AN IRREDUCIBILITY CRITERION FOR COMPOSITION OF POLYNOMIALS

by
Alexandru Zaharescu

Abstract. Let *p* be a prime number, let *f(X), g(X)*0**Z**[X] and let *k* be an integer number . We provide sufficient conditions, in terms of *p, f(X), g(X)* and *k,* in order for the polynomial

$$h_k(X) = p^{k\deg g} g\left(p^{-k} f(X)\right)$$

to be irreducible over **Q**.

2000 Mathematics Subject Classification: 11C08

1. INTRODUCTION

In [2], [4], [5] some results related to Hilbert's irreducibility theorem have been provided. A class of irreducible polynomials over a number field *K* is obtained in [2] as follows. Let *f(X), g(X)* 0 *K[X]* be relatively prime and assume deg *f* < deg *g*. Then it is shown that there are only finitely many prime numbers *p* which remain prime in *K*, for which the polynomial *f(X) + pg(X)* is reducible. An improved version of this result has been obtained in [3], where explicit bounds for *p* in terms of *K*, *f(X)* and *g(X)*are provided, which ensure the irreducibility of the polynomial *f(X)+pg(X).*

In the present paper we take a prime number *p,* two monic polynomials *f(X), g(X) 0* **Z***[X],* and consider for any integer *k* the composition

$$h_k(X) = p^{k\deg g} g\left(p^{-k} f(X)\right)$$

Note that *h*$_k$*(X)* 0 ***Z****[X], h*$_k$*(X)* is monic, $\deg h_k = \deg f \deg g$, and, in case *k* = 0, *h*$_k$*(X)* coincides with the composition *g(f(X)).* We are interested in the problem of describing sufficient conditions for *f(X), g(X), p* and *k* in order for the polynomial *h*$_k$*(X)* to be irreducible over ***Q***.

Before going any further, let us first look at a few examples.

Example 1. Let *g(x) = x*^{2} - 9.

Then, for any monic polynomial *f(X)* 0 ***Z****[X],* any prime number *p,* and any integer *k,* one has the decomposition

$$h_k(X) = f(X)^2 - 9p^{2k} = \left(f(X) - 3p^k\right)\left(f(X) + 3p^k\right)$$

Evidently this happened because our polynomial *g(X)* was reducible over ***Q***. So in the following we will only consider polynomials *g(X)* which are irreducible.

Example 2. Let *f(X)* = *X* + c, for some *c 0* **Z**.
Then, for any monic polynomial *g(X)*0**Z**[X] which is irreducible over ***Q***, any prime number *p,* and any integer *k,* the polynomial

$$h_k(X) = p^{k\deg g} g\left(p^{-k}(X+c)\right)$$

will be irreducible over ***Q***. Let us then restrict our discussion in what follows to the case when $\deg f \geq 2$.

Example 3. Let $g(X) = X$, and $f(X) = X^2 - 9$.
Then, for any prime number *p,* and any integer *k,* the polynomial is the same,

$$h_k(X) = X^2 - 9$$

which is reducible. This of course will also happen if we replace the above *f{X)* by any other reducible polynomial. We will assume from now on that both polynomials *f{X)* and *g(X)* are irreducible.

Example 4. Let $g(X) = X^2$ - 8 and $f(X) = X^2$ - 3.
Take *k* = 0, so that for any *p* we have $h_k(X) = g(f(X))$. Note that, although both polynomials *f(X)* and *g(X)* are irreducible over ***Q***, their composition *g(f(X))* is not. More precisely, we have the factorization.

$$h_k(X) = g(f(X)) = X^4 - 6X^2 + 1 = \left(X^2 - 2X - 1\right)\left(X^2 + 2X - 1\right) \tag{1.1}$$

In this short note we present a simple criterion, easy to use in practice, which provides explicit, sufficient conditions on *f(X), g(X), p* and *k,* under which one can conclude that the polynomial $h_k(X)$ is irreducible over **Q**.

2. AN IRREDUCIBILITY CRITERION OVER $\mathbf{Q}_p$

Let *f(X), g(X)* be monic polynomials in **Z**[X], let *p* be a prime number, and let *k* be an integer number. Define the polynomial $h_k(X)$ as above.

The basic idea in the criterion presented below is to work over the field $\boldsymbol{Q}_p$ of p-adic numbers, and to provide a stronger criterion, which ensures that the composition $h_k(X)$ is irreducible over $\boldsymbol{Q}_p$. Then $h_k(X)$ will also be irreducible over ***Q***.

