On sums and products in $\mathbb{C}[x]$

Ernie Croot and Derrick Hart

February 8, 2010

1 Introduction

Suppose that S is a subset of a ring R (in our case, the real or complex numbers), and define

$$S.S \ := \ \{st \ : \ s, t \in S\}, \text{ and } S + S \ := \ \{s + t \ : \ s, t \in S\}.$$

An old problem of Erdos and Szemerédi [9] is to show that

$$|S.S| + |S + S| \ \gg \ |S|^{2-o(1)}.$$

Partial progress on this problem has been achieved by Erdős and Szemerédi [9], Nathanson [13], Ford [10], Elekes [8], and Solymosi in [17] and in the astounding article [18]. There is the work of Bourgain-Katz-Tao [5] and Bourgain-Glibichuk-Konyagin [4] extending the results to $\mathbb{F}_p$, and then also the recent work of Tao [19] which extends these results to arbitrary rings.

We will prove a theorem below (Theorem 1), which holds for the polynomial ring $\mathbb{C}[x]$ *unconditionally*; but, under the assumption of a certain 24-term version of Fermat's Last Theorem, it holds for $\mathbb{Z}_+$, the positive integers, as we will explain below. This *unconditional* result for $\mathbb{C}[x]$, for which there presently is no analogue for $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Z}$ or $\mathbb{F}_p$ (though, Chang [6, 7] has a related sort of result for $\mathbb{Z}$ as we discuss in remarks below.), is as follows.

Theorem 1 *There exists an absolute constant $c > 0$ such that the following holds for all sufficiently large sets S of monic polynomials of $\mathbb{C}[x]$ of size n:*

$$|S.S| \ < \ n^{1+c} \quad \Longrightarrow \quad |S + S| \ \gg \ n^2.$$

Remark 1. M.-C. Chang [6] has shown that if S is a set of integers such that $|S.S| < n^{1+\varepsilon}$, then $|S+S| > n^{2-f(\varepsilon)}$, where $f(\varepsilon) \to 0$ as $\varepsilon \to 0$. Though, note that this is quite a different sort of result from Theorem 1 above, even given that the two results work in different rings: In the case of Chang's result, the ε has to be essentially 0 in order to deduce that $|S+S| \gg n^2$, whereas in Theorem 1 above, perhaps $c = 0.0001$ is small enough to guarantee $|S+S| \gg n^2$ – the precise value of c needed will come out of the proof.

Remark 2. It is perhaps possible to replace the condition that the polynomials be "monic" with the condition that none is a scalar multiple of another; however, it will make the proof more complicated (if our method of proof is used).

Now let us consider the following conjecture, which can be thought of as a weak 24-term extension of Fermat's Last Theorem.

Conjecture. There exists a positive integer m such that the only solutions to the Diophantine equation

$$\varepsilon_1 x_1^m + \varepsilon_2 x_2^m + \cdots + \varepsilon_{24} x_{24}^m \ = \ 0,\ \varepsilon_i = \pm 1,\ x_1, ..., x_{24} \in \mathbb{Z}_+ \qquad (1)$$

are the trivial ones; that is, solutions where each $\varepsilon_i x_i^m$ can be paired with its negative $\varepsilon_j x_j^m$, so that $x_i = x_j$ and $\varepsilon_i = -\varepsilon_j$.

Under the assumption of this conjecture, we have that Theorem 1 holds for when S is a set of positive integers (instead of monic polynomials); in other words,

Theorem 2 *Suppose that the above* **Conjecture** *is true. Then, there exists an absolute constant $c > 0$ such that the following holds for all sufficiently large sets S of n positive integers:*

$$|S.S| \ < \ n^{1+c} \quad \Longrightarrow \quad |S+S| \ \gg \ n^2.$$

Because the proof of this theorem is virtually identical to the proof of Theorem 1, where every use of Theorem 4 below is simply replaced with the above **Conjecture**, we omit the proof.

We also prove the following theorem, which extends a result of Bourgain and Chang [3] from $\mathbb{Z}$ to the ring $\mathbb{C}[x]$.

Theorem 3 *Given a real $c \geq 1$ and integers $\ell, k \geq 1$, the following holds for all n sufficiently large: Suppose that S is a set of n polynomials of $\mathbb{C}[x]$, where none is a scalar multiple of another, and suppose that*

$$|S^\ell| \;=\; |S.S...S| \;<\; n^c.$$

Then,

$$|kS| \;>\; n^{k-f(c,k,\ell)},$$

where for fixed c and k, $f(c,k,\ell) \to 0$ as $\ell \to \infty$.

Remark 1. It is possible to generalize our method of proof to the case of polynomials over $\mathbb{F}_p[x]$, but in that context there are thorny issues concerning the vanishing of certain Wronskian determinants that make the problem difficult. There are also issues that come up in handling pth powers of polynomials, which the differentiation mapping sends to the 0 polynomial.

Remark 2. If the analogue of this theorem for when $S \subseteq \mathbb{C}$ could be proved, then it would also provide a proof to the above, since we could locate an element $\alpha \in \mathbb{C}$ such that the evaluation map $\alpha : f \in \mathbb{C}[x] \to f(\alpha) \in \mathbb{C}$ preserves the structure of the sums and products of these polynomials.

Remark 3. Using the above results, one can easily prove analogues of them for the polynomial ring $\mathbb{C}[x_1, x_2, ..., x_k]$, simply by applying an evaluation map $\psi : \mathbb{C}[x_1, ..., x_k] \to \mathbb{C}[x_1, \alpha_1, ..., \alpha_k]$, for some carefully chosen $\alpha_1, ..., \alpha_k$.

The proofs of Theorems 2 and 1 rely on the following basic fact about polynomials, which we prove near the end of the paper using ideas of Mason [12]. It has recently been brought to our attention that this theorem follows from results of Pinter [14] and Voloch [20], though we prefer to keep our proof below as it is elementary and self-contained.

Theorem 4 *For every $k \geq 2$, there exists an exponent M such that there are no polynomial solutions to*

$$f_1(x)^m + \cdots + f_k(x)^m \;=\; 0,\; m \geq M, \tag{2}$$

where no polynomial is a scalar multiple of another.

Remark. As a consequence of [1], [2], this equation has no solutions under the condition that all the polynomials are pairwise coprime; though, we can get the theorem without such assumptions by applying results from [14] and [20], as noted above.

We will also make use of the Ruzsa-Plunnecke [15], [16] inequality, stated as follows.

