

LÉPÉS AZ $ax + by = p(z)$ ALAKÚ 2-RAMSEY EGYENLETEK KARAKTERIZÁCIÓJA FELÉ

BAJA ZSOLT, DOBÁK DÁNIEL, KOVÁCS BENEDEK, PIGLER DONÁT
TÉMAVEZETŐ: PACH PÉTER PÁL

KIVONAT. Ebben a dolgozatban az $ax + by = p(z)$ alakú egyenletekre vizsgáljuk a Ramsey-problémát. A fő eredményünk egy tétel, amely elégséges feltételt ad a, b pozitív egész számokra és p polinomra ahhoz, hogy $ax + by = p(z)$ 2-Ramsey legyen, azaz a pozitív egész számok bármely 2-színezése esetén végtelen sok monokromatikus megoldása legyen az $ax + by = p(z)$ egyenletnek. Ez több nevezetes eset 2-Ramseységét vonja maga után, például az $ax + y = z^n$ egyenletét, tetszőleges $a \in \mathbb{Z}^+$ -ra és $n \geq 2$ -re, továbbá az $ax + by = cz^2$ egyenletét, olyan a, b és c számokra, ahol $\text{luko}\left(c, \frac{a}{\text{luko}(a,b)}\right) = 2^\ell$ és $\text{luko}\left(c, \frac{b}{\text{luko}(a,b)}\right) = 2^{\ell'}$ valamilyen $\ell, \ell' \in \mathbb{Z}^{\geq 0}$ -re és végezetül az $ax + by = a_d z^d + \dots + a_1 z \in \mathbb{Z}[z]$ egyenletét, amelyre $\text{luko}(a, b) = 1$, $d \geq 2$, $a_d > 0$ és $a_1 \neq 0$.

1. BEVEZETŐ

A Ramsey-elmélet monokromatikus mintázatokat keres a $\mathbb{Z}^+$ halmaz véges színezéseiben. Ennek hosszú története Schur [20] 1916-os híres tételére vezethető vissza, amely szerint az $x + y = z$ egyenlet *Ramsey*, azaz a $\mathbb{Z}^+$ bármely véges színezése esetén az $x + y = z$ egyenletnek van monokromatikus megoldása. Egy másik klasszikus példa van der Waerden [22] tétele, amely szerint $\{x, x + y, \dots, x + (\ell - 1)y\}$ Ramsey bármely $\ell \in \mathbb{Z}^+$ esetén. Rado [16] később korszakalkotó munkájában megoldotta a Ramsey-problémát minden *lineáris* egyenletre, jellemezve mindazokat, amelyek Ramsey-k. Azóta számos általánosítást tanulmányoztak, lásd pl. Bergelson és Leibman [2] van der Waerden tételének polinomiális kiterjesztését.

Ebben a dolgozatban a Schur-tétel polinomiális kiterjesztéseit vizsgáljuk, nevezetesen az $ax + by = p(z)$ alakú polinomokat. Csikvári, Gyarmati és Sárközy [4] megmutatták, hogy $x + y = z^2$ *nem* 16-Ramsey, azaz szerkesztettek egy olyan 16-színezést $\mathbb{Z}^+$ -ra, amelyre az $x + y = z^2$ egyenletnek nincs más monokromatikus megoldása, mint az $x = y = z = 2$ triviális megoldás. Green és Lindqvist [7] ezt az esetet Fourier-analitikus érvekkel teljesen megoldották, és azt a kielégítő választ adták, hogy a $\mathbb{Z}^+$ bármely 2-színezése *végtelen* sok monokromatikus megoldást tartalmaz, és 3 szín elegendő a nem triviális monokromatikus megoldások elkerüléséhez. Más szóval, $x + y = z^2$ 2-Ramsey, de nem 3-Ramsey. Valójában a [7]-ben található 3-színezés könnyen adaptálható annak kimutatására, hogy $ax + by = p(z)$ nem 3-Ramsey semelyik $a, b \in \mathbb{N}$ és $p(z) \in \mathbb{Z}[z]$ esetén sem, ahol $\deg(p) \geq 2$. Pach [15] egy rövidebb, kombinatorikus bizonyítást adott az $x + y = z^2$ egyenlet 2-Ramseységére. Ezt követően Liu, Pach és Sándor [12] teljesen megoldották a Ramsey-problémát az

$$\{x, y, z : x + y = p(z)\}$$

mintázatra, minden $\mathbb{Z}$ feletti polinomra, így megadva egy polinomiális általánosítását a Schur-tételnek. Bebizonyították, hogy az $x + y = p(z)$ egyenlet akkor és csak akkor 2-Ramsey, ha

$p(1)p(2)$ páros. Ha $p(1)p(2)$ páratlan, akkor p csak páratlan értékeket vesz fel, így az egész számok paritás szerinti színezése elkerüli az $x + y = p(z)$ egyszínű megoldásait. Eredményük szerint ez az oszthatósági korlát az egyetlen akadálya a $x + y = p(z)$ 2-Ramseységének.

Dolgozatunkban a Ramsey-problémát vizsgáljuk az $ax + by = p(z)$ alakú egyenletek esetén, ahol a és b pozitív egész számok. Mint korábban említettük, a mohó színezés segítségével látható, hogy az egyenlet *nem* 3-Ramsey. Az $a = b = 1$ esetben az egyenlet 2-Ramsey-nek bizonyult, hacsak a páratlan-páratlan színezés nem kerüli el a monokromatikus megoldásokat. Ha 1-nél nagyobb együtthatókat engedünk meg, akkor a 2-Ramseység több esetben is megdőlhét. Mielőtt pozitív irányú eredményeinket ismertetnénk, nézzünk néhány példát arra, amikor az egyenlet nem 2-Ramsey. A továbbiakban a színezésünk (amit általában ϕ -vel jelölünk) két színe $+1$ és -1 lesz, amit gyakran $+$ -ra és $-$ -ra fogunk rövidíteni.

1. *Példa* Ha minden z esetén $\text{lko}(a, b) \nmid p(z)$, akkor $ax + by = p(z)$ triviálisan nem 2-Ramsey, sőt az egyenletnek egyáltalán nincs egész számokból álló megoldása.

2. *Példa* Legyen p egy prímszám. Ha $p \mid a$ és $p \nmid b$, akkor az $ax + by = z^{p-1} - 1$ egyenlet nem 2-Ramsey. Legyen $\phi(t) = +$, ha $p \mid t$ és $\phi(t) = -$ másként. Ha $p \mid x, y, z$, akkor $ax + by \equiv 0 \not\equiv -1 \equiv z^{p-1} - 1 \pmod{p}$. Ha $p \nmid x, y, z$, akkor $ax + by \not\equiv 0 \equiv z^{p-1} - 1 \pmod{p}$.

Általánosabban, bármely $n \geq 1$ esetén az $ax + by = z^{p^n - p^{n-1}} - 1$ egyenlet nem 2-Ramsey, ha $p^n \mid a$, $p^n \nmid b$.

3. *Példa* Az $x + 4y = (z + 2)(z + 1) = z^2 + 3z + 2$ egyenlet nem 2-Ramsey. Valóban, a $\phi(t) = +$, ha $t \equiv 0, 1 \pmod{4}$ és $\phi(t) = -$, ha $t \equiv 2, 3 \pmod{4}$ színezés esetén nem létezik monokromatikus megoldás.

A fő eredményünk a következő tétel, amely megmutatja, hogy bizonyos technikai feltételek teljesülése esetén az $ax + by = p(z)$ egyenlet 2-Ramsey.

1.1. Tétel. *Tegyük fel, hogy $p \in \mathbb{Z}[z]$ egy legalább másodfokú polinom pozitív főegyütthatóval, és legyenek a és b pozitív egész számok úgy, hogy $\text{lko}(a, b) = 1$. Tegyük fel továbbá, hogy léteznek olyan d és u pozitív egész számok, valamint olyan t és v egész számok (amelyek mod d illetve mod u maradékosztályokat jelölnek), hogy a következő hat feltétel teljesüljön:*

- (1) $(a + b)t \equiv p(t) \pmod{d}$,
- (2) ha $k \equiv t \pmod{d}$, akkor $a \mid p(k + d) - p(k)$,
- (3) ha $k \equiv t \pmod{d}$, akkor az $m = \frac{p(k+d)-p(k)}{a}$ és $m' = \frac{m}{u}$ számokra teljesül $u \mid m$ és $2 \nmid m'$ és $(a, m') = (b, m') = (u, m') = 1$,
- (4) $p(v) \equiv (a + b)v \pmod{u}$,
- (5) ha $k \equiv t \pmod{d}$, akkor $p(k) \equiv (a + b)v \pmod{u}$,
- (6) ha $j \equiv v \pmod{u}$ és $k \equiv t \pmod{d}$, akkor $b \mid p(k) - aj$.

