Az Élet és Tudomány című folyóirat Gondolkodás iskolája rovatának ez évi 5. feladata a következő volt (némi átfogalmazással):

"Periodikus-e a kettőhatványok utolsó két számjegyéből alkotott sorozat?"

A kérdés az ún. "skatulyaelv" felhasználásával egyszerűen megválaszolható. A skatulyaelv lényege az az egyszerű tény, hogy ha $n+1$ tárgyat legfeljebb n skatulyába helyezünk, akkor valamelyik skatulyába legalább két tárgy kerül. A feladatunkban ezt úgy lehet kihasználni, hogy először megmutatjuk, hogy van két különböző kettőhatvány, amely ugyanarra a kétjegyű számra végződik. Valóban, az utolsó két jegy legfeljebb százféle lehet: 00, 01, ..., 99, és így az első 101 darab kettőhatvány között már lesz két olyan, amelyeknek utolsó két jegye azonos.

A következő észrevétel az, hogy ha a 2^k és a 2^m hatványok ugyanarra a kétjegyű számra végződnek, akkora 2^{k+1}-nek és a 2^{m+1}-nek is azonos az utolsó két jegye. Amikor ugyanis a 2^k számot kettővel szorozzuk, az eredmény utolsó jegye csak a 2^k szám utolsó két jegyétől függ, s ez az utolsó két jegy a 2^k és 2^m számoknál ugyanaz.

Ez azt jelenti, hogy ha 2^k és 2^m $(k<m)$ utolsó két jegye azonos, akkor a 2^{k+1} és 2^{m+1}, a 2^{k+2} és 2^{m+2}, ... számok is ugyanarra a két jegyre végződnek, vagyis a $2^k, 2^{k+1}, 2^{k+2}, \ldots, 2^{m-1}$ kettőhatványok utolsó két jegye a vizsgált sorozat egy periódusát adja.

Azonnal felmerül a kérdés, vajon mekkora a kettőhatványok utolsó két jegyéből alkotott sorozat legrövidebb periódusa. (Periódusón – és annak hosszán – általában a legrövidebb periódust értik, ezentúl mi is egyszerűen periódust mondunk legrövidebb periódus helyett.)

A skatulyaelvre támaszkodó bizonyításból láttuk, hogy 101 egymás utáni kettőhatvány között már van kettő, amelyek azonos kétjegyű számra végződnek, így a periódus hossza a százat nem haladja meg. Némi számolással felírhatjuk a periódust (csak az utolsó két jegyet kell kiszámolnunk), s a következő sorozatot kapjuk :

02, **04**, 08, 16, 32, 64, 28, 56, 12, 24, 48, 96, 92, 84, 68, 36, 72, 44, 88, 76,

52, **04**, 08, 16, ...

Látható tehát, hogy a várt 100 körüli periódushossz helyett a legrövidebb periódus hossza csupán 20.

Még egy fontos észrevételt tehetünk a sorozat kezdetével kapcsolatban. Jogosan merül fel ugyanis, hogy a $2^1=2$ utolsó két jegyén mit értsünk. A fenti sorozatban ezen a 02-t értettük. Jól mutatja azonban ennek a választásnak az önkényességét az, hogy a 02 ezután sehol sem fordul elő a periódusban, így a sorozatban sem. Az ilyen problémák elkerülése végett a sorozat periodikusságán azt értjük, hogy a sorozat valahonnan – nem feltétlenül az első tagtól kezdve – periodikus, s később majd látni fogjuk a magyarázatot a sorozat elejének szabálytalanságára. (A figyelmes olvasó észrevehette, hogy a feladatra adott előző bizonyítás is ilyen értelemben bizonyította a periodikusságot.)

Az eredeti feladatot általánosabban is megfogalmazhattuk volna úgy, hogy a kettőhatványoknak nem az utolsó két, hanem az utolsó k jegyéből alkotunk sorozatot, és ennek a periodikusságát vizsgáljuk. Az előző gondolatmenet minimális változtatással most is alkalmazható.

A bizonyításból azonban ismét csak annyi derül ki, hogy a periódus hossza 10^k-nál nem lehet nagyobb, de konkrét értéket nem kapunk, pedig már a $k=2$ esetben is láttuk, hogy a 10^2 becslés nagyon durva. Az alábbiakban azt vizsgáljuk, hogy hogyan lehetne ezt pontosabbá tenni. (Külön utalás nélkül ezentúl minden betű egész számot jelöl.)

