A FIBONACCI-FÉLE SZÁMOK SZEREPE BIZONYOS PREDIKÁTUMOKNÁL

Írta: SZEDERKÉNYI ANTAL

JU. V. MATIJASZEVICS, HILBERT 10. problémájának megoldása kapcsán [1, 2] bebizonyítja a következőt:

(1) *A „v a 2u-adik Fibonacci-féle szám" predikátum exponenciálisan nő és ugyanakkor diofantoszi is.*

M. DAVIS, M. PUTNAM és J. ROBINSON munkáiból következik, hogy *ha legalább egy diofantoszi predikátum exponenciálisan nő, akkor bármely rekurzíve megszámlálható predikátum diofantoszi.*

Így bizonyítást nyer a következő állítás:

Bármely rekurzíve megszámlálható predikátum diofantoszi.

MATIJASZEVICS az (1) tétel bizonyítását 19 lemma alapján végzi el, de ezek bizonyítására csak utalás történik. Ezért ebben a dolgozatban részletes bizonyítását kívánjuk adni a lemmáknak.

1. definíció. $\varphi_0 = 0, \quad \varphi_1 = 1, \quad \varphi_{n+1} = \varphi_n + \varphi_{n-1} \qquad (n \geqq 1).$

φ_j-t a *j-edik* FIBONACCI-*féle szám*nak nevezzük.

1. lemma. $\varphi_{2(n+1)} = 3\varphi_{2n} - \varphi_{2(n-1)}.$

Bizonyítás. Definíció szerint

$$\varphi_{2n} = \varphi_{2n-1} + \varphi_{2n-2}.$$

Ezt átrendezve a

$$\varphi_{2n-1} = \varphi_{2n} - \varphi_{2n-2}$$

egyenlőséget kapjuk. Adjunk hozzá mindkét oldalhoz $2\varphi_{2n}$-et. Ekkor a bal oldalon, kétszer alkalmazva a definíciót, φ_{2n+2}-t, a jobb oldalon pedig $3\varphi_{2n} - \varphi_{2n-2}$-t kapunk. Így igaz a lemma.

Következmény. $\varphi_{2(n-1)} = 3\varphi_{2n} - \varphi_{2(n+1)}.$

A rövidebb írásmód kedvéért vezessük be az

$$M = \varphi_{2k} + \varphi_{2k+2}$$

jelölést.

2. lemma. $\varphi_{2(k+j)} \equiv -\varphi_{2(k+1-j)} \pmod{M}, \quad 0 \leqq j \leqq k+1.$

Bizonyítás. Teljes indukcióval.

$j=0$-ra igaz a lemma, hiszen $\varphi_{2k} \equiv -\varphi_{2(k+1)} \pmod{M}$,

$j=1$-re igaz a lemma, hiszen $\varphi_{2(k+1)} \equiv -\varphi_{2k} \pmod{M}$.

Legyen j, $(j+1)$-re igaz a lemma. Ekkor bizonyítjuk, hogy $(j+2)$-re is igaz $(j+2 \leqq k+1)$. Bizonyítandó tehát, hogy

$$\varphi_{2(k+j+2)} \equiv -\varphi_{2(k+1-j-2)} \pmod{M}. \tag{2}$$

Az 1. lemma és következménye alapján

$$\varphi_{2(k+j+2)} = 3\varphi_{2(k+j+1)} - \varphi_{2(k+j)},$$

$$\varphi_{2(k-j-1)} = 3\varphi_{2(k-j)} - \varphi_{2(k-j+1)}.$$

Az indukciós feltevés szerint

$$\varphi_{2(k+j+1)} \equiv -\varphi_{2(k-j)} \pmod{M},$$

$$\varphi_{2(k+j)} \equiv -\varphi_{2(k-j+1)} \pmod{M}.$$

Így nyilván igaz (2).

3. lemma. $\varphi_{2(2k+1+j)} \equiv \varphi_{2j} \pmod{M}$.

Bizonyítás. Teljes indukcióval. $j=0$-ra az állítás:

$$\varphi_{2(2k+1)} \equiv \varphi_0 \equiv 0 \pmod{M}.$$

Ez a 2. lemmából következik, ha benne j helyébe $(k+1)$-et teszünk. Az 1. lemmát és a $j=0$-ra vonatkozó eredményünket felhasználva

$$\varphi_{2(2k+2)} \equiv 3\varphi_{2(2k+1)} - \varphi_{2.2k} \equiv -\varphi_{2.2k} \pmod{M}.$$

Ha most $j=k$ esetén alkalmazzuk a 2. lemmát

$$\varphi_{2k(2+2)} \equiv -\varphi_{2.2k} \equiv \varphi_2 \equiv 1 \pmod{M}$$

adódik, ami $j=1$-re a lemma állítását igazolja. Most tegyük fel, hogy igaz a lemma $(j-1)$, j-re $(j>0)$. Feltételezzük tehát a

$$\varphi_{2(2k+j)} \equiv \varphi_{2(j-1)} \pmod{M}$$

és

$$\varphi_{2(2k+1+j)} \equiv \varphi_{2j} \pmod{M}$$

kongruenciák érvényességét. Ezután bizonyítjuk, hogy igaz a lemma $(j+1)$-re. Bizonyítandó, hogy

$$\varphi_{2(2k+1+j+1)} \equiv \varphi_{2(j+1)} \pmod{M}.$$

Az 1. lemma, az indukciós feltevés, ill. újra az 1. lemma alapján kapjuk, hogy

$$\varphi_{2(2k+1+j+1)} \equiv 3\varphi_{2(2k+1+j)} - \varphi_{2(2k+j)} \equiv 3\varphi_{2j} - \varphi_{2(j-1)} \equiv \varphi_{2(j+1)} \pmod{M}.$$

És ezt kellett bizonyítanunk.

