On the Thue-Vinogradov Lemma

Jozsef Solymosi

University of British Columbia, Vancouver
email: solymosi@math.ubc.ca

September 29, 2020

Abstract

We prove an extension of the Thue-Vinogradov Lemma. This paper is another example for the application of the polynomial method; Rényi polynomials and Stepanov's technique.

1 Introduction

In the introduction we state two classical results from elementary number theory, two lemmas from Thue and Vinogradov. In the second part of the paper we extend their results and illustrate the use of the new method by an application.

The lemmas of Thue and Vinogradov are clever applications of Dirichlet's box principle (also called as the pigeonhole principle). Our first result will go beyond that, it works with smaller sets. The technique we are using here is a variant of the so called polynomial method in additive combinatorics. We are going to use Rédei polynomials [8], and the last step in the proof of Theorem 4 (and in its later variants) is based on Stepanov's method [11]; if a degree d polynomial is vanishing on a set of size n with multiplicity at least m then $n \leq d/m$. The same method will be used in the last section, where we prove an inequality in additive combinatorics.

1.1 The lemmas of Thue and Vinogradov

Thue's Lemma is a useful tool in elementary number theory. The most famous application of the lemma is to prove Fermat's theorem on sums of two squares. There is a nice description of Thue's argument in the book *"Proof from THE BOOK"* [1]. The lemma is used in finding solutions of Diophantine equations involving quadratic forms. There are various examples for such theorems and exercises in Nagell's Introduction to Number Theory [6], and in Vinogradov's Elements of Number Theory [15].

Lemma 1 (Thue's Lemma) *[12] Let p be a prime. For any $a \in \mathbb{N}$, $p \nmid a$, there are x, y*

$$x, y \in \{1, 2, \ldots, \lceil \sqrt{p} \rceil\}$$

such that

$$ax \equiv \pm y \pmod{p}.$$

Thue's Lemma was extended by Vinogradov to an asymmetric form. He used it in the paper *"On a general theorem concerning the distribution of the residues and non-residues of powers"* [14, Lemma 1], where he gave an elementary proof of the Pólya-Vinogradov inequality. His extension, the following lemma, can be also used to find solutions for some quadratic forms, more efficiently than Thue's Lemma.

Lemma 2 (Vinogradov's Lemma) *Let p be a prime. For any $a \in \mathbb{N}$, $p \nmid a$, and $\alpha \in \mathbb{F}_p^*$, there are x, y*

$$x \in \{1, 2, \ldots, \alpha\}, \quad y \in \left\{1, 2, \ldots, \left\lfloor \frac{p}{\alpha} \right\rfloor \right\}$$

such that

$$ax \equiv \pm y \pmod{p},$$

or equivalently

$$a \equiv \pm \frac{y}{x} \pmod{p}.$$

Vinogradov's result was generalized to multiple congruences by Brauer and Reynolds in [3] where they provide a complete historic review of re-discoveries and generalizations of the Thue-Vinogradov lemma, up to 1951. In the same paper they proved the following result [3, Theorem 4].

Theorem 3 *Let g and k be positive integers where k is even, p an odd prime with $p \equiv 1 \pmod{k}$ such that $g \le p$. We set $h = \lceil p/g \rceil$. If D is a k-th power residue, then at least one of the numbers $1^k, 2^k, \ldots, h^k$ is congruent to one of the numbers $D, 2^k D, \ldots, (g-1)^k D$.*

Theorem 3 was also proved, independently, by Porcelly and Pall using Farey sequences in [7]. We are going to prove an improvement on this theorem in Section 3.

2 The Extension

The Thue-Vinogradov lemma is about initial segments providing solutions to $ax \equiv \pm y \pmod{p}$ for all a. What can we say about shorter segments? We are going to use the polynomial method – in this case the Rédei polynomial – to prove that initial segments of $\mathbb{F}_p$ give many solutions to the above congruence. Rédei polynomials were used in number theory, group theory, and in the geometry of finite fields. There is a nice survey on basic theorems and examples to such applications of the Rédei polynomial (and other algebraic methods in combinatorics) in [2].

Theorem 4 *Let p be a prime. For any $\alpha, \beta \in \mathbb{N}$, $\alpha(\beta + 1) \le p - 1$, there are at least $\alpha(\beta + 1)$ distinct $a \in \mathbb{F}_p^*$ for which there are x, y*

$$x \in I_\alpha = \{1, 2, \ldots, \alpha\}, \quad y \in I_\beta = \{1, 2, \ldots, \beta\}$$

such that

$$ax \equiv \pm y \pmod{p}. \tag{1}$$

In Vinogradov's Lemma if $\alpha(\beta + 1) > p$, then the conclusion of the theorem holds for every $a \in \mathbb{F}_p^*$, even with $y \in \{1, 2, \ldots, \beta - 1\}$, so there are infinitely many cases when Vinogradov's Lemma gives a better bound (by one) if one needs to capture every $a \in \mathbb{F}_p^*$. The importance of Theorem 4 is that it covers the range when $\alpha\beta < p$, when simple pigeonhole arguments won't work.

