Négyzetszámok kerestetnek

Freud Róbert

2017. december 1

Meg van adva néhány olyan pozitív egész, amely nem osztható egyetlen 30-nál nagyobb prímszámmal sem.

Meg van adva néhány olyan pozitív egész, amely nem osztható egyetlen 30-nál nagyobb prímszámmal sem.

Ilyenek pl. 2^{2017}, $9 \cdot 125 \cdot 29$, $23^5 \cdot 70$ stb.

Meg van adva néhány olyan pozitív egész, amely nem osztható egyetlen 30-nál nagyobb prímszámmal sem.

Ilyenek pl. 2^{2017}, $9 \cdot 125 \cdot 29$, $23^5 \cdot 70$ stb.

Hány ilyen számból tudunk valahányat (akár csak egyet, akár az összeset) biztosan kiválasztani úgy, hogy azok szorzata négyzetszám legyen, akárhogyan is adták meg a számokat?

Meg van adva néhány olyan pozitív egész, amely nem osztható egyetlen 30-nál nagyobb prímszámmal sem.

Ilyenek pl. 2^{2017}, $9 \cdot 125 \cdot 29$, $23^5 \cdot 70$ stb.

Hány ilyen számból tudunk valahányat (akár csak egyet, akár az összeset) biztosan kiválasztani úgy, hogy azok szorzata négyzetszám legyen, akárhogyan is adták meg a számokat?

Pl. $3, 5^3, 10, 15^7$ esetén $3 \cdot 5^3 \cdot 15^7 = 3^8 \cdot 5^{10} = (3^4 \cdot 5^5)^2$.

Meg van adva néhány olyan pozitív egész, amely nem osztható egyetlen 30-nál nagyobb prímszámmal sem.

Ilyenek pl. 2^{2017}, $9 \cdot 125 \cdot 29$, $23^5 \cdot 70$ stb.

Hány ilyen számból tudunk valahányat (akár csak egyet, akár az összeset) biztosan kiválasztani úgy, hogy azok szorzata négyzetszám legyen, akárhogyan is adták meg a számokat?

Pl. $3, 5^3, 10, 15^7$ esetén $3 \cdot 5^3 \cdot 15^7 = 3^8 \cdot 5^{10} = (3^4 \cdot 5^5)^2$.

Általában azért nem elég négy szám, pl. a $2, 3, 5, 7$ számokból nem képezhető négyzetszám-szorzat.

Meg van adva néhány olyan pozitív egész, amely nem osztható egyetlen 30-nál nagyobb prímszámmal sem.

Ilyenek pl. 2^{2017}, $9 \cdot 125 \cdot 29$, $23^5 \cdot 70$ stb.

Hány ilyen számból tudunk valahányat (akár csak egyet, akár az összeset) biztosan kiválasztani úgy, hogy azok szorzata négyzetszám legyen, akárhogyan is adták meg a számokat?

Pl. $3, 5^3, 10, 15^7$ esetén $3 \cdot 5^3 \cdot 15^7 = 3^8 \cdot 5^{10} = (3^4 \cdot 5^5)^2$.

Általában azért nem elég négy szám, pl. a $2, 3, 5, 7$ számokból nem képezhető négyzetszám-szorzat.

Sőt, ha vesszük a 30 alatti prímeket: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$, ezek sem lesznek jók. Vagyis 10 szám sem elég mindig.

Meglepő módon 11 szám viszont már mindig elég. Ezt kétféleképpen is bebizonyítjuk.

Meglepő módon 11 szám viszont már mindig elég. Ezt kétféleképpen is bebizonyítjuk.

Kombinatorikus bizonyítás:

Meglepő módon 11 szám viszont már mindig elég. Ezt kétféleképpen is bebizonyítjuk.

Kombinatorikus bizonyítás:

A négyzetszámok onnan ismerhetők fel, hogy prímtényezős felbontásukban minden prím kitevője páros.

