II. rész

E cikknek az első részében megismerkedtünk a p-adikus egész számokkal. Láttuk, hogy ezek tartalmazzák az összes egész számot; sőt még azokat a törteket is, amelyeket redukált alakban írva a nevezőjükben maga a p prímszám nem lép fel tényezőként. A befejező feladatban az az állítás szerepelt, hogy a most említett törtek éppen a szakaszos p-adikus egész számok lesznek.

1. Ha megkísérelnők ennek a bizonyítását, akkor azt láthatnánk, hogy p-nél kisebb nevezőjű törtek esetében a szakaszosság viszonylag könnyen kimutatható (ezt később látni is fogjuk); míg p-nél nagyobb nevező esetén a „többjegyű osztó" túlságosan nagy bonyodalmakhoz vezetne. Márpedig a bizonyításból ezeket a törteket sem hagyhatjuk ki, hiszen ezek is szakaszos p-adikus egész számok lesznek. Ezen a nehézségen úgy segítünk, hogy másképpen fogjuk felírni a p-adikus egész számokat. A p-adikus egész számban fellépő tagokat k-asával összefoglaljuk, ahol k olyan nagy, hogy p^k már nagyobb legyen a vizsgált tört nevezőjénél. Ezzel a módszerrel az említett nehézséget el tudjuk kerülni. Először a kitevőt tetszőlegesen választjuk, mert az átírásnál ennek nagyságára semmiféle megszorítást nem kell tenni azonkívül, hogy természetes szám legyen. Válasszunk tehát egy k tetszőleges természetes számot és jelöljük q-val a p^k-t. Ekkor az

$$A = a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots$$

p-adikus egész számot a következőképpen írhatjuk fel:

$$A = a'_0 + a'_1 q + a'_2 q^2 + \ldots + a'_n q^n + \ldots$$

amely felírásban:

$$a'_0 = a_0 + a_1 p + \ldots + a_{k-1} p^{k-1}, \qquad a'_1 = a_k + a_{k+1} p + \ldots + a_{2k-1} p^{k-1}, \ \ldots,$$
$$a'_n = a_{nk} + a_{nk+1} p + \ldots + a_{nk+k-1} \cdot p^{k-1}, \ldots :$$

Az a'_i „számjegyek" itt is az alapnál – azaz q-nál – kisebb nemnegatív egész számok. A kapott q-adikus egész számot az eredeti p-adikus egész q-adikus alakjának fogjuk nevezni. Abból, hogy a műveletek során „későbbi számjegyek" nem szerepelnek „korábbi számjegyek" előállításában, belátható, hogy a műveletek eredménye nem függ attól, hogy ezeket a műveleteket a számok p-adikus alakjában vagy q-adikus alakjában végezzük el.

Határozzuk meg most az adott a és b (közönséges) egész számokhoz azt az A p-adikus egész számot, amelyre $aA = b$ teljesül. Természetesen $a \neq 0$, és azt is feltehetjük, hogy a-nak és b-nek nincs közös osztója. Így, kiindulásunk szerint p nem osztója a-nak. Célszerű a k természetes számot olyan nagynak választani, hogy $q = p^k$ nagyobb legyen az a-nál is és a b-nél is. Azt már tudjuk, hogy létezik olyan A p-adikus egész szám, amelyre $aA = b$, és ennek a p-adikus számnak létezik q-adikus alakja:

$$A = x_0 + x_1 q + x_2 q^2 + \ldots + x_n q^n + \ldots,$$

ahol az x_i együtthatók a már ismertetett módon meghatározhatók. Ki fogjuk mutatni, hogy ezek az együtthatók valahonnan kezdve szakaszosan ismétlődnek. Ez már bizonyítja azt is, hogy a számjegyek ismétlődése az eredeti (p-adikus) felírásban is fennáll; csak éppen a szakaszok hossza lesz k-szor akkora, mint a q-adikus felírásban, és az ismétlődés is „k-szor később kezdődik", mint emitt.

