IRREDUCIBILITY CRITERIA FOR COMPOSITIONS OF POLYNOMIALS WITH INTEGER COEFFICIENTS

NICOLAE CIPRIAN BONCIOCAT, YANN BUGEAUD, MIHAI CIPU, AND MAURICE MIGNOTTE

To Professor Kalman Győry, on the occasion of his 75^{th} birthday

Abstract. We provide irreducibility criteria for some classes of compositions of polynomials with integer coefficients of the form $F \circ G$, with F being a quadratic irreducible polynomial and G a polynomial of arbitrary degree.

1. Introduction

The composition $F \circ G$ of two polynomials F, G with integer coefficients, with F irreducible, is by no means necessarily irreducible, as one may see by taking for instance $F(X) = X^2 + X + 1$ and $G(X) = X^2$, or, more generally, $F(X) = aX^2 + (2a-1)X + a$ and $G(X) = aX^2$, where a is a nonzero integer. In these cases, we have $F \circ G(X) = (X^2 + X + 1)(X^2 - X + 1)$ and $F \circ G(X) = a(aX^2 + X + 1)(aX^2 - X + 1)$, respectively.

However, there are some conditions on the roots of G that ensure the irreducibility of $F \circ G$ for some particular classes of irreducible polynomials F. In [6] Brauer, Brauer and Hopf posed the question of the irreducibility of $F \circ G$ if $G(X) = (X - a_1) \cdots (X - a_n)$, where the a_i's are distinct integers. Dorwart and Ore [9] gave several answers for classes of quadratic polynomials. According to one of their results, for any irreducible polynomial $F(X) = b_0X^2 + b_1X + 1$ with integer coefficients and any polynomial $G(X) = (X - a_1) \cdots (X - a_n)$ with $a_1, \ldots, a_n$ distinct integers, $n \geq 5$, the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$. They also proved that for any polynomial $F(X) = cX^2 + 1$ with c an integer such that $-c$ is not a square, and any polynomial $G(X) = (X - a_1) \cdots (X - a_n)$ with $a_1, \ldots, a_n$ distinct integers, the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$, except when it is equivalent to

$$-8(X-1)^2X^2(X+1)^2 + 1 = (2X^2 - 1)(-4X^4 + 6X^2 - 1).$$

Here two polynomials with integer coefficients are said to be *equivalent* if one can be obtained from the other one by a transformation of the type $X \mapsto X - a$ or $X \mapsto -X - a$, where a is an integer. Similar results for certain quartic polynomials F and for G having distinct roots in an imaginary quadratic field have been also obtained in [9]. From the results Wegner [20] obtained for polynomials F of the fourth degree we mention only one, asserting that for any polynomial $F(X) = X^4 + d$ with $d > 0$ an integer, $d \not\equiv 3 \pmod 4$ and

2010 *Mathematics Subject Classification.* Primary 11R09; Secondary 11C08.

Key words and phrases. irreducible polynomials, compositions of polynomials, prime numbers.

any polynomial $G(X) = (X - a_1) \cdots (X - a_n)$ with $a_1, \ldots, a_n$ distinct integers, $n \geq 5$, the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$.

Variations of the Brauer-Hopf problem have been investigated by Győry in a series of papers ([12]–[15]), where the author considers much more general situations, relaxing the requirements on both intervening polynomials. In [12] he studied the case when the roots of G are not necessarily integers, but instead $G(X)$ has a divisor $G_1(X) \in \mathbb{Z}[X]$ with distinct real roots, the root field of F is not real and its maximal real subfield is a normal extension of $\mathbb{Q}$. Under these hypotheses he proved that if the pairs (α_i, α_j) of roots of G_1 satisfying $N(\alpha_i - \alpha_j) > \{2^{\deg F} F^2(0)\}^{[L:\mathbb{Q}]/\deg F}$ (where L is the splitting field of $G_1 F$) form a connected graph with k elements, then the degrees of all the irreducible factors of $F \circ G(X)$ are at least $k \deg F$, so in particular $F \circ G(X)$ has at most $\frac{\deg G}{k}$ irreducible factors. This shows that if all the roots of G are real and distinct and $\min_{i \neq j} |\alpha_i - \alpha_j| > 2|F(0)|^{2/\deg F}$, then $F \circ G$ must be irreducible over $\mathbb{Q}$. Moreover, Győry found all the exceptional polynomials F and G such that $F(0) = 1$, $G(X) = (X - a_1) \cdots (X - a_n)$ with distinct integers a_i such that $F \circ G(X)$ is reducible over $\mathbb{Q}$. In [14] he studied the irreducibility of polynomials $F \circ G(X)$ over an arbitrary but fixed totally real algebraic number field L, assuming that F and G are both monic with integer coefficients in L, F is irreducible over L, and its splitting field is a CM-field. One of the consequences that can be drawn from the main result in [14] states that if F is fixed, then apart from certain exceptional polynomials G of bounded degree, the polynomial $F \circ G(X)$ must be irreducible over L for all the polynomials G that have distinct roots in a given totally real number field. In [15] he studied the case when the splitting field of F is a CM-field, and described explicitly some examples such that apart from these, there exist only finitely many pairwise inequivalent monic polynomials G with integer coefficients and distinct zeros in a totally real algebraic number field, for which the polynomial $F \circ G(X)$ is reducible over $\mathbb{Q}$.

