Събиране на множества

Владимир В. Барзов

Поводът за статията е една задача от теория на числата. Приведени са нейно обобщение и няколко следствия. Действието се развива около остатъци по прост модул, множества от такива остатъци и специален вид събиране на множества.

1 Завръзка

На подготовката на американския отбор за IMO 2001 е предложена следната задача:

Задача 1 (МОР 1999) Дадени са естествени числа d и n и нечетно просто p. Да се докаже, че съществуват естествени числа $x_1, x_2, \ldots, x_d$, такива че $x_1^d + x_2^d + \ldots + x_d^d \equiv n(mod\ p)$.

Задачата може да се реши чисто комбинаторно или алгебрично - с минимален полином. Но и двата подхода са неприложими в една по-обща ситуация. Ще докажем предварително няколко основни твърдения. Вземаме нечетно просто число p и за всяко число $x \in Z_p$ считаме x да е неговото "съответно" цяло неотрицателно число в интервала $[0, p-1]$. По-долу ще бележим елементите на Z_p с цветен шрифт. За произволни множества A и B от елементи на Z_p въвеждаме следните означения:

$$A + B := \{a + b | a \in A, b \in B\}$$

$$D := \{0, 1, 2, \ldots, p-1\}$$

$$t + A := \{t + a | a \in A\}$$

$$cA := \{ca | a \in A\}, c \neq 0$$

$$-A := \{-a | a \in A\} = (p-1)A$$

$$\div A \Rightarrow \exists a, d : A \equiv \{a + d, a+2d, \ldots, a+|A|d\}$$

$$A \sim B \Rightarrow \exists a, b, d(d \neq 0) : A \equiv \{a + d, a+2d, \ldots, a+|A|d\}, B \equiv \{b + d, b+2d, \ldots, b+|B|d\}$$

Всички множества тук и по-долу ще считаме непразни. Да отбележим няколко свойства:

$$A \sim B \Rightarrow \div A, \div B, B \sim A \sim t + A \sim -A \sim A + B \sim D; \quad cA \sim cB \qquad [1]$$

$$(t + A) + B = t + (A + B); \quad cA + cB = c(A + B), c \neq 0 \qquad [2]$$

$$|A + B| = |t + A + B| = |cA + cB|, c \neq 0 \qquad [3]$$

$$1 < |B| < p - 1, A \sim B \sim C \Rightarrow A \sim C \ ^{1} \qquad [4]$$

Ще се интересуваме от размера на множество, което е сума на две други множества. Искаме да определим кога то съвпада с D - множеството от всички елементи в Z_p, а когато не съвпада - колко най-малко елемента съдържа то. За целта ще докажем две теореми.

[1] единствено последното твърдение не е очевидно, но няма да го използваме

Теорема 1 *За всеки две подмножества A и B на D е изпълнено*

$$|A+B| \geq min(|A|+|B|-1, p).$$

Доказателство. Нека $|A|=m, |B|=n$. Ще разгледаме два случая.

Случай 1: $m+n>p$. Да предположим, че $|A+B|<p$, т.е. $\exists t \notin A+B$. Тогава

$$(t+(-B)) \cap A \equiv \oslash, |t+(-B)|+|A| = m+n > p.$$

Последното е невъзможно, следователно

$$|A+B| = p = min(m+n-1, p).$$

Случай 2: $m+n \leq p$. Ще направим индукция по $min(m,n)$. Считаме без ограничение $m \leq n < p$. Ако $m=1$, то

$$|A+B| = |B| = |A|+|B|-1 \tag{1}$$

и всичко е наред.
Нека сега $p > n \geq m > 1$ и да вземем елемент u от множеството $D \backslash B$ и два различни елемента a_1, a_2 от A. Понеже редицата

$$u+i(a_2-a_1), \quad i=1,2,\ldots,p-1$$

обхожда всички елементи на $D\backslash\{u\}$, то има най-малко i, за което елементът $b=c+i(a_2-a_1)$ е от B. Предвид свойства [2] и [3] можем да заменим множеството A с множеството $(b-a_2)+A$, което съдържа елементите $b+(a_1-a_2) \notin B$ и $b \in B$. Ще докажем теоремата за новата двойка множества. Нека