Az $aA = b$ összefüggést felhasználva az osztási eljárás alapján az A q-adikus alakjának az együtthatóira a következő összefüggéseket nyerjük:

$$ax_0 - b = r_1 q, \quad ax_1 + r_1 = r_2 q, \quad \ldots, \quad ax_n + r_n = r_{n+1} q, \ldots..$$

Először is kimutatjuk, hogy esetünkben a fellépő $r_1,\ r_2,\ \ldots,\ r_n,\ \ldots$ hányadosok mindegyike q-nál kisebb nemnegatív egész szám. Ezen állításunkat az indexre vonatkozó teljes indukcióval bizonyítjuk.

A teljes indukciós bizonyítás első lépéseként r_1 re kell bizonyítani az állítást. Mivel a és x_o egyike sem negatív, és b kisebb q-nál, ezért $ax_0 - b$ nagyobb, mint $-q$. Másrészt a és x, mindegyike kisebb q-nál, és b nemnegatív, amiből az $ax_0 - b < q^2$ egyenlőtlenséghez jutunk. Ezeket összevetve az adódik, hogy $-q < r_1 q < q^2$, amiből q-val való osztás útján azt kapjuk, hogy $-1 < r_1 < q$. Mivel r_1 egész, ezért ebből valóban következik az állítás.

Az induktív lépés bizonyítására, azaz a vizsgált tulajdonság öröklődésének a kimutatására tegyük fel, hogy a $0 \leq r_n \leq q-1$ összefüggés teljesül. Felhasználva a $0 \leq a \leq q-1$ és a $0 \leq x_n \leq q-1$ egyenlőtlenségeket, az alábbi egyenlőtlenségsorozatot nyerjük:

$$0 = 0 \cdot 0 + 0 \leq a \cdot x_n + r_n \leq (q-1)^2 + (q-1) = q \cdot (q-1).$$

Így a $0 \leq r_{n+1} q \leq (q-1)$, amiből q-val való osztás útján valóban a kívánt $0 \leq r_{n+1} \leq q-1$ egyenlőtlenség adódik.

Beláttuk tehát, hogy az $r_1,\ r_2,\ \ldots\ r_n\ \ldots$ végtelen számsorozatban csak a $0,\ 1,\ \ldots,\ q-1$ értékek fordulhatnak elő. Mivel ez véges sok lehetőség, azért ebben a sorozatban biztosan van két különböző indexű elem, amelyek megegyeznek. Azt természetesen nem tudhatjuk, hogy milyen „messze" vannak egymástól ezek, vagy hogy mikortól kezdve lép fel ismétlődés; de annyi biztos, hogy vannak megegyező elemek. Legyen két ilyen például az r_s, és az r_{s+t}, ahol t valamilyen természetes szám. Kimutatjuk, hogy ekkor mind az x_n-ek, mind az r_n-ek sorozata az s-ik indextől kezdve szakaszosan ismétlődik, és a szakasz hosszat t. (Ez esetleg több rövidebből állhat.)

Mivel $n \geq s$, ezért $n = i + s$ alakban írható, ahol i nemnegatív egész szám. Azt állítjuk tehát, hogy minden nemnegatív egész i-re $r_{s+i+t} = r_{s+i}$ és $x_{s+i+t} = x_{s+i}$.

Az i-re vonatkozó teljes indukcióval fogjuk bizonyítani, hogy $r_{s+i+t} = r_{s+i}$. Bizonyítás közben azonban az x_n-ekre vonatkozó állítás is adódik. Az $i = 0$ esetben az $r_{s+t} = r_s$, állításhoz jutunk, amely az s és t megválasztása folytán fennáll. Az induktív lépés bizonyításához tegyük fel, hogy valamely i-re $r_{s+i+t} = = r_{s+i}$. Az $aA = b$ felírásból kapott összefüggés szerint:

$$ax_{s+i+t} + r_{s+i+t} = r_{s+i+1+t} \cdot q \quad \text{és} \quad ax_{s+i} + r_{s+i} = r_{s+i+1} \cdot q.$$

