A talk given at the National Sun Yat-sen Univ. (Taiwan) on May 28, 2002.

ON ZERO-SUM PROBLEMS

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093
The People's Republic of China
E-mail: zwsun@nju.edu.cn
Homepage: http://pweb.nju.edu.cn/zwsun

Abstract. Let G be an additive abelian group. The zero-sum problem for G asks for the least positive integer k such that for any $a_1, \cdots, a_k \in G$ there is an $I \subseteq \{1, \cdots, k\}$ of required cardinality satisfying $\sum_{i \in I} a_i = 0$. In this talk we will introduce the famous theorem of P. Erdős, A. Ginzburg and A. Ziv (for $G = \mathbb{Z}_n$), and recent results of L. Rónya on the Kemnitz conjecture concerning the group $\mathbb{Z}_n \oplus \mathbb{Z}_n$, where $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is the additive cyclic group of residue classes modulo n.

1. The Erdős-Ginzburg-Ziv Theorem

In 1961 P. Erdős, A. Ginzburg and A. Ziv [Bull. Research Council Israel, 10(1961)] established the following celebrated theorem.

EGZ Theorem. *Let n be any positive integer, and $S = \{a_i\}_{i=1}^{2n-1}$ be a sequence of integers. Then there is an $I \subseteq \{1, \cdots, 2n-1\}$ with $|I| = n$ such that $\sum_{i \in I} a_i \equiv 0 \pmod{n}$.*

This can be viewed as the first nontrivial result on zero-sum problems.

Let G be a finite additive abelian group. The zero-sum problem for G asks for the least positive integer k such that for any $a_1, \cdots, a_k \in G$ there exists an $I \subseteq \{1, \cdots, k\}$ of required cardinality satisfying $\sum_{i \in I} a_i = 0$. If we simply require $|I| > 0$, then the smallest k is denoted by $D(G)$ and called *Davenport's constant*;

If we require $|I|=|G|$, then the smallest k is denoted by $S(G)$. If $a_1,\cdots,a_n\in G$ and $n=|G|$, then by the Pigeon-hole Principle the following elements (of G)

$$s_0=0,\ s_1=a_1,\ s_2=a_1+a_2,\ \cdots,\ s_n=a_1+\cdots+a_n$$

cannot be pairwise distinct, thus for some $0\leqslant i<j\leqslant k$ we have $0=s_j-s_i=\sum_{i<r\leqslant j}a_r$. So $D(G)$ does exist and $|D(G)|\leqslant|G|$. If $n=|G|$ and $a_1,\cdots,a_{n^2-n+1}\in G$, then for some $a\in G$ the set $J=\{1\leqslant i\leqslant n^2-n+1\colon a_i=a\}$ has cardinality at least n, therefore for $I\subseteq J$ with $|I|=n$ we have $\sum_{i\in I}a_i=na=0$. (Recall that $|G|=n$ and so the additive order of a divides n.) This indicates that $S(G)$ also exists.

Let $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}=\{\bar{a}=a+n\mathbb{Z}\colon a\in\mathbb{Z}\}$ be the ring of residue classes modulo n. Any cyclic group of order n is isomorphic to the additive group of $\mathbb{Z}_n$. For $a_1=\cdots=a_{n-1}=\bar{1}$ and $\emptyset\neq I\subseteq\{1,\cdots,n-1\}$, we clearly have $\sum_{i\in I}a_i=|I|\bar{1}\neq\bar{0}$. So we cannot have $D(\mathbb{Z}_n)\leqslant n-1$. Therefore $D(\mathbb{Z}_n)=n=|\mathbb{Z}_n|$. If $a_1=\cdots=a_{n-1}=\bar{1}$ and $a_n=\cdots=a_{2n-2}=\bar{0}$, then there is no $I\subseteq\{1,\cdots,2n-2\}$ with $|I|=n$ such that $\sum_{i\in I}a_i=\bar{0}$. This together with the EGZ theorem shows that $S(\mathbb{Z}_n)=2n-1$.

It is easy to reduce the EGZ theorem to the case when n is a prime number p. Note that $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$ is a finite field. The EGZ theorem can be deduced from the following classical result.

