Hindawi
Journal of Mathematics
Volume 2020, Article ID 8869499, 4 pages
https://doi.org/10.1155/2020/8869499

Research Article

Irreducibility of a Polynomial Shifted by a Power of Another Polynomial

Artūras Dubickas

Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania

Correspondence should be addressed to Artūras Dubickas; arturas.dubickas@mif.vu.lt

Received 24 September 2020; Revised 17 November 2020; Accepted 20 November 2020; Published 2 December 2020

Academic Editor: Marco Fontana

In this note, we show that, for any $f \in \mathbb{Z}[x]$ and any prime number p, there exists $g \in \mathbb{Z}[x]$ for which the polynomial $f(x) - g(x)^p$ is irreducible over $\mathbb{Q}$. For composite $p \geq 2$, this assertion is not true in general. However, it holds for any integer $p \geq 2$ if f is not of the form $ah(x)^k$, where $a \neq 0$ and $k \geq 2$ are integers and $h \in \mathbb{Z}[x]$.

1. Introduction

A polynomial in one or several variables with coefficients in a field K is reducible over K if it is a product of two nonconstant polynomials with coefficients in K and irreducible otherwise. See, for instance, Schinzel's book [1] for a systematic study of reducibility of polynomials.

Even in the case of univariate polynomials with coefficients in $K = \mathbb{Q}$ or in its ring of integers $\mathbb{Z}$, there are very few criteria when the irreducibility of a given polynomial f can be easily confirmed (Eisenstein's criterion, Cohn's criterion, and Newton polytopes method). However, usually a polynomial does not have a form for which any of the above-mentioned methods can be applied. There are also some more special methods. For instance, reducibility of the polynomial $f(g(x))$ when $f \in K[x]$ is irreducible and $g \in K[x]$ is chosen so that $\deg g < \deg f$ was recently studied in [2–4], whereas reducibility of $f(x) - pg(x)$ has been considered in [5, 6]. In the latter case, it was shown that, for any coprime polynomials $f, g \in \mathbb{Z}[x]$, and for all but finitely many prime numbers p, the polynomial $f(x) - pg(x)$ is irreducible.

In this note, instead of $f(x) - pg(x)$, we consider $f(x) - g(x)^p$ and show the following.

Theorem 1. *Let $p \geq 2$ be a prime number. Then, for each $f \in \mathbb{Z}[x]$ there exists $g \in \mathbb{Z}[x]$ such that the polynomial $f(x) - g(x)^p$ is irreducible over $\mathbb{Q}$.*

In the case when $m = p \geq 2$ is a composite number, the assertion of Theorem 1 is not true. Indeed, suppose that $m = q\ell$, where $q, \ell \geq 2$ are integers. Take, for instance, $f(x) = x^q$. Then, for any $g \in \mathbb{Z}[x]$, we have

$$\begin{aligned} w(x) = f(x) - g(x)^m &= x^q - g(x)^{\ell q} \\ &= \left(x - g(x)^\ell\right)\left(x^{q-1} + x^{q-2}g(x)^\ell + \cdots + g(x)^{\ell(q-1)}\right). \end{aligned} \tag{1}$$

The degree of w is q if g is a constant and otherwise it is $\ell q \deg g$. The degree of the factor $x - g(x)^\ell$ is 1 if g is a constant and otherwise it is $\ell \deg g$. So, in both cases, $x - g(x)^\ell \in \mathbb{Z}[x]$ is a factor of w of degree at least 1 and at most $q^{-1}\deg w$. Hence, w is reducible over $\mathbb{Q}$.

We also state a sufficient condition for f under which the assertion of Theorem 1 is true for composite $m = p$.

Theorem 2. *Let $m \geq 2$ be an integer, and let $f \in \mathbb{Z}[x]$ be a polynomial which is not of the form $ah(x)^k$ with integers $a \neq 0$, $k \geq 2$, and $h \in \mathbb{Z}[x]$. Then, there exists $g \in \mathbb{Z}[x]$ such that the polynomial $f(x) - g(x)^m$ is irreducible over $\mathbb{Q}$.*

Since $f(x)$ can be expressed as $g(x)^p + f(x) - g(x)^p$, we can formulate Theorem 1 in the following equivalent form: for any prime number p each polynomial in $\mathbb{Z}[x]$ is expressible by the sum of a pth power of a polynomial in $\mathbb{Z}[x]$ and an irreducible over $\mathbb{Q}$ polynomial in $\mathbb{Z}[x]$.

