Bevezetés

A Középiskolai Matematikai Lapok 1990/10. számában kitűzött *F. 2826.* feladat a következő volt:

A. Feladat. *Legyen n 1-nél nagyobb pozitív egész. Bizonyítsuk be, hogy ha 6^n-1 osztható n-nel, akkor n osztható 5-tel.*

Hasonló típusú, de lényegesen nehezebb volt a 31. Nemzetközi Matematikai Diákolimpia 3. feladata (Középiskolai Matematikai Lapok, 1990/8–9. szám, 340. oldal):

B. Feladat. *Határozzuk meg az összes olyan $n>1$ egész számot, amelyre $\dfrac{2^n+1}{n^2}$ is egész szám.*

Ezek a feladatok a 6^n-1, illetve a 2^n+1 alakú számok bizonyos speciális alakú osztóinak létezésére, tulajdonságaira vonatkoznak. Az $a^n\pm 1$ alakú számok, és általánosabban az $a^n\pm b^n$ alakú számok prímosztóinak és osztóinak a tulajdonságai sok számelméleti probléma megoldása során szerepet játszanak. A tekintett számokkal már *Fermat, Euler és Legendre* is foglalkozott. Cikkünkben ezen számok osztóinak néhány fontos tulajdonságával ismerkedünk meg. Eközben általánosabb formában oldjuk meg az *A.és B. Feladatokat.* Csupán az az eset érdekes, amikor $a>b>0$ egészek és $(a,b)=1$, ezért ezt a továbbiakban külön említés nélkül is mindig fel fogjuk tételezni.

Az A. feladat vizsgálata

Az *A. Feladat* egy lényeges általánosítása következik az alábbi tételből, amely lényegében *Legendre*-tól származik.

1. Tétel. *Legyen $n>1$ egész szám.*

(i) *Ha p prímosztója a^n-b^n-nek, úgy $p=nk+1$ alakú (ahol $k>0$ egész), vagy az n valamely $m<n$ pozitív osztójára $p|a^m-b^m$.*

(ii) *Ha p páratlan prímosztója a^n+b^n-nek, úgy $p=2nk+1$ alakú (ahol $k>0$ egész) vagy az n valamely $m<n$ pozitív osztójára $p|a^m+b^m$ és n/m páratlan.*

Az *A. Feladat* állítása azonnal következik a tétel alábbi következményének **(i)** állításából az $a=6$, $b=1$ választás mellett.

1. Következmény. *Legyen $n>1$ egész szám.*
(i) *Ha $n|a^n-b^n$, úgy az n legkisebb prímfaktora osztója $a-b$-nek.*
(ii) *Ha $n|a^n+b^n$, úgy az n legkisebb prímfaktora osztója $a+b$-nek.*

Ebből következik, hogy ha $b=a+1$, úgy nincs olyan $n>1$ egész, melyre $n|a^n-b^n$. Később a *2. Következményben* látni fogjuk, hogy minden más esetben van végtelen sok n, melyre $n|a^n-b^n$, s mindig van végtelen sok n, melyre $n|a^n+b^n$.

Az *1. Tétel* bizonyításához szükségünk lesz a következő lemmára.

1. Lemma. *Legyen $n\geqq 1$ egész, legyen p az a^n-b^n egy prímosztója, s legyen m az a legkisebb pozitív egész, melyre $p|a^m-b^m$. Ekkor $m|n$.*

Megjegyezzük, hogy hasonló állítás igaz az a^n+b^n alakú számok páratlan p prímosztóira.

Az 1. Lemma bizonyítása. A lemma állítása közismert, ha $b=1$, s a bizonyítás is erre vezeti vissza az állítást. *(A szerk.)* Az a, b és p-re tett feltevés miatt $(p,ab)=1$. Ezért van olyan c pozitív egész, melyre $bc\equiv 1 \pmod p$ és így $p\nmid c$. A $d=ac$ jelölést bevezetve $p\nmid d$ is teljesül. Az a^n-b^n számot c^n-nel, az a^m-b^m számot c^m-mel megszorozva,

$$d^n\equiv 1 \pmod p \tag{1}$$

és

$$d^m\equiv 1 \pmod p \tag{2}$$

következik, továbbá ekkor m a legkisebb pozitív egész, melyre (2) teljesül. Osszuk el n-et maradékosan m-mel: $n=mu+v$ és $0\leqq v<m$. (1) és (2)-ből $d^v\equiv 1 \pmod p$ adódik. Ezért m minimális volta miatt csak $v=0$ lehet, s így valóban $m|n$. ■

Az 1. Tétel bizonyítása. Először az **(i)**állítást igazoljuk. Legyen p az a^n-b^n egy prímosztója, s jelöljük m-mel azt a legkisebb pozitív egészt, melyre $p|a^m-b^m$. Ekkor az 1. Lemma szerint $m|n$. Mivel $(p,ab)=1$, ezért a *kis Fermat-tétel* szerint $p|a^{p-1}-b^{p-1}$. Így viszont ismét az 1. Lemmát alkalmazva $m|p-1$. Ebből következik, hogy $m=n$ esetén $p=nk+1$ alakú, míg $m<n$ esetén $p|a^m-b^m$.

