Prímtesztelés determinisztikus polinom időben

M. Agrawal, N. Kayal, N. Saxena

és

mások gondolatai nyomán

Rónyai Lajos
MTA SZTAKI, BME

Egy kis história

Prímek: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Pitagoreusok (Kr.e. VI. sz.): minden megragadható számokkal, pl. 220, 284 és a barátság.

Euklidesz (Kr.e. IV. sz.): prímek ∞ sokan vannak, számelmélet alaptétele.

Eratoszthenész szitája (Kr.e. III. sz.): a prímek listája (gyorsan) egy korlátig.

Két alapfeladat

Felismerés: *adott* $n \in \mathbb{Z}^+$*; n prím-e?*

Felbontás: *adott* $n \in \mathbb{Z}^+$*; bontsuk fel prímek szorzatára.*

K. F. Gauß (1801):

A prímeknek az összetett számoktól való megkülönböztetése és az összetettek felbontása prímek szorzatára az egész aritmetika egyik legfontosabb és leghasznosabb problémája. A tudomány méltósága megkövetelni látszik, hogy egy ilyen híres és elegáns probléma megoldásához minden segédeszközt buzgón kifejlesszünk.

Sokáig inkább elméleti érdeklődés; M. Kraitchik, D. H. Lehmer, D. Shanks

Döntő fordulat a 70-es években: kommunikáció, számításelmélet

Kommunikációs robbanás: biztonságos kommunikáció mint tömegigény

Számításelmélet: *könnyű* és *nehéz* az algoritmusok világában, (véletlen-) polinom idő

RSA-kódolás: felbontás nehéz, felismerés könnyű

Kongruenciák

Legyenek $a, b, n \in \mathbb{Z}$, $n > 0$.

$a \equiv b \bmod (n)$, ha n osztója $a - b$-nek.

Fontos és kellemes összefüggések:

Ha $a_1 \equiv b_1 \bmod (n)$ és $a_2 \equiv b_2 \bmod (n)$, akkor

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \bmod (n),$$

$$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \bmod (n).$$

A $0, 1, 2, \ldots, n-1$ maradékokkal számolhatunk.

Szigorúan szólva a színtér $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

Például $5 + 6 \equiv 4 \bmod (7)$ és $5 \cdot 6 \equiv 2 \bmod (7)$.

Az Euler-függvény

$\phi(n)$ az n-hez relatív prím egészek száma $[1, n]$-ben.

A ϕ multiplikatív: ha $(n, m) = 1$, akkor $\phi(nm) = \phi(n)\phi(m)$.

Ha p prím, akkor $\phi(p) = p - 1$.

Ha p, q különböző prímek, akkor $\phi(pq) = (p - 1)(q - 1)$.

Az Euler–Fermat-tétel

Ha $(a, n) = 1$, *akkor* $a^{\phi(n)} \equiv 1 \bmod (n)$.

Köv.: legyenek $e, d \in \mathbb{Z}$, $ed \equiv 1 \bmod (\phi(n))$. Ekkor $(a, n) = 1$ esetén $a^{ed} \equiv a \bmod (n)$.

$$a^{ed} \equiv a^{\phi(n)k+1} \equiv a^{\phi(n)k} a \equiv 1 \cdot a \equiv a \bmod (n).$$

Az RSA titkosító eljárás

Cél: $\mathcal{A}$ titkos levelet küldene $\mathcal{B}$-nek.

Hozzávalók: két nagy titkos prím p, q, $n = pq$ nyilvános.
Az e nyilvános kitevő és a csak $\mathcal{B}$ által ismert d kitevő, melyekre $ed \equiv 1 \bmod (\phi(n))$.

$\mathcal{A}$ nyílt üzenete: $a \in \mathbb{Z}_n$, $(a, n) = 1$.

$\mathcal{A}$ kódolt (titkosított) üzenete: $b := a^e \bmod (n)$.

$\mathcal{B}$ a d segítségével fejti meg (nyeri vissza) az eredeti üzenetet:

$$b^d \equiv a^{ed} \equiv a \bmod (n).$$

Követelmények

1. A normális működés **gyors**.
2. Az illetéktelen megfejtés **lassú**.

Gyorsaság: polinom idejű módszerek. m bites bemeneten legfeljebb m^c lépés.

