Rend. Sem. Mat. Univ. Politec. Torino
Vol. 68, 2 (2010), 183 – 197

**P. Pollack***

# HYPOTHESIS H AND AN IMPOSSIBILITY THEOREM OF RAM MURTY

**Abstract.** Dirichlet's 1837 theorem that every coprime arithmetic progression $a$ mod $m$ contains infinitely many primes is often alluded to in elementary number theory courses but usually proved only in special cases (e.g., when $m = 3$ or $m = 4$), where the proofs parallel Euclid's argument for the existence of infinitely many primes. It is natural to wonder whether Dirichlet's theorem in its entirety can be proved by such "Euclidean" arguments. In 1912, Schur showed that one can construct an argument of this type for every progression $a$ mod $m$ satisfying $a^2 \equiv 1 \pmod{m}$, and in 1988 Murty showed that these are the only progressions for which such an argument can be given. Murty's proof uses some deep results from algebraic number theory (in particular the Chebotarev density theorem). Here we give a heuristic *explanation* for this result by showing how it follows from Bunyakovsky's conjecture on prime values of polynomials.

We also propose a widening of Murty's definition of a Euclidean proof. With this definition, it appears difficult to classify the progressions for which such a proof exists. However, assuming Schinzel's Hypothesis H, we show that again such a proof exists only when $a^2 \equiv 1 \pmod{m}$.

## 1. Introduction

### 1.1. Motivation

Are there infinitely many prime numbers which end in the digit 7? This is a simple and natural question about primes which anyone learning about them for the first time might well be inclined to ask. To number theorists the answer is well known: the boldfaced sequence

$$\mathbf{7}, \mathbf{17}, 27, \mathbf{37}, \mathbf{47}, 57, \mathbf{67}, 77, 87, \mathbf{97}, \mathbf{107}, 117, \mathbf{127}, \mathbf{137}, 147, \mathbf{157}, \ldots$$

does indeed go on forever. Indeed, this theorem is a special case ($a = 7$, $m = 10$) of the following 1837 result of Dirichlet [7], one of the crowning achievements of early analytic number theory:

DIRICHLET'S THEOREM ON PRIMES IN ARITHMETIC PROGRESSIONS. Let $a$ and $m$ be integers with $m$ positive, and suppose that $a$ is relatively prime to $m$. Then the arithmetic progression

$$a, a+m, a+2m, \ldots$$

contains infinitely many primes.

Unfortunately Dirichlet's argument is by no means simple, and our hypothetical questioner might well be a bit put off by all the details necessary to verify the proof

*The author is supported by an NSF postdoctoral research fellowship.

– details from *analysis*, no less, an area which seems quite remote from our opening problem. Proofs which minimize analytic prerequisites exist (e.g., those of Zassenhaus [21], Selberg [18], and Shapiro [19, 20]; see also Granville's article [9]), but these "elementary" proofs exhibit at least as complicated a structure as Dirichlet's original argument. The contortions necessary to establish Dirichlet's theorem stand in stark contrast to the elegant and simple proof offered by Euclid for the infinitude of the primes. Is this difficulty inherent in the problem itself or merely an artifact of our own ignorance?

It is easy to give a simple proof for certain progressions. This is the case, for example, for the progression $3 \pmod 4$: if we already know the primes $p_1, \dots, p_k \equiv 3 \pmod 4$, we can find another by taking a prime divisor congruent to $3 \pmod 4$ of the integer $4p_1 \cdots p_k - 1$. Lebesgue [10] gives a version of this proof, noting that "cette démonstration est imitée d'Euclide," and in the same paper he goes on to give a "Euclidean" proof for the progression 1 mod 4. Dickson's *History* records several further attempts at giving Euclidean proofs for particular progressions (see the listing on [6, pp. 418–420]). More recently, Bateman and Low [3] have given Euclidean proofs for all coprime residue classes mod 24.

Bateman and Low's work makes explicit (in the case $m = 24$) a 1912 result of Schur [17], according to which one can find a Euclidean proof of Dirichlet's theorem whenever

$$a^2 \equiv 1 \pmod m. \tag{1}$$

(Note that every coprime residue class mod 24 has this property; it is not difficult to prove that 24 is the largest integer like this.) In 1988, Murty published a proof of the converse of Schur's result [12] (see also [13]):

MURTY'S IMPOSSIBILITY THEOREM. Unless (1) holds, there is no Euclidean proof of Dirichlet's theorem for the progression $a$ mod $m$.

For example, there is no Euclidean proof that there are infinitely many primes $p \equiv 2 \pmod 5$. Murty's argument rests on some deep results from algebraic number theory (in particular on the Chebotarev density theorem).

Our goal in this paper is twofold. First, after explaining Murty's definition of a "Euclidean proof", we motivate Murty's impossibility theorem by showing that it follows from the classical and easy-to-understand Bunyakovsky conjecture on prime values of a polynomial. One might wonder about the wisdom of deducing a known result from a conjecture that is not only unknown, but is somewhat notorious for its difficulty. To justify this, we introduce and investigate an alternative definition of what it means for the progression $a$ mod $m$ to possess a "Euclidean proof". Any progression for which a Euclidean proof exists in Murty's sense also has one in ours. One suspects that the converse is also true; however, an unconditional proof of this result seems difficult. However, we are able to show that this result follows from the grown-up brother of Bunyakovsky's conjecture, Schinzel's Hypothesis H. From a structural point of view, it is amusing to note that the Chebotarev density theorem, Bunyakovsky's conjecture, and Hypothesis H all contain Dirichlet's theorem as a special case!