Ezután (ii)-t bizonyítjuk. Legyen p az a^n+b^n egy páratlan prímosztója. Ekkor

$$p|a^{2n}-b^{2n}. \tag{3}$$

Legyen t a legkisebb pozitív egész, melyre

$$p|a^t-b^t. \tag{4}$$

Ekkor (3), (4) és az I. Lemma miatt $t|2n$. Amennyiben $t = 2n$, úgy az imént bizonyított **(i)** állítás következtében $p = 2nk + 1$ alakú. Maradt tehát a $t < 2n$ eset. Legyen most m az a legkisebb pozitív egész, melyre

$$p|a^m + b^m. \tag{5}$$

Ekkor $p|a^{2m} - b^{2m}$, s így az 1. Lemma szerint $t|2m$. Ha t páratlan, úgy ebből $t|m$ adódik. Ekkor viszont (4)-ből $p|a^m - b^m$ következik, ami ellentmond (5)-nek és $(p, ab) = 1$-nek. Ha viszont t páros, úgy 4-ből következik, hogy p osztója $a^{t/2} - b^{t/2}$ vagy $a^{t/2} + b^{t/2}$-nek. A t minimális választása miatt csak $p|a^{t/2} + b^{t/2}$ lehet. Ekkor viszont az m minimális választása következtében $t/2 = m$, azaz $t = 2m$. Mivel pedig $t|2n$ volt, ezért $m|n$ és $m < n$. Végül (5) felhasználásával

$$-b^n \equiv a^n = (a^m)^{n/m} \equiv (-b^m)^{n/m} = (-1)^{n/m} b^n \pmod{p},$$

amiből következik, hogy n/m páratlan. Ezzel az állítást bebizonyítottuk. ■

Az 1. Következmény bizonyítása. Először az **(i)** állítást bizonyítjuk. Tegyük fel, hogy $n|a^n - b^n$, és legyen p az n legkisebb prímfaktora. Ekkor p nem lehet $nk + 1$ alakú, ezért az *1. Tétel* **(i)** állítása miatt létezik az n-nek olyan $m < n$ osztója, melyre $p|a^m - b^m$. Ha m-nek van p-től különböző prímosztója, úgy ez p-nél nagyobb (p minimális volta miatt). Ebben az esetben p nem lehet $mk + 1$ alakú, s ezért az *1. Tétel* következtében létezik m-nek olyan $m' < m$ osztója, melyre $p|a^{m'} - b^{m'}$. Ezt az eljárást folytatva, véges sok lépés után az adódik, hogy $p|a^{p^\alpha} - b^{p^\alpha}$ valamely $\alpha \geqq 0$ egész mellett. Viszont a *kis Fermat-tétel* szerint

$$a^{p^\alpha} - b^{p^\alpha} \equiv a^{p^{\alpha-1}} - b^{p^{\alpha-1}} \equiv \ldots \equiv a - b \pmod{p},$$

ezért valóban $p|a - b$.

Ezután tekintsük az **(ii)** állítást. Tegyük fel, hogy $n|a^n + b^n$, s legyen p az n legkisebb prímosztója. Ha $p = 2$, úgy $p|a^n + b^n$ csak úgy lehet, ha a és b páratlan, amikor is $p|a + b$. Ha pedig $p > 2$, úgy az állítás ugyanúgy következik az *1. Tétel* **(ii)** állításából, mint fentebb az **(i)** állítás az *1. Tétel* **(i)** állításából. ■

Térjünk vissza az *1. Tételhez*. Felmerül a kérdés, hogy az **(i)** és **(ii)** állításokban a p prímosztókra vonatkozóan fennállhat-e mindkét eset. A választ a következő tétel adja meg. Az $a^n - b^n$ egy osztóját *primitívnek* nevezzük, ha ez az osztó nem osztója $a^m - b^m$-nek semmilyen pozitív $m < n$-re. Hasonlóan, $a^n + b^n$ egy osztóját *primitívnek* szokás nevezni, ha nem osztója $a^m + b^m$-nek semmilyen pozitív egész $m < n$-re. Könnyű belátni, hogy $a^n - b^n$-nek mindig van nem primitív prímosztója, kivéve azt az esetet, amikor $a = b + 1$ és n prímszám. Az $a^n + b^n$-nek szintén van nem primitív prímosztója, eltekintve attól az esettől, amikor $a + b$ páratlan és n a 2 egy hatványa. *Zsigmondy* 1892-ben bebizonyította a következőt:

2. Tétel. (i) *$a^n - b^n$-nek minden $n > 1$ egészre van primitív prímosztója, kivéve a következő eseteket:*
1) $n = 2$, $a + b$ pedig a 2 egy hatványa;
2) $n = 6$, $a = 2$, $b = 1$.
(ii) *$a^n + b^n$-nek minden $n > 1$ egészre van primitív prímosztója, kivéve azt az esetet, amikor* $n = 3$, $a = 2$, $b = 1$.