Gyorsan megy:

p, q választása (véletlen).
Összeadás, szorzás $\bmod(n)$ $\quad O(\log^2 n)$.
Lnko számítása (euklideszi algoritmus viharsebes változata) $\quad O(\log^2 n)$.
Adott $a, b \in \mathbb{Z}$. Kell $A, B \in \mathbb{Z}$, melyekkel

$$aA + bB = (a, b).$$

Prímtesztelés: véletlennel várhatóan $O(\log^3 n)$, véletlen nélkül $O(\log^{7,5+\epsilon} n)$.
Gyors hatványozás: $a^e \bmod (n)$ $\quad O(\log n)$ moduláris szorzás.

Gyors hatványozás

Adott $a, e \in \mathbb{Z}^+$, $a, e < n$, kell $a^e \bmod (n)$.

Itt a, e, n többszáz bites egészek.

A naiv módszer reménytelen (10^{81} atom a látható Univerzumban).

A gyorsító ötlet már a Rhind-papiruszon (i.e. 1650 körül) is szerepel.

Illusztráció: a^{35} számolása

$$35 = 1 + 2 + 2^5$$

A számolás menete

$$a^2 = a \cdot a,\ a^4 = a^2 \cdot a^2,\ a^8 = a^4 \cdot a^4,$$

$$a^{16} = a^8 \cdot a^8,\ a^{32} = a^{16} \cdot a^{16}.$$

$$a^{35} = a \cdot a^2 \cdot a^{32}.$$

34 helyett 7 szorzás.

Illetéktelen megfejtés

Pusztán e és n ismeretében d kitalálása.

Erre nem ismert jobb módszer, mint p, q megtalálása, n felbontása.

Elég a rendszer teljes feltöréshez, hiszen $\phi(n) = (p-1)(q-1)$ ismeretében d a köv. kongruencia megoldása:

$$ex \equiv 1 \bmod (\phi(n)).$$

Megy euklideszi algoritmussal.

A felbontási feladatra nem ismert hatékony algoritmus. Ez több titkosító eljárás biztonságának az elvi alapja.

A jelenlegi felbontási rekord

Bahr, Franke, Kleinjung, Universität Bonn, 2002

Módszer: általános számtest szita,
ultrapárhuzamos megvalósítással

Becsült CPU-idő (800 Mhz Athlon): 52+ hónap

A felbontott szám (158 decimális jegyű):

395058745832651445264197678006144819960
207764603049364541393760515793556265294
506836097278424682195350935443058704902
519956553357102097992264849779494429556
03

A prímosztói:

33884958374667213943683932046721815228
1583036860499304808492584055528117

11658823406671259903148376558383270818
13101225814639260043952099413134433416
2924536139

Felismerő algoritmusok (prímtesztek)

Az adott n-ről várhatóan $O(\log^k n)$ lépésben eldöntik, hogy prím-e.

Fermat-teszt alapja: ha n prím, és $(a, n) = 1$, akkor $a^{n-1} \equiv 1 \pmod{n}$.

Bánat: Carmichael-számok (∞ sok van)

Valamivel szigorúbb teszt már megteszi...

Solovay-Straßen (1977) alapja: ha n prím, $(a, n) = 1$, akkor

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

Továbbiak: **Rabin-Miller** (1978), **Lehmann** (1982), **Baillie-Wagstaff** (1980).

Ragyogó randomizált rutinok; $\Pi \in$coRP.

Elméleti szirtfokok

L.M. Adleman, C. Pomerance, R.S. Rumely (1983): Prímtesztelés determinisztikus $O((\log n)^{c \log\log\log n})$ időben.

Alapja: algebrai számelmélet, magasabb reciprocitási szabályok.

S. Goldwasser, J. Kilian (1986): Majdnem minden prímre működő, bizonyítványt szolgáltató véletlen polinom idejű teszt.

Alapja: véges testek feletti elliptikus görbék.

L.M. Adleman, M.D.A. Huang (1992): $\Pi \in$RP. Kb. 150 oldalas kötet.

Alapja: véges testek feletti algebrai geometria, Jacobi-sokaságok.

Szükséges-e Tükhé érméje?