Chevalley-Warning Theorem. *Let F be a finite field of order $q=p^\alpha$ where p is a prime. Let $f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n)$ be polynomials over F with $\sum_{i=1}^m\deg f_i<n$. Let N denote the number of solutions of the following system*

$$\begin{cases} f_1(x_1,\cdots,x_n)=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ f_m(x_1,\cdots,x_n)=0\end{cases}$$

of equations over F. Then p divides N, in particular $N\neq1$.

Proof. Clearly $\sum_{a\in F} a^0 = q1 = 0$. Let g be a generator of the multiplicative group $F^* = F\{0\}$ of order $q-1$. For each $k = 1, 2, \cdots, q-2$, we have

$$\sum_{a\in F} a^k = \sum_{a\in F^*} a^k = \sum_{i=0}^{q-2} (g^i)^k = \sum_{i=0}^{q-2} (g^k)^i = \frac{g^{k(q-1)} - 1}{g^k - 1} = 0.$$

So $\sum_{a\in F} a^k = 0$ for all $k = 0, 1, \cdots, q-2$.

Write

$$P(x_1, \cdots, x_n) := \prod_{i=1}^{m} \left(1 - f_i(x_1, \cdots, x_n)^{q-1}\right) = \sum_{\substack{j_1,\cdots,j_n \geqslant 0 \\ j_1+\cdots+j_n < n(q-1)}} c_{j_1,\cdots,j_n} x_1^{j_1} \cdots x_n^{j_n}.$$

For $a_1, \cdots, a_n \in F$, clearly

$$P(a_1, \cdots, a_n) = \begin{cases} 1 & \text{if } f_i(a_1, \cdots, a_n) = 0 \text{ for all } i = 1, \cdots, m, \\ 0 & \text{otherwise.} \end{cases}$$

(Note that $a^{q-1} = 1$ for $a \in F^*$.) Thus,

$$N1 = \sum_{a_1\in F} \cdots \sum_{a_n\in F} P(a_1, \cdots, a_n) = \sum_{\substack{j_1,\cdots,j_n \geqslant 0 \\ j_1+\cdots+j_n < n(q-1)}} c_{j_1,\cdots,j_n} \prod_{i=1}^{n} \left(\sum_{a_i\in F} a_i^{j_i} \right) = 0$$

where in the last step we note that there is an $i \in \{1, \cdots, n\}$ such that $j_i < q-1$ and hence $\sum_{a_i\in F} a_i^{j_i} = 0$. It follows that $p \mid N$. $\square$

Now we explain why the EGZ theorem holds when n is a prime. Let p be a prime and F be a field of order p. Let $a_1, \cdots, a_{2p-1} \in F$, $f_1(x_1, \cdots, 2p-1) = \sum_{k=1}^{2p-1} x_k^{p-1}$ and $f_2(x_1, \cdots, x_{2p-1}) = \sum_{k=1}^{2p-1} a_k x_k^{p-1}$. Note that $\deg f_1 + \deg f_2 < 2p-1$ and $f_1(0, \cdots, 0) = f_2(0, \cdots, 0) = 0$. By the Chevalley-Warning theorem, there are $x_1, \cdots, x_{2p-1} \in F$ such that $I = \{1 \leqslant k \leqslant 2p-1 \colon x_k \neq 0\} \neq \emptyset$ and $f_i(x_1, \cdots, x_{2p-1}) = 0$ for $i = 1, 2$. As $0 = f_1(x_1, \cdots, x_{2p-1}) = \sum_{i\in I} x_i^{p-1} = |I|1$, we must have $p \mid |I|$ and hence $|I| = p$ since $0 < |I| < 2p$. Now that $f_2(x_1, \cdots, x_{2p-1}) = 0$, we also have $\sum_{i\in I} a_i = 0$.

Observe that $S(\mathbb{Z}_n) = 2n-1 = D(\mathbb{Z}_n) + n - 1$. In 1996 W. D. Gao [J. Number Theory, 58(1996)] proved the following general result.

Gao's Relation Formula. *Let G be a finite abelian group. Then $S(G) = D(G) + |G| - 1$.*

2. Rónya's method and the Kemnitz conjecture

In 1983 A. Kemnitz posed the following conjecture.