**Notation**

We use the notation $d \parallel n$ to denote that $d$ is a unitary divisor of $n$, i.e., that $d$ divides $n$ while $d$ is coprime to $n/d$. We use $\mathrm{Res}(f,g)$ to denote the resultant of the two polynomials $f$ and $g$. We put $\mathrm{Disc}(f) := \mathrm{Res}(f,f')$; this coincides with the usual definition of the discriminant of $f$ up to a normalizing factor.

## 2. Just what is a Euclidean proof?

### 2.1. Looking for commonalities

To decide what constitutes a Euclidean proof, we examine two special cases of Dirichlet's theorem with indisputably Euclidean proofs, keeping an eye open for common features. The first proof is the one we saw above for the progression 3 mod 4. The second, for the progression 1 mod 4, runs thus: if we know the primes $p_1,\dots,p_k \equiv 1 \pmod 4$, take a prime divisor $p$ of $4(p_1\cdots p_k)^2+1$. Then $p$ is odd and $-1$ is a square mod $p$, so that $p \equiv 1 \pmod 4$. But $p$ cannot be any of $p_1,\dots,p_k$, and so we have discovered a new prime $p \equiv 1 \pmod 4$.

Call a prime $p$ a *prime divisor* of the polynomial $f(T) \in \mathbb{Z}[T]$ if $f$ has a root modulo $p$, i.e., if $p$ divides $f(n)$ for some integer $n$. In both of the above examples, the new prime $p$ we discover occurs as a prime divisor of an appropriately constructed polynomial. So whatever we decide a Euclidean proof should mean, the existence of one for the progression $a$ mod $m$ should entail the existence of a polynomial $f$ with the property that

(2) infinitely many prime divisors $p$ of $f$ satisfy $p \equiv a \pmod m$.

We would like this polynomial to have the property that, given a list of known primes $p_1,\dots,p_k \equiv a \pmod m$, it is easy to construct a value of $f$ which has a prime divisor congruent to $a \pmod m$ not on our list. This may be hard to arrange if $f$ has many prime divisors outside of the given progression. And this difficult case is in some sense generic; e.g., one can show (cf. [13, Theorem 3]) that any nonconstant polynomial $f(T)$ always has infinitely many prime divisors from the progression 1 mod $m$. So perhaps the best we can hope for is the following:

(3) every prime divisor $p$ of $f$, with at most finitely many exceptions, satisfies $p \equiv 1 \pmod m$ or $p \equiv a \pmod m$.

A polynomial which satisfies both (2) and (3) will be called an *E-polynomial* for the progression $a$ mod $m$. If an $E$-polynomial exists, Murty says that a *Euclidean proof exists for the progression* $a$ mod $m$. We can now state Murty's impossibility theorem in a more precise form:

MURTY'S IMPOSSIBILITY THEOREM. There is no $E$-polynomial for the progression $a$ mod $m$ unless $a^2 \equiv 1 \pmod m$.

| **Progression** | $E$**-polynomial** | $E'$**-polynomial** |
|---|---|---|
| $-1 \bmod 4$ | $T$ | $4T-1$ |
| $1 \bmod 4$ | $T^2+1$ | $4T^2+1$ |
| $4 \bmod 5$ | $T^2-5$ | $100T^2+40T-1$ |
| $1 \bmod 8$ | $T^4+1$ | $16T^4+1$ |
| $3 \bmod 8$ | $T^2+2$ | $4T^2+4T+3$ |
| $5 \bmod 8$ | $T^2+4$ | $4T^2+4T+5$ |
| $7 \bmod 8$ | $T^2-2$ | $4T^2+4T-1$ |
| $7 \bmod 24$ | $T^4+2T^2+4$ | $1296T^4+864T^3+288T^2+48T+7$ |
| $1 \bmod m$ | $\Phi_m(T)$ | $\Phi_m(mT)$ |

Table 7.1: Examples of $E$ and $E'$ polynomials for some arithmetic progressions. Here $\Phi_m(T)$ denotes the $m$th cyclotomic polynomial.

### 2.2. From number theory to epistemology

For someone actually interested in writing down proofs for particular cases of Dirichlet's theorem, the discussion so far may seem less than enlightening. For to say that we have a Euclidean proof for the progression $a \bmod m$ implies, with the above definition, that we have a polynomial $f$ with infinitely many prime divisors $p \equiv a \pmod m$. But how could we know we had such a polynomial without already knowing that there are infinitely many primes $p \equiv a \pmod m$?

The answer lies in the following result, which can be viewed as a formalization of some ideas of Schur (see [17, pp. 45-46]).

LEMMA 1. *Suppose that $f(T)$ is a nonconstant polynomial with integer coefficients satisfying* (3) *above. Assume that $f$ has a prime divisor $p \equiv a \pmod m$ which is sufficiently large (i.e., larger than a computable bound depending on $f$). Then one can construct from $f(T)$ a polynomial $g(T)$ with the following two properties:*

*(i) $g(n)$ has a prime divisor $p \equiv a \pmod m$ for every large enough integer $n$,*

*(ii) $g$ has no fixed prime divisor from the progression $a \bmod m$. That is, if $p \equiv a \pmod m$, then there is some $n$ for which $p$ does not divide $g(n)$.*

*Moreover, the set of primes dividing $f$ coincides with the set of primes dividing $g$ up to finitely many exceptions.*

Since this result is stated for motivational purposes only and will not be used in the sequel, we omit the proof.