A két egyenlőséget kivonva és az indukciós feltételt felhasználva az

$$a(x_{s+i+t} - x_{s+i}) = (r_{s+i+1+t} - r_{s+i+1})q$$

egyenlőséghez jutunk. Itt a jobb oldalon szerepel a q tényező; s ezért q osztója a bal oldalnak is. Mivel csak olyan a-kat tekintettünk, amelyek nem oszthatók p-vel, ezért a-nak a $q = p^k$-nal sincs közös osztója. Így q osztója lesz a bal oldali másik tényezőnek, az $x_{s+i+t} - x_{s+i}$ különbségnek. Figyelembe véve, hogy ennek a különbségnek a tagjai kisebbek a q-nál és nem negatívak, ezért a különbségük, $-q$-nál nagyobb és q-nál kisebb lesz. Ebben a számközben viszont csak egyetlen q-val osztható szám van, nevezetesen 0. Ezzel kimutattuk, hogy $x_{s+i+t} = x_{s+i}$. Ezt felhasználva az előbb felírt egyenlőség jobb oldalára is 0 adódik. Mivel a jobb oldalon fellépő q tényező 0-tól különbözik, ezért a másik tényező lesz egyenlő 0-val, vagyis $r_{s+i+1+t} = r_{s+i+1}$. Ezzel az állítást bebizonyítottuk.

Beláttuk tehát azt, hogy $r_{s+i+t} = r_{s+i}$ fennáll minden nemnegatív i egész számra. Másrészt a teljes indukciós lépés során azt is bizonyítottuk, hogy az $r_{s+i+t} = r_{s+i}$ összefüggésből következik az $x_{s+i+t} = x_{s+i}$ egyenlőség is. Végeredményben tehát ez az egyenlőség is teljesül minden nemnegatív i egész számra. Ezzel bizonyítást nyert az is, hogy A szakaszos p-adikus szám.

2. Most azt fogjuk bizonyítani, hogy ha egy p-adikus egész szám szakaszos, akkor racionális szám lesz. Ehhez azt kell kimutatni, hogy egy alkalmas (közönséges) egész számmal megszorozva ismét egy (közönséges) egész számot nyerünk. Legyen

$$c = a_0 + a_1 p + \ldots + a_{k-1} p^{k-1}$$

az A p-adikus egész számban a szakasz előtti rész és

$$b = b_0 + b_1 p + \ldots + b_{n-1} p^{n-1}$$

a szakasz. Ekkor a A p-adikus egész számot felírhatjuk az

$$A = c + p^k \cdot b \cdot (1 + p^n + p^{2n} + \ldots)$$

alakban. Most már tulajdonképpen csak az $1 + p^n + p^{2n} + \ldots$ p-adikus egész számot kell a kívánt alakban felírni. Azonnal látható, hogy

$$(1 + p + \ldots + p^{n-1})(1 + p^n + p^{2n} + \ldots) = 1 + p + p^2 + \ldots$$

Ha ezt a p-adikus egész számot $(p-1)$-gyel szorozzuk, akkor ahhoz a p-adikus egész számhoz jutunk, amelynek mindegyik jegye $(p-1)$. Ha mármost ehhez 1-et adunk, akkor – ugyanúgy, mint a 10-adikus számok esetében – éppen 0-t kapunk. Tehát a $v_n = (p-1)(1 + p + \ldots + p^{n-1})$ jelöléssel eredményünket a következőképpen fogalmazhatjuk:

$$1 + v_n(l + p^n + p^{2n} + \ldots) = 0,$$

illetve

$$v_n \cdot A = v_n \cdot c - b \cdot p^k,$$

ahol mind v_n mind az $u = v_n c - bp^k$ egész számok. (Sőt még az is látható, hogy a v_n prímtényezős felbontásában nem szerepelhet a p.) Ezzel nemcsak bizonyítottuk az állítást, hanem olyan eljárást adtunk, amelynek a segítségével a törtalakot fel is írhatjuk.

