Eötvös Loránd Tudományegyetem

Természettudományi Kar

Kis Mihály

Prímtesztek és prímfaktorizáció

BSc Szakdolgozat

Témavezető:

Dr. Freud Róbert

Algebra és Számelmélet Tanszék

Budapest, 2013

Tartalomjegyzék

Bevezetés

Mitől lesz egy szám prím és ez hogyan ellenőrizhető, vagy egy összetett számról egyetlen valódi osztójának ismerete nélkül hogyan dönthetjük el, hogy valóban összetett? Az úgynevezett prímtesztek erre a problémára nyújtanak (mára már 100%-os biztonságú) választ. A prímtesztekhez szorosan kapcsolódó témakör a prímfelbontás. A gyakorlat számára már több gyors prímfaktorizációs módszert dolgoztak ki nagy számok felbontására, de ennek a problémának a polinomiális idejű eldönthetősége még mindig nyitott kérdés a matematikában. Ennek a témakörnek az „ereje” – vagyis, hogy egy nagy szám felbontása rengeteg időt vesz igénybe a tudomány jelenlegi állása szerint – pontosan ebben rejlik, ezért remekül alkalmazható a kriptográfiában mint nyílt kulcsú titkosírási módszer. Különböző feladatok megoldásával és saját példák gyártásával hoztam közelebb ezen témaköröket a kevésbé jártas olvasók számára is. Készítettem prímteszteket és prímfelbontásokat illusztrálandó programokat, melyeket C++ nyelvben írtam meg és CD formájában mellékeltem a dolgozathoz.

Ezúton szeretném megköszönni témavezetőmnek, Freud Róbertnek a dolgozat tartalmi és formai részéhez fűzött értékes megjegyzéseit, családomnak és barátaimnak a támogatást és a LaTeX-ben nyújtott segítséget.

1. fejezet

Prímtesztek

Hogyan dönthetjük el egy nagy számról, hogy prím vagy összetett? A kérdés igen érdekes, a válasz pedig az ún. prímtesztekben rejlik, vagyis az olyan számelméleti módszerekben, melyek a valódi osztók ismerete nélkül képesek ezt eldönteni. A következő fejezetben megismerkedünk a prímtesztek családjának alapvetőbb tagjaival, melyek (számítógépen) viszonylag gyorsan megadják a választ arra a kérdésre, hogy egy szám prím-e vagy sem.

1.1. Fermat-féle teszt

A kis Fermat-tétel közvetlen következményeként kapjuk ezt az eljárást, amely majdnem 100%-os pontossággal eldönti egy szám mibenlétét. Aggodalomra csak az ún. álprímek vagy pszeudoprímek adnak okot, de szerencsére ezek a számok ritkán fordulnak elő.

1.1.1. Tétel. (Euler-Fermat-tétel) *Legyenek a, n egészek és $(a, n) = 1$, ekkor igaz az alábbi kongruencia:*

$$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{1.1}$$

Tulajdonképpen a tétel speciális esetére, azaz a kis Fermat-tételre lesz szükségünk.

1.1.2. Tétel. (Kis Fermat-tétel) *Legyen p prím és $p \nmid a$, ekkor*

$$a^{p-1} \equiv 1 \pmod{p} \tag{1.2}$$

Ekkor azt csinálhatjuk, hogy veszünk elég sok (kb. 1000-5000) n-hez relatív prím számot (n-nél kisebbeket) és mindegyikre ellenőrizzük a feltételt. Bármelyiknél is sérül a kongruencia, akkor biztosan összetett a számunk. Viszont, ha az összes próbán átmegy, akkor nagyjából 2^{-1000} (1000 különböző alapra) az esélye annak, hogy tévedtünk, vagyis, hogy az összes a_i alapra $a_i^{n-1} \equiv 1 \pmod{n}$, és az n mégis összetett.
Ugyanis a már említett speciális összetett számok, azaz álprímek átmehetnek a teszten. Ha véletlenül ilyen számmal állunk szemben, és a módszer prímnek gondolja, akkor 100%-osan tévedtünk.

1.1.3. Definíció. *Legyen $n > 1$ összetett és $(a, n) = 1$. Ha $a^{n-1} \equiv 1 \pmod{n}$, akkor n-et a alapú/bázisú álprímnek vagy pszeudoprímnek nevezzük.*

1.1.4. Példa. 2-es alapú álprím a 341, de nem 3-as alapú.
Ugyanis $341 = 11 \cdot 31$, továbbá $2^{10} \equiv 1 \pmod{11}$ és $2^5 \equiv 1 \pmod{31}$, tehát $2^{340} \equiv 1 \pmod{341}$. Viszont nem 3-as alapú, mert $3^{340} = (3^{30})^{10} \cdot 3^{30} \cdot 3^{10} \equiv 3^{10} \equiv -6 \not\equiv 1 \pmod{31}$, így $3^{340} \not\equiv 1 \pmod{341}$.

1.1.5. Példa. 3-as alapú álprím a 91, de nem 2-es alapú.
Ugyanis $91 = 7 \cdot 13$, továbbá $3^6 \equiv 1 \pmod{7}$ és $3^3 \equiv 1 \pmod{13}$, ezekből következik, hogy $3^{90} \equiv 1 \pmod{91}$. De nem 2-es alapú álprím, mert $2^{90} \equiv 2^6 \equiv -1 \pmod{13}$, ebből következik, hogy $2^{90} \not\equiv 1 \pmod{91}$.

1.1.6. Állítás. *Legyen n pozitív összetett egész. Ekkor a következők igazak:*
(i) Az n szám a alapú álprím $\iff \sigma_n(a) \mid n - 1$.
(ii) Ha n az a_1 és az a_2 alapokra álprím $\implies n$ álprím az $a_1 a_2$ és $a_1 a_2^{-1}$ alapokra is.
(iii) Ha $a^{n-1} \not\equiv 1 \pmod{n}$ egy $(a, n) = 1$ alapra, akkor az $a_i \in U(\mathbb{Z}_n)$ alapok legalább a felére bukja a tesztet.

1.1.7. Megjegyzés. Az a^{-1} számon az a szám inverzét értjük az n szerint vett redukált maradékrendszerben, amit $U(\mathbb{Z}_n)$-nel jelölünk. Vagyis a^{-1} az a szám, melyre $a^{-1}a \equiv aa^{-1} \equiv 1 \pmod{n}$, és $U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n : (a, n) = 1\}$.

Bizonyítás.

(i) rész

$\Rightarrow$ irány:

Mivel n egy a alapú álprím, ezért $a^{n-1} \equiv 1 \pmod{n}$ teljesül. Ebből $\sigma_n(a) \mid n-1$ oszthatóság következik.
$\Leftarrow$ irány:
Tudjuk, hogy $\sigma_n(a) \mid n-1 \Leftrightarrow \exists k > 0\ \sigma_n(a)k = n-1$. Ezért az $a^{\sigma_n(a)} \equiv 1 \pmod{n}$ kongruenciát k-adikra emelve kapjuk, hogy $a^{k\sigma_n(a)} \equiv 1 \pmod{n}$, ami pont $a^{n-1} \equiv 1 \pmod{n}$.

(ii) rész
$a_1^{n-1} \equiv 1 \pmod{n}$, ezt jobbról beszorozva a_2^{n-1}-nel kapjuk, hogy $a_1^{n-1} \cdot a_2^{n-1} = (a_1a_2)^{n-1} \equiv 1 \pmod{n}$. Ezt jobbról beszorozva $a_2^{-(n-1)}$-nel $1 \equiv a_1^{n-1} \equiv a_2^{-(n-1)} \pmod{n}$-hez jutunk. Mindent összevetve teljesülnek az $(a_1a_2^{-1})^{n-1} \equiv 1 \pmod{n}$, $(a_1a_2)^{n-1} \equiv 1 \pmod{n}$ kongruenciák.

(iii) rész
Legyen a_1, amire (1.2) teljesül. Ekkor $(aa_1)^{n-1} = a^{n-1} \cdot a_1^{n-1} \equiv a^{n-1} \not\equiv 1 \pmod{n}$. Ha van k db páronként nem kongruens alap, amire (1.2) igaz, akkor ezt mindegyikre elmondhatjuk. Az aa_i-k páronként inkongruensek, ugyanis, ha $a_i \not\equiv a_j \pmod{n}$, akkor $(a_i, n) = 1$ miatt $aa_i \not\equiv aa_j \pmod{n}$ $(i \neq j)$. Tehát akármennyi a_i-t adnak is meg, legalább ennyi aa_i létezik, vagyis egy redukált maradékrendszer elemeinek legalább a fele az összetettség tanúja.
Ezzel az állítást beláttuk. □

1.1.8. Példa. 2-es és 15-ös alapú álprím a 341, tehát 30-as alapú is.
15-ös alapú, mert $15^4 \equiv 2 \pmod{31}$ az 1.1.4 példa miatt pedig $15^{20} \equiv 2^5 \equiv 1 \pmod{31}$, és $15^{10} \equiv 1 \pmod{11}$. Az előző állítás (ii) részéből rögtön következik, hogy $30^{340} \equiv 1 \pmod{341}$.

Sajnos léteznek olyan álprímek, melyek minden a alapra teljesítik a teszt feltételeit, vagyis legyen n ilyen, ekkor $\forall(a, n) = 1$-re $a^{n-1} \equiv 1 \pmod{n}$. Nem olyan reménytelen a helyzet, ugyanis az ilyen ún. univerzális álprímek még inkább ritkábban helyezkednek el. Annak az esélye, hogy biztosan csődöt mond a teszt, gyakorlati szempontból elhanyagolható.

