An. Şt. Univ. Ovidius Constanţa Vol. 19(2), 2011, 37–54

From prime numbers to irreducible multivariate polynomials

Nicolae Ciprian Bonciocat

Abstract

We present several methods to produce irreducible multivariate polynomials, starting from sufficiently large prime numbers.

1 Introduction

There are many irreducibility criteria for multivariate polynomials in the literature. Some recent irreducibility results have been obtained for various classes of polynomials in several variables, such as linear combinations of relatively prime polynomials [11], compositions of polynomials [6], [1], multiplicative convolutions [3], polynomials having one coefficient of dominant degree [7], lacunary polynomials [2], and polynomials obtained from irreducible polynomials in fewer variables [8], [9]. For an excellent account on the techniques used in the study of reducibility of polynomials over arbitrary fields the reader is referred to Schinzel's book [15].

The aim of this expository paper is to present some of the results in [4], [5], [8] and [9] and to show how to use them to provide methods to produce irreducible multivariate polynomials starting from sufficiently large prime numbers. This will be achieved by combining some irreducibility criteria for multivariate polynomials with some irreducibility criteria for polynomials with integer coefficients that rely on the use of prime numbers.

The paper is organized as follows. In Section 2, we first present some classical irreducibility criteria of A. Cohn, J. Brillhart, M. Filaseta and A. Odlyzko for polynomials with integer coefficients, that are obtained by using the digits of a prime number. We then present some irreducibility criteria

Key Words: prime number, irreducibility, nonarchimedean absolute value.
Mathematics Subject Classification: 11R09, 11C08.

for polynomials that have one large coefficient and take a prime value, or a prime power value. Section 3 is devoted to some recent results that provide methods to produce irreducible multivariate polynomials over arbitrary fields from irreducible polynomials in fewer variables. In Section 4 we combine some of the results in Sections 2 and 3, to provide methods to produce irreducible multivariate polynomials directly from prime numbers. Some examples of irreducible multivariate polynomials obtained from prime numbers are given in the last section of the paper.

2 Irreducible polynomials obtained by using the digits of a prime number

One of the most elegant irreducibility criterion that relies on the existence of a suitable prime divisor of the value that a given polynomial takes at a specified integral argument, is due to A. Cohn (see Pólya and Szegö [16]).

Theorem 2.1. *(A. Cohn) If a prime p is expressed in the decimal system as*

$$p=\sum_{i=0}^{n}a_i10^i,\quad 0\leq a_i\leq 9,$$

then the polynomial $\sum_{i=0}^{n}a_iX^i$ is irreducible in $\mathbb{Z}[X]$.

This result was generalised to an arbitrary base b by Brillhart, Filaseta and Odlyzko [10].

Theorem 2.2. *If a prime p is expressed in the number system with base $b\geq 2$ as*

$$p=\sum_{i=0}^{n}a_ib^i,\quad 0\leq a_i\leq b-1,$$

then the polynomial $\sum_{i=0}^{n}a_iX^i$ is irreducible in $\mathbb{Z}[X]$.

For elementary proofs of these results and several nice connections between prime numbers and irreducible polynomials, the reader is referred to [17] and [14]. As expected, primes are not the only numbers enjoying this nice property. In this respect, Filaseta [12] obtained another generalization of Cohn's Theorem by replacing the prime p by a composite number wp with $w<b$:

Theorem 2.3. *(Filaseta) Let p be a prime number, w and b positive integers, $b\geq 2$, $w<b$, $wp\geq b$ and suppose that wp is expressed in the number system with base b as*

$$wp=\sum_{i=0}^{n}a_ib^i,\quad 0\leq a_i\leq b-1.$$

Then the polynomial $\sum_{i=0}^{n} a_i X^i$ *is irreducible over* $\mathbb{Q}$.

Cohn's Theorem was also generalized in [10] and [13] by allowing the coefficients of f to be different from digits. In this respect, the following irreducibility criterion for polynomials with non-negative coefficients was proved in [13].

Theorem 2.4. *(Filaseta) Let* $f(X) = \sum_{i=0}^{n} a_i X^i$ *be such that* $f(10)$ *is a prime. If the* a_i*'s satisfy* $0 \le a_i \le a_n 10^{30}$ *for each* $i = 0, 1, \dots, n-1$, *then* $f(X)$ *is irreducible over* $\mathbb{Q}$.

Inspired by these results, we proved in [4] some irreducibility criteria for polynomials that have one large coefficient and take a prime value.

Theorem 2.5. *Let* $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, $a_0 a_n \neq 0$. *Suppose that for an integer* m, *a prime number* p *and a nonzero integer* q *we have* $f(m) = p \cdot q$ *and*

$$|a_0| > \sum_{i=1}^{n} |a_i| \cdot (|m| + |q|)^i.$$

Then f *is irreducible over* $\mathbb{Q}$.

As an immediate consequence, we obtained the following flexible method to produce irreducible polynomials from prime numbers.

Corollary 2.6. *If we write a prime number as a sum of integers* $a_0, \dots, a_n$, *with* $a_0 a_n \neq 0$ *and* $|a_0| > \sum_{i=1}^{n} |a_i| 2^i$, *then the polynomial* $\sum_{i=0}^{n} a_i X^i$ *is irreducible over* $\mathbb{Q}$.

Theorem 2.7. *Let* $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, $a_0 a_n \neq 0$. *Suppose that for a prime number* p *and two nonzero integers* m *and* q *with* $|m| > |q|$ *we have* $f(m) = p \cdot q$ *and*

$$|a_n| > \sum_{i=0}^{n-1} |a_i| \cdot (|m| - |q|)^{i-n}.$$

Then f *is irreducible over* $\mathbb{Q}$.

The conditions in Theorem 2.7 take a simpler form in the case of Littlewood polynomials (polynomials all of whose coefficients are ± 1).

Corollary 2.8. *If* f *is a Littlewood polynomial and* $f(m)$ *is a prime number for an integer* m *with* $|m| \ge 3$, *then* f *is irreducible over* $\mathbb{Q}$.

