Prímtesztelés

Diplomamunka

Írta: Nagy Gábor

Alkalmazott matematikus szak

Témavezető:

Kátai Imre, egyetemi tanár
Komputeralgebra Tanszék
Eötvös Loránd Tudományegyetem, Informatikai Kar

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2005

Tartalomjegyzék

1. fejezet

Bevezetés

„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."
Disquisitiones Arithmeticae(1801)

Karl Friedrich Gauss

1.1. Az RSA kriptorendszer

Az RSA egy nyilvános kulcsú titkosítást megvalósító algoritmus. 1977-ben alkotta meg Ron Rivest, Adi Shamir, és Leonard Adleman.

1.1.1. Az RSA működése

Tegyük fel, hogy `B` szeretne titkosítva üzenni `A`-nak.

A kulcsválasztás

`A` választ két nagy véletlen prímszámot (egy véletlen szám utáni első prím). Legyenek ezek p és q, a szorzatuk pedig $n = p \cdot q$. Kiszámítjuk $\varphi(n)$ értékét:

$$\varphi(n) = \varphi(p \cdot q) = (p-1)(q-1) = p \cdot q - p - q + 1 = n - p - q + 1$$

`A` választ még egy $\varphi(n)$-nél kisebb véletlen e számot, amire $(e, \varphi(n)) = 1$ (sok ilyen van).

`A` kiszámolja e multiplikatív inverzét $(mod\ \varphi(n))$: d-t, amire $e \cdot d \equiv 1\ (mod\ \varphi(n))$.

Az (n, e) számpár `A` nyilvános kulcsa, a $(d, \varphi(n))$ pedig a titkos kulcsa.

Az algoritmus

`B` címkézi az elküldendő üzenetet egy m 1 és n közötti számmal.

`B` kiszámolja $c = m^e\ (mod\ n)$-et, ez lesz a titkosított üzenet.

A beérkező üzenet elolvasása `A` által: $m = c^d\ (mod\ n)$ meghatározása.

Valóban:

$$c^d \equiv (a^e)^d = a^{e \cdot d} = a^{k \cdot \varphi(n)+1} = \left(a^{\varphi(n)}\right)^k \cdot a \equiv a \ (mod\ n),$$

mivel $a^{\varphi(n)} \equiv 1 \ (mod\ n)$(Euler-Fermat tétel).

Miért megfejthetetlen jelen ismereteink szerint?

Megfejteni csak d ismeretében lehet, ehhez viszont $\varphi(n)$ kell. n ismeretében $\varphi(n)$ kiszámítása viszont ekvivalens p, q kiszámításával, azaz n faktorizálásával. n olyan nagy, hogy jelen ismereteink szerint nem faktorizálható.

$f(x) = x^e$ úgynevezett csapóajtófüggvény, azaz csak a d többletinformáció birtokában invertálható jelen ismereteink szerint.

Az RSA-hoz el kell dönteni egy véletlen szám utáni számokról, hogy azok prímek-e. Ez a következő kérdésre vezet: hogyan lehet eldönteni egy számról, hogy prím-e?

1.2. Prímteszt, prímtesztelés

1.2.1. Definíció. *Prímteszt: egy kritérium arra, hogy egy n szám ne legyen prím. Ha n átmegy a teszten, lehet hogy prím, ha nem megy át (bukik), akkor biztos, hogy összetett.*

Egy adott szám tesztelése prímségre több prímteszt egymás utáni alkalmazásából áll. Ez a prímtesztelés lehet:
a) valószínűségi – a tesztelést túlélő szám „nagy valószínűséggel" prím
b) determinisztikus – a tesztelést túlélő szám biztosan prím
Példa:
a) Valamely $n \in \mathbb{N}$ valamely $a \in \mathbb{N}$, $a < n$-nel való osztása
ha $a \mid n$, akkor n nem prím.
Ez egy prímteszt, melyet próbaosztástesztnek („trial division") nevezünk
b) Ezt a próbaosztástesztet végrehajtva minden $a \leq \sqrt[3]{n}$-re kapjuk, hogy n nem prím, ha $a \mid n$ valamely ilyen a-ra.
Csak kevés n szám éli túl: prímek, valamint az olyan összetett számok, amelyek két $\sqrt[3]{n}$-nél nagyobb prím szorzatai. A túlélők nagy valószínűséggel prímek, ezért ez egy elég jó valószínűségi prímtesztelést ad.
c) $\forall a \leq \sqrt{n}$-nel osztva: ha bukik, akkor n biztosan összetett, ha nem, akkor biztosan prím. Ez determinisztikus tesztelés.

1.3. Gyors hatványozás

Az RSA-algoritmusban a titkosítás során meg kell határoznunk $c = m^e \ (mod\ n)$-et. Vajon ki tudjuk ezt gyorsan számolni? A válasz igen.

$a, m \in \mathbb{Z}$ számok esetén a^m meghatározásának műveletigénye ugyan $O((\log a)^2 \cdot m^2)$ vagyis $O((\log a)^2 \cdot e^{\log m^2})$, így lassú eljárás, viszont ha $(mod\ n)$ tekintjük a hatványozást jobb helyzetben vagyunk:

1.3.1. Tétel. *$a^m \pmod n$ meghatározása $O((\log m)\cdot(\log n)^2)$ műveletet igényel.*

Bizonyítás: Írjuk m-et diadikus alakban:

$$m = \varepsilon_0 + \varepsilon_1 \cdot 2 + \varepsilon_2 \cdot 2^2 + \cdots + \varepsilon_k \cdot 2^k,$$

ahol $\varepsilon_i \in \{0,1\}$, és $k = O(\log m)$.
Legyen a_i az a^{2^i} szám maradéka $(mod\ n)$:

$$a_i \equiv a^{2^i} \ (mod\ n) \quad 0 \le a_i < n \quad i = 0,1,\ldots,k$$

Először határozzuk meg az $a_0, a_1, \ldots, a_k$-t ebben a sorrendben:

$$a_0 \equiv a^{2^0} = a \ (mod\ n)$$

$$a_0 = a \quad \text{(feltéve: } 0 \le a < n)$$

Ha $a_0, \ldots, a_i$ adottak, akkor a_{i+1} kiszámítása a következőképpen történik:

$$a_{i+1} \equiv a^{2^{i+1}} = a^{2^i \cdot 2} = (a^{2^i})^2 = a_i^2 \ (mod\ n)$$

Egy ilyen négyzetreemelés, majd az eredmény n-nel vett maradékának meghatározásának műveletigénye $O((\log n)^2)$.

$$a^n = a^{\varepsilon_0 + \varepsilon_1 \cdot 2 + \cdots + \varepsilon_k \cdot 2^k} = a^{\varepsilon_0} \cdot a^{\varepsilon_1 \cdot 2} \cdots a^{\varepsilon_k \cdot 2^k} = \prod_{i=1}^{k} a^{\varepsilon_i \cdot 2^i} = \prod_{i=1}^{k} a_i^{\varepsilon_i}$$

vagyis azon a_i-k szorzata, melyekre $\varepsilon_i = 1$.
Ezeket sorban szorozva egy-egy szorzás, majd $(mod\ n)$ maradékvétel műveletigénye: $O((\log n)^2)$
Ezt $k = O(\log m)$-szer végrehajtva a teljes műveletigény:

$$k \cdot O(\log n)^2 = O((\log m)\cdot(\log n)^2).$$

A gyors hatványozást a későbbiekben is fogjuk használni.

A továbbiakban adunk egy általános áttekintést a prímszámokról, majd bemutatunk néhány prímtesztelő eljárást, különös tekintettel az AKS-algoritmusra, amely az első polinomiális idejű determinisztikus prímteszt.

2. fejezet

Prímszámok

2.1. Alapok

A prímszámokkal kapcsolatos kérdések több, mint kétezer éve foglalkoztatják az embereket. A különböző elnevezésekből adódó esetleges félreértések elkerülése végett, tekintsük a következő két definíciót.

2.1.1. Definíció. *Legyen R gyűrű, és $U(R)$ az egységek halmaza. Ekkor a $p \in R^* \setminus U(R)$ elem*

1. ***felbonthatatlan(irreducibilis)**, ha minden $a, b \in R$ esetén $p = a \cdot b$-ből $a \in U(R)$ vagy $b \in U(R)$ következik*

2. ***prím**, ha minden $a, b \in R$ esetén $p = a \cdot b$-ből $p \mid a$ vagy $p \mid b$ következik.*

Az olyan, két binér művelettel rendelkező algebrai struktúrákat, amelyekben érvényes a számelmélet alaptétele(Gauss-gyűrűk), a prímek és felbonthatatlanok halmaza egybeesik. Mivel az egész számok halmaza is Gauss-gyűrű az összeadás és szorzás műveletével, bocsánatos bűn, hogy általános és középiskolában a felbonthatatlan elem definícióját használják prímekre.

Azt, hogy végtelen sok prímszám létezik, már Euklidész bizonyította, viszont a mai napig nem tudjuk, hogy az ikerprímek száma véges, vagy végtelen(p_1, p_2 prímek ikerprímek, ha $|p_1 - p_2| = 2$). Nagyon valószínű, hogy az x-nél kisebb ikerprímek száma aszimptotikusan $cx/(\ln^2 x)$, alkalmas c konstanssal. Brun 1919-ben megmutatta, hogy az ikerprímek reciprokösszege konvergens sort alkot. Ez a tény arra utal, hogy ha nincsenek is feltétlenül véges sokan az ikerprímek, de egyre ritkábban fordulnak elő a végtelen felé haladva. A szám, amihez az előbb említett sor konvergál,

$$B = 1.9021605823\ldots,$$

az úgynevezett Brun-konstans. B értékének minél pontosabb meghatározása már a prímrekordok problémakörébe tartozik. Ezen a területen kerülnek terítékre olyan feladatok, mint például: keressünk minél nagyobb, bizonyos tulajdonságokkal rendelkező prímeket, vagy ellenőrizzük egy sejtés helyességét számítógéppel a lehető legnagyobb korlátig. Az egyik ilyen probléma páros Goldbach-sejtés néven vált híressé. 1742-ben egy Eulernek írott levelében vetette fel a gondolatot Goldbach,

miszerint minden $n > 5$ egész szám felírható három prím összegeként. Euler válaszában megírta, hogy ez a probléma ekvivalens azzal, hogy bármely háromnál nagyobb páros egész szám felírható-e két prím összegeként. A „páros" megkülönböztetés azért ragadt a Goldbach-sejtésre, mert korábban a matematikus egy másik gondolata, amely szerint minden 5-nél nagyobb páratlan szám előáll három prím összegeként, kapta a páratlan Goldbach-sejtés elnevezést. Megjegyezzük, hogy általában a páros eset vizsgálata van napirenden, mivel ebből rögtön következik a páratlan eset. Vinogradov 1937-ben bebizonyította a páratlan Goldbach-sejtést „nagy számokra". Sajnos nagy számon, a későbbi tökéletesítések ellenére is 10 a több ezrediken nagyságrendet kell értenünk. Az a tény, hogy számítógéppel a Goldbach-sejtés 2004-ben körülbelül 10^{17} nagyságrendig ellenőrzött, jól mutatja, hogy van még mit „lefaragni" az elméleti korlátból.

Talán a két legfontosabb prímszámokkal kapcsolatos fogalom a faktorizáció és a prímtesztelés. Előbbi azt jelenti, hogy adott számot megpróbálunk felbonthatatlanok szorzataként felírni. Meglepő lehet, hogy a két probléma megoldásának bonyolultsága mennyire eltérő. Míg prímteszt eredményesen végezhető több ezer jegyű számokra is, addig a prímfaktorizációt legfeljebb 150-200 jegyű számokra hajthatjuk végre, legalábbis ez a helyzet 2005-ben. A legmodernebb titkosítási eljárások is azon alapulnak, hogy nagy számokat prímek szorzatára bontani „nehéz" feladat.