Proof. Denote $D \subset \mathbb{F}_p^*$ the set of elements a which are not expressible as in (1). The key of the argument is the construction of a polynomial following Rédei [8] and Szőnyi [9]. Their method was specialized to Cartesian products in [4], in a way that we are going to follow here. The polynomial is defined as

$$H(x,y) = \prod_{i=0}^{\beta} (x-i) \prod_{\substack{1 \le k \le \alpha \\ 0 \le j \le \beta}} (x+ky-j) = \prod_{\substack{0 \le k \le \alpha \\ 0 \le j \le \beta}} (x+ky-j)$$

The important feature of the polynomial above is that whenever $b \in D$, all roots of $H(x,b)$ are distinct elements of $\mathbb{F}_p$, i.e. $H(x,b)$ divides $x^p - x$. To see that, let us consider the two possible cases of repeated roots below

1. If the second product term (with y-s) had two equal roots then we had

$$-kb + j \equiv -k'b + j' \pmod{p},$$

   for some $1 \le k, k' \le \alpha$ and $0 \le j, j' \le \beta$. If $k = k'$ then $j = j'$, but then the two linear terms are the same which is not possible. Note that $b \ne 0$ so

$$|k - k'|b \equiv \pm(j' - j) \pmod{p},$$

   contradicting to the assumption $b \in D$.

2. The remaining case is when

$$-kb + j \equiv j' \pmod{p},$$

   for some $1 \le k \le \alpha$ and $0 \le j, j' \le \beta$, leading to

$$kb \equiv \pm(j' - j) \pmod{p},$$

   contradicting to the assumption $b \in D$.

The degree of H is $\delta = \alpha\beta + \alpha + \beta + 1$. In particular, when $\alpha = \beta$ then the degree is $(\alpha+1)^2$. It was Szőnyi's observation in [9] (see also in [10]) that there is an auxiliary polynomial of degree $p - \delta$, denoted by $f(x,y)$, such that

$$F(x,b) = f(x,b)H(x,b) = x^p - x \quad if \quad b \in D. \tag{2}$$

For the details on how to find f, we refer to [9] and [4]. Let us consider $F(x,y)$ as a polynomial of x with coefficients $h_i(y) \in \mathbb{F}_p[y]$.

$$F(x,y) = f(x,y)H(x,y) = F_y(x) = x^p + h_1(y)x^{p-1} + h_2(y)x^{p-2} + \ldots + h_p(y)$$

where the degree of h_i is at most i. From (2) one can see that $h_i(y)$-s are zero for many y values, whenever $y \in D$. If $h_i(y) = 0$ for more than i distinct y values then $h_i(y) \equiv 0$. This is the crucial point of the application of Rédei's method. If one can show that $h_i \not\equiv 0$ for some i, then $|D| \le i$. When $|D|$ is small, one could use Rédei's theorem, which describes the structure of fully reducible lacunary polynomials (like in [9]), however we follow a simpler calculation which gives a better bound in this case. Let us check the polynomial $F(x,y)$ when $y = 0$.

$$F(x,0) = f(x,0) \left(\prod_{i=0}^{\beta} (x-i) \right)^{\alpha+1}$$

$$= x^p + c_1 x^{p-1} + c_2 x^{p-2} + \ldots + c_p. \tag{3}$$

3

We need to show that a polynomial with form like in (3) has a nonzero c_i coefficient for some, not too large i. Let c_i denote the nonzero coefficient with the smallest index i. Checking the derivatives based on the first and second rows, we see that $F'(x,0)$ will vanish with multiplicity at least α on at least $\beta+1$ places and it has degree $p-i-1$. This implies that $p-i-1 \geq \alpha(\beta+1)$ and then $|D| \leq i \leq p-1-\alpha(\beta+1)$ as needed. $\qquad\square$

Remark 5 *Theorem 4 was stated for initial segments, but the same proof works if one requires*

$$x \in \mu I_\alpha = \{\mu, 2\mu, \ldots, \alpha\mu\}, \quad y \in \nu I_\beta = \{\nu, 2\nu, \ldots, \beta\nu\}$$

for some $\nu, \mu \in \mathbb{N}$ values, where $p \nmid \nu\mu$.