Theorem 5 (Ruzsa-Plunnecke) *Suppose that S is a finite subset of an additive abelian group, and that*

$$|S+S| \ \leq \ K|S|.$$

Then,

$$|kS - \ell S| \ = \ |S+S\cdots+S-S-S-\cdots-S| \ \leq \ K^{k+\ell}|S|.$$

2 Proof of Theorem 1

By invoking Theorem 4, let $M \geq 1$ be the smallest value such that the polynomial equation

$$f_1(x)^m + \cdots + f_k(x)^m \ = \ 0$$

has no solutions for $m \geq M$, and $k \leq 24$, assuming no f_i is a constant multiple of another. And, when we generalize the present proof (of Theorem 1) to handle the proof of Theorem 2, we just assume that M is such that if $m \geq M$, then (1) has no non-trivial solutions.

We assume throughout that

$$|S.S| \ < \ n^{1+c},$$

where $c > 0$ is some parameter that can be determined by working through the proof – the point is that, although c will be quite small, it will be possible to take it to be some explicit value.

Let

$$\varepsilon \ = \ c(M+1),$$

and note that by the Ruzsa-Plunnecke inequality (Theorem 5) we have that since $|S.S| < n^{1+c}$,

$$|S^{M+1}| \ = \ |S...S| \ < \ n^{1+\varepsilon}.$$

(The sole use of $\varepsilon > 0$ in the rest of the proof is to simplify certain expressions.)

Let us begin by supposing that

$$|S+S| \ = \ o(n^2).$$

Then, for all but at most $o(n^2)$ pairs $(x_1, x_2) \in S \times S$, there exists (x_3, x_4) with

$$\{x_3, x_4\} \ \neq \ \{x_1, x_2\},$$

such that

$$x_1 + x_2 \ = \ x_3 + x_4.$$

Let P denote the set of all such $n^2 - o(n^2)$ pairs (x_1, x_2). It is clear that there exists a bijection

$$\varphi \ : \ P \ \rightarrow \ P,$$

where φ maps pairs having sum s to pairs having sum s, and yet where if

$$(x_3, x_4) \ = \ \varphi((x_1, x_2)),$$

then

$$\{x_3, x_4\} \ \neq \ \{x_1, x_2\}.$$

Using such a pairing φ of pairs (x_1, x_2), we then define a set of quadruples

$$Q \ := \ \{(x_1, x_2, x_3, x_4) \ : \ (x_1, x_2) \in P, \ (x_3, x_4) = \varphi((x_1, x_2))\}.$$

Note that

$$|Q| \ = \ |P| \ \sim \ n^2,$$

and

$$(x_1, x_2, x_3, x_4) \in Q \ \ \Longrightarrow \ \ x_1 + x_2 - x_3 - x_4 \ = \ 0.$$

2.1 A lemma about quadruples

To proceed further we require the following lemma.

Lemma 1 *There exists a 5-tuple* $a, b, c, d, t \ \in \ S$ *such that for* $\gg \ n^{2-4\varepsilon}$ *quadruples*

$$(x_1, x_2, x_3, x_4) \ \in \ Q$$

we have that

$$t^M(x_1, x_2, x_3, x_4) \ = \ (at_1^M, bt_2^M, ct_3^M, dt_4^M), \text{ where } t_1, t_2, t_3, t_4 \in S.$$

Proof of the lemma. Let N denote the number of pairs $(x_1, t) \in S \times S$ for which there are fewer than $n^{1-\varepsilon}/40$ pairs $(a, t_1) \in S \times S$ satisfying

$$x_1 t^M \;=\; a t_1^M.$$

Clearly,

$$\begin{aligned} N &\leq (n^{1-\varepsilon}/40)|\{\alpha\beta^M \;:\; \alpha, \beta \in S\}| \\ &\leq (n^{1-\varepsilon}/40)|S^{M+1}| \\ &< n^2/40. \end{aligned}$$

Given $x_1 \in S$ we say that t is "bad" if (x_1, t) is one of the pairs counted by N; otherwise, we say that t is "good". From the bounds above, it is clear that more than $4n/5$ values $x_1 \in S$ have $\leq n/8$ bad values of t; for, if there were fewer than $4n/5$ such $x_1 \in S$, then $\geq n/5$ have $> n/8$ bad values of t, which would show that $N > n^2/40$, a contradiction.

It follows that more than $3n^2/5$ pairs $(x_1, x_2) \in S^2$ have the property that both x_1 and x_2 have at most $n/8$ bad values of t. So, there are at least

$$n \;-\; 2n/8 \;=\; 3n/4$$

values of t that are "good" for both x_1 and x_2.

Clearly, then, by the pigeonhole principle, there are

$$\gtrsim \; n^2/5 \;\; \text{quadruples } (x_1, x_2, x_3, x_4) \in Q,$$

such that there are at least $n/2$ values of t that are good for all x_1, x_2, x_3 and x_4 at the same time (disguised in what we are doing here is the fact that φ is a bijection from $P \to P$).

When t is good for all x_1, x_2, x_3 and x_4, we say that it is "good" for the quadruple (x_1, x_2, x_3, x_4).

By the pigeonhole principle again, there exits $t \in S$ that is good for at least

$$\gtrsim n^2/10$$

quadruples of Q.

Now suppose that $(x_1, x_2, x_3, x_4) \in Q$ is one of these $\sim n^2/10$ quadruples, for some particular value of t. We define

$$\begin{aligned} A &:= \{a \in S \;:\; a t_1^M = x_1 t^M,\; t_1 \in S\} \\ B &:= \{b \in S \;:\; b t_2^M = x_2 t^M,\; t_2 \in S\} \\ C &:= \{c \in S \;:\; c t_3^M = x_3 t^M,\; t_3 \in S\} \\ D &:= \{d \in S \;:\; d t_4^M = x_4 t^M,\; t_4 \in S\}. \end{aligned}$$

