Eötvös Loránd Tudományegyetem

Természettudományi Kar

Marton Péter

Prímtesztek és prímfaktorizáció

BSc szakdolgozat

Témavezető:

Freud Róbert, egyetemi docens

Algebra és Számelmélet Tanszék

Budapest, 2012

Tartalomjegyzék

1. Bevezetés

A szakdolgozat témája a Freud Róbert–Gyarmati Edit: Számelmélet könyvben tárgyalt, illetve feladatként feladott prímtesztek, és a Donald Ervin Knuth: A számítógép-programozás művészete könyv II. Szeminumerikus algoritmusok fejezet Próbaosztás, és különösen a Monte–Carlo-módszer prímfaktorizáció. Ez utóbbinak bizonyos vonatkozásait részletesen is elemzem. A felépítés, a bizonyítás és a leírt feladatok megoldása, példák megírása és megoldása saját munkám eredménye. Az érdeklődésemet prímszámok iránt a 8. születésnapomra kapott Matematika SH atlasz eratoszthenészi szitáról szóló ábrája keltett fel, mert a logika mellett ez volt az egyetlen, amit értettem belőle. Továbbá mivel szívesen programozok, érdekelnek az algoritmusok.

2. Prímtesztek

A prímtesztek olyan eljárások, melyek egy adott számot prímnek vagy összetettnek nyilvánítanak, de általában nem határozzák meg annak egy osztóját sem. Attól függően, hogy a teszt használ-e véletlen számokat, beszélünk determinisztikus és nem determinisztikus (más szóval véletlen) prímtesztekről. A determinisztikus prímtesztektől általában elvárjuk, hogy biztos eredményt adjon, míg a véletlen prímteszteknél megengedünk egy minimális valószínűséget a hibás döntésre.

Minden prímteszt valamilyen módon az Euler–Fermat-tételen alapul.

Euler–Fermat-tétel: Minden egynél nagyobb egész n számra és minden n-hez relatív prím a egészre fennáll az

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

kongruencia.

Bizonyítás:

Legyen az $r_1, \ldots, r_{\varphi(n)}$ egy redukált maradékrendszer (RMR). Ekkor az $ar_1, \ldots, ar_{\varphi(n)}$ szintén RMR tetszőleges n-hez relatív prím a-ra, hiszen bármely kettő különbsége ka alakú, ahol k nem osztható n-nel. Vegyük ezt a két felírását (az egyértelmű) RMR-nek:

$$\prod_{i=1}^{\varphi(n)} r_i \equiv \prod_{i=1}^{\varphi(n)} ar_i \pmod{n}.$$

Egy RMR elemeinek szorzata relatív prím a modulushoz, ezért egyszerűsíthetünk vele:

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

2.1. Fermat-prímteszt

Legyen n egy egynél nagyobb egész szám, melyről szeretnénk eldönteni, hogy prím-e. Válasszunk véletlenszerűen egy n-nél kisebb pozitív a egész számot; ekkor az

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

kongruencia biztosan fennáll, ha n prím, az összetett n-ek túlnyomó többségében legfeljebb 50% eséllyel teljesül. A fennmaradó kivételes esetekben n-et univerzális álprímnek nevezzük, ekkor (1) minden n-hez relatív prím a-ra teljesül.

Bizonyítás:

Prímekre ez az Euler–Fermat tétel következménye, hiszen $\varphi(n) = n - 1$, ha n prím. Ha n összetett, és a nem relatív prím hozzá, akkor a-nak minden hatványa többszöröse lesz a és n legnagyobb közös osztójának, tehát (1) nem állhat fenn. Egyébként lásd az 5.7.13 a) feladatot.

2.2. Solovay–Strassen-prímteszt

Legyen n egynél nagyobb páratlan szám. Ekkor az

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

kongruencia az $1, \ldots, n-1$ számok mindegyikére teljesül, ha n prím, és az $1, \ldots, n-1$ számok kevesebb, mint felére teljesül, ha n összetett.

Bizonyítás:

Ha n prím, az Euler–Fermat-tétel szerint, minden 1 és $n-1$ közötti a-ra

$$a^{n-1} \equiv 1 \pmod{n},$$

továbbá $\mathbb{Z}_p$-ben csak ± 1 második egységgyök, így

$$a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}.$$

A Legendre/Jacobi szimbólum definíciója szerint $\left(\frac{a}{n}\right) = \pm 1$. Tehát bizonyítandó:

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

akkor és csak akkor, ha $\left(\frac{a}{n}\right) = 1$, azaz ha az

$$x^2 \equiv a \pmod{n}$$

kongruencia megoldható. Legyen g primitív gyök modulo n, és számoljunk a g szerinti diszkrét logaritmusokkal (indexekkel):

$$g^{2\mathrm{ind}x} \equiv g^{\mathrm{ind}a} \pmod{n}.$$

Mivel g primitív gyök, azaz minden nem 0 maradékosztály előfordul valamilyen hatványaiként (nyilvánvalóan ciklikusan fordulnak elő), a fenti állítások egyenértékűek

$$2\mathrm{ind}x \equiv \mathrm{ind}a \pmod{n-1} \text{ -gyel.}$$

De 2ind$x$ és $n-1$ is osztható kettővel, tehát ha ind$a$ páratlan, a kongruencia nem oldható meg, míg ha ind$a$ páros, úgy

$$\text{ind}x \equiv g^{\frac{\text{ind}a}{2}} \pmod{\frac{n-1}{2}}$$

$$x \equiv \pm g^{\frac{\text{ind}a}{2}} \pmod{p}$$

megoldás. Összefoglalva:

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

akkor és csak akkor, ha ind$a$ páros, azaz

$$\left(\frac{a}{n}\right) = 1.$$

Térjünk rá arra az esetre, amikor n összetett.

Nevezzük cinkosnak a-t egy összetett n-re vonatkozólag akkor, ha (2) teljesül, egyébként pedig tanúnak. Mivel $\left(\frac{a}{n}\right)$ csak n-hez relatív prím a-k esetén értelmezett, n-hez nem relatív prímekre (2) nem teljesül. A gyakorlatban $\left(\frac{a}{n}\right)$ kiszámításakor tényleg kiderül, ha a és n nem relatív prím, lásd az 5.7.2 feladatot. A továbbiakban tegyük fel, hogy a és n relatív prím. Első lépésben csak annyit mutatunk meg, minden összetett n-re létezik a tanú.

Ha n nem négyzetmentes, ossza mondjuk p^2, akkor egy g primitív gyök modulo p^2 tanú, mert

$$g^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}.$$

Ennek bizonyításához indirekt tegyük fel, hogy

$$g^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n},$$

négyzetre emelve

$$g^{n-1} \equiv 1 \pmod{n},$$

amiből p^2-re is következik

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

Az Euler–Fermat-tétel szerint

$$g^{\varphi(p^2)} \equiv 1 \pmod{p^2},$$

s mivel g primitív gyök, a mod p^2 RMR minden elemét fel kell vennie g hatványainak, tehát semmilyen $\varphi(p^2)$-nél kisebb j-re nem állhat fenn

$$g^j \equiv 1 \pmod{p^2}.$$

Tehát

$$g^{n-1} \equiv 1 \pmod{p^2}\text{-ből}$$

rögtön következik

$$\varphi\left(p^2\right) \mid n-1.$$

Kifejtve

$$p\,(p-1) \mid n-1,$$

de

$$p \mid p^2 \mid n \Longrightarrow p \mid n, n-1.$$

Ellentmondás.

