Erdős-Turán-tétel és általánosításai

Füredi Erik Benjamin

Matematika BSc, matematikus szakirány

Témavezető: Gyarmati Katalin egyetemi docens

Algebra és Számelmélet Tanszék

Szakdolgozat

Eötvös Loránd Tudományegyetem

Természettudományi Kar

Budapest, 2024

Tartalomjegyzék

1. Az Erdős-Turán-tétel, és előzménye

A szakdolgozat kiindulópontja Erdős Pál és Turán Pál alábbi eredménye:

1. Tétel (Erdős-Turán [2]). *Bármely $2^k + 1$ különböző pozitív egész számra, ahol k pozitív egész szám, a kéttagú összegek prímosztóiból van legalább $k + 1$ különböző.*

Itt a kéttagú összegekben a két tagot különbözőnek értjük, a későbbiekben is így teszünk.

A tétel bizonyítása:

A bizonyításban segít az alábbi lemma:

Lemma. *Bármely $2m + 1$ különböző pozitív egész számra és p páratlan prímszámra (m pozitív egész szám) a $2m + 1$ szám közül létezik $m + 1$, amelyből nincs kettő, melyek összege p olyan nagyobb hatványával osztható, amellyel valamelyikük nem.*

A lemma bizonyítása:

Írjuk fel a pozitív egész számokat $p^a h$ alakban, ahol a nemnegatív egész szám és h p-vel nem osztható pozitív egész szám. Ekkor h maradéka p-vel osztva vagy 1 és $\frac{p-1}{2}$, vagy $\frac{p+1}{2}$ és $p-1$ közé esik (a határokat is beleértve), a $2m+1$ számból skatulyaelvvel van legalább $m+1$, amelyre ugyanoda. Ekkor ezekből nincs kettő, melyek összege p olyan nagyobb hatványával osztható, amellyel valamelyikük nem. Ugyanis legyen közülük két szám a korábbi felírással $p^{a_1}h_1$ és $p^{a_2}h_2$. Ha $a_1 \neq a_2$, akkor összegük p^{a_1} és p^{a_2} közül a kisebb kitevős hatvánnyal osztható, de p nagyobb hatványával nem, mert a kisebb hatványt egy p-vel osztható és egy p-vel nem osztható szám p-vel nem osztható összegével beszorozva kapjuk a számot, ilyenkor nincs gond.

Ugyanakkor, ha $a_1 = a_2$, akkor

$$p^{a_1}h_1 + p^{a_2}h_2 = p^{a_1}(h_1 + h_2);$$

itt $h_1 + h_2$ nem osztható p-vel, mert p-vel osztva mindkettő p=2-nél kisebb vagy p=2-nél nagyobb nemnulla maradékot ad, előbbi esetben a $(0; p)$, utóbbiban a $(p; 2p)$ intervallumba esik a maradékok összege, nem osztható p-vel. Így $h_1 + h_2$ sem, ezen esetben a két számra és összegükre is a legnagyobb őket osztó p-hatvány megegyezik, p^{a_1}. A lemmát beláttuk.

Ezután indirekten bizonyítjuk a tételt. $2^k + 1 \geq 3$ miatt van skatulyaelvvel van kettő azonos paritású a $2^k + 1$ különböző pozitív egész számunk közt, melyek összege páros, így a prímosztók közt szerepel a 2. A tétel csak akkor nem teljesülhetne, ha valamely k pozitív egész

számra lenne $2^k + 1$ pozitív egész szám, amelyekre a kéttagú összegek páratlan prímosztói közt csak legfeljebb $k - 1$ prímszám lenne. Legyen a számuk $b \leq k - 1$, jelölje őket $p_1, p_2, \dots, p_b$. Ezeken sorra végigmegyünk és használjuk a lemmát b-szer.
Először p_1-hez találunk az eredeti $2^k + 1$ szám közül $2^{k-1} + 1$ számot, amelyre a belőlük képzett kéttagú összegek egyikében sincs magasabb hatványon p_1, mint az összeget kiadó valamelyik tagban.
Ezután a megmaradt $2^{k-1} + 1$ pozitív egész szám közül p_2-höz találunk $2^{k-2} + 1$ számot, amelyekre a belőlük képzett kéttagú összegek egyikében sincs magasabb hatványon p_2, mint az összeget kiadó valamelyik tagban, és persze p_1-re is megmarad a tulajdonság.
Ezt ismételjük addig, amíg kapunk $2^{k-b} + 1 \geq 3$ pozitív egész számot, amelyekre a belőlük képzett kéttagú összegek bármely páratlan prímosztója bármely kéttagú összegben legfeljebb akkora hatványon van, mint a tagokban.

Legyen a kapott pozitív egész számok közül három x, y és z. Ekkor $x+y$, $x+z$ és $y+z$ közül bármely kéttagú összegben a prímtényezős felbontásban a prímszámokból csak a 2 kitevője lehet nagyobb, mint a tagokban, így nagyobbnak is kell lennie. x-re, y-ra és z-re a legnagyobb őket osztó 2-hatvány egyenlő, ugyanis ha kettejükre ez különbözne, az összegben is a kisebb 2-hatvány lenne a legnagyobb 2-hatvány osztó (ezt már a lemma bizonyításában is használtuk más prímekre). Ekkor ezen közös 2-hatvánnyal leosztva őket olyan x', y', z' páratlan pozitív egész számokat kapnánk, amelyekre szintén nincs olyan páratlan prímszám, amelyre valamely kettő összegét magasabb hatványa osztja, mint bármelyiket a két tag közül.
x', y' és z' közül bármely kettő összege osztható 4-gyel, ugyanis előbbiek különbözősége miatt az összeg több mint kétszerese a kisebb tagnak, és a prímek közül csak a 2 van magasabb hatványon a prímtényezős felbontásában a kisebb taghoz képest.
Ez viszont ellentmodás, mert az $x' + y' + z'$ páratlan lenne, míg duplája,

$$(x' + y') + (x' + z') + (y' + z')$$

4-gyel osztható. Ezzel a tételt tagadva ellentmondásra jutottunk, így bebizonyítottuk.

A bizonyítás forrása a [2]. Az eredeti [3] cikkben $2^k + 1$ helyett $3 \cdot 2^{k-1}$ szerepel, ennyivel gyengébb eredményt kapunk, ha a lemmával prímenként csupán felezzük a számok mennyiségét.

Jelölje $f(n)$ azt a számot ($1 < n \in \mathbb{Z}$), amely n tetszőlegesen kiválasztott különböző pozitív egész számra a belőlük képzett kéttagú összegeket osztó prímszámok lehetséges minimális száma [18]. $f(n)$ értelemszerűen monoton növő, összevetve az Erdős-Turán tétellel adódik a következő állítás:

Következmény. $f(n) \geq \lceil \log_2 n \rceil$.

Már az is érdekes eredmény, hogy a monoton növő $f(n)$ minden pozitív egész számot meghalad, vagyis prímszámok bármely véges halmazára nem lehet akárhány pozitív egész számot kiválasztani úgy, hogy a kéttagú összegek összes prímosztója a véges prímhalmazból kerüljön ki. Ezt látták be a problémakört elindító Grünwald és Lázár [3], Pólya egy tételének segítségével. ($\mathbb{Z}^+$ a pozitív egész számok halmazát jelöli.)

2. Tétel (Pólya [3], [11]). *Ha prímszámok egy véges részhalmazára tekintjük a részhalmazon kívüli prímszámok egyikével sem osztható pozitív egész számok $(q_m)_{m \in \mathbb{Z}^+}$ szigorúan monoton növő sorozatát, akkor*

$$\lim_{m \to \infty} (q_{m+1} - q_m) = \infty.$$

A 2. tétel bizonyítása [11] nyomán:

Legyen a prímszámok véges részhalmazának elemei $p_1, p_2, \ldots, p_r$. Tegyük fel, hogy nem igaz a tétel állítása, ekkor van olyan K pozitív egész szám, amelyre $q_{m+1} - q_m \leq K$ végtelen sokszor teljesül. Ekkor $q_{m+1} - q_m$ végtelen sokszor felveszi az $1, 2, \ldots, K$ értékeket, így van olyan $l \leq K$ pozitív egész szám, amelyre végtelen sok h pozitív egész számra $h + l$ és h prímosztói is csak a megadott r prímszám közül kerülnek ki.

Legyen

$$h + l \text{ prímtényezős felbontása } p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

és

$$h \text{ prímtényezős felbontása } p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}.$$

Itt az összes α_i és β_i alakú kitevőt lecseréljük a 3-as maradékára, amely nála nem nagyobb szám 0, 1 és 2 közül. Ekkor a 3-as maradékot α_i-re a_i, β_i-re b_i alakban jelölve

$$h + l = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} x^3$$

valamely x pozitív egész számra és

$$h = p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r} y^3$$

valamely y pozitív egész számra, ebből a

$$p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} x^3 - p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r} y^3 = l$$

egyenletnek létezik $(x; y)$ pozitív egész megoldása. Itt az a_i és b_i kitevők összesen 3^{2r}-félék lehetnek, ez véges sok eset. Ugyanakkor Thue itt nem bizonyított tételéből következik mindre csak véges sok megoldás van:

3. Tétel (Thue [11])**.** *Egy kétváltozós racionális együtthatós homogén kettőnél magasabb fokú irreducibilis $f(x; y)$ polinomra adott c valós számra az $f(x; y) = c$ egyenletnek véges sok egész számokból álló megoldása van.*

A $p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}x^3 - p_1^{b_1}p_2^{b_2}\ldots p_r^{b_r}y^3 = l$ egyenletben az lnko$(p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}; p_1^{b_1}p_2^{b_2}\ldots p_r^{b_r})$ legnagyobb közös osztóval leosztva a bal oldal csak akkor nem irreduciblis, ha van elsőfokú, $dx + ey$ alakú osztója, de ekkor x^3 és y^3 együtthatóinak hányadosa egy racionális szám köbe, ami csak az

$$x^3 - y^3 = \frac{l}{p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}} = \frac{l}{p_1^{b_1}p_2^{b_2}\ldots p_r^{b_r}}$$

esetben állhat fenn, ekkor az egész $(x; y)$-ra egész szám $x^3 - y^3$-nek véges sokszor lehet csak az adott jobb oldallal egyező értéke, mert $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$-ben $x - y$ véges sokféle lehet, $x^3 - y^3 \neq 0$ ismeretében belőle xy meghatározható, és utána csak legfeljebb két megoldás van. Eszerint mind a 3^{2r} esetben véges sok lehetséges $(x; y)$ és vele véges sok $(h; h + l)$ létezik, ezzel ellentmondásra jutottunk. Ebből következik Pólya tételének állítása.

Pólya tételéből Grünwald és Lázár eredménye könnyen látszik. Ha lenne végtelen sok pozitív egész számunk, amelyre a kéttagú összegek prímosztói véges halmaz, akkor két kéttagú összeg különbsége végtelen sokszor lenne azonos (ti. két számra, legyenek $a_1 < a_2$, a maradékból egy-egy a számot választva párnak

$$0 < a_2 - a_1 = (a_2 + a) - (a_1 + a)$$

fix), Pólya tételének ellentmondva.

2. További eredmények és kérdések konkrét n-ekre és általánosan

A szakdolgozatban saját eredmények a saját készítésű programokkal talált numerikus eredmények (a 2.2. alfejezetben és az 5. fejezetben), az 5. tétel olyan páratlan számokról, melyekre a kéttagú összegek szorzatát legfeljebb 3 prímszám osztja, és a 2.3. alfejezet egy része.

2.1. Az $n = 4$ eset

Az $n = 4$ esetben Erdős és Turán tétele szerint $f(4) \geq 2$. Ezt Wu pontosította az alábbi eredményével:

4. Tétel (Wu [16]). *Ha* 4 *különböző pozitív egész számra, melyek legnagyobb közös osztója* 1*, a kéttagú összegeknek összesen két különböző prímosztója van, akkor a négy szám az* $\{1; 5; 7; 11\}$ *vagy az* $\{1; 7; 17; 47\}$*.*

Mivel mindkét esetben a 2 és a 3 a két prímosztó, ez azt is jelenti, hogy az olyan pozitív egészekből álló számnégyesek, melyekre a különböző számokból álló párok összegeinek összesen két különböző prímosztója van, ezen számnégyesekből kaphatóak valamelyikük összes elemét $2^k 3^l$ alakú számmal szorozva, $k; l$ nemnegatív egész számok.

A tétel bizonyítása (Wu bizonyítása módosított jelölésekkel):

A négy szám közt van kettő azonos paritású, így összegükből a 2 előfordul a prímosztók közt. Emellett az Erdős-Turán-tétel szerint van legalább még egy prímosztó. Feltesszük, hogy négy különöző pozitív egész számra a kéttagú összegeknek összesen két prímosztója van és a négy szám legnagyobb közös osztója 1.
Jelölje p a páratlan prímet, amely legalább egy kéttagú összeget oszt.
Az Erdős-Turán-tétel bizonyítása alapján a négy szám közt már bármely háromra is van köztük kettő, amelynek összegét p nagyobb hatványa osztja, mely a kettő számot külön-külön nem. Emiatt a négy szám közül nincs három, amelyre p más-más hatványa a legnagyobb p-hatvány osztója, hiszen ekkor bármely kettő összegének prímtényezős felbontásában p kitevője akkora lenne, mint a kettő szám prímtényezős felbontásaiban előforduló kisebb kitevője p-nek.

Az sem lehetséges, hogy a négy szám közül háromban megegyezik p kitevője, de a negyedikben eltér. Ugyanis előbbi három közt létezik kettő, amelyek összegében p kitevője annyi, mint külön-külön a számokban, mert a legnagyobb őket osztó p-hatvánnyal leosztva a három számot p-vel nem osztható számokat kapunk, így nem lehet bármely kettő összege p-vel osztható. Ezen kettő számot és a negyediket véve bármely kettő összegére prímtényezős felbontásában p kitevője akkora lenne, mint a kettő számra a prímtényezős felbontásokban előforduló kisebb kitevője p-nek, ami ellentmondás.

Végül az sem lehet, hogy a négy szám közül kettő-kettőben megegyezik p kitevője, de a másik párosban előfordulótól eltér. Legyen m a kisebb kitevő, ami előfordul. Ekkor ugyanis a különböző párosok számait kétféleképp párosíthatjuk össze, ezen két-két kéttagú összegre bármely kéttagú összegben p kitevője m, és a két-két kéttagú összeg összege megegyezik. Ezen négy kéttagú összeg p^m 2-hatványszorosa, így a négy szám összege kétféleképp előáll kettő ilyen összegeként, p^m-ede kétféleképp előáll két 2-hatvány összegeként. Ekkor utóbbi felírásokban az összeg felénél nem kisebb, nála kisebb 2-hatvány, ilyen a két 2-hatvány közül nem kisebb, egyértelmű, és így a másik is, a kéttagú összegek közül kettő-kettő megegyezik úgy, hogy a 4 különböző szám közül nem diszjunkt párosok összegei, ami ellentmondás.

Ezzel megkaptuk, hogy 4 tételbeli tulajdonságú különböző számra bennük p kitevője megegyezik, hiszen legfeljebb kétféle fordul elő, de nem $3 \quad 1$ vagy $2 \quad 2$ arányban. Mivel a 4 különböző pozitív egész szám legnagyobb közös osztója 1, ez azt jelenti, hogy egyik sem osztható p-vel.

Ezután megvizsgáljuk, hogy a négy szám p-vel osztva milyen maradékokat ad, azok közt milyen összefüggések vannak. A kéttagú összegek között már három számnál is van nem 2-hatvány, így a négy szám közül bármely három között van kettő, amelyek összege p-vel osztható.
A négy szám közt kiválasztunk kettőt, jelölje őket x_1 és x_2, melyek összege p-vel osztható.
Az ebben nem szereplő számokat jelölje x_3 és x_4, ezek összege osztható p-vel, hiszen különben az egymással mod p inkongruens x_1 és x_2 (itt használjuk, hogy p páratlan és a négy szám közül egyet sem oszt) közül valamelyikkel egyik sem kongruens, így a másikat az (x_3, x_4) számpárhoz hozzávéve három olyan számot kapnánk, melyek közül semelyik kettő összege sem osztható p-vel, ami ellentmondás. Így $x_3 + x_4$ is osztható p-vel. Ha x_1-gyel x_3 és x_4 is inkongruens lenne mod p, akkor

$$x_1 + x_3 \text{ és } x_2 + x_4,$$

illetve

$$x_1 + x_4 \text{ és } x_2 + x_3$$

sem lenne p-vel osztható, így mind 2-hatvány, előbbiek összege megegyezik utóbbiakéval, ezért előbbi két 2-hatvány közül a nem kisebb megegyezik az utóbbiak közül nem kisebbel, ami ellentmond annak, hogy a 4 szám különböző. Ebből $x_1 \quad x_3$ (mod p) vagy $x_1 \quad x_4$ (mod p), ami azt jelenti, hogy a 4 különböző szám közül kettő-kettő kongruens mod p, és a különböző párokból egy-egy szám összege osztható p-vel.

Új jelölésekkel legyen a 4 különböző szám a, b, c és d úgy, hogy

$$a \quad b \text{ (mod } p\text{) és } c \quad d \text{ (mod } p\text{)},$$

emellett

$$a+b \le c+d;$$

ennyi feltehető. Ekkor $a+b$ és $c+d$ egyike sem osztható p-vel, így mindkettő 2-hatvány, két-két különböző pozitív egész szám összegeként 2-nél nagyobbak, oszthatóak 4-gyel. Így a 4 szám összege páros és nincs közös prímosztójuk, 0 vagy 2 páros közülük. Utóbbi nem lehetséges, mert ekkor a két-két páros és páratlan számra a különböző paritásúak kétféleképp párosíthatóak, a kéttagú összegek p-hatványok, így $a+b+c+d$ kétféleképp írható fel két p-hatvány összegeként, a nem kisebbek egyértelműek ($a+b+c+d$ felénél nem kisebb, $a+b+c+d$-nél kisebb p-hatványként), és nem diszjunkt számpárok összegei, ezért a 4 szám közül nem lenne mind különböző, ellentmondás Vagyis mind a 4 szám páratlan.

$4 \mid a+b$ és $4 \mid c+d$,

előbbi és utóbbi összegben is egy-egy tag ad 1 és 3 maradékot 4-gyel osztva, így még az is feltehető, hogy

$$a \equiv c \equiv 1 \ (\mathrm{mod}\ 4) \text{ és } b \equiv d \equiv 3 \ (\mathrm{mod}\ 4).$$

Ekkor

$$a+b=2^u;$$

$$a+c=2p^y$$

és

$$b+d=2p^z$$

teljesülnek, ahol $u; y; z$ pozitív egész számok.

$a+b \mid c+d$, mert 2-hatványok és előbbi nem nagyobb. Ebből

$$a+b \mid a+b+c+d;$$

így $2^u \mid 2p^y+2p^z$ és

$$2^{u-1} \mid p^y+p^z.$$

Mivel

$$p^y+p^z=p^{\min(y;z)}(1+p^{|y-z|})$$

és $p^{\min(y;z)}$ páratlan, így

$$2^{u-1} \mid 1+p^{|y-z|}.$$

$1+p^{|y-z|}$ prímtényezős felbontásában 2 kitevője nem nagyobb, mint $p+1$-ében.

Ugyanis ha $2 \mid y - z$,

$$1 + p^{|y-z|} \equiv 2 \pmod 8$$

egy páratlan négyzetszámnál eggyel nagyobb számként,

$$2^1 \mid 1 + p^{|y-z|};$$

de 2^2 nem osztja $1 + p^{|y-z|}$-t, míg $p + 1$ páros.
Ha pedig $y - z$ páratlan, akkor

$$1 + p^{|y-z|} = (p + 1)(p^{|y-z|-1} - p^{|y-z|-2} \dots + 1);$$

a jobb oldal páratlan sok ($|y - z|$ darab) páratlan szám összegeként páratlan, így 2 kitevője a szorzatban annyi, mint $p + 1$-ben. Ezzel ezen állításunkat beláttuk, így $2^{u-1} \mid p + 1$ is teljesül,

$$2^u \mid 2p + 2;$$

tehát

$$a + b \mid 2p + 2.$$

Mivel $a + c$ és $b + c$ is páros, emellett p-vel osztható, így

$$2p \mid b - a;$$

ami azt jelenti, hogy

$$|b - a| \geq 2p;$$

és így

$$2p + 2 \geq a + b = |b - a| + 2\min(a; b) \geq |b - a| + 2 \geq 2p + 2.$$

Tehát

$$a + b = 2p + 2;$$

$$|b - a| = 2p;$$

amiből adódóan a és b egyike 1, a másik $2p + 1$, $a \equiv 1 \pmod 4$ alapján

$$a = 1 \text{ és } b = 2p + 1.$$

Ekkor $a + d = 1 + d$ osztható p-vel, így legyen

$$d = wp - 1,$$

ahol w pozitív egész szám.

$$b + d = 2p^z \text{ és } b + d > b > 2p,$$

így

$$p^2 \mid b + d.$$

$p > 2$ miatt ebből

$$wp = a + d = (b + d) - 2p$$

nem osztható p^2-tel, de p-vel igen, w 2-hatvány.

$$(w + 2)p = (2p + 1) + (wp - 1) = b + d = 2p^z,$$

így

$$w + 2 = 2p^{z-1},$$

$w + 2$ egy p-hatvány 2-szerese, $\frac{w}{2} + 1$ p-hatvány és $\frac{w}{2}$ 2-hatvány.
Mivel a pozitív $\frac{w}{2}$ csak 1-gyel kisebb egy p-hatványnál, így $p - 1$ osztja, tehát $p - 1$ is 2-hatvány.

