Háromszögszámok és négyzetszámok összegéről

Maga Balázs és Török Mihály

1 Bevezető

Az alábbiakban azzal fogunk foglalkozni, hogy mely számok állnak elő két négyzetszám összegeként, illetve melyek két háromszögszám összegeként. Az előbbi jobban ismert téma, de azért röviden felvázoljuk. Az utóbbi ehhez szorosan kapcsolódik, mint látni fogjuk. Emellett foglalkozunk a két kisebb négyzetszám összegeként előálló négyzetszámokkal, valamint a két kisebb háromszögszám összegeként előálló háromszögszámokkal. Végezetül eme négy számhalmaznak egyfajta sűrűségével fogunk foglalkozni új definíciók alapján.

2 Számok két négyzetszám összegeként

Kiindulási pontunk az a tény lesz, hogy ez a tulajdonság multiplikatív, azaz ha n_1 és n_2 felírható két négyzetszám összegeként, akkor n_1n_2 is. Ez könnyen látható:

$$n_1 = a_1^2 + b_1^2$$

$$n_2 = a_2^2 + b_2^2$$

$$n_1n_2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = a_1^2a_2^2 + a_1^2b_2^2 + b_1^2a_2^2 + b_1^2b_2^2 = (a_1a_2 + b_1b_2)^2 + (a_1b_2 - b_1a_2)^2$$

Így ha bizonyos prímekről belátjuk, hogy előállnak két négyzetszám összegeként, akkor tetszőleges olyan szám, amit csak ezen prímek osztanak, nyilván előáll hasonló módon. Meg fogjuk hát vizsgálni, mely prímek állnak elő két négyzetszám összegeként.

Ha p prímre $p = a^2 + b^2$, akkor nyilván sem a, sem b nem osztható p-vel. Először tehát vizsgáljuk azt a gyengébb állítást, hogy egyáltalán mely prímeknek van olyan többszörösük, ami felírható ezen prímmel nem osztható négyzetszámok összegeként. Ekkor tehát $a^2 \equiv -b^2 \bmod p$. b^2-tel leosztva $(\frac{a}{b})^2 = -1 \bmod \text{p}$. Tehát az a kérdés, mely prímekhez van olyan négyzetszám, hogy annak p-s maradéka -1, szakszerűbben fogalmazva mely prímekre kvadratikus maradék a -1. $4k+3$ alakú prímekre nem lehet. Válasszunk ki ugyanis mod $4k+3$ egy tetszőleges nemkvadratikus maradékot, m-et. Ilyen maradék nyilván létezik, mivel $4k + 2$ 0-tól eltérő maradék van, és mivel $m^2 = (-m)^2$, így minden maradéknak és ellentettjének ugyanaz a négyzete, azaz a nemnulla maradékok fele biztosan nemkvadratikus. Tekintsük most m^{2k+1}-t. Ez m^{4k+2}-nek a négyzetgyöke, ami a Kis Fermat-tétel alapján p-vel osztva 1-et ad maradékul, tehát $m^{2k+1} \equiv \sqrt{1} \bmod p$. Hány gyöke van az 1-nek mod p, illetve általában egy kvadratikus maradék hány különböző maradék négyzeteként jöhet létre, ez az, amire most kíváncsiak vagyunk. Tegyük fel hát, hogy $a^2 \equiv b^2 \bmod p$. Rendezve $(a-b)(a+b) \equiv 0 \bmod p$. Mivel p prím, ezért ha a szorzatot osztja, valamelyik tényezőjét is osztja. Azaz vagy $a \equiv b \bmod p$, vagy $a \equiv -b \bmod p$. Ennélfogva egy kvadratikus maradéknak általában, s így az 1-nek is két gyöke van. Az 1 esetén ezek ismertek: az 1 és a -1. Tehát $m^{2k+1} \equiv 1$ vagy $m^{2k+1} \equiv -1 \bmod p$. Ha az előbbi teljesül, akkor $m \equiv (\frac{1}{m^k})^2 \bmod p$, azaz m kvadratikus maradék, ami ellentmond a kiindulási feltételünknek. Tehát $m^{2k+1} \equiv -1 \bmod p$. Ha $-1 \equiv x^2$, azaz a -1 kvadratikus maradék mod p, akkor $m \equiv (\frac{x}{m^k})^2$, s ugyanúgy ellentmondásra jutunk, mint az imént. Tehát a -1 nemkvadratikus maradék mod p, ha p egy $4k + 3$ alakú prím. Tehát ha egy n szám két négyzetszám összege, és osztható $4k + 3$-mal, azaz $(4k + 3)n_1 = a^2 + b^2$, akkor a és b is osztható $4k + 3$-mal, azaz $a = (4k + 3)a_1$, $b = (4k + 3)b_1$. Behelyettesítve $(4k + 3)n_1 = (4k + 3)^2a_1^2 + (4k + 3)^2b_1^2$. $4k+3$-mal leosztva a jobb oldal továbbra is osztható lesz $4k+3$-mal, tehát a bal oldalnak is oszthatónak kell lennie. Ennélfogva $n = (4k+3)n_1 = (4k+3)^2 n_2$. Ezt behelyettesítve az iménti egyenletünkbe leoszthatunk $(4k+3)^2$-nel, s az eredmény $n_2 = a_1^2 + b_1^2$. Amennyiben n_2 is osztható $4k+3$-mal, akkor ismét elvégezhető az előbb látott lépes. Tehát n_2 is osztható $(4k+3)^2$-nel. Ezt az algoritmust folytathatjuk addig, amíg a $(4k+3)^2$-nel való osztások eredményeképp egy olyan számot kapunk, ami nem osztható $4k+3$-mal. Azaz ha n felírható két négyzetszám összegeként, és prímtényezős felbontásában van $4k+3$ alakú prím, akkor az páros kitevőn szerepel. Másrészt $(4k+3)^{2m} = ((4k+3)^m)^2 + 0^2$, így a multiplikáció alapján ez elégséges feltétel n egy $4k+3$ alakú prímosztójával kapcsolatban.

$p = 2$-re a -1 kvadratikus maradék: $1^2 = 1 \equiv -1 \bmod 2$. Már csak a $4k+1$ alakú prímeket kell megvizsgálni. Ekkor a Wilson-tétel alapján:

$$-1 \equiv (p-1)! \equiv (4k)! \equiv 1 * 2 * ... * 2k * (-2k) * (-2k+1) * ... * (-2) * (-1) \equiv (1 * 2 * ... * 2k)^2 * (-1)^{2k}$$

Tehát a -1 két négyzetszám szorzata mod $4k+1$, azaz ő maga is kvadratikus maradék. Tehát a 2-nek és a $4k+1$ alakú prímeknek van olyan többszörösük, ami előáll két, p-vel nem osztható négyzetszám összegeként. $p = 2$ esetén triviális, hogy konkrétan p is előall: $2 = 1^2 + 1^2$. Így már csak $p = 4k+1$-re kell belátnunk ugyanezt. Ezt kétféleképpen fogjuk megtenni: skatulyaelvvel és végtelen leszállással.