Legyen a továbbiakban n négyzetmentes. Válasszuk a bizonyítást két részre aszerint, hogy minden n-hez relatív prím a-ra fennáll

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n}, \tag{3}$$

vagy sem. Ha (3) tényleg fennáll minden n-hez relatív prím a-ra, legyen

$$n = q_1 \cdot \ldots \cdot q_s, \qquad \left(\frac{h}{q_1}\right) = -1,$$

és oldjuk meg a

$$w \equiv h \pmod{q_1}, \qquad w \equiv 1 \pmod{q_i} \qquad 2 \leq i \leq s$$

szimultán kongruenciarendszert. Ekkor (3) miatt

$$w^{\frac{n-1}{2}} \equiv 1 \pmod{n},$$

azonban

$$\left(\frac{w}{n}\right) = \left(\frac{h}{q_1}\right) \cdot \left(\frac{1}{q_2}\right) \cdot \ldots \cdot \left(\frac{1}{q_s}\right) = (-1) \cdot 1 \cdot \ldots \cdot 1 = -1.$$

Azt akartuk megmutatni, hogy létezik legalább egy tanú, és ha (3) teljesül minden n-hez relatív prím a-ra, meg is találtunk egyet:

$$1 \equiv w^{\frac{n-1}{2}} \not\equiv \left(\frac{w}{n}\right) = -1 \pmod{n}.$$

Vizsgáljuk most a másik esetet, tehát azt, amikor van olyan n-hez relatív prím a szám, melyre (3) nem teljesül, azaz

$$a^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}.$$

Mivel egy inkongruencia fennáll a modulus legalább egy prímtényezőjére, válasszuk n-nek alkalmas q_1 prímtényezőjét, tehát

$$a^{\frac{n-1}{2}} \not\equiv 1 \pmod{q_1}$$

Oldjuk meg ezzel az a-val a

$$z \equiv a \pmod{q_1}, \qquad z \equiv 1 \pmod{q_i}, \qquad 2 \leq i \leq s$$

szimultán kongruenciarendszert. Erre a z-re

$$z^{\frac{n-1}{2}} \not\equiv 1 \pmod{q_1}, \qquad z^{\frac{n-1}{2}} \equiv 1 \pmod{q_i}, \qquad 2 \leq i \leq s,$$

tehát $z^{\frac{n-1}{2}}$ sem 1-gyel nem kongruens q_1-re, sem -1-gyel q_2-re, így $z^{\frac{n-1}{2}}$ nem kongruens ± 1-gyel n minden prímtényezőjére, azaz

$$z^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}.$$

Ez a z tanú, hiszen

$$z^{\frac{n-1}{2}} \not\equiv \pm 1 = \left(\frac{z}{n}\right) \pmod{n}.$$

Ezzel beláttuk, hogy összetett n esetén mindenképpen létezik n összetettségét igazoló tanú a Solovay–Strassen-tesztben.

Megmutatjuk, hogy ha már *egyetlen* tanú létezik, úgy a RMR *legfeljebb* fele cinkos.

Először legyen t és c relatív prím n-hez — t tanú, c pedig cinkos; indirekt bebizonyítjuk, hogy ezek tc szorzata tanú. Tegyük fel ugyanis az ellenkezőjét, azaz:

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

Használjuk ki, hogy c cinkos, azaz

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

és szorozzuk össze a két fenti kongruenciát:

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

A hatványozás és a Jacobi-szimbólum multiplikatív; egy n-hez relatív prím c cinkos $\frac{n-1}{2}$-edik hatványa kongruens $\left(\frac{c}{n}\right)$-nel, $\left(\frac{c}{n}\right) = \pm 1$, tehát $c^{\frac{n-1}{2}}$ négyzete kongruens ± 1 négyzetével, azaz 1-gyel. E három azonosságot felhasználva adódik, hogy

$$(tc)^{\frac{n-1}{2}}\, c^{\frac{n-1}{2}} \quad = \quad t^{\frac{n-1}{2}} \left(c^{\frac{n-1}{2}}\right)^2 \quad \equiv \quad t^{\frac{n-1}{2}} \pmod{n}$$

$$t^{\frac{n-1}{2}} \equiv \left(\frac{tc}{n}\right)\left(\frac{c}{n}\right) \equiv \left(\frac{t}{n}\right)\left(\frac{c}{n}\right)^2 = \left(\frac{t}{n}\right) \pmod{n}.$$

Ez éppen azt jelenti, hogy t is cinkos — ez ellentmond az indirekt feltevésnek; bebizonyítottuk, hogy cinkos és tanú szorzata tanú.

Most, hogy tudjuk, cinkosokat tanúval szorozva tanúkat kapunk, látni fogjuk, egyetlen t tanú létezéséből következik, hogy a mod n RMR legalább fele tanú: vegyünk ugyanis $c_1, \ldots, c_k$ inkongruens cinkosokat és szorozzuk mindegyiket t-vel: $tc_1, \ldots, tc_k$ mindegyike tanú — és páronként inkongruensek, lásd az Euler–Fermat tétel bizonyítását a fejezet elején.

2.3. Miller–Lenstra–Rabin-prímteszt

A prímteszt egynél nagyobb páratlan n-ekre működik. Írjuk $n-1$-et $2^k r$ alakba, úgy, hogy már r páratlan legyen ($k \geq 1$). Az Euler–Fermat-tétel szerint ha n prím, minden $a \not\equiv 0 \pmod{n}$-re $a^{n-1} = a^{2^k r} \equiv 1 \pmod{n}$. Ha n prím, modulo n csak ± 1 lehet második egységgyök: $a^{2^{k-1} r} \equiv \pm 1 \pmod{n}$. Ha $a^{2^{k-1} r} \equiv +1 \pmod{n}$, akkor $a^{2^{k-2} r} \equiv \pm 1 \pmod{n}$, és így tovább. Ennek alapján a teszt pontos megfogalmazása:

Legyen $n > 1$ és r páratlan, ahol $n - 1 = 2^k r$. Nevezzük jó sorozatnak $a^{2^0 r}, \ldots, a^{2^{k-1} r}$-et, ha $a^r \equiv 1 \pmod{n}$, vagy van olyan, mely -1-et ad n-re maradékul. Ha n prím, minden $a = 1, \ldots, n-1$-re jó sorozatot kapunk, ha n összetett, $a = 1, \ldots, n-1$ számok kevesebb, mint felére kapunk jó sorozatot.

Bizonyítás: $\mathbb{Z}_p$-ben csak ± 1 a két második egységgyök. Emiatt $a^{2^k r} \equiv 1 \pmod{n}$-ből gyököt vonva ± 1-et kell kapnunk. Ha $+1$-et kapunk, az eljárást megismételhetjük, mígnem k-adszor is gyököt vonva $a^r \equiv \pm 1 \pmod{n}$-et kapunk. Ezzel prím n-ekre beláttuk az állítást.

Nem négyzetmentes n-ekre a bizonyítás ugyanúgy megy, mint a Solovay–Strassen igazolásában láttuk.

