ON THE NUMBER OF TERMS IN THE IRREDUCIBLE FACTORS OF A POLYNOMIAL OVER $\mathbb{Q}$

by A. CHOUDHRY AND A. SCHINZEL

(Received 29 June, 1990)

All polynomials considered in this paper belong to $\mathbb{Q}[x]$ and reducibility means reducibility over $\mathbb{Q}$. It has been established by one of us **[5]** that every binomial in $\mathbb{Q}[x]$ has an irreducible factor which is either a binomial or a trinomial. He has further raised the question "Does there exist an absolute constant K such that every trinomial in $\mathbb{Q}[x]$ has a factor irreducible over $\mathbb{Q}$ which has at most K terms (i.e. K non-zero coefficients)?"

A similar question could be asked for a quadrinomial, or, more generally, for a polynomial with m non-zero coefficients. This paper deals with the general problem, that could be formulated as follows:

Given a positive integer m does there exist a number K such that every polynomial in $\mathbb{Q}[x]$ with m non-zero coefficients has a factor irreducible over $\mathbb{Q}$ with at most K non-zero coefficients (K "terms")?

If for a given m numbers K with the above property exist we denote by $K(m)$ the least of them, otherwise we put $K(m) = \infty$.

We shall prove

THEOREM. (i) $K(3) \geq 8$, (ii) $K(4) \geq 13$, (iii) $K(5) \geq 14$, (iv) $K(6) \geq 16$ *and for every* $m > 2$: $K(m) > \max\{2m, c_1 m^{c_2}\}$, *where* $c_1 = 0{\cdot}014$ *and* $c_2 = 1{\cdot}22$ *are both independent of* m.

Proof.

(i) $m = 3$.

This case has been dealt earlier by Bremner **[1]** who has proved $K(3) \geq 8$, without, however explicitly giving the trinomial concerned. We shall obtain the same result by a numerical example. We write

$$f(x) = x^7 + 20x^6 + 200x^5 + 2450x^4 + 29\,000x^3 + 545\,000x^2 + 8\,101\,250x + 35\,275\,000.$$

Then we have the identity

$$f(x)f(-x) = -x^{14} - 27\,180\,501\,562\,500x^2 + 35\,275\,000^2.$$

We prove the irreducibility of $f(x)$ and $f(-x)$ by using the method of G. Dumas **[3]** (cf. Dorwart **[2]**) based on Newton polygon. The Newton polygon corresponding to $f(x)$ for the prime 2 is shown on Figure 1.

It follows from the irreducibility theorem of Dumas that the proper factors of $f(x)$ can only be of degree 1 or 6, thus if $f(x)$ is reducible it has a factor $x - \lambda$, where λ is an integer. We must have $\lambda \mid 35\,275\,000$, also $10 \mid \lambda$ and finitely many possible values of λ are easily ruled out. Therefore $f(x)$ is irreducible and as it has 8 terms $K(3) \geq 8$.

(ii) $m = 4$. Let

$$f(x) = x^{12} + 4x^{11} + 8x^{10} + 16x^9 + 32x^8 + 64x^7 + 128x^6 + 192x^5 + 256x^4 + 384x^3 + 512x^2 + 640x + 512.$$

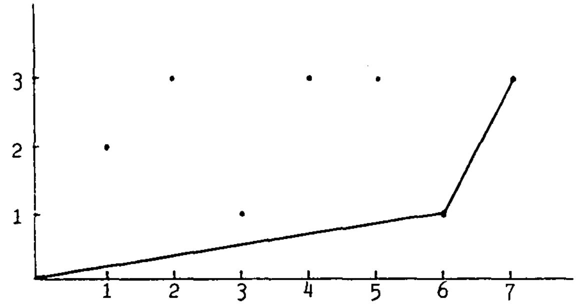

Figure 1.

We have the identity

$$f(x)f(-x) = x^{24} + 32\,768x^4 + 114\,688x^2 + 262\,144.$$

To prove that $f(x)$ is irreducible, we construct the Newton polygon corresponding to $f(x)$ for the prime 2 (Figure 2).

It then follows from the irreducibility theorem of Dumas that the proper factors of $f(x)$ must be of degree 1 or 11. Thus if $f(x)$ is reducible it must have a factor $x - \lambda$, where λ is an integer and $\lambda \mid 512$. All such factors are easily ruled out. Hence $f(x)$ is irreducible and as it has 13 non-zero coefficients $K(4) \geq 13$.

