MBN013E Számelmélet és Alkalmazásai
MMN013E Fejezetek a Számelméletből

előadás vázlat 2015

0. Korábbi kurzusok alapján ismertnek föltételezett anyag.

(1) Az MBN112E kódú, Bevezetés a száelméletbe c. kurzus anyaga, különösen a következők:
- euklideszi algoritmus, oszthatóság, kongruencia, Euler és Fermat kongruencia-tétele;
- prímszámok, a számelmélet alaptétele;
- négyzetösszegekre bontás.

(2) Az elemi analízisből:
- végtelen sorozatok és sorok konvergenciája, a monoton korlátos sorozatok konvergensek;
- a Riemann integrál, parciális integrálás (pl. az $\int p(x)e^{-x}dx$ alakú integrálok, ahol $p(x)$ polinom).

(3) Lineáris algebrából:
- vektortér, lineáris függetlenség,
- bázis, dimenzió.

(4) Absztrakt algebrából:
- csoport, gyűrű, integritástartomány, irreducibilis- és prím elemek, irreducibilis faktorizáció, Gauss-gyűrű;
- test, testbővítés.

1. Klasszikus számelmélet.

1.1. Egy jól ismert fogalom más szemmel: a racionális számok tizedestört alakja.

Legyenek $a, b \in \mathbb{Z},\ b \geq 1$ relatív prím egészek. Ha elvégezzük az $a\colon b$ osztást, akkor az eredmény véges, vagy végtelen tizedestört lesz, az $\frac{a}{b}$ racionális szám *tizedestört alakja*. Egyszerűen megválaszolható az a kérdés, hogy mikor kapunk véges tizedestörtet: pontosan akkor, ha $b = 2^m 5^n$, továbbá a tizedevessző utáni véges sok jegy száma, a *tizedestört hossza* $\max\{m.n\}$.

Megjegyzés. Itt és az elkövetkezőkben föltesszük, hogy a tizedestörtek utolsó jegye nem zérus.

Bonyolultabb a helyzet akkor, ha az osztássorozat nem véges. Ez nyilván akkor fordul elő, ha létezik olyan $p|b$ prímszám, hogy $p \notin \{2, 5\}$. A tapasztalat szerint ez esetben a tizedesjegyek sorozatában létezik olyan véges jegysorozat, amely folytonosan ismétlődik, azaz ekkor a tizedestört

$$\frac{a}{b} = a_0, a_1 a_2 \dots a_k b_1 b_2 \dots b_m b_1 b_2 \dots b_m \dots$$

alakú, ahol $a_i, b_j \in \mathbb{Z}$, $0 \leq a_i, b_j \leq 9$. E tény igen könnyen igazolható az osztási aégoritmusból. Előfordolhat, hogy az ismétlődő $b_1, \ldots, b_m$ sorozat, a *periódus* rögtön a tizedesvessző után kezdődik. Ebben az esetben azt mondjuk, hogy a tizedestört *tisztán periódikus.* Ellenkező esetben létezik az ún. *előperiódus*, az $a_1, a_2, \ldots, a_k$ sorozat. Az előperiódus hosszán a legkisebb ilyen k-t értjük, míg a *periódushossz* a legkisebb m érték. Ezeket rendre l, n fogja jelölni.

Igazolhatók a következő tételek.

1.1.1. Tétel. *Legyenek $a, b \in \mathbb{Z}$, $b \geq 1$, $\ln.\,\mathrm{k.\,o.}(a, b) = 1$ egészek. Az $\frac{a}{b}$ racionális szám tizedestört alakja*

(i) véges, ha $b = 2^r 5^s$, $r, s \in \mathbb{N}_0$,
(ii) tisztán periódikus, ha $\ln.\,\mathrm{k.\,o.}(b, 10) = 1$,
(iii) periódikus nemzéró hosszúságú előperiódussal, ha az előbbi két föltétel egyike sem teljesül.

Ezen tétel jelöléseit és esetfölosztását használva igazolható, hogy

1.1.2. Tétel. *Legyenek $a, b \in \mathbb{Z}$, $b \geq 1$, $\ln.\,\mathrm{k.\,o.}(a, b) = 1$ egészek. Az $\frac{a}{b}$ racionális szám tizedestört alakjában*

(i) a tizedes vessző utáni ún. értékes jegyek száma $\max\{r, s\}$,
(ii) a tisztán periódikus esetben a periódus hossza $n = \mathrm{o}_b(10)$, azaz a 10 multiplikatív rendje modulo b.

1.1.3. Tétel. *Legyenek $a, b \in \mathbb{Z}$, $b \geq 1$, $\ln.\,\mathrm{k.\,o.}(a, b) = 1$ egészek, $b = b_1 b_2$, ahol $b_1 = 2^r 5^s$, $r, s \in \mathbb{N}_0$, továbbá $\ln.\,\mathrm{k.\,o.}(b_2, 10) = 1$. Ekkor az előperiódus hossza $l = \max\{r, s\}$, míg a periódushossz $n = \mathrm{o}_{b_2}(10)$*

Érdekes, de az előbbiek alapján könnyen megválaszolható kérdés az, hogy mi a helyzet akkor, ha a számrendszer alapszáma nem 10, hanem valamely $g \in \mathbb{N}$.

1.2. Prímszámok.

Definíció. A $p \in \mathbb{N}$ természetes szám prímszám, ha pontosan két pozitív osztója van.

Megjegyzés. Érdekességként fölsorolunk két alternatív prímszám-definíciót.

(1) Véges testek karakterisztikája.
(2) Az
$$1 - \frac{\sin \frac{\pi \Gamma(s)}{s}}{\sin \frac{\pi}{s}}$$
analitikus függvény egész zéróhelyei. (Ha $s \in \mathbb{R}^+$, akkor $\Gamma(s) = \int_0^\infty x^{s-1} e^{-x} dx$, amiből $\Gamma(n) = n!$, ha $n \in \mathbb{N}$.)

Bevezetőül két klasszikus tétel

1.2.1. Tétel. (Euklidesz, Elemek IX. 21.) *Végtelen sok prímszám van.*

Megjegyzés. Euklidesz ezt úgy fogalmazta, hogy „prímszámok bármely sokaságánál van több".

1.2.2. Tétel. (Erathosztenesz rostája.) *Legyen $n \in \mathbb{N}$ tetszőleges természetes szám. Az összes n-nél nem nagyobb prímszámot megkapjuk a következő eljárással.*

> *Írjuk föl a természetes számokat 2-től n-ig. Jelöljük meg a 2-t, majd húzzuk át a sorozatban a 2-nél nagyobb páros számokat. Ezután jelöljük meg a 3-ast, majd húzzuk át összes nála nagyobb többszörösét. Tegyük ugyenezt a következő — még jelöletlen — számmal (ez az 5-ös). Az eljárást ismételgessük, mindig a legkisebb jelöletlen számmal mindaddig, amíg az nem haladja meg a $\sqrt{n}$-et.*

Ekkor a bekarikázott, és a még jelöletlen számok az n-nél nem nagyobb prímszámok.

Az elkövetkezőkben néhány speciális típusú, régóta vizsgált prímszámot említünk. Elsősorben olyanokat, amelykre vonatkozóan egyszerűen fogalmazható, de régóta megválaszolatlan sejtés ismert. Ilyenek igen sokan vannak a számelméletben.

(A) Mersenne-prímek, tökéletes számok.

Euklidesz Elemek VII. 23. Definíciója: Egy szám tökéletes, ha megegyezik részei (osztói) összegével.

Megjegyzés. Euklidesznél a szám 1-nél nagyobb természetes számot jelentett, és maga a szám nem volt osztó, hiszen „a rész mindig kisebb az egésznél".

Az Elemek IX. 36. Tétele mai megfogalmazásban úgy szól, hogy a $P_n = 2^{n-1}(2^n - 1)$ alakú számok mindannyiszor tökéletes számok, valahányszor $2^n - 1$ prímszám. A XVIII. században Euler igazolta, hogy minden páros tökéletes szám ilyen alakú. Az első négy tökéletes szám — 6, 28, 496, 8128 — már az ókorban ismert volt.

Az első szisztematikus vizsgálatukat a XVII. században a francia Mersenne végezte. Nyilvánvaló, hogy páros tökéletes számok keresése megvalósítható $M_n = 2^n - 1$ alakú prímek keresésével. Ezeket később *Mersenne-prímeknek* nevezték el. Világos, hogy az előbbi M_n számok közül csak azok lehetnek prímek, amelyekben $n = p$ prímszám, de nem minden ilyen alakú szám prím. A legkisebb ilyen összetett szám az Euler által talált $M_{11} = 247 = 23 \cdot 89$.

Mersenne egy 1664-ben kiadott könyvében azt írta, hogy „M_p prím, ha

$$p = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257,$$

de minden további $p \leq 257$ prímre összetett szám."

Mintegy 200 évig senki sem tudta igazolni/cáfolni Mersenne állítását. 1876-ban Lucas megmutatta, hogy M_{67} öszetett, de prímtényezőkre

bontani nem tudta. Ez csak 1903-ban sikerült Cole-nak:

$$2^{67} - 1 = 193.707.721 \cdot 761.838.257.287$$

Később kiderült, hogy Mersenne listája további négy hibát tartalmaz: $p = 61,\ 89,\ 107$-re M_p prím (ezek hiányozna a listáról), míg M_{257} összetett szám.

Érdekességként megemlítjük, hogy a tökéletes számoknak a kora középkorban mítikus jelentéseket tulajdonítottak, elsősorban a 6-nak (a „világ teremtése") és a 28-nak (egy holdhónap hossza). A velük kapcsolatos első sejtéseket az ókor vége felé fogalmazta meg a görög Nichomachosz. Szerinte a páros tökéletes számok fölváltva 6-ra és 8-ra végződnek, és az n-edik tökéletes szám n jegyű. Az első 4 tökéletes számra ezek teljesülnek, de általános érvényük könnyen cáfolható.

Természetes kérdés, hogy van-e végtelen sok Mersenne-prím. A válasz nem ismert. Azt sejtik, hogy végtelen sok van. Jelenleg explicite 48 ilyen szám ismert. A legnagyobbat, a 48-adikat 2013. februárjában tették közzé a University of Central Missouri matematikusai, ez az $M_{57.885.161}$ amelynek 17.425.171 decimális jegye van. A 47. Mersenne prím az $M_{43.112.609}$, amelynek 12.978.189 jegye van.

Az sem ismert, hogy létezik-e egyáltalán páratlan tökéletes szám.