Ekkor az $ax + by = p(z)$ egyenlet 2-Ramsey.

Az 1.1 tételt fel lehet ahhoz használni, hogy az $ax + by = p(z)$ alakú egyenletek néhány sajátos osztályának a 2-Ramseységét kimutassuk, ahogy ez a továbbiakban látható.

1.2. Következmény. *Legyenek a és b relatív prím pozitív egész számok. Ha a $p(z) = a_d z^d + \dots + a_1 z \in \mathbb{Z}[z]$ polinomra igaz, hogy $d \geq 2$, $a_d > 0$ és $a_1 \neq 0$, akkor az $ax + by = p(z)$ egyenlet 2-Ramsey.*

1.3. Következmény. Legyenek a és n pozitív egész számok úgy, hogy $n \geq 2$. Ekkor az $ax + y = z^n$ egyenlet 2-Ramsey.

1.4. Következmény. Legyenek a, b, c pozitív egész számok, amelyekre $\text{luko}(a, b) = 1$, és legyen p prím. A b számot $b = p^{pn-\varepsilon}B$ alakba írhatjuk, ahol $v_p(b) = pn - \varepsilon$, $n \in \mathbb{Z}$ és $\varepsilon \in \{0, 1, \dots, p-1\}$. Ha $\text{luko}(a, c) = 1$, $\text{luko}(B, c) = 1$ és létezik $t \in \mathbb{Z}_{aBp^n}$, amelyre

$$\begin{cases} t \equiv 0 & (\text{mod } p^n) \\ t^{p-1} \equiv ac^{-1} & (\text{mod } B) \\ t^{p-1} \equiv bc^{-1} & (\text{mod } a), \end{cases}$$

akkor az $ax + by = cz^p$ egyenlet 2-Ramsey.

Figyeljük meg, hogy a $p = 2$ speciális esetben az 1.4 Következmény az alábbiakat adja:

1.5. Következmény. Legyenek a, b, c pozitív egész számok, amelyekre $\text{luko}(a, b) = 1$, $\text{luko}(a, c) = 2^\ell$ és $\text{luko}(b, c) = 2^{\ell'}$ valamilyen $\ell, \ell' \in \mathbb{Z}^{\geq 0}$ esetén. Ekkor az $ax + by = cz^2$ egyenlet 2-Ramsey.

1.6. Következmény. Legyenek a, b és c pozitív egész számok. Ekkor az $ax + by = cz^2$ egyenlet 2-Ramsey, ha $\text{luko}\left(c, \frac{a}{\text{luko}(a, b)}\right) = 2^\ell$ és $\text{luko}\left(c, \frac{b}{\text{luko}(a, b)}\right) = 2^{\ell'}$ valamilyen $\ell, \ell' \in \mathbb{Z}^{\geq 0}$ esetén.

Jelölések. Az m pozitív egész esetén használjuk a $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ jelölést. Ha p prím és a egy nullától különböző egész szám, akkor $v_p(a)$ a legnagyobb egész számot jelöli, amelyre $p^{v_p(a)} \mid a$.

2. BIZONYÍTÁSOK

Ebben a fejezetben bebizonyítjuk az eredményeinket.

Az 1.1 tétel bizonyítása. Először gyorsan belátjuk az állítást az $a = b = 1$ esetben a Liu, Pach és Sándor cikkében a [12, 1.4. következmény] megadott szükséges és elégséges feltétel használatával. Eszerint az eredmény szerint, egy legalább elsőfokú, pozitív főegyütthatójú p polinomra az $x + y = p(z)$ egyenlet pontosan akkor 2-Ramsey, ha $2 \mid p(1)p(2)$. Tehát elég belátnunk, hogy ha minden z egészre $p(z) \equiv 1 \pmod{2}$, akkor az (1)-(6) feltételek nem teljesülhetnek mind. És valóban, ha d, u, t, v -re a feltételek mind teljesülnek, akkor (4) miatt $u \mid p(v) - 2v$, és mivel $p(v)$ páratlan, u -nak is páratlannak kell lennie. $k = t$ -re $m = p(k + d) - p(k)$, ami páros, és mivel u páratlan, ezért $m' = \frac{m}{u}$ (ami a (3) miatt egész) szintén páros. Viszont ez ellentmond annak, hogy a (3) szerint m' páratlan. Ezzel befejeztük a bizonyítást az $a = b = 1$ esetben.

Mostantól feltehetjük, hogy a és b különbözők. Használjuk az $U = \max(a, b)$ és $L = \min(a, b)$ jelöléseket. Legyen $p(z) = c_n z^n + c_{n-1} z^{n-1} + \dots + c_1 z + c_0$, ahol $n \geq 2$ és $c_n > 0$. Vegyünk olyan $d, u \in \mathbb{Z}^+$ számokat és $d\mathbb{Z} + t$ és $u\mathbb{Z} + v$ maradékosztályokat, melyek teljesítik az (1)-(6) feltételeket. Legyen $\phi : \mathbb{Z}^+ \rightarrow \{+, -\}$ tetszőleges 2 színnel való színezés. Be fogjuk látni, hogy az $ax + by = p(z)$ egyenletnek végtelen sok monokromatikus megoldása van. Indirekten tegyük fel, hogy csak véges sok van.

A bizonyításunkban használni fogjuk az $\varepsilon_0 > 0$ és $\varepsilon_1 > 0$ valós konstansokat, melyeket kellően kicsinek választunk meg a, b, p és d függvényében. (A megválasztásuk módját később részletezzük.)

Egy k pozitív egészre, melyre $k \equiv t \pmod{d}$, azt mondjuk, hogy k -nál d -váltás történik, ha $\phi(k) \neq \phi(k+d)$.

1. Állítás. Végtelen sok d -váltás van.

Bizonyítás. Indirekten tegyük fel, hogy csak véges sok d -váltás van. Ekkor létezik olyan $K_0 \in \mathbb{Z}^+$, hogy a $\{k \in \mathbb{Z}^+ : k \equiv t \pmod{d}; k \geq K_0\}$ halmaz monokromatikus. Elegendő belátni, hogy bármely $K_1 > K_0$ -ra, az $ax+by = p(z)$ egyenletnek van olyan monokromatikus megoldása, amelyben $x, y, z \geq K_1$.

Mivel p foka legalább 2, és főegyütthatója pozitív, választhatunk egy olyan $z_1 \geq K_1$ értéket, melyre $z_1 \equiv t \pmod{d}$ és $p(z_1) \geq (a+b)z_1 + 4a^2b^2d$. Ekkor (1) miatt

$$p(z_1) \equiv p(t) \equiv (a+b)t \equiv (a+b)z_1 \pmod{d},$$

legyen $p(z_1) = (a+b)z_1 + \ell d$, ahol tudjuk, hogy $\ell \geq 4a^2b^2$. Írjuk fel ℓ -et $\ell_1 \cdot 2ab + \ell_2$ alakban, ahol ℓ_1, ℓ_2 egészek és $0 \leq \ell_2 < 2ab$. Az ℓ -re vonatkozó alsó becslést használva $\ell_1 \geq 2ab$.