Once we have a polynomial $g(T)$ with properties (i) and (ii), one can give a proof in the style of Euclid that infinitely many primes congruent to $a \pmod m$ appear among the primes dividing $g$: Let $p_1, \dots, p_k$ be a finite (possibly empty) list of primes from the progression $a \bmod m$ that divide $g$. Using condition (ii) above and the Chinese

remainder theorem, choose an integer $n_0$ for which $g(n_0)$ is coprime to $P := p_1 \cdots p_k$. Then for any integer $n$,

$$g(Pn+n_0) \equiv g(n_0) \pmod{P}, \quad \text{hence} \quad \gcd(g(Pn+n_0),P) = 1.$$

For large $n$, condition (i) above guarantees that $g(Pn+n_0)$ has a prime factor in the progression $a$ mod $m$. Since $g(Pn+n_0)$ is coprime to $P$, this must be a different prime from any of the $p_i$.

The upshot of this discussion is that in practice, to prove Dirichlet's theorem for the progression $a$ mod $m$, it suffices to have a polynomial satisfying condition (3) together with a single large prime $p \equiv a \pmod{m}$ which appears as a divisor of $f$. That $f$ also satisfies condition (2), and so is an $E$-polynomial for the progression $a$ mod $m$, then follows *a posteriori*, using the last clause of Lemma 1.

Since Schur has shown that $E$-polynomials exist whenever $a^2 \equiv 1 \pmod{m}$ (cf. [13, Theorem 4]), Murty's impossibility result completes the characterization of the progressions for which $E$-polynomials exist. In the next section we give the promised heuristic argument for Murty's theorem. Notice, however, that to prove the existence of infinitely many primes $p \equiv a \pmod{m}$, all we really need is the existence of a polynomial with properties (i) and (ii) of Lemma 1. Call such a polynomial an $E'$-polynomial for the progression $a$ mod $m$. (Some examples of $E$ and $E'$-polynomials are given in Table 7.1.) In Section 4 we demonstrate the following conditional analogue of Murty's result:

THEOREM 1 (assuming Hypothesis H). *There is no $E'$-polynomial for the progression $a$ mod $m$ unless $a^2 \equiv 1 \pmod{m}$.*

We conclude the paper with some comments on the difficulties of proving Theorem 1 unconditionally.

## 3. Bunyakovsky's conjecture implies Murty's impossibility theorem

Let $f$ be a nonconstant polynomial with integer coefficients. Given a positive integer $m$, let $S(f,m)$ denote that subset of $\mathbb{Z}/m\mathbb{Z}$ consisting of those residue classes which contain infinitely many prime divisors of $f(T)$. Clearly $S(f,m)$ is a subset of $(\mathbb{Z}/m\mathbb{Z})^\times$. Moreover, $S(f,m)$ is nonempty, because every nonconstant polynomial has infinitely many prime divisors (see [17, pp. 40-41] or [13, Theorem 2]). Actually $S(f,m)$ possesses considerably more structure:

THEOREM 2. *If $f$ is irreducible over the rational numbers, then $S(f,m)$ is a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$.*

In fact, if we form a number field $K$ by adjoining a root of $f$ to $\mathbb{Q}$, then Conrad [5] shows that $S(f,m)$ is exactly the image of $\mathrm{Gal}(K(\zeta_m)/K)$ under the restriction map to $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

The impossibility theorem is a straightforward consequence of Theorem 2:

Given an $E$-polynomial for the progression $a \bmod m$, it is easy to see that it must have an irreducible factor which is also an $E$-polynomial for the same progression. Using $f$ to denote this factor, Theorem 2 implies that $S(f,m)$ is a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ satisfying $\{a \bmod m\} \subset S(f,m) \subset \{1 \bmod m,\ a \bmod m\}$. This easily implies that $a^2 \equiv 1 \pmod m$.

We now show that Theorem 2 can be deduced from Bunyakovsky's conjecture on prime values of polynomials. We begin by recalling the statement of Bunyakovsky's conjecture [4]:

BUNYAKOVSKY'S CONJECTURE. Let $f(T)$ be a polynomial with integer coefficients and positive leading coefficient which is irreducible over $\mathbb{Q}$. Let

$$d := \gcd\{f(n)\}_{n\in\mathbb{Z}}.$$

Then $f(n)/d$ is prime for infinitely many positive integers $n$.

For the proof we use the following result, which may be extracted from an argument of Schinzel appearing in [16]:

LEMMA 2. *Let $f$ be a polynomial with integer coefficients, and let $d$ be the greatest fixed divisor of $f$, i.e., $d := \gcd\{f(n)\}_{n\in\mathbb{Z}}$. There exist integers $A, B$ with $A > 0$ so that $\frac{1}{d} f(AT + B)$ has integer coefficients and no fixed prime divisor.*

The next lemma, together with the "subgroup criterion" from a first-course in group theory, completes the proof:

LEMMA 3. *Assume Bunyakovsky's Conjecture. Let $f$ be a nonconstant irreducible polynomial with integer coefficients and $m$ a positive integer. Suppose that $S(f,m)$ contains the residue classes $a_1 \bmod m, \dots, a_k \bmod m$. Then $S(f,m)$ also contains the residue class $a_1^{-1} \cdots a_k^{-1} \bmod m$.*

*Proof.* Observe that the set $S(f,m)$ is unchanged if $f$ is replaced by a polynomial whose set of prime divisors coincides with that of $f$ except at finitely many places. Thus, replacing $f$ with the polynomial whose existence is asserted in Lemma 2, we may assume that $f$ has no fixed prime divisor. Next, replacing $f$ with $f(T + n_0)$ for a suitable $n_0$, we can assume additionally that the constant term of $f$ is prime to $m$. Now replacing $f$ with $f(mT)$, we can also assume that $f$ is constant modulo $m$, i.e., that the reduction $\overline{f}$ of $f$ in $(\mathbb{Z}/m\mathbb{Z})[T]$ actually belongs to $\mathbb{Z}/m\mathbb{Z}$. Let $a_0 \bmod m$ be this reduction. Since $f$ assumes infinitely many prime values by Bunyakovsky's conjecture, it must be that $a_0 \bmod m$ is an element of $S(f,m)$.

