Algoritmuselmélet és bonyolultságelmélet MSc hallgatók számára

Számelméleti algoritmusok, prímtesztelés

2017. Előadó: Hajnal Péter

1. Számhalmazok bizonyíthatósága

Definíció. Egy $A \subset \mathbb{N}$ halmaz bizonyítható, ha van olyan $\mathcal{A}$ hatékony algoritmus, ami egy (a, π) input-bizonyíték pár esetén eldönti, hogy az $a \in \mathbb{N}$ szám esetén $\pi \in \Sigma^*$ bizonyítja-e $a \in A$ tényét. Elvárjuk, hogy ha minden $a \in A$ szám esetén létezzen $\pi(a)$ bizonyíték, amire $\mathcal{A}$ elfogadja $(a, \pi(a))$-t. Míg $a \notin A$ esetén $\mathcal{A}$ elvessen minden π bizonyítékot.

A definícióban szereplő π-t bizonyítéknak nevezzük (matematikai szóhasználat). A jogi szóhasználat is gyakori: ekkor π „neve" tanú.

A hatékonyság egyelőre egy intuitív fogalom. A félév második felében kap pontos értelmet. Az input a szám $\mathcal{O}(\log a)$ számjeggyel írható le. A hatékonyságra úgy kell gondolnunk, hogy az algoritmus futása alatt az előforduló számok a hosszában polinomiálisak és az elvégezendő műveletek száma is a hosszában polinom sok.

A fogalmat példákkal világítjuk meg:

Példa. Legyen $N = \{n^2 : n \in \mathbb{N}\}$ a négyzetszámok halmaza.

Egy $q = n^2 \in \mathbb{N}$ számhoz egy π bizonyíték lehet n. A bizonyítás-ellenőrző algoritmus megkapja (q, n)-et, az n egészet négyzetre emeli és ellenőrzi egyenlő-e q-val. Ezen egyszerű aritmetikai számolás után vagy elveti a bizonyítékot, vagy biztos benne, hogy q négyzetszám.

Példa. Legyen $H = \{n^m : 2 \leq n, m \in \mathbb{N}\}$ a hatványszámok halmaza.

Egy $q = n^m \in \mathbb{N}$ számhoz egy π bizonyíték lehet n, m. A bizonyítás-ellenőrző algoritmus megkapja (q, n, m)-et, az n egészet m-edik hatványra emeli és ellenőrzi egyenlő-e q-val. Ezen egyszerű aritmetikai számolás után vagy elveti a bizonyítékot, vagy biztos benne, hogy q hatványszám.

A fenti gondolatmenetben van egy kis probléma. n^m-edik kiszámolása problémás lehet. Az n szám értéke 2-től $\sqrt{q}$-ig változhat. m értéke 2-től $\log_2 q$-ig változhat. Ha $n = m = \sqrt{q}$-t kapunk és nem gondolkozunk (nem vesszük észre, hogy m túl nagy), akkor n^m kiszámolása nem lesz hatékony. Maga a szám olyan nagy, hogy nemcsak kiszámolása, de leírása sem lesz hatékony. A fenti algoritmust módosítjuk: $n, n^2, n^4, \ldots$ hatványsorozatot ismételt négyzetre emelésekkel számoljuk, de leállunk, ha a kitevő m fölé megy vagy a hatványérték meghaladja q-t. Ez utóbbi esetben elvetjük a bizonyítékot. Az előző esetben a kettő hatvány kitevők összegeként felírjuk m-et és az m-edik hatványt további szorzásokkal kiszámoljuk. Így nincs veszély, hogy túl nagy számokkal történő aritmetika miatt nem lesz hatékony az algoritmusunk.

Példa. Legyen Ö$= \{n : \text{összetett}\}$, az összetett számok halmaza.

$n \in$Ö esetén n összetettségének legtermészetesebb bizonyítéka egy nem-trviális szorzatként való felírása. Azaz π egy t, t' számpár lesz. Az ellenőrző algoritmus

megnézi t, t' valóban két legalább 2, egész szám, összeszorozza őket és ellenőrzi a szorzat egyenlő-e n-nel. Ha igen,a kkor biztos benne, hogy az n szám összetett. ha nem, akkor a bizonyítékot elveti (ettől a szám még lehet összetett is).

Az összetett számok komplementere a prímszámok P halmaza (most $\mathbb{N}$-ben dolgozva 0 és 1 kategórizálásával nem törődünk). A fenti bizonyíthatósági eredmény Ö-re nem mond semmit P-re. Valójában P is tesztlehető. Ez azonban egyáltalában nem triviális. 1975-ben Pratt írt le egy hatékony bizonyítási sémát.

2. Pratt prímséget bizonyító sémája

Páros számok esetén könnyű dolgunk van. Nincs is szükségünk π bizonyítékra. Ha az input n szám 2, akkor elfogadjuk prímnek, ha az input páros szám nagyobb mint 2, akkor elvetjük.

Könnyű látni, hogy n akkor és csak akkor prím, ha $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ egy $n-1$ elemű ciklikus csoport, azaz alkalmas $1 < g < n$ számra a $g, g^2, g^3, \ldots, g^{n-1}$ $\mathbb{Z}/n\mathbb{Z} - \{0\}$ elemeit sorolja fel. (Az aritmetika $\mathbb{Z}/n\mathbb{Z}$ számtana, azaz $\bmod n$ aritmetikában számolunk). Könnyű látni, hogy ez ekvivalens azzal, hogy a fenti „mértani sorozatban" g^{n-1} az első 1 érték.

Persze ha $g^{n-1} = 1$, de ha valamely $1 \leq \nu < n-1$ esetén $g^\nu = 1$ is igaz lenne, akkor $\nu | n-1$ teljesülne. $g^\nu = 1$-vel együtt $g^{2\nu} = 1$, $g^{3\nu} = 1$, ... is bekövetkezne. Tehát, ha a g hatványai között a g^{n-1}-nél korábbi 1-es előfordulást ki akarjuk zárni, akkor elég $g^{n-1/p}$ értékeket ellenőrizni $n-1$ prím osztóira. Ha ezek egyike sem 1 ($g^{n-1} = 1$ mellett), akkor g bizonyítja $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ azon tulajdonságát, ami mellett biztosak lehetünk n prímségében.

Első megközelítésben arra gondolhatunk, hogy π lehet g és $n-1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_\ell^{\alpha_\ell}$ prímtényezős felírás. Azt könnyű ellenőriznünk, hogy a felsorolt számok (multiplicitásukkal) összeszorozva $n-1$-et adják. Azt is ellenőrizhetjük, hogy $g^{n-1} = 1$ míg $g^{(n-1)/p_i} \neq 1$ $(i = 1, 2, \ldots, \ell)$ $(\mathbb{Z}/n\mathbb{Z})^*$-ban. Ez az azonban nem elég.

