Sokszínű gráfok a számelméletben

Gyarmati Katalin

Eötvös Loránd Tudományegyetem
Algebra és Számelmélet tanszék
Budapest

gykati@cs.elte.hu

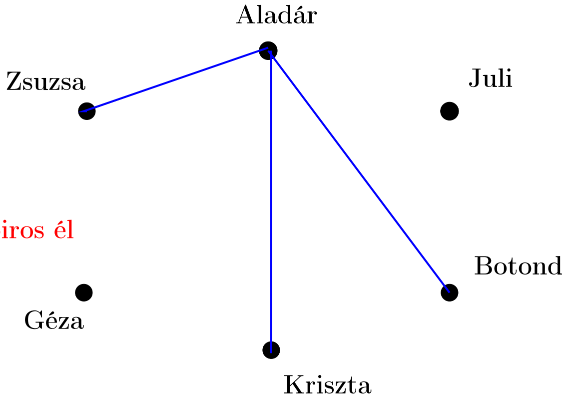
Feladat: Bizonyítsuk be, hogy egy hattagú társaságban mindig vagy van 3 ember, akik kölcsönösen ismerik egymást, vagy van 3 ember, akik kölcsönösen nem ismerik egymást.

Feladat: Bizonyítsuk be, hogy egy hattagú társaságban mindig vagy van 3 ember, akik kölcsönösen ismerik egymást, vagy van 3 ember, akik kölcsönösen nem ismerik egymást.

Gráfokkal...

Feladat: Bizonyítsuk be, hogy egy hattagú társaságban mindig vagy van 3 ember, akik kölcsönösen ismerik egymást, vagy van 3 ember, akik kölcsönösen nem ismerik egymást.

Gráfokkal...

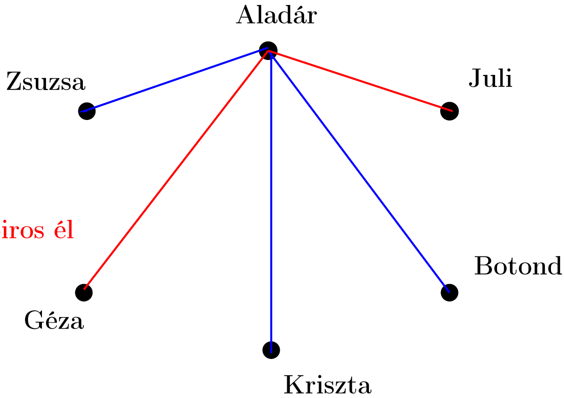


Ismerik egymást: kék él

Nem ismerik egymást: piros él

Feladat: Bizonyítsuk be, hogy egy hattagú társaságban mindig vagy van 3 ember, akik kölcsönösen ismerik egymást, vagy van 3 ember, akik kölcsönösen nem ismerik egymást.

Gráfokkal...

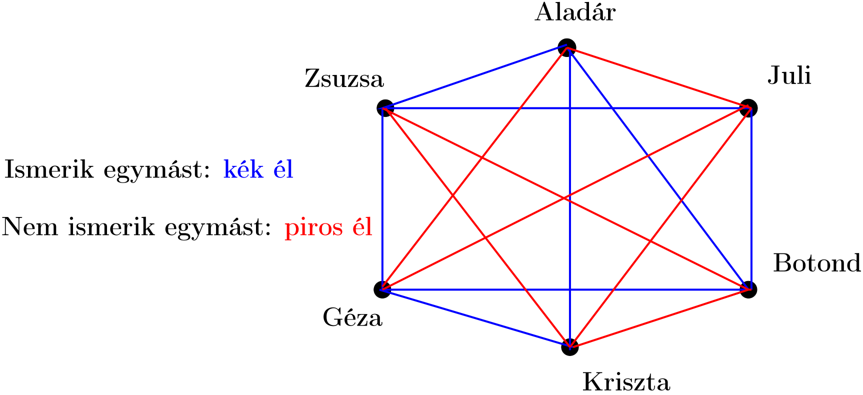


Ismerik egymást: kék él

Nem ismerik egymást: piros él

Feladat: Bizonyítsuk be, hogy egy hattagú társaságban mindig vagy van 3 ember, akik kölcsönösen ismerik egymást, vagy van 3 ember, akik kölcsönösen nem ismerik egymást.

