ON KEMNITZ' CONJECTURE CONCERNING LATTICE POINTS IN THE PLANE

CHRISTIAN REIHER

ABSTRACT. In 1961, P. Erdős, A. Ginzburg, and A. Ziv proved a remarkable theorem stating that each set of $2n-1$ integers contains a subset of size n, the sum of whose elements is divisible by n. We will prove a similar result for pairs of integers, i.e., planar lattice points, usually referred to as Kemnitz' conjecture.

§1. INTRODUCTION

Denoting by $f(n,k)$ the minimal number f, such that any set of f lattice points in the k-dimensional Euclidean space contains a subset of cardinality n, the sum of whose elements is divisible by n, it was first proved by P. Erdős, A. Ginzburg, and A. Ziv [2], that $f(n,1) = 2n-1$.

The problem, however, to determine $f(n,2)$ turned out to be unexpectedly difficult: A. Kemnitz [3] conjectured it to equal $4n-3$ and knew, (1) that $4n-3$ is a rather straighforward lower bound*, (2) that the set of all integers n satisfying $f(n,2) = 4n-3$ is closed under multiplication and that it therefore suffices to prove this equation for prime values of n, and (3) that his assertion was correct for $n = 2, 3, 5, 7$ and, consequently, also for every n that is expressible as a product of these numbers.

Linear upper bounds estimating $f(p,2)$, where p denotes any prime number, appeared for the first time in an article by N. Alon and M. Dubiner [1] who proved $f(p,2) \leqslant 6p-5$ for all p and $f(p,2) \leqslant 5p-2$ for large p. Later this was improved to $f(p,2) \leqslant 4p-2$ by L. Rónyai [4].

In the third section of this article we prove Kemnitz' conjecture.

§2. PRELIMINARY RESULTS

Notational conventions. In the sequel the letter p is always assumed to designate an odd prime number and congruence modulo p is simply denoted by "$\equiv$". Roman capital letters (such as $J, X, \ldots$) will always stand for finite sets of lattice points in the Euclidean plane. The sum of the elements of such a set, taken coordinatewise, will be indicated by a

2010 *Mathematics Subject Classification.* 11B50.

Key words and phrases. zero-sum subsequences, Kemnitz' conjecture.

*In order to prove $f(n,2) > 4n-4$ one takes each of the four vertices of the unit square $n-1$ times.

preposed "$\sum$". Finally the symbol $(n \,|\, X)$ expresses the number of n-subsets of X, the sum of whose elements is divisible by p.

All propositions contained in this section are deduced without the use of combinatorial arguments from the following result due to Chevalley and Warning (see e.g., [5]).

Theorem 2.1. *Let $P_1, P_2, \dots, P_m \in F[x_1, \dots, x_n]$ be some polynomials over a finite field F of characteristic p. Provided that the sum of their degrees is less than n, the number Ω of their common zeros in F^n is divisible by p.*

Proof. It is easy to see that

$$\Omega \equiv \sum_{y_1,\dots,y_n \in F} \quad \prod_{\mu=1}^{m} \big(1 - P_\mu(y_1, \, \dots \, y_n)^{q-1}\big)\,,$$

where $q = |F|$. Expanding the product and taking into account that

$$\sum_{y \in F} y^r \equiv 0 \qquad \text{holds whenever } 1 \leqslant r \leqslant q-2\,,$$

we get indeed $\Omega \equiv 0$. □

Corollary 2.2. *If $|J| = 3p-3$, then $1 - (p-1 \,|\, J) - (p \,|\, J) + (2p-1 \,|\, J) + (2p \,|\, J) \equiv 0$.*

Proof. Let $J = \big\{(a_n, b_n) \,\big|\, 1 \leqslant n \leqslant 3p-3\big\}$ and apply the above theorem to

$$\sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}\,, \ \sum_{n=1}^{3p-3} a_n x_n^{p-1} \qquad \text{and} \qquad \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

considered as polynomials over the field containing p elements. Their common zeros fall into two classes depending on whether $x_{3p-2} = 0$ or not. The first class consists of

$$1 + (p-1)^p (p \,|\, J) + (p-1)^{2p} (2p \,|\, J)$$

solutions, whereas the second class includes

$$(p-1)^p (p-1 \,|\, J) + (p-1)^{2p} (2p-1 \,|\, J)$$

solutions. □

The first of the following two assertions is proved quite analogously and entails the second one immediately.

Corollary 2.3. *If $|J| = 3p-2$ or $|J| = 3p-1$, then $1 - (p \,|\, J) + (2p \,|\, J) \equiv 0$.*

Corollary 2.4. *If $|J| = 3p-2$ or $|J| = 3p-1$, then $(p \,|\, J) = 0$ implies $(2p \,|\, J) \equiv -1$.*

Now we come to an important statement due to N. Alon and M. Dubiner [1].