A lényeges észrevétel az, hogy a periódus hosszára kapott 10^k nagyságú korlát jelentősen javítható, ha figyelembe vesszük, hogy nem az összes legfeljebb k-jegyű szám lehet a vizsgált periódus tagja. Egyrészt a periódus minden tagja osztható 2^k-nal, mint egy k-nál magasabb kettőhatvány és egy 10^k-nal osztható szám különbsége, másrészt egyetlen tag sem osztható 5-tel. Számoljuk össze, hogy hány legfeljebb k -jegyű szám van, amely 2^k-nal osztható, de 5-tel nem. A $0,\ 1,\ 2, \ldots,\ 10^k-1$ számok között nyilván $10^k : 2^k = 5^k$ darab 2^k-nal osztható szám van. Ebből le kell vonnunk a $2^k \cdot 5$-tel is osztható számok számát, ilyenekből $10^k : (2^k \cdot 5) = 5^{k-1}$ darab van. Így azt kaptuk, hogy $4 \cdot 5^{k-1}$ olyan legfeljebb k-jegyű szám van, amely a periódusban – oszthatósági meggondolások miatt – előfordulhat, s mivel a periódusban nincs két azonos tag, ezért legfeljebb ilyen hosszú a periódus.

Észrevehetjük, hogy a $k=1,\ 2$ esetben a periódus hosszára kapott $4 \cdot 5^{k-1}$ felső becslés pontos. Vajon igaz-e ez más k értékekre is?

Ha tudnánk, hogy a periódus hossza pontosan $4 \cdot 5^{k-1}$, akkor ez azt jelentené, hogy minden olyan legfeljebb k-jegyű szám valóban elő is fordul a periódusban, amely 2^k-nal osztható és 5-tel nem. Így pontosan megmondhatnánk, hogy - a sorrendtől eltekintve – mely k-jegyű számokra végződnek a kettőhatványok. Nézzük, mire használható ez a felismerés! Eközben egy kis kitérőt teszünk.

*

Az Élet és Tudomány 1985/51. számában megjelent a kitűzött alapfeladat megoldása, s utána több, igen nehéznek látszó kérdés merült fel a kettőhatványok számjegyeivel kapcsolatban: *Igaz-e például, hogy bizonyos kettőhatványtól kezdve már valamennyi kettőhatvány tízes számrendszerbeli alakjában a* $0, 1, \ldots, 9$ *számjegyek mindegyike előfordul? Vagy ellenkezőleg: van-e végtelen sok kettőhatvány, amely csak bizonyos számjegyeket – például egyest és kettest – tartalmaz?* (Egyáltalán a triviális 2^0 és 2^1-n kívül van-e még ilyen kettőhatvány?)

Megoldani nem fogjuk ezeket a problémákat, de rámutatunk arra, hogy a megoldás egy kézenfekvő útja nem járható, s közben egy érdekes tételt kapunk, amelynek egyszerű bizonyításához a fenti periódushossz pontos ismeretére is szükség van.

Ha azt szeretnénk megmutatni, hogy nem létezik végtelen sok olyan kettőhatvány, amely csak az 1 és a 2 számjegyekből áll, akkor természetesnek látszik a következő gondolat. A kettőhatványok utolsó k jegye (minden k természetes számra) periodikus. Ha tehát sikerülne igazolni, hogy valamely k-ra a kettőhatványok utolsó k jegyéből alkotott soro-

zat periódusának minden tagjában van egyestől és kettestől különböző számjegy, akkor egy bizonyos kettőhatványtól kezdve (ahonnan a periodikusság kezdődik) valamennyi kettőhatványnak már az utolsó k jegye is tartalmazna egyestől és kettestől különböző számjegyet. Úgy tűnik, hogy alkalmas k keresése és a periódus végigvizsgálása már inkább számítástechnikai probléma. Sajnos azonban ilyen k nem létezik, pontosabban igaz a következő:

Tétel: *Jelölje A a* 2, 4, 6, 8; *B az* 1, 3, 5, 7, 9 *számjegyek valamelyikét. Ekkor bármely k természetes szám esetén a kettőhatványok utolsó k jegyéből alkotott sorozat periódusában van olyan tag, amely csak az A és B számjegyekből áll.* (A periodikusság miatt ekkor természetesen végtelen sok olyan kettőhatvány van, amely csak A és B jegyekből álló k jegyű számra végződik.)

