ON A PROBLEM OF P. TURÁN CONCERNING IRREDUCIBLE POLYNOMIALS

A. Bérczes and L. Hajdu

1. Introduction

Many important and interesting problems of mathematics are related to the distribution of irreducible elements in some special structures. It is well-known that the number of primes in $\mathbb{N}$ is infinite. However, the set of prime numbers is of density zero and the gap between two consecuitve primes can be arbitrarily large. In $\mathbb{Z}[x]$ there are infinitely many irreducible polynomials. Nevertheless, it seems that there are only few common properties of the distribution of irreducible elements in $\mathbb{Z}$ and in $\mathbb{Z}[x]$. Indeed, if we denote by $P(N)$ resp. $R(N)$ the number of polynomials resp. irreducible polynomials in $\mathbb{Z}[x]$ of given degree and height at most N, then we have (cf. [7])

$$\frac{R(N)}{P(N)} \to 1 \text{ as } N \to \infty.$$

In other words 'almost all' polynomials in $\mathbb{Z}[x]$ are irreducible.

The above result suggests that the 'gap' between 'neighbouring' irreducible polynomials in $\mathbb{Z}[x]$ cannot be too large. Perhaps these facts led P. Turán in 1962 to propose the following interestring problem. To formulate his problem, we need the concept of the length $|P|$ of a polynomial $P(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x]$ which is defined by the expression

$$|P| = \sum_{k=0}^{n} |a_k| \ .$$

By the distance of $P, Q \in \mathbb{Z}[x]$ we mean $|P - Q|$. It follows easily from Eisenstein's theorem that for given $P \in \mathbb{Z}[x]$ of degree n there is an irreducible polynomial $Q \in \mathbb{Z}[x]$ of degree n such that $|P - Q| \leq n + 2$. P. Turán asked the following (cf.[9]):

Does there exist an absolute constant C_1 such that for every $P(x) \in \mathbb{Z}[x]$ of degree n, there is a polynomial $Q(x) \in \mathbb{Z}[x]$ irreducible over $\mathbb{Q}$, satisfying deg(Q) $\leq$ n and $|P - Q| \leq C_1$?

This problem is very difficult. It turns to be somewhat easier if one removes the condition deg$(Q) \leq$ n. In 1970, A. Schinzel [10] proved the following deep and important theorem:

[0]Research of the first author was supported in part by the Universitas Foundation of Kereskedelmi Bank RT. Research of the second author was supported in part by Grants 014245 and T 016 975 from the Hungarian National Foundation for Scientific Research.

Theorem A. (A. Schinzel [10]) *For any nonzero integers a, b and any polynomial P with integral coefficients, such that $P(0) \neq 0$ and $P(1) \neq -a-b$, there exist infinitely many irreducible polynomials $ax^n + bx^m + P(x)$ with $n > m > deg(P)$. One of them satisfies*

$$n < \exp\{(5\deg(P) + 2\log|ab| + 7)(||P|| + a^2 + b^2)\},$$

where $||P||$ denotes the sum of the squares of the coefficients of P.

As a cosequence of this theorem Schinzel showed that for every $P \in \mathbb{Z}[x]$ of degree n 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

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

This result gives a partial answer to Turán's question.

For the shake of completeness, now we present another, similar problem, which was proposed in 1984 by M. Szegedy (cf. [5]). He asked the following:

Does there exist a constant C_2 depending only on n such that for any $P \in \mathbb{Z}[x]$ of degree n, $P(x) + b$ is irreducible over $\mathbb{Q}$ for some $b \in \mathbb{Z}$ with $|b| \leq C_2$?

This seems also to be a very hard question. In 1994, K. Győry [5] succeeded to give an affirmative answer for Szegedy's problem in case of monic polynomials. This is a consequence of his following

Theorem B. (K. Győry [5]) *Let $P \in \mathbb{Z}[x]$ be a polynomial of degree n with leading coefficient a_0. There exist an effectively computable constant C_3 depending only on n and $\omega(a_0)$, and $b \in \mathbb{Z}$ with $|b| \leq C_3$ for which $P(x) + b$ is irreducible over $\mathbb{Q}$. (Here $\omega(a_0)$ denotes the number of distinct prime divisors of a_0.)*

We remark that in [5] C_3 is given explicitly.

In our recent paper [1] we gave upper bounds for the Turán constant C_1 for monic polynomials P of degree not greater than 22. In fact we could prove that for such polynomials $C_1 = 4$ can be chosen. Slightly improving our algorithms and using more powerful computers now we extend our result to polynomials of degree at most 24.

2. New results

For a positive integer n denote by c_n the smallest integer with the property that for any monic polynomial $P \in \mathbb{Z}[x]$ of degree n one can choose an irreducible monic polynomial $Q \in \mathbb{Z}[x]$ of degree n, such that $|P - Q| \leq c_n$. One can verify easily that for every positive n, c_n exists. Using this notation, our result in [1] says that

$$c_n \leq 4 \quad \text{for every positive integer } n \leq 22.$$

We prove the following extension.

Theorem. *For every positive integer $n \leq 24$ and for every monic polynomial $P \in \mathbb{Z}[x]$ of degree n there exists an irreducible monic polynomial $Q \in \mathbb{Z}[x]$ of degree n such that*

$$|P - Q| \leq 4.$$

For lower degrees, our computations imply a slightly better result. In fact we could prove that $c_1 = 0$, $c_2 = 1$, $c_n = 2$ for $3 \leq n \leq 6$, $c_n \leq 3$ for $7 \leq n \leq 12$, and $c_n \leq 4$ for $13 \leq n \leq 24$ (see our Table I). Summarizing these assertions, we can state that for any positive integer $n \leq 24$, we have $c_n \leq 4$.