We note here that the condition $|m| \geq 3$ is the best possible, in the sense that there exist Littlewood polynomials f such that $f(2)$ or $f(-2)$ is a prime number, and which are reducible. To see this, one may consider $f_1(X) = X^3 - X^2 + X - 1$ and $f_2(X) = -X^3 - X^2 - X - 1$. Here $f_1(2) = 5$, $f_2(-2) = 5$, and f_1, f_2 are obviously reducible. We also note that one may replace in Corollary 2.8 the Littlewood polynomials by integer polynomials with coefficients of modulus at most 1.

Theorem 2.9. *Let $f(X) = \sum_{i=0}^{n} a_i X^{d_i} \in \mathbb{Z}[X]$, with $0 = d_0 < d_1 < \cdots < d_n$ and $a_0 a_1 \cdots a_n \neq 0$. Suppose that for an integer m, a prime number p and a nonzero integer q with $|m| > |q|$ we have $f(m) = p \cdot q$. If for an index $j \in \{1, \ldots, n-1\}$ we have*

$$|a_j| > (|m| + |q|)^{d_n - d_j} \cdot \sum_{i \neq j} |a_i|,$$

then f is irreducible over $\mathbb{Q}$.

One may naturally ask whether Cohn's result will still hold true if we replace the prime number p with p^s, $s \geq 2$. This is by no means necessarily true, as one can see by taking $p = 11$ and considering the polynomial $f(X)$ obtained by replacing the powers of 10 by the corresponding powers of X in the decimal representation of 11^2. In this case $f(10) = 121$, and the polynomial $f(X) = X^2 + 2X + 1$ is obviously reducible. For another example one may consider the decimal representation of 11^7. Here $f(10) = 11^7 = 19\,487\,171$, and the polynomial $f(X)$ is also reducible, being divisible by $X + 1$:

$$\begin{aligned} f(X) &= X^7 + 9X^6 + 4X^5 + 8X^4 + 7X^3 + X^2 + 7X + 1 \\ &= (X+1)(X^6 + 8X^5 - 4X^4 + 12X^3 - 5X^2 + 6X + 1). \end{aligned}$$

In [5] we found some additional conditions that guarantee us the irreducibility of a polynomial that takes a prime power value, and this allowed us to complement the results in [4], by extending them to a larger class of polynomials. This was achieved by adding a natural condition on the derivative of our polynomials. In [5] we also derived upper bounds for the total number of irreducible factors of such polynomials, instead of irreducibility criteria, by considering their higher derivatives. The following result, proved in [5], extends Theorem 2.2 to prime powers, as follows.

Theorem 2.10. *If a prime power p^s, $s \geq 2$, is expressed in the number system with base $b \geq 2$ as $p^s = \sum_{i=0}^{n} a_i b^i$, with $0 \leq a_i \leq b - 1$ and $p \nmid \sum_{i=1}^{n} i a_i b^{i-1}$, then the polynomial $\sum_{i=0}^{n} a_i X^i$ is irreducible over $\mathbb{Q}$.*

The following results give irreducibility conditions for polynomials that have one coefficient of sufficiently large modulus and take a value divisible by a prime power p^s, $s \geq 2$.

Theorem 2.11. *Let $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, $a_0 a_n \neq 0$. Suppose that $f(m) = p^s \cdot q$ for some integers m, s, q and a prime number p, with $s \geq 2$, $p \nmid qf'(m)$ and*

$$|a_0| > \sum_{i=1}^{n} |a_i| \cdot (|m| + |q|)^i.$$

Then f is irreducible over $\mathbb{Q}$.

In particular, for $m = q = 1$ we obtained the following flexible irreducibility criterion, that extends Corollary 2.6 to prime powers.

Corollary 2.12. *If we write a prime power p^s, $s \geq 2$, as a sum of integers $a_0, \ldots, a_n$ with $a_0 a_n \neq 0$, $|a_0| > \sum_{i=1}^{n} |a_i| 2^i$, and $a_1 + 2a_2 + \cdots + na_n$ is not divisible by p, then the polynomial $\sum_{i=0}^{n} a_i X^i$ is irreducible over $\mathbb{Q}$.*

Theorem 2.13. *Let $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, $a_0 a_n \neq 0$. Suppose that $f(m) = p^s \cdot q$, for some integers m, s, q and a prime number p, with $s \geq 2$, $|m| > |q|$, $p \nmid qf'(m)$ and*

$$|a_n| > \sum_{i=0}^{n-1} |a_i| \cdot (|m| - |q|)^{i-n}.$$

Then f is irreducible over $\mathbb{Q}$.

Corollary 2.14. *Let f be a Littlewood polynomial. If $f(m)$ is a prime power p^s, $s \geq 2$, for an integer m with $|m| \geq 3$, and $p \nmid f'(m)$, then f is irreducible over $\mathbb{Q}$.*

Here too, as in Corollary 2.8, one may replace the Littlewood polynomials by integer polynomials with coefficients of modulus at most 1.

Theorem 2.15. *Let $f(X) = \sum_{i=0}^{n} a_i X^{d_i} \in \mathbb{Z}[X]$, with $0 = d_0 < d_1 < \cdots < d_n$ and $a_0 a_1 \cdots a_n \neq 0$. Suppose that $f(m) = p^s \cdot q$, for some integers m, s, q and a prime number p, with $s \geq 2$, $|m| > |q|$ and $p \nmid qf'(m)$. If for an index $j \in \{1, \ldots, n-1\}$ we have*

$$|a_j| > (|m| + |q|)^{d_n - d_j} \cdot \sum_{i \neq j} |a_i|,$$

then f is irreducible over $\mathbb{Q}$.

In particular, Theorems 2.11, 2.13 and 2.15 show that, if $f(m)$ is a prime power for an integer m with $|m| \geq 2$, $f(m)$ and $f'(m)$ are relatively prime, and f has one coefficient of sufficiently large modulus, then f must be irreducible over $\mathbb{Q}$. For the proof of the results in this section we refer the reader to [4] and [5].

