Prime and coprime values of polynomials

Arnaud Bodin, Pierre Dèbes and Salah Najib

Abstract. The Schinzel Hypothesis is a celebrated conjecture in number theory linking polynomial values and prime numbers. In the same vein we investigate the common divisors of values $P_1(n), \ldots, P_s(n)$ of several polynomials. We deduce this coprime version of the Schinzel Hypothesis: under some natural assumption, coprime polynomials assume coprime values at infinitely many integers. Consequences include a version "modulo an integer" of the original Schinzel Hypothesis, with the Goldbach conjecture, again modulo an integer, as a special case.

Given polynomials with integer coefficients, famous results and long-standing questions concern the *divisibility properties* of their values at integers, in particular their *primality*. The polynomial $x^2 + x + 41$ which assumes prime values at $0, 1, \ldots, 39$ is a striking example, going back to Euler. On the other hand, the values of a nonconstant polynomial $P(x)$ cannot be all prime numbers: if $P(0)$ is a prime, then the other value $P(kP(0))$ is of the form $a_d(kP(0))^d + \cdots + a_1 kP(0) + P(0)$, so is divisible by $P(0)$, and, for all but finitely many $k \in \mathbb{Z}$, is different from $\pm P(0)$, and hence cannot be a prime.

Whether a polynomial may assume infinitely many prime values is a deeper question. Even for $P(x) = x^2 + 1$, whether there are infinitely many prime numbers of the form $n^2 + 1$ with $n \in \mathbb{Z}$ is out of reach. Bunyakowsky conjectured that the question always has an affirmative answer, under some natural assumption recalled below. The Schinzel Hypothesis generalizes this conjecture to several polynomials, concluding that they should simultaneously take prime values; see Section 2.

We follow this trend. Our main results are concerned with the *common divisors of values* $P_1(n), \ldots, P_s(n)$ at integers n of several polynomials, see Theorem 1.1 in Section 1 (proved in Section 3) and further complements in Section 4. We can then investigate the *coprimality of values* of polynomials. Generally speaking, we say that n integers, with $n \geq 2$, are coprime if they have no common prime divisor. While the Schinzel Hypothesis is still open, we obtain this "coprime" version: under some suitable assumption, *coprime polynomials assume coprime values at infinitely many integers* (Corollary 1.2).

We deduce a "modulo m" variant of the Schinzel Hypothesis, and versions of the Goldbach and the Twin Primes conjectures, again "modulo m"; see Section 2. A coprimality criterion for polynomials is offered in Section 5. Finally, in Section 6, we discuss generalizations for which $\mathbb{Z}$ is replaced by a polynomial ring.

1. Common divisors of values and the coprimality question

For the whole paper, $f_1(x), \ldots, f_s(x)$ are nonzero polynomials with integer coefficients.

Assume that the polynomials $f_1(x), \ldots, f_s(x)$ are coprime ($s \geq 2$), i.e. they have no common root in $\mathbb{C}$. Interesting phenomena occur when considering the greatest common divisors:

$$d_n = \gcd\big(f_1(n), \ldots, f_s(n)\big) \quad \text{with } n \in \mathbb{Z}.$$

It may happen that $f_1(x), \ldots, f_s(x)$ never assume coprime values, i.e., that none of the integers d_n is 1. A simple example is $f_1(x) = x^2 - x = x(x-1)$ and $f_2(x) = x^2 - x + 2$: all values $f_1(n)$ and $f_2(n)$ are even integers. More generally for $f_1(x) = x^p - x$ and $f_2(x) = x^p - x + p$ with p a prime number, all values $f_1(n), f_2(n)$ are divisible by p, by Fermat's theorem. Rule out these polynomials by assuming that *no prime p divides all values $f_1(n), \ldots, f_s(n)$ with $n \in \mathbb{Z}$.* Excluded polynomials are well-understood: modulo p, they vanish at every element of $\mathbb{Z}/p\mathbb{Z}$, hence are divisible by $x^p - x = \prod_{m \in \mathbb{Z}/p\mathbb{Z}}(x - m)$; so they are of the form $pg(x) + h(x)(x^p - x)$ with $g(x), h(x) \in \mathbb{Z}[x]$ for some prime p.

With this further assumption, is it always true that $f_1(n), \ldots, f_s(n)$ are coprime for at least one integer n? For example this is the case for n and $n+2$ that are coprime when n is odd. In other words, does the set

$$\mathcal{D}^\star = \{d_n \mid n \in \mathbb{Z}\}$$

contain 1? Studying $\mathcal{D}^\star$, which, as we will see, is quite intriguing, is a broader goal.

Example 1. Let $f_1(x) = x^2 - 4$ and $f_2(x) = x^3 + 3x + 2$. These polynomials are coprime since no root of f_1 is a root of f_2. The values $d_n = \gcd(f_1(n), f_2(n))$, for $n = 0, \ldots, 20$ are:

2 3 16 1 6 1 4 3 2 1 24 1 2 3 4 1 6 1 64 3 2

We have in fact $\mathcal{D}^\star = \{1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 64, 96, 192\}$. It seems unclear to highlight a pattern from the first terms, but at least the integer 1 occurs.