In [17] Győry, Hajdu and Tijdeman proved the following elegant result (Theorem 7.1) on the irreducibility of compositions of polynomials $F \circ G$ for quadratic polynomials F and polynomials G of the form $G(X) = (X - a_1) \cdots (X - a_n)$ with $a_1, \ldots, a_n$ distinct rational integers.

Theorem A *Let $F(X)$ be an irreducible polynomial of degree at most 2 with integer coefficients, $F(0) \neq 0$, and $G(X) = (X - a_1) \cdots (X - a_n)$ with $a_1, \ldots, a_n$ distinct rational integers. If*

$$n > 2\tau(F(0))(2 + \lfloor \log_2 |F(0)| \rfloor),$$

then the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$.

Here τ is the usual divisor function. A different idea exploited in the study of irreducibility of compositions of polynomials over integers is to take into consideration properties of the leading coefficients. Thus, in [16] the reader can find irreducibility results for integer polynomials whose leading coefficients have a fixed number of distinct prime factors. There

are also some conditions on the leading coefficient of a polynomial F that will ensure the irreducibility of $F \circ G$ for large classes of polynomials G, as one can see from the following irreducibility criteria proved in [3].

Theorem B *Let $F(X) = \sum_{i=0}^{m} a_i X^i$ and $G(X) = \sum_{i=0}^{n} b_i X^i \in \mathbb{Z}[X]$ be non-constant polynomials of degree m and n respectively, with F irreducible and $a_0 \neq 0$. If $a_m = pq$ with p a prime satisfying*

$$p > |q|^{n-1}|b_n|^{mn} L_1\left(F\left(\frac{X}{|q|^{n/m}|b_n|^n}\right)\right),$$

then the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$.

Theorem C *Let $F(X) = \sum_{i=0}^{m} a_i X^i$ and $G(X) = \sum_{i=0}^{n} b_i X^i \in \mathbb{Z}[X]$ be non-constant polynomials of degree m and n respectively, with $a_0 \neq 0$. If $a_m = pq$ with p a prime satisfying*

$$p > \max\left\{|q|^{m-1} L_1\left(F\left(\frac{X}{|q|}\right)\right),\ |q|^{n-1}|b_n|^{mn} L_1\left(F\left(\frac{X}{|q|^{n/m}|b_n|^n}\right)\right)\right\},$$

then the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$.

Here $L_1(F)$ stands for the sum of the moduli of the coefficients of F, not counting the leading one. These results were proven by adapting some ideas introduced in [7], [8] and [4], where several irreducibility criteria for linear combinations of relatively prime polynomials have been provided. Similar results have been also provided for multiplicative convolutions of polynomials with integer coefficients [1] and [2].

The aim of this paper is to complement Theorems A,B and C, by providing irreducibility conditions for some particular classes of compositions of polynomials $F \circ G$, where F is an irreducible quadratic polynomial whose leading coefficient has a prime factor that does not divide the constant term of F. This choice for F will allow us to explicitly compute some resultants and use their properties to prove the irreducibility of $F \circ G$ for some classes of polynomials G with integer coefficients, with restrictions only on the factorization of their leading coefficients. Our irreducibility conditions will not ask the prime p to exceed a certain lower bound depending on the coefficients of F and G, as in Theorems B and C. Instead, the prime p will be asked not to divide the leading coefficient of G and the constant term of F, thus allowing one to also consider some small primes that are excluded by the conditions in Theorems B and C above. In principle, the procedure that we will use might be also applied to irreducible polynomials F of degree 3 and 4, but with considerable more involved computations. It would be however nice to obtain by a similar procedure divisibility conditions on the coefficients of F and G with respect to a given prime number, that ensure the irreducibility of $F \circ G$ for irreducible polynomials F of arbitrary degree.

For the proof of our results we will adapt some of the ideas employed in [3] and [8], and we will use the following classical theorem of Capelli.

Theorem [18, Theorem 22] *Let K be a field, $G \in K[X]$ be irreducible over K, $G(\beta) = 0$, $H \in K[X]$. If*

$$H(x) - \beta \underset{K(\beta)}{\overset{can}{=}} \text{const} \prod_{\rho=1}^{r} \phi_\rho(x)^{e_\rho}$$

then

$$G(H(x)) \underset{K}{\overset{can}{=}} \text{const} \prod_{\rho=1}^{r} N_{K(\beta)/K} \phi_\rho(x)^{e_\rho}.$$

We will also use the following lemma [5] that relies on a Newton polygon argument, that was crucial in the proof of the results in [5] and [1].