3 Irreducible multivariate polynomials obtained from irreducible polynomials in fewer variables

The reader may naturally ask whether we can produce irreducible multivariate polynomials from irreducible polynomials in fewer variables in the same way in which the irreducible polynomials are constructed from prime numbers in the theorems in Section 2 above. More precisely, given an arbitrary field K, one may ask under what hypotheses a polynomial $F(X,Y) \in K[X,Y]$ such that $F(X,h(X))$ is irreducible over K for some $h \in K[X]$, is necessarily irreducible over $K(X)$. Then, instead of asking $F(X,h(X))$ to be irreducible over K for some $h \in K[X]$, we allow F to satisfy the equality $F(X,h(X)) = f(X)^s \cdot g(X)$, with $f,g \in K[X]$, f irreducible over K, $g \neq 0$, $s \geq 2$, and ask under what hypotheses F will still be irreducible over $K(X)$. In [8] and [9] we established such hypotheses and obtained some efficient methods to construct irreducible multivariate polynomials over an arbitrary field, starting from arbitrary irreducible polynomials in a smaller number of variables. The following two results provide such hypotheses, expressed in terms of the slopes of the edges of a Newton polygon, together with a condition involving a partial derivative of our polynomials.

Theorem 3.1. *Let K be a field and $F(X,Y) = \sum_{i=0}^{n} a_i(X)Y^i \in K[X,Y]$, with $a_i \in K[X]$, $i = 0,\ldots,n$, $a_0a_n \neq 0$. Let us assume that there exist three polynomials $f,g,h \in K[X]$ such that f is irreducible over K, $g \neq 0$ and $F(X,h(X)) = f(X) \cdot g(X)$. Then F is irreducible over $K(X)$ if either $\deg g < \deg h$ and for an index $j \in \{1,\ldots,n\}$ with $a_j \neq 0$ we have*

$$\max_{k<j} \frac{\deg a_k - \deg a_j}{j-k} < \deg h < \min_{k>j} \frac{\deg a_k - \deg a_j}{j-k}, \tag{1}$$

or if

$$\min_{k>0} \frac{\deg a_0 - \deg a_k}{k} > \max\{\deg h,\ \deg g\}. \tag{2}$$

Theorem 3.2. *Let K be a field and $F(X,Y) = \sum_{i=0}^{n} a_i(X)Y^i \in K[X,Y]$, with $a_i \in K[X]$, $i = 0,\ldots,n$, $a_0a_n \neq 0$. Let us assume that there exist three polynomials $f,g,h \in K[X]$ such that f is irreducible over K, $g \neq 0$, $F(X,h(X)) = f(X)^s \cdot g(X)$, for an integer $s \geq 2$, and $\partial F/\partial Y(X,h(X))$ is not* *divisible by f. Then F is irreducible over $K(X)$ if either* $\deg g < \deg h$ *and for an index $j \in \{1, \ldots, n\}$ with $a_j \neq 0$ we have*

$$\max_{k<j} \frac{\deg a_k - \deg a_j}{j-k} < \deg h < \min_{k>j} \frac{\deg a_k - \deg a_j}{j-k}, \tag{3}$$

or if

$$\min_{k>0} \frac{\deg a_0 - \deg a_k}{k} > \max\{\deg h,\ \deg g\}. \tag{4}$$

For the sake of the reader, we will include here a proof of the Theorem 3.1.

Proof: One may prove this result by using a Newton polygon argument. Instead, we will give as in [8] a proof based on the study of the location of the roots of F, regarded as a polynomial in Y with coefficients in $K[X]$. We first introduce a nonarchimedean absolute value $|\cdot|$ on $K(X)$, as follows. We fix an arbitrary real number $\delta > 1$, and for any polynomial $u(X) \in K[X]$ we define $|u(X)|$ by the equality

$$|u(X)| = \delta^{\deg u(X)}.$$

We then extend the absolute value $|\cdot|$ to $K(X)$ by multiplicativity. Thus for any $w(X) \in K(X)$, $w(X) = \frac{u(X)}{v(X)}$, with $u(X), v(X) \in K[X]$, $v(X) \neq 0$, we let $|w(X)| = \frac{|u(X)|}{|v(X)|}$. We note here that for any non-zero element u of $K[X]$ one has $|u| \geq 1$. Let now $\overline{K(X)}$ be a fixed algebraic closure of $K(X)$, and let us fix an extension of our absolute value $|\cdot|$ to $\overline{K(X)}$, which we will also denote by $|\cdot|$.

Assume by contrary that our polynomial F decomposes as $F(X,Y) = F_1(X,Y) \cdot F_2(X,Y)$, with $F_1,\ F_2 \in K[X,Y]$, $\deg_Y F_1 = t \geq 1$ and $\deg_Y F_2 = s \geq 1$. Since

$$F(X, h(X)) = f(X) \cdot g(X) = F_1(X, h(X)) \cdot F_2(X, h(X))$$

and f is irreducible over K, it follows that one of the polynomials $F_1(X, h(X))$, $F_2(X, h(X))$ must divide $g(X)$, say $F_1(X, h(X)) \mid g(X)$. In particular, one has

$$\deg F_1(X, h(X)) \leq \deg g(X). \tag{5}$$

We consider now the factorisation of the polynomial $F(X,Y)$ over $\overline{K(X)}$, say $F(X,Y) = a_n(X)(Y - \xi_1) \cdots (Y - \xi_n)$, with $\xi_1, \ldots, \xi_n \in \overline{K(X)}$. Since $a_0 \neq 0$ we must have $|\xi_i| \neq 0$, $i = 1, \ldots, n$. Let us denote

$$A = \max_{k<j} \frac{\deg a_k - \deg a_j}{j-k} \quad \text{and} \quad B = \min_{k>j} \frac{\deg a_k - \deg a_j}{j-k},$$

and notice that by (1) A is strictly smaller than B. Then for each $i = 1, \dots, n$ we must either have $|\xi_i| \leq \delta^A$, or $|\xi_i| \geq \delta^B$. In order to prove this, let us assume by contrary that for some index $i \in \{1, \dots, n\}$ we have $\delta^A < |\xi_i| < \delta^B$. Since $a_j \neq 0$ we deduce from $\delta^A < |\xi_i|$ that $|a_j| \cdot |\xi_i|^j > |a_k| \cdot |\xi_i|^k$ for each $k < j$, while from $|\xi_i| < \delta^B$ we find that $|a_j| \cdot |\xi_i|^j > |a_k| \cdot |\xi_i|^k$ for each $k > j$. By taking the maximum with respect to k in these inequalities, we obtain

$$|a_j| \cdot |\xi_i|^j > \max_{k \neq j} |a_k| \cdot |\xi_i|^k. \tag{6}$$

On the other hand, since $F(X, \xi_i) = 0$, we must have

$$0 \geq |a_j \xi_i^j| - |\sum_{k \neq j} a_k \xi_i^k| \geq |a_j| \cdot |\xi_i|^j - \max_{k \neq j} |a_k| \cdot |\xi_i|^k,$$

which contradicts (6).