Terjedelmi okok miatt a bizonyítást mellőzzük. A tétel egy elemi bizonyítása megtalálható például W. Narkiewicz „Classical problems in number theory" (Warszawa,1986) című könyvében, a 11–15. oldalon.

Az *1. Tétel* szerint $a^n - b^n$ primitív prímosztói $nk + 1$ alakúak, míg $a^n + b^n$ páratlan primitív prímosztói $2nk + 1$ alakúak. Ezért a *2. Tétel* következtében az is adódik, hogy az **(ii)**-ben szereplő kivételtől eltekintve az $a^n \pm b^n$ számoknak $n > 2$ esetén mindig van n-nél nagyobb prímosztójuk. Újabb kutatások szerint ezeknek a számoknak lényegesen nagyobb prímosztójuk is van, ha n-nek nincs „túl sok" különböző prímosztója. Ennek bizonyításához azonban az elemi módszerek már nem elegendőek.

A B. feladat vizsgálata

Legyenek $a > b > 0$ továbbra is rögzített relatív prím egészek. A B. Feladat általánosításaként tekintsük most az összes olyan n egészeket, melyekre

$$n^2|a^n - b^n,\ n > 1 \text{ egész}, \tag{6}$$

valamint az összes olyan n egészeket, melyekre

$$n^2|a^n + b^n,\ n > 1 \text{ egész}. \tag{7}$$

Ezek tulajdonképpen diofantikus problémák, hiszen (6) egyenértékű az $a^n - b^n = n^2 \cdot m$, (7) pedig az $a^n + b^n = n^2 \cdot m$ diofantikus egyenlet pozitív egész n, m megoldásainak a megkeresésével.

Az 1. és 2. Tételek, valamint az *1. Következmény* felhasználásával be fogjuk bizonyítani a következő tételt. Jelöljük $\omega(n)$-nel egy $n > 1$ egész szám különböző prímosztóinak a számát.

3. Tétel. (i) *Ha $a-b=1$, úgy nincs olyan n egész, melyre* (6) *teljesül. Ha pedig $a-b>1$, úgy bármely $r \geqq 1$ egész esetén van olyan n, melyre* (6) *és $\omega(n)=r$ fennáll. Továbbá, az ilyen n értékek száma véges és mindezen n-ek meghatározhatók.*[1]

(ii) *Ha $(a+b)$ a 2 egy hatványa, úgy nincs olyan n, melyre* (7) *teljesül. Ha pedig $a=2$, $b=1$, úgy $n=3$ az egyetlen olyan n, melyre* (7) *fennáll. Minden más esetben bármely $r \geqq 1$ egészre van olyan n, melyre* (7) *és $\omega(n)=r$ teljesül. Továbbá, az ilyen n-ek száma véges és mindezen n-ek meghatározhatók.*

A tételből speciálisan adódik, hogy a *B. Feladat* egyetlen megoldása $n=3$. Tételünkből az is következik, hogy a *B. Feladat* állítása kivételes esetnek számít, hiszen $a=2$, $b=1$ az egyetlen olyan eset, amikor (7)-nek n-ben van megoldása, de a megoldásszám véges. Megjegyezzük, hogy a *3. Tétel* bizonyítása során a *2. Tételt* csak annak igazolására fogjuk felhasználni, hogy a felsorolt kivételektől eltekintve (6), illetve (7)-nek bármely $r \geqq 1$-re van $\omega(n)=r$ tulajdonságú n megoldása. Így a *B. Feladat* bizonyítása nem igényli a *2. Tétel* alkalmazását.

Tételünk mutatja, hogy a felsorolt a, b kivételektől eltekintve, mind a (6) tulajdonságú, mind a (7) tulajdonságú n-ek száma végtelen. A *3. és 2. Tétel* következményeként megmutatjuk, hogy bizonyos értelemben lényegesen „többen" vannak azok az n értékek, melyekre $n|a^n-b^n$, illetve $n|a^n+b^n$ teljesül.