Lemma 1.1. *Let $f, g \in \mathbb{Z}[X]$ be two polynomials with $\deg g = n$ and $\deg f = n - d$, $d \geq 1$. Let also p be a prime number that divides none of the leading coefficients of f and g, and let k be any positive integer prime to d. If $f(X) + p^k g(X)$ may be written as a product of two non-constant polynomials with integer coefficients, say f_1 and f_2, then one of the leading coefficients of f_1 and f_2 must be divisible by p^k.*

We will first prove the following effective results, that provide divisibility conditions on the coefficients of F and G that force $F \circ G$ to be irreducible over $\mathbb{Q}$.

Theorem 1.2. *Let $F(X) = aX^2 + bX + c$ be an irreducible quadratic polynomial with integer coefficients, with $a = pq$, where p is a prime number and q is an integer such that $p \nmid cq$. Then for any non-constant polynomial G with integer coefficients and leading coefficient not divisible by p, the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$.*

For quadratic irreducible polynomials F with leading coefficient divisible by a prime power we will prove the following result.

Theorem 1.3. *Let $F(X) = aX^2 + bX + c$ be an irreducible quadratic polynomial with integer coefficients, with $a = p^k q$, where p is a prime number, k is a positive integer and q is an integer prime to p. Then for any polynomial G of degree $n \geq 1$ with integer coefficients and leading coefficient not divisible by p, the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$ in each one of the following situations:*

i) $p \nmid b$, $p^k \nmid c$ and k is prime to n;

ii) $b = 0$, $p \nmid c$ and k is prime to $2n$.

We note here that for $k = 1$ Theorem 1.3 provides a result weaker than Theorem 1.2, since, as we shall see in the proof of these results, for $k = 1$ and $b \neq 0$ we do not actually need to assume that $p \nmid b$. The condition $p \nmid b$ for $b \neq 0$ is required for $k \geq 2$ in order to apply Lemma 1.1 to deduce that one of the alleged factors of $F \circ G$ has leading coefficient prime to p.

We will also prove the following similar irreducibility criteria for compositions of polynomials $F \circ G$, where F is an irreducible quadratic polynomial that may be expressed in the form $F(X) = (aX + b)(cX + d) + (eX + f)(gX + h)$ with $a, b, c, d, e, f, g, h \in \mathbb{Z}$.

Theorem 1.4. *Let $F(X) = (aX+b)(cX+d)+(eX+f)(gX+h)$ with $a, b, c, d, e, f, g, h \in \mathbb{Z}$, $aceg \neq 0$ be an irreducible quadratic polynomial. Assume that $ac + eg = pq$, with p a prime number and q an integer prime to p, and that at least one of the integers $(af - be)(ah - bg)$, $(cf - de)(ch - dg)$, $(af - be)(cf - de)$, $(ah - bg)(ch - dg)$ is not divisible by p. Then for any non-constant polynomial G with integer coefficients and leading coefficient prime to p, the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$.*

For the case when the leading coefficient of F is divisible by a prime power we will prove the following result.

Theorem 1.5. *Let $F(X) = (aX+b)(cX+d)+(eX+f)(gX+h)$ with $a, b, c, d, e, f, g, h \in \mathbb{Z}$, $aceg \neq 0$ be an irreducible quadratic polynomial. Assume that $ac + eg = p^k q$, with p a prime number, k a positive integer, and q an integer prime to p, and also assume that at least one of the integers $(af - be)(ah - bg)$, $(cf - de)(ch - dg)$, $(af - be)(cf - de)$, $(ah - bg)(ch - dg)$ is not divisible by p^k. Then for any polynomial G of degree $n \geq 1$ with integer coefficients and leading coefficient prime to p, the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$ in each one of the following situations:*

i) $p \nmid ad + bc + eh + fg$ and k is prime to n;

ii) $ad + bc + eh + fg = 0$, $p \nmid bd + fh$ and k is prime to $2n$.

Here too, for $k = 1$, Theorem 1.5 provides a result weaker than Theorem 1.4, since for $k = 1$ and $ad + bc + eh + fg \neq 0$ the condition $p \nmid ad + bc + eh + fg$ is no longer necessary.

The proofs of the main results are presented in Section 2 below. At the end of Section 2 we will show that the method employed in the proof of our results may be also used to prove the classical Schönemann-Eisenstein irreducibility criterion ([19] and [11]).

A series of examples will be provided in the last section of the paper.

2. Proof of the main results

Proof of Theorem 1.2. We will adapt some of the ideas in [3] and [8]. First of all, let us note that since F was assumed to be quadratic and irreducible, we have $ac \neq 0$ and $\Delta = b^2 - 4ac$ is not a perfect square. Let now $G(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, $a_n \neq 0$, $n \geq 1$, and let us assume on the contrary that $F \circ G$ is reducible, that is

$$F \circ G(X) = aG(X)^2 + bG(X) + c = F_1(X)F_2(X),$$

with $F_1(X), F_2(X) \in \mathbb{Z}[X]$ and $\deg F_1 \geq 1$, $\deg F_2 \geq 1$, say

$$\begin{aligned} F_1(X) &= t_0 + t_1X + \cdots + t_sX^s, \\ F_2(X) &= u_0 + u_1X + \cdots + u_vX^v, \end{aligned}$$