Példaképpen nézzük meg a cikk I. része feladatából a speciális esetet. (Igaz, hogy ezek 10-adikus egész számok, de a fenti eredmények alkalmazhatók, mert 11-nek és 3-nak nem osztója sem a 2, sem az 5.) A $\ldots 2727273$ tört esetében a szakasz előtti szám $c = 3$ és a szakasz $b = 27$. A fenti jelölést használva, $k = 1$ és $n = 2$, amiből $v_n = 9 \cdot 11 = 99$. Így $99 \cdot A = 99 \cdot 3 - 27 \cdot 10 = 27$, azaz $A = \dfrac{3}{11}$. A másik számnál $B = \ldots 33337$; itt $c = 7$, $b = 3$, $k = n = 1$, és $v_n = 9$. Ebből $9B = 63 - 30 = 33$, azaz $B = \dfrac{11}{3}$. Mármost ebből egyrészt $11A = 3$, $3B = 11$, másrészt $AB = 1$ (amint a cikk első részében más úton láttuk).

A feladat végén felvetett kérdésekre is válaszolhatunk.
Ha az $A = x_0 + x_1 \cdot 5 + x_2 \cdot 5^2 + \ldots$ felírást tekintjük, ahol $3A = 1$, akkor – a tárgyalt módon meghatározva az x_n és r_n számokat – a következőket kapjuk:

$$3x_0 - 1 = 5r_0; \text{ amiből } x_0 = 2 \text{ és } r_0 = 1,$$
$$3x_1 + 1 = 5r_1, \text{ amiből } x_1 = 3 \text{ és } r_1 = 2,$$
$$3x_2 + 2 = 5r_2, \text{ amiből } x_2 = 1 \text{ és } r_2 = 1.$$

Mivel $r_0 = r_2$, ezért $A = 2 + \underbrace{3 \cdot 5 + 1 \cdot 5^2}_{} + \ldots$, ahol az alsó kapoccsal megjelölt rész a szakasz.

A másik feladatban legyen $13 \cdot B = 1$, ahol B egy 5-adikus egész szám. Mivel 13 nagyobb 5-nél, de kisebb 25-nél, ezért B-t a $B = x_0 + x_1 \cdot 25 + x_2 \cdot 25^2 + \ldots$ alakban célszerű felírni. Most:

$$\begin{aligned} 13x_0 - \ 1 &= 25r_0, \text{ amiből } x_0 = \ 2 \text{ és } r_0 = 1, \\ 13x_1 + \ 1 &= 25r_1, \text{ amiből } x_1 = 23 \text{ és } r_1 = 12, \\ 13x_2 + 12 &= 25r_2, \text{ amiből } x_2 = \ 1 \text{ és } r_2 = 1. \end{aligned}$$

Megint ismétlődés lépett fel, és így $B = 2 + 23 \cdot 25 + 1 \cdot 25^2 + \ldots$, illetve B-t 5-adikus alakba visszaírva $B = 2 + 0 \cdot 5 + \underbrace{3 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4 + 0 \cdot 5^5}_{} + \ldots$, ahol a megjelölt rész a szakasz. (Látható, hogy a szakasz már egy jeggyel előbb kezdődik; de ez a 25-adikus felírásnál természetesen nem derülhetett ki.)

3. Térjünk most vissza a p-adikus egész számok közötti osztásra. Láttuk azt, hogy ezek körében a p természetes számmal (és ennek többszöröseivel) nem lehet osztani. Ha ezen segíteni szeretnénk, akkor ki kellene bővítenünk a p-adikus egész számok körét. Tekintetbe kellene venni minden p-adikus egész számmal együtt annak „p-edrészét", „p^2-edrészét" és így tovább. Formálisan így

$$a_{-r}p^{-r} + \ldots + a_{-1}p^{-1} + a_0 + a_1p + \ldots + a_np^n + \ldots$$

alakú „számok"-hoz jutunk. Ki lehet mutatni, hogy ezeknek a körében valóban elvégezhető mind a négy alapművelet (persze 0-val itt sem lehet osztani); és a műveletek elvégzése úgy történik, ahogy azt „várjuk is". Ezeket a számokat p-adikus törtszámoknak, vagy röviden p-adikus számoknak nevezik.