$$F := A \cap B, G := A \cup B, \tag{2}$$

като притова $0 < |F| < m \leq n < |G|$. От (2) следва

$$|F|+|G| = |A|+|B| = m+n. \tag{3}$$

В същото време ако $f \in F, g \in G$, то в зависимост дали $g \in A$ или $g \in B$ имаме $\{g,f\} \in A \times B$ или $\{f,g\} \in A \times B$, т.е. $f+g \in A+B$. Така

$$F+G \subseteq A+B. \tag{4}$$

и значи

$$|A+B| \geq |F+G|. \tag{5}$$

Поради (3) остава да докажем твърдението за F и G. Но $|F|<|A|$ и можем да се позовем на индукцията. С това теоремата е доказана. □

Следствие

$$|A_1+A_2+\ldots+A_k| \geq min(|A_1|+|A_2|+\ldots+|A_k|-(k-1), \quad p).$$

Теорема 2 *Ако* $1<|A|,|B|$ *и* $|A|+|B|<p$, *то*

$$|A+B| = |A|+|B|-1 \iff A \sim B.$$

Доказателство. Лявата посока на твърдението е очевидна - ако

$$A \equiv \{a+d, a+2d, \ldots, a+|A|d\}, B \equiv \{b+d, b+2d, \ldots, b+|B|d\},$$

то

$$A+B \equiv \{a+b+2d, a+b+3d, \ldots, a+b+(|A|+|B|)d\}$$

и значи $|A+B| = |A|+|B|-1$.
Остава да докажем дясната посока. Считаме $1 < |A| =: m \leq |B| =: n$. Отново от свойства [2] и [3] следва, че е достатъчно да докажем теоремата за коя да е транслация на A или B или за множествата cA и cB. Вземаме два елемента $a_1, a_2 \in A$ и заменяме A и B съответно с $c(-a_1+A)$ и cB, където $c = (a_2-a_1)^{-1}$. Вече можем да считаме

$$0, 1 \in A. \tag{6}$$

Ще направим индукция по m. При $m = 2$ от (6) следва $A \equiv \{0, 1\}$. Явно съществува най-много един елемент $b \in B$, за който $b+1 \notin B$, иначе бихме имали

$$|A+B| \geq |B|+2 > |A|+|B|-1.$$

Така B се състои от поредни елементи, откъдето $A \sim B$. [2]
Нека сега $2 < m \leq n$.

Случай 1: Да предположим, че за някое $t \in D$ е изпълнено

$$|(t+A) \cap B| \in [2, m-1]. \tag{7}$$

Заменяме A с $t+A$ и полагаме както в (2)

$$F := A \cap B, G := A \cup B,$$

като от (3), (5) и **T1** имаме

$$|F|+|G|-1 \leq |F+G| \leq |A+B| = |A|+|B|-1 = |F|+|G|-1. \tag{8}$$

Тогава F и G изпълняват условията на **T2** и предвид $1 < |F| < |A|$ (следва от (7)) можем да приложим резултата от индукцията - $F \sim G$. От (4) и (8) следва

$$F+G \equiv A+B. \tag{9}$$

Нека $k := |F|, r := |G|, 1 < k < r < p$ и

$$F \equiv \{f+d, f+2d, \ldots, f+kd\}, G \equiv \{g+d, g+2d, \ldots, g+rd\}.$$

От $F \subset G$ следва

$$f+d = g+(q+1)d \tag{10}$$

за някое $q \in [0, r-k]$ (предвид $g, g+(r+1)d \notin G$).
Ако евентуално $q > 1$ ще покажем, че $g+d, g+2d, \ldots, g+qd$ са едновременно елементи или на A или на B. За целта да видим, че $g+id$ и $g+jd$ не могат да принадлежат на различни множества ако $i+j = q$ или $i+j = q+1$. Действително - предвид (9) бихме получили

$$g+id+g+jd = f+i'd+g+j'd$$

за някои $i' \in [1, k], j' \in [1, r]$. Тогава от (10) и $d \neq 0$:

$$i'+j'+q = i+j. \tag{11}$$

В същото време

$$q \leq i+j \leq q+1 < i'+j'+q \leq k+r+q = m+n+q < p+q,$$

[2] релацията $X \sim Y$ включва в себе си твърденията $\div X$ и $\div Y$ - свойство [1]