Az algoritmus korrektsége azonban azt jelenti, hogy nem lehet „hamis tanúkat előállítani". Hogy ebben bizonyosak legyünk, azt is tudnunk kell, hogy a tanúszalagon felírt prímtényezők valóban prímek.

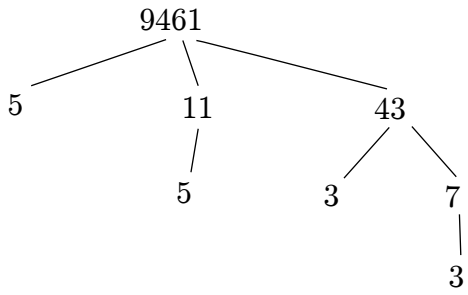
Példa. Tegyük fel, hogy valaki azt bizonyítja, hogy „85 prímszám". Ez nevezséges, de ne feledjük,hogy egy algoritmus az ellenőrző. Egy gépnek kell ítéletet mondani.

A bizonyíték $g = 4$ és $n-1 = 6^1 \cdot 14^1$ prímtényezős felbontás. Minden aritmetika stimmel. Az egyedüli probléma, hogy sem 6, sem 14 nem prímszámok.

A bizonyossághoz látnunk kell, hogy $n-1$ prímtényezős felbontásában szereplő p_i számok valóban prímek. A megoldás egyszerű: rekurzió. Meg kell követelnünk, hogy π tartalmazza $n-1$ prímosztóiról a fent leírt séma szerinti bizonyítást. Azaz mindegyik p_i-hez kell egy g_i szám és $p_i - 1$ prímtényezős felbontása. Az ebben szereplő prímeket is „igazolnunk" kell. És így tovább.

Az input n egy „prímséget állító tétel". π egy g szám és $n-1$ prímtényezős felbontása, amikhez „lemmák" tartoznak (a szerepeltetett p_i-k is prímek). A lemmákhoz segéslemmák tartoznak ... Ezek az állítások egy fastruktúrába rendezhetők. Az input n szám (a főtétel) a gyökérrel van kapcsolatban. Ez alatt vannak $n-1$ páratlan prímosztóira vonatkozó lemmák. Ezek mindegyikének értéke legfeljebb $n - 1/2$. Azaz a fa mélységére az input hoszával arányos ($\mathcal{O}(\log n)$) felső becslést adhatunk. Minden szinten a szereplő számok szorzata n-nél kisebb.

Példa. Tegyük fel, hogy 9461 prímségét igazoljuk. Ehhez a $9461-1 = 2^2 \cdot 5 \cdot 11 \cdot 43$, $43-1 = 2 \cdot 3 \cdot 7$, $11-1 = 2 \cdot 5$, $7-1 = 2 \cdot 3$, $5-1 = 2^2$, $3-1 = 2$ prímtényezős felbontásokat állítjuk. Az állítások struktúrája:



Mindegyik prímséghez egy primitív gyököt is megadunk. Az aritmetika után bizonyosak lehetünk abban, hogy 9461 prím.

Így a szükséges π nem túl hosszú, elolvasható, az ellenőrzéshez szükséges aritmetika hatékonyan elvégezhető.

3. Számhalmazok tesztelése

Definíció. Egy $A \subset \mathbb{N}$ halmaz tesztelhető, ha van olyan hatékony algoritmus, amely adott n input esetén eldönti, hogy $n \in A$ vagy $n \notin A$.

Ismét példákon keresztül legjobb megérteni a fogalmazt.

Példa. Legyen $R(n)$ az n-hez relatív prímek halmaza. Az Euklideszi algoritmus $R(n)$ tesztelhetőségét igazolja.

Példa. Legyen $H = \{n|$ van olyan $2 \leq a, b \in \mathbb{N}$, hogy $n = a^b\}$, a hatványszámok halmaza. H tesztelhető. Adott n-hez a lehetséges b értékek 2 és $\log_2 n$ között vannak. Azaz az összes lehetséges b-re ellenőrizhetjük, hogy n b-edik hatvány. A b-edik hatvány mivolthoz a lehetséges a-t kell megtalálnunk vagy kiszűrnünk. Például $b = 5$ estén azt kell néznünk, hogy $\sqrt[5]{n}$ egész-e. Ha ezt az értéket két egész szomszédos közé be tudjuk szorítani, akkor készen vagyunk. Ez lehetséges numerikus matematikai módszerekkel, de egy algebra nélküli bináris keresés is működik (x^b monoton függvény).

Példa. Legyen $P \subset \mathbb{N}$ a prímek halmaza. Láttuk, hogy P és $\overline{P}$ (az összetett számok halmaza) is bizonyítható. Tesztelhetősége sokkal nehezebb.

A naív algoritmus nem működik. $\sqrt{n}$-ig kellene a számokról (esetleg csak a prímekről) eldöntenünk, hogy osztja-e n-et. A számaink „kicsik”, az oszthatóság hatékonyan tesztelhető. Azonban a $\sqrt{n}$ (esetleg $\pi(\sqrt{n})$) oszthatósági kérdés túl sok. $\sqrt{n}$ exponenciálisan nagy $\log n$-hez képest.

A XXI. század elején történt meg a nagy áttörés: Agrawal, Kayal és Saxena 2002 augusztus 6-án közölte, majd 2004-ben referált publikációként megjelentette az első determinisztikus prímtesztet.

4. Elemi megállapítások

Az alábbiakban p mindig prímszámot, c mindig összetett számot jelöl. A prím/összetett különbség sokszor megjelent számelméleti tanulmányaink során. Ezeket foglaljuk össze. Mindegyik különbség reményt adhat egy tesztelési algoritmus alapjára, de táblázatunkban egyben vázoljuk azt is mi miatt lesz sikertelen az erre alapuló algoritmus.