Now choose prime divisors $p_0, p_1, \dots, p_k$ of $f$ with each $p_i \equiv a_i \pmod m$ and no $p_i$ dividing $\mathrm{Disc}(f)$. For each $i$, choose an integer $r_i$ so that $f(r_i) \equiv 0 \pmod{p_i}$. Since $p \nmid \mathrm{Disc}(f)$, we have $f'(r_i) \not\equiv 0 \pmod{p_i}$. So by replacing $r_i$ with $r_i + p_i$ if necessary, we can assume that $p_i \parallel f(r_i)$ for each $i$. Then choosing $r$ to satisfy $r \equiv r_i \pmod{p_i^2}$ for each $i$, we have $p_0 \cdots p_r \parallel f(r)$. Define a new polynomial $g(T)$ by the

equation

$$f(p_0 \dots p_k T + r) = p_0 \cdots p_k g(T).$$

Then $g(T)$ has integer coefficients, is irreducible over $\mathbb{Q}$, and has no fixed prime divisors. The first two properties are inherited from $f$. To see the third, note that since $f$ has no fixed prime divisors, the only possibilities for fixed prime divisors of $g$ are $p_0$, ..., $p_k$, but none of these divide $g(0) = f(r)/(p_0 \dots p_k)$. It follows that $\gcd\{g(n)\}_{n\in\mathbb{Z}} = 1$. So by Bunyakovsky's conjecture, there are arbitrarily large $n$ for which $g(n)$ is prime. Since

$$g(n) \equiv a_0 a_0^{-1} a_1^{-1} \cdots a_k^{-1} \equiv a_1^{-1} \cdots a_k^{-1} \pmod{m},$$

it follows that $a_1^{-1} \cdots a_k^{-1} \bmod m$ belongs to $S(f,m)$, as we sought to show. □

## 4. Proof of Theorem 1

We begin by recalling Schinzel's Hypothesis H:

HYPOTHESIS H. Let $f_1, f_2, \dots, f_k$ be nonconstant polynomials which have integer coefficients, positive leading coefficients, and which are all irreducible over the rationals. Suppose that $f := f_1 f_2 \dots f_k$ has no fixed prime divisor, i.e., that there is no prime $p$ dividing $f(n)$ for all integers $n$. Then

$$f_1(n), f_2(n), \dots, f_k(n) \text{ are simultaneously prime}$$

for arbitrarily large positive integer values of $n$.

Suppose that $k = 1$, and that $f = f_1$ satisfies the conditions of Hypothesis H. Since $f$ has no fixed prime divisor, it follows that $\gcd\{f(n)\}_{n\in\mathbb{Z}} = 1$, and therefore Bunyakovsky's conjecture predicts that the value $f(n)$ is prime for infinitely many positive integers $n$. In other words, Bunyakovsky's conjecture implies the case $k = 1$ of Hypothesis H. Conversely, Schinzel shows in [16] that the case $k = 1$ of Hypothesis H implies Bunyakovsky's conjecture. So, one may view Hypothesis H as a generalization to several polynomials of Bunyakovsky's conjecture.

LEMMA 4. *If $a \bmod m$ possesses an $E'$-polynomial, then it also possesses an $E'$-polynomial with no fixed prime divisor.*

*Proof.* Let $f$ be an $E'$-polynomial for the given progression, and let $g = \frac{1}{d} f(AT + B)$ be a polynomial as in the conclusion of Lemma 2. Then $g$ has the desired property. Indeed, suppose $n$ is large. Since $f$ satisfies condition (i) in the definition of an $E'$-polynomial, there is a prime $p \equiv a \pmod{m}$ that divides $f(An + B)$; since $f$ satisfies condition (ii), this prime $p$ does not divide $d$, so that it must divide $g(n) = f(An+B)/d$. This shows that (i) holds for $g$. And since $g$ has no fixed prime divisor at all, (ii) holds as well. □

LEMMA 5. *Suppose that the progression $a \bmod m$ has an $E'$ polynomial. Then one can choose an $E'$ polynomial $f(T)$ for $a \bmod m$ with a factorization in $\mathbb{Z}[T]$ of the*

*form*

$$f(T) = f_1(T) \cdots f_k(T)$$

*and where all of the following hold:*

*(i)* $f$ *has no fixed prime divisor,*

*(ii)* $f$ *has constant term coprime to* $m$*,*

*(iii)* $f$ *has positive leading coefficient,*

*(iv) the* $f_i$ *have integer coefficients, positive leading coefficients and are distinct and irreducible over the rationals,*

*(v)* $f$ *and the* $f_i$ *are constant polynomials modulo* $m$*; i.e., the reductions* $\overline{f}(T) \in (\mathbb{Z}/m\mathbb{Z})[T]$ *and* $\overline{f_i}(T) \in (\mathbb{Z}/m\mathbb{Z})[T]$ *are constant polynomials.*

*Proof.* We begin by constructing an $E'$-polynomial $g$ with a factorization $g = g_1 \dots g_k$ for which the analogues of of (i) - (iv) are satisfied, with $g_i$ in place of $f_i$. We then describe the modifications necessary to obtain (v).