Remark 6 *It was noted by the anonymous referee and other readers of an earlier version of this paper that Theorem 4 can be improved for shorter initial segments. For example if*

$$x, y \in I_\alpha = \{1, 2, \ldots, \alpha\},$$

and $2\alpha^2 < p$, then the number of distinct $a \in \mathbb{F}_p^*$, such that $a \equiv \pm x/y \pmod{p}$ is twice the number of (ordered) pairs $(u,v) \in \mathbb{N}^2$, where $(u,v) = 1$, and $u, v \leq \alpha$, which is asymptotically $\frac{12}{\pi^2}\alpha^2 \sim 1.21\alpha^2$ (See e.g. Exercise 21 b, Chapter II in [15]).

Let us denote the difference set of $A \subset \mathbb{F}_p$ by $\bar{A}$,

$$\bar{A} = A - A = \{a - b | a, b \in A\}.$$

Using the above notation we can state a more general theorem with slightly weaker bounds. It is practically the same as Theorem 1 in [4], we include it here for completeness.

Theorem 7 *Let p be a prime. For any $A, B \subset \mathbb{F}_p$, where $|A| = \alpha, |B| = \beta$, there are at least*

$$\min(p, (\alpha - 1)\beta + 1)$$

$a \in \mathbb{F}_p$ for which there are $x \in \bar{A} \setminus \{0\}, y \in \bar{B}$ such that $ax \equiv y \pmod{p}$.

Note that since $\bar{A}$ and $\bar{B}$ are symmetric about 0, we don't need the $\pm$ sign in the modular equation. The proof, which we are going to sketch below follows the proof of Theorem 4.

P r o o f. For $a = 0$ the trivial solution, $ax \equiv b - b \pmod{p}$, works with any $x \in \bar{A}, b \in B$. Let us denote $D \subset \mathbb{F}_p^*$ the set of elements a which are not expressible as $ax \equiv y \pmod{p}$. The Rédei polynomial is now defined as

$$H(x, y) = \prod_{\substack{1 \leq k \leq \alpha \\ 1 \leq j \leq \beta}} (x + a_k y - b_j). \tag{4}$$

Whenever $d \in D$, all roots of $H(x, d)$ are distinct elements of $\mathbb{F}_p$, i.e. $H(x, d)$ divides $x^p - x$. If we had $(x + a_k d - b_j) = (x + a_\ell d - b_s)$ then $(a_k - a_\ell)d \equiv b_j - b_s \pmod{p}$, contradicting the selection $d \in D$. The degree of H is $\delta = \alpha\beta$. There is an auxiliary polynomial of degree $p - \delta$, denoted by $f(x, y)$, such that

$$F(x, d) = f(x, d)H(x, d) = x^p - x \quad \text{if} \quad d \in D. \tag{5}$$

Let us consider $F(x, y)$ as a polynomial of x with coefficients $h_i(y) \in \mathbb{F}_p[y]$.

$$F(x, y) = f(x, y)H(x, y) = F_y(x) = x^p + h_1(y)x^{p-1} + h_2(y)x^{p-2} + \ldots + h_p(y)$$

where the degree of h_i is at most i. If we show that $h_i \not\equiv 0$ for some i, then $|B| \leq i$. The polynomial when $y = 0$ is

$$F(x, 0) = f(x, 0) \left(\prod_{i=1}^{\beta} (x - b_i) \right)^{\alpha} \tag{6}$$
$$= x^p + c_1 x^{p-1} + c_2 x^{p-2} + \ldots + c_p.$$

Let c_i denote the nonzero coefficient with the smallest index i. Checking the derivatives based on the first and second rows, we see that $F'(x, 0)$ will vanish with multiplicity at least $\alpha - 1$ on at least β places and it has degree $p - i - 1$. This implies that $p - i - 1 \geq (\alpha - 1)\beta$ and then $|D| \leq i \leq p - 1 - (\alpha - 1)\beta$ as needed. $\square$

Let $d > 1$ be a divisor of $p - 1$ and let Z_d be a multiplicative subgroup of size d inside $GF(p)$. If there is an $A \subset \mathbb{F}_p$ such that $\bar{A} \subset \{Z_d \cup 0\}$ then by applying Theorem 7 with $A = B$ we obtain the following result, which was recently proved by Hanson and Petridis [5]. (See also Theorem 1. in [4])

Corollary 8 *Let $A \subset \mathbb{F}_p$ be a set such that $A - A \subset Z_d \cup \{0\}$. Then*

$$|A|(|A| - 1) \leq d.$$

A slightly stronger statement in Theorem 7 holds when $0 \notin A$.