p PRÍMSZÁM	c ÖSSZETETT SZÁM
Minden $1 \leq a \leq p-1$ egészre $a \nmid p$.	Van olyan $1 \leq a \leq c-1$ egész, hogy $a \mid c$.
	Sajnos ha c egy prím négyzete, akkor egyetlen ilyen a létezik egy $c-1$ elemszámú számhalmazban, amit mi exponenciálisan nagynak tekintünk.
Minden $1 \leq a \leq p-1$ egészre $(a,p) = 1$.	Van olyan $1 \leq a \leq c-1$ egész, hogy $(a,c) \neq 1$.
	Sajnos ha c egy prím négyzete, akkor csupán $\sqrt{c}-1$ ilyen a létezik egy $c-1$ elemszámú számhalmazban, amit mi exponenciálisan nagynak tekintünk.
Minden $1 \leq a \leq p-1$ egészre $a^{p-1} \equiv 1 \pmod{p}$.	Van olyan $1 \leq a \leq c-1$ egész, hogy $a^{c-1} \not\equiv 1 \pmod{c}$.
	$a^{c-1} \pmod{c}$ kiszámolása hatékonyan megoldható. A c-hez nem realtív prímek „lebuktatják” c-t. A többi értékből $(\mathbb{Z}/c\mathbb{Z})^*$ egy részcsoportja c prímségének lehetőségére „hamis tanú”. Ha ez valódi részcsoport, akkor legalább a lehetséges a-k fele lebuktatja c-t. Sajnos végtelen sok olyan szám van (ezeket nevezik Carmichel-számoknak), amelyek esetén $(\mathbb{Z}/c\mathbb{Z})^*$ összes eleme hamis tanú. A legkisebb ilyen szám $3 \cdot 11 \cdot 17$.
$(p-1)! \equiv -1 \pmod{p}$	$(c-1)! \equiv 0 \pmod{c}$
	Sajnos $(c-1)! \pmod{c}$ számolása nehéz feladat
$p \mid \binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$.	c nem osztja $\binom{c}{1}, \binom{c}{2}, \ldots, \binom{c}{c-1}$ valamelyikét.
	Sajnos túl sok értékkel kell dolgozni. A megkülönböztetés nem használható prímtesztelésre.

A fenti jellemzések közül kiemelkedik a kis Fermat-tételen alapuló megkülönböztetés. „Csupán” a Carmichel-számok miatt nem volt sikeres a próbálkozás.

Az alábbiakban leírt két prímtesztelő algoritmus kiindulópontja is a kis Fermat-tétel.

5. Miller—Rabin–teszt

Feltesszük, hogy c egy páratlan összetett szám. Ez nyilván nem megszorítás. Páros számok esetén a prím/összetett megkülönböztetetés nyilvánvaló.

p PRÍMSZÁM	c PÁRATLAN ÖSSZETETT SZÁM
Legyen $p-1=2^e\cdot t$, ahol t páratlan. Minden $1\le a\le p-1$ egészre $a^t\equiv 1 \pmod p$ vagy $a^{2^{e_0}t}\equiv -1 \pmod p$ valamely $0\le e_0<e$ esetén.	Legyen $c-1=2^e\cdot t$, ahol t páratlan. Van olyan $1\le a\le c-1$ egész, hogy ne teljesüljön a következő: $a^t\equiv 1 \pmod c$ vagy $a^{2^{e_0}t}\equiv -1 \pmod c$ valamely $0\le e_0<e$ esetén.

A fenti karakterizáció elemi számelmélet alapján nyilvánvaló. A mögöttes aritmetika elvégeshető. Például az $n-1=2^e\cdot t$ alak megkeresése szinte triviális, szemben a prímtényezős alak meghatározásával szemben (ami jelen tudásunk szerint hatékonyan megoldhatatlan). Így a jellemzés könnyen használható tesztelésre:

Legyen $n\in\mathbb{N}$ egy input természetes szám. (Azt szeretnénk eldönteni, hogy az előző táblázat PRÍM avgy ÖSSZETETT oszlopához tartozik. Feltesszük, hogy n páratlan. Az alábbiakban mindig feltesszük, hogy $1\le a\le n-1$ egész.

RM-Teszt$_a$: Nézzük meg a és n relatív prím-e. Ha nem, akkor n összetett. Írjuk fel $n-1$-et $2^e\cdot t$ alakban, ahol t páratlan. Számoljuk ki a

$$a^{n-1}=a^{2^e\cdot t}, a^{n-1}=a^{2^{e-1}\cdot t}, a^{n-1}=a^{2^{e-2}\cdot t}, \dots a^{n-1}=a^{2\cdot t}, a^{n-1}=a^t$$

sorozat elemeit modulo n. Ha a teszt nem tartalmaz -1-et a második helytől kezdve, míg utolsó eleme nem 1, akkor az n szám elbukja a tesztet, n `biztos összetett`. Ha a teszt kiszámol -1-et az első érték után vagy összes eleme 1, akkor n átment a teszten, n `prímként viselkedik`.

Nyilván prímek átmennek a teszten bármilyen a-t is vegyünk. Ha n összetett, akkor lehetnek olyan a-k, amelyek (n összetettsége ellenére) átengedik n-et. Az ilyen a-kat *hamis tanúnak* nevezzük.

1. Tétel (Miller—Rabin-tétel). *Legyen $n>9$ páratlan összetett szám, melyre $n-1=2^e\cdot t$. Legyen H a hamis tanúk halmaza, azaz*

$$H=\{a\in(\mathbb{Z}/n\mathbb{Z})^*: a^t\equiv 1\ (mod\ n)\ vagy\ a^{2^{e_0}\cdot t}\equiv -1\ (mod\ n)\ valamely\ 0\le e_0<e\text{-re}\}.$$

Ekkor

$$\frac{|H|}{n-1}\le\frac{|H|}{|(\mathbb{Z}/n\mathbb{Z})^*|}\le\frac{1}{4}.$$

A tételt nem bizonyítjuk (az érdeklődő hallgató Apppendix-ben elolvashatja). Következménye az alábbi algoritmus és analízise.

Miller—Rabin prímtesztelési algoritmus: Ha $n = 2$, akkor n prím. Ha $n > 2$ páros, akkor n összetett. Ha n páratlan akkor válasszunk egy véletlen a elemét az $\{1, 2, \ldots, n-1\}$ halmaznak. Végezzük el az RM-Teszt$_a$-t. Az eredmény (`biztos összetett` vagy `prímként viselkedik`) a tesztelés outputja.

2. Tétel. *A fenti algoritmus prím inputokat elfogadja, összetett inputokat legalább* 3/4 *valószínűséggel felismeri/„lebuktatja".*

Az algoritmusunk hibázhat, de csak egyféleképpen: Összetett számra azt mondjuk, hogy prímként viselkedik. (Egy másik hibázási lehetőség, hogy prímszámra `összetettként viselkedik` outputot adunk. Ez azonban esetünkben nem léphet fel.)

Az 1/4-es hibázási valószínűséget az a véletlen választásának és ismételt tesztelésnek független ismételgetésével kisebbé tehetjük. Az ismételgetős algoritmus csak akkor nyilvánít egy n inputot `prímként viselkedőnek`, ha minden teszten átmegy. S-szeri ismétlés esetén a hibázás valószínűsége nyilvánvalóan legfeljebb $(1/4)^S$.

6. Agrawal—Kayal—Saxena-teszt

A teszt az alábbi matematikai megkülönböztetésen alapul:

p PRÍMSZÁM	c ÖSSZETETT SZÁM
Minden $P(x)$ polinomra $$P^p(x) \equiv P(x^p) \pmod p$$	Legyen $P(x)$ egy legalább két monomot tartalmazó polinom, amely együtthatói relatív prímek c-hez, illetve 0-k. Ekkor $P^c(x) \not\equiv P(x^c) \pmod c$
	Sajnos ha P-t binomnak választjuk, akkor is $P^c(x)$ felírása reménytelen.