1.1.9. Definíció. *Legyen $n > 1$ összetett, ha minden $(a, n) = 1$ esetén $a^{n-1} \equiv 1 \pmod{n}$ igaz, akkor n-et univerzális álprímnek vagy Carmichael-számnak nevezzük.*

1.1.10. Példa. Carmichael-szám a 2821.
Ugyanis $2821 = 7 \cdot 13 \cdot 31$, továbbá legyen $(a, 2821) = 1$ tetszőleges. Ekkor a kis Fermat-tétel miatt $a^6 \equiv 1 \pmod 7$, $a^{12} \equiv 1 \pmod{13}$ és $a^{30} \equiv 1 \pmod{31}$. A Kínai maradéktételből következik, hogy $a^{2820} \equiv 1 \pmod{2821}$.

Eme példán jól látszik az univerzális álprímek egyik karakterizációja, azaz igaz a következő állítás.

1.1.11. Állítás. *Ha n univerzális álprím, akkor négyzetmentes és $p \mid n \Longrightarrow p-1 \mid n-1$.*

Ennek felhasználásával könnyen igazolható például, hogy a Carmichael-számoknak több, mint kettő prímosztójuk van.

1.1.12. Következmény. Egy n univerzális álprímnek legalább három prímosztója van.

Bizonyítás. Tegyük fel indirekt, hogy $n = p \cdot q$ $(p \neq q)$. Tudjuk, hogy $p-1 \mid n-1 = pq-1 = pq-p+p-1 = p(q-1)+p-1$. Tehát azt kaptuk, hogy $p-1 \mid p(q-1)$, viszont $(p, p-1) = 1$ miatt $p-1 \mid q-1$ is igaz. Szerepcserével a $q-1 \mid p-1$ oszthatóság is fennáll, amiből következik, hogy $p = q$, ami ellentmondás. $\square$

A Fermat-féle prímteszt sebességének lelke az $a^{n-1} \pmod n$ érték kiszámításán múlik. Ismételt négyzetre emelésekkel ez gyorsan számítható. A módszer a következő:

- Adott $n-1$ értékét átváltjuk kettes számrendszerbe
- Sorban $\pmod n$ számolva kiszámítjuk az $a, a^2, a^4, ..., a^{2^{\lfloor log_2(n-1) \rfloor}}$ számokat
- Majd az $n-1$ kettes számrendszerben felírt alakjában ahol egyes szerepel, ott az annak megfelelő kettőhatványokat összeszorozzuk ügyelve arra, hogy minden esetben $\pmod n$ redukáljunk

Nézzünk erre is egy példát:

1.1.13. Példa. Számoljuk ki a $3^{102} \pmod{103}$ értéket!

$3 \equiv 3 \pmod{103}$

$3^2 \equiv 9 \pmod{103}$

$3^4 \equiv 81 \pmod{103}$

$3^8 \equiv 72 \pmod{103}$

$3^{16} \equiv 34 \pmod{103}$

$3^{32} \equiv 23 \pmod{103}$

$3^{64} \equiv 14 \pmod{103}$

$102 =_2 1100110 \Rightarrow 102 = 64 + 32 + 4 + 2$

Tehát $3^{102} = 3^{64} \cdot 3^{32} \cdot 3^4 \cdot 3^2 = 14 \cdot 23 \cdot 81 \cdot 9 = 13 \cdot 81 \cdot 9 \equiv 23 \cdot 9 \equiv 207 \equiv 1$. A számolást megspórolhattuk volna, hiszen 103 prím, ezért $3^{102} \equiv 1 \pmod{103}$ rögtön látszik.

Ezek alapján elkészítettem a saját Fermat prímtesztemet. A programot C++ nyelvben írtam meg és a következők a lépései:

Kér egy pozitív egész számot, majd azt átváltja kettes számrendszerbe. Következő lépésben létrehoz egy 25 hosszú vektort, amit feltölt $2-102$ közötti véletlenszámokkal, ezt a C++ beépített ($rand()$) véletlenszám generátorával készíti el. Ezek után pedig a megadott számot és az alapokat rendre teszteli (1.2)-re, csak arra az esetre ügyelve, mikor az alap (véletlenül) pont a mi számunk. Mivel csak a prímeket vettem figyelembe, tehát kihasználva, hogy pontosan 2 osztójuk van, a program nem ellenőrzi minden alapra a relatív prímséget. Ha valamelyiknél (1.2) sérül, akkor megáll és kiírja, hogy „Biztosan összetett". Ha minden bázisra átmegy, akkor a „99,9999%, hogy prím" üzenettel megáll. Az az eset még fennállhat, amikor pl. egy univerzális álprím egyetlen valódi osztója és annak többesei sem alapok, ekkor kudarcot vallottunk.

A programot két tesztnek vetettem alá, az egyikben megvizsgáltam, hogy $2-50000$-ig milyen jól ismeri fel a prímeket, a másikban pedig, hogy az első 12 Carmichael-számot milyen pontossággal mondja összetettnek. Nyilván a kettő összefügg, de érdemes külön-külön megfigyelni. Mindkét esetet 5-ször futtattam. A tesztelések során az eljárás minden esetben hibátlanul működött, vagyis 50000-ig megtalálta az összes prímet a program. Gyorsabb számítógépek képesek 10^{10}-es vagy afölötti nagyságrendig is felismerni a prímeket. A próbák során láthatóvá vált, hogy az univerzális álprímek inkább elméleti akadályt jelentenek, a gyakorlatban úgy tűnik, hogy kis számokra kudarcot vallanak mint prímek. Persze ehhez az is kellett, hogy valamelyik prímtényező osztója legyen egy báziselemnek.

A tesztnek más változatai is léteznek, például gyengébb, de sokkal gyorsabb, ha csak egy alapra vizsgálódunk, de nyilván többször mond csődöt ez a változat. Ha ismerjük mondjuk az első 100-200 prímet, akkor ezek is szolgálhatnak bázisként, de ezek megkereséséhez is szükségünk van egy prímkereső algoritmusra. Ezért is választottam a már említett változatot egy pici módosítással persze, mellette szól, hogy, ha mégis kiszámítanám (a, n) értékét, ami nagyjából $\log(n)$ lépésben számítható, helyette kiszámítom $a^{n-1} \pmod{n}$-t, ami ugyancsak $\log(n)$ lépés. Tehát mindkét változat ugyanolyan gyors. Igazából (a, n) kiszámításával – amikor nem relatív prímek – találhatunk egy valódi osztóját n-nek, de ebben a fejezetben ezzel nem foglalkoztam.

A Fermat-féle tesztnél az álprímeket nem tudjuk teljes biztonsággal kiszűrni (a Carmichael-számokat egyáltalán nem). A következő prímteszt ezt a problémát küszöböli ki, amit egy erősebb „feltétel" alkalmazásával ér el.

1.2. Solovay-Strassen teszt

A Solovay-Strassen prímteszt Robert Martin Solovay és Volker Strassen matematikusok nevéhez fűződik. Ezt az eljárást, amely a Fermat-teszt egy továbbfejlesztett változatának tekinthető, 1974-ben publikálták. A módszer (hasonlóan az előbbihez) véletlenszámok segítségével redukálja annak az esélyét, hogy egy álprímet tévesen prímszámnak gondoljunk. A már említett „feltétel" egy speciális esete a következő:

1.2.1. Definíció. *Legyen $p > 2$ prím és $p \nmid a$ tetszőleges. Ekkor az*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & , \text{ ha } x^2 \equiv a \pmod{p} \text{ megoldható} \\ -1 & , \text{ ha } x^2 \equiv a \pmod{p} \text{ nem oldható meg} \end{cases}$$

számot a per b Legendre-szimbólumnak hívjuk.

1.2.2. Tétel. *Legyen $p > 2$ pozitív prímszám. Ekkor bármely a esetén fennáll az alábbi kongruencia:*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p} \tag{1.3}$$

Bizonyítás. Mivel p prím, ezért tetszőleges a esetén igaz rá (1.2), amiből következik az $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ kongruencia, ami ekvivalens $x^2 \equiv a \pmod{p}$ megoldhatóságával, ebből pedig következik, hogy $\left(\frac{a}{p}\right) = \pm 1$. Azaz a két oldal mindig kongruens.

Ezzel az állítást beláttuk. □

A Legendre-szimbólum általánosítása a Jacobi-szimbólum, ennek felhasználásával már tetszőleges $(a,b)=1$ számok esetén is értelmezhető az $\left(\frac{a}{b}\right)$ szimbólum.

1.2.3. Definíció. *Legyen $b>1$ egész szám és $b=p_1\cdot\ldots\cdot p_k$ prímek szorzata. Legyen $(a,b)=1$, ekkor $\left(\frac{a}{b}\right)=\left(\frac{a}{p_1}\right)\cdot\ldots\cdot\left(\frac{a}{p_k}\right)$, ahol $\left(\frac{a}{p_i}\right)$ a megfelelő Legendre-szimbólum. Az $\left(\frac{a}{b}\right)$ számot a per b Jacobi-szimbólumnak nevezzük.*

1.2.4. Tétel. *Legyen $n\geqslant 3$ páratlan szám. Ekkor az*

$$a^{\frac{n-1}{2}}\equiv\left(\frac{a}{n}\right)\pmod{n} \tag{1.4}$$

kongruenciára igazak a következők:
(i) Ha n prím, akkor tetszőleges a számra teljesül.
(ii) Ha n összetett, akkor egy n szerinti redukált maradékrendszer elemeinek legalább a felére nem teljesül.