Under the assumption that t is good, we have

$$|A|, |B|, |C|, |D| \ \geq \ n^{1-\varepsilon}/40.$$

So, among the $\gtrsim n^2/10$ quadruples for which t is good, by the pigeonhole principle again, there exists $a, b, c, d \ \in \ S$ for which there are

$$\gtrsim \ (n^2/10)(n^{-\varepsilon}/40)^4 \ \gg \ n^{2-4\varepsilon}$$

quadruples $(x_1, x_2, x_3, x_4) \in Q$ satisfying

$$x_1 t^M = a t_1^M, \ ..., \ x_4 t^M = d t_4^M.$$

This completes the proof of the lemma. ■

2.2 Resumption of the proof of Theorem 1

Upon applying the previous lemma, let Q' denote the set of quadruples

$$(t_1, t_2, t_3, t_4) \ \in \ S^4,$$

such that

$$x_1 t^M = a t_1^M, \ ..., \ x_4 t^M = d t_4^M,$$

where (x_1, x_2, x_3, x_4) is one of the $\gg n^{2-4\varepsilon}$ quadruples satisfying the conclusion of the lemma. Note that

$$a t_1^M + b t_2^M - c t_3^M - d t_4^M \ = \ 0.$$

Now we claim that we can find three quadruples

$$(t_1, ..., t_4), \ (u_1, ..., u_4), \ (v_1, ..., v_4) \ \in \ Q',$$

such that

$$t_2/t_1 \neq u_2/u_1, \ t_2/t_1 \neq v_2/v_1, \ u_2/u_1 \neq v_2/v_1, \tag{3}$$

and

$$t_4/t_3 \neq u_4/u_3, \ t_4/t_3 \neq v_4/v_3, \ u_4/u_3 \neq v_4/v_3. \tag{4}$$

The reason that we can find such quadruples is as follows: Suppose we fix $(t_1, ..., t_4)$ to be any quadruple of Q', and suppose that we pick $(u_1, ..., u_4)$ in order to attempt to avoid

$$t_2/t_1 = u_2/u_1. \tag{5}$$

Let $r = t_2/t_1 \in S/S$. If (5) holds for all (u_1, u_2), it means that each pair (u_1, u_2) must be of the form

$$(u_1, u_2) = r(t_1, t_2).$$

But, by Ruzsa-Plunnecke,

$$|S/S| \ < \ n^{1+\varepsilon},$$

so there are at most $n^{1+\varepsilon}$ pairs among the first two entries of quadruples of Q'; but, since there at $\gg n^{2-4\varepsilon}$ quadruples of Q', and since the first two coordinates of the quadruple determine the second pair of coordinates (via the mapping φ) we clearly must not have that all pairs (u_1, u_2) satisfy (5). In fact, there are $\gg n^{2-\varepsilon} - O(n^{1+\varepsilon})$ pairs (quadruples) to choose from!

In a similar vein, we can pick $(u_1, ..., u_4)$ and $(v_1, ..., v_4)$, so that all the remaining conditions (3) and (4) hold.

Before proceeding with the rest of the proof, it is worth pointing out that the sort of condition on our four-tuples that we cannot so easily force to hold is, for example,

$$t_1/t_3 \neq u_1/u_3.$$

The reason for this is that we do not have a good handle on how many pairs (t_1, t_3) or (u_1, u_3) there are – t_3 (or u_3) may be related to t_1 (or u_1) in a completely trivial way, leading to few pairs.

2.3 A lemma about submatrices

Now we require a lemma concerning the matrix

$$T \ := \ \left[\begin{array}{cccc} t_1^M & t_2^M & t_3^M & t_4^M \\ u_1^M & u_2^M & u_3^M & u_4^M \\ v_1^M & v_2^M & v_3^M & v_4^M \end{array} \right].$$

Lemma 2 *Every* 3×3 *submatrix of* T *is non-singular.*

Proof of the lemma. We show that 3×3 matrices are non-singular via contradiction: Suppose, on the contrary, that some 3×3 submatrix *is* singular, and without loss assume (that it is the 'first' 3×3 submatrix):

$$\begin{vmatrix} t_1^M & t_2^M & t_3^M \\ u_1^M & u_2^M & u_3^M \\ v_1^M & v_2^M & v_3^M \end{vmatrix} \;=\; 0.$$

Expanding out the determinant into a polynomial in its entries, we see that it produces a sum of Mth powers equal to 0. Furthermore, since all the t_i, u_j, v_k are monic, none is a scalar multiple of another, except for factors ± 1. Since no non-trivial sum of 24 or fewer Mth powers of polynomials can equal 0, it follows that each must be matched with its negative, in order for this sum of Mth powers to equal 0.

Note, then, that there are $6 = 3!$ possible matchings that can produce a 0 sum. Consider now the matching (assuming we have taken Mth roots)

$$\begin{aligned} t_1u_2v_3 &= t_3u_2v_1 \\ t_2u_3v_1 &= t_2u_1v_3 \\ t_3u_1v_2 &= t_1u_3v_2. \end{aligned}$$

This matching implies

$$t_3/t_1 \;=\; u_3/u_1 \;=\; v_3/v_1. \tag{6}$$

Some of the other possible matchings will lead to equations such as $t_1/t_2 = u_1/u_2$, which we have said was impossible by design; but, there is one other viable chain of equations that we get, using one of these matchings, and that is

$$t_3/t_2 \;=\; u_3/u_2 \;=\; v_3/v_2.$$

In what follows, whether this chain holds, or (6) holds makes little difference, so we will assume without loss of generality that (6) holds, and will let $r = t_3/t_1$ denote the common ratio, which we note is a rational function.

It is clear that assuming that this matching holds, we can reduce the equations

$$\begin{aligned} at_1^M + bt_2^M - ct_3^M - dt_4^M &= 0 \\ au_1^M + bu_2^M - cu_3^M - du_4^M &= 0 \\ av_1^M + bv_2^M - cv_3^M - dv_4^M &= 0 \end{aligned}$$

to

$$\begin{bmatrix} t_1^M & t_2^M & t_4^M \\ u_1^M & u_2^M & u_4^M \\ v_1^M & v_2^M & v_4^M \end{bmatrix} \begin{bmatrix} a - cr^M \\ b \\ -d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Since all the elements of S are monic, none can be 0, and so this column vector is not the 0 vector. It follows that the 3×3 matrix here is singular (from the fact that one of the 3×3 submatrices of T is singular, we just got that another was singular). Upon expanding the determinant of this matrix into a polynomial of its entries, in order to get it to be 0 we must have a matching, much like the one that produced (6). As before, we will get two viable chains of equations: Either

$$t_4/t_1 \;=\; u_4/u_1 \;=\; v_4/v_1, \tag{7}$$

or

$$t_4/t_2 \;=\; u_4/u_2 \;=\; v_4/v_2. \tag{8}$$

Let us suppose that (7) holds, and let s be the common ratio, which is of course a rational function. Then, it follows that

$$\begin{bmatrix} t_1^M & t_2^M \\ u_1^M & u_2^M \end{bmatrix} \begin{bmatrix} a - cr^M - ds^M \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Since (t_1^M, t_2^M) and (u_1^M, u_2^M) are independent, this matrix is non-singular; so, the column vector here must be the 0 vector, which is impossible since $b \neq 0$.