Négyzetmentes n-ekre legyen j a legnagyobb szám, melyre még található olyan a, hogy

$$a^{2^j r} \not\equiv 1 \pmod{n} \tag{4}$$

(a maximum létezik, például $a = -1$, $j = 0$ esetén $(-1)^{2^0 r} = -1$). Ekkor n-nek valamely q_1 prímosztójára

$$a^{2^j r} \not\equiv 1 \pmod{q_1}.$$

Oldjuk meg ezzel az a-val a

$$t \equiv a \pmod{q_1}, \qquad t \equiv 1 \pmod{q_i}, \qquad 2 \leq i \leq s$$

szimultán kongruenciarendszert. A feltétel szerint

$$t^{2^j r} \equiv a^{2^j r} \not\equiv 1 \pmod{q_1}.$$

Azonban

$$t^{2^j r} \equiv 1^{2^j r} \equiv 1 \not\equiv -1 \pmod{q_i}, \qquad 2 \leq i \leq s.$$

Így $t^{2^j r}$ sem 1-gyel, sem -1-gyel nem lehet kongruens modulo n, míg a j-nél nagyobb számokra (így $V = j + 1$-re)

$$t^{2^V r} \equiv 1 \pmod{n},$$

tehát t tanú.

Megmutatjuk, hogy ennek a t tanúnak és egy n-hez relatív prím c cinkosnak a szorzata tanú.

Egy j-nél nagyobb x számra

$$(tc)^{2^x r} \equiv 1 \pmod{n}.$$

Mivel c cinkos,

$$c^{2^j r} \equiv \pm 1 \pmod{n},$$

és t-ről feljebb láttuk, hogy

$$t^{2^j r} \not\equiv \pm 1 \pmod{n},$$

e kettő összevetéséből pedig

$$(tc)^{2^j r} \not\equiv \pm 1 \pmod{n}.$$

Ebből a Solovay–Strassen-prímteszt bizonyításának utolsó bekezdésében látott módon kapjuk, hogy az $1, 2, \ldots, n-1$ számok több, mint fele tanú.

2.3.1. Példa

Legyen $n = 561 = 3 \cdot 11 \cdot 17$. Ez univerzális álprím, a Fermat-prímteszttel csak akkor tudnánk igazolni összetettségét, ha a-t n-hez nem relatív prímnek választjuk. Mivel 561 relatíve kis szám, ennek is

$$\frac{\varphi(561)}{561} = \frac{\varphi(3)\,\varphi(11)\,\varphi(17)}{561} \approx 43\%$$

esélye van minden egyes a kiválasztásakor.

A véletlenszerűen választott a legyen 404, írjuk fel $n-1 = 2^4 \cdot 35$-öt.
$404^{560} \equiv 1 \pmod{561}$, hiszen álprím (és 404 relatív prím 561-hez).
$404^{280} \equiv 1 \pmod{561}$; megjegyezzük, $\left(\frac{280}{561}\right) = 1$, így a Solovay–Strassen-prímteszt sem buktatja le.
$404^{140} \equiv 1 \pmod{561}$,
$404^{70} \equiv 67 \pmod{561}$ tehát 561 összetett.

2.3.2. Példa

Ebben a példában a

http://www.chalcedon.demon.co.uk/rgep/cartable.html

oldalon található Largest first and largest last prime factors táblázat Largest first prime and largest last prime up to 10^{17} első sorában látható $n = 410671 \cdot 577981 \cdot 380251 = 90256390764228001$ univerzális álprímet használom. Ennek a különösen nagy számnak a hatványainak a maradékait az erre a célra készített

http://www.math.umn.edu/ garrett/crypto/a01/FastPow.html

oldalon található eszközzel számoltam.

Ezt az n számot a Fermat-prímteszt csak akkor minősíti összetettnek, ha az a-t véletlenül pont n-hez nem relatív prímnek választjuk, ennek esélye próbálkozásonként mindössze $0,00068\%$. Ez azt jelenti, hogy még 10000 próbálkozással is 93% valószínűséggel hibásan prímnek veszi.

Tehát $n - 1 = 2^5 \cdot 2820512211382125$. Egy véletlenszerűen választott a példánkban legyen 12345678901234.
$12345678901234^{2^5 \cdot 2820512211382125} \equiv 1 \pmod{n}$
$12345678901234^{2^4 \cdot 2820512211382125} \equiv 1 \pmod{n}$
$\left(\frac{12345678901234}{90256390764228001}\right) = 1$ Azaz átmegy a Solovay–Strassen-teszten

$$12345678901234^{2^3 \cdot 2820512211382125} \equiv 1 \pmod{n}$$
$$12345678901234^{2^2 \cdot 2820512211382125} \equiv 1 \pmod{n}$$
$$12345678901234^{2^1 \cdot 2820512211382125} \equiv 1 \pmod{n}$$
$$12345678901234^{2^0 \cdot 2820512211382125} \equiv 15151079460239103 \pmod{n}$$

2.4. Lucas-prímteszt

Legyen n kettőnél nagyobb egész szám. Akkor és csak akkor létezik olyan 1 és n közötti a, melyre

$$a^{n-1} \equiv 1 \pmod{n},$$

de $n-1$ minden q prímosztójára

$$a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n},$$

ha n prím.

Bizonyítás: Ha n prím, létezik primitív gyök modulo n, azaz a feltételt kielégítő a. Ha létezik ilyen a, annak a rendje $n-1$-nek osztója, de nem osztója egyetlen valódi osztójának sem: tehát a rendje $n-1$, ezért n prím.

Megjegyzés: Az állítás akkor is igaz marad, ha csak annyit teszünk fel, hogy $n-1$ minden q prímtényezőjéhez létezik egy olyan q-tól függő a_q egész szám melyre

$$a_q^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$$

2.5. Proth-prímteszt

Legyen $n = k \cdot 2^l + 1$, ahol k egy 2^l-nél kisebb páratlan szám; így n akkor és csak akkor prím, ha található olyan a, melyre

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

Megjegyzés: Ha n prím, a kvadratikus nemmaradékok modulo n alkalmasak. Mivel a kvadratikus maradékok és nemmaradékok fele-fele arányban fordulnak elő a mod n RMR-ben, így minden próbálkozásban 50% esélyünk van alkalmas a-t választani, tehát könnyen találhatunk egyet próbálkozással. Míg ha n összetett, gyakran

$$a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n},$$

és ebből biztosan kiderül, hogy összetett.

Bizonyítás:

Ha n prím, akkor — ahogy fentebb említettük — a kvadratikus nemmaradékok modulo n alkalmasak.

Ha n összetett, indirekt tegyük fel,

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

fennáll. Jelölje n egy prímosztóját p. Ekkor $2^l \mid o(a) \mid p-1$, mert

$$a^{\frac{n-1}{2}} \equiv a^{\frac{k\cdot 2^l+1-1}{2}} \equiv a^{k\cdot 2^{l-1}} \equiv -1 \pmod{p},$$

négyzetre emelve $a^{k\cdot 2^l} \equiv 1 \pmod{p}$, tehát $o(a)$ prímtényezős felbontásában l-edik hatványon szerepel a 2, azaz $2^l \mid o(a)$. Továbbá $o(a) \mid \varphi(p) = p-1$, ezek szerint $2^l \mid p-1$— kongruenciával kifejezve:

$$p \equiv 1 \pmod{2^l}.$$

Ezért $p = 1 + c \cdot 2^l$, továbbá

$$n \equiv k \cdot 2^l + 1 \equiv 1 \pmod{2^l}.$$

Mivel mind p, mind n kongruens 1-gyel modulo 2^l, ezért

$$\frac{n}{p} \equiv 1 \pmod{2^l},$$

így

$$n = p\frac{n}{p} = \left(1 + c \cdot 2^l\right)\left(1 + d \cdot 2^l\right) > 1 + cd2^{2l} > 1 + k2^l = n.$$

Ellentmondás.

