From: Journal of the Madras University, (1988) 161-169.

PRIMES IN CERTAIN ARITHMETIC PROGRESSIONS

M. Ram Murty *

§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, $p_1, p_2, ..., p_k$ say, then the number $p_1...p_k + 1$ is not divisible by any of $p_1, p_2, ..., p_k$ and hence must either be prime or divisible by a prime not in our list. This contradiction forces an infinity of prime numbers provided there is at least one.

To what extent can this ancient proof be generalised ? In 1837, Dirichlet succeeded in showing that for any ℓ and k satisfying $(\ell, k) = 1$, there are infinitely many primes p such that $p \equiv \ell(\bmod k)$. 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 $\equiv 1(\bmod k)$, for any integer k. Such proofs exist for other progressions as well. The progressions $3(\bmod 4)$ and $5(\bmod 6)$ are treated in Hardy and Wright [4]. Bateman and Low [2] give such a proof for every coprime residue class (mod 24). The purpose of this paper is to characterise the arithmetic progressions for which such a proof exists. We prove:

Theorem 1. A "Euclidean proof" exists for the arithmetic progression $\ell(\bmod k)$ if and only if $\ell^2 \equiv 1(\bmod k)$.

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

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 $\ell(\bmod k)$ satisfying $\ell^2 \equiv 1(\bmod k)$. Such a proof already exists in an old paper of I. Schur [7] and we review it in §2. In §3, we deal with the converse problem. 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 $\ell^2 \equiv 1(\bmod k)$.

* Research partially supported by NSERC grant A 9418

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

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

A characteristic feature of both of 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 $\equiv 1(\bmod 4)$. In the second case, $g(x) = 4x-1$, each value at an integer argument is divisible by at least one prime $\equiv 3(\bmod 4)$. 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 a polynomial** $f \in \mathbb{Z}[x]$ if $p|f(n)$ for some $n \in \mathbb{Z}$. Thus the first requirement of a "Euclidean proof" for the arithmetic progression $\ell(\bmod k)$ is the existence of a polynomial with infinitely many prime divisors $\equiv \ell(\bmod k)$.

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 [7, p.41]. Since the proof is in the spirit of Euclid, we give it.

Theorem 2. (I. Schur) If $f \in \mathbb{Z}[x]$ is non-constant, then its set of prime divisors is infinite.

Proof. If $f(0) = 0$, then every prime divides f. Suppose that $f(0) = c \neq 0$. Now, $f(x) = \pm 1$ has only finitely many solutions. Thus, f has at least one prime divisor as it can take on the values ± 1 only finitely many times. Suppose that the set of prime divisors

of f is finite and consists of $p_1, ..., p_k$ (say). Let $A = p_1...p_k$ and consider $f(Acx) = cg(x)$ where $g(x) = 1+c_1x+c_2x^2+... \in \mathbb{Z}[x]$ and $A|c_i$ for every i. If p is a prime divisor of g, then it must be a prime divisor of f and hence must be one of the p_i. This is a contradiction for then $p_i|1$. Therefore, the set of prime divisors of f is infinite.

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 §3.

The next constraint imposed on our hypothetical "Euclidean polynomial" arises from a theorem of Nagell [6]. We give a direct field theoretic proof. A longer, but more elementary proof, was given by Nagell [6].

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

Proof. The set of prime divisors of f are those primes p which have a first degree prime ideal factor in the field K_f obtained from $\mathbb{Q}$ by adjoining a root of f. An analogous statement holds for g. Thus, with obvious notation, if we consider the compositum K_fK_g, then the set of primes with a first degree prime ideal factor in this compositum is infinite. Such primes have a first degree prime ideal factor in both K_f and K_g, and the result follows from our initial remark.

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 $p \equiv 1(\mod k)$. It follows from the theorem of Nagell that any polynomial has infinitely many prime divisors $\equiv 1(\mod k)$ 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 $\ell(\mod k)$ is the existence of a polynomial $f \in \mathbb{Z}[x]$ such that all prime divisors of f (apart from finitely many) are either $\equiv 1(\mod k)$ or $\ell(\mod k)$. We may also suppose that this polynomial is **irreducible**.

We now begin to give a Euclidean proof for every progression $\ell(\mod k)$ satisfying $\ell^2 \equiv 1(\mod k)$.