4. lemma. $\varphi_{2[(2k+1)i+j]} \equiv \varphi_{2j} \pmod{M}$.

Bizonyítás. Teljes indukcióval. $i=0$-ra az állítás triviális. Tegyük fel, hogy i-re igaz az állítás és bizonyítjuk, hogy $(i+1)$-re is igaz, azaz bizonyítjuk a

$$\varphi_{2[(2k+1)(i+1)+j]} \equiv \varphi_{2j} \pmod{M}$$

állítás érvényességét.

Alkalmazva a 3. lemmát, benne j helyett $[(2k+1)i+j]$-t írva, az indukciós feltevés felhasználásával

$$\varphi_{2[(2k+1)(i+1)+j]} \equiv \varphi_{2[(2k+1)i+2k+1+j]} \equiv \varphi_{2[(2k+1)i+j]} \equiv \varphi_{2j} \pmod{M}$$

adódik, q.e.d.

Következmény. $\varphi_{2[(2k+1)i+j]} \equiv \varphi_{2j} \pmod{M}$, ha $0 \leqq j \leqq k$,

$$\varphi_{2[(2k+1)i+j]} \equiv \varphi_{2k} + \varphi_{2k+2} - \varphi_{2(2k+1-j)} \pmod{M}, \quad \text{ha} \quad k+1 \leqq j \leqq 2k.$$

Bizonyítás. Az első állítás a 4. lemma újra állítása j-re vonatkozó megszorítással, míg a második állítás a 4. lemma felhasználásával a 2. lemmából adódik, ha benne j helyett $(j-k)$-t írunk.

2. definíció. Tetszőleges $m(\geqq 2)$-re

$$\psi_{m,0} = 0, \quad \psi_{m,1} = 1,$$

$$\psi_{m,n+1} = m\psi_{m,n} - \psi_{m,n-1} \qquad (n \geqq 1).$$

5. lemma. Ha $m \geqq 2$, $d \mid (m-3)$, akkor $\psi_{m,j} \equiv \varphi_{2j} \pmod{d}$.

Bizonyítás. j szerinti indukcióval. $j=0$-ra $\psi_{m,0} \equiv \varphi_0 \pmod{d}$, $j=1$-re $\psi_{m,1} \equiv \varphi_2 \pmod{d}$ azaz $1 \equiv 1 \pmod{d}$ a lemma állítása, amelyek nyilvánvalóan igazak. Tegyük fel, a lemma feltételei mellett, a

$$\psi_{m,j-1} \equiv \varphi_{2(j-1)} \pmod{d}$$

és

$$\psi_{m,j} \equiv \varphi_{2j} \pmod{d}$$

kongruenciák érvényességét is $(j \geqq 1)$. Ebből bizonyítjuk a

$$\psi_{m,j+1} \equiv \varphi_{2(j+1)} \pmod{d}$$

kongruencia érvényességét.

A 2. definíció szerint, benne n helyett j-t írva és az indukciós feltevés felhasználásával

$$\psi_{m,j+1} \equiv m\psi_{m,j} - \psi_{m,j-1} \equiv m\varphi_{2j} - \varphi_{2(j-1)} \pmod{d}$$

adódik. Végül az 1. lemma és a $d \mid (m-3)$ feltevés alapján kapjuk a

$$\psi_{m,j+1} \equiv m\varphi_{2j} - \varphi_{2(j-1)} \equiv m\varphi_{2j} - 3\varphi_{2j} + \varphi_{2(j+1)} \equiv \varphi_{2(j+1)} \pmod{d}$$

összefüggést, amit éppen bizonyítanunk kellett.

6. lemma. Ha a k, m, n, v számok olyanok, hogy $m \geqq 2$, $v < \varphi_{2k+1}$, $M \mid (m-3)$ és $\psi_{m,n} \equiv v \pmod{M}$, akkor léteznek olyan i, j számok, hogy

$$v = \varphi_{2j}, \quad n = (2k+1)i + j.$$

Bizonyítás. n-et $(2k+1)$-gyel maradékosan osztva, létezik olyan i és $j < 2k+1$, hogy

$$n = (2k+1)i + j.$$

Az 5. lemma és az n-re vonatkozó előbbi összefüggés alapján

$$\psi_{m,n} \equiv \varphi_{2[(2k+1)i+j]} \pmod{M}.$$

A 2. és 4. lemmák következménye alapján

$$\varphi_{2[(2k+1)i+j]} \equiv \varphi_{2j} \pmod{M}$$

vagy

$$\varphi_{2[(2k+1)i+j]} \equiv \varphi_{2k} + \varphi_{2k+2} - \varphi_{2(2k+1-j)} \pmod{M},$$

aszerint, hogy $0 \leqq j \leqq k$ vagy $k+1 \leqq j \leqq 2k$. Mivel $v < \varphi_{2k+1}$, ezért $v = \varphi_{2j}$, ahol $0 \leqq j \leqq k$. Ha $k+1 \leqq j \leqq 2k$, akkor $\varphi_{2(2k+1-j)} \leqq \varphi_{2k}$ és így

$$\varphi_{2k} + \varphi_{2k+2} - \varphi_{2(2k+1-j)} \geqq \varphi_{2k+2} > \varphi_{2k+1}$$

adódik.

Ezzel a lemmát teljes egészében bebizonyítottuk.

7. lemma. Ha $m \geqq 2$, $l \mid (m-2)$, akkor $\psi_{m,j} \equiv j \pmod{l}$.