2.2. Prímszámok karakterizációi

2.2.1. Tétel. *(kis Fermat-tétel)* $\forall p \in P, (p,a) = 1 : a^{p-1} \equiv 1 \ (mod\ p)$

A tétel speciális esete az Euler-Fermat tételnek:

2.2.2. Tétel. *(Euler-Fermat) Ha* $(a,m) = 1$, *akkor* $a^{\varphi(m)} \equiv 1 \ (mod\ m)$.

Bizonyítás: Jelölje rendre $r_1, r_2, \ldots, r_{\varphi(m)}$ a redukált maradékosztályokat $(mod\ m)$. Ha ezeket rendre beszorozzuk a-val, kapjuk: $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(m)}$. Azt állítjuk, hogy a kapott maradékosztályok páronként különbözőek:
ha valamely i, j-re $a \cdot r_i \equiv a \cdot r_j \ (mod\ m)$, akkor $a \cdot (r_i - r_j) \equiv 0 \ (mod\ m)$, s mivel a relatív prím m-hez, ezért $m \mid r_i - r_j$, de ez ellentmond annak, hogy r_i és r_j különböző volt $(mod\, m)$. Ezek szerint az $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(m)}$ maradékosztályok sorrendtől eltekintve megegyeznek $r_1, r_2, \ldots, r_{\varphi(m)}$-mel, és ezért a szorzataik megegyeznek:

$$r_1 \cdot r_2 \cdots r_{\varphi(m)} \equiv a \cdot r_1 \cdot a \cdot r_2 \cdots a \cdot r_{\varphi(m)} \ (mod\ m)$$

Ezt rendezve:

$$r_1 \cdot r_2 \cdots r_{\varphi(m)} \left(a^{\varphi(m)} - 1 \right) \equiv 0 \ (mod\ m)$$

s mivel $r_1 \cdot r_2 \cdots r_{\varphi(m)}$ relatív prím m-hez, ezért $m \mid a^{\varphi(m)} - 1$, és pont ezt kellett bizonyítanunk.

Ha m-et prímnek választjuk, akkor $\varphi(m) = m - 1$, és így azt kapjuk, hogy:

$$a^{m-1} \equiv 1 \ (mod\ m),$$

ami pont a kis Fermat-tétel állítása.

2.2.3. Tétel. *Wilson-tétel:* $n \in P \iff (n-1)! \equiv -1 \ (mod\ n)$

Bizonyítás: Először tegyük fel, hogy $n \in \mathbb{N}$ összetett szám. Ekkor van olyan $d \in \mathbb{N}$ osztója, amelyre $1 < d < n$, és így $d \mid (n-1)!$. Tehát $d \nmid (n-1)!+1$ fennáll, következésképpen $n \nmid (n-1)!+1$, azaz kaptuk, hogy $(n-1)! \not\equiv -1 \ (mod\ n)$.

Most legyen n prímszám! Ha $n = 2$, akkor $(2-1)! = 1 \equiv -1 \ (mod\ 2)$ fennáll, tehát feltehetjük a továbbiakban, hogy $n > 2$. Tudjuk, hogy az $ax \equiv 1 \ (mod\ n)$ kongruenciának pontosan egy megoldása van, ha $(a, n) = 1$. Ez n prím volta miatt teljesül minden $1 \leq a \leq n-1$ esetén. Vegyük észre, hogy $a \equiv a^{-1} \ (mod\ n)$ csak az $a \equiv 1 \ (mod\ n)$ és $a \equiv n-1 \ (mod\ n)$ esetben fordulhat elő. Mivel $\prod_{a=1}^{n-1} a \equiv \prod_{a=1}^{n-1} a^{-1} \ (mod\ n)$ fennáll, és a bal, illetve jobb oldalon lévő tényezőkkel, kivéve $a = 1$ és $a = n-1$ értékeket, egyszerűsíthetünk, tehát kapjuk, hogy $(n-1)! \equiv n-1 \equiv -1 \ (mod\ n)$, amivel az állítást bizonyítottuk.

A Wilson-tétel jó összefüggést ad prímszámok felismerésére, hiszen egyetlen összetett számra sem teljesül, viszont prímtesztelésre sajnos nem használható, mert $(n-1)! \ (mod\ n)$ nem számolható gyorsan.

2.2.4. Tétel. *Legyen* $a, n \in \mathbb{Z}$, *melyekre* $n \geq 2$ *és* $(a, n) = 1$ *fennáll. Ekkor* n *akkor és csak akkor prím, ha*

$$(x+a)^n \equiv x^n + a \ (mod\ n). \tag{2.1}$$

Bizonyítás: Tehát a feladatunk az $f(x) = (x+a)^n - (x^n + a)$ polinom együtthatóinak vizsgálata $(mod\ n)$. Rögtön adódik, hogy $f(x)$ konstans tagja, illetve x^n együtthatója 0, továbbá $0 < i < n$ esetén minden x^i a binomiális tétel értelmében $\binom{n}{i} \cdot a^{n-i}$-nel szorzódik. Az

$$\binom{n}{i} = \frac{n!}{i! \cdot (n-i)!}$$

kifejezés mindig egész számot szolgáltat, tehát $i! \cdot (n-i)!$ osztója $n!$-nak.

Most tegyük fel, hogy n prímszám. Ekkor n nem osztója $i!$ és $(n-i)!$ egyetlen tényezőjének sem, tehát $(n, i! \cdot (n-i)!) = 1$, ami azt jelenti, hogy $i! \cdot (n-i)!$ osztója $(n-1)!$-nak. Kaptuk, hogy minden $\binom{n}{i}$ kifejezés alkalmas $b \in \mathbb{Z}$ elemmel $n \cdot b$ alakban írható fel, ami kongruens 0-val $(mod\ n)$.

Most azt az esetet vizsgáljuk, amikor n összetett. Bontsuk fel n-et prímhatványok szorzatára, és válasszunk a tényezők közül egy p^k számot, amire $p^k || n$. Ekkor p^k relatív prím a^{n-p}-hez és nem osztója $\binom{n}{p}$-nek. Ez azt jelenti, hogy $f(x)$-ben az x^p-es tag együtthatója nem osztható n minden faktorával, azaz n-nel sem, így:

$$\binom{n}{p} \cdot a^{n-p} \not\equiv 0 \ (mod\ n).$$

Tehát, ha n nem prímszám, akkor $f(x)$-nek lesz 0-tól különböző együtthatója, így nem lehet null-polinom $\mathbb{Z}_n$ felett.

Ez a tétel az utolsó fejezetben szereplő AKS-algoritmus alapja.

Megjegyzés: A gyerekek a binomiális tételt gyakran rosszul jegyzik meg, és úgy gondolják, hogy $(x+y)^n = x^n + y^n$; ezt nevezték el a "gyerekek binomiális tételének". A tétel alapján teljesül az egyenlőség $(mod\ n)$, ha n prímszám.

2.3. Speciális prímszámok

Mersenne-prímek

Vizsgáljuk meg, hogy egy $2^n - 1$ alakú szám mikor lehet prímszám.

2.3.1. Állítás. *Ha $2^n - 1$ prímszám, akkor n prím.*

Bizonyítás: Ha $n = d \cdot k$, akkor $2^n - 1 = (2^d - 1) \cdot (2^{d(k-1)} + 2^{d(k-2)} + \cdots + 1)$. Tehát $2^d - 1 \mid 2^n - 1$, ha $d \mid n$.

2.3.2. Definíció. *A $2^n - 1$ alakú számokat Mersenne-számoknak nevezzük, és $M(n)$-nel jelöljük*

2.3.3. Definíció. *A $2^n - 1$ alakú prímeket Mersenne-prímeknek nevezzük.*

A ma ismert legnagyobb prímek közül a legtöbb, köztük a legnagyobb is Mersenne-prím: $2^{25.964.951} - 1$-nek 7.816.230 számjegye van, ez a 42. ismert Mersenne-prím, és 2005. február 18-án találta Dr. Martin Nowak.

Fermat-prímek

Nézzük meg, mi a helyzet a $2^n + 1$ alakú számokkal:

2.3.4. Állítás. *Ha $2^n + 1$ prímszám, akkor $n = 2^m$ alakú.*

Bizonyítás: $2^{q \cdot 2^m} + 1 = (2^{2^m} + 1) \cdot (2^{2^m \cdot (q-1)} - 2^{2^m \cdot (q-2)} + \cdots + 2^0)$

2.3.5. Definíció. *A $2^{2^n} + 1$ alakú számokat Fermat-számoknak nevezzük, és $F(n)$-nel jelöljük.*

2.3.6. Definíció. *A $2^{2^n} + 1$ alakú prímeket Fermat-prímeknek nevezzük.*

$F(0) = 3,\ F(1) = 5,\ F(2) = 17,\ F(3) = 257,$ és $F(4) = 65537$ prímek, ez alapján Fermat azt a sejtést állította fel, hogy az összes Fermat-szám prím. Ez nem igaz, hiszen $F(5) = 4.294.967.297 = 641 \cdot 6.700.417$, sőt az előzőeken kívül nem ismerünk Fermat-prímet.

Pillai-prímek

A Wilson-tételből következik, hogy $p \mid (p-1)! + 1$, ha p prím. Tehát p osztója $f(p-1) = (p-1)! + 1$-nek, és $p \equiv 1 \ (mod\ p-1)$. Felvetődhet a kérdés, hogy vajon $f(n) = n! + 1$ minden q prímosztójára teljesül-e a $q \equiv 1 \ (mod\ n)$ összefüggés. A helyzet az, hogy $1 \leq n \leq 7$-re igaz az állítás, de $n = 8$-ra már nem, ugyanis $8! + 1$-et osztja 61 és 661 is, viszont egyikük sem $\equiv 1 \ (mod\ 8)$.

2.3.7. Definíció. *A p prímet Pillai-prímnek nevezzük, ha található hozzá $n \in \mathbb{N}$ úgy, hogy $p \mid n!+1$ és $p \not\equiv 1 (mod\ n)$.*

Az első 15 Pillai-prím: 23,29,59,61,67,71,79,83,109,137,139,149,193,227,233.
Egy egyszerű algoritmussal találhatunk Pillai-prímeket.

2.3.8. Tétel. *Végtelen sok Pillai-prím van.*

3. fejezet

Valószínűségi prímtesztek

A kis Fermat-tételre alapozva születtek gyors futási idejű valószínűségi prímtesztek. Ezeknek az elve az, hogy $n > 2$ egész számra, ha

$$2^{n-1} \not\equiv 1 \ (mod\ n),$$

akkor n összetett. A

$$2^{n-1} \equiv 1 \ (mod\ n),$$

esetben nem mondhatjuk biztosan, hogy n nem prím. A gyakorlatban a valószínűségi tesztek jól használhatónak bizonyultak gyorsaságuk miatt, és amiatt, hogy kevés olyan összetett szám van, ami „átmegy" a teszten prím minősítéssel. Ezek a nem prímszámok, amelyek mégis prímként viselkednek bizonyos szituációkban, elrontva például prímtesztek determinisztikusságát, fontos szerepet játszanak a számelméleti kutatásokban, így nevesítjük is őket.

3.0.9. Definíció. *Az n páratlan összetett számot a alapú pszeudoprímnek, vagy álprímnek nevezzük, ha*

$$a^{n-1} \equiv 1 \ (mod\ n)$$

fennáll. Az n összetett számot Carmichael-számnak, vagy univerzális álprímnek nevezzük, ha minden $(a, n) = 1$ esetben fennáll az

$$a^{n-1} \equiv 1 \ (mod\ n)$$

kongruencia.

3.0.10. Tétel. *Az $n \in \mathbb{N}$ összetett páratlan szám akkor és csak akkor Carmichael-szám, ha az $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ prímtényezős felbontásban $\alpha_1 = \alpha_2 = \dots = \alpha_r = 1$, $r \geq 3$ és $p_i - 1 \mid n - 1$ $(i = 1, 2, \dots, r)$ teljesül.*

Carl Pomerance bizonyította az állítást, miszerint végtelen sok Carmichael-szám létezik.

Példa: az $n = 91 = 7 \cdot 13$ szám 3 alapú pszeudoprím, de nem pszeudoprím a 2 alaphoz. Az $n = 561 = 3 \cdot 11 \cdot 17$ Carmichael-szám.

3.1. A Miller-Rabin teszt

Ebben a részben egy gyors(polinomiális idejű) prímtesztről, a Miller-Rabin tesztről lesz szó. Ez egy valószínűségi algoritmus, előfordulhat(csak kis valószínűséggel), hogy hibázik.

A fejezet további részére feltesszük, hogy az általunk tesztelni kívánt n egy 1-nél nagyobb páratlan egész.

