Dušan Milijančević i Mihajlo Cekić

Primena polinoma na ograničavanje kardinalnosti zbira skupova u *Z*/*pZ*

U ovom radu dokazujemo dva poznata tvrđenja (Koši-Davenportovu teoremu i Erdoš-Hejlbrunovu nejednakost), ali i jednu novu teoremu koja predstavlja njihovo uopštenje. Dokaz se zasniva na nedavno razvijenom polinomskom pristupu problemu, koji na jedan relativno jednostavan način dokazuje mnoga tvrđenja za koja se smatra da su teško rešiva.

1. Uvod

Aditivna teorija brojeva prvi put se pojavljuje u radovima Košija i Varinga koji su prvi pokazali neke značajne rezultate u ovoj oblasti. Njihovo rad su nastavili Erdoš, pa skorije i Alon, Ruzsa i ostali. I danas ova oblast sadrži dosta otvorenih problema koji se delom odnose na kardinalnosti zbira skupova, kojima ćemo se mi baviti.

Zbir dva podskupa od $Z\ /\ pZ$ definišemo kao skup svih mogućih zbirova njihovih elemenata.

Definicija 1. Definišimo operaciju + nad podskupovima od $Z\ /\ pZ$ gde je p neki prost broj, sa

$$A+B=\left\{a+b\,\middle|\, a\in A, b\in B\right\},$$

za $A, B \subset Z\ /\ pZ$.

Slično možemo definisati i druge operacije između skupova.

Koristićemo samo razliku skupova koju definišemo ispod.

Definicija 2. Definišimo operaciju – nad podskupovima od $Z\ /\ pZ$ gde je p neki prost broj, sa

$$A-B=\left\{a-b\,\middle|\, a\in A, b\in B\right\},$$

za $A, B \subset Z\ /\ pZ$.

Dokažimo nekoliko trivijalnih nejednakosti:

Teorema 1. Ako su A i B konačni neprazni podskupovi skupa $Z\ /\ pZ$ onda važi:

Dušan Milijančević (1991), Šabac, Vojvode Stepe 3, učenik 3. razreda Matematičke gimnazije u Beogradu

Mihajlo Cekić (1991), Beograd, Zidarska 1/21, učenik 3. razreda Matematičke gimnazije u Beogradu

a) $\left|A + B\right| \geq \max\left(\left|A\right|, \left|b\right|\right)$

b) $\left|A + B\right| \leq \left|A\right| \; \left|B\right|$

Dokaz: a) Ako transliramo skup A (na svaki njegov element dodamo jednaku vrednost) tako da on sadrži nulu, onda se kardinalnosti skupova A, B i $\left|A + B\right|$ ne menjaju. Isto možemo da uradimo i sa B. Onda očigledno važi $A, B \subset A + B$, pa je $\left|A + B\right| \geq \max\left(\left|A\right|, \left|b\right|\right)$.

b) Očigledno iz definicije sabiranja skupova skup $A + B$ ne može imati više elemenata od $\left|A\right| \left|B\right|$, pa je nejednakost dokazana.

Dosta rezultata iz ove oblasti dokazao je Erdoš, ali je ostavio nekoliko otvorenih problema, a jedan od tih ćemo dokazati u daljem radu. U svom radu, koji je objavljen 1995. godine (Alon *et al*. 1995), Alon je sa svojim saradnicima uveo polinomski metod koji je omogućio nov pristup problemima ove vrste.

2. Koši-Davenportova nejednakost

U ovom odeljku prikazaćemo dva dokaza Koši-Davenportove nejednakosti. Prvi je potpuno elementaran mada ne i jednostavan. U drugom dokazu koristećimo polinomski metod koji će nam omogućiti da navedenu teoremu uopštimo.

Teorema 2. (Koši-Davenportova nejednakost) Neka su A i B neprazni podskupovi skupa Z / pZ za neki prost broj p. Onda važi nejednakost $\left|A + B\right| \geq \min\left(p, \left|A\right| + \left|b\right| - 1\right)$.

Prvi dokaz: Ako je $\left|A\right| + \left|b\right| - 1 \geq p$ onda skupovi A. $\left\{x\right\} - B$ imaju neprazan presek za svako $x \in Z / pZ$, pa je $A + B = Z / pZ$, što znači da je $\left|A + B\right| = p$, pa u nejednakosti koju treba da dokažemo važi znak jednakosti. Onda možemo pretpostaviti da je $\left|A\right| + \left|b\right| - 1 < p$.

