Eötvös Loránd Tudományegyetem

Természettudományi Kar

Gyarmati Richárd

Számelmélet feladatok szakkörre

Bsc szakdolgozat

Témavezető:

Dr. Szalay Mihály
Algebra és számelmélet tanszék

Budapest, 2016

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani témavezetőmnek, Dr. Szalay Mihálynak, hogy elvállalta a konzulensi teendőket, hogy mindig rendelkezésemre állt és értékes szakmai tanácsaival, útmutatásaival hozzájárult szakdolgozatom elkészüléséhez.

Köszönöm Dr. Fried Katalin Tanárnőnek, hogy mindig készségesen segített, amikor nehézségeim adódtak dolgozatom digitális formába való bevitele közben.

Szintén köszönettel tartozom családomnak és barátaimnak, hogy mindig támogattak és lelkesítettek az évek során.

Végül, de nem utolsó sorban szeretném kifejezni hálámat gimnáziumi és egyetemi tanáraimnak egyaránt, akik hozzájárultak szakmai fejlődésemhez.

Tartalomjegyzék

1. Bevezetés

Középiskolában speciális matematika tagozatra jártam, mindig emelt óraszámban tanultam a matematikát. Az alapórákon ugyan sok mindent megtanultunk, betekintést nyertem az egyetemi tananyagba is, de matematika szakkörre nem, vagy csak korlátozott formában volt lehetőség: az OKTV versenyfelkészítéseken kívül egyik tanár sem tartott matematika szakkört. Az elképzelt szakköröm motivációja, melyről szakdolgozatom szól - éppen az, hogy milyen jó lett volna, ha annak idején egy számomra érdekes matematikai témakörből szakkör lett volna tartva. Mivel a számelmélet mindig is az egyik kedvenc témám volt, ezért dolgozatomban egy fiktív számelméleti szakkört indítottam.

Egy szakkör sikerességének egyik kulcsa az, hogy a nagyobb óraszámban, esetleg jobb matematika oktatásban részesülő diákok éppúgy el legyenek foglalva, mint a kevesebb óraszámban matematikát tanuló diákok. Erre is próbáltam figyelmet fordítani dolgozatom írása közben. Például a kongruenciákat nem minden diák tanulja középiskolában. Sok feladatnál pedig sokkal gyorsabb és egyszerűbb, esetleg elegánsabb lenne a megoldás kongruenciával, mint anélkül, emiatt néhány feladathoz több megoldást is adtam. Így minden tanuló megtalálhatja a megoldások közül a számára legjobban érthető levezetést.

Dolgozatom két részből áll. Az első részben Arany Dániel matematikaversenyre szánt, vagy ott megjelent feladatok megoldását dolgoztam ki. Ezekből a feladatokból érdemes egy szakköri alkalmon egyszerre több feladatot feladni, hogy minden tanuló kiválaszthassa azokat a feladatokat, amikkel ott a legszívesebben foglalkozik. Következő alkalmon pedig meg lehet beszélni az előző szakkör feladatainak megoldását. A kidolgozott feladatok közül vannak olyanok, amelynek megoldásai egy-egy korábbi feladatra épülnek, így fontos a sorrend betartása sok esetben. A dolgozatom második részében pedig egy külön téma szerepel (lánctörtek és Pell-egyenletek), ahol a diákok önállóan tehetnek kisebb felfedezéseket, és a problémák megoldása közben a számítógép erejét is segítségül hívhatják. Programozás közben szembesülhetnek numerikus számítási hibákkal, melyek kiküszöbölésével foglalkozunk is. Ezen túl megismerhetnek néhány egyetemen tanult tételt, és megfigyelhetik, hogy a gyűrűegységek hogyan lehetnek segítségünkre a Pell-egyenlet összes megoldásának megadásában.

2. Definíciók, tételek

2.1. Definíció. (Oszthatóság) Legyenek a, b egész számok (azaz $a, b \in \mathbb{Z}$). Azt mondjuk, hogy az a osztója b-nek (jelölése: $a \mid b$), ha létezik olyan c egész szám, hogy $b = ac$. (Ha az a nem osztója b-nek, azt így jelöljük: $a \nmid b$.)

2.2. Megjegyzés. Ha x, y nem nulla egészek és $x \mid y$, akkor $|x| \leq |y|$. Speciálisan, ha x, y pozitív egészek és $x \mid y$, akkor $x \leq y$.

2.3. Definíció. (Kongruencia) $a, b, m \in \mathbb{Z}$ esetén azt mondjuk, hogy az a kongruens b-vel az m modulusra nézve, ha $m \mid a - b$. Ha az a kongruens b-vel az m modulusra nézve („modulo m"), ezt így jelöljük: $a \equiv b \ (m)$; ha pedig $m \nmid a - b$, akkor azt írjuk, hogy $a \not\equiv b \ (m)$.

2.4. Tétel. („kis" Fermat-tétel) *[1] Tetszőleges p pozitív prímszám esetén érvényesek a következők:*

1. *ha $a \in \mathbb{Z}$, akkor $a^p \equiv a \ (p)$;*
2. *ha $a \in \mathbb{Z}$ és $(a; p) = 1$, akkor $a^{p-1} \equiv 1 \ (p)$.*

2.5. Definíció. (Maradékosztály) Tetszőleges $m \geq 2$ egész esetén az egész számok halmaza m diszjunkt osztály uniójára bomlik fel, mégpedig úgy, hogy $0 \leq i \leq m - 1$ esetén az i-edik osztályban $k \cdot m + i$ alakú számok vannak, ahol $k \in \mathbb{Z}$. Ezeket az osztályokat m szerinti, más néven modulo m maradékosztályoknak nevezzük.

2.6. Megjegyzés. $a \equiv b \ (m)$ pontosan akkor, ha a és b egy maradékosztályba esik modulo m.

2.7. Definíció. (Teljes maradékrendszer) Az $\{a_1, a_2, \ldots, a_m\} \subseteq \mathbb{Z}$ halmaz teljes maradékrendszer modulo m, ha minden mod m maradékosztályból pontosan egy elemet tartalmaz.

2.8. Megjegyzés. [1] Ha egy teljes maradékrendszert a modulushoz relatív prím számmal végigszorzunk, és ehhez egy tetszőleges egészet hozzáadunk, akkor ismét teljes maradékrendszert kapunk.

2.9. Definíció. (Egység) Egy egész számot **egységnek** nevezünk, ha minden egész számnak osztója.

2.10. Definíció. (Felbonthatatlan szám) A b nullától és egységektől különböző egész számot felbonthatatlannak nevezzük, ha bármely $b = cd$ ($c, d \in \mathbb{Z}$) felbontás esetén c vagy d egység.

2.11. Definíció. (Prímszám) A p nullától és egységektől különböző egész szám prím, ha minden olyan a és b egész számra, amelyre $p \mid ab$ teljesül, érvényes $p \mid a$ vagy $p \mid b$ (legalább az egyik).

2.12. Megjegyzés. [3] Az egész számok körében a prímszámok és a felbonthatatlan számok azonosak.

2.13. Tétel. (A számelmélet alaptétele) *[1] Minden 1-nél nagyobb természetes szám felbomlik egyértelműen (a szorzótényezők sorrendjétől eltekintve) pozitív prímszámok szorzatára.*

2.14. Tétel. (A számelmélet alaptétele, általános alak) *[1]*
Minden 0*-tól és egységektől különböző egész szám felbontható véges sok felbonthatatlan szám szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű.*

2.15. Definíció. (Tökéletes szám) Tökéletes számnak nevezzük azokat a természetes számokat, amelyek megegyeznek az önmaguknál kisebb pozitív osztóik összegével.

2.16. Definíció. ($\boldsymbol{H_m}$) Legyen m pozitív egész, amely nem négyzetszám (azaz $b \in \mathbb{Z} \Rightarrow b^2 \neq m$) és nem is osztható 1-nél nagyobb négyzetszámmal. Jelöljük H_m-mel azon valós számok halmazát, amelyek felírhatók $x + y\sqrt{m}$ alakban, ahol x és y egész szám; ezek egyértelműen állnak elő ilyen alakban. Speciálisan H_2 jelölje azon valós számok halmazát, amelyek felírhatók $x+y\sqrt{2}$ alakban, ahol x és y egész szám.

2.17. Definíció. ($\boldsymbol{H_m}$-beli oszthatóság) Legyen $a, b \in H_m$ számok. Azt mondjuk, hogy az a osztója a H_m-beli számok körében b-nek (Jelölése: $a \mid_{H_m} b$), ha létezik olyan $c \in H_m$, hogy $b = ac$. (Ha az a nem osztója a H_m-beli számok körében b-nek, azt így jelöljük: $a \nmid_{H_m} b$.)

2.18. Tétel. (A maradékos osztás tétele) *[1] Legyenek a és b egész számok, $b \neq 0$. Ekkor található olyan q és r egész szám, amelyre $a = bq + r$ és $0 \leq r < |b|$ teljesül. Az ilyen q és r egészek egyértelműen meghatározottak.*

3. Feladatok

3.1. Feladat. (TK 31.) Az a, b, c pozitív egész számokról azt tudjuk, hogy $ac = 284$ és $bc = 497$. Mi lehet az abc?

Megoldás: Mivel c az ac és bc számokat is osztja, ezért c a két szám pozitív közös osztói közül kerül ki. $284 = 2^2 \cdot 71$ és $497 = 7 \cdot 71$. Így $c = 1$ vagy $c = 71$ lehetséges.

I. eset: $c = 1$. Ekkor $a = 284$ és $b = 497$. Tehát $abc = 284 \cdot 497 \cdot 1 = 141148$.
II. eset: $c = 71$. Ekkor $a = 4$ és $b = 7$. Tehát $abc = 4 \cdot 7 \cdot 71 = 1988$. □

3.2. Feladat. (TK 32.) Melyik nagyobb?
1988^{1988} vagy $1987^{1987} + 1988^{1987} + 1987^{1988}$?

Megoldás:
Elég az $1987^{1987} + 1987^{1988} + 1988^{1987} - 1988^{1988}$ előjelét megállapítanunk.
$1987^{1987} + 1987^{1988} + 1988^{1987} - 1988^{1988} =$
$= 1987^{1987} \cdot (1 + 1987) + 1988^{1987} \cdot (1 - 1988) =$
$= 1988 \cdot 1987^{1987} - 1987 \cdot 1988^{1987} = 1987 \cdot 1988 \cdot (1987^{1986} - 1988^{1986})$.
Ez pedig negatív, mivel $1987^{1986} - 1988^{1986} < 0$.
Kaptuk: $1987^{1987} + 1987^{1988} + 1988^{1987} < 1988^{1988}$.
Tehát 1988^{1988} a nagyobb. □

3.3. Feladat. (TK 33.) $1988^{1988} + 1987^{1987} - 1988^{1987} + 1987^{1988}$ osztható-e 13-mal?

Megoldás: (Kongruenciával és Kis-Fermat tétellel)
Az eredeti számok helyett dolgozzunk a 13-mal való osztási maradékokkal!
$1989 \equiv 0\ (13)$, így $1988 \equiv -1\ (13)$ és $1987 \equiv -2\ (13)$.
Vizsgáljuk: $(-1)^{1988} + (-2)^{1987} - (-1)^{1987} + (-2)^{1988} =$
$= 1 + (-2)^{1987} - (-1) + (-2) \cdot (-2)^{1987} = 2 + (-1) \cdot (-2)^{1987} = 2^{1987} + 2$.
Keressük 2^{1987}13-mal való osztási maradékát!
A kis Fermat-tétel (2.4) miatt $2^{12} \equiv\ 1\ (13)$, mivel $(2, 13) = 1$.
$2^{1987} + 2 = 2^{1980} \cdot 2^7 + 2 = 2^{12 \cdot 165} \cdot 2^7 + 2 = (2^{12})^{165} \cdot 2^7 + 2 \equiv$
$\equiv\ 1^{165} \cdot 2^7 + 2 = 128 + 2 = 130 \equiv\ 0\ (13)$.
Így $1988^{1988} + 1987^{1987} - 1988^{1987} + 1987^{1988}$ is osztható 13-mal.
□

Megoldás: (Ugyanez kongruencia nélkül)
$1988^{1988} + 1987^{1987} - 1988^{1987} + 1987^{1988} =$

$= 1988 \cdot 1988^{1987} + 1987^{1987} - 1988^{1987} + 1987 \cdot 1987^{1987} =$
$= 1987 \cdot 1988^{1987} + 1988 \cdot 1987^{1987} = 1988 \cdot 1987 \cdot (1988^{1986} + 1987^{1986})$
Elég lenne bizonyítani, hogy $13 \mid 1988^{1986} + 1987^{1986}$.
$13 \mid 1989$, mivel $1989 = 13 \cdot 153$.
$1988^{1986} + 1987^{1986} = (1989-1)^{1986} + (1989-2)^{1986}$.
Az előbbire alkalmazzuk az $(a-b)^n = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} \cdot a^{n-k} \cdot b^k$ azonosságot!
$\sum_{k=0}^{1986} (-1)^k \cdot \binom{1986}{k} \cdot 1989^{1986-k} \cdot 1^k + \sum_{k=0}^{1986} (-1)^k \cdot \binom{1986}{k} \cdot 1989^{1986-k} \cdot 2^k$

Vegyük észre, hogy az előbbi összegekben minden tag osztható 1989-cel, kivéve mikor 1989 kitevői nullák. Így elég csak ezek összegére felírni az oszthatóság feltételét, a többi (1989-cel osztható) tag elhagyható.

Kell: $13 \mid (-1)^{1986} \cdot \binom{1986}{1986} \cdot 1989^0 \cdot 1^{1986} + (-1)^{1986} \cdot \binom{1986}{1986} \cdot 1989^0 \cdot 2^{1986}$.
Készen lennénk, ha sikerülne belátnunk, hogy $13 \mid 2^{1986} + 1$.
$2^{1986} + 1 = 2^{1986} + 1^{1986} = 2^{6 \cdot 331} + 1^{6 \cdot 331} = (2^6)^{331} + (1^6)^{331}$.
Ismert: $a^{2n+1} + b^{2n+1} = (a+b) \cdot \sum_{k=0}^{2n} (-1)^k \cdot a^{2n-k} \cdot b^k$, ahol $n \in \mathbb{N}$.
Vagyis $a + b \mid a^{2n+1} + b^{2n+1}$.
Az előbbire felírva $2^6 + 1^6 \mid (2^6)^{331} + (1^6)^{331}$, vagyis $65 \mid (2^6)^{331} + (1^6)^{331}$.
Viszont $65 = 13 \cdot 5$, így $13 \mid (2^6)^{331} + (1^6)^{331}$.
Tehát $1988^{1988} + 1987^{1987} - 1988^{1987} + 1987^{1988}$ osztható 13-mal.
$\square$

3.4. Feladat. (TK 34.) Legyenek $a; b; c$ pozitív egészek, $a < b < c$, továbbá tudjuk, hogy $a; b; c$ mindegyike osztója a másik kettő összegének. Határozzuk meg a $\frac{b}{a}$ és $\frac{c}{a}$ hányadosok értékét!

Megoldás:

Mivel $c \mid a + b$, ezért a 2.1. definíció szerint $k \cdot c = a + b$.
$a < c$ és $b < c$ miatt $a + b < c + c = 2c$.
Tehát $k \cdot c < 2c$, ahol $k \in \mathbb{Z}^+$ (mivel $a, b, c > 0$) $\Rightarrow 0 < k < 2 \Rightarrow k = 1$.
$c = a + b$-t írjuk be a többi feltételbe:
$b \mid a + c \Rightarrow b \mid 2a + b$. a 2.1. definíció szerint $l \cdot b = 2a + b$.
Mivel $a < b$ miatt $b < 2a + b < 2b + b = 3b$.
Tehát $b < l \cdot b < 3b$, ahol $l \in \mathbb{Z}^+$ (mivel $a, b, c > 0$) $\Rightarrow 1 < l < 3 \Rightarrow l = 2$.
Vagyis $2b = 2a + b \Rightarrow b = 2a$ és $c = a + b = a + 2a \Rightarrow c = 3a$.
Ekkor $\frac{b}{a} = \frac{2a}{a} = 2$, és $\frac{c}{a} = \frac{3a}{a} = 3$.
$\square$

3.5. Feladat. (TK 35.) Keressük meg az összes olyan pozitív egész számot, amely a tízes számrendszerben négyjegyű, jegyei rendre a; b; c; d ($a \neq 0$), továbbá $ab = c + d$; $bd = a + c$ és $acd = (a + d)^3$.

Megoldás:

A feltételek miatt $ab - bd = c + d - (a + c)$.
Tehát $b \cdot (a - d) = d - a = -(a - d)$.
Átrendezve kapjuk: $(b + 1) \cdot (a - d) = 0$.
Mivel $b + 1 > 0$, így $a - d = 0$, tehát $a = d$. Ezt írjuk be a feltételekbe:
$ab = c + d \Rightarrow ab = c + a$.
$acd = (a + d)^3 \Rightarrow a^2c = (2a)^3 \Rightarrow a^2c = 8a^3$.
Ekkor $c = 8a$ (a^2-tel oszthattunk, mivel $a \neq 0$).
a és c számjegyek, $a \neq 0$, így csak **a=1**; **c=8** lehetséges.
$a = d$ miatt **d=1**. $ab = a + c \Rightarrow b = 1 + 8 \Rightarrow$ **b=9**.
Tehát a keresett szám az 1981, és a szám kielégíti a feltételeket. □

3.6. Feladat. (TK 36.) Határozzuk meg az összes olyan x; y; n számhármast, amelyre teljesül, hogy x; y; n pozitív egész számok, az x és az y a tízes számrendszerben egyaránt n-jegyű, továbbá $x^2 = y^3$.

Megoldás:

Legyen $k = x^2 = y^3$. (azaz $x = \sqrt{k}$ és $y = \sqrt[3]{k}$). Ekkor k négyzetszám és köbszám egyben. Minden négyzetszám, illetve köbszám prímtényezős felbontásában az összes kitevő páros, illetve 3-mal osztható. Így k prímtényezős felbontásában minden kitevő 6-tal osztható lesz, ami azt jelenti, hogy k előáll egy (nemnegatív) egész szám hatodik hatványaként.

Ha x és y pontosan n darab számjegyből áll 10-es számrendszerben, az azt jelenti, hogy $10^{n-1} \leq x, y < 10^n$, ahol x és y pozitív egészek.

Ekkor viszont $10^{2n-2} \leq x^2 < 10^{2n}$ és $10^{3n-3} \leq y^3 < 10^{3n}$.
Tehát $10^{2n-2} \leq k < 10^{2n}$ és $10^{3n-3} \leq k < 10^{3n}$.
Azaz $[10^{2n-2}; 10^{2n}) \cap [10^{3n-3}; 10^{3n}) \neq \emptyset \Leftrightarrow [2n - 2; 2n) \cap [3n - 3; 3n) \neq \emptyset$
Ez pontosan akkor igaz, ha $3n - 3 < 2n$
Átrendezéssel kapjuk: $n < 3$. Tehát $n = 1$ vagy $n = 2$.

I. eset: $n = 1$.
Ekkor $10^0 \leq k < 10^2$ és $10^0 \leq k < 10^3$ egyszerre.
Az erősebb feltétel: $10^0 \leq k < 10^2$

Tehát keressük azon legfeljebb 2 számjegyű pozitív hatodik hatványokat (k), melyre $x = \sqrt{k}$ és $y = \sqrt[3]{k}$ pontosan 1 számjegyből állnak.

II. eset: $n = 2$.

Ekkor $10^2 \leq k < 10^4$ és $10^3 \leq k < 10^6$ egyszerre.

A két feltétel összesítve: $10^3 \leq k < 10^4$.

Tehát keressük azon pontosan 4 számjegyből álló pozitív hatodik hatványokat (k), melyre $x = \sqrt{k}$ és $y = \sqrt[3]{k}$ pontosan 2 számjegyből állnak.

Minket a legfeljebb 4 számjegyű hatodik hatványok érdekelnek, így gyűjtsük össze őket: $1^6 = 1$, $2^6 = 64$, $3^6 = 729$, $4^6 = 4096$

$5^6 = 15625 \ldots$ Utóbbi már túl nagy, nem is érdemes tovább nézni.

Tehát k csak az első 4 szám egyike lehet. Nézzük sorra:

$k = 1 \Rightarrow x = 1$ és $y = 1$. Ez megfelel az I. esetnek.

$k = 64 \Rightarrow x = 8$ és $y = 4$. Ez megfelel az I. esetnek.

$k = 729 \Rightarrow x = 27$ és $y = 9$. Ez nem jó!

$k = 4096 \Rightarrow x = 64$ és $y = 16$. Ez megfelel a II. esetnek.

Tehát a megfelelő (x, y, n) számhármasok a következők:

$(1, 1, 1)$; $(8, 4, 1)$; $(64, 16, 2)$.

□

3.7. Feladat. (TK 37.) Az a; b; c nullától különböző egész számokról azt tudjuk, hogy $a^2 \mid b^2$; $b^2 \mid c^2$ és $c^2 \mid a^2$. Bizonyítandó, hogy ekkor a; b; c közül legalább kettő megegyezik!

Megoldás:

Ha a, b, c nullától különböző egészek, akkor a^2, b^2, c^2 pozitív egészek.

Ekkor a 2.2. megjegyzés miatt $a^2 \leq b^2 \leq c^2 \leq a^2 \Leftrightarrow a^2 = b^2 = c^2$.

Így $|a| = |b| = |c|$, vagyis az a, b, c számok csak előjelükben térhetnek el egymástól. De 3 nemnulla számnak egyenként csak kétféle lehet az előjele, így a skatulyaelv szerint lesz közülük legalább kettő, amely megegyezik. Ezzel bebizonyítottuk a kért állítást.

□

3.8. Feladat. (TK 38.) Keressük meg az összes olyan pozitív egész számot, amely a tízes számrendszerben négyjegyű, jegyei rendre a; b; c; d, egyik jegy sem 0, továbbá $a + c = b$; $4ad = c$.

Megoldás:

Mivel a, b, c, d nemnulla számjegyek, és $c = 4ad$, ezért c néggyel osztható (pozitív) számjegy.

Tehát $c = 4$ vagy $c = 8$.

I. eset: **c=4**.
$4ad = 4 \Leftrightarrow ad = 1 \Leftrightarrow$ **a=d=1**. De $b = a + c$, így **b=5**.

II. eset: **c=8**.
$4ad = 8 \Leftrightarrow ad = 2 \Leftrightarrow a = 2$ és $d = 1$, vagy $a = 1$ és $d = 2$.
De $b = a + c$ számjegy, és $a = 2$ esetén $b = 10$ adódna, ami nem számjegy.
Tehát **a=1** és **d=2** lehetséges csak. Ekkor **b=9**.

Tehát a keresett számok: 1541 és 1982, és ezek a számok valóban kielégítik a kezdeti feltételeket.
□

3.9. Feladat. (TK 39.) A 7-tel való oszthatóság vizsgálatára újabb eljárást nyerhetünk a következő észrevételből (tízes számrendszerbeli felírásnál): $7 \mid \overline{a_k \dots a_1 a_0} \Leftrightarrow 7 \mid \overline{a_k \dots a_1} - 2a_0$.

Keressünk hasonlót a 13; 17; 19; 23; 29 és 31 esetére!

Megoldás:

Tekintsük a következő alapfeladatot: Legyen $x \in \mathbb{N}$ és $p \in \mathbb{N}$ olyan, melyre $(p; 10) = 1$. Ekkor keressünk x p-vel való oszthatóságára eljárást! Legyen $x = \overline{a_k \dots a_1 a_0} = 10b + a_0$, ahol $b = \overline{a_k \dots a_1}$.

Ekkor $p \mid x \Leftrightarrow p \mid 10b + a_0 \Leftrightarrow p \mid 10b + a_0 + (10k - 1) \cdot a_0$, ahol $p \mid 10k - 1$. Ilyen k létezik, mivel $(p; 10) = 1$, így $10k - 1$ teljes maradékrendszert alkot mod p $(k = 0; 1; \dots; p - 1)$ a 2.8. megjegyzés miatt.

De $p \mid 10b + a_0 + (10k - 1) \cdot a_0 \Leftrightarrow p \mid 10b + 10k \cdot a_0 \Leftrightarrow p \mid 10 \cdot (b + k \cdot a_0) \Leftrightarrow p \mid b + k \cdot a_0$, mivel $(10; p) = 1$.