Kemnitz's conjecture. *For any $a_1, \cdots, a_{4n-3} \in \mathbb{Z}_n \oplus \mathbb{Z}_n$, there exists an $I \subseteq \{1, \cdots, 4n-3\}$ with $|I| = n$ such that $\sum_{i\in I} a_i = 0$.*

We mention that $4n - 3$ is the above conjecture cannot be replaced by a smaller number. In fact, let

$$\begin{aligned} &a_1 = \cdots = a_{n-1} = (0,0), \qquad a_n = \cdots = a_{2n-2} = (0,1), \\ &a_{2n-1} = \cdots = a_{3n-3} = (1,0),\ a_{3n-2} = \cdots = a_{4n-4} = (1,1), \end{aligned}$$

then there is no $I \subseteq \{1, \cdots, 4n-4\}$ with $|I| = n$ such that $\sum_{i\in I} a_i = (0,0)$.

In 2000 L. Rónya [Combinatorica, 20(2000)] made an important breakthrough.

Rónya's Theorem. *The Kemnitz conjecture holds if $4n - 3$ is replaced by $[\frac{41}{10}n]$, or $4n - 2$ with n being a prime.*

The mail tool of Rónya is the following lemma.

Rónya's Lemma. *Let F be a field, and V be the linear space $\{f : \{0,1\}^n \to F\}$ over F. Then those functions $\chi_I \in V$ $(I \subseteq \{1, \cdots, n\})$ given by $\chi_I(x_1, \cdots, x_n) = \prod_{i\in I} x_i$ form a basis of the space V.*

Proof. For $\vec{u} = (u_1, \cdots, u_n) \in \{0,1\}^n$, define $\delta_{\vec{u}} : \{0,1\}^n \to F$ as follows:

$$\delta_{\vec{u}}(\vec{v}) = \begin{cases} 1 & \text{if } \vec{u} = \vec{v}, \\ 0 & \text{otherwise} \end{cases} \quad (\vec{v} \in \{0,1\}^m).$$

Clearly any $f \in V$ can be expressed as $\sum_{\vec{u}\in\{0,1\}^n} f(\vec{u})\delta_{\vec{u}}$. Let $U = \{1 \leqslant i \leqslant n\colon u_i = 1\}$ and $\bar{U} = \{1 \leqslant i \leqslant n\colon u_i = 0\}$. For any $\vec{x} = (x_1, \cdots, x_n) \in \{0,1\}^n$, we have

$$\begin{aligned}\delta_{\vec{u}}(\vec{x}) &= \prod_{i\in U} x_i \times \prod_{j\in\bar{U}}(1-x_j)\\ &= \sum_{J\subseteq\bar{U}}(-1)^{|J|}\prod_{i\in J\cup U} x_i = \sum_{U\subseteq I\subseteq\{1,\cdots,n\}}(-1)^{|I\cap\bar{U}|}\prod_{i\in I} x_i.\end{aligned}$$

So those χ_I with $I \subseteq \{1, \cdots, n\}$ form a generating system of V.

Now we show that those χ_I with $I \subseteq \{1, \cdots, n\}$ are linear independent over F. Suppose on the contrary that $\sum_{j=1}^k c_j\chi_{I_j} = 0$ where $c_j \in F^* = F \setminus \{0\}$ and $I_1, \cdots, I_n$ are distinct subsets of $\{1, \cdots, n\}$ with $|I_1| \leqslant |I_2| \leqslant \cdots \leqslant |I_k|$. Let $u_i = 1$ for $i \in I_1$, and $u_i = 0$ for $i \notin I_1$. Then

$$\chi_{I_j}(\vec{u}) = \prod_{i\in I_j} u_i = \delta_{j1}$$

because for $j > 1$ there is an $i \in I_j$ such that $i \notin I_1$ and hence $u_i = 0$. Therefore

$$0 = \sum_{j=1}^k c_j\chi_{I_j}(\vec{u}) = c_1 \neq 0.$$

This contradiction ends our proof. $\square$

Now we give an application the above lemma.