значи

$$i' + j' + q - i - j \in (0, p),$$

което противоречи на (11). Така елементите

$$g{+}qd, g + d, g{+}(q-1)d, g{+}2d, g{+}(q-2)d, g{+}3d, \ldots$$

групирани последователно по двойки гарантират, че $g + d, g{+}2d, \ldots, g{+}qd$ са в едно от множествата A или B. По аналогичен начин се доказва, че елементите $g{+}(q+k+1)d, g{+}(q+k+2)d, \ldots, g{+}rd$ са също в едно множество. Вече е ясно, че и A и B се състоят от поредни елементи в редицата $g + d, g{+}2d, \ldots, g{+}rd$, значи $A \sim B$.

Случай 2: Считаме, че за никое $t \in D$ не е изпълнено (7), т.е.

$$|(t + A) \cap B| \geq 2 \Rightarrow (t + A) \subseteq B. \tag{12}$$

Нека $k \geq 1$ е най-голямото число, за което съществуват k поредни елемента в B, и за някое $w \in D$

$$w, w + 1, \ldots, w + k - 1 \in B.$$

Заменяме B с $-w + B$, откъдето заедно с максималността на k:

$$0, 1, \ldots, k - 1 \in B, -1, k \notin B. \tag{13}$$

Да предположим, че

$$\exists q, q \neq 0 : q \in A, -q \in B, \tag{14}$$

и нека

$$A_1 = -q + A \Rightarrow -q, -q + 1, 0 \in A_1; -q, 0 \in B. \tag{15}$$

Тогава $|A_1 \cap B| \geq 2$ и от (12) следва $A_1 \subseteq B$, в частност от (15) имаме $-q + 1 \in B$. Сега полагаме

$$A_2 = -q + 1 + A \Rightarrow -q + 1, -q + 2, 1 \in A_2; -q + 1, 1 \in B.$$

Отново $|A_2 \cap B| \geq 2 \Rightarrow A_2 \subseteq B \Rightarrow -q + 2 \in B$. Продължаваме по същия начин с $A_3, A_4, \ldots, A_k$. Да проследим последния ход:

$$A_k = -q + k - 1 + A; -q + k - 1, -q + k, k - 1 \in A_k; -q + k - 1, k - 1 \in B.$$

За пореден път $|A_k \cap B| \geq 2 \Rightarrow A_k \subseteq B \Rightarrow -q + k \in B$. Така получихме $k + 1$ поредни елемента в B, а именно $-q, -q + 1, \ldots, -q + k$, което е противоречие с максималността на k.
Следователно (14) не е изпълнено и от (6) и (13)

$$A \cap (-B) \equiv \{0\}. \tag{16}$$

Полагаме

$$A^* = A \backslash \{0\}, 1 < |A^*| < |A|.$$

От (16) имаме

$$0 \notin A^* + B \subseteq A + B \ni 0, \tag{17}$$

следователно от **T1**

$$(m - 1) + n - 1 \leq |A^* + B| < |A + B| = m + n - 1,$$

откъдето

$$|A^* + B| = m + n - 2 = |A^*| + |B| - 1 = |A + B| - 1. \tag{18}$$

От индукционното предположение следва $A^* \sim B$. Нека

$$A^* \equiv \{a + d, a{+}2d, \ldots, a{+}(m-1)d\}, B \equiv \{b + d, b{+}2d, \ldots, b{+}nd\}.$$

Тогава

$A^*+B \equiv \{a+b+2d, a+b+3d, \ldots, a+b+(m+n-1)d\}, D \equiv \{a+b+2d, a+b+3d, \ldots, a+b+(p+1)d\}$.

От (13) имаме $0 = b+rd \in B$ за някое $r \in [1,n]$. В същото време от (17) и (18) виждаме, че

$$(A+B)\backslash(A^*+B) \equiv \{0\},$$

значи

$$B\backslash\{0\} \subseteq (A+B)\backslash\{0\} \equiv A^*+B. \tag{19}$$

Ако $1 < r < n$, то от (19): $b+(r-1)d, b+(r+1)d \in A^*+B$. Но както видяхма по-горе цикличната редица $\{a+b+id\}_{i=2}^{p+1}$ се състои последователно от $m+n-2$ елемента от A^*+B и $p-m-n+2$ елемента от $D\backslash(A^*+B)$ - два блока с дължина поне по 3, т.е. не съществуват три поредни елемента в нея, единствено вторият от които да не принадлежи на A^*+B.
Така $r = 1$ или $r = n$. Ако $r = 1$, то $0 = b+d \notin A^*+B, b+2d \in A^*+B$ и пак от горното наблюдение следва, че $b+d$ може да е единствено $a+b+d$, т.е. $a = 0$. Очевидно тогава