Let ζ_k denote a primitive k-th root of unity. The field $\mathbb{Q}(\zeta_k)$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to the group of coprime residue classes $(\mod k)$ which we denote by $(\mathbb{Z}/k\mathbb{Z})^*$.

Theorem 4. Let H be a subgroup of $(\mathbb{Z}/k\mathbb{Z})^*$. There is an irreducible polynomial f such that all the prime divisors of f, with the exception of finitely many, belong to the residue classes of H.

Proof. The field left fixed by H is a subfield $\mathbb{Q}(\eta)$ of $\mathbb{Q}(\zeta_k)$, where $\eta = h(\zeta)$, $\zeta = \zeta_k$ for some $h \in \mathbb{Z}[x]$. Let $m_1, ..., m_s$ be coset representatives of H in $(\mathbb{Z}/k\mathbb{Z})^*$. Then, $\eta_i = h(\zeta^{m_i})$ for $1 \leq i \leq s$ are the distinct conjugates of η. Indeed, letting σ_i denote the automorphism of $\mathbb{Q}(\zeta_k)/\mathbb{Q}$ sending ζ_k to ζ_k^i, we would otherwise have that the two quantities

$$\sigma_{m_1}(\eta) = h(\zeta^{m_1}), \quad \sigma_{m_2}(\eta) = h(\zeta^{m_2})$$

are equal for some m_1, m_2. But then,

$$\eta = \sigma_{m_2}^{-1}\sigma_{m_1}(\eta) = \sigma_{m_2^{-1}m_1}(\eta)$$

so that $\sigma_{m_2^{-1}m_1}$ is an automorphism of $\mathbb{Q}(\zeta)/\mathbb{Q}$ fixing η and hence fixing $\mathbb{Q}(\eta)$. Thus, $m_2^{-1}m_1 \in H$ contrary to the choice of distinct coset representatives. We therefore set

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

Suppose that p is a prime divisor of k such that $p \nmid k$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\zeta)$ dividing (p). Let a be such that

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

Then, $\mathfrak{p}|(a - \eta_i)$ for some i. Therefore,

$$a \equiv \eta_i(\bmod \mathfrak{p}).$$

By Fermat's little theorem, $a^p \equiv a(\bmod p)$ and so $a^p \equiv a(\bmod \mathfrak{p})$. Hence,

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

As $p \nmid k$, pm_i and k are coprime. Therefore, $h(\zeta^{pm_i})$ is one of $h(\zeta) = \eta_1, ..., \eta_s$. If $h(\zeta^{pm_i}) \neq h(\zeta^{m_i})$, then it follows that p divides the discriminant of f, which has only finitely many prime divisors. If $h(\zeta^{pm_i}) = h(\zeta^{m_i})$ then the automorphism $\zeta \mapsto \zeta^p$ leaves

$\mathbb{Q}(\eta_i)$ fixed. But $\mathbb{Q}(\eta_i) = \mathbb{Q}(\eta)$ as the extension is Galois so that $\mathbb{Q}(\eta)$ is fixed. This means that p belongs to the residue classes contained in H, which completes our proof.

The following is a converse of Theorem 4.

Theorem 5. Let f be the polynomial of Theorem 4. Then, every prime belonging to some residue class of H divides f.

Proof. Adhering to the same notations as in the proof of Theorem 4, let us write $p = kq + r_i$. Then, $h(\zeta) = h(\zeta^{t_i})$ so that $h(\zeta^p) = h(\zeta)$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\zeta)/\mathbb{Q}$ dividing (p). Then,

$$\eta^p = h(\zeta)^p \equiv h(\zeta^p) = \eta (\bmod \mathfrak{p}).$$

By a familiar theorem of algebraic number theory, η is congruent to a rational integer $(\bmod \mathfrak{p})$. Thus, $\eta \equiv a (\bmod \mathfrak{p})$ for some rational integer a. Therefore, $\mathfrak{p} | f(a)$, but as $f(a)$ is a rational integer, it follows that $p | f(a)$, as desired.

Corollary 1. There are infinitely many primes $\equiv 1 (\bmod k)$.