Bizonyítás. j szerinti indukcióval.

$$j = 0\text{-ra} \quad \psi_{m,0} \equiv 0 \equiv j \pmod{l},$$

$$j = 1\text{-re} \quad \psi_{m,1} \equiv 1 \equiv j \pmod{l}$$

nyilvánvalóan.

Legyen a továbbiakban $j \geqq 1$ és tegyük fel, hogy

$$\psi_{m,j-1} \equiv j-1 \pmod{l} \quad \text{és} \quad \psi_{m,j} \equiv j \pmod{l},$$

a lemma feltevései mellett. Ekkor felhasználva $\psi_{m,j+1}$ definícióját, az indukciós feltevéseket, végül az $l \mid (m-2)$ feltevést, kapjuk a

$$\psi_{m,j+1} \equiv m\psi_{m,j} - \psi_{m,j-1} \equiv mj - j + 1 \equiv (m-2)j + 1 \equiv j+1 \pmod{l}$$

összefüggést, ami $(j+1)$-re a lemma állítását igazolja.

8. lemma. $\varphi_{i+1}^2 - \varphi_i \varphi_{i+1} - \varphi_i^2 = (-1)^i$.

Bizonyítás. i szerinti indukcióval. $i=0$-ra igaz a lemma, mivel a

$$\varphi_1^2 - \varphi_0 \varphi_1 - \varphi_0^2 = 1 = (-1)^0$$

összefüggést kapjuk behelyettesítéssel. Most tegyük fel, hogy i-re igaz a lemma és bizonyítsuk be a

$$\varphi_{i+2}^2 - \varphi_{i+1}\varphi_{i+2} - \varphi_{i+2}^2 = (-1)^{i+1}$$

összefüggést.

$$\varphi_{i+2} = \varphi_{i+1} + \varphi_i$$

definíció szerint és így

$$\varphi_{i+2}^2 - \varphi_{i+1}\varphi_{i+2} - \varphi_{i+1}^2 = \varphi_{i+2}(\varphi_{i+2} - \varphi_{i+1}) - \varphi_{i+2}^2 = \varphi_{i+2}\varphi_i - \varphi_{i+2}^2 =$$

$$= (\varphi_{i+1} + \varphi_i)\varphi_i - \varphi_{i+1}^2 = \varphi_{i+1}\varphi_i + \varphi_i^2 - \varphi_{i+1}^2 =$$

$$= -(\varphi_{i+1}^2 - \varphi_i\varphi_{i+1} - \varphi_i^2) = -(-1)^i = (-1)^{i+1},$$

ami $(i+1)$-re bizonyítja a lemmát. Q.e.d.

9. lemma. Ha a $j, k (\geqq 1)$ számok olyanok, hogy

$$(k^2 - jk - j^2)^2 = 1,$$

akkor létezik egy olyan i szám, hogy

$$j = \varphi_i, \quad k = \varphi_{i+1}.$$

Bizonyítás. Indirekt úton. Tegyük fel, hogy van olyan j, k, amelyre

$$(k^2-jk-j^2)^2 = 1,$$

de nem létezik olyan i, hogy

$$j=\varphi_i, \quad k=\varphi_{i+1}.$$

Legyen j, k olyan az előbbi tulajdonságú számok között, amelyre $j+k = n$ minimális. $j=0$ nem lehet, hiszen ekkor $k=1$ a feltevés szerint és $i=0$ jó lenne, mert

$$\varphi_0=0=j, \quad \varphi_1=1=k.$$

Így $j>0$, ekkor $j\leqq k$, mivel $j>k$ esetén $j\geqq k+1$ és ekkor

$$k^2-jk-j^2 \leqq k^2-(k+1)k-(k+1)^2 = -k^2-3k-1 \leqq -5$$

lenne és így

$$(k^2-jk-j^2)^2 \neq 1$$

teljesülne. Ekkor belátjuk, hogy van olyan j_1, k_1, amelyre

$$j_1+k_1< n \quad \text{és} \quad (k_1^2-j_1k_1-j_1^2)^2 = 1.$$

Legyen ugyanis

$$j_1 = k-j, \qquad k_1 = j.$$

Ekkor

$$k_1^2-j_1k_1-j_1^2 = j^2-(k-j)j-(k-j)^2 = j^2+jk-k^2,$$

amiből

$$(k_1^2-j_1k_1-j_1^2)^2 = 1$$

következik.

Ehhez a j_1 és k_1-hez sincs i, hogy

$$j_1=\varphi_i \quad \text{és} \quad k_1=\varphi_{i+1}$$

lenne, ti. ellenkező esetben

$$j_1+k_1 = k = \varphi_i+\varphi_{i+1} = \varphi_{i+2}, \; k_1 = j = \varphi_{i+1}$$

lenne és ekkor $(i+1)$ jó lett volna j, k-hoz, feltevésünkkel ellentétben.

Tehát j_1, k_1 teljesíti a feltételeket, viszont az $n = j+k > j_1+k_1 = k$ összefüggés ellentmond n minimális voltának.

Ez az ellentmondás bizonyítja a lemma állítását.

10. lemma. Tetszőleges $m(\geqq 2)$-re igaz, hogy

$$\psi_{m,i+1}^2-m\psi_{m,i}\psi_{m,i+1}+\psi_{m,i} = 1.$$

Bizonyítás. Teljes indukcióval. $i=0$ esetén a

$$\psi_{m,1}^2-m\psi_{m,0}\psi_{m,1}+\psi_{m,0}^2 = 1^2 = 1$$

összefüggést kapjuk.