Bizonyítás. Ha n prím, akkor az 1.2.2 tétel miatt készen vagyunk. Ezzel (i) kész. Ha n páratlan összetett szám, akkor először is azt kell belátni, hogy minden ilyen n-hez létezik olyan a szám, melyre $a^{\frac{n-1}{2}}\not\equiv\left(\frac{a}{n}\right)\pmod{n}$, nevezzük ezeket tanúnak, mivel az összetettséget tanúsítják, és cinkosnak vagy Euler-féle álprímnek azokat, melyekre teljesül a feltétel.
Két esetet vizsgálunk, amikor n négyzetmentes, és amikor nem.
Tegyük fel tehát, hogy $\exists\ p$ prím, hogy $p^2\mid n$. Legyenek az n prímosztói a $p=p_1,p_2,\ldots,p_k$ prímek. És legyen d primitív gyök $\bmod p^2$, ilyen van, hiszen p prím. Nézzük a következő szimultán kongruenciarendszert:

$$x\equiv d\pmod{p^2}\qquad\text{és}\qquad x\equiv -1\pmod{p_i}\quad(i=2,\ldots,k) \tag{1.5}$$

Mivel a modulusok relatív prímek, ezért $\bmod[p^2p_2\cdot\ldots\cdot p_k]$ kongruencia erejéig egyértelműen létezik megoldás, legyen ez u. Mivel $\forall\ i>1$-re $p_i\nmid u$, ezért $(u,n)=1$. Azt szeretnénk megmutatni, hogy u tanú. Tegyük fel tehát indirekt, hogy Euler-féle álprím, azaz, hogy

$$u^{\frac{n-1}{2}}\equiv\left(\frac{u}{n}\right)\pmod{n} \tag{1.6}$$

teljesül. Ha most (1.6)-ot négyzetre emeljük, akkor kapjuk, hogy

$$u^{n-1} \equiv 1 \pmod{n}.$$

Mivel p^2 osztója n-nek, ezért igaz az alábbi kongruencia is:

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

(1.5) miatt $u \equiv d \pmod{p^2}$, és mivel d primitív gyök $\mod p^2$, ezért $\sigma(d) = \varphi(p^2) = p(p-1)$. Azt kaptuk tehát, hogy $p(p-1) \mid n-1$, amiből következik a $p \mid n-1$ oszthatóság is. Vagyis $p \mid n-1$ és $p \mid n$, ami lehetetlen, tehát u tanú.
Most áttérünk a négyzetmentes esetre. Itt külön fogjuk vizsgálni azt az esetet, amikor minden $(a,n) = 1$ alapra fennáll az

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n} \tag{1.7}$$

kongruencia, és azt, amikor van olyan $(b,n) = 1$, melyre nem.
Kezdjük azzal, amikor minden $(a,n) = 1$ esetén (1.7) igaz. Ekkor legyenek n prímosztói rendre a $p_1, ..., p_k$ prímek és legyen $g^{\frac{p_1-1}{2}} \equiv -1 \pmod{p_1}$, azaz $\left(\frac{g}{p_1}\right) = -1$ (ilyen g létezik, mert p_1 prím), ekkor tekintsük a következő szimultán kongruenciarendszert:

$$x \equiv g \pmod{p_1} \quad \text{és} \quad x \equiv 1 \pmod{p_i} \quad (i = 2, ..., k). \tag{1.8}$$

Legyen ennek v egy megoldása. Ekkor $(v,n) = 1$, tehát (1.7) igaz rá. Behelyettesítve v-t (1.4)-be azt kapjuk, hogy:

$$v^{\frac{n-1}{2}} \equiv \left(\frac{v}{n}\right) = \left(\frac{v}{p_1}\right) \cdot ... \cdot \left(\frac{v}{p_k}\right) \equiv \left(\frac{g}{p_1}\right) \cdot \left(\frac{1}{p_2}\right) \cdot ... \cdot \left(\frac{1}{p_k}\right) = -1 \not\equiv 1 \pmod{n}$$

Tehát v tanú.
Térjünk át arra az esetre, amikor létezik egy $(b,n) = 1$ alap, hogy $b^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}$. Nyilván létezik olyan prímosztója n-nek pl. p_1, hogy $b^{\frac{n-1}{2}} \not\equiv 1 \pmod{p_1}$. Tekintsük a következő szimultán kongruenciarendszert:

$$x \equiv b \pmod{p_1} \quad \text{és} \quad x \equiv 1 \pmod{p_i} \quad (i = 2, ..., k) \tag{1.9}$$

Legyen ennek egy megoldása w. Ekkor w-re igazak a következő kongruenciák:

$$w^{\frac{n-1}{2}} \not\equiv 1 \pmod{p_1} \Longrightarrow w^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}$$

Továbbá igaz az alábbi következtetés is:

$$w^{\frac{n-1}{2}} \equiv 1 \not\equiv -1 \pmod{p_i} \Longrightarrow w^{\frac{n-1}{2}} \not\equiv -1 \pmod{n} \qquad (i = 2, ..., k)$$

Összesítve az eredményt azt kaptuk, hogy $w^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$, de nyilván $\left(\frac{w}{n}\right) = \pm 1$. Tehát w tanú.
Ezzel megmutattuk, hogy minden összetett páratlan számhoz létezik tanú.
Már csak azt kell belátni, hogy egy $\bmod n$ szerinti redukált maradékrendszer legalább a fele az. Ez pedig igaz, hiszen legyen $(z, n) = 1$ egy tanú és $(c, n) = 1$ pedig egy cinkos. Ekkor persze $(cz, n) = 1$ is igaz. Megmutatjuk, hogy cz is tanú. Tegyük fel indirekt, hogy mégis cinkos. Ekkor a következőt kapjuk:

$$z^{\frac{n-1}{2}} \equiv \left(\frac{c}{n}\right) \cdot z^{\frac{n-1}{2}} \equiv c^{\frac{n-1}{2}} \cdot z^{\frac{n-1}{2}} \equiv (cz)^{\frac{n-1}{2}} \equiv \left(\frac{cz}{n}\right) = \left(\frac{c}{n}\right) \cdot \left(\frac{z}{n}\right) \Longrightarrow z^{\frac{n-1}{2}} \equiv \left(\frac{z}{n}\right)$$

Ez pedig ellentmond annak, hogy z tanú. Már csak azt kell, megmutatni, hogy két inkongruens cinkosból inkongruens tanút kapunk. Ez nyilván így van, hiszen, ha $c_1 \not\equiv c_2 \pmod{n}$, akkor $(z, n) = 1$ miatt $c_1 z \not\equiv c_2 z \pmod{n}$.
Ezzel beláttuk, hogy akármennyi inkongruens cinkosunk is van egy $\bmod n$ szerinti redukált maradékrendszerben, legalább annyi tanú is létezik, más szóval egy redukált maradékrendszer elemeinek legalább a fele tanú. □

1.2.5. Megjegyzés. A Solovay-Strassen teszt „feltételének" négyzetre emeléséből következik (1.2), ezért jogos az „erősebb" jelző. Emiatt igaz, hogy ha egy számot a Fermat teszt összetettnek ítél, akkor a Solovay-Strassen teszt „méginkább" annak mond. Tehát a Solovay-Strassen hatékonyabb.

A megjegyzésből kiderült, hogy ebben az esetben is léteznek álprímek, viszont most „sűrűbb szitán" kell, hogy átmenjenek, ezért külön definíciót érdemel ez az eset.

1.2.6. Definíció. *Ha az n összetett számra és az $(a, n) = 1$ alapra teljesül az $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ kongruencia, akkor az n számot a a alapú Euler-féle álprímnek nevezzük.*

1.2.7. Példa. 29-es alapú Euler-féle álprím a 15.
Ugyanis $15 = 3 \cdot 5$, és $29^7 \equiv (-1)^7 \equiv -1 \pmod{15}$, másfelől $\left(\frac{29}{15}\right) = \left(\frac{-1}{15}\right) = -1$.

Nyilván igaz, hogy, ha n Euler-féle álprím az a alapra, akkor „közönséges" a alapú álprím is. Viszont az univerzális álprímeknek nem létezik ilyesfajta megfelelője, hiszen az 1.2.3 tétel szerint az összetett számok egy idő után lelepleződnek. Tehát ez is mutatja, hogy a Solovay-Strassen teszt jóval hatékonyabb.
Most a Jacobi-szimbólum kiszámításához szükséges lépésszámot fogjuk tárgyalni.

1.2.8. Állítás. *A Jacobi-szimbólum kiszámításához elegendő $c \cdot \log n$ lépés.*

Bizonyítás. Adott $(a, n) = 1$ számok Jacobi-szimbólumát szeretnénk kiszámítani. A legnagyobb kettőhatvány leválasztásával és a kvadratikus reciprocitási tétel, valamint maradékos osztások alkalmazásával a $\left(\frac{-1}{p}\right)$ és/vagy $\left(\frac{2}{q}\right)$ Jacobi-szimbólumokhoz lehet eljutni, ezek pedig egy maradék kiszámításával megkaphatók. Így (majdnem) minden lépésben feleződik a számláló, tehát $c \cdot \log_2 n = c \cdot \frac{\log n}{\log 2}$ (ahol $c > 0$ konstans) lépés elegendő. □

1.2.9. Példa. Számítsuk ki $\left(\frac{85}{229}\right)$ értékét!
$\left(\frac{85}{229}\right) = \left(\frac{229}{85}\right) = \left(\frac{59}{85}\right) = \left(\frac{85}{59}\right) = \left(\frac{26}{59}\right) = \left(\frac{2}{59}\right)\left(\frac{13}{59}\right) = -\left(\frac{13}{59}\right) = -\left(\frac{59}{13}\right) = -\left(\frac{7}{13}\right) = \left(\frac{13}{7}\right) = \left(\frac{-1}{7}\right) = -1.$

Ezek alapján a Solovay-Strassen prímteszt számítógépen hasonlóan ($2 \log n$ lépésben) kivitelezhető, mint az elődje. Ugyanis a következők lehetnek a lépései:

- Elkészítjük a véletlenszámokból álló listánkat, ezek képezik az alapokat
- Mindegyik alapra kiszámítjuk $a^{\frac{n-1}{2}} \pmod{n}$ és $\left(\frac{a}{n}\right)$ értékeket
- Ha valamelyik alapra a kongruencia nem teljesül, akkor n biztosan összetett, ha (1.4) mindegyikre igaz, akkor a jelöltünk nagy valószínűséggel prím.