Tehát kaptuk: $p \mid 10b + a_0 \Leftrightarrow p \mid b + k \cdot a_0$, ahol k olyan, hogy $p \mid 10k - 1$.

Megjegyzés $k - p$ értékkel is dolgozhatunk k helyett, ha kényelmesebb. $(p \mid 10 \cdot (k - p) - 1 \Leftrightarrow p \mid 10k - 10p - 1 \Leftrightarrow p \mid 10k - 1.)$

Megjegyzés
Hogyan találunk megfelelő k-t?
p négyféle számjegyre végződhet: 1; 3; 7; 9 számjegyekre.
Ha p 1-re végződik, akkor $-p = 10k - 1 \Leftrightarrow k = \frac{1-p}{10}$ jó választás.

Ha p 3-ra végződik, akkor $3p = 10k - 1 \Leftrightarrow k = \frac{3p+1}{10}$ jó választás.
Ha p 7-re végződik, akkor $-3p = 10k - 1 \Leftrightarrow k = \frac{1-3p}{10}$ jó választás.
Ha p 9-re végződik, akkor $p = 10k - 1 \Leftrightarrow k = \frac{p+1}{10}$ jó választás.

Példák

$p = 7$ esetén $k = \frac{1-3p}{10} = \frac{1-3\cdot 7}{10} = -2$ jó választás, mint ahogy a példában.

$p = 13$ esetén $k = \frac{3p+1}{10} = \frac{3\cdot 13+1}{10} = +4$ jó választás. (Azaz egy szám pontosan akkor osztható 13-mal, ha az utolsó számjegyét elhagyva keletkező számhoz hozzáadva az elhagyott számjegy 4-szeresét, az így kapott szám osztható 13-mal.)

$p = 17$ esetén $k = \frac{1-3p}{10} = \frac{1-3\cdot 17}{10} = -5$ jó választás. (Azaz egy szám pontosan akkor osztható 17-tel, ha az utolsó számjegyét elhagyva keletkező számból kivonva az elhagyott számjegy 5-szeresét, az így kapott szám osztható 17-tel.)

$p = 19$ esetén $k = \frac{p+1}{10} = \frac{19+1}{10} = +2$ jó választás.
$p = 23$ esetén $k = \frac{3p+1}{10} = \frac{3\cdot 23+1}{10} = +7$ jó választás.
$p = 29$ esetén $k = \frac{p+1}{10} = \frac{29+1}{10} = +3$ jó választás.
$p = 31$ esetén $k = \frac{1-p}{10} = \frac{1-31}{10} = -3$ jó választás.
$\square$

Megjegyzés

Fontos hangsúlyozni, hogy bár a feladat csak prímekre kért oszthatósági szabályt, mi általánosan minden 10-hez relatív prímre adtunk a fent leírt módszerrel.

Ezt kombinálhatjuk a 2^n és 5^n-nel való oszthatósági szabállyal, így akármilyen x egész számmal való oszthatóságot tudunk ellenőrizni, mivel bármely pozitív egész előáll $2^l \cdot 5^m \cdot p$ alakban, ahol $(10; p) = 1$. Ekkor elég külön-külön belátni, hogy x-nek 2^l és 5^m és p is osztója, mivel 2, 5, és p páronként relatív prímek.

(Egy számnak pontosan akkor osztója 2^n vagy 5^n, ha az utolsó n számjegyéből alkotott számnak osztója 2^n vagy 5^n.)

3.10. Feladat. (TK 40.) Keressük meg az összes olyan pozitív egész számot, amely a tízes számrendszerben négyjegyű, jegyei rendre a; b; c; d $(a \neq 0)$, továbbá $ab = (a+d)^2$; $a + c = b$; $ac = 2d^2$.

Megoldás: $ac = 2d^2 \Leftrightarrow d^2 = \frac{ac}{2}$

$a + c = b \Leftrightarrow b - a = c$

$ab = (a+d)^2 \Leftrightarrow ab = a^2 + 2ad + d^2 \Leftrightarrow ab = a^2 + 2ad + \frac{ac}{2} \Leftrightarrow b = a + 2d + \frac{c}{2}$ (mivel $a \neq 0$, leoszthattunk vele).

Előbbit átrendezve kapjuk: $b - a = 2d + \frac{c}{2} \Leftrightarrow c = 2d + \frac{c}{2} \Leftrightarrow \frac{c}{2} = 2d \Leftrightarrow c = 4d$. De c és d számjegyek, így $d = 0; 1; 2$ lehetséges csak.

I. eset: **d=0**.
Ekkor $c = 4d \Leftrightarrow$ **c=0**. $a + c = b$ miatt **a=b**.
Ekkor minden feltétel teljesül. (**a=b=1; 2; 3; 4; 5; 6; 7; 8; 9**)

II. eset: $d = 1$.
Ekkor $c = 4d \Leftrightarrow c = 4$. $ac = 2d^2$ miatt $4a = 2 \Leftrightarrow a = \frac{1}{2}$. Ez ellentmondás.

III. eset: **d=2**.
Ekkor $c = 4d \Leftrightarrow$ **c=8**. $ac = 2d^2$ miatt $8a = 8 \Leftrightarrow$ **a=1**.
$b = a + c$ miatt **b=9**.

Tehát a lehetséges számok:
1100; 2200; 3300; 4400; 5500; 6600; 7700; 8800; 9900; 1982, és ezek a számok tényleg kielégítik a kezdeti feltételeket. □

3.11. Feladat. (TK 41.) Keressük meg az összes olyan pozitív egészekből álló g; m; n számhármast, amelyre $1 < g = \overline{ab} (= \overline{ab}_{10})$; $m! = \overline{ab}_g$ és $n! = \overline{ba}_g$ alakú (a jegyek utáni index a felírás alapszáma, a 10-et nem szokás kiírni)!

Megoldás:
$1 < g = \overline{ab}$
$m! = \overline{ab}_g \Leftrightarrow m! = ag + b \Leftrightarrow m! = a \cdot \overline{ab} + b$
$n! = \overline{ba}_g \Leftrightarrow n! = bg + a \Leftrightarrow n! = b \cdot \overline{ab} + a$
Mivel a és b tízes számrendszerbeli számjegyek, ezért $a \leq 9$ és $b \leq 9$.
De ekkor $\max m! = \max n! \leq 9 \cdot 99 + 9 = 900$.
$1! = 1$; $2! = 2$; $3! = 6$; $4! = 24$; $5! = 120$; $6! = 720$; $7! = 5040$ sok!
Tehát $m = 1; 2; 3; 4; 5; 6$

I. eset: $m = 1$.
$m! = 1 = a \cdot \overline{ab} + b \Rightarrow a = 0$; $b = 1$.
De $1 < g = \overline{ab} = 1$ nem teljesül!

II. eset: $m = 2$.

$m! = 2 = a \cdot \overline{ab} + b \Rightarrow a = 0;\ b = 2$.

Ekkor $n! = b \cdot \overline{ab} + a = 2 \cdot 2 + 0 = 4$ nem jó, mivel $n! = 4$-nek nincs n-re egész megoldása.

III. eset: $m = 3$.

$m! = 6 = a \cdot \overline{ab} + b \Rightarrow a = 0;\ b = 6$.

Ekkor $n! = b \cdot \overline{ab} + a = 6 \cdot 6 + 0 = 36$ nem jó, mivel $n! = 36$-nak nincs n-re egész megoldása.

IV. eset: **m=4**.

$m! = 24 = a \cdot \overline{ab} + b \Rightarrow a = 1;\ b = 7$.

Ekkor $n! = b \cdot \overline{ab} + a = 7 \cdot 17 + 1 = 120$ jó, mivel $n! = 120$-ra **n=5** megoldás. Ekkor $\mathbf{g} = \overline{ab} = \mathbf{17}$.

V. eset: $m = 5$.

$m! = 120 = a \cdot \overline{ab} + b = a \cdot (10a + b) + b \Rightarrow a = 3 \Rightarrow 120 = 3 \cdot (30 + b) + b \Rightarrow 90 + 4b = 120 \Rightarrow 4b = 30$. Ekkor b nem lenne egész, nem jó!

VI. eset: $m = 6$.

$m! = 720 = a \cdot \overline{ab} + b = a \cdot (10a + b) + b \Rightarrow a = 8 \Rightarrow 720 = 8 \cdot (80 + b) + b \Rightarrow 640 + 9b = 720 \Rightarrow 9b = 80$. Ekkor b nem lenne egész, nem jó!

Tehát a megoldást adó számhármas $(g; m; n) = (17; 4; 5)$.

□

3.12. Feladat. (TK 42.) Határozzuk meg az összes olyan pozitív egészekből álló a; b; c számhármast, amelyre $a + 2b + 3c \mid b + 2c + 3a$

és $b + 2c + 3a \mid c + 2a + 3b$.

Megoldás: a 2.2. megjegyzés miatt $a + 2b + 3c \leq b + 2c + 3a \leq c + 2a + 3b$.

$a + 2b + 3c \mid c + 2a + 3b$ és $a + 2b + 3c \mid a + 2b + 3c$ miatt

$a + 2b + 3c \mid c + 2a + 3b - (a + 2b + 3c) \Rightarrow a + 2b + 3c \mid a + b - 2c$.

De mivel $a + 2b + 3c \leq c + 2a + 3b$, ezért $0 \leq c + 2a + 3b - (a + 2b + 3c) = a + b - 2c$.

Másrészt $a; b; c > 0$, így $a + b - 2c < a + 2b + 3c$.

Tehát $0 \leq a + b - 2c < a + 2b + 3c$ és $a + 2b + 3c \mid a + b - 2c \Rightarrow a + b - 2c = c + 2a + 3b - (a + 2b + 3c) = 0$.

Így $c+2a+3b = a+2b+3c$, de ekkor $a+2b+3c = b+2c+3a = c+2a+3b$.
$a + 2b + 3c = b + 2c + 3a \Leftrightarrow b = 2a - c$. Ezt írjuk be $a + b - 2c = 0$-ba!
$a + 2a - c - 2c = 0 \Leftrightarrow 3a = 3c \Leftrightarrow a = c$.
Másrészt $b = 2a - c = 2a - a = a$. Kaptuk: **a=b=c**.
Tehát a megfelelő számhármasok $(a; a; a)$ alakúak, ahol a pozitív egész.
□

3.13. Feladat. (TK 43.) Keressük meg az összes olyan pozitív egész számot, amely a tízes számrendszerben négyjegyű, jegyei rendre a; b; c; d ($a \neq 0$), továbbá $a^2 + b^2 = 16c + 2d - 52$; $\quad c^2 + d^2 = 2a + 16b - 73$.

Megoldás:

Induljunk el a 2. egyenletből: a jobb oldal páratlan, mert felírható $2 \cdot (a + 8b - 37) + 1$ alakban. Ekkor a bal oldalnak is páratlannak kell lennie: ez csak úgy teljesülhet, ha c^2 és d^2 különböző paritásúak, ekkor c és d is különböző paritásúak. Használjuk fel, hogy bármely páros négyzetszám 4-gyel osztható, bármely páratlan négyzetszám pedig 4-gyel osztva 1 maradékot ad. Ekkor a 2. egyenlet bal oldalán lévő kifejezés 4-gyel osztva 1 maradékot ad. Így a jobb oldalon is 4-gyel osztva 1 maradékot adó kifejezésnek kell állnia. $16b - 73 \equiv\ 3(4)$, így $2a \equiv\ 2(4)$ kell lennie, hogy az összegük 1 maradékot adjon 4-gyel osztva. De $2a \equiv\ 2(4)$ csak úgy lehet, ha a páratlan.

Az 1. egyenlet jobb oldala páros, mert felírható $2 \cdot (8c + d - 26)$ alakban. Viszont a bal oldal úgy lesz páros, ha a^2 és b^2 azonos paritásúak, de ekkor a és b is azonos paritásúak. Tehát b is páratlan.

Most adjuk össze a két egyenletet: $a^2 + b^2 + c^2 + d^2 = 2a + 16b + 16c + 2d - 125 \Leftrightarrow a^2 - 2a + b^2 - 16b + c^2 - 16c + d^2 - 2d = -125 \Leftrightarrow a^2 - 2a + 1 + b^2 - 16b + 64 + c^2 - 16c + 64 + d^2 - 2d + 1 = -125 + 1 + 64 + 64 + 1 \Leftrightarrow$
$(a - 1)^2 + (b - 8)^2 + (c - 8)^2 + (d - 1)^2 = 5$

Az 5 egyféleképp áll elő 4 négyzetszám összegeként (a sorrendtől eltekintve): 4+1+0+0. Ez 3 páros, és 1 páratlan szám. b páratlan, így $b - 8$ is páratlan. A $a - 1$; $c - 8$; $d - 1$ tehát szükségképpen páros: $c - 8$ páros, így c is páros. $d - 1$ páros, így d páratlan.

A következőkben használjuk fel, hogy bármely páratlan négyzetszám 1 maradékot ad 8-cal osztva.

Tekintsük az 1. egyenletet: $a^2 + b^2 \equiv\ 2(8)$, mivel $a^2 \equiv\ b^2 \equiv\ 1(8)$, mivel mindkettő páratlan négyzetszám. A jobb oldalon $16c - 52 \equiv\ 4(8)$, ezért $2d \equiv\ 6(8)$, hogy az összegük 2 maradékot adjon 8-cal osztva. De ha $2d \equiv\ 6(8)$, akkor $d \equiv 3(4)$. Ekkor viszont $d - 1 \equiv\ 2(4)$. Ekkor viszont

$d-1$ nem 0 és prímtényezős felbontásában a 2 pontosan az első hatványon szerepel, mivel 4-gyel nem osztható, de páros. Így $(d-1)^2 \equiv 4(8)$, mivel $(d-1)^2$ prímtényezős felbontásában a 2 pontosan a második hatványon fog szerepelni, azaz 4-gyel osztható, de 8-cal már nem.

Most már azonosíthatjuk a tagokat: $(b-8)^2 = 1$; $(d-1)^2 = 4$. Így kizárásos alapon $(a-1)^2 = 0$; $(c-8)^2 = 0$.

Ami rögtön látszik: **a=1**; **c=8**. $|d-1| = 2$, de $d-1 \neq -2$, mivel $d \neq -1$ (d számjegy). Tehát $d-1 = 2 \Leftrightarrow$ **d=3**.

Kell még: $|b-8| = 1 \Leftrightarrow b = 7$ vagy $b = 9$.

Rendezve az 1. egyenletet, kapjuk: $b^2 = 16c + 2d - 52 - a^2 = 128 + 6 - 52 - 1 = 81$. Tehát **b=9**.

Tehát a megoldás 1983. Könnyen ellenőrizhető, hogy ez a szám valóban kielégíti mindkét egyenletet.

□

3.14. Feladat. (TK 44.) Mutassuk meg, hogy $2^{12} \mid 1983^{1984} - 1$.

Megoldás: Használjuk az $a^2 - b^2 = (a-b)\cdot(a+b)$ azonosságot!

$1983^{1984} - 1 = (1983^{992} - 1)\cdot(1983^{992} + 1) = (1983^{496} - 1)\cdot(1983^{496} + 1)\cdot(1983^{992} + 1) = (1983^{248} - 1)\cdot(1983^{248} + 1)\cdot(1983^{496} + 1)\cdot(1983^{992} + 1) = (1983^{124} - 1)\cdot(1983^{124} + 1)\cdot(1983^{248} + 1)\cdot(1983^{496} + 1)\cdot(1983^{992} + 1) = (1983^{62} - 1)\cdot(1983^{62} + 1)\cdot(1983^{124} + 1)\cdot(1983^{248} + 1)\cdot(1983^{496} + 1)\cdot(1983^{992} + 1) = (1983^{31} - 1)\cdot(1983^{31} + 1)\cdot(1983^{62} + 1)\cdot(1983^{124} + 1)\cdot(1983^{248} + 1)\cdot(1983^{496} + 1)\cdot(1983^{992} + 1)$.

1983 hatványai páratlanok, így a szorzat minden tagja páros. Elég bebizonyítanunk, hogy az utóbbi 7 szorzótényező egyike osztható $2^6 = 64$-gyel.

Kell: $64 \mid 1983^{31} + 1$

Ismert: $a + b \mid a^p + b^p$, ahol p páratlan természetes szám.

Tehát $1983 + 1 \mid 1983^{31} + 1^{31} \Rightarrow 1984 \mid 1983^{31} + 1$. De $1984 = 64 \cdot 31$, így $64 \mid 1983^{31} + 1$.

Kaptuk: $2^6 \mid (1983^{31} - 1)\cdot(1983^{62} + 1)\cdot(1983^{124} + 1)\cdot(1983^{248} + 1)\cdot(1983^{496} + 1)\cdot(1983^{992} + 1)$, mivel minden tényező páros, és 6 tényezőből áll és $2^6 \mid 1983^{31} + 1$, így $2^{12} \mid 1983^{1984} - 1$. □

3.15. Feladat. (TK 45.) Bizonyítandó, hogy bármely n páratlan pozitív egészre $2^8 \mid n^{1984} - 1$

Megoldás:

A [TK 44.] feladat alapján $n^{1984} - 1 = (n^{31} - 1) \cdot (n^{31} + 1) \cdot (n^{62} + 1) \cdot (n^{124} + 1) \cdot (n^{248} + 1) \cdot (n^{496} + 1) \cdot (n^{992} + 1)$.

n bármely hatványa páratlan, így a szorzat összes tényezője páros. Elég lenne belátni, hogy a 7 tényező közül valamelyik tényező 4-gyel is osztható.

$n^{31} - 1$ és $n^{31} + 1$ szomszédos páros számok, így egyikük $2^2 = 4$-gyel is osztható. Ezzel beláttuk, hogy $2^8 \mid n^{1984} - 1$.

$\square$

3.16. Feladat. (TK 46.) Keressük meg az összes olyan pozitív egész számot, amely a tízes számrendszerben nyolcjegyű, jegyei rendre a; b; c; d; e; f; g; h ($a \neq 0$), továbbá $b = 3d$; $a + d = h$; $bg + cf = d^2h^2$; $f = d^2$; $c + g = h^2$; $h = (a + e)^2$.

Megoldás:

$c + g = h^2$ és $h = (a + e)^2$-ből adódik: $c + g = (a + e)^4$. Mivel c és g számjegyek, így $c + g \leq 18$ fennáll. Ekkor $(a + e)^4 \leq 18$ kell, de mivel $a \neq 0$, ezért $a + e = 1$ vagy $a + e = 2$ lehetséges. Ennek megfelelően bontsunk esetekre:

I. eset:$a = 2$, $e = 0$.
Ekkor $h = (a + e)^2 \Leftrightarrow h = 4$.
$a + d = h \Leftrightarrow d = h - a \Leftrightarrow d = 2$.
$b = 3d \Leftrightarrow b = 6$.
$f = d^2 \Leftrightarrow f = 4$.
Kéne: $bg + cf = d^2h^2$ és $c + g = h^2$. Tehát $6g + 4c = 64$ és $c + g = 16$. Utóbbit szorozva 4-gyel: $4c + 4g = 64$.

$6g + 4c - (4c + 4g) = 64 - 64 \Leftrightarrow 2g = 0 \Leftrightarrow g = 0$, de ekkor $c = 16$. Ellentmondásra jutottunk, mivel c számjegy. Itt nem találtunk megoldást.

II. eset: $a = 1$, $e = 1$.
Ekkor $h = (a + e)^2 \Leftrightarrow h = 4$.
$a + d = h \Leftrightarrow d = h - a \Leftrightarrow d = 3$.
$b = 3d \Leftrightarrow b = 9$.
$f = d^2 \Leftrightarrow f = 9$.
Kéne: $bg + cf = d^2h^2$ és $c + g = h^2$. Tehát $9g + 9c = 144$ és $c + g = 16$.

Ez minden $c + g = 16$ párra jó, tehát $c = 7$ és $g = 9$, vagy $c = 8$ és $g = 8$ vagy $c = 9$ és $g = 7$.

III. eset: $a = 1$, $e = 0$.

Ekkor $h = (a+e)^2 \Leftrightarrow h = 1$.
$a + d = h \Leftrightarrow d = h - a \Leftrightarrow d = 0$.
$b = 3d \Leftrightarrow b = 0$.
$f = d^2 \Leftrightarrow f = 0$.
Kéne: $bg + cf = d^2h^2$ és $c + g = h^2$. Tehát $0 = 0$ és $c + g = 1$.
Ez minden $c + g = 1$ párra jó, tehát $c = 0$ és $g = 1$, vagy $c = 1$ és $g = 0$.

Tehát a számok: 19731994, 19831984, 19931974, 10100001, 10000011, és ezek tényleg kielégítik a kezdeti feltételeket.
□

3.17. Feladat. (TK 47.) Keressük meg az összes olyan pozitív egész számot, amely a tízes számrendszerben nyolcjegyű, jegyei rendre a; b; c; d; e; f; g; h ($a \neq 0$), továbbá $c = 2d$; $a+d = h$; $bg+cf = bd^2$; $c+g = d^2$; $d = (a+e)^2$; $e + g = f$.

Megoldás:
Indirekt tegyük fel, hogy $d \leq 3$.
Ekkor $c = 2d$ miatt $c \leq 6$, tehát $c + g \leq 15$, mivel g számjegy.
$c + g = d^2$ és $d = (a + e)^2$-ből adódik: $c + g = (a + e)^4$.
De $c + g \leq 15$, így $(a + e)^4 \leq 15$, de ekkor $a \neq 0$ miatt csak $a + e = 1$ lehetséges, tehát $a = 1$, $e = 0$.
$d = (a + e)^2 \Leftrightarrow d = 1$.
$c = 2d \Leftrightarrow c = 2$.
Viszont ekkor $c + g = d^2$ nem teljesülhet, mert $c > d^2$. Ellentmondásra jutottunk, tehát az indirekt feltevés nem igaz.
Kaptuk: $d > 3$, azaz $d \geq 4$.
De $c+g = d^2$-ben $c+g \leq 18$, mivel c és g számjegyek. Így $d^2 \leq 18$, vagyis $d \leq 4$.
Így $d = 4$.
$c = 2d \Leftrightarrow c = 8$.
$c + g = d^2 \Leftrightarrow g = d^2 - c \Leftrightarrow g = 8$.
$d = (a + e)^2 \Leftrightarrow a + e = 2$.
Bontsunk esetekre:

I. eset: $a = 1$ és $e = 1$.
$e + g = f \Leftrightarrow f = 9$.
$a + d = h \Leftrightarrow h = 5$.
Kéne: $bg + cf = bd^2$. Tehát $8b + 72 = 16b \Leftrightarrow 8b = 72 \Leftrightarrow b = 9$.

II. eset: $a = 2$ és $e = 0$.
$e + g = f \Leftrightarrow f = 8$.
$a + d = h \Leftrightarrow h = 6$.
Kéne: $bg + cf = bd^2$. Tehát $8b + 64 = 16b \Leftrightarrow 8b = 64 \Leftrightarrow b = 8$.

Tehát a kapott számok: 19841985 és 28840886, és ezek tényleg kielégítik a kezdeti feltételeket.

□

3.18. Feladat. (TK 48.) Határozzuk meg az összes olyan n pozitív egészet, amelyre $n^3 + 1 \mid n^5 + 1$.

Megoldás:

Legyen $k = \frac{n^5+1}{n^3+1}$.
$n^3 + 1 \mid n^5 + 1 \Leftrightarrow k \in \mathbb{Z}$.
Alakítsuk át a törtet a következő módon:
$\frac{n^5+1}{n^3+1} = \frac{n^5+n^2}{n^3+1} - \frac{n^2-1}{n^3+1} = n^2 - \frac{n^2-1}{n^3+1}$.
Mivel $n \in \mathbb{Z}^+ \Rightarrow n^2 \in \mathbb{Z}^+$.
Ahhoz, hogy k egész legyen, kell: $\frac{n^2-1}{n^3+1}$ egész legyen. Tehát $n^3+1 \mid n^2-1$.
Ekkor a 2.2. megjegyzés miatt $n^2 - 1 = 0$ vagy $|n^3 + 1| \leq |n^2 - 1|$.
Előbbi $n = 1$ esetén teljesül a pozitív egészek körében.
Most vizsgáljuk $|n^3 + 1| \leq |n^2 - 1|$ megoldáshalmazát.
$n \geq 1$ esetén $n^3 + 1 \geq 0$ és $n^2 - 1 \geq 0$, így elég a következőt felírni: $n^3 + 1 \leq n^2 - 1$.
Rendezve: $n^3 - n^2 \leq -2 \Leftrightarrow n^2 \cdot (n - 1) \leq -2$.
Tehát keressük $n^2 \cdot (n - 1) \leq -2$ egyenlőtlenség megoldásait. De $n^2 \geq 0$ és $n - 1 \geq 0$, így $n^2 \cdot (n - 1) \geq 0$.
Kaptuk: ennek az egyenlőtlenségnek nincs megoldása.
Tehát csakis $n = 1$ lehetséges, és ekkor valóban igaz, hogy $n^3+1 \mid n^5+1$, mert $2 \mid 2$.