4. A p-adikus számokról beszélve, illő tudni, hogy bevezetésük *Kürschák József*nek, a nagy magyar matematikusnak a nevéhez fűződik. A p-adikus számok fontos szerepet játszanak a „felsőbb" matematikában. Ezek a számok bizonyos értelemben hasonlóképpen származtathatók, mint a valós számok. (Ennek a tárgyalása azonban még az egyetemi általános matematikai képzésben sem szerepel; csupán speciális előadások keretei között szokták tárgyalni.) Más vonatkozásban is kapcsolatban állnak ezek a számok a valós számokkal. Nevezetesen mind a valós számok, mind a p-adikus számok tartalmazzák a racionális számokat. Ezt figyelembe véve, természetesen merül fel az a kérdés, hogy vajon a p-adikus számok ninesenek-e ott a valós számok között; vagy esetleg fordítva, nem lehetséges-e az, hogy a p-adikus számok tartalmazzák az összes valós számot. Ki fogjuk mutatni, hogy sem ez nem áll fenn, sem az; mégpedig tetszőleges p prímszám esetében sem.

Először azt mutatjuk ki, hogy a p-adikus számok nem lehetnek ott a valós számok között; vagyis minden p-hez található olyan p-adikus szám, amely nem lehet valós. Tudjuk, hogy egy valós számnak a négyzete nem lehet negatív. Éppen ezért elég annak a bizonyítása, hogy minden p prímszámhoz található olyan p-adikus szám, amelyik negatív és egy p-adikus számnak a négyzete.

A fenti állítás bizonyítása páratlan prímszámokra egységesen történhet. Azt fogjuk kimutatni, hogy az $(1 - p)$ szám egy alkalmas p-adikus egész számnak a négyzete. (Természetesen $(1 - p)$ minden egyes prímre más és más, de mindig az $(1 - p)$-re lesz szükségünk.) Erről a számról tudjuk, hogy negatív egész szám, hiszen p nagyobb 1-nél. Az $(1 - p)$ számot p-adikus egész számként olyan alakban írhatjuk fel, ahol az első számjegy 1, a többi pedig $(p - 1)$. (Annak megfelelően, hogy $(p - 1)$-et „számlálunk vissza" a számológépen.) Általánosabban, azt fogjuk bizonyítani, hogy tetszőleges

$$B = 1 + b_1p + b_2p^2 + \ldots + b_np^n + \ldots$$

alakú p-adikus egész szám egy alkalmas

$$A = 1 + a_1p + a_2p^2 + \ldots + a_np^n + \ldots$$

alakú p-adikus egész számnak a négyzete. Tulajdonképpen csak azt kell bizonyítani, hogy az A számjegyeit egymás után meghatározhatjuk úgy, hogy az $A^2 = B$ egyenlőség fennálljon. Ehhez– szokásos jelöléseinkkel – az alábbi egyenleteket kell rendre megoldani:

$$\begin{aligned} 2a_1 &= b_1 + r_1p, \\ 2a_2 + a_1^2 + r_1 &= b_2 + r_2p, \\ 2a_3 + 2a_1a_2 + r_2 &= b_3 + r_3p, \\ 2a_4 + 2a_1a_3 + a_2^2 + r_3 &= b_4 + r_4p, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Látjuk, hogy minden egyes egyenlet $2a = c + rp$ alakú, ahol c már ismert szám, és olyan a-t kell keresnünk, amely nemnegatív és kisebb p-nél. Azt pedig már a cikk I. részében láttuk, hogy ez megoldható, mert $2 < p$.

Nézzük most a $p = 2$ esetet. (A 2-adikus számokat diadikus számoknak nevezik.) Most azt fogjuk bebizonyítani, hogy (-7) egy alkalmas A diadikus egész szám négyzete; amelyre tehát $A^2 + 7 = 0$ teljesül. Az A együtthatói helyett kényelmesebb a „részletösszegeket" meghatározni, vagyis az

$$A = a_0 + a_1 2 + a_2 2^2 + \ldots + a_n 2^n + \ldots$$

szám esetében sem az $a_0,\ a_1,\ \ldots,\ a_n,\ \ldots$ számokat, hanem a $A_0 = a_0$, $A_1 = a_0 + a_1 2,\ A_2 = a_0 + a_1 2 + a_2 2^2, \ldots,\ A_n = a_0 + a_1 2 + a_2 2^2 + \ldots + a_n 2^n,\ \ldots$ számokat.