A kis Fermat-tételhez képest van egy különség. A megkülönböztető a ott lehet, hogy nehezen található meg. Itt megkülönböztető P polinomot könnyen elővehetünk.

Van azonban egy hasonlóság is a klasszikus kis Fermat-tételhez. a^{n-1} túl nagy szám lehet. Ott a „számtan" azért végrehajtható, mert modulo n számolunk. Itt a számtan alapból nehéz: még egy binom P esetén is P^p/P^c egy nagyon hosszú polinom.

A megoldás: „Mesterségesen" elővesszünk egy Q polinomot és modulo Q polinom aritmetikával dolgozunk. Ennek egyetlen oka van: Ha Q foka kicsi, akkor az aritmetikai nehézség megszűnik.

p PRÍMSZÁM	c ÖSSZETETT SZÁM
Minden $P(x), Q(x)$ polinomra $$P^p(x) \equiv P(x^p) \pmod{p, Q}$$	Legyen $P(x)$ egy legalább két monomot tartalmazó polinom, amely együtthatói relatív prímek c-hez, illetve 0-k. Legyen $Q(x)$ alkalmas polinom. Ekkor $P^c(x) \not\equiv P(x^c) \pmod{c, Q}$
	Ha $\deg Q = \mathcal{O}(\log^5 n)$, akkor az aritmetika már végrehajtható (számaink nem robbannak fel, a számolás kevés aritmetikai lépéssel megoldható).

A fenti karakterizáció talán nem annyira ismert. Egyszerűsége ellenére belátjuk.

3. Lemma (Polinomiális kis Fermat-tétel). *(i) Legyen $P(x)$ tetszőleges polinom. Ekkor $P^p(x) \equiv P(x^p) \pmod{p}$.*

(ii) Legyen c egy összetett szám. Legyen $P(x)$ egy legalább két monomot tartalmazó polinom, amely együtthatói relatív prímek c-hez, illetve 0-k. $P^c(x) \not\equiv P(x^c) \pmod{c}$

Bizonyítás. (i) Legyen $P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$. Ekkor a multinomiális tétel alapján

$$P^p(x) = a_d^p (x^d)^p + a_{d-1}^p (x^{d-1})^p + \ldots + a_1^p x^p + a_0^p + \text{további tagok.}$$

A kis Fermat-tétel alapján $a_i^p \equiv a_i \pmod{p}$. Nyilván $(x^e)^p = (x^p)^e$. A további tagokban a megfelelő x hatvány együtthatója egy $\frac{p!}{k_d! k_{d-1}! \ldots k_1! k_0!}$ alakú szám, ahol az összes k_i kisebb mint p. Így az összes további tag együtthatója p-vel osztható, azaz modulo p értéke 0. A nem-0 együtthatójú tagok éppen $P(x^p)$-t adják.

(ii) Legyen $P(x) = \alpha x^d + M(x)$, ahol $\deg M(x) = \delta < d$. Legyen $M(x) = \beta x^\delta + \ldots$. legyen $K(< c)$ az a legnagyobb egész, hogy $c \nmid \binom{c}{K}$ Ekkor binomiális tétel alapján

$$P^c(x) = \alpha^c x^{dc} + \ldots + \binom{c}{K} \alpha^K x^{dK} \beta^{c-K} x^{\delta(c-K)} + \ldots$$

ahol a tagok a binomiális együtthatójuk alsó száma szerint csökkennő és azon belül az x hatványának kitevője szerint csökkenő sorrendben vannak felsorolva. A kiemelt két tag között minden együttható osztható c-vel K választása miatt. A végső fel nem sorolt tagok nem ejthetik ki a második feltüntetett monomot, mert fokszámuk kisebb. Ez amely az állítást igazolja. ■

A megkülönböztető tulajdonság után természetes a következő teszt:

AKS-Teszt$_{P,Q}$:

$$P^n(x) \equiv ? P(x^n) \pmod{n, Q}$$

Ha a kongruencia teljesül, akkor n `prímként viselkedik`. Más esetben n `biztos összetett`.

Ha Q foka $\mathcal{O}(\log^5 n)$, akkor a teszt hatékonyan elvégezhető. Prím input esetén a teszt biztosan elfogadja. Összetett input esetén lehetnek hamis tanúk, amely (P, Q) pároknál a teszt prímszerű viselkedést mutat.

4. Tétel (Agrawal—Kayal—Saxena-tétel). *Legyen n egy öszetett szám, amely nem hatványszám. Legyen*

$$\mathcal{P} = \{x+1, x+2, x+3, \ldots, x+\rho\},$$

$$\mathcal{Q} = \{x-1, x^2-1, x^3-1, \ldots, x^\rho - 1\}$$

ahol $\rho = \mathcal{O}(\log^5 n)$. Tegyük fel, hogy $2, 3, \ldots, \rho$ egyike sem osztja n-et, azaz n legkisebb prímosztója $\Omega(\log^5 n)$.

Ekkor van olyan $P \in \mathcal{P}$ lineáris binom és $Q \in \mathcal{Q}$, amelyre (P, Q) „lebuktatja" n-et az AKS-Teszt$_{P,Q}$ teszten .

A tétel következménye az alábbi polinomiális futási idejű prímtesztelési algoritmus.

Agrawal—Kayal—Saxena prímtesztelési algoritmus:
Teszteljük, hogy n prímhatvány-e. Ha igen, akkor n `biztos összetett`.

Legyen $\rho = \mathcal{O}(\log^5 n)$ és ellenőrizzük, hogy $2, 3, \ldots, \rho$ osztja-e n-et. Ha bármelyik oszthatóság teljesül, akkor n `biztos összetett`.

Ha egyik oszthatóság sem teljesül, akkor legyen

$$\mathcal{P}_0 = \{x+1, x+2, x+3, \ldots, x+\rho\},$$

$$\mathcal{Q} = \{x-1, x^2-1, x^3-1, \ldots, x^\rho - 1\}$$

Minden $(P, Q) \in \mathcal{P}_0 \times \mathcal{Q}$ esetén végezzük el az $P^n(x) \equiv ? P(x^n) \pmod{n, Q}$ tesztet. Ha bármelyik nem teljesül, akkor n `biztos összetett`. Ha mindegyiken átmegy az n input, akkor n `biztos prím`.

Az algoritmus korrektsége az AKS tételből nyilvánvaló. A matematikai technikai nehézségeket, bizonyításokat egy appendix-ben részletezzük.

