Másodfokú kongruenciák és alkalmazásaik

Szakdolgozat

Készítette: Varga Ildikó

Matematika BSc
Matematikai elemző szakirány

Témavezető: Károlyi Gyula, Egyetemi docens
Algebra és Számelmélet Tanszék

Eötvös Loránd Tudományegyetem
Természettudományi Kar
Budapest
2010

Tartalom

1. Bevezetés

Szakdolgozatom fő témájaként a prímtesztek tárgyalását jelöltem meg. A prímtesztek olyan algoritmusok, amelyek segítséget nyújtanak abban, hogy egy véletlen egész számról eldöntsük, hogy az prím-e vagy sem. A prímtesztek megértéséhez, értelmezéséhez, elemzéséhez azonban nélkülözhetetlen további lényeges elméleti kérdések tisztázása, ezért erre is külön ki fogok térni. A prímtesztek közül korábban tanultunk a naív módszerről, a Wilson-prímtesztről és a Fermat-prímtesztről, ezért ezekre külön nem térek ki, hanem ehelyett a Solovay-Strassen és a Miller-Lenstra-Rabin tesztet mutatom be részletesen a harmadik fejezetben. Az ezen munkák megértéséhez szükséges elméleti háttér bemutatásának szenteltem a második fejezetet, illetve a harmadik fejezet első felét, minthogy ezen elméletek alapján tudom a legátfogóbb és legérthetőbb képet adni munkám fő tárgyáról, a Solovay-Strassen és a Miller-Lenstra-Rabin tesztről, mint algoritmusokról.

2. Legendre- és Jacobi-szimbólum

2.1. Másodfokú kongruenciák

Az egész fejezet során feltesszük, hogy $p > 2$ prím és $(a, p) = 1$. Bevezetek néhány fogalmat és ezekkel kapcsolatos tételeket, melyeket az egész dolgozat során használni fogok.

2.1.1. Definíció. Az a számot aszerint nevezzük *kvadratikus maradék*nak, illetve *kvadratikus nemmaradék*nak modulo p, hogy az $x^2 \equiv a \pmod{p}$ kongruencia megoldható-e, vagy sem.

Az $a \equiv 0 \pmod{p}$ számok se nem kvadratikus maradékok, se nem kvadratikus nemmaradékok.

2.1.2. Tétel.

1. Az a szám akkor és csak akkor kvadratikus maradék modulo p ha $a^{(p-1)/2} \equiv 1 \pmod{p}$. Ezzel ekvivalens, hogy az a (bármely primitív gyök szerinti) indexe páros.

2. Az a szám akkor és csak akkor kvadratikus nemmaradék modulo p ha $a^{(p-1)/2} \equiv -1 \pmod{p}$. Ezzel ekvivalens, hogy az a (bármely primitív gyök szerinti) indexe páratlan.

3. A (páronként inkongruens) kvadratikus maradékok száma illetve kvadratikus nemmaradékok száma egyaránt $(p-1)/2$.

4. Ha a kvadratikus maradék, akkor az $x^2 \equiv a \pmod{p}$ kongruenciának két (páronként inkongruens) megoldása van.

Bizonyítás: Csak a 2. állítást bizonyítjuk. Az 1-es állításból azt is kapjuk, hogy a akkor és csak akkor kvadratikus nemmaradék, ha $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, illetve ha a indexe páratlan. Így a 2-es állításhoz azt kell már csak belátni , hogy

$$a^{(p-1)/2} \not\equiv 1 \pmod{p} \Longleftrightarrow a^{(p-1)/2} \equiv -1 \pmod{p}$$

Mivel a kis-Fermat tételből tudjuk, hogy ha $(a,p)=1$ és p prím, akkor $a^{p-1} \equiv 1 \pmod{p}$, így kihasználva azt, hogy $p \mid (a^{\frac{p-1}{2}}+1)(a^{\frac{p-1}{2}}-1)$, négyzetgyököt vonhatunk a kongruencia mindkét oldalán és így csak $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ lehetséges. Továbbá feltettük, hogy $p>2$, emiatt $1 \not\equiv -1 \pmod{p}$ és ezzel beláttuk a 2-es állítást. ■

2.1.3. Definíció. Az $\left(\frac{a}{p}\right)$ Legendre - szimbólumot a következőképpen értelmezzük

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

Ezt a definíciót összevetve a 2.1.2 tétellel, illetve annak bizonyításával azt kapjuk, hogy bármely a esetén:

