{p^2}$. But since $p \nmid D(f)$, we have that $f$ has no double roots mod $p$ and so $f'(b) \neq 0 \pmod{p}$. So, $f(b) \equiv 0 \pmod{p^2}$ implies that $f(b+p) \neq 0 \pmod{p^2}$. Thus, replacing $b$ with $b+p$ if necessary, we can choose $b$ so that $p \mid f(b)$ but $p^2 \nmid f(b)$.

Now suppose there are finitely many primes $\equiv l \pmod{k}$ call them $p = p_1, p_2, p_3, \ldots, p_m$. Also let $q_1, \ldots, q_t$ be the prime divisors of $D(f)$. Let $Q = p_2 p_3 \ldots p_m q_1 \ldots q_t$. By the Chinese Remainder Theorem find $c$ so that:

$$c \equiv b \pmod{p^2}$$
$$c \equiv 0 \pmod{kQ}$$

Thus $f(c) \equiv f(b) \pmod{p^2}$ and $f(c) \equiv f(0) \pmod{kQ}$. Now, by Theorem 3 the only prime divisors of $f$ are those primes which divide $k$, divide the discriminant of $f$, or are $\equiv 1$ or $l \pmod{k}$. Since $f(0)$ is only divisible by those primes $\equiv 1 \pmod{k}$ it follows that $f(c)$ is only divisible by those primes $\equiv 1 \pmod{k}$ and $p \equiv l \pmod{k}$. Since $p^2 \nmid f(c)$, it follows that $f(c) \equiv l \pmod{k}$. But $f(c) \equiv f(0) \equiv 1 \pmod{k}$. Contradiction. Thus there must be infinitely many primes $\equiv l \pmod{k}$. ∎

We can utilize these theorems to construct Euclidean proofs for new arithmetic progressions, hitherto unconsidered by these methods. For example, such a proof should exist for primes $\equiv 4 \pmod{15}$. By the methods of the above proof, consider the polynomial

$$f(x) = (x - (\zeta + \zeta^4))(x - (\zeta^2 + \zeta^8))(x - (\zeta^7 + \zeta^{13}))(x - (\zeta^{11} + \zeta^{14}))$$

where $\zeta$ denotes a primitive 15-th root of unity. Simplifying the above gives

$$f(x) = x^4 - x^3 + 2x^2 + 1.$$

Writing $f$ as

$$f(x) = (x^2 - x/2 - 1)^2 + 15x^2/4,$$

we note that -15 is a quadratic residue for every prime divisor of $f$ which is unequal to 3 or 5. By quadratic reciprocity, this means that

$$\left(\frac{p}{3}\right)\left(\frac{p}{5}\right) = 1.$$

Thus, $p \equiv 1, 2, 4,$ or $8 \pmod{15}$. Also, by writing

$$f(x) = (-x^2 + x/2 - 1/2)^2 + 3(x+1)^2/4,$$

we deduce that any prime divisor of $f$ satisfies $\left(\frac{-3}{p}\right) = -1$ which implies $p \equiv 1$ or $11 \pmod{12}$. Similarly,

$$f(x) = (-x^2 + x/2 - 3/2)^2 - 5(x-1)^2/4$$

implies $\left(\frac{5}{p}\right) = 1$ so that $p \equiv 1$ or $4 \pmod{5}$. Putting all this together, we deduce that any prime divisor of $f$ is either $\equiv 1$ or $4 \pmod{15}$. Clearly the polynomial $f(15x+1)$ also has its prime divisors $\equiv 1$ or $4 \pmod{15}$. Since $f(15x+1) = 15xg(x) + 4$, not all prime divisors of $f(15x+1)$ are $\equiv 1 \pmod{15}$. If the primes $\equiv 4 \pmod{15}$ were finite, then let $Q$ denote their product and consider $f(15Q+1) = 15Qg(Q) + 4$. This has no prime divisor $\equiv 4 \pmod{15}$ as it is coprime to $Q$. But this is a clear contradiction. This completes the proof.