7. Appendix I: Elemi számelméleti háttér MR véletlen prímteszteléshez

Jelölés. $\mathbb{Z}$ az egész számok gyűrűje. $n\mathbb{Z}$ az n-nel osztható számok halmaza, egy ideál $\mathbb{Z}$-ben. $\mathbb{Z}/n\mathbb{Z}$ a modulo n maradékosztályok gyűrűje.

p prím esetén $\mathbb{Z}/p\mathbb{Z}$ test lesz, amelyet $\mathbb{F}_p$-vel is jelölünk. $\mathbb{F}_p^*$ elemeit a nem-0 modulo p maradékosztályok alkotják. Ezen a szorzás egy csoport struktúrát ad. Ismert, hogy ez egy ciklikus csoport $p-1$ elemmel.

Általános n egész esetén $(\mathbb{Z}/n\mathbb{Z})^*$ elemei az n-hez relatív prím maradékosztályok. Ezen a szorzás egy csoport struktúrát ad. A csoport elemszáma $\varphi(n)$. Ha $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, akkor

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) = p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1} \cdot (p_1 - 1) \cdot \ldots \cdot (p_k - 1).$$

Ha $n = p^\alpha$ páratlan prímhatvány, akkor $(\mathbb{Z}/n\mathbb{Z})^*$ egy $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$ elemű ciklikus csoport.

A Miller—Rabin-teszthez szükségünk lesz egy új, ℓ paraméterre.

Definíció. Legyen $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Jelölje $\ell = \ell(n)$ azt a maximális természetes számot, amelyre $2^\ell | p_1 - 1, p_2 - 1, \ldots, p_k - 1$.

A paraméter jelentőségét az alábbi lemma mutatja.

5. Lemma. *Ha $x \in H \subset \mathbb{Z}/n\mathbb{Z}$, akkor $x^{2^{\ell-1}t} = \pm 1$.*

Bizonyítás. Ha $x^t = 1$ az oka $x \in H$-nak, akkor az állítás nyilvánvaló. Ha $x^{2^m t} = -1$ $(0 \leq m < e)$ az oka $x \in H$-nak, akkor $x^{2^m t} \equiv -1 \pmod{p_i}$ is igaz minden $p_i | n$ esetén. Tehát $x^{2^{m+1}t} \equiv 1 \pmod{p_i}$, azaz x rendje $(\mathbb{Z}/\mathbb{Z}_{p_i})^*$-ben osztója $2^{m+1}t$-nek. Azaz $p_i - 1 | 2^{m+1}t$ minden $p_i | n$ prímre. Így $m + 1 \leq \ell$, azaz $m \leq \ell - 1$. Az állítás most is adódik. ■

A Lemma állítása másként megfogalmazva:

$$H^+ := \{x \in (\mathbb{Z}/n\mathbb{Z})^* : x^{2^{\ell-1}t} = \pm 1\} \supset H.$$

Belátjuk, hogy $|H^+|/|(\mathbb{Z}/n\mathbb{Z})^*| \leq 1/4$. Ebből a Miller—Rabin-tétel egyből adódik.

$$H^+ = H_1^+ \dot\cup H_{-1}^+ := \{x \in (\mathbb{Z}/n\mathbb{Z})^* : x^{2^{\ell-1}t} = 1\} \dot\cup \{x \in (\mathbb{Z}/n\mathbb{Z})^* : x^{2^{\ell-1}t} = -1\}$$

Először H_1^+ elemszámát vizsgáljuk. Ez azon $x \in (\mathbb{Z}/n\mathbb{Z})^*$-ek száma, amelyek megoldásai az $X^{2^{\ell-1}t} = 1$ egyenletenek. Ez az egyenlet a kínai maradék tétel alapján ekvivalens az alábbi kongruenciarendszerrel.

$$\begin{cases} x^{2^{\ell-1}t} \equiv 1 \pmod{p_1^{\alpha_1}} \\ x^{2^{\ell-1}t} \equiv 1 \pmod{p_2^{\alpha_2}} \\ \qquad \vdots \\ x^{2^{\ell-1}t} \equiv 1 \pmod{p_k^{\alpha_k}} \end{cases}$$

Az i-edik kongruencia a $(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^*$ ciklikus csoportra vonatkozik, megoldás száma

$$lnko(2^{\ell-1}t, p_i^{\alpha_i - 1}(p_i - 1)) = 2^{\ell-1} lnko(t, p_i - 1).$$

Tehát a kongruenciarendszer megoldásainak száma

$$|H_1^+| = \prod_{i=1}^{k} 2^{\ell-1} lnko(t, p_i - 1).$$

A gondolat megismétlésével azt kapjuk, hogy H_{-1}^+ ugyanekkora méretű, azaz $|H^+| = 2|H_1^+|$. Így

$$\frac{|H^+|}{(|\mathbb{Z}/n\mathbb{Z})^*|} = 2\frac{\prod_{i=1}^{k} 2^{\ell-1} lnko(t, p_i - 1)}{\prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)} = 2\prod_{i=1}^{k} \frac{2^{\ell-1} lnko(t, p_i - 1)}{p_i^{\alpha_i - 1}(p_i - 1)}.$$

Vegyük észre, hogy $2^{\ell-1} lnko(t, p_i - 1) | \frac{p_i - 1}{2}$, azaz a produktumjel mögötti i-edik tényező legfeljebb $\frac{1}{2p_i^{\alpha_i - 1}}$. A fenti kifejezésre kell 1/4-es felső becslést adnunk. A bizonyítást egyszerű eset analízis fejezi be:

1. eset: n-nek legalább három különböző prímtényezője van. Ekkor a szorzatunknak legalább három tényezője van a kezdő 2-es faktor után, amelyek mindegyike legfeljebb 1/2, az állítás nyilvánvaló.
2. eset: n-nek pontosan két különböző prímtényezője van és egyik legalább kettő multiplicitással. Legyen p az a prímtényező (amelyről n paritása miatt tudjuk, hogy páratlan), amely multiplicitása legalább 2. Ekkor szorzatunk legfeljebb $2 \cdot \frac{1}{2} \cdot \frac{1}{2p}$. Ez nem nagyobb mint 1/4 (valójában legfeljebb 1/6).
3. eset: n két különböző prím szorzata, $n = p_1 \cdot p_2$ ($p_1 \neq p_2$). Ekkor a becsülendő kifejezés

$$2 \cdot \frac{2^{\ell-1} lnko(t, p_1 - 1)}{p_1 - 1} \cdot \frac{2^{\ell-1} lnko(t, p_2 - 1)}{p_2 - 1}.$$

Ha $2^{\ell-1} lnko(t, p_1 - 1) | \frac{p_1-1}{2}$ és $2^{\ell-1} lnko(t, p_2 - 1) | \frac{p_2-1}{2}$ bal oldalai közül valamelyik valódi osztó, akkor ismét készen vagyunk.