Pretpostavimo da pri gornjem uslovu data nejednakost nije tačna i od svih njenih kontraprimera (A, B) izaberimo onaj kod koga je $\left|A\right|$ najmanje. Neka je to (A, B). Onda možemo pretpostaviti da važi $\left|A\right| \geq 2$ jer u slučaju $\left|A\right| = 1$ nejednakost očigledno važi. Primetimo da zamenom skupa B sa skupom $B + \left\{x\right\}$ za proizvoljno $x \in Z / pZ$ (translacija skupa) i leva i desna strana nejednakosti imaju iste vrednosti kao i pre navedene transformacije, pa skupove A i B možemo translirati za prozivoljne elemente iz Z / pZ. Translirajmo skup B za neki element takav da je $\left|A \cap B\right| \geq 1$.

Neka je $A' = A \cap B$ i $B' = A \cup B$. Očigledno je $\left|A\right| + \left|B\right| = \left|A'\right| + \left|B'\right|$, a kako je $A' + B' \subset A + B$, to je $\left|A'\right| + \left|B'\right| \leq \left|A\right| + \left|B\right|$, pa je i (A', B') kontraprimer date nejednakosti. Po izboru skupa A imamo da je $\left|A'\right| \geq \left|A\right|$, a kako je $A' \subset A$, to je $A' = A$. Sledi da za svaki minimalan kontraprimer (A, B), takav da je $\left|A \cap B\right| \geq 1$ važi $A \subset B$. Međutim ako je (A,B)

minimalan kontraprimer onda je i $\left(A+\{x\},B\right)$ minimalan kotraprimer za svako $x \in Z / pZ$. Da bi se prethodna dva skupa sekla potrebno je da važi $x \in B-A$. Iz ovoga sledi da za svako $x \in B-A$ važi $A+\{x\} \subset B$, tj. važi $A+(B-A) \subset B$ odnosno $B+(A-A) \subset B$, zbog asocijativnosti i komutativnosti sabiranja. Kako skup $A-A$ sadrži 0 to je $B \subset B+(A-A)$, pa važi $B = B+(A-A)$, tj. važi $|B+C| = |B|$, za $C = A-A$. Koristićemo sledeći lemu:

Lema 1. Neka su A i B neprazni podskupovi od G gde je $(G,+)$ konačna abelova grupa. Onda je $|A+B| = |A|$ ako i samo ako je A unija konačnog broja translata od G', a B je podskup jednog od translata od G' gde je $(G',+)$ podgrupa grupe $(G,+)$.

Dokaz leme: Dokažimo da ako je $A = \bigcup_{i=1}^{k}\left(\{a_i\}+G'\right)$ i $B \subset G'+\{b\}$, za neke a_i $(1 \leq i \leq k)$ i $b \in G$, onda važi $|A+B| = |A|$. Primetimo da je presek dva translata podgrupe G' ili prazan skup ili se ta dva translata poklapaju. Na osnovu ovoga možemo pretpostaviti da su translate koji čine A disjunktni. Onda je $A = \{a_1, a_2, \ldots, a_k\} + G' = G + G'$, pa je

$$A+B \subset A'+G'+\{b\}+G' = A'+\{b\}+G' = \{a_1+b, a_2+b, \ldots, a_k+b\}+G'.$$

Ako bi se neka dva od translata oblika $\{a_i+b\}+G'$ i $\{a_j+b\}+G'$ poklapala, za neke $i \neq j$, onda bi se poklapala i dva translata koja čine A što je nemoguće. Znači, svaka dva od datih translata su disjunktna, pa važi $|A+B| \leq k|G'|$. Međutim, slično je $|A| = k|G'|$, pa je $|A+B| \leq |A|$ što znači da je $|A+B| = |A|$, što je i trebalo dokazati.