Mivel $\text{Inko}(a, b) = 1$, a Bézout-lemma szerint léteznek r és s egészek, melyekre $ra+sb = 1$. Könnyen látható, hogy r és s választható úgy, hogy $|r| \leq b$ és $|s| \leq a$ legyen. Tekintsük az alábbi számokat:

$$x = z_1 + (\ell_1 b + \ell_2 r)d,$$

$$y = z_1 + (\ell_1 a + \ell_2 s)d,$$

$$z = z_1.$$

Ekkor mivel $|\ell_2| \leq 2ab$ és $|r| \leq b$, az $\ell_1 \geq 2ab$ becslés használatával kijön, hogy $\ell_1 b + \ell_2 r \geq 0$. Hasonlóan $\ell_1 a + \ell_2 s \geq 0$ is fennáll, így $x, y, z \geq z_1 \geq K_1$. Továbbá tudjuk, hogy $x, y, z \equiv t \pmod{d}$. Valamint

$$\begin{aligned} ax + by &= (a+b)z_1 + (2ab\ell_1 + (ra+sb)\ell_2)d = (a+b)z_1 + (2ab\ell_1 + \ell_2)d = \\ &= (a+b)z_1 + \ell d = p(z_1) = p(z), \end{aligned}$$

tehát egy olyan monokromatikus megoldását találtuk az $ax+by = p(z)$ egyenletnek, melyben mindhárom változó értéke legalább K_1 . Ezzel készen van az 1. állítás bizonyítása. $\square$

Nevezzük a $k_1 < k_2$ számoknál lévő d -váltásokat *szomszédosnak*, ha nincs olyan $k_1 < k_3 < k_2$ szám, aminél d -váltás fordul elő. Emlékeztetőül a jelöléseink $U = \max(a, b)$ és $L = \min(a, b)$.

2. Állítás. Végtelen sok olyan $k_1 < k_2$ szomszédos d -váltásokról álló pár van, amelyre $k_2 < Uk_1$.

Bizonyítás. Indirekten tegyük fel, hogy csak véges sok ilyen d -váltaspár van, és K_0 egy felső korlát az összes ilyen pár elemeire. Legyen K egy kellően nagy egész szám, melyre $K > K_0$, és még további feltételek is teljesülnek rá, melyeket később részletezünk.

Az 1. állítás miatt létezik három szomszédos d -váltás, $k_1 < k_2 < k_3$, úgy, hogy $k_1 > K$. Ekkor mivel $k_1, k_2, k_3 > K_0$, teljesül $k_2 \geq Uk_1$ és $k_3 \geq Uk_2$. Az általánosság csorbítása nélkül feltehetjük, hogy minden $x \in (d\mathbb{Z} + t) \cap (k_1, k_2]$ számra $\phi(x) = -$, és minden $x \in (d\mathbb{Z} + t) \cap (k_2, k_3]$ számra $\phi(x) = +$. Technikai okokból rögzítsünk egy kicsi $\varepsilon > 0$ valós számot, melyre $L + \frac{L}{U} + \varepsilon < U - \varepsilon$ (ez lehetséges, mert $U \geq L + 1$ miatt $L + \frac{L}{U} < U$).

Most vegyünk egy olyan z pozitív egészt, melyre $z \equiv t \pmod{d}$ és

$$\left(L + \frac{L}{U} + \varepsilon\right) k_2 \leq p(z) \leq (U - \varepsilon) k_2.$$

Ehhez vegyük észre, hogy $p(z + d) - p(z)$ egy $n - 1$ -ed fokú polinomja z -nek, $ndc_n > 0$ főegyütthatóval. Tehát léteznek K_1 és D pozitív valós számok, melyekre $p(z + d) - p(z) \leq Dz^{n-1}$ minden $z \geq K_1$ valós számra. Továbbá, mivel $\deg p = n$ és $c_n > 0$, léteznek olyan K_2 és E pozitív valós számok, hogy $p(z) \geq Ez^n$ minden $z \geq K_2$ valós számra. Ha most $z \in \mathbb{R}$ és $z \geq K_1, K_2$, akkor a $\ell = p(z)$ jelöléssel azt kapjuk, hogy $\ell^{\frac{1}{n}} \geq E^{\frac{1}{n}} z$, így $\ell^{\frac{n-1}{n}} \geq z^{n-1} E^{\frac{n-1}{n}}$, tehát $p(z+d) - p(z) \leq Dz^{n-1} \leq DE^{-\frac{n-1}{n}} \ell^{\frac{n-1}{n}}$. Legyen $F = DE^{-\frac{n-1}{n}}$, ez egy pozitív konstans. Mivel $c_n > 0$, létezik $K_3 \geq K_1, K_2$, hogy p monoton nő $[K_3, \infty)$ -en. Legyen $K \geq K_1, K_2, p(K_3)$; ekkor p felveszi az $(L + \frac{L}{U} + \varepsilon) k_2$ értéket valamilyen $z_0 \geq K_3$ helyen. Legyen z_1 a legkisebb olyan eleme $d\mathbb{Z} + t$ -nek, amely nagyobb, mint z_0 . Ekkor $z_1 \leq z_0 + d$ és $p(z_1) \leq p(z_0 + d) \leq p(z_0) + F \cdot (p(z_0))^{\frac{n-1}{n}} = (L + \frac{L}{U} + \varepsilon) k_2 + F \cdot (L + \frac{L}{U} + \varepsilon)^{\frac{n-1}{n}} k_2^{\frac{n-1}{n}} < (U - \varepsilon) k_2$, ha K (és emiatt k_2 is) elegendően nagy. Vagyis $z = z_1$ kielégíti a feltételeinket.

Most pedig különböztessünk meg két esetet z színétől függően.

1. eset: $\phi(z) = -$.

Ebben az esetben a célunk az, hogy olyan $x, y \in d\mathbb{Z} + t$ pozitív egész számokat találjunk, hogy $Lx + Uy = p(z)$ és $k_1 < x, y \leq k_2$. Ekkor $\phi(x) = \phi(y) = -$, és így találtunk egy monokromatikus megoldást, amelyre $\max(x, y, z) \geq K$.

Először is bebizonyítjuk, hogy létezik $x_1, y_1 \in d\mathbb{Z} + t$, hogy $Lx_1 + Uy_1 = p(z)$. A Bézout-lemma szerint vegyünk olyan r, s egészeket, hogy $rL + sU = 1$. Ekkor (1) szerint,

$$p(z) \equiv (L + U)t \pmod{d},$$

tehát $p(z) - (L + U)t = d\ell$ egy bizonyos $\ell \in \mathbb{Z}$ -re. Legyen most $x_1 = t + r\ell d$ és $y_1 = t + s\ell d$, tehát $Lx_1 + Uy_1 = L(t + r\ell d) + U(t + s\ell d) = (L + U)t + \ell d(rL + sU) = (L + U)t + \ell d = p(z)$.

Vegyük észre, hogy bármely $w \in \mathbb{Z}$ esetén az $x = x_1 + wdU$ és $y = y_1 - wdL$ számok szintén kielégítik az $Lx + Uy = p(z)$ és $x, y \in d\mathbb{Z} + t$ feltételeket. Minden alkalommal, amikor w -hez 1-et adunk, az $x - y$ mennyiség $d(L + U)$ -val nő. Tehát létezik olyan $w \in \mathbb{Z}$, hogy $|x - y| \leq d \cdot \frac{L+U}{2}$, és így

$$\frac{p(z)}{L+U} - d \cdot \frac{L+U}{2} \leq x, y \leq \frac{p(z)}{L+U} + d \cdot \frac{L+U}{2}.$$

Elég nagy K (és így k_2) esetén tehát,

$$x, y \geq \frac{(L + \frac{L}{U} + \varepsilon) k_2}{L + U} - d \cdot \frac{L + U}{2} = \frac{LU + L}{U(L + U)} k_2 + \frac{\varepsilon}{L + U} k_2 - d \cdot \frac{L + U}{2} > \frac{1}{U} k_2 \geq k_1$$

és

$$x, y \leq \frac{U - \varepsilon}{L + U} k_2 + d \cdot \frac{L + U}{2} < k_2$$

ahol felhasználtuk, hogy $\frac{1}{U} \leq \frac{LU+L}{U(L+U)}$, ami a nevezőkkel való felszorzással triviálisan adódik. Így találtunk a célunknak megfelelő x, y -t.

2. eset: $\phi(z) = +$

Az előző esethez hasonlóan létezik $x_1, y_1 \in d\mathbb{Z} + t$, hogy $Lx_1 + Uy_1 = p(z)$. Legyen ismét $x = x_1 + wdU$ és $y = y_1 - wdL$ valamely $w \in \mathbb{Z}$ -re, most a célunk az, hogy találjunk $x, y > 0$ -t, hogy $\phi(x) = \phi(y) = +$.