A most következő prímteszt az eddigieknél is hatékonyabban leplezi le az összetett számokat.

1.3. Miller-Rabin teszt

A Miller-Rabin prímteszt alapja a kis Fermat-tétel, pontosabban az, hogy egy p prím és egy $p \nmid a$ pozitív egész által alkotott $a^{p-1}, a^{\frac{p-1}{2}}, a^{\frac{p-1}{4}}, ... \pmod p$ sorozat minden esetben 1-gyel kezdődik, és vagy végig 1-esekből áll, vagy az első nem egyes az éppen -1. A gondolat alapja az, hogy egy prím szerinti redukált maradékrendszerben a legfeljebb másodrendű elemek csak az $1, -1$. Gary Miller és Michael Rabin a következő tesztet találták meg.

1.3.1. Tétel. (Miller-Rabin) *Adott $n > 2$ páratlan egész, és legyen $n - 1 = 2^k r$, ahol r páratlan. Tekintsük a következő sorozatot:*

$$a^r, a^{2r}, a^{4r}, ..., a^{2^{k-1}r} \tag{1.10}$$

Nevezzük ezt jó sorozatnak, ha $\bmod n$ van köztük -1, vagy, ha $\bmod n$ mindegyik 1-es. Ekkor n függvényében (1.10)-re a következők igazak:
(i) Ha n prím, akkor tetszőleges $n \nmid a$ esetén jó sorozatot alkot.
(ii) Ha n összetett, akkor egy n szerinti redukált maradékrendszer kevesebb, mint a felére alkot jó sorozatot.

Bizonyítás. Ha n prím, akkor bármely $(a, n) = 1$ esetén $a^{n-1} \equiv 1 \pmod n \Rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \pmod n$, ugyanis egy p prím számra az $x^2 \equiv 1 \pmod p$ kongruenciának a megoldásai csak az 1 és -1, tehát végig vagy 1-esből áll a sorozat, vagy van -1 benne. Ezzel az (i) rész készen van.
A tétel második feléhez, hasonlóan az 1.2.4 tételhez, nevezzük tanúnak azokat az a-kat, melyekre (1.10) nem alkot jó sorozatot és cinkosnak, melyekre igen. Most is azt fogjuk belátni, hogy minden n-hez létezik tanú.
Legyen $p^2 \mid n$, és q primitív gyök p^2 szerint, és legyenek n prímosztói a $p = p_1, ..., p_s$ prímek. A következőképpen konstruálhatunk tanút, legyen v az alábbi szimultán kongruenciarendszer egy megoldása:

$$x \equiv q \pmod{p^2} \quad \text{és} \quad x \equiv 2 \pmod{p_i} \quad (i = 2, ..., s).$$

Az $x \equiv 2 \pmod{p_i}$ kongruenciák arra kellenek, hogy biztosítsák $(v, n) = 1$-et. Tegyük fel indirekt, hogy v cinkos, azaz, hogy (1.10) jó sorozat. Ekkor az utolsó tagra igaz, hogy $v^{\frac{n-1}{2}} \equiv \pm 1 \pmod n$, ebből következik, hogy $v^{n-1} \equiv 1 \pmod n$, ez elmondható $p^2 \mid n$-re mint modulusra is, vagyis $v^{n-1} \equiv 1 \pmod{p^2}$. Viszont $v \equiv q$

$(\text{mod } p^2)$, tehát $\sigma(q) = p(p-1) \mid n-1$, vagyis $p \mid n-1$, és $p \mid n$, ez pedig lehetetlen, azaz v tanú.

Most tegyük fel, hogy n összetett, négyzetmentes és $n = p_1 p_2 \cdot ... \cdot p_s$. Olyan $(a, n) = 1$ számot kell találnunk, melyre a sorozat lehető legtöbb tagja nem kongruens ± 1-gyel $(\text{mod } n)$. Olyan a létezik, melyre $a^{2^j r} \not\equiv 1 \pmod{n}$, ahol $0 \leq j \leq k-1$, például $a = -1, j = 0$ ilyen. Legyen j a legnagyobb ilyen tulajdonságú (amelyhez van ilyen a). Nézzük a következő szimultán kongruenciarendszert:

$$x \equiv a \pmod{p_s} \quad \text{és} \quad x \equiv 1 \pmod{p_i} \quad (i = 1, ..., s-1)$$

Ennek legyen egy megoldása w. Ekkor w tanú, ugyanis

$$w^{2^j r} \equiv a^{2^j r} \not\equiv 1 \pmod{p_s} \Rightarrow w^{2^j r} \not\equiv 1 \pmod{n}$$

$$w^{2^j r} \equiv 1 \not\equiv -1 \pmod{p_i} \Rightarrow w^{2^j r} \equiv 1 \not\equiv -1 \pmod{n}$$

Tehát $w^{2^j r} \not\equiv \pm 1 \pmod{n}$, viszont j volt a maximális olyan, melyre $w^{2^j r} \not\equiv 1 \pmod{n}$, ezért a $w^{2^{j+1} r} \equiv 1 \pmod{n}$ kongruenciának igaznak kell lennie. Azt kaptuk, hogy $w^r \not\equiv \pm 1, ..., w^{2^j r} \not\equiv \pm 1$, de $w^{2^{j+1} r} \equiv 1 \pmod{n}, ..., w^{n-1} \equiv 1 \pmod{n}$, és ebben nincs -1, és nem végig 1. Azaz w tanúsítja n összetettségét.

Hasonlóan az 1.2.4 tétel és az 1.1.6 állítás bizonyításában látottakhoz belátható, hogy tetszőleges sok páronként inkongruens cinkost végigszorozva w-vel inkongruens tanúkat kapunk, vagyis egy redukált maradékrendszer legalább a fele tanú. $\square$

A Miller-Rabin prímteszt egy lehetséges változata:

Az n számról szeretnénk eldönteni, hogy prím-e. Veszünk k db különböző véletlenszámot, ezek lesznek a b_i alapok, és $n-1$-et előállítjuk $2^s r$ alakban, ahol r páratlan. Kiszámítjuk $b_1^r \pmod{n}$ értéket, ha ez ± 1, akkor a sorozatunk „jó", tehát áttérünk a b_2 bázisra. Most $b_2^r \pmod{n}$ értéket vizsgáljuk, ha mondjuk ez nem ± 1, akkor négyzetre emeljük és $\bmod n$ számoljuk az újabb (legkisebb abszolútértékű) maradékot, ezt addig tesszük, amíg -1-et nem kapunk valahol, ha ez nem fordul elő, akkor n biztosan összetett, ha az összes bázisra n jó sorozatot alkot, akkor több, mint $\frac{1}{2^k}$ valószínűséggel prím. A sorozat tagjainak kiszámítása a Fermat-féle módszernél említett ismételt négyzetre emelésekkel $\log n$ db művelettel végezhető.

A fenti bizonyításban is tulajdonképpen ilyen w alapot „gyártottunk", amelyre $w^{2^{j+1}} \equiv 1 \pmod{n}$ igaz volt, de a sorozat többi tagjára $w^{2^j} \not\equiv \pm 1 \pmod{n}$ $(0 \leq j \leq k-1)$

inkongruenciák teljesültek.
Sajnos ez a teszt sem nyújt 100%-os biztonságot, ugyanis ebben az esetben is léteznek álprímek, viszont univerzális álprímek itt sem fordulnak elő.

1.3.2. Definíció. *Legyen n páratlan összetett szám, és $n-1=2^k r$. Ha egy $(a,n)=1$ számra az n szám a fenti értelemben jó sorozatot alkot, akkor n-et a a alapú erős álprímnek nevezzük.*

A következő példában láthatóvá válik, hogy ha egy n szám $\frac{n-1}{2}$-dik hatványa kongruens -1-gyel $\mod n$, akkor erős álprím.

1.3.3. Példa. A 15 erős álprím a 29-hez, mint alaphoz. A $15(=2\cdot 7+1)$ nem prím, és már láttuk, hogy Euler-féle álprím a 29-hez, azaz $29^7 \equiv \left(\frac{29}{15}\right) = -1 \pmod{15}$, tehát a $29^7, 29^{14} \pmod{15}$ jó sorozatot alkotnak.

Most azt mutatjuk meg, hogy a fenti példa miért is volt jó.

