Furcsa dolog végtelen egész számokról beszélni. A számok körében előfordul ugyan a végtelen fogalma, amikor végtelen tizedestörtekről beszélünk. Az egész számok azonban úgy tükröződnek bennünk, hogy velük kapcsolatban teljesen elképzelhetetlen „végtelenség"-ről beszélni. Természetesen nem azt értjük ezen, hogy csak véges sok egész szám volna, mert tudjuk, hogy ezek végtelen sokan vannak. Az azonban szemléletünktől nagyon távol esik, hogy egyetlen egész számot „végtelen"-nek tekinthetünk.

Ennek ellenére itt mégis ilyesmiről lesz szó. Sőt mi több, ha egy kicsit visszalapozunk e folyóirat előző számaiba, akkor ezt nem is fogjuk olyan nagyon meglepőnek tartani. Egy cikksorozatban a polinomokról és a végtelen polinomokról volt szó. Az is nehezen elképzelhető volt első hallásra, hogy a polinomokhoz hasonlóan végtelen polinomokról beszéljünk, mégis lehetségesnek bizonyult. Még azt is hozzátehetjük, hogy ott a „végtelen"-t nem az analízisben használt segédeszközökkel „fogtuk meg", hanem teljesen algebrai, „formális" módon. Ugyanúgy, ahogyan a polinomoktól eljutottunk a végtelen polinomokhoz, az egész számoktól is el lehet jutni a végtelen egész számokhoz.

A végtelen polinom fogalmának kialakításában a következő utat követtük. Bármely polinomban az „x" határozatlan csak véges sok kitevővel szerepel. Miután kitevőnek megengedtünk bármely nemnegatív egészet, kaptuk a végtelen polinomokat. Azt használtuk tehát ki, hogy a polinom egyetlen „valami" hatványaiból keletkezik, számmal való szorzás és összeadás alkalmazásával.

Ilyesféle felírása a pozitív egész számoknak is van, gondoljunk a számok 10-alapú számrendszerbeli felírására. Céljainknak azonban megfelelőbb lesz, ha nem kötjük magunkat a tízes számrendszerhez. Amit először mondunk el, az korlátozás nélkül igaz lesz bármilyen alapú számrendszerre; a továbbiak. pedig – többek között – a tízes számrendszerre nem lesznek érvényesek.

1. Induljunk ki hát egy tetszőleges g alapú számrendszerből (ahol g az 1-nél nagyobb egész szám). Mint ismeretes, minden N nemnegatív egész szám egyértelműen felírható

$$N = a_0 + a_1 g + a_2 g^2 + \ldots + a_k g^k$$

alakban, ahol az $a_0,\ a_1, \ldots,\ a_k$ számok nemnegatív egészek és mindegyikük kisebb g-nél; továbbá az a_k különbözik 0-tól. Az egyértelműség azt jelenti, hogy a k-t is és az $a_0,\ a_1, \ldots,\ a_k$ számokat is az N egyértelműen meghatározza.

Egy kis „haladást" jelent a végtelen egész számok irányában az, ha megengedjük azt is, hogy $a_k = 0$ legyen, lemondva ezáltal a „teljes" egyértelműségről. Ezt az engedményt akkor is megtesszük például, amikor nem tudjuk, hogy egy szám *pontosan* hány jegyű, csak annyit, hogy *legfeljebb* hány jegye van. Ilyen felírás mellett a tízes számrendszerbeli 537 és 00537 számok – bár alakilag különbözők – értékben megegyeznek. Ennél a felírásnál az egyértelműség csak annyiban módosul, hogy ha az N számnak a g-alapú számrendszerben vett kétféle felírását tekintjük, akkor a „számjegyek" vagy megegyeznek, vagy bizonyos „helyi értékű" számjegy az egyikben nem szerepel, míg a másikban ezen a helyen a 0 számjegy áll.