Agrawal-Kayal-Saxena (2002): NEM! $\Pi \in$P

Kiindulópont: *Legyenek* $a, n \in \mathbb{Z}$, $(a, n) = 1$ *és* $n > 1$. *Az* n *pontosan akkor prím, ha*

$$(x + a)^n \equiv x^n + a \pmod{n}.$$

Biz.: A baloldalon x^i együtthatója $\binom{n}{i}a^{n-i}$. Ha n prím, akkor $n|\binom{n}{i}$, ha $i = 1, \ldots, n-1$. A kis Fermat miatt igaz a kongruencia.

Tfh. n összetett, és legyen q egy prímosztója, $q^k||n$. Ekkor x^q együtthatója nem osztható n-nel, mert

$$\binom{n}{q} = \frac{n(n-1)\cdots(n-q+1)}{1 \cdot 2 \cdots q}$$

csak q^{k-1}-gyel osztható. $\square$

Cseberből vederbe: exponenciális sok vizsgálandó együttható, magas fok.

Javító-egyszerűsítő ötlet: nézzük a kongruenciát modulo $x^r - 1$, ahol az r kis pozitív egész. Azt vizsgáljuk, hogy igaz-e

$$(x+a)^n \equiv x^n + a \bmod (n, x^r - 1).$$

Példa:

$$18x^9 - 4x^5 + 8x^3 \equiv 4x^4 + 3 + x^3 \bmod (7, x^5 - 1).$$

Pontos (algebrai) nézet: a színtér a $\mathbb{Z}_n[x]/(x^r - 1)$ gyűrű.

Megeshet, hogy *egy* ilyen teszt elégtelen (összetett n túléli).

Átütő gondolat (AKS, 2002): *egy jó (kis) r és néhány (nem sok) a választásával már elégséges tesztet nyerünk.*

Madártávlatból az AKS-dolgozatról

Csupán 8 oldal; (logikailag) két fő részből áll:

A par excellence **Teszt**:
mindössze 2 oldalnyi
lényegében elemi
megkapóan egyszerű
boszorkányosan ötletes
Erdős Pál *Köny*vébe kívánkozik

Paraméterek választása:
a polinomiális korlát elemi úton adódik
az erősebb időkorláthoz használják É. Fouvry egy nehéz tételét

Egy fontos fogalom

Def.: Legyenek $n, r \in \mathbb{Z}^+$, $(n, r) = 1$. Az n rendje modulo r az a legkisebb k pozitív egész, melyre $n^k \equiv 1 \bmod (r)$. A jele $o_r(n)$.

Az AKS-teszt

Tétel (AKS, 2003): *Legyenek* $n, r \in \mathbb{Z}$, $n, r > 1$. *Legyen* $\ell = \lfloor 2\sqrt{\phi(r)} \log n \rfloor$, *és tegyük fel a következőket:*

1. n *nem valódi hatvány,*
2. $o_r(n) > 4 \log^2 n$,
3. *a* $[2, r]$ *egészei nem osztói* n*-nek,*
4. $(x + a)^n \equiv x^n + a \bmod (n, x^r - 1)$ *teljesül, ha* $a = 1, \ldots, \ell$.

Ekkor n *prímszám.*

Megjegyzés. Könnyű kideríteni, hogy n valódi hatvány-e.

Állítás: *Legyen* $n > 1$ *egész. Ekkor van olyan* $r \leq \lceil 16 \log^5 n \rceil$ *egész, melyre* $o_r(n) > 4 \log^2 n$.

Megjegyzés. A 3. $O(\log^5 n)$, a 4. $O(\log^{3,5} n)$ esetet jelent.

Bemelegítés: kongruenciák

Legyen R egy gyűrű, $a, b, c \in R$.

$$(*) \qquad a \equiv b \pmod{c}$$

jelentése: c osztja R-ben $a - b$-t.

Modulus osztója is modulus

Ha $(*)$ fennáll, és $d \in A$ osztója c-nek, akkor

$$a \equiv b \pmod{d}.$$

Morfizmus megőrzi

Ha $\phi : A \to B$ egy gyűrű-homomorfizmus, akkor

$$\phi(a) \equiv \phi(b) \pmod{\phi(c)}$$

következik $(*)$-ból.

Bizonyítás: Legyen p az n prímosztója. A 3. miatt $p > r$ és $(n, r) = 1$.