$t_0, \ldots t_s, u_0, \ldots u_v \in \mathbb{Z}$, $t_su_v \neq 0$, and $s \geq 1$, $v \geq 1$, $s + v = 2n$. By equating the coefficients, one finds that

$$t_su_v = aa_n^2 = pqa_n^2. \tag{1}$$

Since by our hypothesis $p \nmid qa_n$, we deduce that precisely one of the leading coefficients t_s and u_v is divisible by p, while the other is prime to p, say $p \mid u_v$ and $p \nmid t_s$, hence t_s must be a divisor of qa_n^2. We have so far proved that

$$t_s \mid qa_n^2. \tag{2}$$

Now we are going to estimate the resultant $R(G(X)^2, F_1(X))$. Since $G(X)^2$ and $F_1(X)$ are algebraically relatively prime, the resultant $R(G(X)^2, F_1(X))$ must be a non-zero rational integer.

On the other hand, if we decompose F_1, say $F_1(X) = t_s(X-\theta_1)\cdots(X-\theta_s)$, with $\theta_1, \ldots, \theta_s \in \mathbb{C}$, then

$$\left|R(G(X)^2, F_1(X))\right| = |t_s|^{2n} \prod_{1\le j\le s} \left|G(\theta_j)^2\right|. \tag{3}$$

Fortunately, since $G(\theta_j)$ is a root of F, and hence

$$\left|G(\theta_j)^2\right| = \frac{|bG(\theta_j)+c|}{|pq|},$$

one may compute exactly $|G(\theta_j)^2|$. We distinguish two cases:

Case 1. Here we assume that the discriminant Δ is negative, so the roots x_1 and x_2 of F must be complex conjugated, and hence $bx_1 + c$ and $bx_2 + c$ must have the same modulus, which by direct computation is easily seen to be equal to

$$|c| = |ax_j^2| = |bx_j + c| = \left|\frac{2ac - b^2 \pm ib\sqrt{4ac-b^2}}{2a}\right|.$$

In view of (3), this shows us that

$$\left|R(G(X)^2, F_1(X))\right| = |t_s|^{2n}\frac{|c|^s}{p^s|q|^s}.$$

Finally, in view of (2), our assumptions that $p \nmid qa_n$ and $p \nmid c$ show that $R(G(X)^2, F_1(X))$ can not be an integer, which is a contradiction.

For use in the proof of later theorems, we note that since F is irreducible, by Capelli's Theorem, $\deg F_1(X) = s$ must be a multiple of $\deg F$, that is s must be an even positive integer, so in this case we actually have

$$\left|R(G(X)^2, F_1(X))\right| = |t_s|^{2n}\left(\frac{c^2}{p^2q^2}\right)^m,$$

for some positive integer m.

Case 2. Here we assume that $\Delta > 0$, so the roots x_1 and x_2 of F are real, and hence $G(\theta_j)$ is real for each $j \in \{1, \ldots, s\}$. Moreover, in this case we have either

$$|bG(\theta_j) + c| = \frac{\left|2ac - b^2 + b\sqrt{\Delta}\right|}{2|a|},$$

or

$$|bG(\theta_j)+c| = \frac{\left|2ac-b^2-b\sqrt{\Delta}\right|}{2|a|},$$

according to which root of F we consider. However, since $R(G(X)^2, F_1(X))$ must be an integer, each of the two above possible expressions (which are algebraically conjugated) must appear in the product in the right side of (3) with exactly the same multiplicity. Therefore, this product must be a power of

$$\frac{|(2ac-b^2)^2-b^2(b^2-4ac)|}{4a^2p^2q^2} = \frac{c^2}{p^2q^2},$$

so we deduce again that

$$\left|R(G(X)^2, F_1(X))\right| = |t_s|^{2n}\left(\frac{c^2}{p^2q^2}\right)^m,$$

for some positive integer m. Recalling now the fact that $t_s \mid qa_n^2$, and using the fact that $p \nmid qca_n$, we conclude as in Case 1 that $R(G(X)^2, F_1(X))$ can not be an integer, again a contradiction. This completes the proof of our theorem. □

Proof of Theorem 1.3. i) Here we note that $b \neq 0$, and since

$$F\circ G(X) = aG(X)^2 + bG(X) + c,$$

we may write $F\circ G(X)$ as $\tilde{f}(X) + p^k\tilde{g}(X)$ with $\tilde{f}(X) = bG(X)+c$ and $\tilde{g}(X) = qG(X)^2$. Now, since $\deg\tilde{g} - \deg\tilde{f} = n$, $p \nmid qa_nb$ and k is prime to n, we deduce by Lemma 1.1 that if $F\circ G$ may be written as a product of two non-constant polynomials with integer coefficients, say $F\circ G(X) = F_1(X)F_2(X)$ with

$$\begin{aligned} F_1(X) &= t_0 + t_1X + \cdots + t_sX^s, \\ F_2(X) &= u_0 + u_1X + \cdots + u_vX^v, \end{aligned}$$

then one of the leading coefficients t_s and u_v, must be divisible by p^k, while the other must be prime to p.