Now, since $F_1(X, Y)$ is a factor of our polynomial $F(X, Y)$, it will factorize over $\overline{K(X)}$ as $F_1(X, Y) = b_t(X)(Y - \xi_1) \cdots (Y - \xi_t)$, say, with $b_t(X) \in K[X]$, $b_t(X) \neq 0$. In particular, we have

$$|b_t(X)| \geq 1. \tag{7}$$

Recalling the definition of our absolute value and using (5) and (7), we then deduce that

$$\begin{aligned} \delta^{\deg g} \geq \delta^{\deg F_1(X, h(X))} &= |F_1(X, h(X))| \\ &= |b_t(X)| \cdot \prod_{i=1}^{t} |h(X) - \xi_i| \geq \prod_{i=1}^{t} |h(X) - \xi_i|. \end{aligned}$$

Now, for any index $i \in \{1, \dots, t\}$ we either have

$$|h(X) - \xi_i| \geq |h(X)| - |\xi_i| \geq \delta^{\deg h} - \delta^A, \quad \text{if} \quad |\xi_i| \leq \delta^A,$$

or

$$|h(X) - \xi_i| \geq |\xi_i| - |h(X)| \geq \delta^B - \delta^{\deg h}, \quad \text{if} \quad |\xi_i| \geq \delta^B.$$

Since $A < \deg h < B$ it follows that for a large enough δ both the quantities $\delta^{\deg h} - \delta^A$ and $\delta^B - \delta^{\deg h}$ become greater than 1, and hence we must have

$$\delta^{\deg g} \geq \min\{\delta^{\deg h} - \delta^A, \ \delta^B - \delta^{\deg h}\},$$

since $t \geq 1$. On the other hand, by our assumption that $A < \deg h < B$ and $\deg g < \deg h$, both the inequalities $\delta^{\deg g} \geq \delta^{\deg h} - \delta^A$ and $\delta^{\deg g} \geq \delta^B - \delta^{\deg h}$ must fail for a large enough δ, and this completes the proof of the first part of the theorem.

Assume now that the inequality (2) holds. In this case all the ξ_i's satisfy $|\xi_i| \geq \delta^B$ with $B = \min_{k>0} \frac{\deg a_0 - \deg a_k}{k}$ and hence we have $|h(X) - \xi_i| \geq \delta^B - \delta^{\deg h}$, for each $i \in \{1, \ldots, n\}$. This implies that for a large enough δ we must have $\delta^{\deg g} \geq \delta^B - \delta^{\deg h}$. On the other hand, this inequality can not hold for a large enough δ, since $B > \max\{\deg g, \deg h\}$, and this completes the proof of the theorem. □

Even though Theorems 3.1 and 3.2 may be in some cases difficult to apply, they have a series of corollaries that are extremely useful to test the irreducibility of a given polynomial on the one hand, and to provide methods to produce irreducible multivariate polynomials, on the other hand. The first two such corollaries are the following irreducibility criteria that use the Euclidean algorithm.

Corollary 3.3. *Let K be a field, $f, h \in K[X]$, f irreducible over K, $\deg h \geq 1$ and express the polynomial f "in base h" via the Euclidean algorithm, say $f = \sum_{i=0}^{n} a_i h^i$, with $a_0, a_1, \ldots, a_n \in K[X]$. Then the polynomial $\sum_{i=0}^{n} a_i(X)Y^i$ is irreducible over $K(X)$.*

Corollary 3.4. *Let K be a field, $f, g, h \in K[X]$, f irreducible over K, $g \neq 0$, $\deg g < \deg h$, and assume that for an integer $s \geq 2$ the polynomial $f^s \cdot g$ is expressed "in base" h via the Euclidean algorithm as $f^s \cdot g = \sum_{i=0}^{n} a_i h^i$, with $a_0, a_1, \ldots, a_n \in K[X]$. If $\sum_{i=1}^{n} i a_i h^{i-1}$ is not divisible by f, then the polynomial $\sum_{i=0}^{n} a_i(X)Y^i \in K[X,Y]$ is irreducible over $K(X)$.*

A more efficient method (that requires no division) to obtain irreducible multivariate polynomials starting from an irreducible univariate polynomial is given by the following two results.

Corollary 3.5. *If we write an irreducible polynomial $f \in K[X]$ as a sum of polynomials $a_0, \ldots, a_n \in K[X]$ with $\deg a_0 > \max_{1 \leq i \leq n} \deg a_i$, then $F(X,Y) = \sum_{i=0}^{n} a_i(X)Y^i$ is irreducible over $K(X)$.*

Corollary 3.6. *Let $f \in K[X]$ be an irreducible polynomial. If for an integer $s \geq 2$ we write f^s as a sum of polynomials $a_0, \ldots, a_n \in K[X]$ with $\deg a_0 > \max_{1 \leq i \leq n} \deg a_i$, and $a_1 + 2a_2 + \cdots + na_n$ is not divisible by f, then the polynomial $F(X,Y) = \sum_{i=0}^{n} a_i(X)Y^i$ is irreducible over $K(X)$.*

Another way to produce irreducible multivariate polynomials is to replace the monomials $b_k X^k$ of an irreducible univariate polynomial with monomials of the form $b_k X^i Y^j$, $i + j = k$.

