Trends in Mathematics
Information Center for Mathematical Sciences
Volume 3, December 2000, Pages 87–92

SUMS OF POLYNOMIALS AND NUMBER THEORY

SEON-HONG KIM

Abstract. The article focuses on sums of polynomials that have some number theoretic components. More precisely, we consider two topics: Fermat-type problems on polynomials such as Mason's theorem and abc-conjecture influenced by Mason's theorem, and number theoretic results derived from zero distribution of sums of two polynomials with each having real zeros symmetric with the other.

1. Introduction

To what extent can a sum and its factorization both be known? More precisely, if A and B belong to a ring, to what extent can we simultaneously know the factorizations of A, B and C where $A + B = C$? There is an inverse problem: Given C, find A and B with factorizations of a specific type such that $A + B = C$. Much of the original motivation comes from results and questions about integers and power series. In the ring of integers, the undecided Goldbach problem is whether $2n = A + B$ where n is an integer > 2 and A, B are odd primes. The problem of whether z^n $(n \geq 2)$ can be written as the sum of two numbers whose factorization is of the same type is the famous Fermat problem. Affirmative answers for $n = 2$ were well known in classical times; Wiles has shown, in 1993, that for $n \geq 3$ there are no nontrivial solutions. One of the most glorious results in this direction for power series is Jacobi's theta-function identity (see p. 35 of [1]).

In this article, we focuses on sums of polynomials and their factorizations that have some number theoretic components. More precisely, we will consider two topics: Fermat-type problems on polynomials such as Mason's theorem and abc-conjecture influenced by Mason's theorem, and number theoretic results derived from sums of two polynomials with each having real zeros symmetric with the other.

2. The $abc-$conjecture and Fermat-type problem on polynomials

In mathematics history, new insights have been gained in old problems combined with new ones. In number theory, great coherence has been achieved in understanding a number of diophantine inequalities. Some of these results can be formulated in very simple terms. In this section, we start with these formulations, relations among polynomials, and end with the $abc-$conjecture for integers.

The Fermat last theorem suggests the problem of whether $A(x) + B(x) = C(x)$ is possible where the polynomials $A(x), B(x)$ and $C(x)$ have very few distinct zeros

2000 *Mathematics Subject Classification.* Primary 11C08; Secondary 30C15.
Key words and phrases. sums, polynomials, $abc-$conjecture, Mason's theorem, arithmetic progression, geometric progression.
Received August 31, 2000.

and deg $A(x)$ = deg $B(x)$ = deg $C(x)$. Here Mason's ABC polynomial theorem (see [11]) gives a negative result. In 1981, Stothers [17] proved a theorem on polynomials, which did not attract too much attention until 1983, when Mason [14] started a new trend of thought about polynomials by discovering the same theorem. In 1998, Snyder gave his own version of proof for this theorem when he was still a high school student.

Theorem 2.1. (Stothers-Mason-Snyder) *Let $m(P) = m(P(x))$ be the number of distinct zeros of a polynomial $P(x)$. Let*

$$A + B = C,$$

where A, B and C are relatively prime polynomials. Then

$$max\ deg(A, B, C) \le m(ABC) - 1.$$

The cases of equality in Mason's ABC polynomial theorem are linked to numerous results in number theory; triple of integers generated by these cases lead, by using the $abc-$conjecture, to optimal minoration of $Q(G(A, B))$ (where $G \in \mathbb{Z}[X, T]$ is a form, A, B are relatively prime integers, and $Q(k)$ denotes the product of the distinct primes dividing k); in these polynomial constructions of integers, the role of the Mason's theorem is crucial (See [12], [13]). A new identity (see [10]) that shows a case of equality (related to Chebyshev polynomials) in Mason's theorem is

$$x^{2k} = \left(x^k T_k\left(\frac{i}{x}\right)\right)^2 + (x^2+1)\left(x^{k-1}U_{k-1}\left(\frac{i}{x}\right)\right)^2,$$

where T and U denote the Chebyshev polynomials of the first and the second, respectively. Their factorizations are of course completely known.

Another Fermat-type problem on polynomials is the question of the existence of relatively prime polynomials $P(x), Q(x), R(x)$ over the complex number field such that for some integer $n > 2$ $[P(x)]^n + [Q(x)]^n = [R(x)]^n$. The answer, due to an application of Mason's theorem (see [11]), is that no such polynomials exist.