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

2.1.4. Tétel.

1. $a \equiv b \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4} \\ -1, & \text{ha } p \equiv -1 \pmod{4}. \end{cases}$

Bizonyítás: (1)-ből a tétel mindhárom állítása adódik, a levezetést csak a másodikra tesszük meg:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Tehát a bal és jobb oldal kongruensek egymással modulo p. Korábbról tudjuk, hogy ha két szám kongruens egymással modulo p, akkor különbségük osztható p-vel. Így, ha kivonjuk a bal oldalból a jobbat, amúgy is csak 0-át, illetve ± 2-őt kaphatunk. Tehát a különbség értéke valóban 0, hiszen esetünkben $p>2$. ■

2.2. Kvadratikus reciprocitás

Továbbra is feltesszük, hogy $p > 2$, illetve hogy $q > 2$ egy p-től különböző prím.

2.2.1. Tétel (Gauss-lemma). Legyen $(a, p) = 1$, és tekintsük az $a, 2a, \ldots, \frac{p-1}{2}a$ számok modulo a vett legkisebb pozitív maradékait. Jelölje v ezek közül a $\frac{p}{2}$-nél nagyobbak számát. Ekkor

$$\left(\frac{a}{p}\right) = (-1)^v.$$

Bizonyítás: Az adott $\frac{p-1}{2}$ darab szám legkisebb pozitív maradékai közül a $\frac{p}{2}$-nél kisebbeket jelölje $r_1, \ldots, r_u$, a $\frac{p}{2}$- nél nagyobbakat pedig $p - s_1, \ldots, p - s_v$. Itt $u + v = \frac{p-1}{2}$. Ekkor azt kapjuk, hogy bármely $1 \leq t \leq \frac{p-1}{2}$ esetén alkalmas i-vel és j-vel:

$$ta \equiv \begin{cases} \text{vagy } r_i \\ \text{vagy } p - s_j \end{cases} \pmod{p} \tag{2}$$

teljesül. Itt az r_i és s_j számok az $1, 2, \ldots, \frac{p-1}{2}$ értékek valamelyikével egyenlőek.

Azt fogjuk megmutatni, hogy az r_i és s_j számok mind különbözőek, és valamilyen sorrendben az $1, 2, \ldots, \frac{p-1}{2}$ számokkal egyenlőek. Először azt látjuk be, hogy nem lehetnek egyenlőek. Ha valamely $i \neq k$-ra $r_i = r_k$, akkor alkalmas $1 \leq \lambda < \mu \leq \frac{p-1}{2}$ számokkal

$$\lambda a \equiv r_i = r_k \equiv \mu a \pmod{p}$$

teljesül. A jobb és bal oldalt egyszerűsíthetjük a-val, mert $(a, p) = 1$ és így jutunk a $\lambda \equiv \mu \pmod{p}$ ellentmondáshoz. Ugyanígy kaphatjuk meg az s_j számokra is.

Másodszor pedig, ha $r_i = s_j$, akkor

$$\lambda a \equiv r_i = s_j \equiv -\mu a \pmod{p},$$

vagyis $p \mid a(\lambda+\mu)$. Ez azonban ellentmond a p prím voltának, mert a szorzat egyik tényezőjének sem osztója p: a-nak azért nem, mert $(a,p)=1$, illetve $(\lambda+\mu)$-nek azért nem, mert feltettük, hogy $1 \le \lambda < \mu \le \frac{p-1}{2}$ vagyis $(\lambda+\mu) < p$.

A következő lépésben összeszorozva a (2)-es kongruenciákat egymással azt kapjuk, hogy:

$$\begin{aligned}\left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} &\equiv r_1 \cdots r_u (p-s_1)\cdots(p-s_v) \equiv \\ &\equiv (-1)^v r_1 \cdots r_u s_1 \cdots s_v = (-1)^v \left(\frac{p-1}{2}\right)! \pmod{p}.\end{aligned}$$

Ezt egyszerűsíthetjük $\left(\frac{p-1}{2}\right)!$-sal, mert p relatív prím a $\left(\frac{p-1}{2}\right)!$-höz. Ekkor azt kapjuk, hogy

$$a^{\frac{p-1}{2}} \equiv (-1)^v \pmod{p}, \quad \text{azaz} \quad \left(\frac{a}{p}\right) = (-1)^v.$$

■

A következő tételt bizonyítás nélkül tanultuk korábban. Láthatjuk majd, hogy a Gauss lemma segítségével könnyen számolhatóak a 2 kvadratikus maradékai.