Dokažimo drugi smer leme. Neka je $A, B \subset G$ i neka je $|A+B| = |A|$. Posmatrajmo skup $G' = \{g \mid g \in G, \{\pm g\}+A = A\}$. Očigledno $0 \in G'$. Da bi G' bila grupa dovoljno je dokazati da za $g_1, g_2 \in G'$ važi $g_1 - g_2 \in G'$. Kako je $\{g_1 - g_2\}+G' = \{g_1\} + \left(\{-g_2\}+G'\right)$ $= \{g_1\}+G' = G'$ to $g_1 - g_2 \in G'$, što znači da je G' grupa sa operacijom +. Skup A je unija translata od G' zbog $A = G'+A$. Neka je $b \in B$. Onda je $|A+\{b\}| = |A|$, a kako je $A+\{b\} \subset A+B$ to je $A+B = A+\{b\}$. Kako je b proizvoljan element iz B to je $A+\{b\} = A+\{b'\}$ za svaka dva elementa b i b' iz B, tj. $\{b'-b\}+A = A$, što znači da $b'-b \in G'$, tj. B je podskup nekog translata od G', što je i trebalo dokazati. Ovim je dokaz leme završen.

Primenjujući ovu lemu na jednakost $|B+C| = |B|$, dobijamo da je B unija nekoliko translata neke podgrupe grupe Z / pZ i da je C podskup nekog translata iste podgrupe. Kako su jedine podgrupe od Z / pZ cela ta grupa ili samo $\{0\}$, to je, ili $B = Z / pZ$, ili $|B| = 1$. Međutim ovo je kontradikcija jer u oba slučaja važi data nejednakost. Ovim je dokaz teoreme završen.

Drugi dokaz: Kao i prvom dokazu možemo pretpostaviti da je $|A| + |B| - 1 < p$. Neka je $|A| = k$, $|B| = l$ i $|A + B| = n$. Pretpostavimo suprotno, tj. da je $n < \min(p, k + l - 1)$ odnosno $n < p$ i $n < k + l - 1$. Uočimo polinom

$$f(x,y) = \prod_{c \in A+B} (x + y - c) = \sum_{\substack{i+j \le 1 \\ i,j \in N_0}} f_{i,j} x^i y^j$$

gde su $f_{i,j}$ neki celi brojevi. Ovaj polinom možemo napisati u sledećem obliku:

$$f(x,y) = \sum_{\substack{i<k,j<l \\ i+j \le n \\ i,j \in N_0}} f_{i,j} x^i y^j + \sum_{\substack{i \ge k,j<l \\ i+j \le n \\ i,j \in N_0}} f_{i,j} x^i y^j + \sum_{\substack{i<k,j \ge l \\ i+j \le n \\ i,j \in N_0}} f_{i,j} x^i y^j + \sum_{\substack{i \ge k,j \ge l \\ i+j \le n \\ i,j \in N_0}} f_{i,j} x^i y^j$$

Koristićemo sledeću lemu:

Lema 2. Neka je A podskup od Z / pZ takav da je $|A| = k$. Onda za svako prirodno m, $m \ge k$ postoji polinom g_m, $g_m \in Z_p[x]$ stepena najviše $k - 1$ takav da je $g_m(a) = a^m$ za svako $a \in A$ (u Z / pZ).

Dokaz: Neka je $A = \{a_1, a_2, \ldots, a_k\}$ i posmatrajmo sledeći sistem linearnih jednačina po c_0, c_1, …, c_{k-1} u Z / pZ:

$$\begin{aligned} c_0 + c_1 a_1 + \ldots + c_{k-1} a_1^{k-1} &= a_1^m \\ c_0 + c_1 a_2 + \ldots + c_{k-1} a_2^{k-1} &= a_2^m \\ &\ldots \\ c_0 + c_1 a_k + \ldots + c_{k-1} a_k^{k-1} &= a_k^m \end{aligned}$$

Njegova determinanta je Vandermondova tj. jednaka je $\prod_{1 \le i < j \le n} (a_i - a_j)$, pa je različita od 0, jer je $a \ne a_j$. Iz ovoga sledi da naš sistem linearnih jednačina ima rešenje. Samim tim možemo uzeti da je traženi polinom $g(x) = c_0 + c_1 x + \ldots + c_{k-1} x^{k-1}$, gde je $(c_0, c_1, \ldots, c_{k-1})$ rešenje datog sistema, čime je lema dokazana.