1. *Bizonyítás.* Azt használjuk ki, hogy létezik i maradékosztály mod p, amire $i^2 \equiv -1 \bmod p$. Vizsgáljuk az $x + yi$ kifejezést minden olyan x, y egészekből álló számpárra, ahol $0 \leq x, y < \sqrt{p}$. Tehát összesen $(\lfloor\sqrt{p}\rfloor + 1)^2$ kifejezést vizsgálunk. Minthogy $\sqrt{p}$ egy prím négyzetgyöke, bizonyosan nem egész. Tehát $\lfloor\sqrt{p}\rfloor + 1 > \sqrt{p}$, következésképp a vizsgált kifejezések száma nagyobb, mint p. Tehát van kettő, ami azonos maradékot ad p-vel osztva:

   $$x_1 + y_1 i \equiv x_2 + y_2 i$$

   Rendezve, majd négyzetre emelve:

   $$(x_1 - x_2)^2 \equiv -i^2 (y_2 - y_1)^2$$

   Kihasználva, hogy $i^2 \equiv -1 \bmod p$:

   $$(x_1 - x_2)^2 + (y_2 - y_1)^2 \equiv 0$$

   Legyen $X = |x_1 - x_2|$, $Y = |y_2 - y_1|$. Ekkor az X, Y számok legalább egyike eltér 0-tól, hiszen ellenkező esetben az x_1, y_1 és az x_2, y_2 számpárok egyeznének. Ugyanakkor $X, Y < \sqrt{p}$. Tehát $0 < X^2 + Y^2 < 2p$, és $p | X^2 + Y^2$, hiszen $X^2 + Y^2 = (x_1 - x_2)^2 + (y_2 - y_1)^2 \equiv 0 \bmod p$. Ennélfogva $X^2 + Y^2 = p$, s nyilván nem osztható X és Y is p-vel, hiszen ekkor négyzetösszegük osztható lenne p^2-tel. Tehát ha p egy $4k+1$ alakú prím, akkor két hozzá relatív prím egész négyzetének összege, amit bizonyítani akartunk. □

2. *Bizonyítás.* Annyit használunk fel, hogy létezik q, a, b, hogy $qp = a^2 + b^2$, ahol $q > 1$ egész ($q = 1$ esetén ugyebár készen vagyunk), és sem a, sem b nem osztható p-vel. Azt nyilván feltehetjük, hogy $a, b < p$, hiszen csak a^2 és b^2 $p-s$ maradéka számit, ami a-t vagy b-t p-vel arrébb léptetve nyílván változatlan. Ennél azonban több is feltehető: nevezetesen hogy $a, b < \frac{p}{2}$. Ugyanis $\frac{p}{2}$ és p között ugyanazok a kvadratikus maradékok fordulnak elő, mint 0 és $\frac{p}{2}$ között, tekintettel arra, hogyha $0 < x < \frac{p}{2}$, akkor $\frac{p}{2} < p - x < p$, és $x^2 \equiv (p-x)^2 \bmod p$. Ebből következik, hogy $0 < qp = a^2 + b^2 \leq \frac{p^2}{2} < p^2$, tehát $0 < q < p$, azaz $(q, p) = 1$. Most már ezt is tudjuk. A továbbiakban legyen $A \equiv a$, $B \equiv b \bmod q$, mégpedig úgy, hogy mind A, mind B abszolút értéke a lehető legkisebb legyen. Ekkor $|A|, |B| \leq \frac{q}{2}$, következésképp $A^2 + B^2 \leq \frac{q^2}{2} < q^2$. Ekkor teljesülnek a következő kongruenciák mod q:

   $$aA + bB \equiv a^2 + b^2 \equiv 0$$

   $$aB - bA \equiv ab - ba \equiv 0$$

   Tehát az $(\frac{aA+bB}{q})^2$ és az $(\frac{aB-bA}{q})^2$ számok egészek. Másrészt összegüknek van számunkra két igen kedves tulajdonsága, ami a következő felírásból látszik:

   $$\left(\frac{aA+bB}{q}\right)^2 + \left(\frac{aB-bA}{q}\right)^2 = \frac{(aA)^2 + (bB)^2 + (aB)^2 + (bA)^2}{q^2} = \frac{A^2+B^2}{q^2} * (a^2+b^2) = \frac{A^2+B^2}{q^2} * qp$$

Mivel $(q, p) = 1$, az utolsó kifejezésből következik, hogy ez a négyzetösszeg is osztható p-vel. Másreszt viszont kisebb, mint qp, ugyanis qp-t egy 1-nél kisebb számmal szorozzuk (ugyanakkor nyílván pozitív). Tehát létezik $0 < q' < q$, amire $q'p$ felírható két négyzetszám összegeként. Ha most $q' = 1$ akkor készen vagyunk. Ha nem, akkor megismételhető $q'p$-re a fenti lépes, s ezáltal p együtthatója tovább csökkenthető. Mivel ez az együttható legfeljebb $p-1$ volt eredetileg, és a továbbiakban is pozitív egész marad, legfeljebb $p-2$ lépésben eléri az 1-et. Tehát ha p egy $4k+1$ alakú prím, akkor két hozzá relatív prím szám négyzetének összege, amit bizonyítani akartunk. □

Tehát a 2 és a $4k + 1$ alakú prímek felírhatóak két négyzetszám összegeként. Az eddigiekből következik, hogy általában mely számoknak van meg ez a tulajdonsága: pontosan azoknak, melyek prímtényezős felbontásában minden $4k + 3$ alakú prím páros kitevőn szerepel.

Két négyzetszám összegeként előálló prímekről mutatunk be még egy kevésbé ismert tételt.

Állítás 1. *Ha egy prím felírható két négyzétszám összegeként, akkor ez a felírás egyértelmű.*

Bizonyítás. Tegyük fel, hogy nem egyértelmű a felírás egy bizonyos p prímre. Ekkor $p = a^2 + b^2 = c^2 + d^2$, ahol a, b, c, d pozitív egészek, és $a \neq c$, $a \neq d$. Ekkor:

$$(ad + bc)(ad - bc) = a^2d^2 - b^2c^2 = a^2d^2 + b^2d^2 - b^2d^2 - b^2c^2 = (a^2 + b^2)d^2 - (c^2 + d^2)b^2 = p(d^2 - b^2)$$

Tehát $p|(ad + bc)(ad - bc)$. Tehát $p|ad + bc$ vagy $p|ad - bc$. A feltételekből egyértelműen adódik, hogy $0 < a, b, c, d < \sqrt{p}$. Tehát ha $p|ad+bc$, akkor $ad+bc = p$, ha $p|ad-bc$, akkor $ad-bc = 0$. Ezeket külön-külön vizsgáljuk meg.