(iii) $m = 5$. Let

$$\begin{aligned} f(x,t) &= 8x^{13} - 16x^{12} + 16x^{11} - 16x^{10} + 16x^9 - 16x^8 + 16x^7 - 8tx^6 \\ &\quad + (16t - 16)x^5 - (20t - 24)x^4 + (24t - 32)x^3 - (27t - 38)x^2 \\ &\quad + (30t - 44)x + 2t^2 - 23t + 30 \\ &= 2t^2 - t(8x^6 - 16x^5 + 20x^4 - 24x^3 + 27x^2 - 30x + 23) + 8x^{13} - 16x^{12} + 16x^{11} \\ &\quad - 16x^{10} + 16x^9 - 16x^8 + 16x^7 - 16x^5 + 24x^4 - 32x^3 + 38x^2 - 44x + 30. \end{aligned}$$

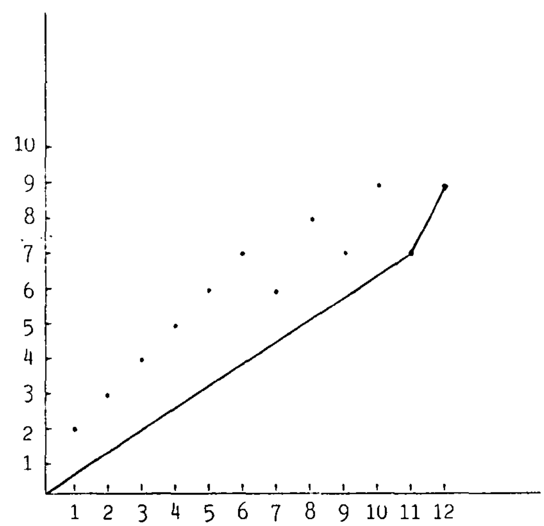

Figure 2.

https://doi.org/10.1017/S001708950000848X Published online by Cambridge University Press

As the coefficients of t^2, t, t^0 have the highest common factor 1, $f(x,t)$ has no factors depending only on x. Moreover its discriminant with respect to t is not a perfect square and $f(x,t)$ is thus irreducible in x, t. By virtue of Hilbert's irreducibility theorem ([**4**], cf. also [**6**], p. 179) there exist infinitely many integers t for which $f(x,t)$ is irreducible. The identity

$$\begin{aligned} f(x,t)f(-x,t) = &-64x^{26} - (32t^3 + 88t^2 - 608t + 608)x^6 \\ &- (80t^3 - 305t^2 + 324t - 68)x^4 \\ &- (108t^3 - 494t^2 + 728t - 344)x^2 + (2t^2 - 23t + 30)^2 \end{aligned}$$

provides us with infinitely many examples which show that

$$K(5) \geq 14.$$

(iv) $m = 6$.

To prove $K(6) \geq 16$, we use another polynomial defined by

$$\begin{aligned} f(x,t) = &(575 - 2t)x^{15} + (2t^3 - 444t^2 + 30\,032t - 582\,402)x^{14} \\ &+ (t^3 - 222t^2 + 15\,016t - 291\,070)x^{13} + (-2t^2 + 304t - 7708)x^{12} \\ &+ (-t^2 + 152t - 3812)x^{11} + (4t - 28)x^{10} + 2tx^9 + 74x^8 \\ &+ 42x^7 + 20x^6 + 12x^5 + 6x^4 + 4x^3 + 2x^2 + 2x + 1 \\ = &(2x^{14} + x^{13})t^3 - (444x^{14} + 222x^{13} + 2x^{12} + x^{11})t^2 \\ &- (2x^{15} - 30\,032x^{14} - 15\,016x^{13} - 304x^{12} - 152x^{11} - 4x^{10} - 2x^9)t \\ &+ 575x^{15} - 582\,402x^{14} - 291\,070x^{13} - 7708x^{12} - 3812x^{11} \\ &- 28x^{10} + 74x^8 + 42x^7 + 20x^6 + 12x^5 + 6x^4 + 4x^3 + 2x^2 + 2x + 1. \end{aligned}$$

The polynomial $f(x,t)$ is irreducible as a polynomial in two variables. Indeed, it has no factor depending only on x, since the coefficients of t^3 and t^0 are relatively prime. Therefore the only possible factorisation would be

$$f(x,t) = \{a(x)t + b(x)\}\{c(x)t^2 + d(x)t + e(x)\}.$$

Hence

(i) $a(x)c(x) = 2x^{14} + x^{13}$
(ii) $a(x)d(x) + b(x)c(x) = -444x^{14} - 222x^{13} - 2x^{12} - x^{11}$
(iii) $a(x)e(x) + b(x)d(x) = -2x^{15} + \ldots + 2x^9$
(iv) $b(x)e(x) = f(x,0)$

Let a, b, c, d, e be divisible exactly by $x^\alpha, x^\beta, x^\gamma, x^\delta, x^\epsilon$ respectively. By (i) $\alpha + \gamma = 13$, by (iv) $\beta = \epsilon = 0$, hence by (iii) either $\alpha \geq 9$, $\delta \geq 9$ or $\alpha = \delta$. In the former case, the degrees with respect to x of both factors of the first term on the left hand side of (ii) are at least 9, hence the degree of the product is at least 18, a contradiction. In the latter case by (ii) either $\alpha + \delta = 2\alpha \geq 11$, $\beta + \gamma = 13 - \alpha \geq 11$, hence $26 = 2\alpha + 2(13 - \alpha) \geq 33$, a contradiction, or $\alpha + \delta = \beta + \gamma$; $2\alpha = 13 - \alpha$, $3\alpha = 13$, a contradiction.