1.3.4. Állítás. *Ha $n \equiv 3 \pmod 4$, akkor n pontosan akkor erős álprím az a alapra, ha egyben Euler-féle álprím is.*

Bizonyítás. Ha n erős álprím, akkor $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod n$ teljesül, $n \equiv 3 \pmod 4$ miatt pedig $\left(\frac{\pm 1}{n}\right) = \pm 1$, így $\left(\frac{a}{n}\right)^{\frac{n-1}{2}} = \left(\frac{a^{\frac{n-1}{2}}}{n}\right) = \pm 1 \equiv a^{\frac{n-1}{2}} \pmod n$. Mivel $n-1$ kettőnek csak az első hatványával osztható, ezért csak az $a^{\frac{n-1}{2}}$ tag fordul elő a sorozatban, és, ha n Euler-féle álprím, akkor $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod n$ igaz. $\square$

Általában a két fajta „álprímség" nem ekvivalens, vagyis abból, hogy n Euler-féle álprím egy $(a,n)=1$ alapra nem következik, hogy erős álprím is.

1.3.5. Példa. Az $1729 = 7\cdot 13\cdot 19$ Euler-féle álprím az 5 alapra, de nem erős, ugyanis $(5,1729)=1$-re $5^{27} \equiv 1217 \pmod{1729}$, $5^{54} \equiv 1065 \pmod{1729}$, $5^{108} \equiv 1 \pmod{1729}$, ..., $5^{864} \equiv 1 \equiv \left(\frac{5}{1729}\right) = \left(\frac{5}{7}\right)\left(\frac{5}{13}\right)\left(\frac{5}{19}\right) = \left(\frac{7}{5}\right)\left(\frac{13}{5}\right)\left(\frac{19}{5}\right) = \left(\frac{2}{5}\right)^2\left(\frac{-1}{5}\right)^2$. Tehát a Solovay-Strassen-teszten átmegy, viszont a Miller-Rabin-tesztnél nem alkot jó sorozatot.

Most belátjuk, hogy a Miller-Rabin prímteszt hatékonyabban leplezi le az összetett számokat a Solovay-Strassen tesztnél.

1.3.6. Állítás. *A Miller-Rabin teszt hatékonyabb, mint a Solovay-Strassen teszt, azaz, ha az n szám a alapú erős álprím, akkor a alapú Euler-féle álprím is.*

Bizonyítás. Legyen $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, és $n-1 = 2^s r$, ahol r páratlan, és tegyük fel, hogy n erős álprím az a alapra, azaz $a^r, a^{2r}, ..., a^{2^{s-1}r} = a^{\frac{n-1}{2}}$ jó sorozatot alkot. Azt kell megmutatni, hogy ekkor $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)$. Két eset lehetséges:

1. eset:
$a^r \equiv 1 \pmod{n}$, most $\left(\frac{a}{n}\right) = 1$ kell nekünk. De $1 = \left(\frac{1}{n}\right) = \left(\frac{a^r}{n}\right) = \left(\frac{a}{n}\right)^r = \left(\frac{a}{n}\right)$, hiszen r páratlan.

2. eset:
Ebben az esetben létezik -1-gyel kongruens tag a sorozatban. Két alesetet vizsgálunk. Elsőként nézzük azt, amikor van olyan $0 \leq j < s-1$, hogy:

$$a^{2^j} r \equiv -1 \pmod{n} \quad \text{és} \quad a^{2^{j+1}r} \equiv 1 \pmod{n} \tag{1.11}$$

Tehát $a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$, ezért a cél $\left(\frac{a}{n}\right) = 1$ megmutatása. Az (1.11) kongruenciák igazak minden p_i prímosztóra is, ezért $\sigma_{p_i}(a) \nmid a^{2^j} r$, de $\sigma_{p_i}(a) \mid a^{2^{j+1}} r$, ezért $\sigma_{p_i}(a) = 2^{j+1} r_i$, ahol $r_i \mid r$. Másrészt p_i prím volta és a rend definíciója miatt $a^{2^j} r_i \equiv -1 \pmod{p_i}$ lehet csak. A kis Fermat tétel miatt pedig $\sigma_{p_i}(a) \mid p_i - 1$, tehát létezik t_i, melyre

$$p_i - 1 = 2^{j+1} r_i t_i$$

Ezt felhasználva adódik, hogy

$$\left(\frac{a}{p_i}\right) \equiv a^{\frac{p_i-1}{2}} = a^{2^j r_i t_i} \equiv (-1)^{t_i} \pmod{p_i}$$

Ebből következik, hogy

$$\left(\frac{a}{n}\right) = \left(\frac{a}{\prod_{i=1}^{k} p_i^{\alpha_i}}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{k} (-1)^{\alpha_i t_i} = (-1)^{\sum_{i=1}^{k} \alpha_i t_i}$$

Tehát $\sum_{i=1}^{k} \alpha_i t_i$-ról kell belátni, hogy páros.

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{k} (1 + 2^{j+1} r_i t_i)^{\alpha_i} = \prod_{i=1}^{k} (1 + \alpha_i 2^{j+1} r_i t_i + \binom{\alpha_i}{2} 2^{2j+2} r_i^2 t_i^2 + ...$$

$$... + \binom{\alpha_i}{\alpha_i - 1} 2^{(j+1)(\alpha_i - 1)} r_i^{\alpha_i - 1} t_i^{\alpha_i - 1} + 2^{(j+1)\alpha_i} r_i^{\alpha_i} t_i^{\alpha_i}) = 1 + 2^{j+1} \sum_{i=1}^{k} \alpha_i r_i t_i + 2^{j+2} K$$

Mivel $n-1=2^s r$, ezért azt kapjuk, hogy

$$2^{j+1}\sum_{i=1}^{k}\alpha_i r_i t_i = 2^s r - 2^{j+2}K$$

2^{j+1}-vel való egyszerűsítés után $\sum_{i=1}^{k}\alpha_i r_i t_i = 2^{s-j-1}r - 2K$ adódik, azaz $\sum_{i=1}^{k}\alpha_i r_i t_i = 2l$ alakú, mivel minden r_i páratlan, ezért $\sum_{i=1}^{k}\alpha_i t_i$ is páros kell, hogy legyen, azaz $\left(\frac{a}{n}\right) = 1$.

A másik aleset – vagyis mikor $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ teljesül – is hasonlóan belátható. Ekkor $j = s-1$-re nézve a $\sum_{i=1}^{k}\alpha_i r_i t_i = 2^{s-j-1}r - 2K$ egyenletet, kapjuk, hogy $\sum_{i=1}^{k}\alpha_i r_i t_i = 2^0 r - 2K = r - 2K$, mivel r és minden r_i is páratlan, ezért $\sum_{i=1}^{k}\alpha_i t_i$ is az, így megkaptuk, hogy $\left(\frac{a}{n}\right) = -1$. $\square$

Az ebben a fejezetben említett tesztek által prímnek vélt számokat egy egyszerű eljárással „leellenőrizhetjük”, azaz megvizsgálhatjuk, hogy valóban prím-e a számunk. A módszer lényege az, hogy az n pontosan akkor prím, ha létezik olyan $(a,n)=1$, amelyre $\sigma_n(a) = n-1$ (vagyis a primitív gyök). Tehát kiszámítjuk minden $p_i \mid n-1$ prímosztóra és az a alapra az $a^{\frac{n-1}{p_i}} \pmod{n}$ értéket, és, ha ezek között nem fordul elő 1-es, akkor n prím. Ennek a módszernek a hátránya az, hogy nagy számoknál a prímosztók megtalálása reménytelen feladatnak ígérkezik.

A most következő fejezetben ezt a problémát fogom körbejárni, és különböző módszereket mutatok be a prímtényezőkre bontáshoz.

2. fejezet

Prímfaktorizáció

A prímfaktorizációs módszerek olyan számelméleti eljárások, amelyek egy szám prímtényezős felbontását adják meg. Legtöbb esetben célszerű elsőként elvégezni egy prímtesztet, hogy a felesleges számolást megspóroljuk. Nagyon nagy számok esetén még így is szinte lehetetlen megállapítani a prímfaktorokat, ha mondjuk egy 30000 jegyű számon szeretnénk egy ilyet elvégezni, akkor a jelenlegi leggyorsabb számítógépnek – ami másodpercenként több millió műveletet végez – is több időbe tellene kiszámítania, mint az ősrobbanástól eddig a pillanatig eltelt összes másodperc. Ennek tükrében a legtöbb ilyen algoritmust a nagy számok felbontására alkották meg, elsőként említem a legegyszerűbb prímfaktorizációs módszert, ami jól mutatja, hogy „nyers erővel" egy örökkévalóságig tartana felbontani egy nagy számot.

2.1. Próbaosztásos módszer

Ennek a módszernek a lényege, hogy veszünk egy számsorozatot $[\sqrt{n}]+1$-ig, legjobb lenne a csak prímeket tartalmazó sorozat, de ez nem kényelmes, inkább vegyük az $a_1 = 2, a_2 = 3, a_3 = 5, a_4 = 7, ..., a_i, a_i + 2, ..., [\sqrt{n}] + 1$ sorozatot, és ennek a tagjai mentén addig osztjuk n-et, amíg osztót nem találunk, majd a hányadossal folytatjuk a számolást. Készíthetünk egy prímtáblázatot is, vagyis csak a prímekből álló sorozatot is nézhetjük, de ez nem mindig áll a rendelkezésünkre.
Nézzük meg, hogyan is néz ki ez az algoritmus!

2.1.1. Algoritmus. Az algoritmus egy N számnak a prímosztóit keresi meg.
1. lépés: Legyenek $n := N$, $a_1, ..., a_k = [\sqrt{N}] + 1$ a próbaosztók és $p_1, ...$

a prímosztók.

2. lépés: n-et a sorozat tagjaival addig osztjuk maradékosan ($n = a_i q + r$), amíg a maradék nem nulla vagy véget nem ér a sorozat.

3. lépés: Ha a maradék nulla, akkor osztót találtunk, $n := n/q$, $p_j = a_i$ (a_i prím, hiszen a sorozatunk ezt garantálja).