So, (8) above must hold. Redefining s to be the common ratio t_4/t_2 here, it leads to the equation

$$\begin{bmatrix} t_1^M & t_2^M \\ u_1^M & u_2^M \end{bmatrix} \begin{bmatrix} a - cr^M \\ b - ds^M \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Since the matrix is non-singular, it follows that

$$a = cr^M \quad \text{and} \quad b = ds^M.$$

But this implies that

$$at_1^M \;=\; cr^M t_1^M \;=\; ct_3^M, \tag{9}$$

and

$$bt_2^M \;=\; ds^M t_2^M \;=\; dt_4^M, \tag{10}$$

So, (t_1, t_2, t_3, t_4) couldn't have been a quadruple of Q', because if so, then for some $(x_1, x_2, x_3, x_4) \in Q$ we would have had

$$t^M(x_1, x_2, x_3, x_4) \;=\; (at_1^M, bt_2^M, ct_3^M, dt_4^M),$$

and then the equations (9) and (10) imply that

$$(x_1, x_2) = (x_3, x_4),$$

a contradiction. This completes the proof of the lemma. ■

2.4 Continuation of the proof

In addition to the quadruples $(t_1, ..., t_4), (u_1, ..., u_4), (v_1, ..., v_4)$, let $(w_1, ..., w_4)$ be another quadruple (we will later show that we can choose it in such a way that we contradict the assumption $|S + S| = o(n^2)$). We have that

$$\Gamma \;:=\; \begin{bmatrix} t_1^M & t_2^M & t_3^M & t_4^M \\ u_1^M & u_2^M & u_3^M & u_4^M \\ v_1^M & v_2^M & v_3^M & v_4^M \\ w_1^M & w_2^M & w_3^M & w_4^M \end{bmatrix}$$

is singular, as the vector $(a, b, -c, -d)$ (written as a column vector) is in its kernel. Expanding out its determinant, we find that it must be 0; and, we know from Theorem 4 that this is impossible, except if we can match up terms, as we did in the proof of Lemma 2. Just so the reader is clear, an example of just one equation from such a matching is perhaps, say,

$$(t_1 u_2 v_3 w_4)^M \;=\; (t_2 u_1 v_3 w_4)^M.$$

In total, there will be $12 = 4!/2$ different equations that make up such a matching. Let us suppose that in a hypothetical matching we got an equation of the form

$$(t_i u_j v_k w_1)^M \;=\; (t_{i'} u_{j'} v_{k'} w_2)^M,$$

and for our purposes we just need to write this as

$$\alpha w_1^M \;=\; \beta w_2^M, \tag{11}$$

where $(\alpha, \beta) \in \mathbb{C}[x] \times \mathbb{C}[x]$ can be any of at most 6^2 polynomials (according to which combination of i, j, k, i', j', k' is chosen). So, we would have $w_2^M / w_1^M =$

α/β; that is, w_2/w_1 takes on at most 36 possible values. What this would mean is that the pair (w_1, w_2) is essentially determined by w_1, and that it can take on at most $36n$ possible values – far too few to consume the majority of the $\gg n^{2-4\varepsilon}$ pairs (w_1, w_2) making up the first part of a quadruple of Q'.

We conclude that all but $O(n)$ of the quadruples $(w_1, w_2, w_3, w_4) \in Q'$ cannot lead to a solution to (11) under any matching; moreover, all but $O(n)$ will also avoid

$$\alpha w_3^M \ = \ \beta w_4^M. \tag{12}$$

We also have that there are at most $O(n)$ quadruples can lead to solutions to

$$\alpha w_1^M \ = \ \beta w_3^M, \text{ and } \alpha' w_1^M \ = \ \beta' w_4^M, \tag{13}$$

because it would imply that w_4/w_3 is fixed, and we are back in the situation (12). Furthermore, there are at most $O(n)$ quadruples leading to solutions to any of the following pairs:

$$\alpha w_2^M \ = \ \beta w_3^M, \text{ and } \alpha' w_2^M \ = \ \beta' w_4^M, \tag{14}$$

or

$$\alpha w_3^M \ = \ \beta w_1^M, \text{ and } \alpha' w_3^M \ = \ \beta' w_2^M, \tag{15}$$

or

$$\alpha w_4^M \ = \ \beta w_1^M, \text{ and } \alpha' w_4^M \ = \ \beta' w_2^M. \tag{16}$$

We can also avoid a matching that produces three equations (indexed by j) of the form

$$\alpha_j w_i^M = \beta_j w_i^M, \ j = 1, 2, 3, \tag{17}$$

because it would mean that the 3×3 submatrix of T with the ith column deleted, is singular (these α_j, β_j have the property that the determinant of this submatrix is $\sum_{j=1}^{3}(\alpha_j - \beta_j)$).

Furthermore, we cannot even have a *pair* of equations of the type (17), for the same value i, because it would imply that in fact we get three equations upon taking a product of the two and doing some cancellation; for example, suppose that $i = 4$, and that we have two equations of (17) holding. Then, there is a matching between two pairs of terms, upon expanding the determinant of the following matrix in terms of its entries:

$$\begin{bmatrix} t_1^M & t_2^M & t_3^M \\ u_1^M & u_2^M & u_3^M \\ v_1^M & v_2^M & v_3^M \end{bmatrix}. \tag{18}$$

The matching corresponds, say, to $\alpha_1 = \beta_1$ and $\alpha_2 = \beta_2$; and, say, these correspond to the equations

$$\begin{aligned}(t_1 u_2 v_3)^M &= (t_3 u_2 v_1)^M \\ (t_2 u_3 v_1)^M &= (t_2 u_1 v_3)^M.\end{aligned}$$

Multiplying left and right sides together, and cancelling, produces

$$(t_1 u_3)^M \ = \ (t_3 u_1)^M;$$

and, multiplying both sides by v_2^M produces the missing matching

$$(t_1 u_3 v_2)^M \ = \ (t_3 u_1 v_2)^M,$$

which proves that the matrix (18) is singular. But this is impossible, since it contradicts Lemma 2. We conclude therefore that, as claimed, we cannot have even a pair of equations from (17) hold, for any $i = 1, ..., 4$.