A first general observation is that the set $\mathcal{D}^\star$ is finite. This was noticed for two polynomials by Frenkel–Pelikán [FP]. In fact they showed more: the sequence $(d_n)_{n \in \mathbb{Z}}$ is periodic. We will adjust their argument. A new result about the set $\mathcal{D}^\star$ is the stability assertion of the following statement, which is proved in Section 3.

Theorem 1.1. *Let $f_1(x), \ldots, f_s(x) \in \mathbb{Z}[x]$ be nonzero coprime polynomials ($s \geqslant 2$). The sequence $(d_n)_{n \in \mathbb{Z}}$ is periodic and the finite set $\mathcal{D}^\star = \{d_n\}_{n \in \mathbb{Z}}$ is stable under gcd and under lcm. Consequently, the gcd $d^\star$ and the lcm $m^\star$ of all integers d_n ($n \in \mathbb{Z}$) are in the set $\mathcal{D}^\star$.*

The stability under gcd means that for every $n_1, n_2 \in \mathbb{Z}$, there exists $n \in \mathbb{Z}$ such that $\gcd(d_{n_1}, d_{n_2}) = d_n$. In Example 1, the sequence $(d_n)_{n \in \mathbb{Z}}$ can be checked to be periodic of period 192 and the set $\mathcal{D}^\star$ is indeed stable under gcd and lcm.

A consequence of Theorem 1.1 is the following result, proved in [Sch3, Theorem 1]; as discussed below in Section 3, it is a "coprime" version of the Schinzel Hypothesis.

Corollary 1.2. *Assume that $s \geqslant 2$ and $f_1(x), \ldots, f_s(x)$ are coprime polynomials. Assume further that no prime number divides all integers $f_1(n), \ldots, f_s(n)$ for every $n \in \mathbb{Z}$. Then there exist infinitely many $n \in \mathbb{Z}$ such that $f_1(n), \ldots, f_s(n)$ are coprime integers.*

In Example 1, we have $f_1(1) = -3$ and $f_2(0) = 2$, so no prime number divides $f_1(n), f_2(n)$ for every $n \in \mathbb{Z}$. Corollary 1.2 asserts that $f_1(n)$ and $f_2(n)$ are coprime integers for infinitely many $n \in \mathbb{Z}$.

Assuming Theorem 1.1, here is how Corollary 1.2 is deduced.

Proof. The integer $d^\star$, defined as the gcd of all the d_n, is also the gcd of all values $f_1(n), \ldots, f_s(n)$ with $n \in \mathbb{Z}$. The assumption of Corollary 1.2 exactly says that $d^\star = 1$. By Theorem 1.1, we have $1 \in \mathcal{D}^\star$, that is: there exists $n \in \mathbb{Z}$ such that $f_1(n), \ldots, f_s(n)$ are coprime. Due to the periodicity of $(d_n)_{n \in \mathbb{Z}}$, the set of such n is infinite. $\qquad\square$

2. The Schinzel Hypothesis

The Schinzel Hypothesis is the following statement; it was denoted by (H) in [SS].

Schinzel Hypothesis. *Assume that $s \geq 1$ and $f_1(x), \ldots, f_s(x)$ are irreducible in $\mathbb{Z}[x]$. Assume further that no prime number divides the product $\prod_{i=1,\ldots,s} f_i(n)$ for every $n \in \mathbb{Z}$. Then there exist infinitely many integers n such that $f_1(n), \ldots, f_s(n)$ are all prime numbers.*

This statement would imply many other conjectures in number theory. For instance with $f_1(x) = x$ and $f_2(x) = x+2$, it yields the Twin Primes conjecture: there exist infinitely many primes p such that $p + 2$ is also a prime number. It also provides infinitely many prime numbers of the form $n^2 + 1$ with $n \in \mathbb{Z}$; see [SS] and [Rib, Ch. 3 and Ch. 6] for other problems.

The Schinzel Hypothesis is however wide open. It is only known true when $s = 1$ and $\deg(f_1) = 1$, and this case is already quite deep. It is indeed the Dirichlet theorem: if a, b are coprime nonzero integers, then there are infinitely many $\ell \in \mathbb{Z}$ such that $a + \ell b$ is a prime number.

Corollary 1.2 at least provides a "coprime" version of the Schinzel Hypothesis. This coprime version can then be conjoined with the Dirichlet theorem. This yields the following.