Corollary 3.7. *Let K be a field, $f(X) = b_0 X^{n_0} + b_1 X^{n_1} + \ldots + b_k X^{n_k} \in K[X]$, $0 = n_0 < n_1 < \cdots < n_k$, $b_0 \cdots b_k \neq 0$, f being irreducible over K,* *and construct from f the polynomial* $F(X,Y)=b_0X^{i_0}Y^{j_0}+b_1X^{i_1}Y^{j_1}+\ldots+b_kX^{i_k}Y^{j_k}\in K[X,Y]$, *with* $i_l,j_l\geq 0$, $i_l+j_l=n_l$, $l=0,\ldots,k$. *If for an index* $t\in\{0,\ldots,k\}$ *we have*

$$\max_{j_s<j_t}\frac{i_s-i_t}{j_t-j_s}<1<\min_{j_s>j_t}\frac{i_s-i_t}{j_t-j_s},$$

then F is irreducible over $K(X)$.

Corollary 3.8. *Let K be a field, $f\in K[X]$ be irreducible over K, and assume that for an integer $s\geq 2$ we have* $f(X)^s=b_0X^{n_0}+b_1X^{n_1}+\ldots+b_kX^{n_k}\in K[X]$, $0=n_0<n_1<\cdots<n_k$, $b_0\cdots b_k\neq 0$. *Let us construct from f^s the polynomial* $F(X,Y)=b_0X^{i_0}Y^{j_0}+b_1X^{i_1}Y^{j_1}+\ldots+b_kX^{i_k}Y^{j_k}\in K[X,Y]$, *with* $i_l,j_l\geq 0$, $i_l+j_l=n_l$, $l=0,\ldots,k$. *If $\partial F/\partial Y(X,X)$ is not divisible by f and for an index $t\in\{0,\ldots,k\}$, we have*

$$\max_{j_v<j_t}\frac{i_v-i_t}{j_t-j_v}<1<\min_{j_v>j_t}\frac{i_v-i_t}{j_t-j_v},$$

then F is irreducible over $K(X)$.

Another method to construct irreducible polynomials in two variables is to simply replace the variable X by Y in some of the monomials of an irreducible univariate polynomial $f(X)$.

Corollary 3.9. *Let K be a field,* $f(X)=b_0X^{n_0}+b_1X^{n_1}+\ldots+b_kX^{n_k}\in K[X]$, $0=n_0<n_1<\cdots<n_k$, $b_0b_1\cdots b_k\neq 0$, *f being irreducible over K. Then for every partition of the set $S=\{0,1,\ldots,k\}$ into two disjoint nonempty subsets S_1,S_2 with $k\in S_1$, the polynomial in two variables*

$$F(X,Y)=\sum_{i\in S_1}b_iX^{n_i}+\sum_{i\in S_2}b_iY^{n_i}\in K[X,Y]$$

is irreducible over $K(X)$.

Corollary 3.10. *Let K be a field, $f\in K[X]$ irreducible over K, and assume that for an integer $s\geq 2$ we have* $f(X)^s=b_0X^{n_0}+b_1X^{n_1}+\ldots+b_kX^{n_k}\in K[X]$, $0=n_0<n_1<\cdots<n_k$, $b_0\cdots b_k\neq 0$. *Then, for every partition of the set $S=\{0,1,\ldots,k\}$ into two disjoint nonempty subsets S_1,S_2 with $k\in S_1$, the polynomial in two variables*

$$F(X,Y)=\sum_{i\in S_1}b_iX^{n_i}+\sum_{i\in S_2}b_iY^{n_i}\in K[X,Y]$$

is irreducible over $K(X)$, if $\partial F/\partial Y(X,X)$ is not divisible by f.

Theorems 3.1 and 3.2 also provide irreducibility criteria for compositions of polynomials, as follows.

Corollary 3.11. *Let K be a field of characteristic* 0 *and let $f_1, f_2 \in K[X]$ with* $\deg f_1 \geq 1$, $\deg f_2 \geq 2$. *If $f_1 \circ f_2(X)$ is irreducible over K, then $f_1 \circ (f_2(X) - X + Y) \in K[X, Y]$ is irreducible over $K(X)$.*

Corollary 3.12. *Let K be a field of characteristic* 0 *and let $f, f_1, f_2, f_3 \in K[X]$ with* $\deg f_2 \geq 2$, $\deg f_3 < \deg f_1$ *and f irreducible over K. If $f_1 \circ f_2 + f_3 = f^s$ for an integer $s \geq 2$ and $f_1' \circ f_2 + f_3'$ is not divisible by f, then the polynomial $f_1 \circ (f_2(X) - X + Y) + f_3(Y) \in K[X, Y]$ is irreducible over $K(X)$.*

As an immediate consequence of previous results, one may formulate similar irreducibility criteria for polynomials in $r \geq 3$ variables $X_1, X_2, \ldots, X_r$ over K. For any polynomial $f \in K[X_1, \ldots, X_r]$ we denote by $\deg_r f$ the degree of f as a polynomial in X_r with coefficients in $K[X_1, \ldots, X_{r-1}]$. For instance, the next result follows from Corollary 3.5 by writing Y for X_r, X for X_{r-1} and by replacing K with $K(X_1, \ldots, X_{r-2})$.

Corollary 3.13. *If $f \in K[X_1, \ldots, X_{r-1}]$ is irreducible over $K(X_1, \ldots, X_{r-2})$ and we write f as a sum of polynomials $a_0, \ldots, a_n \in K[X_1, \ldots, X_{r-1}]$ with* $\deg_{r-1} a_0 > \max_{1 \leq i \leq n} \deg_{r-1} a_i$, *then $F(X_1, \ldots, X_r) = \sum_{i=0}^{n} a_i(X_1, \ldots, X_{r-1}) X_r^i$ is irreducible over $K(X_1, \ldots, X_{r-1})$.*

The above results allow on the one hand to test the irreducibility of various polynomials when other irreducibility criteria fail, and on the other hand to construct various classes of irreducible multivariate polynomials from arbitrary irreducible polynomials in a smaller number of variables. For the proof of the results in this section we refer the reader to [8] and [9].

4 Irreducible multivariate polynomials obtained from prime numbers

In this section we give some results that provide methods to obtain irreducible multivariate polynomials directly from prime numbers, by combining some of the irreducibility criteria in Sections 2 and 3 above. The first such results combine the methods in Theorem 2.2 and Corollary 3.5.