Minden $a = 1, \ldots, \ell$ egészre 4. alapján

$$(x + a)^n \equiv x^n + a \bmod (n, x^r - 1),$$

tehát

$$(x + a)^n \equiv x^n + a \bmod (p, x^r - 1).$$

A modulo p binomiális tétel miatt

$$(x + a)^p \equiv x^p + a \bmod (p, x^r - 1).$$

Def. Az $m \in \mathbb{Z}^+$ az $f(x)$ polinom *bebújó* kitevője, ha $f(x)^m \equiv f(x^m) \bmod (p, x^r - 1)$.

Az $x + a$ polinomoknak n, p bebújó kitevői.

Ha $m, k \in \mathbb{Z}^+$ az $f(x)$ bebújó kitevői, akkor mk is az.

Mivel m bebújó:

$$(\clubsuit) \qquad f(x)^{mk} \equiv f(x^m)^k \bmod (p, x^r - 1).$$

Mivel k bebújó (az x helyett x^m változóval):

$$f(x^m)^k \equiv f(x^{mk}) \bmod (p, x^{m \cdot r} - 1).$$

Az $(y-1)|(y^m - 1)$ azonosság szerint $x^r - 1$ osztója az $x^{m \cdot r} - 1$ polinomnak, vagyis

$$f(x^m)^k \equiv f(x^{mk}) \bmod (p, x^r - 1).$$

Előző és ($\clubsuit$) alapján

$$f(x)^{mk} \equiv f(x^{mk}) \bmod (p, x^r - 1).$$

$\square$

Ha m bebújó kitevője $f(x)$-nek és $g(x)$-nek, akkor $f(x)g(x)$-nek is.

Modulo $(p, x^r - 1)$ számolva

$$(f(x)g(x))^m \equiv f(x)^m g(x)^m \equiv f(x^m)g(x^m).$$

$\square$

A két kis állítás szerint $I = \{n^i p^j : \ i, j \geq 0\}$ minden eleme bebújó a

$$P = \{\prod_{a=1}^{\ell}(x+a)^{e_a} : \ e_a \geq 0\}$$

minden elemére nézve. *Ez túl sok a jóból!*

Legyen G az $I \bmod (r)$. Ekkor $G \leq \mathbb{Z}_r^*$, mert $(n, r) = (p, r) = 1$.

Legyen $t := |G|$. Igaz, hogy $t > 4\log^2 n$, mert $o_r(n) > 4\log^2 n$.

Legyen $h(x) \in \mathbb{F}_p[x]$, $h(x)|x^r - 1$ az r-edik körosztási polinom egy irreducibilis osztója. Másként mondva:

x primitív r-edik egységgyök az $\mathbb{F} := \mathbb{F}_p[x]/(h(x))$ testben.

Új helyszín: az $\mathbb{F} = \mathbb{F}_p[x]/(h(x))$ test

Legyen $\mathcal{G}$ a P elemei által generált multiplikatív részcsoport $\mathbb{F}^*$-ban (nulla maradékot kidobjuk).

A $\mathcal{G}$-t generálja $\mathbb{F}^*$-ban $x + 1, x + 2, \ldots, x + \ell$.

Fontos: Két polinom, $f(x), g(x)$ akkor egyenlő $\mathbb{F}$-ben, ha $f(x) \equiv g(x) \bmod (p, h(x))$.

Ez teljesül, ha $f(x) \equiv g(x) \bmod (p, x^r - 1)$, mert $h(x)|x^r - 1$.

1. Lemma: (H. W. Lenstra, jr.)

$$|\mathcal{G}| \geq \binom{t+\ell-2}{t-1}.$$

Biz.: Megmutatjuk, hogy ha $f_1(x), f_2(x) \in P$ különbözőek modulo p, és t-nél kisebb fokúak, akkor $\mathbb{F}$ ben is különbözőek.

Ellenkező esetben, ha $\mathbb{F}$-ben $f_1(x) = f_2(x)$ akkor $f_1(x)^m = f_1(x)^m$ is igaz minden $m \in I$-re. De m bebújó mindkét polinomnál, tehát **Fontos** szerint $f_i(x)^m = f_i(x^m)$ igaz $\mathbb{F}$-ben, azaz

$$f_1(x^m) = f_2(x^m) \text{ érvényes } \mathbb{F}\text{-ben.}$$

Az x^m tehát gyöke a $Q(y) := f_1(y) - f_2(y)$ polinomnak, minden $m \in G$-re.