Néhány valószínűségi prímteszt, beleértve a Miller-Rabin tesztet is, a következő általános struktúrával rendelkezik. Jelöljük $\mathbb{Z}_n^+$-szal $\mathbb{Z}_n$ nemnulla elemeit; így: $|\mathbb{Z}_n^+| = n-1$, és ha n prím, akkor $\mathbb{Z}_n^+ = \mathbb{Z}_n^*$. Definiáljuk továbbá az $L_n \subset \mathbb{Z}_n^+$ halmazt a következőképpen:

- Létezik egy hatékony algoritmus annak eldöntésére, hogy adott n, és $\alpha \in \mathbb{Z}_n^+$ esetén $\alpha \in L_n$ teljesül-e
- Ha n prím, akkor $L_n = \mathbb{Z}_n^*$
- Ha n összetett, akkor $|L_n| \leq c \cdot (n-1)$ valamilyen $c < 1$ konstansra

n prímségének teszteléséhez beállítunk egy t "hibaparamétert", és véletlenszerűen választunk $\alpha_1, \ldots, \alpha_t \in \mathbb{Z}_n^+$-t. Ha $\alpha_i \in L_n$ minden $i = 1, \ldots, t$, akkor az output "igaz", különben pedig "hamis".

Könnyen látható, hogy ha n prím, akkor az algoritmus mindig "igaz" értékkel tér vissza, ha pedig összetett, akkor legfeljebb c^t valószínűséggel. Ha $c = 1/2$, és t-t elég nagynak választjuk, mondjuk $t = 100$, akkor a tévedés valószínűsége elhanyagolhatóan kicsi.

Teszünk egy kísérletet megfelelő L_n halmaz definiálására. Legyen:

$$L_n := \{\alpha \in \mathbb{Z}_n^+ : \ \alpha^{n-1} = 1\}.$$

Tudjuk, hogy $L_n \subset \mathbb{Z}_n^*$, mivel ha $\alpha^{n-1} = 1$, akkor α-nak létezik multiplikatív inverze, mégpedig α^{n-2}. A gyors hatványozást használva annak eldöntése, hogy $\alpha \in L_n$ $O((\log n)^3)$ műveletet igényel.

3.1.1. Tétel. *Ha n prím, akkor $L_n = \mathbb{Z}_n^*$. Ha n összetett, és $L_n \subsetneq \mathbb{Z}_n^*$, akkor $|L_n| \leq (n-1)/2$.*

Bizonyítás: Vegyük észre, hogy L_n a $\mathbb{Z}_n^*$-beli $(n-1)$-edik hatványleképzés magja, és ezért $\mathbb{Z}_n^*$ részcsoportja.

Ha n prímszám, akkor $\mathbb{Z}_n^*$ rendje $n-1$. Mivel a csoport rendje többszöröse az elemeinek rendjének, ezért $\alpha^{n-1} = 1$ teljesül bármely $\alpha \in \mathbb{Z}_n^*$, és így $L_n = \mathbb{Z}_n^*$.

Most tegyük fel, hogy n összetett, és $L_n \subsetneq \mathbb{Z}_n^*$. Mivel részcsoport rendje osztója a csoport rendjének, ezért $|\mathbb{Z}_n^*| = m \cdot |L_n|$, valamely $m > 1$ egészre. Ebből pedig következik, hogy:

$$|L_n| = \frac{1}{m}|\mathbb{Z}_n^*| \leq \frac{1}{2}|\mathbb{Z}_n^*| \leq \frac{n-1}{2}.$$

Sajnos vannak olyan páratlan összetett számok, amelyekre $L_n = \mathbb{Z}_n^*$. Ezek a Carmichael-számok.

Ahhoz, hogy egy jó prímtesztet kapjunk, egy új, $L_n^{'}$ halmazt kell definiálnunk, amit a következőképpen teszünk meg. Legyen $n-1 = 2^h \cdot m$, ahol m páratlan és $h \geq 1$, és legyen

$$L_n^{'} := \{\alpha \in \mathbb{Z}_n^+ : \ \alpha^{m \cdot 2^h} = 1, \text{ és } \alpha^{m \cdot 2^{j+1}} = 1 \Rightarrow \alpha^{m \cdot 2^j} = \pm 1, \text{ ha } j \in \{0, \ldots, h-1\}\}.$$

A Miller-Rabin teszt ezt az $L_n^{'}$ halmazt használja L_n helyett. A definícióból adódik, hogy $L_n \subseteq L_n^{'}$.

Annak eldöntése, hogy $\alpha \in \mathbb{Z}_n^+$ $L_n^{'}$-höz tartozik-e a következő eljárással ellenőrizhető:

$\beta \leftarrow \alpha^m$

if $\beta = 1$ then return **true**

for $j \leftarrow 0$ to $h-1$ do

if $\beta = -1$ then return **true**

if $\beta = +1$ then return **false**

$\beta \leftarrow \beta^2$

false

Világos, hogy ismételt négyzetreemelést használva az eljárás műveletigénye $O((\log n)^3)$.

3.1.2. Tétel. *Ha n prím, akkor $L_n^{'} = \mathbb{Z}_n^*$. Ha n összetett, akkor $|L_n^{'}| \leq (n-1)/4$.*

Bizonyítás:

1.eset: ha n prím.

Legyen $\alpha \in \mathbb{Z}_n^*$. Mivel $\mathbb{Z}_n^*$ rendje $n-1$, és elem rendje osztja a csoport rendjét, ezért $\alpha^{m \cdot 2^h} = \alpha^{n-1} = 1$. Most tekintsük valamely $j \in \{1, \ldots, h-1\}$ indexet, amire $\alpha^{m \cdot 2^{j+1}} = 1$, és legyen $\beta := \alpha^{m \cdot 2^j}$. Mivel $\beta^2 = \alpha^{m \cdot 2^{j+1}} = 1$, ezért β lehetséges értékei: ± 1. Ez azért van, mert $\mathbb{Z}_n^*$ páros rendű ciklikus csoport, ezért pontosan két elem van, aminek a rendje osztja 2-t, ezek pedig $+1$ és -1. Tehát $L_n^{'} = \mathbb{Z}_n^*$.

2.eset: $n = p^e$, ahol p prím és $e > 1$.

$L_n^{'}$-t tartalmazza a $\mathbb{Z}_n^*$-beli $n-1$-edik hatványleképezés K magja. Tudjuk, hogy $|K| = lnko(\varphi(n), n-1)$. Mivel $n = p^e$, ezért $\varphi(n) = p^{e-1} \cdot (p-1)$, és így

$$|L_n^{'}| \leq |K| = lnko(p^{e-1} \cdot (p-1), p^e - 1) = p - 1 = \frac{p^e - 1}{p^{e-1} + \cdots + 1} \leq \frac{n-1}{4}.$$

3.eset: $n = p_1^{e_1} \cdots p_r^{e_r}$ n prímfelbontása, $r > 1$.

Jelölje R_i, $i = 1, \ldots, r$ a $\mathbb{Z}_{p_i^{e_i}}$ gyűrűt, és legyen

$$\theta : R_1 \times \cdots \times R_r \to \mathbb{Z}_n$$

a kínai maradéktétel által adott gyűrűizomorfizmus. Legyen még $\varphi(p_i^{e_i}) = m_i \cdot 2^{h_i}$, ahol m_i páratlan, $i = 1, \ldots, r$-re, és $l := \min\{h, h_1, \ldots, h_r\}$. Vegyük észre, hogy $l \geq 1$, és minden egyes R_i^* $m_i \cdot 2^{h_i}$ rendű ciklikus csoport.

Először belátjuk, hogy ha $\alpha \in L_n^{'}$, akkor $\alpha^{m \cdot 2^l} = 1$. Ennek a belátásához először vegyük észre, hogy ha $l = h$, akkor definíció szerint $\alpha^{m \cdot 2^l} = 1$, ezért tegyük fel, hogy $l < h$. Indirekt tegyük fel, $\alpha^{m \cdot 2^l} \neq 1$, és legyen j a legkisebb index az $l, \ldots, h-1$ tartományból, amire $\alpha^{m \cdot 2^{j+1}} = 1$. $L_n^{'}$ definíciója miatt $\alpha^{m \cdot 2^j} = -1$. Mivel $l < h$, ezért $l = h_i$ valamely $i \in \{1, \ldots, r\}$ indexre. $\alpha = \theta(\alpha_1, \ldots, \alpha_r)$ esetén $\alpha_i^{m \cdot 2^j} = -1$. Ebből az következtetik, hogy α_i^m multiplikatív rendje 2^{j+1}. Mivel $j \geq l = h_i$, ezért ellentmondáshoz jutunk, mert egy csoport elemének (ebben az esetben α_i^n-nek) a rendje osztója a csoport (jelen esetben R_i^*) rendjének.

Az előző bekezdés állításából, és $L_n^{'}$ definíciójából következik, hogy $\alpha \in L_n^{'}$ implikálja $\alpha^{m \cdot 2^{l-1}} = \pm 1$ összefüggést. Most tekintsünk egy kísérletet, melyben α-t véletlenül választjuk $\mathbb{Z}_n^*$-ból (egyenletes eloszlás szerint), és megmutatjuk, hogy ekkor $P(\alpha^{m \cdot 2^{l-1}} = \pm 1) \leq 1/4$, amiből következik a tétel.

Legyen $\alpha = \theta(\alpha_1, \ldots, \alpha_r)$. Mivel α egyenletes eloszlású $\mathbb{Z}_n^*$-on, ezért α_i egyenletes eloszlású R_i^*-on, és az α_i-k függetlenek. Jelölje $i = 1, \ldots, r$-re és $j = 0, \ldots, h$-ra $G_i(j)$ az $m \cdot 2^j$-edik hatványleképezés képét R_i^*-on. Tudjuk, hogy

$$|G_i(j)| = \frac{m_i \cdot 2^{h_i}}{lnko(m_i \cdot 2^{h_i}, m \cdot 2^j)}.$$

Mivel $l \leq h$ és $l \leq h_i$, egyszerű számolással kapjuk, hogy:

$$|G_i(h)| \mid |G_i(l)| \text{ és } 2|G_i(l)| = |G_i(l-1)|.$$

Azaz $G_i(l-1)$ páros, és nem kisebb, mint $2|G_i(h)|$. Abból, hogy $G_i(l-1)$ páros következik, hogy $-1 \in G_i(l-1)$. Az $\alpha^{m \cdot 2^{l-1}} = \pm 1$ esemény pontosan akkor lép fel, ha
(E_1) $\alpha^{m \cdot 2^{l-1}} = 1$ $i = 1, \ldots, r$ vagy
(E_2) $\alpha^{m \cdot 2^{l-1}} = -1$ $i = 1, \ldots, r$.
Mivel az (E_1) és (E_2) események diszjunktak, és mivel az $\alpha^{m \cdot 2^{l-1}}$ értékek függetlenek, és $\alpha^{m \cdot 2^{l-1}}$ egyenletes eloszlású $G_i(l-1)$-en, és $G_i(l-1)$ tartalmazza ± 1-et, ezért azt kapjuk, hogy:

$$P(\alpha^{m \cdot 2^{l-1}} = \pm 1) = P(E_1) + P(E_2) = 2 \prod_{i=1}^{r} \frac{1}{|G_i(l-1)|},$$

és mivel $|G_i(l-1)| \geq 2|G_i(h)|$, ezért

$$P(\alpha^{m \cdot 2^{l-1}} = \pm 1) \leq 2^{-r+1} \prod_{i=1}^{r} \frac{1}{|G_i(h)|}. \tag{3.1}$$

Ha $r \geq 3$, akkor 3.1 közvetlenül implikálja, hogy $P(\alpha^{m \cdot 2^{l-1}} = \pm 1) \leq 1/4$, és kész vagyunk. Tegyük fel, hogy $r = 2$. Ekkor n nem lehet Carmichael-szám, ezért valamely $i \in \{1, \ldots, r\}$-re $G_i(h) \neq \{1\}$, így $|G_i(h)| \geq 2$, és ekkor 3.1-ből ismét következik $P(\alpha^{m \cdot 2^{l-1}} = \pm 1) \leq 1/4$, és ezzel befejeztük a bizonyítást.

3.2. A Solovay-Strassen teszt

3.2.1. A Legendre- és Jacobi-szimbólumok

3.2.1. Definíció. *Legyen $p > 2$ prím és $(a, p) = 1$. Ekkor az a számot kvadratikus maradéknak nevezzük, ha megoldható az*

$$x^2 \equiv a \ (mod\ p)$$

kongruencia, és kvadratikus nemmaradéknak, ha nem oldható meg.

Megjegyezzük, hogy az $a \equiv 0 \ (mod\ p)$ számokat egyik kategóriába sem soroljuk be.