4. lépés: Ha a maradék nem nulla és $q > a_i$, akkor még nem értük el egy $\sqrt{n}$-nél nagyobb prímosztóját n-nek, tehát újra osztunk (2. lépés). Ha $q \leq a_i$, akkor n prím, mert nem találtunk osztót.

Ha marad a sorozatban összetett szám, akkor is helyes eredményt kapunk, hiszen minden páratlan számot tartalmaz, ezért ennek az összetettnek a prímtényezőit is, melyek előrébb szerepelnek, azaz, ha ez a szám osztója N-nek, akkor ez már előbb kiderül.
Nézzük az alábbi számpéldát a próbaosztások módszerére:

2.1.2. Példa. Bontsuk tényezőkre az $N = 349625(=: n)$ számot!
Sorban haladva kapjuk, hogy $5 \mid 349625$, tehát $n := \frac{N}{5} = 69925$. Ekkor elegendő onnan folytatnunk, ahol abbahagytuk, vagyis $a_3 = 5$-től. Rögtön látszik, hogy $5 \mid 69925$, ezért $n := 13985$, ami szintén osztható 5-tel, tehát $n := \frac{13985}{5} = 2797$, ekkor $p_1 = p_2 = p_3 = 5$. Sorban haladva a_3-tól egyetlen osztót sem találunk, de azt kapjuk, hogy $a_{27} = 53$-ra $2797 = 53 \cdot 52 + 41$ (ami nem meglepő, ugyanis $[\sqrt{2797}] = 53$), vagyis $52 \leq 53$, ezért $p_4 = 53$. Tehát $349625 = 5^3 \cdot 2797$. Ebben a példában 28 osztást végeztünk, nézzünk egy másik példát.

2.1.3. Példa. Legyen $N = 102043(=: n)$ (prím).
Mivel N prím, ezért a sorozatban egyetlen osztóra sem lelünk, de $[\sqrt{102043}]+1 = 320$ miatt $a_{161} = 321$-ig kell elmennünk, ezzel 161 osztást végzünk el (ami papíron nem kevés, már a 28 sem az), amikor is kapjuk, hogy $102043 = 321 \cdot 317 + 286$, és $317 \leq 321$ miatt pedig biztosak lehetünk benne, hogy N prím.

Ezekben a példákban láthattuk, hogy kézzel elég sok lépést kell végrehajtani már „viszonylag” kis számokon is. Nyilván a számítógépek körében ezek a számítások pillanatok alatt lefutnak, de ha egy nagyon nagy szám négyzetét nézzük, akkor ez óriási időt vesz igénybe. Az eljárás két kimenettel érhet véget, vagy megtalálja az összes prímosztót, vagy a felbontani kívánt szám prím. Ezért is igaz, hogy a lépésszám

$\max(p_{j-1}, \sqrt{p_j})$-vel arányos, ahol j a legnagyobb prímosztó indexét jelöli, tehát kis számoknál optimális. A sebességet úgy növelhetjük, hogy a prímek többeseit szisztematikusan kivesszük a sorozatból (pl. 3-mal, 5-tel osztható számokat, és így tovább). A következő eljárás már sokkal nagyobb sikerrel bontja prímtényezőkre a nagy számokat.

2.2. Monte Carlo módszer

J. M. Pollard 1975-ös módszere azon a tényen alapul, hogy a $\bmod n$ vett maradékok ciklizálnak, hiszen $\mathbb{Z}_n$ véges, így egy idő után olyan maradékot kapunk, ami már egyszer előfordult. A véletlenszámoknak most is nagy jelentőségük van, de ebben az esetben más a szerepük, arra kellenek, hogy a keresett osztók nagyobb valószínűséggel essenek bele egy n szerinti ciklusba. Ezeket az (ál)véletlenszámokat egy f másodfokú rekurzió fogja nekünk biztosítani (pl. $f(x) = x^2 + 1$), azaz $x_{i+1} = f(x_i)$. Ekkor kiszámítjuk az $(x_i - x_j, n)$ $(i > j)$ értékeket és abban bízunk, hogy x_i és x_j az n-nek egy p prímosztója szerint ugyanabban a maradékosztályban vannak, de n szerint nem, ezért, ha $(x_i - x_j, n) > 1$, akkor egy valódi osztót találtunk. Ezért nem vezet eredményhez, ha $f(x) = ax + b$ alakú függvényt adunk meg, ugyanis, ha $x_i \equiv x_j \pmod{n} \Rightarrow f(x_i) \equiv f(x_j) \pmod{n} \Rightarrow f(x_i) \equiv f(x_j) \pmod{p}$, így nem kaphatunk nem triviális osztót.
A módszer igazából nem számítja ki minden (x_i, x_j) párra az $(x_i - x_j, n)$ értéket, hiszen ekkor nagyon sokat is kellene számolni, illetve nehezen is követhető. A trükk az, hogy a sorozatban a 2^k-dik elemmel számítjük ki a legnagyobb közös osztót, amíg el nem érjük a 2^{k+1}-dik tagot, így megspórolva sok számolást, másrészt exponenciálisan növekszik a x_i-k közti távolság, így nagyobb eséllyel hamarabb elérjük egy $p \mid n$ szerinti periódus hosszát. Vagyis a helyzet a következő.

Legyen $f : \mathbb{Z}_n \to \mathbb{Z}_n$ és x_0 tetszőleges kezdőérték. Jelölje k a kettes számrendszerbeli számok számjegyeinek a számát, ekkor $2^k - 1$ a legnagyobb k jegyű kettes számrendszerbeli szám ($k = 0$ esetén x_0-t értünk).

$$
\begin{aligned}
&x_0, \ (k = 0) \\
&x_1 = f(x_0) \Rightarrow (x_1 - x_0, n), \ (k = 1) \\
&x_2 = f(x_1) \Rightarrow (x_2 - x_1, n), \ (k = 2) \\
&x_3 = f(x_2) \Rightarrow (x_3 - x_1, n), \ (k = 2)
\end{aligned}
$$

$$
\begin{aligned}
x_4 = f(x_3) &\Rightarrow (x_4 - x_3, n),\ (k = 3)\\
x_5 = f(x_4) &\Rightarrow (x_5 - x_3, n),\ (k = 3)\\
x_6 = f(x_5) &\Rightarrow (x_6 - x_3, n),\ (k = 3)\\
x_7 = f(x_6) &\Rightarrow (x_7 - x_3, n),\ (k = 3)\\
x_8 = f(x_7) &\Rightarrow (x_8 - x_7, n),\ (k = 4)\\
&\vdots\\
x_i = f(x_{i-1}) &\Rightarrow (x_i - x_{2^k-1}, n),\ i \geq 2^k
\end{aligned}
$$

Így egy idő után belefutunk egy olyan esetbe, ahol a legnagyobb közös osztó nagyobb, mint egy.
Ezek alapján a Monte Carlo módszer lépései a következők.

2.2.1. Algoritmus. Monte Carlo módszer

0. lépés: Prímteszt $N(=: n)$-re, ha prím, akkor megállunk.

1. lépés: A fenti módon kiszámítjuk a legnagyobb közös osztót, a sorozat tagjait pedig $\bmod n$ számoljuk.

2. lépés: Ha a legnagyobb közös osztó 1 és n közé esik, akkor elvégzünk rá egy prímtesztet, ha n-nel egyenlő, akkor megállunk, ha 1-gyel, akkor kiszámítjuk a következő lnko-t.

3. lépés: Ha az osztó prím, akkor $p_t = (x_i - x_{2^k-1}, n)$ és $n := n/p_t$, ha nem, akkor valószínűleg kudarcot vallottunk, azaz ezzel a módszerrel nem tudjuk felbontani (de később külön elvégezhetjük erre az osztóra az algoritmust más paraméterekkel), majd tovább lépünk a sorozatban.

2.2.2. Példa. Bontsuk prímtényezőkre $N = 34203$-at, $f(x) = x^2 + 1$ és $x_0 = 1$ mellett!

$$
\begin{aligned}
&x_1 = f(x_0) = 2 \Rightarrow (2 - 1, 34203) = 1\\
&x_2 = f(x_1) = 5 \Rightarrow (5 - 2, 34203) = 3 \text{ (prím)}\\
&\Rightarrow n := \tfrac{34203}{3} = 11401,\ (5 - 2, 11401) = 1\\
&x_3 = f(x_2) = 26 \Rightarrow (26 - 2, 11401) = 1\\
&x_4 = f(x_3) = 677 \Rightarrow (677 - 26, 11401) = 1\\
&x_5 = f(x_4) = 458330 \equiv 2290 \pmod{11401} \Rightarrow (2290 - 26, 11401) = 1\\
&x_6 = f(x_5) \equiv 11042 \pmod{11401} \Rightarrow (11042 - 26, 11401) = 1\\
&x_7 = f(x_6) \equiv 3471 \pmod{11401} \Rightarrow (3471 - 26, 11401) = 13 \text{ (prím)}
\end{aligned}
$$

$\Rightarrow n := \frac{11401}{13} = 877$ (prím)

Tehát $34203 = 3 \cdot 13 \cdot 877$.