2. Következmény. (i) *Ha $a-b>1$, úgy bármely $r \geqq 1$ egész esetén létezik végtelen sok olyan n, melyre $n|a^n-b^n$, és $\omega(n)=r$.*

(ii) *Bármely $r \geqq 2$ egész esetén létezik végtelen sok olyan n, melyre $n|a^n+b^n$ és $\omega(n)=r$.*

A *3.Tétel* bizonyításához szükségünk lesz két lemmára. Közülük az alábbi önmagában is érdekes állítás.

2. Lemma. *Legyen p egy prímszám. Ekkor*

$$\left(a-b,\ \frac{a^p-b^p}{a-b}\right)=\begin{cases}1, & \text{ha} \quad p\nmid a-b,\\ p, & \text{ha} \quad p|a-b.\end{cases}$$

Ha $p>2$, úgy az utóbbi esetben $p^2\nmid \dfrac{a^p-b^p}{a-b}$.

A második állítás $p=2$ esetén nem igaz, mint erről az $a=3,\ b=1$ választás mellett könnyen meggyőződhetünk.

A lemmából azonnal adódik, hogy

$$\text{ha} \quad p|a-b, \quad \text{úgy} \quad p^2|a^p-b^p, \tag{8}$$

továbbá

$$\text{ha} \quad p>2 \quad \text{és} \quad p|a+b, \quad \text{úgy} \quad p^2|a^p+b^p. \tag{9}$$

Ezeket az állításokat többször felhasználjuk, esetenként külön említés nélkül.

A *2. Lemma bizonyítása.* Az $a-b=u$, $\dfrac{a^p-b^p}{a-b}=v$ és $(u,v)=d$ jelöléseket bevezetve,

$$v=\frac{(b+u)^p-b^p}{u}=u^{p-1}+\binom{p}{1}u^{p-2}b+\ldots+\binom{p}{p-1}b^{p-1}. \tag{10}$$

Ebből következik, hogy $d|p\cdot b^{p-1}$. Mivel (d,b) osztója (u,b)-nek, (u,b) pedig (a,b)-nek, ezért $(d,b)=1$. Így viszont $d|p$, azaz $d=1$ vagy $d=p$. Ha $p|u$, úgy (10)-ből $p|v$, azaz $d=p$ következik. Ha pedig $p\nmid u$, úgy csak $d=1$ lehet. Ezzel az első állítást igazoltuk.

Ezután tegyük fel, hogy $p>2$ és $d=p$. Amennyiben $p^2|v$ volna, úgy (10)-ből $p^2|p\cdot b^{p-1}$, azaz $p|b$ következne. Ám ebben az esetben $p|u$ miatt $p|a$ adódna, ami nem lehetséges. Tehát valóban $p^2\nmid v$. ■

3. Lemma. (i) *Legyen $n>1$ egy* (6)*-ot kielégítő egész szám, s $2^\alpha\cdot k$ ($\alpha \geqq 0$ egész, k páratlan egész) az n legnagyobb olyan pozitív osztója, melynek minden prímfaktora osztója $a-b$-nek. Ekkor $2^\alpha k>1$, $k|a-b$ és ha $\alpha>0$, úgy $2^{\alpha+1}|a^2-b^2$.*

(ii) *Legyen $n>1$ egy* (7)*-et kielégítő egész szám, s $2^\alpha k$ ($\alpha \geqq 0$ egész, k páratlan) az n legnagyobb olyan pozitív osztója, melynek minden prímfaktora osztója $(a+b)$-nek. Ekkor $2^\alpha k>1$, $k|a+b$ és $2^\alpha|a^2-b^2$.*

A 3. Lemma bizonyítása. A bizonyítás során általánosabb formában fel fogjuk használni Pataki János egy ötletét a *B. Feladatra* adott megoldásából (Középiskolai Matematikai Lapok, 1990/8–9. szám, 340. old.)[2]

Először az **(i)** állítást bizonyítjuk. Az *1.Következmény***(i)** állításából következik, hogy n legkisebb prímfaktora osztója $2k$-nak, ezért $2^\alpha k>1$. Legyen p a $2^\alpha\cdot k$ egy tetszőleges prímfaktora, legyen $p^\beta \parallel 2^\alpha\cdot k$, és legyen $n=p^\beta\cdot m$ alkalmas $\beta \geqq 1$, m egészekkel. Ekkor $p\nmid m$, továbbá nyilván

[1] Ezen azt értjük, hogy a bizonyítás során egy olyan eljárást adunk, mely bármely konkrét a, b és r érték esetén elvileg lehetővé teszi az összes ilyen n-ek megtalálását. Ha a, b és r nem nagyok, akkor az eljárás a gyakorlatban is jól alkalmazható.

[2] Használjuk továbbá a $p^\delta \parallel A$ jelölést. Ez azt jelenti, hogy $p^\delta|A$, de $p^{\delta+1}\nmid A$, tehát A prímtényezős felbontásában a p prímszám kitevője δ.