## 3. The converse problem

Suppose that we are given a polynomial $\in \mathbb{Z}[x]$ such that all its prime divisors (with finitely many exceptions) are either $\equiv 1$ or $l \pmod{k}$. We would like to show that this implies that $l^2 \equiv 1 \pmod{k}$. We prove:

**Theorem 7. (Murty)** *Let $f \in \mathbb{Z}[x]$. Suppose that with finitely many exceptions, all prime divisors of $f$ are either $\equiv 1$ or $l \pmod{k}$. Then $l^2 \equiv 1 \pmod{k}$.*

**Proof.** A classical theorem of Bauer [1] states that if $H$ is normal over $\mathbb{Q}$ and every prime which has a first degree prime ideal factor in $K$ splits completely in $H$ then $H \subset K$. We apply this to our situation. Let $K$ be the field obtained from $\mathbb{Q}$ by adjoining a root of $f$. Let $L$ denote the compositum of $\mathbb{Q}(\zeta)$ and $K$, where $\zeta$ is a $k$-th root of unity. Then $L/K$ is Galois, as $L$ is the splitting field of the cyclotomic polynomial over $K$. Let $H_l$ denote the subfield of $\mathbb{Q}(\zeta)$ left fixed by $(l)$. By the theorem of Bauer cited above, it follows that $H_l \subset K$. Moreover, $\mathbb{Q}(\zeta) \cap K = H_l$ because $K$ has, by hypothesis infinitely many prime ideals of degree one whose norms are $\equiv l \pmod{k}$. Then, $\mathrm{Gal}(L/K)$ injects into $\mathrm{Gal}(\mathbb{Q}(\zeta)/H_l)$ because any automorphism of $L/K$ which when restricted to $\mathbb{Q}(\zeta)$ is trivial, is also trivial on $Q$ and hence on $H_l$. Moreover, this map is surjective since there are infinitely many prime ideals of degree one in $K$ which when restricted to $\mathbb{Q}(\zeta)$ reduce to $\sigma_l$, the automorphism which has the property $\sigma(\zeta) = \zeta^l$. Hence, in our case, $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/H_l)$.

By the Chebotarev density theorem [11], there are infinitely many prime ideals of $K$ of degree one whose Frobenius automorphism is any given conjugacy class of our Galois group. By the surjectivity established above, it follows that there are infinitely many prime ideals of $K$ of degree one whose Frobenius automorphism restricts to any given element of $(l)$. In particular, there are infinitely many prime divisors of $f$ which are $\equiv l^2 \pmod{k}$. This forces $l^2 \equiv 1$ or $l \pmod{k}$. Hence, $l^2 \equiv 1 \pmod{k}$ since $(l,k) = 1$. ∎

Thus, philosophically, Dirichlet's theorem in its entirety cannot be proved by "Euclidean" methods. This fact was first proved by the author in [6] over ten

years ago but subject to the additional hypothesis that we consider only abelian polynomials. Subsequently, this hypothesis was weakened to allow normal polynomials. But even this last restriction has been removed and now the theorem stands in its complete aesthetic form.

The methods of the paper can be generalized. One can prove in a similar spirit the following.

**Theorem 8.** *Let $H$ be a subgroup of $(\mathbb{Z}/k\mathbb{Z})^*$. There is a polynomial $\in \mathbb{Z}[x]$ such that it has infinitely many prime divisors belonging to a non-trivial residue class of $H$.*

## 4. Generalizations

Let $K/k$ be abelian with Galois group $G$. Let $\sigma \in G$. Then a very weak form of the Chebotarev density theorem is the statement that there exist infinitely many prime ideals $\wp \subset k$ so that $\mathfrak{p}$ has Frobenius element $\sigma$ for each $\mathfrak{p}$ lying above $\wp$. We can generalize the methods of Section 2 to give a Euclidean proof of this statement for any $\sigma$ of order 2. The work of K. Conrad [3] generalizes the theorem of Murty in Section 3 and shows that no Euclidean proof is possible if the order of $\sigma$ is not 2.