Eszerint $p - 1$ és $a + b = 2p + 2$ is 2-hatvány.
$p > 3$ esetén

$$2(p - 1) < 2p + 2 < 4(p - 1)$$

miatt ez ellentmondás, így p páratlan prímként csak a 3 lehet. Eszerint

$$a = 1 \text{ és } b = 7.$$

c-re és d-re teljesül, hogy a náluk 1-gyel és 7-tel nagyobb számok $2^k 3^l$ alakúak (k és l nemnegatív egész számok), és 6 a különbségük. Ilyen $2^k 3^l$ alakú számokból álló számpárokból viszont nincs sok.

Ha egy ilyen számpárból valamelyik szám nem osztható 3-mal, a másik sem, mindkettő 2-hatvány, a nagyobb 6-nál nagyobb számként legalább 8, de más nem is lehet, mert a nála kisebb másik szám legalább a felével kisebb nála, csak a $(2, 8)$ számpár van, de ez nem ad c-t vagy d-t, mert $8 - 7 = 2 - 1 = 1$. Ha a számpárból valamelyik szám nem osztható 2-vel, a másik sem, mindkettő 3-hatvány, a nagyobb 6-nál nagyobb számként legalább 9, de más nem is lehet, mert a nála kisebb másik szám legalább a kétharmadával kisebb nála, csak a $(3; 9)$ számpár van, de ez nem ad c-t vagy d-t, mert $9 - 7 = 3 - 1 = 2$ és beláttuk, hogy mind a négy számunk páratlan.

Végül maradt azon eset, amikor a 2^k3^l alakú számokból álló 6 különbségű számpárból mindkét szám osztható 6-tal. Ilyenek a $(6; 12)$, $(12; 18)$, $(18; 24)$ és $(48; 54)$ számpárok, amikor mindkét szám kisebb 60-nál. Más eset nincs, ugyanis 6-tal leosztva a számokat két 2^k3^l alakú számot kapunk, melyek különbsége 1, van köztük 2-vel nem osztható és 3-mal nem osztható is, az egyik 2-hatvány, a másik 3-hatvány. Ha mindkettő legalább 8, a 2-hatvány osztható 8-cal, így a 3-hatvány az eggyel nagyobb, mert a 3-hatványok 8-cal osztva felváltva 1 és 3 maradékot adnak. Ekkor viszont a 3-hatványban a kitevő páros, négyzetszám, így a 2-hatvány négyzetszám -1 alakú számként két olyan szám szorzata, melyek különbsége 2, ezek 2-hatványként (a kisebb nem osztható 4-gyel) csak a 2 és 4 lehetnek a $(8; 9)$ esetben, ami a korábbi $(48; 54)$-nek felel meg.

Így c és d a

$$12 - 7 = 6 - 1 = 5;$$

$$18 - 7 = 12 - 1 = 11;$$

$$24 - 7 = 18 - 1 = 17$$

és

$$54 - 7 = 48 - 1 = 47$$

számok közül kerülhet ki. $c + d$ 2-hatvány, ahogy már beláttuk, így az $(5; 11)$ és $(17; 47)$ párok lehetségesek, $c \equiv 1 \pmod 4$ miatt ez c és d sorrendje. Összesítve $(a; b; c; d) = (1; 7; 5; 11)$ és $(a; b; c; d) = (1; 7; 17; 47)$ a lehetséges számnégyesek, nagyság szerinti sorrendbe állítva őket a tétel állítását kapjuk. A tételt bebizonyítottuk.

2.2. Nagyobb n-ek 5-től 8-ig

Ez az alfejezet döntően saját eredményeket tartalmaz.

Már láttuk, hogy az Erdős-Turán-tétel következményeként $f(n) \geq \lceil \log_2 n \rceil$. Ha $2 \leq n \leq 4$, akkor egyenlőség van,

$$f(2) = 1$$

és

$$f(3) = f(4) = 2.$$

Az $n = 5$ esetben is egyenlőség van, $f(5) = 3$-at bizonyítja az $1, 3, 7, 17, 47$ számötös, ahol a kéttagú összegek prímosztói közt csak a 2, a 3 és az 5 szerepelnek. Általánosan igaz, ahogy a Wu-tételnél, elég azon szám n-esekből, melyek kéttagú összegei minimális számú prímmel oszthatóak, olyanokat nézni, ahol 1 a számok legnagyobb közös osztója. Ezeket a kéttagú összegek $f(n)$ prímosztójából néhány hatványának szorzataként előálló számok valamelyikével megszorozva kapható meg az összes ilyen tulajdonságú szám n-es. $n = 5$ esetén Python nyelvű programmal megvizsgáltam azon eseteket, amikor az 5 pozitív egész szám mindegyike legfeljebb 2500. Csak az alábbi 8 esetben teljesült, hogy a kéttagú összegeknek 3 prímosztója van és az 5 szám legnagyobb közös osztója 1:

számötös	prímosztók
1, 2, 7, 11, 25	2, 3, 13
1, 3, 5, 11, 13	2, 3, 7
1, 3, 7, 17, 47	2, 3, 5
1, 5, 31, 49, 59	2, 3, 5
1, 19, 31, 89, 161	2, 3, 5
3, 7, 13, 17, 47	2, 3, 5
3, 7, 17, 33, 47	2, 3, 5
5, 11, 25, 245, 475	2, 3, 5

Ugyancsak programmal, a prímosztók irányából vizsgálva nem sikerült több ilyen számötöst találni 500 milliónál nem nagyobb számokra, ahol a 2, 3 és 5 fordulnak elő a kéttagú prímosztók prímosztói közt, illetve 50 milliónál nem nagyobb számokra, ahol a kéttagú összegek prímosztói közt a $(2; 3; 7)$, $(2; 3; 11)$, $(2; 3; 13)$ vagy $(2; 5; 7)$ számhármas elemei fordulnak elő.

Programmal végignézve az $n = 6$ esetben 75 olyan számhatost találtam, ahol a 6 pozitív egész szám egyike sem nagyobb 900-nál, összesen legfeljebb és egyben pontosan 4 prím osztja a kéttagú összegek valamelyikét, és a hat szám legnagyobb közös osztója 1. Egy példa erre az $1; 2; 3; 5; 7; 13$ számok, ahol a kéttagú összegek prímosztói közt a 2, 3, 5 és 7 prímszámok fordulnak elő. Érdekes módon a 75 számhatosban legnagyobbként előforduló két legnagyobb szám az 501 és a 805, így az ilyen számhatosokból egy sincs, ahol az $[502; 804]$ intervallumba esne a legnagyobb szám.

Így $f(6) \le 4$. Ugyanakkor az Erdős-Turán-tétel alapján $f(6) \ge 3$. Ezek alapján a következőt sejtem:

1. Sejtés (F.). $f(6) = 4$, vagyis nincs olyan számhatos, amelyre a kéttagú összegek prímosztói közt pontosan 3 szám fordul elő.

$\omega(n)$ jelölje azt bármely n pozitív egész számra, hogy hány különböző prímszám osztója van az n-nek. A következőt bizonyítottam:

5. Tétel (F.). Ha az A halmaz elemei pozitív páratlan számok és $|A| \ge 7$, akkor

$$\omega\Bigg(\prod_{\substack{a,a' \in A;\\ a \ne a'}} (a+a')\Bigg) \ge 4.$$

A tétel bizonyítása:

Tegyük fel, hogy nem igaz az állítás, ekkor létezik 6-nál több pozitív páratlan szám, amelyekre a kéttagú összegek prímosztói közt legfeljebb 3 szám fordul elő. Ezen páratlan számok 4-es maradéka kétféle lehet, így lenne 3-nál több pozitív páratlan szám, amelyekre a kéttagú összegek prímosztói közt legfeljebb 3 szám fordul elő, és mod 4 megegyezik a maradékuk. Ezekből négyet kiválasztva lenne négy pozitív páratlan szám, amelyekre a kéttagú összegek prímosztói közt legfeljebb 3 szám fordul elő, és mod 4 ugyanaz a maradékuk. Belátjuk, hogy ez nem lehetséges.

Ekkor 4 ilyen számra bármely kettő összege osztható lenne 2-vel, de nem lenne osztható 4-gyel, a legfeljebb 3 prímosztó közül az egyik a 2. A 4 számot a páratlan legnagyobb közös osztójukkal leosztva szintén négy pozitív páratlan számot kapnánk, amelyekre a kéttagú összegek prímosztói közt legfeljebb 3 szám fordul elő, és mod 4 ugyanaz a maradékuk. Innentől feltehetjük, hogy a négy szám legnagyobb közös osztója az 1. A négyből bármely két u, v számra van olyan r prímszám és m pozitív egész szám, amelyekre $r^m \mid u+v$, de $r^m \nmid u$ és $r^m \nmid v$. Az $u+v$ összeg a két számból kisebbnek több mint kétszerese és $4k+2$ alakú, így a 2-n kívül is van ilyen r prímszám. Egy ilyen r prímre az u-ra és v-re ugyanaz, az összeg $u+v$-énél kisebb r legnagyobbot osztó hatványa.

A 6 kéttagú összeg mindegyikét osztja a 2-n kívül is prím. Sőt, mivel a 4 szám relatív prím, nem oszthatja bármely kettő összegét ugyanazon páratlan prím, mert akkor bármely 3-ra közülük mindhármuk összegének dupláját, mindhármuk összegét és ezzel mindhármukat is osztaná. Ebből mind a 4 számot osztaná, ami a relatív prímségnek ellentmond. Eszerint legalább két páratlan prímnek elő kell fordulni a kéttagú összegek osztói közt, csak a pontosan 3 prímosztó képzelhető el, legyen a kettő páratlan p és q.

A 4 számunk legyen a, b, c és d.
Bebizonyítjuk, hogy

$$p \mid a+b+c+d \text{ és } q \mid a+b+c+d.$$

Ugyanis ha $a+b+c+d$ pl. p-vel nem lenne osztható, akkor az $(a+b; c+d)$, $(a+c; b+d)$ és $(a+d; b+c)$ párokra mindegyik párban legalább az egyik szám p-vel nem osztható lenne, így $2q^n$ alakú, ahol $n > 0$. Így a, b, c és d közül kiválasztható háromféleképp két szám úgy, hogy a kiválasztott párokban az összeg $2q^n$ alakú, és a kiválasztott párok közt nincs két diszjunkt. A 3 párnak kell, hogy legyen közös száma, mert enélkül 3 különböző pozitív páratlan számra ($\{a; b; c; d\}$-ből) bármely kettő összege a 2 q-hatványszorosa lenne, és egymástól különböző. A két kisebb összeg összege kisebb lenne, mint a nagyobb, mivel mindkettő legfeljebb $1/q$-szorosa, de ez ellentmondás, mert három pozitív egész számra a két nagyobb összegénél a másik két párbeli összeg összege a legkisebb szám duplájával nagyobb.

Így csak pontosan 3 pár lehet, amelyekre az összeg nem osztható p-vel, egy negyedik már ilyen hármast okozna. A maradék 3 számpárra az összeg osztható p-vel, és mivel a többi összeg osztható q-val, nem oszthatók q-val, mert akkor $q \mid a+b+c+d$ miatt mindegyik párra q-val osztható lenne az összeg, ami $\mathrm{lnko}(a; b; c; d) = 1$ miatt lehetetlen. Eszerint a maradék 3 számpárra mind három összeg $2p^m$ alakú lenne, ahol m pozitív egész szám, és 3 különböző pozitív páratlan számra ($\{a; b; c; d\}$-ből) bármely kettő összege a 2 p-hatványszorosa és így különböző, ami az előbbi részhez hasonlóan ellentmondás. A legnagyobb számpár összeg túl nagy lenne ahhoz, hogy mind a 4 szám pozitív legyen. Ezzel beláttuk, hogy $p \mid a+b+c+d$, logikai szimmetriából az is kijön, hogy $q \mid a+b+c+d$.

A 4 számunkra a kéttagú összegek közt van, ami p-vel nem osztható, ezért a kimaradt két szám összege is az, és van olyan kéttagú összeg, ami q-val nem osztható, ezért a kimaradt két szám összege is az. Ekkor feltehetjük, hogy $a+b$ és $c+d$ az előbbi, $a+c$ és $b+d$ az utóbbi esetet teljesítő kéttagú összeg pár. Tehát

$$a+b = 2q;$$
$$c+d = 2q'';$$
$$a+c = 2p;$$
$$b+d = 2p:$$

A kitevok nemnegatív egész számok, sot mivel két különbözo pozitív egész szám összege 2-nél nagyobb, pozitív egész számok. Logikai szimmetria miatt feltehető, hogy

" és ,

egyenlőség egyikről sem lehet, mert akkor $a+b+c+d$ egy prímhatvány 4-szereseként nem lenne p-vel és q-val is osztható. Emiatt

$$c+d=q^{"} \quad (a+b) \quad 3(a+b)$$

és

$$b+d=p \quad (a+c) \quad 3(a+c);$$

´ıgy

$$(c+d)+(b+d) \quad \frac{3}{4}(a+b+c+d)+\frac{3}{4}(a+b+c+d)=\frac{3}{2}(a+b+c+d):$$

Ebbol

$$(a+b+c+d)+d>\frac{3}{2}(a+b+c+d)$$

és vele

$$d>a+b+c:$$

A megmaradt két összeg $a+d$ és $b+c$, $a+d>b+c$, ´ıgy van olyan prímszám, amelynek $a+d$-t osztó legnagyobb hatványa nagyobb, mint a $b+c$-t osztó legnagyobb hatványa, ez a prímszám p és q közül valamelyik(ek). Legyen egy ilyen p, logikai szimmetriával ez is feltehető. Ekkor $a+b+c+d$ prímtényezős felbontásában p kitevője akkora, mint amelyikre $a+d$ és $b+c$ közül a prímtényezős felbontásban kisebb, $b+c$-ben. Ugyanakkor

$$(a+c)+(b+d)=2p \quad +2p \quad =2p \quad (p \quad +1);$$

´ıgy

$$b+c=2p \quad q^{v}$$

egy v nemnegatív egész számra.

$$2p \quad | \; a+c \text{ és } 2p \quad | \; b+c$$

miatt

$$2p \quad | \; b \quad a;$$

´gy mivel a és b pozit´v egész számok, amelyekre $a + b = 2q$,

$$p < q :$$

Ha $a + d$ és $b + c$ pr´mtényezos felbontásában a q kitevoje különbözne, mivel az összeg

$$(a + b) + (c + d) = 2q + 2q^{"} = 2q (q^{"} + 1) ;$$

mindkét szám q többszöröse lenne, ekkor

$$2q \ j \ a + b \text{ és } 2q \ j \ b + c$$

is teljesülne, vele

$$2q \ j \ c \quad a \text{ és } a + c = 2p < 2q$$

egyszerre teljesülne, ami pozit´v egész a 6= c-kre ellentmondás. Ebbol

$$a + d = 2p \ q^{v} ;$$

ahol v ugyanaz a szám, mint $b + c$-re, pedig nemnegat´v egész szám.
$>$, ahogy már láttuk. $v <$, mert

$$2q \ j \ (b + c) \quad (a + b)$$

miatt itt is ellentmondást kapnánk ($a + c = 2p$).

E szerint $a + b + c + d$ háromféleképp fe´lrva

$$(a + c) + (b + d) = 2p \ (p \quad + 1) ;$$

$$(a + b) + (c + d) = 2q \ (q^{"} \quad + 1)$$

és

$$(a + d) + (b + c) = 2p \ q^{v} + 2p \ q^{v} = 2p \ q^{v} (p \quad + 1) :$$

$v > 0$, hiszen a 6= b és ´gy $a + c$ 6= $b + c$. Az elso és utolsó összegekbol

$$(p \quad + 1) \ q^{v} = p \quad + 1 :$$

Itt $< \ <$.

$$p \quad +1 \mid p \quad +1$$

miatt páratlan számszorosa , ugyanis mod p + 1 nézve p hatványait először maguk a számok különböző maradékok 1-tol p < p + 1-ig, utóbbi 1 maradékot ad, innen rendre a -val kisebb kitevős hatványa 1-szeresegyjn, ebből az 1 újra p^0 után először $p^{2(\quad)}$-nál jelenik meg, 2( ) a rend. p hatványai 2( )-nként periodikusak mod p + 1. Így először

$$p \qquad 1$$

és utána 2( )-nként kongruensek 1-gyel a p-hatványok mod p + 1.

Legyen $K \stackrel{def}{=} \overline{\quad}$, $K > 0$ páratlan szám.

$$2q\ (q^{"} + 1) = a + b + c + d = 2p\ q^{v}(p \quad + 1)$$

miatt a legnagyobb p + 1-et osztó q-hatvány a q^{v}. Így

$$(p \quad + 1)\,q^{v} = p \quad + 1$$

miatt a legnagyobb p + 1-et osztó q-hatvány a q .

$v > 0$, ahogy már láttuk. Ezután belátjuk, hogy ebből $K = \overline{\quad}$ osztható q^{v}-vel. Ez az ún. LTE lemma speciális esete, de itt bizonyítjuk.

$K = q^{x} m$ alakban felírva, ahol x 0 és $m > 0$ egész számok, lnko$(q; m) = 1$,

$$\begin{aligned} p \quad + 1 &= p^{K(\quad)} + 1 = (p^{q^{x}(\quad)})^{m} + 1 \\ &= (p^{q^{x}(\quad)} + 1)(p^{q^{x}(\quad)(m\ 1)} \quad p^{q^{x}(\quad)(m\ 2)} \quad + 1): \end{aligned}$$

$$q \mid q^{\ v} \mid p \quad + 1$$

miatt

$$p^{q^{x}(\quad)} \qquad 1 \bmod q,$$

így a jobb oldalon m db mod q 1 maradékot adó számot adunk össze, összegük nem osztható q-val, ugyanannyi a szorzatban q kitevoje, mint $p^{q^{x}(\quad)} + 1$-ben. Tehát K-tól annyiban függ q kitevoje $p^{K(\quad)+1}$ prímtényezős felbontásában, hogy aszerint dől el, K prímtényezős felbontásában mekkora q kitevoje. Ezután belátjuk, hogy a $p^{q^x(\ )}+1$-et osztó legnagyobb q-hatvány q^x-szerese a $p\quad+1$-et osztó legnagyobb q-hatványnak minden x pozitív egész számra.

Ehhez elég, hogy a $p^{q^x(\ )}+1$-et osztó legnagyobb q-hatvány q-szorosa a $p^{q^{x\ 1}(\ )}+1$-et osztó legnagyobb q-hatványnak minden x pozitív egész számra.

$$p^{q^x(\ )}+1=(p^{q^{x\ 1}(\ )})^q+1=$$

$$(p^{q^{x\ 1}(\ )}+1)(p^{(q\ 1)q^{x\ 1}(\ )}\quad p^{(q\ 2)q^{x\ 1}(\ )}\qquad p^{q^{x\ 1}(\ )}+1).$$

Ha q^r a legnagyobb $p^{q^{x\ 1}(\ )}+1$-et osztó q-hatvány,

$$q\quad^v\ j\ p^{(\ )}+1$$

miatt $r>\ 0$, a jobb oldali $p^{(q\ 1)q^{x\ 1}(\ )}\quad p^{(q\ 2)q^{x\ 1}(\ )}\qquad p^{q^{x\ 1}(\ )}+1$ összegben minden tag kongruens 1-gyel mod q^r; így kongruens q-val mod q^r. $r>\ 1$-re nem osztható q^2-tel, de osztható q-val és ezzel a $p^{q^x(\ )}+1$-et osztó legnagyobb q-hatvány q-szorosa a $p^{q^{x\ 1}(\ )}+1$-et osztó legnagyobb q-hatványnak.

Ha q a legnagyobb $p^{q^{x\ 1}(\ )}+1$-et osztó q-hatvány, akkor

$$p^{q^{x\ 1}(\ )}=\ lq\quad 1$$

egy lnko$(l;q)=1$-et kielégíto l pozitív egész számra. Ekkor

$$p^{q^x(\ )}+1=(\ lq\quad 1)^q+1;$$

binomiális tétellel q^3-bel osztható részen kívül

$$\frac{q}{2}\quad l^2q^2+\ q\ \ lq\quad 1+1=\ q^2\qquad l^2q\frac{q\quad 1}{2}+\ l$$

a jobb oldal, q^2-tel osztható, de q^3-bel nem. Így ekkor is igaz, hogy a $p^{q^x(\ )}+1$-et osztó legnagyobb q-hatvány q-szorosa a $p^{q^{x\ 1}(\ )}+1$-et osztó legnagyobb q-hatványnak.

Ezzel beláttuk, hogy a legnagyobb $p^{K(\ )}+1$-et osztó q-hatvány a legnagyobb $K\ (p^{(\ )}+1)$-et osztó q-hatvány minden K pozitív páratlan számra.

Így megkaptuk, hogy $q^v \mid K$.

$$q^v(p \quad + 1) = p^{K(\quad)} + 1$$

miatt

$$K(p \quad + 1) \quad p^{K(\quad)} + 1 :$$

Legyen

$$A \stackrel{def}{=} \quad ;$$

ekkor

$$K(p^A + 1) \quad p^{KA} {}^{+1} :$$

Így

$$K \quad \frac{p^{KA+1}}{p^A + 1} = p^{(K \quad 1)A} \quad p^{(K \quad 2)A} \quad + 1 > p^{(K \quad 1)A} \quad p^{(K \quad 2)A} = (p \quad 1)p^{(K \quad 2)A} :$$

$$p \quad 1 \quad 2 \text{ és } A \quad 1,$$

ezért

$$K \quad (p \quad 1)p^{(K \quad 2)A} \quad 2 \ 3^{K \quad 2} :$$

Ugyanakkor K q^v-vel osztható páratlan szám, legalább 3, ekkor $K \quad 2 \quad 3^{K \quad 2}$ nem teljesülhet, mert 3-ra nem teljesül, $3 < 6$ és utána a jobb oldal K-t 2-esével növelve jobban nő, 9-szereződik, a bal oldal először 5/3-szorozódik, majd még kisebb számokkal szorzódik. Ezzel ellentmondást kaptunk azon feltevésre, hogy létezne négy különböző 4-gyel osztva azonos maradékot adó pozitív páratlan szám, melyekre a kéttagú összegek prímosztói közt csak legfeljebb 3 prímszám szerepel, vele pedig a tétel állítását megkaptuk.

