

# On the Thue–Vinogradov Lemma

Jozsef Solymosi<sup>a</sup>

Received August 1, 2020; revised September 27, 2020; accepted June 5, 2021

*On the 130th anniversary  
of Ivan Matveevich Vinogradov's birth*

**Abstract**—We prove an extension of the Thue–Vinogradov lemma. This paper is another example for the application of the polynomial method, Rédei polynomials, and Stepanov's technique.

**DOI:** 10.1134/S0081543821040179

## 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 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 [9]; 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.

**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 *Proofs 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, Ch. 6, pp. 188–226] and in Vinogradov's *Elements of Number Theory* [14].

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

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

*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" [13, Lemma 1], where he gave an elementary proof of the Pólya–Vinogradov inequality. His extension, the following lemma, can also be used to find solutions for some quadratic forms, more efficiently than Thue's lemma.

---

<sup>a</sup> University of British Columbia, 2329 West Mall, Vancouver, BC, V6T 1Z4, Canada.

E-mail address: solymosi@math.ubc.ca

**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  $x$  and  $y$ ,*

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

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

Theorem 3 was also proved, independently, by Porcelli 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 polynomials—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 of such applications of the Rédei polynomials (and other algebraic methods in combinatorics) in [2].

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

$$x \in I_\alpha = \{1, 2, \dots, \alpha\} \quad \text{and} \quad y \in I_\beta = \{1, 2, \dots, \beta\},$$

such that

$$ax \equiv \pm y \pmod{p}. \tag{2.1}$$

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  $y \in \{1, 2, \dots, \beta - 1\}$ , 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 do not work.

**Proof.** Denote by  $D \subset \mathbb{F}_p^*$  the set of elements  $a$  which are not expressible as in (2.1). The key of the argument is the construction of a polynomial following Rédei [8] and Szőnyi [10]. Their method was specialized to Cartesian products in [4], in a way that we are going to follow here. The polynomial is defined as

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

An 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 two possible cases of repeated roots below.

1. If the second product term (with  $y$ ) had two equal roots, then we would have

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

for some  $1 \leq k, k' \leq \alpha$  and  $0 \leq j, j' \leq \beta$ . If  $k = k'$  then  $j = j'$ , but then the two linear terms are the same, which is impossible. Note that  $b \neq 0$ , so

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

which contradicts the assumption  $b \in D$ .

2. The remaining case is when

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

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

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

which contradicts the assumption  $b \in D$ .

The degree of  $H$  is  $\delta = \alpha\beta + \alpha + \beta + 1$ . In particular, when  $\alpha = \beta$ , the degree is  $(\alpha + 1)^2$ . It was Szőnyi's observation in [10] (see also [11]) that there is an auxiliary polynomial of degree  $p - \delta$ , denoted by  $f(x, y)$ , such that

$$F(x, b) = f(x, b)H(x, b) = x^p - x \quad \text{if } b \in D. \tag{2.2}$$

For the details on how to find  $f$ , we refer to [10] and [4]. Let us consider  $F(x, y)$  as a polynomial in  $x$  with coefficients  $h_i(y) \in \mathbb{F}_p[y]$ :

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

where the degree of  $h_i$  is at most  $i$ . From (2.2) one can see that  $h_i(y)$  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  $|D| \leq i$ . When  $|D|$  is small, one could use Rédei's theorem, which describes the structure of fully reducible lacunary polynomials (like in [10]); however, we follow a simpler calculation which gives a better bound in this case. Let us check the polynomial  $F(x, y)$  when  $y = 0$ :

$$\begin{aligned} F(x, 0) &= f(x, 0) \left( \prod_{i=0}^{\beta} (x - i) \right)^{\alpha+1} \\ &= x^p + c_1x^{p-1} + c_2x^{p-2} + \dots + c_p. \end{aligned} \tag{2.3}$$

We need to show that a polynomial with form like in (2.3) 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  $\alpha$  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.  $\square$

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

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

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

**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

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

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  $(u, v) \in \mathbb{N}^2$  with  $(u, v) = 1$  and  $u, v \leq \alpha$ , which is asymptotically  $12\pi^{-2}\alpha^2 \sim 1.21\alpha^2$  (see, e.g., [14, Ch. II, Problem 21, b]).

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

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

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  $|A| = \alpha$  and  $|B| = \beta$ , there are at least*

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

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

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

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

$$H(x, y) = \prod_{\substack{1 \leq k \leq \alpha \\ 1 \leq j \leq \beta}} (x + a_k y - b_j). \tag{2.4}$$

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

$$F(x, d) = f(x, d)H(x, d) = x^p - x \quad \text{if } d \in D. \tag{2.5}$$

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

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

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 with  $y = 0$  is

$$\begin{aligned} F(x, 0) &= f(x, 0) \left( \prod_{i=1}^{\beta} (x - b_i) \right)^\alpha \\ &= x^p + c_1 x^{p-1} + c_2 x^{p-2} + \dots + c_p. \end{aligned} \tag{2.6}$$

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  $\beta$  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  $\text{GF}(p)$ . 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 [4, Theorem 1]).