Gráfokkal...

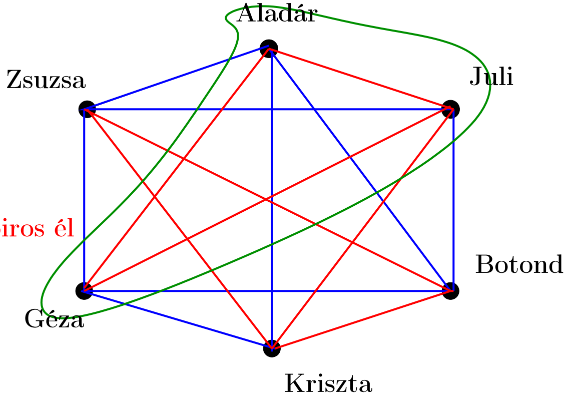


Feladat: Bizonyítsuk be, hogy egy hattagú társaságban mindig vagy van 3 ember, akik kölcsönösen ismerik egymást, vagy van 3 ember, akik kölcsönösen nem ismerik egymást.

Gráfokkal...

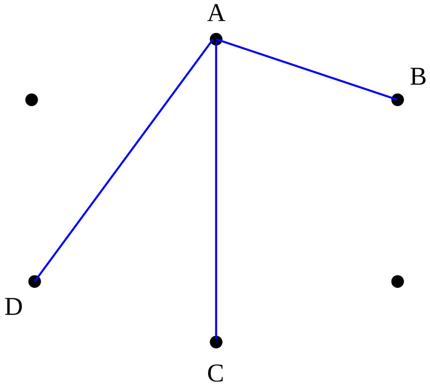
Ismerik egymást: kék él

Nem ismerik egymást: piros él



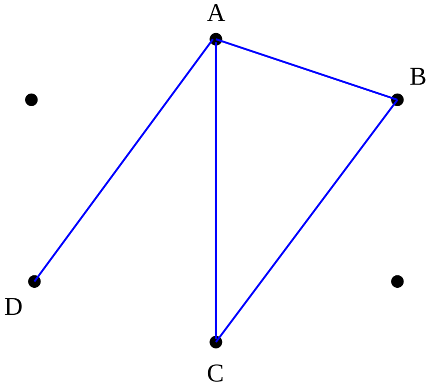
Feladat: Egy 6 szögpontú teljes gráf éleit 2 színnel színezve mindig lesz a gráfban egyszínű háromszög.

Rögzítsük a gráf egy szögpontját, mondjuk A-t. A-ból öt másik csúcsba fut él. Skatulyaelv miatt van 3 csúcs (legyenek ezek B, C, D), amelybe azonos színű él fut mondjuk kék.



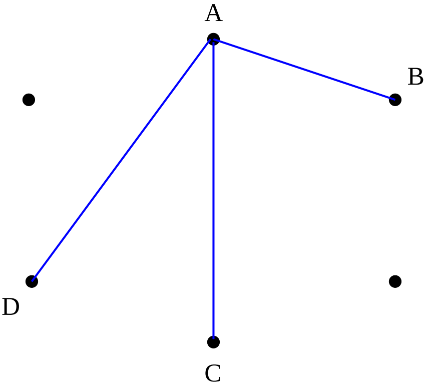
Feladat: Egy 6 szögpontú teljes gráf éleit 2 színnel színezve mindig lesz a gráfban egyszínű háromszög.

Rögzítsük a gráf egy szögpontját, mondjuk A-t. A-ból öt másik csúcsba fut él. Skatulyaelv miatt van 3 csúcs (legyenek ezek B, C, D), amelybe azonos színű él fut mondjuk kék.