Corollary 2.1. *Assume that $f_1(x)$ and $f_2(x)$ are coprime polynomials and that no prime number divides $f_1(n)$ and $f_2(n)$ for every $n \in \mathbb{Z}$. Then, for infinitely many $n \in \mathbb{Z}$, there exist infinitely many $\ell \in \mathbb{Z}$ such that $f_1(n) + \ell f_2(n)$ is a prime number.*

Proof. As no prime number divides $f_1(n)$ and $f_2(n)$ for every $n \in \mathbb{Z}$, we can apply Corollary 1.2 to get infinitely many integers $n \in \mathbb{Z}$ such that $f_1(n)$ and $f_2(n)$ are coprime. By the Dirichlet theorem for primes in an arithmetic progression, for each of these n except roots of the product $f_1 f_2$, there exist infinitely many $\ell \in \mathbb{Z}$ such that $f_1(n) + \ell f_2(n)$ is a prime number. $\square$

Corollary 2.1 extends to the case $s \geq 2$. Under the generalized assumption that no prime divides all $f_1(n), \ldots, f_s(n)$ for every $n \in \mathbb{Z}$, the conclusion becomes: *for infinitely many $n \in \mathbb{Z}$, there exists a "large"[1] set $\mathcal{L} \subset \mathbb{Z}^{s-1}$ of tuples $(\ell_2, \ldots, \ell_s)$ such that $f_1(n) + \ell_2 f_2(n) + \cdots + \ell_s f_s(n)$ is a prime number.* We leave the reader work out the generalization.

---

[1] "Large" should be understood as *Zariski dense* in $\mathbb{Z}^{s-1}$; this is the generalization of "infinite" for a subset $\mathcal{L} \subset \mathbb{Z}^{s-1}$: if a polynomial $P(x_2, \ldots, x_s)$ vanishes at every point of $\mathcal{L}$, it has to be the zero polynomial.

We also obtain this "modulo m" version of the Schinzel Hypothesis.

Corollary 2.2. *For $s \geqslant 1$, assume that no prime integer divides $\prod_{i=1,\dots,s} f_i(n)$ for every $n \in \mathbb{Z}$. Then, given any integer $m > 0$, there exist $n \in \mathbb{Z}$ such that each of the values $f_1(n), \dots, f_s(n)$ is congruent to a prime number modulo m. In fact, there are infinitely many integers n such that for each $i = 1, \dots, s$, there are infinitely many prime numbers p_i such that $f_i(n) = p_i \pmod{m}$.*

Proof. Fix an integer $m > 0$. Consider the two polynomials $F_1(x) = \prod_{j=1,\dots,s} f_j(x)$ and $F_2(x) = m$. Clearly, $F_1(x)$ and $F_2(x)$ satisfy the assumptions of Corollary 1.2. It follows that there exists $n \in \mathbb{Z}$ such that $F_1(n) = f_1(n) \cdots f_s(n)$ is coprime with m. In particular, each of the integers $f_1(n), \dots, f_s(n)$ is coprime with m. Hence, by the Dirichlet theorem, there exists a prime number p_j such that $p_j = f_j(n) + a_j m$ (for some $a_j \in \mathbb{Z}$). In fact the Dirichlet theorem asserts that there are infinitely many such primes p_j. For $j = 1, \dots, s$ the congruences,

$$f_j(n + \ell m) = f_j(n) \pmod{m}$$

provide the infiniteness of the integers n. These congruences are easily deduced from the basic ones for which $f_j(x)$ is a monomial x^k; they will again be used later. $\square$

Corollary 2.2 has this nice special case, which can also be found in Schinzel's paper [Sch2] following works of Sierpiński.

Example 2 (Goldbach Theorem modulo m). Let m, ℓ be two positive integers. Then there exist infinitely many prime numbers p and q such that $p + q = 2\ell \pmod{m}$.

Proof. Take $f_1(x) = x$ and $f_2(x) = 2\ell - x$. As $f_1(1)f_2(1) = 2\ell - 1$ and $f_1(-1)f_2(-1) = -(2\ell + 1)$, no prime number divides $f_1(n)f_2(n)$ for every $n \in \mathbb{Z}$. By Corollary 2.2, there exist $n \in \mathbb{Z}$ and prime numbers p and q such that $f_1(n) = n$ is congruent to $p \pmod{m}$ and $f_2(n) = 2\ell - n$ is congruent to $q \pmod{m}$, whence $p + q = 2\ell \pmod{m}$. $\square$

Another example with $f_1(x) = x$ and $f_2(x) = x + 2$ gives the *Twin Primes Theorem modulo m: For every $m > 0$, there are infinitely many primes p, q such that $q = p + 2 \pmod{m}$.*

3. Proof of Theorem 1.1

After a brief reminder in Section 3.1, Theorem 1.1 is proved in Sections 3.2 and 3.3. Recall that $f_1(x), \ldots, f_s(x)$ are nonzero polynomials with integer coefficients.