Először egy segédtételt igazolunk :

Lemma: *Létezik olyan pontosan k jegyű szám, amely osztható 2^k-nal és csak az A és B számjegyeket tartalmazza.*

k-ra vonatkozó teljes indukciót használunk.

$k = 1$ esetben az állítás nyilvánvaló, hiszen az egyjegyű A szám megfelel, mert osztható kettővel.

Tegyük fel, hogy valamely $k = m$ értékre már igazoltuk az állítást, igazoljuk most $k = m + 1$-re.

Az indukciós feltevés szerint van olyan s számunk, amely pontosan m jegyű, 2^m-nel osztható és csak az A és B jegyekből áll. Tekintsük az $s' = 10^m A + s$ és az $s'' = 10^m B + s$ számokat. Ezek nyilván $m + 1$ jegyű, csak az A és a B számjegyekből álló számok. Az is látszik, hogy mindkettő osztható 2^m-nel. Tegyük fel, hogy 2^{m+1}-nel már egyikük sem osztható. Ekkor $s' = 2^m r$, $s'' = 2^m p$ alakú, ahol r és p páratlan számok. De ekkor az $s' - s'' = 2^m(r - p)$ szám már 2^{m+1}-nel is osztható, ami nem lehetséges, mert $s' - s'' = 10^m(A - B)$ kettőnek csak az m-edik hatványával osztható (hiszen $A - B$ páratlan). Az ellentmondás azt igazolja, hogy s' és s'' közül az egyik 2^{m+1}-nel is osztható, s ezzel igazoltuk az állítást $k = m + 1$-re.

Most rátérünk a tétel bizonyítására. A lemma szerint létezik olyan k jegyű N szám, amely osztható 2^k-nal és csak az A és B számjegyekből áll. Természetesen ekkor N nem osztható 5-tel. Ez azt jelenti, hogy N teljesíti mindazokat a feltételeket, amelyek alapján az előző gondolatmenetben a periódus hosszára vonatkozó felső becslést 10^k-ról $4 \cdot 5^{k-1}$-re szorítottuk le (azaz 2^k-nal osztható, de 5-tel nem). Mint ahogy már előbb megjegyeztük, ha tudnánk, hogy a periódus hossza pontosan $4 \cdot 5^{k-1}$, akkor minden 2^k-nal osztható, de nem 0-ra végződő szám előfordulna a periódusban, tehát N is, azaz valóban lenne olyan kettőhatvány, amelynek utolsó k jegyéből alkotott szám éppen az N.

A következőkben megmutatjuk, hogy a vizsgált sorozat periódusának hossza pontosan $4 \cdot 5^{k-1}$, s ezzel tételünk bizonyítása is teljessé válik.

Keressük tehát a kettőhatványok sorozatában azt a két legközelebbi tagot, amelyeknek utolsó k jegye megegyezik. (Azt már láttuk $k = 2$ esetén, hogy ha két ilyen tagot találunk, akkor egyszersmind ennek a két tagnak a "távolsága" lesz a periódus hossza, és ez nyilván igaz tetszőleges k számra is.) Legyen tehát ez a két kettőhatvány 2^m és 2^{m+f} (f a periódus hossza). Az, hogy 2^m és 2^{m+f} azonos k jegyű számra végződik, nyilván ekvivalens azzal, hogy $10^k \mid 2^{m+f} - 2^m$, azaz $2^k \cdot 5^k \mid 2^m(2^f - 1)$. Megállapodtunk abban, hogy a sorozat periodikusságát egy bizonyos tagtól kezdve vizsgáljuk, célszerű tehát csak a legalább k jegyből álló kettőhatványoktól kezdeni a vizsgálatot. Ennek magyarázata nemcsak az, hogy pontosan értelmezhessük az utolsó k jegyet, hanem az, hogy $2^n > 10^k$ miatt $m \geqq k$ legyen, vagyis a fenti oszthatóságban 2^k-nal "egyszerűsíthessünk", azaz áttérhessünk az $5^k \mid 2^{m-k}(2^f - 1)$ feltételre. Az 5 és a 2^{m-k} relatív prímek, így ez az oszthatóság csak úgy teljesülhet, ha $5^k \mid 2^f - 1$.

Átfogalmaztuk tehát a feladatot: meg kell keresnünk azt a *legkisebb* f pozitív kitevőt, amelyre $5^k \mid 2^f - 1$. (Azért a legkisebbre van szükség, mert a lehető legrövidebb periódus hosszát keressük.)