3.2.2. Definíció. *Legyen p páratlan prím. A Legendre-szimbólumot $\left(\frac{a}{p}\right)$-vel jelöljük, és a következőképpen definiáljuk:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & , \text{ ha } p \mid a \\ 1 & , \text{ ha } a \text{ kvadratikus maradék } (mod\ p) \\ -1 & , \text{ ha } a \text{ kvadratikus nemmaradék } (mod\ p) \end{cases}$$

Világos, hogy $a_1 \equiv a_2 \ (mod\ p)$ esetén $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right)$, továbbá

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

A Legendre-szombólum azon tulajdonságát, amely több valószínűségi prímtesztelő algoritmus alapját képezi, Euler-kritériumnak nevezik.

3.2.3. Lemma. *(Euler) Bármely $p > 2$ prímre és $0 < a < p$-re*

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

Nagy számok prímtesztelésénél gyakran használjuk a Legendre-szimbólum általánosítás tetszőleges egész számra:

3.2.4. Definíció. *Legyen $m = p_1 \cdot p_2 \cdots p_n$ páratlan egész, ahol p_i-k nem feltétlenül különböző prímek, és $(a, m) = 1$. Ekkor a következő szorzatot Jacobi-szimbólumnak nevezzük:*

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

Vegyük észre, hogy prímszámokra a Legendre- és Jacobi-szimbólum megegyezik. Könnyen belátható az alábbi hét állítás, melyek segítségével egyszerűen kiszámolhatjuk a Jacobi-szimbólumot:

(1) $a \equiv b \ (mod\ m) \Longrightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

(2) $\left(\frac{a \cdot b}{m}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{b}{m}\right)$

(3) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$

(4) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$

(5) $\left(\frac{a}{m}\right) \cdot \left(\frac{a}{m'}\right) = \left(\frac{a}{m \cdot m'}\right)$

(6) $\left(\frac{a^2}{m}\right) = \left(\frac{a}{m^2}\right)$

(7) $\left(\frac{a}{m}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{m-1}{2}} \cdot \left(\frac{m}{a}\right)$

3.2.2. A Solovay-Strassen-teszt

Az Euler-kritérium vizsgálatán alapszik a Solovay-Strassen-teszt néven ismert eljárás, amelynek ismertetésénél felhasználjuk a JACOBI(A,N) eljárást, ami kiszámolja az $\left(\frac{a}{m}\right)$ Jacobi-szimbólumot, illetve a RANDOM(X,Y) függvényt, ami egy véletlen számot ad az $[x, y]$ intervallumból.

SOLOVAY-STRASSEN-PRÍMTESZT(N)

1. $d \leftarrow$ RANDOM(1,N)
2. if $a^{(n-1)/2} \not\equiv$ JACOBI(A,N) $(mod\ n)$
3. then return ÖSSZETETT
4. else return VALÓSZÍNŰLEG PRÍM

Az eljárás érdekessége, hogy valójában valószínűségi teszt, de a szerzők megmutatták, hogy csak véges sok összetett szám esetén „téved", azaz n bemeneti érték esetén legfeljebb $(n-1)/2$ összetett szám elégíti ki a vizsgált kongruenciát. Ez azt jelenti, hogy az algoritmus megfelelő számú ismétléssel és megfelelően választott a értékekkel tetszőlegesen megbízhatóvá tehető.

4. fejezet

Prímtesztek speciális alakú prímek esetén

4.1. Mersenne-prímek

4.1.1. Tétel. *Legyen p prím, $s_1 = 4$, $s_k = s_{k-1}^2 - 2$, $k = 1, 2, \ldots$. Az $M(p)$ szám akkor és csak akkor prím, ha $M(p)$ az s_{p-1} osztója.*

Bizonyítás: Először néhány segédtételt és észrevételt közlünk. Legyen $\alpha = 1 + \sqrt{3}$, $\overline{\alpha} = 1 - \sqrt{3}$, továbbá $E_n := \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}}$, $F_n := \alpha^n + \overline{\alpha}^n$. Nyilvánvaló, hogy $\alpha + \overline{\alpha} = 2$ és $\alpha\overline{\alpha} = -2$. A binomiális tételből következik, a (0) észrevétel.

(0) $E_n = \binom{n}{1} + \binom{n}{3} \cdot 3 + \binom{n}{5} \cdot 3^2 + \ldots$, $F_n = 2 \cdot \left\{1 + \binom{n}{2} \cdot 3 + \binom{n}{4} \cdot 3^2 + \ldots\right\}$
(1) $2E_{k+l} = E_k \cdot F_l + F_k \cdot E_l$
(2) $(-2)^{l+1} \cdot E_{k-l} = E_l \cdot F_k - E_k \cdot F_l \qquad k > l$
(3) $E_{2k} = E_k \cdot F_k$
(4) $F_{2k} = F_k^2 + (-2)^{k+1}$
(5) $F_k^2 - 12E_k^2 = (-2)^{k+2}$
(6) $2F_{k+l} = F_k \cdot F_l + 12E_k \cdot E_l$

Adott páratlan q prímre jelölje $\omega(q)$ azt az n legkisebb pozitív egész számot, amelyre $q | E_n$. Ha nincs ilyen n, akkor $\omega(q) = \infty$.

4.1.2. Lemma. *Legyen $S = \{\nu \in \mathbb{N},\ q \mid E_\nu\}$. Ekkor*

$$S = \{k \cdot \omega(q) \mid k \in \mathbb{N}\}.$$

Bizonyítás: Ha $k, l \in S$, akkor (1) és (2) miatt $k + l$, és $k > l$ esetén $k - l \in S$. Ezért $\omega(q)$ többszörösei S-hez tartoznak. Tegyük fel indirekt módon, hogy létezik $m \in S$, amelyre $\omega(q) \nmid m$. Ekkor $m = l \cdot \omega(q) + r$, $0 < r < \omega(q)$, és $m \in S$, $l \cdot \omega(q) \in S$ miatt

$$m - l \cdot \omega(q) = r \in S.$$

Ez ellentmond $\omega(q)$ definíciójának.

4.1.3. Lemma. *Ha $q > 3$ prím, akkor*
(7) $q | E_q - 3^{\frac{q-1}{2}}$,
és
(8) $q | F_q - 2$

Bizonyítás: (0) és $q \mid \binom{q}{j}$ $1 \leq j \leq q-1$ miatt

$$E_q \equiv \binom{q}{q} \cdot 3^{\frac{q-1}{2}} \equiv 3^{\frac{q-1}{2}} \ (mod\ q)$$

valamint

$$F_q \equiv 2 \ (mod\ q).$$

4.1.4. Lemma. *Ha $q > 3$ prím, és $\omega(q)$ létezik, akkor*

$$\omega(q) \leq q + 1.$$

Bizonyítás: $E_1 = 1$, $F_1 = 2$. Alkalmazzuk a az (1) és (2) egyenlőségeket $k = q$ és $l = 1$ választással. Ekkor $2E_{q+1} = 2E_q + F_q$, $-4E_{q-1} = 2E_q - F_q$, azaz

$$-8E_{q-1} \cdot E_{q+1} = 4E_q^2 - F_q^2 \equiv 4 \cdot 3^{q-1} - 4 \equiv 0 \ (mod\ q)$$

s ezért

$$q \mid E_{q-1} \cdot E_{q+1},$$

amivel a lemma bizonyítását befejeztük.

4.1.5. Lemma. *Ha $p \equiv 7 \ (mod\ 12)$, akkor $\left(\frac{3}{p}\right) = -1$, és így*

$$p \mid 3^{\frac{p-1}{2}} + 1.$$

Bizonyítás: Legyen $p \equiv 7 \ (mod\ 12)$. Ekkor

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} \cdot \left(\frac{p}{3}\right) = -1 \cdot \left(\frac{p}{3}\right) = -1.$$

Most rátérünk a tétel elegendőségének bizonyítására. Legyen p páratlan prím, és $M(p) \mid s_{p-1}$. Ekkor
(9) $M(p) \mid 2^{2^{p-2}} \cdot s_{p-1}$.
Belátjuk, hogy $F_{2^n} = 2^{2^{n-1}} \cdot s_n$ $(n = 1, 2, \dots)$. Mivel $2s_1 = F_2$, ez igaz, ha $n = 1$. Tegyük fel, hogy beláttuk az állítást n-ig. Mivel $s_{n+1} = s_n^2 - 2$, ezért

$$2^{2^n} \cdot s_{n+1} = (2^{2^{n-1}} \cdot s_n)^2 - 2^{2^n+1}.$$

(4) miatt $k = 2^n$-re:

$$F_{2^{n+1}} = F_{2^n}^2 - 2^{2^n+1},$$

ezért

$$F_{2^{n+1}} = 2^{2^n} \cdot s_{n+1},$$

így $n = p-1$-re

(10) $2^{2^{p-2}} \cdot s_{p-1} = F_{2^{p-1}}$.

Ekkor (9) és (10) miatt

(11) $M(p) \mid F_{2^{p-1}}$,

ahonnan (3)-at $k = 2^{p-1}$-re alkalmazva kapjuk, hogy

(12) $M(p) | E_{2^p}$.

Legyen most q prím, $q \mid M(p)$. Ekkor $q \neq 2, 3$, tehát $q > 3$. (12) miatt $q \mid E_{2^p}$. Ekkor 4.1.2 miatt $\omega(q) \mid 2^p$. Ha $\omega(q) \neq 2^p$ teljesülne, akkor $\omega(q) \mid 2^{p-1}$ lenne, és így $q \mid E_{2^{p-1}}$ fennállna. Ekkor (11) és (5) miatt q valamely 2-hatvány osztója lenne, ami nem lehet. Tehát $\omega(q) = 2^p$. 4.1.4 miatt $2^p \leq q+1$, azaz $q \geq 2^p - 1 = M(p),\ q | 2^p - 1$, és így $q = M(p)$, amivel az elégségességet beláttuk.

A tétel szükségességének bizonyításához legyen $p > 2$, $M(p) = q$ prím. Ekkor $8 \mid 2^p = q+1$, $q \equiv 7\ (mod\ 8)$. Mivel p páratlan, ezért

$$q = 2^p - 1 \equiv 2 - 1 \equiv 1\ (mod\ 3),$$

és így $q \equiv 7\ (mod\ 24)$, azaz $q = 24r + 7$ alakban írható alkalmas $r \in \mathbb{N}_0$-ra. Alkalmazzuk (4)-et $k = 2^{p-1}$ választással. Ekkor:

(13) $F_{2^p} = F_{2^{p-1}}^2 - 4 \cdot 2^{2^{p-1}-1}$.

Mivel $q = 24r + 7 = 8 \cdot 3r + 7$, ezért

$$q \mid M\left(\frac{q-1}{2}\right) = 2^{\frac{q-1}{2}} - 1.$$

Ez a

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = 1$$

és a

$$2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right)\ (mod\ q)$$

formulából azonnal következik. Mivel $M\left(\frac{q-1}{2}\right) = M(2^{p-1} - 1)$, ezért $q \mid 2^{2^{p-1}-1} - 1$, ahonnan

(14) $q \mid F_{2^p} - F_{2^{p-1}}^2 + 4$.

(6)-ot $k = q$ és $l = 1$ választással alkalmazva, $q + 1 = 2^p$ miatt:

$$2F_{2^p} = F_q F_1 + 12 E_q E_1 = 2F_q + 12E_q.$$

Tehát

(15) $F_{2^p} = F_q + 6E_q = (F_q - 2) + 6(E_q + 1) - 4$.

A 4.1.5 miatt $q \mid 3^{\frac{q-1}{2}} + 1$, továbbá (7) miatt $q \mid E_q + 1$, (8) miatt $q | F_q - 2$. Ezért (15) miatt $q \mid F_{2^p} + 4$, és így (14) miatt $q \mid F_{2^{p-1}}^2$. (10) miatt, $q = M(p)$ páratlan volta miatt $M(p) \mid s_{p-1}$. A szükségességet beláttuk, ezáltal a tételt is.