For ii), since $b = 0$ we may write $F\circ G(X)$ as $\tilde{f}(X) + p^k\tilde{g}(X)$ with $\tilde{f}(X) = c$ and $\tilde{g}(X) = qG(X)^2$. Here $\deg\tilde{g} - \deg\tilde{f} = 2n$, so in order to apply Lemma 1.1 we have to ask k to be prime to $2n$, and $p \nmid qa_nc$. In this case too, one of the leading coefficients t_s and u_v, must be divisible by p^k, while the other must be prime to p. In both cases i) and ii), we may assume without loss of generality that $p^k \mid u_v$ and $p \nmid t_s$, hence t_s must be a divisor of qa_n^2. The rest of the proof is similar to that of Theorem 1.2, and we deduce in this case that $|R(G(X)^2, F_1(X))|$ must be of the form

$$\left|R(G(X)^2, F_1(X))\right| = |t_s|^{2n}\cdot\left(\frac{c^2}{p^{2k}q^2}\right)^m,$$

for some positive integer m. The desired contradiction is obtained in case i) by observing that since $p \nmid qa_n$ and $p^k \nmid c$, the resultant $R(G(X)^2, F_1(X))$ can not be an integer. The same conclusion is obtained in case ii) using the fact that $p \nmid qca_n$. $\square$

Proof of Theorem 1.4. We will use the same notations as in the proof of Theorems 1.2 and 1.3. First of all, let us note that since F was assumed to be quadratic and irreducible, we have $ac+eg \neq 0$, $af \neq be$, $ah \neq bg$, $cf \neq de$, $ch \neq dg$, and $\Delta = (ad+bc+eh+fg)^2 - 4(ac+eg)(bd+fh)$ is not a perfect square. Let now $G(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, $a_n \neq 0$, $n \geq 1$, and let us assume to the contrary that $F \circ G$ is reducible, that is

$$F \circ G(X) = (aG(X)+b)(cG(X)+d) + (eG(X)+f)(gG(X)+h) = F_1(X)F_2(X),$$

with $F_1(X), F_2(X) \in \mathbb{Z}[X]$ and $\deg F_1 \geq 1$, $\deg F_2 \geq 1$, say

$$\begin{aligned} F_1(X) &= t_0 + t_1X + \cdots + t_sX^s, \\ F_2(X) &= u_0 + u_1X + \cdots + u_vX^v, \end{aligned}$$

$t_0, \ldots t_s, u_0, \ldots u_v \in \mathbb{Z}$, $t_su_v \neq 0$, and $s \geq 1$, $v \geq 1$, $s+v = 2n$. By equating the coefficients, one finds that

$$t_su_v = (ac+eg)a_n^2 = pqa_n^2. \tag{4}$$

Since by our hypothesis $p \nmid qa_n$, we deduce again that precisely one of the leading coefficients t_s and u_v is divisible by p, while the other is prime to p, say $p \mid u_v$ and $p \nmid t_s$, hence

$$t_s \mid qa_n^2. \tag{5}$$

Let us first assume that $p \nmid (af-be)(ah-bg)$. Now we are going to estimate the resultant $R(aG(X)+b, F_1(X))$. Suppose first that $aG(X)+b$ and $F_1(X)$ are not algebraically relatively prime, so they have a non-constant irreducible common factor $H(X)$, say. Then H will be also a factor of $(eG(X)+f)(gG(X)+h)$, so at least one of $eG(X)+f$ and $gG(X)+h$ will be divisible by H. Consider first the case that H is a factor of $eG(X)+f$. Then H will be also a factor of $a(eG(X)+f) - e(aG(X)+b)$, that is $H(X)$ must divide $af-be$, which is a non-zero constant, and this is a contradiction. Similarly, since $ah \neq bg$, H can not be a factor of $gG(X)+h$, which shows that in fact $aG(X)+b$ and $F_1(X)$ must be relatively prime, and hence the resultant $R(aG(X)+b, F_1(X))$ must be a non-zero rational integer.

If we decompose F_1, say $F_1(X) = t_s(X-\theta_1)\cdots(X-\theta_s)$, with $\theta_1, \ldots, \theta_s \in \mathbb{C}$, then

$$|R(aG(X)+b, F_1(X))| = |t_s|^n \prod_{1 \leq j \leq s} |aG(\theta_j)+b|. \tag{6}$$

Since $G(\theta_j)$ is a root of F, one may compute exactly $|aG(\theta_j)+b|$. We distinguish again two cases:

Case 1. Here we assume that the discriminant Δ is negative, so the roots x_1 and x_2 of F must be complex conjugated, and hence ax_1+b and ax_2+b must have the same modulus,

which by direct computation is easily seen to satisfy the equalities

$$\begin{aligned} |ax_1+b|^2 &= |(ax_1+b)(ax_2+b)| = |a^2x_1x_2+ab(x_1+x_2)+b^2| \\ &= \left|a^2\cdot\frac{bd+fh}{ac+eg}-ab\cdot\frac{ad+bc+eh+fg}{ac+eg}+b^2\right| \\ &= \frac{|(af-be)(ah-bg)|}{|ac+eg|}, \end{aligned}$$

so

$$|aG(\theta_j)+b| = \sqrt{\frac{|af-be|\cdot|ah-bg|}{|ac+eg|}}.$$

In view of (6), this shows us that

$$\begin{aligned} |R(aG(X)+b,F_1(X))| &= |t_s|^n\prod_{1\le j\le s}\sqrt{\frac{|af-be|\cdot|ah-bg|}{|ac+eg|}} \\ &= |t_s|^n\cdot\left(\frac{|af-be|\cdot|ah-bg|}{|ac+eg|}\right)^{s/2}. \end{aligned}$$