$$A \equiv \{a, a+d, a+2d, \ldots, a+(m-1)d\} \Rightarrow A \sim B$$

и готово. Ако ли пък $r = n$ получаваме аналогично

$$A \equiv \{a+d, a+2d, \ldots, a+(m-1)d, a+md\} \Rightarrow A \sim B.$$

Теоремата е доказана. □

Възниква въпросът какво става ако премахнем изискванията в **T2** за $|A|$ и $|B|$. Както се изясни в (1) при $|A| = 1$, при $|B| = 1$, или при $|A|+|B| = p+1$ винаги е изпълнено $|A+B| = |A|+|B|-1$. Ако $|A|+|B| > p+1$, то $|A+B| \leq p < |A|+|B|-1$.
Да видим какво се случва при $|A|+|B| = p$. За да бъде изпълнено $|A+B| = |A|+|B|-1$ трябва $|A+B| = p-1$, значи $D\backslash(A+B) = \{t\}$ и

$$(t+(-A)) \cap B \equiv \oslash.$$

Тъй като $|(t+(-A))| = |A| = p-|B|$, последното е еквивалентно с

$$A \equiv t-(D\backslash B).$$

Лесно се проверява, че двойките $\{A,B\}$ които търсим са от вида

$$\{t-(D\backslash B), B\}$$

за произволни $t \in D, B \subset D$.

Резюме на резултатите от **T1** и **T2**:
Ако A и B са (строги) подмножества на D, то

(i) $$|A| = 1 \ \ (|B| = 1) \Rightarrow |A+B| = |A|+|B|-1 < p;$$

(ii) $$|A|+|B| > p \Rightarrow |A+B| = p < |A|+|B|;$$

(iii) $$|A|+|B| \leq p, A \sim B \Rightarrow |A+B| = |A|+|B|-1;$$

(iv) $$A \equiv t-(D\backslash B) \Rightarrow |A+B| = p-1 = |A|+|B|-1;$$

(v) $$\sim i, \sim ii, \sim iii, \sim iv \Rightarrow |A+B| \geq |A|+|B|.$$

2 Теорията в действие

Вече сме готови да решим задачата, която формулирахме в началото.

Решение: Нека в Z_p положим $A_d = \{0, 1^d, 2^d, \ldots, (p-1)^d\}$. Понеже уравнението $x^d - c = 0, c \neq 0$ няма повече от d корена в Z_p, то измежду числата $1^d, 2^d, \ldots, (p-1)^d$ поне $\frac{p-1}{d}$ са различни, значи $|A_d| \geq 1 + \frac{p-1}{d}$. Оттук според следствието от **T1** имаме $|A_d + A_d + \ldots + A_d|$ (d - пъти) $\geq min(d|A_d| - (d-1), p) = p$. В частност $n \in (A_d + A_d + \ldots + A_d)$ и задачата е решена. □

Коментар: Може да се докаже, че минималният полином на $f(A_d)$ над Q е от степен $m = (p-1, d)$. Това позволява да решим задачата без да използваме теоремите. За беда в общия случай $h(A) < deg_Q f(A)$, така че оценките с полиноми са слаби.

За да оправдаем смисъла от теоремите ще решим няколко задачи.

Задача[3] **2** A и B са два срещуположни върха в правилен $2p$-ъгълник, p - просто. От останалите върхове са маркирани $k \leq p$ и са прекарани всички диагонали (поне един) с маркирани краища, които пресичат AB. Да се докаже, че измежду тези диагонали има поне $k-1$, никои два от които не са успоредни или перпендикулярни.