Since we work over $\boldsymbol{Q}_p$, the above assumptions that *f(X)* and *g(X)* are irreducible over ***Q*** are not helpful, and it is natural to assume the stronger condition that *f(X)* and *g(X)* are irreducible over $\boldsymbol{Q}_p$.

Clearly, this assumption is not enough in order to be able to conclude that $h_k(X)$ is also irreducible over $\boldsymbol{Q}_p$. For instance, if we take in Example 4 above any prime number *p* for which none of the numbers 2 or 3 is a quadratic residue modulo *p,* then both polynomials X^2-8 and X^2-3 will be irreducible over $\boldsymbol{Q}_p$, and still the polynomial $h_k(X)$ is reducible over $\boldsymbol{Q}$, and so also over $\boldsymbol{Q}_p$.

Denote by $\overline{Q}_p$ a fixed algebraic closure of $\overline{Q}_p$. In the following we assume that the polynomials *f(X)* and *g(X)* satisfy a stronger irreducibility property. Namely, we will assume that if η 0 $\overline{Q}_p$ is a root of *g(X)* and if γ 0 $\overline{Q}_p$ is a root of *f(X),* then

$$(2.1) \qquad \lfloor Q_p(\eta,\gamma) : Q_p \rfloor = \deg f \deg g$$

Here the condition (2.1) is equivalent to asking that *g(X)* remains irreducible over $\boldsymbol{Q}_p(\gamma)$, or, similarly, that *f(X)* remains irreducible over $\boldsymbol{Q}_p(\eta)$.

It may be worthed to remark, for practical purposes, that theabove condition (2.1) holds automatically when the degrees of *f(X)* and *g(X)* are relatively prime we are still under the assumption that both *f(X)* and *g(X)* are irreducible over $\boldsymbol{Q}_p$. Indeed, both $\deg f$ and $\deg g$ divide the number $\lfloor Q_p(\eta,\gamma) : Q_p \rfloor$, and on the other hand one always has

$$\lfloor Q_p(\eta,\gamma) : Q_p \rfloor \leq \deg f \deg g$$

So, if $\deg f$ and $\deg g$ are relative prime, then (2.1) holds true.

Let us also remark that even if we assume that (2.1) holds, we can not conclude that *g(f(X))* is irreducible. To see this, let us take $p = 3$ in Example 4 above. Note that since 8 is not a quadratic residue modulo 3, *g(X)* is an unramified, irreducible polynomial over $\boldsymbol{Q}_3$. On the other hand, *f(X)* is an Eisenstein polynomial, so it is irreducible over $\boldsymbol{Q}_3$. The field $\boldsymbol{Q}_3(\eta, \gamma)$, where η *0* $\overline{Q}_3$ is a root *of g(X)* and γ 0 $\overline{Q}_3$ is a root of *f(X),* contains an unramified quadratic extension of $\boldsymbol{Q}_3$, and also a ramified quadratic extension of $\boldsymbol{Q}_3$. Thus (2.1) holds in this case, while our polynomial $h_k(X) = g(f(X))$ is not irreducible.

Let now p be a prime number, and denote as usual by Z_p the ring of p-adic integers. Although we are mainly interested in the case when *f(X), g(X)* 0 $\boldsymbol{Z}$, we will assume from now on that *f(X), g(X)* 0 $\mathbf{Z}_p[X]$, *f(X), g(X)* monic, irreducible over $\boldsymbol{Q}_p$, and satisfying (2.1). Next, take a positive integer *k*.

We show that if *k* is large enough, then the polynomial

$$(2.2) \qquad h_k(X) = p^{k \deg g} g\left(p^{-k} f(X)\right)$$

is irreducible over $\boldsymbol{Q}_p$.

To fix some notation, let

$$f(X) = X^r + b_1 X^{r-1} + \ldots + b_r$$

$$g(X) = X^d + c_1 X^{d-1} + \ldots + c_d$$

and denote by $\gamma_1, \ldots, \gamma_r$ and respectively by $\eta_1, \ldots, \eta_d$, the roots of *f(X)* and *g(X)* in $\mathbf{Q}_p$. Denote by v the unique extension of the *p*-adic valuation to $\mathbf{Q}_p$, normalized such that *v(p)* = 1.