Choose some $E'$-polynomial $g(T)$ for the progression $a$ mod $m$ with no fixed prime divisor. This is possible by Lemma 4. Then already (i) is satisfied. Apply the Chinese remainder theorem to find an integer $n$ with $g(n)$ coprime to $m$, and then replace $g$ with $g(T+n)$; this gives (ii). Write

$$g(T) = \pm g_1(T) \cdots g_k(T) \tag{4}$$

where the $g_i$ are irreducible over the integers and the leading coefficient of each $g_i$ is positive. Since $g$ has no fixed prime divisor, the $g_i$ are nonconstant, and so each $g_i$ is irreducible also over the rationals. Now replace $g$ by the product of the distinct $g_i$. This gives (iii) and (iv); note that $g$ remains an $E'$-polynomial after this transformation.

To obtain (v), set $f(T) := g(mT)$ and $f_i(T) := g_i(mT)$ for $1 \le i \le k$. Clearly (ii)-(v) now hold. Since $g$ was without fixed prime divisor, all fixed prime divisors of $f$ divide $m$. But $f(0) = g(0)$ is coprime to $m$, so (i) holds as well. Finally, $f$ is still an $E'$-polynomial for $a$ mod $m$, since property (i) in the definition of an $E'$-polynomial is inherited from $g$ and property (ii) of the same definition is weaker than condition (i) above. □

We also require an easy but technical consequence of Hypothesis H:

LEMMA 6. *Assume Hypothesis H. Suppose* $f_1, \dots, f_k$ *are distinct nonconstant polynomials with integer coefficients, positive leading coefficients, all irreducible over the rationals and such that the product* $f := f_1 \dots f_k$ *has no fixed prime divisor. Let* $0 \le r \le k$ *and suppose that for each* $1 \le i \le r$ *we are given a prime divisor* $p_i$ *of* $f_i$*. Moreover, suppose that*

$$p_1 p_2 \cdots p_r \text{ is coprime to } \prod_{1 \le i \le k} \operatorname{Res}(f_i, f_i') \prod_{1 \le i < j \le k} \operatorname{Res}(f_i, f_j). \tag{5}$$

*Then there are arbitrarily large n for which*

$$f_1(n) = p_1q_1, \;\; f_2(n) = p_2q_2, \;\; \ldots, \;\; f_r(n) = p_rq_r, \;\; f_{r+1}(n) = q_{r+1}, \;\; \ldots, \;\; f_k(n) = q_k,$$

*where all the $q_i$ are prime.*

Note that under the hypotheses of the lemma, the product appearing in (5) is nonvanishing. Indeed, every term in the product is nonzero since the $f_i$ are nonassociated over the rationals and (being irreducible) have no multiple roots.

*Proof.* Let $1 \le i \le r$. Since $p_i$ divides $f_i$, we can choose an integer $n_i$ with $f_i(n_i) \equiv 0 \pmod{p_i}$. Since $p_i \nmid \mathrm{Res}(f_i, f_i')$, we have $f_i'(n_i) \not\equiv 0 \pmod{p_i}$, and hence by adjusting $n_i$ by a multiple of $p_i$ we can in fact assume $p_i \parallel f_i(n_i)$. Choose $n_0$ with $n_0 \equiv n_i \pmod{(\prod p_j)^2}$ for all $1 \le i \le r$. Then $p_i \parallel f_i(n_0)$ for each $i$.

Let $P := (\prod p_i)^2$. Define polynomials $g_1, \ldots, g_k$ by

$$f_1(PT + n_0) = p_1g_1(T), f_2(PT + n_0) = p_2g_2(T), \ldots, f_r(PT + n_0) = p_rg_r(T),$$
$$f_{r+1}(PT + n_0) = g_{r+1}(T), f_{r+2}(PT + n_0) = g_{r+2}(T), \ldots, f_k(PT + n_0) = g_k(T).$$

It suffices to check that the conditions of Hypothesis H hold for $g_1, \ldots, g_k$.

The polynomials $g_i$ all have integer coefficients. Moreover, the $g_i$ are nonconstant and irreducible over the rationals, since the $f_i$ are. So we need only verify that the product

$$g(T) := (g_1 \cdots g_k)(T) = \frac{(f_1 \cdots f_k)(PT + n_0)}{p_1 \cdots p_r}$$

has no fixed prime divisor. Any such is also a fixed prime divisor of $f(PT + n_0)$ and so necessarily divides $P$. That is, any fixed prime divisor is one of the $p_i$. But if $p_i$ divides $g(0)$, then $p_i^2 \mid \prod f_i(n_0)$, and we deduce that

$$p_i \mid f_j(n_0) \quad \text{for some } j \ne i,$$

since $p_i \parallel f_i(n_0)$. This implies that $f_i$ and $f_j$ have a common root modulo $p_i$, so that $p_i \mid \mathrm{Res}(f_i, f_j)$, a contradiction. □

*Proof of Theorem 1.* We shall show that if $f$ and $f_i$ are as in Lemma 5, then one of the $f_i$ is an $E$-polynomial for the progression $a \bmod m$. Theorem 1 then follows from Murty's characterization of $E$-polynomials (the impossibility theorem). Renumbering if necessary, we may assume that the constant term of $f_i$ is congruent to $a \pmod{m}$ precisely for $1 \le i \le r$.