Influenced by Mason's theorem, Masser and Oesterlé formulated the $abc-$conjecture for integers as follows. The well known $abc-$conjecture states : Given $\epsilon > 0$, there is a number C_ϵ such that for any prime positive integers a, b, c with $a + b = c$, we have

$$c < C_\epsilon \left(Q(abc)\right)^{1+\epsilon}, \tag{2.1}$$

where $Q(k) = \prod_{p|k} p$ denotes the product of the distinct primes dividing k. Unlike the polynomial case, it is necessary to have the ϵ in the formulation of the conjecture, and C_ϵ on the right side. The conjecture implies that many prime factors of abc occur to the first power, and that if some prime numbers occur to hight powers, then they have to be compensated by "large" primes, or many primes, occurring to the first power. See [11] for a discussion of the history and implications of the conjecture. Although the $abc-$conjecture seems completely out of reach, there are some results towards the truth of this conjecture. In 1986, Stewart and Tijdeman

[15] obtained an upper bound $\exp\{C_1 Q(abc)^{15}\}$ for c of the type (2.1) for some absolute constant C_1. In 1991, Stewart and Yu [16] improved the upper bound by $c < \exp\{C_2 Q(abc)^{2/3+\epsilon}\}$, where C_2 is a positive effectively computable constant in terms of ϵ. There is another way to attack the abc-conjecture. Taking log of each side of the inequality (2.1) derives

$$\log(a+b) < (1+\epsilon)\log Q(ab(a+b)) + \log C_\epsilon.$$

Denote

$$L_{a,b} = \frac{\log(a+b)}{\log Q(ab(a+b))}, \tag{2.2}$$

and let $\{L_{a,b}\}$ denote a sequence whose values are these numbers $L_{a,b}$, taken in some fixed order. If the $abc-$conjecture holds, the greatest limit point of the double sequence $\{L_{a,b}\}$ would in fact equal to 1. To see this, take $a = 1$, $b = 2^n - 1$. Then

$$Q(ab(a+b)) = 2 \prod_{p|2^n-1} p < 2^{n+1},$$

so $L_{a,b} > \frac{n}{n+1} \to 1$ as $n \to \infty$. Hence we can reformulate the $abc-$conjecture: The double sequence $\{L_{a,b}\}$ is a bounded sequence with its greatest limit point equal to 1. Let S be the set of all limit points of $\{L_{a,b}\}$. Browkin, Filaseta, Greaves, Schinzel [2] showed that $[1/3, 15/16] \subseteq S$ by use of a sieve method, and the $abc-$conjecture is in fact equivalent to the assertion that S is the interval $[1/3, 1]$. Here the entry $1/3$ is best possible because $\log(a+b) \geq 1/3 \log(ab(a+b)) \geq 1/3 \log Q(ab(a+b))$ in (2.2). Polynomial identities of Greaves and Nitaj [5] implie that $[1/3, 36/37] \subseteq S$. It is not known 1 is a limit point. However, Filaseta and Konyagin showed in [4] that $S \cap [1, 3/2) \neq \emptyset$. Hence for the truth of this conjecture it is enough to show that $S \cap [1, 3/2) = \{1\}$.

3. Sums of two polynomials with each having real zeros symmetric with the other

Perhaps the most immediate question of sums of polynomials, $A + B = C$, is "given bounds for the zeros of A and B, what bounds can be given for the zeros of C?" By Fell [3], if all zeros of A and B lie in $[-1, 1]$ with A, B monic and deg $A =$ deg $B = n$, then no zero of C can have modulus exceeding $\cot(\pi/2n)$, the largest zero of $(x+1)^n + (x-1)^n$. Hence it is natural to study polynomials having a form something like $A(x)+B(x)$ where all zeros of $A(x)$ are negative and all zeros of $B(x)$ are positive. All zeros of the polynomial equation $\prod_{i=1}^n (x - r_i) + \prod_{i=1}^n (x + r_i) = 0$, where $0 < r_1 \leq r_2 \leq \cdots \leq r_n$ lie on the imaginary axis. Kim [8] characterized the set S_n of all positive numbers $\{s_1, \cdots, s_{\lfloor n/2 \rfloor}\}$ such that $\{\pm i\, s_1, \cdots, \pm i\, s_{\lfloor n/2 \rfloor}\}$ is the set of nonzero zeros of some $P(x) = \prod_{i=1}^n (x - r_i) + \prod_{i=1}^n (x + r_i)$, where $0 < r_1 \leq r_2 \leq \cdots \leq r_n$. We remark that an $\{s_i\} \in S$ does not determine an $\{r_i\}$ uniquely, for example, $(x-1)(x-2)(x-3) + (x+1)(x+2)(x+3) = (x-\alpha)^3 + (x+\alpha)^3$, where $\alpha = \sqrt{22/6} = 1.914\cdots$. In general no two of the s_i can be equal. Of special interest (in number theory) is to investigate whether elements of S_n can be arithmetic or geometric progressions. Kim [8] proved that the gaps between the zeros on the imaginary axis increase as one proceeds upwards. Hence there are no arithmetic progressions in S_n. We can, however, find some geometric progressions in S_6, S_8 and S_{10} (see [8]). Some simple examples of geometric progressions in S_6 arise from the identity