Meglepő módon 11 szám viszont már mindig elég. Ezt kétféleképpen is bebizonyítjuk.

Kombinatorikus bizonyítás:

A négyzetszámok onnan ismerhetők fel, hogy prímtényezős felbontásukban minden prím kitevője páros.

Így a feladat szempontjából mindegy, hogy pl. 3-at vagy 3^{2017}-t nézünk, csak a kitevők paritása számít.

Meglepő módon 11 szám viszont már mindig elég. Ezt kétféleképpen is bebizonyítjuk.

Kombinatorikus bizonyítás:

A négyzetszámok onnan ismerhetők fel, hogy prímtényezős felbontásukban minden prím kitevője páros.

Így a feladat szempontjából mindegy, hogy pl. 3-at vagy 3^{2017}-t nézünk, csak a kitevők paritása számít.

Mivel 10 prímünk van, egy számban mindegyik kitevője páros vagy páratlan, ez minden kitevőre 10 lehetőség, a 10 kitevőre összesen 2^{10} lehetőség.

Meglepő módon 11 szám viszont már mindig elég. Ezt kétféleképpen is bebizonyítjuk.

Kombinatorikus bizonyítás:

A négyzetszámok onnan ismerhetők fel, hogy prímtényezős felbontásukban minden prím kitevője páros.

Így a feladat szempontjából mindegy, hogy pl. 3-at vagy 3^{2017}-t nézünk, csak a kitevők paritása számít.

Mivel 10 prímünk van, egy számban mindegyik kitevője páros vagy páratlan, ez minden kitevőre 10 lehetőség, a 10 kitevőre összesen 2^{10} lehetőség.

Vagyis 2^{10}-féleképpen nézhet ki egy ilyen szám a mi szempontunkból.

Vegyük most a 11 tetszőlegesen megadott számunkat, és képezzük az összes lehetséges szorzatot belőlük. Hány ilyen szorzat van?

Vegyük most a 11 tetszőlegesen megadott számunkat, és képezzük az összes lehetséges szorzatot belőlük. Hány ilyen szorzat van?

Mindegyik számot vagy bevesszük a szorzatba, vagy sem, tehát minden számnál két választásunk van, ez összesen

Vegyük most a 11 tetszőlegesen megadott számunkat, és képezzük az összes lehetséges szorzatot belőlük. Hány ilyen szorzat van?

Mindegyik számot vagy bevesszük a szorzatba, vagy sem, tehát minden számnál két választásunk van, ez összesen

2^{11} lehetőség,

Vegyük most a 11 tetszőlegesen megadott számunkat, és képezzük az összes lehetséges szorzatot belőlük. Hány ilyen szorzat van?

Mindegyik számot vagy bevesszük a szorzatba, vagy sem, tehát minden számnál két választásunk van, ez összesen

2^{11} lehetőség,

de ebből 1-et le kell vonnunk, azt az esetet, amikor egyiket sem vettük be a szorzatba.

Vegyük most a 11 tetszőlegesen megadott számunkat, és képezzük az összes lehetséges szorzatot belőlük. Hány ilyen szorzat van?

Mindegyik számot vagy bevesszük a szorzatba, vagy sem, tehát minden számnál két választásunk van, ez összesen

2^{11} lehetőség,

de ebből 1-et le kell vonnunk, azt az esetet, amikor egyiket sem vettük be a szorzatba.

Tehát $2^{11} - 1$ szorzatunk keletkezik.

Mivel $2^{11} - 1$ szorzatunk van és csak 2^{10}-féle „kitevőeloszlásunk”, ezért lesz két olyan szorzat, amelyben a kitevőrendszer ugyanolyan (paritás szempontjából).

Mivel $2^{11} - 1$ szorzatunk van és csak 2^{10}-féle „kitevőeloszlásunk”, ezért lesz két olyan szorzat, amelyben a kitevőrendszer ugyanolyan (paritás szempontjából).

Legyen pl. az $A = abc$ és $B = adef$ szorzatok kitevőrendszere azonos.