(11) $$a^n - b^n = (a^m)^{p^\beta} - (b^m)^{p^\beta} = (a^m - b^m)\prod_{i=1}^{\beta}\frac{(a^m)^{p^i} - (b^m)^{p^i}}{(a^m)^{p^{i-1}} - (b^m)^{p^{i-1}}}.$$

Először tekintsük a $p = 2$ esetet. Ekkor $\beta = \alpha$. A (11) jobb oldalán a β tényezős szorzat tényezői $i = 2, \ldots, \beta$-ra 2-vel kongruensek $\pmod 4$. Ezért (11)-ből következik, hogy

(12) $$2^{\alpha+1} | a^{2m} - b^{2m}.$$

Ám $2|a^2 - b^2$ miatt

$$\frac{a^{2m} - b^{2m}}{a^2 - b^2} \equiv m(b^2)^{m-1} \pmod 2,$$

s minthogy $2 \nmid mb$, ezért (12)-ből $2^{\alpha+1}|a^2 - b^2$ következik.

Ezután tegyük fel, hogy $p > 2$. Mivel $p|a^{mp^{i-1}} - b^{mp^{i-1}}$ minden $1 \leqq i \leqq \beta$-ra, ezért a *2. Lemma* következtében a (11) jobb oldalán a β tényezős szorzat minden tényezője p-nek pontosan az első hatványával osztható. Így viszont (6)-ból és (11)-ből következik, hogy

(13) $$p^\beta | a^m - b^m.$$

Viszont $p|a - b$ miatt

$$\frac{a^m - b^m}{a - b} \equiv mb^{m-1} \pmod p,$$

s mivel $p \nmid mb$, ezért (13)-ból következik, hogy $p^\beta | a - b$. Mivel pedig ez a k minden prímhatványosztójára teljesül, ezért $k|a - b$ következik, s ezzel az állítást bebizonyítottuk.

Ezután rátérünk az **(ii)** állítás bizonyítására. Az *1. Következmény* **(ii)** állításából következik, hogy n legkisebb prímosztója osztója $a + b$-nek, tehát $2^\alpha \cdot k > 1$. Legyen p a $2^\alpha \cdot k$ egy tetszőleges prímfaktora, s legyen ismét $p^\beta \parallel 2^\alpha \cdot k$. Ekkor (7), $a^n + b^n | (a^2)^n - (b^2)^n$ és a fentebb bizonyított **(i)** állítás miatt $p^\beta | a^2 - b^2$, ha $p > 2$, és $p^{\alpha+1} | a^4 - b^4$, ha $p = 2$. Ám $p = 2$ esetén ebből $p^\alpha | a^2 - b^2$ következik, mivel $a^4 - b^4 = (a^2 - b^2)(a^2 + b^2)$ és $a^2 + b^2 \equiv 2 \pmod 4$. Ha viszont $p > 2$, úgy $p \nmid a - b$, ezért $p^\beta | a + b$. Ezzel a lemma **(ii)** állítását is igazoltuk. ■

A *3. Tétel bizonyítása.* Először az **(i)**állítást bizonyítjuk. Ha n eleget tesz (6)-nak, úgy az *1. Következmény* miatt n legkisebb prímfaktora osztója $(a - b)$-nek. Következésképpen $a - b = 1$ esetén valóban nincs olyan n, melyre (6) teljesül.

Ezután tegyük fel, hogy $a - b > 1$. Az r szerinti teljes indukcióval megmutatjuk, hogy bármely $r \geqq 1$ esetén van olyan n_r, melyre (6) és $\omega(n_r) = r$ teljesül. Legyen p_1 az $a - b$ legnagyobb prímfaktora. Ekkor (8) következtében $n_1 = p_1$-re teljesül (6) és $\omega(n_1) = 1$. *A 2. Tétel* **(i)** állítása szerint $a^{p_1} - b^{p_1}$-nek van primitív prímosztója, mondjuk p_2, kivéve azt az esetet, amikor $p_1 = 2$ és $(a + b)$ a 2 egy hatványa, azaz $a = 2^{\beta+1}$, $b = 2^\beta - 1$ valamely $\beta \geqq 1$ egésszel. Ettől az esettől eltekintve $p_2^2 | (a^{p_1})^{p_2} - (b^{p_1})^{p_2}$. Mivel az *1. Tétel* szerint $p_2 > p_1$, ezért innen kapjuk, hogy (6) $n_2 = p_1 p_2$ -re is teljesül és $\omega(n_2) = 2$. Először vegyük azt az esetet, amikor $\{a, b\}$ különbözik az említett kivételektől. Tegyük fel, hogy $r \geqq 2$-re már igazoltuk n_r létezését a (6) és $\omega(n_r) = r$ tulajdonsággal. Az *1. és 2. Tétel* szerint $a^{n_r} - b^{n_r}$-nek van egy $p_{r+1} > n_r$ primitív prímosztója, melyre (8) miatt $p_{r+1}^2 | (a^{n_r})^{p_{r+1}} - (b^{n_r})^{p_{r+1}}$. Így viszont $n_{r+1} = n_r p_{r+1}$-re (6) és $\omega(n_{r+1}) = r + 1$ teljesül, amivel az állítást bebizonyítottuk.