Proof. By Theorems 5 and 6, the k-th cyclotomic polynomial has all its prime divisors either divisors of k or $\equiv 1 (\bmod k)$. By Schur's theorem (Theorem 2), this set is infinite.

Corollary 2. If $\ell^2 \equiv 1 (\bmod k)$, then there are infinitely many primes $\equiv \ell (\bmod k)$, provided there is at least one.

Proof. We apply Theorems 4 and 5 to the subgroup $\{1, \ell\}$ whose corresponding fixed field is $\mathbb{Q}(\zeta + \zeta^\ell)$. This field can be generated in many ways. Let $h(\zeta) = (u - \zeta)(u - \zeta^\ell)$ where u is a rational integer soon to be specified. Let $m_1, ..., m_s$ denote the coset representatives of $(\mathbb{Z}/k\mathbb{Z})^*/\langle \ell \rangle$. We will choose u so that $h(\zeta^{m_i})$ for $i = 1, ..., s$ are all distinct. Thus, apart from a finite set of values, u is an arbitrary integer. For such a choice, $h(\zeta)$ generates this field. This yields a polynomial all of whose prime divisors (apart from finitely many) are $\equiv 1$ or $\ell (\bmod k)$. In fact, this polynomial can be described explicitly:

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

Moreover, $f(0) = \phi_k(u)$ where ϕ_k denotes the k-th cyclotomic polynomial. We choose u to be a non-zero multiple of k so that

$$f(0) \equiv \phi_k(0) \equiv 1 (\bmod k).$$

By corollary 1, we know that all the prime divisors of $\phi_k(0)$ are either divisors of k or $\equiv 1(\mod k)$. Since $\phi_k(0) \equiv 1(\mod k)$, the former possibility cannot occur. Thus, all prime divisors of $f(0)$ are $\equiv 1(\mod k)$. Let $p \equiv \ell(\mod k)$ be a prime. By Theorem 5, there is a b such that $p|f(b)$. Moreover, it is possible to choose b such that $p^2 \not| f(b)$. Indeed, if $p^2|f(b)$, then $f(b+p) \equiv f(b) + pf'(b)(\mod p^2)$. As p does not divide the discriminant of f, $f'(b) \not\equiv 0(\mod p^2)$. Thus, $f(b+p) \not\equiv 0(\mod p^2)$. So such a choice of b is possible. Now suppose that there are only finitely many primes $\equiv \ell(\mod k)$. Let Q be the product of all such primes with p excluded. (If p is the only such prime, then set $Q = 1$.) Let c be a solution of the system

$$c \equiv b(\mod p^2)$$

$$c \equiv 0(\mod kQ)$$

guaranteed by the Chinese remainder theorem. Then, $f(c) \equiv f(b)(\mod p^2)$ and $f(c) \equiv f(0)(\mod kQ)$. Therefore, $p|f(c)$ and $p^2 \not| f(c)$. Moreover, $f(c)$ and Q are relatively prime for if they had a common prime factor $\equiv \ell(\mod k)$ then $f(0)$ would have such a factor, which is a contradiction. Similarly, if $f(c)$ had a prime divisor of k or $D(f)$, the discriminant of f, then $f(0)$ would also be divisible by such a prime which is again a contradiction. Thus, apart from p, $f(c)$ has only prime divisors $\equiv 1(\mod k)$. Hence, $f(c) \equiv p \equiv \ell(\mod k)$. But this contradicts $f(c) \equiv f(0) \equiv 1(\mod k)$. Hence, $f(c)$ has a prime divisor $\equiv \ell(\mod k)$ which is not a divisor of Q. This completes the proof.

We can utilise these theorems to construct Euclidean proofs for new arithmetic progressions, hitherto unconsidered by these methods. For example, such a proof should exist for primes $\equiv 4(\mod 15)$. 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 ζ denotes a primitive 15-th root of unity. Simplifying the above gives

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

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

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

That is, $p \equiv 1(\bmod 3)$ and $p \equiv 1(\bmod 5)$ **or** $p \equiv 2(\bmod 3)$ and $p \equiv 3(\bmod 5)$. Thus, $p \equiv 1(\bmod 15)$ or $p \equiv 4(\bmod 15)$ or $p \equiv 2(\bmod 15)$ or $p \equiv 8(\bmod 15)$. 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 $(-3/p) = -1$ which implies $p \equiv 1$ or $11(\bmod 12)$. Similarly,