Ha $ad - bc = 0$, akkor $ad = bc$. $a|bc$, másrészt $(a, b) = 1$, tehát $c = ma$. Eszerint $d = mb$, tehát $p = c^2 + d^2 = (ma)^2 + (mb)^2 = a^2 + b^2$. Tehát $m = 1$, $a = c$, $b = d$, ellentmondásra jutottunk.

Ha $ad + bc = p$, akkor $p^2 = (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 = p^2 + (ac - bd)^2$. Tehát $ac - bd = 0$, azaz $ac = bd$. Így azonban ellentmondásra jutunk, hiszen ez lényegileg azonos az imént taglalt ellentmondásra vezető $ad = bc$ egyenlőséggel, ugyanis a szimmetrikus szerepű c, d változókat cseréltük fel. Ezzel készen vagyunk. □

A téma zárásaképp egy egyszerű lemmát közlünk és igazolunk:

Állítás 2. *Mind $4k + 1$, mind $4k + 3$ alakú prímből végtelen sok van.*

Bizonyítás. Elsőként a $4k + 3$ alakú prímek végtelen számosságat bizonyítjuk. Tegyük fel, hogy csak véges sok ilyen prím van: p_1, p_2, ..., p_n. Tekintsük az $N = 2p_1p_2...p_n + 1$ számot. Ez egyrészt 3 maradékot ad 4-gyel osztva, mivel $2p_1p_2...p_n$ egy páratlan szám 2-szerese, így 4-es maradéka 2. Tehát N-nek nem lehetnek kizárólag $4k+1$ alakú osztói, mivel azok szorzata csak 1 maradékot adhat 4-gyel osztva. Másrészt viszont sem 2-vel, sem a $4k + 3$ alakú prímekkel nem osztható N, mivel az összessel 1 maradékot ad, ami ellentmondás. Tehát $4k+3$ alakú prímből valóban végtelen sok van. Most tegyük fel, hogy $4k+1$ alakú prímből csak véges sok van: q_1, q_2, ..., q_n. Tekintsük az $M = (2q_1q_2...q_n)^2 + 1$ számot. Ennek nem lehetnek $4k+3$ alakú osztói, hiszen két négyzetszám összege, és egyik tagnak sincs $4k + 3$ alakú osztója. Ugyanakkor sem 2-vel, sem a $4k + 1$ alakú prímekkel nem osztható, mivel az összessel 1 maradékot ad, ami ellentmondás. Tehát $4k + 1$ alakú prímből is végtelen sok van, amit bizonyítani akartunk. □

Megjegyzés: ezen lemmában állítottak a Dirichlet-tételnek speciális esetei, miszerint minden számtani sorozat végtelen sok prímet tartalmaz, ha kezdőtagja és differenciája relatív prím. Az érdeklődő Szalay Mihály: Számelmélet című könyvében találhat rá bizonyítast.

3 Négyzetszámok két kisebb négyzetszám összegeként

Állítás 3. *Egy négyzetszám, jelölje n^2, pontosan akkor írható fel két kisebb négyzetszám összegeként, ha n prímtényezős felbontásában van $4k + 1$ alakú prím.*

Bizonyítás. Először azt az irányt igazoljuk, hogy ha n prímtényezős felbontásában van $4k+1$ alakú prím, akkor n^2 két kisebb négyzetszám összege. Ekkor n felírható a következőképpen: $n = p{*}m$, ahol p ez a bizonyos $4k+1$ alakú prím, m pedig egy egész szám. Tehát $n^2 = p^2 * m^2$. Az előző részben áttekintettek alapján léteznek a, b pozitív egészek, amikre $p = a^2 + b^2$, ahol továbbá bizonyosan $a \neq b$, mivel négyzetösszegük páratlan. Így a multiplikációs tulajdonságot kihasználva:

$$p^2 = (a^2 + b^2)^2 = (a^2 - b^2)^2 + (2ab)^2$$

Azaz p^2 is pozitív számok négyzetösszege. Tehát $a' = a^2 - b^2$, $b' = 2ab$ helyettesítést alkalmazva:

$$n^2 = (a'^2 + b'^2) * m^2 = (a'm)^2 + (b'm)^2$$

Mivel az a', b', m számok mindegyike pozitív, ezért ez a felírás n^2 két kisebb négyzetszám összegére való bontása. Tehát valóban, ha n prímtényezős felbontásaban van $4k+1$ alakú prím, akkor n^2 felírható két kisebb négyzetszám összegeként. Ezzel az egyik iránnyal készen vagyunk, következzék a másik. Indirekte tegyük fel, hogy n prímtényezős felbontásában kizárólag a 2 és $4k+3$ alakú prímek szerepelnek, s n^2 mégis előáll két kisebb négyzetszám összegeként. Tehát $n^2 = a^2 + b^2$, ahol a, b pozitív egészek. Vegyük a legkisebb, ezen feltételeknek megfelelő pozitív n-t. Válasszuk ki n egy tetszőleges p prímosztóját. Ekkor p a-t és b-t is kénytelen osztani: ha p egy $4k+3$ alakú prím, akkor a már korábban látottak miatt, nevezetesen hogy a -1 nem kvadratikus maradék mod p, így két négyzetszám összege csak akkor osztható $4k+3$-mal, ha mindkét tag osztható $4k+3$-mal; ha pedig $p = 2$, akkor n^2 osztható 4-gyel, márpedig mod 4 csak a 0 és az 1 kvadratikus maradék, így $a^2 + b^2$ csak akkor lehet osztható 4-gyel, ha $a^2 \equiv b^2 \equiv 0$ mod 4, azaz $a \equiv b \equiv 0$ mod 2. Tehát ha $p|n$, akkor $p|a, b$, így ha $n = pN$, $a = pA$, $b = pB$, akkor ezt a jelölésrendszert alkalmazva p^2-tel leosztva az egyenlőséget $N^2 = A^2 + B^2$-t kapunk. Ekkor N-nek csak olyan prímosztói lehetnek, amik n-t is osztották, azaz N-nek sincs $4k+1$ alakú prímosztója. Másrészt, mivel $p > 1$, $0 < N < n$. Mindezek alapján ellentmondásra jutottunk azon feltételünkkel, hogy az n a legkisebb olyan pozitív egész, aminek nincs $4k+1$ alakú prímosztója, s n^2 felírható két kisebb négyzetszám összegeként. Ezzel igazoltuk a másik irányt is. □

Ennek a témának geometriai vonatkozása is van. A Pitagorasz-tétel alapján ugyanis egy derékszögű háromszögben, ha az átfogó hosszát c, a befogókét pedig a és b jelöli, akkor $c^2 = a^2 + b^2$, és fordítva, azaz ha $c^2 = a^2 + b^2$, akkor az a, b, c oldalhosszokkal derékszögű háromszög szerkeszthető. Tehát az imént azon egészeket kerestük meg, amik lehetnek egész oldalú derékszögű háromszög átfogói. A fentieket másképp fogalmazva azon számok ilyenek, amelyek két pozitív szám négyzetösszegének többszörösei, azaz ha $n = (a^2 + b^2)m$. Lehetséges egész befogóhosszokat jelent az $(a^2 - b^2)m, 2abm$ számpár, hiszen:

$$((a^2 - b^2)m)^2 + (2abm)^2 = (a^4 + 2a^2b^2 + b^4)m^2 = ((a^2 + b^2)m)^2 = n^2$$

