Publ. Math. Debrecen
65/3-4 (2004), 363–370

Irreducible polynomials in arithmetic progressions and a problem of Szegedy

By LAJOS HAJDU (Debrecen)

To the memory of Professor B. Brindza

Abstract. In this paper we show that under certain assumptions, every sufficiently long arithmetic progression of polynomials in $\mathbb{Z}[x]$ contains an irreducible polynomial. Our result is effective, and can be considered as an extension of a result of Győry on a problem of Szegedy concerning irreducible polynomials. We also derive a lower bound for the constant $C_1(m)$ occurring in Szegedy's problem. Finally, we provide some numerical results, and propose a quantitative version of this problem.

1. Introduction

In 1984 M. Szegedy proposed the following problem (cf. e.g. [3]):

Does there exist a constant $C_1(m)$ depending only on m such that for any $P \in \mathbb{Z}[x]$ of degree m, $P(x) + b$ is irreducible over $\mathbb{Q}$ for some $b \in \mathbb{Z}$ with $|b| \leq C_1(m)$?

Under an extra condition, this problem was solved by K. Győry [3], who proved the following

Mathematics Subject Classification: 11C08.
Key words and phrases: irreducible polynomials, arithmetic progressions, Szegedy's problem, Turán's problem.
Research supported in part by the János Bolyai Research Fellowship of the Hungarian Academy of Sciences and by the OTKA grants T042985 and F034981.

Theorem A. *Let $P \in \mathbb{Z}[x]$ be a polynomial of degree m with leading coefficient a_0 and let $\omega(a_0)$ denote the number of distinct prime divisors of a_0. There exist an effectively computable constant C_2 depending only on m and $\omega(a_0)$ and an integer b with $|b| \leq C_2$ for which $P(x) + b$ is irreducible over $\mathbb{Q}$.*

If P is monic, then $\omega(a_0) = 0$. Thus in this case the above deep result of Győry provides an affirmative answer to Szegedy's problem. We also note that in [3] the constant C_2 is given explicitly.

In the above problem of Szegedy one is allowed to change only the constant term of P in order to obtain an irreducible polynomial. In 1962 P. Turán proposed a similar problem where one is allowed to change each coefficient of P (cf. [4]). To formulate Turán's problem, for $P \in \mathbb{Z}[x]$ denote by $|P|$ the length of P, i.e. the sum of the absolute values of the coefficients of P. By the distance of two polynomials $P, Q \in \mathbb{Z}[x]$ we mean $|P - Q|$. Turán asked the following:

Does there exist an absolute constant C_3 such that for every $P(x) \in \mathbb{Z}[x]$ of degree m, there is a polynomial $Q(x) \in \mathbb{Z}[x]$ irreducible over $\mathbb{Q}$, satisfying $\deg(Q) \leq m$ and $|P - Q| \leq C_3$?

This question is also very deep and hard. On omitting the condition for the degree of the irreducible polynomial Q, A. Schinzel [5] provided a positive answer to this problem. More precisely, he proved the following nice result.

Theorem B. *For every $P \in \mathbb{Z}[x]$ of degree m there are infinitely many irreducible $Q \in \mathbb{Z}[x]$ such that*

$$|P - Q| \leq \begin{cases} 2, & \text{if } \ P(0) \neq 0, \\ 3, & \text{otherwise.} \end{cases}$$

Further, one of these irreducible polynomials Q satisfies

$$deg(Q) \leq e^{(5m+7)(|P|^2+3)}.$$

We note that the results of A. Bérczes and L. Hajdu [1], [2] imply that $C_3 \geq 2$ and that for polynomials of degree ≤ 24 we have $C_3 \leq 5$.

Theorem A can be interpreted as follows: for any $P \in \mathbb{Z}[x]$ of degree m the arithmetic progression $P(x) + b$ ($b \in \mathbb{Z}$) contains an irreducible polynomial with $|b| \leq C_2$. In this paper we extend this result to the case of

any arithmetic progression of polynomials of the form $P(x)+bQ(x)$, where $P, Q \in \mathbb{Z}[x]$ with $\deg(P) > \deg(Q)$ and $\gcd(P, Q) = 1$ in $\mathbb{Q}[x]$. By finding suitable "extremal" polynomials, we also give an explicit lower bound for the Szegedy constant $C_1(m)$. Finally, we present some numerical results which might indicate that the answer to Szegedy's problem is affirmative, with a very good value of $C_1(m)$. Based upon our results, we propose a quantitative version of Szegedy's problem.