Aszerint az indirekt feltevésünk szerint, hogy csak véges sok "közele" d -váltaspár van, könnyen láthatóan következik, hogy léteznie kell L egymást követő $d\mathbb{Z} + t$ alakú pozitív egészeknek, amelyek mindegyike $+$ színű. Így lehetőségünk van w -t úgy beállítani, hogy $y = y_1 - wdL$ egyenlő legyen ezek egyikével. Ekkor

$$x = \frac{p(z)}{L} - \frac{U}{L}y \geq \left(1 + \frac{1}{U} + \frac{\varepsilon}{L}\right)k_2 - \frac{U}{L}y > k_2$$

elégg nagy K -ra (és így k_2 -re is). Továbbá nyilvánvaló, hogy $x \leq p(z) < Uk_2 \leq k_3$. Ezért $\phi(x) = +$, hiszen $x \in (k_2, k_3]$. Tehát ismét találtunk egy monokromatikus megoldást, amelyre $\max(x, y, z) \geq K$ (mivel $x > k_2 > K$).

Mindkét esetben egy-egy monokromatikus megoldást találtunk, amelyre $\max(x, y, z) \geq K$. Mivel K tetszőlegesen nagy lehetett, ez azt jelenti, hogy $ax + by = p(z)$ egyenletnek végtelen sok monokromatikus megoldása van. Ezzel az ellentmondással befejeztük a 2. állítás bizonyítását. $\square$

A továbbiakban legyen k_1 és k_2 két szomszédos d -váltás, melyekre $k_1 < k_2 < Uk_1$. A 2. állítás miatt k_1 tetszőlegesen nagy lehet; vegyük $\frac{1}{\varepsilon_0}M$ -nél nagyobbak, ahol M a $\max(x, y, z)$ maximális értéke az $ax + by = p(z)$ egyenlet összes monokromatikus megoldása között. (Az ε_0 értéket 1-nél kisebbnek vesszük, hogy ez M -nél is nagyobb legyen.) Később néhány további feltételt is meg fogunk határozni arra vonatkozóan, hogy mekkora k_1 -t vegyünk. Most k egyezzen meg vagy k_1 -gyel, vagy k_2 -vel. Az általánosság csorbítása nélkül feltételezhetjük, hogy $\phi(k) = +$ és $\phi(k + d) = -$.

Vegyünk egy tetszőleges $0 < j < \frac{p(k)}{a}$ egészt, melyre $j \equiv v \pmod{u}$. Ekkor (6) miatt adódik, hogy $b \mid p(k) - aj$. Tekintsük a következő két egyenletet, ahol m a (3) feltétel szerint van definiálva (és (2) miatt egész):

$$aj + b \cdot \frac{p(k) - aj}{b} = p(k)$$

$$a(j + m) + b \cdot \frac{p(k) - aj}{b} = p(k + d)$$

Mivel az $ax + by = p(z)$ minden monokromatikus megoldására $\max(x, y, z) < k$, ezért a $\left(j, \frac{p(k)-aj}{b}, k\right)$ és a $\left(j + m, \frac{p(k)-aj}{b}, k + d\right)$ hármasok egyike sem lehet monokromatikus. Ebből következik, hogy $\phi(j) \leq \phi(j + m)$, hiszen máskülönben $\phi(j) = +$ és $\phi(j + m) = -$, és függetlenül $\frac{p(k)-aj}{b}$ színétől, az említett két hármas egyike monokromatikus lesz.

Tehát minden olyan $\gamma \in \mathbb{Z}_m$ maradékosztály esetén, ahol $\gamma \equiv v \pmod{u}$ (vegyük észre, hogy ez értelmes, hiszen $u \mid m$), ϕ monoton $(m\mathbb{Z} + \gamma) \cap \left[1, \frac{p(k)}{a}\right)$ elemein. Minden ilyen γ maradékosztály esetében legyen $\beta(\gamma)$ a $(m\mathbb{Z} + \gamma) \cap \left[1, \frac{p(k)}{a}\right)$ legkisebb olyan eleme, amely $+$ színű. Ha nincs ilyen, legyen $\beta(\gamma) = \frac{p(k)}{a}$.

Ezután definiáljuk a következő halmazt:

$$A = \left\{ \gamma \in u\mathbb{Z}_m + v : \beta(\gamma) \geq \frac{p(k)}{a+b+\varepsilon_1} \right\}.$$

3. Állítás. Minden $\gamma \in u\mathbb{Z}_m + v$ esetén létezik egy egyértelmű $\gamma' \in u\mathbb{Z}_m + v$, amelyre $a\gamma' \equiv p(k) - b\gamma \pmod{m}$, ez pedig megad egy $u\mathbb{Z}_m + v \rightarrow u\mathbb{Z}_m + v$, $\gamma \mapsto \gamma'$ bijekciót.

Bizonyítás. Mivel $\text{luko}(m', u) = 1$, a $\gamma, \gamma + u, \gamma + 2u, \dots, \gamma + (m' - 1)u \pmod{m}$ maradékok teljes maradékrendszert alkotnak $\pmod{m'}$. Ez viszont az összes olyan $\pmod{m}$ maradék, amely kongruens v -vel $\pmod{u}$. Mivel $\text{luko}(a, m') = 1$ is teljesül, $\{a\gamma, a(\gamma + u), a(\gamma + 2u), \dots, a(\gamma + (m' - 1)u)\}$ szintén teljes maradékrendszert alkot $\pmod{m'}$. Az (5) feltétel miatt $p(k) \equiv (a+b)\gamma \pmod{u}$. Tehát az $a\gamma' \equiv p(k) - b\gamma$ szükséges feltétel teljesül $\pmod{u}$, függetlenül attól, hogy $u\mathbb{Z}_m + v$ melyik elemét választjuk. Mivel $m = um'$ és $\text{luko}(u, m') = 1$, a feltételnek már csak $\pmod{m'}$ kell teljesülnie. Létezik egy egyértelmű $w \in \{0, 1, 2, \dots, m' - 1\}$, amelyre $a(\gamma + wu) \equiv p(k) - b\gamma \pmod{m'}$, és így $\gamma' = \gamma + wu$ az egyetlen megoldás. A leképezés injektív, mert $a\gamma' \equiv a\gamma'' \equiv p(k) - b\gamma \pmod{m}$ azt jelentené, hogy $m' \mid m \mid a(\gamma' - \gamma'')$, és mivel $\text{luko}(a, m') = 1$, ez azt jelenti, hogy $\gamma' \equiv \gamma'' \pmod{m'}$, de $u\mathbb{Z}_m + v$ minden eleme különböző $\pmod{m'}$, ami ellentmondás. $\square$

4. Állítás. Minden $\gamma \in u\mathbb{Z}_m + v$ esetén vagy γ vagy γ' eleme A -nak.

Bizonyítás. Tegyük fel, hogy egyikük sem eleme A -nak. Ebben az esetben az $ax + by = p(z)$ -ra adunk egy monokromatikus megoldást, amelyben $z = k$, ami ellentmondást eredményez (mivel tudjuk, hogy minden ilyen megoldás esetén $\max(x, y, z) < k_1$). Ismét legyen $ra + sb = 1$, $r, s \in \mathbb{Z}$, és legyenek x_0, y_0 egész számok, amelyekre $x_0 \equiv \gamma'$ és $y_0 \equiv \gamma \pmod{m}$. Tudjuk, hogy $a\gamma' + b\gamma \equiv p(k) \pmod{m}$, ezért $ax_0 + by_0 = p(k) + \ell m$ valamilyen $\ell \in \mathbb{Z}$ esetén. Ha $x_1 = x_0 - r\ell m$ és $y_1 = y_0 - s\ell m$, akkor $ax_1 + by_1 = p(k)$. Minden $w \in \mathbb{Z}$ esetén, ha $x = x_1 + wbm$ és $y = y_1 - wam$, akkor $ax + by = p(k)$, ahol $x \equiv \gamma'$ és $y \equiv \gamma \pmod{m}$. A 2. állítás bizonyításánál látott érveléshez hasonlóan létezik olyan w , hogy

$$\frac{p(k)}{a+b} - \frac{a+b}{2} \cdot m \leq x, y \leq \frac{p(k)}{a+b} + \frac{a+b}{2} \cdot m.$$

Mivel ε_1 -t k_1 -től függetlenül választottuk, és m egy olyan polinom k -ban, amelynek a foka kisebb mint p -nek, ezért k_1 -t (és így k -t) vehetjük elég nagynak ahhoz, hogy

$$\frac{p(k)}{a+b+\varepsilon_1} \leq \frac{p(k)}{a+b} - \frac{a+b}{2} \cdot m \leq x, y \leq \frac{p(k)}{a+b} + \frac{a+b}{2} \cdot m < \frac{p(k)}{a}.$$

Mivel $\gamma, \gamma' \notin A$, az $m\mathbb{Z} + \gamma$ és $m\mathbb{Z} + \gamma'$ halmazok minden $\left[\frac{p(k)}{a+b+\varepsilon_1}, \frac{p(k)}{a} \right)$ -beli eleme + színű. Tehát $\phi(x) = \phi(y) = +$, és azt is tudjuk, hogy $\phi(k) = +$, tehát $z = k$ -val (x, y, z) egy monokromatikus megoldás, ez pedig ellentmondás. $\square$

5. Állítás. $aA + bA = u\mathbb{Z}_m + p(v)$.