3.1. Reminder on coprimality of polynomials.

Denote the gcd of $f_1(x), \ldots, f_s(x)$ in $\mathbb{Q}[x]$ by $d(x)$; it is a polynomial in $\mathbb{Q}[x]$, well-defined up to a nonzero multiplicative constant in $\mathbb{Q}$. Polynomials $f_1(x), \ldots, f_s(x)$ are said to be *coprime* if $d(x)$ is the constant polynomial equal to 1. These characterizations are well-known:

Proposition 3.1. *For $s \geqslant 2$, the following assertions are equivalent:*

(i) $f_1(x), \ldots, f_s(x)$ *are coprime polynomials (i.e., $d(x) = 1$),*

(ii) *the gcd of $f_1(x), \ldots, f_s(x)$ in $\mathbb{Z}[x]$ is a constant polynomial,*

(iii) $f_1(x), \ldots, f_s(x)$ *have no common complex roots,*

(iv) *there exist $u_1(x), \ldots, u_s(x) \in \mathbb{Q}[x]$ such that a Bézout identity is satisfied, i.e.:*

$$u_1(x) f_1(x) + \cdots + u_s(x) f_s(x) = 1.$$

A brief reminder: (iv) $\Rightarrow$ (iii) is obvious; so is (iii) $\Rightarrow$ (ii) (using that $\mathbb{C}$ is algebraically closed); (ii) $\Rightarrow$ (i) is an exercise based on "removing the denominators" and Gauss's Lemma [Lan, IV, §2]; and (i) $\Rightarrow$ (iv) follows from $\mathbb{Q}[x]$ being a Principal Ideal Domain.

In the case of two polynomials, we have this additional equivalence: $f_1(x)$ and $f_2(x)$ are coprime if and only if their resultant $\mathrm{Res}(f_1, f_2) \in \mathbb{Z}$ is non-zero. Section 5 offers an alternate method to check coprimality of two or more polynomials.

For the rest of this section, assume that $s \geqslant 2$ and $f_1(x), \ldots, f_s(x)$ are coprime. Denote by δ the smallest positive integer such that there exist $u_1(x), \ldots, u_s(x) \in \mathbb{Z}[x]$ with $u_1(x) f_1(x) + \cdots + u_s(x) f_s(x) = \delta$. Such an integer exists from the Bézout identity of Proposition 3.1, rewritten after multiplication by the denominators.

3.2. Finiteness of $\mathcal{D}^\star$ and periodicity of $(d_n)_{n \in \mathbb{Z}}$.

Proposition 3.2. *We have the following:*

- *Every integer d_n divides δ ($n \in \mathbb{Z}$). In particular, the set $\mathcal{D}^\star$ is finite.*
- *The sequence $(d_n)_{n \in \mathbb{Z}}$ is periodic of period δ.*

Note that the integer δ need not be the smallest period. Proposition 3.2 is an improved version of results by Frenkel and Pelikán [FP]: for two coprime polynomials $f_1(x)$, $f_2(x)$, they show that every d_n divides the resultant $\mathrm{Res}(f_1, f_2)$ of $f_1(x)$ and $f_2(x)$. In fact our δ divides $\mathrm{Res}(f_1, f_2)$. Next example shows that $\mathrm{Res}(f_1, f_2)$ and δ may be huge and the sequence $(d_n)_{n\in\mathbb{Z}}$ may have a complex behavior despite being periodic.

Example 3.   Let $f(x) = x^8 + x^6 - 3x^4 - 3x^3 + x^2 + 2x - 5$ and $g(x) = 3x^6 + 5x^4 - 4x^2 - 9x + 21$. These two polynomials were studied by Knuth [Knu, Division of polynomials, p. 427]. We have $\mathrm{Res}(f, g) = 25\,095\,933\,394$ and $\delta = 583\,626\,358 = 2 \times 7^2 \times 43 \times 138\,497$. Here are the terms d_n for $0 \leqslant n \leqslant 39$:

1 2 1 2 7 2 1 2 1 2 1 14 1 2 1 2 1 2 7 2 1 86 1 2 1 14 1 2 1 2 1 2 7 2 1 2 1 2 1 98

Higher values occur: for instance $d_{1999} = 4214$, $d_{133\,139} = 276\,994$. For this example, the set $\mathcal{D}^\star$ is exactly the set of all divisors of δ and the smallest period is δ.

Proof of Proposition 3.2. The identity $u_1(n)f_1(n) + \cdots + u_s(n)f_s(n) = \delta$ implies that $d_n = \gcd(f_1(n), \ldots, f_s(n))$ divides δ ($n \in \mathbb{Z}$). To prove that the sequence $(d_n)_{n\in\mathbb{Z}}$ is periodic, we use again that $f_j(n + \ell\delta) = f_j(n) \pmod{\delta}$ for every $\ell \in \mathbb{Z}$ and every $n \in \mathbb{Z}$.

Fix $n, \ell \in \mathbb{Z}$. As d_n divides $f_j(n)$ and δ, then by this congruence, d_n divides $f_j(n + \ell\delta)$. This is true for $j = 1, \ldots, s$, whence d_n divides $d_{n+\ell\delta}$. In the same way we prove that $d_{n+\ell\delta}$ divides d_n ($n, \ell \in \mathbb{Z}$). Thus $d_{n+\ell\delta} = d_n$ and $(d_n)_{n\in\mathbb{Z}}$ is periodic of period δ. □

3.3. Stability by gcd and lcm.

Proposition 3.3. *The set $\mathcal{D}^\star$ is stable under gcd and lcm.*

Denote by $d^\star$ the gcd of all elements of $\mathcal{D}^\star$ and by $m^\star$ the lcm of those of $\mathcal{D}^\star$. Using that $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$ we obtain:

Corollary 3.4. *The integers $d^\star$ and $m^\star$ are elements of $\mathcal{D}^\star$. Furthermore $d^\star = \min(\mathcal{D}^\star)$ is the greatest integer dividing $f_1(n), \ldots, f_s(n)$ for every $n \in \mathbb{Z}$. Similarly $m^\star = \max(\mathcal{D}^\star)$.*

Proof of Proposition 3.3 for the gcd. We only prove the gcd-stability part and leave the lcm part (which we will not use) to the reader.