Megmutatjuk, hogy valóban $f = 4 \cdot 5^{k-1}$ a keresett érték.

$k = 1$ esetben könnyen ellenőrizhető, hogy a 2^1, 2^2, 2^3, 2^4, ... sorozatban 2^4 az első, amely 1-et ad maradékul 5-tel osztva.

$k = 2$ esetben rövid számolás után adódik, hogy $25 \mid 2^{20} - 1$ és $f = 20$ az első ilyen szám. (Ennek a bizonyítása egyébként lényegében már megtörtént, amikor megállapítottuk, hogy a kettőhatványok utolsó két jegyéből alkotott sorozat periódusának hossza 20.)

Most tetszőleges $k > 2$ esetén igazoljuk az állítást.

Írjuk fel $2^4 = 16$-ot az alábbbi alakban:

$$2^4 = 1 + 5 \cdot t_0, \quad \text{ahol} \quad t_0 = 3, \quad \text{vagyis} \quad 5 \nmid t_0.$$

Ötödik hatványra emelve és a binomiális tétel szerint kifejtve:

$$2^{4 \cdot 5} = (1 + 5 \cdot t_0)^5 = 1 + \binom{5}{1} \cdot 5t_0 + \binom{5}{2} \cdot 5^2 t_0^2 + \binom{5}{3} \cdot 5^3 t_0^3 + \binom{5}{4} 5^4 t_0^4 + 5^5 t_0^5 =$$

$$= 1 + 5^2 \left(t_0 + \binom{5}{2} t_0^2 + \binom{5}{3} 5t_0^3 + \binom{5}{4} 5^2 t_0^4 + 5^3 t_0^5 \right) = 1 + 5^2 t_1.$$

Vegyük észre, hogy a zárójelben t_0 kivételével minden tag osztható 5-tel, így $5 \nmid t_1$.

Most újra ötödik hatványra emelünk, és az összevonások után alkalmas t_2 számmal a

$$2^{4 \cdot 5^2} = 1 + 5^3 t_2$$

egyenlőséget kapjuk, ahol $5 \nmid t_2$.

Ezt az eljárást folytatjuk tovább; általában az i-edik ismétlés után a $2^{4\cdot 5^i} = 1 + 5^{i+1} \cdot t_i$ egyenlőséget kapjuk, ahol $5 \nmid t_i$. Innen a $k-1$-edik ismétlés után:

$$2^{4\cdot 5^{k-2}} = 1 + 5^{k-1} \cdot t_{k-2} \text{ és} \tag{1}$$
$$2^{4\cdot 5^{k-1}} = 1 + 5^k \cdot t_{k-1}, \text{ahol } 5 \nmid t_{k-2}.$$

Az állítás egyik fele innen már következik, ugyanis az utóbbi egyenlőség éppen azt jelenti, hogy $5^k \mid 2^{4\cdot 5^{k-1}} - 1$. Meg kell még mutatnunk, hogy $f = 4 \cdot 5^{k-1}$ a *legkisebb* olyan pozitív szám, amelyre $5^k \mid 2^f - 1$, azaz f a legrövidebb periódus.

Jelölje q a legrövidebb periódus hosszát. (Azaz a legkisebb x számot, amelyre $5^k \mid 2^x - 1$.) Nyilvánvaló, hogy minden periódus a legrövidebb periódus többszöröse, azaz $q \mid f$. Figyelembe véve f prímtényezős felbontását, q csak $2^a \cdot 5^b$ alakú lehet, ahol a a 0, 1, 2 és b a 0, 1, ..., $k-1$ számok valamelyike.

Először megmutatjuk, hogy $b = k-1$. Tegyük fel, hogy $b < k-1$, ekkor $q \mid 4 \cdot 5^{k-2}$ lenne, azaz valamely u egész számra $4 \cdot 5^{k-2} = qu$ teljesülne. Felhasználva q tulajdonságát, kapjuk, hogy

$$5^k \mid (2^q)^u - 1^u, \quad \text{azaz} \quad 5^k \mid 2^{4\cdot 5^{k-2}} - 1.$$

Viszont (1) egyenlőség szerint $5^k \nmid 2^{4\cdot 5^{k-2}} - 1$ (lévén $5 \nmid t_{k-2}$). Az ellentmondás azt mutatja, hogy $b = k-1$. Megvizsgáljuk most, hogy a milyen értéket vehet fel:

$a = 0$ esetben $5^k \mid 2^{5^{k-1}} - 1$ lenne. Ez azért lehetetlen, mert $4 \mid 5^{k-1}$ ($k \geqq 2$), s így $5^{k-1} = 4v + 1$, azaz $2^{5^{k-1}} - 1 = 2\left[(2^4)^v - 1^v\right] + 1$, s itt az első tag osztható 5-tel, tehát $2^{5k-1} - 1$ nem osztható 5-tel.