Bizonyítás. Tekintsük az $i : \gamma \mapsto \gamma'$ permutációt az $u\mathbb{Z}_m + v$ halmazon, és írjuk i -t diszjunkt ciklusok szorzataként. A 4. állítás szerint egy tetszőleges ciklusban, bármely két szomszédos elem közül legalább az egyiknek A -hoz kell tartoznia, tehát a ciklus tagjainak legalább a fele

A -ban van. Ezt összevetve azzal a ténnyel, hogy az alaphalmaz számossága páratlan (m' páratlan (3) szerint), azt kapjuk, hogy $|A| > \frac{1}{2}|u\mathbb{Z}_m + v|$.

Tetszőleges $\gamma_1, \gamma_2 \in A$ esetén $a\gamma_1 + b\gamma_2 \equiv (a+b)v \pmod{u}$, tehát (4) szerint $a\gamma_1 + b\gamma_2 \equiv p(v) \pmod{u}$, vagyis $aA + bA \subseteq u\mathbb{Z}_m + p(v)$. Most rögzítsünk egy $\delta \in u\mathbb{Z}_m + p(v)$ elemet. A 3. állításban bebizonyítottuk, hogy létezik egy $i : u\mathbb{Z}_m + v \rightarrow u\mathbb{Z}_m + v$ bijekció, amelyre minden $\gamma \in u\mathbb{Z}_m + v$ esetén $ai(\gamma) + b\gamma \equiv p(k) \pmod{m}$. Az egyetlen feltétel, amit ebben a bizonyításban használtunk, hogy $(a+b)v \equiv p(k) \pmod{u}$. Tehát ugyanígy bebizonyíthatjuk, hogy létezik egy olyan $j : u\mathbb{Z}_m + v \rightarrow u\mathbb{Z}_m + v$ bijekció, hogy minden γ esetén $aj(\gamma) + b\gamma \equiv \delta \pmod{m}$. Ez azért van így, mert a (4) alapján tudjuk, hogy $\delta \equiv p(v) \equiv (a+b)v \pmod{u}$. A j permutáció ismét kifejezhető diszjunkt ciklusok szorzataként, és mivel $|A| > \frac{1}{2}|u\mathbb{Z}_m + v|$, legalább egy ciklus elemeinek több mint fele A -ban van. Ekkor ennek a ciklusnak van két szomszédos eleme, ami A -ban van, tehát létezik $\gamma \in A$, amelyre $j(\gamma) \in A$. Ekkor $\delta \equiv aj(\gamma) + b\gamma \pmod{m}$, tehát $\delta \in aA + bA$. Ezzel az 5. állítás bizonyítását befejeztük. $\square$

6. Állítás. Az $[\varepsilon_0 k, (1 - \varepsilon_0)k] \cap (u\mathbb{Z} + v)$ halmaz minden eleme + színű.

Bizonyítás. Először is rögzítsük az ε_0 értékét úgy, hogy $0 < \varepsilon_0 < \frac{1}{2}$ és $\frac{1}{v}(1 - \varepsilon_0) > \varepsilon_0$ teljesüljön. (Az $\varepsilon_0 < \frac{1}{2}$ feltétel szükséges ahhoz, hogy ez az intervallum ne legyen üres, a másik feltételre később lesz szükség.)

Legyen $i \in [\varepsilon_0 k, (1 - \varepsilon_0)k]$ egy egész szám, amelyre $i \equiv v \pmod{u}$. Ekkor $p(i) \equiv p(v) \pmod{u}$. Az 5. állításban láttuk, hogy függetlenül attól, hogy $p(i)$ milyen mod m maradékosztályban van (ezt az osztályt jelöljük $\overline{p(i)}$ -vel), felírhatjuk mint $\overline{p(i)} = a\bar{j}_1 + b\bar{j}_2$ ahol $\bar{j}_1, \bar{j}_2 \in A$. A $\bar{j}_1$ és $\bar{j}_2$ modulo m osztályoknak rögzítsük a j_1 és j_2 tetszőleges reprezentánsait. Ekkor $aj_1 + bj_2 = p(i) + \ell m$ valamilyen $\ell \in \mathbb{Z}$ esetén. Legyen $ra + sb = 1$ és helyettesítsük j_1 -t és j_2 -t a $j_1 - rlm$ és $j_2 - slm$ reprezentánsokkal. Így feltételezhetjük, hogy $\ell = 0$, vagyis $aj_1 + bj_2 = p(i)$.

Megmutatjuk, hogy léteznek olyan j'_1 és j'_2 reprezentánsai az említett osztályoknak, hogy $aj'_1 + bj'_2 = p(i)$ és $0 < j'_1, j'_2 < \frac{p(k)}{a+b+\varepsilon_1}$. Ha ezt sikerül kimutatni, akkor A definíciója szerint $\phi(j'_1) = \phi(j'_2) = -$, és a $\phi(i) = -$ indirekt feltételezésre alapozva az $ax + by = p(z)$ egy olyan monokromatikus megoldás lenne, amelyre $\max(x, y, z) \geq i \geq \varepsilon_0 k > M$, ami ellentmond az M definíciójának.

Tetszőleges $w \in \mathbb{Z}$ esetén legyen $j'_1 = j_1 + wbm$ és $j'_2 = j_2 - wam$. Ekkor $aj'_1 + bj'_2 = p(i)$ és a szokásos érveléssel kiválaszthatjuk w -t úgy, hogy

$$\frac{p(i)}{a+b} - \frac{a+b}{2}m \leq j'_1, j'_2 \leq \frac{p(i)}{a+b} + \frac{a+b}{2}m.$$

A $p(z)$ és $p(z+d) - p(z)$ olyan n , illetve $n-1$ fokú polinomok, amelyek főegyütthatója pozitív. Így léteznek a K_1, K_2, C, D, E, F pozitív valós számok (p, d és ε_0 függvényében), amelyekre $Ez^n \leq p(z) \leq Fz^n$ minden $z \geq K_1$ valós számra, és $Cz^{n-1} \leq p(z+d) - p(z) \leq Dz^{n-1}$ minden $z \geq K_2$ valós számra. Itt $\frac{F}{E}$ bármilyen 1-nél nagyobb valós szám lehet, így megkövetelhetjük, hogy $F < E \cdot \frac{1}{(1-\varepsilon_0)^n}$ teljesüljön. Továbbá létezik $K_3 > 0$ úgy, hogy p monoton nő a $[K_3, \infty)$ halmazon.