Az egyértelműség „hiányát" megszüntethetjük azáltal, hogy a számok felírásánál nem állunk meg ott, ahol a szám „befejeződik", hanem tovább írjuk a számjegyeket, de ettől kezdve már csak a 0 szerepel számjegyként. Ezzel tulajdonképpen már el is jutottunk a „végtelen egész számok"-hoz, csak itt a számjegyek úgy vannak korlátozva, hogy valahonnan kezdve mindig csak a 0-t engedjük meg. Ha ezt a feltételt elejtjük, már el is jutottunk a végtelen egész számokhoz. Már most megjegyezzük, hogy más-más „fajta" végtelen egész számokat kapunk attól függően, hogy mit választunk a számrendszer alapszámául.

A g-alapú számrendszerben felírt végtelen egész számnak vagy röviden g-adikus egész számnak nevezik az

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

végtelen kifejezést, ahol az a_i nemnegatív egészek mind kisebbek g-nél.

Ezzel a formális értelmezéssel természetesen még nem mentünk sokra. Először is meg kell mondani azt, hogy hogyan végezzük e számokkal a műveleteket; másodszor pedig azt kell megnézni, hogy ezután e számok között megtaláljuk-e az eredeti egész számokat (éppen úgy, ahogy a végtelen polinomok között is ott voltak az „igazi" polinomok).

2. Hogyan „célszerű" végezni az összeadást? Célszerűségen azt értjük, hogy ha a számokban valahonnan kezdve minden együttható 0, akkor ugyanez legyen az összeg, mint ha „igazi" számokat adnánk össze. A g-adikus számok összeadását annak alapján értelmezzük tehát, ahogyan azt a g-alapú számrendszerben elvégezzük; vagyis „az éppen tekintetbe vett helyen" az egymás alatt álló számjegyeket összeadjuk, ennek utolsó számjegyét leírjuk, a „maradékot" hozzáadjuk az előző oszlophoz, s ezt az eljárást folytatjuk, amíg véget nem ér – mert az „igazi" számok körében biztosan véget ér. Esetünkben az eljárás természetesen – általában – nem érhet véget; de azért az összeg „együtthatóit" megadhatjuk abban az értelemben, hogy „rekurzíven" megmondjuk őket egymás után.

Feladatunk tehát az adott

$$A = a_0 + a_1 g + \ldots + a_n g^n + \ldots \quad \text{és} \quad B = b_0 + b_1 g + \ldots + b_n g^n + \ldots$$

g-adikus számokhoz annak a

$$C = c_0 + c_1 g + \ldots + c_n g^n + \ldots$$

g-adikus számnak a meghatározása, amelyre $A + B = C$ legyen. Mivel azt akarjuk, hogy $a_0 + b_0$ „utolsó jegye" c_0 -val egyezzék meg, ezért c_0 -t az $a_0 + b_0$ összeg g-vel való osztási maradékaként értelmezzük, azaz $a_0 + b_0 = r_1 g + c_0$. (Érdekes,

hogy a matematikai elnevezésekben is rejlenek ellentmondások; hiszen ami itt a „hányados”, azt az összeadásnál éppen úgy idézik, hogy „marad r_1 ”.) A továbbiaknál már az előző maradékos osztás hányadosát is tekintetbe kell venni; azaz c_1 és r_2 az $a_1 + b_1 + r_1 = r_2 g + c_1$ összefüggésből adódik. Általában rekurzíve a következőt kapjuk: Ha r_i már ismert, akkor r_{i+1} és c_i az $a_i + b_i + r_i = r_{i+1} g + c_i$, $0 \leqq c_i < g$ összefüggésből adódik. Ez az értelmezés az r_1 t és c_0-t is szolgáltatja, ha „kezdeti feltételként” azt mondjuk, hogy legyen $r_0 = 0$.

Könnyen belátható, hogy amennyiben mind az A-ban, mind a B-ben valahonnan kezdve 0 áll, akkor az összegük is ilyen lesz; továbbá az $A + B = C$ összefüggés e számokra mint g-alapú számrendszerben felírt számokra fenn fog állni. Ennek a figyelembevételével könnyen belátható, hogy az összeadás a g-adikus egészek körében is kommutatív és asszociatív. (Nem a bizonyítást mondjuk el, amely – a maga teljes precízségében – kellemetlenül hosszadalmas és aprólékos, csupán azt a gondolatot, amelynek alapján a bizonyítás elvégezhető.)