A tétel állítása annyiban gyengébb a sejtésénél, hogy csak csupa páratlan számról szól és ott is 6 számot (melyekből három-három ad mod 4 1, illetve 3 maradékot) megenged. Az 5 számra programmal talált relatív prím számötös esetek legtöbbjében mindegyik szám páratlan, amelynek megvan azon előnye, hogy a 2 kitevője bármely két szám összegében nagyobb, mint külön-külön a számokban. Ugyanakkor ez az eset jobban kezelhetőnek tűnt a tétel bizonyításához, nagyobb a szabályosság és kevesebb az aleset mod 4 kongruens páratlan számokat vizsgálva, amelyekre viszont csak eggyel nagyobb a prímtényezős felbontásban a 2 kitevője a kéttagú összegekben, mint tagoknál. Emellett az is kiderült belőle, hogy számötösöknél 5 páratlan számra, amelyekre a kéttagú összegek közül legalább egyet legfeljebb (így pontosan) három prímszám oszt, 3 : 2 arányban oszlik el az 5 szám a mod 4 redukált maradékosztályok közt.

Programmal végignézve az $n = 7$ esetben 508 olyan számhetes van, ahol a 7 pozitív egész szám egyike sem nagyobb 600-nál, összesen legfeljebb 5 és egyben pontosan 5 prímszám osztja a kéttagú összegek valamelyikét, és a hét szám legnagyobb közös osztója 1. Egy példa erre az 1; 2; 3; 4; 6; 12; 24 számhetes, amelyre a kéttagú összegek prímosztói közt a 2, 3, 5, 7 és 13 prímszámok fordulnak elő. Egy, az $n = 6$-os esetet is vizsgáló másik Python nyelvű programom eredménye, hogy nincs olyan számhetes 900-nál nem nagyobb számokból, ahol legfeljebb 4 prímszám osztja a kéttagú összegek valamelyikét.

Végül az $n = 7$ esetben számheteseket találó program befejező részében végignézve az $n = 8$ esetben 16 olyan számnyolcast találtam, ahol a 8 pozitív egész szám egyike sem nagyobb 600-nál, összesen legfeljebb 5 és egyben pontosan 5 prím osztja a kéttagú összegek valamelyikét, és a nyolc szám legnagyobb közös osztója 1. Ezekről szól a következő táblázat:

számnyolcas	prímosztók
1, 2, 3, 5, 7, 13, 23, 47	2, 3, 5, 7, 13
1, 2, 3, 5, 7, 23, 25, 47	2, 3, 5, 7, 13
1, 2, 4, 6, 8, 12, 24, 48	2, 3, 5, 7, 13
1, 2, 4, 6, 14, 26, 34, 94	2, 3, 5, 7, 19
1, 2, 5, 9, 13, 19, 23, 31	2, 3, 5, 7, 11
1, 3, 5, 6, 9, 15, 27, 39	2, 3, 5, 7, 11
1, 3, 5, 7, 8, 17, 19, 47	2, 3, 5, 11, 13
1, 3, 6, 9, 15, 21, 27, 39	2, 3, 5, 7, 11
1, 3, 6, 15, 21, 27, 29, 69	2, 3, 5, 7, 11
1, 3, 6, 15, 21, 27, 39, 69	2, 3, 5, 7, 11
2, 3, 6, 12, 18, 30, 42, 78	2, 3, 5, 7, 11
3, 7, 21, 42, 63, 105, 147, 189	2, 3, 5, 7, 11
3, 7, 21, 42, 105, 147, 189, 483	2, 3, 5, 7, 11
6, 10, 15, 30, 60, 90, 210, 390	2, 3, 5, 7, 11
6, 14, 21, 42, 84, 126, 210, 294	2, 3, 5, 7, 11
7, 14, 18, 42, 70, 182, 238, 378	2, 3, 5, 7, 11

2.3. Felső becslés és megválaszolatlan kérdések

Erdős és Turán cikkükben [3] úgy vélték, hogy k pozitív egész számokra nézve a legnagyobb $n(k)$ pozitív egész számot, amelyre létezik $n(k)$ pozitív egész szám, ahol a kéttagú összegeknek legfeljebb k különböző prímosztója van, $n(k) = O(k^{1+c})$ bármely $c > 0$ valós számra. Ezt azonban nem sikerült bizonyítaniuk.
Erdős egy későbbi, Stewart és Tijdeman cikkében [12] idézett 1976-os írásában (Problems in number theory and combinatorics) ennek megfelelően $f(n) \le n^{1-\varepsilon}$-t sejtett, sőt $\frac{n}{\log n}$-es nagyságrendű alsó becslést sem tartott kizártnak. Ugyanakkor megjegyezte, hogy a prímszámtételből $(2+\varepsilon)\frac{n}{\log n}$ semmilyen $\varepsilon > 0$-ra nem lehet alsó becslés $f(n)$-re az $\{1, 2, \dots, n\}$ számhalmaz alapján, ahol $n > 2$-re kéttagú összeget a $2n-1$-nél nem nagyobb prímszámok osztanak, de $(2+o(1))\frac{n}{\log n}$ nem lehetetlen alsó becslés.

Ugyanide tartozik Erdős alábbi 250 dolláros megoldatlan kérdése:
Kérdés: (Erdős [18]) Igaz-e, hogy $n \to \infty$ esetén $\frac{f(n)}{\log n} \to \infty$?

$f(n)$-re nem ismert a prímszámtételből $\{1, 2, \dots, n\}$ szám n-esre következő $\frac{n}{\log n}$-es nagyságrendűnél jobb felső becslés.

Kérdés: (F.) Mely n pozitív egész számokra van csupán véges sok olyan szám n-es pozitív egész számokból, ahol minimális számú, azaz $f(n)$ prím oszt a kéttagú összegek közül legalább egyet, és az n szám legnagyobb közös osztója 1?

Tudjuk, hogy 3-ra végtelen sok ilyen számhármas van, például már olyan számhármasokkal is, ahol a kéttagú összegek 3^k, 3^{k+1} és a $2 \cdot 3^k$ és $4 \cdot 3^k$ közé eső 2-hatvány (k nemnegatív egész szám), míg 4-re Wu tételéből csak 2.

f monoton nő és $\lim_{n\to\infty} f(n) = \infty$, így $f(n+1) > f(n)$ végtelen sok n pozitív egész számra teljesül. Ugyanakkor a felső becslésből $\lim_{n\to\infty} \frac{n}{f(n)} = \infty$ miatt

$$f(n) = f(n+1)$$

végtelen sokszor fennáll, hiszen ha egy K korláttól $n \ge K$-ra

$$f(n) + 1 \le f(n+1)$$

teljesülne, $2K < n$-re

$$\frac{n}{f(n)} < 2$$

teljesülne. Sőt $\lim_{n\to\infty} \frac{n}{f(n)} = 1$ miatt az

$$f(n) = f(n+1)\text{-et}$$

kielégítő n pozitív egész számok aránya adott $K \in \mathbb{Z}^+$ korlátokra 1-től K-ig K-val a végtelenbe tartva 1-hez tart.

A témába vágó következő kérdés azonban nehéznek tűnik.

Kérdés: (F.) $f(n+1) \le f(n) + 1$ teljesül-e minden $n > 1$ pozitív egész számra?

3. $a + b$ alakú számok prímosztói két halmaznál

Térjünk át arra az esetre, amikor egy helyett két halmazunk van pozitív egész (esetleg nemnegatív egész) számokból, A és B, és azt vizsgáljuk $|A|$ és $|B|$ függvényében, hogy legalább hány prím oszt $a + b$ alakú összeget, ahol $a \in A$ és $b \in B$. Rendszerint A elemei sorrendben $a_1 < a_2 < \dots$ és B elemei $b_1 < b_2 < \dots$ Ezzel már Erdős és Turán is foglalkoztak cikkükben [3]. Megmutatták, hogy miért nem érdekes azon eset, amikor A és B is végtelen sok elemet tartalmaz. Az alábbi állítással ekvivalenset láttak be:

6. Tétel (Erdős-Turán). Ha $a_1 < a_2 < \cdots < a_{k+1}$ pozitív egész számok és $a_{k+1}^k < b$ mellett b is pozitív egész szám, akkor k-nál több prímszám van, amely az $a_1 + b, a_2 + b, \dots, a_{k+1} + b$ számok közül legalább egynek osztója.

A tétel bizonyítása:

Indirekten bizonyítunk. Ha legfeljebb k prímszám osztana az $a_i + b$ alakúak közül legalább egyet, akkor mivel az összes $a_i + b > b > a_{k+1}^k$, mindegyik $a_i + b$ alakú számot osztaná egy a_{k+1}-nél nagyobb prímhatvány. A $k + 1$ összegre lenne kettő, ahol ez ugyanazon prímnek lenne a hatványa, legyen ezen prímnek legkisebb a_{k+1}-nél nagyobb hatványa q. q ezen $a_i + b$-k közül mindkettőt osztaná. Ugyanakkor ezen $a_i + b$-k különbözőek és különbségük legfeljebb $a_{k+1} - a_1$, a_{k+1}-nél nem nagyobb pozitív egész szám, ami ellentmondás, mert ezt is osztania kellene az a_{k+1}-nál nagyobb q-nak. Ezzel a tételt bebizonyítottuk.

A tétel következménye, hogy prímszámok egy véges részhalmazát lerögzítve nem lehet végtelen nagy A és B halmazokat megadni úgy, hogy az $a + b$ alakú számok egyikét sem osztja a véges részhalmazon kívüli prím. Ugyanis ekkor ha s elemű a kijelölt prímszámok részhalmaza, az A halmaz $s+1$ különböző elemére $k = s$-sel $a_1, a_2, \ldots, a_{k+1}$ szerepében, és B egy a_{s+1}^s-nél nagyobb elemére a tételt alkalmazva már $a_1 + b, a_2 + b, \ldots, a_{s+1} + b$ prímosztói közt is s-nél több szám fordulna elő.

Ugyanakkor ez Pólya tételéből is következik ahhoz hasonlóan, hogy nincs végtelen nagy halmaz pozitív egész számokból, amelyből képezve az összes kéttagú összeget a prímosztóik halmaza véges. Itt is csak az A halmaz két elemére, $a_1 < a_2$-re és $b \in B$-re kell az $(a_2 + b) - (a_1 + b)$ különbséget figyelni, végtelen sokszor kapjuk meg ugyanazt, így az $a_i + b$ $(i = 1, 2)$ alakú számok prímosztói közt végtelen sok szám előfordul.

Így még az is következik, hogy ha A és B közül az egyik végtelen sok, a másik legalább 2 pozitív egész számot tartalmaz, már akkor is végtelen sok prímszám előfordul az $a + b$ $(a \in A; b \in B)$ alakú számok osztói között. Az elemien bizonyított előbbi Erdős-Turán eredményből ez nem következik. Az viszont igen, hogy ha A és B közül az egyik halmaz legalább $k+1$ elemű egy k másik elemnél is nagyobb c elemmel, a másik legalább $c^k + 1$ elemű (ti. ebből van benne c^k-nál nagyobb elem) akkor van legalább $k+1$ eltérő prímosztója az $a + b$ $(a \in A, b \in B)$ alakú összegeknek.
Ebben a részben innentől $|A|$ és $|B|$ véges.

3.1. Alsó becslés a prímosztók minimális számára

Legyen S egy s darab prímszámból álló halmaz, a, b, c nemnulla egész számok. Ekkor az

$$ax + by = cz$$

alakú egyenletet, ahol azon x, y, z egész megoldásokat keressük, amelyek csak S-beli prímekkel oszthatóak, ($\mathbb{Q}$ feletti) S-egységegyenleteknek hívjuk [1].

S-egységegyenletek más algebrai számtestek felett is értelmezettek, természetesen prím alatt akkor már nem a szokásos prímszámokat értve. Ilyenkor prímek egy véges halmazát, amelyben az összes végtelen típusú prím benne van, jelöljük S-sel, az S-egységek pedig azok, amelyekre bármely S-en kívüli prímhez tartozó értékelésnél 1-et kapunk eredményül. Ennek speciális esete a $\mathbb{Q}$ feletti definíció, ahol a véges típusú prímek megfeleltethetők a pozitív egész számok közti prímszámoknak, az egyetlen végtelen típusú prímhez tartozó értékelés pedig a szokásos abszolútérték [4].

Evertse bizonyította S-egységegyenletekre az alábbi állítást:

7. Tétel (Evertse [4]) Legyen K d-edfokú algebrai számtest és S olyan prímek véges, s-elemu halmaza K-n, melyekben az összes végtelen típusú prím benne van, a és b pedig K nemnulla elemei. Ekkor az $ax + by = 1$ egyenletnek legfeljebb $3 \cdot 7^{d+2s}$ megoldása van, ahol x és y S-egységek.

Ezt itt nem bizonyítjuk, a bizonyítás megtalálható [4]-ben.
Evertse tételének fontos következménye a racionális számokra alkalmazva [7], [10]:

Lemma. Legyen S prímszámok egy véges, s-elemu halmaza, , és pedig 0-tól különbözo egész számok. Ekkor az $x + y = z$ egyenletnek legfeljebb $6 \cdot 7^{2s+3}$ megoldása van, ahol x, y és z relatív prímek, és összes prímosztójuk S-beli.

Itt az Evertse tételében $ax + by = 1$ egy megoldásából $x + y = z$ két lemma szerinti megoldását kapjuk, amelyekben egymás ellentettei a megoldások. A kitevoben azért áll 3-as az Evertse tételbeli $d = 1$ helyett, mert a lemma szerinti S-hez hozzá kell tenni az egyetlen végtelen típusú prímet az ottani párhoz (S-hez).

Gyory, Stewart és Tijdeman a [10] cikkükben még $3 \cdot 7^{2s+3}$-mal kimondott lemmából bizonyított az Erdos-Turán-tételbol következohöz hasonlóan "logos" alsó becslést a két halmazos esetben az $a + b$ alakú számokat osztó különbözo prímek számáról:

8. Tétel (Gyory-Stewart-Tijdeman [10].) Van olyan C_1 hatékonyan kiszámolható pozitív konstans, amelyre teljesül, hogy ha A és B pozitív egész számokból álló halmazok, melyekre $|A| \geq |B| \geq 2$, akkor több mint $C_1 \log |A|$ prímszám van, amely oszt $a + b$ alakú számot ($a \in A; b \in B$).

A tétel bizonyítása (Evertse tételét használva):

Legyen B két eleme $b_1 < b_2$. Álljon S az $A + B = \{a + b : a \in A; b \in B\}$ Minkowski-összeg elemeinek prímszám osztóiból. Ekkor A bármely a_j elemére a lemmában $= 1$, $= 1$, $= b_2 - b_1$ szereposztással $x - y = (b_2 - b_1)z$-nek $x = a_j + b_2$, $y = a_j + b_1$ és $z = 1$ megoldása, relatív prímek, melyeket S-en kívüli prímszám nem oszt. Így legfeljebb $6 \cdot 7^{2|S|+3}$ megoldás lehet, miközben a_j-hoz tartozik egy-egy páronként eltéro. Tehát $|S|$ prímszám osztó esetén a nem kisebb A halmaz legfeljebb $6 \cdot 7^{2|S|+3}$ elemu lehet. Sot, ezen a_j-khez tartozó megoldások ellentettei is azok, de ezeket a_j-nél nem számoltuk, mert pl. negatívak az x-ek, így A nem lehet $3 \cdot 7^{2|S|+3}$-nél nagyobb méretu. Mindenesetre ebbol következik az állítás, pl. $7^{6|S|} = (7^6)^{|S|}$-nél kisebb $|A|$ pontosan $|S|$ prímszám osztónál. Ebből $\frac{\log|A|}{\log(7^6)}$-nál több prímszám létezik, amely oszt $a+b$ alakú számot.

A tételből következik, hogy létezik olyan pozitív valós C szám is, amelyre egy pozitív egész számokból álló A halmaznál a kéttagú összegek szorzatainak több mint $C\log|A|$ prímosztója van. (Ez az Erdős-Turán-tételből is kiderült.) Ugyanakkor ehhez nem lehet $A=B$-t feltenni, mert a kéttagú összegekbe a számok kétszereseit nem értjük bele (ebben a szakirodalom nem egységes, az Erdős-Turán-tétel első megjelenésénél Grünwald és Lázár kérdésénél a_i+a_j $(i\neq j)$ alakú kéttagú összegek vannak, a cikkben kimondott tétel állítása erre külön nem tér ki, bizonyítása nem igényli a számok kétszereseit, és például pont a következő elemien bizonyított tételt tartalmazó Stewart-Tijdeman cikkben [12] máshogy van). Viszont az egy A halmaz elemeit kettéosztva két lehető legkevésbé eltérő méretű új kisebb diszjunkt A és B halmazba már az összes $a+b$ alakú összeg az eredeti A-nak kéttagú összege. Ez is bizonyítja, hogy ez a tétel ilyen téren erősebb, mint az egy halmazos esetben a hasonló logos alsó becslés az Erdős-Turán-tételből.

Az előbbi tétel bizonyítása ugyanakkor Evertse tételén múlt, amelynek bizonyítása hosszadalmas és nem elemi. Stewart és Tijdeman ezzel szemben az Erdős-Turán-tételénél bonyolultabb, de elemi bizonyítást adott ennél kevesebb, $\log|B|/\log\log|B|$-s nagyságrendű prímosztó létezésére:

9. Tétel (Stewart, Tijdeman, az előző tétel gyengítése [12]). *Van olyan C_2 hatékonyan kiszámolható pozitív konstans, amelyre teljesül, hogy ha A és B pozitív egész számokból álló halmazok, melyekre $|A|=|B|=k\geq 3$, akkor több mint $\frac{C_2\log k}{\log\log k}$ prímszám van, amely oszt $a+b$ alakú számot ($a\in A, b\in B$).*

A tétel az elemi bizonyítás miatt figyelemreméltó, habár élesebb becslés is létezik. Természetesen az egyik halmazhoz további elemeket hozzávéve a prímosztók száma nem csökken, így ezt $C_2\log(\min(A,B))/\log\log(\min(A,B))$-s alsó becslésnek is lehet tekinteni $\min(A,B)>2$ feltevéssel élve. Ehhez képest az előző becslés tágabb érvényességgel ($\min(A,B)=2$-re is) $C_1\log(\max(A,B))$-vel becsült alulról.

A tétel bizonyítása:

Először egymásra épülő lemmákkal kezdünk:

Lemma (Stewart-Tijdeman általánosabban [12]) Legyenek x és n 1-nél nagyobb egész számok, t és g pedig 1-nél nagyobb valós számok, amelyekre $g < t \le x$ és $d_1, d_2, \ldots, d_m$ olyan különböző egész számok, amelyekre $t \le d_i \le x$ teljesül $i = 1, \ldots, m$ esetén. Legyen a d_i-k közül legalább egyet osztó prímszámok száma s. Tegyük fel, hogy

$$m \ge n((3e \log x)/\log(t/g))^s.$$

Ekkor kiválasztható a d_i-k közül n darab, $d_{l_1}, d_{l_2}, \ldots, d_{l_n}$, amelyekre $\mathrm{lnko}(d_{l_1}; d_{l_2}; \ldots; d_{l_n}) \ge g$.

Stewart és Tijdeman cikkében t és g is egész (nemcsak valós) az állításban, de ez a következő lemmánál nem lenne elég, és nem szükséges a lemma igazságához.

A lemma bizonyítása:

A d_i-k közül legalább egyet osztó prímszámok legyenek $p_1, p_2, \ldots, p_s$. $i = 1, \ldots, s$ esetén d_i prímtényezős felbontása legyen $d_i = p_1^{r_{i1}} p_2^{r_{i2}} \cdots p_s^{r_{is}}$. Mindegyik d_i-hez hozzárendeljük a

$$v_i \stackrel{\text{def}}{=} (r_{i_1} \log p_1; r_{i_2} \log p_2; \ldots; r_{i_s} \log p_s) \in \mathbb{R}^s \text{ pontot.}$$

A lemma bizonyítása azon múlik, hogy a v_i pontok száma, m elég nagy ahhoz, hogy legyen n darab, amelyeknek mindegyik koordinátája közel van egymáshoz, mind az s prímre közeli a legnagyobb őket osztó hatványának kitevője, és így legnagyobb közös osztójuk is kellően nagy.