Ekkor $F(1 - \varepsilon_0)^n < E$ alapján választhatunk egy $\varepsilon_1 > 0$ elég kicsi számot, amelyre

$$\frac{F(1 - \varepsilon_0)^n}{a + b} < \frac{E}{a + b + \varepsilon_1}. \quad (*)$$

Elég nagy k esetén $\varepsilon_0 k \geq K_3, K_1$, ami azt jelenti, hogy

$$E(\varepsilon_0 k)^n \leq p(\varepsilon_0 k) \leq p(i) \leq p((1 - \varepsilon_0)k) \leq F((1 - \varepsilon_0)k)^n. \quad (**)$$

Továbbá $k \geq K_2$ esetén azt kapjuk, hogy

$$\frac{Ck^{n-1}}{a} \leq m = \frac{p(k + d) - p(k)}{a} \leq \frac{Dk^{n-1}}{a}. \quad (***)$$

A (*), (**) és (***) egyenlőtlenségek alapján kellően nagy k esetén az alábbiakat kapjuk

$$j'_1, j'_2 \leq \frac{p(i)}{a + b} + \frac{a + b}{2}m \leq \frac{F(1 - \varepsilon_0)^n}{a + b}k^n + \frac{a + b}{2} \cdot \frac{D}{a}k^{n-1} < \frac{E}{a + b + \varepsilon_1}k^n$$

ahol $k \geq K_1$ esetén $Ek^n \leq p(k)$, tehát $j'_1, j'_2 < \frac{p(k)}{a + b + \varepsilon_1}$.

Továbbá, a (**) és a (***) felhasználásával, elég nagy k esetén azt kapjuk, hogy

$$j'_1, j'_2 \geq \frac{p(i)}{a + b} - \frac{a + b}{2}m \geq \frac{E\varepsilon_0^n}{a + b}k^n - \frac{D}{a}k^{n-1} > 0.$$

Tehát igazoltuk, hogy $\phi(i) = +$, és ezzel a 6. állítás bizonyítását befejeztük. $\square$

Az 1.1 tétel bizonyításának befejezéséhez figyeljük meg, hogy az eddigi érvelés $k = k_1$ és $k = k_2$ esetén is fennáll. Az általánosság csorbítása nélkül feltételezhetjük, hogy $\phi(k_1) = +$ és $\phi(k_2) = -$. Ekkor (mivel feltételeztük, hogy $\phi(k) = +$) a 6. állítás szerint az $[\varepsilon_0 k_1, (1 - \varepsilon_0)k_1] \cap (u\mathbb{Z} + v)$ minden eleme $+$ színű, és az $[\varepsilon_0 k_2, (1 - \varepsilon_0)k_2] \cap (u\mathbb{Z} + v)$ minden eleme $-$ színű. Ha a két halmaznak van közös eleme, akkor ellentmondást kapunk. Ehhez elégséges feltétel, hogy $(1 - \varepsilon_0)k_1 \geq \varepsilon_0 k_2 + u$. Mivel $\varepsilon_0 < \frac{1}{U}(1 - \varepsilon_0)$, elég nagy k_1 (és így k_2) esetén $\varepsilon_0 k_2 + u < \frac{1}{U}(1 - \varepsilon_0)k_2 < (1 - \varepsilon_0)k_1$. (Itt használjuk azt a tényt, hogy $k_2 < Uk_1$.)

Ezzel befejeztük az 1.1 tétel bizonyítását. $\square$

1.2 Következmény bizonyítása. Írjuk fel a -t és b -t $a = 2^{\alpha_1} \prod_{i=2}^r p_i^{\alpha_i}$, $b = \prod_{j=1}^s q_j^{\gamma_j}$ alakban, ahol a p_i -k és q_j -k páronként különböző prímek, $p_1 = 2$, $\alpha_1 \geq 0$ és minden más kitevő pozitív. (Ha a páratlan és b páros, akkor felcseréljük őket.)

Legyen

$$d = \prod_{i=1}^r p_i^{\max\{\alpha_i, \nu_{p_i}(a_1)+1\}} \cdot \prod_{j=1}^s q_j^{\max\{\gamma_j, \nu_{q_j}(a_1)+1\}}$$

és $t = 0$ (megjegyezzük, hogy $a_1 \neq 0$ miatt $\nu_q(a_1)$ jól definiált minden q prímre). Legyen

$$u = \prod_{i=1}^r p_i^{\max\{\nu_{p_i}(a_1), 2\nu_{p_i}(a_1)+1-\alpha_i\}} \cdot \prod_{j=1}^s q_j^{\max\{\gamma_j + \nu_{q_j}(a_1), 2\nu_{q_j}(a_1)+1\}}$$

és $v = 0$. Ezek a választások kielégítik az 1.1 tétel feltételeit, mivel ha feltesszük, hogy $d \mid k$ és $u \mid j$:

- (1) $(a + b) \cdot 0 = 0 \equiv p(0) \pmod{d}$
- (2) Mivel $a \mid d$, ezért $a \mid p(k + d) - p(k)$.
- (3) Azt kapjuk, hogy

$$m = \frac{p(k + d) - p(k)}{a} = \frac{\sum_{i=1}^d a_i [(k + d)^i - k^i]}{a}.$$

Mivel $d \mid k$, $d^i \mid (k + d)^i - k^i$. Vegyük észre, hogy bármely $q \in \{p_i, q_j \mid i = 1, \dots, r, j = 1, \dots, s\}$ esetén $v_q(d^2) > v_q(a_1 d)$, így

$$v_q(p(k + d) - p(k)) = v_q(a_1 d),$$

amiből következik, hogy

$$v_q(m) = v_q(a_1) + v_q(d) - v_q(a).$$

Tehát $v_q(m) = v_q(u)$, ezért $u \mid m$ és $\text{Inko}(m', 2ab) = 1$.

- (4) $(a + b) \cdot 0 = 0 \equiv p(0) \pmod{d}$
- (5) $u \mid p(k)$, mivel $d \mid k$, $u \mid d^2$ és $u \mid a_1 d$. Emiatt $(a + b) \cdot 0 = 0 \equiv p(k) \pmod{u}$.
- (6) $b \mid p(k) - a_j$, mert $b \mid u$, $u \mid j$ és $u \mid p(k)$ teljesülnek (5) miatt.

□

2.1. Megjegyzés. Ez a bizonyítás megmutatja, hogy az állítás akkor is igaz, ha $p(z)$ -hoz a_0 konstans tagot adunk, amely kielégíti a $d \mid a_0$ és $u \mid a_0$ feltételeket. Itt $d \mid a_0$ biztosítja, hogy (1) igaz maradjon, $u \mid a_0$ pedig azt, hogy (4) és (5) továbbra is érvényes maradjon.

Megjegyezzük, hogy a és b szerepe a bizonyításban felcserélhető, hogy u -ra más értéket kapjunk, amelyet szintén használhatunk a fenti megfigyelésünkben.

1.3 Következmény bizonyítása. Írjuk n -t $n = 2^\gamma \prod_{i=1}^r p_i^{\gamma_i}$ alakba, ahol a p_i -k különböző páratlan

prímek, γ nemnegatív egész és γ_i -k pozitív egészek. Fejezzük ki a -t a $a = 2^\alpha a' \prod_{i=1}^r p_i^{\alpha_i}$ alakban, ahol α és az α_i -k nemnegatív egészek és $\text{Inko}(a', 2n) = 1$. Az általánosság csorbítása nélkül feltehetjük, hogy $\alpha = \alpha' n - \alpha_0$ valamilyen α' , $\alpha_0 \in \mathbb{Z}^{\geq 0}$ -ra. α' és α_0 választása nem feltétlenül egyértelmű, azonban megválaszthatjuk őket úgy, hogy ha $\alpha = 0$, akkor $\alpha' = \alpha_0 = 0$. Legyen most

$$d = 2^{\alpha'} a'', \text{ és } u = 2^{\alpha_0} \cdot \prod_{\substack{p \mid \text{Inko}(n, a) \\ p \geq 3 \text{ prím}}} p^{v_p(n)},$$

ahol $a'' = a' \prod_{i=1}^r p_i^{\alpha_i}$. Könnyen láthatóan $u = 2^{\alpha_0} \cdot \prod_{i \in J} p_i^{v_{p_i}(n)}$ egy ekvivalens definíció u -ra, ahol

$$J = \{i \in \{1, 2, \dots, r\} : p_i \mid a''\} = \{i \in \{1, 2, \dots, r\} : \alpha_i \neq 0\}.$$

t -t úgy fogjuk definiálni, hogy az kielégítse az alábbi kongruencia relációkat:

$$\begin{cases} t \equiv 0 & (\text{mod } 2^{\alpha'}) \\ t \equiv 1 & (\text{mod } a'') \end{cases}$$

v -t pedig úgy, hogy $v \equiv (a+1)^{-1} t^n \pmod{u}$. Ez a definíció a következő két tény miatt értelmes:

- Először is használtuk, hogy $a+1$ -nak létezik multiplikatív inverze modulo u .

