Ramanujan J (2007) 13:333–337
DOI 10.1007/s11139-006-0256-y

On Kemnitz' conjecture concerning lattice-points in the plane

Christian Reiher

Dedicated to Richard Askey on the occasion of his 70th birthday.
Received: 25 May 2004 / Accepted: 14 February 2005

Abstract In 1961, Erdős, Ginzburg and 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.

Keywords Zero-sum-subsets · Kemnitz' Conjecture

2000 Mathematics Subject Classification Primary—11B50

1 Previous work

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 Erdős, Ginzburg and Ziv [2], that $f(n,1)=2n-1$.

The problem, however, to determine $f(n,2)$ turned out to be unexpectedly difficult: Kemnitz [4] conjectured it to equal $4n-3$, but all he knew were (1°), that $4n-3$ is a rather straighforward lower bound,[1] (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 being representable as a product of these numbers.

Linear upper bounds estimating $f(p,2)$, where p denotes any prime, appeared for the first time in a paper by Alon and Dubiner [1] who proved $f(p,2)\le 6p-5$ for

C. Reiher (✉)
Oxford University, UK
e-mail: christian.reiher@keble.ox.ac.uk

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

all p and $f(p,2) \leq 5p-2$ for large p. Later this was improved to $f(p,2) \leq 4p-2$ by Rónyai [5].

In the third section of this paper we give a rigorous proof of Kemnitz' conjecture.

2 Preliminary results

Notational conventions. In the sequel the letter p is always assumed to designate any odd prime and congruence modulo p is simply referred to as '$\equiv$'. Uppercase Roman letters (such as $J, X, \ldots$) will always denote finite sets of lattice-points in the Euclidean plane. The sum of elements of such a set, taken coordinatewise, will be indicated by a preposed 'Σ'. 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

Theorem (Chevalley and Warning; see, e.g. [6]). *Let $P_1, P_2, \ldots, P_m \in F[x_1, \ldots, x_n]$ 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

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

where q is supposed to denote the number of elements contained in F. Expanding the product and taking into account that

$$\sum_{y \in F} y^r \equiv 0 \text{ for } 1 \leq r \leq q-2$$

gives indeed $\Omega \equiv 0$. □

Corollary I. *If $|J| = 3p-3$, then*

$$1 - (p-1 \mid J) - (p \mid J) + (2p-1 \mid J) + (2p \mid J) \equiv 0.$$

Proof: Let (a_n, b_n) denote the elements of J $(1 \leq n \leq 3p-3)$ and apply the above theorem to

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

considered as polynomials over the field containing p elements. Their common zeros fall into two classes, according to whether $x_{3p-2} = 0$ or not. The first class consists of $1 + (p-1)^p(p \mid J) + (p-1)^{2p}(2p \mid J)$ solutions, whereas the second class includes $(p-1)^p(p-1 \mid J) + (p-1)^{2p}(2p-1 \mid J)$ solutions. □

Among the following two assertions the first one is proved quite analogously[2] and entails the second one immedeatedly.

Corollary IIa. *If* $|J| = 3p - 2$ *or* $|J| = 3p - 1$, *then*

$$1 - (p \mid J) + (2p \mid J) \equiv 0.$$

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

Corollary III (Alon and Dubiner [1]). *If* J *contains exactly* $3p$ *elements whose sum is* $\equiv (0,0)$, *then* $(p, J) > 0$.

Proof: Intending to construct a contradiction thereof we assume that $(p|J) = 0$. This obviously implies $(p \mid J - \mathfrak{A}) = 0$, where $\mathfrak{A}$ denotes an arbitrary element of J. But as $| J - \mathfrak{A} | = 3p - 1$ we obtain $(2p, J - \mathfrak{A}) \equiv -1$, which entails $(2p \mid J - \mathfrak{A}) > 0$ and in particular $(2p \mid J) > 0$. The condition $\Sigma J \equiv (0,0)$, however, yields $(2p \mid J) = (p \mid J)$ and hence $(p \mid J) > 0$. $\square$

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

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

$$-1 + (p \mid X) - (2p \mid X) + (3p \mid X) \equiv 0. \tag{a}$$

and

$$(p - 1 \mid X) - (2p - 1 \mid X) + (3p - 1 \mid X) \equiv 0. \tag{b}$$

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

$$3 - 2(p - 1 \mid X) - 2(p \mid X) + (2p - 1 \mid X) + (2p \mid X) \equiv 0.$$

Proof: The first corollary implies

$$\sum \{1 - (p - 1 \mid I) - (p \mid I) + (2p - 1 \mid I) + (2p \mid I)\} \equiv 0,$$

where the sum is extended over all $I \subset X$ of cardinality $3p - 3$.

[2] The polynomials to be used are both times exactly the same ones as in the preceeding proof, except for the replacement of the upper summation index by $3p - 2, 3p - 1$ resp. and the omission of the term x_{3p-2}^{p-1}.

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 leads directly to the claim. □

3 Resolution of Kemnitz' conjecture

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

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

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

and furthermore

$$\Sigma A \equiv (0,0), \quad \Sigma B \equiv \Sigma X, \quad \Sigma C \equiv (0,0).$$

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

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

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 . *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 IVa, IVb, V 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 III. □

It was already known to Kemnitz [4], that the above result is also true for $p = 2$, which is easily seen by means of the box-principle. As according to fact (1°) mentioned in our first section the general statement $f(n, 2) = 4n - 3$ (for every positive integer n) immedeatedly follows from the special case where n is a prime, we have thereby proven Kemnitz’ conjecture.

References

1. Alon, N., Dubiner, D.: A lattice point problem and additive number theory. Combinatorica **15**, 301–309 (1995)
2. Erdős, P., Ginzburg, A., Ziv, A.: Theorem in the additive number theory. Bull Research Council Israel **10F**, 41–43 (1961)
3. Gao, W.: Note on a zero-sum problem. J. Combin. Theory, Series A **95**, 387–389 (2001)
4. Kemnitz, A.: On a lattice point problem. Ars Combin. **16b**, 151–160 (1983)
5. Rónyai, L.: On a conjecture of Kemnitz. Combinatorica **20**, 569–573 (2000)
6. Schmidt, W.M.: Equations Over Finite Fields, An Elementary Approach. Springer Verlag, Lecture Notes in Math (1976)