In particular, selecting $p = 2$ (or $p = 3$), we can claim that each polynomial in $\mathbb{Z}[x]$ is the sum of a square (resp. cube) in $\mathbb{Z}[x]$ and an irreducible over $\mathbb{Q}$ integer polynomial. A corresponding problem for integers asserts that each sufficiently large integer is either a square (resp. cube) in $\mathbb{Z}$ or the sum of a square (resp. cube) in $\mathbb{Z}$ and a prime number (see the paper of Hardy and Littlewood (p. 49 in [][][7]) and (p. 51 in [][][7]). Both these problems are wide open, see, e.g., [8–11] for some progress on the representations of integers by the sum of a square and a prime number.

It is not surprising at all that an additive problem in integer polynomials involving irreducible polynomials is much easier than the corresponding problem in integers involving prime numbers, since "almost all" integer polynomials are irreducible (see [12], for a precise statement), whereas "almost none" integer is a prime number. The same happens with Goldbach-type problems in polynomials with integer coefficients when much more is known compared to classical Goldbach problems for integers. There is a considerable literature concerning this, see, for instance, [13–22].

Throughout, without loss of generality, we may assume that f is nonconstant. Indeed, for $f(x) = a \in \mathbb{Z}$, it suffices to take any constant polynomial $g(x) = b \in \mathbb{Z}$. Then, for each $m \in \mathbb{N}$, the polynomial $f(x) - g(x)^m = a - b^m$ is a constant, so it is irreducible over $\mathbb{Q}$.

In Section 2, we give some auxiliary results. Then, in Section 3, we complete the proofs of the theorems.

2. Auxiliary Results

We first recall the simplest version of Hilbert's irreducibility theorem (see p. 298 in [1]).

Lemma 1. *Let $F(x, y) \in \mathbb{Z}[x, y]$ be an irreducible over $\mathbb{Q}$ polynomial. Then, there are infinitely many $y_0 \in \mathbb{Z}$ for which the polynomial $F(x, y_0) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$.*

The next lemma follows from the result of Davenport et al. [23].

Lemma 2. *Let $k \geq 2$ be an integer and let $f \in \mathbb{Z}[x]$ be a nonconstant polynomial such that, for each $x \in \mathbb{Z}$, there is $\ell(x) \in \mathbb{Z}$ for which $f(x) = \ell(x)^k$. Then, there exists $h \in \mathbb{Z}[x]$ such that $f(x) = h(x)^k$.*

Here is a more special version of the above result due to Perelli and Zannier [24].

Lemma 3. *Let $f \in \mathbb{Z}[x]$ be a nonconstant polynomial such that, for each $x \in \mathbb{Z}$, there are $a(x), \ell(x) \in \mathbb{Z}$ and $k(x) \in \mathbb{N} \setminus \{1\}$ satisfying $f(x) = a(x)\ell(x)^{k(x)}$. If the prime divisors of all $a(x)$ belong to a finite set S, then there are integers $a \neq 0$, $k \geq 2$, and a polynomial $h \in \mathbb{Z}[x]$ such that $f(x) = ah(x)^k$.*

Next, we recall a theorem of Capelli, which was generalized by Kneser, see p. 92 in [1].

Lemma 4. *Let K be a field and let $m \geq 2$ be an integer. The polynomial $x^m - a$, where $a \in K$, is irreducible over K except when, for some $b \in K$, either $a = -4b^4$ and $4|m$ or $a = b^p$ with some prime $p|m$.*

We conclude this section with several simple lemmas.

Lemma 5. *Let K be a field and let $m \geq 2$ be an integer. Suppose that $F(x, y) \in K[x, y]$ is a polynomial of degree m in y with coefficient $c \in K \setminus \{0\}$ for y^m. If $F(x, y)$ is reducible over K, then $F(x_0, y) \in K[y]$ is reducible over K for each $x_0 \in K$.*

Proof. Since F is reducible, there are $c_1, c_2 \in K \setminus \{0\}$ satisfying $c_1 c_2 = c$, $n, k \in \mathbb{N}$ satisfying $n + k = m$, and $u, v \in K[x, y]$ such that

$$F(x, y) = \left(c_1 y^n + u(x, y)\right)\left(c_2 y^k + v(x, y)\right), \tag{2}$$

where u is of degree at most $n - 1$ in y and v is of degree at most $k - 1$ in y. Hence, for any $x_0 \in K$, the degrees of the polynomials $c_1 y^n + u(y, x_0)$ and $c_2 y^k + v(y, x_0)$ are n and k, respectively. In particular, these polynomials are both nonconstant. This implies that their product $F(x_0, y) \in K[y]$ is reducible over K.