Belátjuk, hogy ez szükségszerű. Tegyük fel, hogy $2^{\ell-1} lnko(t, p_1 - 1) = \frac{p_1-1}{2}$ és $2^{\ell-1} lnko(t, p_2 - 1) = \frac{p_2-1}{2}$, azaz $2^{\ell} lnko(t, p_1 - 1) = p_1 - 1$ és $2^{\ell} lnko(t, p_2 - 1) = p_2 - 1$. Nyilván $p_1 - 1 = 2^{\ell} \cdot t_1$ és $p_2 - 1 = 2^{\ell} \cdot t_2$, ahol t_1, t_2 páratlan számok és osztják t-t. Tudjuk, hogy $n - 1 = p_1 p_2 - 1 = 2^e \cdot t$, azaz $p_1 - 1 = 2^e \cdot t - p_1(p_2 - 1)$. Ebből következik, hogy $t_1 | t_2$. Hasonlóan adódik, hogy $t_2 | t_1$, azaz $t_1 = t_2$. Ez ellentmond annak, hogy $p_1 \neq p_2$. Az állítás adódik.
4. eset: n prímhatvány, azaz $n = p_1^{\alpha_1}$. Ekkor a kifejezésünk felülről becsülhető $2 \cdot 1/2p_1^{\alpha-1}$ kifejezéssel. Mivel n (így p_1 is) páratlan és nagyobb mint 9 az állítás most is adódik.

Megjegyzés. Ha $|H|/(n-1)$ felső becslésénél megelégedtünk volna 1/2-del, akkor egyszerűbb lett volna végső eset analízisünk.

8. Appendix II: Számelméleti háttér AKS prímtesztéshez

A következő célt tűzzük ki: Legyen n egy összetett szám. Mutatunk egy kicsi, alacsonyfokú $\mathcal{Q}$ polinomhalmazt és egy $\mathcal{P}$ lineáris binom-halmazt a következő tulajdonságokkal

(i) $|\mathcal{Q}| = |\mathcal{P}| = \mathcal{O}(log^5 n)$, azaz $\mathcal{Q}, \mathcal{P}$ elemei kimeríthetően végignézhetők.

(ii) $\mathcal{P}$ elemei binomok, $\mathcal{Q}$ elemeinek fokszáma $\mathcal{O}(\log^5 n)$, azaz az AKS-Teszt$_{P,Q}$ hatékonyan elvégezhető.

(iii) $\mathcal{Q}$ elemei között lesz egy Q_0 olyan, amelyre $\mathcal{P}$-nek nem lesz minden P eleme olyan, hogy (P, Q_0) hamis tanú lesz az AKS-Teszt$_{P,Q_0}$-re nézve, ha n-et teszteljük.

A cél teljesülése esetén egy egyszerűen adódik az AKS algoritmus helyessége. A cél elérhető, ha n nem hatványszám és nincs kis prímosztója.

6. Tétel (Agrawal—Kayal—Saxena-tétel). *Legyen n egy öszetett szám, amely nem hatványszám, és amely összes prím osztója $\Omega(\log^5 n)$. Legyen*

$$\widehat{\mathcal{P}} = \{x, x+1, x+2, x+3, \ldots, x+(n-1)\},$$

$$\mathcal{Q} = \{x-1, x^2-1, x^3-1, \ldots, x^\rho - 1\}$$

ahol $\rho = \alpha \log^5 n$ *alkalmas* α *konstanssal. Ekkor van olyan* $Q_0 \in \mathcal{Q}$*, hogy legfeljebb* $\mathcal{O}(\log^5 n)$ *olyan* $P \in \widehat{\mathcal{P}}$ *lineáris binom van, amelyre az AKS-Teszt*$_{P,Q_0}$ *teszten átmegy* n*.*

Matematikailag a modulo n számolásnál algebrai szempontok miatt egyszerűbb a moduláris aritmetika, ha a modulus p prím.

Például ha $P \in \mathbb{F}_p[x]$ egy $d > 0$-ed fokú polinom, akkor legfeljebb d gyöke lehet multiplicitással számolva. Valóban: Ha $r \in \mathbb{F}_p$ gyök, akkor P maradékos osztással felírható $(x-r)M(x)$ alakban. M-re megismételgetve az eljárást P-t felírhatjuk

$$P(x) = (x-r_1)(x-r_2)\ldots(x-r_s)M_0(x)$$

alakban, ahol M_0-nak már nincs gyöke. Jól látszik az összes gyök: az r_i-k és a fokszám feltétel miatt számuk legfeljebb d. Nem ilyen egyszerű ha $P(x) \in \mathbb{Z}_n[x]$. A fenti felírás ekkor is ugyanígy megkapható. Látjuk az r_i gyököket. Az összes gyök azonban nem látszik. Ha az r_i-ktől különböző értéket helyettesítünk be, akkor nem-nulla értékek szorzatát kapjuk. Ez modulo n aritmetikában lehet 0. Az r_i-ken túl lehetnek új gyökök, számuk becslése nem annyira egyszerű.

Hasonló jelenség igaz moduláris polinom aritmetikánál. Ha a modulus irreducibilis polinom, akkor matematkailag jobb viselkedéssel találkozunk.

7. Lemma (Alap-lemma). *Legyen* $I(x) \in \mathbb{F}_p[x]$ *egy irreducibilis polinom. Legyen* $P(Y) \in \mathbb{F}_p[Y]$ *polinom, amely foka* $d > 0$*. Vegyük azokat az* $R(x) \in \mathbb{F}_p[x]/(I(x))$ *polinomokat, amelyek* P *gyökei, azaz* $P(R(x)) = 0$ $\mathbb{F}_p[x]/(I(x))$*-ben. Ezekből a gyökökből legfeljebb* d *darab lehet.*

Bizonyítás. Legyen $R(x)$ egy gyök. Végezzünk $P(Y) \in \mathbb{F}_p[Y] \subset (\mathbb{F}_p[x]/(I(x)))[Y]$-en $Y - R(x)$-szel maradékos osztást. Kapjuk, hogy $P(Y) = (Y - R(x))M$, ahol $M \in (\mathbb{F}_p[x]/(I(x)))[Y]$. M-re ismételgetve az eljárást $P(Y)$-t felírhatjuk

$$P(Y) = (Y-R_1)(Y-R_2)\ldots(Y-R_s)M_0(Y,x)$$

alakban, ahol M_0-nak már nincs gyöke $\mathbb{F}_p[x]/(I(x))$-ben. Jól látszik az összes gyök: az R_i-k és a fokszám feltétel miatt számuk legfeljebb d. Hogy ez nyilvánvaló legyen lényeges, hogy I egy irreducibilis polinom. ■

A továbbiakban szeretnénk a fent vázolt matematikai „előnyöket" használni. Legyen p az n szám egy prím osztója. Legyen I a $Q \pmod p$ polinom egy irreducibilis faktora.