Let d_{n_1} and d_{n_2} be two elements of $\mathcal{D}^\star$. Let $d(n_1, n_2)$ be their gcd. The goal is to prove that $d(n_1, n_2)$ is an element of $\mathcal{D}^\star$. The integer $d(n_1, n_2)$ can be written:

$$d(n_1, n_2) = \prod_{i \in I} p_i^{\alpha_i}$$

where, for each $i \in I$, p_i is a prime divisor of δ (see Proposition 3.2) and $\alpha_i \in \mathbb{N}$ (maybe $\alpha_i = 0$ for some $i \in I$). Fix $i \in I$. As $p_i^{\alpha_i+1}$ does not divide $d(n_1, n_2)$, $p_i^{\alpha_i+1}$ does not divide d_{n_1} or does not divide d_{n_2}; we name it d_{m_i} with m_i equals n_1 or n_2.

The Chinese remainder theorem provides an integer n, such that

$$n = m_i \pmod{p_i^{\alpha_i+1}} \quad \text{for each } i \in I.$$

By definition, $p_i^{\alpha_i}$ divides $d(n_1, n_2)$, so $p_i^{\alpha_i}$ divides all $f_1(n_1), \ldots, f_s(n_1)$, $f_1(n_2), \ldots, f_s(n_2)$. In particular $p_i^{\alpha_i}$ divides $f_1(m_i), \ldots, f_s(m_i)$, hence also $f_1(n), \ldots, f_s(n)$. Whence $p_i^{\alpha_i}$ divides d_n for each $i \in I$.

Now $p_i^{\alpha_i+1}$ does not divide $f_{j_0}(m_i)$, for some $j_0 \in \{1, \ldots, s\}$. As $f_{j_0}(n) = f_{j_0}(m_i) \pmod{p_i^{\alpha_i+1}}$, then $p_i^{\alpha_i+1}$ does not divide $f_{j_0}(n)$. Hence $p_i^{\alpha_i+1}$ does not divide d_n.

We have proved that $p_i^{\alpha_i}$ is the greatest power of p_i dividing d_n, for all $i \in I$. As d_n divides δ, each prime factor of d_n is one of the p_i. Conclude that $d(n_1, n_2) = d_n$. $\qquad\square$

4. More on the set $\mathcal{D}^\star$

Further questions on the set $\mathcal{D}^\star$ are of interest. The stability under gcd and lcm gives it a remarkable ordered structure. Can more be said about elements of $\mathcal{D}^\star$? The smallest element $d^\star$ particularly stands out: it is also the gcd of all values $f_1(n), \ldots, f_s(n)$ with $n \in \mathbb{Z}$. Can one determine or at least estimate $d^\star$?

Proposition 4.1. *Assume that $f_1(x), \ldots, f_s(x)$ are monic. Then $d^\star$ divides each of the integers $(\deg f_1)!, \ldots, (\deg f_s)!$.*

The proof relies on the following result.

Lemma 4.2. *Let $f(x) = a_d x^d + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}[x]$ of degree d. Fix an integer $T > 0$ and fix $m \in \mathbb{Z}$. If an integer k divides each of $f(m), f(m+T), f(m+2T), \ldots$ then k divides $a_d T^d d!$.*

For $T = 1$, this lemma was obtained by Schinzel in [Sch1]. If $f(x)$ is assumed to be a primitive polynomial (i.e., the gcd of its coefficients is 1) and k divides $f(m+\ell T)$ (for all $\ell \in \mathbb{Z}$) then Bhargava's paper [Bha] implies that k divides $T^d d!$ (see theorem 9 and example 17 there). Moreover using a theorem of Pólya

(see [Bha, Theorem 2]), in Proposition 4.1, we could replace the hypothesis "$f_j(x)$ is monic" by "$f_j(x)$ is primitive" with the same conclusion on $d^\star$.

We give an elementary proof below of Lemma 4.2 which was suggested to us by Bruno Deschamps. It uses the following operator:

$$\Delta: \quad \mathbb{Q}[x] \quad \longrightarrow \quad \mathbb{Q}[x]$$
$$P(x) \quad \longmapsto \quad \frac{P(x+T)-P(x)}{T}.$$

If $P(x) = a_d x^d + \cdots + a_0$ is a polynomial of degree d, then $\Delta(P)(x)$ is a polynomial of degree $d - 1$ of the form $\Delta(P)(x) = da_d x^{d-1} + \cdots$ By induction, if we iterate this operator d times, we obtain that $\Delta^d(P)(x) = d!a_d$ is a constant polynomial. The polynomial $\Delta(P)(x)$ is a discrete analog of the derivative $P'(x)$. In particular $\Delta^d(P)(x) = d!a_d$ should be related to the higher derivative $P^{(d)}(x) = d!a_d$.