We first show that $r \ge 1$, i.e., that some $f_i$ has constant term congruent to $a \pmod{m}$. Supposing the contrary, we apply Hypothesis $H$ to obtain arbitrarily large values of $n$ for which $f_i(n)$ is prime for each $1 \le i \le k$ (the conditions of Hypothesis H are implied by conditions (i) and (iv) of Lemma 5). Then, recalling (v) of the same lemma,

$$f_i(n) \equiv f_i(0) \not\equiv a \pmod{m} \qquad \text{for } 1 \le i \le k,$$

and so $f(n) = \prod_{i=1}^{k} f_i(n)$ has no prime factors from the progression $a$ mod $m$ for these values of $n$. But this contradicts that $f$ is an $E'$-polynomial for $a$ mod $m$.

Now fix $1 \le i \le r$, and that suppose that $f_i$ is not an $E$-polynomial for the progression $a$ mod $m$. Then either

(i′) $f_i$ has infinitely many prime divisors outside of the progressions 1 mod $m$ and $a$ mod $m$, or

(ii′) $a \not\equiv 1 \pmod{m}$, and all but finitely many of $f_i$'s prime divisors belong to the residue class 1 mod $m$.

But (ii′) is easily seen to be impossible. For in this case let $Q$ be the product of those prime divisors of $f_i$ that do not belong to the residue class 1 mod $m$. Since $f$ has no fixed prime divisor, neither does $f_i$, so again the Chinese remainder theorem allows us to find arbitrarily large $n$ with $f_i(n)$ coprime to $Q$. Since

$$f_i(n) \equiv f_i(0) \equiv a \pmod{m},$$

for large enough $n$ of this type we get a positive integer congruent to $a \pmod{m}$ all of whose prime factors are from the progression 1 mod $m$, which is absurd.

Hence if none of $f_1, \dots, f_r$ is an $E$-polynomial for $a$ mod $m$, then for every $1 \le i \le r$ the polynomial $f_i$ must have infinitely many prime divisors outside the progressions 1 mod $m$ and $a$ mod $m$. Choose such a prime divisor $p_i$ for each $1 \le i \le r$ in such a way that Lemma 6 can be applied (e.g., it suffices to take choose the $p_i$ all sufficiently large). Then we obtain arbitrarily large $n$ for which

$$f_1(n) = p_1 q_1, \quad f_2(n) = p_2 q_2, \quad \dots, \quad f_r(n) = p_r q_r,$$
$$f_{r+1}(n) = q_{r+1}, \quad f_{r+2}(n) = q_{r+2}, \quad \dots, \quad f_k(n) = q_k,$$

where all the $q_i$ are prime. Since $f = \prod f_i$ is an $E'$-polynomial for $a$ mod $m$, for sufficiently large $n$ of this type the list

$$p_1, p_2, \dots, p_r, q_1, \dots, q_r, q_{r+1}, \dots, q_k$$

must contain a prime congruent to $a \pmod{m}$.

But this is not possible: The $p_i$ were chosen outside the progression $a$ mod $m$, the $q_j$ for $j > r$ satisfy

$$q_j = f_j(n) \equiv f_j(0) \not\equiv a \pmod{m},$$

and for $1 \le j \le r$,

$$p_j q_j \equiv f_j(n) \equiv f_j(0) \equiv a \pmod{m},$$

so that

$$q_j \equiv a p_j^{-1} \not\equiv a \pmod{m},$$

since $p_j \not\equiv 1 \pmod{m}$. This contradiction completes the proof. □

REMARK 1. Keeping closer track of the transformations of this section, one can obtain from our arguments a stronger result than claimed in Theorem 1, namely that (assuming Hypothesis H) any $E'$-polynomial for the progression $a$ mod $m$ is divisible by an $E$-polynomial for the same progression.

## 5. Concluding Remarks

### 5.1. Lessons from *History*

As we have already mentioned, the first volume of Dickson's *History of the Theory of Numbers* chronicles the early attempts to obtain special cases of Dirichlet's theorem. There are two entries that deserve special attention. While nearly all the results are for progressions $a$ mod $m$ with $a^2 \equiv 1 \pmod{m}$, Dickson also reports, more surprisingly, that

> A.S. Bang [gave a proof] for the differences 4, 6, 8, 10, 12, 14, 18, 20, 24, 30, 42, 60,

and

> E. Lucas for $5n+2$, $8n+7$.

But the first progression attributed to Lucas, as well as many of the progressions here attributed to Bang, have no Euclidean proofs in our sense (assuming Hypothesis H). How then did these authors proceed?

Bang's entry is a healthy reminder that we ought not equate Euclidean proofs with elementary proofs. His arguments (which may be found in [1] or [2]) are based not on Euclid's approach to prime number theory but on Chebyshev's. Forty years later, similar proofs would be given by Erdös [8] and Ricci ([14, 15]), both of whom were apparently unaware of Bang's work.