2.6. Pepin-prímteszt

Legyen $F_n = 2^{2^n} + 1$. $n > 0$ esetén F_n akkor és csak akkor prím, ha

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

Bizonyítás:

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

négyzetre emelésével

$$3^{F_n-1} \equiv 1 \pmod{F_n}$$

adódik. Így $o(3) \mid 2^{2^n}$, de $o(3) \nmid 2^{2^{n-1}}$, ezért $o(3) = 2^{2^n}$, így legalább ennyi relatív prím van 0 és F_n között F_n-hez, tehát F_n prím. A másik irány bizonyításához tegyük fel, F_n prím. Az Euler-feltétel szerint

$$3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}.$$

$$2^2 \equiv 1 \pmod{3},$$

tehát ezt $n-1$-szer négyzetre emelve is

$$2^{2^n} \equiv 1 \pmod{3}.$$

Emiatt

$$F_n \equiv -1 \pmod{3},$$

$$F_n - 1 = 2^{2^n} \equiv 0 \pmod{4},$$

tehát a kvadratikus reciprocitási tétel szerint

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = -1.$$

2.7. Pocklington-prímteszt

Legyen $N > 1$ egész, $q > \sqrt{N} - 1$ prímosztója $N - 1$-nek. Az N biztosan prím, ha találunk olyan a-t, melyre

$$a^{N-1} \equiv 1 \pmod{N}, \qquad \text{és} \qquad \left(a^{\frac{N-1}{q}} - 1, N\right) = 1.$$

Megjegyzés: Az első feltétel nem teljesülése esetén az Euler–Fermat tétel miatt N biztosan összetett. Ha

$$1 < \left(a^{\frac{N-1}{q}} - 1, N\right) < N,$$

akkor N-nek még egy osztóját is megtaláltuk. Ezért tekinthetnénk prímfaktorizációnak, mely előtt végrehajtottunk egy Fermat-prímtesztet.

Bizonyítás:

Indirekt tegyük fel, N összetett. Ezért létezik $p \leq \sqrt{N}$ prímosztója. Tehát $p \leq q$, így $(p - 1, q) = 1$. Ezért alkalmas u-ra

$$uq \equiv 1 \pmod{p-1}.$$

$$a^{N-1} \equiv 1 \pmod{N}$$

miatt

$$a^{N-1} \equiv 1 \pmod{p},$$

emiatt

$$\left(a^{N-1}\right)^u = \left(a^{\frac{N-1}{q}}\right)^{uq} \equiv a^{\frac{N-1}{q}} \equiv 1 \pmod{p}.$$

Ez viszont ellentmond

$$\left(a^{\frac{N-1}{q}} - 1, N\right) = 1\text{-nek.}$$

3. Prímfaktorizációk

3.1. Próbaosztás

Lényeges kérdés, milyen sorrendben próbáljuk ki a $2 \leq d \leq \lfloor\sqrt{n}\rfloor$ próbaosztókat. Ugyanis, ha a vizsgált n számra nem teszünk feltételeket,

$$\mathrm{P}\left(d \mid n\right) = \frac{1}{d},$$

tehát a kisebb számok valószínűbben osztanak egy véletlenszerűen választott összetett számot. Ha egy véletlenszerűen választott számról csak bizonyos p hiba valószínűséggel szeretnénk eldönteni, hogy prím-e, ismét célszerű az első néhány kis számmal osztani. Tegyük fel, $p_i \nmid n$, ahol p_i néhány különböző prímszám. Ekkor

$$\mathrm{P}\left(\nexists p_i \mid n\right) = \prod_i \left(1 - \frac{1}{p_i}\right)$$

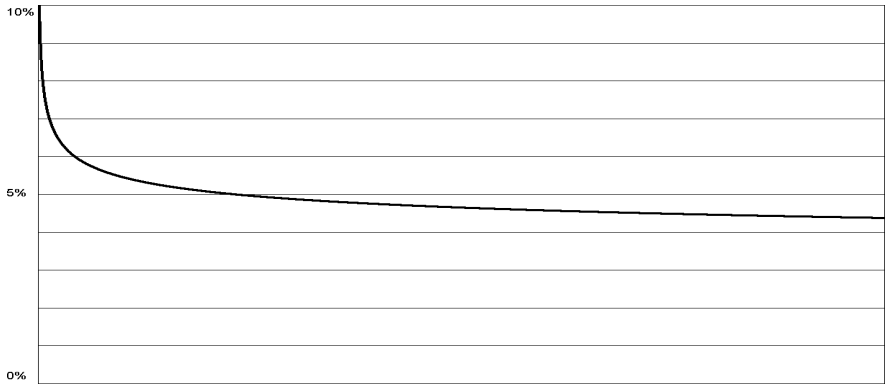
Ez érvényes akkor is, ha n-ről feltesszük, hogy összetett, hiszen a prímek sűrűsége 0, azaz

$$\lim_{n\to\infty} \frac{\pi\left(n\right)}{n} = 0.$$

Emiatt *elméletileg* kiváló prímteszt, ha minden számot összetettnek minősítünk, a hiba valószínűsége határértékben 0 (prímeket összetettnek minősíthet). Ami a *gyakorlatban* használható, az mindent prímnek minősít, kivéve, amiről biztosan kiderül, hogy összetett. Ezek a bizonytalan számok, melyeket prímnek minősít, 1 valószínűséggel összetettek: a hiba valószínűsége tehát egyenlő a bizonytalan számok arányával. Mindezt egy táblázatban szemléltetjük: az első k prímszámmal való próbaosztás után milyen E valószínűséggel döntünk hibásan? Jól látszik, hogy a 15–20%-os hibahatárt szinte azonnal elérjük, a 10%-osért már jóval többet kell dolgoznunk, kb. az 5%-os, amit számítógéppel érdemes kitűzni, aztán elképesztően lassan tart E a nullához a vizsgált prímszámok függvényében. Mindez még látványosabb, ha megtekintjük a vizsgált prímszámok nagyságrendjét (a p_k oszlopban) a túloldali ábrákon. Gyorsabban tudunk számokat szorozni, mint

osztani, ezért a számok méretétől és mennyiségétől függően érdemes lehet sok próbaosztót inkább összeszorozni modulo n, majd ennek legnagyobb közös osztóját kiszámítani a faktorizálandó n számmal. Ilyenkor tovább kényelmesedik a helyzetünk: szóba jövő próbaosztók helyett teljesen véletlenszerűen választott számok szorzatának is kiszámíthatjuk a legnagyobb közös osztóját n-nel. Vegyük észre, hogy a szorzások folyamán a legnagyobb közös osztó nem csökkenhet.