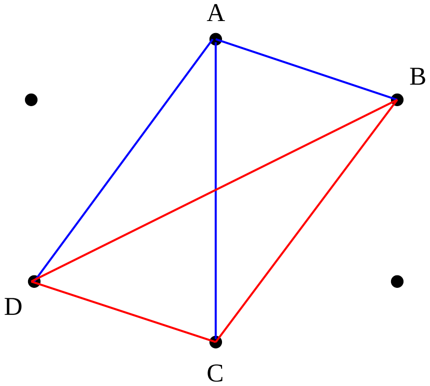
Feladat: Egy 6 szögpontú teljes gráf éleit 2 színnel színezve mindig lesz a gráfban egyszínű háromszög.

Rögzítsük a gráf egy szögpontját, mondjuk A-t. A-ból öt másik csúcsba fut él. Skatulyaelv miatt van 3 csúcs (legyenek ezek B, C, D), amelybe azonos színű él fut mondjuk kék.

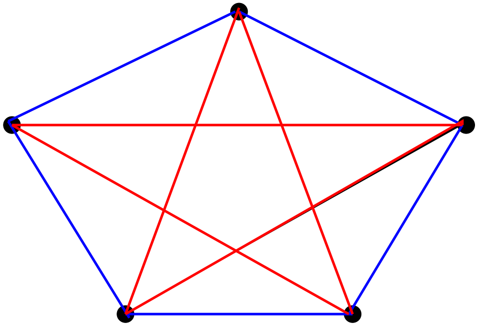


Feladat: Egy 6 szögpontú teljes gráf éleit 2 színnel színezve mindig lesz a gráfban egyszínű háromszög.

Rögzítsük a gráf egy szögpontját, mondjuk A-t. A-ból öt másik csúcsba fut él. Skatulyaelv miatt van 3 csúcs (legyenek ezek B, C, D), amelybe azonos színű él fut mondjuk kék.



Igaz-e az állítás 5 szögpontból álló gráfra? Nem, tekintsük például a következő gráfot:



Ebben a gráfban nincs egyszínű háromszög.

Általánosítható-e a feladat több színre?

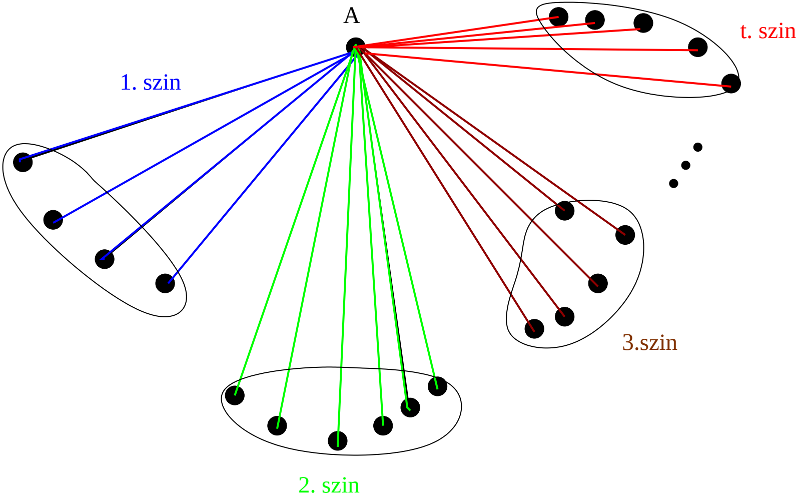
Jelölje $R(t)$ azt a legkisebb pozitív egész számot, n-et, amelyre igaz, hogy egy legalább n darab szögpontból álló teljes gráf éleit t darab színnel színezve, mindig lesz egyszínű háromszög.

Eddig láttuk: $R(1) = 3$, $R(2) = 6$.

Ismert: $R(3) = 17$.

Vajon milyen becslések adhatóak $R(t)$-re?