Tekintsük most az algoritmust, aminek a bemenete egy $m > 2$ páratlan egész szám.
LUCAS-LEHMER-PRÍMTESZT(m)

1. $M \leftarrow 2^m - 1$
2. $v \leftarrow 4$
3. **for** $i \leftarrow 1$ **to** $m - 2$
4. **do** $v \leftarrow v^2 - 2$
5. **if** $v \equiv 0 \ (mod\ M)$
6. **then return** PRÍM
7. **else return** ÖSSZETETT

4.2. Fermat-prímek

4.2.1. Tétel. *Ha F_m jelöli a $2^{2^m} + 1$ alakú Fermat-számot, akkor $m > 1$ esetén F_m akkor és csak akkor prím, ha $5^{(F_m - 1)/2} \equiv -1 \ (mod\ F_m)$*

Bizonyítás: Mivel $F_m - 1$ egyetlen prímosztója 2, a kongruencia teljesülése esetén F_m prím, hiszen ekkor 5 rendje $F_m - 1 \ (mod\ F_m)$.
A másik irány bizonyításához azt kell megmutatnunk, hogy 5 kvadratikus nemmaradék $mod\ F_m$. Tudjuk, hogy $2^4 \equiv 1 \ (mod\ 5)$ Mivel 2^m 4 többszöröse, ezért: $F_m = 2^{2^m} + 1 \equiv 2 \ (mod\ 5)$. Az $\left(\frac{5}{F_m}\right)$ Legendre-szimbólum a kvadratikus reciprocitási tétellel számolva: $\left(\frac{5}{F_m}\right) = \left(\frac{F_m}{5}\right) = \left(\frac{2}{5}\right) = -1$

5. fejezet

Prímtesztelés elliptikus görbékkel

5.1. Elliptikus görbék

Egy elliptikus görbe $\mathbb{R}$ felett azon síkbeli (x, y) párok halmaza, amelyek kielégítik az

$$y^2 = x^3 + a \cdot x + b$$

egyenletet, ahol a, b valós konstansok, amelyekre $4a^3 + 27b^2 \neq 0$. Világos, hogy ha az (x, y) pont a görbén van, akkor az $(x, -y)$ pont is. (A $4a^3 + 27b^2 \neq 0$ feltétel azt biztosítja, hogy az $f(x, y) = 0$, $f(x, y) = y^2 - x^3 - a \cdot x - b$ görbe minden (x_0, y_0) pontjában létezzen egyértelmű érintő.) Ha egy (nem függőleges) egyenes metszi ezt a görbét két pontban, akkor egy harmadikban is. A görbe egy érintőjét úgy tekintjük, mint amelynél a két metszéspont egybeesik.

Ha (x_1, y_1) és (x_2, y_2) a két metszéspont, akkor a harmadik koordinátái:

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda \cdot (x_3 - x_1) + y_1$$

ahol

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \text{ ha } x_1 \neq x_2 \text{ és egyébként } \lambda = \frac{3x_1^2 + a}{2y_1}.$$

Világos, hogy λ az egyenes meredeksége. Érintő esetén ezt az implicit függvény differenciálásával kapjuk.

Az $(x_1, y_1) + (x_2, y_2) = (x_3, -y_3)$ összefüggéssel egy összeadást definiálhatunk. Ha a függőleges egyeneseknek megfelelő ∞ szimbólumot, mint nullelemet definiáljuk, azaz

$$(x, y) + (x, -y) = (x, -y) + (x, y) = \infty,$$

akkor megmutatható, hogy egy Abel-csoportot kapunk.

Ha a, b racionálisak, tekinthetünk csak racionális koordinátájú pontokat, és egy másik csoportot kapunk. Általánosabban, tekinthetünk elliptikus görbéket egy tetszőleges $\mathbb{F}$ felett, amelynek karakterisztikája különbözik 2-től és 3-tól. Meg lehet mutatni, hogy mindig Abel-csoportot kapunk. Még ha csak egy egységelemes kommutatív gyűrű adott, például $\mathbb{Z}/n\mathbb{Z}$, $lnko(n, 6) = 1$, akkor is definiálhatjuk a fenti műveleteket parciálisan, azaz ha az osztás elvégezhető; természetesen ekkor nem

kapunk csoportot. Fontos azonban észrevennünk, hogy ha $lnko(n, 4a^3 + 27b^2) = 1$, akkor bármely p prímosztójára n-nek modulo p is egy elliptikus görbét kapunk, és ha $\mathbb{Z}/n\mathbb{Z}$ felett el tudunk végezni egy összeadást, akkor bármely p prímosztójára n-nek, az eredmény $(mod\ p)$ redukálva ugyanaz, mintha előbb elvégezzük a $(mod\ p)$ redukálást, és aztán végezzük el a műveletet $(mod\ p)$. (A ∞ szimbólum redukálva saját maga.)

Prímteszteléshez csak ilyen, modulo n vett elliptikus görbékre lesz szükségünk.

5.1.1. Tétel. *(Hasse tétele) Ha $p > 3$ prím, akkor egy $\mathbb{Z}/p\mathbb{Z}$ felett vett elliptikus görbe rendje $p + 1 - 2\sqrt{p}$ és $p + 1 + 2\sqrt{p}$ között van.*

Meg lehet mutatni azt is, hogy az elliptikus görbék rendje meglehetősen egyenletesen oszlik el ebben az intervallumban, legalábbis az intervallum közepén.

5.2. Prímtesztelés elliptikus görbékkel

Az elliptikus görbékkel történő prímtesztelés az alábbi tételen alapszik:

5.2.1. Tétel. *Legyen $n \in \mathbb{N}$, $lnko(6, n) = 1$ és legyen E_n egy $\mathbb{Z}/n\mathbb{Z}$ feletti elliptikus görbe pontjainak a halmaza. Legyenek m és s egészek úgy, hogy $s \mid m$. Tegyük fel, hogy találtunk olyan P pontot E_n-ben, amelyre*

$$m \cdot P = 0 \text{ és } \frac{m}{q} \cdot P \neq 0$$

q minden prímfaktorára s-nek. Ekkor minden p prímosztójára n-nek $|E_p| \equiv 0\ (mod\ s)$. Továbbá, ha $s > (\sqrt[4]{n} + 1)^2$, akkor n prím.

Bizonyítás: Legyen p egy prímosztója n-nek, és legyen

$$Q = \frac{m}{s} \cdot P_p \in E_p.$$

Ekkor $s \cdot Q = m \cdot P_p = (m \cdot P)_p = 0$, így Q rendje osztja s-et. Ha q egy prímosztója s-nek, akkor

$$\frac{s}{q} \cdot Q = \frac{m}{q} \cdot P_p = (\frac{m}{q} \cdot P)_p \neq 0, \text{ mivel } \frac{m}{q} \cdot P \neq 0$$

Így Q rendje nem osztója s/q-nak. Mivel q tetszőleges volt, Q rendje s, így $|E_p| = 0\ (mod\ s)$.

Hasse tétele szerint $|E_p| = p + 1 - t$ valamely $|t| \leq 2\sqrt{p}$ egészre. Ebből $(p^{1/2} + 1)^2 \geq |E_p|$. Ha $s > (n^{1/4} + 1)^2$, akkor azt kapjuk, hogy $(\sqrt{p} + 1)^2 > (n^{1/4} + 1)^2$, amiből $p > \sqrt{n}$.

A prímtesztek vázlata:

Az n valószínű prím prím voltának bizonyításához válasszunk egy elliptikus görbét $\mathbb{Z}/n\mathbb{Z}$ felett, és egy m számot, amelyre a görbe rendje m – legalábbis ha n prím. Ha m felírható $f \cdot n_1$ alakban, ahol f faktorait ismerjük, n_1 pedig valószínű prím, és $n_1 > (n^{1/4} + 1)^2$, akkor n prím voltát ezen pont első tétele segítségével be tudjuk bizonyítani. Válasszunk ugyanis egy olyan P pontot, amely eleget tesz a tétel feltételeinek $s = n_1$ választással. Ehhez válasszunk egy véletlen P pontot a görbén(x véletlen, y-t kiszámítjuk). Számítsuk ki $(m/n_1) \cdot P = f \cdot P$-t; ha nincs definiálva, akkor megtaláltuk n_1 egy valódi osztóját, ami nagyon valószínűtlen. Annak valószínűsége, hogy $k \cdot P = 0$ legyen, az előző tétel szerint kisebb, mint $1/2$, ha n prím, ebben az esetben válasszunk új pontot.

Egyébként ellenőrizzük, hogy $n_1 \cdot (f \cdot P) = m \cdot P = 0$, aminek teljesülnie kell, ha n prím. Így P létezése bizonyítja, hogy n prím, ha n_1 prím. Most alkalmazzuk az eljárást n_1-re, stb.

A Goldwasser-Kilian teszt. A fenti gondolat Goldwassertől és Kiliantól származik. Javaslatuk szerint véletlenszerűen választunk egy elliptikus görbét $\mathbb{Z}/n\mathbb{Z}$ felett, meghatározzuk m-et, és ha $f = 2$ választással teljesülnek a fenti feltételek, akkor megyünk tovább. Természetesen a gyakorlatban nem érdemes f-et korlátozni, hanem m kis faktorait próbaosztással keressük meg. A módszerrel az a probléma, hogy egy véletlen elliptikus görbére m-et meghatározni nagyon nehéz, bár van rá polinomiális futásidejű $\left(O(n^8)\right)$ algoritmus.

Atkin tesztje. A teszt alapgondolata az, hogy megfordítjuk m és a görbe megválasztásának sorrendjét. Ezt úgy érjük el, hogy egy alkalmas D negatív egészre a $\mathbb{Q}(\sqrt{D})$ test ν egészei között keresünk egy olyat, amelyre $|\nu|^2 = n$ (ha van ilyen). Ha ez megvan, akkor $m = |\nu \pm 1|^2$ rendű elliptikus görbéket „könnyen” találhatunk. Így m-et már akkor tudjuk, amikor a görbét még nem: azt ráérünk később is meghatározni.

6. fejezet

Az AKS-algoritmus

6.1. Az AKS-algoritmus

Az esetleges félreértések elkerülése végett teszünk néhány megjegyzést a fejezetben használt jelölésekkel kapcsolatban. log minden esetben kettes alapú logaritmust jelöl. A bonyolultságelméletből ismert fogalmakat a szokásos módon értelmezzük. A szakirodalomban algoritmusok vizsgálatánál általában n bites bemenetet tételeznek fel, és n függvényében vizsgálják a futási időt. Prímtesztek esetében viszont, ha n pozitív egész a vizsgálandó szám, akkor ábrázolásához $\lceil \log(n) \rceil$ bitre van szükség, tehát a bonyolultsági korlátok $\lceil \log(n) \rceil$ függvényeiben értendőek. Használni fogjuk továbbá a $\widetilde{O}(t(n))$ kifejezést $O(t(n) \cdot poly(\log t(n)))$ jelölésére, ahol $t(n)$ tetszőleges függvénye n-nek, és $poly(\log t(n))$ polinomiális függvénye $\log t(n)$-nek, azaz

$$poly(\log t(n)) = a_0 + a_1 \log t(n) + \cdots + a_r \log^r t(n),$$

valamely r pozitív egészre, és $a_0, a_1, \ldots, a_r$ valós együtthatókra. Például, ha t éppen a log függvénnyel egyenlő, akkor

$$\widetilde{O}(\log^k(n)) = O(\log^k(n) \cdot poly(\log \log n)) = O(\log^{k+\varepsilon} n)$$

tetszőleges pozitív ε-ra.

Agrawal, Kayal és Saxena 2002-ben közöltek egy algoritmust, amely nagy áttörésnek számít a prímtesztek történetében. Mondhatjuk ezt azért, mert a szerzők bizonyítják, hogy a prímszámok halmaza a P nyelvosztályba tartozik. Ez azt jelenti, hogy egy n pozitív egész szám prím mivoltának eldöntése megoldható annyi idő alatt, amely $\lceil \log n \rceil$-nek polinomiális függvénye. Ráadásul ez az algoritmus determinisztikus, vagyis a valószínűségi tesztekkel ellentétban itt a legkisebb esélye sincs annak, hogy valamely álprímet véletlenül prímnek nyilvánítsunk.

Az algoritmus a 2.2.4 tételen alapszik. Az alapgondolat: bemenetként adott n természetes számhoz keressünk megfelelő a egészet és ellenőrizzük, hogy teljesül-e a 2.1 kongruencia. Ez így természetesen nagyon egyszerű, de mivel mintegy n tagról kell eldönteni, hogy kongruens-e 0-val $(mod\, n)$, nem hatékony eljárás. A továbbiakban szeretnénk a számolásokat egy megfelelően választott relatíve kevés elemből álló véges struktúra felett végezni, azt remélve, hogy így le tudjuk csökkenteni $f(x)$ vizsgálandó együtthatóinak számát.