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

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

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

**Proof.** Indeed, in this case instead of the polynomial (2.4) we can use

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

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

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

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

### 3. CONGRUENT PAIRS

In this section we illustrate how to use Theorem 4 when we need many, almost  $p$ , solutions in (2.1). 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, and let  $p$  be an odd prime with  $p \equiv 1 \pmod{k}$  such that  $g \leq p$ . Let  $h \in \mathbb{N}$  be a number given by*

$$h = \left\lceil \frac{p - k - g}{g - 1} \right\rceil. \tag{3.1}$$

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

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

**Proof.** The equation  $x^k \equiv D \pmod{p}$  has  $k$  solutions (see, e.g., [14, Ch. VI, §5]). By Theorem 4, if

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

which is provided by condition (3.1), then there is an  $a \in \mathbb{F}_p$  such that  $a^k \equiv D \pmod{p}$  and

$$ax \equiv \pm y \pmod{p} \quad \text{where} \quad x \in \{1, 2, \dots, g - 1\} \quad \text{and} \quad y \in \{1, 2, \dots, h\}.$$

The equations

$$\begin{aligned} ax &\equiv \pm y \pmod{p}, \\ a^k x^k &\equiv y^k \pmod{p}, \\ Dx^k &\equiv y^k \pmod{p} \end{aligned}$$

show that there is at least one congruent pair between

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

as required.  $\square$

#### 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  $\text{GF}(q)$  of  $q$  elements. Given a set  $M$  of  $n$  points, what is the minimum number of directions determined by  $M$ ? We say that a 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 [10, 11], due to the special structure of the point set. In the next result we generalize Theorem 7.

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

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

and the ratio set

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

The ratio set contains all directions determined by  $S$  with the possible exception of the  $\infty$  direction.

**Theorem 11.** *With the above notation, if  $S$  is not collinear, i.e., if 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  $|Q| \geq |S| - |\Delta_\alpha| + 1$ .*

**Proof.** We are going to use the Rédei polynomial as before. Set

$$H(x, y) = \prod_{(a_i, b_i) \in S} (x + a_i y - b_i) \tag{4.1}$$

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  $y = -\alpha$ :

$$F(x, -\alpha) = f(x, -\alpha) \prod_{(a_i, b_i) \in S} (x - \alpha a_i - b_i) = x^p + c_1 x^{p-1} + c_2 x^{p-2} + \dots + c_p. \tag{4.2}$$

As in the proof of Theorem 4, we check the derivatives to show that there is a small index  $i$  such that  $c_i \neq 0$ , 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 (4.2) 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.  $\square$

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

#### ACKNOWLEDGMENTS

I would like to thank the anonymous referee for the helpful report and in particular for the improvement mentioned in Remark 6. I am also thankful to Andrew Granville, Ilya Shkredov, and Ethan White for helpful discussions.

## FUNDING

The research was supported in part by an NSERC Discovery grant as well as by the OTKA K 119528 and NKFI KKP 133819 grants.

## REFERENCES

1. M. Aigner and G. M. Ziegler, “Representing numbers as sums of two squares,” in *Proofs from THE BOOK* (Springer, Berlin, 2018), Ch. 4, pp. 19–26.
2. N. Alon, “Tools from higher algebra,” in *Handbook of Combinatorics*, Ed. by R. L. Graham, M. Grötschel, and L. Lovász (Elsevier, Amsterdam, 1995), Vol. 2, pp. 1749–1783.
3. A. Brauer and R. Reynolds, “On a theorem of Aubry–Thue,” *Can. J. Math.* **3**, 367–374 (1951).
4. D. Di Benedetto, J. Solymosi, and 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,” *Proc. London Math. Soc.* **122** (3), 353–358 (2021); arXiv:1905.09134 [math.NT].
6. T. Nagell, *Introduction to Number Theory* (AMS Chelsea Publ., Providence, RI, 2001), AMS Chelsea Publ. Ser. **163**.
7. P. Porcelli and G. Pall, “A property of Farey sequences, with applications to  $q$ th power residues,” *Can. J. Math.* **3**, 52–53 (1951).
8. L. Rédei, *Lückenhafte Polynome über endlichen Körpern* (Birkhäuser, Basel, 1970). Engl. transl.: *Lacunary Polynomials over Finite Fields* (North Holland, Amsterdam, 1973).
9. S. A. Stepanov, “An elementary method in algebraic number theory,” *Math. Notes* **24** (3), 728–731 (1978) [transl. from *Mat. Zametki* **24** (3), 425–431 (1978)].
10. T. Szőnyi, “On the number of directions determined by a set of points in an affine Galois plane,” *J. Comb. Theory, Ser. A* **74** (1), 141–146 (1996).
11. T. Szőnyi, “Around Rédei’s theorem,” *Discrete Math.* **208–209**, 557–575 (1999).
12. A. Thue, “Et par antydninger til en taltheoretisk methode,” *Kra. Vidensk. Selsk. Forh.* **7**, 1–21 (1902); in *Selected Mathematical Papers of Axel Thue* (Universitetsforlaget, Oslo, 1977), pp. 57–75.
13. I. M. Vinogradov, “On a general theorem concerning the distribution of the residues and non-residues of powers,” *Trans. Am. Math. Soc.* **29**, 209–217 (1927).
14. I. M. Vinogradov, *Elements of Number Theory* (Gostekhizdat, Moscow, 1949; Dover Publ., New York, 1954).