Theorem [W. D. Gao, 1996; J. X. Liu and Z. W. Sun, 2001]**.** *Let F be a field of prime characteristic p, and G be a subgroup of the additive group of F with $|G| = n$. Let $S = \{a_i\}_{i=1}^{2n-1}$ be a sequence of $2n-1$ elements of G. Then*

$$(*) \qquad r(S,a) \equiv \begin{cases} 0 \pmod p & \text{if } a \neq 0,\\ 1 \pmod p & \text{otherwise}\end{cases}$$

where

$$r(S,a) = \left|\left\{I \subseteq \{1, 2, \cdots, 2n-1\} : |I| = n \ \&\ \sum_{i\in I} a_i = a\right\}\right|.$$

Proof of Theorem in the case $|F| = p$. (H. Pan) Let

$$\begin{aligned}\mathcal{I} =& \left\{ I \subseteq \{1, \cdots, 2p-1\} \colon p \mid |I| \ \& \ \sum_{i \in I} a_i = a \right\} \\ =& \left\{ I \subseteq \{1, \cdots, 2p-1\} \colon |I| = p \ \& \ \sum_{i \in I} a_i = a \right\} \cup \begin{cases} \{\emptyset\} & \text{if } a = 0, \\ \emptyset & \text{if } a \neq 0. \end{cases}\end{aligned}$$

We also set

$$\begin{aligned}P(x_1, \cdots, x_{2p-1}) =& \left(\left(\sum_{i=1}^{2p-1} x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^{2p-1} a_i x_i - a \right)^{p-1} - 1 \right) \\ =& \sum_{\substack{j_1, \cdots, j_{2p-1} \geqslant 0 \\ j_1 + \cdots + j_{2p-1} < 2p-1}} c_{j_1, \cdots, j_n} x_1^{j_1} \cdots x_{2p-1}^{j_{2p-1}}.\end{aligned}$$

Fix $\vec{x} = (x_1, \cdots, x_{2p-1}) \in \{0, 1\}^{2p-1}$. Then

$$P(x_1, \cdots, x_{2p-1}) = \sum_{I \subset \{1, \cdots, 2p-1\}} c(I) \prod_{i \in I} x_i$$

where

$$c(I) = \sum_{\substack{j_i > 0 \text{ for } i \in I \\ j_i = 0 \text{ for } i \notin I \\ \sum_{i \in I} j_i < 2p-1}} c_{j_1, \cdots, j_n}.$$

Observe that

$$P(x_1, \cdots, x_{2p-1}) = \begin{cases} 1 & \text{if } \{1 \leqslant i \leqslant 2p-1 \colon x_i = 1\} \in \mathcal{I}, \\ 0 & \text{otherwise.} \end{cases}$$

So

$$\begin{aligned}P(x_1, \cdots, x_{2p-1}) =& \sum_{I \in \mathcal{I}} \prod_{i \in I} x_i \times \prod_{j \notin I} (1 - x_j) \\ =& \sum_{I \in \mathcal{I}} \sum_{J \subset \bar{I}} (-1)^{|J|} \prod_{i \in I \cup J} x_i + \sum_{I \in \mathcal{I}} (-1)^{|\bar{I}|} \prod_{i=1}^{2p-1} x_i.\end{aligned}$$

In view of the above and Rónya's Lemma, we must have

$$0 = \sum_{I \in \mathcal{I}} (-1)^{|\bar{I}|} = \delta_{a,0} (-1)^{2p-1} + r(S, a)(-1)^{p-1}$$

and hence $(*)$ holds. $\square$

Lemma (Alon, Dubiner). *Let p be a prime, $v_1, \cdots, v_{3p} \in \mathbb{Z}_p \oplus \mathbb{Z}_p$ and $v_1 + \cdots + v_{3p} = (0,0)$. Then there exists an $I \subseteq \{1, \cdots, 3p\}$ with $|I| = p$ such that $\sum_{i\in I} v_i = (0,0)$.*

Proof. Write $v_i = (a_i, b_i)$ for $i = 1, \cdots, 3p$ where $a_i, b_i \in \mathbb{Z}_p$. The polynomial

$$P(x_1, \cdots, x_{3p}) = \left(\left(\sum_{i=1}^{3p} x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{3p} a_i x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{3p} b_i x_i\right)^{p-1} - 1\right)$$

can be written in the form

$$\sum_{\substack{I\subseteq\{1,\cdots,3p\}\\ |I|\leqslant 3p-3}} c_I \prod_{i\in I} x_i^{n_i(I)}$$

where $c_I \in \mathbb{Z}_p$ and $n_i(I) \in \mathbb{Z}^+$.