Az algebrában jól ismert tény, hogy tetszőleges R főideálgyűrűben $R/\langle a\rangle$ akkor és csak akkor lesz test. ha a felbonthatatlan elem R-ben. $\langle a\rangle$ itt az a elem által generált főideált jelenti. Tehát tekintsük az F_p véges test feletti $h(x)$ d-edfokú irreducibilis, azaz felbonthatatlan polinomot. Ekkor $F_p[x]/\langle h(x)\rangle$ egy p^d elemszámú testet alkot, amelynek elemei az F_p feletti legfeljebb $(d-1)$-edfokú polinomok. A továbbiakban alkalmazzuk a következő jelölést: ha $f(x) \equiv g(x)$ teljesül $\mathbb{Z}_n/\langle h(x)\rangle$-ben, akkor azt írjuk, hogy

$$f(x) \equiv g(x) \ (mod\ n, h(x).$$

Megjegyezzük, hogy $\mathbb{Z}_n$ akkor és csak akkor alkot testet, ha n prímszám, tehát a $\mathbb{Z}_n[x]/\langle h(x)\rangle$ gyűrű nem feltétlenül test, és legfeljebb $(deg(h(x)) - 1)$-edfokú polinomkifejezésekből áll, amelyek együtthatói $\mathbb{Z}_n$-beliek. Az AKS-algoritmusban $h(x) = x^r - 1$, ahol r egy „megfelelően kicsi" pozitív egész. A továbbiakban természetesen a „megfelelően kicsi" kifejezés értelmét pontosítjuk. Tehát a prímek azonosítására használjuk 2.1 helyett a

$$(x + a)^n \equiv x^n + a \ (mod\ n, x^r - 1) \tag{6.1}$$

kongruenciát. A 2.2.4 tételből közvetlenül következik, hogy ha n prímszám, akkor kielégíti a 6.1 összefüggést, minden a és r esetén. Látható továbbá, hogy ha r elég kicsi n-hez képest, akkor kevesebb együtthatót kell megvizsgálnunk. Sajnos cserébe azt az árat kell fizetnünk, hogy bizonyos a és r értékek esetén előfordulhat, hogy valamely n összetett szám is kielégíti a kongruenciát. Viszont bizonyítható, hogy megfelelően választott r esetén nem túl sok a értékre elvégezve a vizsgálatot, csak olyan összetett számok mehetnek át a teszten, amelyek prímhatványok. Az AKS-algoritmus annak köszönheti a gyorsaságát, hogy mind r értékére, mind a különböző a-k számára olyan felső korlát adható, amely $\lceil \log n \rceil$-nek polinomiális függvénye. Ezen tények, és az, hogy n-ről eldönteni prímhatvány mivoltát nem tart sokáig, eredményezi a $\lceil \log n \rceil$-ben polinomiális futási időt. Ráadásul, ahogy azt a későbbiekben látni fogjuk, ennyi vizsgálat is elég ahhoz, hogy n prím voltát száz százalékos biztonsággal eldöntsük, azaz az algoritmus determinisztikus is, ami miatt kiemelkedik az eddig ismert prímtesztek közül.

Az algoritmus lépései

- Megvizsgáljuk, hogy n teljes hatvány-e. Ennek a lépésnek a műveletigénye $\widetilde{O}((\log n)^3)$
- Keresünk egy r egészet, amire n rendje $mod\ r > (\log n)^2$. Ennek a kézenfekvő módja, hogy kiszámítjuk $n^j \ (mod\ r)$-et $j = 1, \ldots, [(\log n)^2]$-re és minden $q > [(\log n)^2]$ egészre, az első q-ig, amire a maradékok egyike sem 1. Az így megtalált q jó lesz r-nek. r megtalálása $\widetilde{O}(r \cdot (\log n)^2)$ lépés.
- Meghatározzuk, hogy $(a, n) > 1$ teljesül-e valamely $a \leq r$-re, amihez $\widetilde{O}(r \cdot (\log n)^2)$ művelet kell.
- Ellenőrizzük, hogy fennáll-e az $(x+a)^n \equiv x^n + a \ (mod\ n, x^r - 1)$ összefüggés $a = 1, 2, \ldots, [\sqrt{r} \cdot \log n]$-re. Egy ilyen kongruencia ellenőrzésének műveletigénye $\widetilde{O}(r \cdot (\log n)^2)$, így a teljes műveletigény $\widetilde{O}(r^{\frac{3}{2}} \cdot (\log n)^3)$.

Be fogjuk látni, hogy létezik megfelelő $r \leq 2(\log n)^5$, és így az algoritmus műveletigénye: $\widetilde{O}((\log n)^{10,5})$.

Agrawal, Kayal és Saxena tételének bizonyítása:

Feltesszük, hogy adott egy $n > 1$ egész, ami nem teljes hatvány, nincs r-nél kisebb prímosztója, a rendje $d > (\log n)^2 \ (mod\ r)$, és

$$(x+a)^n \equiv x^n + a \ (mod\ n, x^r - 1) \tag{6.2}$$

minden a-ra: $1 \leq a \leq A$, ahol $A = \sqrt{r} \cdot \log n$ A 2.2.4 tétel miatt tudjuk, hogy ezek a feltételek teljesülnek, ha n prím, tehát azt kell bizonyítanunk, hogy nem állhatnak fönt, ha n összetett. Legyen p egy prímosztója n-nek. Ekkor

$$(x+a)^n \equiv x^n + a \ (mod\ p, x^r - 1) \tag{6.3}$$

minden a-ra: $1 \leq a \leq A$. $x^r - 1$-et fel tudjuk bontani irreducibilis polinomok szorzatára a következő alakban: $\prod_{d|r} \Phi_d(x)$, ahol $\Phi_d(x)$ a d-edik körosztási polinom, aminek a gyökei a d-edik primitív egységgyökök. Minden egyes $\Phi_d(x)$ irreducibilis $\mathbb{Z}[x]$-ben, de nem feltétlenül az $(\mathbb{Z}/p\mathbb{Z})[x]$-ben, ezért legyen $h(x)$ egy irreducibilis faktora $\Phi_d(x)$-nek $(mod\ p)$. Ekkor 6.3-ból következik, hogy:

$$(x+a)^n \equiv x^n + a \ (mod\ p, h(x)) \tag{6.4}$$

minden a-ra: $1 \leq a \leq A$, mivel $h(x) \mid x^r - 1$.

A $(mod\ p, h(x))$ maradékosztályokat tekinthetjük az $\mathbb{F} :\equiv \mathbb{Z}/(p, h(x))$ gyűrű elemeinek, ami izomorf a p^m elemű testtel (ahol m a h polinom foka). $\mathbb{F}$ nemnulla elemei $p^m - 1$ rendű ciklikus csoportot alkotnak.

6.1.1. Állítás. *x primitív r-edik egységgyök $\mathbb{F}$-ben.*

Bizonyítás: $h(x) \mid x^r - 1$ miatt x r-edik egységgyök $(mod\ h(x))$, ezért x rendje valamely l, amelyre $l \mid r$. Ha

$$x^l - 1 \equiv 0 \ (mod\ h(x)), \text{ és } h(x) = \prod_{j=1}^{d} (x - \xi_j),$$

akkor $h(x) \mid x^l - 1$ miatt $\xi_j^l = 1$, másrészt $h(x) \mid \Phi_r(x)$ miatt $\xi_j = \zeta^s$ alkalmas $s : \ (s, r) = 1$ értékre, ahol ζ primitív r-edik egységgyök. Triviálisan igaz, hogy $1 = \xi_j^l = \zeta^{s \cdot l}$ nem teljesülhet, ha $l < r$. azaz $x \ (mod\ h(x))$ rendje r.

Álljon H az $x, x+1, x+2, \ldots, x+[A]$ által multiplikatívan generált elemekből $(mod\ p, x^r - 1)$. G legyen az $\mathbb{F}$ $x, x+1, x+2, \ldots, x+[A]$ által generált (ciklikus) részcsoportja; másszóval G H-nak a redukálása $(mod\ p, h(x))$.

6.1.2. Állítás. *G minden eleme nemnulla.*

Bizonyítás: Tegyük fel, hogy $x + a = 0$ $\mathbb{F}$-ben. Ekkor $x^n + a = (x+a)^n = 0$ $\mathbb{F}$-ben 6.4 miatt, tehát $x^n = -a = x$ $\mathbb{F}$-ben, amiből következne, hogy $n \equiv 1 \ (mod\ r)$, és így $d = 1$, ami ellentmond a feltevésnek.
Ha $g(x) = \prod_{0 \leq a \leq A} (x+a)^{e_a} \in H$, akkor

$$g(x)^n = \prod_a ((x+a)^n)^{e_a} \equiv \prod_a (x^n + a)^{e_a} = g(x^n) \quad (mod\ p, x^r - 1)$$

6.3 miatt. Legyen S azon pozitív egész k-k halmaza, amelyekre $g(x^k) = g(x)^k \ (mod\ p, x^r - 1)$ minden $g \in H$-ra. Ekkor $g(x^k) \equiv g(x)^k$ $\mathbb{F}$-ben minden $k \in S$-re. Tudjuk, hogy $p, n \in S$.

G méretére fogunk alsó és felső becslést adni, és ebből szeretnénk ellentmondásra jutni.

Felső becslés $|G|$-re

6.1.3. Lemma. *Ha $a, b \in S$, akkor $a \cdot b \in S$.*

Bizonyítás: Ha $g(x) \in H$, akkor $g(x^b) \equiv g(x)^b \ (mod\ p, x^r - 1)$. Helyettesítsünk x helyére x^a-t, és így kapjuk: $g((x^a)^b) \equiv g(x^a)^b \ (mod\ p, (x^a)^r - 1)$, és a kongruencia teljesül $(mod\ p, x^r - 1)$, mivel $x^r - 1$ osztja $x^{a \cdot r} - 1$. Tehát

$$g(x)^{a \cdot b} = (g(x)^a)^b \equiv g(x^a)^b \equiv g((x^a)^b) = g(x^{a \cdot b}) \ (mod\ p, x^r - 1),$$

amit bizonyítanunk kellett.

6.1.4. Lemma. *Ha $a, b \in S$, és $a \equiv b \ (mod\ r)$, akkor $a \equiv b \ (mod\ |G|)$.*

Bizonyítás: Minden $g(x) \in \mathbb{Z}[x]$-re igaz, hogy $u - v$ osztja $g(u) - g(v)$-t. Emiatt $x^r - 1$ osztja $x^{a-b} - 1$-et, ami osztja $x^a - x^b$-t, ami osztja $g(x^a) - g(x^b)$-t, és így arra jutunk, hogyha $g(x) \in H$, akkor

$$g(x)^a \equiv g(x^a) \equiv g(x^b) \equiv g(x)^b \ (mod\ p, x^r - 1).$$

Tehát ha $g(x) \in G$, akkor $g(x)^{a-b} \equiv 1$ $\mathbb{F}$-ben; de G ciklikus csoport, ezért g-t generátornak választva kapjuk, hogy $|G|$ osztja $a - b$-t.

Legyen R a $(\mathbb{Z}/r\mathbb{Z})^*$ n és p által generált részcsoportja. Mivel n p-nek nem hatványa, ezért az $n^i \cdot p^j$ egészek mind különbözőek $i, j \geq 0$ esetén. Több, mint $|R|$ különböző számot kapunk, ha $0 \leq i, j \leq \sqrt{|R|}$, így van köztük kettő kongruens $(mod\ r)$, legyen:

$$n^i \cdot p^j \equiv n^I \cdot p^J \ (mod\ r).$$

6.1.3 miatt mind $n^i \cdot p^j$, mind $n^I \cdot p^J$ S-ben van, valamint 6.1.4 miatt a különbségük osztható $|G|$-vel, és így:

$$|G| \leq |n^i \cdot p^j - n^I \cdot p^J| \leq (n \cdot p)^{\sqrt{|R|}} - 1 < n^{2\sqrt{|R|}} - 1.$$

($n^i \cdot p^j - n^I \cdot p^J$ nem lehet 0, mert n nem prím, és nem is teljes hatvány.) Élesíteni fogjuk az egyenlőtlenséget azzal, hogy megmutatjuk: $n/p \in S$, és n helyébe n/p-t helyettesítve a fenti okoskodásból kapjuk:

$$|G| \leq n^{\sqrt{|R|}} - 1 \tag{6.5}$$

Mivel n rendje d $(mod\ r)$: $n^d \equiv 1 \ (mod\ r)$, és így $x^{n^d} \equiv x \ (mod\ x^r - 1)$. Tegyük fel, hogy $a \in S$, és $b \equiv a \ (mod\ n^d - 1)$. Ekkor $x^r - 1$ osztja $x^{n^d} - x$-et, ami osztja $x^b - x^a$-t, ami osztja $g(x^b) - g(x^a)$-t bármely $g(x) \in \mathbb{Z}[x]$ esetén. Ha $g(x) \in H$, akkor $g(x)^{n^d} \equiv g(x^{n^d}) \ (mod\ p, x^r - 1)$ 6.1.3 miatt, mivel $n \in S$, és $g(x^{n^d}) \equiv g(x) \ (mod\ p, x^r - 1)$(mivel $x^r - 1$ osztja $x^{n^d} - x$-et), és így $g(x)^{n^d} \equiv g(x) \ (mod\ p, x^r - 1)$. De ekkor $g(x)^b \equiv g(x)^a \ (mod\ p, x^r - 1)$, mivel $n^d - 1$ osztja $b - a$-t. Innen:

$$g(x^b) \equiv g(x^a) \equiv g(x)^a \equiv g(x)^b \ (mod\ p, x^r - 1),$$

mivel $a \in S$, amiből következik, hogy $b \in S$. Most legyen $b = n/p$ és $a = n \cdot p^{\varphi(n^d-1)-1}$, és így $a \in S$ 6.1.3 miatt, mivel $p, n \in S$; valamint $b \equiv a \ (mod\ n^d - 1)$, és így $b = n/p \in S$ a fentiek miatt.