Tekintsük ezután azt az esetet, amikor $a = 2^\beta + 1$, $b = 2^\beta - 1$. Könnyű belátni, hogy (6) teljesül $n_1 = 2^\beta$-ra, ha $\beta \geqq 2$, és $n_1 = 2^{\beta+1}$-re, ha $\beta = 1$, másfelől mindkét esetben $\omega(n_1) = 1$. Ezután a bizonyítás r szerinti indukcióval folytatható a fenti módon, és ismét adódik az állítás.

Ezután megmutatjuk, hogy adott a, b és $r \geqq 1$ esetén csak véges sok olyan n van, melyre (6) és $\omega(n) = r$ teljesül, és eljárást adunk az összes ilyen n meghatározására. Legyen n egy tetszőleges pozitív egész, melyre (6) fennáll, s legyen $2^{\alpha_1} k_1$ ($\alpha_1 \geqq 0$, k_1 páratlan) az n legnagyobb olyan pozitív osztója, melynek minden prímosztója $a - b$-nek is osztója. Ekkor a *3. Lemma* szerint $2^{\alpha_1} k_1 > 1$, $k_1 | a - b$ és ha $\alpha_1 > 0$, úgy $2^{\alpha_1+1} | a^2 - b^2$. Tehát α_1 és k_1 csak véges sok értéket vehet fel, és a, b ismeretében az összes lehetséges értékek meghatározhatók. Ismételjük most ezt az eljárást n helyett $n_1 = n/2^{\alpha_1} k_1$-re, ahol $2^{\alpha_1} \cdot k_1$ értelmezése folytán relatív prím n_1-hez. Ha $n_1 > 1$, legyen $2^{\alpha_2} k_2$ az n_1 legnagyobb olyan pozitív osztója, melynek minden prímfaktora osztója $a^{2^{\alpha_1} k_1} - b^{2^{\alpha_1} k_1}$-nek. Mivel $(n_1,\ a - b) = 1$, ezért egyben $(2^{\alpha_2} k_2, a - b) = 1$. Az n-re (6) teljesül, ezért $n_1^2 | (a^{2^{\alpha_1} k_1})^{n_1} - (b^{2^{\alpha_1} k_1})^{n_1}$. Így $n_1 > 1$ esetén ismét alkalmazhatjuk a *3. Lemmát,* s arra jutunk, hogy $2^{\alpha_2} k_2 > 1$, $k_2 | (a^{2^{\alpha_1} k_1} - b^{2^{\alpha_1} k_1})/(a - b)$ és $2^{\alpha_2+1} | (a^{2^{\alpha_1+1} k_1} - b^{2^{\alpha_1+1} k_1})/a - b$. Itt α_2, k_2 ismét csupán véges sok és meghatározható értéket vehet fel. Ezt az eljárást n helyett az $n_i = n/(2^{\alpha_1} k_1) \ldots (2^{\alpha_i} k_i)$ számokkal $i = 2, 3, \ldots$ -ra folytatva, véges sok lépésben arra jutunk, hogy

(14) $$n = (2^{\alpha_1} k_1)(2^{\alpha_2} k_2) \ldots (2^{\alpha_s} k_s),$$

ahol $\alpha_i \geqq 0,\ k_i$ páratlan, $2^{\alpha_i} \cdot k_i > 1$, a $2^{\alpha_i} \cdot k_i$ számok páronként relatív prímek, s az α_i-k és k_i-k mindegyike csak véges sok és meghatározható értéket vehet fel minden i -re, $1 \leqq i \leqq s$. Itt nyilván $s \leqq \omega(n)$. Ha most $r \geqq 1$ adott, és az $\omega(n) = r$ tulajdonságú megoldásait keressük (6)-nak, úgy elegendő valamennyi $s \leqq r$-re az összes (14) alakú számot meghatározni, s ezek közül kiválogathatjuk (6)-nak az $\omega(n) = r$ tulajdonságú megoldásait.