Since F is irreducible, by Capelli's Theorem, s must be a multiple of $\deg F$, that is s must be an even positive integer, say $s=2m$ with $m\in\mathbb{N}\setminus\{0\}$, so we have

$$|R(aG(X)+b,F_1(X))| = |t_s|^n\cdot\left(\frac{|af-be|\cdot|ah-bg|}{|ac+eg|}\right)^{m}.$$

Finally, in view of (5), our assumptions that $p\nmid qa_n$ and $p\nmid(af-be)(ah-bg)$ show that $R(aG(X)+b,F_1(X))$ can not be an integer, which is a contradiction.

Case 2. Here we assume that $\Delta>0$, so the roots x_1 and x_2 of F are both real, and hence $G(\theta_j)$ is real for each $j\in\{1,\dots,s\}$. Moreover, if we let $\Gamma:=ad+bc+eh+fg$, then in this case we have either

$$|aG(\theta_j)+b| = \frac{\left|2b(ac+eg)-a\Gamma+a\sqrt{\Delta}\right|}{2|ac+eg|},$$

or

$$|aG(\theta_j)+b| = \frac{\left|2b(ac+eg)-a\Gamma-a\sqrt{\Delta}\right|}{2|ac+eg|},$$

according to which root of F we consider. However, since $R(aG+b,F_1(X))$ must be an integer, each of the two above possible expressions (which are algebraically conjugated) must appear in the product in the right side of (3) with exactly the same multiplicity. Therefore, this product must be a power of

$$\frac{\left|2b(ac+eg)-a\Gamma+a\sqrt{\Delta}\right|\cdot\left|2b(ac+eg)-a\Gamma-a\sqrt{\Delta}\right|}{4|ac+eg|^2} = \frac{|af-be|\cdot|ah-bg|}{|ac+eg|},$$

so we deduce again that

$$|R(aG(X)+b,F_1(X))| = |t_s|^n \cdot \left|\frac{(af-be)\cdot(ah-bg)}{ac+eg}\right|^m,$$

for some positive integer m. Recalling now the fact that $t_s \mid qa_n^2$, and using the fact that $p \nmid qa_n(af-be)(ah-bg)$, we conclude as in Case 1 that $R(aG(X)+b,F_1(X))$ can not be an integer, again a contradiction.

For the remaining three cases that $p \nmid (cf-de)(ch-dg)$, $p \nmid (af-be)(cf-de)$ and $p \nmid (ah-bg)(ch-dg)$, all we need to do is to repeat the above computations with $aG(X)+b$ replaced by $cG(X)+d$, $eG(X)+f$ and $gG(X)+h$, respectively. This completes the proof of the theorem. □

Proof of Theorem 1.5. i) Here we note that $ad+bc+eh+fg \neq 0$, and since

$$F\circ G(X) = (ac+eg)G(X)^2 + (ad+bc+eh+fg)G(X) + bd + fh,$$

we may write $F\circ G(X)$ as $\tilde{f}(X)+p^k\tilde{g}(X)$ with $\tilde{f}(X) = (ad+bc+eh+fg)G(X)+bd+fh$ and $\tilde{g}(X) = qG(X)^2$. Now, since $\deg\tilde{g} - \deg\tilde{f} = n$, $p \nmid qa_n(ad+bc+eh+fg)$ and k is prime to n, we deduce again by Lemma 1.1 that if $F\circ G$ may be written as a product of two non-constant polynomials with integer coefficients, say $F\circ G(X) = F_1(X)F_2(X)$ with

$$\begin{aligned} F_1(X) &= t_0 + t_1X + \cdots + t_sX^s, \\ F_2(X) &= u_0 + u_1X + \cdots + u_vX^v, \end{aligned}$$

then one of the leading coefficients t_s and u_v, must be divisible by p^k, while the other must be prime to p.