We have eliminated a great many possible matchings that could occur in order that the matrix Γ be singular: Our 12 equations in a matching can include at most one of each of the four types

$$\alpha w_1^M = \beta w_1^M,\ \alpha' w_2^M = \beta' w_2^M,\ \alpha'' w_3^M = \beta'' w_3^M,\ \alpha''' w_4^M = \beta''' w_4^M,$$

and so must include at least 8 of the form

$$\alpha w_1^M = \beta w_3^M,\ \alpha' w_1^M = \beta' w_4^M, \alpha'' w_2^M = \beta'' w_3^M,\ \alpha''' w_2^M = \beta''' w_4^M, \qquad (19)$$

all the while avoiding pairs (13), (14), (15), and (16).

Let us consider what would happen if we had a pair

$$\alpha w_1^M = \beta w_3^M \ \text{ and } \ \alpha''' w_2^M = \beta''' w_4^M, \qquad (20)$$

or a pair

$$\alpha' w_1^M = \beta' w_4^M \ \text{ and } \ \alpha'' w_2^M = \beta'' w_3^M. \qquad (21)$$

Without loss of generality in what follows, we just assume that (20) holds. Then, we would have that the equation

$$a w_1^M + b w_2^M - c w_3^M - d w_4^M \ = \ 0$$

becomes

$$(a - c\alpha/\beta)w_1^M + (b - d\alpha'''/\beta''')w_2^M \ = \ 0.$$

Now, if we had any other quadruple $(z_1, z_2, z_3, z_4) \in Q'$ that also satisfied

$$\alpha z_1^M = \beta z_3^M \ \text{ and } \ \alpha''' z_2^M = \beta''' z_4^M,$$

we would likewise get

$$(a - c\alpha/\beta)z_1^M + (b - d\alpha'''/\beta''')z_2^M \ = \ 0,$$

and then we would get the equation

$$\begin{bmatrix} w_1^M & w_2^M \\ z_1^M & z_2^M \end{bmatrix} \begin{bmatrix} a - c\alpha/\beta \\ b - d\alpha'''/\beta''' \end{bmatrix} \ = \ \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

So, either we get

$$a = c\alpha/\beta, \ b = d\alpha'''/\beta''',$$

or else this matrix is singular. If the former holds, it implies that

$$(aw_1^M, bw_2^M) \ = \ (cw_3^M, dw_3^M),$$

which contradicts the hypotheses about the sets of quadruples Q and Q'.

So, the matrix must be singular; in other words,

$$(w_1, w_2) \ = \ \gamma(z_1, z_2), \ \gamma \in S/S.$$

But since by the Ruzsa-Plunnecke inequality $|S/S| < n^{1+\varepsilon}$, there can be at most $n^{1+\varepsilon}$ such vectors (z_1, z_2), given (w_1, w_2).

In particular, this means that there can be only very few quadruples $(w_1, w_2, w_3, w_4) \in Q'$ that satisfy (20) or (21), for any particular combination of $\alpha, \beta, \alpha'', \beta'', \alpha''', \beta'''$. Since there are at most 6^6 possibilities for all these, (they are products of entries from T), we deduce that there are $\gg n^{2-4\varepsilon} - O(n^{1+\varepsilon})$ quadruples of Q' that do not satisfy a pair of equations of the sort (20) or (21). So, we may safely assume that $(w_1, ..., w_4)$ does not satisfy these equations.

We may assume, then, that all 8 of our equations of the type (19) involve the same pair of w_i's, and do not involve w_1, w_2 or w_3, w_4. So, for example, our matching includes 8 equations of the form

$$\alpha_j w_1^M = \beta_j w_3^M, \ j = 1, ..., 8$$

(or 8 analogous equations for w_1, w_4 or w_2, w_3 or w_2, w_4). But, thinking about where such equations come from (from a matching on the matrix Γ), there simply *cannot be* 8 equations: α_j is any of the 6 terms (times possibly -1) making up the determinant of the submatrix of Γ gotten by deleting the last row and the first column (or just the first column of T), while the β_j corresponds to possible terms in the determinant of the submatrix gotten by deleting the last row and third column of Γ. So, each of the six terms in the first determinant, matched with a unique term of the second, produces only 6 equations, not 8.

We have now exhausted all of the possibilities, reached a contradiction in each case, and so shown that Γ must be non-singular for some choice of $(w_1, w_2, w_3, w_4) \in Q'$. This then means that we couldn't have had so many quadruples in Q', and therefore Q. Therefore, $|S+S| \gg n^2$, and we are done.

3 Proof of Theorem 3

Let us suppose that $\varepsilon > 0$ is some constant that we will allow to depend on c, k, and a certain parameter t mentioned below, but is not allowed to depend on ℓ. This $\varepsilon > 0$ will later be chosen small enough to make our proofs work. Also, we suppose that

$$|S^\ell| \ = \ |S.S...S| \ \leq \ n^c, \tag{22}$$

where $\ell \geq 1$ is as large as we might happen to require, as a function of c and k (and implicitly, ε). [1]

If (22) holds, it follows that

$$n = |S| \leq |S.S| \leq \cdots \leq |S^\ell| < n^c.$$

Letting $M \geq 1$ be some integer depending on c and k that we choose later, we have that for ℓ large enough, it is obvious that for some $t < \ell/M$, [2]

$$|S^t|^{1+\varepsilon} \ \geq \ |S^{Mt+1}|.$$

[1] The reason we may choose ℓ as large as needed, in terms of c and k, is that we have freedom to choose $f(c,k,\ell)$ any way we please, so long as for fixed c, k we have $f(c,k,\ell) \to 0$ as $\ell \to \infty$.

[2] In other words, there must be a long interval $[t, Mt+1]$ such that for j in this interval S^j is not much smaller than S^{Mt+1}.

Furthermore, if we let

$$S_M \;:=\; \{s^M \;:\; s \in S\},$$

then since

$$S_M^t S = \{(s_1 \cdots s_t)^M s' \;:\; s_1, ..., s_t, s' \in S\} \;\subseteq\; S^{Mt+1},$$

it follows that

$$|S^t| \;=\; |S_M^t| \;\leq\; |S_M^t S| \;\leq\; |S^{Mt+1}| \;\leq\; |S^t|^{1+\varepsilon} \;=\; |S_M^t|^{1+\varepsilon}. \qquad (23)$$

In other words, $S_M^t S$ is not appreciably larger than S_M^t.