Hagyjuk el A-ban is és B-ben is valahonnan kezdve a jegyeket (azaz írjunk helyükbe 0-t). E két számot a két lehetséges sorrendben összeadva az $A + B$, illetve a $B + A$ „elejét” kapjuk; hiszen a „későbbi jegyek nem hatnak az előzőekre”. Mivel az így kapott számok „igazi” egész számok, ezért az összeadás körükben kommutatív. Ez azt jelenti, hogy az $A+B$ és a $B+A$ eleje – akármilyen messze megyünk is el – mindig megegyezik, amiből pedig azonnal következik az $A + B = B + A$ egyenlőség. (Formailag azonnal beláthattuk volna a kommutativitást, hiszen $a_i + b_i = b_i + a_i$; de a fenti meggondolás olyan mélyen mutat rá az összefüggésekre, hegy segítségével más esetekben is azonnal eldönthető valamely összefüggés fennállása.) Ugyanígy gondolható végig az asszociativitás is.

3. Már az összeadás értelmezése után is igen különös jelenségeket tapasztalhatunk e számok körében. Képzeljük el számainkat, most egyszerűség kedvéért tízes alappal, egy „végtelen mérőórában” felírva. Tekintsünk egy ilyen „asztali végtelen. számológépet” és induljunk ki a csupa 0 „állásból”. A számlálókar minden egyes fordulata után a jelzett szám 1-gyel nő, a gép egymás után szolgáltatja a természetes számokat. Itt valójában az történik, hogy tízes számrendszerben felírva egymás után mindig 1-et adunk a már felírt számhoz. Mi történik azonban akkor, ha visszafelé kezdünk el 1-esével forgatni? Akik már találkoztak ilyen géppel, tapasztalhatták, hogy ilyenkor a csupa 0 állás után a számológép csönget és csupa 9-es jelenik meg. A csengetés azt jelzi, hogy „valahol már nem tudja mérni a gép a számjegyben beállt változást”. A mi gépünk azonban végtelen és ezért akármilyen messze elmehetünk. Más szóval a csupa 9-esből álló 10-adikus szám éppen $0 - 1$, azaz -1, Valóban, ha ehhez hozzáadunk 1-et – a fenti értelmezésnek megfelelően –, akkor éppen a 0-t kapjuk. Hasonlóképpen állítható elő rendre „egyre tovább forgatva a kart visszafelé”, minden negatív egész szám is. A műveleti azonosságok biztosítják, hogy ezek körében az összeadás ugyanúgy végezhető el, mint ha ki sem léptünk volna az egész számok köréből. (Egyébként ezért is mondunk g-adikus egészeket és nem g-adikus természetes számokat.)

Az előzőek általánosabban is érvényesek, azaz a g-adikus egészek körében mindig elvégezhető a kivonás. Ennek a bizonyítása úgy történhet, hogy rekurzív módon meghatározzuk a különbség együtthatóit. Ezt annak alapján tehetjük, ahogy a számok körében a kivonást végezzük; itt a „végtelenség” biztosítja, hogy mindig van következő jegy, amit „kisebb egységekre válthatunk”.

Példaképpen végezzük el az alábbi kivonást:

$$\begin{array}{r} \ldots\ 3\ 5\ 2\ 3\ 5\ 2\ 3\ 5\ 2\ 4\ 7 \\ \underline{-\ldots\ 2\ 1\ 1\ 3\ 2\ 1\ 1\ 3\ 2\ 1\ 8} \end{array}$$

(A számokat 10-adikus számoknak tekintjük, de a szokásos irányban írjuk fel őket. Az elöl álló pontokkal azt kívánjuk jelezni, hogy az elsőben jobbról bal felé a 2, 5, 3, a másodikban az 1, 2, 3, 1 számjegycsoport ismétlődik.) Az utolsó két jegyből álló számok különbsége 29. Mivel 12 jegyenként mindkét szakasz ismétlődik, ezért a különbségben a $352352352352 - 113211321132 = 239141031220$ számjegycsoport fog ismétlődni. A különbség tehát $\ldots \underbrace{239141031220}_{\text{szakasz}}29$.