Here is a simple corollary of Lemma 4: □

Lemma 6. *The polynomial $y^p - f(x)$, where $f \in \mathbb{Z}[x]$ and $p \geq 2$ is a prime number, is irreducible over $\mathbb{Q}$ except when $f(x) = h(x)^p$ for some $h \in \mathbb{Z}[x]$.*

Proof. Suppose that $y^p - f(x)$ is reducible. Then, for each $x_0 \in \mathbb{Z}$, by Lemma 5 with $K = \mathbb{Q}$, $c = 1$, and $m = p$, the polynomial $y^p - f(x_0) \in \mathbb{Z}[y]$ is reducible over $\mathbb{Q}$. Thus, by Lemma 4 with $K = \mathbb{Q}$ and $m = p$, we must have $f(x_0) = b^p$ for some $b \in \mathbb{Q}$. Moreover, from $f(x_0) \in \mathbb{Z}$, it follows that $b \in \mathbb{Z}$. Therefore, by Lemma 2, we conclude that there is a polynomial $h \in \mathbb{Z}[x]$ such that $f(x) = h(x)^p$.

We also have the following. □

Lemma 7. *Let $h \in \mathbb{Z}[x]$ be a nonconstant polynomial and let p be a prime number. Then, the polynomial*

$$\frac{(h(x) + y)^p - h(x)^p}{y} = \sum_{j=1}^{p} \binom{p}{j} y^{j-1} h(x)^{p-j} \in \mathbb{Z}[x, y], \tag{3}$$

is irreducible over $\mathbb{Q}$.

Proof. Denote the polynomial by $u(x, y)$. Suppose u is reducible over $\mathbb{Q}$. Fix any $x_0 \in \mathbb{Z}$ for which $h(x_0) \neq 0$. From Lemma 5, it follows that $u(x_0, y) \in \mathbb{Z}[y]$ must be reducible over $\mathbb{Q}$. Since $h(x_0) \in \mathbb{Z}$, the polynomial

$$h(x_0)^{1-p}u(x_0, yh(x_0)) = \frac{(1+y)^p - 1}{y} = \sum_{j=1}^{p} \binom{p}{j} y^{j-1} \in \mathbb{Z}[y], \tag{4}$$

must be reducible over $\mathbb{Q}$ as well. However, by Eisenstein's criterion, this is not the case. Hence, u is irreducible over $\mathbb{Q}$. □

3. Proof of Theorems 1 and 2

Proof of Theorem 1. Suppose first that the polynomial $f(x) - y^p \in \mathbb{Z}[x, y]$ is irreducible over $\mathbb{Q}$. Then, by Lemma 1, for some $y_0 \in \mathbb{Z}$ the polynomial $f(x) - y_0^p \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, so we can simply take the constant polynomial $g(x) = y_0$.

The only alternative is indicated by Lemma 6. Then, $f(x) = h(x)^p$, where $h \in \mathbb{Z}[x]$. Consider $g(x) = h(x) + y$ with some $y \in \mathbb{Z}$ to be chosen later. It is clear that

$$f(x) - g(x)^p = h(x)^p - (h(x) + y)^p = -y\frac{(h(x) + y)^p - h(x)^p}{y}. \tag{5}$$

By Lemma 7 combined with Lemma 1, there is an integer $y_0 \neq 0$ for which $v(x) = ((h(x) + y_0)^p - h(x)^p)/y_0$ is irreducible over $\mathbb{Q}$. Hence, so is the polynomial $-y_0 v(x) = f(x) - (h(x) + y_0)^p$ too, which is the desired conclusion. □

Proof of Theorem 2. If $f(x) - y^m \in \mathbb{Z}[x, y]$ is irreducible over $\mathbb{Q}$, then the argument is the same as that in the Proof of Theorem 1. Suppose $f(x) - y^m$ is reducible over $\mathbb{Q}$. Then, by Lemma 5, for each $x \in \mathbb{Z}$, the polynomial $y^m - f(x) \in \mathbb{Z}[y]$ is reducible over $\mathbb{Q}$. By Lemma 4, for each $x \in \mathbb{Z}$, we have $f(x) = a(x)\ell(x)^{k(x)}$, where $a(x) \in \{1, -4\}$, $\ell(x) \in \mathbb{Z}$ and $k(x)$ is prime divisor of m or $k(x) = 4$. Thus, by Lemma 3, we must have $f(x) = ah(x)^k$ for some integer $a \neq 0$ and some polynomial $h \in \mathbb{Z}[x]$. This is not the case by the assumption of the theorem, which completes the proof. □

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was funded by European Social Fund (Project no. 09.3.3-LMT-K-712-01-0037) under grant agreement with the Research Council of Lithuania (LMTLT).

References

[1] A. Schinzel, *Polynomials with Special Regard to Irreducibility*, Cambridge University Press, Cambridge, UK, 2000.

