MBL013E Számelmélet és Alkalmazásai

előadás vázlat 2013

0. Korábbi kurzusok alapján ismertnek föltételezett anyag.

1. Az MBL112E kódú, Bevezetés a száelméletbe c. kurzus anyaga, különösen a következők:
- euklideszi algoritmus, oszthatóság, kongruencia, Euler és Fermat kongruenciatétele;
- prímszámok, a számelmélet alaptétele;
- négyzetösszegekre bontás.

2. Az elemi analízisből:
- végteles 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. A racionális számok tizedestört alakja.

Legyenek $a, b \in \mathbb{Z},\ b \geq 1$ 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* $\max\{m.n\}$.

Bonyolultabb a helyzet akkor, ha az osztássorozat nem véges. Ez nyilván akkor fordul elő, ha létezik olyan $p|b$ prímszám, hogy $\notin \{2, 5\}$. A tapasztalat szerint ekkor a tizedesjegyek sorozatában létezik egy 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 $a_i, b_j \in \mathbb{Z}$, $0 \leq a_i, b_j \leq 9$. Előfordolhat, hogy az ismétlődő $b_1, \dots, b_m$ 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 $a_1, a_2, \dots, a_k$ 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 $a, b \in \mathbb{Z},\ b \geq 1$ 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 $a, b \in \mathbb{Z},\ b \geq 1$ 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 $a, b \in \mathbb{Z},\ b \geq 1$ 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 nem 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.*

1.2.1. Tétel. (Eratosztenesz 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.

A számelméletben számos olyan egyszerűnek látszó állítás fogalmazható meg, amelyek gyakran évszázadok óta nyitott kérdések. Ezek közül említünk néhányat.

(1) Tökéletes számok.

Az $M_n = 2^n - 1$ alakú számok közül csak azok lehetnek prímek, amelyeben $n = p$ prímszám, de nem minden ilyen alakú szám prím. A legkisebb ilyen összetett szám az M_{11}. Az ilyen prímeket *Mersenne-prímeknek* nevezzük. Kérdés, hogy van-e végtelen sok Mersenne-prím. Jelenleg explicite 48 ilyen szám ismert. A legbagyobbat,

a 48-adikat 2013. februárjában tették közzé a University of Central Missouri matematikusai, ez az $M_{57.885.161}$ amelynek 17.425.171 jegye van. A 47. Mersenne prím az $M_{43.112.609}$, amelynek 12.978.189 jegye van.
A (nem bizonyított) sejtés az, hogy végtelen sokan vannak. E kérdést az teszi érdekessé, hogy már Euklidesz tudta, hogy a $P_k = 2^{k-1}(2^k - 1)$ alakú számok, ahol a második tényező prím, ún. tökéletes számok (megegyeznek náluk kisebb pozitív osztóik összegével). Euler igazolta, hogy minden páros tökéletes szám ilyen alakú. Így az előbbi kérdés egyenértékű azzal, hogy létezik-e végtelen sok páros tökéletes szám. Az sem ismert, hogy létezik-e páratlan tökéletes szám.

(2) 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.
Megjegyzések.
(1) A 2011. közepén ismert legnagyobb ikerprím pár:

$$66.516.468.355 \cdot 2^{333333} \pm 1$$

(2) A 2 helyett tetszőleges páros számot is választhatunk. Megoldatlan az a kérdés is, hogy van-e végtelen sok olyan prímszám pár, amelyek különbsége $2k$ valamely rögzített k-ra.
(3) Egy lehetséges további általánosítás az, hogy prímpárok helyett prím hármasokat, prím négyeseket vizsgálunk. Például n, $n+2$, $n+4$ mindegyike prím, ha $n = 3$. Vannak-e további ilyen hármasok, esetleg végtelen sok?
(4) Az ikerprímkérdés úgy is fogalmazkató, hogy vajon két szomszédos prímszám különbsége végtelen sokszor lesz „elegendően kicsi".
(5) Ugyancsak nyitott kérdés, hogy két szomszédos négyzetszám között van-e mindig prímszám. Másképpen fogalmazva: a szomszédos prímszámok különbsége nem nőhet „túlságosan gyorsan", bár tudjuk, ogy bármekkora hézag előfordulhat.
(6) Az ikerprímek (ha végtelen sokan vannak is) nagyon ritkán fordulnak elő a prímek között. Ugyanis míg a prímek reciprokaiból álló sor divergens, addig az ikerprímek reciprokai sora konvergens.
(7) Végül egy érdekes eredmény: végtelen sok olyan p prímszám létezik, amelyre $p+2$ prímszám, vagy két prímszám szorzata. Innen már csak egyetlen „kis" lépés az ikerprím-probléma megoldása.

(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 sejtése szerint 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 lényegében be is bizonyította. Nevezetesen igazolta, 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) Bizonyították, hogy minden 2-nél nagyobb páros szám előáll legföljebb 6 prímszám összegeként.
(3) 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.)
(4) 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".

(4) 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.

1.3. Prímtesztek speciális alakú prímszámokra.

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

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

alakú, ahol $p_1, p_2, \dots, p_k$ 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). Ma azt tudjuk, hogy, ha $5 \le n \le 23$, akkor F_n összetett szám, és ugyanezt tudjuk néhány további n-re is. A rekorder Fermat-szám az $F_{23.471}$, amelynek több mint $10^{7.000}$ decimális jegye van, és osztható $5 \cdot 2^{23.473} + 1$-gyel.