Po prethodnoj lemi postoji polinomi $g_i \in Z_p[x]$ stepena najviše $k - 1$ i $h_j \in Zp[x]$ stepena najviše $l - 1$, takvi da je $g_i(x) = x^i$(za sve $x \in A$) i $h_j(x) = x^j$(za sve $x \in B$) za $i \ge k$, $j \ge 1$, $i, j \in N$. Onda je

$$f(x,y) = \sum_{\substack{i<k,j<l \\ i+j \le n \\ i,j \in N}} f_{i,j} x^i y^j + \sum_{\substack{i \ge k,j<l \\ i+j \le n \\ i,j \in N}} f_{i,j} g_{i,j}(x) y^j + \sum_{\substack{i<k,j \ge l \\ i+j \le n \\ i,j \in N}} f_{i,j} x^i h_j(y) + \sum_{\substack{i \ge k,j \ge l \\ i+j \le n \\ i,j \in N}} f_{i,j} g_i(x) h_j(y)$$

za $(x, y) \in A \times B$. Označimo sa $p(x, y)$ prethodni polinom. Stepen uz promenljivu x je najviše $k - 1$, a uz promenljivu y najviše $l - 1$, a kako je $p(x, y) = 0$, za $(x, y) \in A \times B$, to je $p(x, y) \equiv 0$ za sve $x, y \in Z / pZ$.

Po pretpostavci Koši-Davenportova nejednakost nije tačna, pa postoje $0 \le u, v \le p - 1$ takvi da je $u + v = n < p$, $u < k$ i $j < l$. Posmatrajmo koeficijente uz $x^u y^v$u polinomima $f(x, y)$ i

$p(x,y)$. Kako je $u+v=n$ koeficijent uz $x^u y^v$ je isti i u oba polinoma (nad Z/pZ), jer se pri našoj transformaciji stepen članova polinoma strogo smanjuje, kako se ovaj član nije transformisao njegov koeficijent se nije mogao promeniti. Međutim u polinomu $f(x,y)$ taj koeficijent je $\binom{n}{u}$, a u polinomu $p(x,y)$ je 0. Kako je $n<p$, to p ne deli $\binom{n}{u}$, što je kontradikcija. Samim tim početna pretpostvaka je netačna, čime smo dokazali traženu teoremu.

3. Erdoš-Hejlbrunova teorema

Cilj ovog odeljka je dokaz Erdoš-Hejlbrunove teoreme koja je postavljena kao hipoteza 1964. godine, a rešena je tek 1994. Rešenje ćemo zasnivati na maloj promeni drugog dokaza Koši-Davenportove nejednakosti. Dokazaćemo sledeće uopštenje:

Teorema 3. Neka su A i B neprazni podskupovi iz Z/pZ, gde je p prost broj. Definišimo operaciju $+_1$ nad podskupovima od Z/pZ kao $A+_1 B=\{a+b \mid a\in A, b\in B, a\neq b\}$. Onda je $|A+_1 B|\geq \min(p,|A|+|B|-2)$.

Dokaz: Ukoliko je $|A|+|B|-2\geq p$ presek skupova A i $\{x\}-B$ ima bar dva različita elementa, pa važi $A+_1 B=Z/pZ$. Samim tim nejednakost važi u ovom slučaju. Možemo pretpostaviti da je $|A|+|B|-2<p$. Neka je $|A|=k$, $|B|=l$ i $|A+B|=n$. Pretpostavimo suprotno tj. da je $n<p$ i $n<k+l-2$. Uočimo polinom

$$f(x,y)=(x-y)\prod_{c\in A+_1 B}(x+y-c)=\sum_{\substack{i+j\leq n\\ i,j\in N_0}} f_{i,j}x^i y^j,$$

za neke cele brojeve $f_{i,j}$. Onda je $f(x,y)=0$ za sve $(x,y)\in A\times B$. Primenjući lemu pokazanu u dokazu Koši-Davenportove nejednakosti možemo na isti način transformisati polinom $f(x,y)$ u polinom $p(x,y)$ čiji je stepen po x manji od k i stepen po y manji od l koji ima iste vrednosti kao $f(x,y)$ nad Z/pZ.

Samim tim je $p(x,y)\equiv 0$ u Z/pZ. Posmatrajmo koeficijent uz $x^u y^v$ gde je $u+v=$ $=\deg f$ i $u<k$, $v<l$. Ovakvi brojevi očigledno postoje zbog $\deg f<k+l$. Onda je koeficijent uz $x^u y^v$ u f jednak

$$\binom{u+v-1}{u-1}-\binom{u+v-1}{v-1}=\frac{(u+v-1)!}{(u-1)!(v-1)!}\left(\frac{1}{v}-\frac{1}{u}\right)=\frac{(u-v)(u+v-1)!}{uv(u-1)!(v-1)!},$$

što ne može da bude deljivo sa p jer je $u+v-1<p$. Ovo je kontradikcija jer je koeficijent uz $x^u y^v$ u polinomu f jednak 0.