Corollary 4.1. *If a prime number p is expressed in the number system with base $b \geq 2$ as $p = a_0 + a_1 b + \cdots + a_n b^n$, $0 \leq a_i \leq b - 1$, then for every permutation σ of the set $\{0, 1, \ldots, n\}$ with $\sigma(0) = 0$ and $a_{\sigma^{-1}(n)} \neq 0$, the polynomial*

$$f(X, Y) = \sum_{i=0}^{n} a_i X^{n-i} Y^{\sigma(i)}$$

is irreducible over $\mathbb{Q}(X)$.

Corollary 4.2. *If a prime number* p *is expressed in the number system with base* $b \geq 2$ *as* $p = a_0 + a_1 b + \cdots + a_n b^n$, $0 \leq a_i \leq b-1$, *then for every permutation* σ *of the set* $\{0, 1, \ldots, n\}$ *with* $\sigma(0) = 0$ *and* $a_{\sigma^{-1}(n)} \neq a_{\sigma^{-1}(n)+1}$, *the polynomial*

$$f(X, Y) = \sum_{i=0}^{n} (a_i - a_{i+1})(1 + X + \cdots + X^i) Y^{\sigma(i)}, \quad a_{n+1} := 0$$

is irreducible over $\mathbb{Q}(X)$.

For the proof of Corollaries 4.1 and 4.2 we first note that one may extend Corollary 3.5 to a larger class of polynomials, as follows:

Corollary 4.3. *If we write an irreducible polynomial* $f \in K[X]$ *as a sum of polynomials* $f_0, \ldots, f_n \in K[X]$ *with* $\deg f_0 > \max\limits_{1 \leq i \leq n} \deg f_i$, *then for every permutation* σ *of the set* $\{0, 1, \ldots, n\}$ *with* $\sigma(0) = 0$ *and* $f_{\sigma^{-1}(n)} \neq 0$, *the polynomial* $F(X, Y) = \sum_{i=0}^{n} f_i(X) Y^{\sigma(i)}$ *is irreducible over* $K(X)$.

Proof. This follows easily by Theorem 3.1 using (2) with $F(X, Y) = \sum_{i=0}^{n} f_{\sigma^{-1}(i)}(X) Y^i$, $f(X) = \sum_{i=0}^{n} f_i(X)$ and $g(X) = h(X) = 1$. Thus, by writing an arbitrary irreducible polynomial $f \in K[X]$ as $f(X) = \sum_{i=0}^{n} f_i(X)$ with $\deg f_0 > \max\limits_{1 \leq i \leq n} \deg f_i$, one may construct polynomials $F(X, Y) = \sum_{i=0}^{n} f_i(X) Y^{\sigma(i)} \in K[X, Y]$ of arbitrarily large degrees with respect to Y, and which are irreducible over $K(X)$. □

In particular, from Corollary 4.3, we obtain the following irreducibility criterion.

Corollary 4.4. *Let* $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$ *be an irreducible polynomial. Then for every permutation* σ *of the set* $\{0, 1, \ldots, n\}$ *with* $\sigma(0) = 0$ *and* $a_{n-\sigma^{-1}(n)} \neq 0$, *the polynomial* $F(X, Y) = \sum_{i=0}^{n} a_{n-i} X^{n-i} Y^{\sigma(i)}$ *is irreducible over* $K(X)$.

Proof. Here we write $f(X) = \sum_{i=0}^{n} f_i(X)$ with $f_i(X) = a_{n-i} X^{n-i}$, $i = 0, 1, \ldots, n$, and we obviously have $\deg f_0 > \max\limits_{1 \leq i \leq n} \deg f_i$. The conclusion follows by Corollary 4.3. □

We return now to the proof of Corollaries 4.1 and 4.2. First, by Theorem 2.2, the polynomial $f(X) = a_n X^n + \cdots + a_1 X + a_0$ is irreducible over $\mathbb{Q}$, hence its reciprocal $\bar{f}(X) = X^n f(1/X) = a_0 X^n + \cdots + a_{n-1} X + a_n$ is also irreducible over $\mathbb{Q}$. Since one may write $\bar{f}$ as $\bar{f} = f_0 + f_1 + \cdots + f_n$ with $f_i(X) = a_i X^{n-i}$,

$i = 0, 1, \dots, n$, and $\deg f_0 > \max_{1\le i\le n} \deg f_i$, the proof of Corollary 4.1 follows by Corollary 4.3 with f replaced by $\bar{f}$.

For the proof of Corollary 4.2, we observe that $f(X) = a_nX^n + \cdots + a_1X + a_0$ may be written as $f(X) = \sum_{i=0}^{n}(a_i - a_{i+1})(1+X+\cdots+X^i)$, with $a_{n+1} = 0$. This shows that f may be written as $f = f_0 + f_1 + \cdots + f_n$ with $f_i(X) = (a_i - a_{i+1})(1 + X + \cdots + X^i)$, $i = 0, 1, \dots, n$. Since $\deg f_0 > \max_{1\le i\le n} \deg f_i$, the conclusion follows again by Corollary 4.3.

In a similar way one may produce irreducible multivariate polynomials by combining the methods in Theorem 2.10 and Corollary 4.4, as follows.

Corollary 4.5. *If a prime power p^s, $s \ge 2$ is expressed in the number system with base $b \ge 2$ as $p^s = \sum_{i=0}^{n} a_ib^i$ with $0 \le a_i \le b-1$ and $p \nmid \sum_{i=1}^{n} ia_ib^{i-1}$, then for every permutation σ of the set $\{0, 1, \dots, n\}$ with $\sigma(0) = 0$ and $a_{n-\sigma^{-1}(n)} \ne 0$, the polynomial $F(X, Y) = \sum_{i=0}^{n} a_{n-i}X^{n-i}Y^{\sigma(i)}$ is irreducible over $\mathbb{Q}(X)$.*

Another method to produce irreducible multivariate polynomials from prime numbers is obtained by combining Corollary 2.8 and Corollary 4.4, as follows.