B. Ikerprímek.

Az $\{3,5\},\ \{5,7\},\ \{11,13\},\ \{17,19\},\ \{29,31\},\ldots$ párok (egymást követő páratlan számok) mindkét tagja prímszám. Előfordul-e végtelen sokszor, hogy két egymást követő páratlan szám mindegyike prímszám? Másképpen mondva, létezik-e végtelen sok ikerprím. A kérdés nyitott, megválaszolása nagyon nehéznek tűnik. Egy egyszerűbbnek látszó kérdés az, hogy van-e végtelen sok olyan prímszám pár, amelyek különbsége elegendően kicsi, azaz egy adott korlátnál kisebb. Ha találunk egy ilyen korlátot, akkor „már csak" azt kell csökkenteni egészen 2-ig.

2013. elején jelentette be a Nature-ben Jilang Csang azon eredményét, miszerint végtelen sok olyan prímszám pár létezik, amelyek különbsége kisebb 70 milliónál. Ez az első igazolt korlát, de meglehetősen nagy. Minden esetre ez az első eredmény az ikerprím-probléma megoldása felé vezető úton. Várható, hogy a 70 milliós korlátot rövidesen jelentősen csökkenteni tudják, de a 2 elérése, azaz annak igazolása, hogy végtelen sok ikerprím létezik, még mindig messze van.

Itt is vannak empírikus eredmények, állandóan keresik az egyre nagyobb ikerprímeket. A 2009-es rekorder pár a 100355 decimális jegyű

$$65.516.468.355 \cdot 2^{333333} \pm 1$$

volt, míg a jelenlegi csúcstartó a 2011-ben talált 200700 jegyű

$$3.756.801.695.685 \cdot 2^{666669} \pm 1.$$

Néhány elméleti eredményt is említünk.

(1) Az n és $n+2$ egészek prímszám volta független események.

(2) 1948-ban Clement igazolta, hogy n és $n+2$ pontosan akkor pímek, ha

$$4((n-1)!+1) \equiv -n \pmod{n(n+2)}.$$

(3) Tudjuk (Euler bizonyította), hogy a prímszámok reciprokaiból álló sor divergens. Annak ellenére, hogy nem ismert az ikerprím párok száma (végtelen sokan vannak-e) tudjuk, hogy e párok összege véges, azaz létezik olyan B valós szám, hogy

$$B = \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\ldots,$$

mmásképpen mondva a jobb oldalon álló sor, az ikerprímek reciprokai alkotta sor, konvergens. Ezt Brun igazolta 1918-ban, természetesen föltételezte, hogy végtelen sok ilyen pár létezik. A B konstansra a jelenleg ismert legjobb becslést 2002-ben adta Sebah, föltételezve Hardy és Littlewood azon sejtését, miszerint $\pi(x+y)-\pi(y) \leq \pi(x)$, valahányszor $x, y \geq 2$. ($\pi(x)$ az $x \in \mathbb{R}$-nél nem nagyobb prímszámok száma.) Eredménye:

$$B \approx 1,902160583104.$$

(4) Végtelen sok olyan p prímszám létezik, amelyre $p+2$ prímszám, vagy két prímszám szorzata. Innen már csak egyetlen „kis" lépés az ikerprím-probléma megoldása.

C. Sophie Germain prímek.

Ezek olyan p prímek, amelyekre $2p+1$ is prím . Például a $p = 2, 3, 5, 11$ ilyen, de a $p = 7, 13, 17$ nem. Kérdés, van-e végtelen sok ilyen prímszám. Ez is egy nyitott képdés. 2011. közepén a legnagyobb ismert Sophie Germain prím a

$$183.027 \cdot 2^{265.440} - 1,$$

amelynek 79.911 decimális jegye van.

D. Fermat-prímek.

Az előbb említett Mersenne-prímek mellett egy másik típusú prímeknek is fontos — talán még fontosabb — alkalmazásai vannak. Fermat a 2^k+1 alakú számokat vizsgálva az vette észre, hogy egyrészt ha egy ilyen alakú szám prím, akkor $k = 2^n$, másrészt az $F_n = 2^{2^n}+1$ alakú számok $n = 0, 1, 2, 3, 4$-re prímek. Azt sejtette, hogy ezek mindig prímek. Ezt a sejtést Euler cáfolta meg azzal, hogy $641 | F_5$.

Ezen, ún. Fermat-számok (Fermat-prímek) vizsgálata akkor került a matematikusok fókuszába, amikor Gauss igazolta, hogy a szabályos n-szög pontosan akkor szerkeszthető meg körzővel és egyélű vonalzóval (véges sok lépésben), ha

$$n = 2^t p_1 p_2 \ldots p_k$$

alakú, ahol $p_1, p_2, \ldots, p_k$ különböző Fermat-prímek, $t \in \mathbb{N}_0$, de $k = 0$ esetén $t > 1$.

Sajnos jelenleg csak 5 Fermat-prím ismert (amelyeket már Fermat is ismert), ezek a következők:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65.537$$

Ma azt tudjuk, hogy, ha $5 \leq n \leq 23$, akkor F_n összetett szám, és ugyanezt tudjuk néhány további n-re is. A rekorder explicite vizsgált Fermat-szám az $F_{23.471}$, amelynek több mint $10^{7.000}$ decimális jegye van, és osztható $5 \cdot 2^{23.473} + 1$-gyel.

Egyszerűen igazolható a következő állítás.

1.2.3. Tétel. *A különböző Fermat-számok relatív prímek.*

Bizonyítás. Legyen $n, k \in \mathbb{N}$ és $\ln.\,\mathrm{k.\,o.}(F_n, F_{n+k}) = d$. Világos, hogy $x + 1 | x^{2^k} - 1$ amiből $x = 2^{2^n}$ helyettesítéssel

$$2^{2^n} + 1 \left| \left(2^{2^n}\right)^{2^k} - 1 \right.$$

adódik. Ebből következik, hogy $F_n | 2^{2^{n+k}} - 1$, azaz

$$F_n | F_{n+k} - 2.$$

Így $d|2$, ami csak úgy lehetséges, hogy $d = 1$ hiszen d két páratlan szám legnagyobb köztös osztója.

Következmény. *Végtelen sok prímszám van.*

E. Prímszámokból álló számtani sorozatok.

Régi kérdés, hogy milyen hoszúságú lehet egy csupa prímszámokból álló számtani sorozat. Azt, hogy végtelen sok háromtagú sorozat — mint például a 3, 5, 7 — létezik, 1939-ben igazolta Johannes van der Corput holland matematikus. Kb. ekkor fogalmazta meg Erdős Pál és Turán Pál azt a sejtést, miszerint „a természetes számok egy pozitív sűrűségű halmazában van tetszőleges hosszúságú számtani sorozat". Másképpen fogalmazva, ha elég sok szomszédos természetes számból választunk ki egy nem sokkal kisebb részhalmazt, akkor abban lehet találni olyan elemeket, amelyek számtani sorozatot alkotnak. Ezt a sejtést 1975-ben igazolta Szemerédi Endre. E tétel jelentős szerpet játszott abban, hogy Szemerédi a közelmúltban Abel-díjat kapott. 2004-ben Tao és Green — fölhasználva Szemerédi e tételét — közösen igazolták, hogy létezik prímszámokból álló tetszőleges hosszúságú (DE NEM végtelen!) számtani sorozat. Ez egy igen meglepő eredmény.

F. Prímtesztek speciális alakú prímekre.

Feltehetően először Euler alkalmazta a következő eredményt, amely az F_n Fermat-számok (prím)osztóit írja le. Ennek értelmében az F_5 prímosztói $128k + 1$ alakúak, amelyek közül az első kettő a 257 és a 641.

1.2.4. Tétel. *$n \geq 2$-re az F_n (pozitív) osztói $r2^{n+2}+1$ alakúak.*
Bizonyítás. Az állítást prímosztókra igazoljuk részletesen, az általános esetre csak utalunk. Legyen a p prím osztója az F_n Fermat-számnak. Ekkor teljesül, hogy

$$2^{2^n} \equiv -1 \pmod{p}. \tag{1}$$

Ha ezt négyzetre emeljük, akkor az

$$2^{2^{n+1}} \equiv 1 \pmod{p} \tag{2}$$

kongruenciát kapjuk, amiből látható, hogy

$$\mathrm{o}_p(2) | 2^{n+1},$$

de (1) alapján

$$\mathrm{o}_p(2) \nmid 2^n,$$

hiszen $p > 2$, s ezért $-1 \not\equiv 1 \pmod{p}$. Mindez azt jelenti, hogy

$$\mathrm{o}_p(2) = 2^{n+1}.$$

Tudjuk, hogy $\mathrm{o}_p(2) | p-1$, azaz most $2^{n+1} | p-1$, ami maga után vonja, hogy alkalmas k egészre $p = k2^{n+1}+1$.

Ha $n \geq 2$, akkor $p = 8s+1$ alakú, és így

$$\left(\frac{2}{p}\right) = 1, \qquad \text{azaz} \qquad 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Ebből következik, hogy

$$\mathrm{o}_p(2) = 2^{n+1} \left| \frac{p-1}{2}, \right.$$

vagyis valamely r egészre $p = r2^{n+2}+1$.

Legyen $d | F_n$ tetszőleges (pozitív)osztó, és írjuk föl (nem föltétlenül különböző) prímszámok szorzataként, majd használjuk föl, hogy a prímszámokra igazolt eredményünk úgy is írható, hogy $p \equiv 1 \pmod{2^{n+1}}$, illetve az $n \geq 2$ esetben $p \equiv 1 \pmod{2^{n+2}}$.

1.2.5. Tétel. (Pepin-teszt) *Az F_n Fermat-szám pontosan akkor prím, ha*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}. \tag{3}$$

A tételt nem bizonyítjuk, csak megmutatjuk hogyan használható az F_5 összetett voltának igazolására.

Számoljuk ki $3^{2^{31}}$ modulo F_5 maradékát, amely 31 négyzetreemeléssel (közben mindig modulo F_5 redukálva) kiszámolható, és megállapítható, hogy a kérdéses maradék nem -1.

Vegyük észre azt is, hogy pusztán az ún. „kis Fermat-tétel" alkalmazásával is megkapható ezen eredmény, „csak" 32 négyzetre emeléssel és redukciós lépésekkel kaphatjuk, hogy

$$3^{F_5-1} = 3^{2^{32}} \not\equiv 1 \pmod{F_5},$$

azaz F_5 nem lehet prím. Ez a számunkra kissé elképesztő számolás nem volt idegen Fermat kortársaitól, ennél többet is számoltak „papírral és ceruzával".

Bár a Pepin-teszt elvileg hatékony módszert szolgáltat, de a Fermat-számok gyors növekedése miatt hatalmas mennyiségű számolást kell elvégezni (az előbbi utat, tehát négyzetreemeléseket és redukciókat alkalmazva). Ugyanis a lépésszám $2^{n-1} \approx \log_2 F_n$. Ez a mai gyors számítógépekkel is lehetetlen vállalkozás nagy n-ekre.