Most tegyük fel, hogy $(i-1)$-re igaz az állítás $(i\geqq 1)$. Ekkor $\psi_{m,i+1}$ definíciója és az indukciós feltevés miatt

$$\psi_{m,i+1}^2-m\psi_{m,1}\psi_{m,i+1}+\psi_{m,i}^2 = (m\psi_{m,i}-\psi_{m,i-1})^2-m\psi_{m,i}(m\psi_{m,i}-\psi_{m,i-1})+$$
$$+\psi_{m,i}^2 = \psi_{m,i}^2-m\psi_{m,i}\psi_{m,i-1}+\psi_{m,i-1}^2 = 1. \qquad \text{Q. e. d.}$$

11. lemma. Ha a j, k, m számok olyanok, hogy $m\geqq 2$, $j\leqq k$, és $k^2-mjk+j^2 = 1$ akkor létezik olyan i szám, hogy

$$j=\psi_{m,i}, \quad k=\psi_{m,i+1}.$$

Bizonyítás. Ha $k^2-mjk+j^2=1$ és $j\leqq k$, akkor $j<k$, ti. $j=k$ esetén

$$k^2-mk^2+k^2 \leqq 0.$$

Tegyük fel a továbbiakban, hogy $m\geqq 2$, $j\leqq k$, $k^2-mjk+j^2=1$ és nem létezik i, amelyre

$$j=\psi_{m,i},\ k=\psi_{m,i+1}.$$

Tegyük még fel azt is, hogy az ilyen tulajdonságú j, k számokra $(mk-j)$ minimális. [$(mk-j)$ legkisebb lehetséges értéke $m\cdot 1-0=m$ lenne.]

Megjegyzés. A feltevések között megemlítjük, hogy $(m-1)j<k\leqq mj$, ti. ellenkező esetben $mj<k$ vagy $k\leqq(m-1)j$. Az első esetben $mj+1\leqq k$ lenne. Ekkor

$$k^2-mjk+j^2 \geqq k^2+j^2-k(k-1)=j^2+k \geqq k \geqq 1$$

és egyenlőség csak $k=1$ és $j=0$ esetén áll fenn. Mivel

$$j=0=\psi_{m,0},\quad k=1=\psi_{m,1},$$

ezek a számok nem teljesítik a feltevést. Ha $k\leqq(m-1)j$ lenne, akkor $k+j\leqq mj$ miatt

$$k^2-mjk+j^2 \leqq k^2+j^2-k(k+j)=j^2-kj=j(j-k)\leqq 0$$

teljesülne, ami ellentmond a feltevésnek.

Legyen most $k_1=j$, $j_1=mj-k$. Ekkor

$$k^2-mj_1k_1+j_1^2=j^2-m(mj-k)j+(mj-k)^2=j^2-mjk+k^2=1.$$

$(m-1)j<k$ miatt $j_1=mj-k\leqq k_1=j$. Továbbá, nem létezik i, hogy

$$j_1=\psi_{m,i},\quad k_1=\psi_{m,i+1}$$

lenne. Ha ugyanis

$$j_1=mj-k=\psi_{m,i}\quad\text{és}\quad k_1=j=\psi_{m,i+1}$$

egy bizonyos i-re, akkor

$$k=mj-j_1=m\psi_{m,i+1}-\psi_{m,i}=\psi_{m,i+2}$$

és a j, k számokhoz is lenne megfelelő i. Tehát j_1, k_1 teljesíti a feltételeket, és

$$mk_1-j_1<mk-j,$$

hiszen

$$j<k\leqq(m-1)k=mk-k$$

miatt

$$mk_1-j_1=mj-(mj-k)=k<mk-j.$$

Ez pedig ellentmond $mk-j$ minimális voltának. A bizonyítást ezzel befejeztük.

Most kimondunk néhány olyan tételt, amelyek szükségesek a további lemmák bizonyításához.

1. tétel. $\varphi_{n+m}=\varphi_{n-1}\varphi_m+\varphi_n\varphi_{m+1}$.

Bizonyítás. [2]-ben.

12. lemma. $(\varphi_i,\varphi_j)=\varphi_{(i,j)}$.

Bizonyítás. [2]-ben

Következmény. $\varphi_n | \varphi_{jn}$.

Könnyen belátható a

2. tétel. $m|n$ akkor és csak akkor, ha $\varphi_m|\varphi_n$.

Bizonyítás. A 12. lemma következménye alapján ha $m|n$, akkor $\varphi_m|\varphi_n$. Most tegyük fel, hogy $\varphi_m|\varphi_n$. Ekkor egyrészt

$$(\varphi_m, \varphi_n)=\varphi_m,$$

másrészt a 12. lemma alapján

$$(\varphi_m, \varphi_n)=\varphi_{(m,n)}.$$

Ekkor $m=(m, n)$, azaz $m|n$. Q.e.d.

Vezessük be a következő jelölést:

$$a=M(b) \text{ akkor és csak akkor, ha } a\equiv b \pmod{\varphi_n}.$$

Ekkor nyilvánvalóan igazak a következő összefüggések: $a=M(b)$ akkor és csak akkor, ha $a=\varphi_n \cdot T+b$ bizonyos T-re.

(3)
$$M(a)+M(b) = M(a+b).$$
$$M(a)M(b)=M(ab).$$
$$a=M(a),\ M(\varphi_n)=0.$$

3. tétel.

$$\varphi_{kn+1}=M(\varphi_{n-1}^k).$$

Bizonyítás. k szerinti indukcióval. $k=0$-ra $\varphi_1=1=M(\varphi_{n-1}^0)=M(1)$ nyilvánvalóan teljesül. Tegyük fel, hogy $(k-1)$-re $(k\geqq 1)$ igaz a tétel és bizonyítsuk, hogy k-ra is igaz. Az 1. tétel, a (3) összefüggések és az indukciós feltevés alapján kapjuk, hogy

$$\varphi_{kn+1} = \varphi_{(n+1)+(k-1)n} = \varphi_n\varphi_{(k-1)n}+\varphi_{n+1}\varphi_{(k-1)n+1} = M(\varphi_{n-1})M(\varphi_{n-1}^{k-1}) = M(\varphi_{n-1}^k).$$

Tehát igaz a tétel k-ra. Így a tételt bebizonyítottuk.