Mind az m darab v_i-re teljesül, hogy nemnegatív az összes koordinátájuk, és koordinátáik összege, $\log d_i$-re,

$$\log d_i \le \log x.$$

Jelölje D azon poliédert, amelyre ezek teljesülnek,

$$D = \{(h_1; h_2; \ldots; h_s) : 0 \le h_1; h_2; \ldots; h_s; h_1 + h_2 + \cdots + h_s \le \log x\}.$$

Legyen

$$w \stackrel{\text{def}}{=} [s \log x/\log(t/g)] + 1;$$

a legkisebb $s \log x/\log(t/g)$-nél nagyobb egész szám. $s \log x/\log(t/g) = \log(x^s)/\log(t/g)$ nagyobb 1-nél, hiszen

$$x^s \ge x \ge t > t/g$$

és $t/g > 1$ miatt a nevező is pozitív. Ebből

$$s\log x/\log(t/g) < w < 2s\log x/\log(t/g).$$

Ezután doboznak nevezett $\frac{\log x}{w}$ élhosszú hiperkockákra bontjuk $\mathbb{R}^s$ kis részét, tekintünk olyanokat, amelyeknek egyik csúcsa $\left(\frac{k_1\log x}{w};\frac{k_2\log x}{w};\dots;\frac{k_s\log x}{w}\right)$, ahol

$$0\le k_1;k_2;\dots;k_s\in\mathbb{Z} \text{ és } k_1+k_2+\cdots+k_s\le w,$$

ők maguk pedig a

$$\left[\frac{k_1\log x}{w};\frac{(k_1+1)\log x}{w}\right]\times\left[\frac{k_2\log x}{w};\frac{(k_2+1)\log x}{w}\right]\times\cdots\times\left[\frac{k_s\log x}{w};\frac{(k_s+1)\log x}{w}\right]$$

térrészt foglalják el. Számuk legyen M.

Ezen dobozokra az említett csúcsra minimális a koordináták összege, így lefedik D-t és vele az összes v_i pontot. Ugyanis

$$k_1+k_2+\cdots+k_s\le w$$

ekvivalens a

$$\frac{k_1\log x}{w}+\frac{k_2\log x}{w}+\cdots+\frac{k_s\log x}{w}\le\log x$$

egyenlőtlenséggel, így azon pontok, amelyek koordinátái nemnegatívak $\log x$-nél nem nagyobb összeggel, lefedésre kerülnek.

A dobozainkra a koordináták összege bármely pontra legfeljebb $s\log x/\log w$-gyel nagyobb mint egy csúcsában. Ebből az M közös belső ponttal nem rendelkező dobozunk mindegyik pontjára a koordináták összege legfeljebb $\frac{(s+w)\log x}{w}$, emellett természetesen nemnegatív az összes koordináta. Így az M darab $(\log x/w)^s$ térfogatú közös belső ponttal nem rendelkező doboz egy $\frac{\left(\frac{(s+w)\log x}{w}\right)^s}{s!}$ térfogatú poliéderben van, ebből

$$M(\log x/w)^s\le\frac{\left(\frac{(s+w)\log x}{w}\right)^s}{s!};$$

így

$$M\le\frac{(s+w)^s}{s!}.$$

$s!\ge\left(\frac{s}{e}\right)^s$ teljesül minden s pozitív egész számra, ez indukcióval az $e>\left(1+\frac{1}{s}\right)^s$

egyenlőtlenségből könnyen következik. Így

$$M \le \frac{(s+w)^s}{s!} \le \frac{(s+w)^s}{\left(\frac{s}{e}\right)^s} = e^s\left(1+\frac{w}{s}\right)^s.$$

$$1 < \frac{\log x}{\log \frac{t}{g}} \text{ és } w < 2s\log x/\log(t/g)$$

miatt

$$e^s\left(1+\frac{w}{s}\right)^s < e^s\left(1+\frac{2\log x}{\log\frac{t}{g}}\right)^s < \left(\frac{3e\log x}{\log\frac{t}{g}}\right)^s.$$

Ezzel megkaptuk, hogy

$$M < \left(\frac{3e\log x}{\log\frac{t}{g}}\right)^s.$$

Most használjuk a

$$m \ge n((3e\log x)/\log(t/g))^s$$

feltételt, ebből

$$M < \frac{m}{n},$$
$$Mn < m$$

és létezik az M dobozba osztott m pontra olyan doboz, amely legalább n (sőt legalább $n+1$) pontot tartalmaz.

Legyen $v_{l_1}, v_{l_2}, \dots, v_{l_n}$ egy dobozba eső n pont a v_i-k közül. Bármely két pontra közülük az s koordináta bármelyikében legfeljebb $(\log x)/w$ a különbség, így a legnagyobb közös osztójukat osztó legnagyobb p_i-hatvány logaritmusai ($i = 1, \dots, s$ esetén) legfeljebb $\log x/w$-vel kisebb, mint bármelyik d_i-re azot osztó legnagyobb p_i-hatványé, a legnagyobb közös osztójuk logaritmusa legfeljebb $s\log x/w$-vel kisebb, mint bármelyik d_i-é. Ebből

$$\log(\mathrm{lnko}(d_{l_1}, d_{l_2}, \dots, d_{l_n})) \ge \log d_{l_1} - \frac{s\log x}{w}$$

és vele

$$\mathrm{lnko}(d_{l_1}, d_{l_2}, \dots, d_{l_n}) \ge d_{l_1}x^{-s/w} \ge tx^{-s/w}.$$

Ugyanakkor

$$w > s\log x/\log(t/g) \text{ miatt } \log(t/g) > (s\log x)/w$$

és így

$$t/g > x^{s/w} \text{ miatt } tx^{\ \ s/w} \quad g.$$

Ezzel

$$\text{lnko}(d_{l_1}; d_{l_2}; \dots; d_{l_n}) \quad d_{l_1} x^{\ \ s/w} \quad tx^{\ \ s/w} \quad g;$$

amiből

$$\text{lnko}(d_{l_1}; d_{l_2}; \dots; d_{l_n}) \quad tx^{\ \ s/w} \quad g:$$

A lemmát bebizonyítottuk.

Az előző lemmából következik az alábbi, az a_i-k és b_j-k közt a nullát is megengedve:

Lemma (Stewart-Tijdeman általánosabban [12]) Legyenek $c \quad 6$, $k; s \quad 2$ egész számok, amelyekre teljesül, hogy $k > 2(10cs)^{2s}$. Tegyük fel, hogy emellett az $a_1 < a_2 < \quad < a_k$ és $b_1 < b_2 < \quad < b_k$ nemnegatív egész számokra teljesül, hogy

$$!\Big(\prod_{1 \quad i;j \quad k} (a_i + b_j)\Big) = s;$$

végül $N = a_k + b_k$ jelölés mellett $b_k > N^{1 \quad 1/cs}$. Ekkor $a_k > N^{1 \quad 2/cs}$ teljesül, és vannak olyan l és g pozitív egész számok, amelyekre $l \quad k$, $g > N^{1 \quad 6/c}$ és bármely $j \quad 2 \quad f1; 2; \dots; kg$-ra $a_l + b_j$ osztható g-vel.

A lemma bizonyítása:

Először alkalmazzuk az előző lemmát az $a_1 + b_k$, $a_2 + b_k$, $\dots$, $a_k + b_k$ számokra, amelyek $N^{1 \quad 1/cs}$ és N közé esnek, így $m = k$, $t = N^{1 \quad 1/cs}$, $x = N$, emellett legyen $g = N^{1 \quad 2/cs}$ (itt t és g valós számok, míg x egész). A prímosztók s prím közül kerülnek ki. Ekkor

$$m \quad n((3e\log x)/\log(t/g))^s \tag{1}$$

érdekében

$$k > 2(10cs)^{2s}$$

és

$$((3e\log x)/\log(t/g))^s = ((3e\log N)/(\log(N^{1/cs})))^s = (3ecs)^s < (10cs)^s \quad 1 < \frac{2(10cs)^{2s}}{2(10cs)^s + 1}$$

miatt pl. $n = 2(10cs)^s + 1$ is lehetséges, van olyan

$$n > 2(10cs)^s$$

egész szám, amelyre teljesül az előbbi (1) egyenlőtlenség. Ez maga után vonja, hogy kiválasztható $n > 2(10cs)^s$ szám az $a_i + b_k$-k közül,

$$a_{i_1} + b_k < a_{i_2} + b_k < \cdots < a_{i_n} + b_k;$$

melyre

$$g_1 \stackrel{def}{=} \mathrm{lnko}(a_{i_1} + b_k; a_{i_2} + b_k; \dots ; a_{i_n} + b_k) \geq g = N^{1-2/cs}$$

(ezen g az előző lemma jelölései szerinti szerepeült be).

Ekkor

$$g_1 \mid a_{i_2} - a_{i_1} \text{ és } N^{1-2/cs} \leq g_1 \leq a_{i_2}.$$

Ezzel

$$a_k \geq a_{i_2} \geq N^{1-2/cs};$$

így az állítás első részét beláttuk.

Ezután ismét alkalmazzuk az előző lemmát, mégpedig minden $1 \leq j \leq k$ egész számra külön-külön az $a_{i_2} + b_j, a_{i_3} + b_j, \dots, a_{i_n} + b_j$ számokra. Ezek $N^{1-2/cs}$ és N közé esnek, így $m = n - 1$, $t = N^{1-2/cs}$ és $x = N$ feltehető. Prímosztóik szintén az $a_i + b_j$-k közül legalább egyet osztó s prím közül kerülnek ki. Az előző lemmabeli n szerepét a 2 veszi át és $g = N^{1-3/cs}$. Ekkor az (1) feltétel teljesül, mert

$$n - 1 \geq 2((3e \log N)/(\log N^{1/cs}))^s = 2(3ecs)^s;$$

hiszen

$$n > 2(10cs)^s\text{-ből } n > 2(9cs)^s + 1 > 2(3ecs)^s + 1.$$

Ebből bármely $j \in \{1; 2; \dots ; k\}$ esetén az $a_{i_2} + b_j, a_{i_3} + b_j, \dots, a_{i_n} + b_j$ számok közül létezik 2, amelyek legnagyobb közös osztója legalább $N^{1-3/cs}$. Legyen egy ilyen pár $a_{i_{j_1}} + b_j$ és a nagyobb $a_{i_{j_2}} + b_j$, legnagyobb közös osztójuk $g_2(j)$.

Ekkor

$$g_1 \mid (a_{i_{j_2}} + b_k) - (a_{i_{j_1}} + b_k)$$

és

$$g_2(j)\ j\ (a_{i_{j\,2}} + b_j) \quad (a_{i_{j\,1}} + b_j)$$

mindkét esetben két többszörösének különbségeként, ́gy bármely 1 j k egész számra g_1 és $g_2(j)$ is osztja $a_{i_{j\,2}}$ $a_{i_{j\,1}}$-et, amely kisebb a_k $0 = a_k$-nál és vele N-nél is. Így g_1 és $g_2(j)$ legkisebb közös többszöröse, lkkt$(g_1; g_2(j))$, nem nagyobb N-nél. Ekkor

$$\text{lnko}(g_1; g_2(j)) = \frac{g_1 g_2(j)}{\text{lkkt}(g_1; g_2(j))} \quad \frac{N^{1\ \ 2=cs} N^{1\ \ 3=cs}}{N} = N^{1\ \ 5=cs}:$$

Így

$$g_3(j) \stackrel{\text{def}}{=} \text{lnko}(g_1; g_2(j)) \quad N^{1\ \ 5=cs}:$$

Legyen

$$g_4 \stackrel{\text{def}}{=} \text{lnko}(g_3(1): g_3(2); :::; g_3(k)):$$

Ekkor g_4 is közvetve néhány $a_i + b_j$ alakú szám legnagyobb közös osztójából van származtatva legnagyobb közös osztó képzésekkel, ́gy csak s pŕımszám közül kerülnek ki az osztói. Mivel g_1 2 $[N^{1\ \ 2=cs}; N]$ is ilyen, és mindegyik $g_3(j)$-nek többszöröse, az s pŕımszám közül bármelyik p-re és bármelyik 1 j k-ra p legnagyobb hatványa, amely a g_1-et osztja, legfeljebb $N^{5=cs}$-szerese azon legnagyobb p-hatványnak, amely az $N^{1\ \ 5=cs}$-nél nem kisebb $g_3(j)$-t osztja. Ebből mind az s darab ilyen p pŕımszámra g_1-hez képest az lnko$(g_3(1): g_3(2); :::; g_3(k))$-re azot osztó legnagyobb p-hatvány legalább $N^{5=cs}$-szerese. Így

$$g_4 \quad g_1(N^{\ 5=cs})^s \quad N^{1\ \ 2=cs\ \ 5=c} \quad N^{1\ \ 6=c}:$$

Egyenlőség persze nem lehet mindenütt, pl. nem lehet az s-bol 2 darab p pŕımszámra is g_1-hez képest az lnko$(g_3(1): g_3(2); :::; g_3(k))$-re azot osztó legnagyobb p-hatvány ugyanannyiszorosa, de nem egyszerese. (Ez és az hasońıt az előző lemma bizonýıtásának végére.)

Ezzel van egy $g_4 > N^{1\ \ 6=c}$ szám, amely $g_3(1), g_3(2), :::, g_3(k)$ legnagyobb közös osztója, ő legyen (az új) g. l pedig i_1 lesz, ekkor persze

$$g > N^{1\ \ 6=c} \text{ és } g\ j\ a_l + b_j$$

is fennáll minden 1 j k egész számra. Utóbbihoz

$$g\ j\ g_3(1)\ j\ g_1\ j\ a_l + b_k\text{-ból } g\ j\ a_l + b_k,$$

emellett

$$g\ j\ g_3(j)\ j\ a_{i_{j\,1}} + b_j$$

és
$$g \mid g_1 \mid a_{i_{j_1}} + b_k.$$
Különbségükből
$$g \mid b_k - b_j$$
és vele
$$g \mid a_l + b_j$$
minden $1 \le j \le k$ egész számra az
$$a_l + b_k = (a_l + b_j) + (b_k - b_j)$$
felírásából. Ezzel megvan az állítás második része is. A lemma állításait bebizonyítottuk.

Végül jöjjön a tétel bizonyítása az előző lemma segítségével:

Belátjuk, hogy ha A és B is k nemnegatív egész számot tartalmaz, ahol
$$k > 10^{6s} s^{2s},$$
akkor az $a_i + b_j$ alakú összegek ($a_i \in A$, $b_j \in B$) közül legalább egyet több mint s prímszám oszt. A elemei
$$a_1 < a_2 < \cdots < a_k,$$
míg B-é
$$b_1 < b_2 < \cdots < b_k.$$
Tegyük fel, hogy valamely s pozitív egész számra és $k > 10^{6s}s^{2s}$ egész számra van olyan k-k nemnegatív egész számot tartalmazó A és B, melyre pontosan s prímszám oszt $a_i + b_j$ alakú számot ($1 \le i, j \le k$), $10^{6s}s^{2s}$ nemnegatív egész számokon szigorú monotonitása miatt ha az előbbi állítás nem teljesülne, lenne ilyen ellenpélda.

Ekkor olyan ellenpélda is lenne, ahol az $a_i + b_j$ alakú összegek legnagyobb közös osztója 1. Ugyanis az eredeti ellenpéldában ha
$$o > 1$$
lenne a legnagyobb közös osztó, A és B elemei is egy-egy halmazon belül egyenlő maradékot adnának o-val osztva, így A elemeiből az eredeti a_1-et kivonva, B elemeihez (a_1-et) hozzáadva az összes $a_i + b_j$ alakú összeg az eredeti, így o-val osztható lenne, ráadásul A és B összes

eleme is. Leosztva c-val mindkét módosítással kapott halmaz elemeit, az $a_i + b_j$ alakú összegek prímosztóinak száma nem nőne, az $a_i + b_j$-k legnagyobb közös osztója 1 lenne, így esetlegesen kisebb s-sel (az c-val osztással eltűnhetnek prímszámok az $a_i + b_j$-k $(1 \le i; j \le k)$ osztóiból) ugyanúgy ellenpéldát kapnánk az $a_i + b_j$-k 1 legnagyobb közös osztójával.

Itt használtuk, hogy nemnegatív egészek vannak a halmazokban, pl. $A = B = \{1; 3\}$ esetén ilyen módosításnál az új halmazokra az összes $a_i + b_j$-t $(1 \le i; j \le 2)$ a legnagyobb közös osztójukkal leosztva

$$a_1 + b_1 = 1$$

lenne, így nem lehet minden szám pozitív egész a módosítás után. Ezért tettük fel az előző lemmában, hogy a k-k szám nemnegatív egész, és nem azt, hogy pozitív egész, az eredeti Stewart-Tijdeman cikkel ellentétben.

Ellentmondást abból fogunk kapni, hogy a második lemmából mégis mindenképp lenne 1-nél nagyobb közös osztója az $a_i + b_j$ alakú $(1 \le i; j \le k)$ számoknak. Legyen

$$a_k + b_k = N \text{ és } b_k \le a_k.$$

$s = 1$ esetén

$$10^6 > k\text{-ra}$$

pl.

$$b_k < a_2 + b_k < a_3 + b_k < 2b_k$$

miatt lenne két 1-nél nagyobb szám, $a_2 + b_k$ és $a_3 + b_k$ az összegek közt, amelyek hányadosa 1-nél nagyobb és 2-nél kisebb, így nem lehetnek ugyanazon prím hatványai, ebből lenne két prímosztó és ellentmondás. Innentől $s > 1$.

Használjuk az előző lemmát $c = 20$ mellett.

$b_k \le a_k$ miatt

$$b_k \le N/2;$$

továbbá

$$k > 10^{6s} s^{2s} > 8^{6s} 2^{2s} = 2^{20s};$$

és vele

$$N = a_k + b_k \ge 2^{20s}.$$

Ebből

$$b_k \le N/2 \le N^{1-1/20s}$$

és tényleg alkalmazható a lemma. Eszerint van olyan

$$l \quad k$$

pozitív egész szám és

$$g_4 > N^{1 \quad 6=20} = N^{7=10}$$

pozitív egész szám, hogy mindegyik $a_l + b_j$ $(1 \quad j \quad k)$ osztható g_4-gyel. Emellett

$$a_k > N^{1 \quad 2=20s} = N^{1 \quad 1=10s}:$$

Még egyszer használjuk a második lemmát, most $c = 10$ mellett az a_i-k és b_j-k szerepét felcserélve.

$$a_k > N^{1 \quad 1=10s};$$

így vannak olyan pozitív egész

$$J \quad k \text{ és } g_5 > N^{1 \quad 6=10} = N^{2=5}$$

számok, amelyre mindegyik $a_i + b_J$ $(1 \quad i \quad k)$ osztható g_5-tel.

A lemma használata után jön egy bizonyításához hasonló rész, becsüljük

$$g_6 \stackrel{\text{def}}{=} \text{lnko}(g_4; g_5)\text{-t.}$$

$g_4 \mid a_l + b_J$ és $g_5 \mid a_l + b_J$ miatt

$$\text{lkkt}(g_4; g_5) \quad a_l + b_J \quad a_k + b_k = N;$$

ugyanis $a_l + b_J$ pozitív egész szám, nem lehet 0. Ebből

$$g_6 = \frac{g_4 g_5}{\text{lkkt}(g_4; g_5)} \quad \frac{N^{7=10} N^{2=5}}{N} = N^{1=10}:$$

Így g_6 1-nél nagyobb.

Ugyanakkor bármely $1 \quad i; j \quad k$ esetén

$$g_6 \mid g_5 \mid a_i + b_J;$$

$$g_6 \mid g_4 \mid a_l + b_j$$

és

$$g_6 \mid a_l + b_J;$$

így g_6 osztja

$$(a_i + b_J) + (a_l + b_j) - (a_l + b_J) = a_i + b_j\text{-t.}$$

Így megkaptuk egy 1-nél nagyobb közös osztóját az $a_i + b_j$ alakú számoknak, ami ellentmondás. Ezzel beláttuk, hogy bármely k és s pozitív egész számokra $k > 10^{6s}s^{2s}$ esetén k-k elemű pozitív egész számokból álló A és B halmazokra az $a_i + b_j$ $(1 \le i; j \le k)$ alakú számoknak s-nél több prímszám osztója van.

Ebből már könnyebben következik, hogy a tétel állítása szerinti olyan C_2 létezik $k \ge 3$-ra, amelyre k elemre több mint $C_2 \log k / \log\log k$ prímszám van, amely $a + b$ alakú számot ($a \in A$, $b \in B$) oszt. Ugyanis

$$(\log x / \log\log x)' = \frac{\frac{\log\log x}{x} - \frac{1}{x}}{(\log\log x)^2};$$

így e^e-ben 0, e és e^e közt negatív, e^e-nél nagyobb x-ekre pozitív. Eszerint e^e-nél nagyobb számokra adott s pozitív egész szám mellett s prímosztónál az elképzelhető legnagyobb $10^{6s}s^{2s}$ miatt kell a legkisebbnek lennie C_2-nek ahhoz, hogy igaz legyen az állítás.
$s \ge 2$-re eszerint elég, ha

$$s > C_2 \log(10^{6s}s^{2s})/\log\log(10^{6s}s^{2s}).$$

Itt

$$\log(10^{6s}s^{2s})/\log\log(10^{6s}s^{2s}) = \frac{6s\log 10 + 2s\log s}{\log(6s\log 10 + 2s\log s)} < \frac{6s\log(5s) + 2s\log(5s)}{\log(5s)} = 8s;$$

így

$$C_2 \log(10^{6s}s^{2s})/\log\log(10^{6s}s^{2s}) < 8C_2 s$$

miatt $C_2 \le 1/8$ esetén 10^6-nál nagyobb számokra megleszünk.

$s = 1$-re viszont $k \ge 3$-re nézve $\log x / \log\log x$ viselkedéséből

$$e < 3 < e^e < 10^6$$

miatt

$$N = 3 \text{ és } N = 10^6$$

adja a legerősebb becslést,

$$1 > C_2 \log(10^6)/\log\log(10^6) \text{ és } 1 > C_2 \log(3)/\log\log(3)$$

közül előbbire

$$6 < \log(10^6) < 18$$

és

$$\log\log(10^6) > 2$$

miatt

$$1 > 9C_2$$

elég, utóbbinál pedig

$$\log 3 \approx 11/10,\ \log\log 3 \approx 1/10{,}63$$

miatt

$$1 \geq 12C_2$$

elégséges. Így például $C_2 = 1/12$ esetén teljesül a tételállítása. A tételállítását bebizonyítottuk.