$$\begin{aligned}(x-a)^3(x-b)^3+(x+a)^3(x+b)^3 &= 2(u+ab)(u^2+(3a^2+8ab+3b^2)u+(ab)^2)\\ &= 2\,Q_1(u)Q_2(u),\ \ u=x^2, \quad \text{say},\end{aligned}$$

since the product of the zeros of Q_2 is the square of the zero of Q_1. A further question of interest is whether <u>both</u> the r_i and the s_i can be in geometric progression. Observe the identity

$$\begin{aligned}&(x-h)(x-hq^2)(x-hq^4)(x-hq^6)(x-hq^8)(x-hq^{10})\\ &\quad+(x+h)(x+hq^2)(x+hq^4)(x+hq^6)(x+hq^8)(x+hq^{10})\\ =&2(x^2+1)(x^2+h^2q^{10})(x^2+h^4q^{20})\\ &\quad-2x^2(x^2+h^2q^{10})\left(1-q^2(q^4+1)\frac{q^7-1}{q-1}\frac{q^7+1}{q+1}h^2+h^4q^{20}\right).\end{aligned}$$

If we take $q=2$ and $h=0.5950\cdots$, a zero of

$$2^{20}h^4-371348h^2+1,$$

the last factor on the right side of the identity becomes zero and we have a case in which the r_i and the s_i are both in geometric progression, <u>and</u> the r_i are all distinct. An example (3.1) below is also a case in which <u>both</u> the r_i and the s_i are in geometric progression. Moreover (3.1) below is of considerable interest in connection with [9]. Observe that $(x-1)^6+(x+1)^6=2(x^2+1)(x^2+(2-\sqrt{3})^2)(x^2+(2+\sqrt{3})^2)$. Let r_1 and r_3 be the real and mutually reciprocal zeros of

$$E_m(u) := u^{2m}-u^{m+1}-2u^m-u^{m-1}+1=0, \quad m\geq 2,$$

and set $r_2=1$. Then we have

$$\prod_{i=1}^{3}(x-r_i)^2+\prod_{i=1}^{3}(x+r_i)^2=2\prod_{i=1}^{3}(x^2+r_i^{2m}). \tag{3.1}$$

Also, for $j=1,3$, as $m\to\infty$, $r_j\to 1$ and $r_j^m\to 2\pm\sqrt{3}$. On the other hand, Kim studied in [9] as follows. A simple equality $(x-1)^4+(x+1)^4=2(x^2+(\sqrt{2}-1)^2)(x^2+(\sqrt{2}+1)^2)$ is in fact the limiting case $m\to\infty$ of the sequence of readily verified identities

$$\prod_{i=1}^{2}(x-r_i)^2+\prod_{i=1}^{2}(x+r_i)^2=2\prod_{i=1}^{2}(x^2+r_i^{2m}), \quad m\geq 2, \tag{3.2}$$

where $r_1=r_m$ is the unique positive zero of $F_m(u) := u^{2m}-u^{m+1}-u^{m-1}-1$, and $r_2=1/r_m$. As $m\to\infty$,

$$(x-r_m)^n(x-\frac{1}{r_m})^n+(x+r_m)^n(x+\frac{1}{r_m})^n\to(x-1)^{2n}+(x+1)^{2n}. \tag{3.3}$$

