

- 9.5.4 Let Z be an additive group of order n and let k be a positive integer divisible by n . Prove that for any sequence of elements of Z of length $k + n - 1$ there is a subsequence of length divisible by n whose sum is 0.
- 9.5.5 [6] Let p be a prime, and let $v_1, \dots, v_{3p} \in \mathbf{Z}_p^2$ be such that $\sum_{i=1}^{3p} v_i = 0$. Then there is a subset $J \subset [1, 3p]$ such that $|J| = p$ and $\sum_{j \in J} v_j = 0$. (Hint: modify the argument in Lemma 9.31.)

9.6 Kemnitz's conjecture

Define a parameter $s(n, d)$ as the smallest integer s such that any sequence of s elements from \mathbf{Z}_n^d contains a subsequence of length n whose sum is 0 in \mathbf{Z}_n^d . In this terminology, Theorem 9.28 states that $s(n, 1) = 2n - 1$. Harborth [176] considered the problem of controlling $s(n, d)$ for higher d . He first observed the easy estimates

$$(n-1)2^d + 1 \leq s(n, d) \leq (n-1)n^d + 1 \quad (9.13)$$

and also derived a recursive inequality

$$s(mk, d) \leq s(n, d) + m(s(k, d) - 1); \quad (9.14)$$

we leave the proofs as exercises.

Exact computation of $s(n, d)$ is a difficult task, especially for large d ; for instance the quantity $s(3, d)$ is closely related to the still unsolved problem of obtaining sharp constants for Roth's theorem in \mathbf{Z}_3^d (see Exercise 10.2.4). But in the case when d is fixed and n is large, more is known. Alon and Doubnier [6] proved that $s(n, d) = O_d(n)$. Kemnitz conjectured that the lower bound in (9.13) is sharp for $d = 2$:

Conjecture 9.35 [200] For any $n \geq 1$, we have $s(n, 2) = 4n - 3$.

In [200] the conjecture was verified when the prime factors of n are from the set $\{2, 3, 5, 7\}$. Alon and Doubnier [6] proved that $s(n, 2) \leq 6n - 5$. They also sketched an argument which gives $s(p, 2) \leq 5p - 2$ for all sufficiently large prime p .

Rónyai [286] made a significant progress by proving

Theorem 9.36 [286] For every prime p we have $s(p, 2) \leq 4p - 2$.

Theorem 9.36 and (9.14) imply that $s(n, 2) \leq \frac{41}{11}n$; see Exercise 9.6.3.

Proof The case $p = 2$ is trivial so we can assume that p is odd. Set $m := 4p - 2$, and let $v_1 = (a_1, b_1), \dots, v_m = (a_m, b_m)$. By Exercise 9.5.5, it suffices to show that

there is a subset $J \subset \{1, \dots, m\}$ with $|J| = p$ or $|J| = 3p$ such that $\sum_{j \in J} v_j = 0$. Assume, for contradiction, that there is no such J . Let $\sigma, P_1, P_2 \in F_p(t_1, \dots, t_m)$ be the polynomials

$$\begin{aligned} \sigma(t_1, \dots, t_m) &:= \sum_{I \subset [1, m], |I|=p} \prod_{i \in I} t_i \\ P_1(t_1, \dots, t_m) &:= \left(1 - \sum_{i=1}^m a_i t_i\right)^{p-1} \left(\left(1 - \sum_{i=1}^m b_i t_i\right)^{p-1} - 1 \right) \\ &\quad \times \left(1 - \left(\sum_{i=1}^m t_i\right)^{p-1}\right) (2 - \sigma(t_1, \dots, t_m)) \\ P_2(t_1, \dots, t_m) &:= \prod_{i=1}^m (1 - t_i) \end{aligned}$$

and set $P := P_1 - 2P_2$.

We now claim that $P(x_1, \dots, x_m) = 0$ whenever $x_1, \dots, x_m \in \{0, 1\} \subset F_p$. There are several cases to consider, depending on the size of the set $J := \{i \in [1, m] : x_i = 1\}$. When J is empty then it is easy to see that $P_1(x_1, \dots, x_m) = 2$ and $P_2(x_1, \dots, x_m) = 1$. When J is non-empty, then $P_2(x_1, \dots, x_m)$ is zero. To see that $P_1(x_1, \dots, x_m)$ is also zero, we observe from (9.8) that $1 - (\sum_{i=1}^m x_i)^{p-1} = 0$ when $|J|$ is not divisible by p , and from Wilson's theorem (Exercise 9.4.9) that $\sigma(x_1, \dots, x_m) = 2$ when $|J| = 2p$. Finally, when $|J| = p$ or $|J| = 3p$, we have by hypothesis that $\sum_{i=1}^m (a_i, b_i)x_i = \sum_{i \in J} (a_i, b_i) \neq 0$, and hence $(1 - \sum_{i=1}^m a_i x_i)^{p-1} ((1 - \sum_{i=1}^m b_i x_i)^{p-1} - 1) = 0$.

Thus P vanishes on $\{0, 1\} \times \dots \times \{0, 1\}$. Also, $\deg(P_1) = 4p - 3$ and $\deg(P_2) = m = 4p - 2$, thus $\deg(P) = 4p - 2$. Moreover, the coefficient of the monomial $x_1 \cdots x_m$ in P is $2(-1)^m \cdot 1 \neq 0$. This contradicts the combinatorial Nullstellensatz and concludes the proof. \square

Remark 9.37 In the above proof one only used a very special case of the combinatorial Nullstellensatz; indeed one could rely just on Exercise 9.1.5, which can be proven by more elementary means – in fact, this was the original approach in [286].

Remark 9.38 Very recently, Reiher [279] has proved Kemnitz's conjecture, using the Chavelley–Warning theorem combining with a clever combinatorial argument.

For a further survey of results in this area, see [81].