Erdős-Ginzburg-Ziv

Tétel. $2n-1$ egész szám között mindig kiválasztható n, aminek az összege osztható n-nel.

Bizonyítás. Először belátjuk, hogy ha az állítás igaz n-re és m-re, akkor igaz nm-re. Ha adva van $2nm-1$ egész szám, akkor, nézve például az első $2n-1$-et, található n, aminek az összeg osztható n-nel. Ezt az n számot félretéve, a maradékban ismét találhatunk n-et, amelyeknek az összege n-nel osztható. Ezeket ismét félretéve, az eljárást addig folytathatjuk, amíg a megmaradt számok száma $2n-1$ alá nem csökken. Ez akkor fordul elő, amikor már $2m-1$ olyan csoportot kiválasztottunk, amelyek mindegyike n darab számból áll úgy, hogy összegeik az n-nel osztható $na_1, na_2, \ldots, na_{2m-1}$ számok. Ezután az állítás m-re vonatkozó esetét alkalmazva kapunk az $a_1, \ldots, a_{2n-1}$ számok között m-et, amelyeknek az összege osztható m-mel, ez az eredeti számokra azt jelenti, hogy találtunk mn-et, amelyeknek az összege osztható mn-nel.

A fenti megjegyzés miatt elég az állítást prímekre igazolni.

Legyen tehát p prímszám, és legyenek adva az $a_1, \ldots, a_{2p-1}$ egész számok. Készen vagyunk, ha van p vagy több olyan szám, ami azonos maradékot ad (közülük p összege nyilvánvalóan osztható p-vel). Feltehetjük tehát, hogy minden maradékosztályba legfeljebb $p-1$ esik számaink közül.

Ha $2t-1 > 3$ szám adott, akkor legfeljebb 2 olyan maradékosztály lehet, amibe $t-1$ elem esik, hiszen $2t-1 < 3(t-1)$.

Ezért a következőt csináljuk. A $2p-1$ számból kiválasztunk egyet-egyet a két legnagyobb (legtöbb elemet tartalmazó) maradékosztályból: b_1 és c_1. A megmaradt $2p-3$ szám ezután úgy helyezkedik el, hogy minden maradékosztályban legfeljebb $p-2$ szám van, ismét kiválasztunk egy-egy elemet a két legnagyobb maradékosztályból: b_2 és c_2. Ezt folytatva egészen addig jutunk, amíg csak három elem marad, ezek között van két inkongruens, legyenek ők b_{p-1} és c_{p-1}. Az utolsó elem pedig a.

Tehát elrendeztük a számokat így:

$$\begin{array}{ccccccc} b_1 & b_2 & b_3 & \ldots & b_{p-1} & & \\ & & & & & a & \\ c_1 & c_2 & c_3 & \ldots & c_{p-1} & & \end{array}$$

úgy, hogy az egymás felett lévő b_i, c_i számok inkongruensek mod p.

Ezután belátjuk, hogy $1 \leq t \leq p-1$-re legalább $t+1$ különböző maradékot kapunk, ha vesszük azokat az összegeket, amelyek tartalmazzák a-t, és minden $1 \leq i \leq t$-re b_i és c_i közül pontosan az egyiket tartalmazzák.

$t = 1$-re ez világos: mivel $b_1 \not\equiv c_1 (p)$, $b_1 + a$ és $c_1 + a$ két különböző maradék. Tegyük fel, hogy t-re tudjuk az állítást; a megadott módon készíthető összegek maradékok legalább $t+1$ elemű A halmazát adják. A $t+1$-re kszített összegek a következő alakúak: $x + b_{t+1}$ vagy $x + c_{t+1}$, ahol $x \in A$. Azt kell tehát belátni, hogy

$$\{x + b_{t+1} : x \in A\} \cup \{x + c_{t+1} : x \in A\}$$

elemszáma legalább $t + 2$. Ha az első halmazt B-vel jelöljük, akkor, mivel B A-nak elforgatottja, $|B| = |A| \geq t+1$. A második halmaz B-nek elforgatottja a mod p nemnulla $y = c_{t+1} - b_{t+1}$ értékkel, ezért ez is $|A|$ elemű. A két halmaz egyesítése csak akkor nem nagyobb náluk, ha az y-nal való forgatás egymásba viszi őket. Azaz, ha $x \in B$, akkor $x+y \in B$. De ekkor $x+2y, x+3y, \ldots \in B$, és így az összes maradékot megkapjuk mod p, azaz B minden maradékot tartalmaz.

A fenti állítást $t = p - 1$-re alkalmazva, azt kapjuk, hogy mod p a nulla maradék elő áll olyan összegként, amiben szerepel a és minden i-re b_i vagy c_i. De ez p tagú összeg.