2. Notation and results

To formulate our results we need some notation. As usual, for any non-zero integer u let $\omega(u)$ denote the number of distinct prime divisors of u, with the agreement that $\omega(\pm 1) = 0$. If $P, Q \in \mathbb{Q}[x]$ then we will write $\mathrm{Res}(P, Q)$ for the resultant of P and Q. In case of $P(x) = \sum_{i=0}^{n} a_i x^i$ define the height of P by $H(P) = \max_{i=0,\ldots,n} |a_i|$.

The following result is an extension of Theorem A of Győry to the case of arithmetic progressions of polynomials, where the difference is not necessarily a constant.

Theorem 1. *Suppose that $P, Q \in \mathbb{Z}[x]$ are relatively prime polynomials in $\mathbb{Q}[x]$, and that $m = \deg(P) > \deg(Q)$. Let a_0 denote the leading coefficient of P. Then there exists an integer b with $0 \le b \le c_1$ for which $P(x) + bQ(x)$ is irreducible over $\mathbb{Q}$. Here $c_1 = c_1(m, \omega(a_0 Res(P, Q)))$ is an effectively computable constant depending only on m and $\omega(a_0 \mathrm{Res}(P, Q))$.*

Remark 1. If we further assume that P has only simple zeros, the above statement easily follows from Theorem 7 of Győry [3]. We also mention that as $\mathrm{Res}(P, 1) = 1$, Theorem 1 can be considered as a generalization of Theorem A of Győry indeed.

Remark 2. We derive Theorem 1 from two lemmas. One of them (Lemma 2) is a variant of the above mentioned Theorem 7 of Győry [3], which uses Schmidt's well-known subspace theorem. So we can say that our Theorem 1 ultimately relies on this deep result of number theory.

The next theorem provides an explicit lower bound for the value of $C_1(m)$, provided that this constant exists.

Theorem 2. *Let m be an integer with $m \geq 2$, and suppose that the assertion of the problem of Szegedy holds true for this m. Then we have $C_1(m) > m/2$.*

Remark 3. It was noted by Győry [3] that the constant $C_1(2)$ exists, and $C_1(2) = 2$ holds. This follows from the fact that four distinct squares cannot form an arithmetic progression.

In the following statement we give an upper bound for $C_1(m)$, for polynomials of small degree and height. As the number of polynomials to be considered rapidly grows with the degree and the height, we could cover only a little set. The aim of the forthcoming theorem is to get some impression about how far the lower bound $m/2$ obtained for $C_1(m)$ in Theorem 2 can be from the real value.

Theorem 3. *Let m be an integer with $3 \leq m \leq 5$, and write $H(3) = 50$, $H(4) = 25$ and $H(5) = 10$. Then for every polynomial $P \in \mathbb{Z}[x]$ of degree m and of height at most $H(m)$ there exists an integer b with $|b| \leq 3$ such that $P(x) + b$ is irreducible over $\mathbb{Q}$.*

Remark 4. The polynomials $4x^3 - 5x$, $4x^4 + 6x^3 + 2x^2 + x - 1$, and $x^5 - x^4 - 5x^3 + 2x^2 + 6x + 2$ show that the bound for $|b|$ in Theorem 3 cannot be improved.

In the following theorem we allow to modify both the constant and the leading coefficients of the polynomials. The reason why we do so is that this statement is proved via reducing the polynomials modulo p for the appropriate prime p. To handle degenerate cases, i.e. when the leading coefficient a_0 is divisible by p, it is helpful if we can modify a_0. Moreover, letting a_0 being changed simplifies the situation considerably, and makes it possible to investigate more cases.