Hasonlóan a Fermat-számokhoz, a Mersenne-számok prímosztói is leírhatók, és teszt is létezik prím voltuk megállapítására.

1.2.6. Tétel. *Ha $p > 2$ prím, akkor M_p bármely prímosztója egyidejűleg $2kp + 1$ és $8r \pm 1$ alakú.*

Példa. Legyen $p = 47$. M_{47} prímosztói egyidejűleg $94k + 1$, és $8r \pm 1$ alakúak. Így amennyiben valamely q prímszám osztója M_{47}-nek, akkor megoldása az

$$x \equiv 1 \pmod{94}$$
$$x \equiv \pm 1 \pmod{8}$$

lineáris kongruenciarendszernek, tehát

$$x \equiv 1 \quad \text{és} \quad 95 \pmod{168}$$

Az első három prím, amelyek megoldások a

$$q = 1129,\ 1223,\ 2351.$$

ezek közül $2351 | M_{47}$, tehát ezen Mersenne-szám összetett.

Megjegyzés. Föltételezhető, hogy Mersenne ezen prímosztót megtalálta, azaz tudatosan hagyta ki listájáról a 47-et, de az is lehet, hogy csak jól „tippelt".

Bizonyítás. Ha egy q prímre

$$q | 2^p - 1, \quad \text{azaz} \quad 2^p \equiv 1 \pmod{q},$$

akkor $\mathrm{o}_q(2) | p$, s mivel $\mathrm{o}_q(2) \neq 1$, $\mathrm{o}_q(2) = p$. Ez azt jelenti, hogy $p | q - 1$, azaz $q = tp + 1$ valamely t természetes számra. Mivel p, q páratlanok, t szükségképp páros. Kaptuk, hogy $q = 2kp + 1$ alakú.

A $q = 8r \pm 1$ állításhoz azt kell megmutatni, hogy a 2 négyzetes maradék mod q. Láttuk, hogy $2^p \equiv 1 \pmod{q}$, p páratlan, ezért

$$\left(\frac{2}{q}\right) = \left(\frac{2}{q}\right)^p = \left(\frac{2^p}{q}\right) = \left(\frac{1}{q}\right) = 1.$$

1.2.7. Tétel. (Lucas-Lehmer teszt) *Legyen p prím, és alkossuk meg az $a_1 = 4$ és $a_{k+1} \equiv a_k^2 - 2 \pmod{M_p}$ $(k \geq 1)$ sozozatot. M_p pontosan akkor prím, ha $a_{p-1} \equiv 0 \pmod{M_p}$.*

A tételt nem bizonyítjuk, csak egyrészt rámutatunk arra, hogy az igényelt lépésszám $p-2 \approx \log_2 M_p$, másrészt megmutatjuk segítségével, hogy M_5 prím.

Valóban a sorozat

$$a_1 = 4,\ a_2 = 14,\ a_3 = 194 \equiv 8 \pmod{31},\ a_4 \equiv 62 \equiv 0 \pmod{31},$$

azaz M_5 prímszám.

G. Prímtesztek tetszőleges prímekre.

1.2.8. Állítás. *Egy $n > 1$ egész pontosan akkor összetett szám, ha valamely $p \leq \sqrt{n}$ prímszámra $p|n$.*

Az állítás alkalmazását megkönnyíti, ha ismerünk oszthatósági teszteket. Iskolai tanulmányaiban mindenki találkozott ilyenekkel a $p = 2, 3, 5, 11$ prímekre. Kérdés, hogy alkotható-e ilyen tetszőleges p prímre. A válasz igen. A konkrét megfogalmazásokhoz vegyük észre, hogy az ismert tesztek azon alapultak, hogy egyrészt a $2, 5$ osztója a 10-nek, míg a $p = 3, 11$ esetén egyrészt $10 \equiv 1 \pmod 3$, másrészt $10 \equiv -1 \pmod{11}$ volt az alapja a tesztnek.

Fermat tétele alapján tetszőleges $p > 5$ prímre

$$10^{p-1} \equiv 1 \pmod p.$$

Mivel $p-1$ páros, ezért a $10^{p-1} - 1 = \left(10^{\frac{p-1}{2}} - 1\right)\left(10^{\frac{p-1}{2}} + 1\right)$, a jobb oldalon álló két tényező valamelyike osztható p-vel, így csökkenthető a kitevő.

A teszt a következőképp működik. Jelölje $k > 1$ azt a legkisebb kitevőt, amelyre $10^k \equiv \pm 1 \pmod p$. Ha valamely $a \in \mathbb{N}$ esetén arra vagyunk kíváncsiak, hogy $p|a$ teljesül-e, akkor a következő eljárást kell alkalmaznunk. Jobbról balra haladva az a egészt osszuk be k jegyű számokra.

(1) Ha $10^k \equiv 1 \pmod p$, akkor kapott k jegyű számok összegét kell vizsgálnunk. Ha ez több, mint k (decimális) jegyű, ismét alkalmazzuk az iménti eljárást. Tesszük ezt addig, amíg egy legföljebb k jegyű egészhez jutunk.
(2) Ha $10^k \equiv -1 \pmod p$, akkor kapott k jegyű számokat váltakozó előjellel adjuk össze (emlékezzünk a 11-re ismert tesztre). A további lépések ugyanazok, mint az előző pontban.

Ha b jelöli az eljárás végén kapott legföljebb k jegyű számot, akkor $a \equiv b \pmod p$ lévén $p|a$ pontosn akkor teljesül, ha $p|b$. Ezzel a kérdést visszavezettük legföljebb k jegyű számok vizsgálatára.

Ez az eljárás „nem nagy” n-ekre viszonylag hatékony prímtesztet eredményez, hiszen

$$\pi(\sqrt{n}) \approx \frac{\sqrt{n}}{\log\sqrt{n}} = \frac{2\sqrt{n}}{\log n},$$

azaz ilyen esetekben a $\sqrt{n}$-nél nem nagyobb prímek száma sem „túl nagy”.

De már akkor, ha n kb. 100 jegyű, azaz $n \approx 10^{100}$ (ilyen, sőt ennél jóval nagyobb nagyságrendű prímeket gyakran alkalmaznak a

kriptográfiában), akkor mintegy $8 \cdot 10^{47}$ prímet kellene megvizsgálnunk. Ez azonban gyakorlatilag lehetetlen, hiszen egy olyan számítógépnek is, amely másodpercenként 10^{26} számú műveletet végez el (az elektron 10^{-26} másodperc alatt ugrik az egyik pályáról egy másikra!), akkor ez a feladat nagyságrendileg 10^{10} évig tartana (e szám a Naprendszer életkora közelítőleg).

Mindezek ellenére léteznek „gyors prímtesztek", ezek azonban nem osztókat keresnek, hanem olyan gyorsan ellenőrizhető tulajdonságokat vizsgálnak, amelyekkel a prímszámok rendelkeznek, de az összetettek gyakorlatilag nem. Ez utóbbi kitétel azt jelenti, hogy csak ritka kivételek vannak, tehát a tévedés esélye kicsi.

Általános prímtesztek tárgyalása előtt megemlítünk néhány olyan számelméleti feladatot, amelynek megoldására létezik gyors algoritmus.

1.2.9. Tétel. *Legyenek $a, b, c, m \in \mathbb{Z}$, ahol $b > 1,\ m > 0$. Ekkor*

(1) *a^b maradéka modulo m,*
(2) *$\ln.\,k.\,o.(a, b)$,*
(3) *az $\left(\frac{a}{b}\right)$ Jacobi-szimbólum, páratlan b és $\ln.\,k.\,o.(a, b)$ esetén,*
(4) *az $ax + by = c$ lineáris diofantikus egyenlet megoldásai, és*
(5) *az $ax \equiv b \pmod m$ kongruencia megoldásai*

kiszámíthatók legföljebb $5 \log_2 b$ lépésben, ahol egy lépés két egész szám összeadását, kivonását, szorzását vagy maradékos osztását jelenti.

Megjegyzés. Ha $m > 1$ páratlan egész, $m = p_1 \dots p_k$, ahol a p_i tényezők prímek és $\ln.\,k.\,o.(a, m) = 1$, akkor az $\left(\frac{a}{m}\right)$ *Jacobi-szimbólum* az $\left(\frac{a}{p_i}\right)$ Legendre-szimbólumok szorzata, azaz

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right).$$

Ezek után néhány általános prímtesztet ismertetünk.

1. Az ún. kis-Fermat tétel alapján, ha valamely $n > 2$ egészre $2^{n-1} \not\equiv 1 \pmod n$, akkor n összetett szám. Ez a kritérium könnyen ellenőrizhető. Fontos kérdés azonban, hogy mi következik abból, hogy $2^{n-1} \equiv 1 \pmod n$?

Sajnos ebből nem következik, hogy n prímszám. Például, $2^{340} \equiv 1 \pmod{341}$, de $341 = 11 \cdot 31$, azaz nem prím.

Definíció. Azon $n \in \mathbb{N}$ összetett számokat, amelyekre $2^{n-1} \equiv 1 \pmod n$, 2-es alapú *álprímeknek*, vagy *pszeudoprímeknek* nevezzük.

1.2.10. Állítás. *A pszeudoprímek száma végtelen, de „ritkák" a prímekhez képest.*

Az állítás második részének illusztrálására megemlítjük, hogy 10^{10}-ig 455.052.511 prímszám van, míg pszeudoprím csak 14.887, azaz arányuk kb. egy a harmincezerhez.

A tesztet úgy javíthatjuk, hogy az a^{n-1} maradékát modulo n nemcsak $a = 2$ re vizsgáljuk, hanem az 1000-nél kisebb összes prímre megvizsgáljuk. Ha ez legalább egy prímre nem 1, és $n > 1000$, akkor n a kis-Fermat tétel alapján biztosan összetett. Az eljárás hatékonyságát növelhetjük azzal, hogy az első néhány prím helyett véletlenszerűen választott, n-nel nem osztható számokat veszünk a-nak. Ezen az úton azonban csak addig juthatunk el, hogy az adott n „még inkább majdnem prím".

Léteznek ugyanis olyan m összetett számok, amelykre az $a^{m-1} \equiv 1 \pmod{m}$ kongruencia minden $a \in \mathbb{N}$-re teljesül.

Definíció. Az $m \in \mathbb{N}$, $m > 1$ összetett szám *abszolut pszeudoprím* vagy másképpen mondva *Carmichael-szám*, ha minden $a \in \mathbb{N}$-re $a^{m-1} \equiv 1 \pmod{m}$.

1.2.11. Állítás. *Végtelen sok abszolut pszeudoprím létezik.*

Ezen állítást csak 1992-ben sikerült igazolni. A legkisebb abszolut pszeudoprím a 1729.