Koristeći ovo tvrđenje dokazaćemo sledeću teoremu:

Teorema 4. (Erdoš-Hejlbrunova teorema) Neka je A neprazan podskup od Z/pZ. Onda je $|A+_1 A|\geq \min(p, 2|A|-3)$.

Dokaz: Primenimo prethodnu teoremu na skupove A i B gde je $B = A \setminus \{x\}$ gde je x neki proizvoljan element iz A. Kako je $A +_1 A = A +_1 B$ zato što svi brojevi oblika $a + x$ ($a \neq x$) gde $a \in A$ pripadaju i $A +_1 B$ zbog $x \in A$, $a \in B$ i $a \neq x$. Onda je $|A +_1 A| \geq |A +_1 B| \geq$ $\geq \min(p, |A| + |B| - 2) = \min(p, 2|A| - 3)$, što je trebalo dokazati.

4. Uopštenje Koši-Davenportove nejednakosti i Erdoš-Hejlbrunove teoreme

U ovom odeljku prikazaćemo jedan način na koji se mogu uopštiti predhodne teoreme nastavljajući korišćenje polinomskog metoda.

Definicija 2. Za polinom $h = h(x_0, x_1, \ldots, x_k)$ nad Z / pZ (gde je p neki prost broj) i skupove $A_0, A_1, \ldots, A_k$ definišemo skup

$$\oplus_h \sum_{i=1}^{k} A_i = \left\{ \sum_{i=1}^{k} a_i \;\middle|\; a_i \in A_i, h(a_0, a_1, \ldots, a_k) \neq 0 \right\}.$$

Dokazujemo sledeću teoremu iz koje prethodne dve teoreme slede kao specijalani slučajevi i po broju skupova i po ograničenjima. Malo ćemo promeniti izbor karakterističnog polinoma da bi mogli da specificiramo koje koeficijent ćemo iskoristiti za kontradikciju.

Teorema 5. Neka je p prost broj i $h = h(x_0, x_1, \ldots, x_k)$ polinom nad Z / pZ. Ako su A_0, $A_1, \ldots, A_k$ neprazni podskupovi od Z / pZ gde je $|A_i| = c_i + 1$. Neka je $m = -\deg h + \sum_{i=0}^{k} c_i$ i neka važi $m \geq 0$. Ako je koeficijent uz $x_0^{c_0}, x_1^{c_1}, \ldots, x_k^{c_k}$ u polinomu

$(x_0 + x_1 + \ldots + x_k)^m h(x_0, x_1, \ldots, x_k)$

različit od 0 onda važi

$$\left| \oplus_h \sum_{i=1}^{k} A_i \right| \geq m + 1.$$

Dokaz: Pretpostavimo da je tvrđenje netačno tj. $\left| \oplus_h \sum_{i=1}^{k} A_i \right| < m + 1$. Onda postoji multi-skup E od m elemenata iz Z/pZ koji sadrži skup $\oplus_h \sum_{i=1}^{k} A_i$. Neka je $Q = Q(x_0, x_1 \ldots x_k)$ polinom definisan na sledeći način:

$$Q(x_0, x_1, \ldots, x_k) = h(x_0, x_1, \ldots, x_k) \cdot \prod_{t \in \oplus_h E} (x_0 + x_1 + \ldots + x_k - t).$$

Primetimo da

$$Q(x_0, x_1, \ldots, x_k) = 0 \text{ za sve } (x_0, x_1, \ldots, x_k) \in A_0 \times A_1 \times \ldots \times A_k.$$

Ovo je posledica toga da je $\forall\, x_0, x_1, \ldots, x_k$, ili $h(x_0, x_1, \ldots, x_k) = 0$, ili $(x_0, x_1, \ldots, x_k) \in$ $\in \oplus_h \sum_{i=1}^{k} A_i$, pa je $x_0 + x_1 + \ldots + x_k - t = 0$, za odgovarajuće $t \in \oplus_h \sum_{i=1}^{k} A_i \subset E$. Primetimo takođe da je $\deg Q = m + \deg h = \sum_{i=0}^{k} c_i$ i zbog toga je koeficijent od $x_0^{c_0}, x_1^{c_1}, \ldots, x_k^{c_k}$ u polinomu Q isti kao i kod polinoma $(x_0 + x_1 + \ldots + x_k)^m h(x_0, x_1, \ldots, x_k)$, koji je nenula, prema pretpostavci. Prema lemi pokazanoj u drugom dokazu Koši-Davenportove nejednakosti koja tvrdi da svaki stepen od x_i veći od c_i u našem polinomu možemo da transformišemo na stepen najviše c_i, tako da se na skupu A_i ne menja vrednost polinoma. Kako je stepen dobijenog polinoma po svakoj promenljivoj x_i manji ili jednak c_i, a pritom se anulira na $A_0 \times A_1 \times \ldots \times A_k$ onda je on nula polinom, što znači da su mu svi koeficijenti jednaki nuli (naravno u Z/pZ).