Vajon milyen becslések adhatóak $R(t)$-re?



$$R(t) \leq 1 + t \cdot (R(t-1) - 1) + 1$$

Jelölje $R(t)$ azt a legkisebb pozitív egész számot, n-et, amelyre igaz, hogy egy legalább n darab szögpontból álló teljes gráf éleit t darab színnel színezve, mindig lesz egyszínű háromszög.

Eddig: $R(1) = 3$, $R(2) = 6$. $t \geq 2$ esetén
$R(t) \leq 2 + t \cdot (R(t-1) - 1)$.

A fenti rekurzióból teljes indukcióval könnyen igazolható:

$$R(t) \leq 3t!$$

Kezdőlépés: $t = 1$: $R(1) = 3 \leq 3 \cdot 1! \checkmark$

Indukciós lépés ($t \geq 2$): $t - 1 \Rightarrow t$:

$$R(t) \leq 2+t\cdot(R(t-1)-1) \leq 2+t\cdot(3(t-1)!-1) = 3t!-t+2 \leq 3t!$$

$\checkmark$

Ramsey-tételek

A Ramsey-elmélet Frank Plumpton Ramsey matematikus-közgazdász harmincas években publikált eredménye által elindított igen fontos ága a kombinatorikának.

A leggyakoribb esetben egy teljes gráf éleinek két darab színnel való színezése esetén vizsgálja azt, hogy milyen esetekben lesz a gráfban egy nagy monokromatikus részgráf.

Mi eddig egy ritkábban használt esetet néztünk: több szín esetén mikor lesz a gráfban egyszínű háromszög.

Színezéses tételek a Számelméletben

Van der Waerden tétel:

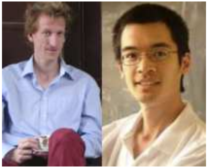
Bárhogyis színezzük a természetes számokat t darab színnel mindig lesz tetszőlegesen hosszú egyszínű számtani sorozat.

Szemerédi tétel:

$\forall \varepsilon, k$-hoz $\exists$ egy $N_0 = N_0(\varepsilon, k)$ egész szám, hogy ha $N > N_0$, és $\mathcal{A} \subseteq \{1, 2, 3, \ldots, N\}$ melyre $|\mathcal{A}| \geq \varepsilon N$, akkor $\mathcal{A}$ tartalmaz k-tagú számtani sorozatot.

Green-Tao tétel:

A prímszámok tartalmaznak tetszőlegesen hosszú számtani sorozatot.



Néhány példa:

3 hosszú számtani sorozat: 3,5,7
4 hosszú számtani sorozat: 61,67,73,79
5 hosszú számtani sorozat: 7,37,67,97,127
...
(A prímszámok NEM tartalmaznak végtelen hosszú számtani sorozatot.)

Schur tétel:

Bárhogyis színezzük a természetes számokat t darab színnel mindig lesz egyszínű megoldása az

$$x + y = z$$

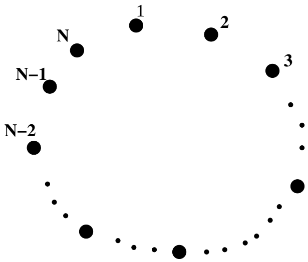
egyenletnek.

Schur tétel (kvantitatív változat): Ha N és t pozitív egész számok, akkor $N \geq 3t!$ esetén bárhogy színezzük az $\{1, 2, 3, \ldots, N\}$ halmaz elemeit t darab színnel mindig lesz egyszínű megoldása az

$$x + y = z$$

egyenletnek.

Bizonyítás: A G gráf szögpontjai az $1, 2, 3, \ldots, N$ természetes számok.

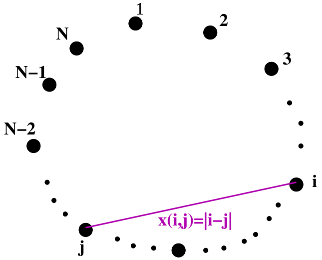


Schur tétel (kvantitatív változat): Ha N és t pozitív egész számok, akkor $N \geq 3t!$ esetén bárhogy színezzük az $\{1, 2, 3, \ldots, N\}$ halmaz elemeit t darab színnel mindig lesz egyszínű megoldása az

$$x + y = z$$

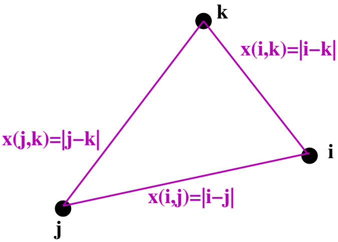
egyenletnek.