A következő két — az előbbinél lényegesen bonyolultabb — prímteszt már az álprímeket (pszeudoprímeket) is leleplezi. Mindkettő véletlen számsorozatokat használ. Ilyenek számítógéppel kaphatók, de pénzfeldobások sorozatával (persze így kettes számrendszerbeli alakban) is megkaphatók. Persze így csak ún. álvéletlen számsorozatok kaphatók, de ezek „igen jól utánozzák" a ténylegesen véletlen sorozatokat.

1.2.12. Tétel. (Solovay-Strassen prímteszt)
(A) *Legyen $n > 1$ páratlan egész, és tekintsük az*

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \tag{4}$$

kongruenciát, ahol $\left(\frac{a}{n}\right)$ Jacobi-szimbólum.
Ha n prím, akkor (4) minden $a \not\equiv 0 \pmod{n}$ esetén teljesül.
Ha n összetett, akkor (4) egy modulo n teljes maradékrendszer elemeinek kevesebb, mint felére teljesül.
(B) *Az (A) kritérium alapján a következőképp dönthető el egy nagy páratlan n-ről, hogy prím-e vagy összetett. Válasszunk (mondjuk) 1000 véletlen $a \not\equiv 0 \pmod{n}$ számot, és mindegyikre vizsgáljuk meg, hogy a (4) föltétel teljesül-e. Ha legalább egy esetben nem teljesül, akkor az n biztosan összetett. Ha mind az 1000 esetben teljesül, akkor 2^{-1000}-nél kisebb annak a valószínűsége, hogy n összetett.*

Megjegyzés. A (B) pontban említett valószínűség olyan kicsi, hogy a teszt gyakorlatilag biztosnak tekinthető.

1.2.13. Tétel. (Miller-Lenstra-Rabin prímteszt) *Legyen $n > 1$ páratlan egész, $n - 1 = 2^k r$, ahol r páratlan. Az*

$$a^r,\ a^{2r},\ a^{4r}, \ldots, a^{2^{k-2}r} = a^{\frac{n-1}{4}},\ a^{2^{k-1}r} = a^{\frac{n-1}{2}} \tag{5}$$

számokat „jó sorozatnak" nevezzük, ha ezek modulo n vett legkisebb abszolút értékű maradékai között előfordul a -1, vagy pedig a^r maradéka 1.
Ha n prím, akkor (5) minden $a \not\equiv 0 \pmod{n}$ esetén jó sorozat.
Ha n összetett akkor (5) egy modulo n teljes maradékrendszer elemeinek kevesebb, mint felére alkot jó sorozatot.

1.3. A Goldbach sejtés.

Ismeretes, hogy

$$4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 5 + 3,\ 10 = 7 + 3,\ 12 = 7 + 5, \ldots$$

azaz az első néhány páros szám mindegyike előáll két prímszám összegeként. Goldbach 1742-ben Eulerhez írott levelében azt a sejtését fogalmazta meg, hogy minden 2-nél nagyobb páros szám előáll két prímszám összegeként.

Megjegyzések.

(1) Az előbbi problémát/sejtést szokás „páros Goldbach sejtésnek" nevezni. A páratlan úgy szól, hogy 7-től kezdve minden páratlan szám előáll 3 prímszám összegeként. E sejtés következik a párosból. Vinogradov 1935-ben bizonyította, hogy minden „elegendően nagy" páratlan szám előáll 3 prímszám összegeként. Sajnos az elegendően nagy kitétel nem helyettesíthető egy explicit számmal, így a kimaradó esetek nem ellenőrizhetők számítógéppel.

(2) A XX. század első harmadában Schnirelmann megmutatta, hogy van olyan C konstans, hogy minden 2-nél nagyobb páros szám előáll legföljebb C (később Schnirelmann-konstansnak nevezték) számú prímszám összegeként. Ő sajnos csak azt tudta megmutatni, hogy $C \leq 800.000$.

(3) 1973-ban Chen Jingrun igazolta, hogy minden elegendően nagy páros szám előáll egy prímszám és legföljebb két prímszám szorzata összegeként. Az „elegendően nagy" kitételt nem sikerült explicit konstanssal helyettesíteni mindeddig.

(4) 1995-ben Oliver Ramaré bebizonyította, hogy a Schnirelmann konstans nem nagyobb 6-nál.

(5) Minden elég nagy páros szám fölírható $p + m$ alakban, ahol p prím, az m pedig vagy prímszám, vagy két prímszám szorzata. (Az első ilyen jellegű tételt Rényi Alfréd igazolta 1947-ben, ahol alkalmas rögzített k-val az m legföljebb k számú prímszám szorzata.)

(5) Csak „megfelelő értelemben vett ritka kivételek" lehetnek azok a legalább 4 páros számok, amelyek nem írhatók 2 prímszám összegeként. Sajnos a „ritka" jelsző nem helyettesíthető „véges sokkal".

1.4. Titkosírások.

Minden titkosírás, titkos (kódolt) üzenetváltás egyszerűsített formában a következőképp működik. A feleket jelölje **A** és **B**. Az **A** által elküldendő szöveg (betűsorozat) legyen $\mathcal{S}$.

($\imath$) **A legegyszerűbb változat.**

(a) A két fél megállapodik egy Φ kódoló függvényben, és az $\mathcal{S}\Phi = \mathcal{U}$ üzenetek küldi el **A** **B**-nek.
(b) **B** a kapott üzenetből a kódoló függvény inverze, $\Psi = \Phi^{-1}$ segítségével dekódolja az üzenetet: $\mathcal{U}\Psi = \mathcal{S}$.

Megjegyzések.
(1) A rendszer egyszerű, pl. kódoló függvénynek egyszerű betűeltolás tekinthető. Ez esetben az inverz is könnyen kapható.
(2) Ha az üzenetet nyilvánosan küldjük el, vagy egy ellenérdekelt fél megszerzi azt, az üzenet viszonylag könnyen dekódolható.

($\imath\imath$) **Ún. „rostély" alkalmazása.**

Ilyennel a legtöbben találkozhattak Verne Sándor Mátyás című regényében. Ez esetben csak a rostélyra kell vigyázni, hogy ne kerüljön illetéktelen kézbe.

($\imath\imath\imath$) **Ún. kódkönyv alkalmazása.**

($\imath\nu$) **Egy biztonságossá tehető eljárás: a kódoló kulcs nyilvános, de a dekódoló nem az.**

Ez utóbbi első látásra „fából vaskarika", de megmutatjuk, hogy nem az. Az ötletet 1975-ben publikálta Diffie és Hellman.

A működése:
(a) Az ábécé betűit természetes számokkal helyettesítjük, mondjuk az $1, 2, \ldots, N$ számokkal. A Φ kódoló függvény most az $\{1, 2, \ldots, N\}$ halmaz egy bijekciója.
(b) A $\Phi^{-1} = \Psi$ dekódoló függvényt csak a címzett(ek) ismerik, és azzal egyszerűen dekódolhatják az üzenetet.

Megjegyzés. Látszólag egyszerű Φ ismeretében inverzének meghatározása tekintettel arra, hogy az $\{1, 2, \ldots, N\}$ halmaz véges. Pl. ha meg akarjuk határozni $k\Psi$ értékét, akkor egyszerűen képezni kell az $1\Phi, 2\Phi, \ldots$ sorozatot addig, amíg k-t nem kapunk. DE gondoljuk meg meddig tart ez minden egyes számnál akkor, ha mondjuk $N = 500$?

Megmutatható, hogy minden olyan titkosírás, amelyben a betűket természetes számokkal helyettesítjük visszavezethető arra az esetre, amikor a kódoló és a dekódoló függvény az $\{1, 2, \ldots, N\}$ halmaz egy-egy bijekciója alkalmas (nagy) N-re.

Az iménti Diffie-Hellman-féle elv egy gyakorlati megvalósítását, és egyben biztonsága növelését valósította meg 1976-ban Rives, Shamir és Adleman. Rendszerüket *RSA-rendszernek* nevezik az irodalomban. Ezen rendszer egy „nyilvános kódú" rendszer, amelyben a kódoló függvény (a kódoló függvények, ha a rendszerben nem ketten, hanem többen vesznek részt) és a kódolt üzenet is nyilvánossá tehető, de a titkosított (kódolt) üzenetet gyakorlatilag csak a címzett tudja dekódolni.

Előkészületként az ábécé betűihez és az írásjelekhez (a szóközt is ideértve) rendeljünk kétjegyű számokat, például

$$\mathrm{A} \mapsto 01, \mathrm{Á} \mapsto 02, \mathrm{B} \mapsto 03, ..., \mathrm{Z} \mapsto 35$$

A „szóköz" lehet 00, a pont a 36, stb. 4-4 ilyen kétjegyű szám alkosson egy-egy nyolcjegyű blokkot (számot), azaz az üzenet nyolcjegyű számok sorozata. Így egy kódolandó szöveg nyolcjegyű számokból áll, tehát a korábban említett kódolásnál N választható 10^8-nak, azaz a Φ kódoló függvény az $\{1, 2, \ldots, 10^8\}$ halmaz egy permutációja. Például a „számelmélet" szó ilyetén kódolt alakja:

$$25350216|06151607|150626,$$

ahol már jelöltük a nyolcjegyű számokká alakítást is. Ha az utolsó blokk nem lenne 8 jegyű, akkor nullákkal egészítjük ki. Ezek után a kódoló függvényt a 25350216, 06151607, 15062600 számokra kell alkalmazni.

A három szerző a kódoló-dekódoló függvénypár megadására a következőt javasolta.

1. A titkos levelezést folytatni akaró társaság minden egyes tagja választ két „nagy" prímszámot, legyenek ezek az **A** esetén p, q, és $N = pq$. A két prímet titokban tartja, az N-et nyilvánosságra hozza. Ezek után választ egy olyan $t > 1$ egészet, amelyre $\ln. \mathrm{k.\,o.}(t, \varphi(N)) = 1$, ahol φ az Euler-függvény.

2. Jelölje Φ azt a kódoló függvényt, amelyet akkor kell alkalmazni, ha valaki a társaságból titkos üzenetet akar küldeni **A**-nak. Ez a függvény is nyilvánosságra hozható. E függvény definíciója a következő.

$$r\Phi = r^t \text{ legkisebb nemnegatív maradéka modulo } N, \tag{6}$$

ahol $1 \leq r \leq N$.

3. A $\Psi = \Phi^{-1}$ meghatározására keressük Ψ-t a következő alakban:

$$s\Psi = s^m \text{ legkisebb nemnegatív maradéka modulo } N, \tag{7}$$

ahol $1 \leq r \leq N$. Ez a függvény akkor lesz megfelelő, ha minden $r \in \{1, \ldots, N\}$-re

$$r = r\Phi\Psi = r\Psi\Phi = r^{tm} \text{ legkisebb nemnegatív maradéka modulo } N,$$

azaz, ha minden r-re

$$r^{tm} \equiv r \pmod{N}. \tag{8}$$

A kis-Fermat tételből egyszerűen adódik a p, q prímekre, hogy tetszőleges $k \in \mathbb{N}$-re

$$r^{1+k\varphi(N)} \equiv r \pmod{N} \tag{9}$$

minden r-re teljesül.