Mivel $2^{11} - 1$ szorzatunk van és csak 2^{10}-féle „kitevőeloszlásunk”, ezért lesz két olyan szorzat, amelyben a kitevőrendszer ugyanolyan (paritás szempontjából).

Legyen pl. az $A = abc$ és $B = adef$ szorzatok kitevőrendszere azonos.

Ekkor AB négyzetszám.

Mivel $2^{11} - 1$ szorzatunk van és csak 2^{10}-féle „kitevőeloszlásunk”, ezért lesz két olyan szorzat, amelyben a kitevőrendszer ugyanolyan (paritás szempontjából).

Legyen pl. az $A = abc$ és $B = adef$ szorzatok kitevőrendszere azonos.

Ekkor AB négyzetszám.

Ugyanis szorzáskor a kitevők összeadódnak, és ha egy prím kitevője A-ban és B-ben is páros, akkor ennek a prímnek a kitevője AB-ben páros+páros=páros, ha pedig A-ban és B-ben is páratlan, akkor ez a kitevő AB-ben páratlan+páratlan=páros. Vagyis AB-ben minden prím kitevője páros, ezért AB négyzetszám.

Mivel $2^{11} - 1$ szorzatunk van és csak 2^{10}-féle „kitevőeloszlásunk”, ezért lesz két olyan szorzat, amelyben a kitevőrendszer ugyanolyan (paritás szempontjából).

Legyen pl. az $A = abc$ és $B = adef$ szorzatok kitevőrendszere azonos.

Ekkor AB négyzetszám.

Ugyanis szorzáskor a kitevők összeadódnak, és ha egy prím kitevője A-ban és B-ben is páros, akkor ennek a prímnek a kitevője AB-ben páros+páros=páros, ha pedig A-ban és B-ben is páratlan, akkor ez a kitevő AB-ben páratlan+páratlan=páros. Vagyis AB-ben minden prím kitevője páros, ezért AB négyzetszám.

Azonban $AB = a^2bcdef$, az a számot többször használtuk.

Mivel $2^{11} - 1$ szorzatunk van és csak 2^{10}-féle „kitevőeloszlásunk”, ezért lesz két olyan szorzat, amelyben a kitevőrendszer ugyanolyan (paritás szempontjából).

Legyen pl. az $A = abc$ és $B = adef$ szorzatok kitevőrendszere azonos.

Ekkor AB négyzetszám.

Ugyanis szorzáskor a kitevők összeadódnak, és ha egy prím kitevője A-ban és B-ben is páros, akkor ennek a prímnek a kitevője AB-ben páros+páros=páros, ha pedig A-ban és B-ben is páratlan, akkor ez a kitevő AB-ben páratlan+páratlan=páros. Vagyis AB-ben minden prím kitevője páros, ezért AB négyzetszám.

Azonban $AB = a^2bcdef$, az a számot többször használtuk.

De ekkor $AB/a^2 = bcdef$ is négyzetszám, és ezzel az állítást beláttuk.

Egyenletrendszeres bizonyítás:

Egyenletrendszeres bizonyítás:

Mivel csak a prímek kitevőinek a paritása számít, ezért a számok jellemezhetők egy 10 komponensű „kitevővektorral”, amelynek az egyes komponensei a $2, 3, 5, ..., 29$ prímek kitevőinek páros vagy páratlan voltát jelzik; páros esetben 0-t, páratlan esetben 1-et írunk. Pl. a $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ szám kitevővektora $(1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$.

Egyenletrendszeres bizonyítás:

Mivel csak a prímek kitevőinek a paritása számít, ezért a számok jellemezhetők egy 10 komponensű „kitevővektorral”, amelynek az egyes komponensei a $2, 3, 5, ..., 29$ prímek kitevőinek páros vagy páratlan voltát jelzik; páros esetben 0-t, páratlan esetben 1-et írunk. Pl. a $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ szám kitevővektora $(1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$.