#Prímek	Utolsó	Hiba esélye	Megjegyzés
k	p_k	$E = \prod_i \left(1 - \frac{1}{p_i}\right)$	
1	2	0,5	
2	3	0,3333	
3	5	0,2667	
4	7	0,2286	
10	29	0,1579	
55	257	0,09996	$< 10\%$
100	541	0,08875	
168	997	0,08097	$p_k < 1000$
1000	7919	0,06247	
1229	9973	0,06088	$p_k < 10000$
7398	75037	0,0499996	$< 5\%$
32768	386093	0,04364	Diagram vége
5761455	99999989	0,03048	$p_k < 100000000$
6000000	104395301	0,03041	



3.2. Monte–Carlo-módszer

A Monte–Carlo-módszerrel adott n összetett számot bonthatunk prímtényezőire. Az algoritmus:

1. Válasszunk egy a_0 kezdőértéket, egy g összehasonlító és egy $f : \mathbb{Z}_n \to \mathbb{Z}_n$ iterációs függvényt. Jelölés: $a_{n+1} = f(a_n)$.
2. Számítsuk ki $(a_k - g(a_k), n) = d_k$ legnagyobb közös osztókat (ha $g(a_k)$-t értelmeztük), mígnem $d_k \neq 1$.
3. Ha $d_k \neq n$, megtaláltunk egy osztót; ha $\dfrac{n}{d_k}$ összetett, helyettesítsünk n helyébe, és folytassuk az algoritmust attól az a_k-tól, ahol tartunk. Bár d_k tipikusan prím lesz, de ha d_k véletlenül mégis összetett, ezzel a módszerrel valószínűleg nem tudjuk faktorizálni. Ahhoz, hogy d_k-t faktorizálni tudjuk, válasszunk másik f függvényt (például $\tilde{f} = f + 1$-et), és a_0-tól kezdjük újra d_k faktorizálását; vagy, ha d_k kicsi, érdemesebb a próbaosztást elvégezni.
4. Ha $d_k = n$, nem kaptunk nemtriviális osztót, az eljárás csődöt mondott.

Megjegyzés: nem csak a 3., 4. lépésben található d_k és n/d_k értékekre, hanem n-re is érdemes prímtesztet végrehajtani.

Magyarázat: Vizsgáljuk meg, miért érdemes vennünk két szám, a_k és a_j különbségét, és kiszámítanunk legnagyobb közös osztóját n-nel. Abban reménykedünk ugyanis, hogy n-nek van olyan p prímtényezője, melyre

$$a_k \equiv a_j \pmod{p},$$

hiszen ekkor mind n-nek, mind $a_k - a_j$-nek osztója p. A második kérdés, miért érdemesebb egy f függvénnyel generált sorozat elemeinek különbségét venni, és ezzel kiszámítani n legnagyobb közös osztóját, mint véletlenszerűen választott x_i számokra ellenőrizni (x_i, n)-et, ahogy a próbaosztás című fejezet végén olvashattuk. Ehhez tisztázzuk, hogyan nézzünk az f függvényre.

Első próbálkozásként f helyébe valószínűleg valamilyen lineáris függvényt helyettesítenénk:

$$f(x) = ax + c.$$

Előre közöljük, ebben az esetben semmi értelme nem lenne a módszernek: ilyenkor f általában körbevezet minket a mod n TMR-en. Vizsgáljunk egy bonyolultabb f függvényt egy n faktorizálandó szám p osztója (elsősorban prímtényezője) szerint. Hangsúlyozzuk, ez a vizsgálat teljesen független n-től, csak n-egy p osztójára van szükségünk. Legyen például

$$f(x) = \left(x^2 + 1\right) \bmod n,$$

és egészen mást tapasztalunk: sokkal kisebb körben jön egymás után néhány maradékosztály — megeshet, ebbe a körbe néhány további maradékosztályon keresztül csatlakozunk be, lásd a túloldali ábrán. A tervünk az, hogy egy kis kerületű körben ténylegesen benne lévő p szerint q maradékosztályba tartozó a_0 számot összehasonlítunk a körben következő maradékosztályba tartozó a_1 számmal, majd a rákövetkező maradékosztályba tartozó a_2 számmal, és így tovább. Előbb utóbb körbeérünk, mondjuk a_λ ugyanabba a maradékosztályba a q maradékosztályba tartozik p szerint, mint a_0. Ekkor $a_0 - a_\lambda$-nak és n-nek is osztója p, a legnagyobb közös osztó végre nem 1 lesz. Tervünkben a kisebb probléma az, hogy mennyire hosszú körbe találunk bele a_0 kiválasztásakor. Mondjuk azt, hogy az f függvény megválasztásakor elég ügyesek voltunk ahhoz, hogy egy hosszabb kör is megfeleljen az igényeinknek. A nagyobb probléma az, hogy a_0 egyáltalán nem biztos, hogy egy körön fekszik: lehet, hogy csak egy körbe vezető úton; ez a lehetőség több kellemetlenség forrása. Sajnos képtelenek vagyunk ránézésre eldönteni, vajon egy körön fekszik egy bizonyos a_i szám, vagy sem. Az persze biztos, hogy minél tovább haladunk előre, annál valószínűbb, hogy már tényleg körbe-körbe lépkedünk a maradékosztályokon, de sosem lehetünk benne biztosak. Nincs mit tenni: ha úgy érezzük, túl sokat próbálkoztunk $a_1,\ldots,a_t$-vel, következtessünk arra, a_0 nincs is rajta a körön — válasszunk helyére egy későbbi számot, az ugyanis valószínűbb, hogy már beért a körbe.

mod 2

0 ↔ **1**

---

mod 3

0 → 1 → **2**

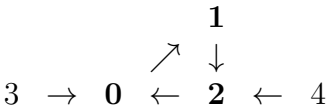
---

mod 4

0 → **1** ↔ **2** ← 3

---

mod 5



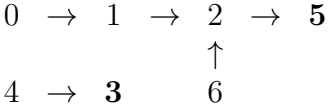
---

mod 6

0 → 1 → **2** ↔ **5** ← 4 ← 3

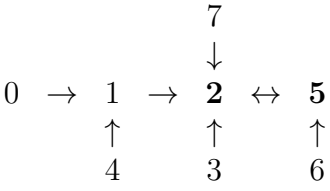
---

mod 7

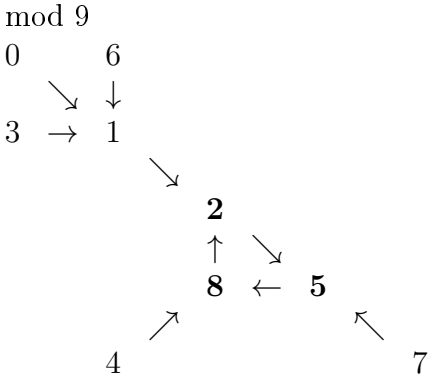


---

mod 8

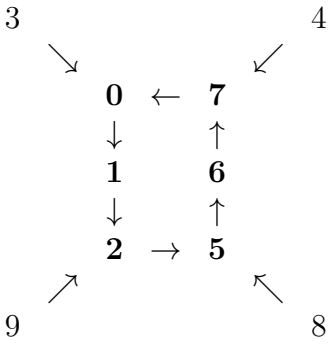


mod 9



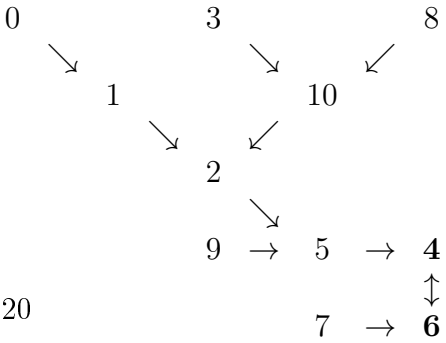
---

mod 10



---

mod 11



Praktikusnak látszik az utolsó kiszámított szám (azaz a_t) maradékosztályát választani: innentől kezdve átveszi a_0 szerepét a_t és mindent újrakezdünk. Másfelől nem korlátozhatjuk egy fix számmal (mondjuk 1000-rel) t-t: ha mindig csak $a_1, a_2, \ldots, a_{1000}$-rel dolgoznánk, sohasem találnánk meg például egy 1001 hosszú periódust. Ezért t-t célszerű folyamatosan nagyobbra és nagyobbra választani: egy lehetséges megoldás, ha t a kettőhatványokon fut végig az eljárás során.