4. (9) alapján (8) és (7)-ben megfelelő m-hez jutunk, ha megoldjuk az

$$mt = 1 + k\varphi(N) \tag{10}$$

diofantoszi egyenletet m-re és k-ra. Az $\ln.\,\mathrm{k.\,o.}(t, \varphi(N)) = 1$ föltétel miatt van megoldás, és az euklideszi algoritmussal megkapható.
5. Mindezt azonban csak a kulcstulajdonos, a címzett tudja kiszámolni, hiszen csak ő képes meghatározni $\varphi(N)$ értékét, ugyanis ehhez tudni kell az N prímtényezőit.
6. Hogyan működtethető az eljárás, mennyire biztonságos?

A kulcstulajdonos a szükséges p, q prím párt a következőképp generálja.

- Sorra választ (mondjuk) 250 és 300 jegyű páratlan véletlen számokat, és valamilyen prímteszttel kiválaszt közülük egy prím párt. Mivel a prímtesztek elég gyorsak és „elég sok" 300 jegyű prím van (a prímszámtétel szerin közelítőleg minden $\log(10^{300})/2 \approx$ 350- ötödik 300 jegyű páratlan szám prím).
- (6) és (7) alapján - ismételt négyzetreemelésekkel — az $r\Phi$ és az $s\Psi$ függvényértékek meghatározhatók (természetesen ehhez ismerni kell a p, q prímeket).

7. Mennyire biztonságos ez a rendszer? Ha néhány óvatossági szabályt betartunk, akkor a biztonsági szint igen magas.

- A p és q prímek ne legyenek „közel" egymáshoz, mert ellenkező esetben könnyű az N-et faktorizálni. Az biztosan elég, ha néhány 10-zel eltér a (decimális) jegyeik száma.
- Hasonló okból arra is ügyelni kell, hogy a $p-1$ és a $q-1$-nek ne legyenek nagy prímosztói.
- Mindez addig van így, ameddig valaki nem talál igen gyors prímfaktorizációs eljárást.

Az előbbieket a következő tételben foglalhatjuk össze.

1.4.1. Tétel. *Legyen p, q két nagy prímszám, $N = pq$ és* $\ln.\,\mathrm{k.\,o.}(t, \varphi(N)) = 1$. *Definiáljuk (3) és (4) alapján a Φ, Ψ kulcspárt, ahol m-re teljesül (7). Nyilvánosságra hozható Φ, N és t, míg titokban kell tartani a p, q prímeket és $\varphi(N)$-et. Ekkor a $\Psi = \Phi^{-1}$ dekódoló függvény a nyilvános adatokból nem határozható meg. Maga a kódolt üzenet nyilvánosan küldhető el.*

Megjegyzések.
(1) Az iménti RSA rendszert és a hozzá hasonlókat *nyilvános kódú titkosírásoknak* nevezik.
(2) Hasonló elveken alapulnak a modern bankbiztonsági rendszerek.

2. Átmenet az Analitikus Számelmélet Felé: Lánctörtek, Kongruenciák.

2.1. Történeti bevezetés. Az általános vélekedéssel szemben nem Diofantosz volt az első, aki egész együtthatós határozatlan egyenletek egész megoldásait kereste, hanem az I.sz. VI.–VII. században élt hindu Aryabhata I. és Brahmagupta. Ezen egyenletek megoldását lényegében az Euklideszi algoritmusra alapozták, és egy új, egyedi jelölésrendszert is bevezettek, ami a mai lánctört egyik ősének is tekinthető.

A lánctört egy másik ősének a pisai Leonardo érdekes — bizonyos láncolást, folytonosságot sugalló — indus eredetű írásmódja tekinthető. Az 1202-ben elkészült Liber abaci c. könyvében szerepel többek közt az $\frac{111}{345}$ jelsorozat, amelynek a maitól eltérő jelentése a következő volt:

$$\frac{1+\frac{1+\frac{1}{5}}{4}}{3}=\frac{1}{3}+\frac{1}{3\cdot 4}+\frac{1}{3\cdot 4\cdot 5}.$$

Itt a jobb oldalon föllelhető az — először az Egyiptomi Középbirodalomban használt — ún. elemi törtekre bontás is.

Az olasz matematika professzor Raffaela Bombelli 1572-es L'Algebra Opera c. könyvében szerepel a $\sqrt{2}$, és a $\sqrt{13}$ alábbi közelítése:

$$\sqrt{2}=1+\frac{1}{2+2+2+2} \quad \text{és} \quad \sqrt{13}=3+\frac{4}{6+6+6+6}.$$

Ezen „fura" írásmóddal a következő két törtet adta meg:

$$\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\frac{1}{2}}}} \qquad \sqrt{13}=3+\cfrac{4}{6+\cfrac{4}{6+\cfrac{1}{6+\frac{4}{6}}}}$$

Vizsgáljuk meg a $\sqrt{2}$-re adott érték pontosságát. Bombelli racionális (közelítése) $\frac{41}{29}$, ami $4\cdot 10^{-4}$-nél kevesebbel tér el a helyes (irracionális) értéktől. A másik közelítés is hasonló pontosságú. Bombellinél még ha föl is merült, hogy az általa adott szám csak közelítés, meg volt győződve arról, hogy véges sok lépéssel folytatva eljárását eljut a korrekt értékhez. A korrekt érték — mint látni fogjuk — egy „ilyen alakú" tagokból álló sorozat határértéke:

$$\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{\ddots}}}} \qquad \sqrt{13}=3+\cfrac{4}{6+\cfrac{4}{6+\cfrac{1}{6+\cfrac{4}{\ddots}}}}$$

Bombelli volt Diophantosz Aritmetikájának (az 1-4. könyvek) első (nem görög vagy iszlám) népszerűsítője Európában, amelyet kortársa — a számolómester — Tartaglia fordított le latinra. Abban még

$$\frac{170}{53} = 3 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{2}}}}$$

alakú számolás is szerepelt (szintén mai szimbolikát használva). Ez korrekt.

2.2. Véges lánctörtek.

Definíció. Legyenek $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_n, b_1, \ldots, b_{n-1} \in \mathbb{N}$. Az

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{\ddots + \cfrac{b_{n-1}}{a_{n-1} + \cfrac{b_n}{a_n}}}}$$

alakú kifejezést véges lánctörtnek nevezzük. Azt mondjuk, hogy e kifejezés *egyszerű lánctört*, ha $b_1 = \ldots = b_{n-1} = 1$, azaz

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

alakú. A továbbiakban lánctörtön mindig egyszerű lánctörtet fogunk érteni.

2.2.1. Tétel. *Bármely racionális szám fölírható véges (egyszerű) lánctörtként.*

Bizonyítás. Lényegében ugyanazt az eljárást fogjuk követni, amelyet már a kora középkori hindu Aryabhata I. is ismert.

Legyen $a, b \in \mathbb{Z},\ b > 0$. Végezzünk euklideszi algoritmust a és b-n.

$$\begin{aligned} a &= ba_0 + r_1 \\ b &= r_1a_1 + r_2 \\ r_1 &= r_2a_2 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}a_{n-1} + r_n \\ r_{n-1} &= r_na_n. \end{aligned} \tag{1}$$

Tudjuk, hogy $r_1, \ldots, r_n, a_1, \ldots, a_n \in \mathbb{N}$, és $a_0 \in \mathbb{Z}$.
Osszuk el az (1)-beli egyenlőségeket rendre $b, r_1, \ldots, r_n$-nel:

$$\begin{aligned}
\frac{a}{b} &= a_0 + \frac{1}{\frac{b}{r_1}} \\
\frac{b}{r_1} &= a_1 + \frac{1}{\frac{r_1}{r_2}} \\
\frac{r_1}{r_2} &= a_2 + \frac{1}{\frac{r_2}{r_3}} \\
&\vdots \\
\frac{r_{n-1}}{r_n} &= a_n,
\end{aligned}$$

amiből szukcesszív helyettesítésekkel kapjuk, hogy

$$\frac{a}{b} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}} = \ldots$$

Az eljárás végén az

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} \tag{2}$$

lánctörtet kapjuk.

Megjegyzés. Az előbbi tétel megfordítása triviálisan igaz.

Példa. $\frac{51}{19}$ lánctört alakja a következő.

$$\begin{aligned}
51 &= 2 \cdot 19 + 13 \\
19 &= 1 \cdot 13 + 6 \\
13 &= 2 \cdot 6 + 1 \\
6 &= 1 \cdot 6
\end{aligned}$$

Az imént ismertetett eljárást követve

$$\frac{51}{19} = 2 + \frac{13}{19} = 2 + \frac{1}{\frac{19}{13}}$$
$$\frac{19}{13} = 1 + \frac{6}{13} = 1 + \frac{1}{\frac{13}{6}}$$
$$\frac{13}{6} = 2 + \frac{1}{6},$$

amiből helyettesítésekkel kapjuk, hogy

$$\frac{51}{19} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}} \tag{3}$$

Világos, hogy a (2) lánctörtet az $a_0, a_1, \ldots, a_n$ egészek egyértelműen meghatározzák, így egyszerűen

$$\frac{a}{b} = \langle a_0, a_1, \ldots, a_n \rangle\text{-t} \tag{4}$$

írhatunk helyette. Ezt fölhasználva

$$\frac{51}{19} = \langle 2, 1, 2, 6 \rangle.$$

Természetes az a kérdés, hogy hányféle lánctört előállítása lehet egy racionális számnak. Az előbbi példából ugyanis nyilvánvaló, hogy

$$\langle 2, 1, 2, 6 \rangle = \langle 2, 1, 2, 5, 1 \rangle,$$

sőt (2) alapján az általános

$$\langle a_0, a_1, \ldots, a_n \rangle = \langle a_0, a_1, \ldots, a_n - 1, 1 \rangle$$

egyenlőség is nyilvánvaló. Ennek elkerülésére megállapodhatunk abban, hogy a második fajta alakoktól tartózkodunk, azaz mindig föltesszük, hogy lánctörtjeinkben az utolsó jegy nagyobb egynél. Ez a megállapodás hasonló a tizedestörtek fölírásánál tetthez, mely szerint a tizedestörtjeink nem végződhetnek végtelen sok 9-esre, azaz a tizedesjegyek nem lehetnek véges sok jegytől eltekintve kilencesek. Ezen megállapodást elfogadva már egyértelmű a racionális számok lánctört alakja.