Corollary 4.6. *If we write a prime number as $a_0 + a_1m + \cdots + a_nm^n$ with $a_i \in \{-1, 1\}$ and m an integer with $|m| \ge 3$, then for every permutation σ of the set $\{0, 1, \dots, n\}$ with $\sigma(0) = 0$ and $a_{n-\sigma^{-1}(n)} \ne 0$, the polynomial $F(X, Y) = \sum_{i=0}^{n} a_{n-i}X^{n-i}Y^{\sigma(i)}$ is irreducible over $\mathbb{Q}(X)$.*

Proof. By Corollary 2.8, the Littlewood polynomial $f(X) = \sum_{i=0}^{n} a_iX^i$ is irreducible over $\mathbb{Q}$, so by Corollary 4.4, $F(X, Y) = \sum_{i=0}^{n} a_{n-i}X^{n-i}Y^{\sigma(i)}$ is irreducible over $\mathbb{Q}(X)$. □

By combining now Theorem 2.2 and Corollary 3.9, one obtains the following result.

Corollary 4.7. *If a prime number is expressed in the number system with base $b \ge 2$ as $p = a_0b^{n_0} + a_1b^{n_1} + \ldots + a_kb^{n_k}$, $0 = n_0 < n_1 < \cdots < n_k$, $a_0 \cdots a_k \ne 0$, then for every partition of the set $S = \{0, 1, \dots, k\}$ into two disjoint, nonempty subsets S_1, S_2 with $k \in S_1$, the polynomial in two variables*

$$F(X, Y) = \sum_{i\in S_1} a_iX^{n_i} + \sum_{i\in S_2} a_iY^{n_i} \in \mathbb{Q}[X, Y]$$

is irreducible over $\mathbb{Q}(X)$.

The last result in this section combines Theorem 2.2 and Corollary 3.11, as follows.

Corollary 4.8. *If a prime number p is expressed in the number system with base $b \geq 2$ as $p = a_0 + a_1 b^k + a_2 b^{2k} + \cdots + a_n b^{nk}$ with $0 \leq a_i \leq b-1$, $k \geq 2$, $n \geq 1$, then the polynomial*

$$F(X,Y) = \sum_{i=0}^{n} a_i \cdot (X^k - X + Y)^i$$

is irreducible over $\mathbb{Q}(X)$.

Proof. Here we use the fact that the polynomial $f(X) = \sum_{i=0}^{n} a_i X^{ki}$ may be written as $f = f_1 \circ f_2$ with $f_1(X) = \sum_{i=0}^{n} a_i X^i$ and $f_2(X) = X^k$. By Theorem 2.2, the polynomial $f_1 \circ f_2$ must be irreducible over $\mathbb{Q}$, hence by Corollary 3.11 the polynomial in two variables $F(X,Y) = \sum_{i=0}^{n} a_i \cdot (X^k - X + Y)^i$ must be irreducible over $\mathbb{Q}(X)$. $\square$

5 Examples

1) Let $p = 20102009200820072006200520042003$. Since p is a prime number, by Cohn's Theorem, the polynomial

$$\begin{aligned} f(X) &= 2X^{31} + X^{29} + 2X^{27} + 9X^{24} + 2X^{23} + 8X^{20} + 2X^{19} + 7X^{16} \\ &+ 2X^{15} + 6X^{12} + 2X^{11} + 5X^8 + 2X^7 + 4X^4 + 2X^3 + 3 \end{aligned}$$

must be irreducible over $\mathbb{Q}$. Then, by Corollary 3.9, the polynomial

$$\begin{aligned} F(X,Y) &= 2X^{31} + 2X^{27} + 2X^{23} + 2X^{19} + 2X^{15} + 2X^{11} + 2X^7 + 2X^3 \\ &+ Y^{29} + 9Y^{24} + 8Y^{20} + 7Y^{16} + 6Y^{12} + 5Y^8 + 4Y^4 + 3 \in \mathbb{Q}[X,Y] \end{aligned}$$

is irreducible over $\mathbb{Q}(X)$. We note that in this way one may produce from $f(X)$ a number of $2^{15} - 1$ polynomials $F(X,Y) \in \mathbb{Q}[X,Y]$ which are irreducible over $\mathbb{Q}(X)$.

2) Let $p = 1222333444555666777888999$. We may write the prime p as $p = a_0 + a_1 + a_2 + \cdots + a_9$ with

$$\begin{array}{lcllcl} a_0 &=& 10^{24} & a_5 &=& 666 \cdot 10^9 \\ a_1 &=& 222 \cdot 10^{21} & a_6 &=& 777 \cdot 10^6 \\ a_2 &=& 333 \cdot 10^{18} & a_7 &=& 888 \cdot 10^3 \\ a_3 &=& 444 \cdot 10^{15} & a_8 &=& 99 \\ a_4 &=& 555 \cdot 10^{12} & a_9 &=& 9 \end{array}$$

We obviously have $|a_0| > 2|a_1| + 2^2|a_2| + \cdots + 2^9|a_9|$, so, by Corollary 2.6, the polynomial

$$\begin{aligned} f(X) &= a_0 + a_1 X + \cdots + a_9 X^9 \\ &= 10^{24} + 222 \cdot 10^{21} X + 333 \cdot 10^{18} X^2 + 444 \cdot 10^{15} X^3 + 555 \cdot 10^{12} X^4 \\ &+ 666 \cdot 10^9 X^5 + 777 \cdot 10^6 X^6 + 888 \cdot 10^3 X^7 + 99 X^8 + 9 X^9 \end{aligned}$$

is irreducible over $\mathbb{Q}$. Write now $f(X) = a_0(X) + a_1(X) + a_2(X) + a_3(X) + a_4(X)$ with

$$\begin{aligned} a_0(X) &= 99X^8 + 9X^9 \\ a_1(X) &= 777 \cdot 10^6 X^6 + 888 \cdot 10^3 X^7 \\ a_2(X) &= 555 \cdot 10^{12} X^4 + 666 \cdot 10^9 X^5 \\ a_3(X) &= 333 \cdot 10^{18} X^2 + 444 \cdot 10^{15} X^3 \\ a_4(X) &= 10^{24} + 222 \cdot 10^{21} X. \end{aligned}$$

Since $\deg a_0 > \max\{\deg a_1, \deg a_2, \deg a_3, \deg a_4\}$, by Corollary 3.5 the polynomial in two variables $F(X,Y) = a_0(X) + a_1(X)Y + a_2(X)Y^2 + a_3(X)Y^3 + a_4(X)Y^4$ is irreducible over $\mathbb{Q}(X)$.