We generalize the idea of a prime divisor and a Euclidean proof in the natural way. We call a prime ideal $\wp \subset k$ a **prime divisor** of a polynomial $f$ if $\wp \mid f(a)$ for some $a \in O_k$. Likewise, a **Euclidean proof** for $\sigma \in \mathrm{Gal}(K/k)$ is the existence of a polynomial $f \in O_k[x]$ so that all of the prime divisors of $f$ (apart from finitely many) have Frobenius element either 1 or $\sigma$. With these definitions in hand, we proceed to show that a Euclidean proof exists if $\sigma$ has order 2.

**Theorem 9.** *Let $k \subset K$ be algebraic number fields, where $K$ is a Galois extension of $k$. Let $H$ be a subgroup of $Gal(K/k)$. Then there exists an irreducible polynomial $f(x) \in O_k[x]$ such that all (but finitely many) of the prime divisors, $\wp$, of $f$ have $Frob(\mathfrak{p}) \in \langle H \rangle$ for all primes $\mathfrak{p}$ lying above $\wp$.*

**Proof.** We suppose that $K = k(\alpha)$. Now, if we let $L$ be the fixed field of $H$, then $L = k[\eta]$ where $\eta = h(\alpha)$ for some polynomial $h \in k[x]$. Let $\sigma_1, ..., \sigma_s$ be the coset representatives of $H$ in $\mathrm{Gal}(K/k)$. Set $\eta_i = \sigma_i(\eta) = h(\sigma_i(\alpha))$ for each $1 \leqslant i \leqslant s$.

Suppose $\eta_i = \eta_j$ for $i \neq j$. Then $\sigma_j^{-1}\sigma_i$ fixes $\eta$ and so $\sigma_j$ and $\sigma_i$ are in the same coset of $H$, which is a contradiction. Thus the $\eta_i$ are the distinct conjugates of $\eta$.

It follows that the minimal polynomial of $\eta$ is

$$f(x) = \prod_{i=1}^{s}(x - \eta_i).$$

By the above, $f(x)$ is irreducible in $k[x]$. We will show that $f$ satisfies the conditions of the theorem.

Let $\wp$ be a prime divisor of $f$ so that $\wp$ does not ramify and so that $\wp \nmid D(f)$, the discriminant of $f$. We have only excluded a finite set of primes. Since $\wp$ is a prime divisor of $f$, there exists an $a \in O_k$ such that $f(a) = \prod(a - \eta_i) \equiv 0 \pmod{\wp}$. Let $\mathfrak{p}$ be any prime ideal of $O_K$ dividing $\wp$. Then $\mathfrak{p}$ divides $(a - \eta_i)$ for some $i$. If $\psi$ is the Frobenius automorphism of $\mathfrak{p}$, we have $\psi(a) \equiv a \pmod{\wp}$ so $\psi(a) \equiv a \pmod{\mathfrak{p}}$.

From this simple identity, we get:

$$\psi(a) \equiv \psi(\eta_i) \equiv h(\psi \circ \sigma_i(\alpha)) \equiv a \equiv \eta_i \equiv h(\sigma_i(\alpha)) \pmod{\mathfrak{p}}.$$

In particular, $h(\sigma_i(\alpha)) \equiv h(\psi \circ \sigma_i(\alpha)) \pmod{\mathfrak{p}}$. Now, $h(\psi \circ \sigma_i(\alpha)) = \psi(\eta_i) = \eta_j = h(\sigma_j(\alpha))$ for some $j$. If $j \neq i$, then $\mathfrak{p} \mid D(f)$. Since $D(f) \in k$ this would mean that $\wp \mid D(f)$, contradicting our choice of $\wp$. Thus $j = i$ and so $\psi(\eta_i) = \eta_i$. Thus $\psi$ fixes a conjugate field of $k(\eta)$ and so $\psi \in \langle H \rangle$. ■

**Theorem 10.** *For $f$ as in the theorem above, if $\wp$ is a prime with $Frob(\mathfrak{p}) \in \langle H \rangle$ for some $\mathfrak{p}$ lying above $\wp$ then $\wp$ divides $f$.*