Jelölés. Tetszőleges $a \in \mathbb{R}$-re jelölje $[a]$, ill. $\{a\}$ az a *egészrészét*, ill. *törtrészét.* Azaz

$$[a] = \max\{x \in \mathbb{Z} \mid x \leq a\},$$

továbbá

$$\{a\} = a - [a].$$

2.2.2. Tétel. *Ha* $\langle a_0, a_1 \ldots, a_k \rangle, \langle b_0, a_1 \ldots, b_l \rangle$ *olyan lánctörtek, ame-*

lyekben $a_k, b_l > 1$, *akkor*

$$\langle a_0, a_1 \ldots, a_k\rangle = \langle b_0, a_1 \ldots, b_l\rangle$$

maga után vonja, hogy $k = l$, *és minden* $0 \le i \le k$-ra $a_i = b_i$.
Bizonyítás. Vezessük be a következő jelöléseket:

$$\begin{aligned} r_0 &= \langle a_0, a_1, \ldots, a_k\rangle, & t_0 &= \langle b_0, a_1 \ldots, b_l\rangle, \\ r_i &= \langle a_i, a_{i+1}, \ldots, a_k\rangle, & t_j &= \langle b_j, b_{j+1}, \ldots, b_l\rangle, \\ 1 &\le i \le k, & 1 &\le j \le l. \end{aligned}$$

A tétel föltétele szerint $r_0 = t_0$. Tetszőleges $1 \le i < k$-ra

$$r_i = a_i + \frac{1}{\langle a_{i+1}, \ldots, a_k\rangle},$$

azaz

$$r_i = a_i + \frac{1}{r_{i+1}}.$$

Hasonlóan kapható, hogy bármely $1 \le j < l$-re

$$t_i = b_i + \frac{1}{t_{i+1}}.$$

Az is világos, hogy egyrészt $r_i > a_i$ és $t_j > b_j$, és speciálisan $r_k = a_k > 1$ és $t_l > b_l > 1$. Másrészt,

$$a_i = [r_i] \quad \text{és} \quad \frac{1}{r_{i+1}} = r_i - [r_i] = \{r_i\},$$

továbbá

$$b_j = [t_j] \quad \text{és} \quad \frac{1}{t_{j+1}} = t_j - [t_j] = \{t_j\}.$$

Ezek alapján az

$$r_0 = a_0 + \frac{1}{r_1}, \qquad t_0 = b_0 + \frac{1}{t_1}$$

egyenlőségekből — mivel $a_0 = b_0$ — az $r_1 = t_1$ egyenlőség adódik. Eljárásunkat folytatva véges sok lépés után a tétel állítását kapjuk.

2.3. Végtelen (egyszerű) lánctörtek.

Definíció. Legyen $a_0, a_1, \ldots$ egész számok olyan sorozata, amelyben legföljebb a_0 nem pozitív. Az

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}} = \langle a_0, a_1, a_2, a_3, \ldots\rangle$$

kifejezést *végtelen egyszerű lánctörtnek* nevezzük. Azt mondjuk, hogy e lánctört az $\alpha \in \mathbb{R}$ számot reprezentálja, ha

$$\alpha = \lim_{n\to\infty} \langle a_0, a_1, \ldots, a_n \rangle.$$

Megjegyzés. A definícióban természetesen föl kell tételeznünk, hogy a határérték létezik. Ezt rövidesen be fogjuk bizonyítani, de addig is használni fogjuk az $\alpha = \langle a_0, a_1, \ldots, a_n, \ldots \rangle$ írásmódot, továbbá tetszőleges $n \in \mathbb{N}_0$ esetén használjuk az $\alpha_n = \langle a_0, a_1, \ldots, a_n \rangle$ jelölést is. Ez utóbbit az α lánctört alakjának *n-edik kezdő szeletének* nevezzük.

Első feladatunk tehát az, hogy a definícióbeli határérték létezését bizonyítsuk. Eljárásunkban (és a későbbi alkalmazásokban is) alapvető szerepet fog játszani a következő két sorozat.

Definíció. Tekintsük az $a_0 \in \mathbb{Z}$ és $a_1, a_2, \ldots \in \mathbb{N}$ egészeket, és alkossuk meg belőlük az $(p_i)_{i\in\mathbb{N}_0}$ és $(q_i)_{i\in\mathbb{N}_0}$ sorozatokat.

$$\begin{aligned} p_0 &= a_0 & q_0 &= 1 \\ p_1 &= a_1 a_0 + 1 & q_1 &= a_1 \\ &\vdots & &\vdots \\ p_k &= a_k p_{k-1} + p_{k-2} & q_k &= a_k q_{k-1} + q_{k-2} \\ &\vdots & &\vdots \end{aligned} \tag{5}$$

2.3.1. Lemma. *Legyenek $a_0 \in \mathbb{Z}$ és $a_1, a_2, \ldots \in \mathbb{N}$ egészek, és alkossuk meg az (5)-ben definiált sorozatokat. Ekkor tetszőleges $n \in \mathbb{N}_0$-ra*

$$\alpha_n = \langle a_0, a_1, \ldots, a_n \rangle = \frac{p_n}{q_n}.$$

Bizonyítás. n-szerinti teljes indukciót fogunk alkalmazni. A lemma állítása $n = 0$-ra triviális, míg $n = 1, 2$-re egyszerű számolással kapható. Ezek után tegyük föl, hogy valamely $m > 2$-re

$$\langle a_0, a_1, \ldots, a_m \rangle = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}}. \tag{6}$$

Az indukciós föltevés alapján tudjuk, hogy $p_{m-1}, p_{m-2}, q_{m-1}, q_{m-2}$ csak az $a_0, a_1, \ldots, a_{m-1}$ egészektől függ, így független a_m-től. Ezért a (6)-ban — kihagyva a középső tagot — a_m helyett $a_m + \frac{1}{a_{m+1}}$-et írhatunk, és ekkor az

$$\frac{\left(a_m + \dfrac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \dfrac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}} = \langle a_0, a_1, \ldots, a_{m-1}, a_m, a_m + \frac{1}{a_{m+1}} \rangle \tag{7}$$

egyenlőséget kapjuk. A jobb oldalon formálisan nem egyszerű lánctört áll, de ezen lánctört nyilván egyenlő az $\langle a_0, a_1, \ldots, a_{m-1}, a_m, a_{m+1} \rangle$ egyszerű lánctörttel. Ezzel a bizonyítás kész, hiszen az iménti észrevételünk,

és egy egyszerű számolás után (7)-ből a bizonyítandó

$$\langle a_0, a_1, \ldots, a_m, a_{m+1}\rangle = \frac{p_{m+1}}{q_{m+1}}$$

egyenlőség adódik.

2.3.2. Lemma. *Az* (5)*-ben definiált* (p_i), (q_i) *és a belőlük nyerhető* $(\alpha_i) = \left(\dfrac{p_i}{q_i}\right)$ *sorozatokra,*

$$\begin{vmatrix} p_{i-1} & p_i \\ q_{i-1} & q_i \end{vmatrix} = (-1)^i \quad (i \geq 1), \tag{a}$$

$$\begin{vmatrix} p_{i-2} & p_i \\ q_{i-2} & q_i \end{vmatrix} = (-1)^i a_i \quad (i \geq 2), \tag{b}$$

$$\alpha_i - \alpha_{i-1} = \frac{(-1)^{i-1}}{q_{i-1}q_i} \quad (i \geq 1), \tag{c}$$

$$\alpha_i - \alpha_{i-2} = \frac{(-1)^i}{q_{i-2}q_i} \quad (i \geq 2), \tag{d}$$

$$\text{ln. k. o.}(p_i, q_i) = 1 \quad (i \geq 0). \tag{e}$$

Bizonyítás. Az (a) és a (b) állításokat i-szerinti teljes indukcióval igazoljuk.
(a) Egyszerű számolással kapjuk, hogy $i = 1$-re az állítás igaz. Legyen $m > 1$, és tegyük föl, hogy állításunk $i = m - 1$-re igaz.

$$\begin{aligned}
\begin{vmatrix} p_{m-1} & p_m \\ q_{m-1} & q_m \end{vmatrix} &= \begin{vmatrix} p_{m-1} & a_m p_{m-1} + p_{m-2} \\ q_{m-1} & a_m q_{m-1} + q_{m-2} \end{vmatrix} \\
&= \begin{vmatrix} p_{m-1} & a_m p_{m-1} \\ q_{m-1} & a_m q_{m-1} \end{vmatrix} + \begin{vmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{vmatrix} \\
&= -\begin{vmatrix} p_{m-2} & p_{m-1} \\ q_{m-2} & q_{m-1} \end{vmatrix} \\
&= -(-1)^{m-1} = (-1)^m
\end{aligned}$$

(b) Ugyanúgy igazolható, mint az (a) állítás, csak a kezdő lépés az $i = 2$.
(c) Ha $k \geq 2$ egész, akkor

$$\begin{aligned}
\alpha_k - \alpha_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} &= \frac{p_k q_{k-1} - p_{k-1} q_k}{q_k q_{k-1}} \\
&= \frac{-(p_{k-1}q_k - p_k q_{k-1})}{q_k q_{k-1}} = -\frac{\begin{vmatrix} p_{k-1} & p_k \\ q_{k-1} & q_k \end{vmatrix}}{q_k q_{k-1}} \\
&= -\frac{(-1)^k}{q_k q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}.
\end{aligned}$$

(d) Ugyanúgy igazolható, mint a (c) állítás.
(e) Az (a) állítás alapján nyilvánvaló.

2.3.3. Lemma. *Legyen $a_0, a_1, a_2, \ldots$ egészekből álló (végtelen) sorozatot, és tegyük föl, hogy legföljebb a_0 nem pozitív. Alkossuk meg az (5)-ben definiált két sorozatot, és tekintsük a belőlük képezhető $(\alpha_i) = \left(\frac{p_i}{q_i}\right)$ sorozatot. Az (α_i) sorozat páros indexű tagjai szigorúan monoton növekvő, míg páratlan indexű tagjai szigorúan monoton csökkenő sorozatot alkotnak. Továbbá tetszőleges $m, n \in \mathbb{N}_0$-ra*

$$\alpha_{2m} < \alpha_{2n+1},$$

azaz bármely páros indexű tag kisebb bármelyik páratlan indexű tagnál.
Bizonyítás. Vegyük észre, hogy az (5)-ben definiált (q_i) sorozat minden tagja pozitív, így a 2.3.2. Lemma (d) állítása szerint egyrészt bármely $k \geq 1$-re

$$\alpha_{2k} - \alpha_{2k-2} = \frac{(-1)^{2k}}{q_{2k}q_{2k-2}} > 0,$$

másrészt

$$\alpha_{2k+1} - \alpha_{2k-1} = \frac{(-1)^{2k-1}}{q_{2k+1}q_{2k-1}} < 0,$$

amelyek igazolják a lemmában állított monotonitásokat.