4. tétel. $\varphi_{kn}=\varphi_n \cdot M(k \cdot \varphi_{n-1}^{k-1})$ $(k\geqq 1)$.

Bizonyítás. $k=1$-re az állítás

$$\varphi_n=\varphi_n \cdot M(1 \cdot \varphi_{n-1}^0)=\varphi_n,$$

ami nyilvánvalóan igaz.

Most tegyük fel, hogy k-ra igaz a tétel $(k\geqq 1)$ és bizonyítjuk $(k+1)$-re. Az 1. tétel alapján:

$$\varphi_{(k+1)n} = \varphi_{n+kn} = \varphi_{n-1}\varphi_{kn}+\varphi_n\varphi_{kn+1}.$$

Így az indukciós feltevés és a 3. tétel alapján

$$\varphi_{(k+1)n} = \varphi_{n-1}\varphi_n \cdot M(k \cdot \varphi_{n-1}^{k-1})+\varphi_n \cdot M(\varphi_{n-1}^k).$$

A (3) összefüggések alapján

$$\varphi_{(k+1)n} = \varphi_n \cdot M[(k+1)\varphi_{n-1}^k],$$

ami éppen a $(k+1)$-re vonatkozó állítás. Q.e.d.

5. tétel. Ha $4|\varphi_n$, akkor $8|\varphi_n$.

Bizonyítás. Feltesszük, hogy $8\nmid\varphi_n$. Ekkor $6\nmid n$, mivel $\varphi_6=8$ és $\varphi_6|\varphi_n$ akkor és csak akkor, ha $6|n$ a 2. tétel alapján. Így $n=6k+r$, ahol $0<r<6$. Ha r az 1, 2, 4, 5 számok valamelyike, akkor $3\nmid n$ és így $\varphi_3=2\nmid\varphi_n$ a 2. tétel szerint, tehát $4\nmid\varphi_n$. Ha $r=3$, $k>0$, akkor

$$\varphi_n=\varphi_{6k+3}=\varphi_{6k-1}\varphi_3+\varphi_{6k}\cdot\varphi_4=2\varphi_{6k-1}+3\varphi_{6k},$$

az 1. tétel és φ_3, φ_4 definíciója alapján.

Mivel $8|\varphi_{6k}$, ezért $4|3\varphi_{6k}$, de $2\nmid\varphi_{6k-1}$ és így $4\nmid 2\varphi_{6k-1}$, tehát $4\nmid\varphi_n$. Ha $r=3$, $k=0$ $\varphi_n=\varphi_3=2$ így $4\nmid\varphi_n$ ebben az esetben is. Következésképpen $4\nmid\varphi_n$ mindegyik esetben, ami bizonyítja a tételt.

6. tétel. $\varphi_{kn+1}\equiv\varphi_{n+1}^k \pmod{\varphi_n^2}$.

Bizonyítás. Teljes indukcióval. $k=0$-ra az állítás

$$\varphi_1\equiv\varphi_{n+1}^0 \pmod{\varphi_n^2},$$

ami nyilvánvalóan igaz. Tegyük fel, hogy igaz a tétel k-ra és bizonyítsuk be $(k+1)$-re is. Az 1. tétel, a 12. lemma következménye, az n indukciós feltevés alapján kapjuk, hogy

$$\varphi_{(k+1)n+1}\equiv\varphi_{(kn+1)+n}\equiv\varphi_{kn}\cdot\varphi_n+\varphi_{kn+1}\varphi_{n+1}\equiv\varphi_{kn+1}\varphi_{n+1}\equiv\varphi_{n+1}^{k+1} \pmod{\varphi_n^2},$$

ami a kívánt összefüggés. Ezzel a tételt bebizonyítottuk.

7. tétel. $\varphi_{pn}=\varphi_n\cdot\sum_{k=0}^{p-1}\varphi_{(p-1-k)n+1}\varphi_{n-1}^k \qquad (p\geqq 1)$.

Bizonyítás. p szerinti indukcióval. Ha $p=1$, akkor a

$$\varphi_n=\varphi_n\cdot\varphi_1\cdot\varphi_{n-1}^0$$

összefüggést kapjuk, ami igaz. Tegyük fel, hogy igaz az állítás p-re. Ekkor az 1. tétel szerint

$$\varphi_{(p+1)n}=\varphi_{n+pn}=\varphi_{n-1}\varphi_{pn}+\varphi_n\varphi_{pn+1}.$$

Ezután az indukciós feltevést használva kapjuk, hogy

$$\varphi_{(p+1)n}=\varphi_{n-1}\cdot\varphi_n\cdot\sum_{k=0}^{p-1}\varphi_{(p-1-k)n+1}\cdot\varphi_{n-1}^k+\varphi_n\cdot\varphi_{pn+1}=$$

$$=\varphi_n\left(\sum_{k=0}^{p-1}\varphi_{(p-1-k)n+1}\varphi_{n-1}^{k+1}+\varphi_{pn+1}\right)=\varphi_n\left(\sum_{k=1}^{p}\varphi_{(p-k)n+1}\varphi_{n-1}^k+\varphi_{pn+1}\right)=$$

$$=\varphi_n\cdot\sum_{k=0}^{p}\varphi_{(p-k)n+1}\varphi_{n-1}^k,$$

azaz igaz az állítás $(p+1)$-re is. Q.e.d.