Решение: Да номерираме точките по часовниковата стрелка от A (включително) към B съответно с $0, 1, \ldots, p-1$ и да ги наречем "леви" точки. Същото правим и с "десните" точки от B към A (в същата посока). Да вземем един от исканите диагонали с ляв и десен край съответно a_1 и b_1. Той е успореден на друг диагонал с краища a_2 и b_2 точно когато $a_1 + b_1 = a_2 + b_2$; перпендикулярен е пък ако $a_1 + b_1 = a_2 + b_2 \pm p$. Остава да цитираме **T1**. □

Задача 3 Дадено е просто число $p > 2$ и ненулеви полиноми $a(x), b(x), c(x)$ с коефициенти единици и степени по-малки от p. Да се докаже, че ако $a(1) + b(1) + c(1) = p + 2$, то

$$\sum_{i=0}^{p-1} a(\omega^i) b(\omega^i) c(\omega^i) > 0,$$

където ω е примитивен p-ти корен на 1.

Решение: Нека A е множеството, състоящо се от тези a, за които коефициентът пред x^a в $a(x)$ е ненулев. Аналогично дефинираме множествата B и C. От $a(1) + b(1) + c(1) = p + 2$ имаме $|A| + |B| + |C| = p + 2$, значи от следствието на **T1** $A + B + C \equiv D$. Последното показва, че $0 \in A + B + C$, и в развитието на $a(x)b(x)c(x)$ поне един от мономите x^0, x^p, x^{2p} участва с положителен коефициент. В същото време сумата в условието на задачата е именно $p\times$ сумата от коефициентите пред x^0, x^p и x^{2p}. □

Задача 4 (Контролно за малка Балканиада) Дадени са седем числа, които не се делят на седем. Да се докаже, че с произволните им суми можем да получим всеки остатък по модул седем.

Упътване: Ако числата са a_i разгледайте множествата $A_i \equiv \{0, a_i\}$.

[3] тази и следващата задачи са еквивалентни на **T1**

3 Някои специални множества

3.1 Геометрични прогресии

Да изследваме по-обстойно множествата A_d от първата задача. Нека ξ е примитивен корен в Z_p. За всяко $A \in D$ дефинираме $nA = A + A + \ldots + A$ (n-пъти) [4] и

$$h(d) = min\ n : nA_d \equiv D.$$

Ако $\delta = (p-1, d)$ то $\exists a, b \in \mathbb{Z} : (p-1)a + db = \delta$. Тогава за всяко $x \in D \backslash \{0\}$ и подходящо u

$$x^{\delta} = (\xi^u)^{\delta} = \xi^{(p-1)au+dbu} = (\xi^{bu})^d = y^d.$$

Също така $0^{\delta} = 0^d$. Обратно - $x^d = (x^{d/\delta})^{\delta} = y^{\delta}$, значи $A_{\delta} \equiv A_d$. Полагаме $m := \dfrac{p-1}{\delta}$. Да отбележим, че множеството A_{δ} по същество е

$$\{0, \xi^{\delta}, \xi^{2\delta}, \ldots, \xi^{m\delta}\}. \tag{20}$$

За δ има няколко възможности:

$$\delta = p-1 \Rightarrow A_{\delta} \equiv \{0, 1\} \Rightarrow h(p-1) = p-1,$$

$$\delta = \frac{p-1}{2} \Rightarrow A_{\delta} \equiv \{-1, 0, 1\} \Rightarrow h(\frac{p-1}{2}) = \frac{p-1}{2},$$

$$\delta = 2 \Rightarrow |A_{\delta}| = m + 1 = \frac{p+1}{2} \Rightarrow h(2) = 2,$$

$$\delta = 1 \Rightarrow A_{\delta} \equiv D \Rightarrow h(1) = 1.$$

Сега считаме $2 < \delta < \dfrac{p-1}{2}$, т.е.

$$3 \leq \delta \leq \frac{p-1}{3} \iff 3 \leq m \leq \frac{p-1}{3}. \tag{21}$$

Да предположим, че $\div A_{\delta}$, т.е. (предвид (20))

$$\exists a, t \in D : \{a, a+t, \ldots, a+mt\} \equiv \{0, \xi^{\delta}, \xi^{2\delta}, \ldots, \xi^{m\delta}\}. \tag{22}$$

От (21) имаме $\xi^{\delta} \neq \pm 1$ и значи от (22):

$$0 = \sum_{i=0}^{m} \xi^{i\delta} = \sum_{i=0}^{m} (a+it) = (m+1)a + \frac{m(m+1)}{2}t, \tag{23}$$

$$0 = \sum_{i=0}^{m} (\xi^{i\delta})^2 = \sum_{i=0}^{m} (a+it)^2 = (m+1)a^2 + \frac{m(m+1)(2m+1)}{6}t^2 + atm(m+1). \tag{24}$$