Az előbbiek szerint bármely $n, k \in \mathbb{N}$-re

$$\alpha_{2n} < \alpha_{2n+2k}, \quad \text{és} \quad \alpha_{2n+2k-1} < \alpha_{2k-1}. \tag{8}$$

A 2.3.2. Lemma (c) állítása szerint pedig

$$\alpha_{2n+2k} < \alpha_{2n+2k-1}. \tag{9}$$

(8) és (9) már maga után vonja az

$$\alpha_{2n} < \alpha_{2k-1}$$

egyenlőtlenséget, ami a lemma bizonyítását teljessé teszi.

2.3.4. Tétel. *Tekintsük egészek egy olyan $a_0, a_1, a_2, \ldots$ (végtelen) sorozatát, amelyben legföljebb a_0 nem pozitív, és alkossuk meg belőle az (5)-szerinti (p_i), (q_i) sorozatokat. Legyen minden $n \in \mathbb{N}$-re $\alpha_n = \frac{p_n}{q_n}$. Az (α_n) sorozat konvergens.*
Bizonyítás. A 2.3.3. Lemma szerint az (α_n) sorozat páros indexű tagjai szigorúan monoton növekvő, fölülről korlátos, míg páratlan indexű tagjai szigorúan monoton csökkenő, és alulról korlátos sorozatot alkotnak. Így mindkét részsorozat konvergens.

A 2.3.2. Lemma (c) és (d) állítása alapján az

$$(\alpha_0, \alpha_1),\ (\alpha_2, \alpha_3),\ (\alpha_4, \alpha_5), \ldots \tag{10}$$

intervallum sorozatra egyrészt

$$(\alpha_0, \alpha_1) \supset (\alpha_2, \alpha_3) \supset (\alpha_4, \alpha_5) \supset \ldots, \tag{11}$$

másrészt az előbbi Lemma (c) állítása — lévén a (q_k) sorozat pozitív tagú és szigorúan monoton növekvő — maga után vonja, hogy

$$\lim_{k\to\infty} |\alpha_{2k+1} - \alpha_{2k}| = \lim_{k\to\infty} \frac{|(-1)^{2k}|}{q_{2k+1}q_{2k}} = 0. \tag{12}$$

(11) és (12) együtt azt jelenti, hogy a (10) intervallum sorozatnak egyetlen közös pontja van, amely nem más, mint

$$\lim_{n\to\infty} \alpha_n.$$

Előbbi tételünk teszi értelmessé a fejezet elején bevezetett fogalmat, a végtelen egyszerű lánctört fogalmát.

2.3.5. Tétel. *Minden végtelen egyszerű lánctört irracionális számot reprezentál.*

Bizonyítás. Legyen $\alpha = \langle a_0, a_1, a_2, \ldots\rangle$ végtelen egyszerű lánctört, és jelölje α_k a k-adik kezdő szeletét. Tudjuk, a 2.3.4. Tétel alapján, hogy bármely $n \in \mathbb{N}$-re α α_{n-1} és α_n között van, így

$$0 < |\alpha - \alpha_n| < |\alpha_n - \alpha_{n-1}| = \frac{1}{q_n q_{n-1}},$$

azaz

$$0 < |\alpha - \alpha_n| < \frac{1}{q_n q_{n-1}}. \tag{13}$$

Mivel $\alpha_n = \dfrac{p_n}{q_n}$ kapjuk, hogy

$$|\alpha - \alpha_n| = |\alpha - \frac{p_n}{q_n}| = q_n^{-1}|\alpha q_n - p_n|,$$

azaz fölhasználva a (13) egyenlőtlenségeket

$$|\alpha q_n - p_n| < \frac{1}{q_{n-1}} \tag{14}$$

adódik. (14) azonban egyetlen racionális α-ra sem állhat fönn, ugyanis, ha valamely $a, b \in \mathbb{Z}$-re $\alpha = \frac{a}{b}$, akkor

$$\left|\frac{a}{b}q_n - p_n\right| = \frac{1}{|b|}|aq_n - bp_n| < \frac{1}{q_{n-1}},$$

amiből

$$|aq_n - bp_n| < \frac{|b|}{q_{n-1}}. \tag{15}$$

Az (5) definícióból nyilvánvaló, hogy a (q_n) pozitív tagú sorozat szigorúan monoton nő, így (15) jobb oldala 0-hoz tart, míg a bal oldalon természetes szám áll. Ezen ellentmondás igazolja tételünket.

2.3.6. Tétel. *A különböző végtelen egyszerű lánctörtek különböző valós számokat reprezentálnak.*

Bizonyítás. Tételünk azonnal következik azon egyszerű észrevételből, hogy ha
$\alpha = \langle a_0, a_1, a_2, a_3, \ldots \rangle$, akkor

$$\alpha = a_0 + \frac{1}{\beta},$$

ahol $a_0 = [\alpha]$ és $\beta = \langle a_1, a_2, a_3 \ldots \rangle$.

2.3.7. Tétel. *Bármely valós irracionális szám reprezentálható végtelen egyszerű lánctörttel.*
Bizonyítás. Olyan eljárást adunk meg, amellyel tetszőleges $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ irracionális számhoz megadhatjuk az azt reprezentáló végtelen egyszerű lánctörtet.

Előbb egy $x_0, x_1, \ldots$ valós számokból álló sorozatot, majd ennek segítségével egy egészekből álló $a_0, a_1, \ldots$ sorozat adunk meg.

Legyen először

$$x_0 = \alpha,$$
$$x_i = \frac{1}{x_{i-1} - [x_{i-1}]}, \quad \text{ha } i > 0,$$

amely nyilván egy végtelen sorozat, ugyanis mindegyik tagja irracionális.

Ezek után alkossuk meg a következő — egészekből álló — sorozatot.

$$a_i = [x_i] \qquad \text{minden} \quad i \in \mathbb{N}_0\text{-ra.}$$

A definíciók alapján egyrészt $a_0 = [\alpha]$, másrészt minden $k \geq 1$-re

$$a_k = [x_k] = \left[\frac{1}{x_{k-1} - a_{k-1}}\right].$$

Következő lépésként azt mutatjuk meg, hogy ha $k \geq 1$, akkor $a_k \in \mathbb{N}$. Valóban,

$$0 < x_k - a_k = x_k - [x_k] < 1,$$

amiből

$$x_{k+1} = \frac{1}{x_k - a_k} > 1. \tag{16}$$

Végül meg kell még mutatni, hogy a kapott $\langle a_0, a_1, a_2, \ldots \rangle$ végtelen egyszerű lánctört az α valós számot reprezentálja, azaz

$$\alpha = \lim_{n \to \infty} \langle a_0, a_1, \ldots, a_n \rangle.$$

Ezen állításunk a következő lemmából fog következni, amely alapján a tétel bizonyítását befejezhetjük.

2.3.8. Lemma. *Legyen $a_0, a_1, a_2, \ldots$ egészek olyan sorozata, amelyben legföljebb a_0 nem pozitív, és alkossuk meg az* (5)*-ben definiált*

(p_n), (q_n) sorozatot. Tetszőleges $x \in \mathbb{R}^+$ valós számra és $n \geq 2$ indexre

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{x}}}} = \langle a_0, a_1, \ldots, a_{n-1}, x \rangle = \frac{xp_{n-1} + p_{n-2}}{xq_{n-1} + q_{n-2}}.$$

Megjegyzés. E lemma láthatóan a 2.3.1. Lemma általánosítása, csak most
$\langle a_0, a_1, \ldots, a_{n-1}, x \rangle$ nem egyszerű lánctört, hanem csak egy arra hasonlító formális kifejezés. Mivel tetszőleges k-ra p_k, q_k számok csak $a_0, a_1, \ldots, a_k$-tól függenek, azért a p_i, q_i számok $i < k$ esetén a jelen esetben is egészek.

Bizonyítás. n-szerinti teljes indukciót alkalmazunk.
$n = 2$.

$$\begin{aligned}\langle a_0, a_1, x \rangle &= a_0 + \frac{1}{a_1 + \dfrac{1}{x}} = a_0 + \frac{x}{a_1 x + 1} \\ &= \frac{a_0(a_1 x + 1) + x}{x a_1 + 1} = \frac{x(a_1 a_0 + 1) + a_0}{x a_1 + 1} \\ &= \frac{x p_1 + p_0}{x q_1 + q_0}.\end{aligned}$$

Legyen $n > 2$ és tegyük föl, hogy állításunk igaz minden $2 \leq k < n$-re. Mivel

$$\langle a_0, a_1, \ldots, a_n, x \rangle = \langle a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{x} \rangle,$$

az indukciós föltétel alapján

$$\begin{aligned}\langle a_0, a_1, \ldots, a_n, x \rangle &= \frac{\left(a_n + \dfrac{1}{x}\right) p_{n-1} + p_{n-2}}{\left(a_n + \dfrac{1}{x}\right) q_{n-1} + q_{n-2}} \\ &= \frac{p_n + \dfrac{1}{x} p_{n-1}}{q_n + \dfrac{1}{x} q_{n-1}} \\ &= \frac{x p_n + p_{n-1}}{x q_n + q_{n-1}}\end{aligned}$$

A tétel bizonyításának folytatása.
Írjuk át (16)-ot

$$x_k = a_k + \frac{1}{x_{k+1}} \qquad (k \geq 0)$$

alakba, és alkalmazzuk az (x_n) sorozat konstrukciójában.

$$\alpha = x_0 = a_0 + \frac{1}{x_1} = a_0 + \frac{1}{a_1 + \dfrac{1}{x_2}} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + \dfrac{1}{x_3}}} = \dots,$$

amiből

$$\alpha = \langle a_0, a_1, a_2, \dots, a_n, x_{n+1} \rangle$$

adódik tetszőleges n-re.

Vegyük észre, hogy rögzített n-re az első $n+1$ kezdő szelete az $\langle a_0, a_1, a_2, \dots \rangle$ végtelen lánctörtnek ugyanaz, mint az $\langle a_0, a_1, a_2, \dots, a_n, x_{n+1} \rangle$ lánctörté.