Vezessük be a következő jelöléseket is:

$$A=\sum_{k=0}^{p-1}\varphi_{(p-1-k)n+1}\varphi_{n-1}^k,$$

$$B=\sum_{k=0}^{p-1}\varphi_{n+1}^{p-1-k}\cdot\varphi_{n-1}^k.$$

8. tétel. $A \equiv B \pmod{\varphi_n^2}$.

Bizonyítás. Ha A-nak minden tagjában az első tényezőre alkalmazzuk a 6. tételt akkor megkapjuk a kívánt állítást.

9. tétel.

$$B = \sum_{k=1}^{p-1} \binom{p}{k} \varphi_n^{p-1-k} \cdot \varphi_{n-1}^k.$$

Bizonyítás. Nyilvánvalóan

$$\varphi_{n+1}^p - \varphi_{n-1}^p = (\varphi_{n+1} - \varphi_{n-1}) \cdot B = \varphi_n \cdot B. \tag{4}$$

Most használjuk a $\varphi_{n+1} = \varphi_n + \varphi_{n-1}$ összefüggést. Így

$$\varphi_{n+1}^p - \varphi_{n-1}^p = (\varphi_n + \varphi_{n-1})^p - \varphi_{n-1}^p = \sum_{k=0}^{p} \binom{p}{k} \varphi_n^{p-k} \varphi_{n-1}^k - \varphi_{n-1}^p = \sum_{k=0}^{p-1} \binom{p}{k} \varphi_n^{p-k} \cdot$$

$$\cdot \varphi_{n-1}^k + \binom{p}{p} \varphi_n^0 \varphi_{n-1}^p - \varphi_n^p - 1 = \sum_{k=0}^{p-1} \binom{p}{k} \varphi_n^{p-k} \varphi_{n-1}^k = \varphi_n \cdot \sum_{k=0}^{p-1} \binom{p}{k} \varphi_n^{p-1-k} \varphi_{n-1}^k,$$

amit (4)-gyel összevetve, kapjuk a kívánt összefüggést.

13. lemma. a) Ha p, q törzsszámok és $p \mid \varphi_n$, $q \neq p$, akkor $p\varphi_n \nmid \varphi_{qn}$.

b) Ha p törzsszám és $p \neq 2$, $p \mid \varphi_n$, akkor $p\varphi_n \mid \varphi_{pn}$, de $p^2 \varphi_n \nmid \varphi_{pn}$.
c) Ha $2 \mid \varphi_n$, $4 \nmid \varphi_n$, akkor $4\varphi_n \mid \varphi_{2n}$, de $8\varphi_n \nmid \varphi_{2n}$.
d) Ha $4 \mid \varphi_n$, akkor $2\varphi_n \mid \varphi_{2n}$, de $4\varphi_n \nmid \varphi_{2n}$.

Bizonyítás. Ad a) Nyilvánvalóan, ha p, q prímszámok, $p \neq q$ és $p \mid \varphi_n$ akkor $p \nmid \varphi_{n-1}$ és igazak a következő ekvivalenciák:

$$p\varphi_n \mid \varphi_{qn} \Leftrightarrow p\varphi_n \mid \varphi_n \cdot M(q \cdot \varphi_{n-1}^{q-1})$$

(most a 4. tételt alkalmaztuk $k = q$-ra) $\Leftrightarrow p \mid M(q \cdot \varphi_{n-1}^{q-1}) = \varphi_n \cdot T + q\varphi_{n-1}^{q-1}$ bizonyos T-re $\Leftrightarrow p \mid q$ vagy $p \mid \varphi_{n-1}^{q-1} \Leftrightarrow p \mid q$ vagy $p \mid \varphi_{n-1}$. De $p \nmid q$ és $p \nmid \varphi_{n-1}$. Tehát $p\varphi_n \nmid \varphi_{qn}$.
Ad b). Most legyen $p \neq 2$ prímszám és $p \mid \varphi_n$. Ekkor

$$\varphi_{pn} = \varphi_n \cdot M(p\varphi_{n-1}^{p-1})$$

a 4. tétel szerint. Tehát $p\varphi_n \mid \varphi_{pn}$ akkor és csak akkor, ha $p \mid \varphi_n \cdot T + p \cdot \varphi_{n-1}^{p-1}$ bizonyos T-re. Ez utóbbi pedig nyilvánvalóan teljesül. $p^2 \varphi_n \nmid \varphi_{pn}$ bizonyításához elegendő belátni, hogy $p^2 \nmid B$, ti. a 7. tétel alapján $\varphi_{pn} = \varphi_n \cdot A$, és így $p^2 \varphi_n \nmid \varphi_{pn}$ akkor és csak akkor, ha $p^2 \nmid A$. Azonban a 8. tétel alapján $A = B + \varphi_n^2 \cdot T$ bizonyos T-re, és $p \mid \varphi_n$ miatt, $p^2 \nmid A$ akkor és csak akkor, ha $p^2 \nmid B$.

A 11. tétel összefüggését használva B-re kapjuk, hogy ha $p \mid \varphi_n$, akkor $p - 1 \geqq 2$ miatt $p^2 \mid \varphi_n^{p-1}$, $p \mid \binom{p}{k}$ miatt

$$p^2 \mid \binom{p}{k} \varphi_n^{p-1-k} \cdot \varphi_{n-1}^k, \quad \text{ha} \quad 0 < k < p - 1,$$

azonban $p^2 \nmid p \cdot \varphi_{n-1}^{p-1}$, mivel $p \nmid \varphi_{n-1}^{p-1}$. Tehát $p^2 \nmid B$.