Bizonyítás. u minden p prímosztójára, vagy $p = p_i$ valamely $i \in J$ -re, vagy $p = 2$. Ha $p = p_i$, akkor $p \mid a'' \mid a$, ezért $p \nmid a+1$. Ha $p = 2$, akkor $\alpha_0 \neq 0$, amiből következik, hogy $\alpha \neq 0$, így $p \mid a$ and $p \nmid a+1$. Ebből azt kapjuk, hogy $\text{lko}(u, a+1) = 1$, innen adódik az állítás. $\square$

- Másrészt, mivel t egy modulo $d = 2^{\alpha'} a''$ maradékosztály és nem pedig modulo u , be kell látnunk, hogy ha $t_1 \equiv t \pmod{d}$ akkor $(a+1)^{-1} t_1^n \equiv (a+1)^{-1} t^n \pmod{u}$. Ez az eredmény a következő állítás következménye.

Állítás. Ha $t_1 \equiv t \pmod{d}$, akkor $t_1^n \equiv t^n \pmod{u}$, ahol d -t, u -t és t -t a fentiek szerint definiáljuk.

Bizonyítás. Valóban, ha $t_1 \equiv t \pmod{d}$, akkor $t_1 = t + t_2 d$ valamilyen t_2 egészre. t definíciójából azt kapjuk, hogy $t = 2^{\alpha'} t'$ valamilyen t' egészre, így

$$t_1^n - t^n = \left(2^{\alpha'} t' + t_2 2^{\alpha'} a''\right)^n - \left(2^{\alpha'} t'\right)^n = 2^{\alpha' n} \left[(t' + t_2 a'')^n - (t')^n\right],$$

ezért mondhatjuk, hogy $v_2(t_1^n - t^n) \geq \alpha' n = \alpha + \alpha_0 \geq \alpha_0 = v_2(u)$. Ha veszünk egy másik $p \geq 3$ prímet, hogy $p \mid u$, akkor tudjuk, hogy $p = p_i$ valamilyen $i \in J$ -re. $p > 2$ -ből következik, hogy $p \mid a''$, ami maga után vonja, hogy

$$\text{lko}(p, t) = \text{lko}(p, t_1) = 1,$$

mert t és t_1 invertálhatók modulo a'' . Másrészt $p = p_i \mid dt_2 = t_1 - t$, így az ún. Lifting-the-exponent lemmából adódik, hogy

$$\begin{aligned} v_p(t_1^n - t^n) &= v_p(n) + v_p(dt_2) = \gamma_i + v_p(2^{\alpha'}) + v_p(a'') + v_p(t_2) \\ &= \gamma_i + 0 + \alpha_i + v_p(t_2) \geq \gamma_i = v_p(u). \end{aligned}$$

Mivel $v_p(u) \leq v_p(t_1^n - t^n)$ igaz u bármely p prímosztójára, $t_1^n \equiv t^n \pmod{u}$. $\square$

Most már készen állunk annak bizonyítására, hogy az 1.1 Tétel feltételei teljesülnek. Valóban:

- (1) Az $(a+1)t \equiv t^n$ összefüggés teljesül modulo $2^{\alpha'}$ és modulo a'' , továbbá, $\text{lko}(2^{\alpha'}, a'') = 1$, tehát szintén teljesül modulo $2^{\alpha'} a'' = d$;
- (2) Tudjuk, hogy $k + d \equiv k \equiv t \pmod{d}$, tehát a fenti Állítás bizonyításában szereplő érvelést használva minden $i \in J$, $p = p_i$ -re:

$$v_p((k+d)^n - k^n) = \gamma_i + \alpha_i + v_p(1) = \gamma_i + \alpha_i \geq \alpha_i = v_p(a),$$

és $p = 2$ -re:

$$v_p((k+d)^n - k^n) = \alpha + \alpha_0 \geq \alpha = v_p(a).$$

Most bebizonyítjuk, hogy $a' \mid (k+d)^n - k^n$, így az előző állításokkal együtt azt kapjuk, hogy $a \mid (k+d)^n - k^n$. Valóban, mivel $k \equiv t \equiv 1 \pmod{a''}$, ezért $k = 1 + k_1 a'$ valamilyen k_1 egészre, és $d = d_1 a'$, ahol $d_1 = 2^{\alpha'} \prod_{i=1}^r p_i^{\alpha_i}$. A lifting-the-exponent lemma segítségével minden $p \mid a'$ prímre adódik, hogy

$$\begin{aligned} v_p((k+d)^n - k^n) &= v_p((1 + (k_1 + d_1)a')^n - (1 + k_1 a')^n) \\ &= v_p(n) + v_p(a' d_1) = v_p(a'), \end{aligned}$$

ahol az utolsó egyenlőség $\text{lno}(a', n) = \text{lno}(a', d_1) = 1$ következménye.

- (3) A (2) apró módosításával könnyen látható, hogy $au \mid (k+d)^n - k^n$, ezért $u \mid m$. Még egyszer a (2)-beli eredményeket használva és a tényt, hogy $v_p(m') = v_p((k+d)^n - k^n) - v_p(u) - v_p(a)$ minden p prímre, igaz, hogy

$$v_p(m') = \begin{cases} \alpha + \alpha_0 - \alpha_0 - \alpha, & p = 2; \\ \gamma_i + \alpha_i - \gamma_i - \alpha_i, & p = p_i, i \in J; \\ v_p(a') - v_p(a'), & p \mid a'; \\ v_p(m'), & \text{otherwise.} \end{cases},$$

amelyből (3) további feltételei következnek.

- (4) (1)-ből az állításunk alkalmazásával megkapjuk, hogy $t^n \equiv \left((1+a)^{-1} t^n\right)^n \pmod{u}$, amely ekvivalens $(1+a)v \equiv v^n \pmod{u}$ -val;
 (5) Kihasználva azt a tényt, hogy $(1+a)v \equiv (1+a)(1+a)^{-1} t^n \pmod{u}$, ismét alkalmazhatjuk az állításunkat, hogy megkapjuk, hogy $k^n \equiv (1+a)v \pmod{u}$;
 (6) $b = 1$ -ből következik, hogy $b \mid p(k) - aj$, minden $k, j \in \mathbb{Z}$ -re.

□

1.4 Következmény bizonyítása. Legyen $d = aBp^n$ és legyen t a tétel állítása szerint. $p \neq 2$ esetén legyen $u = 2^{v_2(c)} p^{v_p(c)+pn} B$, míg $p = 2$ esetén legyen $u = p^{v_p(c)+pn} B$. Válasszuk $v \in \mathbb{Z}_u$ -t úgy, hogy a

$$\begin{cases} v \equiv 0 & \pmod{p^{v_p(c)+pn}} \\ v \equiv 0 & \pmod{2^{v_2(c)}} \\ v \equiv t & \pmod{B} \end{cases}$$

kongruenciák teljesüljenek. Megjegyezzük, hogy a tétel feltételei alapján minden esetben létezik ilyen v (vegyük észre, hogy ha $2 \mid B$, akkor $v_2(c) = 0$). Ezek a választások kielégítik a 1.1 Tétel feltételeit, ha feltesszük, hogy $k \equiv t \pmod{d}$ és $j \equiv v \pmod{u}$:

- (1) $(a+b) \cdot t \equiv ct^p \pmod{d}$ teljesül a t -re tett kikötések miatt.
 (2) Mivel $a \mid d$, azt kapjuk, hogy $a \mid c(k+d)^p - ck^p$.
 (3) Először is jegyezzük meg, hogy mivel a, B és c páronként relatív prímek és $\text{lno}(a, b) = 1$, k relatív prím a -hoz és B -hez. Adódik, hogy

$$m = c \cdot \frac{(k+d)^p - k^p}{a} = c \cdot \sum_{i=1}^p \binom{p}{i} \frac{d^i}{a} k^{p-i}.$$

Mivel $a \mid d$, az összeg minden tagja osztható a -val, az első tagot, $\frac{pdk^{p-1}}{a}$ kivéve, amelyek relatív prím a -hoz. Ezért $\text{Inko}(a, m) = 1$. Hasonlóan, $B \mid m$, de $\text{Inko}(\frac{m}{B}, B) = 1$.