Az előbbi Lemma szerint

$$\begin{aligned} \alpha = x_0 &= \langle a_0, a_1, a_2, \dots, a_n, x_{n+1} \rangle \\ &= \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}, \end{aligned}$$

így ha a korábbi jelölésekkel $\alpha_k = \dfrac{p_k}{q_k}$ minden $k \leq n$, akkor

$$\begin{aligned} \alpha - \alpha_n &= \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{(-1)(p_n q_{n-1} - p_{n-1}q_n)}{(x_{n+1}q_n + q_{n-1})q_n} \\ &= \frac{(-1)^n}{(x_{n+1}q_n + q_{n-1})q_n}. \end{aligned}$$

Ezek után a tétel igazolásához már csak egy rutin becslést kell alkalmaznunk, amelyben fölhasználjuk, hogy $x_{n+1} > a_{n+1}$, ami a definícióból világos.

$$\begin{aligned} |\alpha - \alpha_n| &= \frac{1}{(x_{n+1}q_n + q_{n-1})q_n} \\ &< \frac{1}{(a_{n+1}q_n + q_{n-1})q_n} \\ &= \frac{1}{q_n q_{n+1}}, \end{aligned}$$

amiből már következik, hogy $\lim\limits_{n\to\infty} \alpha_n$ létezik, továbbá

$$\alpha = \lim_{n\to\infty} \alpha_n = \lim_{n\to\infty} \langle a_0, a_1, a_2, \dots, a_n \rangle.$$

2.3.9. Következmény. *Legyen α irracionális szám. A korábbi jelölésekkel tetszőleges $n \in \mathbb{N}$-re*

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

Példák.1. Megadjuk $\alpha = \sqrt{23}$ lánctört előállítása.

Vegyük észre, hogy $4 < \sqrt{23} < 5$, és alkalmazzuk az 2.3.7. Tétel bizonyításához használt eljárást.

$$
\begin{aligned}
x_0 &= \sqrt{23} = 4 + (\sqrt{23} - 4) && a_0 = 4 \\
x_1 &= \frac{1}{x_0 - [x_0]} = \frac{1}{\sqrt{23} - 4} = \frac{\sqrt{23} + 4}{7} \\
&= 1 + \frac{\sqrt{23} - 3}{7} && a_1 = 1 \\
x_2 &= \frac{1}{x_1 - [x_1]} = \frac{7}{\sqrt{23} - 3} = \frac{\sqrt{23} + 3}{2} \\
&= 3 + \frac{\sqrt{23} - 3}{2} && a_2 = 3 \\
x_3 &= \frac{1}{x_2 - [x_2]} = \frac{2}{\sqrt{23} - 3} = \frac{2(\sqrt{23} + 3)}{14} \\
&= \frac{\sqrt{23} + 3}{2} = 1 + \frac{\sqrt{23} - 4}{7} && a_3 = 1 \\
x_4 &= \frac{1}{x_3 - [x_3]} = \frac{7}{\sqrt{23} - 4} = \frac{7(\sqrt{23} + 4)}{7} \\
&= \sqrt{23} + 4 = 8 + (\sqrt{23} - 4) && a_4 = 8 \\
x_5 &= \frac{1}{x_4 - [x_4]} = \frac{1}{\sqrt{23} - 4} = \frac{\sqrt{23} + 4}{7} \\
&= 1 + \frac{\sqrt{23} - 3}{7} && a_5 = 1
\end{aligned}
$$

Látható, hogy $x_5 = x_1$, s ha az eljárást folytatjuk, akkor a továbbiakban $x_6 = x_2,\ x_7 = x_3, \ldots x_9 = x_5 = x_1$ adódik, ami a lánctört valamiféle periódikusságát jelenti. Kaptuk tehát, hogy a $\sqrt{23}$-at előállító lánctört nem más, mint

$$\sqrt{23} \cong \langle 4, 1, 3, 1, 8, 1, 3, 1, 8, \ldots \rangle = \langle 4, \overline{1, 3, 1, 8} \rangle,$$

ahol a tizedestörteknél szokásos írásmódot használtuk. E „jelenséggel” rövidesen foglalkozni fogunk.

2. A π lánctört alakja.
Ha fölhasználjuk, hogy

$$\pi = 3,141592653\ldots,$$

akkor az előbbi módon számolva kapjuk, hogy

$$\begin{aligned}
x_0 &= \pi = 3 + (\pi - 3) && a_0 = 3\\
x_1 &= \frac{1}{x_0 - [x_0]} = \frac{1}{0,141592\ldots} = 7,06251330\ldots && a_1 = 7\\
x_2 &= \frac{1}{x_1 - [x_1]} = \frac{1}{0,06251330\ldots} = 15,99659440\ldots && a_2 = 15\\
x_3 &= \frac{1}{x_2 - [x_2]} = \frac{1}{0,99659440\ldots} = 1,00341723\ldots && a_3 = 1\\
x_4 &= \frac{1}{x_3 - [x_3]} = \frac{1}{0,00341723\ldots} = 292,63724\ldots && a_4 = 292\\
&\vdots
\end{aligned}$$

Ha tovább számolunk ílymódon, akkor a

$$\pi \cong \langle 3, 7, 15, 1, 292, \ldots \rangle$$

lánctört előállítást kaphatjuk, amit tetszőleges sok nevezőre számíthatunk ki. A lánctört nem véges, tehát π irracionális szám.

3. Az e lánctört előállítása.
Fölhasználva, hogy $e = 2,718281828\ldots$, 1737-ben Euler megmutatta, hogy

$$\frac{e-1}{e+1} \cong \langle 0, 2, 5, 10, 14, 18, \ldots \rangle,$$

ahol a nevezők a 10-estől kezdve számtani sorozatot alkotnak.

Tovább számolva kapta, hogy

$$\frac{e^2-1}{e^2+1} \cong \langle 0, 1, 3, 5, 7, 9, \ldots \rangle,$$

ahol a nevezők szintén számtani sorozatot alkotnak.

Végül az előbbi két lánctörtből már megkapta az e előállítását,

$$e \cong \langle 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots \rangle,$$

ahol az egymást követő páros számokat rendre két-két 1-es választja el. Mivel e lánctört végtelen, adódik az e irracionális volta.

Egy érdekes tény, hogy az e tizedestört alakjában a tizedesvessző utáni 7-es jegy után a kétszer (és nem többször!) előforduló 1828 éppen Lev Tolsztoj, a nagy orosz regényíró, születési éve.

Megjegyzés. Az előbbi két példa volt az első lépés Euler azon sejtésének bizonyítása felé, hogy e két nevezetes konstans — Euler elnevezésével — *transzcendens szám*, mert „a velük való foglalkozás meghaladja az algebrai módszerek erejét”.

2.4. Periódikus lánctörtek.

Definíció. Azt mondjuk, hogy az $\alpha = \langle a_0, a_1, a_2, \ldots \rangle$ végtelen egyszerű lánctört *periódikus*, ha van olyan $n \in \mathbb{N}$ egész, hogy minden elég nagy r egészre $a_r = a_{n+r}$, azaz fölírható

$$\langle a_0, a_1, \ldots, a_m, b_1, \ldots, b_n, b_1, \ldots, b_n, \ldots \rangle.$$

Ez esetben gyakran alkalmazzuk az

$$\langle a_0, a_1, a_2, \ldots \rangle = \langle a_0, a_1, \ldots, a_m, \overline{b_1, \ldots, b_n} \rangle$$

írásmódot. Azt is mondjuk, hogy $(b_1, \ldots, b_n)$ az α lánctört egy lehetséges *periódusa*. A legkisebb ilyen n-et az α lántört periódusa hosszának nevezzük.

Megjegyzés. Vegyük észre, hogy $\sqrt{23}$ lánctört alakja periódikus, míg e, π lánctört alakja nem periódikus.

Tekintsük a $\gamma = \langle 5, 2, 3, 2, 3, 2, 3, \ldots \rangle = \langle 5, \overline{2, 3} \rangle$ végtelen egyszerű lánctörtet. Ha β-val jelöljük a $\langle 2, 3, 2, 3, \ldots \rangle = \langle \overline{2, 3} \rangle$ lánctörtet, akkor γ

$$\gamma = 5 + \frac{1}{\beta} \tag{17}$$

alakban írható.

A β lánctörtre fönnáll a

$$\beta = 2 + \frac{1}{3 + \frac{1}{\beta}}$$

egyenlőség, amelyből β-ra a

$$3\beta^2 - 6\beta - 2 = 0$$

másodfokú egyenlet adódik. Ennek pozitív gyöke (hiszen $\beta > 0$)

$$\beta = \frac{3 + \sqrt{15}}{3}.$$

Ezt (17)-be helyettesítve kapjuk, hogy

$$\gamma = \frac{27 + \sqrt{15}}{6},$$

amely szintén tekinthető egy alkalmas másodfokú egyenlet egy (pozitív) gyökének.

Definíció. Azt mondjuk, hogy az $\alpha \in \mathbb{R}$ valós szám *kvadratikus irracionális*, ha

$$\alpha = \frac{a + b\sqrt{c}}{d}$$

alakban írható, ahol $a, b, c, d \in \mathbb{Z}$, továbbá $d \neq 0$ és $c > 0$ nem négyzetszám.

Megjegyzések.

($\imath$) Világos, hogy a kvadratikus irracionálisok épp az egész együtthatós

másodfokú polinomok irracionális zéróhelyei. Maga az elnevezés is innen ered.
(*ii*) Látható, hogy az előbbi γ, β periódikus lánctörtek kvadratikus irracionálisok.

Észrevételünk speciális esete a következő tételnek.

2.4.1. Tétel. *Bármely periódikus egyszerű lánctört kvadratikus irracionális szám és megfordítva, minden (valós) kvadratikus irracionális szám egyszerű lánctört alakja periódikus.*

Tételünket nem bizonyítjuk. Az első állítás igazolásának önálló elvégzését ajánljuk. A második rész már munkaigényesebb. Az érdeklődők megtalálják például Niven és Zuckermann Bevezetés a számelméletbe c. könyvében.

Emlékezzünk vissza, hogy

$$\sqrt{23} = \langle 4, \overline{1, 3, 1, 8} \rangle,$$

azaz a periódus közvetlenül az első jegy, a $\sqrt{23}$ egész része után kezdődött, amit úgy is mondhatunk, hogy lánctört alakja „tisztán periódikus". Megmutatható, hogy bármely $d \in \mathbb{N}$-re, valahányszor d nem négyzetszám, mindannyiszor $\sqrt{d}$ lánctört alakja tisztán periódikus. Sőt még ennél is több igaz, a periódus bizonyos szimmetria tulajdonsággal is rendelkezik. Nevezetesen, a következő tétel igazolható.

2.4.2. Tétel. *Ha $d \in \mathbb{N}$ nem négyzetszám, akkor*

$$\sqrt{d} = \langle a_0, \overline{a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0} \rangle,$$

ahol $a_0 = [\sqrt{d}]$. **Példák.**

$$\sqrt{19} = \langle 4, \overline{2, 1, 3, 1, 2, 8} \rangle$$
$$\sqrt{73} = \langle 8, \overline{1, 1, 5, 5, 1, 1, 16} \rangle$$
$$\sqrt{94} = \langle 9, \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18} \rangle$$

Megemlítjük, hogy a száznál kisebb nem négyzetszámok közül a $\sqrt{94}$ lánctört alakjának a leghosszabb a periódusa, 16 elemű.