Let us now define

$$R \;:=\; S_M^t \;=\; \{(s_1 \cdots s_t)^M \;:\; s_i \in S\},$$

so that (23) becomes

$$|RS| \;\leq\; |R|^{1+\varepsilon}. \qquad (24)$$

We now arrive at the following useful lemma.

Lemma 3 *Suppose that (24) holds. Then, there exists*

$$s \in S, \text{ and } r' \in R,$$

such that for at least $n^{1-O(t\varepsilon)}$ values $s' \in S$ we have that there exists $r \in R$ satisfying

$$rs \;=\; r's'.$$

Note. Since we can choose ε as small as desired in terms of t, we have that $n^{1-O(t\varepsilon)}$ is basically $n^{1-\delta}$, where $\delta > 0$ is as small as we might happen to require later on in the argument (δ is allowed to depend on c and k, but not on ℓ).

Proof of the lemma. Inequality (24) easily implies that

$$|\{(s, s', r, r') \in S^2 \times R^2 \;:\; rs = r's'\}| \;\geq\; |R|^{1-\varepsilon} n^2.$$

So, extracting the pair s, r' producing the maximal number of pairs s', r satisfying $rs = r's'$, we find that this pair leads to at least

$$n|R|^{-\varepsilon} \;\geq\; n|S^t|^{-O(\varepsilon)} \;\geq\; n^{1-O(t\varepsilon)}$$

such pairs $(s', r) \in S \times R$.

$\blacksquare$

Let S' denote the set of s' produced by this lemma, for the fixed pair (r', s). We will show that

$$|kS'| \ \geq \ n^{k-O(\delta)}, \tag{25}$$

from which it will follow that

$$|kS| \ \geq \ |kS'| \ \geq \ n^{k-O(\delta)},$$

thereby establishing Theorem 3, since the larger we may take $\ell \geq 1$, the smaller we may take $\delta > 0$ (so, our $f(c, k, \ell) = O(\delta) \to 0$ for fixed c, k as $\ell \to \infty$).

To prove (25), it suffices to show that the only solutions to

$$x_1 + \cdots + x_k \ = \ x_{k+1} + \cdots + x_{2k}, \ x_i \in S', \tag{26}$$

are trivial ones: Suppose that, on the contrary, this equation has a non-trivial solution. Then, upon multiplying through by r', we are led to the equation

$$sr_1 + \cdots + sr_k \ = \ sr_{k+1} + \cdots + sr_{2k}, \text{ where } r_i \in R.$$

Cancelling the s's, and writing $r_i = y_i^M$, $y_i \in S^t$, produces the equation

$$y_1^M + \cdots + y_k^M \ = \ y_{k+1}^M + \cdots + y_{2k}^M. \tag{27}$$

In order to be able to apply Theorem 4 to this to reach a contradiction, we need to show that this equation is non-trivial, given that we have a non-trivial solution to (26). First observe that

$$x_i = \lambda x_j \iff r'x_i = \lambda(r'x_j) \iff sr_i = \lambda sr_j \iff r_i = \lambda r_j,$$

which means that certain of the y_i^M's are scalar multiples of one another if and only if the corresponding x_i's are scalar multiples of one another, and in fact with the same scalars λ.

After cancelling common terms from both sides of (27), we move the remaining terms from among $y_{k+1}^M + \cdots + y_{2k}^M$ to the left-hand-side, writing

$$-y_{k+j}^M \ = \ (e^{\pi i/M} y_{k+j})^M.$$

We also must collect together duplicates into a single polynomial: Say, for example, $y_1 = \cdots = y_j$. Then, we collapse the sum $y_1^M + \cdots + y_j^M$ to $(j^{1/M} y_1)^M$.

For M large enough in terms of k, Theorem 4 tells us that our collapsed equation can have no non-trivial solutions, and therefore neither can (27). Theorem 3 is now proved.

4 Proof of Theorem 4

The proof of this theorem will make use of the ideas that go into the proof of the so-called ABC-theorem, which is also known as Mason's Theorem [12] (see also [11] for a very nice introduction). Although there are versions of Mason's theorem already worked out for some quite general contexts, in our useage of the ideas that go into the proof of this theorem, we will need to allow some of the polynomials to have common factors. Our proof is similar in many respects to the one appearing in [1] and [2] – the only difference is that we consider polynomials where none is a scalar multiple of another, and impose no coprimeness condition.

4.1 The basic ABC theorem

Before we embark on this task, let us recall the most basic ABC theorem, and see its proof.

Theorem 6 *Suppose that $A(x), B(x), C(x) \in \mathbb{C}[x]$ are coprime polynomials, not all constant, such that*

$$A(x) + B(x) \ = \ C(x).$$

(Note that if any two share a common polynomial factor, then so must all three.) Then, if we let k denote the number of distinct roots of $A(x)B(x)C(x)$, we have that

$$\max(\deg(A), \deg(B), \deg C) \ \leq \ k - 1.$$

Remark 1. This theorem easily implies that the "Fermat" equation

$$f(x)^n + g(x)^n \ = \ h(x)^n$$

has no solutions for $n \geq 3$, except trivial ones: Suppose that at most one of f, g, h is constant, and that this equation does, in fact, have solutions. Letting f be the polynomial of maximal degree, we find that

$$n\deg(f) \ = \ \deg(f^n) \ \leq \ k-1 \ \leq \ \deg(fgh)-1 \ \leq \ 3\deg(f)-1.$$

So, $n \leq 2$ and we are done.

Proof. The proof of the theorem makes use a remarkably simple, yet powerful "determinant trick". First, consider the determinant

$$\Delta \ := \ \left| \begin{array}{cc} A(x) & B(x) \\ A'(x) & B'(x) \end{array} \right|. \tag{28}$$

Note that this matrix is a Wronskian.

Let us see that $\Delta \neq 0$: If $\Delta = 0$, we would have that

$$A(x)B'(x) \ = \ B(x)A'(x).$$

Since $A(x)$ and $B(x)$ are coprime, we must have that

$$A(x) \mid A'(x), \text{ and } B(x) \mid B'(x).$$

Both of these are impossible, unless of course both $A(x)$ and $B(x)$ are constants. If both are constants, then so is $C(x)$, and we contradict the hypotheses of the theorem. So, we are forced to have $\Delta \neq 0$.