Now suppose that the desired result fails. Fix $x_1, \cdots, x_{3p} \in \{0,1\}$ and let $I = \{1 \leqslant i \leqslant 3p : x_i = 1\}$. If $P(x_1, \cdots, x_{3p}) \neq 0$, then we must have $p \mid |I|$ and $\sum_{i\in I} v_i = (\sum_{i\in I} a_i, \sum_{i\in I} b_i) = (0,0)$, hence $|I| = 0$ or $3p$. (If $|I| = 2p$ then $|\bar{I}| = p$ and $\sum_{j\in\bar{I}} v_j = \sum_{i=1}^{3p} v_i - \sum_{i\in I} v_i = (0,0)$.) However, $P(0, \cdots, 0) = P(1, \cdots, 1) = -1$. So,

$$\begin{aligned} P(x_1, \cdots, x_{3p}) &= -\,\delta_{(0,\cdots,0)}(x_1, \cdots, x_{3p}) - \delta_{(1,\cdots,1)}(x_1, \cdots, x_{3p}) \\ &= -\prod_{i=1}^{3p}(1 - x_i) - \prod_{i=1}^{3p} x_i = \sum_{J\subset\{1,\cdots,3p\}} (-1)^{|J|-1} \prod_{j\in J} x_j. \end{aligned}$$

For $J = \{1, \cdots, 3p-1\}$ we have $|J| = 3p - 1 > 3p - 3$. In view of Rónya's Lemma we get a contradiction. $\square$

Proof of Rónya's Theorem in the case when n is a prime p. Let

$$v_1 = (a_1, b_1),\ \cdots,\ v_{4p-2} = (a_{4p-2}, b_{4p-2}) \in \mathbb{Z}_p \oplus \mathbb{Z}_p.$$

Suppose that there is no $I \subseteq \{1, \cdots, 4p-2\}$ with $|I| = p$ such that $\sum_{i\in I} v_i = (0,0)$. Let

$$P(x_1, \cdots, x_{4p-2}) := \Big(\Big(\sum_{i=1}^{4p-2} x_i\Big)^{p-1} - 1\Big)\Big(\Big(\sum_{i=1}^{4p-2} a_i x_i\Big)^{p-1} - 1\Big) \times \Big(\Big(\sum_{i=1}^{4p-2} b_i x_i\Big)^{p-1} - 1\Big)\Big(\sum_{\substack{J\subseteq\{1,\cdots,4p-2\}\\ |J|=p}} \prod_{j\in J} x_j - 2\Big).$$

We can write $P(x_1, \cdots, x_{4p-2})$ in the form

$$\sum_{\substack{I\subseteq\{1,\cdots,4p-2\}\\ |I|\leqslant 3p-3+p=4p-3}} c_I \prod_{i\in I} x_i^{n_i(I)}$$

where $c_I \in \mathbb{Z}_p$ and $n_i(I) \in \mathbb{Z}^+$.

Let $x_1, \cdots, x_{4p-2} \in \{0,1\}$ and $I = \{1 \leqslant i \leqslant 4p-2 \colon x_i = 1\}$. As

$$\binom{2p}{p} = \frac{2p(2p-1)\cdots(2p-(p-1))}{p \times 1 \times \cdots \times (p-1)} \equiv 2 \pmod p,$$

if $|I| = 2p$ then

$$\sum_{\substack{J\subseteq\{1,\cdots,4p-2\}\\ |J|=p}} \prod_{j\in J} x_j = \sum_{\substack{J\subseteq I\\ |J|=p}} 1 = \binom{2p}{p} 1 = 2.$$

When $P(x_1, \cdots, x_{4p-2}) \neq 0$, we must have $p \mid |I|$, $\sum_{i\in I} v_i = 0$ and $|I| \neq 2p$, therefore $I = \emptyset$ since we cannot have $|I| = 3p$ by Lemma 2.

Observe that $P(0, \cdots, 0) = (-1)(-1)(-1)(-2) = 2$. By the above, whenever $x_1, \cdots, x_{4p-2} \in \{0,1\}$ we have

$$\begin{aligned} P(x_1, \cdots, x_{4p-2}) &= 2\delta_{(0,\cdots,0)}(x_1, \cdots, x_{4p-2}) = 2 \prod_{i=1}^{4p-2} (1 - x_i) \\ &= \sum_{I\subseteq\{1,\cdots,4p-2\}} (-1)^{|I|} \prod_{i\in I} x_i. \end{aligned}$$

As $(-1)^{|\{1,\cdots,4p-2\}|} \neq 0$, we get a contradiction in view of Rónya's Lemma. $\square$