Bizonyítás: A G gráf szögpontjai az $1, 2, 3, \ldots, N$ természetes számok.

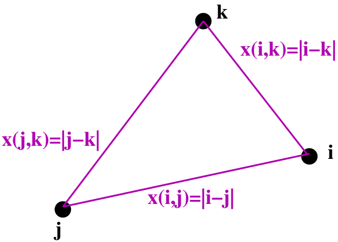


Az i és j szögpont között futó él színe az $x(i,j) \stackrel{\text{def}}{=} |i-j|$ elemnek a színe. (Itt $x(i,j) \in \{1, 2, \ldots, N\}$, amely halmaz t darab színnel van színezve.) $N \geq 3t! \Rightarrow$ Lesz egyszínű háromszög!

Van egyszínű háromszög:



Van egyszínű háromszög:

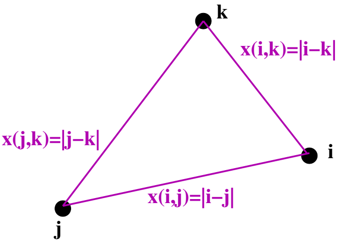


Feltehető $i < j < k$. Ekkor legyen

$$a \stackrel{\text{def}}{=} x(i,j) = |i-j| = j-i, \qquad b \stackrel{\text{def}}{=} x(j,k) = |j-k| = k-j$$

$$c \stackrel{\text{def}}{=} x(i,k) = |i-k| = k-i.$$

Van egyszínű háromszög:



Feltehető $i < j < k$. Ekkor legyen

$$a \stackrel{\text{def}}{=} x(i,j) = |i-j| = j-i, \qquad b \stackrel{\text{def}}{=} x(j,k) = |j-k| = k-j$$
$$c \stackrel{\text{def}}{=} x(i,k) = |i-k| = k-i.$$

a, b és c színe azonos. Továbbá:

$$a + b = (j-i) + (k-j) = k-i = c,$$

így találtunk egy monokromatikus megoldását az $x + y = z$ egyenletnek. ✓

Schur tétel: Ha N és t pozitív egész számok, akkor $N \geq 3t!$ esetén bárhogy színezzük az $\{1, 2, 3, \ldots, N\}$ halmaz elemeit t darab színnel mindig lesz egyszínű megoldása az

$$x + y = z$$

egyenletnek.

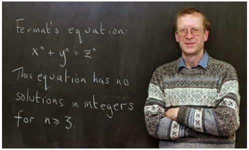
Milyen alkalmazásai vannak a Schur tételnek?

Nagy-Fermat tétel

Pierre de Fermat a következő megjegyzést fűzte Diophantosz Aritmetika című könyvéhez:

Lehetetlen egy egész szám másodiknál nagyobb hatványát két ugyanannyiadfokú hatvány összegére bontani ..., csak „kevés a margó semhogy befogadná”.

Az $a^n + b^n = c^n$ diofantoszi egyenletnek nincs megoldása a pozitív egész számok körében, ha $n \geq 3$.



A Fermat-sejtést Andrew Wiles oldotta meg az 1990-es évek közepén.

Számelméleti alapok: Kongruenciák

Azt mondjuk:

$$a \equiv b \pmod{m},$$

ha az a és b egész számoknak az m egész számmal vett osztási maradéka ugyanaz. Más szóval: $m \mid a - b$.

Például: $15 \equiv 27 \pmod{12}$, de $3 \not\equiv 14 \pmod{12}$.