For ii), since $ad+bc+eh+fg = 0$ one may write $F\circ G(X)$ as $\tilde{f}(X)+p^k\tilde{g}(X)$ with $\tilde{f}(X) = bd+fh$ and $\tilde{g}(X) = qG(X)^2$. Here $\deg\tilde{g} - \deg\tilde{f} = 2n$, so in order to apply Lemma 1.1 we have to ask k to be prime to $2n$, and $p \nmid qa_n(bd+fh)$. In this case too, one of the leading coefficients t_s and u_v, must be divisible by p^k, while the other must be prime to p. In both cases i) and ii), we may assume without loss of generality that $p^k \mid u_v$ and $p \nmid t_s$, hence t_s must be a divisor of qa_n^2. The rest of the proof is similar to that of Theorem 1.4, and we deduce again that $|R(aG+b,F_1)|$ must be of the form

$$|R(aG(X)+b,F_1(X))| = |t_s|^n \cdot \left(\frac{|af-be|\cdot|ah-bg|}{p^k|q|}\right)^m,$$

for some positive integer m. In this case we obtain the desired contradiction by observing that since $p \nmid qa_n$ and $p^k \nmid (af-be)(ah-bg)$, the resultant $R(aG(X)+b,F_1(X))$ can not be an integer. □

Remark 2.1. We note here that the case ii) of Theorems 1.3 and 1.5 may be also proved by using the famous irreducibility criterion of Dumas [10]:

Irreducibility criterion of Dumas *Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ be a polynomial with integer coefficients, and let p be a prime number. If*

i) $\frac{\nu_p(a_i)}{i} > \frac{\nu_p(a_n)}{n}$ *for* $i = 1, \ldots, n-1$,
ii) $\nu_p(a_0) = 0$,
iii) $\gcd(\nu_p(a_n), n) = 1$,

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

Here for an integer n and a prime number p, $\nu_p(n)$ stands for the largest integer i such that $p^i \mid n$ (by convention, $\nu_p(0) = \infty$).

Remark 2.2. We end this section by noting that the method employed in the proof of Theorems 1.2 and 1.3 may be also used to prove the classical Schönemann-Eisenstein irreducibility criterion. To see this, let $F(X) = a_nX^n + \cdots + a_1X + a_0$ be a polynomial with integer coefficients, and assume that p is a prime number such that $p \nmid a_0$, $p \mid a_i$ for $i = 1, \ldots, n$ and $p^2 \nmid a_n$. We therefore may write F as $F(X) = p \cdot \tilde{F}(X) + a_0$ with

$$\tilde{F}(X) = \frac{a_n}{p}X^n + \cdots + \frac{a_1}{p}X \in \mathbb{Z}[X].$$

Let us assume now that F is reducible, that is

$$F(X) = p \cdot \tilde{F}(X) + a_0 = F_1(X)F_2(X),$$

with $F_1(X), F_2(X) \in \mathbb{Z}[X]$ and $\deg F_1 = s \geq 1$, $\deg F_2 = v \geq 1$, say

$$\begin{aligned} F_1(X) &= t_0 + t_1X + \cdots + t_sX^s, \\ F_2(X) &= u_0 + u_1X + \cdots + u_vX^v, \end{aligned}$$

$t_0, \ldots t_s, u_0, \ldots u_v \in \mathbb{Z}$, $t_su_v \neq 0$, and $s + v = n$. By equating the coefficients, one finds that $a_n = t_su_v$, and since $p^2 \nmid a_n$, precisely one of the leading coefficients t_s and u_v is divisible by p, while the other is prime to p, say $p \mid u_v$ and $p \nmid t_s$. Since the polynomials $\tilde{F}$ and F_1 are relatively prime, their resultant must be a non-zero integer. On the other hand, if we decompose F_1, say $F_1(X) = t_s(X - \theta_1) \cdots (X - \theta_s)$, with $\theta_1, \ldots, \theta_s \in \mathbb{C}$, then

$$|R(\tilde{F}(X), F_1(X))| = |t_s|^n \prod_{1 \leq j \leq s} |\tilde{F}(\theta_j)|.$$

Now, since θ_j is also a root of F, we have $p\tilde{F}(\theta_j) + a_0 = 0$, so $\tilde{F}(\theta_j) = -\frac{a_0}{p}$ for $j = 1, \ldots, s$, which shows that

$$|R(\tilde{F}(X), F_1(X))| = \frac{|t_s|^n |a_0|^s}{p^s},$$

which can not be an integer, since $p \nmid t_sa_0$. This completes the proof.

3. Examples

1) *For any prime number p, any non-constant polynomial $F \in \mathbb{Z}[X]$ with leading coefficient not divisible by p, the polynomial $pF(X)^2 + F(X) + p + 1$ is irreducible over $\mathbb{Q}$.*

The result follows immediately by Theorem 1.2.

2) *For any prime number p, any non-constant polynomial $F \in \mathbb{Z}[X]$ with leading coefficient not divisible by p, any positive integer k prime to $\deg F$, and any integer s with $0 \le s < k$, the polynomial $p^k F(X)^2 + F(X) + p^s$ is irreducible over $\mathbb{Q}$.*

The proof follows by Theorem 1.3, since the polynomial $p^k X^2 + X + p^s$ is irreducible and its constant term is not divisible by p^k.