4 Számok két háromszögszám összegeként

Definíció 4.1. *Legyen n nemnegatív egész szám. Az n. háromszögszámot jelölje h_n. Ekkor $h_n = 0 + 1 + 2 + \ldots + n$. A háromszögszám elnevezés abból a tényből következik, hogy h_n darab pontból egy háromszög rakható ki, mégpedig úgy, hogy az újabb sorokba mindig eggyel több pontot teszünk. Értékük expliciten is megadható a jól ismert képlettel az első n szám összegére: $h_n = \frac{n(n+1)}{2}$.*

Állítás 4. *Tetszőleges n pozitív egész akkor és csak akkor áll elő két háromszögszám összegeként, ha $4n+1$ prímtényezős felbontásában a $4k+3$ alakú prímek páros kitevőn szerepelnek.*

Bizonyítás. Tegyük fel, hogy n előáll két háromszögszám összegeként. Formálisan:

$$n = h_a + h_b = \frac{a(a+1)}{2} + \frac{b(b+1)}{2}$$

Szorozzunk fel 4-gyel, és adjunk 1-et mindkét oldalhoz:

$$4n + 1 = 2a^2 + 2a + 2b^2 + 2b + 1 = (a + b + 1)^2 + (a - b)^2$$

Tehát ha n felírható két háromszögszám összegeként, akkor $4n+1$ felírható két négyzetszám összegeként, azaz prímtényezős felbontásában a $4k+3$ alakú prímek páros kitevőn szerepelnek. Ezzel az egyik irányt bizonyítottuk. Most jöhet a másik irány: tegyük fel, hogy $4n+1$ prímtényezős felbontásában a $4k+3$ alakú prímek páros kitevőn szerepelnek. Ekkor előáll két négyzetszám összegeként. A kvadratikus maradékok mod 4 a 0 és az 1. Tehát ha egy $4n+1$ alakú szám előáll két négyzetszám összegeként, az csak úgy lehetséges, ha az egyik 4-gyel osztva 0, a másik pedig 1 maradékot ad, azaz az egyik egy páros szám négyzete, a másik egy páratlané. Tehát:

$$4n+1=(2p)^2+(2q+1)^2$$

Itt most p és q egymáshoz mért viszonyától függően választunk a-t és b-t, mi ugyanis nemnegatív a-t és b-t szeretnénk (p és q nemnegativitása triviálisan elérhető). Legyen tehát $a=p+q$, és legyen $b=p-(q+1)$, ha $q \leq p-1$, $b=q-p$, ha $q \geq p$. Ezzel garantáltuk, hogy a és b nemnegatívak (ez a hozzárendelés nem csak p,q-hoz rendel egyértelműen a,b-t, minden a,b csak egyszer fordulhat elő, mivel az egyik esetben $a+b$ páratlan, a másikban páros, így nem lehet egyezés). Ez alapján az egyik esetben $2p=a+b+1$, $2q+1=a-b$, a másikban pedig épp fordítva, $2p=a-b$, $2q+1=a+b+1$. Behelyettesítve azonban mindenképp:

$$4n+1=(a+b+1)^2+(a-b)^2=2a^2+2a+2b^2+2b+1$$

1-et levonva és 4-gyel osztva:

$$n=\frac{a(a+1)}{2}+\frac{b(b+1)}{2}=h_a+h_b$$

Tehát n felírható két háromszögszám összegeként. Készen vagyunk. □

Ennek nyilvánvaló következménye, hogy végtelen sok pozitív egész van, ami nem áll elő két háromszögszám összegeként, továbbá olyanból is végtelen sok van, ami előáll. Előbbire végtelen sok példát jelent két különböző $4k+3$ alakú prím szorzataként kapott $4n+1$ alakú számból generált n, utóbbira pedig $4k+3$ alakú prímek négyzeteként kapott $4n+1$ alakú számból generált n.

5 Háromszögszámok két kisebb háromszögszám összegeként

Örömmel adnánk explicit formulát arra, hogy mely háromszögszámok állnak elő két háromszögszám összegeként, ez azonban meglehetősen nehéz feladat: mint azt látni fogjuk, egyszerűbbnek tűnő kérdések is megválaszolatlanok még.

Állítás 5. *Végtelen sok háromszögszám előáll két, nála kisebb háromszögszám összegeként.*

Bizonyítás. Explicit formulát adunk két maradékosztályra is mod 5. Ez nyilván elegendő, már egy is elég lenne, egy későbbi eredmény érdekében adunk meg kettőt. A következő egyenlőségek könnyen ellenőrizhetőek a zárójelek felbontásával:

$$\frac{(5k+1)(5k+2)}{2}=\frac{(4k+1)(4k+2)}{2}+\frac{3k(3k+1)}{2}$$

$$h_{5k+1}=h_{4k+1}+h_{3k}$$

$$\frac{(5k+3)(5k+4)}{2}=\frac{(4k+2)(4k+3)}{2}+\frac{(3k+2)(3k+3)}{2}$$

$$h_{5k+3}=h_{4k+2}+h_{3k+2}$$

Tehát az $5k+1$. és az $5k+3$. háromszögszámok egy apró kivételtől eltekintve felírhatóak két kisebb háromszögszám összegeként. Ezt az apró kivételt az első háromszögszám jelenti, ami ezen explicit felírás szerint a 0. és az első háromszögszám összege. Egyébként viszont nem ütközünk ilyen problémába. □

Könnyen meggondolható, ebből következik, hogy 3 egymást követő háromszögszámból legalább egy mindig felírható kisebb háromszögszámok összegeként.