És mely számoknak lesz csupa 0 a kitevővektorában?

Egyenletrendszeres bizonyítás:

Mivel csak a prímek kitevőinek a paritása számít, ezért a számok jellemezhetők egy 10 komponensű „kitevővektorral”, amelynek az egyes komponensei a $2, 3, 5, ..., 29$ prímek kitevőinek páros vagy páratlan voltát jelzik; páros esetben 0-t, páratlan esetben 1-et írunk. Pl. a $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ szám kitevővektora $(1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$.

És mely számoknak lesz csupa 0 a kitevővektorában?

Amelyekben mind a 10 prím kitevője páros, vagyis ezek éppen a négyzetszámok.

Egyenletrendszeres bizonyítás:

Mivel csak a prímek kitevőinek a paritása számít, ezért a számok jellemezhetők egy 10 komponensű „kitevővektorral”, amelynek az egyes komponensei a $2, 3, 5, ..., 29$ prímek kitevőinek páros vagy páratlan voltát jelzik; páros esetben 0-t, páratlan esetben 1-et írunk. Pl. a $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ szám kitevővektora $(1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$.

És mely számoknak lesz csupa 0 a kitevővektorában?

Amelyekben mind a 10 prím kitevője páros, vagyis ezek éppen a négyzetszámok.

Amikor két számot összeszorzunk, akkor a kitevővektorok összeadódnak, de itt $1 + 1 = 0$, azaz úgy számolunk, mint a 2-vel való osztási maradékokkal.

Egyenletrendszeres bizonyítás:

Mivel csak a prímek kitevőinek a paritása számít, ezért a számok jellemezhetők egy 10 komponensű „kitevővektorral”, amelynek az egyes komponensei a $2, 3, 5, ..., 29$ prímek kitevőinek páros vagy páratlan voltát jelzik; páros esetben 0-t, páratlan esetben 1-et írunk. Pl. a $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ szám kitevővektora $(1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$.

És mely számoknak lesz csupa 0 a kitevővektorában?

Amelyekben mind a 10 prím kitevője páros, vagyis ezek éppen a négyzetszámok.

Amikor két számot összeszorzunk, akkor a kitevővektorok összeadódnak, de itt $1 + 1 = 0$, azaz úgy számolunk, mint a 2-vel való osztási maradékokkal.

Amikor a 11 számból valahánynak a szorzatát képezzük, akkor az ezeknek megfelelő kitevővektorokat adjuk össze. Ez akkor lesz négyzetszám, ha az összeg a nullvektor.

Legyenek a számokhoz tartozó kitevővektorok $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_{11}}$. Ha 0 együtthatóval vesszük azokat közülük, amelyekhez tartozó számok nincsenek a szorzatban, és 1 együtthatóval a szorzat tényezőihez tartozókat, akkor az egészet úgy is elképzelhetjük, hogy az

$$x_1\mathbf{a_1} + x_2\mathbf{a_2} + \ldots + x_{11}\mathbf{a_{11}} = \mathbf{0}$$

vektoregyenletet kell megoldanunk, ahol minden x_i értéke 0 vagy 1.

Legyenek a számokhoz tartozó kitevővektorok $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_{11}}$. Ha 0 együtthatóval vesszük azokat közülük, amelyekhez tartozó számok nincsenek a szorzatban, és 1 együtthatóval a szorzat tényezőihez tartozókat, akkor az egészet úgy is elképzelhetjük, hogy az

$$x_1\mathbf{a_1} + x_2\mathbf{a_2} + \ldots + x_{11}\mathbf{a_{11}} = \mathbf{0}$$

vektoregyenletet kell megoldanunk, ahol minden x_i értéke 0 vagy 1.

Ez a vektoregyenlet mind a 10 komponensére egy közönséges egyenletet jelent (ahol persze minden mint 2-vel való osztási maradék értendő).