Példa feladat: Bontsuk tényezőkre az adott $n = 91$ számot a Monte–Carlo-módszer segítségével az adott $f(x) = x^2 + 1$ és $x_0 = 2$ paraméterek segítségével. Az aktuális x_k-t (ahol k egy $h + 1$ bites egész) csak a $j = 2^h - 1$-edik elemmel hasonlítsuk össze.

A feladat a fent leírt Monte–Carlo-módszer algoritmusának első lépését írja elő, azaz $x_0 = 2$ kezdőérték és $f(x) = x^2 + 1$ megválasztását. Összehasonlítás alatt pedig a 2. lépést érti, azaz a legnagyobb közös osztó kiszámítását. Íme $f(x_0)$ értéke, amit a tömörség kedvéért x_1-gyel jelöltünk

$$x_1 = x_0^2 + 1 = 2^2 + 1 = 5.$$

Míg x_0-t nem volt mivel összehasonlítani, a most kiszámolt x_1-re már alkalmazhatjuk a 2. lépést:

$$(a_1 - a_0, n) = (5 - 2, 91) = 1.$$

Ez a legnagyobb közös osztó számítás arra volt jó, hogy megnézzük, 91-nek osztója-e a 3; láthatjuk, nem.

Meghatároztuk tehát x_1-et, és nem értünk célt:

$$x_2 = f(x_1) = 5^2 + 1 = 26.$$

Most már $k = 2$-t helyettesítve $j = 2^{\lceil \log_2 k \rceil - 1} - 1$-be nem 0, hanem 1 adódik, ezért x_2-t, azaz 26-ot, nem x_0-lal, hanem x_1-gyel hasonlítjuk össze — azaz 5-tel. Ez pedig

$$(26 - 5, 91) = 7$$

legnagyobb közös osztót jelenti. Szerencsére a 7 prím, ahogy $\frac{91}{7}$ (azaz 13) is az: a Monte–Carlo-módszer véget ért.

Pollard a következőket javasolta: a kezdőértéket válasszuk a tervezett iterációk számának mondjuk tizedének; továbbá ne végezzünk el minden legnagyobb közös osztó számítást — csak tízesével összevonva. Például

$$(a_{64} - a_{63}, n), \ldots, (a_{73} - a_{63}, n)$$

legnagyobb közös osztók kiszámítása helyett csak az alábbi legnagyobb közös osztót számítsuk ki:

$$((a_{64} - a_{63}) \cdot \ldots \cdot (a_{73} - a_{63}), n).$$

Láthatjuk, hogy így nem „vesztünk el" osztót, ugyanis ha

$$(a_i - a_{63}, n) = p,$$

akkor

$$p \mid ((a_i - a_{63}) \cdot (a_j - a_{63}), n).$$

Gond lehet viszont, ha két egytől különböző szám is előfordul az

$$(a_{64} - a_{63}, n), (a_{65} - a_{63}, n), \ldots, (a_{127} - a_{63})$$

tényezők között; ekkor ugyanis (szinte mindig) többletmunkát okozna a szorzatra lefuttatni egy hosszú Monte–Carlo-módszert, amiért cserébe megspóroltunk 9 legnagyobb közös osztó számítást. Ezért ha egy összevont legnagyobb közös számítás eredményére összetett számot kapunk, érdemes leellenőrizni, nem kerülte két (vagy akár még több) kis szám összevonásra.

Egy másik gyorsítási lehetőség, ha becslést készítünk a nemperiodikus szakasz hosszára és a periódushosszra. Ezután nem hasonlítunk össze minden számot, hanem csak akkor számítjuk ki az

$$(a_j - a_k, n)$$

legnagyobb közös osztót, ha egyrészt j nagyobb, mint a nemperiodikus szakaszra vonatkozó becslésünk, másrészt, ha $k - j$ nagyobb, mint a periódushosszra vonatkozó becslésünk. Például:

$$a_0 \quad a_1 \quad \overbrace{\overbrace{a_2 \quad a_3}^{(a_3-a_2,n)\overset{?}{=}1} \quad a_4 \quad a_5 \quad a_6 \quad a_7}^{(a_i-a_4,n)\overset{?}{=}1}$$

túl korai értékek: várhatóan a nemperiódikus szakaszba esnek

$$\overbrace{a_8 \quad a_9 \quad a_{10} \quad a_{11} \quad a_{12} \quad a_{13} \quad a_{14} \quad a_{15}}^{(a_i-a_8,n)\overset{?}{=}1}$$

túl közeli értékek: nem érik el a periódushossz várható értékét

$$a_{16} \quad a_{17} \quad a_{18} \quad a_{19} \quad a_{20} \quad a_{21} \quad a_{22} \quad a_{23}$$

$$\underbrace{a_{24} \quad a_{25} \quad a_{26} \quad a_{27} \quad a_{28} \quad a_{29} \quad a_{30} \quad a_{31}}$$

Ezeket érdemes összehasonlítani a_{16}-tal

A módszer akkor talál meg egy p prímtényezőt, ha az

$$(a_j - g(a_j), n)$$

legnagyobb közös osztó kiszámításakor

$$a_j \equiv g(a_j) \pmod{p}.$$

A módszer akkor mond csődöt, ha n-nek van két olyan p és q prímosztója, melyekre

$$a_j \equiv g(a_j) \pmod{p}, \qquad a_j \equiv g(a_j) \pmod{q},$$

de

$$a_l \not\equiv g(a_l) \pmod{p}, \qquad a_l \not\equiv g(a_l) \pmod{q}, \qquad \text{minden } l < j\text{-re.}$$

Miután megtaláltuk n egy d osztóját, sem $\frac{n}{d}$ faktorizálásánál, sem d faktorizálásánál nem érdemes újra kezdeni a Monte–Carlo-módszert: ha eddig nem állt fenn

$$a_j \equiv g(a_j) \pmod{p}$$

egy prímosztóra, természetesen az osztás után sem fog: folytatnunk kell azokkal a paraméterekkel, amelyeknél az osztáskor tartottunk.

4. Feladatok

Freud Róbert–Gyarmati Edit: Számelmélet

5.7.1 Tekintsük az $a > b > 0$ számokra a szokásos euklideszi algoritmust, ahol a keletkező maradékokra $b = r_0 > r_1 > r_2 > \ldots \geq 0$ teljesül.

a) Mutassuk meg, hogy bármely k-ra $r_{k+2} < \frac{r_k}{2}$.

A maradékokra tett $r_k > r_{k+1}$ feltétel és $a > b$ miatt a maradékos osztás képletében ($r_k = qr_{k+1} + r_{k+2}$) szereplő q biztosan nem nulla, ezért $r_k \geq r_{k+1} + r_{k+2}$. A maradékokra vonatkozó feltétel ismételt alkalmazásával $r_{k+1} > r_{k+2}$ miatt $r_k > r_{k+2} + r_{k+2}$, amit bizonyítani akartunk.
Megjegyzés: ugyanebben a fejezetben olvasható a módszer javítása, melyben a legkisebb abszolútértékű maradékokkal már $r_k \geq 2r_{k+1}$ is elérhető.

b) Milyen felső becslés adódik innen az algoritmus lépésszámára?

Használjuk az $r_{k+2} \leq \left\lceil \frac{r_k}{2} \right\rceil - 1$ képletet. Ebből $0 = r_n \leq \frac{r_{n-2}}{2} - 1 \leq \frac{r_{n-4}-6}{4} \leq \frac{r_{n-6}-14}{8} \leq \ldots \leq \frac{r_{n-2m}-2^{m+1}+2}{2^m}$. Átrendezve $r_{n-2m} \geq 2^{m+1} - 2$. Tehát, ha $b \leq 2^{m+1} - 2$, akkor a lépésszám legfeljebb $2m$. Explicite: $2\left(1 + \log_2(b+2)\right)$.