Uočimo da je koeficijent uz $x_0^{c_0}, x_1^{c_1}, \ldots, x_k^{c_k}$ u početnom polinomu Q jednak koeficijentu u novodobijenom polinomu, zato što nije bilo njegove izmene u navedenim transformacijama, jer bi u suprotnom stepen polinoma Q bio veći od $c_0 + c_1 + \ldots + c_k$, što je nemoguće. Kako je prema početnoj pretpostavci taj koeficijent u polinomu Q različit od 0, a u transformisanom polinomi jednak 0, dobijamo kontradikciju, čime je ovo tvrđenje dokazano.

Primetimo da za $m < 0$ važi

$$\left| \oplus_h \sum_{i=1}^{k} A_i \right| \geq 0 \geq m + 1,$$

što znači da data nejednakost važi i za negativno m.

Pod dati uslovima teoreme važi i

$$p \geq \left| \oplus_h \sum_{i=1}^{k} A_i \right| \geq m + 1,$$

pa je $m < p$.

Alternativni dokaz Koši-Davenportove nejednakosti može se sprovesti ukoliko posle dobijene nejednakosti $|A| + |B| - 1 < p$ primenimo prethodnu teoremu na slučajeve $k = 1$ i $h \equiv 1$. Slično se i alternativni dokaz Teoreme 3. može sprovesti ukoliko posle dobijene nejednakosti $|A| + |B| - 2 < p$ i eliminisanja trivijalnog slučaja $|A| = |B| = 1$, primeni prethodna teoremu na slučajeve $k = 1$ i $h(x_0, x_1) \equiv x_0 - x_1$. Izborom raznih drugih polinoma za h možemo da napravimo dosta sličnih tvrđenja. Problem kod više promenjlivih nastaje kada treba da sračunamo koeficijent koji se nije transformisao, što u nekim slučajevima može da predstavlja neki od otvorenih kombinatornih problema. Jedan od zanimljivih rezultati iz ovog konteksta dokazali su Dias de Silva i Hamidoune koji glasi:

Teorema 6. Neka je p prost broj, A podskup od Z/pZ i $k \in N$. Ako je polinom h definisan sa $h(x_0, x_1, \ldots, x_k) = \prod_{\substack{0 \leq i < j \leq k \\ i,j \in N_0}} \left(x_i - x_j \right)$ onda je

$$\left| \oplus_h \sum_{i=0}^{k} A_k \right| \geq \min \left(p, (k+1) \; |A| - (k+1)^2 + 1 \right).$$

Dokaz se može naći u članku Alona i saradnika (Alon *et al*. 1996).

5. Zaključak

U ovom radi dokazali smo teoremu koja je uopštenje nekoliko osnovnih tvrđenja aditivne teorije brojeva iz Z/pZ. Modifikovali smo ideju iz dokaza Koši-Davenportove nejednakosti koristeći polinomski pristup. Data teorema može se dalje uopšiti na proizvoljna polja (videti Alon 1999) koja se dosta primenjuje u raznim oblastima matematike.

Literatura

Alon N., Nathanson M. B., Ruzsa I. 1995. Adding distinct congruence classes modulo a prime. *American Math. Monthly*, **102**: 250.

Alon N., Nathanson M. B., Ruzsa I. 1996. The polynomial method and restricted sums of congruence classes. *J. of Number Theory*, **56**: 404.

Alon N. 1999. Combinatorial Nullstellensatz. *Combinatorics, Probability and Computing*, **8**: 729.

Dušan Milijančević and Mihajlo Cekić

Polynomial Method and Cardinality of Sumsets in Z/pZ

In this paper we prove two well known theorems (Cauchy-Davenport inequality and Erdosh-Heilbrunn theorem) and one new result which is their extension. Proofs are based on a recently developed polynomial method, which in a relatively simple way proves many facts which are considered to be very difficult to solve.