Ezekre a számokra nyilván igaz, hogy $A_{n+1} - A_n$, vagy 0, vagy 2^{n+1}, aszerint, hogy $a_{n+1} = 0$, vagy $a_{n+1} = 1$. Ha az A_n, számokat így adjuk meg, akkor az $a_{n+1} = 2^{-n-1}(A_{n+1} - A_n)$ számokkal elkészíthetjük a fenti diadikus egészet. (Hiszen az a_n számok mindegyike 0 vagy 1 lesz.) Az is világos, hogy ha $A_n^2 + 7$ mindig osztható 2^{n+1}-gyel, akkor $A^2 + 7$ mindegyik jegye 0 lesz; aminek a bizonyítását éppen célul tűztük ki.

Mivel kéttagúak négyzeténél a tagok kétszeres szorzata is fellép, ezért a diadikus egészek körében a négyzetre emelésnél bizonyos nehézség lép fel (amit tapasztalhatunk, ha a fenti bizonyítást minden módosítás nélkül megpróbáljuk végrehajtani). A nehézséget úgy tudjuk elkerülni, hogy azt bizonyítjuk be, hogy $A_n^2 + 7$ osztható 2^{n+2}-vel. Ha $n = 0$, akkor legyen $A_0 = a_0 = 1$; $A_0^2 + 7 = 1 + 7 = 2^3$. $n = 1$ esetében legyen $a_1 = 0$, azaz $A_1 = A_0 = 1$; most is $A_1^2 + 7 = 2^3$, ami tényleg osztható 2^{1+2}-vel. Tegyük most fel, hogy valamilyen pozitív n egész számra már fennáll az $A_n^2 + 7 = 2^{n+2} r_n$ összefüggés. Ha r_n páros, akkor legyen $a_{n+1} = 0$, azaz $A_{n+1} = A_n$. Az $r_n = 2r_{n+1}$ jelöléssel $A_{n+1}^2 + 7 = 2^{(n+1)+2} \cdot r_{n+1}$, és így az állítás $(n+1)$ esetén is teljesül. Ha r_n páratlan, akkor legyen $a_{n+1} = 1$. Ekkor $A_{n+1} = A_n + 2^{n+1}$, és így

$$A_{n+1}^2 + 7 = (A_n + 2^{n+1})^2 + 7 = (A_n^2 + 7) + 2^{n+2} A_n + 2^{2n+2} = (r_n + A_n) 2^{n+2} + 2^{2n+2}.$$

Azt szeretnénk belátni, hogy a jobb oldali összeg osztható 2^{n+3}-mal. Az első tagra ez azért igaz, mert mind r_n, mind A_n páratlan. A második tag esetében pedig azt kell bizonyítani, hogy $2n + 2 \geq n + 3$, azaz hogy $n \geq 1$, ami feltétel szerint igaz. Ezzel a teljes indukciós bizonyítást befejeztük, a kérdéses tulajdonsága tehát a diadikus számoknak is megvan.

5. Most bizonyítjuk a fordított állítást, azaz azt, hogy minden p prímszámhoz található olyan valós szám, amely nincs a p-adikus számok között. Ezt is a „négyzetgyökvonás" segítségével mutatjuk ki. Tudjuk, hogy minden p (pozitív) prímszámhoz található olyan valós szám, amelynek a négyzete p. Bebizonyítjuk, hogy ilyen szám a p-adikus számok között viszont nincs.

Értelmezzük az első részben definiált φ függvényt a p-adikus racionálisokra is, a következőképpen: ha

$$A = a_{-r} p^{-r} + \ldots + a_{-1} p^{-1} + a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^2 + \ldots,$$

ahol $a_{-r} \neq 0$, akkor legyen $\varphi(A) = p^r$. Itt is azonnal belátható, hogy

$$\varphi(AB) = \varphi(A) \cdot (B)$$

Ennek alapján tetszőleges A p-adikus szám mellett $\varphi(A^2) = (\varphi(A))^2$; azaz $\varphi(A^2)$ a p prímnek egy páros kitevőjű hatványa. Mivel, másrészről $\varphi(p) = p^{-1}$ nem páros kitevőjű hatványa p-nek, ezért p nem lehet egy p-adikus szám négyzete.