Lucas's argument [11, p. 309] is intriguing but erroneous. Let $L_0 = 2$, $L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for $n = 0, 1, 2, \ldots$; these "Lucas numbers" satisfy many well-known identities, in particular

$$L_{2n} = L_n^2 - 2(-1)^n \quad \text{and} \quad L_n^2 - 5F_n^2 = 4(-1)^n,$$

where $F_n$ is the $n$th Fibonacci number (indexed so that $F_0 = 0$). The first identity implies that $L_{2^k} \equiv 2 \pmod{5}$ for $k \geq 2$, while the second implies that $\left(\frac{-5}{p}\right) = 1$ for each prime divisor $p$ of $L_{2^k}$, whence $p \equiv 1, 3, 7$ or $9 \pmod{20}$. From these two facts, Lucas wants us to conclude that each $L_{2^k}$, with $k \geq 2$, has a prime divisor congruent to $2 \pmod{5}$. However,

$$L_{2^7} = 119809 \cdot 469816763452337987 5583,$$

and neither prime on the right-hand side belongs to the progression 2 mod 5.

### 5.2. Obstructions to an unconditional proof of Theorem 1

Fix a progression $a$ mod $m$ for which $a^2 \not\equiv 1 \pmod{m}$. Then it not only appears difficult to establish unconditionally that there is no $E'$-polynomial for the progression $a$ mod $m$, but it is not even obvious how to show that a specific polynomial $f(T)$ is not an $E'$-polynomial for the specified progression. To take a very concrete example, the author is unaware of any solution to the following exercise:

PROBLEM. Show that $T^2+2$ is not an $E'$-polynomial for the progression 2 mod 7. Equivalently, prove that there are infinitely many integers $n$ for which $n^2+2$ is free of prime factors congruent to $2 \pmod 7$.

We might expect problems of this kind to be difficult because elementary sieve methods easily establish that for almost all $n$ (that is, all $n$ outside a set of asymptotic density 0) the integer $n^2+2$ does have a prime factor congruent to $2 \pmod 7$.

Somewhat surprisingly, some problems of this type do have simple solutions. For example, H. W. Lenstra has pointed out to the author the following demonstration that $n^2+1$ is infinitely often free of prime factors congruent to $2 \pmod 5$: There is certainly at least one $n$ for which $n^2+1$ is free of prime factors from the progression 2 mod 5, namely $n=2$. But then $(n^5)^2+1$ is another, since the quotient

$$\frac{n^{10}+1}{n^2+1} = \Phi_{10}(n^2) \qquad \text{has only prime divisors congruent to 0 or 1} \pmod 5.$$

Alternatively, Don Coppersmith notes that by quadratic reciprocity, $n^2+1$ is free of prime factors congruent to 2 or $3 \pmod 5$ whenever it admits a representation in the form $x^2-5y^2$ with $x$ and $y$ coprime and of opposite parity. He completes his proof by observing that

$$(10k^2)^2+1 = 100k^4+1 = (10k^2+1)^2 - 5(2k)^2.$$

Both methods are capable of generalization. For example, Coppersmith's method shows that $n^2+2$ is free of prime factors congruent to $2 \pmod 5$ whenever the positive integer $n$ corresponds to a solution of the generalized Pell equation $n^2-3m^2=-242$. For example, taking a reasonably large solution of this Pell equation, we find

$$760577608550439702331^2+2 = \\ 3 \cdot 2539 \cdot 316981018521 \cdot 295798907466244259932289011,$$

and as predicted none of the right-hand primes are congruent to $2 \pmod 5$.

### Appendix: A remark on Bunyakovsky's conjecture

The concern of this paper has been clarifying logical relations between certain conjectures, theorems, and methods of proof. In this appendix, we point out a further such relation, relevant to the discussion of Section 3. Consider the following assertion:

BUNYAKOVSKY'S CONJECTURE (WEAK FORM). Let $f$ be a polynomial with integer coefficients and positive leading coefficients which is irreducible over $\mathbb{Q}$. Let

$$d := \gcd\{f(n)\}_{n\in\mathbb{Z}}.$$

Then $f(n)/d$ is prime for at least one positive integer $n$.

The hypotheses here are the same as in Bunyakovsky's conjecture from Section 3, but the conclusion is weaker. In this appendix, we show that one can derive the full Bunyakovsky conjecture from this seemingly weaker version.

THEOREM 3. *The weak form of Bunyakovsky's conjecture implies the full Bunyakovsky conjecture (i.e., the conjecture as stated in Section 3).*

*Proof.* We show that the weak Bunyakovsky conjecture implies that the following assertion holds for every positive integer $k$:

($B_k$) If $f$ satisfies the hypotheses of Bunyakovsky's conjecture, then $f(n)/d$ is prime for at least $k$ distinct positive integers $n$.

The assertion ($B_1$) is exactly the weak form of Bunyakovsky's conjecture. We continue by induction. Suppose that ($B_k$) is known, and let $f$ be a polynomial satisfying the hypotheses of Bunyakovsky's conjecture. If $f(T) = cT$ for some positive integer $c$, then $\gcd\{f(n)\}_{n\in\mathbb{Z}} = c$, and so $f(n)/d = n$. Since there are infinitely many primes, it is clear in this case that $f(n)/d$ represents primes for at least $k+1$ distinct positive integers $n$; thus ($B_{k+1}$) holds for these $f$. So we can assume that $f(0) \neq 0$. By the induction hypothesis, there are positive integers $n_1 < n_2 < \cdots < n_k$ for which each $f(n_i)/d$ is prime. Choose a prime $q > n_k$ for which $q \nmid f(0)$, and define an auxiliary polynomial $F$ by putting

$$F(T) := f(qT).$$

Since $f$ is irreducible over $\mathbb{Q}$, so is $F$. Let $D := \gcd\{F(n)\}_{n\in\mathbb{Z}}$. We claim that $D = d$. Assuming this for now, the weak Bunyakovsky conjecture implies that $F(n)/D = f(qn)/d$ is prime for some positive integer $n$. Putting $n_{k+1} := qn$, we have $n_{k+1} \geq q > n_k$, and so $f(m)/d$ is prime for at least the $k+1$ integers $m \in \{n_1, \ldots, n_{k+1}\}$. Thus, ($B_{k+1}$) holds in general.