2.3. Fermat módszere

Fermat módszerének lényege, hogy egy $N = rs$ $(r \leq s)$ összetett páratlan számra léteznek $a \neq b \in [0, ..., N]$ egészek, hogy $N = a^2 - b^2 = (a+b)(a-b)$, így nyilván $a = \frac{r+s}{2}$, $b = \frac{r-s}{2}$ jó lesz. Az algoritmus akkor a leghatásosabb, ha r és s is közel vannak $\sqrt{N}$-hez, emiatt a^2 „nagy" – vagyis $\sqrt{N}$-hez közeli – és b^2 „kicsi" lesz. Tehát a következő egyenletrendszer megoldásával kapjuk a Fermat-féle felbontást.

$$a^2 - N = b^2, \qquad 0 \leq b < a \leq N$$

Ha találtunk egy a, b megoldást, akkor $r = a + b$ és $s = a - b$ összefüggések alapján megkapjuk az osztópárokat is.

A következő algoritmus abból indul ki, hogy r és s is $\sqrt{N}$-hez közeli értékek, konkrétan az $r = \lfloor \sqrt{N} \rfloor = s$ feltételből. Feltehető, hogy N páratlan, hiszen ellenkező esetben 2 hatványok leválasztásával páratlant kapunk. Az algoritmus az $r + s + 1 = 2a + 1 = 2\lfloor \sqrt{N} \rfloor + 1 =: a'$ és $r - s + 1 = 2b + 1 = 1 =: b'$ értékekkel dolgozik és addig növeli, illetve csökkenti ezeket, amíg $N = \frac{a'-b'}{2} \cdot \frac{a'+b'-2}{2}$ nem teljesül.

2.3.1. Algoritmus. Egy lehetséges eljárás

1. lépés: Legyenek a', b' és m segédváltozók. A kezdeti feltétel és a paritás szempontjából legyen $a' = 2\lfloor \sqrt{N} \rfloor + 1$, $b' = 1$, $m = \lfloor \sqrt{N} \rfloor^2 - N$. $|m| < a'$ és $b' < a'$ mindig igazak, ezek garantálják, az eljárás véges voltát.
2. lépés: Vizsgáljuk a maradék előjelét, vagyis, ha $m > 0$, akkor m-et csökkentjük b'-vel és b'-t növeljük 2-vel, hogy a paritás ne változzon, ha $m < 0$, akkor m-et növeljük a'-vel, a'-t pedig szintén 2-vel növeljük.
3. lépés: Ha $m = 0$, akkor $N = \frac{a'-b'}{2} \cdot \frac{a'+b'-2}{2}$, így megkaptuk a kívánt felbontást.

2.3.2. Példa. Bontsuk tényezőkre az $N = 459$-et!

$\lfloor \sqrt{459} \rfloor = 21$, így $m = 21^2 - 459 = -18$, $a' = 43$ és $b' = 1$.

$$\Downarrow m < 0$$

$$m = 25 \text{ és } \underline{a' = 45}$$

$$\Downarrow m > 0$$

$$
\begin{aligned}
m = 24 \text{ és } b' &= 3 \\
&\Downarrow m > 0 \\
&\vdots \\
&\Downarrow m > 0 \\
m = 9 \text{ és } b' &= 9 \\
&\Downarrow m > 0 \\
m = 0 \text{ és } \underline{b' &= 11} \\
&\Downarrow m = 0 \\
459 = \tfrac{45-11}{2} \cdot \tfrac{45+11-2}{2} &= 17 \cdot 27 = 17 \cdot 3^3
\end{aligned}
$$

A 27-et a módszer 2-szeri alkalmazásával hasonlóan tényezőkre bonthatjuk.

A Fermat-féle felbontásnak léteznek más megvalósításai is. Például vizsgálhatjuk az $N = a^2 - b^2$ egyenletet (b^2-re rendezve) az $a^2 - N = b^2$ alakban, vagyis, hogy az $a^2 - N = c$ egyenletben mikor lesz c négyzetszám. Ekkor a helyére $(\lceil\sqrt{N}\rceil + 1)$-gyel kezdve helyettesítünk $\lceil\sqrt{N}\rceil + i$-t $(i = 2, ...)$, amíg c megfelelő nem lesz.

2.3.3. Példa. Bontsuk tényezőkre az $N = 87$-et!
$\lceil\sqrt{87}\rceil + 1 = 11 \Rightarrow 11^2 - 87 = 34$, ami nem négyzetszám. $\lceil\sqrt{87}\rceil + 2$-vel folytatva kapjuk, hogy $12^2 - 87 = 57$, ami szintén nem az. A következő próba a $\lceil\sqrt{87}\rceil + 3 = 13$-mal történik, így $13^2 - 87 = 82$, de ez sem teljes négyzet. Sorban haladva a $\lceil\sqrt{87}\rceil + 5 = 16$-nál fordul elő, hogy $16^2 - 87 = 169 = 13^2$, ezért $87 = (16-13)(16+13) = 3 \cdot 29$.

A következő változat alapja az, hogy ha van k db különböző p_i prímünk és $k + 1$ db olyan b_i számunk, melyeknek nincs a p_i-ktől különböző prímosztójuk, akkor mindig kiválasztható néhány b_i, melyek szorzata négyzetszám. Mielőtt rátérnék a bizonyításra, definiálom a faktor bázis és a hasonlósági vektor fogalmát.

2.3.4. Definíció. *Egy $B = \{(p_1 = -1), p_2, ..., p_k\}$ különböző (kivéve $p_1 = -1$-et, ő a negatív maradékok miatt szerepel) prímek halmazát faktor bázisnak nevezzük. Egy b egész B-szám egy adott n-re, ha (a legkisebb abszolút értékben vett) $b^2 \pmod n$ felírható B-beli elemek szorzataként.*

2.3.5. Definíció. *Egy $b_i = \prod_{j=1}^{k} p_j^{\alpha_j}$ B-szám hasonlósági vektora az a v_i $\mathbb{Z}_2^k$-beli vektor, amelynek koordinátáira $v_i^j = (\alpha_j \pmod 2)$.*

2.3.6. Állítás. *Legyen $B = \{(p_1 = -1), p_2, ..., p_k\}$ és legyenek $b_1, b_2, ..., b_k, b_{k+1}$ különböző B-számok. Ekkor létezik $1 \leq j$ db b_i, melyek szorzata teljes négyzet.*

Bizonyítás. Legyenek a $b_1, b_2, ..., b_{k+1}$ B-számok hasonlósági vektorai rendre a $v_1, v_2, ..., v_{k+1}$ $\mathbb{Z}_2^k$ vektorok. Mivel $k+1$ db $\mathbb{Z}_2^k$-beli vektorról van szó, ezért ezek lineárisan összefüggnek, azaz nem csak triviálisan adják ki a nullvektort. Ebben az összegben az 1 együtthatójú v_i-knek megfelelő b_i-k szorzatában lévő p_i-k kitevője páros, vagyis négyzetszám. □

Ekkor azt csinálhatjuk, hogy veszünk egy ilyen $B = \{p_1, p_2, ..., p_k\}$-t és n-et, és két különböző módon gyártunk olyan számokat, melyeknek a négyzeteik kongruensek mod n, de ők maguk abszolútértékben nem azok. Tegyük fel, hogy ismerünk $(2 \leq)q$ db b_i B-számot, melyek hasonlósági vektoraik lineárisan összefüggnek, ekkor a következőt tesszük: kiszámítjuk $\prod_{i=1}^{q} b_i \pmod n$-et, jelöljük β_i-vel a legkisebb abszolút értékű maradékát a $b_i^2 \pmod n$ értéknek. Ekkor $\beta_i = \prod_{j=1}^{k} p_j^{\alpha_{ij}}$, így $\prod \beta_i = \prod_{j=1}^{k} p_j^{\sum_i \alpha_{ij}}$, és most abban bízunk, hogy $\prod_{j=1}^{k} p_j^{\frac{\sum_i \alpha_{ij}}{2}} \not\equiv \pm \prod_{i=1}^{q} b_i \pmod n$ (mert, ha $x^2 \equiv y^2 \pmod n$ és $x \not\equiv \pm y \pmod n$, akkor $(x+y, n)$ vagy $(x-y, n)$ n-nek egy valódi osztóját adják). Előfordulhat, hogy kongruensek, ekkor más B-számokkal (melyek hasonlósági vektoraik összefüggnek) sikeresebben járhatunk el. Mivel egy $b_i = \prod_{i=1}^{k} p_i^{\alpha_i}$ szám esetén az $x^2 \equiv c^2 \pmod n$ kongruenciának pontosan 2^k különböző megoldása van, ezért annak az esélye, hogy $\prod_{j=1}^{k} p_j^{\frac{\sum_i \alpha_{ij}}{2}} \equiv \pm \prod_{i=1}^{q} b_i \pmod n$ teljesül kevesebb, mint $\frac{1}{2}$. A gyakorlatban egy ilyen B faktor bázis előállítása kérdéses, vehetjük például az első k db prímet, ekkor egy véletlen módszer segítségével a megfelelő prímekkel és kitevőkkel előállítjuk a b_i-ket. A következő példa ezt mutatja be.