Now suppose that

$$A(x)B(x)C(x) \ = \ c\prod_{i=1}^{k}(x-\alpha_i)^{a_i},$$

so that A, B, C have only the roots $\alpha_1, ..., \alpha_k$, with multiplicities $a_1, ..., a_k$, respectively. We will now see that

$$R(x) \ := \ \prod_{i=1}^{k}(x-\alpha_i)^{a_i-1}$$

divides Δ. To see this, note that for each $i = 1, ..., k$, $(x-\alpha_i)^{a_i}$ divides either $A(x), B(x)$, or $C(x)$, since all three are coprime. Note also that adding the first column of the matrix in (28) to the second does not change the determinant, so that

$$\Delta \;=\; \begin{vmatrix} A(x) & C(x) \\ A'(x) & C'(x) \end{vmatrix}. \tag{29}$$

(Note that here we have used the fact that differentiation is a linear map from the space of polynomials to itself.) Now using the fact that

$$(x-\alpha_i)^{a_i} \mid f(x) \;\;\Longrightarrow\;\; (x-\alpha_i)^{a_i-1} \mid f'(x),$$

it follows that $(x-\alpha_i)^{a_i-1}$ divides all the elements of some column of either the matrix (28), or (29). It follows that

$$(x-\alpha_i)^{a_i-1} \mid \Delta, \text{ and therefore } R(x)|\Delta.$$

So,

$$\deg(\Delta) \;\geq\; \deg(R(x)) \;=\; \deg(ABC)-k.$$

But we also have a simple upper bound on the degree of Δ,

$$\begin{aligned} \deg(\Delta) \;&\leq\; \min(\deg(AB)-1, \deg(AC)-1, \deg(BC)-1) \\ &=\; \deg(ABC)-1-\max(\deg(A), \deg(B), \deg(C)). \end{aligned}$$

Collecting together the above inequalities clearly proves the theorem. ■

4.2 Two lemmas about polynomials

We will require the following basic fact about Wronskians, which we will not bother to prove.

Lemma 4 *Suppose that $f_1, ..., f_\ell \in \mathbb{C}[x]$, or even $\mathbb{F}_p[x]$, are non-zero polynomials and that*

$$\begin{vmatrix} f_1 & f_2 & \cdots & f_\ell \\ f_1' & f_2' & \cdots & f_\ell' \\ f_1'' & f_2'' & \cdots & f_\ell'' \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(\ell-1)} & f_2^{(\ell-1)} & \cdots & f_\ell^{(\ell-1)} \end{vmatrix} \;=\; 0.$$

Then, we have that there are polynomials

$$\alpha_1, ..., \alpha_\ell,$$

not all 0*, such that*

$$\alpha_1 f_1 + \cdots + \alpha_\ell f_\ell \;=\; 0, \tag{30}$$

where

$$\alpha_1' \;=\; \cdots \;=\; \alpha_\ell' \;=\; 0. \tag{31}$$

Note that this last condition is equivalent to saying that α_i *are constants in the* $\mathbb{C}[x]$ *settting, and pth powers of some polynomials in the* $\mathbb{F}_p[x]$ *setting.*

We will also require the following lemma.

Lemma 5 *For* $k \geq 2$ *and* $\varepsilon > 0$ *there exists* $M \geq 1$ *such that the following holds: Suppose that*

$$f_1, ..., f_{k-1} \;\in\; \mathbb{C}[x]$$

are linearly independent over $\mathbb{C}$*. Then, the equation*

$$f_1^M + \cdots + f_{k-1}^M + G^M f_k \;=\; 0$$

has no solutions with G *satisfying the following two conditions:*

- $\deg(G) \;\geq\; \varepsilon D$*, where*

$$D \;:=\; \max(\deg(f_1), ..., \deg(f_{k-1}), \deg(G^M f_k)/M);$$

- $\deg(\gcd(G, f_j)) < \varepsilon D/2k$*, for all* $j = 1, ..., k-1$*.*

Proof of the lemma. Suppose, in fact, that there are such solutions, where we will later choose M purely as a function of ε and k, in order to reach a contradiction.

Then, consider the determinant

$$\Delta \;:=\; \left| \begin{array}{ccc} f_1^M & \cdots & f_{k-1}^M \\ (f_1^M)' & \cdots & (f_{k-1}^M)' \\ \vdots & \ddots & \vdots \\ (f_1^M)^{(k-2)} & \cdots & (f_{k-1}^M)^{(k-2)} \end{array} \right|.$$

The hypotheses of the lemma, along with Lemma 4, imply that $\Delta \neq 0$.

It is easy to see, upon using your favorite expansion for the determinant, that

$$\deg(\Delta) \;\leq\; M \deg(f_1 \cdots f_{k-1}) - k + 2.$$

On the other hand, the jth column of the matrix is divisible by f_j^{M-k+2}, so that

$$(f_1 \cdots f_{k-1})^{M-k+2} \mid \Delta.$$

And, upon adding the first $k-2$ columns to the last column, we see that Δ is also divisible by G^{M-k+2}. So,

$$(f_1 \cdots f_{k-1})^{M-k+2} \frac{G^{M-k+2}}{\gcd(G^{M-k+2}, f_1^M \cdots f_{k-1}^M)} \mid \Delta.$$

Using again the hypotheses of the lemma, we can easily bound the degree of this gcd from above by

$$M \sum_{j=1}^{k-2} \varepsilon D/2k \ < \ \varepsilon MD/2.$$

So,

$$\deg(\Delta) \ \geq \ (M-k+2)\deg(f_1 \cdots f_{k-1} G) - \varepsilon MD/2.$$

Combining our upper and lower bounds on $\deg(\Delta)$, we deduce

$$\deg(G) \ \leq \ \frac{k-2}{M-k+2}(\deg(f_1 \cdots f_{k-1}) - 1) + \frac{\varepsilon MD}{2(M-k+2)}.$$

This is impossible for M large enough in terms of ε and k, since

$$\deg(G) \ > \ \varepsilon D,$$

and our lemma is therefore proved.

4.3 An iterative argument

To apply the above lemmas, we begin by letting $\varepsilon = 1$, and suppose that

$$f_1^M + \cdots + f_k^M \ = \ 0 \tag{32}$$

has a non-trivial solution (none is a scalar multiple of another), where M can be taken as large as we might happen to need. And, assume that we have pulled out common factors among all the f_i.