Theorem 4. *Let m be an integer with $3 \leq m \leq 6$, and write $(A_m, B_m) = (1, 2)$, $(2, 2)$, $(2, 11)$, $(5, 11)$ for $m = 3, 4, 5, 6$, respectively. Then for every polynomial $P \in \mathbb{Z}[x]$ of degree m there exist integers a and b with $|a| \leq A_m$ and $|b| \leq B_m$ such that $P(x) + ax^m + b$ is irreducible over $\mathbb{Q}$. Moreover, if $m = 3$ and we further assume that the leading coefficient of P is not divisible by 7, then $P(x) + b$ is irreducible over $\mathbb{Q}$ for some integer b with $|b| \leq 3$.*

Using Theorem 3, Remark 4, and Theorem 4 we obtain the following simple

Corollary. *For every polynomial $P(x)$ of degree 3 with leading coefficient not divisible by 7 there exists an integer b with $|b| \leq 3$ for which $P(x) + b$ is irreducible over $\mathbb{Q}$. Moreover, this bound for $|b|$ cannot be improved.*

Based upon Theorem 2 and our numerical results we propose the following quantitative form of the problem of Szegedy:
Is it true that for any $P \in \mathbb{Z}[x]$ of degree m, $P(x)+b$ is irreducible over $\mathbb{Q}$ for some $b \in \mathbb{Z}$ with $|b| \leq C_1(m)$, where $C_1(m)$ is a linear function of m?

We note that Theorem A of Győry was proved with the value

$$C_2 = \exp\exp\left\{(\omega(a_0)+1)^6 2^{19(m+1)!}\right\}.$$

It was also mentioned in [3] that using a result of Evertse this value could be reduced to

$$C_2 = \exp\left\{(\omega(a_0)+1)\log(\omega(a_0)+2)(2^{17}m)^{m^3}\right\}.$$

So the above formulation of Szegedy's problem predicts a huge improvement in C_2.

3. Proofs

To prove Theorem 1, we need two lemmas. The first one is new, while the second one is due to Győry [3].

Lemma 1. *Let P, Q be relatively prime polynomials in $\mathbb{C}[x]$ with $\deg(P) = m$, $\deg(Q) = n$, $m+n > 0$. Then there exists an integer b_0 with $0 \leq b_0 \leq m+n-1$ for which $P(x) + b_0 Q(x)$ has only simple zeros.*

Proof. If $P(x) + bQ(x)$ has a multiple zero x_0, then

$$P(x_0) + bQ(x_0) = P'(x_0) + bQ'(x_0) = 0, \tag{1}$$

hence $P(x_0)Q'(x_0) - P'(x_0)Q(x_0) = 0$. However, since $\gcd(P, Q) = 1$, $m+n > 0$, the polynomial $PQ' - P'Q$ is not identically zero, of degree at

most $m+n-1$. Thus the number of x_0's satisfying (1) is at most $m+n-1$. For every such x_0 we have $Q(x_0) \neq 0$, otherwise $P(x_0) = 0$, contrary to $\gcd(P, Q) = 1$. Hence to every x_0 there corresponds exactly one b and the number of admissible b's is at most $m+n-1$. Since the number of integer b's satisfying $0 \leq b \leq m+n-1$ is $m+n$, the lemma follows. □

Lemma 2. *Let P, Q, a_0 and m be as in Theorem 1, with the further assumption that P has only simple zeros. Then the number of non-negative integers α for which $P(x) + 2^{\alpha}Q(x)$ is reducible is bounded by an effectively computable constant $c_2(m, \omega(a_0\mathrm{Res}(P, Q)))$, depending only on m and $\omega(a_0\mathrm{Res}(P, Q))$.*

Proof. The statement is a straightforward consequence of Theorem 7 of Győry [3]. □

Proof of Theorem 1. Let P and Q be fixed. By Lemma 1 there exists an integer b_0 with $0 \leq b_0 \leq 2m-1$ such that the polynomial $P(x) + b_0Q(x)$ has only distinct zeros. Fix such a b_0 and put $P_0(x) = P(x) + b_0Q(x)$. Note that the leading coefficient of P_0 is a_0 and that $\mathrm{Res}(P_0, Q) = \mathrm{Res}(P, Q)$.