$a = 1$ eset, azaz $5^k \mid 2^{2\cdot 5^{k-1}} - 1$ szintén ellentmondásra vezet, ugyanis az előzőek szerint $2 \cdot 5^{k-1} = 2(4v+1) = 4v' + 2$, s így $2^{2\cdot 5^{k-1}} - 1 = 4\left[(2^4)^{v'} - 1^{v'}\right] + 3$, s az első tag itt is osztható 5-tel.

Marad tehát az $a = 2$ eset, vagyis $f = q$. Ezzel igazoltuk, hogy az $f = 4 \cdot 5^{k-1}$ szám a legkisebb, amelyre $5^k \mid 2^f - 1$, tehát a kettőhatványok utolsó k jegye valóban $4 \cdot 5^{k-1}$ szerint periodikus.

Ezzel a bizonyítást befejeztük, és így a Tétel bizonyítása is teljes.

*

Most bizonyítás nélkül röviden összefoglaljuk azokat a számelméleti tényeket, amelyek kapcsolatban vannak az itt megoldott feladattal. Ezek felhasználásával általánosabban is vizsgálhatjuk a problémát; pl. mi a helyzet, ha más számrendszerben és esetleg 2 helyett más szám hatványainak utolsó k jegyével foglalkozunk?

Jelölje $\varphi(n)$ az n-nél nem nagyobb, n-hez relatív prím számok számát. Euler tétele kimondja, hogy

$$n \mid a^{\varphi(n)} - 1,$$

ha a és n relatív prímek. Az $n = 5^k$ esetben könnyen ellenőrizhető, hogy $\varphi(5^k) = 4 \cdot 5^{k-1}$, tehát az előző bizonyításunknak az az eredménye, hogy $5^k \mid 2^{4\cdot 5^{k-1}} - 1$, egyszerű következménye a fenti tételnek. Euler tétele arra is rámutat, hogy a periódus hosszára kapott $4 \cdot 5^{k-1}$ érték nemcsak úgy sejthető meg, ahogyan mi tettük, hanem annak alapján is, hogy $\varphi(5^k) = 4 \cdot 5^{k-1}$.

Ez a tétel azonban nem ad választ arra, hogy vajon $\varphi(n)$ a *legkisebb* olyan f kitevő-e, amelyre $n \mid a^f - 1$. Ezt minden a-ra nem is várhatjuk (pl. $a = 1$ vagy $a = n-1$ esetekben ez nyilvánvaló). Létezik-e azonban minden n-re olyan a szám, amelyre az $n \mid a^f - 1$ oszthatóságnak az $f = \varphi(n)$ érték a legkisebb pozitív "megoldása"? Az ilyen a számot modulo n szerinti primitív gyöknek nevezzük.

A következő tétel a primitív gyök létezéséről szól:

Modulo n szerinti primitív gyök csak $n = 1,\ 2,\ 4,\ p^k,\ 2p^k$ számok esetén létezik, ahol p tetszőleges páratlan prím. ($k \geqq 1$ egész szám.)

Az előző részben pontosan ezt a tételt bizonyítottuk $n = 5^k$ esetben, azaz ott megmutattuk, hogy $a = 2$ primitív gyök modulo 5^k.

A primitív gyök definíciója és létezésének problémaköre első látásra mesterkéltnek tűnik, pedig láttuk, hogy az általunk vizsgált sorozat legrövidebb periódusának hossza és a primitív gyök fogalma között szoros kapcsolat van.

Az Euler-tétel és a primitív gyök létezéséről szóló tétel bizonyítása megtalálható többek között *Niven-Zuckermann: Bevezetés a számelméletbe* (Műszaki Könyvkiadó, 1978) című könyvének 38., ill. 49. oldalán. Ugyanitt a $\varphi(n)$ függvény és a primitív gyök fogalmának további alkalmazásai is megtalálhatók.

Erdős László matematikus hallgató
ELTE