Alsó becslés $|G|$-re

Azt szeretnénk megmutatni, hogy sok különböző eleme van G-nek. Ha $f(x), g(x) \in \mathbb{Z}[x]$, és $f(x) \equiv g(x) \ (mod\ p, h(x))$, akkor igaz, hogy $f(x) - g(x) \equiv h(x) \cdot k(x) \ (mod\ p)$ valamely $k(x) \in \mathbb{Z}[x]$-re. Ha f és g is alacsonyabb fokú, mint h, akkor $k(x) \equiv 0 \ (mod\ p)$, és így $f(x) \equiv g(x) \ (mod\ p)$. Ennélfogva a $\prod_{1 \le a \le A}(x+a)^{e_a}$ alakú, m-nél($h(x)$ foka) alacsonyabb fokú polinomok G különböző elemei. Ennek következtében ha m, p rendje $(mod\ r)$, nagy, akkor jó alsó becslést tudunk adni $|G|$-re.

6.1.5. Lemma. *Tegyük fel, hogy $f(x), g(x) \in \mathbb{Z}[x]$, $f(x) \equiv g(x) \ (mod\ p, h(x))$, és f, g egyszerüsítései $\mathbb{F}$-ben G-ben vannak. Ha f és g foka alacsonyabb $|R|$-nél, akkor $f(x) \equiv g(x) \ (mod\ p)$.*

Bizonyítás: Legyen $\Delta(y) := f(y) - g(y) \in \mathbb{Z}[x]$ $\mathbb{F}$-beli redukálása. Ha $k \in S$, akkor:

$$\Delta(x^k) = f(x^k) - g(x^k) \equiv f(x)^k - g(x)^k \equiv 0 \ (mod\ p, h(x)).$$

Mivel x rendje r $\mathbb{F}$-ben, így $\{x^k : k \in R\}$ mind különböző gyöke $\Delta(y)$-nak $(mod\ p, h(x))$. Tehát $\Delta(y)$ foka kisebb, mint $|R|$, de $\ge |R|$ különböző gyöke van $(mod\ p, h(x))$, és így $\Delta(y) \equiv 0 \ (mod\ p, h(x))$, amiből következik, hogy $\Delta(y) \equiv 0 \ (mod\ p)$, mivel az együtthatók függetlenek x-től.

A definíció miatt R tartalmazza az összes n által generált elemet $(mod\ r)$, és így R elemeinek a száma legalább d, n rendje $(mod\ r)$, ami $> (\log n)^2$ a feltevés miatt. Ennélfogva $|R| > B$, ahol $B := [\sqrt{|R|} \cdot \log n]$. 6.1.5-ből következik, hogy a $\prod_{a \in T}(x+a)$ szorzatok G különböző elemei G-nek minden alkalmas $T \subset \{0, 1, 2, \ldots, B\}$-re, és így:

$$|G| \ge 2^{B+1} - 1 > n^{\sqrt{|R|}} - 1,$$

ami ellentmond 6.5-nek. Ezzel befejeztük a bizonyítást.

Megfelelő r létezése:

A prímszámtétel átfogalmazható a következő alakba: az x-nél kisebb prímek szorzata megközelítőleg e^x. Egy gyenge explicit változat szerint: az N és $2N$ közötti prímek szorzata $\ge 2^N$ $N \ge 1$-re.

6.1.6. Lemma. *Ha $n \ge 6$, akkor létezik $r \in [(\log n)^5, 2(\log n)^5]$ prím, amire n rendje $(mod\ r)$ $> (\log n)^2$*

Bizonyítás:Tegyük fel indirekt, hogy nem igaz az állítás, vagyis bármely $r \in [N, 2N]$, $N = (\log n)^5$ prímre n rendje $(mod\ r)$ $\le I := (\log n)^2$, és így a szorzatuk osztja $\prod_{i \le I}(n^i - 1)$-et. De ekkor

$$2^N \le \prod_{N \le r \le 2N\, r \text{ prím}} r \le \prod_{i \le I}(n^i - 1) < n^{\sum_{i \le I} i} < 2^{(\log n)^5}$$

ami $n \ge 6$-ra ellentmondás.

6.1.1. Az algoritmus tökéletesítése

Az eljárás gyorsítására több lehetőség is kínálkozik. Ezek lényege, hogy az r érték becslését finomítsuk. Látható, hogy ideális esetben r értéke $O((\log n)^2)$ nagyságrendű, így az egész algoritmus időigénye $O((\log n)^6)$ lehet. A következő két sejtés azt sugallja, hogy jó esély van $O((\log n)^5)$ nagyságrendnél kisebb r-et találni.

Az egyik az Artin-sejtés:

6.1.7. Sejtés. *Legyen $a \in \mathbb{Z}$ nem teljes négyzet, továbbá $a \neq 0, \pm 1$. Jelölje N_a azon p prímeknek a halmazát, amelyekre a a p prímszám primitív gyöke, továbbá legyen*

$$n_a(x) = |\{N_a \cap [1, x]\}|,$$

valamint $\pi(x)$ az x-nél nem nagyobb prímek száma. Ekkor Artin sejtése szerint

$$\lim_{n \to \infty} \frac{n_a(x)}{\pi(x)} = A(a),$$

ahol $A(a)$ az úgynevezett Artin-konstans, az a-tól függő pozitív állandó(amelyről tudjuk, hogy $A(a) > 0.35$).

6.1.8. Sejtés. *Azon $q \leq m$ prímek száma, melyekre $2q + 1$ is prím, aszimptotikusan*

$$\frac{2C_2 \cdot m}{(\ln m)^2},$$

ahol C_2 az úgynevezett ikerprím konstans, amelynek közelítő értéke 0.66.

Megjegyezzük, hogy utóbbi a Sophie-Germain prímek sűrűségére vonatkozó sejtésként ismeretes a szakirodalmakban.

Az Artin-sejtés igaz volta közvetlenül maga után vonná, hogy $O((\log n)^2)$ nagyságrendű m-re található olyan $r = (O(\log n)^2)$, amely kielégíti a kívánt feltételeket. Sajnos jelenleg az sem bizonyított, hogy minden nem négyzetszám n esetén végtelen sok q prímszámra teljesül az $o_q(n) = n - 1$ összefüggés.

Ami a Sophie-Germain prímeket illeti, ha igaz a rájuk vonatkozó sejtés, akkor biztosan létezik legalább $(\log n)^2$ ilyen prím $(\log n)^2$ és $c \cdot (\log n)^2 \cdot (\log \log n)^2$ között, megfelelő c konstans szorzóval. Minden ilyen q prímszám esetén vagy $o_q(n) \leq 2$ áll fenn, vagy $o_q(n) \geq \frac{q-1}{2}$. Bármely olyan q, amire $o_q(n) \leq 2$ igaz, osztója $(n-1) \cdot (n^2 - 1)$-nek, és így számuk $O(\log n)$ nagyságrendű. Ez a tény implikálja olyan $r = \widetilde{O}((\log n)^2)$ létezését, ami kielégíti az $o_r(n) \geq 4(\log n)^2$ feltételt. Egy ilyen nagyságrendű r érték az AKS-algoritmusnak $\widetilde{O}((\log n)^6)$ futási időt eredményez.

Az időkorlát elméleti leszorítására az AKS-algoritmus szerzőinek konkrét eredménye is született. Jelölje $P(m)$ az m legnagyobb prímosztóját. Goldfeld megmutatta, hogy pozitív valószínűséggel fordulnak elő olyan q prímek, melyekre $P(q-1) > q^{\frac{1}{2}+c}$, ahol $c \approx 1/12$. Ezt az eredményt Fouvry tökéletesítette, bizonyítva a következő állítást.

6.1.9. Lemma. *Létezik olyan $c > 0$ konstans és n_0 pozitív egész, hogy minden $x \geq n_0$ esetén:*

$$\left| \left\{ q \,|\, q \text{prímszám}, \; q \leq x \text{ és } P(q-1) > q^{\frac{2}{3}} \right\} \right| \geq c \frac{x}{\ln x}.$$

A lemmát már igazolták 0.6683-as kitevőig. Ezen eredmények felhasználásával tudták a szerzők az AKS-algoritmus időigényét elméleti úton leszorítani.

6.1.10. Tétel. *Az AKS-prímteszt algoritmus aszimptotikus időigénye* $\widetilde{O}((\log n)^{7.5})$.

Bizonyítás: A fentiek értelmében az olyan q prímek, melyekre $P(q-1) > q^{\frac{2}{3}}$, nagy sűrűsége azt eredményezi, hogy a 2. programrészben az eljárás talál olyan $r = O((\log n)^3)$ értéket, amire fennáll, hogy $o_r(n) > 4(\log n)^2$. Emiatt lehet az algoritmusnak $\widetilde{O}((\log n)^{7.5})$ nagyságrendű futási ideje.

Biztató lehet a jövőre nézve a következő sejtés, amely ha igaz, akkor az AKS-prímteszt algoritmus aszimptotikus időigénye $\widetilde{O}((\log n)^3)$-re módosítható. Megjegyezzük, hogy az állítás helyességét $r \leq 100$ és $n \leq 10^{10}$ esetre már ellenőrizték.

6.1.11. Sejtés. *Legyen r olyan prím, amely nem osztója n-nek. Ha fennáll az*

$$(x-1)^n \equiv x^n - 1 \ (mod\ x^r - 1, n) \tag{6.6}$$

kongruencia, akkor n prím, vagy $n^2 \equiv 1 \ (mod\ r)$.

Ha a sejtés igaz, akkor az a teendőnk, hogy olyan r értéket keresünk, amely nem osztója $n^2 - 1$-nek. Ilyen r biztosan található a $[2, 4\log n]$ intervallumban. Ez abból következik, hogy az x-nél kisebb prímek szorzata legalább e^x. Ezután már csak 6.6 teljesülését kell ellenőrizni, amelynek az időigénye $\widetilde{O}((\log n)^2)$, vagyis az AKS-prímteszt futási ideje $\widetilde{O}((\log n)^3)$.

6.2. Az algoritmus megvalósíthatósága

Az AKS-algoritmus gyakorlati megvalósításával kapcsolatban fel kell hívnunk a figyelmet egy fontos dologra. Ez nevezetesen az, hogy bonyolultságelméleti szempontból a futásidő nagyon kedvezően alakul, viszont a tárigény olyan mértékűnek mutatkozik, ami viszonylag kicsi számoknál is óriási operatív memóriát feltételez. A gyorsaság érdekében az egy lépésben vizsgált polinom együtthatóit mind az operatív tárban célszerű tartani.

Egy $(x+a)^n - x^n - a$ alakú polinom osztási maradéka a $(mod\ x^r - 1, n)$ modulus szerint egy legfeljebb $(r-2)$-edfokú polinom lesz, amelynek együtthatói legfeljebb az $n-1$ értéket vehetik fel. Tehát legrosszabb esetben $(r-1)$ darab együtthatót kell ellenőriznünk, amelyek tárigénye akár $(r-1)\cdot\lceil\log(n-1)\rceil$ bit is lehet. Legyen n a legnagyobb 1000 decimális számjegyű pozitív egész. Tegyük fel, hogy r értéke eléri a bizonyításban szereplő $\lceil 2(\log n)^5\rceil$ korlátot. Ekkor egyszerű számolással belátható, hogy a tárigény túllépheti a $3\cdot 10^{14}$ gigabájtot. Manapság egy 1000 számjegyű egész szám nem számít nagynak prímtesztelés szempontjából, de ekkora operatív tár nem áll rendelkezésre.