□

3.19. Feladat. (TK 49.) Legyenek a;b;n ($n \neq 1$) pozitív egészek. Mikor teljesül, hogy $n^a + 1$ osztható $(n^b + 1)$-gyel?

Megoldás:

A [TK 48.] feladat mintájára:
Először belátjuk, hogy $b > a$ esetén a következő feladatoknak nincs megoldása $n > 1$ feltétel mellett:

1. $n^b + 1 \mid (n^a + 1)$

2. $n^b + 1 \mid (n^a - 1)$

Először keressük 1. megoldását $b > a$ feltétel mellett:
a 2.2. megjegyzés miatt $n^a + 1 = 0$ vagy $|n^b + 1| \leq |n^a + 1|$.
Előbbi sosem teljesül a pozitív egészek körében.
Most vizsgáljuk $|n^b + 1| \leq |n^a + 1|$ megoldáshalmazát.
$n > 1$ esetén $n^b + 1 > 0$ és $n^a + 1 > 0$, így elég a következőt felírni: $n^b + 1 \leq n^a + 1$.
Rendezve: $n^b - n^a \leq 0 \Leftrightarrow n^a \cdot (n^{b-a} - 1) \leq 0$.
Tehát keressük $n^a \cdot (n^{b-a} - 1) \leq 0$ egyenlőtlenség megoldásait. De $n^a > 0$ és $n^{b-a} - 1 > 0$, ha $n > 1$, így $n^a \cdot (n^{b-a} - 1) > 0$.
Kaptuk: ennek az egyenlőtlenségnek nincs megoldása.

Most keressük 2. megoldását $b > a$ feltétel mellett:
a 2.2. megjegyzés miatt $n^a - 1 = 0$ vagy $|n^b + 1| \leq |n^a - 1|$.
Előbbi sosem teljesül $n > 1$ esetén.
Most vizsgáljuk $|n^b + 1| \leq |n^a - 1|$ megoldáshalmazát.
$n > 1$ esetén $n^b + 1 > 0$ és $n^a - 1 > 0$, így elég a következőt felírni: $n^b + 1 \leq n^a - 1$.
Rendezve: $n^b - n^a \leq -2 \Leftrightarrow n^a \cdot (n^{b-a} - 1) \leq -2$.
Tehát keressük $n^a \cdot (n^{b-a} - 1) \leq -2$ egyenlőtlenség megoldásait. De $n^a > 0$ és $n^{b-a} - 1 > 0$, ha $n > 1$, így $n^a \cdot (n^{b-a} - 1) > 0$.
Kaptuk: ennek az egyenlőtlenségnek sincs megoldása.

Világos, hogy 1.-nek $b = a$ esetén minden n megoldása lesz.
2.-nak $b = a$ esetén pedig nem lesz megoldása, mivel $n^b + 1 > n^b - 1$ és $n^b - 1 \neq 0$, ha $n > 1$, ez pedig ellentmond a 2.2 megjegyzésnek.

Most vizsgáljuk $b < a$ feltétel mellett az eredeti $n^b + 1 \mid (n^a + 1)$ feladatot. Elég lenne: visszavezethető 1, vagy 2 valamelyikére. $b \geq a$ feltétel mellett.
Legyen $k = \frac{n^a+1}{n^b+1}$.
$n^b + 1 \mid n^a + 1 \Leftrightarrow k \in \mathbb{Z}$.
Alakítsuk át a törtet a következő módon:
$\frac{n^a+1}{n^b+1} = \frac{n^a+n^{a-b}}{n^b+1} - \frac{n^{a-b}-1}{n^b+1} = n^{a-b} - \frac{n^{a-b}-1}{n^b+1}$.
Mivel $n \in \mathbb{Z}^+ \Rightarrow n^{a-b} \in \mathbb{Z}^+$.
Ahhoz, hogy k egész legyen, kell: $\frac{n^{a-b}-1}{n^b+1}$ egész legyen. Tehát $n^b + 1 \mid n^{a-b} - 1$

Ha $a-b \leq b$, akkor visszavezettük a feladatot 2.-ra.

Ha $a-b > b$, iteráljuk az előbbi eljárást:

$n^b+1 \mid n^{a-b}-1 \Leftrightarrow \frac{n^{a-b}-1}{n^b+1} \in \mathbb{Z}$.

$\frac{n^{a-b}-1}{n^b+1} = \frac{n^{a-b}+n^{a-2b}}{n^b+1} - \frac{n^{a-2b}+1}{n^b+1} = n^{a-2b} - \frac{n^{a-2b}+1}{n^b+1}$.

$n^{a-b} \in \mathbb{Z}$, ezért elég: $\frac{n^{a-2b}+1}{n^b+1} \in \mathbb{Z}$, vagyis $n^b+1 \mid n^{a-2b}+1$.

Ha $a-2b \leq b$, akkor visszavezettük a feladatot 1.-re.

Ha $a-2b > b$, akkor folytatjuk az átalakítást. Látható: ha páros számú átalakítás után lesz igaz először, hogy $a-m\cdot b \leq b$ (vagyis m páros), akkor 1.-re vezettük vissza, ha pedig páratlan sok átalakítás után (vagyis ha m páratlan), akkor 2.-ra vezettük vissza a feladatot.

Láttuk korábban: csak akkor lehet megoldás, ha 1.-re visszavezethető $b = a$-val. Tehát ha m páros, $a-m\cdot b = b$ esetén az eredeti oszthatósági feladat bármilyen n-re teljesül, ellenkező esetben pedig nincs megfelelő $n > 1$ szám.

Legyen $m = 2l$. Ekkor kell: $a - 2l\cdot b = b \Leftrightarrow a = (2l+1)\cdot b$. Tehát ha b-nek pozitív páratlan számszorosa a, pontosan akkor lesz megoldása $n^b+1 \mid (n^a+1)$-nek, és ekkor n tetszőleges értéke mellett teljesül az oszthatóság.

$\square$

3.20. Megjegyzés. Ennek mintájára a 2. egyenletnek pontosan akkor lesz megoldása, ha b-nek pozitív páros számszorosa a.

Megoldás: [Ugyanez rövidebben]

Kell: $n^b+1 \mid n^a+1$. Ezt írjuk át kongruenciás alakba:

$n^a+1 \equiv\ 0\ (n^b+1)$.

Ebből kapjuk: $n^a \equiv\ -1\ (n^b+1)$.

Ezt úgy is írhatjuk, hogy $n^a \equiv\ n^b\ (n^b+1)$. Tehát $n^b \equiv\ n^a \equiv\ -1\ (n^b+1)$.

Az 2.18. tétel (a maradékos osztás tétele) szerint $a = bq+r$, ahol $0 \leq r < |b|$.

Tehát $n^{bq+r} \equiv\ -1\ (n^b+1) \Leftrightarrow (n^b)^q \cdot n^r \equiv\ -1\ (n^b+1)$.

Ebből: $(-1)^q \cdot n^r \equiv\ -1\ (n^b+1)$.

I. eset: q páros

Ekkor $n^r \equiv\ -1\ (n^b+1) \Leftrightarrow n^b+1 \mid n^r+1 \Rightarrow n^b \leq n^r$.

Mivel $n > 1$, ez $r = b$ esetén teljesülne először, de a feltétel szerint $r < |b|$, tehát ez nem jó.

II. eset: q páratlan

Ekkor $n^r \equiv\ 1\ (n^b+1) \Rightarrow n^b+1 \mid n^r-1 < n^b+1 \Rightarrow r = 0$.

Kaptuk: $a = q \cdot b$, ahol $q > 0$ páratlan.

Tehát a feladatban szereplő $n^b + 1 \mid n^a + 1$ pontosan akkor teljesül, ha a pozitív páratlanszorosa b-nek.

□

3.21. Megjegyzés. $n = 0$ vagy $n = 1$ bármilyen $a, b \in \mathbb{Z}^+$ mellett teljesíti a $n^b + 1 \mid n^a + 1$ oszthatóságot.

3.22. Feladat. (TK 50.) Az $a_1 < a_2 < \ldots < a_n$ egész számokról azt tudjuk, hogy mindegyiküknek a négyzete is szerepel köztük. Legfeljebb mekkora lehet az n?

Megoldás:

Jelölje a legnagyobb abszolút értékű számot a_{max}! Ha $|a_{max}| > 1$, akkor a_{max} négyzetének abszolút értéke nagyobb lesz, mint a_{max} abszolút értéke. Viszont a_{max}^2-nek is a számok között kell szerepelni. De ez ellentmondás, mivel a_{max} abszolút értéke maximális volt, de van egy nála nagyobb abszolút értékű tag a sorozatban. Tehát csak $|a_{max}| \leq 1$ lehetséges. De ekkor minden $i = 1; 2; \ldots ; n$-re $|a_i| \leq 1$. Ilyen egész számból összesen 3 darab van: {-1, 0, +1}, és ha ezeket választom rendre a_1, a_2, a_3-nak, akkor teljesül a feladat szövegében leírt feltétel, mivel $-1 < 0 < 1$ és $(-1^2) = 1$, $1^2 = 1$ és $0^2 = 0$. Tehát n értéke legfeljebb 3 lehet, és ez megvalósítható.

□

3.23. Feladat. (TK 51.) Van-e olyan $n, m \in \mathbb{Z}$, hogy $nm \neq 0$ és $\frac{2}{n^2} + \frac{3}{m^3} + \frac{4}{n^4} = 0$?

Megoldás:

$\frac{2}{n^2} + \frac{3}{m^3} + \frac{4}{n^4} = 0 \Leftrightarrow \frac{2}{n^2} + \frac{4}{n^4} = -\frac{3}{m^3} \Leftrightarrow \frac{2n^2}{n^4} + \frac{4}{n^4} = -\frac{3}{m^3} \Leftrightarrow \frac{2n^2+4}{n^4} = -\frac{3}{m^3}$

Átrendezve kapjuk:

$\frac{m^3 \cdot (2n^2+4)}{n^4} = -3$

$2n^2 + 4$ páros, így a tört számlálója páros. De a tört értéke páratlan, és ez csak úgy fordulhat elő, ha a számláló és a nevező parítása megegyezik. Tehát n^4 is páros, de ez csak úgy lehet, ha n páros. Legyen $n = 2k$, ahol $k \neq 0$ egész.

$\frac{m^3 \cdot (2 \cdot (2k)^2+4)}{(2k)^4} = -3 \Leftrightarrow \frac{m^3 \cdot (8k^2+4)}{16k^4} = -3 \Leftrightarrow \frac{m^3 \cdot (2k^2+1)}{4k^4} = -3$

A nevező páros. A tört értéke úgy lehet egész, ha a számlálóban van páros tényező. De a számlálóban szereplő $2k^2 + 1$ páratlan, így m^3 páros. De ekkor m páros. Legyen $m = 2t$, ahol $t \neq 0$ egész.

$\frac{(2t)^3\cdot(2k^2+1)}{4k^4} = -3 \Leftrightarrow \frac{8t^3\cdot(2k^2+1)}{4k^4} = -3 \Leftrightarrow \frac{2t^3\cdot(2k^2+1)}{k^4} = -3.$

$2t^2$ páros, így a tört számlálója páros. De a tört értéke páratlan, és ez csak úgy fordulhat elő, ha a számláló és a nevező paritása megegyezik. Tehát k^4 páros, de ez csak úgy lehetséges, ha k páros. Legyen $k = 2l$, ahol $l \neq 0$ egész.

$\frac{2t^3\cdot(2\cdot(2l)^2+1)}{(2l)^4} = -3 \Leftrightarrow \frac{2t^3\cdot(8l^2+1)}{16l^4} = -3 \Leftrightarrow \frac{t^3\cdot(8l^2+1)}{8l^4} = -3.$

A nevező páros. A tört értéke úgy lehet egész, ha a számlálóban van páros tényező. De a számlálóban szereplő $8l^2+1$ páratlan, így t^3 páros. De ekkor t páros. Legyen $t = 2p$, ahol $p \neq 0$ egész.

$\frac{(2p)^3\cdot(8l^2+1)}{8l^4} = -3 \Leftrightarrow \frac{8p^3\cdot(8l^2+1)}{8l^4} = -3 \Leftrightarrow \frac{64p^3\cdot(8l^2+1)}{64l^4} = -3.$

$(8l^2+1)\cdot(8l^2-1) = 64l^4 - 1$. Tehát $64l^4$ 1 maradékot ad $(8l^2+1)$-gyel osztva. Így legnagyobb közös osztójuk 1. Tehát a két számnak nincs közös prímosztója.

Vagyis $(8l^2+1; 64l^4) = 1$. De ekkor $(8l^2+1; l^4) = 1$.

$\frac{64p^3\cdot(8l^2+1)}{64l^4} = -3 \Leftrightarrow \frac{p^3\cdot(8l^2+1)}{l^4} = -3 \Leftrightarrow (8l^2+1)\cdot\frac{p^3}{l^4} = -3.$

Mivel $(8l^2+1; l^4) = 1$, ezért a bal oldalon álló kifejezés csak akkor lehet egész, ha $\frac{p^3}{l^4}$ egész. Mivel $p \neq 0$, így $\frac{p^3}{l^4} \neq 0$ egész.

De $8l^2+1 \geq 9$, mert $l \neq 0$ egész. Ekkor $|(8l^2+1)\cdot\frac{p^3}{l^4}| \geq 9$, és ez ellentmondás, mivel a tört abszolút értéke 3.

Vagyis az eredeti egyenletnek nincs megoldása.

□

Megoldás: [Ugyanez rövidebben]

$\frac{2}{n^2} + \frac{3}{m^3} + \frac{4}{n^4} = 0 \Leftrightarrow \frac{2}{n^2} + \frac{4}{n^4} = -\frac{3}{m^3} \Leftrightarrow \frac{2n^2}{n^4} + \frac{4}{n^4} = -\frac{3}{m^3} \Leftrightarrow \frac{2n^2+4}{n^4} = -\frac{3}{m^3}$

Átrendezve kapjuk:

$\frac{m^3\cdot(2n^2+4)}{n^4} = -3$

$2n^2+4$ páros, így a tört számlálója páros. De a tört értéke páratlan, és ez csak úgy fordulhat elő, ha a számláló és a nevező parítása megegyezik. Tehát n^4 is páros, de ez csak úgy lehet, ha n páros. Legyen $n = 2k$, ahol $k \neq 0$ egész.

$\frac{m^3\cdot(2\cdot(2k)^2+4)}{(2k)^4} = -3$. Átrendezés vége: $m^3\cdot(2k^2+1) = -3\cdot 4k^4$.

$4k^4 = (2k^2+1)\cdot(2k^2-1)+1$, ezért $(2k^2+1; 4k^4) = 1$. De $2k^2+1 \mid -3\cdot 4k^4$, így kapjuk: $2k^2+1 \mid -3$.

Mivel $k \neq 0$, így $2k^2+1 > 1$. Tehát csak $2k^2+1 = 3$ lehetséges. Ebből $k^2 = 1 \Leftrightarrow k = \pm 1$.

Ekkor $m^3\cdot(2k^2+1) = -3\cdot 4k^4 \Leftrightarrow 3m^3 = -3\cdot 4 \Leftrightarrow m^3 = -4$, ez pedig lehetetlen, mivel a -4 nem köbszám.

Tehát az egyenletnek nincs megoldása.

□

3.24. Feladat. (TK 52.) Határozzuk meg az összes olyan p prímszámot és k pozitív egész számot, amelyre $p^k - 1$ köbszám!

Megoldás: A feladat szerint $p^k - 1 = n^3 \Leftrightarrow p^k = n^3 + 1$.

I. eset: p pozitív prímszám.

Ismert: $p^k = n^3 + 1 = (n+1) \cdot (n^2 - n + 1)$.

$n^2 - n + 1 = (n - 0,5)^2 + 0,75 \geq 0,75 > 0$ minden $n \in \mathbb{N}$ esetén.

$p > 1 \Rightarrow p^k > 1 \Rightarrow n^3 + 1 > 1 \Leftrightarrow n^3 > 0 \Leftrightarrow n > 0$.

$p^k = (n+1) \cdot (n^2 - n + 1)$, ezért $n + 1 = p^a$ és $n^2 - n + 1 = p^b$ alakú, ahol $a, b \geq 0$ egészek.

$p^a - 1 = n + 1 - 1 = n$ és $p^b - 1 = n^2 - n + 1 - 1 = n^2 - n = n \cdot (n-1)$.

Ebből látható: $(p^a - 1) \mid (p^b - 1)$.

Ezzel visszavezettük a feladatot a [TK 49.] feladathoz hasonló feladatra, annyi különbséggel, hogy most $a, b = 0$ is megengedett.

Ha $a = 0 \Leftrightarrow p^a - 1 = 0 \Leftrightarrow n = 0$. De ez ellentmondás, mivel $n > 0$.

Ha $b = 0 \Leftrightarrow p^b - 1 = 0 \Leftrightarrow n \cdot (n-1) = 0$. Tehát $n = 0$ vagy $n = 1$. De $n = 0$ nem felel meg a feltételnek, tehát elég $n = 1$ ellenőrzése.

$n^3 + 1 = 1^3 + 1 = 2 = p^k$. Vagyis $p = 2, k = 1$ megoldása a feladatnak.

Keressük $(p^a - 1) \mid (p^b - 1)$ megoldásait, ahol $a, b > 0$, $p > 1$ prím.

[TK 49.] mintájára:

Először keressük a megoldást $a > b$ feltétel mellett:

a 2.2. megjegyzés miatt $p^b - 1 = 0$ vagy $|p^a - 1| \leq |p^b - 1|$.

Előbbi sosem teljesül, ha $b > 0$.

Most vizsgáljuk $|p^a - 1| \leq |p^b - 1|$ megoldáshalmazát.

$p > 1$ és $a, b > 0$, ezért $p^a - 1 > 0$ és $p^b - 1 > 0$, így elég a következőt felírni: $p^a - 1 \leq p^b - 1$.

Rendezve: $p^a - p^b \leq 0 \Leftrightarrow p^b \cdot (p^{a-b} - 1) \leq 0$.

Tehát keressük $p^b \cdot (p^{a-b} - 1) \leq 0$ egyenlőtlenség megoldásait. De $p^b > 0$ és $p^{a-b} - 1 > 0$, így $p^b \cdot (p^{a-b} - 1) > 0$.

Kaptuk: ennek az egyenlőtlenségnek nincs megoldása.

Világos, hogy $a = b$ esetén minden p prím megoldása lesz a részfeladatnak.

Most vizsgáljuk $a < b$ feltétel mellett a $(p^a - 1) \mid (p^b - 1)$ feladatot. Elég lenne: visszavezethető $b < a$ vagy $b = a$ valamelyikére.

$p^a - 1 \mid p^b - 1 \Leftrightarrow \frac{p^b - 1}{p^a - 1} \in \mathbb{Z}$.

Alakítsuk át a törtet a következő módon:

$\frac{p^b-1}{p^a-1} = \frac{p^b-p^{b-a}}{p^a-1} + \frac{p^{b-a}-1}{p^a-1} = p^{b-a} + \frac{p^{b-a}-1}{p^a-1}$.

Mivel $p \in \mathbb{Z}^+ \Rightarrow p^{b-a} \in \mathbb{Z}^+$.

Ahhoz, hogy a tört egész legyen, kell: $\frac{p^{b-a}-1}{p^a-1}$ egész legyen. Tehát $p^a - 1 \mid p^{b-a} - 1$.

Ha $b - a \leq a$, akkor visszavezettük a feladatot.

Ha $b - a > a$, iteráljuk az előbbi eljárást.

Legyen m az az egész szám, ahány iteráció után teljesül először, hogy $b - m \cdot a \leq a$.

Láttuk korábban: csak akkor lehet megoldás, ha $a = b$-re visszavezethető. Tehát kell: $b - m \cdot a = a \Leftrightarrow b = (m+1) \cdot a$.

Tehát $p^{(m+1)\cdot a} = p^b$.

Tudjuk: $(n+1) \cdot (n^2 - n + 1) = n^3 + 1 = p^a \cdot p^b$.

Tehát $p^a \cdot p^{(m+1)\cdot a} = n^3 + 1 \Leftrightarrow p^{(m+2)\cdot a} = n^3 + 1 \Leftrightarrow (p^a)^{m+2} = n^3 + 1$.

De $p^a = n + 1$, tehát $(n+1)^{m+2} = n^3 + 1$.

Milyen m-re lehet igaz, hogy $(n+1)^{m+2} = n^3 + 1$?

Ha $m + 2 = 3$, akkor $(n+1)^3 = n^3 + 3n^2 + 3n + 1 > n^3 + 1$, mivel $3n^2 + 3n > 0$ teljesül $n > 0$ miatt. Ez nem jó!

Ha $m + 2 > 3$, akkor $(n+1)^{m+2} = (n+1)^3 \cdot (n+1)^{m-1} > n^3 + 1$, mivel $(n+1)^{m-1} > 1$. Ez se jó!

$m \geq 0$, így maradt: $m + 2 = 2$.

Kell: $(n+1)^2 = n^3 + 1 \Leftrightarrow n^2 + 2n + 1 = n^3 + 1 \Leftrightarrow n^3 - n^2 - 2n = 0$.

Kiemelve: $n \cdot (n^2 - n - 2) = 0 \Leftrightarrow n \cdot (n-2) \cdot (n+1) = 0$.

A szorzat pontosan akkor lehet 0, ha bármelyik tényezője 0. Azaz $n = 0$ vagy $n = 2$ vagy $n = -1$ lehetséges.

De $n > 0$ feltételt ezek közül csak $n = 2$ teljesíti. Ellenőrizzük le: $n^3 + 1 = 2^3 + 1 = 9 = p^k$.

Tehát $p = 3, k = 2$ megoldása a feladatnak.

II. eset: p negatív prímszám.

Ha k páros, akkor $p^k > 0$, így az I. esetben kapott p értékek ellentettjei lesznek a megoldások, feltéve ha az ott szereplő k is páros.

Tehát $p = -3, k = 2$ megoldás.

Az érdekes eset, ha k nem páros.

Ekkor $n^3 + 1 = p^k < 0 \Leftrightarrow n^3 < -1 \Leftrightarrow n < -1$.

Próbáljuk visszavezetni a feladatot pozitív p esetére.

Legyen $q := -p$ pozitív prím ($p < -1 \Leftrightarrow q > 1$).

$q^k = (-p)^k = -p^k = -(n^3 + 1) = -n^3 - 1$.