2.2.2. Tétel.

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{ha } p \equiv \pm 1 \pmod 8 \\ -1 & \text{ha } p \equiv \pm 3 \pmod 8. \end{cases}$$

Bizonyítás: $a = 2$-re alkalmazzuk a fenti Gauss-lemmát. Ehhez először ki kell számolnunk v értékét, vagyis hogy a $2, 4, 6, \ldots, p-1$ számok közül hány darab $\frac{p}{2}$-nél nagyobb van. Összesen $\frac{p-1}{2}$ darab szám van, ebből a $\frac{p}{2}$-nél kisebbek száma $\left\lfloor \frac{p-1}{4} \right\rfloor$, tehát a keresett v érték

$$v = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor.$$

Ha $p = 8k+1$ alakú, akkor $v = 4k-2k = 2k$, vagyis $\left(\frac{2}{p}\right) = (-1)^{2k} = 1$. Ha $p = 8k+3$ alakú, akkor $v = 4k+1-2k = 2k+1$, tehát $\left(\frac{2}{p}\right) = (-1)^{2k+1} = -1$.

Itt tehát az előző esettel ellentétben kvadratikus nemmaradékot kaptunk. A többi két esetet is ugyanígy kapjuk. ■

2.2.3. Tétel (Kvadratikus reciprocitási tétel). Ha $p > 2$ és $q > 2$ két különböző prím, akkor

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

azaz

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{ha } p \equiv q \equiv -1 \pmod 4 \\ \left(\frac{p}{q}\right) & \text{egyébként.} \end{cases}$$

Mivel a szakdolgozatom fő témája a prímtesztek bemutatása, ezért a fenti tételt nem bizonyítom, azonban a Gauss lemma segítségével könnyen belátható.

Tekintsük a következő példát: Megoldaható-e az

$$x^2 \equiv 66 \pmod{191}$$

kongruencia? Ehhez a $\left(\frac{66}{191}\right)$ Legendre-szimbólumot kell kiszámolni.
Mivel $66 = 2 \cdot 3 \cdot 11$, ezért átírható:

$$\left(\frac{2}{191}\right)\left(\frac{3}{191}\right)\left(\frac{11}{191}\right)$$

alakban. A 2.2.2 tétel alapján $\left(\frac{2}{191}\right) = 1$, mivel $191 \equiv -1 \pmod 8$.
Az 2.2.3 tétel szerint $\left(\frac{3}{191}\right) = -\left(\frac{191}{3}\right)$, mivel $191 \equiv 3 \equiv -1 \pmod 4$. Amely tovább egyszerűsíthető $-\left(\frac{2}{3}\right)$ alakra, ugyanis $191 \equiv 2 \pmod 3$, és $-\left(\frac{2}{3}\right) = -(-1) = 1$. Végül $\left(\frac{11}{191}\right) = -\left(\frac{191}{11}\right)$, ismét a 2.2.3 tételt felhasználva, mivel $11 \equiv 191 \equiv -1 \pmod 4$, és $-\left(\frac{191}{11}\right) = -\left(\frac{4}{11}\right) = -\left(\frac{2}{11}\right)\left(\frac{2}{11}\right) = -(-1)(-1) = -1$. Tehát

$$\left(\frac{2}{191}\right)\left(\frac{3}{191}\right)\left(\frac{11}{191}\right) = 1 \cdot 1 \cdot (-1) = -1.$$

Vagyis az $x^2 \equiv 66 \pmod{191}$ kongruencia nem oldható meg.

A példán keresztül láthatjuk, hogy gyorsan tudunk számolni a kvadratikus reciprocitási tétel segítségével 2-3 jegyű számok esetén. Azonban nagyobb, összetett számok esetén már ismét hosszadalmas számolásokat kellene végeznünk. Ez újabb problémát vet fel, ezért bevezetjük a Jacobi-szimbólumot.