A fenti 10-adikus számokat könnyen megadhattuk azzal, hogy mindegyikben szakaszosan ismétlődnek a jegyek. Általában ez nincs így, nincs mindig valamiféle „könnyű” eljárás, amely a számjegyeket szolgáltatná. Ezen nem kell meglepődni, hiszen az „igazi” számok körében is, pl. $\sqrt{2}$ vagy π tizedes jegyeinek meghatározására nincs egyszerű eljárás.

4. Térjünk most rá a g-adikus egészek szorzására. Az az eljárás, amit a számok szorzásánál végzünk, nem hozható át ide minden további nélkül. Ugyanis itt „végtelen tagú összeg” keletkezne, amelyet itt sem tudunk meghatározni. Azaz, mégis meghatározhatjuk, mert „egy-egy oszlopban” mindig csak véges sok tagot kellene összeadni. Lényegében ezt is fogjuk tenni; csak egy kicsit „előbbre” megyünk vissza. A szorzásnak az ismert alakban való elvégezhetősége a disztributivitáson múlik. Mi is úgy fogjuk értelmezni a szorzást, mintha a disztributivitás igaz volna. (Azért írtuk azt, hogy „volna”, mert egyelőre nem tudhatjuk, hogy a fentiek szemmel tartása esetén mindig igaz-e; majd belátjuk, hogy valóban igaz.) Tekintsük a fentebbi A és B g-adikus számokat; s egy olyan

$$D = d_0 + d_1 g + d_2 g^2 + \ldots + d_n g^n + \ldots$$

g-adikus számot akarunk meghatározni, amelyet az A és B szorzatának nevezhetünk. Arra kell vigyázni, hogy amennyiben A és B igazi számok, akkor D is az legyen, és $D = AB$-nek is fenn kell állnia. Ugyanúgy, mint az összeadásnál; a szorzásnál is rá lehet jönni a rekurzív definícióra.

A szorzat utolsó jegye $a_0 b_0$ utolsó jegye lesz, azaz $a_0 b_0 = s_1 g + d_0$, ahol d_0 az utolsó jegy. A „hátulról” második jegy meghatározásánál már a d_0-ra nincs szükségünk, csak a szorzat s_1 hányadosára, és - természetesen - a tényezők második

jegyeire. Így a_0+a_1g és b_0+b_1g szorzata $d_0+(s_1+a_0b_1+a_1b_0)g+a_1b_1g^2$ lesz. E szorzatban az utolsó jegy természetesen d_0, míg a következő jegyet a g mellett álló tényezőnek g-vel való osztási maradéka adja: $a_0b_1+a_1b_0+s_1=s_2g+d_1$. Így továbbmenve látható, hogy a d_2-t az $a_0b_2+a_1b_1+a_2b_0+s_2=s_3g+d_2$ összefüggésből határozhatjuk meg, és így tovább. Megjegyezzük még, hogy a d_0 meghatározásánál a hal oldalt $a_0b_0+s_0$ alakba írhatjuk, ahol s_0 persze 0. Ez csak, azért célszerű, mert így egyöntetűbb definíciót kapunk. Általában tehát az alábbi módon határozhatjuk meg a szorzat jegyeit.

Legyen $s_0=0$, és tegyük fel, hogy s_i már értelmezve van. Ekkor a $k_i=a_0b_i+a_1b_{i-1}+a_2b_{i-2}+\ldots+a_{i-1}b_1+a_ib_0+s_i$ számot g-vel osztva a kapott maradék lesz d_i, a hányados pedig s_{i+1}; azaz $k_i=s_{i+1}g+d_i$.