[2] P. Drungilas and A. Dubickas, "Reducibility of polynomials after a polynomial substitution," *Publicationes Mathematicae Debrecen*, vol. 96, no. 1-2, pp. 185–194, 2020.

[3] P. Müller, "A note on a conjecture by Ulas on polynomial substitutions," *Journal of Number Theory*, vol. 205, pp. 122-123, 2019.

[4] M. Ulas, "Is every irreducible polynomial reducible after a polynomial substitution?" *Journal of Number Theory*, vol. 202, pp. 37–59, 2019.

[5] M. Cavachi, "On a special case of Hilbert's irreducibility theorem," *Journal of Number Theory*, vol. 82, no. 1, pp. 96–99, 2000.

[6] M. Cavachi, M. Vâjâitu, and A. Zaharescu, "A class of irreducible polynomials," *Journal of the Ramanujan Mathematical Society*, vol. 17, pp. 161–172, 2002.

[7] G. H. Hardy and J. E. Littlewood, "Some problems of "Partitio numerorum"; III: on the expression of a number as a sum of primes," *Acta Mathematica*, vol. 44, pp. 1–70, 1923.

[8] R. Brünner, A. Perelli, and J. Pintz, "The exceptional set for the sum of a prime and a square," *Acta Mathematica Hungarica*, vol. 53, no. 3-4, pp. 347–365, 1989.

[9] A. Languasco and A. Zaccagnini, "A Cesàro average of Hardy-Littlewood numbers," *Journal of Mathematical Analysis and Applications*, vol. 401, no. 2, pp. 568–577, 2013.

[10] A. Languasco and A. Zaccagnini, "A Cesàro average of generalised Hardy-Littlewood numbers," *Kodai Mathematical Journal*, vol. 42, no. 2, pp. 358–375, 2019.

[11] Y. Suzuki, "A remark on the conditional estimate for the sum of a prime and a square," *Functiones et Approximatio Commentarii Mathematici*, vol. 57, no. 1, pp. 61–76, 2017.

[12] B. L. Waerden, "Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt," *Monatshefte für Mathematik und Physik*, vol. 43, no. 1, pp. 133–147, 1936.

[13] C. Betts, "Additive and subtractive irreducible monic decompositions in $\mathbb{Z}[x]$," *Comptes Rendus Mathematiques de l'Academie des Sciences. La Societe Royale du Canada*, vol. 20, pp. 86–90, 1998.

[14] A. Dubickas, "Polynomials expressible by sums of monic integer irreducible polynomials," *Bulletin mathématique de la Société des Sciences Mathématiques de Roumanie*, vol. 54, no. 102, pp. 65–81, 2011.

[15] G. W. Effinger and D. R. Hayes, "A complete solution to the polynomial 3-primes problem," *Bulletin of the American Mathematical Society*, vol. 24, no. 2, pp. 363–370, 1991.

[16] D. R. Hayes, "A Goldbach theorem for polynomials with integral coefficients," *The American Mathematical Monthly*, vol. 72, no. 1, pp. 45-46, 1965.

[17] D. Hayes, "The expression of a polynomial as a sum of three irreducibles," *Acta Arithmetica*, vol. 11, no. 4, pp. 461–488, 1966.

[18] M. Kozek, "An asymptotic formula for Goldbach's conjecture with monic polynomials," *American Mathematical Monthly*, vol. 117, pp. 365–369, 2010.

[19] A. Lemos and A. L. A. de Araujo, "An asymptotic formula for Goldbach's conjecture with monic polynomials in \(\mathbb{Z}[\theta][x]\) $\mathbb{Z}[\theta][x]$," *Colloquium Mathematicum*, vol. 148, no. 2, pp. 215–223, 2017.

[20] P. Pollack, "On polynomial rings with a Goldbach property," *American Mathematical Monthly*, vol. 118, pp. 71–77, 2011.

[21] A. Rattan and C. Stewart, "Goldbach's conjecture for $\mathbb{Z}[x]$," *Comptes Rendus Mathematiques de l'Academie des Sciences. La Societe Royale du Canada*, vol. 20, pp. 83–85, 1998.

[22] F. Saidak, "On Goldbach's conjecture for integer polynomials," *The American Mathematical Monthly*, vol. 113, no. 6, pp. 541–545, 2006.
[23] H. Davenport, D. Lewis, and A. Schinzel, "Polynomials of certain special types," *Acta Arithmetica*, vol. 9, no. 1, pp. 107–116, 1964.
[24] A. Perelli and U. Zannier, "Una proprietà arithmetica dei polinomi," *Bollettino dell'Unione Matematica Italiana A (5)*, vol. 17, pp. 199–202, 1980.