We furthermore assume that any subset of size $k-1$ of the polynomials $f_1^M, ..., f_k^M$, is linearly independent over $\mathbb{C}$, since otherwise we have a solution to (32), but with a smaller value of k (we could pull the coefficients in the linear combination into the Mth powers, as every element of $\mathbb{C}$ has an Mth root in $\mathbb{C}$).

Without loss of generality, assume that f_k has the highest degree among $f_1, ..., f_k$, and let D denote its degree.

Now suppose that

$$\deg(\gcd(f_k, f_j)) \ > \ \varepsilon D/2k, \text{ for some } j = 1, ..., k-1. \tag{33}$$

Without loss of generality, assume that $j = k-1$. Then, we may write

$$f_k^M + f_{k-1}^M \ = \ G_1^M g_k, \text{ where } \deg(G_1) > \varepsilon D/2k,$$

so that

$$f_1^M + \cdots + f_{k-2}^M + G_1^M g_k \ = \ 0.$$

Note that this last term is non-zero by the assumption that no $k-1$ of the polynomials f_i^M can be linearly dependent over $\mathbb{C}$.

Then, we set

$$\varepsilon_1 \ = \ \varepsilon/2k,$$

and observe that

$$\deg(G_1) \ > \ \varepsilon_1 D.$$

On the other hand, if (33) does not hold, then we proceed on to the next subsection.

Now suppose that

$$\deg(\gcd(f_i, G_1)) \ > \ \varepsilon_1 D/2(k-1), \text{ for some } i = 1, ..., k-2, \tag{34}$$

where here we redefine D to

$$D \ = \ \max(\deg(f_1), ..., \deg(f_{k-2}), \deg(G_1^M g_k)/M).$$

(Note that we still have $\deg(G_1) > \varepsilon_1 D$). Without loss of generality, assume $i = k-2$. Then, we may write

$$f_k^M + f_{k-1}^M + f_{k-2}^M \ = \ G_2^M g_{k-2}, \text{ where } \deg(G_2) > \varepsilon_1 D/2(k-1),$$

so that

$$f_1^M + \cdots + f_{k-3}^M + G_2^M g_{k-2} \ = \ 0.$$

Of course, we also have to worry about whether this final term is 0, but that is not a problem as it would imply that $k-1$ of the polynomials f_i^M are dependent over $\mathbb{C}$.

On the other hand, if (34) does not hold, then we proceed on to the next subsection.

We repeat this process, producing $\varepsilon_2, \varepsilon_3, ...,$ and $G_3, G_4, ...$ We cannot continue to the point where our equation is

$$f_1^M + G_{k-2}^M g_2 \ = \ 0,$$

with G_{k-2} non-constant, because then we would have that f_1 has a common factor with G_{k-2}, and therefore all of $f_1, ..., f_k$ would have to have a common factor. So, the process must terminate before reaching G_{k-2}.

4.4 Conclusion of the proof of Theorem 4

When we come out of the iterations in the previous section, we will be left with an equation of the form

$$f_1^M + \cdots + f_J^M + G_{k-J-1}^M g_{J-1} \ = \ 0,$$

where

$$\deg(G_{k-J-1}) \ > \ \gamma(k) D,$$

where

$$D \ = \ \max(\deg(f_1), ..., \deg(f_J), \deg(G_{k-J-1}^M g_{J-1})/M)),$$

and where $\gamma(k)$ is a function depending only on k. Applying now Lemma 5 to this, we find that this is impossible once M is large enough. So, our theorem is proved.

5 Acknowledgment

We would like to thank Jozsef Solymosi for his suggestion to include Theorem 2. We would also like to thank Ákos Pintér for pointing out to us his paper [14].

References

[1] M. Bayat and H. Teimoori, *A generalization of Mason's theorem for four polynomials*, Elem. der Mathematik **59** (2004), 23-28.

[2] M. Bayat and H. Teimoori, *A new bound for an extension of Mason's theorem for functions of several variables*, Arch. Math **82** (2004), 230-239.

[3] J. Bourgain and M.-C. Chang, *On the size of k-fold sum and product sets of integers*, J. Amer. Math. Soc. **17** (2004), 473-497.

[4] J. Bourgain, A. Glibichuk, and S. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, J. London Math. Soc. **73** (2006), 380-398.

[5] J. Bourgain, N. Katz, and T. Tao *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), 27-57.

[6] M.-C. Chang, *Erdős-Szemerédi problem on sum set and product set*, Ann. of Math. **157** (2003), 939-957.

[7] ———, *Sum and product of different sets*, Cont. to Disc. Math. **1** (2006), 47-56.

[8] G. Elekes, *On the number of sums and products*, Acta. Arith. **81** (1997), 365-367.

[9] P. Erdős and E. Szemerédi, *On sums and products of integers*, Studies in Pure Mathematics; To the memory of Paul Turán. P. Erdos, L. Alpar, and G. Halasz, editors. Akademiai Kiado-Birkhauser Verlag, Budapest-Basel-Boston, Mass. 1983, 213-218.

[10] K. Ford, *Sums and products from a finite set of real numbers*, Ramanujan Jour. **2** (1998), 59-66.

[11] A. Granville and T. Tucker, *It's as easy as ABC*, Notices of the AMS **49** (2002), 1224-1231.

[12] R. C. Mason, *Diophantine equations over function fields*, Cambridge, England: Cambridge University Press, 1984.

[13] M. Nathanson, *On sums and products of integers*, Proc. Amer. Math. Soc. **125** (1997), 9-16.

[14] Á. Pintér, *Exponential diophantine equations over function fields*, Publ. Math. Debrecen **41** (1992), 89-98.

[15] H. Plünnecke, *Eine Zahlentheoretische Anwendung der Graphtheorie*, J. Reine Angew. Math **243** (1970), 171-183.

[16] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Scientia, Ser. A **3** (1989), 97-109.

[17] J. Solymosi, *On sums-sets and product-sets of complex numbers*, J. Th. Nomb. Bordeaux **17** (2005), 921-924.

[18] ———-, *Bounding multiplicative energy by the sumset*, Advances in Math. **222** (2009), 402-408.

[19] T. Tao, *The sum-product phenomenon in arbitrary rings*, Cont. to Disc. Math. **4** (2009), 59-82.

[20] J. F. Voloch, *Diagonal equations over function fields*, Bol. Soc. Bras. Mat. **16** (1985), 29-39.