Fix Q polinomra szeretnénk felülről becsülni azon polinomok számát, akik hamis tanúk n-hez, azaz $P^n(x) \equiv P(x^n) \pmod{n, Q}$. Sokkal kényelmesebb lesz azon polinomok számát becsülni, amelyek $P^n(x) \equiv P(x^n) \pmod{p, I}$ értelemben hamis tanúk. Ezt fogjuk tenni. Ez matematikailag könnyebb lesz, algoritmus elméletileg pedig megfelelő: Ha P olyan, hogy az n szám a $P^n(x) \stackrel{?}{\equiv} P(x^n) \pmod{p, I}$ teszten lebukik, akkor természetesen a $P^n(x) \stackrel{?}{\equiv} P(x^n) \pmod{n, Q}$ teszten is lebukik. Így igaz, hogy a modulo p, I tesztet nem tudjuk elvégezni (magát p-t sem tudjuk kiszámolni), de az eredeti (számunkra elvégezhető) tesztre ott lesz a „sok" lebuktató P, ami szükséges az algoritmusunk helyességéhez.

⋆ ⋆ ⋆

Lássuk a matematikai lényeget.

Fixáljunk egy r kitevőt, azaz vele egy $Q = x^r - 1$ polinomot.

Definíció. Legyen

$$H_r = \{P(x) \in \mathbb{Z}[x] : P^n(x) \equiv P(x^n) \pmod{n, x^r - 1}\},$$

azaz azon P polinomok halmaza, amelyek $x^r - 1$-gyel együtt hamis tanúk lesznek n számára.

8. Lemma. *Ha $P, P_1, P_2 \in H_r$, akkor*

(i) $P + S_1 \cdot (x^r - 1) + S_2 \cdot n \in H_r$ is teljesül tetszőleges $S_1, S_2 \in \mathbb{Z}[x]$ polinomra,

(ii) $P_1 P_2 \in H_r$ is teljesül,

Bizonyítás. (i)

$$(P(x)+S_1(x)(x^r-1)+S_2(x)\cdot n)^n \equiv P^n(x) \equiv P(x^n) \equiv P(x^n)+S(x^n)((x^n)^r-1) \pmod{n, x^r-1},$$

használva a trinomiális tételt, a $P \in H_r$ feltevést és azt hogy $x^r-1 | x^{nr}-1 = (x^n)^r-1$.

(ii)

$$(P_1P_2)^n(x) = (P_1(x)P_2(x))^n = P_1^n(x)P_2^n(x) \equiv P_1(x^n)P_2(x^n) = (P_1P_2)(x^n) \pmod{n, x^r-1}.$$

■

Ezek után H_r-re tekinthetünk mint $\mathbb{Z}_n[x]/(x^r - 1)$ osztályainak uniójára, amely zárt a szorzásra. Ezzel a szemüveggel H_r már véges lesz.

Definíció. Legyen

$$\mathcal{E} = \{x^{n^i \cdot p^j} : i, j \in \mathbb{N}\}.$$

A következő lemma rámutat $\mathcal{E}$ jelentőségére.

9. Lemma. *Legyen $N = n^i p^j$ $(i, j \in \mathbb{N})$, azaz $X^N \in \mathcal{E}$. Ekkor $P \in H_r$ esetén*

$$P^N(x) \equiv P(x^N) \pmod{p, I}.$$

Bizonyítás. Legyen

$$\mathcal{N} = \{N : P^N(x) \equiv P(x^N) \pmod{p, I} \text{ minden } P \in H_r \text{ esetén}\}.$$

Nyilván $1, p, n \in \mathcal{N}$. Elég bizonyítani, hogy $\mathcal{N}$ zárt a szorzásra. Ha $N, M \in \mathcal{N}$ és $P \in H_r$, akkor

$$P^{NM}(x) = \left(P^N(x)\right)^M \equiv \left(P(x^N)\right)^M \equiv P((x^N)^M) = P(x^{NM}) \pmod{n, x^r - 1},$$

ahol az utolsó kongruencia $M \in \mathcal{N}$ miatt modulo $\left(x^N\right)^r - 1$ látható, de ez számunkra jó. ■

Fixáltuk r-et. Nézzük az x^r-1-hez hamis tanúkat, ha a polinomainkat redukáljuk modulo p, ahol p az n szám egy prím osztója.

$$\widetilde{H}_r = \widetilde{H}_r(p) = \{P(x) \in \mathbb{Z}[x] : P^n(x) \equiv P(x^n) \pmod{p, x^r-1}\}.$$

Fixáltuk r-et. Nézzük az x^r-1-hez hamis tanúkat, ha a polinomainkat redukáljuk modulo p és moduló I, ahol p az n szám egy prím osztója, I az $1+x+\ldots+x^{r-1} = x^r-1/x-1$ polinom egy irreducibilis tényezője.

$$\widehat{H}_r = \widehat{H}_r(p, I) = \{P(x) \in \mathbb{Z}[x] : P^n(x) \equiv P(x^n) \pmod{p, I}\}.$$

Mint fent $\widehat{H}_r$ a $\mathbb{F}_p[x]/(I)$ osztályainak uniójaként fogható fel. p prím, I irreducibilis így $\mathbb{F}_p[x]/(I)$ egy test. Tehát H_r elemeit tekinthetjük mint $\mathbb{F}_p[x]$ test feletti polinomgyűrű elemeit, vagy $\mathbb{F}_p[x]/(I)$ test elemeit.

A következő paraméter nagyon fontos lesz a későbbiekben.

Definíció. Legyen L az $x^{n^i p^j}$ különböző polinomok modulo p, I (azaz $\mathbb{F}_p[x]/(I)$-beli elemek) száma.

10. Lemma. *$P_1, P_2 \in \mathbb{F}_p[x]$ két elem $\widehat{H}_r$-ből. Tegyük fel, hogy P_1, P_2 foka legfeljebb $d < L$. Amennyiben $P_1 = P_2$ teljesül $\mathbb{F}_p[x]/(I)$-ben, akkor $P_1 = P_2$ $\mathbb{F}_p[x]$-ben is igaz.*

Bizonyítás. Vegyük a $P_1(Y) - P_2(Y) \in \mathbb{F}_p[Y]$ polinomot. Foka legfeljebb d és $\mathcal{E}$ minden eleme gyöke (lásd korábbi lemma). Ha ezen gyökök száma meghaladja a d felső becslést a fokra az alap-lemma szerint csak úgy lehet, ha $P_1(Y) - P_2(Y) = 0 \in \mathbb{F}_p[Y]$ ■

11. Következmény. *Tegyük fel, hogy*

$$x + a_1, x + a_2, \ldots, x + a_\ell \in H_r$$

különböző binomok $\mathbb{F}_p[x]$-ből és ezekből formálisan különböző legfeljebb $L-1$ tényezős szorzatokat készítünk. Ekkor a kapott szorzatok H_r elemei lesznek és $\mathbb{F}_p[x]/(I)$-ben különböznek.