Természetes s talán egyszerű kérdésnék hat ezek után, hogy vajon létezik-e végtelen sok olyan háromszögszám, ami nem írható fel két pozitív háromszögszám összegeként. Ez a kérdés itt nem válaszoltatik meg: mind a mai napig megoldatlan probléma. Egyfajta elindulást azonban mutatunk, szükséges és elégséges feltételt adunk arra, hogy egy háromszögszám előálljon két kisebb háromszögszám összegeként Tegyük fel, hogy az n. háromszögszám felírható két pozitív háromszögszám összegeként. Ekkor:

$$h_n = h_a + h_b$$

Itt $a, b > 0$. Kifejtve:

$$\frac{n(n+1)}{2} = \frac{a(a+1)}{2} + \frac{b(b+1)}{2}$$

Alkalmazzuk az imént is hasznos trükköt: szorozzunk fel 4-gyel és adjunk hozzá mindkét oldalhoz 1-et.

$$2n^2 + 2n + 1 = 2a^2 + 2a + 2b^2 + 2b + 1$$

Mindkét oldal felírható négyzetszámok összegeként:

$$n^2 + (n+1)^2 = (a+b+1)^2 + (a-b)^2$$

Tehát a $2n^2 + 2n + 1$ egy olyan szám, ami legalább kétféleképpen felírható két négyzetszám összegeként. Könnyen látható, hogy ez elégséges feltétel is egyúttal: ekkor ugyanis az egyik lehetséges felírás nyilván a $n^2 + (n+1)^2$, s ha létezik egy másik is, az 4-es maradék alapján ($2n^2 + 2n + 1 \equiv 1 \bmod 4$) egy páratlan és egy páros szám négyzetének az összege. Tehát:

$$2n^2 + 2n + 1 = 4m + 1 = (2p)^2 + (2q+1)^2$$

Ez éppen az az alak, amit már láttunk az 1. állítás bizonyításánál, tehát megfelelő helyettésítéssel:

$$2n^2 + 2n + 1 = 4m + 1 = (a+b+1)^2 + (a-b)^2 = 2a^2 + 2a + 2b^2 + 2b + 1$$

Azaz:

$$\frac{n(n+1)}{2} = \frac{a(a+1)}{2} + \frac{b(b+1)}{2}$$

Ami éppen azt jelenti, hogy $h_n = h_a + h_b$.

Jól látszik, hogy éppen akkor forog ki az $n^2 + (n+1)^2$ eset, amikor $b = 0$. Tehát az n. háromszögszám pontosan akkor írható fel két pozitív háromszögszám összegeként, ha $2n^2 + 2n + 1$ a triviális $n^2 + (n+1)^2$ felírás mellett másképpen is felírható két négyzetszám összegeként.

Mi arra vagyunk tehát kíváncsiak, hogy van-e végtelen sok $2n^2+2n+1$ alakú szám, ami csak egyféleképpen írható fel két négyzetszám összegeként. Milyen prímtényezői lehetnek $2n^2 + 2n + 1$-nek? A 2 nyilván nem. Tegyük fel, hogy van $4k+3$ alakú osztója. Tehát $n^2+(n+1)^2 \equiv 0 \bmod 4k+3$. Másképp $n^2 \equiv (-1)*(n+1)^2 \bmod 4k+3$. Ez csak úgy lehetséges, ha n és $n+1$ is osztható $4k+3$-mal, ugyanis a -1 nem kvadratikus maradék mod $4k+3$, tehát egy négyzetszám -1-szerese nem lehet négyzetszám, csak abban az esetben, ha mindkettő 0. Viszont n^2 és $(n+1)^2$ relatív prímek, nem oszthatja mindkettőt $4k+3$. Tehát $n^2+(n+1)^2$-nek kizárólag $4k+1$ alakú prímosztói vannak.

Állítás 6. *: Nem feltétlenül különböző, legalább két darab $4k+1$ alakú prím szorzata legalább kétféleképpen felírható két négyzetszám összegeként, ha a 0-t használatát is megengedjük.*

Bizonyítás. Először vizsgáljuk egy $4k+1$ alakú prím hatványait. $p = a^2 + b^2$. Itt $a \neq b$, mivel p páratlan, s egyikük sem 0, mivel p nem négyzetszám. Az általánosság megszorítása nélkül feltehető hát, hogy $a > b > 0$. Tegyük fel, hogy $p^n = a_n^2 + b_n^2$, ahol sem a_n, sem b_n nem 0. Itt, az iméntiekhez hasonlóan, feltehető, hogy $a_n > b_n > 0$. Ekkor, a négyzetszámösszeg már a koraiakban tárgyalt multiplikatív tulajdonságát kihasználva:

$$p^{n+1} = (a^2+b^2)(a_n^2+b_n^2) = (aa_n + bb_n)^2 + (ab_n - ba_n)^2 = (aa_n - bb_n)^2 + (ab_n + ba_n)^2$$

Még azt szeretnénk látni, hogy ez valóban két különböző felírás. Ehhez elegendő azt igazolni, hogy $|aa_n + bb_n| \neq |aa_n - bb_n|$ és $|aa_n + bb_n| \neq |ab_n + ba_n|$. Az előbbi teljesül, hiszen egyrészt b és b_n pozitivitása miatt $aa_n + bb_n \neq aa_n - bb_n$, másrészt a és a_n pozitivitása miatt $aa_n - bb_n \neq -(aa_n + bb_n)$. Az utóbbi teljesülése is magától értetődő, hiszen ha nem így lenne, rendezve azt kapnánk, hogy $(a-b)a_n = (b-a)b_n$, s itt a bal oldal pozitív, a jobb oldal meg negatív. Tehát ha p^n felírható úgy két négyzetszám összegeként, hogy egyik sem 0, akkor p^{n+1} felírható kétféleképpen. Ebből következik, hogy minden prímhatvány, ahol a kitevő legalább 2, felírható így, ugyanis ennek következtében a p^2 nyilván felírható kétfeleképpen, s ha egy hatvány felírható kétféleképpen, akkor a 2-ből az egyik mód nyilván nem használ 0-t, így innentől kezdve mindig megtehető a továbblépés.

Ha a vizsgált szám prímtényezős felbontásában vannak különböző $4k+1$ alakú prímek, akkor teljes indukcióval bizonyítunk, a $4k+1$ alakú prímosztók számára vonatkozóan.

Először legyen $N = p_1^{q_1} * p_2^{q_2}$, ahol p_1 és p_2 $4k+1$ alakú prímek. Ekkor léteznek $a_1 > b_1$ és $a_2 > b_2$ pozitív egészek, amikre $p_1^{q_1} = a_1^2 + b_1^2$, $p_2^{q_2} = a_2^2 + b_2^2$. Ekkor ez iméntiekhez hasonlóan:

$$N = (a_1a_2 + b_1b_2)^2 + (a_1b_2 - b_1a_2)^2 = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2$$

Ezen felírások most is különbözőek, a bizonyítás analóg az iméntivel, mivel csak annyit használunk ki, hogy az a_1, a_2, b_1, b_2 számok egyike sem 0. Ennélfogva ha egy számnak csak két különböző $4k+1$ alakú osztója van, akkor felírható két négyzetszám összegeként kétféleképpen. Tegyük fel hát, hogy $N = p_1^{q_1} * p_2^{q_2} * ... * p_r^{q_r}$ $r = i$-re mindig felírható kétfelékeppen négyzetszámok összegeként. Nézzük $r = i+1$-re. Ekkor $N = (p_1^{q_1} * p_2^{q_2} * ... p_{r-1}^{q_{r-1}}) * (p_r^{q_r}) = N_1 * N_2$. Ekkor N_1 bizonyosan felírható kétfelékeppen négyzetszámok összegeként, következésképp van olyan felírás, ami nem használ 0-t. N_2-nek is nyílván van ilyen felírása. Tehát $N_1 = a_1^2 + b_1^2$ valamely $a_1 > b_1 > 0$-ra, $N_2 = a_2^2 + b_2^2$ valamely $a_2 > b_2 > 0$-ra. Így:

$$N = N_1N_2 = (a_1a_2 + b_1b_2)^2 + (a_1b_2 - b_1a_2)^2 = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2$$

ami megintcsak két különböző felírást jelent. Ezzel a tételt bizonyítottuk. □

Tehát $2n^2 + 2n + 1$ felírása négyzetszámok összegeként csak akkor egyértelmű, ha $2n^2 + 2n + 1$ prím. Az a kérdés tehát, hogy a $2n^2 + 2n + 1$ polinom felvesz-e végtelen sok egész helyen prím értéket, másképp lesz-e két szomszédos négyzetszám összege végtelen sokszor prím. Ez azonban egy globálisan is megválaszolatlan kérdés.