3.2. Felső becslés a prímosztók minimális számára

A Győry-Stewart-Tijdeman-féle $\log|A|$-s alsó becslés az összegek prímosztóira nincs olyan messze a lehetséges minimális értéktől az alábbi felső becslés szerint:

10. Tétel (Erdős-Stewart-Tijdeman [1], [9]) Van olyan C pozitív valós szám, amelyre bármely $n \geq 3$ pozitív egész számra vannak olyan A és B halmazok pozitív egész számokból, hogy $n = |A| > |B| = 2$ és az $a + b$ $(a \in A; b \in B)$ alakú számokat összesen legfeljebb $C(\log|A|)^2 \log\log|A|$ különböző prímszám osztja.

Mivel a prímszámtétel alapján n-ig kb. $\frac{n}{\log n}$ prímszám van, ehhez elég, ha az $a + b$ alakú számok szorzatának nincsenek túl nagy, $(\log|A|)^2(\log\log|A|)^2$ konstansszorosánál nagyobb prímosztói, ekkor egyik $a + b$-nek sem lesznek, és ezzel $(\log|A|)^2 \log\log|A|$ valamilyen megfelelő konstansszorosánál több prímszám semmilyen $|A|$-ra sem osztja őket (minden 2-nél nagyobb véges elemszámra létezik megfelelő A, és hozzá kételemű B). Jelölje $P(k)$ bármely $k > 1$ pozitív egész számra a legnagyobb prímosztóját [1]. A 10. tételt a következő tételen keresztül látták be ([1] alapján haladunk).

11. Tétel (Erdős-Stewart-Tijdeman [1]) Legyen f olyan, az 1-nél nagyobb valós számok halmazáról $\mathbb{R}$-be képező függvény, amelyre $f(x)/\log x$ monoton csökken, és $x \to \infty$ esetén $f(x) \to \infty$. Emellett legyen $0 < \varepsilon < 1$. Tegyük fel, hogy k nagyobb egy f-től és ε-tól függően elég nagy hatékonyan kiszámolható valós számnál és $2 \le l \le (\log k)/f(k)$ az l pozitív egész számra. Ekkor létezik olyan A különböző pozitív egész számokból álló halmaz és B különböző nemnegatív egész számokból álló halmaz, amelyekre $|A| = k$, $|B| = l$, és

$$P\left(\prod_{a\in A, b\in B}(a+b)\right) \le \left((1+\varepsilon)\frac{\log k}{l}\log\left(\frac{\log k}{l}\right)\right)^{l}.$$

A 11. tétel bizonyítása:

A tétel bizonyításához három lemmára van szükségünk. Az első kombinatorikai jellegű:

Lemma (Erdős-Stewart-Tijdeman [1]) Legyen N pozitív egész szám, $H \subseteq \{1, 2, \dots, N\}$ nemüres halmaz, és $1 \le l \le |H|$ egész szám. Ekkor léteznek olyan A és B halmazok nemnegatív egész számokból, amelyekre $A + B \subseteq H$, $0 \in B$, $|B| = l$, és

$$|A| \ge \binom{|H|}{l} \Big/ \binom{N-1}{l-1}.$$

A lemma bizonyítása:

H-ból l elemet $\binom{|H|}{l}$-féleképpen választhatunk ki. Ha a kiválasztott elemek

$$h_1 < h_2 < \dots < h_l,$$

akkor tekintsük a $\{h_2 - h_1, h_3 - h_1, \dots, h_l - h_1\}$ szám $l-1$-est, amely $\{1, 2, \dots, N-1\}$ részhalmazaként (legfeljebb) $\binom{N-1}{l-1}$-féle lehet. Az ilyen kiválasztásokból bármely H-ra van olyan, amelyre legalább $\binom{|H|}{l}/\binom{N-1}{l-1}$-szer ugyanaz $\{h_2 - h_1, h_3 - h_1, \dots, h_l - h_1\}$. Ekkor mindre azok h_1-ei eltérők és bármely ilyen h_1-re az ezen kiválasztásokra állandó $\{0, h_2 - h_1, h_3 - h_1, \dots, h_l - h_1\}$ halmaz bármelyik elemét hozzáadva H elemét kapjuk. Ily módon B-nek egy legalább $\binom{|H|}{l}/\binom{N-1}{l-1}$ kiválasztáshoz tartozó $\{0, h_2 - h_1, h_3 - h_1, \dots, h_l - h_1\}$ halmazt választva ezek h_1-eit A-nak választva teljesülnek a kikötések a két nemnegatív egész számokat tartalmazó halmazra, $A + B \subseteq H$, $0 \in B$, $|B| = l$ és $|A| \ge \binom{|H|}{l}/\binom{N-1}{l-1}$. A lemmát bebizonyítottuk.

Jelölje $\Psi(x; y)$ azon x-nél nem nagyobb pozitív egész számok darabszámát, amelyeknek nincs y-nál nagyobb prímszám osztója. Legyen $\exp(z) \stackrel{\text{def}}{=} e^z$ a szokásos módon.

Lemma (Canfield-Erdős-Pomerance [1]) Létezik olyan c hatékonyan kiszámolható valós konstans, amelyre ha x pozitív egész szám és $u \geq 3$ valós szám,

$$\Psi(x, x^{1/u}) \geq x \exp\left(-u\left(\log u + \log\log u - 1 + c\frac{\log\log u}{\log u}\right)\right).$$

A lemmát nem bizonyítjuk.

Az előbbi két lemma miatt teljesül a következő, amelyből pedig a 11. tétel.

Lemma (Erdős-Stewart-Tijdeman [1]) Legyenek $c \geq 1$ és $0 < \varepsilon < 1$ valós számok. Legyen f az 1-nél nagyobb valós számok halmazáról R-be képező függvény, amelyre $f(x)/\log x$ monoton csökkenő, és $x \to \infty$ esetén $f(x) \to \infty$. Legyenek N és l olyan pozitív egész számok, amelyekre N nagyobb egy c-től, ε-tól és f-től függő hatékonyan kiszámolható valós számnál, emellett $2 \leq l \leq (\log N)/f(N)$. Legyen

$$m = \left\lfloor \exp\left((1-\varepsilon)\frac{\log N}{\log\frac{\log N}{l}}\left(1 + \frac{\log c}{l}\right)\right)\right\rfloor$$

és

$$t = \left[c\left(\frac{\log N}{l}\right)^{l}\right].$$

Ekkor vannak olyan $a_1 < a_2 < \dots < a_m \leq N$ pozitív egész számok és $0 = b_1 < b_2 < \dots < b_l < N$ nemnegatív egész számok, amelyekre

$$P\left(\prod_{i=1}^{m}\prod_{j=1}^{l}(a_i + b_j)\right) \geq t.$$

A lemma bizonyítása:

A bizonyítás során használjuk a standard o jelölést, mely szerint az $o(r)/r$ tört $N \to \infty$ esetén 0-hoz tart.

Mivel

$$l \leq \frac{\log N}{f(N)};$$

$$f(N) \leq \frac{\log N}{l};$$

ebbol

$$[c(f(N))^l] \quad t$$

és´gy

$$(N;t) \quad (N;[c(f(N))^l]) \quad [c(f(N))^l] \quad [(f(N))^l] > f(N)$$

kelloen nagy N-re. Elég nagy N-re

$$(f(N))^l > l^3$$

minden $l \quad 2$ egész számra, pl. $f(N) \quad 8$-ra ez teljesül. Ilyenkor

$$(N;t) \quad l^3:$$

Használjuk a tétel után elsonek kimondott lemmát, H azon $(N;t)$ darab N-nél nem nagyobb pozitív egész számot tartalmazza, amelyeknek nincs t-nél nagyobb prímosztója. A lemma feltételei teljesülnek, $(N;t) \quad l$ miatt vannak olyan A és B halmazok nemnegatív egész számokból, amelyekre $A + B \quad H$, $0 \; 2 \; B$, $jBj = l$, és

$$jAj \quad \frac{jHj \cdot N \quad 1}{l \quad l \quad 1} = \frac{(N;t) \cdot N \quad 1}{l \quad l \quad 1} > \frac{(\ (N;t) \quad l)^l \cdot}{l!} \frac{N^{l \quad 1}}{(l \quad 1)!} =$$

$$\frac{(\ (N;t) \quad l)^l}{lN^{l \quad 1}} = (1 + o(1)) \frac{(\ (N;t))^l}{lN^{l \quad 1}} ;$$

ehhez a binomiális együtthatókból az egyiket csökkentettük, a másikat növeltük.

Itt

$$\frac{(N;t)}{(N;t) \quad l}^{\ l} ! \quad 1$$

teljesül $N \; ! \; 1$ esetén. Ehhez elég a reciprokot nézni,

$$1 \quad \frac{l}{(N;t)}^{\ l} ! \quad 1;$$

ugyanis

$$1 \quad 1 \quad \frac{l}{(N;t)}^{\ l} \quad 1 \quad \frac{l^2}{(N;t)}:$$

Tehát

$$\frac{l^2}{(N;t)} ! \quad 0$$

teljesülése $N \; ! \; 1$ esetén elegséges. Itt a számláló nem nagyobb, mint $\frac{\log N}{f(N)}^{\ 2}$, a nevezo legalább

$$(N;[cf(N)^l]) \qquad (N;[f(N)^2])$$

´gy $f(N) > 3$-ra

$$0 \quad \frac{l^2}{(N;t)} \quad \frac{\frac{\log N}{3}\;^2}{(N;t)} \quad \frac{\frac{\log N}{3}\;^2}{(N;[f(N)^2])} \quad \frac{\frac{\log N}{3}\;^2}{(N;9)}:$$

Itt $N^{1=3}$-ig kb. $\log N$-nel arányos számú 2, 3 és 5-hatvány miatt nagy N-ekre ilyenek szorzatainak $(N;9)$-hez hozzájárulásából

$$(N;9) > c_0(\log N)^3$$

fennáll kis $c_0 > 0$ konstansra, ´gy még $\frac{\frac{\log N}{3}\;^2}{(N;9)}$ is 0-hoz tart, ha N a végtelenhez. Rendelvvel $\frac{l^2}{(N;t)}$! 0 és belőle

$$\frac{(N;t)}{(N;t) \quad l}\;^l \; ! \quad 1$$

is teljesülnek N ! 1 esetén, jogos az $o(1)$ használata.

Ha ezzel $jAj \quad m$ is teljesülne, kész lennénk a lemma bizonyításával, ugyanis A m elemét $a_1 < a_2 < \quad < a_m$-nek és B elemeit $b_1 < b_2 < \quad < b_l$-be választva egyik $a_i + b_j$ alakú összegnek sem lehet m-nél nagyobb prímszám osztója.

Eszerint elég belátni, hogy $jAj \quad m$, amihez

$$jAj \quad (1 + o(1))\frac{(\;\;(N;t))^l}{lN^{l \quad 1}}$$

miatt

$$(1 + o(1))\frac{(\;\;(N;t))^l}{lN^{l \quad 1}} \qquad m$$

elég nagy N-ekre elegendő.

Itt $(N;t) \quad l^3$ miatt az előző lemmát használhatjuk x helyett N-nel, az ottani u szerepét $\frac{\log N}{\log t}$ tölti be. Ekkor

$$\frac{\log N}{\log t} = \frac{\log N}{\log \;\; c \; h\frac{\log N}{l} \; i^{\,l}} = \frac{\log N}{\log c + l\log \;\; \frac{\log N}{l} \;\; + o(1)};$$

mert $N \to \infty$ esetén

$$t \to \infty\,;$$

hiszen

$$\frac{\log N}{l} \geq f(N) \text{ és } f(N) \to \infty$$

ilyenkor. Ezt átírva

$$\frac{\log N}{\log t} = \frac{\log N}{\log c + l \log\left(\frac{\log N}{l}\right) + o(1)}$$
$$= \frac{\log N}{l \log\left(\frac{\log N}{l}\right)} - \frac{\log N\,(\log c + o(1))}{l \log\left(\frac{\log N}{l}\right)\left(\log c + l \log\left(\frac{\log N}{l}\right) + o(1)\right)}$$
$$= \frac{\log N}{l \log\left(\frac{\log N}{l}\right)} - \frac{\log N\,(\log c + o(1))}{l^2 \log^2\left(\frac{\log N}{l}\right)}:$$

Ugyanis

$$\frac{\log N\,(\log c + o(1))}{l \log\left(\frac{\log N}{l}\right)\left(\log c + l \log\left(\frac{\log N}{l}\right) + o(1)\right)} - \frac{\log N \log c}{l^2 \log^2\left(\frac{\log N}{l}\right)}$$

$$= \log N \frac{(\log c + o(1))\, l \log\left(\frac{\log N}{l}\right) - \log c\left(\log c + l \log\left(\frac{\log N}{l}\right) + o(1)\right)}{l^2 \log^2\left(\frac{\log N}{l}\right)\left(\log c + l \log\left(\frac{\log N}{l}\right) + o(1)\right)}$$
$$= \log N \frac{o(1)\, l \log\left(\frac{\log N}{l}\right) - (\log c)^2 - o(1)\log c}{l^2 \log^2\left(\frac{\log N}{l}\right)\left(\log c + l \log\left(\frac{\log N}{l}\right) + o(1)\right)}$$
$$= \left(\frac{1}{l^2 \log^2\left(\frac{\log N}{l}\right)}\right)\left(\frac{\log N\left(o(1)\, l \log\left(\frac{\log N}{l}\right) - (\log c)^2 - o(1)\log c\right)}{\log c + l \log\left(\frac{\log N}{l}\right) + o(1)}\right):$$

A jobb oldali tényező $1/\log N$-szerese 0-hoz tart $N \to \infty$ esetén, így a $\log N\ o(1)$-gyel helyettesítése szabályos volt.

Ugyanakkor

$$\frac{\log N}{\log t} = \frac{\log N}{l \log\left(\frac{\log N}{l}\right)} - \frac{\log N\,(\log c + o(1))}{l^2 \log^2\left(\frac{\log N}{l}\right)}$$

´rható

$$\frac{\log N}{l\log \frac{\log N}{l}} + o(1)\frac{\log N}{l\log \frac{\log N}{l}}$$

alakba is, ebbol

$$\frac{\log N}{\log t} = (1+ o(1))\frac{\log N}{l\log \frac{\log N}{l}}:$$

Így

$$\log \frac{\log N}{\log t} = \log \frac{\log N}{l} \quad \log\log \frac{\log N}{l} + o(1)$$

és

$$\log\log \frac{\log N}{\log t} = \log\log \frac{\log N}{l} + o(1):$$

Az elozo lemmából $u = \frac{\log N}{\log t}$ 3-mal

$$(N;t) \quad N\exp \quad u \quad \log u + \log\log u \quad 1 + c\frac{\log\log u}{\log u} =$$

$$N\exp \quad \frac{\log N}{l\log \frac{\log N}{l}} + \frac{\log N(\log c + o(1))}{l^2 \log \frac{\log N}{l}^2} \quad \log \frac{\log N}{l} \quad 1+o(1) \quad ,$$

itt $c\frac{\log\log u}{\log u}$ helyére is´rjuk az $o(1)$-et. Ebbol

$$(1+o(1))\frac{((N;t))^l}{lN^{l-1}} =$$

$$(1+o(1)) \quad N\exp \quad \frac{\log N}{l\log \frac{\log N}{l}} + \frac{\log N(\log c + o(1))}{l^2 \log \frac{\log N}{l}^2} \quad \log \frac{\log N}{l} \quad 1+o(1) \quad ^l . \quad (lN^{l-1})$$

$$= (1+o(1))\frac{N}{l}\exp \quad \frac{\log N}{\log \frac{\log N}{l}} + \frac{\log N(\log c + o(1))}{l \log \frac{\log N}{l}^2} \quad \log \frac{\log N}{l} \quad 1+o(1)$$

$$= (1+o(1))\frac{N}{l}\exp \quad \log N + \frac{\log N}{\log \frac{\log N}{l}} + \frac{\log N(\log c + o(1))}{l \log \frac{\log N}{l}} \quad \frac{\log N(\log c + o(1))}{l \log \frac{\log N}{l}^2}$$

$$+ \quad \frac{\log N}{\log \frac{\log N}{l}} + \frac{\log N(\log c + o(1))}{l \log \frac{\log N}{l}^2} \quad (o(1))$$

$$= (1+o(1))\frac{1}{l}\exp \quad \frac{\log N}{\log \frac{\log N}{l}} + \frac{\log N(\log c + o(1))}{l \log \frac{\log N}{l}} \quad \frac{\log N(\log c + o(1))}{l \log \frac{\log N}{l}^2} + \quad \frac{\log N}{\log \frac{\log N}{l}}$$

$$+\frac{\log N(\log c+o(1))}{l\log\left(\frac{\log N}{l}\right)^{2}}(o(1))$$

$$=(1+o(1))\frac{1}{l}\exp\left(\frac{\log N}{\log\frac{\log N}{l}}\left(1+\frac{\log c}{l}+o\left(\frac{\log N}{\log\frac{\log N}{l}}\right)\right)\right).$$

E szerint

$$(1+o(1))\frac{((N;t))^{l}}{lN^{l-1}}=(1+o(1))\frac{1}{l}\exp\left(\frac{\log N}{\log\frac{\log N}{l}}\left(1+\frac{\log c}{l}+o\left(\frac{\log N}{\log\frac{\log N}{l}}\right)\right)\right):$$

Az $\frac{1}{l}$-es szorzó

$$l \quad \frac{\log N}{f(N)}$$

miatt elég nagy N-ekre $l<\log N$-nel jár, így

$$\log l<\log\log N:$$

Ugyanakkor $l<\log N$-re

$$\frac{\log N}{\log\frac{\log N}{l}}>\frac{\log N}{\log\log N};$$

ezzel $\log l$ beleszámolható a kitevőbeli $o\left(\frac{\log N}{\log\frac{\log N}{l}}\right)$-be, ha $N\to 1$,

$$(\log l)\Big/\left(\frac{\log N}{\log\frac{\log N}{l}}\right)\to 0:$$

Így

$$(1+o(1))\frac{((N;t))^{l}}{lN^{l-1}}=(1+o(1))\exp\left(\frac{\log N}{\log\frac{\log N}{l}}\left(1+\frac{\log c}{l}+o\left(\frac{\log N}{\log\frac{\log N}{l}}\right)\right)\right)$$

$$=\exp\left((1+o(1))\frac{\log N}{\log\frac{\log N}{l}}\left(1+\frac{\log c}{l}\right)\right).$$

$o(1)$-et bevittük a kitevőbe és $o(1)\left(\frac{\log N}{\log\frac{\log N}{l}}\right)\left(1+\frac{\log c}{l}\right)$ lecserélhető $o\left(\frac{\log N}{\log\frac{\log N}{l}}\right)$-re.

Adott c, és f esetén elég nagy N-ekre

$$2 \quad l \quad (\log N)=f(N)$$

mellett itt

$$(1+o(1))\frac{(\ (N;t))^{l}}{lN^{l\ \ 1}} = \exp\ (1+o(1))\ \frac{\log N}{\log \frac{\log N}{l}}\ 1+\frac{\log c}{l}$$

$$\exp\ (1\quad)\frac{\log N}{\log\frac{\log N}{l}}\ 1+\frac{\log c}{l} \quad = m.$$

Ezzel a kapott A halmazra $jAj \quad m$ elég nagy N-ek és megfelelő l esetén. A lemma állítását bebizonyítottuk.

A 11. tétel bizonyításához az előző lemmát alkalmazzuk. Legyen

$$N = \exp\ (1+")\log k \log\frac{\log k}{l}\ ,\quad = \frac{"}{5}$$ és $c = 1$. Elég nagy k-kra N elég nagy lesz, emellett k-nál nagyobb, így

$$l \quad \frac{\log N}{f(N)}$$

a $\frac{\log x}{f(x)}$ függvény monoton növekedéséből, az előző lemma alkalmazható. A lemmában

$$t = c\ \frac{\log N}{l} = \frac{\log\exp\ (1+")\log k\log\frac{\log k}{l}}{l}$$

$$\frac{(1+")\log k\log\frac{\log k}{l}}{l} \qquad \frac{(1+")\log k\log\frac{\log k}{l}}{l}\ ;$$

így a kapott A és B halmazokra (amelyek az a_i-kból és a b_j-kből állnak) a legnagyobb prímosztóra vonatkozó állítás teljesül. Az f függvényre vonatkozó kikötései a tételnek a lemmában is megvannak.

Már csak az kell, hogy A-nak van k eleme, vagyis $k \quad m$.

$$m = \exp\ (1\quad)\frac{\log N}{\log\frac{\log N}{l}}\ 1+\frac{\log c}{l}$$

$$= \exp\ 1\ \frac{"}{5}\ \frac{\log\exp\ (1+")\log k\log\frac{\log k}{l}}{\log\frac{\log\exp\ (1+")\log k\log\frac{\log k}{l}}{l}}\ 1\ :$$

Elég nagy k-kra
$$l < \frac{\log k}{2}$$
és
$$m = \left\lfloor \exp\left(\frac{\left(1-\frac{\varepsilon}{5}\right)\log\left\lfloor \exp\left((1+\varepsilon)\log k \log \frac{\log k}{l}\right)\right\rfloor}{\log \frac{\log\left\lfloor \exp\left((1+\varepsilon)\log k \log \frac{\log k}{l}\right)\right\rfloor}{l}} \right)\right\rfloor \geq$$
$$\geq \exp\left(\frac{\left(1-\frac{\varepsilon}{5}\right)\log\left\lfloor \exp\left((1+\varepsilon)\log k \log \frac{\log k}{l}\right)\right\rfloor}{\log \frac{\log\left\lfloor \exp\left((1+\varepsilon)\log k \log \frac{\log k}{l}\right)\right\rfloor}{l}} \right) \geq$$
$$\geq \exp\left(\frac{\left(1+\frac{\varepsilon}{2}\right)\log k \log \frac{\log k}{l}}{\left(1+\frac{\varepsilon}{2}\right)\log \frac{\log k}{l}} \right) = k^{\frac{\left(1+\frac{\varepsilon}{2}\right)\log \frac{\log k}{l}}{\left(1+\frac{\varepsilon}{2}\right)\log \frac{\log k}{l}}} = k.$$

Itt a kitevőben a számlálót és a nevezőt rendre csökkentettük és növeltük. Ezzel A-nak megvan a k eleme. A 11. tételt bebizonyítottuk.