Mivel a maradékos osztás maradéka mindig g-nél kisebb nemnegatív egész, ezért valóban egy g-adikus egészet kaptunk. Tekintettel arra, hogy a disztributivitás a számok szorzására igaz, ezért olyan definíciót adtunk, amely számok esetében valóban a szorzatukat szolgáltatja. Az összeadásnál mondottak alapján ebből következik, hogy itt is igazak a számok körében megismert azonosságok; azaz a szorzás kommutativitása és asszociativitása, továbbá a disztributivitás is.

Példaképpen szorozzuk össze a $\ldots2727273$ és a $\ldots33337$ 10-adikus számokat, mintha tízes számrendszerben felírt számok volnának. (A pontok itt is ismétlődést jelentenek, természetesen a „részletszorzatokban" is.)

$$
\begin{array}{ccccccccccccccccccc}
\ldots & 2 & 7 & 2 & 7 & 2 & 7 & 3 & \times & \ldots & 3 & 3 & 3 & 3 & 3 & 3 & 7 \\
\hline
\ldots & 9 & 0 & 9 & 0 & 9 & 1 & 1 & & & & & & & & & \\
\ldots & 1 & 8 & 1 & 8 & 1 & 9 & & & & & & & & & & \\
\ldots & 8 & 1 & 8 & 1 & 9 & & & & & & & & & & & \\
\ldots & 1 & 8 & 1 & 9 & & & & & & & & & & & & \\
\ldots & 8 & 1 & 9 & & & & & & & & & & & & & \\
\ldots & 1 & 9 & & & & & & & & & & & & & & \\
\ldots & 9 & & & & & & & & & & & & & & & \\
\hline
\ldots & 0 & 0 & 0 & 0 & 0 & 0 & 1 & & & & & & & & &
\end{array}
$$

Látható, hogy az eljárást akármeddig folytatjuk, mindig a 0 számjegyet kapjuk; mert az egy oszlopban álló számjegyek összege váltakozva vagy 10-zel ($9+1$-gyel) nagyobb a jobbra utána levő oszlopban álló számjegyek összegénél, vagy 1-gyel kisebb annál (9-cel csökken és 8-cal nő), ennek megfelelően a következő oszlophoz „hozzáadandó maradék" az első esetben 1-gyel növekszik, míg a második esetben nem változik.

Érdekes, hogy e két szám szorzata tehát 1. Az egész számok körében ez csak úgy volna lehetséges, ha a két összeszorzott szám megegyezne és vagy 1-gyel vagy (-1)-gyel volnának egyenlők. A továbbiakban majd látunk hasonló példákat; és a cikk végén található feladat rávilágít arra hogy a fenti esetben miért kell a szorzatnak 1-gyel megegyeznie.

Következő példánk sem igaz az „igazi" számok körében. Két olyan 10-adikus számot fogunk megadni, amelyeknek a szorzata 0, anélkül, hogy bármelyikük is 0 volna. (Nem a jegyeiket adjuk meg konkrétan, mert ha e számok valahol „véget érnének", akkor két igazi számot kapnánk. Csupán azt fogjuk belátni, hogy a számok jegyeit „meg lehet határozni".)

Olyan A és B 10-adikus számokat szeretnénk tehát megadni, amelyekre $AB=D=0$, azaz $d_0=d_1=\ldots=d_n=\ldots=0$. Ez azt jelenti, hogy az a_i és b_i számokat úgy kell meghatározni, hogy a fenti k_i számok mindig 10-zel oszthatók legyenek. $s_0=0$ alapján $k_0=a_0b_0$. Mivel a_0 és b_0 mindegyike 10-nél kisebb kell hogy legyen, azért megfelel $a_0=2$ és $b_0=5$, amikor is $s_1=1$. Most:

$$k_1=a_0b_1+a_1b_0+s_1=2b_1+5a_1+1.$$

Itt $a_1=1$ és $b_1=2$ választás mellett $k_1=10$; amiből $d_1=0$, $s_2=1$. Ekkor

$$k_2=a_0b_2+a_1b_1+a_2b_0+s_2=2b_2+2+5a_2+1=2b_2+5a_2+3.$$

Itt választható $a_2=3$ és $b_2=6$, amely esetben $k_2=30$ és $s_3=3$ lesz.