Legyen $t := -n$ pozitív szám. ($n < -1 \Leftrightarrow t > 1$)
Ekkor vegyük észre, hogy az alábbi két egyenlet ekvivalens:

1. $-p^k = -n^3 - 1$
2. $q^k = t^3 - 1$

Ismert: $q^k = t^3 - 1 = (t-1) \cdot (t^2 + t + 1)$.
$t^2 + t + 1 = (t + 0,5)^2 + 0,75 \geq 0,75 > 0$ minden $t \in \mathbb{N}$ esetén.
$q > 0 \Rightarrow q^k > 0 \Rightarrow t^3 - 1 > 0 \Leftrightarrow t^3 > 1 \Leftrightarrow t > 1$.
$q^k = (t-1) \cdot (t^2 + t + 1)$, ezért $t - 1 = q^a$ és $t^2 + t + 1 = q^b$ alakú, ahol $a, b \geq 0$ egészek.
$q^a + 1 = t - 1 + 1 = t$ és $q^b - 1 = t^2 + t + 1 - 1 = t^2 + t = t \cdot (t+1)$.
Ebből látható: $(q^a + 1) \mid (q^b - 1)$.
Ezt pedig már megoldottuk a [TK 49.] feladatban részfeladatként, annyi különbséggel, hogy most $a, b = 0$ is megengedett.
$a > b > 0$ esetben a feladatnak nem volt megoldása. Vizsgáljuk meg, hogy $a = 0$, vagy $b = 0$ megoldás-e.
Ha $a = 0 \Leftrightarrow q^a + 1 = 2 \Leftrightarrow t = 2$. $q^k = t^3 - 1 = 7$. Ekkor $q = 7, k = 1$ jó.
Ez $p = -7, k = 1$-nek felel meg, és ez valóban megoldás, mivel $(-7)^1 - 1 = (-2)^3$.
Ha $b = 0 \Leftrightarrow q^b - 1 = 0 \Leftrightarrow t \cdot (t+1) = 0$. Tehát $t = 0$ vagy $t = -1$. De ez ellentmond $t > 1$ feltételnek.
Maradt $b \geq a$ vizsgálata:
$b = a$ lehetetlen.
$b > a$ esetén a 3.20. megjegyzés szerint szerepcserével $q^a + 1 \mid q^{a \cdot 2k} - 1$.
$q^b - 1 = q^{a \cdot 2k} - 1 = t \cdot (t+1) = (q^a + 1) \cdot (q^a + 2) \Leftrightarrow t \cdot (t+1) = q^{2a} + 3q^a + 2$
Tehát $q^{a \cdot 2k} = q^{2a} + 3q^a + 3$.
Kell: $q^a \mid 3$. Ebből $q^a = 3$, vagyis $q = 3$ és $a = 1$.
Ekkor $3^{2k} = 21$ lehetetlen.

Tehát a megoldást nyújtó (p, k) számpárok: $p = 2, k = 1$; $p = 3, k = 2$; $p = -3, k = 2$; $p = -7, k = 1$.
És ezek tényleg kielégítik a kezdeti feltételeket.
$\square$

Megoldás: [Ugyanez kongruenciákkal] A feladat szerint $p^k - 1 = n^3 \Leftrightarrow p^k = n^3 + 1$.

I. eset: p pozitív prímszám.

Ismert: $p^k = n^3 + 1 = (n+1) \cdot (n^2 - n + 1)$.

$n^2 - n + 1 = (n - 0,5)^2 + 0,75 \geq 0,75 > 0$ minden $n \in \mathbb{N}$ esetén.

$p > 1 \Rightarrow p^k > 1 \Rightarrow n^3 + 1 > 1 \Leftrightarrow n^3 > 0 \Leftrightarrow n > 0$.

$p^k = (n+1) \cdot (n^2 - n + 1)$, ezért $n + 1 = p^a$ és $n^2 - n + 1 = p^b$ alakú, ahol $a, b \geq 0$ egészek.

$p^a - 1 = n + 1 - 1 = n$ és $p^b - 1 = n^2 - n + 1 - 1 = n^2 - n = n \cdot (n-1)$.

Ebből látható: $(p^a - 1) \mid (p^b - 1)$.

Ezzel visszavezettük a feladatot a [TK 49.] feladathoz hasonló feladatra, annyi különbséggel, hogy most $a, b = 0$ is megengedett.

Ha $a = 0 \Leftrightarrow p^a - 1 = 0 \Leftrightarrow n = 0$. De ez ellentmondás, mivel $n > 0$.

Ha $b = 0 \Leftrightarrow p^b - 1 = 0 \Leftrightarrow n \cdot (n-1) = 0$. Tehát $n = 0$ vagy $n = 1$. De $n = 0$ nem felel meg a feltételnek, tehát elég $n = 1$ ellenőrzése.

$n^3 + 1 = 1^3 + 1 = 2 = p^k$. Vagyis $p = 2, k = 1$ megoldása a feladatnak.

Keressük $(p^a - 1) \mid (p^b - 1)$ megoldásait, ahol $a, b > 0$, $p > 1$ prím.

[TK 49.] mintájára:

Írjuk át kongruenciás alakba:

$p^b - 1 \equiv\ 0\ (p^a - 1)$.

Ebből kapjuk: $p^b \equiv\ 1\ (p^a - 1)$.

Ezt úgy is írhatjuk, hogy $p^b \equiv\ p^a\ (p^a - 1)$. Tehát $p^a \equiv\ p^b \equiv\ 1\ (p^a - 1)$.

Az 2.18. tétel (a maradékos osztás tétele) szerint $b = am + r$, ahol $0 \leq r < |a|$.

Tehát $p^{am+r} \equiv\ 1\ (p^a - 1) \Leftrightarrow (p^a)^m \cdot p^r \equiv\ 1\ (p^a - 1)$.

Ebből: $1^m \cdot p^r \equiv\ 1\ (p^a - 1) \Rightarrow r = 0$.

Kaptuk: $a = m \cdot b$, ahol $m > 0$ egész.

Tehát $p^{m \cdot a} = p^b$.

Tudjuk: $(n+1) \cdot (n^2 - n + 1) = n^3 + 1 = p^a \cdot p^b$.

Tehát $p^a \cdot p^{m \cdot a} = n^3 + 1 \Leftrightarrow p^{(m+1) \cdot a} = n^3 + 1 \Leftrightarrow (p^a)^{m+1} = n^3 + 1$.

De $p^a = n + 1$, tehát $(n+1)^{m+1} = n^3 + 1$.

Milyen m-re lehet igaz, hogy $(n+1)^{m+1} = n^3 + 1$?

Ha $m + 1 = 3$, akkor $(n+1)^3 = n^3 + 3n^2 + 3n + 1 > n^3 + 1$, mivel $3n^2 + 3n > 0$ teljesül $n > 0$ miatt. Ez nem jó!

Ha $m + 1 > 3$, akkor $(n+1)^{m+1} = (n+1)^3 \cdot (n+1)^{m-2} > n^3 + 1$, mivel $(n+1)^{m-2} > 1$. Ez se jó!

$m > 0$, így maradt: $m + 1 = 2$.

Kell: $(n+1)^2 = n^3 + 1 \Leftrightarrow n^2 + 2n + 1 = n^3 + 1 \Leftrightarrow n^3 - n^2 - 2n = 0$.

Kiemelve: $n \cdot (n^2 - n - 2) = 0 \Leftrightarrow n \cdot (n-2) \cdot (n+1) = 0$.

A szorzat pontosan akkor lehet 0, ha bármelyik tényezője 0. Azaz $n = 0$ vagy $n = 2$ vagy $n = -1$ lehetséges.

De $n > 0$ feltételt ezek közül csak $n = 2$ teljesíti. Ellenőrizzük le: $n^3+1 = 2^3 + 1 = 9 = p^k$.

Tehát $p = 3, k = 2$ megoldása a feladatnak.

II. eset: p negatív prímszám.

Ha k páros, akkor $p^k > 0$, így az I. esetben kapott p értékek ellentettjei lesznek a megoldások, feltéve ha az ott szereplő k is páros.

Tehát $p = -3, k = 2$ megoldás.

Az érdekes eset, ha k nem páros.

Ekkor $n^3 + 1 = p^k < 0 \Leftrightarrow n^3 < -1 \Leftrightarrow n < -1$.

Próbáljuk visszavezetni a feladatot pozitív p esetére.

Legyen $q := -p$ pozitív prím ($p < -1 \Leftrightarrow q > 1$).

$q^k = (-p)^k = -p^k = -(n^3 + 1) = -n^3 - 1$.

Legyen $t := -n$ pozitív szám. ($n < -1 \Leftrightarrow t > 1$)

Ekkor vegyük észre, hogy az alábbi két egyenlet ekvivalens:

1. $-p^k = -n^3 - 1$
2. $q^k = t^3 - 1$

Ismert: $q^k = t^3 - 1 = (t - 1) \cdot (t^2 + t + 1)$.

$t^2 + t + 1 = (t + 0,5)^2 + 0,75 \geq 0,75 > 0$ minden $t \in \mathbb{N}$ esetén.

$q > 0 \Rightarrow q^k > 0 \Rightarrow t^3 - 1 > 0 \Leftrightarrow t^3 > 1 \Leftrightarrow t > 1$.

$q^k = (t - 1) \cdot (t^2 + t + 1)$, ezért $t - 1 = q^a$ és $t^2 + t + 1 = q^b$ alakú, ahol $a, b \geq 0$ egészek.

$q^a + 1 = t - 1 + 1 = t$ és $q^b - 1 = t^2 + t + 1 - 1 = t^2 + t = t \cdot (t + 1)$.

Ebből látható: $(q^a + 1) \mid (q^b - 1)$, ahol q pozitív prím.

Ezzel visszavezettük a feladatot a [TK 49.] feladathoz hasonló feladatra, annyi különbséggel, hogy most $a, b = 0$ is megengedett.

Ha $a = 0 \Leftrightarrow q^a + 1 = 2 \Leftrightarrow t = 2$. $q^k = t^3 - 1 = 7$. Ekkor $q = 7, k = 1$ jó.

Ez $p = -7, k = 1$-nek felel meg, és ez valóban megoldás, mivel $(-7)^1 - 1 = (-2)^3$.

Ha $b = 0 \Leftrightarrow q^b - 1 = 0 \Leftrightarrow t \cdot (t + 1) = 0$. Tehát $t = 0$ vagy $t = -1$. De ez ellentmond $t > 1$ feltételnek.

Tehát keressük $(q^a + 1) \mid (q^b - 1)$ megoldásait, ahol $a, b > 0$, $q > 1$ prím.

[TK 49.] mintájára:

Írjuk át kongruenciás alakba:

$q^b - 1 \equiv\ 0\ (q^a + 1)$.

Ebből kapjuk: $q^b \equiv\ 1\ (q^a + 1)$.

Tudjuk: $p^a \equiv\ -1\ (p^a + 1)$.

Az 2.18. tétel (a maradékos osztás tétele) szerint $b = am + r$, ahol $0 \leq r < |a|$.

Tehát $q^{am+r} \equiv\ 1\ (q^a + 1) \Leftrightarrow (q^a)^m \cdot q^r \equiv\ 1\ (q^a + 1)$.

Ebből: $(-1)^m \cdot q^r \equiv\ 1\ (q^a + 1)$.

I. eset: m páros

Ekkor $q^r \equiv\ 1\ (q^a + 1) \Rightarrow r = 0$.

II. eset: m páratlan

Ekkor $q^r \equiv\ -1\ (q^a + 1) \Leftrightarrow q^r \equiv\ q^a\ (q^a + 1)$.

Mivel $q > 1$, ez $r = a$ esetén teljesülne először, de a feltétel szerint $r < |a|$, tehát ez nem jó.

Kaptuk: $b = m \cdot a$, ahol $m > 0$ páros.

Legyen $m = 2l$. Tehát $q^{2l \cdot a} = q^b$.

Tudjuk: $(t - 1) \cdot (t^2 + t + 1) = t^3 - 1 = q^a \cdot q^b$.

Tehát $q^a \cdot q^{2l \cdot a} = t^3 - 1 \Leftrightarrow q^{(2l+1) \cdot a} = t^3 - 1 \Leftrightarrow (q^a)^{2l+1} = t^3 - 1$.

De $q^a = t - 1$, tehát $(t - 1)^{m+1} = t^3 - 1$.

Milyen l-re lehet igaz, hogy $(t - 1)^{2l+1} = t^3 - 1$? $(t \geq 2)$.

$t = 2$ mellett sosem teljesülhet, mivel $1 \neq 2^3 - 1$.

Ha $2l + 1 = 3$, akkor $(t - 1)^3 = t^3 - 3t^2 + 3t - 1 < t^3 - 1$, mivel $-3t^2 + 3t = -3t \cdot (t - 1) < 0$ teljesül $t > 2$ miatt. Ez nem jó!

Ha $2l + 1 = 5$, akkor $(t - 1)^5 \geq 4 \cdot (t - 1)^3 > t^3 - 1$ minden $t \geq 3$-ra. Ez se jó!

(Megj: $t = 3$-ra $4 \cdot 2^3 = 32 > 3^3 - 1 = 26$. A $4 \cdot (t - 1)^3$ függvény meredeksége $12 \cdot (t - 1)^2 = 12t^2 - 24t + 12$. Ez $t \geq 3$ esetén nagyobb, mint a $t^3 - 1$ függvény meredeksége, azaz $3t^2$. Ugyanis: $12t^2 - 24t + 12 > 3t^2 \Leftrightarrow 9t^2 - 24t + 12 > 0 \Leftrightarrow (3t - 2) \cdot (3t - 6) > 0 \Leftrightarrow \{t < \frac{2}{3}$ vagy $t > 2$ esetén$\}$. Ez teljesül!)

Ha $2l + 1 > 5$, akkor $(t - 1)^{2l+1} = (t - 1)^5 \cdot (t - 1)^{2l-4} > t^3 - 1$, mivel $(t - 1)^{2l-4} > 1$. Ez se jó!

$l > 0$, így ennek nincs megoldása.

Tehát a megoldást nyújtó (p, k) számpárok: $p = 2, k = 1$; $p = 3, k = 2$; $p = -3, k = 2$; $p = -7, k = 1$.

És ezek tényleg kielégítik a kezdeti feltételeket.

□

3.25. Feladat. (TK 53.) Van-e olyan n páratlan pozitív egész, amelyre $n+2$ négyzetszám és $n-2$ köbszám?

Megoldás:

$n+2$ négyzetszám és a feladat szövege szerint $n>0$ volt.

$n+2=a^2$ és $n-2=b^3$. Mivel n páratlan, így $n+2$ és $n-2$ páratlan $\Leftrightarrow a^2$ és b^3 páratlan $\Leftrightarrow a$ és b páratlan.

$a^2-2=n$ és $b^3+2=n$. Ekkor $b^3 \geq -1 \Rightarrow b \geq -1$.

Látszik: $a^2-2=b^3+2 \Leftrightarrow a^2-4=b^3 \Leftrightarrow (a-2)\cdot(a+2)=b^3$.

b^3 prímtényezős felbontásában minden kitevő 3-mal osztható, mivel köbszám (és minden egység köbszám).

$a-2$ és $a+2$ legnagyobb közös osztója osztója a különbségüknek, azaz a 4-nek.

Tehát $(a-2;a+2)$ az 1, 2, 4 számok valamelyike közül kerül ki.

Viszont $a-2$ és $a+2$ is páratlan, így $(a-2;a+2)=1$.

Tehát $a-2$ és $a+2$ nem rendelkezik közös prímosztóval. Ekkor viszont $(a-2)$ és $(a+2)$ prímtényezős felbontásában minden kitevő hárommal osztható, azaz $a-2$ és $a+2$ is köbszám.

Van-e két olyan köbszám, melyeknek különbsége 4?

Keressük $u^3-v^3=4$ megoldásait. (Feltehető: $u>v\geq -1$.)

Vegyük észre, hogy u és v paritása megegyezik.

Szorzattá alakítással: $u^3-v^3=(u-v)\cdot(u^2+uv+v^2)$

Ha u és v mindketten párosak, akkor a szorzat első tényezője páros, a másik tényezője 4-gyel osztható, tehát $8 \mid u^3-v^3$ kéne. Ez ellentmondás.

Ha u és v mindketten páratlanok, akkor a szorzat első tényezője páros, a második tényezője páratlan.

$(u-v)\cdot(u^2+uv+v^2)=4 \Leftrightarrow u-v=4$ és $u^2+uv+v^2=1$ (Itt figyelembe vettük, hogy $u>v$.)

$u-v=4 \Leftrightarrow u=v+4$. Behelyettesítve: $(v+4)^2+(v+4)\cdot v+v^2=1 \Leftrightarrow v^2+8v+16+v^2+4v+v^2=1$.

Rendezve kapjuk: $3v^2+12v+15=0 \Leftrightarrow v^2+4v+5=0 \Leftrightarrow (v+2)^2+1=0$. De $(v+2)^2+1\geq 1$ tetszőleges v esetén.

Tehát a feladatnak nincsen megoldása.

□

3.26. Feladat. (TK 54.) Határozzuk meg az összes olyan p pozitív prímszámot, amelyhez léteznek olyan a; b; c nemnegatív egészek, hogy $p+a=b^p$ és $p-a=c^p$.

Megoldás:

Vonjuk ki az első egyenletből a másodikat:

$(p+a)-(p-a)=b^p-c^p \Leftrightarrow 2a=b^p-c^p$.

Mivel $2a \geq 0 \Leftrightarrow b^p-c^p \geq 0 \Leftrightarrow b^p \geq c^p \Leftrightarrow b \geq c$. ($b$ és c nemnegatívak)

Másrészt b^p-c^p páros, és ez csak úgy lehet, ha b és c paritása megegyezik.

Ha összeadjuk a két egyenletet, kapjuk: $(p+a)+(p-a)=b^p+c^p \Leftrightarrow 2p=b^p+c^p$.

$p=2$ esetén:

$2+a=b^2$ és $2-a=c^2$

Mivel $2-a \leq 2 \Rightarrow c^2 \leq 2$.

Ekkor $c=0$ vagy $c=1$ lehetséges.

Ha $c=0$, $a=2$, $b^2=4 \Rightarrow b=2$. Ez megoldása a feladatnak.

Ha $c=1$, $a=1$, $b^2=3 \Rightarrow b=\sqrt{3}$. Ez nem megoldás, mert ilyenkor b nem egész.

Ezután vizsgáljuk p páratlan prím esetét:

$2p=b^p+c^p=(b+c)\cdot(b^{p-1}-b^{p-2}c+b^{p-3}c^2-b^{p-4}c^3+\ldots+b^2c^{p-3}-bc^{p-2}+c^{p-1})$.

Így $b+c \mid 2p$, illetve $b+c \geq 0$.

$b+c=1$ vagy $b+c=2$ vagy $b+c=p$ vagy $b+c=2p$.

Láttuk: b és c paritása megegyezik, így $b+c$ páros.

Tehát $b+c=2$ vagy $b+c=2p$ maradt.

I. eset: $b+c=2$.

Volt: $b \geq c \Rightarrow b=2, c=0$, vagy $b=1, c=1$.

Ha $b=2, c=0$, akkor $p+a=2^p$ és $p-a=0^p=0 \Rightarrow p=a$. Ebből: $2p=2^p$. Ennek pedig $p \geq 3$ esetén nincs megoldása.

Ha $b=1, c=1$, akkor $p+a=1^p=1$ és $p-a=1^p=1$. Ezeket összeadva kapjuk: $2p=2 \Leftrightarrow p=1$. De ez nem jó, mert 1 nem prím.

II. eset: $b+c=2p$.

Ekkor $(b^{p-1}-b^{p-2}c+b^{p-3}c^2-b^{p-4}c^3+\ldots+b^2c^{p-3}-bc^{p-2}+c^{p-1})=1$.

b és c azonos paritásúak. Ha b-t és c-t is párosnak választanánk, az összeg minden tagja páros lenne, pedig az összeg páratlan. Tehát b és c páratlanok.

Használjuk fel, hogy $b \geq c$. Ekkor $b^kc^l \geq b^{k-1}c^{l+1} \Leftrightarrow b^kc^l-b^{k-1}c^{l+1} \geq 0$.

A $b^{p-1}-b^{p-2}c+b^{p-3}c^2-b^{p-4}c^3+\ldots+b^2c^{p-3}-bc^{p-2}+c^{p-1}$ kifejezésben vegyük párosával a tagokat (az utolsó tag kimarad):

$b^{p-1}-b^{p-2}c \geq 0$, $b^{p-3}c^2-b^{p-4}c^3 \geq 0$, …, $b^2c^{p-3}-bc^{p-2} \geq 0$.

Akkor ezek összege $z := b^{p-1}-b^{p-2}c+b^{p-3}c^2-b^{p-4}c^3+\ldots+b^2c^{p-3}-bc^{p-2} \geq 0$.

Tehát $z + c^{p-1} = 1$, ahol $z \geq 0$ és c páratlan. Ekkor csak $c = 1$ lehetséges.

Ekkor $z = 0$, speciálisan a z-ben levő egymást követő tagok különbsége is 0.

Tehát $b^{p-1} - b^{p-2}c = 0 \Leftrightarrow b^{p-2} \cdot (b - c) = 0$.

De $b \geq c$ miatt $b \neq 0$, így $b - c = 0 \Leftrightarrow b = c = 1$.

Itt $b + c = 2p \Leftrightarrow 2p = 2 \Leftrightarrow p = 1$. Ez nem jó, mert 1 nem prím.

Láttuk: csak $p = 2$ esetén lehet megoldás, ekkor $a = 2$, $b = 2$, $c = 0$. Ez valóban kielégíti a kezdeti feltételeket.

$\square$

3.27. Feladat. (TK 55.) Jelöljük p_n-nel az n-edik pozitív prímszámot ($p_1 = 2$; $p_2 = 3$; $p_3 = 5$; $p_4 = 7$; $p_5 = 11$; $\ldots$). A p_n-et meg nem haladó pozitív egészek közül maximálisan hány választható ki úgy, hogy közülük bármely kettő relatív prím legyen?

Megoldás:

Állítás: maximálisan $n + 1$ darabot tudok kiválasztani. Ezt a következő módon fogom belátni: mutatok $n + 1$ darabot, ami megfelel a feltételeknek, majd bebizonyítom, hogy ennél többet nem tudok így kiválasztani.

Az $1; p_1; p_2; p_3; \ldots; p_n$ számok jók lesznek, mivel $n + 1$ darab páronként relatív prím.

A skatulyaelv miatt nem fogok tudni kiválasztani $n + 1$-nél több számot így.

Ugyanis legyenek a skatulyák rendre $1; p_1; p_2; p_3; \ldots; p_n$ jelzésűek. Minden kiválasztott szám abba a jelzésű skatulyába kerül, amelyik a legkisebb prímosztója, illetve az 1 szám kerüljön az 1 jelzésű skatulyába. Ezt meg tudom tenni, mivel a 2.13 tétel (számelmélet alaptétele) szerint minden 1-nél nagyobb természetes szám felírható egyértelműen (a szorzótényezők sorrendjétől eltekintve) pozitív prímek szorzataként, így minden 1-nél nagyobb természetes számhoz hozzá tudom rendelni a legkisebb prímosztóját. Másrészt a p_n-nél nem nagyobb számoknak nem lehet p_n-nél nagyobb prímosztójuk.

Nyilvánvaló, hogy az 1 jelzésű skatulyába csak az 1 kerülhet, így oda nem kerülhet 1-nél több szám. Viszont ha akármelyik p_i jelzésű skatulyába legalább 2 szám kerül, akkor azoknak a számoknak p_i közös osztójuk lesz, így nem lehetnek relatív prímek. Mivel $n + 1$ darab skatulyám van, akárhogy választok ki ennél több számot, biztosan lesz olyan p_i jelzésű skatulya, amelybe legalább két szám kerül, így a kiválasztott számok nem lesznek relatív prímek.

Ezzel beláttuk, hogy legfeljebb $n+1$ darab szám választható ki a feladat feltételeinek megfelelően.

□

3.28. Feladat. (TK 56.) Legyenek p és q prímszámok, $3 \leq p < q$; $4 \mid p+1$; $4 \mid q+1$. Bizonyítandó, hogy $q^2 - p^2$ nem lehet négyzetszám!

Megoldás:

Mi $q-p$ és $q+p$ legnagyobb közös osztója?

$(q-p; q+p) \mid (q+p) - (q-p)$, illetve $(q-p; q+p) \mid (q-p) + (q+p)$.

Tehát $(q-p; q+p) \mid 2p$, és $(q-p; q+p) \mid 2q$, de ekkor $(q-p; q+p) \mid (2p; 2q)$.

De $(2p; 2q) = 2$, mivel p és q különböző prímek. Tehát $(q-p; q+p) \mid 2$.

Viszont $q-p$ és $q+p$ is páros, így $(q-p; q+p) = 2$.

Ekkor $(\frac{q-p}{2}; \frac{q+p}{2}) = 1$.

Tegyük fel indirekt, hogy $c^2 = q^2 - p^2$.

$c^2 = (q-p) \cdot (q+p) = 2^2 \cdot \frac{q-p}{2} \cdot \frac{q+p}{2}$.

Ez csak úgy lehet, ha $\frac{q-p}{2}$ és $\frac{q+p}{2}$ is négyzetszám, mivel relatív prímek.

Tehát $a^2 = \frac{q-p}{2}$ és $b^2 = \frac{q+p}{2}$.