Тъй като $m+1, t \neq 0$ от (23) следва

$$at^{-1} = -m2^{-1}. \tag{25}$$

В (24) умножаваме двете страни с $t^{-2}(m+1)^{-1}$ и заместваме at^{-1} от (25):

$$-m^2 4^{-1} + m(2m+1)6^{-1} = 0.$$

Последното се свежда до $m = -2 \Rightarrow m = p-2$, което противоречи на (21). Следователно и еквивалентността (22) не е възможна.
Ще докажем

$$h(\delta) \leq \left\lfloor \frac{\delta}{2} \right\rfloor + 1. \tag{26}$$

[4] забележете разликата м/у cA и kA

Да предположим противното и нека $|kA_\delta| < p, k = 1, 2, \ldots, h(\delta) - 1$. Ще докажем с индукция по k, че $|kA_\delta| \geq (2k-1)m+1$. При $k = 1$ всичко е ясно. Нека сега $h(\delta) > k > 1$ и сме доказали, че $|(k-1)A_\delta| \geq (2k-3)m+1$. Разглеждаме биекцията $g : (kA_\delta \backslash \{0\}) \to (kA_\delta \backslash \{0\})$, дефинирана чрез $g(x) = \xi^\delta x$. Всяка орбита в тази биекция е с дължина m и затова

$$m \ / \ |kA_\delta| - 1. \tag{27}$$

Също $m/|(k-1)A_\delta| - 1, m/|A_\delta| - 1$. Тогава $|A_\delta| + |(k-1)A_\delta| \equiv 2 (mod\ m)$, а $p \equiv 1 (mod\ m)$, т.е. $|A_\delta| + |(k-1)A_\delta| \neq p$. Но $|A_\delta| + |(k-1)A_\delta| \leq |A_\delta + (k-1)A_\delta| + 1 \leq p - 1 + 1 = p$ и значи $|A_\delta| + |(k-1)A_\delta| < p$. Следователно, също предвид че A_δ не е аритметична прогресия, можем да приложим **T2** - резултат (v) - към множествата A_δ и $(k-1)A_\delta$. Така $|kA_\delta| \geq |A_\delta| + |(k-1)A_\delta| \geq m + 1 + (2k-3)m + 1 = (2k-2)m + 2$. Вече от (27) заключаваме $|kA_\delta| \geq (2k-1)m + 1$ и индукцията е завършена.

Остава да приложим резултата й за $k = h(\delta) - 1 \geq \left\lfloor \frac{\delta}{2} \right\rfloor + 1$:

$$p > |kA_\delta| \geq (2k-1)m + 1 \geq \delta m + 1 = p,$$

което е невъзможно. Противоречието дойде от допускането, че $h(\delta) > \left\lfloor \frac{\delta}{2} \right\rfloor + 1$. С това твърдението (26) е доказано.

При $\delta = 1, 2$ проверяваме, че (26) отново е в сила. Накрая можем да обобщим:

Теорема 3 *За всяко естествено число d е изпълнено*

$$h(d) \leq \left\lfloor \frac{(p-1, d)}{2} \right\rfloor + 1,$$

с изключение на случаите $(p-1, d) = \frac{p-1}{2}, p-1$, когато $h(d) = (p-1, d)$.

Следната задача илюстрира горния резултат.

Задача 5 Нека n е най-малкото естествено число, за което $2^n - 1$ се дели на простото $p > 3$. Тогава за всяко цяло d съществува цяло $D \in [1, 2^n]$, така че p дели $d + D$ и D има в двоичния си запис най-много $\left\lfloor \frac{p-1}{2n} \right\rfloor + 1$ единици.

Коментар: Ако заменим в условието оценката $\left\lfloor \frac{p-1}{2n} \right\rfloor + 1$ с $\frac{p-1}{n}$ задачата се облекчава значително и решението ползва единствено **T1**.

Ще отбележим, че множествата $A_d \backslash \{0\}$ са всички подгрупи на Z_p^* - мултипликативната група на Z_p.