Next, let θ *0* $\overline{Q}_p$ be a root of $h_k(X)$. Note that $\gamma_1,\ldots, \gamma_r, \eta_1, \ldots, \eta_d$, as well as θ, are algebraic integers.

Note also that from (2.2) it follows that

$$g\left(p^{-k} f(\theta)\right) = 0$$

This means that $p^{-k} f(\theta)$ coincides with one of the roots of *g(X)*. Let *s 0{1,...,d},* such that

$$(2.3) \qquad p^{-k} f(\theta) = \eta_s$$

As a consequence of (2.3) we have

$$v(f(\theta)) = v\left(p^k \eta_s\right) = k + v(\eta_s) \geq k$$

This gives in turn

$$k \leq v(f(\theta)) = \sum_{1 \leq i \leq r} v(\theta - \gamma_i)$$

Let *m 0{1,...,r}* such that

$$(2.4) \qquad v(\theta - \gamma_m) = \max_{1 \leq i \leq r} v(\theta - \gamma_i)$$

The last two relations imply that

$$v(\theta - \gamma_m) \geq \frac{k}{r}$$

Denote

$$\omega(\gamma_m) := \max\{v(\gamma_m - \gamma_i) : 1 \leq i \leq r, i \neq m\}$$

Let now *Δ(f)* denote the discriminant of *f(X)*. This is easy to compute in practice, in terms of the given coefficients $b_1,\ldots, b_r$ of *f(X)*. By the expression of *v*(Δ(f)) as a sum of terms of the form $v(\gamma_i - \gamma_j)$,and the fact that all these terms are nonnegative since the roots $\gamma_1,\ldots, \gamma_r$ of *f(X)* are *p*-adic integers, it follows that each such term $v(\gamma_i - \gamma_j)$ is bounded by *v*(Δ(f)). Therefore

$$(2.5) \qquad \omega(\gamma_m) \le v(\Delta(f))$$

Assume now that

$$(2.6) \qquad k > rv(\Delta(f))$$

Combining (2.4) with (2.5) and (2.6), we find that

$$(2.7) \qquad v(\theta - \gamma_m) > \omega(\gamma_m)$$

By Krasner's Lemma (see [1], p. 66) it follows from (2.7) that

$$(2.8) \qquad Q_p(\gamma_m) \subseteq Q_p(\theta)$$

Now from (2.7) and (2.3) we see that

$$(2.9) \qquad Q_p(\gamma_m, \eta_s) \subseteq Q_p(\theta)$$

Since

$$\lfloor Q_p(\gamma_m, \eta_s) : Q_p \rfloor = \deg f \deg g$$

by (2.1) , from (2.9) it follows that

$$\lfloor Q_p(\theta) : Q_p \rfloor \ge \deg f \deg g = \deg h_k$$

We conclude that h_k is irreducible over $\boldsymbol{Q}_p$.

We have obtained the following irreducibility result.

Theorem 1. *Let p be a prime number, let f(X), g(X) 0 Zp[X] be monic, irreducible, and satisfying (2.1), and let k be an integer number satisfying (2.6). Then the polynomial* $h_k(X)$ *defined by (2.2) is irreducible over* $\boldsymbol{Q}_p$.

In particular, if *f(X), g(X) 0* ***Z****[X]*, then $h_k(X)$ *0* ***Z****[X],* and being irreducible over Q_p, $h_k(X)$ will also be irreducible over ***Q***.

References

[1]E. Artin, *Algebraic numbers and algebraic functions,* Gordon and Breach Science Publishers, New York-London-Paris 1967.

[2]M. Cavachi, *On a special case of Hilbert's irreducibility theorem,* J. Number Theory **82** (2000), no. 1, 96-99.

[3]M. Cavachi,M. Vâjâitu and A. Zaharescu, *A class of irreducible polynomials,*J. Ramanujan Math. Soc. **17** (2002), no. 3, 161-172.

[4]M. Fried, *On Hilbert's irreducibility theorem,* J. Number Theory **6** (1974), 211-231.

[5]K. Langmann, *Der Hilbertsche Irreduzibiliäitssatz und Primzahlfragen,* J. Reine Angew.Math. **413** (1991), 213-219.

A ZAHARESCU DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, 1409 W. GREEN STREET, URBANA, IL, 61801, USA

E-mail address,: zaharesc@math.uiuc.edu