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.

1.3.1. Tétel. *$n \ge 2$-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, amiból 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 $p \equiv 1 \pmod{2^{n+2}}$.

1.3.2. 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.

Vegyük $3^{2^{31}}$ 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.

A Mersene-prímek jelentőségét — mint már említettük —Euklidesz Elemek című műve IX.36. Tétele adja, mely szerint valahányszor $M_n = 2^n - 1$ prím, mindannyiszor $P_n = 2^{n-1}(2^n - 1)$ tökéletes szám. Euler igazolta, hogy minden páros tökéletes szám ilyen alakú. A legkisebb olyan p prímszám, amelyre M_p összetett a 11. Ugyanis $2^{11} - 1 = 2047 = 23 \cdot 89$.

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 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.

E számokat először a 17. században élt Marin Mersenne (élénk levelezést folytatott a többek között Fermattal és Descartessel) vizsgálta kiterjedten. Egy 1644-ben megjelent könyvében igen nehéz feladatnak minősítette az ilyen alakú számok prím voltának ellenőrzését. 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.

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

1.3.3. 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

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

1.3.4. 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.

1.4. Prímtesztek tetszőleges prímekre.

Amennyiben $n \in \mathbb{N}$ „nem nagy", egyszerűen kipróbálhatjuk, hogy osztható-e a $\sqrt{n}$-nél nem nagyobb prímekkel. Ha nem, akkor prímszám. Így a prímfölbontás is megkapható. Ha azonban egy 500 jegyű számot — amelynek nincsenek „kis-", vagy „speciális alakú" prímosztói — akarunk prímtényezőkre bontani, akkor ez lehetetlen vállalkozás még a leggyorsabb számítógépekkel is a ma ismert módszerekkel.

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.

1.4.1. Tétel. *Legyenek $a, b, c, m \in \mathbb{Z}$, ahol $b > 1$, $m > 0$. Ekkor*
(*i*) *a^b maradéka modulo m,*
(*ii*) *$\ln. \mathrm{k}. \mathrm{o}.(a, b)$,*
(*iii*) *az $\left(\frac{a}{b}\right)$ Jacobi-szimbólum, páratlan b és $\ln. \mathrm{k}. \mathrm{o}.(a, b)$ esetén,*
(*iv*) *az $ax + by = c$ lineáris diofantikus egyenlet megoldásai, és*

(ν) *az* $ax \equiv b \pmod m$ *kongruencia megoldásai kiszámíthatók legfőljebb* $5\log_2 b$ *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 $\text{ln. k. o.}(a, m) = 1$, 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 $361 = 11 \cdot 31$, 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.

1.4.1. 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 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, amelyekre 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 $a^{m-1} \equiv 1 \pmod m$.

1.4.2. 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.

1.4.3. Tétel. (Solovay-Strassen prímteszt)

(A) *Legyen* $n > 1$ *páratlan egész, és tekintsük az*

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

kongruenciát, ahol $\left(\frac{a}{n}\right)$ *Jacobi-szimbólum.*
Ha n *prím, akkor* (1) *minden* $a \not\equiv 0 \pmod{n}$ *esetén teljesül.*
Ha n *összetett, akkor* (1) *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 az* (1) *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.

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

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

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* (2) *minden* $a \not\equiv 0 \pmod{n}$ *esetén jó sorozat.*
Ha n *összetett akkor* (2) *egy modulo* n *teljes maradékrendszer elemeinek kevesebb, mint felére alkot jó sorozatot.*

1.5. Titkosírások.

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

1. 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.

2. Ún. „rostély" alkalmazása. Ilyennel a legtöbben találkozhattunk Verne Sándor Mátyás című regényében. Ez esetben csak a rostélyra kell vigyázni, hogy ne kerüljön illetéktelen kézbe.

3. A kódoló kulcs nyilvános, de a dekódoló nem az.

Ez 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 $1, 2, \dots, N$ számokkal. A Φ kódoló függvény most az $\{1, 2, \dots, N\}$ 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 akajuk 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 yakorlati 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, pl.
A$\mapsto$ 01, Á$\mapsto$ 02, B$\mapsto$ 03, ... , 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 válasz 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 $\text{ln. k. o.}(t, \varphi(N)) = 1$, 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.

(3) $\quad r\Phi = r^t$ legkisebb nemnegatív maradéka modulo N, $\quad 1 \le r \le N$.

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

(4) $\quad s\Psi = s^m$ legkisebb nemnegatív maradéka modulo N, $\quad 1 \le r \le N$.

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

$$r^{tm} \equiv r \pmod{N}. \tag{5}$$

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

$$r^{1+k\varphi(N)} \equiv r \pmod{N} \tag{6}$$

minden r-re teljesül.
4. (6) alapján (5) és (4)-ben megfelelő m-hez jutunk, ha megoldjuk az

$$mt = 1 + k\varphi(N) \tag{7}$$

diofantoszi egyenletet m-re és k-ra. Az $\ln.\,k.\,o.(t, \varphi(N)) = 1$ 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?

($\imath$) 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).
- (3) és (4) 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.

1.5.1. Tétel. *Legyen p, q két nagy prímszám, $N = pq$ és $\ln.\,k.\,o.(t, \varphi(N)) = 1$. Definiáljuk (3) és (4) alapján a Φ, Ψ kulcspárt, ahol m-re teljesül (7). Myilvánosságra 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.