Jellemzően ez polinomfüggvények esetén így van, eltekintve olyan polinomoktól, ahol ez triviálisan nem teljesül, mint például az $x^2 + x$, ami mindig páros értéket vesz fel egész helyen, s legfeljebb 4 helyen prím (mivel legfeljebb két helyen 2). Így sok mindent ehhez a kérdéshez már nem tudunk hozzátenni, a téma befejezéseképp szerepeljen itt Bunyakovszkij 1857-es sejtése, ami a már említett Dirichlet-tétel általánosítása. Eszerint egy egyváltozós egész együtthátós polinom végtelen sok egész helyen vesz fel prímértéket amennyiben teljesülnek rá a következők: a polinom egészek felett irreducibilis, és nincs olyan 1-nél nagyobb egész, ami a polinom összes pozitív egész helyen vett értekét osztaná. Amennyiben csak pozitív prímeket engedünk meg, ezekhez egy triviális harmadik feltétel társul: a főegyüttható pozitív. S hogy miért emeltük ezt ki? Mert a $2n^2 + 2n + 1$, azaz a vizsgált polinom eleget tesz ezen feltételeknek! Egyrészt a pozitív egész helyeken vett függvényértekeknek nincs közös osztója, hiszen már rögtön az első kettőnek nincs: $2 * 1^2 + 2 * 1 + 1 = 5$, $2 * 2^2 + 2 * 2 + 1 = 13$. Másrészt ez a polinom irreducibilis az egészek fölött: ha így lenne, felbomlana két elsőfokú polinom szorzatára, azaz lenne két gyöke, de egy sincs, hiszen két olyan elsőfokú polinom négyzetösszege, melyeknek nincs azonos helyen gyökük. Tehát ha a Bunyakovszkij-sejtés igaz, akkor van végtelen sok háromszögszám, ami nem áll elő két kisebb háromszögszám összegeként.

6 Rések és tömbök

Létrehozunk két fogalmat, amivel számsorozatok sűrűségét szándékozzuk kézzelfoghatóbbá tenni.

Definíció 6.1 (Rés, résesség). *Legyen A egy nemnegatív egészekből álló végtelen halmaz. k-nagyságú résnek nevezünk egy olyan, k darab egymást követő pozitív egészből álló halmazt, amelynek egyik eleme sem eleme*

A-nak. Továbbá, A-t k-résesnek nevezzük, ha a legnagyobb rés, ami végtelen sokszor megjelenik A elemei között, k nagyságú, ha létezik ilyen. Jelölése $R_A = k$. Más esetben a halmaz tetszőlegesen nagy réses.

Definíció 6.2 (Tömb, tömbösség)**.** *Legyen A egy nemnegatív egészekből álló végtelen halmaz. k-nagyságú tömbnek nevezünk egy olyan, k darab egymást követő pozitív egészből álló halmazt, amelynek minden eleme eleme A-nak. Továbbá, A-t k-tömbösnek nevezzük, ha a legnagyobb tömb, ami végtelen sokszor megjelenik A elemei között, k nagyságú, ha létezik ilyen. Jelölése $T_A = k$. Más esetben a halmaz tetszőlegesen nagy tömbös.*

Egyszerű példákon szemléltetve, például a pozitív páros számok halmaza egy 1-réses és egyúttal 1-tömbös halmaz. Ugyanakkor a 100-nál nagyobb páros számok halmaza szintén egy 1-réses, 1-tömbös halmaz. A továbbiakban a már eddig vizsgált halmazok résességet és tömbösségét fogjuk vizsgálni.

6.1 Két négyzetszám összegeként felírható számok halmaza

Állítás 7. *A két négyzetszám összegeként felírható számok N_2 halmaza tetszőlegesen nagy réses.*

Bizonyítás. Keresni fogunk a halmazban r nagyságú rést. Az első r darab $4k+3$ alakú prímet jelölje p_1, p_2, ... p_r. A következő kongruenciarendszerre fogunk megoldást keresni: $x \equiv p_1 \bmod p_1^2$, $x \equiv p_2 - 1 \bmod p_2^2$, ... $x \equiv p_r - (r-1) \bmod p_r^2$. Ezek a modulusok relatív prímek így a kínai maradéktétel alapján ezen kongruenciarendszernek egyértelmű megoldása van mod $p_1^2 p_2^2 ... p_r^2$. Számunkra azonban csak az a fontos, hogy van megoldása. Így létezik x szám, amire x osztható p_1-gyel, de p_1^2-tel nem, $x+1$ osztható p_2-vel, de p_2^2-tel nem, stb. Ennélfogva az x, $x+1$, ..., $x+r-1$ számok egyike sem írható fel két négyzetszám összegeként, következésképp a vizsgált halmazban ezen számok egy r nagyságú rést képeznek. Minthogy végtelen sok $4k+3$ alakú prím van, így r tetszőlegesen nagy értéket felvehet, azaz a két négyzetszám összegeként felírható számok halmaza tetszőlegesen nagy réses. □

Megjegyzés: a kínai maradéktétel bizonyítása viszonylag egyszerű, Szalay Mihály: Számelmélet című könyvében ez is fellelhető.