Tétel

Ha $a \equiv x \pmod{m}$ *és* $b \equiv y \pmod{m}$, *akkor*

$$a + b \equiv x + y \pmod{m} \quad \text{és } ab \equiv xy \pmod{m}.$$

Vajon a Fermat kongruencia

$$x^n + y^n \equiv z^n \pmod{p}$$

minden p prímre megoldható?

Vajon a Fermat kongruencia

$$x^n + y^n \equiv z^n \pmod{p}$$

minden p prímre megoldható?

Igen, pl. $x \equiv 0 \pmod{p}$ és $y \equiv z \pmod{p}$ mindig megoldás.

Vajon a Fermat kongruencia

$$x^n + y^n \equiv z^n \pmod{p}$$

minden p prímre megoldható?

Igen, pl. $x \equiv 0 \pmod{p}$ és $y \equiv z \pmod{p}$ mindig megoldás.

Triviális megoldások: $x \equiv 0 \pmod{p}$ vagy $y \equiv 0 \pmod{p}$ vagy $z \equiv 0 \pmod{p}$ valamelyike teljesül.

Vajon a Fermat kongruencia

$$x^n + y^n \equiv z^n \pmod{p}$$

minden p prímre megoldható?

Igen, pl. $x \equiv 0 \pmod{p}$ és $y \equiv z \pmod{p}$ mindig megoldás.

Triviális megoldások: $x \equiv 0 \pmod{p}$ vagy $y \equiv 0 \pmod{p}$ vagy $z \equiv 0 \pmod{p}$ valamelyike teljesül.

De vajon mindig létezik nem triviális megoldás is?

A Fermat-sejtés megoldása céljából, sokan próbáltak végtelen sok p_i prímet találni, hogyha

$$x^n + y^n \equiv z^n \pmod{p_i}$$

teljesül, akkor p_i osztója az xyz szorzatnak (azaz a Fermat-kongruenciának csak a triviális megoldásai vannak).

(Ugyanis, $x^n + y^n = z^n$-ből következik, hogy

$$x^n + y^n \equiv z^n \pmod{p_i}$$

minden p_i prímre, és így ha a fenti állítás igaz lenne, az xyz-nek végtelen sok prímosztója lenne: $p_1, p_2, \ldots$, ami ellentmondás hiszen xyz egy véges pozitív egész.)

Egyszer csak kiderült: így NEM LEHET megoldani a Fermat-sejtést!

Tétel: Legyen n természetes szám, p prím. Ha $p > 3n!$, akkor az

$$x^n + y^n \equiv z^n \pmod{p}$$

Fermat-kongruenciának mindig van nem triviális megoldása.

Tétel: Legyen n természetes szám, p prím. Ha $p > 3n!$, akkor az

$$x^n + y^n \equiv z^n \pmod{p}$$

Fermat-kongruenciának mindig van nem triviális megoldása.

Bizonyítás: Mivel $p > 3n!$, Schur tétele szerint, bárhogy színezzük az n darab színnel a $\{1, 2, \ldots, p-1\}$ halmaz elemeit, mindig lesz egyszínű megoldása az

$$x + y = z$$

egyenletnek.

Tétel: Legyen n természetes szám, p prím. Ha $p > 3n!$, akkor az

$$x^n + y^n \equiv z^n \pmod{p}$$

Fermat-kongruenciának mindig van nem triviális megoldása.

Bizonyítás: Mivel $p > 3n!$, Schur tétele szerint, bárhogy színezzük az n darab színnel a $\{1, 2, \dots, p-1\}$ halmaz elemeit, mindig lesz egyszínű megoldása az

$$x + y = z$$

egyenletnek.

Most rögzítjük az $\{1, 2, \dots, p-1\}$ halmaz színezését. Megadunk egy konkrét színezést.

Rögzítjük az $\{1, 2, \ldots, p-1\}$ halmaz színezését:

Rögzítjük az $\{1, 2, \ldots, p-1\}$ halmaz színezését:

Legyen g egy *primitív gyök*, azaz olyan egész szám, amelyre a $g^0, g^1, g^2, \ldots, g^{p-2}$ számok p-vel vett osztási maradéka az $1, 2, 3, \ldots, p-1$ számok (nem feltétlen ebben a sorrendben).