Ezeket összeadva, illetve kivonva egymásból, kapjuk: $q = a^2 + b^2$ és $p = b^2 - a^2$.

Most használjuk fel, hogy $4 \mid q+1 \Leftrightarrow q \equiv\ 3\ (4)$.

De $q = a^2 + b^2$, és ismert: bármely négyzetszám 0 vagy 1 maradékot adhat 4-gyel osztva.

Tehát $a^2 + b^2$ lehetséges maradékai 4-gyel osztva: 0; 1; 2.

Ellentmondásra jutottunk, mivel $q = a^2 + b^2 \equiv\ 3\ (4)$.

Tehát $q^2 - p^2$ nem lehet négyzetszám. Ezzel beláttuk az állítást.

□

3.29. Megjegyzés. Fontos megjegyzés, hogy a feladat megoldásához nem használtuk ki mindkét oszthatóságot, tehát egy erősebb feladatot is beláttunk ezzel.

3.30. Feladat. (TK 57.) Jelöljük p_k-val a k-adik pozitív prímszámot ($p_1 = 2$; $p_2 = 3$; $p_3 = 5$; $p_4 = 7$; $p_5 = 11$; $\ldots$). Legyen $n \in \mathbb{Z}$; $n \geq 3$; $N = \frac{1}{2}(p_n + 1)$. Bizonyítandó, hogy az 1^2; 2^2; 3^2; $\ldots$; $(N-1)^2$; N^2 számok közül ki lehet választani legalább $N - n + 1$ darab különbözőt úgy, hogy a kiválasztottak közül bármely két különböző szám különbsége összetett szám legyen!

Megoldás:

A feladatban leírt $A^2 - B^2$ különbségek felírhatóak $(A - B) \cdot (A + B)$ alakban. (Feltehető: $A > B$. Ekkor $2 \leq A \leq N$.)

$(A - B) \cdot (A + B)$ mindig összetett szám, kivéve ha $A - B = 1$, mivel ha ekkor $A + B$ prím, akkor a szorzat is prím lesz. Tehát érdemes csak az $A - B = 1$ esettel foglalkozni.

Fontos megjegyzések $A - B = 1$ esetén:

1. $A - B = 1$ pontosan akkor, ha a A^2 és B^2 szomszédos négyzetszámok. ($N - 1$ darab ilyen számpár létezik, mivel $2 \leq A \leq N$.)

2. $A^2 - B^2 = (A - B) \cdot (A + B) = A + B = (A + (A - 1)) = 2A - 1$.

3. $\min(A^2 - B^2) = \min(2A - 1) = 2 \cdot 2 - 1 = 3$ és $\max(A^2 - B^2) = \max(2A - 1) = 2N - 1 = 2 \cdot \frac{1}{2}(p_n + 1) - 1 = p_n + 1 - 1 = p_n$.

4. $A^2 - B^2 = 2A - 1$ minden $3 \leq k \leq p_n$ páratlan számot pontosan egyszer vesz fel, ahol $2 \leq A \leq N$ egész. Ezek közül $n - 1$ darab prím, mivel a 2 nem fordulhat elő.

Vizsgáljuk meg sorra a szomszédos négyzetszámokat (mondjuk növekvő sorrendben)! Ha az éppen vizsgált négyzetszámok különbsége prím, dobjuk ki a listából a kettő közül a nagyobbik négyzetszámot. 4. miatt $n - 1$ darab olyan négyzetszámpár van, melyek különbsége prím. Tehát az N darab négyzetszámból legfeljebb $(n-1)$ darabot kell kivennem, hogy a megmaradó négyzetszámok különbsége ne lehessen prím. Mivel a különbség 1 nem lehet, ezért ez éppen azt jelenti, hogy ki tudok választani legalább $N-(n-1) = N-n+1$ darabot az $1^2; 2^2; 3^2; \ldots; (N-1)^2; N^2$ számok közül úgy, hogy bármely kettő különbsége összetett szám legyen. Ezzel bebizonyítottuk az állítást. $\square$

3.31. Megjegyzés. Érdekes kérdés, hogy lehet-e javítani a feladat által megadott alsó korlátot, azaz tudunk-e olyan N-től és n-től függő számot mondani, amennyi biztosan kiválasztható $1^2; 2^2; 3^2; \ldots; (N - 1)^2; N^2$ közül, hogy közülük bármely kettő különbsége összetett szám legyen.

Legyenek $2K - 1$ és $2K + 1$ ikerprímek. Vegyük észre, hogy ha K^2-et elhagyom az $1^2; 2^2; 3^2; \ldots; (N - 1)^2; N^2$ listából, akkor se $2K - 1$, se $2K + 1$ nem fog többé előállni a maradék négyzetszámok közül kettő különbségeként. Ugyanis $2K - 1 = K^2 - (K - 1)^2$ és $2K + 1 = (K + 1)^2 - K^2$, és a feladatban beláttuk, hogy minden prímszámnak egyértelmű az ilyen alakú felírása. Vagyis ikerprímenként elég csak 1 darab négyzetszámot eltörölnöm kettő helyett, ezáltal eggyel több négyzetszámot hagyhatok bent a listában, mint egyébként. Fontos megjegyezni, hogy az egyetlen "ikerprímhármas" 3;5;7 számok esetén két négyzetszámot kell elhagyni, vagyis ott 1 négyzetszámmal kevesebbet dobtam ki a háromhoz képest. ($3 = 2^2 - 1^2$ és $7 = 4^2 - 3^2$.)

A feladat $n \geq 3$ feltétele szerint $p_n \geq 5$. Ekkor egy négyzetszámmal többet tarthatok meg a 3; 5 ikerprímek miatt. A 7-tel már nem tudok újabb négyzetszámot megtartani.

Jelölje j a 7-től nagyobb, de p_n-től nem nagyobb pozitív ikerprímpárok számát, ha $n \geq 5$. $n = 3$ és $n = 4$ esetén legyen $j = 0$. Ekkor $n \geq 3$ esetén legfeljebb $N-n+1+(j+1)$, vagyis $N-n+j+2$ darab négyzetszámot tudok kiválasztani az 1^2; 2^2; 3^2; $\ldots$; $(N-1)^2$; N^2 számok közül úgy, hogy bármely kettő különbsége összetett szám legyen, és ennyit valóban kiválasztható.

3.32. Megjegyzés. A 3.31. megjegyzésben $j \geq 0$. Az eredeti feladatot akár a következő formában is feladhattuk volna: Bizonyítandó, hogy $n \geq 3$ esetén az 1^2; 2^2; 3^2; $\ldots$; $(N-1)^2$; N^2 számok közül ki lehet választani legalább $N - n + 2$ darab különbözőt úgy, hogy a kiválasztottak közül bármely két különböző szám különbsége összetett szám legyen!

3.33. Feladat. (TK 58.) A p; q; r különböző prímszámok, m; n pozitív egészek úgy, hogy az $(m+1)$-től $(m+n)$-ig terjedő egész számok egyike sem osztható a p-től, q-tól, r-től különböző prímszámmal. Legfeljebb mekkora lehet az n?

Megoldás:

Érdekesebb a feladat, ha pozitív prímekre szorítkozunk.

Minden k-adik pozitív szám osztható k-val. Ekkor ha n legalább 5, akkor van 2-vel, 3-mal, 5-tel osztható is köztük. Tehát $p = 2$; $q = 3$; $r = 5$.

Legfeljebb hány egymást követő számot sorolhatok fel, hogy mindegyiknek csak 2, 3, vagy 5 lehessen a prímosztója?

7-et biztosan nem, mivel minden hetedik egész szám osztható 7-tel.

6 darab felsorolható-e?

Nem, mivel 6 darab egymást követő szám tartalmaz $6k + 1$ és $6l + 5$ típusú számot is ($k - l = 0$ vagy $k - l = 1$). Ezek egyike sem osztható 2-vel, vagy 3-mal, így csak $5 \mid 6k + 1$ és $5 \mid 6l + 5$ lehetséges. De ekkor $5 \mid 6k + 1 - (6l + 5) \Leftrightarrow 5 \mid 6 \cdot (k - l) - 4$.

Viszont $k - l = 0$ vagy $k - l = 1$ esetén ez nem teljesül. Tehát $n < 6$.

$n = 5$ lehetséges?

Igen. Például $2, 3, 4, 5, 6$ jó. Ekkor $m = 1$; $n = 5$.

Tehát n értéke legfeljebb 5.

□

3.34. Megjegyzés. Ha a feladatban nem csak pozitív prímszámokra szorítkozunk, a megoldás a következő:

Most 2; -2; 3; -3; ... prímszámok különbözőnek tekinthetők.

Minden k-adik pozitív szám osztható k-val. Ekkor ha n legalább 3, akkor van 2-vel, -2-vel, 3-mal és -3-mal osztható is köztük. Ez ellentmondás, tehát $n \leq 2$.

$n = 2$ lehetséges?

Nem, ugyanis két szomszédos természetes szám közül az egyik páros, a másik páratlan. A párosnak osztója a 2, de ekkor -2 is. A páratlannak pedig nem osztója a 2, viszont van prímosztója, legyen például p ilyen. De ekkor $-p$ is osztó, ami ellentmondás.

Tehát n értéke legfeljebb 1 lehet, és ez meg is valósítható $m = p^k - 1$ választással, ahol p prímszám, $k \in \mathbb{Z}^+$.

3.35. Feladat. (TK 59.) Az a; b; m; n pozitív egészekről azt tudjuk, hogy az $(m + 1)$-től $(m + n)$-ig terjedő egész számok mindegyike az a és b közül legalább az egyiknek egész kitevős hatványa (a különböző számok előállításában a hatványkitevők nem szükségképpen azonosak). Legfeljebb mekkora lehet az n?

Megoldás:

A feladat megoldása előtt válaszoljunk a következő kérdésekre:

1. Mikor lehet $a^k - a^l = 1$? ($a, k, l \in \mathbb{Z}^+$, $a \geq 2$.)
2. Mikor lehet $a^k - a^l = 2$? ($a, k, l \in \mathbb{Z}^+$, $a \geq 2$.)

Először válaszoljunk az 1. kérdésre: $a^k - a^l = 1 \Rightarrow a \mid 1$. Ellentmondás, mivel $a \geq 2$.

Válaszoljunk a 2. kérdésre: $a^k - a^l = 2 \Rightarrow a \mid 2$. $a \geq 2$ miatt $a = 2$.

Tehát az a alapú és b alapú hatványok szükségképpen felváltva fognak szerepelni a sorozatban.

Ha $n \geq 4$, akkor lesz két a alapú hatvány, és lesz két b alakú hatvány a számok között. A sorrendjük az előzőek alapján: $a^e; b^f; a^g; b^h$ vagy fordítva. De ekkor $a = b = 2$ kellene, ezt pedig kizárhatjuk $a \neq b$ miatt.

Tehát $n \leq 3$. $n = 3$ pedig megvalósítható $m = 1$ választásával. Ekkor $a = 2$ és $b = 3$. ($2 = 2^1$; $3 = 3^1$; $4 = 2^2$.)

$\square$

3.36. Feladat. (TK 60.) Határozzuk meg az összes olyan k pozitív egész számot, amelyhez találhatók olyan n; m pozitív egészek, hogy
$\frac{1}{n^2} + \frac{1}{m^2} = \frac{k}{n^2+m^2}$.

Megoldás:

$\frac{1}{n^2} + \frac{1}{m^2} = \frac{k}{n^2+m^2} \Leftrightarrow \frac{m^2+n^2}{m^2n^2} = \frac{k}{n^2+m^2} \Leftrightarrow (n^2+m^2)^2 = km^2n^2$.

Átalakítva: $n^4 + 2m^2n^2 + m^4 = km^2n^2 \Leftrightarrow n^4 + (2-k) \cdot m^2n^2 + m^4 = 0$.

Ez n^2-re nézve másodfokú egyenlet m paraméterrel. A megoldóképletet felírva:

$n^2_{1;2} = \frac{(k-2)\cdot m^2 \pm \sqrt{(2-k)^2\cdot m^4 - 4m^4}}{2}$

Egy egész szám gyöke csak akkor lehet egész, ha maga a szám négyzetszám volt. Különben a gyök irracionális szám (vagy esetleg komplex).

Tehát kell: $(2-k)^2 \cdot m^4 - 4m^4$ négyzetszám.

$(2-k)^2 \cdot m^4 - 4m^4 = (k^2-4k+4)\cdot m^4 - 4m^4 = (k^2-4k)\cdot m^4 = k\cdot(k-4)\cdot m^4$.

Mivel m^4 négyzetszám, ezért elég: $k \cdot (k-4)$ négyzetszám.

Másrészt a megoldás elején található átalakításban $(n^2+m^2)^2$ és m^2n^2 négyzetszám, így k is szükségképpen négyzetszám.

Most keressünk olyan négyzetszámokat, amelyek között a különbség 4!

Mivel a négyzetszámok közti különbség folyamatosan növekszik, ezért elég az első néhány négyzetszám között keresni.

$0^2 = 0$; $1^2 = 1$; $2^2 = 4$; $3^2 = 9$; $4^2 = 16$; $5^2 = 25$; ...

Látható: csak a 4 és a 0 az egyetlen négyzetszám pár, hogy a különbségük 4.

Tehát $k = 4$ az egyetlen pozitív egész, ami mellett találhatunk megoldást.

Már csak le kell ellenőriznünk, hogy $k = 4$-hez valóban találhatók-e olyan m és n pozitív egészek, amik kielégítik a kezdeti egyenletet.

Vizsgáljuk az $n^4 + (2-k) \cdot m^2n^2 + m^4 = 0$ egyenlet megoldáshalmazát $k = 4$ esetén:

$n^4 - 2m^2n^2 + m^4 = 0 \Leftrightarrow (n^2-m^2)^2 = 0 \Leftrightarrow n^2 - m^2 = 0 \Leftrightarrow n^2 = m^2$.

Mivel n és m pozitív egészek, így ez csak akkor lehet, ha $n = m$.

Ha $n = m$ tetszőleges pozitív egészek, és $k = 4$, akkor valóban igaz, hogy $\frac{1}{n^2} + \frac{1}{n^2} = \frac{4}{2n^2} = \frac{2}{n^2}$, és csak $k = 4$ mellett találunk megoldást.

$\square$

3.37. Feladat. (TK 23.) Mutassuk meg, hogy csak *egyetlen* olyan p prímszám van, amelyre $p+1$ négyzetszám!

Megoldás: Tehát p prím, $p+1=n^2$, ahol n nemnegatív egész.
Ekkor $n^2-1=p$. Átrendezve $n^2-1=(n-1)\cdot(n+1)=p$.
Ez csak úgy lehet, ha a szorzat valamelyik tényezője egység.

I. eset: $n-1=-1$, és $n+1=+1$.
Ekkor $n=0$, $p=-1$, de -1 nem prím!

II. eset: $n-1=1$.
Ekkor $n=2$, $p=3$. Ez tényleg prím.

III. eset: $n+1=-1$
Ekkor $n=-2$, de feltettük, hogy $n\geq 0$.

Ezzel beláttuk, hogy tényleg csak egy ilyen p van, és $p=3$.
□

3.38. Feladat. (TK 26.) Legyen a pozitív egész. Mutassuk meg, hogy ha 2^a+1 prímszám, akkor $a=2^n$ (n nemnegatív egész) alakú!

Megoldás:
A következőt fogom bizonyítani: Ha a nem 2^n alakú, akkor 2^a+1 nem prím. Ebből következni fog az eredeti állítás helyessége.
Először vizsgáljuk meg a 2^a típusú számok tulajdonságait:
$2^1\equiv\ 2\ (3)$; $2^2\equiv\ 1\ (3)$; $2^3\equiv\ 2\ (3)$; $2^4\equiv\ 1\ (3)$; …
Vegyük észre a szabályosságot:
Ha a páratlan, akkor $2^a\equiv\ 2\ (3)$. Ha a páros, akkor $2^a\equiv\ 1\ (3)$.
Tehát ha a páratlan, akkor 2^a+1 osztható hárommal. Ez csak akkor prím, ha $2^a+1=3\Leftrightarrow 2^a=2\Leftrightarrow a=1=2^0$.
Érdekes eset: ha a páros. Tegyük fel, hogy a nem 2^n alakú. Ekkor $a=2^n\cdot(2k+1)$, ahol k pozitív egész. Ekkor $2k+1\geq 3$.
Ekkor $2^a+1=2^{2^n\cdot(2k+1)}+1=(2^{2^n})^{2k+1}+1^{2k+1}$. Ennek pedig valódi osztója $2^{2^n}+1$, vagyis nem prím.
Kaptuk: 2^a+1 csak akkor lehet prím, ha a 2^n alakú. Ezzel bebizonyítottam az állítást.
□

3.39. Megjegyzés. [5]

Az $F_n = 2^{2^n} + 1$ számokat Fermat-számoknak nevezzük. Azokat a Fermat-számokat pedig, amelyek prímek, Fermat-prímeknek nevezzük.

Összesen 5 Fermat-prímet ismerünk: $F_0 = 3$; $F_1 = 5$; $F_2 = 17$; $F_3 = 257$; $F_4 = 65537$.

Fermat azt sejtette, hogy minden ilyen alakú szám prímszám. Euler 1732-ben, első számelméleti cikkében megcáfolta ezt, kimutatva, hogy $641 \mid F_5$.

Ennek egy bizonyítása a következő:

Egyrészt $641 = 5^4 + 2^4$, ezért $5^4 \equiv\ -2^4\ (641)$.

Másrészt $641 = 5 \cdot 2^7 + 1$, ezért $5 \cdot 2^7 \equiv\ -1\ (641)$.

Utóbbiból következik, hogy $5^4 \cdot 2^{28} \equiv\ 1\ (641)$.

De $5^4 \equiv\ -2^4\ (641)$, így helyettesítve kapjuk:

$-2^4 \cdot 2^{28} \equiv\ 1\ (641) \Leftrightarrow 2^{32} \equiv\ -1\ (641) \Leftrightarrow 641 \mid 2^{32} + 1$.

Már több száz Fermat-számról belátták, hogy nem prím. Ma F_{11}-ig ismert a Fermat-számok teljes prímtényezős felbontása, az utána következőknek csupán néhány valódi osztója ismert. Sok esetben pedig valódi osztó sem ismert, csak belátták, hogy F_n összetett szám. Ilyenek például F_{20} és F_{24}. Máig a legnagyobb Fermat-szám, amiről belátták, hogy összetett: $F_{3329780}$, és prímosztója $193 \cdot 2^{3329782} + 1$. [6]

Bebizonyították: ha $n \geq 2$, akkor F_n minden prímosztója $p = k \cdot 2^{n+2} + 1$ alakú. ($k \in \mathbb{Z}$)

Manapság számítógépekkel keresnek bizonyítékot arra nézve, hogy egy Fermat-szám összetett. A Fermat-számok nagyon speciálisak, ugyan exponenciális a kitevő, mégis létezik rájuk egyszerű prímteszt, aminek segítségével gyorsan (polinomiális időben) el lehet dönteni egy Fermat-számról, hogy összetett-e vagy sem. Ilyen a Pépin-féle prímteszt, miszerint F_n pontosan akkor prím, ha $3^{\frac{F_n - 1}{2}} \equiv\ -1\ (F_n)$, ahol $n > 0$. [3]

Ellenőrizzük le a prímtesztet az ismert F_n $(n > 0)$ Fermat-prímekre:

$F_1 = 5$: $3^{\frac{5-1}{2}} \equiv\ -1\ (5) \Leftrightarrow 3^2 \equiv\ -1\ (5)$.

Valóban: $9 \equiv\ -1\ (5)$, mivel $9 = 2 \cdot 5 - 1$.

$F_2 = 17$: $3^{\frac{17-1}{2}} \equiv\ -1\ (17) \Leftrightarrow 3^8 \equiv\ -1\ (17)$.

Valóban: $6561 \equiv\ -1\ (17)$, mivel $6561 = 386 \cdot 17 - 1$.

$F_3 = 257$: $3^{\frac{257-1}{2}} \equiv\ -1\ (257) \Leftrightarrow 3^{128} \equiv\ -1\ (257)$.

Ezt már nehezebb ellenőrizni. Vizsgáljuk 3 kettő-hatványait:

$3^1 \equiv\ 3\ (257)$.

$3^2 \equiv\ (3^1)^2\ (257) \Leftrightarrow 3^2 \equiv\ 9\ (257)$.

$3^4 \equiv\ (3^2)^2\ (257) \Leftrightarrow 3^4 \equiv\ 81\ (257)$.

$3^8 \equiv\ (3^4)^2\ (257) \Leftrightarrow 3^8 \equiv\ -121\ (257)$.

$3^{16} \equiv (3^8)^2 \ (257) \Leftrightarrow 3^{16} \equiv -8 \ (257)$.
$3^{32} \equiv (3^{16})^2 \ (257) \Leftrightarrow 3^{32} \equiv 64 \ (257)$.
$3^{64} \equiv (3^{32})^2 \ (257) \Leftrightarrow 3^{64} \equiv -16 \ (257)$.
$3^{128} \equiv (3^{64})^2 \ (257) \Leftrightarrow 3^{128} \equiv -1 \ (257)$.

$F_4 = 65537$: $3^{\frac{65537-1}{2}} \equiv -1 \ (65537) \Leftrightarrow 3^{32768} \equiv -1 \ (65537)$.
Ellenőrizzük itt is 3 hatványaival:
$3^1 \equiv 3 \ (65537)$.
$3^2 \equiv (3^1)^2 \ (65537) \Leftrightarrow 3^2 \equiv 9 \ (65537)$.
$3^4 \equiv (3^2)^2 \ (65537) \Leftrightarrow 3^4 \equiv 81 \ (65537)$.
$3^8 \equiv (3^4)^2 \ (65537) \Leftrightarrow 3^8 \equiv 6561 \ (65537)$.
$3^{16} \equiv (3^8)^2 \ (65537) \Leftrightarrow 3^{16} \equiv -11088 \ (65537)$.
$3^{32} \equiv (3^{16})^2 \ (65537) \Leftrightarrow 3^{32} \equiv -3668 \ (65537)$.
$3^{64} \equiv (3^{32})^2 \ (65537) \Leftrightarrow 3^{64} \equiv 19139 \ (65537)$.
$3^{128} \equiv (3^{64})^2 \ (65537) \Leftrightarrow 3^{128} \equiv 15028 \ (65537)$.
$3^{256} \equiv (3^{128})^2 \ (65537) \Leftrightarrow 3^{256} \equiv 282 \ (65537)$.
$3^{512} \equiv (3^{256})^2 \ (65537) \Leftrightarrow 3^{512} \equiv 13987 \ (65537)$.
$3^{1024} \equiv (3^{512})^2 \ (65537) \Leftrightarrow 3^{1024} \equiv 8224 \ (65537)$.
$3^{2048} \equiv (3^{1024})^2 \ (65537) \Leftrightarrow 3^{2048} \equiv -8 \ (65537)$.
$3^{4096} \equiv (3^{2048})^2 \ (65537) \Leftrightarrow 3^{4096} \equiv 64 \ (65537)$.
$3^{8192} \equiv (3^{4096})^2 \ (65537) \Leftrightarrow 3^{8192} \equiv 4096 \ (65537)$.
$3^{16384} \equiv (3^{8192})^2 \ (65537) \Leftrightarrow 3^{16384} \equiv -256 \ (65537)$.
$3^{32768} \equiv (3^{16384})^2 \ (65537) \Leftrightarrow 3^{32768} \equiv -1 \ (65537)$.
Tehát az ismert Fermat-prímekre működik a prímteszt.

Ma azt sejtik a matematikusok, hogy nem létezik az ismert 5 darabon kívül más Fermat prím, vagy ha igen, akkor is csak véges sok. Ezt senki nem tudta máig bebizonyítani, és az sem biztos, hogy egyáltalán valaha be tudják látni ezt matematikai módszerekkel.

A Fermat-prímeket összefüggésbe lehet hozni a geometriával is. Gauss tétele szerint a szabályos n-szög pontosan akkor szerkeszthető euklideszi szerkesztéssel, ha n páratlan prímtényezői valamennyien Fermat-prímek és mind csak az első hatványon szerepel.

3.40. Feladat. (TK 27.) Legyen m pozitív egész. Mutassuk meg, hogy ha $2^m - 1$ prímszám, akkor m maga is prímszám!

Megoldás:

A következőt fogom bizonyítani: Ha m nem prímszám, akkor $2^m - 1$ nem prím. Ebből következni fog az eredeti állítás helyessége.