6. Beláttuk tehát, hogy a p-adikus számok másféle számok, mint a valós számok. Azt is ki lehet mutatni, hogy ezek a „számfajták" különböző prímszámokat véve kiindulásul, ugyancsak különbözőek lesznek. Precízebben szólva: ha p és q különböző prímszámok, akkor mindig létezik olyan p-adikus szám, amely nem lehet ott a q-adikus számok között.

Olyan számkört építettünk fel, amely a szemléletes számfogalomtól egészen távol esik. A felépítésnél – a számok „elkészítésénél" – az analógiák vezettek minket. Sok minden furcsa dolgot tapasztaltunk e számkörben. A furcsaságokon túl e számoknak más hasznuk is van, például az absztrakt algebrának több ágában is felhasználják őket.

Azok kedvéért, akik ismerik a komplex számokat, megemlítjük, hogy a komplex számok közé már „elhelyezhetők" a p-adikus számok. Azt azonban, hogy – akár rögzített p esetében is – egy-egy p-adikus számnak melyik komplex szám „felel meg", nem lehet tudni, mert a p-adikus számokat többféleképpen is megtalálhatjuk a komplex számok között. Ennek ellenére nem lehet a p-adikus számokat úgy előállítani, hogy bizonyos komplex számokat tekintünk, mert a többféle lehetőség közül egyet sem tudunk konkrétan megadni.

Feladatok

1. Páratlan p prímszám esetén írjuk fel a $\left(-\frac{1}{2}\right)$-et és a $\left(+\frac{1}{2}\right)$-et, mint p-adikus egészeket.

2. Határozzuk meg, hogy mely számokat lehet p-adikus számként tiszta szakaszos alakban felírni.

3. Bizonyítsuk be, hogy van olyan 5-adikus szám, amelynek a négyzete -1.

4. Bizonyítsuk be, hogy van olyan p prímszám, amelyhez található olyan p-adikus egész, amelynek a negyedik hatványa -1. Határozzuk meg a legkisebb ilyen prímet.

5. Legyen $f(x)$ tetszőleges egész együtthatós polinom és a egy tetszőleges egész. Tegyük fel továbbá, hogy van olyan p prímszám, amely osztója az $f(a)$-nak, de nem osztója az $f(a)$-nak az $f'(a) - nak$ ($f'(x)$ szokás szerint az $f(x)$ polinom deriváltját jelöli). Bizonyítsuk be, hogy ekkor az $f(x)$ polinomnak van gyöke a p-adikus egészek körében.

6. Igaz-e a fenti állítás megfordítása: Ha az $f(x)$ egész együtthatós polinomnak van gyöke a p-adikus egész számok körében, akkor van olyan a egész szám, amelyre $f(a)$ osztható p-vel, de $f'(a)$ nem osztható p-vel.

7. Bizonyítsuk be, hogy tetszőleges p páratlan prímszámra igaz az alábbi állítás:

Ha van olyan egész szám, amelynek a négyzete p-vel osztva a_0-t ad maradékul, akkor létezik olyan B p-adikus szám, amelynek négyzete

$$A = a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots \qquad \text{(pozitív } a_0 - ra\text{)}.$$

8. Legyen p páratlan prímszám és q tetszőleges prímszám. Bizonyítsuk be, hogy $p \neq q$ esetén $(p+q)q$ négyzete egy p-adikus számnak, de nem lehet négyzete egyetlen q-adikus számnak sem.

9. Ha A olyan diadikus szám, amelyre $\varphi(A) = 2^{-1}$, akkor létezik olyan B diadikus szám, amelyre $B^3 = A$.

10. Bizonyítsuk be, hogy tetszőleges p páratlan prímszámra $p^2(p+2)$ nem lehet köbe egyetlen p-adikus számnak sem, de köbe lesz egy alkalmas diadikus számnak.

11. Legyen p és q két különböző prímszám. Bizonyítsuk be, hogy van olyan p-adikus szám, amely nem lehet a q-adikus számok között.

A feladatokra beküldött megoldásokat elfogadunk.