By Lemma 2 we obtain that for some α_0 with

$$0 \leq \alpha_0 \leq c_2(m, \omega(a_0\mathrm{Res}(P_0, Q)))$$

the polynomial $P_0(x) + 2^{\alpha_0}Q(x)$ is irreducible over $\mathbb{Q}$. Now in view of $\mathrm{Res}(P_0, Q) = \mathrm{Res}(P, Q)$ and $0 \leq b_0 \leq 2m-1$, the theorem follows with $c_1 = 2m - 1 + 2^{c_2(m, \omega(a_0\mathrm{Res}(P,Q)))}$. □

Remark 5. Note that using a more sophisticated approach, it is possible to derive a better constant than our c_1 in Theorem 1. For this purpose one can follow the proof of Theorem 1 of Győry [3].

Proof of Theorem 2. Define the polynomials $f_m(x)$ in the following way. Put $f_0(x) = 1$, and if $f_{m-1}(x)$ is already defined for some integer m with $m \geq 1$ then write

$$f_m(x) = (1 - (m+1)x)f_{m-1}(x) + m + 1.$$

One can easily check by induction that for every $m \in \mathbb{N}$ and $i \in \{1, \ldots, m+1\}$ we have $f_m(1/i) = i$. Write

$$g_m(x) = f_m(x) - [m/2] - 1.$$

Then for each m with $m \geq 2$ and for every integer b with $|b| \leq m/2$ we have that $g_m(x) + b$ has a rational zero, hence it is reducible. As clearly $g_m(x)$ is a polynomial of degree m with integer coefficients, the theorem follows. □

PROOF OF THEOREM 3. To prove the statement we simply checked all the polynomials in question, using the program package MAPLE. (Note that in view of the Corollary of Theorem 4, for $m = 3$ it is sufficient to consider only polynomials with leading coefficient divisible by 7.) □

PROOF OF THEOREM 4. As is well-known, if $Q \in \mathbb{Z}[x]$ and p is a prime such that p does not divide the leading coefficient of Q, then the irreducibility of Q modulo p implies the irreducibility of Q over $\mathbb{Q}$.

To prove the statement for $m = 3$ and 4 we simply used the above observation, and by the help of MAPLE we checked all the polynomials modulo 7 and 5, respectively.

In case of $m = 5$ we worked modulo 11. A computation with MAPLE yielded the statement with $(A_5, B_5) = (2, 2)$, except for polynomials of the shape $P(x) = a_0x^5 + 11a_1x^4 + 11a_2x^3 + 11a_3x^2 + 11a_4x + a_5$. However, for such polynomials the assertion trivally holds by the irreducibility criterion of Eisenstein.

When $m = 6$, we worked with $p = 11$ again. By a preliminary computation we obtained the statement with $(A_6, B_6) = (5, 5)$, except for polynomials of the form $P(x) = a_0x^6 + 11a_1x^5 + 11a_2x^4 + 11a_3x^3 + 11a_4x^2 + 11a_5x + a_6$. Using again Eisenstein's criterion, the theorem follows also in this case. □

ACKNOWLEDGEMENTS. The author is grateful to professor K. GYŐRY for his helpful and useful remarks. The author is indebted to the referee for his guiding suggestions. In particular, the present formulation and proof of Lemma 1 is due to the referee, and means a significant simplification compared to the previous version.

References

[1] A. Bérczes and L. Hajdu, Computational experiences on the distances of polynomials to irreducible polynomials, *Math. Comp.* **66** (1997), 391–398.

[2] A. Bérczes and L. Hajdu, On a problem of P. Turán concerning irreducible polynomials, Number Theory: Diophantine, Computational and Algebraic Aspects, (K. Győry, A. Pethő and V. T. Sós, eds.), *Walter de Gruyter*, *Berlin – New York*, 1998, 95–101.

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

[4] A. Schinzel, Reducibility of polynomials and covering systems of congruences, *Acta Arith.* **13** (1967), 91–101.

[5] A. Schinzel, Reducibility of lacunary polynomials II, *Acta Arith.* **16** (1970), 371–392.

LAJOS HAJDU
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF DEBRECEN
AND THE NUMBER THEORY RESEARCH GROUP
OF THE HUNGARIAN ACADEMY OF SCIENCES
H-4010 DEBRECEN, P.O.B. 12
HUNGARY

E-mail: hajdul@math.klte.hu

(Received April 22, 2004; revised July 16, 2004)