Mivel $p^n \mid k$, $k = p^n \ell$ valamely $\ell \in \mathbb{Z}^+$ -re. Ekkor

$$(k + d)^p - k^p = p^{pn} ((\ell + aB)^p - \ell^p).$$

$(\ell + aB)^p - \ell^p \equiv \ell + aB - \ell = aB \not\equiv 0 \pmod{p}$, ezért $v_p(m) = v_p(c) + pn$.

Így, ha $p = 2$, akkor $m' = \frac{m}{u} \in \mathbb{Z}$ és $\text{Inko}(m', a) = \text{Inko}(m', B) = \text{Inko}(m', 2) = 1$.

Ha $p \neq 2$, akkor is azt kapjuk, hogy $m'' = \frac{m}{p^{v_p(c)+pn}B} \in \mathbb{Z}$, amelyre $\text{Inko}(m'', a) = \text{Inko}(m'', B) = \text{Inko}(m'', p) = 1$. Ha $2 \mid a$ vagy $2 \mid B$, akkor $v_2(c) = 0$, $m'' = m'$ és $\text{Inko}(m', 2) = 1$. Máskülönben $m' = \frac{m''}{2^{v_2(c)}} = \frac{m}{u} \in \mathbb{Z}$ és $\text{Inko}(m', 2) = 1$, mivel $2 \nmid (k + d)^p - k^p$, hiszen d páratlan.

Így mindkét esetben $u \mid m$, $2 \nmid m'$ és $(a, m') = (b, m') = (u, m') = 1$.

- (4) $(a + b)v \equiv 0 \equiv cv^p \pmod{2^{v_2(c)}}$, $(a + b)v \equiv 0 \equiv cv^p \pmod{p^{v_p(c)+pn}}$ és $(a + b)v \equiv at \equiv ct^p \equiv cv^p \pmod{B}$, t választása miatt. Így az ekvivalencia teljesül modulo u is.
- (5) $(a + b)v \equiv 0 \equiv ck^p \pmod{2^{v_2(c)}}$, $(a + b)v \equiv 0 \equiv ck^p \pmod{p^{v_p(c)+pn}}$, hiszen $p^n \mid k$ és $(a + b)v \equiv at \equiv ct^p \equiv ck^p \pmod{B}$. Vagyis az ekvivalencia teljesül modulo u is.
- (6) Az (5) miatt kapjuk, hogy $B \mid ck^p - aj$, ugyanis $aj \equiv (a + b)v \pmod{B}$. Továbbá $p^{pn-\varepsilon} \mid ck^p - aj$, mivel p^{pn} osztja mind k^p -t és j -t. Tehát $b \mid ck^p - aj$.

□

1.5 Következmény bizonyítása. Az általánosság csorbítása nélkül feltételezhetjük, hogy a páratlan. Ekkor alkalmazhatjuk az 1.4 következményt az $ax + by = cz^2$ egyenletre, mert a kongruencia-rendszer megoldhatóságára vonatkozó feltétel automatikusan érvényes, ha $p = 2$. Tehát az $ax + by = cz^2$ egyenlet 2-Ramsey. □

A következő lemma segítségével kiterjeszthetjük $ax + by = cz^2$ (ahol a, b, c páronként relatív prímek) 2-Ramseységét $d(ax + by) = cz^2$ -re.

2.2. Lemma. *Tegyük fel, hogy az $ax + by = p(z) = \sum_{i=0}^d a_i c^{i-2} z^i$ egyenlet 2-Ramsey, ahol*

$a, b, c, a_d \in \mathbb{Z}^+$, $p \in \mathbb{Z}[z]$, $c \mid a_1$ és $c^2 \mid a_0$. Ekkor az $acx + bcy = p'(z) = \sum_{i=0}^d a_i z^i$ egyenlet 2-Ramsey.

Bizonyítás. Legyen ϕ a $\mathbb{Z}^+$ halmaz egy 2-színezése. Tekintsük az $acx + bcy = p(z)$ egyenletnek csak azokat a megoldásait, amelyekre x, y, z mind osztható c -vel. Legyen $x = cx'$, $y = cy'$ és $z = cz'$. Az egyenletbe behelyettesítve az x, y, z hármast akkor és csak akkor kapunk megoldást, ha

$$ax' + by' = \sum_{i=0}^d a_i c^{i-2} (z')^i = p'(z').$$

Legyen $\psi(j) := \phi(cj)$ a $\mathbb{Z}^+$ egy másik 2-színezése. Ekkor a feltétel szerint végtelen sok olyan x', y', z' megoldás létezik, hogy $ax' + by' = p'(z')$ és $\psi(x') = \psi(y') = \psi(z')$. Az ilyen

megoldások esetén viszont $acx + bcy = p(z)$ és a ψ definíciója szerint $\phi(x) = \phi(y) = \phi(z)$. Tehát az $acx + bcy = p'(z)$ egyenlet 2-Ramsey. $\square$

Az 1.6 Következmény bizonyítása. Az állítás közvetlenül adódik az 1.5 következményből és a 2.2 lemmából. $\square$

HIVATKOZÁSOK

- [1] V. Bergelson, *Ergodic Ramsey theory. In Logic and combinatorics* (Arcata, Calif., 1985), Contemp. Math., 65, (1987), 63–87, Amer. Math. Soc., Providence, RI, 1987.
- [2] V. Bergelson, A. Leibman, *Polynomial extensions of van der Waerden's and Szemerédi's theorems*, J. Amer. Math. Soc., 9(3), (1996), 725–753.
- [3] S. Chow, S. Lindqvist, S. Prendiville, *Rado's criterion over squares and higher powers*, arXiv:1806.05002.
- [4] P. Csikvári, K. Gyarmati, A. Sárközy, *Density and Ramsey type results on algebraic equations with restricted solution sets*, Combinatorica, 32, (2012), 425–449.
- [5] M. Di Nasso, L. Luperi Baglini, *Ramsey properties of nonlinear Diophantine equations*, Advances in Mathematics, 324, (2018), 84–117.
- [6] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. d'Analyse Math., 31, (1977), 204–256.
- [7] B. Green, S. Lindqvist, *Monochromatic solutions to $x + y = z^2$* , Canadian Journal of Mathematics, to appear.
- [8] B. Green, T. Sanders, *Monochromatic sums and products*, Discrete Analysis, 5, (2016), 48pp.
- [9] A. Khalafallah, E. Szemerédi, *On the Number of Monochromatic Solutions of $x + y = z^2$* , Combinatorics, Probability and Computing, 15, (2006), 213–227.
- [10] M. Kneser, *Abschätzungen der asymptotischen Dichte von Summenmengen*, Math. Zeitschr., 58, (1958), 459–484.
- [11] S. Lindqvist, *Partition regularity for generalised Fermat equations*, Combinatorica, to appear.
- [12] H. Liu, P. P. Pach, Cs. Sándor, *Polynomial Schur's theorem*, arXiv: 1811.05200
- [13] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. reine angew. Math., 78, (1874), 199–245.
- [14] J. Moreira, *Monochromatic sums and products in $\mathbb{N}$* , Annals of Mathematics, (2) 185, (2017), 1069–1090.
- [15] P. P. Pach, *Monochromatic solutions to $x + y = z^2$ in the interval $[N, cN^4]$* , arXiv:1805.06279.
- [16] R. Rado, *Studien zur Kombinatorik*, Math. Z., 36, (1933), 424–470.
- [17] A. Robertson, D. Zeilberger, *A 2-coloring of $[1, N]$ can have $(1/22)N^2 + O(N)$ monochromatic Schur triples, but not less!*, Electronic Journal of Combinatorics, 5 (1998), R19.
- [18] A. Sárközy, *On difference sets of sequences of integers. I*, Acta Math. Acad. Sci. Hungar., 31, (1978), 125–149.
- [19] T. Schoen, *The number of monochromatic Schur triples*, Euro. J. Combinatorics, 20, (1999), 855–866.
- [20] I. Schur, *Über die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$* , Jahresber. Dtsch. Math.-Ver., 14, (1916), 114–117.
- [21] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arithmetica, 27, (1975), 199–245.
- [22] B.L. van der Waerden, *Beweis einer boudetschen vermutung*, Nieuw. Arch. Wisk., 15, (1927), 212–216.

A pályamunka lezárásának dátuma: 2022. szeptember 30.