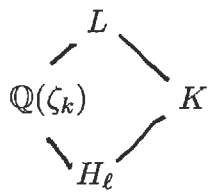
$$f(x) = (-x^2 + x/2 - 3/2)^2 - 5(x-1)^2/4$$

implies $(5/p) = 1$ so that $p \equiv 1$ or $4(\bmod 5)$. Putting all this together, we deduce that any prime divisor of f is either $\equiv 1(\bmod 15)$ or $4(\bmod 15)$. Clearly the polynomial $f(15x+1)$ also has its prime divisors $\equiv 1$ or $\equiv 4(\bmod 15)$. Since $f(15x+1) = 15xg(x) + 4$, not all prime divisors of $f(15x+1)$ are $\equiv 1(\bmod 15)$. If the primes $\equiv 4(\bmod 15)$ were finite, then let Q denote the product and consider $f(15Q+1) = 15g(Q)Q + 4$ has no prime divisor $\equiv 4(\bmod 15)$ 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 $\equiv 1(\bmod k)$ or $\equiv \ell(\bmod k)$. We would like to show that this implies $\ell^2 \equiv 1(\bmod k)$. We prove:

Proposition. Let $f \in \mathbb{Z}[x]$. Suppose that with finitely many exceptions, all prime divisors of f are either $\equiv 1(\bmod k)$ or $\ell(\bmod k)$. Then, $\ell^2 \equiv 1(\bmod k)$.

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 $H \subseteq K$. 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 $\mathbb{Q}(\zeta_k)$ and K. Then L/K is Galois, as L is the splitting field of the cyclotomic polynomial over K. Let H_ℓ denote the subfield of $\mathbb{Q}(\zeta_k)$ left fixed by $\langle \ell \rangle$. By the theorem of Bauer cited above, it follows that $H_\ell \subseteq K$. Moreover, $\mathbb{Q}(\zeta_k) \cap K = H_\ell$ because K has, by hypothesis, infinitely many prime ideals of degree one whose norms are $\equiv \ell(\bmod k)$. Thus, we have the following diagram:



Then, $Gal(L/K)$ injects into $Gal(\mathbb{Q}(\zeta_k)/H_\ell)$ because any automorphism of L/K which when restricted to $\mathbb{Q}(\zeta_k)$ is trivial, is also trivial on $\mathbb{Q}$ 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 $\mathbb{Q}(\zeta_k)$ reduce to σ_ℓ, the automorphism which has the property $\sigma(\zeta_k) = \zeta_k^\ell$. Hence, in our case, $Gal(L/K) \approx Gal(\mathbb{Q}(\zeta_k)/H_\ell)$. By the Chebotarev density theorem [8], 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 $\langle \ell \rangle$. In particular, there are infinitely many prime divisors of f which are $\equiv \ell^2 (\bmod k)$. This forces, $\ell^2 \equiv 1$ or $\ell (\bmod k)$. Hence, $\ell^2 \equiv 1 (\bmod k)$, since $(\ell, k) = 1$. This completes the proof.

Thus, philosophically, Dirichlet's theorem in its entirety cannot be proved by "Euclidean" methods. This fact was first proved by the author in [5] 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 generalised. One can prove in a similar spirit the following.

Theorem 6. 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.

REFERENCES

[1] M. Bauer, Zur Theorie der algebraischen Zahlkörper, *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] I. Gerst and J. Brillhart, On the prime divisors of polynomials, *Amer. Math. Monthly,* **78** (1971) 250-266.

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

[5] M. Ram Murty, On the existence of "Euclidean proofs" of Dirichlet's theorem on primes in arithmetic progressions, B. Sc. Thesis, 1976, (unpublished) Carleton University.

[6] T. Nagell, Sur les diviseurs premiers del polynômes, *Acta Arith.,* **15** (1969) 235-244.

[7] I. Schur, Über die existenz unendlich vieler primzahlen in einiger speziellen arithmetischen progressionen, *S-B Berlin Math. Ges.* **11** (1912) 40-50.

[8] B. Wyman, What is a reciprocity law, *Amer. Math. Monthly,* **79** (1972) 571-586.

M. Ram Murty
McGill University
Montréal, Canada