3.2 Аритметични прогресии

Аритметичните прогресии - множествата $\div A$ - се описват лесно с комплексни числа. Нека ω е примитивен n-ти корен на 1. Дефинираме функцията $f : \{A | A \subset D\} \to R$ по следния начин:

$$f(A) = \sum_{a \in A} \omega^a.$$

Това, че полиномът $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$ е неразложим над Q, позволява да идентифицираме множествата с техните f-стойности, а именно: $A \equiv B \iff f(A) = f(B)$. Явно тогава от $\div A$ следва, че съществуват цели числа $a \in [0, p-1]$ и $d \in [1, p-1]$, такива че

$$f(A) = \omega^a + \omega^{a+d} + \omega^{a+2d} \ldots + \omega^{a+(m-1)d} = \frac{\omega^{a+md} - \omega^a}{\omega^d - 1},$$

където $m = |A|$. При $m = 1, p-1$ всичко е ясно. Считаме $1 < m < p-1$ - ще покажем, че има точно две двойки $\{a, d\}$ задаващи A. Нека

$$\frac{\omega^{a+md} - \omega^a}{\omega^d - 1} = f(A) = \frac{\omega^{a'+md'} - \omega^{a'}}{\omega^{d'} - 1}.$$

Прехвърляме всичко от едната страна, помнейки, че всеки едночлен на ω със знак "+" трябва да се съкрати със същия със знак "-":

$$\omega^{a+md+d'} + \omega^a - \omega^{a+md} - \omega^{a+d'} - \omega^{a'+md'+d} - \omega^{a'} + \omega^{a'+md'} + \omega^{a'+d} = 0.$$

Понеже $\omega^a \neq \omega^{a+md}, \omega^{a+d'}$ и $\omega^{a+md+d'} \neq \omega^{a+md}, \omega^{a+d'}$ то или

$$\{\omega^{a+md+d'}, \omega^a\} = \{\omega^{a'+md'+d}, \omega^{a'}\},$$

или

$$\{\omega^{a+md+d'}, \omega^a\} = \{\omega^{a'}, \omega^{a'+md'+d}\},$$

като горните двойки са наредени. Първата възможност води до $\omega^{(m-1)(d-d')} = 1$, т.е. $d = d', a = a'$; втората води до $\omega^{(m+1)(d+d')} = 1$, а значи и $d' = p-d, a' \equiv a+(m-1)d \ (mod\ p)$. Това показва, че всяко множество $\div A : 1 < |A| < p-1$ се задава единствено чрез двойките $\{a, d\}, \{a', p-d\}$. Не е трудно оттук да се съобрази свойство [4], което обещах да не използваме.
Един интересен факт - броят на всички множества $\div A, A \subset D$ е

$$p + \frac{p(p-1)(p-3)}{2} + p = \frac{p(p^2-4p+7)}{2}.$$

Аритметични прогресии можем да дефинираме за всякакво естествено число p, не задължително просто. Но при съставно p и двете теореми губят вярност: ако $p = mn$, където $m, n > 1$, и

$$\div A = \{0, n, 2n, \ldots, (m-1)n\},$$

то $A + A = A$ и $m = |A| = |A + A| < |A| + |A| - 1$, но $A + A \not\equiv D$. За сметка на това обаче (съобразете) и двете теореми остават в сила над Z, стига да премахнем ограниченията, касаещи по някакъв начин p. Последното ще го формулираме като теорема, чието доказателство предоставяме на читателя.

Теорема 4 *За всеки две множества A и B от цели числа е изпълнено*

$$|A + B| \geq |A| + |B| - 1,$$

като равенство при $|A|, |B| > 1$ се достига точно когато A и B са аритметични прогресии с еднаква разлика.

Ще приключим темата с една задача за аритметични прогресии в Z_p.

Задача 6 Нека $p > 5$ е просто число, а d и n са цели числа, такива че $2 \leq d \leq p-2$ и $3 \leq n \leq p-3$. Известно е, че за някое цяло a за всяко едно от числата $a + jd, j = 1, 2, \ldots, n$, съществува цяло число b_j, $0 \leq b_j \leq n$, така че $b_j \equiv a + jd (mod\ p)$. Да се докаже, че $n = p-3$.

Упътване: Разгледайте $a + jd$ геометрично като точки от окръжност.

$\diamondsuit\diamondsuit\diamondsuit$