Érdemes elvégezni ugyanezt a számolást úgy, hogy feltesszük, hogy a 6.1.11 sejtés igaz. Ekkor találunk olyan r-et, amelyre $r \leq 4(\log n)$, ami azt jelenti, hogy a tárigény 5,27 gigabájt alá csökken.

A fenti számítások azt támasztják alá, hogy nem kell teljesen elfelejteni gyakorlati alkalmazások szempontjából az AKS-prímteszt eljárást, viszont ahhoz, hogy valóban egy determinisztikus, nagy számok prímtesztelésére is alkalmas számítógépes program születhessen, még szükség van új matematikai eredményekre, elsődlegesen a 6.1.11 sejtés bizonyítására gondolunk, a hardverek fejlődésére, valamint ügyes programozói megoldásokra.

6.3. Lenstra és Pomerance változata

Lenstra és Pomerance jelentősen megváltoztatta az AKS-algoritmust, aminek így $\widetilde{O}((\log n)^6)$ lett a műveletigénye. A kulcsötletük a $\Phi_r(x)$ polinom kicserélése egy bizonyos tulajdonságokkal rendelkező $f(x)$ polinomra.

Adott $f(x)$ egészegyüttthatós, 1 főegyüttthatós d-edfokú polinom és n pozitív egész szám esetén azt mondjuk, hogy $\mathbb{Z}[x]/(n, f(x))$ pszeudotest, ha

1. $f(x^n) \equiv 0 \ (mod\ n, f(x))$,
2. $x^{n^d} - x \equiv 0 \ (mod\ n, f(x))$, és
3. $x^{n^{d/q}} - x$ egység $\mathbb{Z}[x]/(n, f(x))$ minden prím q-ra, ami osztja d-t

Ha n prím, és $f(x)$ irreducibilis $(mod\ n)$, akkor teljesülnek ezek a feltételek, és $\mathbb{Z}[x]/(n, f(x))$ test.

Adott $n > 2$ egész számhoz legyen $d \in ((\log n)^2, n)$ olyan egész, amire létezik az $f(x)$ egészegyüttthatós, 1 főegyüttthatós d-edfokú polinom úgy, hogy $\mathbb{Z}[x]/(n, f(x))$ pszeudotest. Ekkor n prím akkor és csak akkor, ha

- n nem teljes hatvány
- n-nek nincs olyan prímosztója, ami $\leq d$
- $(x + a)^n \equiv x^n + a \ (mod\ n, f(x))$ minden a egész számra, amire $1 \leq a \leq A := \sqrt{d} \cdot \log n$

Ránézésre látszik, hogy ez a tétel Agrawal, Kayal és Saxena munkájából gyökerezik, de már általánosabb. Ebből az általánosságból adódik, hogy sokkal kevesebb lépést igényel.

Nyilvánvaló, hogy adott f-re gyorsan meg lehet határozni, hogy pszeudotestet kapunk-e, és ha igen, akkor teljesülnek-e a feltételek. Ennélfogva ha gyorsan tudunk találni olyan f-et, ami pszeudotestet ad, akkor ez a megközelítés egy gyors prímteszthez vezet. f megkonstruálása Lenstra és Pomerance által Gausshoz nyúlik vissza, a szabályos n-szögek szerkesztéséhez, ahhoz a témához amit manapság Gauss-periódusokként ismerünk.

A karakterizáció bizonyítása:

Tegyük fel, hogy n összetett és teljesíti a három feltevést. Legyen p n egy prímosztója, és $h(x)$ $f(x)$ irreducibilis faktora $(mod\ p)$, és így $\mathbb{F} \equiv \mathbb{Z}[x]/(p, h(x))$ izomorf egy véges testtel.

Ahogy a 6.1 részben is , álljon H $(mod\, p, f(x))$ azon elemeiből amelyeket $x, x+1, x+2, \ldots, x+[A]$ multiplikatívín generálnak; legyen G $\mathbb{F}$ azon részcsoportja, amit $x, x+1, x+2, \ldots, x+[A]$ generálnak; és legyen S a $p^i \cdot n^j,\ i, j \geq 0$ alakú pozitív egészek halmaza. Definiáljuk r-et, mint x rendje $(mod\ p, f(x))$, így d lesz n rendje $(mod\ r)$ (2) és (3) miatt, és $x^{n^0}, x^{n^1}, \ldots, x^{n^{d-1}}$ különbözőek $(mod\ p, f(x))$, sőt különbözőek $(mod\ p, h(x))$ is. Ennélfogva a $g(T) := \prod_{i=0}^{d-1}(T - x^{n^i}) \in \mathbb{F}[T]$ polinom gyökei különbözőek; továbbá $g(x^p) = g(x)^p = 0$ $\mathbb{F}$-ben, ezért x^p-nek egyenlőnek kell lennie x^{n^j}-nel $\mathbb{F}$-ben valamely j-re. Ebből következik, hogy $p \equiv n^j \ (mod\ r)$, és ezért ha R $(\mathbb{Z}/r\mathbb{Z})^*$-nak n és p által generált részcsoportja, akkor R-et n egyedül is generálja, és R-nek d eleme van.

A 6.1 részben leírt bizonyítás működik a 6.1.3 lemmára, leszámítva azt az észrevételt miszerint $x^r - 1$ osztja $x^{k \cdot r} - 1$-et bármely $k \in S$-re. Ezt lecseréljük arra a tényre, hogy $f(x^k) \equiv$

$0\ (mod\ p, f(x))$ minden $k \in S$-re, ami azért áll fenn, mert $f(x^n) \equiv 0\ (mod\ p, f(x))$ (1) miatt, és $f(x^p) \equiv f(x)^p\ (mod\ p) \equiv 0\ (mod\ p, f(x))$ a "gyerekek binomiális tétele" miatt.

A 6.1.4 lemma adódik nagyon hasonló bizonyítással($(p, x^r - 1)$-et cseréljük $(p, f(x))$-re), mivel $(p, f(x))$ osztja $(p, x^r - 1)$-et. A 6.5 utáni megjegyzések egyszerűen következnek, ha az ottani első mondatot lecseréljük (2)-re, és a továbbiakban $(p, x^r - 1)$ helyére $(p, f(x))$-et írjuk. Ennélfogva 6.5 és 6.1.5 lemma fennáll, ezért ugyanúgy, mint a 6.1 részben $|G| \geq 2^{B+1} - 1$, ahol $B := [A]$, és így $|G| > n^{\sqrt{|R|}} - 1$ ami ellentmondásban van 6.5-tel.

f megkonstruálása:

Legyen $\zeta_r = e^{2\pi i/r}$ prím r-re. Ha q osztja $r-1$-re, definiáljuk a Gauss-periódust a következőképpen: $\eta = \sum_{j \in J} \zeta_r^j$, ahol $J = J_{r,q} = \{j\ (mod\ r) :\ j^{(r-1)/q} \equiv 1\ (mod\ r)\}$ azon maradékosztályok halmaza $(mod\ r)$, amelyek relatív prímek r-hez, és q-adik hatványok $(mod\ r)$. J részcsoportja a $(\mathbb{Z}/r\mathbb{Z})^*$ ciklikus csoportnak, és így $J = \{g^{q \cdot i} :\ 0 \leq i \leq (r-1)/q\}$ $(\mathbb{Z}/r\mathbb{Z})^*$ g generátorára. Továbbá J-nek q darab mellékosztálya van $(\mathbb{Z}/r\mathbb{Z})^*$-ban, ezek $g^i \cdot J$, ahol $0 \leq i \leq q-1$. Így $\eta = \eta_0$ konjugáltjai: $\eta_i := \sum_{j \in J} \zeta_r^{g^i \cdot j},\ i = 0, 1, 2, \ldots, q-1$. η $\mathbb{Q}$ fölötti minimálpolinomja: $f(x) = \prod_{i=0}^{q-1}(x - \eta_i)$, ami egészegyütthatós 1 főegyütthatós q-adfokú polinom.

Legyen p r-től különböző prímszám. A $\mathbb{Q}(\zeta_r)$ testben a $\mathbb{Q}$ fölötti prímek(mint például p) esetleg továbbbonthatóak prímideálokra, ezért tegyük fel, hogy $\mathcal{P}$ p egy prímideálfaktora $\mathbb{Q}(\zeta_r)$-ben. Elképzelhető, hogy $f(x)$ is felbontható $(mod\ p)$, így legyen $g(x)$ $f(x)$ azon faktora $(mod\ p)$, amelyre $g(\eta) \equiv 0\ (mod\ \mathcal{P})$. A "gyerekek binomiális tétele" szerint $g(x^p) \equiv g(x)^p\ (mod\ p)$, és így $(mod\ \mathcal{P})$ is, ennélfogva $g(\eta^p) \equiv g(\eta)^p \equiv 0\ (mod\ \mathcal{P})$. Innen $\eta^p \equiv \eta_k\ (mod\ p)$, ahol $\eta_k \in g^k \cdot J$ gyöke $g(x)$-nek $(mod\ \mathcal{P})$, és hasonló okoskodással azt kapjuk, hogy $\eta_{ik\ (mod\ q)}$ is az $i = 0, 1, \ldots, q-1$-re. Ezek pontosan akkor különbözőek, ha $p^{(r-1)/q}$ rendje $(mod\ r)$ éppen q. Ebből arra következtethetünk, hogy $f(x)$ pontosan akkor irreducibilis $(mod\ p)$, ha $p^{(r-1)/q}$ rendje $(mod\ r)$ éppen q.

Ilymódon tudunk konstruálni egy q-adfokú irreducibilis polinomot $\mathbb{F}_p$ fölött, az η Gauss-periódus minimálpolinomját. Továbbá, ha van néhány prímünk: $r_1, r_2, \ldots, r_k$, és páronként relatív prím pozitív egész számunk: $q_1, q_2, \ldots, q_k$, amelyekre igaz, hogy q_i osztja $r_i - 1$-et minden egyes i-re, akkor $f(x)$: $\eta_1 \cdot \eta_2 \cdots \eta_k$ minimálpolinomja $\mathbb{Q}$ fölött $q_1 \cdot q_2 \cdots q_k$-adfokú, és irreducibilis $(mod\ p)$ pontosan akkor, ha $p^{(r_i-1)/q_i}$ rendje $(mod\ r)$ éppen q_i minden egyes i-re. Ez a gondolat elvezet f megkonstruálásához: adott n-re keressünk q_i-t és r_i-t mint fönt, p-t n-re cserélve. Ha n prím, akkor $\mathbb{Z}[x]/(n, f(x))$ pszeudotest. Ha n összetett, akkor $\mathbb{Z}[x]/(n, f(x))$ vagy nem pszeudotest, és ebben az esetben bizonyítékunk van arra, hogy n összetett; vagy az, és ekkor alkalmazhatjuk Lenstra és Pomerance tételét, feltéve hogy $q_1 q_2 \cdots q_k > (\log n)^2$ n tesztelésére. Valójában ők bebizonyították, hogy létezik ilyen f $q_1 q_2 \cdots q_k$-val, ami nem sokkal nagyobb $(\log n)^2$-nél:

Feladat: Létezik n_0 konstans, amelyre $n \geq n_0$ esetén léteznek $r_1, r_2, \ldots, r_k < (\log n)^2$ prímek és $q_1, q_2, \ldots, q_k$ páronként relatív prím pozitív egészek, amelyekre q_i osztja $r_i - 1$-et, és $n^{(r_i-1)/q_i}$ rendje $(mod\ r)$ éppen q_i minden egyes i-re úgy, hogy $(\log n)^2 < q_1 q_2 \cdots q_k < 4(\log n)^2$.

Annak meghatározásához, hogy $n^{(r_i-1)/q_i}$ rendje $(mod\ r)$ éppen q_i-e csak azt kell ellenőriznünk, hogy $n^{r_i-1} \equiv 1\ (mod\ r_i)$ teljesül-e, miközben $n^{(r_i-1)/q} \equiv 1\ (mod\ r_i)$. A fenti feladatot felhasználva egyszerűen meg tudunk határozni megfelelő r_i és q_i értékeket $O((\log n)^3)$ lépésben.

Irodalomjegyzék

[1] Farkas Gábor, Kátai Imre: Informatikai algoritmusok 2. Számelmélet című része

[2] Andrew Granville: It Is Easy to Determine Whether a Given Integer Is Prime

[3] David M. Bressoud: Factorization and Primality Testing

[4] Victor Shoup: A Computational Introduction to Number Theory and Algebra

[5] Járai Antal: Számítógépes számelmélet