Vagyis összességében van egy 10 egyenletből álló, 11 ismeretlenes lineáris egyenletrendszerünk, és azt akarjuk belátni, hogy van olyan megoldása, ahol nem mindegyik $x_i = 0$.

Vagyis összességében van egy 10 egyenletből álló, 11 ismeretlenes lineáris egyenletrendszerünk, és azt akarjuk belátni, hogy van olyan megoldása, ahol nem mindegyik $x_i = 0$.

Az 1. egyenlet segítségével kiköszöbölhetünk egy ismeretlent a többi egyenletből, majd a 2. egyenlet segítségével egy másik ismeretlent küszöbölhetünk ki a 3–11. egyenletből stb. Az utolsó egyenletben így is legalább két ismeretlen marad, tehát valamelyik értékét megválaszthatjuk 1-nek, és ebből visszafelé meg tudjuk határozni a többi ismeretlen értékét (lehet, hogy nemcsak egy, hanem több „szabad paraméter" marad, ha a kitevővektorok „összefüggtek").

Vagyis összességében van egy 10 egyenletből álló, 11 ismeretlenes lineáris egyenletrendszerünk, és azt akarjuk belátni, hogy van olyan megoldása, ahol nem mindegyik $x_i = 0$.

Az 1. egyenlet segítségével kiköszöbölhetünk egy ismeretlent a többi egyenletből, majd a 2. egyenlet segítségével egy másik ismeretlent küszöbölhetünk ki a 3–11. egyenletből stb. Az utolsó egyenletben így is legalább két ismeretlen marad, tehát valamelyik értékét megválaszthatjuk 1-nek, és ebből visszafelé meg tudjuk határozni a többi ismeretlen értékét (lehet, hogy nemcsak egy, hanem több „szabad paraméter" marad, ha a kitevővektorok „összefüggtek").

Tehát biztosan van nem csupa 0 megoldás, és ezzel az állítást beláttuk.

Melyik bizonyítás „jobb"?

Melyik bizonyítás „jobb"?

Ha ténylegesen elő akarunk állítani egy ilyen szorzatot (és mondjuk nem 10, hanem 1000 prím esetén), akkor melyikkel megy gyorsabban?

Melyik bizonyítás „jobb"?

Ha ténylegesen elő akarunk állítani egy ilyen szorzatot (és mondjuk nem 10, hanem 1000 prím esetén), akkor melyikkel megy gyorsabban?

A kombinatorikusnál esetleg a szorzatok felét is fel tudjuk úgy érni, hogy még nem működik a skatulyaelv. Az egyenletrendszer megoldása viszont sokkal gyorsabb.

Melyik bizonyítás „jobb"?

Ha ténylegesen elő akarunk állítani egy ilyen szorzatot (és mondjuk nem 10, hanem 1000 prím esetén), akkor melyikkel megy gyorsabban?

A kombinatorikusnál esetleg a szorzatok felét is fel tudjuk úgy érni, hogy még nem működik a skatulyaelv. Az egyenletrendszer megoldása viszont sokkal gyorsabb.

De kinek jutna eszébe ilyen őrültség, hogy egy megfelelő szorzatot ténylegesen előállítsunk?

Meglepő módon, ennek fontos alkalmazása van. Egy nagy összetett számról gyorsan el tudjuk dönteni, hogy prím-e vagy összetett, azonban ha összetett, akkor (jelenleg) nem ismerünk gyors algoritmust, amivel az emberiség kihalása előtt ezt az egy számot a leggyorsabb számítógépek két valódi osztója szorzatára tudnák bontani.

Meglepő módon, ennek fontos alkalmazása van. Egy nagy összetett számról gyorsan el tudjuk dönteni, hogy prím-e vagy összetett, azonban ha összetett, akkor (jelenleg) nem ismerünk gyors algoritmust, amivel az emberiség kihalása előtt ezt az egy számot a leggyorsabb számítógépek két valódi osztója szorzatára tudnák bontani.