A 11. tételt pl. $f(x) = \frac{\log x}{2}$-re alkalmazva $l = 2$ és tetszőleges $0 < \varepsilon < 1$ mellett elég nagy k-k esetén van olyan k elemű A halmaz pozitív egész számokból, és 2 elemű B halmaz nemnegatív egész számokból, amelyekre
$$P\left(\prod_{a\in A, b\in B}(a+b)\right) \leq \left((1+\varepsilon)\frac{\log k}{2}\log\frac{\log k}{2}\right)^2;$$
ezzel $\left(\frac{1}{4}+\varepsilon\right)(\log|A|)^2(\log\log|A|)^2$-nél kisebb a legnagyobb prímosztója az $a+b$ ($a \in A$; $b \in B$) alakú számoknak. Így mivel a prímszámtétel szerint $n \to \infty$ esetén
$$\pi(n) \Big/ \frac{n}{\log n} \to 1,$$
ahol $\pi(n)$ az n pozitív egésznél nem nagyobb prímszámok száma, elég nagy (ε-tól függő) k-kra $\left(\frac{1}{8}+\varepsilon\right)(\log|A|^2)\log\log|A|$-nél kevesebb különböző prímosztója van a 11. tétel segítségével kapott halmazokra az $a+b$ ($a \in A$; $b \in B$) alakú számoknak. Ugyanakkor itt B-ben az egyik

elem a 0, míg

$$A + B \subseteq \{1, 2, \dots, 2N\} \subseteq \{1, 2, \dots, 2k^{2\log\log k}\};$$

de B elemeihez 1-et hozzáadva, A elemeiből 1-et kivonva és az esetlegesen A-ra került 0-t más k-nál nem nagyobb pozitív egész számra cserélve $A+B$-be csak utóbbi miatt kerülhetnek új számok, de azok ketten $2k^{2\log\log k}$-nél kisebbként $(\log k)\log\log k$-val arányos számú új prímosztót hozhatnak. Ebből elég nagy k-kra pozitív egész számokból van k elemű A és 2 elemű B halmaz, amelyekre az $a+b$ alakú összegek prímosztóinak száma pl. legfeljebb $(\log|A|)^2\log\log|A|$. A véges sok kisebb $k \geq 3$ pozitív egész számra az ilyen esetben a minimális száma az $a+b$ alakú összegek prímosztóinak mindre $(\log k)^2\log\log k$ pozitív konstansszorosa, az ezekből és előbbi 1-ből kapott maximális szükséges pozitív valós szorzóval teljesül a 10. tétel, kapunk hozzá C-t.

Itt az $l = o(\log k)$-s esetre kaptunk becslést a 11. tételből. Erdős, Stewart és Tijdeman $\log k$-s nagyságrendű l-ekre is adtak becslést a legnagyobb prímosztóra [1].

A felső becslés eltér az alsó becsléstől abból a szempontból, hogy a legnagyobb prímosztó felső becslése elegendő hozzá. A legnagyobb prímosztó alsó becslésénél viszont a különböző prímosztók számának alsó becslése használható.

Az összegként vagy mint a későbbi részben, szorzat+1 alakban előforduló m számokra az összesített legnagyobb prímosztót és m-ekre a prímosztók számát végignézve ezek maximumát is becsülték alulról az egy, illetve két halmazos esetekre is olyan eredményekben, amelyeknél ugyanakkor a halmazok legnagyobb elemétől is van függés (pl. N-nél nem nagyobb elemeket tartalmaznak a halmazok, legalább cN elemet), sűrűek a halmazok, ebben eltérnek az ezen dolgozatban ismertetett tételek döntő részétől. Ilyeneket említ [1], [8], [9] és [10] is.

4. $ab+1$ alakú számok prímosztói két halmaznál

4.1. Az alsó becslés

Sárközy indította el az $ab+1$-es eset tanulmányozását [9], amelyben az $a+b$-shez hasonlóan szintén két, pozitív egész számokat tartalmazó halmaz van, A és B, de az $ab+1$ alakú számok legalább egyikét osztó különböző prímosztók száma került becslésre, ahol $a \in A$ és $b \in B$. Itt az $ab+1$ alakú számok jellemzően nagyobbak, mint a másik esetben az $a+b$ alakúak, adott A és B mellett.

Az alsó becslésre a következő eredmény ismert:

12. Tétel (Győry-Sárközy-Stewart [9]). Létezik olyan C_3 hatékonyan kiszámolható pozitív konstans, amelyre ha A és B pozitív egész számokból álló halmazok, ahol $|A| \ge |B| \ge 2$, akkor több mint $C_3 \log |A|$ darab prímszám oszt legalább egyet az $ab+1$ $(a \in A, b \in B)$ alakú számok közül.

Az $a+b$-s esethez hasonlóan ezt is általánosabb algebrai jellegű lemma speciális eseteként bizonyították.

Lemma (Győry-Sárközy-Stewart [9]). Legyen $n \ge 2$ egész szám, A és B pedig legyenek $(\mathbb{Z}^+)^n$ véges részhalmazai, amelyekre $|A| \ge |B| \ge 2n-2$. A-ban mindegyik elem n. koordinátája 1 és $B \cup \{(0,0,\dots,0,1)\}$-ben bármely n vektor lineárisan független. Ekkor van olyan C_4 hatékonyan kiszámolható pozitív konstans, amelyre

$$\omega\left(\prod_{\substack{(a_1,a_2,\dots,a_n)\in A,\\ (b_1,b_2,\dots,b_n)\in B}} (a_1b_1+a_2b_2+\cdots+a_nb_n)\right) > C_4 \log|A|.$$

A lemma bizonyítása ([9] alapján):

Legyen $F(x) = F(x_1,x_2,\dots,x_n) \in \mathbb{Z}[x_1,x_2,\dots,x_n]$ lebontható forma, olyan polinom, amely $\mathbb{Q}$ egy véges fokú bővítésében

$$F(x) = l_1(x)l_2(x)\dots l_h(x)$$

alakban homogén elsőfokú tényezők szorzatára bomlik. Legyen $R \supseteq \mathbb{Z}$ egy véges bővítése, amely egyben $\mathbb{Q}$ részgyűrűje, így

$$R = \mathbb{Z}\left[\frac{1}{p_1p_2\dots p_s}\right]$$

különböző $p_1, p_2, \dots, p_s$ prímszámokra, itt $s \ge 0$ egész szám. Ekkor olyan $x \in R$-eket keresünk, amelyekre $F(x) \in R^*$, ahol R^* az R invertálható elemei által alkotott csoport a szorzásra, azon racionális számokat tartalmazza, amelyek egyszerűsített alakjában a számláló és a nevező is legfeljebb csak a $p_1, p_2, \dots, p_s$ prímszámok közül néhánnyal osztható egész szám.

Ha $x \in R$-re $F(x) \in R^*$, akkor bármely $r \in R^*$ esetén $F(rx) \in R^*$ szintén, így az ilyen megoldásokat egynek tekinthetjük, nem különböztetünk meg két megoldást, ha egymásból

R-beli számmal szorzással megkaphatóak. Az ilyen tekintetben egyező megoldások egy R-mellékosztályba tartoznak.

Ezután kimondunk egy lemmát, amely két [9]-ben kimondott lemma állításának egyesítése.

Lemma (Evertse és Győry eredményei [5], [6] alapján Győry-Stewart-Tijdeman [9])

F lineáris tényezői a rendre racionális együtthatós $l_1(x), l_2(x), \ldots, l_h(x)$. Az alábbi állítások ekvivalensek:

1. Egy az $l_1(x), l_2(x), \ldots, l_h(x)$ lineáris tényezők közül páronként lineárisan függetlenek által alkotott egy maximális részhalmaz L_0. Az L_0 vektorrendszer rangja n $\mathbb{Q}$ felett. Ekkor L_0 bármely valódi nemüres L_1 részhalmazára létezik olyan eleme L_0-nak, amely $V(L_1) \cap V(L_0 \setminus L_1)$-beli, ahol vektorok L halmazára $V(L)$ az L-beli vektorok által generált vektortér $\mathbb{Q}$ felett.
2. $\mathbb{Q}$ bármely R végesen generált részgyűrűjére $F(x) \in R$ megoldásai véges sok különböző R-mellékosztályba tartoznak, ekkor $(2^{33}h^2)^{n^3(s+1)}$-nél nincsenek többen.

Ezen lemma részeinek bizonyításai a [6] (a 2.-beli becslést leszámítva) és [5] (a mellékosztályok számának becslése) cikkekben találhatóak.

Az újabb lemma segítségével folytatjuk az előbbi bizonyítását. A feltételeknek megfelelő $A, B \subseteq (\mathbb{Z}^+)^n$-re ha csak $p_1, p_2, \ldots, p_s$ a prímszám osztói $\prod_{(a_1,a_2,\ldots,a_n)\in A,\ (b_1,b_2,\ldots,b_n)\in B}(a_1b_1 + a_2b_2 + \cdots + a_nb_n)$-nek, akkor $R = \mathbb{Z}\left[\frac{1}{p_1p_2\cdots p_s}\right]$-re nézzük az újabb lemmát.

Legyen

$$h = 2n - 1$$

és

$$l_i(x) = (x_1b_1 + x_2b_2 + \cdots + x_nb_n)$$

$i = 1, 2, \ldots, h-1$ esetén különféle $(b_1, b_2, \ldots, b_n) \in B$-kre, míg

$$l_h(x) = (0 \cdot x_1 + 0 \cdot x_2 + \cdots + 1 \cdot x_n) = x_n.$$

Emellett legyen $F(x) = l_1(x)l_2(x)\cdots l_h(x)$. Ezekből bármely n lineárisan független $\mathbb{Q}$ felett, és minden $(a_1, a_2, \ldots, a_n) \in A$-ra $F(a) \in R$.

Ekkor $L_0 = \{l_1, l_2, \ldots, l_h\}$, rangja n a B-re vonatkozó feltételből. Belátjuk az utóbbi lemma 1. állításának teljesülését. $|L_0| = 2n - 1$, így nemüres valódi L_1 részhalmazra $L_0 \setminus L_1$ és L_1

közül pontosan egy legalább n elemű, bármelyik n eleme lineárisan független Q felett, így rangja n. Ekkor a másik bármely eleme benne van tetszőlegesen az őt tartalmazó vektorrendszer által generált vektortérben, és az n-dimenziós, a nagyobb halmaz által generált vektortérben is, eleme $V(L_0 \setminus L_1) \cap V(L_1)$-nek. Ebből az 1. állítás teljesül, így a 2. is.

Mivel A összes elemében 1 az n. koordinátája, ezek különböző R-mellékosztályba tartoznak A különböző elemeire, hiszen másként A két elemére mindegyik koordinátájuk megegyezne. Ebből pontosan s prímszám osztóinál a 2. állítás szerint

$$|A| \le (2^{33}h^2)^{n^3(s+1)} = (2^{33}(2n-1)^2)^{n^3(s+1)}.$$

Ebből a lemma állítása következik. Ugyanis $s > 0$ és vele

$$(2^{33}(2n-1)^2)^{n^3(s+1)} \le (2^{33}(2n-1)^2)^{n^3(2s)},$$

így

$$\log|A| \le 2n^3 s \log(2^{33}(2n-1)^2)$$

és

$$\frac{\log|A|}{2n^3\log(2^{33}(2n-1)^2)} \le s = \omega\Bigg(\prod_{\substack{(a_1,a_2,\dots,a_n)\in A,\\ (b_1,b_2,\dots,b_n)\in B}} (a_1b_1 + a_2b_2 + \dots + a_nb_n)\Bigg).$$

A tétel bizonyítása:

Egyszerűen alkalmazzuk a lemmát az $n = 2$ esetben olyan $B \subseteq (Z^+)^2$-re, ahol mindegyik elem 2. koordinátája 1, a tételbeli B bármely b elemére $(b,1)$ lesz az ilyen B eleme és a tételbeli A bármely a elemére $(a,1)$-et vesszük a lemmabeli A-ba, kielégítve a lemma feltételeit. Ezek bijekciót adnak, így a tételbeli halmazokra sem lehet $\log|A|$ konstansszorosánál nem nagyobb $\omega\left(\prod_{a\in A, b\in B}(ab+1)\right)$. A szorzat prímosztói pedig pontosan azon prímszámok, amelyek legalább egy $ab+1$ alakú ($a \in A$, $b \in B$) számot osztanak. (Ezen esetben s prímosztónál

$$|A| \le (2^{33}\cdot 3^2)^{8(s+1)}$$

teljesül a lemma bizonyításából, a másik lemma alapján.)

A lemmát $n = 2$-re B bármely elemére a lemmabeli B-be $(b,1)$ helyett $(1,b)$-t téve az is megkapható, hogy $\log|A|$ konstansszorosánál nem nagyobb $\omega(\prod_{a\in A;b\in B}(a+b))$ bármely $|A|\geq|B|\geq 2$-t teljesítő pozitív egész számokból álló halmazokra, vagyis ebből is következik a Győry-Stewart-Tijdeman-tétel, az $a+b$-s eset alsó becslése.

4.2. A felső becslés

Győry, Sárközy és Stewart az $a+b$-s esethez több szempontból hasonlóan adtak felső becslést két, A és B pozitív egész számokat tartalmazó halmazra az $ab+1$ $(a\in A; b\in B)$ alakú számok különböző prímszám osztóinak számára, vagyis a legnagyobb prímszám osztóra adtak olyan felső korlátot, amelyénél bizonyos feltételek mellett kisebb, $|A|$ és $|B|$ függvényében. Abban az esetben, amikor $|B|$ meghatározott értelemben jóval kisebb, mint $|A|$, az alábbi becslést adták az $ab+1$ alakú számok legnagyobb prímosztójára.

13. Tétel (Győry-Sárközy-Stewart [9]). Legyenek k és l pozitív egész számok, amelyekre $k\geq 16$, $2\leq l\leq\left(\frac{\log\log k}{\log\log\log k}\right)^{1/2}$, továbbá ε pozitív valós szám. Ekkor ha k nagyobb egy ε-tól függő hatékonyan kiszámolható valós számnál, akkor vannak olyan A és B pozitív egész számokat tartalmazó halmazok, amelyekre $|A|=k$, $|B|=l$, és

$$P\Big(\prod_{a\in A;b\in B}(ab+1)\Big)<(\log k)^{l+1+\varepsilon}.$$

A tétel bizonyítása annyiban hasonlít a 11. tételére, hogy kombinatorikai jellegű lemmát használ, és $\Psi(x;y)$ ugyanazon becslését. Ugyanakkor ezen tétel bizonyításához további eredményekre is szükség van, döntően multiplikatív karakterekés nagy szita témaköréből.

A 13. tétel bizonyítása, 1. rész (lemmák):

Lemma (Győry-Sárközy-Stewart [9]). Legyenek $l\leq L\leq N$ pozitív egész számok, X és Y pedig pozitív egész számokat tartalmazó halmazok, amelyekre $|X|\geq 4lL$. Emellett bármely $x\in X$ esetén az $\{1;2;\dots;N\}$ halmazból legyen legalább N/L darab j szám, amelyekre $jx\in Y$. Ekkor vanak olyan A és B halmazok, amelyekre $A\subseteq\{1;2;\dots;N\}$, $B\subseteq X$, $|A|\geq\frac{N}{(4L)^l}$, $|B|=l$ és $A\cdot B\subseteq Y$.

A lemma bizonyítása:

Először belátjuk az alábbi segédállítást (a bizonyítást tartalmazó [9]-ben külön lemma):

Állítás (Győry-Sárközy-Stewart) Ha l, L, N és t pozitív egész számok, $t \ge 4lL$, és egy N elemű halmaznak kiválasztjuk t egyenként legalább N/L elemű részhalmazát, akkor ezek között van l, amelyek metszete legalább $\frac{N}{(4L)^l}$ elemű.

Az állítás bizonyítása:

Legyen az N elemű halmaz H.

A t kiválasztott részhalmaz halmazára az l elemű részhalmazainak metszetei közül a legnagyobb mérete legyen M, a méreteik összege pedig Z. Mivel $\binom{t}{l}$-féleképp választhatunk ki t-ből l darab részhalmazt és mindegyik metszet legfeljebb M elemű,

$$Z \le M\binom{t}{l} \le M\frac{t^l}{l!}.$$

Ugyanakkor Z-t megkaphatjuk úgy, hogy az N elemű H halmaz elemeire adjuk össze, hogy hányféleképp választhatunk ki l halmazt a t közül, amelyek metszetében az adott elem benne van (kettős leszámlálás). Ha elemenként rendre b_i halmazban szerepelnek H kiválasztott részhalmazai közül az i elemek,

$$\sum_{i\in H}\binom{b_i}{l} = Z.$$

Ugyancsak kettős leszámlálással H kiválasztott részhalmazaira a méreteik összege legalább $t\frac{N}{L}$, illetve elemenként nézve, hogy hány halmazban vannak benne, $\sum_{i\in H} b_i$. Eszerint

$$t\frac{N}{L} \le \sum_{i=1}^{N} b_i.$$

Tekintsük H azon i elemeit, amelyek legalább $\frac{t}{2L}$ kiválasztott részhalmazban szerepelnek, legyen a halmazuk J.

Ezekre $b_i \ge 2l$ miatt

$$\binom{b_i}{l} = \frac{b_i(b_i-1)\cdots(b_i-l+1)}{l!} \ge \frac{(b_i/2)^l}{l!} = \frac{b_i^l}{2^l l!}.$$

Ugyanakkor

$$\sum_{i\in J} b_i = \sum_{i\in H} b_i - \sum_{i\in H\setminus J} b_i \ge t\frac{N}{L} - N\frac{t}{2L} = \frac{Nt}{2L}.$$

Mivel J elemeire a kiválasztott halmazokban szereplések pozitív számaira

$$\frac{(\sum_{i\in J} b_i^l)}{|J|} \ge \frac{(\sum_{i\in J} b_i)^l}{|J|^l};$$

az l. hatványok átlaga legalább az átlag l. hatványa, így

$$\sum_{i\in J} b_i^l \ge \frac{(\sum_{i\in J} b_i)^l}{|J|^{l-1}}.$$

Az eddigiekből

$$M\frac{t^l}{l!} \ge Z = \sum_{i\in H}\binom{b_i}{l} \ge \sum_{i\in J}\binom{b_i}{l} \ge \sum_{i\in J}\frac{b_i^l}{2^l l!} \ge \frac{(\sum_{i\in J} b_i)^l}{2^l l! |J|^{l-1}} \ge \frac{\left(\frac{Nt}{2L}\right)^l}{2^l l! |J|^{l-1}} \ge \frac{\left(\frac{Nt}{2L}\right)^l}{2^l l! N^{l-1}}.$$

Összevetve a széleket

$$M\left(\frac{t^l}{l!}\right) \ge \frac{\left(\frac{Nt}{2L}\right)^l}{2^l l! N^{l-1}}$$

miatt

$$M \ge \frac{N}{(4L)^l};$$

vagyis H-nak van l kiválasztott részhalmaza, melyek metszete legalább $\frac{N}{(4L)^l}$ elemű. Az állítást beláttuk.

Az állítás alkalmazásával kapjuk a lemmát. Az állításban N elemű halmaza legyen az $\{1,2,\dots,N\}$ halmaz, ennek kiválasztott legalább N/L elemű részhalmazai minden $x \in X$-re azon $j \in \{1,2,\dots,N\}$-ek, amelyekre $jx \in Y$. t szerepében $|X|$ van. A kiválasztott részhalmazok közül van l, amelyekre a metszet legalább $\frac{N}{(4L)^l}$ elemű, az ezen részhalmazokhoz tartozó $x \in X$-ek (l darab) kerülnek B-be és a metszet A-ba, ekkor bármely $a \in A$ és $b \in B$ esetén $ab \in Y$ (a $jx \in Y$-os feltételből). Ezzel a lemmát bebizonyítottuk.

Definíció. Egy m pozitív egész számra multiplikatív karakternek (vagy gyakran csak m karakternek) nevezünk egy $\chi : \mathbb{Z} \to \mathbb{C}$ függvényt, ha $a \equiv b \pmod m$ esetén $\chi(a) = \chi(b)$, $\chi(xy) = \chi(x)\chi(y)$ minden $x,y \in \mathbb{Z}$ számpárra, m-hez nem relatív prím k egész számokra $\chi(k) = 0$, de ugyanakkor χ nem a konstans 0 függvény [8].

Egy m pozitív egész számra multiplikatív karakternek (vagy gyakran csak m karakternek) nevezünk egy $\chi : \mathbb{Z} \to \mathbb{C}$ függvényt, ha $a \equiv b \pmod m$ esetén $\chi(a) = \chi(b)$, $\chi(xy) =$

$\chi(x)\chi(y)$ minden $x, y \in \mathbb{Z}$ számpárra, m-hez nem relatív prím k egész számokra $\chi(k) = 0$, de ugyanakkor χ nem a konstans 0 függvény [8].