Since $f(x,t)$ is irreducible as a polynomial in x and t, Hilbert's theorem gives the existence of infinitely many integers such that $f(x,t)$ is irreducible in x. We also note that in the product $f(x,t)f(-x,t)$ only the coefficients of $x^{30}, x^{28}, x^{26}, x^{24}, x^{22}$ and x^0 are not

https://doi.org/10.1017/S001708950000848X Published online by Cambridge University Press

zero. The other coefficients are all 0, so we have only six non-zero terms in the product and it follows that

$$K(6) \geq 16.$$

(v) For the general case of a polynomial with m non-zero terms, we establish $K(m) \geq 2m$ by an explicit example.

Let

$$f(x) = px^{2m-1} + 2px^{2m-2} + 2px^{2m-3} + \ldots + 2px^3 + p^2x^2 + 2p(p-1)x + 2(p-1)^2.$$

Then the only non-zero terms in the product $f(x)f(-x)$ are the coefficients of x^{4m-2}, x^{2m-2}, x^{2m-4}, $x^{2m-6}, \ldots, x^4$ and x^0. Thus, the product $f(x)f(-x)$ has only m non-zero terms and if we take p as an odd prime, both $f(x)$ and $f(-x)$ are irreducible in view of Einstenstein's criterion.

This proves that

$$K(m) \geq 2m.$$

To prove $K(m) > c_1 m^{c_2}$, we use a result of Verdenius [7] who has established that for every positive integer n, there exists a polynomial $f(x)$ of the n^{th} degree with real integer coefficients such that $f^2(x)$ consists of less than $\frac{1}{5}(162n^{\log_9 6} - 12)$ terms. For any such polynomial $f(x)$, we have the identity

$$\{f(px) - pf(x)\}\{f(px) + pf(x)\} = f^2(px) - p^2f^2(x).$$

While the two factors on the left hand side have n and $(n+1)$ terms respectively, their product has m terms, $m < \frac{1}{5}(162n^{\log_9 6} - 12)$. Also, if $f(x) = a_0x^n + \ldots + a_n$ and p is a prime number such that $p \nmid a_0$ and $p \nmid a_n$, both factors on the left hand side are irreducible in view of Einsenstein's criterion.

It follows that $K(m) \geq n$.

Now

$$m < \tfrac{1}{5}(162n^{\log_9 6} - 12)$$

yields

$$n > \left(\frac{5m + 12}{162}\right)^{\log_6 9}$$

or

$$n > c_1 m^{c_2}$$

where

$$c_1 = 0{\cdot}014\ldots$$

$$c_2 = 1{\cdot}22\ldots.$$

Hence for every integer m, $K(m) \geq c_1 m^{c_2}$.

Thus, for each m, $K(m) \geq 2m$ and also $K(m) > c_1 m^{c_2}$, so we have

$$K(m) \geq \max\{2m, c_1 m^{c_2}\}$$

where $c_1 = 0{\cdot}014\ldots$ and $c_2 = 1{\cdot}22\ldots.$

https://doi.org/10.1017/S001708950000848X Published online by Cambridge University Press

REFERENCES

1. A. Bremner, On reducibility of trinomials, *Glasgow Math. J.* **22** (1981), 155–156.

2. H. L. Dorwart, Irreducibility of polynomials, *Amer. Math. Monthly* **42** (1935), 369–381.

3. G. Dumas, Sur quelques cas d'irréductibilité des polynômes à coefficients rationels, *Journal Math. pures appl* (2) **6** (1906) 191–258.

4. D. Hilbert, Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, *Ges. Abh. Bd II* 264–286.

5. A. Schinzel, Some unsolved problems in polynomials, *Matematicka biblioteka*, **25** (1963) 63–70.

6. A. Schinzel, *Selected Topics on Polynomials*, (The University of Michgan Press, 1982).

7. W. Verdenius, On the number of terms of the square and the cube of polynomials, *Indag. Math.* **11** (1949) 459–465.

Deputy High Commissioner,
High Commission of India,
31 Grange Road,
Singapore 0923.

Mathematical Institute,
Polish Academy of Sciences,
P.O. Box 137, 00 950 Warszawa,
Poland.