2.3.7. Példa. Legyen $B = \{-1, 2, 3, 5, 7\}$ és $N = 2451$. Nyilván $\lceil \sqrt{2451} \rceil = 50$ körüli számokkal érdemes kezdeni, hiszen ekkor kicsi a maradék $\bmod 2451$, így kapjuk, hogy:

$$48^2 \equiv -147 = -3 \cdot 7^2 \pmod{2451} \Rightarrow v_1 = (1, 0, 1, 0, 0)$$
$$49^2 \equiv -50 = -2 \cdot 5^2 \pmod{2451} \Rightarrow v_2 = (1, 1, 0, 0, 0)$$
$$50^2 \equiv 49 = 7^2 \pmod{2451} \Rightarrow v_3 = (0, 0, 0, 0, 0)$$
$$51^2 \equiv 150 = 2 \cdot 3 \cdot 5^2 \pmod{2451} \Rightarrow v_4 = (0, 1, 1, 0, 0).$$

Láthatjuk, hogy $v_1 + v_2 + v_4 = 0$ ($b_1 = 48, b_2 = 49, b_3 = 51$). Tehát lineárisan összefüggnek, ezért minden kitevőből páros sok van, tehát kiszámíthatjuk a fentebb említett szorzatokat.

$$\prod_{i=1}^{3} b_i = 48 \cdot 49 \cdot 51 \equiv -147 \pmod{2451} \text{ és}$$

$$\prod_{j=1}^{5} p_j^{\frac{\sum_i \alpha_{ij}}{2}} = (-1) \cdot 2 \cdot 3 \cdot 5^2 \cdot 7 \equiv 1401 \pmod{2451}.$$

Ezek pedig nem kongruensek (de $(-147)^2 \equiv 1401^2$), vagyis $(1401 - 147, 2451) = 3$(prím) és $(1401 + 147, 2451) = 129$ osztókat kaptuk, így $\frac{2451}{129} = 19$(prím), tehát már két prímosztónk van, ezekből $\frac{2451}{3 \cdot 19} = 43$(prím), vagyis $2451 = 3 \cdot 19 \cdot 43$ felbontást kaptuk.

Mivel arra törekszünk, hogy a $b_i^2 \pmod n$ maradékok kicsik és viszonylag kis prímek szorzatai legyenek, ezért a $b_i^2 \pmod n$ felbontását számítógépen akár a próbaosztások módszerével is elvégezhetjük. A következő algoritmusban összegzem a fenti példában látott eljárást.

2.3.8. Algoritmus. Faktor bázissal való felbontás.

1. lépés: Legyen $B = \{-1 = p_1, p_2, ..., p_k\}$ az első $k-1$ prím (gyakorlati szempontból az első 15-20 elegendő, ha nem, akkor növeljük)
2. lépés: Teszteljük sorra a $\sqrt{ln}$ és $\sqrt{ln} + 1$ ($l = 1, 2, ...$) számok közötti értékeket, hogy jók-e B-számnak
3. lépés: A hasonlósági vektorokból válasszunk ki lineárisan összefüggő rendszert
4. lépés: Számítsuk ki az $a := \prod_{i=1} b_i$-t és a $b := \prod_{j=1}^{k} p_j^{\frac{\sum_i \alpha_{ij}}{2}}$ értékeket, ha ezek inkongruensek ($a \not\equiv \pm b \pmod n$), akkor $(a \pm b, n)$ valódi osztókat kapjuk, ha kongruensek, akkor próbálkozzunk más B-számok keresésével.

Igazából Fermat az 1640-es években nem pontosan így bontotta szorzattá a számokat. Ő is az $a^2 - N$ értéket nézte, hogy mikor lesz teljes négyzet, de nem közvetlen próbálgatással járt el, hanem bizonyos számokra megnézte, hogy egy négyzetszám milyen maradékot adhat ezekre a modulusokra, és így következtetett az a tulajdonságaira, majd csak a megfelelő a-kat helyettesítette be.
Ez szolgál alapul a következő prímfaktorizációs eljárásban, vagyis a szitamódszerben.

2.4. Szitamódszer

A szitamódszerben egymáshoz és N-hez relatív prímeket veszünk modulusnak és a segítségükkel vizsgáljuk $a^2 - N$ az ezekre a számokra vett osztási maradékait. Tehát mondhatni, hogy Fermat eredeti módszerének a kidolgozott változata. Pontosabban arról van szó, hogy ha vesszük például az $N = 20203$ számot és nézzük a következő maradékokat:

m	$a \pmod m$	$a^2 \pmod m$	$a^2 - N \pmod m$
3	$0, 1, -1$	$0, 1, 1$	$-1, 0, 0$
5	$0, 1, 2, -2, -1$	$0, 1, -1, -1, 1$	$2, -2, 1, 1, -2$
7	$0, 1, 2, 3, -3, -2, -1$	$0, 1, -3, 2, 2, -3, 1$	$-1, 0, 3, 1, 1, 3, 0$
8	$0, 1, 2, 3, 4, -3, -2, -1$	$0, 1, 4, 1, 0, 1, 4, 1$	$-3, -2, 1, -2, -3, -2, 1, -2$

Ezekből kiolvasható például, hogy ha $a^2 - N$ teljes négyzet, akkor $a \not\equiv 0 \pmod 3$ lehet csak, szintén ezért $a \equiv \pm 2 \pmod 5$, $a \equiv \pm 1, \pm 3 \pmod 7$ és $a \equiv \pm 2 \pmod 8$, vagyis a páros, elég a $\lceil \sqrt{20203} \rceil = 145$-nél nagyobb vagy egyenlő 2-vel osztható számokat keresnünk. Szerencsére hamar megtaláljuk a $158^2 - 20203 = 4761 = 69^2$ megoldást. Tehát $20203 = 89 \cdot 227$.

Készítsük el a szitatáblázatot a fenti ábra szerint, és ebből könnyen leolvasható, hogy $a^2 - N$ lehet-e teljes négyzet (van-e közös elem a második és harmadik oszlopban). A következő algoritmushoz legyenek N a felbontandó szám, m_i $(i = 1, 2, ..., k)$ páronként relatív prím modulusok, valamint $(m_i, N) = 1$ és legyen $a = \lceil \sqrt{n} \rceil$. Ekkor az eljárás minden m_i-re megvizsgálja az $a^2 - N \pmod{m_i}$ maradékot és, ha minden m_i-re ez lehet négyzetszám, akkor leellenőrzi, hogy $a^2 - n$ valóban négyzetszám-e. Az m_i-kből célszerű minél többet bevenni, ezáltal sokkal kevesebb tényleges próbát kell elvégezni, más szóval hamarabb kiderül az a-ról, hogy nem „jó”, azaz $a^2 - N$ nem lehet teljes négyzet.

2.4.1. Algoritmus. Szitamódszer

1. lépés: Legyen $a = \lceil \sqrt{N} \rceil$
2. lépés: Ha $a^2 - N \pmod{m_i}$ minden $i = 1, ..., k$-ra ad olyan maradékot, ami lehet négyzetszám, akkor $b := \lceil \sqrt{N} \rceil$ vagy $b := \lfloor \sqrt{N} \rfloor$, ha van olyan $1 \leq t \leq k$, melyre $a^2 - N \pmod{m_t}$ nem lehet négyzetszám, akkor $x := x + 1$ és kezdjük elölről a 2. lépést
3. lépés: Ha $a^2 - N = b^2$, akkor $a - b$ és $a + b$ osztókat találtuk meg, ha $a^2 - N \neq b^2$,

akkor $x := x + 1$, és menjünk a 2. lépésre

A táblázat alapján gyorsíthatunk az eljáráson, ha bizonyos oszthatóságok is fennállnak például, ha $(2 \leq) l \mid N$, akkor elegendő a $[\sqrt{N}] + l$ alakú számokat leellenőrizni.

Utószó

Az eddigi prímtesztek nem 100%-os, hanem csak 99,9999...%-os biztonsággal állították egy számról, hogy prím és hosszú évekig nem tudták, hogy létezik-e olyan teszt, amely tévedhetetlen és gyorsan számítható is egyben. 2002-ben változott a helyzet, ugyanis három indiai matematikus, név szerint Manindra Agrawal, Neeraj Kayal és Nitin Saxena kidolgoztak egy olyan prímtesztet, ami nem csakhogy 100%-os biztonságot nyújt, polinom időben számítható. Az alapkoncepció az, hogy, ha n prím, akkor $\mathbb{Z}_n$-ben az n-edikre emelés tagonként végezhető, azaz $(x-a)^n = x^n - a^n$. Ekkor a kis Fermat-tétel miatt $(x-a)^n \equiv x^n - a \pmod{n}$. Viszont $(x-a)^n$-ben a binomiális együtthatók kiszámítására nem ismert hatékony módszer, ezért az eljárás azt csinálja, hogy $x^r - 1$ alakú polinomra, mint modulusra vizsgálja az $x^n - c \equiv^? (x-c)^r$ kongruenciát. Ekkor az n prím $\Leftrightarrow x^n - c \equiv (x-c)^n \pmod{x^r - 1}$ tétel biztosítja a teszt tévedhetetlenségét.

Az általam C++ nyelvben megírt tesztek kb. 50000-ig képesek eldönteni egy számról, hogy prím-e. A prímfaktorizációs programokban, mint pl. a Monte Carlo felbontásban lehet más másodfokú függvényt is alkalmazni vagy más konstans tagot szerepeltetni, így bizonyos esetekben – amikor nem tudjuk felbontani n-et az $f(x) = x^2 + 1$ függvény használatával – is sikerrel járhatunk. Végül megjegyzem, hogy a prímfaktorizáció problémájának eldönthetősége (vagyis, hogy létezik-e gyors módszer, ami megtalálja egy n szám prímfelbontását) máig nem ismert, de „valószínű”, hogy nincs is ilyen. Viszont a jövőbeni kvantumszámítógépekkel már elképzelhető lehet egy ilyen felbontás gyors megtalálása.

Irodalomjegyzék

[1] Freud Róbert, Gyarmati Edit, *Számelmélet*, Nemzeti Tankönyvkiadó, 2006, 199-213

[2] Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1998, 125-154

[3] Donald E. Knuth, *A számítógépprogramozás művészete 2. kötet*, Műszaki Könyvkiadó, 1987, 371-387

[4] Freud Róbert, *Lineáris algebra*, ELTE Eötvös Kiadó, 2006, 258-262