Here $r_m \to 1$ and $r_m^m \to 1+\sqrt{2}$ as $m \to \infty$. Thus we have a situation quite analogous to that of (3.2). The limit (3.3) motivates the introduction to new analogues

$$2\binom{n}{\frac{k}{2}}{}_2F_1\left(-\frac{k}{2}, -\frac{1}{2}(2n-k); \frac{1}{2}; \frac{1}{4}\left(r_m + r_m^{-1}\right)^2\right) \tag{3.4}$$

of $2\binom{2n}{k}$ (k even). Kim [9] studied their minimal polynomials which are related to Chebyshev polynomials. Moreover, he showed that the analogue of $2\binom{2n}{2}$ is the only real zero of its minimal polynomial, and has a different representation, by using a polynomial of smaller degree than $F_m(u)$. He also described how to compute the minimal polynomial of an analogue of $2\binom{2n}{k}$ $(k > 2)$ by using an analogue of $2\binom{2n}{2}$.

We end up this section with following Kim's questions and conjecture in this direction. Are there geometric progressions in S_n $(n \geq 10)$? If so, are there examples with both the r_i and the s_i in geometric progression? From (3.1) we can derive similar analogues of $2\binom{2n}{k}$ (k even) to (3.4) and study their minimal polynomials. Are there appropriate settings? Finally we conjecture the following: Suppose $r_i = q^i$, where $q > 0$. Let $\epsilon > 0$ be given. Then for n sufficiently large

$$\left|\frac{s_{m+1}}{s_m} - q^2\right| < \epsilon$$

for $n/4 \leq m \leq 3n/8$. Some related results to the topic of this section are also given in [6] and [7].

References

[1] J. M. Borwein, P. B. Borwein, *Pi and the AGM*, John Wiley & Sons, Inc., New York, 1998.

[2] J. Browkin, M. Filaseta, G. Greaves, A. Schinzel, *Squarefree values of polynomials and the abc-conjecture*, Sieve Methods, Exponential Sums, and their Applications in Number Theory (G. Greaves, G. Harman, M. Huxley, eds.), Cambridge Univ. Press, Cambridge, 1997, pp. 65–85.

[3] H. J. Fell, *On the zeros of convex combinations of polynomials*, Pacific J. Math. **89** (1980), 43–50.

[4] M. Filaseta, S. Konyagin, *On a limit point associated with the abc-conjecture*, Colloq. Math. **76** (1998), 265–268.

[5] G. Greaves, A. Nitaj, *Some polynomial identities related to the abc-conjecture*, Number Theory in Progress (K. Gyoery et al, eds.), Proceedings of the international conference organized by the Stefan Banach International Mathematical Center in honor of the 60th birthday of Andrzej Schinzel, Berlin, 1999, pp. 229–236.

[6] S. H. Kim, *Bad pairs of polynomial zeros*, Commun. Korean Math. Soc. (to appear).

[7] ———, *Convex combinations of products of finite geometric series* (preprint).

[8] ———, *Sums of two polynomials with each having real zeros symmetric with the other* (preprint).

[9] ———, *The analogues of* $2\binom{2n}{k}$ *with* k *even* (preprint).

[10] ———, *Zeros of certain sums of two polynomials* (preprint).

[11] S. Lang, *Old and new conjectured diophantine inequalities*, Amer. Math. Bull. **23** (1990), 37–50.

[12] M. Langevin, *Sur quelques conséquences de la conjecture (abc) en arithmétique et en logique*, Rocky Mount. J. of Math **26** (1996), 1031–1042.

[13] ———, *Imbrications entre le théoréme de Mason, la descente de Belyi et les différentes formes de la conjecture (abc)*, J. Théor. Nombres Bordeaux **11** (1999), 91–109.

[14] R. C. Mason, *Diophantine equations over functional fields*, London Mathematical Society Lecture Note Series, 96, Cambridge University Press, Cambridge, New York, 1984.

[15] C. L. Stewart, R. Tijdeman, *On the Oesterle-Masser conjecture*, Monatsh. Math. **102** (1986), 251–257.

[16] C. L. Stewart, K. Yu, *On the abc conjecture*, Math. Ann. **291 No. 2** (1991), 225–230.
[17] W. W. Stothers, *Polynomial identities and Hauptmodulen*, Quart. J. Math. Oxford Ser. (2) **32** (1981), 349–370.

Department of Mathematics, Seoul National University, Seoul, 151-742, Korea
E-mail address: shkim@math.snu.ac.kr