It remains to prove that $D = d$. Since the image of $F$ is contained in the image of $f$, it is immediate that $d$ divides $D$. Suppose that $r$ is a prime dividing $D$, and choose $e \geq 1$ with $r^e \parallel D$. Notice that $r$ divides $F(0) = f(0)$, and so $r \neq q$. Since $r^e \mid D$, it follows that $F(T) = f(qT)$ defines the zero function as a map from $\mathbb{Z}/r^e\mathbb{Z}$ to itself. But $q$ is coprime to $r^e$, so that multiplication by $q$ merely permutes the elements of $\mathbb{Z}/r^e\mathbb{Z}$. Hence, $f$ also defines the zero function as a map from $\mathbb{Z}/r^e\mathbb{Z}$ to itself, which implies that $r^e$ divides $d$. Thus, $r \nmid D/d$. Since this holds for every prime divisor $r$ of $D$, the positive integer $D/d$ has no prime divisors at all; thus $D/d = 1$, and $D = d$, as desired. □

**Acknowledgements**

I would like to thank Noah Snyder for proposing the notion of $E'$-polynomials, Keith Conrad for comments on an early draft, my thesis advisor Carl Pomerance for helpful suggestions and constant encouragement, H. W. Lenstra and Don Coppersmith for permission to include their ingenious arguments, and the referee for suggesting the contents of the appendix.

**References**

[1] BANG A. S. Om Primtal af bestemte Former. *Nyt Tidsskrift for matematik, B (advanced) 2* (1891), 73–82.

[2] BANG A. S. *Elementære Beviser for specielle Tilfælde af Dirichlets Sætning om Differensrækker*. H. Chr. Bakkes Boghandel, København, 1937.

[3] BATEMAN P. T. AND LOW M. E. Prime numbers in arithmetic progressions with difference 24. *Amer. Math. Monthly 72* (1965), 139–143.

[4] BUNYAKOVSKY V. Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs. *Mém. Acad. Sc. St. Pétersbourg 6* (1857), 305–329.

[5] CONRAD K. Euclidean proofs of Dirichlet's theorem. Available from `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/dirichleteuclid.pdf`.

[6] DICKSON L. E. *History of the Theory of Numbers. Vol. I: Divisibility and Primality.* Chelsea Publishing Co., New York, 1966.

[7] DIRICHLET P. G. L. Beweis der Satz, dass jede unbegrentze arithmetische progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftliche Factor sind, unendliche viele Primzahlen enthält. Abh. der Königlichen Preuss. Akad. der Wiss., 1837, pp. 45–81.

[8] ERDÖS P. Über die Primzahlen gewisser arithmetischer Reihen. *Math Z. 39* (1935), 473–491.

[9] GRANVILLE A. On elementary proofs of the prime number theorem for arithmetic progressions, without characters. In *Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989) (Salerno)*. Univ. Salerno, 1992, pp. 157–194.

[10] LEBESGUE V. A. Remarques diverses sur les nombres premiers. *Nouv. Ann. Math. 15* (1856), 130–134, 236–239.

[11] LUCAS E. Theorie des fonctions numeriques simplement periodiques. *Amer. J. Math. 1* (1878), 289–321.

[12] MURTY M. R. Primes in certain arithmetic progressions. *Journal of the Madras University* (1988), 161–169.

[13] MURTY M. R. AND THAIN N. Prime numbers in certain arithmetic progressions. *Funct. Approx. Comment. Math. 35* (2006), 249–259.

[14] RICCI G. Sul teorema di Dirichlet relativo alla progressione aritmetica. *Boll. Un. Mat. Ital. 12* (1933), 304–309.

[15] RICCI G. Sui teoremi di Dirichlet e di Bertrand–Tchebychef relativi alla progressione aritmetica. *Boll. Un. Mat. Ital. 13* (1934), 7–17.

[16] SCHINZEL A. Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers". *Acta Arith. 7* (1961/1962), 1–8.

[17] SCHUR I. Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen. *Sitzungsber Berl. Math. Ges. 11* (1912), 40–50.

[18] SELBERG A. An elementary proof of Dirichlet's theorem about primes in an arithmetic progression. *Ann. of Math. 50* (1949), 297–304.

[19] SHAPIRO H. N. On primes in arithmetic progressions. I. *Ann. of Math. 52* (1950), 217–230.

[20] SHAPIRO H. N. On primes in arithmetic progression. II. *Ann. of Math. 52* (1950), 231–243.

[21] ZASSENHAUS H. Über die Existenz von Primzahlen in arithmetischen Progressionen. *Comment. Math. Helv. 22* (1949), 232–259.

**AMS Subject Classification: 11A41, 11N05**

Paul POLLACK
Mathematics Department, University of Illinois
1409 W. Green Street, Urbana, IL 61801, USA
e-mail: pppollac@illinois.edu

*Lavoro pervenuto in redazione il 09.07.2010 e, in forma definitiva, il 27.07.2010*