3) Let $p = 9988776655443322110053$. Since p is a prime number, by Cohn's Theorem the polynomial

$$\begin{aligned} f(X) &= 9X^{21} + 9X^{20} + 8X^{19} + 8X^{18} + 7X^{17} + 7X^{16} + 6X^{15} + 6X^{14} + 5X^{13} \\ &+ 5X^{12} + 4X^{11} + 4X^{10} + 3X^9 + 3X^8 + 2X^7 + 2X^6 + X^5 + X^4 + 5X + 3 \end{aligned}$$

must be irreducible over $\mathbb{Q}$. By Corollary 4.4 with $\sigma(i) = i + 1$ for $i = 1, 2, \ldots, 20$ and $\sigma(21) = 1$, the polynomial

$$\begin{aligned} F(X,Y) &= 5XY^{21} + X^4Y^{18} + X^5Y^{17} + 2X^6Y^{16} + 2X^7Y^{15} + 3X^8Y^{14} + 3X^9Y^{13} \\ &+ 4X^{10}Y^{12} + 4X^{11}Y^{11} + 5X^{12}Y^{10} + 5X^{13}Y^9 + 6X^{14}Y^8 + 6X^{15}Y^7 \\ &+ 7X^{16}Y^6 + 7X^{17}Y^5 + 8X^{18}Y^4 + 8X^{19}Y^3 + 9X^{20}Y^2 + 3Y + 9X^{21} \end{aligned}$$

is irreducible over $\mathbb{Q}(X)$.

4) For an example related to Corollary 4.8, let

$$\begin{aligned} p_1 &= 9007005003001, \\ p_2 &= 90007000500030001, \\ p_3 &= 9000007000005000003000001. \end{aligned}$$

Since p_1, p_2 and p_3 are prime numbers, by Corollary 4.8 the polynomials

$$\begin{aligned} F_1 &= 1 + 3(X^3 - X + Y) + 5(X^3 - X + Y)^2 + 7(X^3 - X + Y)^3 + 9(X^3 - X + Y)^4 \\ F_2 &= 1 + 3(X^4 - X + Y) + 5(X^4 - X + Y)^2 + 7(X^4 - X + Y)^3 + 9(X^4 - X + Y)^4 \\ F_3 &= 1 + 3(X^6 - X + Y) + 5(X^6 - X + Y)^2 + 7(X^6 - X + Y)^3 + 9(X^6 - X + Y)^4 \end{aligned}$$

are irreducible over $\mathbb{Q}(X)$.

Acknowledgements. This work was supported by CNCSIS-UEFISCSU, project PNII-IDEI 443, code 1190/2008.

References

[1] M. Ayad, *Irreducibility of $f(u(x), v(y))$,* J. Algebra **279** (2004), 302–307.

[2] A.I. Bonciocat, N.C. Bonciocat, *Some classes of irreducible polynomials,* Acta Arith. **123** (2006) no. 4, 349–360.

[3] A.I. Bonciocat, N.C. Bonciocat, *A Capelli type theorem for multiplicative convolutions of polynomials,* Math. Nachr. **281** (2008) no. 9, 1240–1253.

[4] A.I. Bonciocat, N.C. Bonciocat, *The irreducibility of polynomials that have one large coefficient and take a prime value,* Canad. Math. Bull. **52** (2009) no. 4, 511–520.

[5] A.I. Bonciocat, N.C. Bonciocat, A. Zaharescu, *On the irreducibility of polynomials that take a prime power value,* to appear in Bull. Math. Soc. Sci. Math. Roumanie vol. **54** (102) (2011).

[6] A.I. Bonciocat, A. Zaharescu, *Irreducibility results for compositions of polynomials in several variables,* Proc. Indian Acad. Sci. (Math. Sci.) **115** (2005) no. 2, 117–126.

[7] N.C. Bonciocat, *On an irreducibility criterion of Perron for multivariate polynomials,* Bull. Math. Soc. Sci. Math. Roumanie **53** (101) (2010), no. 3, 213–217.

[8] N.C. Bonciocat, A. Zaharescu, *Irreducible multivariate polynomials obtained from polynomials in fewer variables,* J. Pure Appl. Algebra **212** (2008), 2338–2343.

[9] N.C. Bonciocat, A. Zaharescu, *Irreducible multivariate polynomials obtained from polynomials in fewer variables, II,* to appear in Proc. Indian Acad. Sci. (Math. Sci.).

[10] J. Brillhart, M. Filaseta, A. Odlyzko, *On an irreducibility theorem of A. Cohn,* Canad. J. Math. **33** (1981) no. 5, 1055–1059.

[11] M. Cavachi, M. Vajaitu, A. Zaharescu, *An irreducibility criterion for polynomials in several variables,* Acta Math. Univ. Ostrav. **12** (2004), no. 1, 13–18.

[12] M. Filaseta, *A further generalization of an irreducibility theorem of A. Cohn,* Canad. J. Math **40** (1988), no. 2, 339–351.

[13] M. Filaseta, *Irreducibility criteria for polynomials with non-negative coefficients,* Canad. J. Math **34** (1982), no. 6, 1390–1395.

[14] K. Girstmair, *On an Irreducibility Criterion of M. Ram Murty,* Amer. Math. Monthly **112** (2005) no. 3, 269–270.

[15] A. Schinzel, Polynomials with special regard to reducibility, Encyclopedia Math. Appl. 77, Cambridge Univ. Press, 2000.

[16] G. Pólya, *Verschiedene Bemerkungen zur Zahlentheorie*, Jahresber. Deutschen Math. Ver., **28** (1919), 31–40.

[17] M. Ram Murty, *Prime numbers and irreducible polynomials,* Amer. Math. Monthly **109** (2002) no. 5, 452–458.

Institute of Mathematics of the Romanian Academy,
P.O. Box 1-764, Bucharest 014700, Romania
e-mail: Nicolae.Bonciocat@imar.ro