Állítás 8. *A két négyzetszám összegeként felírható számok N_2 halmazára $T_{N_2} = 3$.*

Bizonyítás. Először megmutatjuk, hogy $T_{N_2} \leq 3$. Tegyük fel ugyanis, hogy van N_2-ben egy 4-nagyságú tömb. Ennek ekkor szükségszerűen minden mod 4 maradékosztályból kerül ki eleme. Tehát ezen tömb egyik eleme 3 maradékot ad 4-gyel osztva, és eleme N_2-nek. Azt azonban már megtárgyaltuk, hogy ez nem lehetséges, hiszen a négyzetszámok 4-es maradéka 0 vagy 1, így két négyzetszám összege nem adhat 3 maradékot. Tehát $T_{N_2} \leq 3$. Már csak az a feladatunk, hogy végtelen sok 3-nagyságú tömböt mutassunk. Vegyünk egy páratlan számot, ez legyen $2a+1$. Ekkor a $(2a^2+2a)^2$, a $(2a^2+2a)^2+1$, s a $(2a^2+2a)^2+2$ számok mindegyike felírható két négyzetszám összegeként: a két előbbi nyilván, hiszen egy négyzetszámként deklarált számhoz adunk 0^2-t, illetve 1^2-t. Ugyanakkor a harmadik is:

$$(2a^2+2a)^2+2 = 4a^4+8a^3+4a^2+2 = (4a^4+8a^3-4a+1)+(4a^2+4a+1) = (2a^2+2a-1)^2+(2a+1)^2$$

Így ahogy a végigfut a pozitív egészeken, végtelen sok 3-nagyságú tömb gyártható le. Tehát $T_{N_2} = 3$. □

6.2 Két háromszögszám összegeként felírható számok halmaza

Állítás 9. *A két háromszögszám összegeként felírható számok H_2 halmaza tetszőlegesen nagy réses.*

Bizonyítás. Keresni fogunk a halmazban r nagyságú rést. Az első r darab $4k+3$ alakú prímet jelölje p_1, p_2, ... p_r. A következő kongruenciarendszerre fogunk megoldást keresni: $x \equiv \frac{p_1-1}{4} \bmod p_1^2$, $x \equiv \frac{p_2-1}{4} - 1 \bmod p_2^2$, ... $x \equiv \frac{p_1-1}{4} - (r-1) \bmod p_r^2$. Ezek a modulusok relatív prímek így a kínai maradéktétel alapján ezen kongruenciarendszernek egyértelmű megoldása van mod $p_1^2 p_2^2 ... p_r^2$. Számunkra azonban csak az a fontos, hogy van megoldása. Így létezik x szám, amire $4x+1$ osztható p_1-gyel, de p_1^2-tel nem, $4(x+1)+1$ osztható p_2-vel, de p_2^2-tel nem, stb. Ennélfogva az $x+1$, $x+1$, ..., $x+r-1$ számok egyike sem írható fel két háromszögszám összegeként, következésképp a vizsgált halmazban ezen számok egy r nagyságú rést képeznek. Minthogy végtelen sok $4k+3$ alakú prím van, így r tetszőlegesen nagy értéket felvehet, azaz a két háromszögszám összegeként felírható számok halmaza tetszőlegesen nagy réses. □

Állítás 10. *A két háromszögszám összegeként felírható számok H_2 halmazára $T_{H_2} = 5$.*

Bizonyítás. Először megmutatjuk, hogy $T_{H_2} \leq 5$. Tegyük fel ugyanis, hogy van H_2-ben egy 6-nagyságú tömb. Ennek ekkor hat szomszédos mod 9 maradékosztályból kerül ki eleme. Tehát ezen tömb egyik i eleme 5 vagy 8 maradékot ad 9-cel osztva, és eleme H_2-nek. Tehát $4i+1$ felírható két négyzetszám összegeként. Ez azonban $4*5+1 \equiv 3$ vagy $4*8+1 \equiv 6 \bmod 9$, azaz 3-mal osztható, de 9-cel nem, így nem írható fel két négyzetszám összegeként, ami ellentmondás. Tehát $T_{H_2} \leq 5$. Már csak az a feladatunk, hogy végtelen sok 5-nagyságú tömböt mutassunk.

Vegyük az n. háromszögszámot, h_n-t. Ekkor h_n, h_n+1 és h_n+3 nyílván eleme H_2-nek. Tehát ha végtelen sok n-et találunk, amire h_n-1 és h_n+2 is eleme H_2-nek, akkor készen vagyunk. $h_n - 1 = h_{n-2} + 2n - 2$, $h_n + 2 = h_{n-1} + n + 2$. Tehát ha végtelen sok olyan n-t találunk, amire $n+2$ és $2n-2$ egyidejűleg háromszögszám, akkor készen vagyunk. Legyen tehát $n + 2 = \frac{a^2+a}{2}$, $2n - 2 = \frac{b^2+b}{2}$. Az első egyenletet szorozzuk 16-tal, majd adjunk hozzá 2-t, a második egyenletet szorozzuk fel 8-cal, majd adjunk hozzá 1-et. Eredményul a következő egyenleteket kapjuk:

$$16n + 34 = 8a^2 + 8a + 2 = 2*(2a+1)^2$$

$$16n - 15 = 4b^2 + 4b + 1 = (2b+1)^2$$

Legyen $2b+1 = x$, $2a+1 = y$. Így az egyenletek különbségét véve az eredmény $-49 = x^2 - 2y^2$. Ezen diofantoszi egyenletre keresünk végtelen sok, páratlan számokból álló, megoldást jelentő x, y számpárt. Észrevehető, hogy $x = x_1 = 1$, $y = y_1 = 5$ feltételeinknek megfelelő megoldást jelent. Rekurzióval adunk végtelen sok megoldást. Legyen $x_{i+1} = 3x_i + 4y_i$, $y_{i+1} = 2x_i + 3y_i$. x helyébe x_{i+1}-t, y helyébe y_{i+1}-t írva az eredmény a rekurziót kihasználva:

$$x_{i+1}^2 - 2y_{i+1}^2 = (3x_i+4y_i)^2 - 2*(2x_i+3y_i)^2 = (9x_i^2+24x_iy_i+16y_i^2) - (8x_i^2+24x_iy_i+18y_i^2) = x_i^2 - 2y_i^2 = -49$$

Tehát ez a számpár újabb megoldást jelent, mivel az egyenletet kielégíti, nyilván $x_{i+1} > x_i$ és $y_{i+1} > y_i$, és könnyen ellenőrizhető, hogyha x_i, y_i páratlan számokból álló számpár, akkor x_{i+1}, y_{i+1} is. Így végtelen sok páratlan x, y-t generálható, amire $-49 = x^2 - 2y^2$. A páratlan számok négyzetei 1 vagy 9 maradékot adnak 16-tal osztva, ezek kétszerese pedig 2-t. Tehát $2y^2 \equiv 2 \bmod 16$, azaz $16n + 34 = 16(n+1) + 2$ alakba írható. Ezen esetekben nyilván teljesül az is, hogy $x^2 = 16n - 15$, hiszen $x^2 - 2y^2 = -49$. Tehát az eredeti $16n + 34 = 2y^2$ és $16n - 15 = x^2$ egyenletek végtelen sok esetben kielégíthetőek egyidejűleg, amiből egyértelműen adódik végtelen sok a, b pár. Így végtelen sok esetben $\{h_n - 1, h_n, h_n + 1, h_n + 2, h_n + 3\} \subset H_2$, azaz $T_{H_2} = 5$. □

Megjegyzés: az $x^2 - dy^2 = 1$ alakú egyenleteket (d pozitív egész) Pell-egyenleteknek nevezzük. Ezeknek végtelen sok x, y egészekből álló megoldása van, ha d nem négyzetszám. Olykor az $x^2 - dy^2 = k$ egyenleteket is Pell-egyenletnek nevezik. Ezekről is érdemes tudni, ha legalább egy x, y egészekből álló megoldásuk van, akkor végtelen sok van. A Pell-egyenletekről bővebben olvashatunk például Maurer I. Gyula: Tizedes törtek és lánctörtek című könyvében.