Igazából csak a mod q multiplikatív karakterekre lesz szükségünk, ahol q prímszám. Ilyenkor adott q-ra $\varphi(q) = q - 1$ különböző multiplikatív karakter létezik, amelyeket egy mod q primitív gyökben felvett, a multiplikativitás következményeként (benne $\chi(1) = 1$-en keresztül) $q-1$-adik egységgyök értékük meghatároz. Azon mod q multiplikatív karaktert, amelynek értéke a q-val osztható számokra 0, máshol 1, fokarakternek nevezzük.

A következő lemma, a nagy szita Gallagher-féle változata.

Lemma (Gallagher [8], [9]) Legyen M egész szám, N pozitív egész szám, $a_{M+1}, a_{M+2}, \ldots, a_{M+N}$ komplex számok. Ekkor bármely $Q \geq 1$ valós számra

$$\sum_{q \leq Q} \frac{q}{\varphi(q)} \sum^{*}_{\chi \pmod q} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \ll (Q^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2,$$

ahol az első összegzésben q a prímeken fut végig, $\sum^{*}_{\chi \pmod q}$ pedig a mod q multiplikatív karaktereken végzett összegzés a mod q fokarakter kihagyásával.

A lemmát itt nem bizonyítjuk, bizonyítása benne van a [8] jegyzetben.

Innentől [9] nyomán folytatjuk a bizonyítást. Az előzőnek következménye az alábbi lemma:

Lemma (Győry-Sárközy-Stewart) Legyen N pozitív egész szám és $J \subseteq \{1, 2, \ldots, N\}$. Tetszőleges p prímre jelölje $F(J;p)$ az $rr' \equiv 1 \pmod p$ kongruencia $r, r' \in J$-t kielégítő megoldásainak számát, és jelölje $G(J;p)$ a J halmaz p-vel osztható elemeinek számát. Ekkor bármely $Q \geq 1$ valós számra

$$\sum_{p \leq Q} p \left| F(J;p) - \frac{1}{p-1}(|J| - G(J;p))^2 \right| \ll (Q^2 + N)|J|.$$

A bal oldalon a Q-nál nem nagyobb p prímeken összegzünk.

A lemma bizonyítása:

$$F(J;p) = \frac{1}{p-1} \sum_{r, r' \in J} \sum_{\chi \pmod p} \chi(rr');$$

ugyanis ha a mod p multiplikatív karakterek összegét vesszük rr' maradékosztályán, az p, ha $rr' \equiv 1 \pmod p$, és 0 minden más esetben. $rr' \equiv 1 \pmod p$ és $rr' \equiv 0 \pmod p$ esetén 1 illetve 0 mind a $p - 1$ db karakterre $\chi(rr')$, más esetekben egy primitív gyökre mod p, és $p - 1$-gyel nem osztható k pozitív egész számokra

$$\sum_{\chi \,(\bmod p)} \chi(g^k) = \sum_{\chi \,(\bmod p)} (\chi(g))^k = \sum_{h=1}^{p-1} \exp\left(\frac{2\pi i h}{p-1}\right)^k = \frac{\exp\left(\frac{2\pi i k p}{p-1}\right) - \exp\left(\frac{2\pi i k}{p-1}\right)}{\exp\left(\frac{2\pi i k}{p-1}\right) - 1} = 0.$$

$$\frac{1}{p-1} \sum_{r,r' \in J} \sum_{\chi \,(\bmod p)} \chi(r\overline{r'}) = \frac{1}{p-1} \sum_{\chi \,(\bmod p)} \sum_{r,r' \in J} \chi(r\overline{r'}) = \frac{1}{p-1} \sum_{\chi \,(\bmod p)} \sum_{r,r' \in J} \chi(r)\overline{\chi}(r') =$$

$$\frac{1}{p-1} \sum_{\chi \,(\bmod p)} \Big(\sum_{r \in J} \chi(r) \Big)^2.$$

Utóbbi összeget kettészedve a χ_0 főkarakterre és a többire, mivel előbbi $|J| - G(J;p)$ helyen 1-et és $G(J;p)$ helyen 0-t vesz fel,

$$\frac{1}{p-1} \sum_{\chi \,(\bmod p)} \Big(\sum_{r \in J} \chi(r) \Big)^2 = \frac{1}{p-1}(|J| - G(J;p))^2 + \frac{1}{p-1} \sum_{\chi \neq \chi_0 \,(\bmod p)} \Big(\sum_{r \in J} \chi(r) \Big)^2.$$

Ezzel megkaptuk, hogy

$$F(J;p) = \frac{1}{p-1}(|J| - G(J;p))^2 + \frac{1}{p-1} \sum_{\chi \neq \chi_0 \,(\bmod p)} \Big(\sum_{r \in J} \chi(r) \Big)^2,$$

így

$$F(J;p) - \frac{1}{p-1}(|J| - G(J;p))^2 = \frac{1}{p-1} \sum_{\chi \neq \chi_0 \,(\bmod p)} \Big(\sum_{r \in J} \chi(r) \Big)^2.$$

Ebből

$$\left| F(J;p) - \frac{1}{p-1}(|J| - G(J;p))^2 \right| = \frac{1}{p-1} \left| \sum_{\chi \neq \chi_0 \,(\bmod p)} \Big(\sum_{r \in J} \chi(r) \Big)^2 \right|.$$

Összeadva az összes Q-nál nem nagyobb prímszámra ezek p-szereseit

$$\sum_{p \le Q} p \left| F(J;p) - \frac{1}{p-1}(|J| - G(J;p))^2 \right| = \sum_{p \le Q} \frac{p}{p-1} \left| \sum_{\chi \neq \chi_0 \,(\bmod p)} \Big(\sum_{r \in J} \chi(r) \Big)^2 \right|.$$

A jobb oldalra

$$\sum_{p \le Q} \frac{p}{p-1} \left| \sum_{\chi \neq \chi_0 \,(\bmod p)} \Big(\sum_{r \in J} \chi(r) \Big)^2 \right| \le \sum_{p \le Q} \frac{p}{p-1} \sum_{\chi \neq \chi_0 \,(\bmod p)} \left| \sum_{r \in J} \chi(r) \right|^2.$$

Az $a_1, a_2, \ldots, a_N$ számokat a J-beli indexűekre 1-nek, a többire 0-nak választva használjuk az előbbi lemmát, eszerint

$$\sum_{p \le Q} \frac{p}{p-1} \sum_{\chi \neq \chi_0 \,(\bmod p)} \left| \sum_{r \in J} \chi(r) \right|^2 \le (Q^2 + \pi N)|J|.$$

A kapott egyenlőtlenség-láncból

$$\sum_{p \le Q} p|F(J;p)| \ge \frac{1}{p-1}(|J| - G(J;p))^2| \le (Q^2 + N)|J|.$$

Ezzel a lemma állítását bebizonyítottuk.

A 13. tétel bizonyítása, 2. rész:

Elég $0 < \varepsilon < 1$ valós számokat nézni és egy 0 végpontú ott nyílt nemüres intervallumon bizonyítani, nagyobb ε-ra is jó korlát az, ami ittenire. Ezért innentől egy $0 < \varepsilon < 1$ valós számot lerögzítve látjuk be a tételt, a végső ε ennek duplája lesz. Legyen $N > 30$ pozitív egész szám, ekkor $N > e^e$ miatt

$$\log\log\log N > 0.$$

Legyen $2 \le l \le \left(\frac{\log\log N}{\log\log\log N}\right)^{1/2}$ egész szám. Bevezetjük az alábbi számokat:

$$R \stackrel{\text{def}}{=} [N^{\frac{l+1}{2l}}];$$

$$Q \stackrel{\text{def}}{=} 2N^{1/l}$$

és

$$y \stackrel{\text{def}}{=} (\log R)^{l+1+\varepsilon}.$$

Jelölje J az R-nél nem nagyobb, y-nál nagyobb prímszámmal nem osztható pozitív egész számok halmazát. Ekkor

$$|J| = \Psi(R;y).$$

$y = R^{\frac{\log y}{\log R}}$, itt

$$\frac{\log R}{\log y} = \frac{\log R}{(l+1+\varepsilon)\log\log R}.$$

Elég nagy N-ekre, itt és általában később is az elég nagyhoz elérendő hatékonyan kiszámolható korlát ε-tól függ, mivel pl.

$$R \ge [N^{1/2}] \ge N^{1/3} \text{ és } l \le \log\log N$$

a számláló $\log N$-es, a nevező legfelejebb $(\log\log N)^2$-es nagyságrendű, ez legalább 3, így alkalmazható a korábban kimondott becslés $\Psi(x; x^{1/u})$-ról.

Ilyenkor

$$\Psi(R;y) \geq R\exp\left(-\frac{\log R}{\log y}\left(\log\frac{\log R}{\log y} + \log\log\frac{\log R}{\log y} - 1 + c\,\frac{\log\log\frac{\log R}{\log y}}{\log\frac{\log R}{\log y}}\right)\right)$$

egy c valós konstansra. A kitevő

$$-\frac{\log R}{\log y}\left(\log\frac{\log R}{\log y} + \log\log\frac{\log R}{\log y} - 1 + c\,\frac{\log\log\frac{\log R}{\log y}}{\log\frac{\log R}{\log y}}\right)$$

$$= -\frac{\log R}{\log y}\Big((\log\log R - \log\log y) + \log(\log\log R - \log\log y) - 1 + o(1)\Big)$$
$$= -\frac{\log R}{(l+1+\varepsilon)\log\log R}\Big((\log\log R - \log((l+1+\varepsilon)\log\log R))$$
$$+ \log\big(\log\log R - \log((l+1+\varepsilon)\log\log R)\big) - 1 + o(1)\Big) > -\frac{\log R}{l+1+\varepsilon}$$

elég nagy N-ekre (és velük elég nagy R-ekre), itt $o(1)$ azt jelöli, hogy $N \to \infty$ esetén

$$c\,\frac{\log\log\frac{\log R}{\log y}}{\log\frac{\log R}{\log y}} \to 0.$$

Ezzel beláttuk, hogy elég nagy N pozitív egész számokra

$$|J| \geq R\exp\left(-\frac{\log R}{l+1+\varepsilon}\right) = R^{1-\frac{1}{l+1+\varepsilon}} = R^{\frac{l}{l+1}+\frac{\varepsilon}{(l+1)(l+1+\varepsilon)}}.$$

Így ekkor

$$|J| \geq \left[N^{\frac{l+1}{2l}}\right]^{\frac{l}{l+1}}\left[N^{\frac{l+1}{2l}}\right]^{\frac{\varepsilon}{(l+1)(l+1+\varepsilon)}}.$$

ε-tól függő hatékonyan kiszámolható számnál nagyobb N számokra

$$\left[N^{\frac{l+1}{2l}}\right]^{\frac{l}{l+1}}\left[N^{\frac{l+1}{2l}}\right]^{\frac{\varepsilon}{(l+1)(l+1+\varepsilon)}} \geq N^{\frac{1}{2}}N^{\frac{\varepsilon}{3l(l+1)}}.$$

(Ennek indoklása: az egészrészek nélkül bal oldal

$$N^{\frac{l+1}{2l}} \quad \frac{l}{l+1} N^{\frac{l+1}{2l} \quad \frac{\varepsilon}{(l+1)(l+1+\varepsilon)}} = N^{\frac{1}{2}} N^{\frac{\varepsilon}{3l(l+1)}} \quad N^{\frac{\varepsilon(l+1 \quad 2\varepsilon)}{6l(l+1)(l+1+\varepsilon)}}$$

lenne.

Így ha

$$\left\lfloor N^{\frac{l+1}{2l}} \right\rfloor \quad N^{\frac{l+1}{2l}} N^{\frac{\varepsilon(l+1 \quad 2\varepsilon)}{6l(l+1)(l+1+\varepsilon)}}$$

teljesülne, meglennénk. Ehhez elég

$$N^{\frac{l+1}{2l}} \quad 1 \quad N^{\frac{l+1}{2l}} N^{\frac{\varepsilon(l+1 \quad 2\varepsilon)}{6l(l+1)(l+1+\varepsilon)}};$$

vagyis

$$\left(N^{\frac{l+1}{2l}} \quad 1\right)\left(N^{\frac{\varepsilon(l+1 \quad 2\varepsilon)}{6l(l+1)(l+1+\varepsilon)}} \quad 1\right) \quad 1.$$

Ugyanakkor elég nagy N-re

$$N^{\frac{\varepsilon(l+1 \quad 2\varepsilon)}{6l(l+1)(l+1+\varepsilon)}} \quad 2;$$

mert logaritmusa $\frac{\varepsilon \log N}{l^2}$-es nagyságrendű.)

Ezzel megkaptuk, hogy elég nagy N-re

$$|J| \quad N^{\frac{1}{2}+\frac{\varepsilon}{3l(l+1)}}.$$

Legyen

$$F \overset{\text{def}}{=} \{rr' \quad 1 : r, r' \in J\}$$

és bármely p prímszámra legyen $F(J;p)$ az $rr' \quad 1$ (mod p) feltételt teljesítő $r, r' \in J$ párok száma, $G(J;p)$ pedig a J halmaz p-vel osztható elemeinek száma.

Álljon E azon p prímszámokból , amelyekre $Q/2 < p \quad Q$ teljesül, és $F(J;p) > \frac{|J|^2}{2Q}$. Belátjuk, hogy E mérete kellően nagy.

Tudjuk, hogy $Q/2 = N^{1/l}$ és

$$y = (\log R)^{l+1+\varepsilon} = \left(\log N^{\frac{l+1}{2l}}\right)^{l+1+\varepsilon} < (\log N)^{l+1+\varepsilon}.$$

Itt adott N-re $N^{1/l}$ nagyobb l-re kisebb, míg $(\log N)^{l+1+\varepsilon}$ nagyobb l-re nagyobb, így $Q/2 \leq y$ esetén

$$\log\log N > l$$

miatt

$$N^{1/\log\log N} < (\log N)^{\log\log N+2}$$

is teljesülne, ami elég nagy N-ekre nem áll fenn, olyankor $Q/2 > y$. Így ekkor J-ben nem lehet $Q/2$-nél nagyobb p prímmel osztható szám,

$$G(J;p) = 0.$$

Ebből

$$\frac{1}{p-1}(|J| - G(J;p))^2 = \frac{|J|^2}{p-1}$$

minden $p \in (Q/2;Q]$ prímszámra, ha N elég nagy.

Legyen $\overline{E}$, azon p prímek halmaza, amelyre $Q/2 < p \leq Q$, de nincsenek benne E-ben, vagyis $F(J;p) \leq \frac{|J|^2}{2Q}$. Ekkor

$$\frac{1}{p-1}(|J| - G(J;p))^2 = \frac{|J|^2}{p-1} > \frac{|J|^2}{Q}$$

minden $p \in \overline{E}$ esetén, $\overline{E}$ definíciójából

$$\left|F(J;p) - \frac{1}{p-1}(|J| - G(J;p))^2\right| > \frac{|J|^2}{2Q}$$

is teljesül. A bal oldal p-szereseit összeadva minden $p \in \overline{E}$-re a korábbi lemmából

$$\sum_{p\in\overline{E}} p\left|F(J;p) - \frac{1}{p-1}(|J| - G(J;p))^2\right| \leq \sum_{p\leq Q} p\left|F(J;p) - \frac{1}{p-1}(|J| - G(J;p))^2\right| \leq (Q^2 + R)|J|.$$

Ebből

$$(Q^2 + R)|J| \geq \sum_{p\in\overline{E}} p\left|F(J;p) - \frac{1}{p-1}(|J| - G(J;p))^2\right| \geq \sum_{p\in\overline{E}} p\frac{|J|^2}{2Q} \geq \sum_{p\in\overline{E}} \frac{Q}{2}\frac{|J|^2}{2Q} = |\overline{E}|\frac{|J|^2}{4}.$$

Az elejét és a végét összevetve

$$Q^2 + R \geq |\overline{E}|\frac{|J|}{4}.$$

Ebből

$$|\overline{E}| \leq \max\left(\frac{8Q^2}{|J|}; \frac{8R}{|J|}\right) \leq 32\max\left(\frac{N^{2/l}}{|J|}; \frac{\left[N^{\frac{l+1}{2l}}\right]}{|J|}\right).$$

$l = 2$ esetén

$$|\overline{E}| \leq 32\frac{N}{|J|} \leq 32N^{\frac{1}{2} - \frac{\varepsilon}{18}};$$

így

$$|\overline{E}| \leq N^{\frac{1}{2} - \frac{\varepsilon}{20}}$$

elég nagy N-re.

$l > 2$ esetén pedig

$$|\overline{E}| \leq 32\frac{\left[N^{\frac{l+1}{2l}}\right]}{|J|} \leq 32N^{\frac{l+1}{2l} - \frac{1}{2} - \frac{\varepsilon}{3l(l+1)}},$$

ezért elég nagy N-re

$$|\overline{E}| \leq N^{\frac{1}{2l}}.$$

Elég nagy N-re Q is elég nagy ahhoz, hogy olyan p prímszámból, amelyre $Q/2 < p \leq Q$, legyen legalább $\dfrac{Q}{3\log Q}$ (például a prímszámtételből). Ugyanakkor eléggé nagy N-ekre teljesül az is, hogy

$$|\overline{E}| \leq \frac{Q}{6\log Q},$$

ugyanis

$$\frac{Q}{6\log Q} = \frac{2N^{1/l}}{6\log(2N^{1/l})},$$

ami $l = 2$-re $\dfrac{2N^{1/2}}{3\log N + 6\log 2}$, ami adott ε mellett elég nagy N-re nagyobb $N^{\frac{1}{2} - \frac{\varepsilon}{20}}$-nál, $|\overline{E}|$ felső becslésénél.

$l > 2$-re pedig elég nagy N-re és vele elég nagy $N^{1/l}$-ekre

$$\frac{2N^{1/l}}{6\log(2N^{1/l})} > N^{\frac{1}{2l}} \geq |E|.$$

Eszerint elég nagy N-ekre

$$|E| > \frac{Q}{6\log Q}.$$

Tehát ilyenkor $\frac{Q}{6\log Q}$-nál több olyan p prímszám létezik, amelyre

$$Q/2 < p \leq Q \text{ és } F(J;p) > \frac{|J|^2}{2Q}.$$

Jelölje $d(n)$ az n pozitív egész szám osztóinak számát. Ekkor ismert, hogy

$$\max_{n \leq R} d(n) < e^{\frac{\log R}{\log\log R}}$$

és vele

$$\max_{n \leq R} d(n) < e^{\frac{\log N}{\log\log N}}$$

elég nagy N-ekre és velük elég nagy R-ekre. Ilyen tételt előbb Wigert bizonyított, majd Ramanujan újabb bizonyítást adott rá, igazából $e^{\frac{\log N}{\log\log N}}$-ben az alap e helyett bármely 2-nél nagyobb valós szám lehet [2]. Legyen

$$D \stackrel{\text{def}}{=} \max_{n \leq R} d(n).$$

Az rr' $(r, r' \in J)$ alakú szorzatok közt bármely szám legfeljebb D^2-szer szerepelhet. Ugyanis ha rr' alakban felírjuk, az összes osztója "r egy osztója szorozva r egy osztójával" alakban előáll, $d(r)d(r') \leq D^2$-nél nincs több osztója, így legfeljebb D^2-féleképp állhat elő két pozitív egész szám szorzataként (a sorrend számít, J elemei R-nél nem nagyobbak).

Ezzel megkaptuk, hogy E bármely elemére az

$$rr' \equiv 1 \pmod p),\ r, r' \in R$$

$F(J;p)$ darab megoldása több mint $\frac{|J|^2}{2D^2Q}$ különböző értékű rr' szorzathoz tartozik. Így bármely $p \in E$-re létezik $\frac{|J|^2}{2D^2Q}$-nál több olyan j pozitív egész szám, amelyre $jp+1$ előáll két (nem feltétlenül különböző) R-beli elem szorzataként. Itt a jp-k az előbbi r, r' párokra az $rr' - 1$

alakú számok.

A most következő számolások célja, hogy az első lemma alkalmazhatóságát igazolják elég nagy N-ekre.

Legyen

$$L \stackrel{\text{def}}{=} \frac{1}{4} N^{\frac{1}{l} \quad \frac{''}{4l(l+1)}} :$$

Ekkor elég nagy N-ekre

$$\frac{jJj^2}{2D^2Q} \quad \frac{N}{L} :$$

Ugyanis elég nagy N-ekre

$$\frac{jJj^2}{2D^2Q} \quad \frac{N^{1+\frac{2''}{3l(l+1)}}}{4e^{\frac{2\log N}{\log\log N}} N^{\frac{1}{l}}} = \frac{1}{4} N^{1+\frac{2''}{3l(l+1)} \quad \frac{1}{l} \quad \frac{2}{\log\log N}} ;$$

míg

$$\frac{N}{L} = 4N^{1 \quad \frac{1}{l} + \frac{''}{4l(l+1)}} ;$$

így elegendő, ha

$$N^{\frac{5''}{12l(l+1)} \quad \frac{2}{\log\log N}} \quad 16;$$

ami

$$\frac{5''}{12l(l+1)} > \frac{5'' \log\log\log N}{24 \log\log N}$$

miatt elég nagy $''$-tól függő N-re teljesül.

Ezután alkalmazzuk az elsőként kimondott lemmát. Az E-beli prímek bármelyikére van legalább $N=L$ olyan f pozitív egész szám, ahol azzal megszorozva F-beli ($rr^0 \quad 1$ alakú, ahol $r; r^0\ 2\ R$) pozitív egész számot kapunk. Mindre

$$pf < R^2 \qquad N^{\frac{l+1}{2l}^{\#_2} ''} \qquad N^{1+\frac{1}{l}}$$

és

$$p > N^{\frac{1}{l}} ;$$

így
$$f < N$$
minden f-re. Emellett
$$|E| \ge 4lL$$
elég nagy N-ekre, ugyanis $|E| \ge \frac{Q}{6\log Q}$ teljesüléséből
$$|E| \ge \frac{2N^{\frac{1}{l}}}{6\log\left(2N^{\frac{1}{l}}\right)} = \frac{N^{\frac{1}{l}}}{3\left(\log 2 + \log N\,\frac{1}{l}\right)}$$
és
$$4lL = lN^{\frac{1}{l}-\frac{\varepsilon}{4l(l+1)}};$$
ilyenkor $|E| \ge 4lL$-hez elegendő, ha
$$\frac{N^{\frac{\varepsilon}{4l(l+1)}}}{3} \ge l\log 2 + \log N;$$
ami $l < \log\log N$ miatt elég nagy N-ekre teljesül.