Ennek fontos szerepe van a nyilvános jelkulcsú titkosításokban, amelyen pl. a bankkártyáink biztonsága is múlik.

Meglepő módon, ennek fontos alkalmazása van. Egy nagy összetett számról gyorsan el tudjuk dönteni, hogy prím-e vagy összetett, azonban ha összetett, akkor (jelenleg) nem ismerünk gyors algoritmust, amivel az emberiség kihalása előtt ezt az egy számot a leggyorsabb számítógépek két valódi osztója szorzatára tudnák bontani.

Ennek fontos szerepe van a nyilvános jelkulcsú titkosításokban, amelyen pl. a bankkártyáink biztonsága is múlik.

A négyzetszámos feladat a ma ismert relatíve leggyorsabb faktorizációs eljárásokban játszik szerepet! És ott alapvetően fontos, hogy a négyzetszámot adó szorzat tényezőit gyorsan ténylegesen meg is találjuk!

A feladat négyzetszámok helyett más hatványokra is általánosítható.

A feladat négyzetszámok helyett más hatványokra is általánosítható.

Vegyünk k darab prímszámot és olyan számokat amelyek más prímszámmal nem oszthatók. Hány ilyen számra van szükség kell, hogy akármilyen megadásuk esetén biztosan ki tudjunk közülük választani néhányat, amelyek szorzata köbszám?

A feladat négyzetszámok helyett más hatványokra is általánosítható.

Vegyünk k darab prímszámot és olyan számokat amelyek más prímszámmal nem oszthatók. Hány ilyen számra van szükség kell, hogy akármilyen megadásuk esetén biztosan ki tudjunk közülük választani néhányat, amelyek szorzata köbszám?

Itt is elég könnyű mondani minél több olyan számot, amelyekre ez még nem igaz. És be lehet látni, hogy ennél eggyel több számból már biztosan kiválasztható egy köbszám-szorzat. A bizonyításhoz azonban egészen más módszer kell, mint a négyzetszámokra. Ez az új módszer p-edik hatványokra is működik, ahol p prímszám.

A feladat négyzetszámok helyett más hatványokra is általánosítható.

Vegyünk k darab prímszámot és olyan számokat amelyek más prímszámmal nem oszthatók. Hány ilyen számra van szükség kell, hogy akármilyen megadásuk esetén biztosan ki tudjunk közülük választani néhányat, amelyek szorzata köbszám?

Itt is elég könnyű mondani minél több olyan számot, amelyekre ez még nem igaz. És be lehet látni, hogy ennél eggyel több számból már biztosan kiválasztható egy köbszám-szorzat. A bizonyításhoz azonban egészen más módszer kell, mint a négyzetszámokra. Ez az új módszer p-edik hatványokra is működik, ahol p prímszám.

Sőt, egy megint újabb módszerrel 4-edik hatványokra is általánosíthatunk.

A feladat négyzetszámok helyett más hatványokra is általánosítható.

Vegyünk k darab prímszámot és olyan számokat amelyek más prímszámmal nem oszthatók. Hány ilyen számra van szükség kell, hogy akármilyen megadásuk esetén biztosan ki tudjunk közülük választani néhányat, amelyek szorzata köbszám?

Itt is elég könnyű mondani minél több olyan számot, amelyekre ez még nem igaz. És be lehet látni, hogy ennél eggyel több számból már biztosan kiválasztható egy köbszám-szorzat. A bizonyításhoz azonban egészen más módszer kell, mint a négyzetszámokra. Ez az új módszer p-edik hatványokra is működik, ahol p prímszám.

Sőt, egy megint újabb módszerrel 4-edik hatványokra is általánosíthatunk.

Azonban például 6-odik hatványokra megoldatlan, hol a határ.

Ha valakinek kérdése (vagy megoldása van), írhat nekem a `freud@math.elte.hu` `címre.`

Ha valakinek kérdése (vagy megoldása van), írhat nekem a `freud@math.elte.hu` `címre.`

Köszönöm a figyelmet!