***c)** Igazoljuk, hogy ha az algoritmus lépésszáma pontosan s, akkor b lehető legkisebb értéke φ_{s+1}, ahol φ_j a j-edik Fibonacci-szám.

Az algoritmus utolsó lépésében $r_{n-2} = q_{n-1}r_{n-1} + r_n$ osztásban $r_n = 0$-t kapunk, ahol $q_{n-1} \geq 2$. A maradékokra tett $r_k > r_{k+1}$ feltétel és $a > b$ miatt a maradékos osztás képletében ($r_k = q_k r_{k+1} + r_{k+2}$) szereplő q_k biztosan nem nulla, ezért $r_k \geq r_{k+1} + r_{k+2}$ egyenlőtlenség áll fenn, mégpedig élesen: vegyen fel mind az r_{n-1}, mind pedig a q_k minden k-ra a lehető legkisebb

értéket, azaz 1-et. Konkrétan:

$$\begin{aligned} 2 &= 2 \cdot 1 + 0 \\ 3 &= 1 \cdot 2 + 1 \\ 5 &= 1 \cdot 3 + 2 \\ 8 &= 1 \cdot 5 + 3 \\ 13 &= 1 \cdot 8 + 5 \end{aligned}$$

Mint láthatjuk, a fenti egyenletek bal oldalából képzett sorozata csak annyiban tér el a Fibonacci sorozattól, hogy nincs benne 2 darab 1-es, tehát a válasz (azaz a lépésszám felső becslése, az s) a b függvényében:

$$\begin{aligned} 0 \leq b \leq 0 &\Rightarrow s = 0 \\ 1 \leq b \leq 1 &\Rightarrow s = 1 \\ 2 \leq b \leq 2 &\Rightarrow s = 2 \\ 3 \leq b \leq 3 &\Rightarrow s = 3 \\ 4 \leq b \leq 5 &\Rightarrow s = 4 \\ 6 \leq b \leq 8 &\Rightarrow s = 5 \\ 9 \leq b \leq 13 &\Rightarrow s = 6 \end{aligned}$$

5.7.2 Tekintsük az $\left(\frac{a}{b}\right)$ Jacobi-szimbólum kiszámítására a következő rekurzív definíciót:

1. $\left(\frac{1}{b}\right) := 1$
2. $\left(\frac{a}{b}\right) := \left(\frac{a \bmod b}{b}\right)$
3. $\left(\frac{2^s \alpha}{b}\right) := \begin{cases} -\left(\frac{\alpha}{b}\right) & \text{, ha } s \text{ páratlan, és } b \equiv \pm 3 \pmod 8 \\ \left(\frac{\alpha}{b}\right) & \text{egyébként} \end{cases}$
4. $\left(\frac{a}{b}\right) := \begin{cases} -\left(\frac{b}{a}\right) & \text{, ha } a \equiv b \equiv 3 \pmod 4 \\ \left(\frac{\alpha}{b}\right) & \text{egyébként (ha } a \text{páratlan)} \end{cases}$

Mutassuk meg, hogy ha ezt $(a, b) = d > 1$ mellett alkalmazzuk, akkor végül egy olyan helyzethez jutunk, ahol a „számláló" d, a „nevező" pedig többszöröse d-nek. (Ez azt jelenti, hogy ily

módon is kiderül, ha a Jacobi-szimbólum nem értelmes, és így a és b relatív prímségét nem kell előre külön ellenőrizni.)

A Jacobi-szimbólumot nem értelmezzük $2 \mid b$ esetén. Egyébként egy páratlan $(a, b) = d$ az algoritmus során végzett kongruens érték behelyettesítésétől, 2-vel osztástól és felcseréléstől nem változik. Mivel a és b csökken, előbb utóbb az első lépésben $a \mid b$ fog fennállni. Ez azt jelenti, hogy $(a, b) = a$, ami egyenlő d-vel, tehát tényleg igaz, hogy a „számláló" d, a „nevező" pedig többszöröse d-nek.

5.7.3 Mutassuk meg, hogy a 341 kettes alapú álprím, de nem hármas alapú álprím.

Mivel $2^{10} \equiv 1 \pmod{341}$, ezért $(2^{10})^{34}$ is. Mivel $3^3 \equiv 1 \pmod{13}$, ezért $3^{340} = 3 \cdot (3^3)^{131} \equiv 3 \pmod{13}$, tehát $3^{340} \not\equiv 1 \pmod{11 \cdot 13}$

5.7.4 Bizonyítsuk be, hogy ha n kettes alapú álprím, akkor $2^n - 1$ is az.

Az, hogy n kettes alapú álprím, azt jelenti, hogy n összetett és $n \mid 2^{n-1} - 1$. Szorozzuk kettővel: $n \mid 2^n - 2$. Ezért $2^{2^n-2} = (2^n)^k$. Az, hogy $2^n - 1$ kettes alapú álprím, azt jelenti, hogy $2^{2^n-2} = (2^n)^k \equiv 1 \pmod{2^n - 1}$. Ez nyilván fennáll, hiszen $2^n \equiv 1 \pmod{2^n - 1}$. Végül $2^n - 1$ nem lehet valódi prím, hiszen n összetett (mondjuk $n = ab$), és ezért $2^{ab} - 1 = (2^a - 1) \sum_{i=0}^{b-1} 2^{ai}$.

5.7.6 Igazoljuk, hogy az 561 univerzális álprím.

Lássuk be 561 minden p prímtényezőjére (azaz 3-ra, 11-re és 17-re), hogy $a^{561} \equiv 1 \pmod{p}$, azaz $p - 1 \mid 561 - 1$. Csakugyan: $2 \cdot 280 = 10 \cdot 56 = 16 \cdot 40 = 560$.

5.7.9 a) A tárgyalt prímteszteknél a feltétel ellenőrzése előtt nem volt szükséges külön megnézni, hogy a kipróbált a és a vizsgált n relatív prímek-e. Milyen előny származhat abból, ha mégis kiszámítjuk (a, n) értékét?

Ha $(a, n) \neq 1$ adódik, akkor nem csupán azt mutattuk meg, hogy n összetett, hanem még egy osztóját is meghatároztuk.

5.7.9 b) Ha az n két százjegyű prím szorzata, akkor „nagyjából" mekkora a valószínűsége annak, hogy egy véletlenszerűen választott a szám és az n *nem* relatív prím?

Ekkor n kétszáz jegyű, $n-\varphi(n)$ pedig (a két prím összege mínusz 1) százjegyű. A hányadosuk nagyjából 10^{-100}, körülbelül annak az esélye, hogy negyedéven át egyfolytában telitalálatunk legyen a lottón az 1,2,3,4,5 tippel.

5.7.10 Mutassuk meg, hogy ha $a^2 \equiv 1 \pmod{n}$, de $a \not\equiv \pm 1 \pmod{n}$, akkor az n-nek gyorsan meg tudjuk határozni egy nemtriviális osztóját.