Ezután az **(ii)** állítást bizonyítjuk. Ha $(a+b)$ a 2 egy hatványa, és (7) teljesülne valamely n-re, úgy az *1. Következmény* miatt az n páros volna. Ekkor viszont (7) miatt $2^2 | a^n + b^n$ következne, ami nem lehetséges. Ezért csupán azzal az esettel foglalkozunk, amikor $(a+b)$ nem 2-hatvány. Tegyük fel, hogy az $\{a, b\}$ pár különbözik a $\{2, 1\}$ pártól. Az r szerinti teljes indukcióval megmutatjuk, bármely $r \geqq 1$ esetén van olyan n_r, melyre (7) és $\omega(n_r) = r$ teljesül. Legyen p_1 az $(a+b)$ egy páratlan prímfaktora. Ekkor (9) miatt $n_1 = p_1$-re teljesül (7) és $\omega(n_1) = 1$. Tegyük fel, hogy valamely $r \geqq 1$ mellett már igazoltuk n_r létezését a (7) és $\omega(n_r) = r$ tulajdonsággal. A *2. Tétel* szerint $(a^{n_r} + b^{n_r})$-nek van egy p_{r+1} primitív prímfaktora, s könnyű belátni, hogy $p_{r+1} > 2$. Az *1. Tétel* szerint $p_{r+1} > n_r$, és (9) miatt $p_{r+1}^2 | (a^{n_r})^{p_{r+1}} + (b^{n_r})^{p_{r+1}}$. Ebből következik, hogy (7) $n_{r+1} = n_r p_{r+1}$-re is teljesül és $\omega(n_{r+1}) = r+1$. Ezzel az állítást igazoltuk.

A következőkben megmutatjuk, hogy adott $r \geqq 1$ mellett csak véges sok olyan n létezik, melyre (7) és $\omega(n) = r$ teljesül, s az összes ilyen n meghatározható. Legyen n egy tetszőleges egész, melyre (7) teljesül, s legyen $2^{\alpha_1} k_1$ ($\alpha_1 \geqq 0$ egész, k_1 páratlan) az n legnagyobb olyan pozitív osztója, melynek minden prímfaktora osztója $(a+b)$-nek. Ekkor a *3. Lemma* szerint $2^{\alpha_1} k_1) > 1,\ k_1 | a+b$ és $2^{\alpha_1} | a^2 - b^2$, ezért α_1, k_1 csak véges sok és meghatározható értéket vehet fel. Legyen $n_1 = n/2^{\alpha_1} k_1$. Ekkor n_1 és $a+b$ relatív prímek. Ha $n_1 > 1$, ismételjük meg ezt az okoskodást n helyett n_1-gyel. Legyen $2^{\alpha_2} k_2$ az n_1 legnagyobb olyan pozitív osztója, melynek minden prímosztója osztója $a^{2^{\alpha_1} k_1} + b^{2^{\alpha_1} k_1}$-nek. Mivel $n_1^2 | (a^{2^{\alpha_1} k_1})^{n_1} + (b^{2^{\alpha_1} k_1})^{n_1}$, ismét a *3. Lemma* szerint $2^{\alpha_2} | a^{2^{\alpha_1+1} k_1} + b^{2^{\alpha_1+1} k_1}$ és $k_2 | a^{2^{\alpha_1} k_1} + b^{2^{\alpha_1} k_1}$. Továbbá $(k_2, a+b) = 1$. Ha $a = 2,\ b = 1$, úgy ebből $\alpha_1 = 0,\ k_1 = 3,\ \alpha_2 = 0,\ k_2 = 1$ adódik. Tehát ekkor $n_1 = 1$, azaz $n = 3$ az egyetlen megoldása (7)-nek, s ezzel megkaptuk az olimpiai feladat megoldását. A továbbiakban az $a = 2,\ b = 1$ esetet kizárjuk.

A (7)-ből következik, hogy

$$n^2 | (a^2)^n - (b^2)^n. \tag{15}$$

Ezért alkalmazhatjuk az **(i)** részben bemutatott eljárást a, b helyett a^2, b^2-tel, s arra jutunk, hogy csak véges sok n létezik a (15) és $\omega(n) = r$ tulajdonsággal, s mindezen n-ek meghatározhatók. Ezen n-ek közül pedig kiválogathatók azok, melyekre nemcsak (15), hanem még (7) is fennáll. Ezzel a tételt bebizonyítottuk. ■

A 2. *Következmény bizonyítása.* Először az **(i)** állítást igazoljuk. Legyen $a - b > 1$. Elég megmutatni egy olyan, $\omega(n) = r$ tulajdonsággal rendelkező $n > 1$ egész létezését, melyre minden $k \geqq 1$ egész mellett

$$n^k | a^{nk} - b^{nk}. \tag{16}$$

A k szerinti teljes indukcióval bizonyítunk. $k = 1$ esetén ilyen n létezik a 3. *Tétel* **(i)** állítása következtében. Rögzítsünk egy ilyen n-et. Feltéve, hogy (16) valamely $k \geqq 1$-re már bizonyított, $a^{n^k} = b^{n^k} + n^k \cdot t$ következik alkalmas t egésszel. Mindkét oldalt n-edik hatványra emelve és a binomiális tételt alkalmazva adódik (16) k helyett $k+1$-gyel, s így (16) valóban minden k-ra teljesül.