Theorem 9 *Let $A \subset \mathbb{F}_p^*$, $B \subset \mathbb{F}_p$, where $|A| = \alpha, |B| = \beta$. There are at least*

$$\min(p, \alpha\beta + 1)$$

$a \in \mathbb{F}_p$ for which there are $x \in \{\{A \cup \bar{A}\} \setminus \{0\}\}$, and $y \in \bar{B}$ such that $ax \equiv y \pmod{p}$.

Indeed, in this case instead of polynomial (4) we can use

$$H(x, y) = \prod_{\ell=1}^{\beta} (x - b_j) \prod_{\substack{1 \leq k \leq \alpha \\ 1 \leq j \leq \beta}} (x + a_k y - b_j),$$

increasing the degree of $H(x, y)$ by β. The roots are still distinct for any $d \in D$, since $-b_\ell = a_i d - b_j$ would lead to the $ad \equiv y \pmod{p}$ equation where $x \in A$ and $y \in \bar{B}$. The polynomial when $y = 0$ now is

$$F(x, 0) = f(x, 0) \left(\prod_{i=1}^{\beta} (x - b_i) \right)^{\alpha+1}$$

with the $\alpha + 1$ exponent instead of α, leading to the improvement.

3 Congruent pairs

In this section we illustrate how to use Theorem 4 when we need many, almost p solutions in (1). The proof is similar to classical applications of the Thue-Vinogradov inequality. We are going to show a variant of Theorem 3 stated in the introduction.

Theorem 10 *Let g and k be positive integers where k is even, p an odd prime with $p \equiv 1 \pmod{k}$ such that $g \leq p$. Let $h \in \mathbb{N}$ be a number given by*

$$h = \left\lceil \frac{p - k - g}{g - 1} \right\rceil.$$

If D is a k-th power residue, then at least one of the numbers $1, 2^k, \ldots, h^k$ is congruent to one of the numbers $D, 2^k D, \ldots, (g-1)^k D$.

If $g \geq h$ then the above h is at most as as large as in Theorem 3 and h is smaller here by at least one whenever $g(k + g) \geq p$.

P r o o f. The equation $x^k \equiv D \pmod{p}$ has k solutions (see e.g. in [15], page 113). By Theorem 4 if

$$(g - 1)(h + 1) + 1 \geq p - k,$$

which is provided by the condition

$$h = \left\lceil \frac{p - k - g}{g - 1} \right\rceil,$$

then there is an $a \in \mathbb{F}_p$ such that $a^k \equiv D \pmod{p}$ and

$$ax \equiv \pm y \pmod{p}. \tag{7}$$

where x, y are

$$x \in \{1, 2, \ldots, g - 1\}, \quad y \in \{1, 2, \ldots, h\}.$$

The following equations

$$ax \equiv \pm y \pmod{p}$$
$$a^k x^k \equiv y^k \pmod{p}$$
$$Dx^k \equiv y^k \pmod{p}$$

show that there is at least one congruent pair between

$$\left\{D, 2^k D, \ldots, (g - 1)^k D\right\} \quad \text{and} \quad \left\{1, 2^k, \ldots, h^k\right\},$$

as required. □

4   Sumsets vs. Directions

In this section we are going to leave the Cartesian product structure and prove a result which generalizes Theorem 7 and other results. One of the most striking applications of Rédei's method is the bound on the number of directions determined by a set of points in the affine plane over the finite field $GF(q)$ of q elements. Given a set M of n points what is the minimum number of directions determined by M? We say that the direction m is determined by M if there is a line $mx + b - y = 0$ spanned by two points of M, i.e. there are points $(a_i, b_i), (a_j, b_j) \in M$ such that $m = (a_i - a_j)/(b_i - b_j)$ if $b_i \neq b_j$. If $b_i = b_j$ and $a_i \neq a_j$ then the two points determine the $m = \infty$ direction.

In Theorem 7 we proved a lower bound on the number of directions determined by a Cartesian product. It was better than Szőnyi's bound in [9, 10], due to the special structure of the pointset. In the next result we generalize Theorem 7.

Given an n-element subset $S \subset \mathbb{F}_p^2$, and an $\alpha \in \mathbb{F}_p^*$. Let us suppose that $n < p$. We define the weighted sumset

$$\Delta_\alpha = \{\alpha a_i + b_i \quad | \quad (a_i, b_i) \in S\},$$

and the ratio set

$$Q = \left\{ \frac{a_i - a_j}{b_i - b_j} \quad | \quad (a_i, b_i), (a_j, b_j) \in S, b_i \neq b_j \right\}.$$

The ratio set contains all directions determined by S with the possible exception of the (∞) direction.