6.3 Négyzetszámok két kisebb négyzetszám összegeként

Ha konkrétan ezen számok halmazát néznénk, akkor abban nyilván egyre nagyobb rések és csak 1-nagyságú tömbök lennének. Tehát kissé más halmazt vizsgálunk: n akkor legyen eleme az N_α halmaznak, ha n^2 felírható két kisebb négyzetszám összegeként. Ezeket a jelöléseket alkalmazva $1 \leq R_{N_\alpha} \leq 4$. Az alsó korlát azért igaz, mert végtelen sok olyan szám van, aminek prímtényezős felbontásában nincs $4k+1$ alakú prím, a felső pedig azért, mert minden 5-tel osztható szám eleme N_α-nak. Ez egy nem túl erős állítás, de a szűkebb határok közé szorítás meglehetősen nehéz.

Állítás 11. *N_α halmaz tetszőlegesen nagy tömbös.*

Bizonyítás. A bizonyítás hasonlóan zajlik két korábban látotthoz is. Keresni fogunk a halmazban t nagyságú tömböt. Az első t darab $4k+1$ alakú prímet jelölje p_1, p_2, ... p_t. A következő kongruenciarendszerre fogunk megoldást keresni: $x \equiv 0 \mod p_1$, $x \equiv -1 \mod p_2$, ... $x \equiv -(t-1) \mod p_t$. Ezek a modulusok relatív prímek így a kínai maradéktétel alapján ezen kongruenciarendszernek egyértelmű megoldása van mod $p_1 p_2 ... p_t$. Számunkra azonban csak az a fontos, hogy van megoldása. Így létezik x szám, amire x osztható p_1-gyel, $x+1$ osztható p_2-vel, stb. Ennélfogva az x, $x+1$, ..., $x+t-1$ számok mindegyike eleme N_α-nak, következésképp a vizsgált halmazban ezen számok egy t nagyságú tömböt képeznek. Minthogy végtelen sok $4k+1$ alakú prím van, így t tetszőlegesen nagy értéket felvehet, azaz N_α tetszőlegesen nagy tömbös. □

6.4 Háromszögszámok két kisebb háromszögszám összegeként

Itt az iméntihez hasonló halmazt tekintünk: n akkor eleme H_α-nak, ha az n. háromszögszám előáll két kisebb háromszögszám összegeként. Ekkor $0 \leq R_{H_\alpha} \leq 2$, mint azt már láttuk, s amennyiben a Bunyakovszkij-sejtés igaz, ez az alsó korlát felvihető 1-re.

Állítás 12. *H_α halmaz tetszőlegesen nagy tömbös.*

Bizonyítás. Keresni fogunk a halmazban t nagyságú tömböt. Ehhez t darab egymás utáni olyan n-t keresünk, amire $2n^2+2n+1$ nem prím. Az első t darab $4k+1$ alakú prímet jelölje p_1, p_2, ... p_t. Igazolunk egy lemmát, mégpedig azt, hogy tetszőleges p_i prímhez van olyan n_i maradékosztály, amire $p_i | 2n_i^2 + 2n_i + 1$. Ez ugyanis ekvivalens azzal, hogy $p_i | 4n_i^2 + 4n_i + 2$, mivel $(2, p_i) = 1$. Tehát $p_i | (2n_i + 1)^2 + 1$. A -1 kvadratikus maradék mod p_i, tehát létezik m, amire $m^2 \equiv -1 \mod p_i$. Így $n_i \equiv \frac{m-1}{2} \mod p_i$ esetén $p_i | (2n_i+1)^2+1$. Ezzel a lemmát bizonyítottuk. Tehát az egyes p_i-khez ez alapján rendelhetünk n_i-ket. A következő kongruenciarendszerre fogunk megoldást keresni: $n \equiv n_1 \mod p_1$, $n \equiv n_2 - 1 \mod p_2$, ... $n \equiv n_t - (t-1) \mod p_t$. Ezek a modulusok relatív prímek így a kínai maradéktétel alapján ezen kongruenciarendszernek egyértelmű megoldása van mod $p_1 p_2 ... p_t$. Ennélfogva van tetszőlegesen nagy megoldása, azaz van olyan megoldása, amire $n > p_t$, következésképp $2n^2 + 2n + 1 > p_t$. Így létezik n szám, amire $2n^2 + 2n + 1$ osztható p_1-gyel, de ugyanakkor nagyobb, mint p_1, azaz nem lehet prím, $2(n+1)^2 + 2(n+1) + 1$ osztható p_2-vel, de ugyanakkor nagyobb, mint p_2, azaz ez sem lehet prím, stb. Tehát az n, $n+1$, ..., $n+t-1$ számok mindegyike eleme H_α-nak, következésképp a vizsgált halmazban ezen számok egy t nagyságu tömböt képeznek. Minthogy végtelen sok $4k+1$ alakú prím van, így t tetszőlegesen nagy értéket felvehet, azaz H_α is tetszőlegesen nagy tömbös. □

7 Források és köszönetnyilvánítás

Ezen cikk második részében taglaltakkal a szerzők alapvetően a középiskolai matematikaórákon találkoztak. A később bemutatásra kerültek saját kutatás eredményei. Ezentúl csak a 4. részben megjelenő megválaszolatlan kérdést "ellenőriztük", hogy vajon globálisan is megválaszolatlan-e, ahogy azt sejtettük azok után, hogy a problémáról beláttuk, ekvivalens azzal a kérdéssel, hogy vajon végtelen sok prímértéket vesz-e fel egész helyen a $2x^2 + 2x + 1$ függvény. Ez több cikkben is megtalálható, szintén megoldatlan problémaként behivatkozva, például Wacław Sierpiński: Sur les nombres triangulaires qui sont sommes de deux nombres triangulaires című cikkében, ami fellelhető a göttingeni egyetem digitális könyvtárában a http://gdz.sub.uni-goettingen.de/ címen.

A kongruenciák kezelése során minden magyarázat nélkül tettünk meg olyan lépéseket, amik korrektsége a kongruenciákkal végezhető műveleteket nem ismerők számára nem magától értetődő. Emellett már a cikken belül utalást tettünk a Dirichlet-tételre és felhasználtuk a kínai maradéktételt. Mindezek miatt felhasznált irodalomként tekinthetünk Szalay Mihály: Számélmélet című könyvére.

A szerzők mindemelett köszönetüket fejezik ki tanáraiknak - elsősorban Hraskó Andrásnak, Hegedüs Pálnak és Kiss Gergelynek - a beléjük fektetett munkáért, valamint Tossenberger Tamásnak a cikk lektorálásáért.