Megjegyzés. A következményben szereplő $\ell := |\widehat{H}_r \cap \mathcal{P}|$ paramétert a későbbiekben is használjuk.

Bizonyítás. H_r zárt a szorzásra, tehát a képzett szorzatok H_r elemei lesznek.

Másrészt a szorzatok gyökei mint $\mathbb{F}_p$ feletti multihalmazok különböznek. Így különböző $\mathbb{F}_p[x]$-beli polinomokról beszélünk. A korábbi lemma alapján készen vagyunk. ■

12. Következmény.

$$|\widehat{H}_r| \geq \binom{L+\ell-1}{L-1} \geq \left(\frac{\ell}{L}\right)^{L-1}.$$

Bizonyítás. Az ℓ különböző binomból legfeljebb $L-1$ fokú szorzatot $\binom{L+\ell-1}{L-1}$-féleképpen készíthetünk.

$$\binom{L+\ell-1}{L-1} = \frac{(\ell+L-1)(\ell+L-2)\ldots(\ell+3)(\ell+2)(\ell+1)}{(L-1)(L-2)\ldots\cdot 3\cdot 2\cdot 1}.$$

A számláló mind a $L-1$ tényezője nagyobb mint ℓ, a nevező mind a $L-1$ tényezője kisebb mint L. Ebből az utolsó egyenlőtlenség nyilvánvaló. ■

$|\widehat{H}_r|$-et a másik oldalról is becsülhetjük.

13. Lemma.

$$|\widehat{H}_r| \leq n^{2\sqrt{L}}.$$

Bizonyítás. Legyen

$$\mathcal{E}_0 = \{x^{n^i \cdot p^j} : 0 \leq i, j \leq \sqrt{L}\}.$$

Nyilván $|\mathcal{E}_0| > L$. Gondoljunk bele a „nyilván" módosítószó-ba; itt használjuk, hogy n nem hatványszám! Azaz lesz két eleme (mondjuk x^N és x^M, ahol $N \neq M$), amelyek $\mathbb{F}_p[x]/(I)$-ben azonosak.

Ekkor $Y^N - Y^M$ egy legfeljebb $n^{2\sqrt{L}}$ fokú polinom, amelynek minden $\widehat{H}_r$-beli polinom (mint $\mathbb{F}_p[x]/(I)$-beli elem) gyöke (lásd korábbi lemma).

Ismét az alap-lemmára kell hivakoznunk és készen vagyunk. ■

A kétféle becslés összevetéséből adódik, hogy

$$\left(\frac{\ell}{L}\right)^{L-1} \leq n^{2\sqrt{L}},$$

azaz

$$\ell \leq L \cdot 2^{2\log n \frac{\sqrt{L}}{L-1}}.$$

A bizonyítás befejezése, hogy ez a felső becslés $\log n$ hatvány lesz, ha r-et alkalmasan választjuk (ahol elköteleztük magunkat kicsi r érték mellett).

Először is rögzítjük, hogy r-et p-től különböző prímszámnak választjuk.

14. Lemma. *r prímkénti választása után L értékére teljesül, hogy*

$$ord_{\mathbb{F}_r^*}(n) \leq L \leq r.$$

Bizonyítás. Legyen t maximiális pozitív egész, hogy $x^1, x^2, x^3, \ldots, x^t$ különböző elemek legyenek $\mathbb{F}_p[x]/(I)$-ben. Mivel $x^r = 1$ $\mathbb{F}_p[x]/(I)$-ben ezért $t|r$. r prím választása miatt $t = 1$ vagy $t = r$.

Ha $t = 1$ lenne, akkor $x = 1$ $\mathbb{F}_p[x]/(I)$-ben. Ezért $I|x^{r-1} + x^{r-2} + \ldots + x + 1$, tova'bba' $r \neq 0$ $\mathbb{F}_p[x]/(I)$-ben. Ez ellentmondás.

Tudjuk, hogy $t = r$ és az x hatványok között $t = r$ darab különböző elem van $\mathbb{F}_p[x]/(I)$-ben. Ebből $L \leq r$ adódik.

Legyen $t' = \mathrm{ord}_{\mathbb{F}_r^*}(n)$. Másrészt x^n, x^{n^2}, …, $x^{n^{t'}}$ kitevői modulo r különbözőek $\mathrm{ord}_{\mathbb{F}_r^*}(n)$ definíciója miatt. Emiatt redukció után $x^1, x^2, x^3, \ldots, x^r$ egy t' elemű részhalmazát alkotják. Tehát $t' \leq L$. ■

15. Lemma. *r megválasztható úgy, hogy alkalmas $\alpha, \beta > 0$ konstansokra*

$$\alpha \log^2 n \leq L \leq r \leq \beta \log^5 n$$

teljesüljön. Így igaz lesz, hogy

$$\ell = \mathcal{O}(\log^5 n).$$

***B*izonyítás.** Válasszunk t és T értéket, célunk az lesz, hogy $\mathrm{ord}_{\mathbb{F}_r^*}(n) > t$ legyen, továbbá $r < T$ is teljesüljön.

$\mathrm{ord}_{\mathbb{F}_r^*}(n) = \tau$ esetén r osztja $n^\tau - 1$-et. $\mathrm{ord}_{\mathbb{F}_r^*}(n) \leq t$ esetén r osztja $(n-1)(n^2-1)\ldots(n^{t-1}-1)(n^t-1)$-et. Ha $\mathrm{ord}_{\mathbb{F}_r^*}(n) \leq t$ igaz lenne $r = 2, 3, 5, 7, 11, \ldots, p_{\pi(T)}$-re

— azaz az összes T-t nem meghaladó prímszámra — akkor $\prod_{q \text{ prím},\, q \le T} q$ osztja $(n-1)(n^2-1)\dots(n^{t-1}-1)(n^t-1)$-et.

Ez nem lehetséges, ha

$$\prod_{q \text{ prím},\, q \le T} q \ge 2^{\pi(T)} \ge n^{t^2} > (n-1)(n^2-1)\dots(n^{t-1}-1)(n^t-1).$$

Ez pedig igaz, ha $t = \alpha \log^2 n$ és $T = \beta \log^5 n$.

A fentiek alapján választva r-et teljesülni fog, hogy

$$\ell \le L \cdot 2^{2 \log n \frac{\sqrt{L}}{L-1}} \le T \cdot \gamma \le \delta \log^5 n. \quad \blacksquare$$

A fentiek alapján készen vagyunk. $\{x+1, x+2, \dots, x+\rho\}$ elemei $\mathbb{F}_p[x]$ különböző elemei, hiszen a halmaz „elővétele” előtt biztosítottuk, hogy $p > \rho$ teljesüljön. Így köztük csak ℓ sok lehet hamis tanú és $\ell < \rho$ is igaz.