Általában, ha az $a_0,a_1,\ldots,a_{i-1}$ és $b_0,b_1,\ldots,b_{i-1}$ már meg vannak választva, akkor (feltéve, hogy $a_0=2$ és $b_0=5$) a

$$k_i=2b_i+5a_i+n_i,\qquad n_i=a_1b_{i-1}+\ldots+a_{i-1}b_1+s_i$$

összefüggéshez jutunk, ahol n_i egy – már meghatározott – természetes szám. Mármost n_i-t 10-zel osztva az $n_i=10p_i+q_i$ alakhoz jutunk. Legyen $a_i=q_i$ és $b_i=2q_i$ vagy $b_i=2q_i-10$ (aszerint, hogy q_i kisebb-e 5-nél vagy sem), ekkor $k_i=10(p_i+q_i)$ vagy $k_i=10(p_i+q_i-1)$ adódik, továbbá a konstrukció miatt mind a_i, mind b_i 10-nél kisebb nemnegatív egész szám lesz.

Eredményünket úgy is megfogalmazhatjuk, hogy lehet bizonyos nem 0-ra végződő, tízes számrendszerbeli számokat újabb és újabb jegyek eléjeírásával úgy kiegészíteni, hogy e számok 2-nek, illetve 5-nek egyre magasabb hatványával legyenek oszthatók.

Bebizonyítható, hogy ez a kellemetlen jelenség azért lép fel, mert 10-nek két különböző prímtényezője van. Más szóval csak olyan alapokat érdemes figyelembe venni, amelyek egyetlen prímszám hatványai; különben mindig találhatunk olyan 0-tól különböző számokat, amelyeknek a szorzata 0 lesz. Arra is könnyen rá lehet jönni, hogy ha egy p

prímszám p^k hatványát vesszük kiindulásul, akkor ugyanazt kapjuk, mintha eleve a p-t tekintettük volna, de a tagokat k-asával egybefoglaltuk volna:

$$(a_0 + a_1 p + \ldots + a_{k-1}p^{k-1}) + (a_k + \ldots + a_{2k-1}p^{k-1})p^k + \ldots$$

Éppen ezért *ezentúl csak prímszámot tekintünk alapnak, és a kapott számokat p-adikus egész számoknak nevezzük.*

5. A szorzás vizsgálata után természetesen felmerül az is, hogy mit mondhatunk az osztásról. Először azt fogjuk bebizonyítani, hogy az

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

p-adikus egész számmal minden p-adikus egész számot lehet osztani, feltéve, hogy$a_0 \neq 0$. Adott

$$D = d_0 + d_1 p + d_2 p^2 + \ldots + d_n p^n + \ldots$$

p-adikus szám mellett olyan

$$B = b_0 + b_1 p + b_2 p^2 + \ldots + b_n p^n + \ldots$$

p-adikus számot keresünk, amelyre $AB = D$ teljesül. A szorzási eljárás megfordítása alapján ehhez arra van szükségünk, hogy a B jegyein kívül úgy határozzuk meg rekurziven az s_i-ket, hogy$s_0 = 0$ legyen; továbbá

$$k_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_{i-1} b_1 + a_i b_0 + s_i$$

mellett $k_i - d_i$ osztható legyen p-vel; és s_{i+1}-et $k_i - d_i = s_{i+1} p$ definiálja, A b_i meghatározásánál tehát csupán az a feladat, hogy az oszthatóság fennálljon; ebből az s_{i+1} már automatikusan definiálhatóvá válik. Az

$$n_i = d_i - a_1 b_{i-1} - \ldots - a_{i-1} b_1 - a_i b_0 - s_i$$

jelölést használva feladatunk b_i-t úgy meghatározni, hogy $a_0 b_i$-t p-vel osztva ugyanazt a maradékot adja, mint n_i. Megjegyezzük, hogy az n_i felírásában szereplő számokat már előzőleg ismerjük, tehát az n_i már meghatározott.