**Proof.** Let $\psi$ be the Frobenius element of $\mathfrak{p}$. Then $\psi$ fixes $k(\eta_i)$ for some $i$. In particular, $\psi(\eta_i) = \eta_i$. Thus

$$\eta_i^{Norm_{K/k}(\wp)} \equiv \eta_i \pmod{\mathfrak{p}}.$$

Since $O_K/\mathfrak{p}$ is a field, the equation $x^{Norm_{K/k}(\wp)} \equiv x \pmod{\mathfrak{p}}$ has at most $Norm_{K/k}(\wp)$ distinct solutions. Notice that the elements of $O_k$ already provide us with this many solutions. Thus $\eta_i \equiv a \pmod{\mathfrak{p}}$ for some $a \in O_k$. So, $\mathfrak{p} \mid f(a)$ and since $f(a) \in k$ we have $\wp \mid f(a)$ as required. ■

**Corollary 2.** *If $\phi$ is the minimum polynomial of $\alpha$ then the prime divisors of $\phi$ either divide $d_{K/k}$ or have Frobenius element 1.*

**Proof.** Set $H = 1$ in the theorem above, and note that $\wp$ divides $d_{K/k} = D(f)$ if and only if it ramifies. ■

**Theorem 11.** *Let $k \subset K$ be algebraic number fields where $K$ is an abelian extension of $k$. Choose any $\sigma \in Gal(K/k)$ of order 2. Then there are infinitely many prime ideals in $O_k$ with Frobenius element $\sigma$, provided there is at least 1 not dividing $D(f)$.*

**Proof.** Let $\mathfrak{c}$ be a conductor of $K/k$ whose only prime divisors are ramified primes and let $\mathfrak{c}_0$ be its finite part. Let $K = k(\alpha)$. We may suppose that $Norm_{K/k}(\alpha) \equiv 1 \pmod{\mathfrak{c}_0}$ and $Norm_{K/k}(\alpha) \equiv 1 \pmod{d_{K/k}}$. Indeed, if $\alpha$ generates $K$ then so does $x\alpha + y$ for any non-zero $x$ and any $y$ in $k$. Thus choosing $x \in d_{K/k}\mathfrak{c}_0$ and $y = 1$ guarantees the above conditions.

Now we apply the above two theorems to the subgroup $H = \{1, \sigma\}$ of $\mathrm{Gal}(K/k)$. Suppose $L$ is the fixed field of $H$. We set $h(\alpha) = (u - \alpha)(u - \sigma(\alpha))$ for $u \in O_k$, to be chosen later. If $\sigma_1, \ldots, \sigma_s$ denote the coset representatives of $H$ in $\mathrm{Gal}(K/k)$, and if we pick $u$ so that the $h(\sigma_i(\alpha))$ are distinct, then $h(\alpha)$ generates $L$. We have only discarded a finite set of $u$.

Thus, the above theorems give us a polynomial $f(x)$ all (but finitely many) of whose prime divisors have Frobenius element 1 or $\sigma$. In fact, our choice of $h(\alpha)$ ensures that $f(0) = \phi(u)$ (where $\phi$ is the minimal polynomial of $\alpha$). So, by the corollary above, we have that every prime divisor of $f(0)$ has Frobenius element 1 or divides $d_{K/k}$. If we choose $u \in d_{K/k}$, then $f(0) \equiv Norm_{K/k}(\alpha) \equiv 1 \pmod{d_{K/k}}$. Thus, the only prime divisors of $f(0)$ will have Frobenius element 1.

Now pick some prime $\wp$ with Frobenius element $\sigma$ so that $\wp$ does not divide $D(f)$. By Theorem 10 we may find a $b \in O_k$ so that $\wp \mid f(b)$. In fact, we can choose $b$ so that $\wp^2 \nmid f(b)$. Indeed, if $\wp^2 \mid b$ choose some $l \in \wp$ so that $l \notin \wp^2$. Then $f(l+b) \equiv f(b) + lf'(b) \equiv lf'(b) \pmod{\wp^2}$. Since $\wp \nmid D(f)$ and $\wp \mid f(b)$, we have that $\wp \nmid f'(b)$. Thus $\wp \mid f(l+b)$ but $\wp^2 \nmid f(l+b)$. Thus we may replace $b$ with $l+b$ if necessary to ensure that $\wp \mid f(b)$ and $\wp^2 \nmid f(b)$.