Theorem 11 *With the above notation, if S is not collinear, i.e. there are no elements $m, \beta \in \mathbb{F}_p$ such that $ma_i + \beta - b_i \equiv 0 \pmod{p}$ for all $(a_i, b_i) \in S$, then $|Q| \geq |S| - |\Delta_\alpha| + 1$.*

P r o o f. We are going to use the Rédei polynomial as before. Set

$$H(x, y) = \prod_{(a_i, b_i) \in S} (x + a_i y - b_i), \tag{8}$$

and find $f(x, y)$ such that $f(x, y_0) H(x, y_0) = x^p - x$ whenever $y_0 \notin Q$. Let us check the polynomial when we set $y = -\alpha$.

$$F(x, \alpha) = f(x, \alpha) \prod_{(a_i, b_i) \in S} (x - \alpha a_i - b_i)$$
$$= x^p + c_1 x^{p-1} + c_2 x^{p-2} + \ldots + c_p. \tag{9}$$

Like in the proof of Theorem 4, we check the derivatives to show that there is a small index i where $c_i \neq 0$, so Q is large. A root $\alpha a_i + b_i$ is a multiple root if there is an $(a_j, b_j) \in S$, $i \neq j$, such that $\alpha a_i + b_i \equiv \alpha a_j + b_j \pmod{p}$. The derivative of the polynomial in (9) has at least $d = |S| - |\Delta_\alpha|$ roots, so $i - 1 \leq p - d$, unless $F(x, \alpha) = (x + c)^p$, when S is collinear. $\qquad \square$

Note that setting $\alpha = 0$ for a Cartesian product, S, gives back Theorem 7.

5 Acknowledgements

References

[1] M. Aigner and G. M. Ziegler, Proofs from THE BOOK, Chapter 4, Representing numbers as sums of two squares, Springer-Verlag Berlin Heidelberg (2018) 19–26.

[2] N. Alon, Tools from higher algebra, in: Handbook of combinatorics (vol. 2) (R.L. Graham, M. Grötschel, L. Lovász, eds.) Elsevier ; Cambridge (Mass.) : the MIT Press, 1995. Pages 1749–1783

[3] A. Brauer,R. Reynolds, On a Theorem of Aubry-Thue, Canadian Journal of Mathematics,(1951) 3, 367–374.

[4] D. Di Benedetto, J. Solymosi, E. White, On the directions determined by a Cartesian product in an affine Galois plane, arXiv:2001.06994 [math.CO]

[5] B. Hanson and G. Petridis, Refined estimates concerning sumsets contained in the roots of unity, Proceedings of the London Mathematical Society, doi.org/10.1112/plms.12322 (to appear) arXiv:1905.09134

[6] T. Nagell Introduction to Number Theory, AMS Chelsea Publishing, Volume: 163; (2001) 309 pp; Chapter 6, 188–226.

[7] P. Porcelli and G. Pall A property of Farey sequences, Can. J. Math., vol. 3 (1951) 52–53.

[8] L. Rédei, Lückenhafte Polynome über endlichen Körperrn, Birkhäuser, Basel, 1970 (Engl. trans. Lacunary Polynomials over Finite Fields, North Holland, Amsterdam, 1973).

[9] T. Szőnyi, On the Number of Directions Determined by a Set of Points in an Affine Galois Place, *J. Combin. Theory*, Ser. A **74** (1996), no. 1, 141–146.

[10] T. Szőnyi, Around Rédei's theorem, *Discrete Math.*, 208/209 (1999), 557–575.

[11] S. A. Stepanov, An elementary method in algebraic number theory, Mat. Zametki, 24:3 (1978), 425–431; Math. Notes, 24:3 (1978), 728–731.

[12] A. Thue, Et par antydninger ti1 en taltheoretisk metode, Kra. Vidensk. Selsk. Forh. 7 (1902), 57–75.

[13] I. M. Vinogradov, 1. Über eine asymptotische Formel aus der Theorie der binären quadratischen Formen. 2. Sur la distribution des rèsidus et des nonrésidus des puissances. 3. Über die Verteilung der quadratischen Reste und Nichtreste. (Russian. French summary) J. Soc. Phys. Math. Univ. Perm 1, 18–28 (1919)

[14] I.M. Vinogradov, On a general theorem concerning the distribution of the residues and non-residues of powers. Trans. Amer. Math. Soc. 29 (1927), 209–17.

[15] I.M. Vinogradov, Elements of number theory, Translated from the 5th rev. ed. by Saul Kravetz. New York, Dover Publications (1954) reprinted in 2016.

[16] A. Weil, On some exponential sums, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.