Feladatunk tehát az alábbira egyszerűsödött. Adva van egy p prímszám és egy a egész szám, amelyre $0 < a < p$ teljesül. Tetszőleges n egész számhoz olyan b egész számot kell találnunk, amelyre ab ugyanazt a maradékot adja p-vel osztva, mint az n. Azt fogjuk ehhez belátni, hogy ha az a számot rendre megszorozzuk 0-val, 1-gyel, …, $(p-1)$-gyel, és e szorzatokat elosztjuk p-vel, akkor minden lehetséges maradékot megkapunk. E lehetséges maradékok a $0,\ 1, \ldots,\ p-1$ számok, amelyeknek a száma éppen úgy p, mint a $0 \cdot a,\ 1 \cdot a,\ 2 \cdot a, \ldots,\ (p-1)a$ szorzatok száma. Éppen ezért elég annak a kimutatása, hogy ezek a szorzatok p-vel osztva mind különböző maradékot adnak, hiszen ekkor minden maradéknak fel is kell lépnie.

A bizonyításhoz tegyük fel, hogy az $a \cdot i$ és $a \cdot j$ szorzatok p-vel osztva ugyanazt a maradékot adják, ahol $0 \leqq i \leqq j \leqq p-1$. Ebből azonnal következik, hogy különbségük osztható p-vel, azaz $p|a(j-i)$. Mivel a kisebb a p prímszámnál és pozitív, ezért relatív prím hozzá; amiből $p|(j-i)$ következik. Tekintettel arra, hogy $j - i$ nem negatív és p-nél kisebb, csak úgy lehet a p prímszámmal osztható, hogy $j - i = 0$, azaz $i = j$. Ez azt jelenti, hogy két szorzat csak akkor adhatja p-vel osztva ugyanazt a maradékot, ha ugyanazt a szorzatot vettük mindkét esetben. Ezzel az állítást bebizonyítottuk, azaz ha A olyan p-adikus egész szám, amelyre $a_0 \neq 0$, akkor valóban osztója minden p-adikus egész számnak.

6. Avégett, hogy a p-adikus egészek oszthatóságát általában tárgyalhassuk, egy olyan „mértéket” vezetünk be, amely azt mutatja meg, hogy egy p-adikus szám a p-nek hányadik hatványával osztható. Legyen az

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

p-adikus szám olyan, hogy $a_0 = a_1 = a_2 = \ldots = a_{r-1} = 0$, de $a_r \neq 0$. Ekkor a következő jelölést használjuk:

$$\varphi(A) = p^{-r}.$$

Először kimutatjuk, hogy ennek a φ függvénynek az abszolút értékhez hasonló tulajdonságai vannak. Legyen adva az A p-adikus szám mellett még egy $B = b_0 + b_1 p + \ldots + b_s p^s + b_{s+1} p^{s+1} + \ldots..$ p-adikus szám is, ahol $\varphi(B) = p^{-s}$. Ha most képezzük az $A + B$ összeget, akkor az $a_0 + b_0,\ a_1 + b_1, \ldots$ összegek mind 0-nak adódnak egészen addig, amíg el nem érjük az s és r indexek közül a kisebbiket. Legyen ez például az r. Az $a_r + b_r$ összeg már biztosan nem lesz 0, de előfordulhat az, hogy p-vel osztható. Így $\varphi(A + B) \leqq \varphi(A)$; azaz általában azt mondhatjuk, hogy

$$\varphi(A + B) \leqq \text{ maximum } (\varphi(A), \varphi(B)).$$

Nézzük most meg az AB szorzatot. A képzés szerint az első $r+s$ tag mind 0 lesz. Az $(r+s+1)$-ik tag pedig megegyezik az $a_r b_s$ szorzat p-vel való osztási maradékával. Mivel p prímszám, és a_r, b_s egyike sem osztható p-vel, ezért ez a szorzat sem lesz p-vel osztható, vagyis:

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

Az összegre vonatkozó tulajdonság nem ugyanaz, mint amit az abszolút értéknél látunk, hanem annál még erősebb is – hiszen esetünkben $\varphi(A + B)$ biztosan kisebb lesz a $\varphi(A) + \varphi(B)$ összegnél vagy egyenlő vele. Ez az „abszolút” érték

– röviden *értékn*ek nevezik – olyan tulajdonságú, hogy azt a számot tekinti „kicsinek”, ami p-nek magas hatványával osztható. Kicsit naivan így is fogalmazhatnánk: ami a szám végén van, azzal tudunk számolni; minél előbbre levő számjegyeket vizsgálunk, annál „érdektelenebbek” azok számunkra.

Visszatérve az oszthatóságra, azonnal megállapíthatjuk a következőket. Ha A osztója B-nek, azaz létezik olyan C, amelyre $B = AC$, akkor $\varphi(AC) \leqq \varphi(A)$, hiszen a φ értéke 1-nél nem nagyobb pozitív szám, tehát $\varphi(B) \leqq \varphi(A)$. Ez azonban fordítva is igaz. Legyen ugyanis $\varphi(B) = p^{-s} \leqq p^{-r} = \varphi(A)$. Ez azt jelenti, hogy $s \geqq r$; és így A-t $p^r A_1$, B-t $p^r B_1$ alakban írhatjuk, ahol $A_1 = a_r + a_{r+1}p + \ldots$, $B_1 = b_r + b_{r+1}p + \ldots$, továbbá $a_r \neq 0$. Így – mint láttuk – A_1 minden p-adikus egésznek osztója; tehát létezik olyan C, amelyre $B_1 = A_1 C$. Ebből pedig azonnal következik a $B = AC$ összefüggés is.

A mostani megállapításaink szerint egy A p-adikus egész szám pontosan akkor lesz minden más p-adikus egész számnak osztója, ha $\varphi(A) = 1$. Ezeket a számokat p-adikus egységeknek nevezik. (Az egész számok körében is egységeknek nevezik azokat a számokat, amelyek minden egész számnak osztói, azaz a $(+1)$-et és a (-1)-et.) Azt is láthatjuk, hogy a p-adikus egészek körében az osztás „majdnem” elvégezhető; szinte mindennel oszthatunk, csak p-vel és p hatványaival nem - azaz, ha az osztás nem végezhető el, az mindig erre vezethető vissza. Ezek szerint a p-adikus egészek között ott találhatjuk az összes olyan törtet is, amelynek nevezője – redukált alakban – a p-hez relatív prím.

*

Cikkünk második részében meg fogjuk adni, hogy miképpen ismerhetők fel azok a p-adikus egész számok, amelyek ilyen törtet állítanak elő (lásd a feladatot). Meg fogjuk azt is nézni, hogy miképpen lehetne p-vel is osztani. Arról is fogunk beszélni, hogy a p-adikus egész számok körében hogyan végezhető el a gyökvonás.

Feladat: Az $a_0 + a_1 p + \ldots + a_n p^n + \ldots$ p-adikus egész számot szakaszosnak nevezik, ha valamilyen r és k természetes számokra és minden, az r-nél nagyobb n természetes számra fennáll az $a_{n+k} = a_n$ összefüggés. Bizonyítsuk be, hogy az előbbi típusú racionális számokat éppen a szakaszos p-adikus egész számok állítják elő.

Speciális esetként vizsgáljuk a $11 \cdot (\ldots 2727273)$ és $3 \cdot (\ldots 33337)$ 10-adikus számokat és magyarázzuk meg, miért lesz a második tényezők szorzata 1.

Ugyancsak határozzuk meg $p = 5$ esetben azt az A és B p-adikus egész számot, amelyre $3A = 1$, illetve $13B = 1$.