Proof of Lemma 4.2. The key observation is that if k divides $f(m)$ and $f(m+T)$, then k divides $T\Delta(f)(m)$. We prove the statement by induction on the degree d.

- For $d = 0$, "k divides $f(m)$" is exactly saying "k divides a_0".
- Fix $d > 0$ and suppose that the statement is true for polynomials of degree less than d. Let $f(x) = a_d x^d + \cdots + a_0$ be a polynomial of degree d satisfying the hypothesis. As k divides $f(m + \ell T)$ for all $\ell \in \mathbb{N}$, then k divides
$$T\Delta(f)(m + \ell T) = f(m + (\ell + 1)T) - f(m + \ell T).$$
  By induction applied to $T\Delta(f)(x) = Tda_d x^{d-1} + \cdots$, the integer k divides the integer $(Tda_d)T^{d-1}(d-1)! = a_d T^d d!$. □

Proof of Proposition 4.1. For each $j = 1, \ldots, s$, the integer $d^\star$ divides $f_j(n)$ for every $n \in \mathbb{Z}$. Thus $d^\star$ divides $(\deg f_j)!$ by Lemma 4.2 (applied with $T = 1$ and $a_d = 1$). □

We can also derive a result for $m^\star = \max(\mathcal{D}^\star) = \operatorname{lcm}(\mathcal{D}^\star)$.

Proposition 4.3. *Let* T *be the smallest period of the sequence* $(d_n)_{n \in \mathbb{Z}}$ *and* $f_1(x) = a_d x^d + \cdots$ *be a polynomial of degree* d*. Then:*

$$T \mid m^\star \qquad and \qquad m^\star \mid a_d T^d d!$$

Proof. The proof that $m^\star$ is a period is the same as the one for δ (see Proposition 3.2). It follows that T divides $m^\star$. On the other hand, if $(d_n)_{n \in \mathbb{Z}}$ is periodic of period T, then every term d_n divides $f_1(n + \ell T)$ for all $\ell \in \mathbb{Z}$. By Lemma 4.2, d_n divides $a_d T^d d!$. This is true for each n, so $m^\star = \operatorname{lcm}\{d_n\}_{n \in \mathbb{Z}}$ also divides $a_d T^d d!$. □

5. A coprimality criterion for polynomials

A constant assumption of the paper has been that our polynomials $f_1(x), \dots,$ $f_s(x)$ are coprime. To test this condition, we offer here a criterion only using the values $f_1(n), \dots, f_s(n)$ that may be more practical than the characterizations from Proposition 3.1.

Define the *normalized height* of a degree d polynomial $f(x) = a_d x^d + \dots + a_0$ by

$$H(f) = \max_{i=0,\dots,d-1} \left| \frac{a_i}{a_d} \right|.$$

Proposition 5.1. *Let H be the minimum of the normalized heights $H(f_1), \dots, H(f_s)$. The polynomials $f_1(x), \dots, f_s(x)$ are coprime if and only if there exists $n \geq 2H + 3$ such that $\gcd(f_1(n), \dots, f_s(n)) \leq \sqrt{n}$.*

In particular if $f_1(n), \dots, f_s(n)$ are coprime (as integers) for some sufficiently large n then $f_1(x), \dots, f_s(x)$ are coprime (as polynomials).

Example 4.

- Take $f_1(x) = x^4 - 7x^3 + 3$, $f_2(x) = x^3 - 3x + 3$. We have $H(f_1) = 7$, $H(f_2) = 3$, so $H = 3$. For $n = 9 (= 2H + 3)$, we have $f_1(n) = 1461$, $f_2(n) = 705$. Thus $\gcd(f_1(n), f_2(n)) = 3 \leq \sqrt{n}$. From Proposition 5.1, the polynomials $f_1(x)$ and $f_2(x)$ are coprime.

- Here is an example for which the polynomials are not coprime. Take $f_1(x) = x^2 - 1 = (x + 1)(x - 1)$, $f_2(x) = x^2 + 2x + 1 = (x + 1)^2$. Then $\gcd(f_1(x), f_2(x)) = x + 1$ and $\gcd(f_1(n), f_2(n)) \geq n + 1$.

Remark. Proposition 5.1 is a coprime analog of the classical idea consisting in using prime values of polynomials to prove their irreducibility. For instance there is this irreducibility criterion by Ram Murty [RM], which can be seen as a converse to the Bunyakovsky conjecture: *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of normalized height H. If $f(n)$ is prime for some $n \geq H + 2$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.*

We first need a classical estimate for the localization of the roots of a polynomial, as in [RM].