Tegyük fel ugyanis, hogy $m = a \cdot b$, ahol $a \geq 2$; $b \geq 2$, azaz m nem prím.

Ekkor $2^m - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1^b$, melynek valódi osztója $2^a - 1$. Ekkor $2^m - 1$ nem prím, ebből pedig következik az eredeti állítás helyessége.

□

3.41. Megjegyzés. [7]

Mersenne-prímeknek hívjuk azokat a prímeket, amelyek előállnak $2^m - 1$ alakban, ahol m prím.

Fontos, hogy abból, hogy m prím, nem következik, hogy $2^m - 1$ is prím. Például $2^5 - 1 = 31$ Mersenne-prím, mert 5 prím, és 31 is prím. Viszont $2^{11} - 1 = 2047$ nem prím, mivel $23 \mid 2047$.

A modern kor legnagyobb ismert prímei általában Mersenne-prímek. A ma ismert legnagyobb prímszám is Mersenne-prím, 2016. január 7-én fedezték fel, ez a $2^{74207281} - 1$ szám, és több, mint 22 millió számjegyből áll. Ez a 49. ismert Mersenne-prím.

Nem ismert, hogy véges vagy végtelen sok Mersenne-prím létezik.

Manapság a Mersenne-prímeket együttes erővel keresik hálózatba kötött számítógépek a GIMPS (Great Internet Mersenne Prime Search) projekt keretében. Ehhez bárki be tud csatlakozni saját számítógépével egy program feltelepítését követően. [8]

A Mersenne-prímek felismerésére alkalmas a Lucas-Lehmer prímteszt, miszerint adott $p > 2$ prímre pontosan akkor lesz $M_p = 2^p - 1$ is prím, ha $M_p \mid S_{p-2}$, ahol S_k az a rekurzív sorozat, ahol $S_0 = 4$ és $S_k = S_{k-1}^2 - 2$, ha $k \geq 1$. [3]

A Mersenne-prímek érdekes kapcsolatban állnak a tökéletes számokkal (Lásd: 2.15. definíció). Már Eukleidész bebizonyította, hogy minden esetben, amikor $2^n - 1$ prím, $2^{n-1} \cdot (2^n - 1)$ tökéletes szám lesz. Azonban az, hogy az összes páros tökéletes szám elő is áll ilyen alakban, nagyon sokáig csak sejtés volt. Először Euler bizonyította a XVIII. században. [9]

Máig megválaszolatlan kérdés, hogy létezik-e páratlan tökéletes szám. Így szintén nem tudjuk, hogy véges vagy végtelen sok tökéletes szám van-e. [3]

3.42. Feladat. (TK 6.) Mutassuk meg, hogy az 1-en és -1-en kívül $1+\sqrt{2}$ és $3+2\sqrt{2}$ is egység H_2-ben, sőt $\pm(1+\sqrt{2})^n$ is egység H_2-ben minden n egész kitevőre!

A feladathoz tartoznak a 2.16. és a 2.17. definíciók.

Megoldás: Először lássuk be, hogy két H_2 beli szám összege, különbsége és szorzata is H_2-beli.

$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$.
$(a+b\sqrt{2})-(c+d\sqrt{2})=(a-c)+(b-d)\sqrt{2}$.
$(a+b\sqrt{2})\cdot(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}$.
Ennek következménye, hogy $(a+b\sqrt{2})^k\in H_2$, ha $k\geq 0$ egész.
(Speciálisan $(a+b\sqrt{2})^2=(a^2+2b^2)+(2ab)\sqrt{2}$.)

Elég lenne belátni, hogy $\pm(1+\sqrt{2})^n$ egység H_2-ben, mivel ekkor 1 és -1 és $1+\sqrt{2}$ és $3+2\sqrt{2}$ is egységek lesznek, ugyanis $\pm 1=\pm(1+\sqrt{2})^0$; $1+\sqrt{2}=(1+\sqrt{2})^1$ és $3+2\sqrt{2}=(1+\sqrt{2})^2$.

Mi $(1+\sqrt{2})$ negatív kitevős hatványai?
$(1+\sqrt{2})^{-1}=\frac{1}{1+\sqrt{2}}=\frac{-1+\sqrt{2}}{(1+\sqrt{2})\cdot(-1+\sqrt{2})}=\frac{-1+\sqrt{2}}{(-1+2)+(-1+1)\sqrt{2}}=-1+\sqrt{2}$.
$(1+\sqrt{2})^{-k}=(-1+\sqrt{2})^k$.
Tehát $\pm(1+\sqrt{2})^n\in H_2$ tetszőleges n egész számra.
Kéne: tetszőleges $x,y\in\mathbb{Z}$ esetén $\frac{x+y\sqrt{2}}{\pm(1+\sqrt{2})^n}$ is H_2-beli.
$\frac{x+y\sqrt{2}}{\pm(1+\sqrt{2})^n}=\pm(x+y\sqrt{2})\cdot(1+\sqrt{2})^{-n}$.
Ez értelmes, mivel előbb láttuk: $(1+\sqrt{2})^{-n}\in H_2$ tetszőleges n egészre.

A kapott kifejezés pedig H_2-beli, mivel H_2-beli számok szorzataként áll elő. Ezzel beláttuk, hogy a feladat szövegében szereplő számok egységek H_2-ben.

□

3.43. Feladat. (Aktuális feladat) Keressük meg az összes olyan pozitív egész számot, amely a tízes számrendszerben nyolcjegyű, jegyei rendre a; b; c; d; e; f; g; h ($a\neq 0$), továbbá $a^2+b^2=6d-4c-28$; $c^2+d^2=2a-4b+33$; $e^2+f^2=6h-4g+26$; $g^2+h^2=12f-8e-59$.

Megoldás:

[TK 43.] mintájára: Az első két egyenletet összeadva kapjuk: $a^2+b^2+c^2+d^2=2a-4b-4c+6d+5$. Átrendezve: $(a-1)^2+(b+2)^2+(c+2)^2+(d-3)^2=23$. A 23 sorrendtől és egységszorzóktól eltekintve egyféleképp áll elő négy négyzetszám összegeként: $23=9+9+4+1$. Már csak a 4 tag sorrendjét kell eldönteni.

Mivel a második egyenlet jobb oldala páratlan, így c és d különböző paritásúak. De ekkor c^2+d^2 1 maradékot ad 4-gyel osztva, így $2a$ is 4-gyel osztható, mert ekkor ad a jobb oldal is 1 maradékot 4-gyel osztva. Vagyis a páros. Az első egyenlet jobb oldala páros, emiatt a és b azonos paritásúak, vagyis b is páros. Ekkor $b+2$ is az. De ekkor $(b+2)^2=4$ lehet csak. Ebből adódóan $b+2=\pm 2\Rightarrow b=0$.

$(c+2)^2 \geq 4$ miatt $(c+2)^2 = 9$ (hiszen a 4 már foglalt) $\Rightarrow c+2 = \pm 3 \Rightarrow c = 1$.

Ezeket visszaírva a második egyenletbe: $1+d^2 = 2a+33 \Leftrightarrow d^2 = 2a+32$. Mivel a páros, a értéke legalább 0, legfeljebb 8. Tehát $2a+32$ minimuma 32, maximuma 48.

Vagyis $32 \leq d^2 \leq 48$, ebből $d^2 = 36 \Rightarrow d = 6$. Ekkor $a = 2$.

Az utolsó két egyenletet összeadva kapjuk: $e^2+f^2+g^2+h^2 = -8e+12f-4g+6h-33$. Átrendezve: $(e+4)^2+(f-6)^2+(g+2)^2+(h-3)^2 = 32$. A 32 sorrendtől és egységszorzóktól eltekintve egyféleképp áll elő négy négyzetszám összegeként: $32 = 16+16+0+0$. Már csak a 4 tag sorrendjét kell eldönteni.

$(e+4)^2 \geq 16$. Ekkor $(e+4)^2 = 16$ lehet csak. Ebből $e+4 = \pm 4 \Rightarrow e = 0$.

$(g+2)^2 \geq 4$ Ekkor csak $(g+2)^2 = 16$ lehetséges. Ebből $g+2 = \pm 4 \Rightarrow g = 2$.

Maradt: $(f-6)^2 = 0 \Rightarrow f = 6$, valamint $(h-3)^2 = 0 \Rightarrow h = 3$.

Tehát a megoldást adó nyolcjegyű szám 20160623, és ez valóban kielégíti az egyenleteket.

□

3.44. Megjegyzés. A négy-négyzetszám tétel szerint minden pozitív egész felírható négy darab négyzetszám összegeként. [3]

Egy ilyen feladat konstruálásához érdemes megkeresni azokat a számokat, amelyek egyértelműen állnak elő ilyen módon.

Vizsgáljuk meg, hogy $n \geq 49$ esetén milyen számoknak lehet egyértelmű az ilyen felírása!

A három-négyzetszám tétel szerint minden pozitív egész felírható három darab négyzetszám összegeként, kivéve a $4^l \cdot (8m+7)$ alakú számok. ($l, m \geq 0$ egészek) [3]

Annak bizonyítására, hogy egy n pozitív egész szám többféleképp is felírható négy négyzetszám összegeként, azt fogjuk vizsgálni, hogy van-e négy különböző n-nél kisebb négyzetszám ($a^2, b^2, c^2, d^2 < n$), hogy $n-a^2$ és $n-b^2$ és $n-c^2$ és $n-d^2$ közül egyik sem $4^l \cdot (8m+7)$ alakú, és $a^2+b^2+c^2+d^2$-nek nem egyértelmű a négy négyzetszám összegeként való felírása.

Használjuk fel, hogy bármely páratlan négyzetszám $8k+1$ alakú, és bármely páros négyzetszám $8k+0$ vagy $8k+4$ alakú.

Most be fogjuk látni, hogy $n \geq 49$ esetén csak a $8k+0$ típusú számoknak lehet egyértelmű az ilyen felírása.

A $8k+2$ és $8k+4$ és $8k+6$ alakú számoknak nem egyértelmű az ilyen felírása, mivel 1^2 és 3^2 és 5^2 és 7^2 mellé is tudunk 3 másik négyzetszámot találni, hogy a négy négyzetszám összege kiadja n-et, mivel $n-1^2$, $n-3^2$, $n-5^2$, $n-7^2$ is páratlan, de nem $8m+7$ alakú. Így a különbség nem lehet $4^l \cdot (8m+7)$ alakú. $1^2+3^2+5^2+7^2 = 84 = 9^2+1^2+1^2+1^2$ is.

A $8k+3$ és $8k+7$ alakú számoknak sem egyértelmű az ilyen felírása, mivel 1^2 és 3^2 és 5^2 és 7^2 mellé is tudunk 3 másik négyzetszámot találni, hogy a négy négyzetszám összege kiadja n-et, mivel $n-1^2$, $n-3^2$, $n-5^2$, $n-7^2$ is páros, de néggyel nem osztható, így a különbség nem lehet $4^l \cdot (8m+7)$ alakú.

A $8k+1$ és $8k+5$ alakú számoknak sem egyértelmű az ilyen felírása, mivel 0^2 és 2^2 és 4^2 és 6^2 mellé is tudunk 3 másik négyzetszámot találni, hogy a négy négyzetszám összege kiadja n-et, mivel $n-0^2$, $n-2^2$, $n-4^2$, $n-6^2$ is páratlan, de nem $8m+7$ alakú. Így a különbség nem lehet $4^l \cdot (8m+7)$ alakú. $0^2+2^2+4^2+6^2 = 56$ pedig $8k+0$ alakú.

Tehát kaptuk: $n \geq 49$ esetén csak a $8k+0$ alakú számok között lehetnek olyanok, melyeknek négy négyzetszám összegeként való felírása egyértelmű.

Most felhasználjuk, hogy 0^2, 2^2, 4^2, 6^2 16-tal osztva 0 vagy 4 maradékot ad .

Ekkor $n > 56$ esetén a $16k+8$ alakú számoknak sem egyértelmű az ilyen felírása, mivel 0^2 és 2^2 és 4^2 és 6^2 mellé is tudunk 3 másik négyzetszámot találni, hogy a négy négyzetszám összege kiadja n-et, mivel $n-0^2$, $n-2^2$, $n-4^2$, $n-6^2$ is $16k+8$ vagy $16k+4$ alakú. Ha $16k+8$ alakú, akkor 8-cal osztható, de 16-tal nem, tehát a különbség nem lehet $4^l \cdot (8m+7)$ alakú. Ha pedig $16k+4$ alakú, akkor $4 \cdot (4k+1)$ alakú, de ez nem lehet $4^l \cdot (8m+7)$ alakú.

Tehát $n > 56$ esetén elég csak a 16-tal osztható számokat vizsgálni.

A 0 és 100 közé eső számok közül a következő számoknak egyértelmű az ilyen felírása:

$0 = 0^2+0^2+0^2+0^2$	$11 = 3^2+1^2+1^2+0^2$
$1 = 1^2+0^2+0^2+0^2$	$14 = 3^2+2^2+1^2+0^2$
$2 = 1^2+1^2+0^2+0^2$	$15 = 3^2+2^2+1^2+1^2$
$3 = 1^2+1^2+1^2+0^2$	$23 = 3^2+3^2+2^2+1^2$
$5 = 2^2+1^2+0^2+0^2$	$24 = 4^2+2^2+2^2+0^2$
$6 = 2^2+1^2+1^2+0^2$	$32 = 4^2+4^2+0^2+0^2$
$7 = 2^2+1^2+1^2+1^2$	$56 = 6^2+4^2+2^2+0^2$
$8 = 2^2+2^2+0^2+0^2$	$96 = 8^2+4^2+4^2+0^2$

4. Bevezetés a lánctörtek világába

A következő fejezeteket úgy építem fel, hogy a szakkör résztvevői úgy ismerkedjenek meg a témakörrel, hogy közben átélhessék az önálló felfedezés örömét. Ezt rávezető feladatokkal, példákkal segítem elő, majd az észrevételeket közösen matematikai formába öntjük: definíciók és tételek kimondásával. A szakkörre szánt idő végessége és az anyag mélysége miatt inkább a matematikai tények felfedeztetése és kimondása a célom, semmint a bizonyítások részletezése. A kimaradt bizonyításokat az érdeklődő diákok elolvashatják a bibliográfiában szereplő számelmélet könyvekben.

A legtöbb diák legkésőbb ötödikes korában találkozik törtekkel. Megtanulja, hogyan adjon össze vagy hogyan szorozzon össze két törtet. Azt is megtanulja, hogy hogyan kezelje az emeletes törteket, de ennél jobban nem mélyül el a témakörben. Vannak olyan problémák a matematikában, amiknek a megoldásához elengedhetetlenek a lánctörtek, emiatt vizsgáljuk a témakört. Mik azok a lánctörtek?

4.1. Definíció. Tetszőleges $x = x_0$ valós szám esetén tekintsük a következő algoritmust:

Legyen $a_0 = \lfloor x_0 \rfloor$.

Ha $x_i - a_i \neq 0$, akkor legyen $x_{i+1} = \frac{1}{x_i - a_i}$ és $a_{i+1} = \lfloor x_{i+1} \rfloor$. $(i \geq 0)$

Ekkor $x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ldots a_n + \frac{1}{x_{n+1}}}}}$.

Könnyen látható, hogy $i > 0$ esetén a_i-k pozitív egészek, és a_0 is egész.

Ha x_{n+1} egész (azaz $x_{n+1} - a_{n+1} = 0$), akkor az eljárás véget ér. Az ily módon kapott $a_0, a_1, \ldots, a_n, x_{n+1}$ egész számokat x lánctörtjegyeinek nevezzük.

A jobb oldalon álló sokemeletes törtet (véges) lánctörtnek nevezzük, és vezessük be rá a következő jelölést: $[a_0; a_1; a_2; \ldots; a_n; x_{n+1}]$.

4.2. Megjegyzés. Ha nem találunk olyan n-et, amelyre x_{n+1} egész, akkor beszélhetünk végtelen lánctörtről, de ennek értelmét majd óvatosan meg kell vizsgálnunk.

4.3. Feladat. Fejtsük lánctört alakba a következő törtet: $\frac{45}{16}$.

Megoldás:
$\frac{45}{16} = 2 + \frac{13}{16} = 2 + \frac{1}{\frac{16}{13}} = 2 + \frac{1}{1+\frac{3}{13}} = 2 + \frac{1}{1+\frac{1}{\frac{13}{3}}} = 2 + \frac{1}{1+\frac{1}{4+\frac{1}{3}}} = [2; 1; 4; 3].$

□

A diákok meglátják, hogy minden véges lánctört racionális számot reprezentál és fordítva: minden racionális számnak véges hosszú a lánctört alakja. De vajon egyértelmű-e ez a lánctört alak racionális szám esetén?

4.4. Megjegyzés. Ha nem teljesen az algoritmus szerint képezzük a lánctörtalakot, előállhat a $\frac{45}{16}$ másik lánctörtszerű alakban:
$\frac{45}{16} = 2 + \frac{1}{1+\frac{1}{4+\frac{1}{3}}} = 2 + \frac{1}{1+\frac{1}{4+\frac{1}{2+\frac{1}{1}}}} = [2; 1; 4; 2; 1].$

Itt a korábbi 3 jegyet folytattuk $2 + \frac{1}{1}$ alakban. Ez az algoritmusban nem áll elő, de szokás ezt is lánctörtnek hívni. Ebben az esetben a következő bizonyítható:

4.5. Tétel. *[2] Minden véges lánctört racionális számot reprezentál. Fordítva: minden racionális szám kifejezhető véges lánctörtként, pontosan kétféle módon.*

4.6. Definíció. Legyen $n \geq 0$-ra $r_n = [a_0; a_1; \ldots; a_n]$, akkor $r_n = \frac{h_n}{k_n}$, ahol k_n pozitív egész és a tört tovább nem egyszerűsíthető.

4.7. Feladat. Próbáljuk meg kiszámítani a következő törtek értékét:
$1;\ 1 + \frac{1}{1};\ 1 + \frac{1}{1+\frac{1}{1}};\ 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1}}};\ 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}};\ 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}}};\ \ldots$

(A szigorúan vett lánctörtalakban ez nem fordulhat elő, de most a fenti szokást követjük.)

Akár versenyt is lehet rendezni: ki tudja a legtöbb ilyen tört értékét kiszámolni 2 perc alatt? A legtöbben hamar észre veszik, hogy nem kell minden törtnél elölről kezdeni a számítást, és felhasználják a korábbi eredményeket:

$r_0 = 1 = 1$

$r_1 = 1 + \frac{1}{1} = \frac{2}{1} = 2$

$r_2 = 1 + \frac{1}{1+\frac{1}{1}} = 1 + \frac{1}{2} = \frac{3}{2} = 1,5$

$r_3 = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1}}} = 1 + \frac{1}{\frac{3}{2}} = 1 + \frac{2}{3} = \frac{5}{3} = 1,6666\ldots$

$$r_4 = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}} = 1 + \frac{1}{\frac{5}{3}} = 1 + \frac{3}{5} = \frac{8}{5} = 1,6$$

$$r_5 = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}}} = 1 + \frac{1}{\frac{8}{5}} = 1 + \frac{5}{8} = \frac{13}{8} = 1,625$$

$$r_6 = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}}}} = 1 + \frac{1}{\frac{13}{8}} = 1 + \frac{8}{13} = \frac{21}{13} = 1,615\ldots$$

$$r_7 = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}}}}} = 1 + \frac{1}{\frac{21}{13}} = 1 + \frac{13}{21} = \frac{34}{21} = 1,619\ldots$$

$\ldots$

Az egyik diák észre veszi, hogy az egyszerűsített törtek számlálója és nevezője szomszédos Fibonacci-számok lettek.

Egy másik diák a tizedestört alakot figyelte, és azt vette észre, hogy míg $r_0; r_2; r_4; r_6; \ldots$ résztörtek szigorúan monoton növő sorozatot alkotnak, addig $r_1; r_3; r_5; r_7$ résztörtek szigorúan monoton csökkenő sorozatot alkotnak. Ráadásul olyan módon, hogy az egymást követő törtek értékei egymásba skatulyázott zárt intervallumokat alkotnak.

Egy harmadik diák pedig megkérdezte ezek után, hogy vajon mi történne, ha ”végtelen sokáig” vennénk ezeket a törteket? Az értékek egyre közelednének egymáshoz, esetleg egy érték körül ingadoznak? Lesz-e határérték?

Tegyük fel, hogy értelmes a végtelenítés gondolata!

Ekkor legyen $x = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\ldots}}}}$. De ekkor $x = 1 + \frac{1}{x}$ igaz.

Tehát ha létezik x határérték, akkor teljesíti az $x^2 = x+1 \Leftrightarrow x^2-x-1 = 0$ másodfokú egyenletet. A megoldóképletet alkalmazva: $x_{1;2} = \frac{1\pm\sqrt{5}}{2}$.

Meg lehet kérdezni a szakkör résztvevőit, hogy lehet-e egyszerre két határérték. Azok, akik tanultak már egy kis analízist, rögtön rávágják, hogy nem, mert legfeljebb egy határérték lehet. A szemfülesebbek észre is veszik, hogy az $\frac{1-\sqrt{5}}{2}$ tört értéke negatív, emiatt ha van határérték, csak az $\frac{1+\sqrt{5}}{2}$ lehet. De vajon létezik-e határérték?

A válasz igen, ugyanis a Cantor-axióma szerint egymásba skatulyázott zárt intervallumok metszete nem üres. Másrészt a rendőr-elv miatt a határérték nagyobb lesz bármely páros indexű résztörtnél, de kisebb lesz bármely páratlan indexű résztörtnél. (Megjegyezzük, hogy a fentiekből is kiderül, hogy a szomszédos Fibonacci-számok hányadosa az aranymetszés számához tart.)

De mi a helyzet tetszőleges végtelen lánctört esetében? Vajon minden végtelen lánctörtnek létezik határértéke? És tetszőleges esetben hogyan lehet kiszámolni ügyesen a résztörtjeit?

4.8. Feladat. Nézzük például a következő lánctörtet: $[1; 2; 3; 4; 5; 6; 7; \ldots]$. Vajon konvergens? Vajon igaz rá, amiket az előző példánál megállapítottunk?

Rendezzünk ismét versenyt: számítsák ki a diákok a résztörteket. Ki tudja 2 percen belül a legtöbb résztörtet kiszámítani?

Látszik, hogy a 3 perc elteltével a diákok sokkal kevesebb résztörtet tudtak kiszámítani, mint az első esetben, mivel itt nem vettek észre olyan ismétlődést. Így a következő törtnél nem tudták az előző eredményeit felhasználni.

A szakkör résztvevői valahogy így kezdhettek neki:

$r_0 = 1 = 1$

$r_1 = 1 + \frac{1}{2} = \frac{3}{2} = 1,5$

$r_2 = 1 + \frac{1}{2+\frac{1}{3}} = 1 + \frac{1}{\frac{7}{3}} = 1 + \frac{3}{7} = \frac{10}{7} = 1,428571\ldots$

$r_3 = 1+\frac{1}{2+\frac{1}{3+\frac{1}{4}}} = 1+\frac{1}{2+\frac{1}{\frac{13}{4}}} = 1+\frac{1}{2+\frac{4}{13}} = 1+\frac{1}{\frac{30}{13}} = 1+\frac{13}{30} = \frac{43}{30} = 1,433333\ldots$

$r_4 = 1 + \frac{1}{2+\frac{1}{3+\frac{1}{4+\frac{1}{5}}}} = 1 + \frac{1}{2+\frac{1}{3+\frac{1}{\frac{21}{5}}}} = 1 + \frac{1}{2+\frac{1}{3+\frac{5}{21}}} = 1 + \frac{1}{2+\frac{1}{\frac{68}{21}}} = 1 + \frac{1}{2+\frac{21}{68}} = 1 + \frac{1}{\frac{157}{68}} = 1 + \frac{68}{157} = \frac{225}{157} = 1,433121\ldots$

$r_5 = 1 + \frac{1}{2+\frac{1}{3+\frac{1}{4+\frac{1}{5+\frac{1}{6}}}}} = 1 + \frac{1}{2+\frac{1}{3+\frac{1}{4+\frac{1}{\frac{31}{6}}}}} = 1 + \frac{1}{2+\frac{1}{3+\frac{1}{4+\frac{6}{31}}}} = 1 + \frac{1}{2+\frac{1}{3+\frac{1}{\frac{130}{31}}}} = 1+\frac{1}{2+\frac{1}{3+\frac{31}{130}}} = 1+\frac{1}{2+\frac{1}{\frac{421}{130}}} = 1+\frac{1}{2+\frac{130}{421}} = 1+\frac{1}{\frac{972}{421}} = 1+\frac{421}{972} = \frac{1393}{972} = 1,433127\ldots$

A leggyorsabb diák az ötödik közelítő törtig jut el legfeljebb, mivel a számítások minden résztörtnél egyre hosszabbak.