Now suppose that there are only finitely many primes with Frobenius element $\sigma$, call them $\wp = \wp_1, \wp_2, \ldots, \wp_m$. By the Chinese remainder theorem, we may find $c \in O_k$ so that:

$$c \equiv b \pmod{\wp^2}$$
$$c \equiv 0 \pmod{\wp_2\wp_3 \ldots \wp_m D(f)\mathfrak{c}_0}$$

Thus, $f(c) \equiv f(b) \pmod{\wp^2}$ and $f(c) \equiv f(0) \pmod{\wp_2\wp_3 \ldots \wp_m D(f)\mathfrak{c}_0}$. Now, by Theorem 9 the only prime divisors of $f$ are those which divide $d_{K/k}$ or $D(f)$ or have Frobenius element in $H$. Since $f(0)$ is only divisible by those primes with Frobenius element 1, the congruence conditions guarantee that $f(c)$ is divisible only by those primes with Frobenius element 1 and $\wp$ but not $\wp^2$. Thus $f(c)$ has Frobenius element $\sigma$. But $f(c) \equiv 1 \pmod{\mathfrak{c}_0}$. Replacing $c$ with $c+n$ if necessary (where $n \in \mathbb{Z} \cap \wp^2\wp_2\wp_3 \ldots \wp_m D(f)\mathfrak{c}_0$), we ensure that $f(c) \equiv 1 \pmod{*\ \mathfrak{c}}$. And so $f(c)$ has Frobenius element 1. Contradiction. ∎

The converse problem is tackled by K. Conrad in [3]. Suppose $K/k$ is an abelian extension and let $f \in O_k[x]$. Set $S = \{\sigma \mid \sigma$ is the Frobenius element of $\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ in $K$ dividing $f\}$. In his paper, Conrad proves that $S$ is a group. Thus if $f$ is a polynomial arising from a Euclidean proof for $\sigma \in \mathrm{Gal}(K/k)$, then $S = \{1, \sigma\}$ is a group. Thus $\sigma$ must have order 2.

## References


[1] M. Bauer, *Zur Theorie der algebraischen Zahlkoerper*, Math. Annalen, **77** (1916), 353–356.

[2] P. Bateman and M.E. Low, *Prime numbers in arithmetic progression with difference 24*, Amer. Math. Monthly, **72** (1965), 139–143.

[3] K. Conrad, *Euclidean Proofs of Dirichlet's Theorem*, Website: http://www.math.uconn.edu/ kconrad/blurbs/dirichleteuclid.pdf.

[4] I. Gerst and J. Brillhart, *On the prime divisors of polynomials*, Amer. Math. Monthly, **78** (1971), 250–266.

[5] G.H. Hardy & E.M. Wright, *An introduction to the theory of numbers*, 4th Edition, Oxford, 1960.

[6] M.R. Murty, *On the existence of "Euclidean proofs" of Dirichlet's theorem on primes in arithmetic progressions*, B. Sc. Thesis, 1976, (unpublished) Carleton University.
[7] M.R. Murty, *Primes in Certain Arithmetic Progressions*, J. Madras Univ., Section B, **51** (1988), 161–169.
[8] M.R. Murty & J. Esmonde, *Problems in Algebraic Number Theory*, Second Edition, Graduate Texts in Mathematics **190**, (2005).
[9] T. Nagell, *Sur les diviseurs premiers des polynômes*, Acta Arith, **15** (1969), 235–244.
[10] I. Schur, *Uber die Existenz unendlich vieler Primzahlen in einiger speziellen arithmetischen Progressionen*, S-B Berlin. Math. Ges., **11** (1912), 40–50.
[11] B. Wyman, *What is a reciprocity law*, Amer. Math. Monthly, **79** (1972), 571–586.

**Addresses:** M. Ram Murty, Department of Mathematics, Jeffery Hall, 99 University Avenue, Queen's University, Kingston, Ontario, K7L 3N6, Canada;
Nithum Thain, Department of Mathematics, Jeffery Hall, 99 University Avenue, Queen's University, Kingston, Ontario, K7L 3N6, Canada
**E-mail:** murty@mast.queensu.ca; nithum@mast.queensu.ca
**Received:** 6 February 2006; **revised:** 5 May 2006