Lemma 5.2 (Cauchy bound). *Let $f(x) = a_d x^d + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial of degree d and of normalized height H. Let $\alpha \in \mathbb{C}$ be a root of f. Then $|\alpha| < H + 1$.*

Proof of Lemma 5.2. We may assume $|\alpha| > 1$, since for $|\alpha| \leqslant 1$, Lemma 5.2 is obviously true. As $f(\alpha) = 0$, α satisfies:

$$\left| a_d \alpha^d \right| = \left| a_{d-1} \alpha^{d-1} + \cdots + a_1 \alpha + a_0 \right| \leqslant \sum_{i=0}^{d-1} \left| a_i \alpha^i \right|.$$

By dividing by a_d, we get:

$$\left| \alpha^d \right| \leqslant \sum_{i=0}^{d-1} H \left| \alpha^i \right| = H \frac{|\alpha|^d - 1}{|\alpha| - 1} \quad \text{then} \quad |\alpha| - 1 \leqslant H \frac{|\alpha|^d - 1}{|\alpha^d|} = H \left(1 - \frac{1}{|\alpha|^d} \right).$$

So that $|\alpha| - 1 \leqslant H$ and the proof is over.   □

Proof of Proposition 5.1.

- $\implies$ Since $f_1(x), \ldots, f_s(x)$ are coprime polynomials, we have a Bézout identity: $u_1(x) f_1(x) + \cdots + u_s(x) f_s(x) = 1$ for some $u_1(x), \ldots, u_s(x)$ in $\mathbb{Q}[x]$. By multiplying by an integer $k \in \mathbb{Z} \setminus \{0\}$, we obtain $\tilde{u}_1(x) f_1(x) + \cdots + \tilde{u}_s(x) f_s(x) = k$, with $\tilde{u}_1(x), \ldots, \tilde{u}_s(x)$ being this time in $\mathbb{Z}[x]$. This gives $\tilde{u}_1(n) f_1(n) + \cdots + \tilde{u}_s(n) f_s(n) = k$ for all $n \in \mathbb{Z}$, so that $\gcd(f_1(n), \ldots, f_s(n))$ divides k. Thus the gcd of $f_1(n), \ldots, f_s(n)$ is bounded, hence it is $\leqslant \sqrt{n}$ for all sufficiently large n.

- $\impliedby$ Let $d(x) \in \mathbb{Z}[x]$ be a common divisor of $f_1(x), \ldots, f_s(x)$ in $\mathbb{Z}[x]$. By contradiction, assume that $d(x)$ is not a constant polynomial. Consider an integer $n \geqslant 2H + 3$ such that $\gcd(f_1(n), \ldots, f_s(n)) \leqslant \sqrt{n}$. On the one hand $d(n)$ divides each of the $f_1(n), \ldots, f_s(n)$, so $|d(n)| \leqslant \gcd(f_1(n), \ldots, f_s(n)) \leqslant \sqrt{n}$.

  On the other hand

  $$d(n) = c \prod_{i \in I} (n - \alpha_i)$$

  for some roots $\alpha_i \in \mathbb{C}$, $i \in I$, of f_1 (and of the other f_j), and $c \in \mathbb{Z} \setminus \{0\}$. By Lemma 5.2, we obtain:

  $$|d(n)| = |c| \prod_i |n - \alpha_i| > |c| \prod_i |n - (H+1)| \geqslant |n - (H+1)|.$$

  We obtain $|n - (H+1)| \leqslant \sqrt{n}$, which is impossible for $n \geqslant 2H + 3$.

  We conclude that the common divisors of $f_1(x), \ldots, f_s(x)$ in $\mathbb{Z}[x]$ are constant. Therefore by Proposition 3.1, the polynomials $f_1(x), \ldots, f_s(x)$ are coprime.   □

6. Polynomials in several variables

The Schinzel Hypothesis and its coprime variant can be considered with the ring $\mathbb{Z}$ replaced by a more general integral domain Z. Papers [BDN1] and [BDN2] are devoted to this. The special case that Z is a polynomial ring $\mathbb{Z}[\underline{u}]$ stands out; here $\underline{u}$ can be a single variable or a tuple $(u_1, \ldots, u_r)$ of several variables. "Prime in $\mathbb{Z}[\underline{u}]$" then means "irreducible in $\mathbb{Z}[\underline{u}]$".

In [BDN1], we prove the Schinzel Hypothesis for $\mathbb{Z}[\underline{u}]$ instead of $\mathbb{Z}$:

Theorem 6.1. *With $s \geqslant 1$, let $f_1(\underline{u}, x), \ldots, f_s(\underline{u}, x)$ be s polynomials, irreducible in $\mathbb{Z}[\underline{u}, x]$, of degree $\geqslant 1$ in x. Then there are infinitely many polynomials $n(\underline{u}) \in \mathbb{Z}[\underline{u}]$ (with partial degrees as large as desired) such that*

$$f_i\big(\underline{u}, n(\underline{u})\big)$$

is an irreducible polynomial in $\mathbb{Z}[\underline{u}]$ for each $i = 1, \ldots, s$.