Viszont a szakkör résztvevői itt is érzik, hogy a résztörtekből álló sorozat konvergens lesz, és igaz, hogy $r_0; r_2; r_4; \ldots$ résztörtek szigorúan monoton növő, $r_1; r_3; r_5; \ldots$ résztörtek szigorúan monoton csökkenő sorozatot alkotnak.

Ezek után mondjuk ki együtt:

4.9. Tétel. *[2] A 4.6. definícióban definiált r_n értékek kielégítik az $r_0 < r_2 < r_4 < r_6 < \ldots \quad \ldots < r_7 < r_5 < r_3 < r_1$ végtelen egyenlőtlenségláncot. Szavakkal: a páros indexű r_n-ek növekvő sorozatot alkotnak, és minden r_{2n} kisebb, mint bármely r_{2j-1}. Továbbá: $\lim\limits_{n\to\infty} r_n$ létezik és minden $j \geq 0$-ra $r_{2j} < \lim\limits_{n\to\infty} r_n < r_{2j+1}$.*

4.10. Tétel. *[2] Minden $[a_0; a_1; a_2; \ldots]$ végtelen lánctört értéke irracionális.*

4.11. Tétel. *[2] Különböző végtelen lánctörtek különböző értékhez konvergálnak.*

Összefoglalás [2] Bármely x valós irracionális szám egyértelműen felírható – a 4.1. definícióban adott eljárással – $[a_0; a_1; a_2; \ldots]$ végtelen lánctörtként. Megfordítva: bármely $[a_0; a_1; a_2; \ldots]$ végtelen lánctört, amelyben a_i minden $i > 0$-ra pozitív egész, irracionális számot reprezentál. Az $[a_0; a_1; a_2; \ldots; a_n]$ véges lánctörtet az x n-edik szeletének nevezzük; e lánctört értéke: $\frac{h_n}{k_n}$. $n = 0; 2; 4; \ldots$-ra ezek a szeletek monoton növekvő sorozatot alkotnak, amelynek határértéke x. Hasonlóan $n = 1; 3; 5; \ldots$-re a megfelelő szeletek monoton csökkenő sorozatot alkotnak, ugyancsak x határértékkel. A szeletek k_n nevezője $n > 0$-ra pozitív egész számokból álló növekvő sorozat. Végül, ha az x_i-t a 4.6. definíció szerint definiáljuk, akkor $[a_0; a_1; \ldots] = [a_0; a_1; \ldots; a_{n-1}; x_n]$ és $x_n = [a_n; a_{n+1}; a_{n+2}; \ldots]$.

4.12. Megjegyzés. Felmerül a kérdés, hogy hogyan lehetett volna a 4.8. feladatban kiszámolt $\frac{h_n}{k_n}$ szeleteket egyszerűbb módon meghatározni. Erre szolgál a következő tétel:

4.13. Tétel. *[3] Legyenek $a_0; a_1; a_2; \ldots$ egész számok az x lánctörtjegyei. Ekkor h_i és k_i értékei rekurzívan kaphatóak a következő sorozatból:*

$h_0 = a_0$; $h_1 = a_0 \cdot a_1 + 1$; $h_i = a_i \cdot h_{i-1} + h_{i-2}$, ha $i \geq 2$,

$k_0 = 1$; $k_1 = a_1$; $k_i = a_i \cdot k_{i-1} + k_{i-2}$, ha $i \geq 2$.

(Felhasználtuk, hogy $r_0 = \frac{h_0}{k_0} = a_0 = \frac{a_0}{1}$ és $r_1 = \frac{h_1}{k_1} = a_0 + \frac{1}{a_1} = \frac{a_0 \cdot a_1 + 1}{a_1}$. Ebből kaptuk h_0; k_0; h_1; k_1 értékeit.)

4.14. Megjegyzés. [2] Akit nem zavarnak a negatív indexek, az nyugodtan használhatja h_i és k_i értékeinek meghatározására a következő rekurziót is:

$h_{-2} = 0$; $h_{-1} = 1$; $h_i = a_i \cdot h_{i-1} + h_{i-2}$, ha $i \geq 0$,

$k_{-2} = 1$; $k_{-1} = 0$; $k_i = a_i \cdot k_{i-1} + k_{i-2}$, ha $i \geq 0$.

4.15. Feladat. Most próbáljuk meg a 4.13. tétel alapján megcsinálni a 4.8. feladatot:

Tehát $h_{-2} = 0$; $h_{-1} = 1$; $k_{-2} = 1$; $k_{-1} = 0$ és $r_i = \frac{h_i}{k_i} = \frac{a_i \cdot h_{i-1} + h_{i-2}}{a_i \cdot k_{i-1} + k_{i-2}}$, ha $i \geq 0$.

Ez alapján keressük $[1; 2; 3; 4; 5; 6; 7; \ldots]$ szeleteit.

$r_0 = \frac{1}{1}$.

$r_1 = \frac{1\cdot 2+1}{2} = \frac{3}{2}$.
$r_2 = \frac{3\cdot 3+1}{3\cdot 2+1} = \frac{10}{7}$.
$r_3 = \frac{4\cdot 10+3}{4\cdot 7+2} = \frac{43}{30}$.
$r_4 = \frac{5\cdot 43+10}{5\cdot 30+7} = \frac{225}{157}$.
$r_5 = \frac{6\cdot 225+43}{6\cdot 157+30} = \frac{1393}{972}$.
$\dots$
Látható: a rekurzióval sokkal egyszerűbben megkaphatóak a szeletek.

4.16. Feladat. Próbáljuk meg **számológép** segítségével megkeresni a $\sqrt[3]{2}$ lánctört alakjának első 7 lánctörtjegyét (a_6-ig)!
$x = x_0 = \sqrt[3]{2} = 1,2599\dots$
$a_0 = \lfloor x_0 \rfloor = 1$.
$x_1 = \frac{1}{x_0 - a_0} = 3,8473\dots$ és $a_1 = \lfloor x_1 \rfloor = 3$.
$x_2 = \frac{1}{x_1 - a_1} = 1,1801\dots$ és $a_2 = \lfloor x_2 \rfloor = 1$.
$x_3 = \frac{1}{x_2 - a_2} = 5,5497\dots$ és $a_3 = \lfloor x_3 \rfloor = 5$.
$x_4 = \frac{1}{x_3 - a_3} = 1,8190\dots$ és $a_4 = \lfloor x_4 \rfloor = 1$.
$x_5 = \frac{1}{x_4 - a_4} = 1,2209\dots$ és $a_5 = \lfloor x_5 \rfloor = 1$.
$x_6 = \frac{1}{x_5 - a_5} = 4,5264\dots$ és $a_6 = \lfloor x_6 \rfloor = 4$.
Tehát $\sqrt[3]{2} = [1;3;1;5;1;1;4;\dots]$.

5. Periodikus lánctörtek és Pell-egyenletek

5.1. Definíció. Az $[a_0; a_1; a_2; \dots]$ végtelen lánctörtről akkor mondjuk, hogy *periodikus*, ha van olyan n egész szám, hogy $a_r = a_{n+r}$ minden elég nagy r egészre. Tehát egy periodikus lánctörtet a következő alakban lehet felírni:
$[b_0; b_1; b_2; \dots; b_j; a_0; a_1; \dots; a_{n-1}; a_0; a_1; \dots; a_{n-1}; \dots] =$
$= [b_0; b_1; b_2; \dots; b_j; \overline{a_0; a_1; \dots; a_{n-1}}]$, ahol az $a_0; a_1; \dots; a_{n-1}$ fölötti vonal azt jelenti, hogy ezt az egész számokból álló együttest végtelenül sokszor kell ismételni. Például $[\overline{1;3}]$ jelöli az $[1;3;1;3;1;3;\dots]$-et; ennek értékét könnyen ki lehet számítani. Ha az $[\overline{1;3}]$-at x-el jelöljük, akkor $x = 1 + \frac{1}{3+\frac{1}{x}}$.

Ebből: $x = 1 + \frac{1}{\frac{3x+1}{x}} \Leftrightarrow x = 1 + \frac{x}{3x+1} \Leftrightarrow x \cdot (3x+1) = 3x + 1 + x \Leftrightarrow 3x^2 + x = 4x + 1 \Leftrightarrow 3x^2 - 3x - 1 = 0$. Ebből $x_{1;2} = \frac{3 \pm \sqrt{21}}{6}$. A negatív gyököt kizárhatjuk, tehát $x = \frac{3+\sqrt{21}}{6}$.

5.2. Feladat. Számítsuk ki $[2;1;\overline{1;3}]$ értékét is!

Az előzőekből $[2;1;\overline{1;3}] = 2 + \frac{1}{1+\frac{1}{x}}$, ahol $x = \frac{3+\sqrt{21}}{6}$.

$2 + \frac{1}{1+\frac{1}{x}} = 2 + \frac{1}{\frac{x+1}{x}} = 2 + \frac{x}{x+1} = 2 + \frac{\frac{3+\sqrt{21}}{6}}{\frac{3+\sqrt{21}}{6}+1} = 2 + \frac{\frac{3+\sqrt{21}}{6}}{\frac{9+\sqrt{21}}{6}} = 2 + \frac{3+\sqrt{21}}{9+\sqrt{21}}$.

Ezt bővítve a nevező konjugáltjával:

$2+\frac{3+\sqrt{21}}{9+\sqrt{21}} = 2 + \frac{(3+\sqrt{21})\cdot(9-\sqrt{21})}{(9+\sqrt{21})\cdot(9-\sqrt{21})} = 2 + \frac{27-21-3\cdot\sqrt{21}+9\cdot\sqrt{21}}{81-21} = 2 + \frac{6+6\cdot\sqrt{21}}{60} = 2 + \frac{1+\sqrt{21}}{10} = \frac{21+\sqrt{21}}{10}$.

A példák után a szakkör résztvevői már sejtik, hogy a periodikus lánctörtek milyen alakúak, így ezt fogalmazzuk meg tétel formájában:

5.3. Tétel. *[2] Bármely periodikus lánctört kvadratikus irracionális szám, és viszont. (Kvadratikus számoknak mondjuk az $\frac{a+\sqrt{b}}{c}$ alakú számokat, ahol a; b; c egész, és $b > 0$, $c \neq 0$).*

5.4. Megjegyzés. Ebből következően a $\sqrt{d}$ alakú számok is periodikusak, ahol d nem négyzetszám.

5.5. Feladat. Határozzuk meg a következő számok lánctörtalakját számológép nélkül: $\sqrt{50}$; $\sqrt{38}$.

Az algoritmus szerint $a_0 = \left[\sqrt{50}\right] = 7$. $x_0 = \frac{1}{\sqrt{50}-7} = \frac{\sqrt{50}+7}{(\sqrt{50}-7)\cdot(\sqrt{50}+7)} = \frac{\sqrt{50}+7}{50-49} = 14+(\sqrt{50}-7)$. Látszik, hogy találtunk egy periódust, mivel $\sqrt{50}-7$ újra előfordult. Így $\sqrt{50} = [7;\overline{14}]$.

Hasonlóan $\sqrt{38}$-ra:

$a_0 = \left[\sqrt{38}\right] = 6$. $x_0 = \frac{1}{\sqrt{38}-6} = \frac{\sqrt{38}+6}{(\sqrt{38}-6)\cdot(\sqrt{38}+6)} = \frac{\sqrt{38}+6}{2}$.

$a_1 = \left[\frac{\sqrt{38}+6}{2}\right] = 6$. $x_1 = \frac{1}{\frac{\sqrt{38}+6}{2}-6} = \frac{2}{\sqrt{38}-6} = \frac{2\cdot(\sqrt{38}+6)}{(\sqrt{38}-6)\cdot(\sqrt{38}+6)} = \frac{2\cdot(\sqrt{38}+6)}{2}$.

Ezt érdemes egyszerűsíteni: $\frac{2\cdot(\sqrt{38}+6)}{2} = \sqrt{38}+6 = 12+(\sqrt{38}-6)$. Mivel $\sqrt{38}-6$ újra előfordult, periódust találtunk, így $\sqrt{38} = [6;\overline{6;12}]$.

Legyen házi feladat az informatika szakkörösök számára egy olyan számítógépes program írása, amely kiszámolja 20 lánctörtjegyig $\sqrt{d}$ lánctörtalakját azon $1 < d < 100$ egészekre, ahol d nem négyzetszám. A többieknek házi feladat számológéppel kiszámítani $\sqrt{50}$ és $\sqrt{38}$ első 15 lánctörtjegyét, papírra leírni, majd összehasonlítani a szakkörön közösen kiszámolt lánctört alakkal.

Következő órán bemutatták a diákok az eredményeiket.

Az egyik diák számológéppel számolt a következő módon: mindig kivonta a szám egészrészét, és a kapott eredmény reciprokát vette. Ő a következő lánctört alakokat kapta:

$\sqrt{38} = [6; 6; 12; 6; 12; 6; 12; 6; 1; 1; 2; 1; 1; 4; 4; \ldots]$.

$\sqrt{50} = [7; 14; 14; 14; 14; 14; 10; 1; 2; 2; 1; 2; 2; 1; 1; \ldots]$.

Egy másik diák írt egy számítógépes programot, amely a 4.1. algoritmust használja. A program kimenete a következő oldali ábrán látható.

A diákok látják, hogy $\sqrt{38}$-nak és $\sqrt{50}$-nek a szakkörön kiszámolt lánctörtalakja, a számológéppel kiszámolt lánctörtalakja, és a számítógéppel kiszámolt lánctört alakja is különböző. De akkor melyiknek hihetnek? Vajon a szakkörön számoltuk el, vagy a számológép állítódott el, vagy a program hibás?

A szakkörön mindent jól számoltunk, a számológép jól működik és jó gombokat is nyomott le a diák a házi feladat megoldásakor. A program pedig nem elvi hibás. Akkor mi lehet a probléma?

Ahhoz, hogy megértsék a diákok, hogy digitális eszközökkel számított eredmény miért megbízhatatlan jelen formában, érdemes a gépi számábrázolással megismertetni őket.

Minden digitális eszköz $\pm m \cdot 2^k$ alakban tárolja a számokat (m a mantissza, k a karakterisztika; $m \in \mathbb{Z}^+$; $k \in \mathbb{Z}$). m és k lehetséges értékei alulról és felülről is korlátosak, ezek előre adottak, az eszköz pontosságának mérőeszköze. Tehát az eszközök meghatározott pontossággal tudnak számolni, és ha nem gépi számmal kell számolniuk (hiszen egyik irracionális szám se $\pm m \cdot 2^k$ alakú), akkor az input szám helyett a hozzá legközelebb eső gépi számmal számol. Ezt a jelenséget hívjuk numerikus hibának. Az egészrész levonása után kapott $[0; 1)$-beli tényleges érték és a hozzá legközelebb eső gépi szám között ugyan lehet, hogy kicsi a különbség, de a reciprokuk között már sokkal nagyobb különbségek lesznek. Ráadásul a két lépést iteráljuk: az egészrészt levonjuk és az így kapott szám reciprokát vesszük egymás után. Így pár iteráció után teljesen hibás értékek keletkezhetnek.

Mit tudunk csinálni, hogy kiküszöböljük a numerikus hibákat?

Módosítsunk a program algoritmusán: a program számoljon formálisan $\frac{m+b\cdot\sqrt{d}}{c}$ alakú számokkal ($m; b; c; d$ egészek, d adott, pozitív és nem négyzetszám, $c \neq 0$, valamint a törtet minden lépésben tovább nem egyszerűsíthető alakban adjuk meg. A program számoljon úgy, mint ahogy mi számoltunk számológép nélkül lánctörtalakot: egy iterációban két lépést hajtunk végre: kivonjuk a szám egészrészét, és vesszük az így kapott érték reciprokát. Az

```
C:\Users\Elitebook\Documents\Szakdoga\prog\numhiba\main.exe
sqrt(2)=[1;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2;...]
sqrt(3)=[1;1;2;1;2;1;2;1;2;1;2;1;2;1;2;1;2;1;2;1;...]
sqrt(5)=[2;4;4;4;4;4;4;4;4;4;4;4;4;2;1;10;2;1;7;8;...]
sqrt(6)=[2;2;4;2;4;2;4;2;4;2;4;2;4;2;4;2;2;1;48;2;...]
sqrt(7)=[2;1;1;1;4;1;1;1;4;1;1;1;4;1;1;1;4;1;1;1;...]
sqrt(8)=[2;1;4;1;4;1;4;1;4;1;4;1;4;1;4;1;4;1;4;1;...]
sqrt(10)=[3;6;6;6;6;6;6;6;6;6;7;1;1;1;10;5;16;1;16;12;...]
sqrt(11)=[3;3;6;3;6;3;6;3;6;3;6;3;6;6;1;1;2;2;43;2;...]
sqrt(12)=[3;2;6;2;6;2;6;2;6;2;6;2;6;2;5;33;1;3;1;1;...]
sqrt(13)=[3;1;1;1;1;6;1;1;1;1;6;1;1;1;1;6;1;1;1;1;...]
sqrt(14)=[3;1;2;1;6;1;2;1;6;1;2;1;6;1;2;1;6;1;2;1;...]
sqrt(15)=[3;1;6;1;6;1;6;1;6;1;6;1;6;1;6;1;6;1;8;1;...]
sqrt(17)=[4;8;8;8;8;8;8;8;8;7;3;1;1;1;1;1;1;6;2;1;...]
sqrt(18)=[4;4;8;4;8;4;8;4;8;4;7;1;1;8;2;3;1;1;3;4;...]
sqrt(19)=[4;2;1;3;1;2;8;2;1;3;1;2;8;2;1;3;1;2;9;12;...]
sqrt(20)=[4;2;8;2;8;2;8;2;8;2;8;2;8;1;2;5;5;1;3;17;...]
sqrt(21)=[4;1;1;2;1;1;8;1;1;2;1;1;8;1;1;2;1;1;8;1;...]
sqrt(22)=[4;1;2;4;2;1;8;1;2;4;2;1;8;1;2;4;2;1;9;2;...]
sqrt(23)=[4;1;3;1;8;1;3;1;8;1;3;1;8;1;3;1;8;1;3;1;...]
sqrt(24)=[4;1;8;1;8;1;8;1;8;1;8;1;8;1;8;1;5;1;23;1;...]
sqrt(26)=[5;10;10;10;10;10;10;10;7;4;1;6;83;1;12;2;3;11;1;1;...]
sqrt(27)=[5;5;10;5;10;5;10;5;10;4;1;11;3;2;4;8;2;1;1;1;...]
sqrt(28)=[5;3;2;3;10;3;2;3;10;3;2;3;10;2;1;3;3;1;25;3;...]
sqrt(29)=[5;2;1;1;2;10;2;1;1;2;10;2;1;1;2;10;2;1;1;2;...]
sqrt(30)=[5;2;10;2;10;2;10;2;10;2;10;2;10;1;2;4;1;1;11;2;...]
sqrt(31)=[5;1;1;3;5;3;1;1;10;1;1;3;5;3;1;1;10;1;1;7;...]
```

```
C:\Users\Elitebook\Documents\Szakdoga\prog\numhiba\main.exe
sqrt(32)=[5;1;1;1;10;1;1;1;10;1;1;1;10;1;1;1;10;1;1;1;...]
sqrt(33)=[5;1;2;1;10;1;2;1;10;1;2;1;10;1;2;1;10;1;2;1;...]
sqrt(34)=[5;1;4;1;10;1;4;1;10;1;4;1;10;1;4;1;10;1;55;1;...]
sqrt(35)=[5;1;10;1;10;1;10;1;10;1;10;1;10;1;11;23;1;5;2;1;...]
sqrt(37)=[6;12;12;12;12;12;12;12;1;1;2;3;1;1;8;3;5;1;19;1;...]
sqrt(38)=[6;6;12;6;12;6;12;6;11;1;3;1;1;1;1;3;1;36;1;2;...]
sqrt(39)=[6;4;12;4;12;4;12;4;12;4;38;3;2;4;1;4;2;9;2;92;...]
sqrt(40)=[6;3;12;3;12;3;12;3;12;3;15;3;5;10;8;2;8;24;15;1;...]
sqrt(41)=[6;2;2;12;2;2;12;2;2;12;2;2;12;2;1;5;1;7;1;1;...]
sqrt(42)=[6;2;12;2;12;2;12;2;12;2;12;2;288;1;5;1;1;3;7;2;...]
sqrt(43)=[6;1;1;3;1;5;1;3;1;1;12;1;1;3;1;5;1;3;1;1;...]
sqrt(44)=[6;1;1;1;2;1;1;1;12;1;1;1;2;1;1;1;12;1;1;1;...]
sqrt(45)=[6;1;2;2;2;1;12;1;2;2;2;1;12;1;2;2;2;1;13;9;...]
sqrt(46)=[6;1;3;1;1;2;6;2;1;1;3;1;12;1;3;1;1;2;6;2;...]
sqrt(47)=[6;1;5;1;12;1;5;1;12;1;5;1;12;1;5;1;11;1;1;1;...]
sqrt(48)=[6;1;12;1;12;1;12;1;12;1;12;1;12;1;10;16;1;8;8;3;...]
sqrt(50)=[7;14;14;14;14;14;14;11;1;1;6;2;1;7;262;1;7;3;4;2;...]
sqrt(51)=[7;7;14;7;14;7;14;7;20;8;39;5;5;7;4;2;6;1;1;1;...]
sqrt(52)=[7;4;1;2;1;4;14;4;1;2;1;4;14;4;1;3;7;1;5;3;...]
sqrt(53)=[7;3;1;1;3;14;3;1;1;3;14;3;1;1;3;14;1;4;2;1;...]
sqrt(54)=[7;2;1;6;1;2;14;2;1;6;1;2;14;2;1;6;1;1;2;1;...]
sqrt(55)=[7;2;2;2;14;2;2;2;14;2;2;2;14;2;2;1;1;6;1;22;...]
sqrt(56)=[7;2;14;2;14;2;14;2;14;2;14;2;2;1;1;15;1;6;2;1;...]
sqrt(57)=[7;1;1;4;1;1;14;1;1;4;1;1;14;1;1;4;1;1;14;1;...]
sqrt(58)=[7;1;1;1;1;1;1;14;1;1;1;1;1;1;14;1;1;1;1;1;...]
sqrt(59)=[7;1;2;7;2;1;14;1;2;7;2;1;14;1;2;7;1;1;2;9;...]
```

egészrész levonása után is $\frac{m+b\cdot\sqrt{d}}{c}$ alakú szám marad módosított m és b értékekkel, illetve a reciprok vétele után ügyeskedjünk a nevező gyöktelenítésének módszerével (bővítünk a nevező konjugáltjának (-1)-szeresével, majd egyszerűsítsünk, ha tudunk). Így minden iteráció után valamilyen $\frac{m+b\cdot\sqrt{d}}{c}$ alakú számot kapunk. A program az algoritmus futása során végig csak m; b; c; d értékeket tárolja, ahol d adott, m; b; c pedig minden lépés után változik.

Ezzel elkerültük, hogy a számítógép irracionális számokkal számoljon. Ha így írjuk meg a programot, a lánctört alakban végig pontos értékeket kapunk.

Az informatika szakkörösök számára házi feladat a programot így átírni. A program keresse meg a legrövidebb periódust is és írja ki a periódushosszat.

Egy kis segítséget nyújt legrövidebb periódus kereséséhez az alábbi tétel:

5.6. Tétel. *[2]*

Ha a d pozitív egész és nem négyzetszám, akkor a $\sqrt{d}$ lánctört-kifejtésének alakja: $\sqrt{d} = [a_0; \overline{a_1; a_2; \ldots; a_{r-1}; 2a_0}]$, ahol $a_0 = \left[\sqrt{d}\right]$. Továbbá, ha $x_0 = \sqrt{d}$, $c_0 = 1$, $m_0 = 0$, úgy az egyszerűsített törtben $|c_i|$ akkor és csak akkor egyenlő 1-gyel, ha $r \mid i$. Itt r a $\sqrt{d}$ kifejtésében a legrövidebb periódus hosszát jelöli, m_i és c_i pedig az előbb leírt $\frac{m+b\cdot\sqrt{d}}{c}$-beli m és c értékek az egyes iterációk után az egyszerűsített törtben.