Ezután az **(ii)** állítást igazoljuk. A 3. *Tétel* **(ii)** állításából következik, hogy az ott felsorolt $\{a, b\}$ kivételektől eltekintve bármely $r \geqq 2$ egészre van olyan n, melyre

$$n | a^n + b^n \text{ és } \omega(n) = r. \tag{17}$$

Megmutatjuk, hogy ez az állítás a *3. Tétel* **(ii)** állításának $\{a, b\}$ kivételeire is teljesül. Legyen $(a+b)$ először a 2 egy hatványa. Ekkor $2 | a^2 + b^2$. Az r szerinti teljes indukcióval bebizonyítjuk, hogy létezik olyan n_r, hogy $n = 2n_r$-re (17) teljesül. Nyilván $a^2 + b^2$-nek van egy p_1 páratlan prímosztója, s így (17) $r = 2$-re az $n = 2n_2,\ n_2 = p_1$ választás mellett teljesül. Ezután feltéve, hogy valamely $r \geqq 2$ -re az állítás már bizonyított, $a^{2n_r} + b^{2n_r}$-nek a *2.* és *1. Tétel* következtében van egy $p_{r+1} > n_r$ páratlan primitív prímosztója. Így viszont (17) az $n = 2n_{r+1},\ n_{r+1} = n_r p_{r+1}$ mellett r helyett $r+1$-re is teljesül.

Ezután legyen $a = 2,\ b = 1$. Az r szerinti teljes indukcióval belátjuk, hogy van olyan $n = n_r$, melyre (17) teljesül. Ha $r = 1$, úgy $n_1 = 3$ választható. Feltéve, hogy az állítás valamely $r \geqq 1$-re már bizonyított, a *2. és 1. Tétel* szerint $a^{n_r} + b^{n_r}$-nek van egy páratlan $p_{r+1} > n_r$ primitív prímosztója. Ekkor pedig (17) az $n_{r+1} = n_r p_{r+1}$ választással $r+1$-re is teljesül, s ezzel az állítást bebizonyítottuk.

Adott $r \geqq 2$ mellett legyen most n egy (17) tulajdonsággal rendelkező egész szám, s legyen $n = 2^\alpha m$, ahol $2 \nmid m$. Mivel $\omega(n) \geqq 2$, ezért $m \geqq 1$. A k szerinti teljes indukcióval megmutatjuk, hogy bármely $k \geqq 1$ egészre

$$2^\alpha m^k | a^{2^\alpha m^k} + b^{2^\alpha m^k}, \tag{18}$$

amiből már adódik a következmény állítása. (17) szerint (18) $k = 1$-re igaz. Feltéve, hogy (18) már valamely $k \geqq 1$-re igazolt, úgy $a^{2^\alpha m^k} = -b^{2^\alpha m^k} + 2^\alpha m^k \cdot t$ valamely t egésszel Itt mindkét oldalt m-edik hatványra emelve és a jobb oldalon a binomiális tételt alkalmazva adódik (18) a k helyett $k+1$-gyel, s így (18) valóban minden k-ra igaz. Ezzel a *3. Tétel 2. Következményének* bizonyítását befejeztük. ■

Természetes kérdésként merül fel, hogy általánosabban, adott $k \geqq 2$ egész esetén mit lehet mondani azon n-ekről, melyekre

$$n^k | a^n - b^n, \quad \text{illetve} \tag{19}$$

$$n^k | a^n + b^n, \quad n > 1 \quad \text{egész.} \tag{20}$$

A *3. Tételből* azonnal következik, hogy adott $r \geqq 1$ egész mellett legfeljebb véges sok n létezik a (19) vagy (20) tulajdonsággal, melyre $\omega(n) = r$, s mindezen n-ek meghatározhatók. Annak eldöntése azonban, hogy a, b-től függően mely r számokra vagy hány r számra létezik ilyen n, a $k > 2$-re már jóval nehezebb problémának látszik, mint a $k = 2$ esetben (amikor is ezt a problémát a *3. Tétellel* elintéztük).

Végül megjegyezzük, hogy az $a^n \pm b^n$ alakú számok osztóival kapcsolatos további eredmények, alkalmazások és irodalmi hivatkozások találhatók például Erdős Pál és Surányi János „Válogatott fejezetek a számelméletből" (Tankönyvkiadó, Budapest, 1960) című könyvében, L. E. Dickson „History of the theory of numbers" (New York, 1971) című könyvének I. kötetében, Narkiewicz említett munkájában, valamint C. L. Stewart „On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers" (Proc. London Math. Soc. 35 (1977), 425–447) cikkében.