We remark that in principle, results on the distribution of irreducible polynomials (mod p) (see e.g. [2], [3], [4], [6] or [8]) could make it easier to determine the Turán constant, at least for fixed degree. However, these results contain asymptotic formulas, hence it seems to be difficult to apply them in practical computations.

The investigation of Szegedy's constants C_2 by computational methods seems to be much more difficult.

In view of our result mentioned above, it suffices to prove our Theorem for polynomials of degre 23 and 24. As the proof is similar to the proof given in [1] for polynomials of degree ≤ 22, we do not detail it now. However, for the convenience of the reader we give an outline of the method used. For this purpose we need some further notation.

Let p be any prime. For every polynomial $T \in \mathbb{Z}[x]$ denote by $T_p(x)$ the corresponding polynomial in $\mathbb{Z}_p[x]$. If $T(x)$ is of degree k, then it has a unique representation of the form

$$\sum_{i=0}^{k} a_i x^i \ ,$$

with $-p/2 < a_i \leq p/2$ for $i = 0, ..., k$. Now by the p-length $|T|_p$ of $T(x)$ we mean the number $\sum_{i=0}^{k} |a_i|$. The p-distance of $S, T \in \mathbb{Z}[x]$ is $|S - T|_p$. Denote by $c_n(p)$ the least positive integer such that for every monic $P \in \mathbb{Z}_p[x]$ of degree n one can find an irreducible monic $Q \in \mathbb{Z}_p[x]$ of degree n with $|P - Q|_p \leq c_n(p)$.

The main idea of the proof is the following. If $Q \in \mathbb{Z}[x]$ is a monic polynomial which is irreducible (mod p) for some prime p, then $Q(x)$ must be irreducible in $\mathbb{Z}[x]$, too. This implies that if a monic polynomial $P \in \mathbb{Z}[x]$ and a prime p are given, then for any $Q \in \mathbb{Z}[x]$ which is (mod p) irreducible and monic and has the property $\deg(Q) = \deg(P)$, there exists an irreducible monic polynomial $R \in \mathbb{Z}[x]$ of the same degree as P, such that $|R - P|$ is not greater than the distance of Q and P in $\mathbb{Z}[x]$ (mod p). Hence to get bounds for Turán's constant for monic polynomials (of fixed degree) it is sufficent to deal with polynomials in $\mathbb{Z}[x]$ (mod p), for some prime p.

In our algorithms we worked with the primes 2 and 3. However, the prime $p = 3$ could be used only for small values of the degree n ($n \leq 12$), because in this case the number of polynomials to be considered is much larger than for $p = 2$. Nevertheless, even in this simplest case of $p = 2$, we had to stop at the degree $n = 24$. The reason of this is the fact that the number of polynomials in $\mathbb{Z}_p[x]$ grows exponentially with the degree.

In the following two tables we summarize our results. The first one is in fact an extended version of Table IV of our paper [1], and contains estimates concerning the values of c_n for $1 \leq c_n \leq 24$. The second table, similarly to Table I of [1], contains so called 'extreme polynomials', which show that the coresponding values of $c_n(2)$ are sharp. We *conjecture* that for every $n \geq 10$ there exists an extreme polynomial $P_n(x) \in \mathbb{Z}_2[x]$ of degree n such that $P_n(x) - x^n + 1$ is irreducible (mod 2). For $n = 23$ and 24 we found extreme polynomials having this property (see Table II).

We mention that in [1] we published another table, presenting the result of our computation using the prime $p = 3$.

Table I.

Degree n	*Bound for* c_n
1	0
2	1
3	2
4	2
5	2
6	2
7	3
8	3
9	3
10	3
11	3
12	3
13	4
14	4
15	4
16	4
17	4
18	4
19	4
20	4
21	4
22	4
23	4
24	4

Table II.

n	*Extreme polynomials*
23	$x^{23} + x^{21} + x^{20} + x^{16} + x^{15} + x^{11} + x^{10}$
24	$x^{24} + x^{23} + x^7 + x^6 + x^2$

Acknowledgements

We would like to thank Professors K. Győry and A. Schinzel for their valuable remarks.

References

1. A. Bérczes and L. Hajdu, *Computational experiences on the distances of polynomials to irre-*

ducible polynomials, Math. Comp. **66** (1997), 391-398.
2. S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. **17** (1970), 255–271.
3. S. D. Cohen, *The distribution of polynomials over finite fields, II*, Acta Arith. **20** (1972), 53–62.
4. S. D. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. **6** (1972), 93–102.
5. K. Győry, *On the irreducibility of neighbouring polynomials*, Acta Arith. **67** (1994), 283–294.
6. D. R. Hayes, *The distribution of irreducibles in* GF[q,x], Trans. Amer. Math. Soc. **117** (1965), 101–127.
7. H.-W. Knobloch, *Zum Hilbertschen Irreduzibilitätssatz*, Abh. Math. Sem. Univ. Hamburg **19** (1955), 176-190.
8. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge Univ. Press, 1986.
9. A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. **13** (1967), 91–101.
10. A. Schinzel, *Reducibility of lacunary polynomials II*, Acta Arith. **16** (1970), 371–392.

Department of Mathematics and Informatics, Kossuth Lajos University, 4010 Debrecen, Pf. 12, Hungary

E-mail address: berczes@dragon.klte.hu, hajdul@math.klte.hu