3) *For any odd prime number p, any non-constant polynomial $F \in \mathbb{Z}[X]$ with leading coefficient not divisible by p, the polynomial $pF(X)^2 + (p^2 - 2p + 4)F(X) + p$ is irreducible over $\mathbb{Q}$.*

Note that one can not apply Theorem 1.2, since the constant term of the polynomial $pX^2 + (p^2 - p + 4)X + p$ is divisible by p. On the other hand, this polynomial is irreducible, since its discriminant $(p-2)^2(p^2+4)$ can never be a perfect square for odd primes p, and one may also write it as

$$pX^2 + (p^2 - p + 4)X + p = (aX + b)(cX + d) + (eX + f)(gX + h)$$

with $a = d = p - 1$, $b = c = e = f = g = h = 1$. Since $(af - be)(ah - bg) = (p-2)^2$, which is not divisible by p, one can apply Theorem 1.4 to conclude that $pF(X)^2 + (p^2 - 2p + 4)F(X) + p$ is irreducible over $\mathbb{Q}$. We also note here that for $p = 2$ our polynomial is $2(F(X)+1)^2$, which is obviously reducible.

4) *For any polynomial F of odd degree with integer coefficients and leading coefficient not divisible by 3, the polynomial $9F(X)^2 + 73F(X) + 36$ is irreducible over $\mathbb{Q}$.*

Here we can not apply Theorem 1.3 with $p = 3$ and $k = 2$, since the constant term of the irreducible polynomial $9X^2 + 73X + 36$ is divisible by 9. Instead, one may write

$$9X^2 + 73X + 36 = (8X + 4)(X + 8) + (X + 1)(X + 4),$$

so by Theorem 1.5 with $a = 8$, $b = 4$, $c = 1$, $d = 8$, $e = f = g = 1$ and $h = 4$, since

$$(af - be)(ah - bg) = 112,$$

which is not divisible by 9, we conclude that $9F(X)^2 + 73F(X) + 36$ is irreducible over $\mathbb{Q}$.

Acknowledgements The authors are grateful to an anonymous referee for suggestions that improved the presentation of the paper. This work was supported by a 2015 LEA math-mode project.

References

[1] A.I. Bonciocat, N.C. Bonciocat, M. Cipu, *Irreducibility criteria for compositions and multiplicative convolutions of polynomials with integer coefficients*, An. Şt. Univ. Ovidius Constanţa, vol. 22 (1) (2014), 73–84.

[2] A.I. Bonciocat, N.C. Bonciocat, A. Zaharescu, *On the number of factors of convolutions of polynomials with integer coefficients*, Rocky Mountain J. Math. 38 (2)(2008), 417–431.

[3] A.I. Bonciocat, A. Zaharescu, *Irreducibility results for compositions of polynomials with integer coefficients*, Monatsh. Math. 149 (1)(2006), 31–41.

[4] N.C. Bonciocat, *Upper bounds for the number of factors for a class of polynomials with rational coefficients*, Acta Arith. 113 (2)(2004), 175–187.

[5] N.C. Bonciocat, Y. Bugeaud, M. Cipu, M. Mignotte, *Irreducibility criteria for sums of two relatively prime polynomials*, Int. J. Number Theory 9 (6) (2013), 1529–1539.

[6] A. Brauer, R. Brauer, H. Hopf, *Über die Irreduzibilität einiger spezieller Klassen von Polynomen*, Jahresber Deutsch Math-Verein 35 (1926), 99–112.

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

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

[9] H.L. Dorwart, O. Ore, *Criteria for the irreducibility of polynomials*, Ann. of Math. 34 (1934), 81–94.

[10] G. Dumas, *Sur quelques cas d'irreductibilité des polynômes à coefficients rationnels*, Journal de Math. Pures et Appl. 2 (1906), 191–258.

[11] G. Eisenstein, *Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. Reine Angew. Math. 39 (1850), 160–182.

[12] K. Győry, *Sur l'irreducibilité d'une classe des polynômes. I*, Publ. Math. Debrecen 18 (1972), 289–307.

[13] K. Győry, *Sur l'irreducibilité d'une classe des polynômes. II*, Publ. Math. Debrecen 19 (1973), 293–326.

[14] K. Győry, *On the irreducibility of a class of polynomials. III*, J. Number Theory 15 (1982), 164–181.

[15] K. Győry, *On the irreducibility of a class of polynomials. IV*, Acta Arith. 62 (1992), 399–405.

[16] K. Győry, *On the irreducibility of neighbouring polynomials*, Acta Arith. 67 (1994), 283–294.

[17] K. Győry, L. Hajdu, R. Tijdeman, *Irreducibility criteria of Schur-type and Pólya-type*, Monatsh. Math. 163 (4)(2011), 415–443.

[18] A. Schinzel, *Polynomials with special regard to reducibility.* In Encyclopedia of Mathematics and its Applications, 77, Cambridge Univ. Press, 2000.

[19] T. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, J. Reine Angew. Math. 32 (1846), 93–105.

[20] U. Wegner, *Über die Irreduzibilität einer Klasse von ganzen rationalen Funktionen*, Jahresber Deutsch Math Verein 40 (1931), 239–241.

Institute of Mathematics of the Romanian Academy, Research Unit 5, P.O. Box 1-764, Bucharest 014700, Romania

E-mail address: Nicolae.Bonciocat@imar.ro, Mihai.Cipu@imar.ro

Université de Strasbourg, Mathématiques, 7, rue René Descartes, 67084 Strasbourg Cedex, France

E-mail address: yann.bugeaud@math.unistra.fr, maurice.mignotte@math.unistra.fr