We also prove the Goldbach conjecture for polynomials: *any nonconstant polynomial in $\mathbb{Z}[\underline{u}]$ is the sum of two irreducible polynomials of lower or equal degree.* Furthermore, Theorem 6.1 is shown to also hold with the coefficient ring $\mathbb{Z}$ replaced by more general rings R, e.g. $R = \mathbb{F}_q[t]$. However not all integral domains are allowed. For example, with $\underline{u}$ a single variable, the result is obviously false with $R = \mathbb{C}$, is known to be false for $R = \mathbb{F}_q$ by a result of Swan [Swa] and is unclear for $R = \mathbb{Z}_p$.

In contrast, we prove in [BDN2] that the coprime analog of Theorem 6.1 holds in a much bigger generality.

Theorem 6.2. *Let R be a Unique Factorization Domain and assume that $R[\underline{u}]$ is not the polynomial ring $\mathbb{F}_q[u_1]$ in a single variable over a finite field. With $s \geqslant 2$, let $f_1(\underline{u}, x), \ldots, f_s(\underline{u}, x)$ be s nonzero polynomials, with no common divisor in $R[\underline{u}, x]$ other than units of R. Then there are infinitely many polynomials $n(\underline{u}) \in R[\underline{u}]$ such that*

$$f_1\big(\underline{u}, n(\underline{u})\big), \ \ldots, \ f_s\big(\underline{u}, n(\underline{u})\big)$$

have no common divisor in $R[\underline{u}]$ other than units of R.

Theorem 6.2 fails if $R[\underline{u}] = \mathbb{F}_q[u_1]$. Take indeed $f_1(u_1, x) = x^q - x + u_1$ and $f_2(u_1, x) = (x^q - x)^2 + u_1$. For every $n(u_1) \in \mathbb{F}_q[u_1]$, the constant term of $n(u_1)^q - n(u_1)$ is zero, so $f_1(u_1, n(u_1))$ and $f_2(u_1, n(u_1))$ are divisible by u_1.

References

[BDN1]   A. BODIN, P. DÈBES and S. NAJIB, The Schinzel hypothesis for polynomials. Preprint (2019a). arXiv:1902.08155. To appear in *Trans. Math. AMS*.

[BDN2]   —— The relative Schinzel hypothesis. Preprint (2019b). arXiv:2002.05030

[Bha]   M. BHARGAVA, The factorial function and generalizations. *Amer. Math. Monthly* **107** (2000), 783–799. Zbl 0987.05003 MR 1792411

[FP]   P. E. FRENKEL and J. PELIKÁN, On the greatest common divisor of the value of two polynomials. *Amer. Math. Monthly* **124** (2017), 446–450. Zbl 1391.11059 MR 3633975

[Knu]   D. E. KNUTH, *The Art of Computer Programming*. Vol. 2. *Seminumerical Algorithms*, Third edition. Addison-Wesley, Reading, MA (1998). Zbl 0895.65001 MR 3077153

[Lan]   S. LANG, *Algebra*. Vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third ed. (2002). Zbl 0984.00001 MR 1878556

[Rib]   P. RIBENBOIM, *The New Book of Prime Number Records*. Springer-Verlag, New York (1996). Zbl 0856.11001 MR 1377060

[RM]   M. RAM MURTY, Prime numbers and irreducible polynomials. *Amer. Math. Monthly* **109** (2002), 452–458. Zbl 1053.11020 MR 1901498

[Sch1]   A. SCHINZEL, Sur les diviseurs naturels des polynômes. *Matematiche* (*Catania*) **12** (1957), 18–22. Zbl 0178.37402 MR 0130248

[Sch2]   —— Démonstration d'une conséquence de l'hypothèse de Goldbach. *Compositio Math.* **14** (1959), 74–76. Zbl 0101.03302 MR 0103870

[Sch3]   —— A property of polynomials with an application to Siegel's lemma. *Monatsh. Math.* **137** (2002), 239–251. Zbl 1116.11304 MR 1942622

[SS]   A. SCHINZEL and W. SIERPIŃSKI, Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.* **4** (1958), 185–208; erratum 5 (1958), 259. Zbl 0082.25802 MR 0106202

[Swa]   R. G. SWAN, Factorization of polynomials over finite fields. *Pacific J. Math.* **12** (1962), 1099–1106. projecteuclid.org/euclid.pjm/1103036322 Zbl 0113.01701 MR 0144891

(Reçu le 7 février 2020)

Arnaud BODIN, Université de Lille, CNRS, Laboratoire Paul Painlevé, 59000 Lille, France

e-mail: arnaud.bodin@univ-lille.fr

Pierre Dèbes, Université de Lille, CNRS, Laboratoire Paul Painlevé,
59000 Lille, France

e-mail: pierre.debes@univ-lille.fr

Salah Najib, Laboratoire ATRES, Faculté Polydisciplinaire de Khouribga,
Université Sultan Moulay Slimane, BP 145, Hay Ezzaytoune,
25000 Khouribga, Maroc

e-mail: slhnajib@gmail.com