Ha $m, k \in G$ különbözők, akkor $G \leq \mathbb{Z}_r$ miatt $\mathbb{F}$-ben $x^m \neq x^k$. Eszerint $Q(y)$-nak legalább $|G| = t$ gyöke van, ami nem lehet, mert a foka $< t$. Tehát $f_1 \neq f_2$.

Ha $1 \leq i \neq j \leq \ell$, akkor $i \neq j$ $\mathbb{F}_p$-ben mert

$$\ell = \lfloor 2\sqrt{\phi(r)} \log n \rfloor < 2\sqrt{r} \log n < r,$$

és $r < p$. Tehát

$$x+1, x+2, \ldots, x+\ell$$

mind különbözők $\mathbb{F}$-ben, és legfeljebb egyikük lehet 0.

Vegyünk $\ell - 1$ nem nullát közülük és ezekből a $< t$ tényezős szorzatokat. Ezek mind különböznek $\mathbb{F}$-ben. A számuk:

$\ell - 1$ elem $\leq t-1$-tagú ismétléses kombinációi

$$\Longleftrightarrow$$

ℓ elem pontosan $t-1$-es ism. kombinációi, azaz

$$\binom{t+\ell-2}{t-1}.$$

$\square$

2. Lemma: *Ha $n \neq p$, akkor $|\mathcal{G}| < \frac{1}{2} n^{2\sqrt{t}}$.*

Biz.: (A. Kalai, A. Sahai, M. Sudan)
Nézzük az $n^i p^j$ számokat, ahol $0 \leq i, j \leq \lfloor \sqrt{t} \rfloor$.
Mivel n nem hatványa p-nek, ezek száma $(\lfloor \sqrt{t} \rfloor + 1)^2 > t$.

Igaz továbbá, hogy $1 \leq n^i p^j \leq (np)^{\lfloor \sqrt{t} \rfloor}$.

A skatulyaelv miatt van köztük $m_1 > m_2$, hogy $m_1 \equiv m_2 \bmod (r)$. Ekkor $x^{m_1} = x^{m_2}$ igaz $\mathbb{F}$-ben.
Legyen $f(x) \in P$. $\mathbb{F}$-beli egyenlőségekkel

$$f(x)^{m_1} = f(x^{m_1}) = f(x^{m_2}) = f(x)^{m_2}.$$

Magyarán: a $\mathcal{G}$ elemei gyökei az $R(y) = y^{m_1} - y^{m_2} \in \mathbb{F}[y]$ polinomnak.

$$|\mathcal{G}| \leq R \text{ foka } = m_1 \leq (np)^{\lfloor \sqrt{t} \rfloor} < \frac{1}{2} n^{2\sqrt{t}}.$$

$\square$

A bizonyítás vége

Ha $n \neq p$, akkor a Lemmák szerint

$$\binom{t+\ell-2}{t-1} \leq |\mathcal{G}| < \frac{1}{2} n^{2\sqrt{t}}.$$

A másik irányban használjuk a következőket:

$$t > 2\sqrt{t} \log n,$$

$$\ell = \lfloor 2\sqrt{\phi(r)} \log n \rfloor \geq \lfloor 2\sqrt{t} \log n \rfloor.$$

Arra jutunk, hogy

$$\binom{t+\ell-2}{t-1} \geq \binom{\ell - 1 + \lfloor 2\sqrt{t} \log n \rfloor}{\lfloor 2\sqrt{t} \log n \rfloor} \geq$$

$$\geq \binom{2\lfloor 2\sqrt{t} \log n \rfloor - 1}{\lfloor 2\sqrt{t} \log n \rfloor} \geq 2^{\lfloor 2\sqrt{t} \log n \rfloor}.$$

Használtuk, hogy $\lfloor 2\sqrt{t} \log n \rfloor \geq 3$. Végül

$$2^{\lfloor 2\sqrt{t} \log n \rfloor} \geq 2^{2\sqrt{t} \log n - 1} = \frac{1}{2} n^{2\sqrt{t}}.$$

Ez ellentmondás. $\square$

Az r választása

Állítás: *Tfh.* $n > 1$. *Létezik* $1 < r \leq \lceil 16 \log^5 n \rceil$ *egész, mellyel* $o_r(n) > 4 \log^2 n$.