Mivel $n \mid a^2-1 = (a+1)(a-1)$, ezért nyilván $((a+1)(a-1), n) = n$. Emiatt nem lehet, hogy $(a+1, n)$ és $(a-1, n)$ egyszerre 1-gyel legyen egyenlő. Azonban sem $(a+1, n)$, sem $(a-1, n)$ nem egyenlő n-nel. Tehát $(a+1, n)$ vagy $(a-1, n)$ valódi osztó. (Egyébként világos, hogy mindkettő valódi osztó, mert ha az egyik tényező relatív prím lenne n-hez és a másik nem többszöröse, akkor a szorzat sem lehetne többszöröse).

5.7.12 Vizsgáljuk meg, hogy alkalmas-e prímtesztnek a Wilson-tétel és megfordítása, azaz ha azt ellenőrizzük, hogy n osztója-e $(n-1)!+1$-nek.

Alkalmatlan, mert ehhez kb. n darab szorzást el kell végeznünk. Próbaosztással is kb. $\sqrt{n}$ darab osztással végzünk.

5.7.13 a) Mutassuk meg, hogy ha az n összetett szám nem univerzális álprím, akkor $a^{n-1} \equiv 1 \pmod{n}$ egy modulo n teljes maradékrendszer elemeinek kevesebb, mint felére teljesül.

Nevezzük a-t tanúnak, ha $a^{n-1} \not\equiv 1 \pmod{n}$, egyébként cinkosnak. Ha $(a, n) \neq 1$, akkor a nyilván tanú. Legyenek $c_1, \ldots, c_k$ páronként inkongruens cinkosok és $(t, n) = 1$ tanú (ha nem létezik ilyen t, akkor hívjuk az n összetett számot univerzális álprímnek). Ekkor $tc_1, \ldots, tc_k$ számok páronként inkongruensek, hiszen egy RMR részének t-szerese, t pedig relatív prím a modulushoz (azaz n-hez). Emellett $tc_1, \ldots, tc_k$ számok tanúk, hiszen

$$(tc_i)^{n-1} = t^{n-1}c_i^{n-1} \equiv t^{n-1} \not\equiv 1 \pmod{n}.$$

Tehát a RMR legalább fele tanú, a nála szigorúan bővebb TMR többi része meg mind az.

5.7.13 b) Írjuk le az a) részen alapuló konkrét prímtesztet.

A dolgozat elején szerepel Fermat-prímteszt néven.

5.7.15 Legyen $n = 2^k r + 1$, ahol $k \geq 1$, r páratlan és $0 < r < 2^k$. Tegyük fel, hogy egy a egész számra

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

Lássuk be, hogy ekkor n prím.

A dolgozatban Proth-prímteszt néven szerepel.

5.7.16 Legyen $n > 2$. Mutassuk meg, hogy az alábbi feltételek bármelyikéből következik, hogy az n prím.

a) Van olyan a egész szám, amelyre $a^{n-1} \equiv 1 \pmod{n}$, és az $n-1$ bármely p_i prímosztójára:

$$a^{\frac{n-1}{p_i}} \not\equiv 1.$$

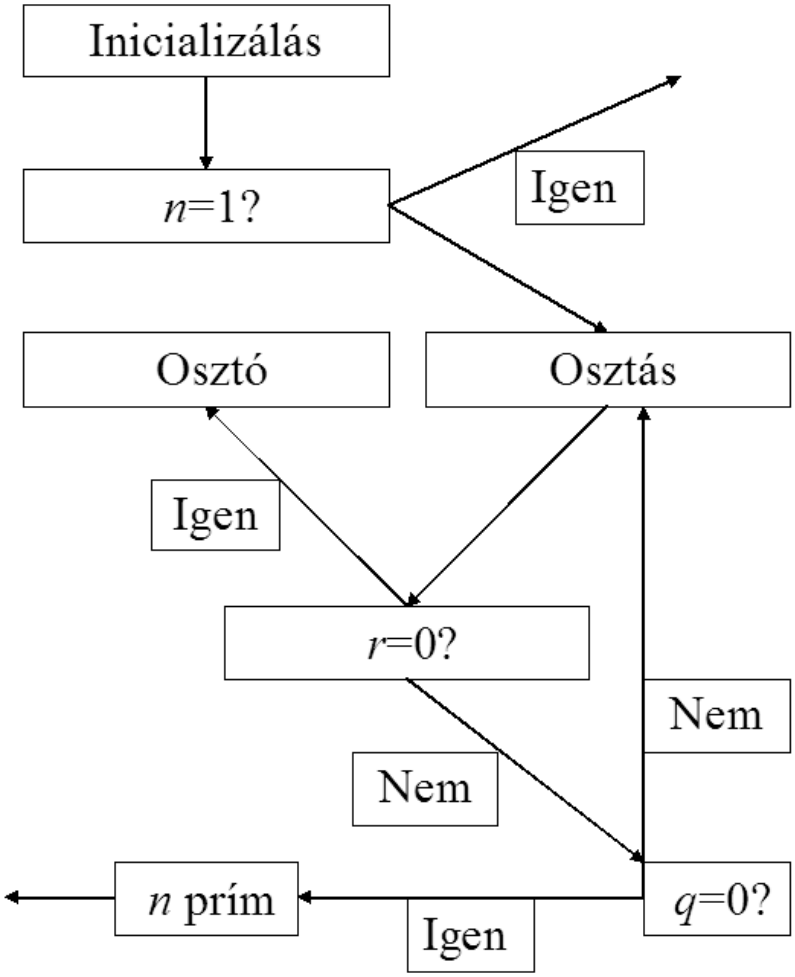
A dolgozatban Lucas-prímteszt néven szerepel.

***c)** Létezik az $n-1$-nek egy $\sqrt{n}$-nél nagyobb c osztója a következő tulajdonságokkal: a c bármely p_i prímosztójához van olyan a_i egész szám, amelyre

$$a_i^{n-1} \equiv 1 \pmod{n} \qquad \text{és} \qquad \left(a_i^{\frac{n-1}{p_i}} - 1, n\right) = 1.$$

A dolgozatban Pocklington-prímteszt néven szerepel.

A következő feladatban hivatkozunk A algoritmus néven a próbaosztás alábbi algoritmusára:



Donald Ervin Knuth: A számítógép-programozás művészete 2. — Szeminumerikus Algoritmusok

4.5.4/1 Ha az A Algoritmus próbaosztóinak $d_0, d_{1,}, d_2, \ldots$ sorozatában szerepel egy összetett szám, ez miért nem lép fel soha az outputban?

Mert d_i prímfelbontásában szereplő $d_k, \ldots, d_m$ prímek mind kisebbek nála és szerepelnek a próbaosztók között, ez azok lehető legmagasabb hatványával már elosztottuk az inputot, így d_i nem osztja n-et (sőt relatív prím hozzá).

4.5.4/3 Adjunk meg olyan P számot, amely rendelkezik az alábbi

tulajdonságokkal: Ha $1000 \leq n \leq 1000000$, úgy n akkor és csak akkor prím, ha $(n, P) = 1$.

Legyen P az 1000-nél kisebb prímszámok szorzata. Ez nyilván relatív prím egy 1000-nél nagyobb prímszámhoz. Ám ha egy 1000000-nál nem nagyobb szám összetett, annak legalább két prímtényezője közül van 1000-nél kisebb prím, így nem relatív prím P-hez.

5. Irodalomjegyzék

Freud Róbert–Gyarmati Edit: Számelmélet

Donald Ervin Knuth: A számítógép-programozás művészete II. Szeminumerikus algoritmusok

Neal Koblitz: A Course in Number Theory and Criptography

Wikipédia

http://www.math.umn.edu/~garrett/crypto/a01/FastPow.html

http://www.chalcedon.demon.co.uk/rgep/cartable.html