Ad c) Tegyük fel, hogy $2 \mid \varphi_n$, $4 \nmid \varphi_n$. Mivel $\varphi_3 = 2$ és $\varphi_6 = 8$, a 2. tétel alapján $n = 6k + 3$ alakú. Ekkor az 1. tétel miatt

$$\varphi_{2n} = \varphi_{n+n} = \varphi_{n-1}\varphi_n + \varphi_n\varphi_{n+1} = \varphi_n(\varphi_{n-1} + \varphi_{n+1}).$$

Tehát $v\varphi_n|\varphi_{2n}$ akkor és csak akkor, ha

$$v|\varphi_{n-1}+\varphi_{n+1} = 2\varphi_{n-1}+\varphi_n. \tag{5}$$

Most k szerinti indukcióval bebizonyítjuk, hogy

$$4|2\varphi_{n-1}+\varphi_n, \quad \text{de} \quad 8\nmid 2\varphi_{n-1}+\varphi_n.$$

$k=0$ esetén

$$\varphi_{n-1}+\varphi_{n+1} = \varphi_2+\varphi_4 = 1+3 = 4,$$

tehát igaz az állítás.

Most tegyük fel, hogy k-ra, azaz n-re igaz. Ekkor bizonyítjuk, hogy $(k+1)$-re is, azaz $(n+6)$-ra is igaz. Mivel $\varphi_6=5$, $\varphi_5=8$, $\varphi_7=13$, az 1. tétel alapján

$$2\varphi_{n+5}+\varphi_{n+6} = 2(\varphi_{n-1}\varphi_5+\varphi_n\varphi_6)+\varphi_{n-1}\varphi_6+\varphi_n\varphi_7 =$$

$$= 18\varphi_{n-1}+29\varphi_n = 8\varphi_{n-1}+24\varphi_n+5(\varphi_n+2\varphi_{n-1})$$

adódik. Ebből az indukciós feltevést használva könnyen kapjuk az állítást.

Ad d) Ha $4|\varphi_n$ akkor $|\varphi_n+2\varphi_{n-1}$ és $4\nmid\varphi_n+2\varphi_{n-1}$, $4\nmid 2\varphi_{n-1}$ miatt (ti. $2\nmid\varphi_{n-1}$). Ekkor az (5) összefüggést figyelembe véve $2\varphi_n|\varphi_{2n}$, de $4\varphi_n\nmid\varphi_{2n}$.

14. lemma. Ha p törzszám és $p|\varphi_n$, $p\nmid r$, akkor $p\varphi_n\nmid\varphi_{rn}$.

Bizonyítás. A 4. tétel szerint

$$\varphi_{rn} = \varphi_n \cdot M(r\cdot\varphi_{n-1}^{r-1}) \quad r\geqq 1\text{-re.}$$

Így $p\varphi_n|\varphi_{rn}$ akkor és csak akkor, ha $p|M(r\cdot\varphi_{n-1}^{r-1})$, illetve ha $p|r\cdot\varphi_{n-1}^{r-1}$. Ez utóbbi pedig nyilvánvalóan nem teljesül

$$(\varphi_{n-1}, \varphi_n)=\varphi_{(n-1,n)}=1$$

miatt.

15. lemma. Ha p törzsszám és $p\neq 2$, $p|\varphi_n$, akkor

$$p^i\varphi_n|\varphi_{p^in}, \quad \text{de} \quad p^{i+1}\cdot\varphi_n\nmid\varphi_{p^in}.$$

Bizonyítás. i szerinti indukcióval. Tegyük fel, hogy p törzsszám, $p\neq 2$ és $p|\varphi_n$. $i=0$-ra nyilvánvalóan igaz az állítás.

Most tegyük fel, hogy $i(\geqq 0)$-ra igaz az állítás azaz

$$p^i\varphi_n|\varphi_{p^in}, \quad \text{de} \quad p^{i+1}\varphi_n\nmid\varphi_{p^in}, \tag{6}$$

és bizonyítjuk, hogy $(i+1)$-re is igaz tehát, hogy

$$p^{i+1}\varphi_n|\varphi_{p^{i+1}n}, \quad \text{de} \quad p^{i+2}\varphi_n\nmid\varphi_{p^{i+1}n}.$$

A 2. tétel szerint, ha $p|\varphi_n$, akkor $p|\varphi_{p^in}$. Alkalmazva a 13. lemma *b)* állítását

$$p\varphi_{p^in}|\varphi_{p^{i+1}n}, \quad \text{de} \quad p^2\varphi_{p^in}\nmid\varphi_{p^{i+1}n}.$$

Ha ezt kombináljuk a (6) indukciós feltevéssel, az $(i+1)$-re vonatkozó állítást kapjuk.

16. lemma. Ha $4|\varphi_n$, akkor $2^i\varphi_n|\varphi_{2^in}$, de $2^{i+1}\varphi_n\nmid\varphi_{2^in}$.

Bizonyítás. A 15. lemma bizonyításához hasonlóan történik.

17. lemma. $\varphi_s^2|\varphi_{rs}$ akkor és csak akkor, ha $\varphi_s|r$.