Ahhoz, hogy bemutathassam a lánctörtek gyakorlati alkalmazásait, egy kicsit látszólag kezdjünk el mással foglalkozni:

5.7. Definíció. (Pell-egyenletek) Pell-egyenletnek az $x^2 - dy^2 = 1$ alakú diofantikus egyenletet nevezünk, ahol a d (rögzített) pozitív egész és nem négyzetszám.

Kérdezzük meg a szakkör résztvevőit, tudnak-e kapásból megoldást adni egy ilyen egyenletre. Szinte mindenki látja, hogy $x = \pm 1$, $y = 0$ megoldása az egyenletnek. Ezeket hívjuk az egyenlet triviális megoldásainak. De van-e az egyenletnek nemtriviális (azaz ezektől eltérő) megoldása?

Alakítsuk szorzattá a Pell-egyenlet bal oldalát:

$(x + y \cdot \sqrt{d}) \cdot (x - y \cdot \sqrt{d}) = 1.$

Ebből következik, hogy ha x és y megoldása a Pell-egyenletnek, akkor az $a + b \cdot \sqrt{d}$ alakú számok körében (a és b egészek), az $x + y \cdot \sqrt{d}$ és $x - y \cdot \sqrt{d}$ számok osztói az 1-nek, így mindketten egységek. Mivel egy egység tetszőleges hatványa is egység, ezért ha létezik egy $\epsilon \neq \pm 1$ egység, akkor az ϵ hatványai végtelen sok egységet adnak. Ez azt jelenti, hogy ha létezik a Pell-egyenletnek nemtriviális megoldása, akkor végtelen sok megoldás van. [3]

5.8. Tétel. *[2] Legyen d olyan pozitív egész, amely nem négyzetszám. Ekkor az $x^2 - dy^2 = 1$ Pell-egyenletnek végtelen sok megoldása van.*

5.9. Megjegyzés. Ez azt jelenti, hogy az $x^2 - dy^2 = 1$ Pell-egyenletnek van ($x + y \cdot \sqrt{d}$; $x, y > 0$ értelemben) legkisebb pozitív megoldása. Ezt a megoldást az egyenlet alapmegoldásának is szokták nevezni.

5.10. Tétel. *[3] Legyen d olyan pozitív egész, amely nem négyzetszám, és x_0, y_0 az $x^2 - dy^2 = 1$ Pell-egyenletnek az a(z egyértelműen meghatározott) megoldása, amelyre $x_0 > 0$, $y_0 > 0$ és $x_0 + y_0 \cdot \sqrt{d}$ minimális. Ekkor az összes megoldást a következő képlettel megadott x és y egész számpárok adják:*
$x + y \cdot \sqrt{d} = \pm(x_0 + y_0 \cdot \sqrt{d})^n$, $n = 0; \pm 1; \pm 2; \ldots$

Ezek szerint ha tudnánk a Pell-egyenlet legkisebb pozitív megoldását, akkor az összeset tudnánk. De hogyan találjuk meg a legkisebb pozitív megoldást? Erről szól a következő tétel:

5.11. Tétel. *[2], [4] Az $x^2 - dy^2 = 1$ egyenlet minden pozitív megoldása megtalálható az $x = h_n$, $y = k_n$ értékek között, ahol a $\frac{h_n}{k_n}$ számok $\sqrt{d}$ kifejtésének szeletei. Legyen a $\sqrt{d}$ kifejtésének periódusa r. Az $x^2 - dy^2 = 1$ összes pozitív megoldását az $x = h_{nr-1}$, $y = k_{nr-1}$ értékek adják, ahol $n = 1; 2; 3; \ldots$, ha r páros és $n = 2; 4; 6; \ldots$, ha r páratlan.*

5.12. Megjegyzés. Ezek szerint az $x^2 - dy^2 = 1$ Pell-egyenlet alapmegoldása $x = h_{r-1}$, $y = k_{r-1}$, ha r páros és $x = h_{2r-1}$, $y = k_{2r-1}$, ha r páratlan.

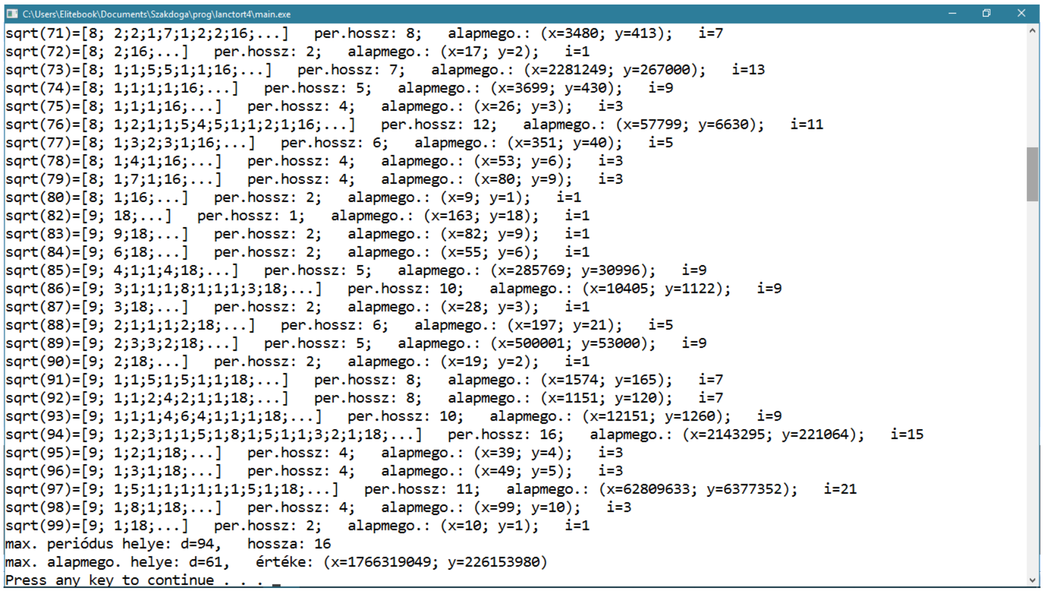
Házi feladat az informatika szakkörösök számára a programot olyan módon továbbfejleszteni, hogy kiírja az $x^2 - dy^2 = 1$ Pell-egyenlet alapmegoldását is, illetve azt is, hogy hanyadik $\frac{h_n}{k_n}$ szelet adta az alapmegoldást $\sqrt{d}$ lánctörtalakjából.

A program általam megírt változatának outputja a következő oldalakon megtalálható.

```
C:\Users\Elitebook\Documents\Szakdoga\prog\lanctort4\main.exe
sqrt(2)=[1; 2;...]   per.hossz: 1;   alapmego.: (x=3; y=2);   i=1
sqrt(3)=[1; 1;2;...]   per.hossz: 2;   alapmego.: (x=2; y=1);   i=1
sqrt(5)=[2; 4;...]   per.hossz: 1;   alapmego.: (x=9; y=4);   i=1
sqrt(6)=[2; 2;4;...]   per.hossz: 2;   alapmego.: (x=5; y=2);   i=1
sqrt(7)=[2; 1;1;1;4;...]   per.hossz: 4;   alapmego.: (x=8; y=3);   i=3
sqrt(8)=[2; 1;4;...]   per.hossz: 2;   alapmego.: (x=3; y=1);   i=1
sqrt(10)=[3; 6;...]   per.hossz: 1;   alapmego.: (x=19; y=6);   i=1
sqrt(11)=[3; 3;6;...]   per.hossz: 2;   alapmego.: (x=10; y=3);   i=1
sqrt(12)=[3; 2;6;...]   per.hossz: 2;   alapmego.: (x=7; y=2);   i=1
sqrt(13)=[3; 1;1;1;1;6;...]   per.hossz: 5;   alapmego.: (x=649; y=180);   i=9
sqrt(14)=[3; 1;2;1;6;...]   per.hossz: 4;   alapmego.: (x=15; y=4);   i=3
sqrt(15)=[3; 1;6;...]   per.hossz: 2;   alapmego.: (x=4; y=1);   i=1
sqrt(17)=[4; 8;...]   per.hossz: 1;   alapmego.: (x=33; y=8);   i=1
sqrt(18)=[4; 4;8;...]   per.hossz: 2;   alapmego.: (x=17; y=4);   i=1
sqrt(19)=[4; 2;1;3;1;2;8;...]   per.hossz: 6;   alapmego.: (x=170; y=39);   i=5
sqrt(20)=[4; 2;8;...]   per.hossz: 2;   alapmego.: (x=9; y=2);   i=1
sqrt(21)=[4; 1;1;2;1;1;8;...]   per.hossz: 6;   alapmego.: (x=55; y=12);   i=5
sqrt(22)=[4; 1;2;4;2;1;8;...]   per.hossz: 6;   alapmego.: (x=197; y=42);   i=5
sqrt(23)=[4; 1;3;1;8;...]   per.hossz: 4;   alapmego.: (x=24; y=5);   i=3
sqrt(24)=[4; 1;8;...]   per.hossz: 2;   alapmego.: (x=5; y=1);   i=1
sqrt(26)=[5; 10;...]   per.hossz: 1;   alapmego.: (x=51; y=10);   i=1
sqrt(27)=[5; 5;10;...]   per.hossz: 2;   alapmego.: (x=26; y=5);   i=1
sqrt(28)=[5; 3;2;3;10;...]   per.hossz: 4;   alapmego.: (x=127; y=24);   i=3
sqrt(29)=[5; 2;1;1;2;10;...]   per.hossz: 5;   alapmego.: (x=9801; y=1820);   i=9
sqrt(30)=[5; 2;10;...]   per.hossz: 2;   alapmego.: (x=11; y=2);   i=1
sqrt(31)=[5; 1;1;3;5;3;1;1;10;...]   per.hossz: 8;   alapmego.: (x=1520; y=273);   i=7
sqrt(32)=[5; 1;1;1;10;...]   per.hossz: 4;   alapmego.: (x=17; y=3);   i=3
sqrt(33)=[5; 1;2;1;10;...]   per.hossz: 4;   alapmego.: (x=23; y=4);   i=3
sqrt(34)=[5; 1;4;1;10;...]   per.hossz: 4;   alapmego.: (x=35; y=6);   i=3
sqrt(35)=[5; 1;10;...]   per.hossz: 2;   alapmego.: (x=6; y=1);   i=1
sqrt(37)=[6; 12;...]   per.hossz: 1;   alapmego.: (x=73; y=12);   i=1
```

```
C:\Users\Elitebook\Documents\Szakdoga\prog\lanctort4\main.exe
sqrt(38)=[6; 6;12;...]   per.hossz: 2;   alapmego.: (x=37; y=6);   i=1
sqrt(39)=[6; 4;12;...]   per.hossz: 2;   alapmego.: (x=25; y=4);   i=1
sqrt(40)=[6; 3;12;...]   per.hossz: 2;   alapmego.: (x=19; y=3);   i=1
sqrt(41)=[6; 2;2;12;...]   per.hossz: 3;   alapmego.: (x=2049; y=320);   i=5
sqrt(42)=[6; 2;12;...]   per.hossz: 2;   alapmego.: (x=13; y=2);   i=1
sqrt(43)=[6; 1;1;3;1;5;1;3;1;1;12;...]   per.hossz: 10;   alapmego.: (x=3482; y=531);   i=9
sqrt(44)=[6; 1;1;1;2;1;1;1;12;...]   per.hossz: 8;   alapmego.: (x=199; y=30);   i=7
sqrt(45)=[6; 1;2;2;2;1;12;...]   per.hossz: 6;   alapmego.: (x=161; y=24);   i=5
sqrt(46)=[6; 1;3;1;1;2;6;2;1;1;3;1;12;...]   per.hossz: 12;   alapmego.: (x=24335; y=3588);   i=11
sqrt(47)=[6; 1;5;1;12;...]   per.hossz: 4;   alapmego.: (x=48; y=7);   i=3
sqrt(48)=[6; 1;12;...]   per.hossz: 2;   alapmego.: (x=7; y=1);   i=1
sqrt(50)=[7; 14;...]   per.hossz: 1;   alapmego.: (x=99; y=14);   i=1
sqrt(51)=[7; 7;14;...]   per.hossz: 2;   alapmego.: (x=50; y=7);   i=1
sqrt(52)=[7; 4;1;2;1;4;14;...]   per.hossz: 6;   alapmego.: (x=649; y=90);   i=5
sqrt(53)=[7; 3;1;1;3;14;...]   per.hossz: 5;   alapmego.: (x=66249; y=9100);   i=9
sqrt(54)=[7; 2;1;6;1;2;14;...]   per.hossz: 6;   alapmego.: (x=485; y=66);   i=5
sqrt(55)=[7; 2;2;2;14;...]   per.hossz: 4;   alapmego.: (x=89; y=12);   i=3
sqrt(56)=[7; 2;14;...]   per.hossz: 2;   alapmego.: (x=15; y=2);   i=1
sqrt(57)=[7; 1;1;4;1;1;14;...]   per.hossz: 6;   alapmego.: (x=151; y=20);   i=5
sqrt(58)=[7; 1;1;1;1;1;1;14;...]   per.hossz: 7;   alapmego.: (x=19603; y=2574);   i=13
sqrt(59)=[7; 1;2;7;2;1;14;...]   per.hossz: 6;   alapmego.: (x=530; y=69);   i=5
sqrt(60)=[7; 1;2;1;14;...]   per.hossz: 4;   alapmego.: (x=31; y=4);   i=3
sqrt(61)=[7; 1;4;3;1;2;2;1;3;4;1;14;...]   per.hossz: 11;   alapmego.: (x=1766319049; y=226153980);   i=21
sqrt(62)=[7; 1;6;1;14;...]   per.hossz: 4;   alapmego.: (x=63; y=8);   i=3
sqrt(63)=[7; 1;14;...]   per.hossz: 2;   alapmego.: (x=8; y=1);   i=1
sqrt(65)=[8; 16;...]   per.hossz: 1;   alapmego.: (x=129; y=16);   i=1
sqrt(66)=[8; 8;16;...]   per.hossz: 2;   alapmego.: (x=65; y=8);   i=1
sqrt(67)=[8; 5;2;1;1;7;1;1;2;5;16;...]   per.hossz: 10;   alapmego.: (x=48842; y=5967);   i=9
sqrt(68)=[8; 4;16;...]   per.hossz: 2;   alapmego.: (x=33; y=4);   i=1
sqrt(69)=[8; 3;3;1;4;1;3;3;16;...]   per.hossz: 8;   alapmego.: (x=7775; y=936);   i=7
sqrt(70)=[8; 2;1;2;1;2;16;...]   per.hossz: 6;   alapmego.: (x=251; y=30);   i=5
```

5.13. Megjegyzés. Érdemes megjegyezni, hogy Waclaw Sierpiński: "Elementary Theory of Numbers" (PWN, Warszawa, 1987) könyv [4] 334. oldalán lévő táblázatában hibás érték szerepel $d = 29$ esetén a Pell-egyenlet alapmegoldására. A táblázat szerint az alapmegoldás (hibásan) $x = 4901$; $y = 1820$. A program természetesen $d = 29$-re is helyesen adja meg az alapmegoldást: $x = 9801$; $y = 1820$. Ez valóban jó, mivel $9801^2 - 29 \cdot 1820^2 = 1$.



```
C:\Users\Elitebook\Documents\Szakdoga\prog\lanctort4\main.exe
sqrt(71)=[8; 2;2;1;7;1;2;2;16;...]   per.hossz: 8;   alapmego.: (x=3480; y=413);   i=7
sqrt(72)=[8; 2;16;...]   per.hossz: 2;   alapmego.: (x=17; y=2);   i=1
sqrt(73)=[8; 1;1;5;5;1;1;16;...]   per.hossz: 7;   alapmego.: (x=2281249; y=267000);   i=13
sqrt(74)=[8; 1;1;1;1;16;...]   per.hossz: 5;   alapmego.: (x=3699; y=430);   i=9
sqrt(75)=[8; 1;1;1;16;...]   per.hossz: 4;   alapmego.: (x=26; y=3);   i=3
sqrt(76)=[8; 1;2;1;1;5;4;5;1;1;2;1;16;...]   per.hossz: 12;   alapmego.: (x=57799; y=6630);   i=11
sqrt(77)=[8; 1;3;2;3;1;16;...]   per.hossz: 6;   alapmego.: (x=351; y=40);   i=5
sqrt(78)=[8; 1;4;1;16;...]   per.hossz: 4;   alapmego.: (x=53; y=6);   i=3
sqrt(79)=[8; 1;7;1;16;...]   per.hossz: 4;   alapmego.: (x=80; y=9);   i=3
sqrt(80)=[8; 1;16;...]   per.hossz: 2;   alapmego.: (x=9; y=1);   i=1
sqrt(82)=[9; 18;...]   per.hossz: 1;   alapmego.: (x=163; y=18);   i=1
sqrt(83)=[9; 9;18;...]   per.hossz: 2;   alapmego.: (x=82; y=9);   i=1
sqrt(84)=[9; 6;18;...]   per.hossz: 2;   alapmego.: (x=55; y=6);   i=1
sqrt(85)=[9; 4;1;1;4;18;...]   per.hossz: 5;   alapmego.: (x=285769; y=30996);   i=9
sqrt(86)=[9; 3;1;1;1;8;1;1;1;3;18;...]   per.hossz: 10;   alapmego.: (x=10405; y=1122);   i=9
sqrt(87)=[9; 3;18;...]   per.hossz: 2;   alapmego.: (x=28; y=3);   i=1
sqrt(88)=[9; 2;1;1;1;2;18;...]   per.hossz: 6;   alapmego.: (x=197; y=21);   i=5
sqrt(89)=[9; 2;3;3;2;18;...]   per.hossz: 5;   alapmego.: (x=500001; y=53000);   i=9
sqrt(90)=[9; 2;18;...]   per.hossz: 2;   alapmego.: (x=19; y=2);   i=1
sqrt(91)=[9; 1;1;5;1;5;1;1;18;...]   per.hossz: 8;   alapmego.: (x=1574; y=165);   i=7
sqrt(92)=[9; 1;1;2;4;2;1;1;18;...]   per.hossz: 8;   alapmego.: (x=1151; y=120);   i=7
sqrt(93)=[9; 1;1;1;4;6;4;1;1;1;18;...]   per.hossz: 10;   alapmego.: (x=12151; y=1260);   i=9
sqrt(94)=[9; 1;2;3;1;1;5;1;8;1;5;1;1;3;2;1;18;...]   per.hossz: 16;   alapmego.: (x=2143295; y=221064);   i=15
sqrt(95)=[9; 1;2;1;18;...]   per.hossz: 4;   alapmego.: (x=39; y=4);   i=3
sqrt(96)=[9; 1;3;1;18;...]   per.hossz: 4;   alapmego.: (x=49; y=5);   i=3
sqrt(97)=[9; 1;5;1;1;1;1;1;1;5;1;18;...]   per.hossz: 11;   alapmego.: (x=62809633; y=6377352);   i=21
sqrt(98)=[9; 1;8;1;18;...]   per.hossz: 4;   alapmego.: (x=99; y=10);   i=3
sqrt(99)=[9; 1;18;...]   per.hossz: 2;   alapmego.: (x=10; y=1);   i=1
max. periódus helye: d=94,   hossza: 16
max. alapmego. helye: d=61,   értéke: (x=1766319049; y=226153980)
Press any key to continue . . . _
```

Úgy gondolom, a bevezetésben összefoglalt célokat sikeresen megvalósítottam. A hitelesség érdekében a program C++forráskódja is megtalálható lentebb.

```
#include <iostream>
#include <cstdlib>
#include <math.h>
#include <stdio.h>
#include <windows.h>
#include <vector>
using namespace std;

int lnko(int a, int b)
{
    int tmp;
    a=fabs(a);
    b=fabs(b);
    if(a<b)
    {
        tmp=b;
        b=a;
        a=tmp;
    }
    while(b>0)
    {
        tmp=b;
        b=a%b;
        a=tmp;
    }
```

```
    return a;
}

int main()
{
    setlocale(LC_ALL, "hun");
    int d=1;
    int maxper=0;
    int maxperhely=0;
    long long int maxmegox=0;
    long long int maxmegoy=0;
    int maxmegohely=0;
    while(d<=100)
    {
        vector<int> a;
        vector<int> b;
        vector<int> c;
        vector<int> egesz;
        int p;
        int q;
        int r;
        int o;
        int perhossz;
        bool per=false;
        if(sqrt(d)!=floor(sqrt(d)))
        {
            egesz.push_back(floor(sqrt(d)));
            a.push_back(-egesz[0]);
            b.push_back(1);
            c.push_back(1);
            while(!per)
            {
                p=-c.back()*a.back();
                q=c.back()*b.back();
                r=d*(b.back())*(b.back())-(a.back())*(a.back());
                o=lnko(lnko(p,q),r);
                p=p/o;
                q=q/o;
                r=r/o;
                egesz.push_back(floor((p+q*sqrt(d))/r));
                a.push_back(p-r*egesz.back());
                b.push_back(q);
                c.push_back(r);
                if(a.back()==a.at(0) && b.back()==b.at(0) && c.back()==c.at(0))
                {
                    perhossz=a.size()-1;
                    per=true;
                }
            }
        cout << "sqrt(" << d <<")=[" << egesz[0] << "; ";
        for(unsigned int i=1; i<egesz.size(); ++i)
        {    cout << egesz.at(i) << ";";}
        cout << "...]" << "    per.hossz: " << perhossz;
        if(perhossz>maxper)
        {
            maxper=perhossz;
```

```
            maxperhely=d;
        }
        vector<long long int> h;
        vector<long long int> k;
        int alapindex;
        h.push_back(0);
        k.push_back(1);
        h.push_back(1);
        k.push_back(0);
        h.push_back(egesz.at(0));
        k.push_back(1);
        if(perhossz%2==0)
        {    alapindex=perhossz-1;}
        else
        {    alapindex=2*perhossz-1;}
        for(int i=0; i<alapindex; ++i)
        {
            h.push_back(egesz.at(((i)%perhossz)+1)*h.at(i+2)+h.at(i+1));
            k.push_back(egesz.at(((i)%perhossz)+1)*k.at(i+2)+k.at(i+1));
        }
        cout << ";   alapmego.:  (x=" << h.back() << "; y=" << k.back() << ");   i=" << alapindex << endl;
        if(h.back()>maxmegox)
        {
            maxmegox=h.back();
            maxmegoy=k.back();
            maxmegohely=d;
        }
    }
    d=d+1;
    }
    cout << "max. periodus helye: d=" << maxperhely << ",   hossza: " << maxper << endl;
    cout << "max. alapmego. helye: d=" << maxmegohely << ",   erteke: (x=" << maxmegox << "; y=" << maxmegoy << ")" << endl;

    system("pause");
    return 0;
}
```

Hivatkozások

[1] Szalay Mihály: Számelmélet (3. kiadás), Typotex kiadó, Budapest, 2009.

[2] L. Niven - H. S. Zuckerman: Bevezetés a számelméletbe, Műszaki Könyvkiadó, Budapest, 1978

[3] Freud Róbert - Gyarmati Edit: Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2000

[4] Waclaw Sierpiński: Elementary Theory of Numbers, PWN, Warszawa, 1988

[5] `https://hu.wikipedia.org/wiki/Fermat-prímek`

`https://en.wikipedia.org/wiki/Fermat_number`

Utolsó letöltés dátuma: 2015.05.26.

[6] `http://www.prothsearch.net/fermat.html#Summary`

Utolsó letöltés dátuma: 2015.05.26.

[7] `https://hu.wikipedia.org/wiki/Mersenne-prímek`

`https://en.wikipedia.org/wiki/Mersenne_prime`

Utolsó letöltés dátuma: 2015.05.26.

[8] `http://www.mersenne.org/`

Utolsó letöltés dátuma: 2015.05.26.

[9] `https://hu.wikipedia.org/wiki/Tökéletes_számok`

Utolsó letöltés dátuma: 2015.05.26.