Ezek alapján, $X = E$ és $Y = F$ szereposztással használva a lemmát, léteznek
$$A_1 \subseteq \{1;2;\ldots;N\} \text{ és } B \subseteq E$$
halmazok, amelyekre
$$|A_1| \ge \frac{N}{(4L)^l},\ |B| = l \text{ és } A\,B \subseteq F.$$
A-ba az f-fel jelölt számoknak megfelelőek kerülnek, $|B|$-be pedig $N^{\frac{1}{l}}$-nél nagyobb, de $2N^{\frac{1}{l}}$-nél nem nagyobb prímek.

Eddig bizonyos tulajdonságokat kielégítő N, L és ε esetén láttunk be eredményt, most bevezetjük a k-t, és N-et és ε-t olyanná tesszük, hogy az eddigi feltételek is teljesüljenek.
Legyen $k > 15$ pozitív egész szám, amelyre így $k > e^e$.
Legyen
$$2 \le l \le \left(\frac{\log\log k}{\log\log\log k}\right)^{1/2}$$
pozitív egész szám.

Legyen N olyan pozitív egész szám, amelyre $k = \left\lfloor N^{\frac{\varepsilon}{4(l+1)}} \right\rfloor$, a kitevő 1-nél kisebb, így a pozitív egészek ennyiedik hatványai közt 1-nél nem nagyobb különbségek vannak, létezik ilyen N, amire

$$N > 30 \text{ és } k \le N.$$

Így megvan az előbbi rész A_1 és B (pozitív egész számokból álló) halmaza, ahol az $A_1 \cup B$ elemeinél 1-gyel nagyobb számok nem oszthatóak $(\log R)^{l+1+\varepsilon}$-nál nagyobb prímszámmal, $|B| = l$. Ekkor A_1-ből kiválasztható egy k elemű A részhalmaz. Ugyanis elég nagy k-ra

$$|A_1| \ge \frac{N}{(4L)^l} = \frac{N}{\left(N^{\frac{1}{l} - \frac{\varepsilon}{4l(l+1)}}\right)^l} = N^{\frac{\varepsilon}{4(l+1)}} \ge \left\lfloor N^{\frac{\varepsilon}{4(l+1)}} \right\rfloor = k.$$

Elég nagy k-ra

$$\left\lfloor N^{\frac{\varepsilon}{4(l+1)}} \right\rfloor = k > N^{\frac{\varepsilon}{5(l+1)}};$$

így

$$\frac{\varepsilon}{5(l+1)} \log N < \log k.$$

Emellett

$$\frac{l+1}{2l} \log N \ge \log R;$$

ebből

$$\log R \le \frac{l+1}{2l} \log N \le \log k \cdot \frac{5(l+1)^2}{2l\varepsilon}.$$

Így

$$y = (\log R)^{l+1+\varepsilon} \le \left(\log k \cdot \frac{5(l+1)^2}{2l\varepsilon}\right)^{l+1+\varepsilon}.$$

Elég nagy ε-tól függő k-kra

$$\left(\log k \cdot \frac{5(l+1)^2}{2l\varepsilon}\right)^{l+1+\varepsilon} \le (\log k)^{l+1+2\varepsilon}.$$

Ehhez elégséges, ha

$$\frac{5(l+1)^2}{2\varepsilon l} \le (\log k)^{\frac{\varepsilon}{l+1+\varepsilon}};$$

amihez
$$\left(\frac{5(l+1)^2}{2\varepsilon l}\right)^{l+1+\varepsilon} \le (\log k)^{\varepsilon}.$$
Itt a bal oldal $l \ge 2$-re monoton nő, de ha k eléggé nagy, még $l = \log\log k$-ra is kisebb.

Eszerint vannak megfelelő méretű A és B halmazaink elég nagy $0 < \varepsilon < 1$-től függő k-ra, k-tól függő N-re, és elég nagy l-re, ahol az $ab+1$ $(a \in A, b \in B)$ alakú számok szorzatának összes prímosztója legfeljebb $(\log k)^{l+1+2\varepsilon}$. Így a tétel állítása az ottani ε helyett 2ε-nal teljesül és természetesen ahhoz, hogy ε jöjjön ki a végén, $\frac{\varepsilon}{2}$-től függően választhattuk a változókat
$$0 < \varepsilon < 2\text{-re.}$$
Emellett a bizonyítás során az elég nagy számokhoz végig vannak hatékonyan kiszámolható korlátok, így az eredeti ε mellett is k-hoz. Ez elegendő a tétel igazságához. A tételt bebizonyítottuk.

Ezen tétel $l = 2$-re és ε-tól függően elég nagy k-ra $(\log k)^{3+\varepsilon}$-nál nem nagyobb prímosztókat és így a prímszámtétellel összesen legfeljebb kb. $\frac{(\log k)^{3+\varepsilon}}{(3+\varepsilon)\log\log k}$ különböző prímosztót jelent az $ab+1$ $(a \in A, b \in B)$ alakú számoknak.

Az előző tétel a $2 \le l \le \left(\frac{\log\log k}{\log\log\log k}\right)^{1/2}$ esetre adott becslést elég nagy k-k esetén. Győry, Sárközy és Stewart ugyanazon cikkükben gyengébb felső becslést adtak ennél szélesebb intervallumon a legnagyobb prímosztóra:

14. Tétel (Győry-Sárközy-Stewart [9])**.** *Léteznek olyan c_1 és c_2 hatékonyan kiszámolható pozitív konstansok, amelyekre c_1-nél nagyobb $k \ge 3$ és $2 \le l \le c_2\frac{\log k}{\log\log k}$ esetén vannak olyan $A, B \subseteq \{1, 2, \dots, k^3\}$ halmazok, amelyekre $|A| = k$, $|B| = l$ és*
$$P\Big(\prod_{a\in A, b\in B} (ab+1)\Big) < (\log k)^{5l}.$$

A tétel bizonyítása hasonlít az előzőéhez, megtalálható a [9] cikkben.

5. $aa'+1$ alakú számok prímosztói egy halmaznál - kis esetek

Ebben a részben egy halmazunk van pozitív egész számokból, de nem a kéttagú összegek, hanem a kéttényezős szorzatoknál (ahol a tényezők különböznek) 1-gyel nagyobb számok prímosztóit vizsgáljuk.

Az alsó becslést adó Győry-Sárközy-Stewart-tétel következménye egy halmazra az alábbi, itt is a halmazt két hasonló méretű diszjunkt részhalmazára kettébontva adódik a két halmazoséhoz hasonló állítás a két halmazos esetből:

Következmény (Győry-Sárközy-Stewart [9])**.** *Létezik olyan C hatékonyan kiszámolható pozitív konstans, amelyre bármely $n \geq 2$ elemű A pozitív egész számokból álló halmazra több mint $C \log n$ prímszám van, amely oszt legalább egy $aa' + 1$ alakú számot, ahol $a, a' \in A$ és $a \neq a'$.*

Az egy halmazos, kéttagú összegeket vizsgáló esethez és két halmazos párjához hasonlóan itt is a két halmazos esetnél a minimális számú prímosztókról szóló felső becslések megléte nem ad az egy halmazos esetre felső becslést. Ugyanakkor az A halmaz elemeit a legkisebb számoknak választva $|A| = n$ elemnél csupa $n^2 + 1$-nél nem nagyobb szám fordul elő az $aa' + 1$ $(a, a' \in A)$ alakú számok közt. Ezeknek $n^2 + 1$-nél nem nagyobbak a prímosztói, így $\frac{n^2}{2 \log n}$ konstansszorosánál nem lehet több a prímosztók száma. Ugyanakkor ha az $aa' + 1$ alakú számok közt sok egybeesést szeretnénk, $|A|$ elemei lehetnek egy mértani sorozat egymás utáni elemei. Viszont ekkor a szorzatok nagyobbak, így a prímosztók számát csak az $aa' + 1$ alakú számok logaritmusaival becsülve négyzetes, gyengébb becslést kapnánk.

Ezután konkrét n-ekre vizsgáljuk, hogy n különböző pozitív egész számot tartalmazó A halmazra az $aa' + 1$ alakú számoknak $(a, a' \in A, a \neq a')$ összesen n-től függően minimum hány különböző prímszám osztója van. Másképp fogalmazva a kérdés, hogy az $aa' + 1$ alakú számok $\binom{n}{2}$ -tényezős szorzatát legalább hány különböző prímszám osztja. Ebben az esetben már nem lehet feltenni, hogy optimális esetben a legnagyobb közös osztó 1. Emellett nincs olyan prímszám, amely elég nagy n-re legalább egy $aa' + 1$ alakú számot oszt, hiszen például lehetséges, hogy A összes eleme osztható az adott prímszámmal. $n \geq 2$-re értelmes a kérdés, $n = 2$-re 1 a válasz, ha a két szám egyike az 1, a másik 2, egyenlőség van, kevesebb nem lehet. Az $n = 3$ az első érdekes eset.

15. Tétel. *Ha van 3 pozitív egész számunk, $a < b < c$, akkor $\omega((ab + 1)(ac + 1)(bc + 1)) \geq 2$. $\omega((ab + 1)(ac + 1)(bc + 1)) = 2$-re van példa.*

A tétel komolyabb, előbbi irányát Szalay és Ziegler bizonyította ([13]-ban "Corollary 2."), a most következőtől eltérő módon.

A tétel bizonyítása:

Az egyenlőség lehetséges például az $(a; b; c) = (1; 2; 4)$ esetben, amikor csak a 3 és az 5 prímszámok osztanak a 3, 5 és 9 számok közül legalább egyet.
Tegyük fel, hogy létezik olyan $(a; b; c)$ számhármas, amikor legfeljebb egy prímszám oszt az $ab + 1$, $ac + 1$ és $bc + 1$ számok közül legalább egyet, $ab + 1 > 1$ miatt mind a három számnak egy adott p prímszám pozitív egész kitevős hatványának kell lennie. Legyen

$$ab + 1 = p^k.$$

$p \mid ac + 1$, így c nem osztható p-vel.

$$ab + 1 < ac + 1 \text{ és } ab + 1 < bc + 1$$

miatt

$$ab + 1 \mid ac + 1 \text{ és } ab + 1 \mid bc + 1,$$

így

$$ab + 1 \mid bc + 1 - (ac + 1)$$

és

$$ab + 1 \mid c(b - a).$$

c és $ab + 1$ relatív prímek, mert előbbi nem osztható p-vel, utóbbi p-hatvány, így

$$ab + 1 \mid b - a.$$

Ugyanakkor

$$0 < b - a < b \leq ab < ab + 1,$$

így az $ab + 1$ pozitív egész szám nem oszthatja a nála kisebb $b - a$ pozitív egész számot, ellentmondás. Így a tétel állításának első része is teljesül, mert a tagadása ellentmondásra vezetett.

Ezután a $4 \leq n \leq 8$ esetre mutatunk a halmaz legnagyobb elemét lekorlátozva Python programmal talált halmazokat, amelyekre ilyen korlátozás mellett összességében a lehető legkevesebb prímszám oszt az $aa' + 1$ alakú számok közül legalább egyet.

Python nyelvű programmal megvizsgáltam az $n = 4$ esetben 500-nál nem nagyobb pozitív egész számokat tartalmazó négyelemű A halmazokat. Legalább egy $aa' + 1$ alakú számot ($a \neq a'$ és $a, a' \in A$) legalább 3 darab prímszám oszt, pontosan 3 a következő 3 esetben:

számnégyes	prímosztók
1, 3, 5, 7	2, 3, 11
1, 3, 7, 21	2, 11, 37
1, 5, 7, 23	2, 3, 29

Emellett programmal megvizsgáltam a 750-nél nem nagyobb pozitív egész számokat tartalmazó négyelemű A halmazokat is. Nincs olyan, amelyre legalább egy $aa' + 1$ alakú számot legfeljebb 2 darab prímszám osztana.

Ebben az esetben Szalay és Ziegler cikke alapján [13] szintén számítógépes vizsgálatra hivatkozva 1000-nél nem nagyobb pozitív egész számokat tartalmazó négyelemű A halmazokra is csak 3 esetben van legfeljebb 3 prímszám, amely $aa' + 1$ alakú számot oszt. Ugyancsak ebben a cikkben szerepel az alábbi sejtés:

2. Sejtés (Szalay-Ziegler [13]). *Bármely 4 különböző pozitív egész számra legalább 3 prímszám oszt a kéttényezős szorzatoknál eggyel nagyobb számok közül legalább egyet.*

Erre a kérdésre később is visszatértek, vizsgálva egy esetleges ellenpéldára teljesülő követelményeket. Algoritmust adtak arra, hogy két prímszámnál hogyan lehet(ne) megtalálni az összes számnégyest, ahol a pozitív egész számok páronkénti szorzatainál 1-gyel nagyobb számok prímosztói csak a két lerögzített prímszám [14]. Bebizonyították az alábbiakat kicsit más megfogalmazásban:

16. Tétel (Szalay-Ziegler [15]). *Ha adott két prímszám, amelyeken kívül másik nem fordul elő 4 pozitív egész szám A halmazára az $aa' + 1$ alakú számok prímosztói közt, akkor nem lehet mindkettő $4k + 3$ alakú.*

17. Tétel (Szalay-Ziegler [14])). *Ha adott két prímszám, amelyeken kívül másik nem fordul elő 4 pozitív egész szám A halmazára az $aa' + 1$ alakú számok prímosztói közt, akkor nem fordulhat elő, hogy a két prím egyike a 2, a másik $4k + 3$ alakú.*

A 16. tétel bizonyítása teljesen elemi és a $4k + 3$ alak jelentősége, hogy $4k + 3$ alakú p prímszámra a 1 kvadratikus nemmmaradék, így nem lehetséges, hogy három pozitív egész szám közül bármely kettő szorzata kongruens 1 mod p. A 15. tétel előbbi irányának általuk belátott erősítését alkalmazták, $a < b < c$ pozitív egész számokra $bc + 1$ nem lehet $ac + 1$ többszöröse. A bizonyítás emellett jelentős esetszétválasztást tartalmaz.

Ezenkívül Sage program segítségével belátták, hogy:

18. Tétel (Szalay-Ziegler [14]). *Ha adott két prímszám, amelyeken kívül másik nem fordul elő 4 pozitív egész szám A halmazára az* $aa' + 1$ *alakú számok prímosztói közt, akkor ha az egyik 2, a másik nem lehet* 10^9*-nél kisebb. Az sem lehetséges, hogy mindkét prímszám kisebb legyen* 10^5*-nél.*

Ziegler algoritmust adott arra az esetre is, amikor 3 adott prímszámra keressük az összes pozitív egész számokból álló négyest, ahol a kéttényezős szorzatoknál 1-gyel nagyobb számoknak nincs a 3 prímtől eltérő prímosztója. Sage programmal megvizsgálva abban az esetben, amikor mindhárom prímszám legfeljebb 100, a már említett 3 eseten kívül nem talált mást (4 nap futásidővel), így nincs több [17].

Programmal megvizsgálva az $n = 5$ esetet kiderült, hogy 300-nál nem nagyobb pozitív egész számokból álló ötelemű A halmazokra minimum egy $aa' + 1$ alakú számot legalább 5 darab prímszám oszt, pontosan ennyi 32 esetben, egy ilyen az $(1; 2; 3; 5; 7)$, ahol az $aa' + 1$ alakú számok prímszám osztói között az öt legkisebb prímszám szerepel (2, 3, 5, 7 és 11). Ezt már Szalay és Ziegler is említik [13], szintén 300-nál nem nagyobb pozitív egész számokból álló számötösből számítógépes programmal ugyanennyit találtak az $aa' + 1$ alakú számok prímszám osztói között legfeljebb 5 prímszámmal, mindnél pontosan öttel.

Számítógéppel elért saját eredményem, hogy 400-nál nem nagyobb pozitív egész számokból álló ötelemű A halmazokra nem lehet legfeljebb 4 az $aa' + 1$ alakú számok prímosztóinak száma.

Python nyelvű programmal megvizsgálva az $n = 6$ esetben beláttam, hogy a 250-nél nem nagyobb pozitív egész számokból álló hatelemű A halmazokra minimum egy $aa' + 1$ alakú számot legalább 6 darab prímszám oszt, pontosan ennyi az alábbi 3 esetben:

számhatos	prímosztók
1, 2, 3, 5, 7, 13	2, 3, 5, 7, 11, 23
1, 2, 5, 7, 13, 137	2, 3, 5, 7, 11, 23
1, 3, 7, 9, 17, 23	2, 3, 5, 7, 11, 13

Az $n = 7$ esetben a programom szerint 250-nél nem nagyobb pozitív egész számokból álló hételemű A halmazra legalább egy $aa' + 1$ alakú számot minimum 7 prímszám oszt, egyenlőség csak az $(1; 2; 3; 5; 7; 13; 137)$ számhetesre van. Itt a 7 prímosztó a 2, 3, 5, 7, 11, 23 és 103.

Végül $n = 8$ esetén programmal meghatároztam, hogy 120-nál nem nagyobb pozitív egész számokat tartalmazó nyolcelemű A halmazra legalább 10 prímszám oszt legalább egy $aa' + 1$

alakú számot, egyenlőségre 41 példa van, egy ilyen az $(1; 2; 3; 4; 5; 7; 11; 13)$ számnyolcas. Itt a 10 prímosztó a 2, 3, 5, 7, 11, 13, 17, 23, 29 és 53. Ugyanakkor 140-nél nem nagyobb pozitív egész számokat tartalmazó nyolcelemű A halmazból sincs olyan, ahol legfeljebb 9 prímszám oszt legalább egy $aa' + 1$ alakú számot, ez ugyancsak Python programmal elért eredmény, ahogy az összes saját programmal megtalált eredmény.

Zárásként összehasonlításképp egy táblázat arról, hogy mit tudunk a prímosztók lehetséges minimális számáról $a + a'$, illetve $aa' + 1$ alakú számokat nézve az egy halmazos eset 3 8 elemű halmazainál. Ha több szám lehetséges, a legnagyobb az, amire van gépi példa.

Pozitív egész számokból álló A halmaz mérete	$a + a'$ alakú számok különböző prímosztóinak minimális száma	$aa' + 1$ alakú számok különböző prímosztóinak minimális száma
3	2	2
4	2	2-3
5	3	2-5
6	3-4	2-6
7	3-5	2-7
8	3-5	2-10

Irodalomjegyzék

[1] P. Erdős, C.L. Stewart és R. Tijdeman: Some diophantine equations with many solutions, *Compositio Mathematica* 66: 37-56, 1988

[2] P. Erdős és J. Surányi: Válogatott fejezetek a számelméletből, Polygon, Szeged, 2004, 3. kiadás

[3] P. Erdős és P. Turán: On a problem in the elementary theory of numbers, *American Mathematical Monthly* 41: 608-611, 1934

[4] J.-H. Evertse: On equations in S-units and the Thue-Mahler equation, *Inventiones mathematicae* 75: 561-584, 1984

[5] J.-H. Evertse: The number of solutions of decomposable form equations, *Inventiones mathematicae* 122: 559-602, 1995

[6] J.-H. Evertse és K. Győry: Finiteness criteria for decomposable form equations, *Acta Arithmetica* 50: 357-379, 1988

[7] J.-H. Evertse, K. Győry, C. L. Stewart és R. Tijdeman: S-unit equations and their applications, In: A. Baker. (ed.): New advances in Transcendence Theory: 110-174, Cambridge University Press, Cambridge, 1988

[8] K. Gyarmati és A. Sárközy: Exponenciális és karakterösszegek, Egyetemi jegyzet, 2024

[9] K. Győry, A. Sárközy és C. L. Stewart: On the number of prime factors of integers of the form $ab + 1$, *Acta Arithmetica* 74 (4): 365-385, 1996

[10] K. Győry, C. L. Stewart és R. Tijdeman: On prime factors of sums of integers I, *Compositio Mathematica* 59: 81-88, 1986

[11] G. Pólya: Zur arithmetischen Untersuchung der Polynome, *Mathematische Zeitschrift* 1: 143-148, 1918

[12] C. L. Stewart és R. Tijdeman: On prime factors of sums of integers II, In: J. H. Loxton és A. J. van der Poorten (eds.): Diophantine Analysis: 83-98, Cambridge University Press, Cambridge, 1986

[13] L. Szalay és V. Ziegler: On an S-unit variant of Diophantine m-tuples, *Publicationes Mathematicae Debrecen* 83 (1-2): 97-121, 2013

[14] L. Szalay és V. Ziegler: S-Diophantine quadruples with $S = \{2; q\}$, *International Journal of Number Theory* 11 (3): 849-868, 2015

[15] L. Szalay és V. Ziegler: S-Diophantine quadruples with two primes congruent to 3 modulo 4, *Integers* 13: No. A80, 9, 2013

[16] B.-L. Wu: Sumsets with restricted number of prime factors, *Lithuanian Mathematical Journal* 59 (2): 251-260, 2019

[17] V. Ziegler: Finding all S-Diophantine quadruples for fixed set of primes S, *Monatshefte für Mathematik* 196: 617-641, 2021

[18] https://www.erdosproblems.com/go_to/126