Corollary 2.5. *If J contains exactly $3p$ elements whose sum is $\equiv (0,0)$, then $(p\,|\,J) > 0$.*

Proof. Let $\mathfrak{A} \in J$ be arbitrary. Arguing indirectly we assume that $(p\,|\,J) = 0$. This obviously implies $(p\,|\,J - \mathfrak{A}) = 0$ and owing to $|J - \mathfrak{A}| = 3p - 1$ the above Corollary 2.4 yields $(2p, J - \mathfrak{A}) \equiv -1$. So in particular we have $(2p\,|\,J - \mathfrak{A}) > 0$ and the condition $\sum J \equiv (0,0)$ entails indeed $(p\,|\,J) = (2p\,|\,J) \geqslant (2p\,|\,J - \mathfrak{A}) > 0$. □

The next two statements are similar to Corollary 2.3 and may also be proved in the same manner.

Corollary 2.6. *If $|X| = 4p - 3$, then*

(*a*) $-1 + (p\,|\,X) - (2p\,|\,X) + (3p\,|\,X) \equiv 0$

(*b*) *and* $(p-1\,|\,X) - (2p-1\,|\,X) + (3p-1\,|\,X) \equiv 0$.

Corollary 2.7. *If $|X| = 4p-3$, then $3 - 2(p-1\,|\,X) - 2(p\,|\,X) + (2p-1\,|\,X) + (2p\,|\,X) \equiv 0$.*

Proof. Corollary 2.2 implies

$$\sum_I \big[1 - (p-1\,|\,I) - (p\,|\,I) + (2p-1\,|\,I) + (2p\,|\,I)\big] \equiv 0\,,$$

where the sum is extended over all $I \subseteq X$ of cardinality $3p - 3$. Analysing the number of times each set is counted one obtains

$$\binom{4p-3}{3p-3} - \binom{3p-2}{2p-2}(p-1\,|\,X) - \binom{3p-3}{2p-3}(p\,|\,X) + \binom{2p-2}{p-2}(2p-1\,|\,X) + \binom{2p-3}{p-3}(2p\,|\,X) \equiv 0\,.$$

The reduction of the binomial coefficients modulo p leads directly to the claim. □

§3. Resolution of Kemnitz' Conjecture

Lemma 3.1. *If $|X| = 4p - 3$ and $(p\,|\,X) = 0$, then $(p-1\,|\,X) \equiv (3p-1\,|\,X)$.*

Proof. Let χ denote the number of partitions $X = A \cup B \cup C$ satisfying

$$|A| = p - 1, \qquad |B| = p - 2, \qquad |C| = 2p\,,$$

and moreover

$$\sum A \equiv (0,0), \qquad \sum B \equiv \sum X, \qquad \sum C \equiv (0,0)\,.$$

To determine χ, at least modulo p, we first run through all admissible A and employing Corollary 2.4 we count for each of them how many possibilities for B are contained in its complement, thus getting

$$\chi \equiv \sum_A (2p\,|\,X - A) \equiv \sum_A -1 \equiv -(p-1\,|\,X)\,.$$

Working the other way around we infer similarly

$$\chi \equiv \sum_{B} (2p \,|\, X - B) \equiv \sum_{X-B} -1 \equiv -(3p-1 \,|\, X)\,.$$

Therefore indeed, by counting the same entities twice, $(p-1 \,|\, X) \equiv (3p-1 \,|\, X)$. □

Theorem 3.2. *Any choice of $4p-3$ lattice–points in the plane contains a subset of cardinality p whose centroid is a lattice-point as well.*

Proof. Adding up the congruences obtained in the Corollaries 2.6(a), 2.6(b), 2.7, and the previous lemma one deduces $2 - (p \,|\, X) + (3p \,|\, X) \equiv 0$. Since p is odd, this implies that $(p \,|\, X)$ and $(3p \,|\, X)$ cannot vanish simultaneously which in turn yields our assertion $(p \,|\, X) \neq 0$ via Corollary 2.5 □

As Kemnitz [3] remarked, for $p = 2$ the above result is an easy consequence of the box-principle. Since according to fact (1) mentioned in the introduction the general statement $f(n, 2) = 4n - 3$ (for every positive integer n) follows immediately from the special case where n is a prime number, we have thereby proved Kemnitz' conjecture.

References

[1] N. Alon and M. Dubiner, *A lattice point problem and additive number theory*, Combinatorica **15** (1995), no. 3, 301–309, DOI 10.1007/BF01299737. MR1357277 ↑1, 2

[2] P Erdős, A Ginzburg, and A Ziv, *Theorem in the additive number theory*, Bull Research Council Israel **10F** (1961), 41–43. ↑1

[3] A. Kemnitz, *On a lattice point problem*, Ars Combin. **16** (1983), no. B, 151–160. MR737118 ↑1, 3

[4] L. Rónyai, *On a conjecture of Kemnitz*, Combinatorica **20** (2000), no. 4, 569–573, DOI 10.1007/s004930070008. MR1804827 ↑1

[5] W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin-New York, 1976. MR0429733 ↑2

Fachbereich Mathematik, Universität Hamburg, Hamburg, Germany

E-mail address: `Christian.Reiher@uni-hamburg.de`