Legyen $m > 0$ egész. Jelölje $LCM(m)$ az $1, \ldots, m$ egészek legkisebb közös többszörösét.

Tétel: *Ha* $m > 6$ *akkor* $LCM(m) \geq 2^m$.

Ha $o_r(n) \leq 4 \log^2 n$ akkor r osztja az

$$M = \prod_{i=1}^{\lfloor 4 \log^2 n \rfloor} (n^i - 1)$$

szorzatot. Mármost

$$M < n^{16 \log^4 n} \leq 2^{16 \log^5 n}.$$

A Tétel alkalmazzuk $m = \lceil 16 \log^5 n \rceil$ választással.

$$LCM(m) \geq 2^{\lceil 16 \log^5 n \rceil} > M,$$

tehát van $1 < r \leq m$, ami nem osztója M-nek. $\square$

Az időigény (vázlat)

A munka dandárja az ℓ darab

$$(x+a)^n \equiv x^n + a \bmod (n, x^r - 1)$$

kongruencia tesztelése.

Egy ilyen teszt: kb. $\log n$ polinomszorzás (fok$\leq r$).

Az együtthatók mérete kb. $\log n$ bit.

Egy ilyen polinomszorzás ára – FFT-t használva – $O^{\sim}(r \log n)$.

Egy teszt ára $O^{\sim}(r \log^2 n)$.

$\ell = O(r^{0,5} \log n)$ db. teszt ideje $O^{\sim}(r^{1,5} \log^3 n)$.

Mivel $r = O(\log^5 n)$, az eljárás teljes költsége $O^{\sim}(\log^{10,5} n)$ bitművelet.

Erősebb eszköz – jobb korlát

Def. A q prímszám *érdes*, ha $q-1$-nek van $q^{\frac{2}{3}}$-nál nagyobb prímosztója.

Étienne Fouvry tétele (1985): *Alkalmas $c^* > 0$ konstanssal*

$$|\{q \leq x : \ q \textit{ érdes prím}\}| \geq c^* \frac{x}{\ln x}.$$

Ezt alkalmazva adódik olyan $r = O(\log^3 n)$ (érdes prím), amelyre $o_r(n) > 4 \log^2 n$.

Az idő: $O^\sim(r^{1,5} \log^3 n) = O^\sim(n^{7,5})$.

Még ez is pesszimista becslés...

Javítási (javulási) lehetőség

Az $(r, \frac{r-1}{2})$ alakú prímpárokat – Marie-Sophie Germain után – *Germain-pároknak* nevezzük. Az r ekkor egy *G-felső*.

A G-felsők a lehető legérdesebb prímek.

Példák: $(5, 2)$, $(7, 3)$, $(11, 5)$, $(23, 11)$.

Sejtés G. H. Hardy–J.E. Littlewood (1922):
A G-felsők száma x-ig $\sim \frac{Dx}{\log^2 x}$.

Itt $D = 0,6601618\ldots$.

Ha a sejtés igaz, akkor $r = O(\log^2 n)$ is elérhető.

Innen $O^{\sim}(\log^6 n)$ időkorlát nyerhető.

Egy szép sejtés (R. Battacharjee, P. Pandey (2001))

Ha r prím, r nem osztója $n(n^2-1)$-nek, akkor

$$(x-1)^n \equiv x^n - 1 \bmod (n, x^r - 1)$$

esetén n prímszám.

Teljesül az $r \leq 100$, $n \leq 10^{10}$ tartományban.

Ha a sejtés igaz, akkor *egyetlen* teszt elégséges alkalmas $[2, 4\log n]$-beli r-rel.

Ennek az összköltsége $O^{\sim}(r\log^2 n) = O^{\sim}(\log^3 n)$.

Záró szavak

- Óriási elvi jelentőségű áttörés: $\Pi \in$P
- A gyakorlatban messze elmarad a véletlen tesztektől
- A Teszt (és eszmeköre) nem látszik hasznosnak a felbontáshoz
- Nem veszélyezteti az RSA és atyafiai biztonságát
- A Teszt még zsenge korú.

Hasznos címek

`http://www.utm.edu/research/primes/prove/`

`http://www.cse.iitk.ac.in/news/primality_v3.ps`

`http://www.sztaki.hu/~ronyai/ak2.ps`