Bizonyítás. I. Tegyük fel először, hogy $\varphi_s | r$ és bizonyítsuk, hogy $\varphi_s^2 | \varphi_{rs}$. Írjuk fel φ_s-et kanonikus alakban és legyen ennek p^α valamelyik tényezője. Így $p^\alpha | r$. Ha $p \neq 2$, $p | \varphi_s$, akkor $p^\alpha \varphi_s | \varphi_{p^\alpha s} | \varphi_{rs}$ a 15. lemma alapján. Ha $p=2$, $\alpha=1$ azaz $2 | \varphi_s$, $4 \nmid \varphi_s$, akkor a 13. lemma alapján

$$2\varphi_s | 4\varphi_s | \varphi_{2s} | \varphi_{rs}.$$

Ha $p=2$, $\alpha>1$ azaz $4 | \varphi_s$, akkor a 16. lemma alapján kapjuk, hogy

$$2^\alpha \varphi_s | \varphi_{2^\alpha s} | \varphi_{rs}.$$

Így mindenképpen $p^\alpha \varphi_s | \varphi_{rs}$. Ebből pedig

$$\varphi_s \cdot \varphi_s = \varphi_s^2 | \varphi_{rs}$$

következik. (φ_s a prímhatványtényezőinek legkisebb közös többszöröse).

II. Most tegyük fel, hogy $\varphi_s \nmid r$ és bizonyítsuk, hogy $\varphi_s^2 \nmid \varphi_{rs}$. Ekkor vagy van olyan p prímszám, hogy $p | \varphi_s$, de $p \nmid r$, vagy van olyan p prímszám és $\alpha \geqq 1$ szám, hogy $p^{\alpha+1} | \varphi_s$, és $p^\alpha | r$, de $p^{\alpha+1} \nmid r$.

Az első esetben, ha $\varphi_s^2 | \varphi_{rs}$ volna, akkor $p\varphi_s | \varphi_{rs}$ következne, ami ellentmond a 14. lemma állításának.

A második esetben $r = p^\alpha \cdot T$ egy bizonyos T-re, ahol $p \nmid T$. Most tegyük fel, hogy $\varphi_s^2 | \varphi_{rs}$. A 15. illetve a 16. lemma szerint

$$p^{\alpha+1} \varphi_s \nmid \varphi_{p^\alpha \cdot s}. \tag{7}$$

A 2. tétel szerint

$$p | \varphi_s | \varphi_{p^\alpha s} | \varphi_{p^\alpha Ts},$$

így a 14. lemma alapján

$$p\varphi_{p^\alpha s} \nmid \varphi_{p^\alpha \cdot T \cdot s} = \varphi_{rs} \quad \text{(ugyanis } p \nmid T\text{)}.$$

Ezt (7)-tel összevetve kapjuk, hogy

$$p^{\alpha+1} \varphi_s \nmid \varphi_{rs},$$

ami $p^{\alpha+1} | \varphi_s$ miatt, ellentmond a $\varphi_s^2 | \varphi_{rs}$ feltételnek.

Következmény. Ha $\varphi_s^2 | \varphi_t$, akkor $\varphi_s | t$.

Bizonyítás. Ha $\varphi_s^2 | \varphi_t$, akkor $\varphi_s | \varphi_t$. Ebből, a 2. tétel alapján, $s | t$ következik, azaz $t = rs$, egy bizonyos r számra. Ekkor

$$\varphi_s^2 | \varphi_{rs},$$

amiből a 17. lemma alapján

$$\varphi_s | r | t$$

következik.

18. lemma. $2\varphi_{2n} < \varphi_{2(n+1)} \leqq 3\varphi_{2n}$ $\quad (n \geqq 1)$.

Bizonyítás. $n=1$-re az állítás:

$$2\varphi_2 = 2 < \varphi_4 = 3 \leqq 3\varphi_2 = 3,$$

ami nyilvánvalóan igaz. Ha $n>1$, akkor $\varphi_n < \varphi_{n+1}$ minden n-re és így

$$2\varphi_{2n} = \varphi_{2n} + \varphi_{2n} < \varphi_{2n} + \varphi_{2n+1} = \varphi_{2n+2},$$

illetve mivel $\varphi_{2(n-1)} \geqq 0$, az I. lemma alapján

$$\varphi_{2(n+1)} \leqq 3\varphi_{2n}.$$

19. lemma. $n \leqq 2^{n-1} \leqq \varphi_{2n} < 3^n \qquad (n \geqq 1).$

Bizonyítás. n szerinti indukcióval. $n=1$-re igaz az állítás, mivel

$$1 \leqq 2^0 \leqq \varphi_2 < 3^1.$$

Most tegyük fel, hogy igaz n-re és bizonyítsuk $(n+1)$-re. Az indukciós feltevés alapján

$$n+1 \leqq 2n \leqq 2 \cdot 2^{n-1} = 2^n,$$

illetve $2^{n-1} \leqq \varphi_{2n}$-ből, a 18. lemma felhasználásával

$$2^n \leqq 2\varphi_{2n} < \varphi_{2(n+1)},$$

azonkívül

$$\varphi_{2n} < 3^n\text{-ből} \quad \varphi_{2(n+1)} \leqq 3\varphi_{2n} < 3^{n+1}$$

következik.

IRODALOM

[1] Ju. V. Matijaszevics: Hilbert 10. problémájának megoldása. Matematikai Lapok, 21, 83—87, 1970.

[2] Ю. В. Матиясевич: Диофантовость перечислимых множеств. Доклады Акад. Наук СССР, 191, 279—282. 1970.

[3] N. N. Worobjow: Die Fibonaccischen Zahlen. Dt. Verlag der Wissenschaften Berlin, 1954.

РОЛЬ ЧИСЕЛ ФИБОНАЧЧИ У НЕКОТОРЫХ ПРЕДИКАТОВ

А. Седеркени

В этой работе автор даёт детальные доказательства лемм, выступающих в работе [1] Ю. В. Матиясевича.

DIE ROLLE DER FIBONACCISCHEN ZAHLEN BEI GEWISSEN PREDIKATEN

A. Szederkényi

In dieser Arbeit werden ausführliche Beweise der Hilfsätze, die in der Arbeit [1] von Ju. W. Matijasewitsch auftreten, angegeben.