Egy $m \in \{1, 2, \ldots, p-1\}$ elem színe az s-edik szín (ahol $0 \leq s \leq n-1$), ha létezik olyan $t(m)$ (csak m-től függő) egész szám, hogy

$$m \equiv g^{t(m)n+s} \pmod{p}.$$

Rögzítjük az $\{1, 2, \ldots, p-1\}$ halmaz színezését:

Legyen g egy *primitív gyök*, azaz olyan egész szám, amelyre a $g^0, g^1, g^2, \ldots, g^{p-2}$ számok p-vel vett osztási maradéka az $1, 2, 3, \ldots, p-1$ számok (nem feltétlen ebben a sorrendben).

Egy $m \in \{1, 2, \ldots, p-1\}$ elem színe az s-edik szín (ahol $0 \leq s \leq n-1$), ha létezik olyan $t(m)$ (csak m-től függő) egész szám, hogy

$$m \equiv g^{t(m)n+s} \pmod{p}.$$

Erre a színezésre is létezik az $x + y = z$ egyenletnek monokromatikus megoldása. Azaz létezik olyan x, y, z megoldás, amelyre

$$x \equiv g^{t(x)n+s},\ y \equiv g^{t(y)n+s},\ z \equiv g^{t(z)n+s} \pmod{p}$$

ugyanazzal a $0 \leq s \leq n-1$ egész számmal teljesül mindhárom kongruenciában.

Összefoglalva: $x + y = z$ és

$$x \equiv g^{t(x)n+s},\ y \equiv g^{t(y)n+s},\ z \equiv g^{t(z)n+s} \pmod p$$

ugyanazzal a $0 \leq s \leq n-1$ egész számmal.

Összefoglalva: $x + y = z$ és

$$x \equiv g^{t(x)n+s},\ y \equiv g^{t(y)n+s},\ z \equiv g^{t(z)n+s} \pmod{p}$$

ugyanazzal a $0 \leq s \leq n-1$ egész számmal. Ekkor:

$$x + y = z,$$

$$x + y \equiv z \pmod{p}$$

$$g^{t(x)n+s} + g^{t(y)n+s} \equiv g^{t(z)n+s} \pmod{p} \qquad / : g^s$$

$$g^{t(x)n} + g^{t(y)n} \equiv g^{t(z)n} \pmod{p}$$

$$\left(g^{t(x)}\right)^n + \left(g^{t(y)}\right)^n \equiv \left(g^{t(z)}\right)^n \pmod{p}$$

Összefoglalva: $x + y = z$ és

$$x \equiv g^{t(x)n+s},\ y \equiv g^{t(y)n+s},\ z \equiv g^{t(z)n+s} \pmod{p}$$

ugyanazzal a $0 \leq s \leq n-1$ egész számmal. Ekkor:

$$\begin{aligned} x + y &= z, \\ x + y &\equiv z \pmod{p} \\ g^{t(x)n+s} + g^{t(y)n+s} &\equiv g^{t(z)n+s} \pmod{p} \qquad / : g^s \\ g^{t(x)n} + g^{t(y)n} &\equiv g^{t(z)n} \pmod{p} \\ \left(g^{t(x)}\right)^n + \left(g^{t(y)}\right)^n &\equiv \left(g^{t(z)}\right)^n \pmod{p} \end{aligned}$$

Bevezetve az

$$a \stackrel{\text{def}}{=} g^{t(x)},\ b \stackrel{\text{def}}{=} g^{t(y)},\ c \stackrel{\text{def}}{=} g^{t(z)}$$

jelöléseket, azt kapjuk, hogy

$$a^n + b^n \equiv c^n \pmod{p}.$$

Vagyis találtunk egy nem-triviális megoldását a Fermat-kongruenciának.

Köszönöm a figyelmet!