2.3. Jacobi-szimbólum

2.3.1. Definíció. Legyen $m > 1$ páratlan szám, $m = p_1 \cdots p_r$, ahol a p_i számok (nem feltétlenül különböző) pozitív prímek. Legyen továbbá $(a, m) = 1$. Ekkor az $\left(\frac{a}{m}\right)$ *Jacobi-szimbólumot* mint az $\left(\frac{a}{p_i}\right)$ Legendre- szimbólumok szorzatát értelmezzük:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

2.3.2. Tétel.

Feltesszük, hogy mindegyik állítás esetén alul egy 1-nél nagyobb páratlan szám van (az 5. állításnál fenn is), amely relatív prím a fenti számhoz.

1. $a \equiv b \pmod{m} \Longrightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$
2. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right), \qquad \left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$
3. $\left(\frac{-1}{m}\right) = \begin{cases} 1 & \text{ha } m \equiv 1 \pmod{4} \\ -1 & \text{ha } m \equiv -1 \pmod{4} \end{cases}$
4. $\left(\frac{2}{m}\right) = \begin{cases} 1 & \text{ha } m \equiv \pm 1 \pmod{8} \\ -1 & \text{ha } m \equiv \pm 3 \pmod{8} \end{cases}$
5. $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{ha } n \equiv m \equiv -1 \pmod{4} \\ \left(\frac{n}{m}\right) & \text{egyébként.} \end{cases}$

Bizonyítás: Tekintsük a 2. állítást. Legyen $m = p_1 \cdots p_r$. Ekkor

$$\left(\frac{ab}{m}\right) = \left(\frac{ab}{p_1}\right)\left(\frac{ab}{p_2}\right)\cdots\left(\frac{ab}{p_r}\right).$$

Az 2.1.4 tétel alapján ezek - a már Legendre-szimbólumok - felbonthatók

$$\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{a}{p_n}\right)\left(\frac{b}{p_n}\right) =$$

$$= \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_n}\right)\left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_n}\right)$$

alakba, melyet visszaalakítva a Jacobi-szimbólum definíciója szerint kapjuk, hogy $\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.

Az 5. állításnál legyen ismét $m = p_1 \cdots p_r$, és $n = q_1 \cdots q_s$ (ahol $p_i \neq q_j$).

Ekkor adódik a Legendre-szimbólum multiplikativitásából és a Jacobi-szimbólum definíciójából, hogy :

$$\left(\frac{m}{n}\right) = \prod_{\substack{1\leq j\leq r\\ 1\leq j\leq s}} \left(\frac{p_i}{q_j}\right), \qquad \left(\frac{n}{m}\right) = \prod_{\substack{1\leq j\leq r\\ 1\leq j\leq s}} \left(\frac{q_j}{p_i}\right). \tag{3}$$

Legyen a p_i-k közül u darab, a q_j-k közül v darab $4k-1$ alakú. Erre az uv darab p_i, q_j párra $\left(\frac{p_i}{q_j}\right) = -\left(\frac{q_j}{p_i}\right)$, a többi p_i, q_j párra pedig $\left(\frac{p_i}{q_j}\right) = \left(\frac{q_j}{p_i}\right)$, a kvadratikus reciprocitási tétel alapján. Ezeket összeszorozva kapjuk, hogy

$$\left(\frac{m}{n}\right) = (-1)^{uv}\left(\frac{n}{m}\right).$$

Tehát átfogalmazva az érdekel minket, hogy a produktumban az eltérőek száma páros vagy páratlan, vagyis hogy a szorzatban hány darab (-1)-es tag van.

Így kapjuk, hogy

$$\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right) \Longleftrightarrow \text{uv páratlan} \Longleftrightarrow$$
$$\text{u és v páratlan} \Longleftrightarrow m \equiv n \equiv -1 \pmod 4.$$

■

3. Prímszámok

3.1. Fermat- és Mersenne-prímek

Ebben a fejezetben a $2^k + 1$ alakú Fermat-, és a $2^k - 1$ alakú Mersenne-prímeket tárgyaljuk. Még nem ismeretes, hogy ezek száma végtelen vagy sem.
Tudjuk, hogy ha $2^k + 1$ prím, akkor $k = 2^n$, illetve ha a $2^k - 1$ prím, akkor k maga is egy prím szám. Ezért a továbbiakban csak az $F_n = 2^{2^n} + 1$ alakú Fermat-számokkal, illetve az $M_p = 2^p - 1$ (ahol p prím) alakú Mersenne-számokkal foglalkozunk.
Összesen öt Fermat-szám ismeretes:

1. $F_o = 2^{2^0} + 1 = 3$
2. $F_1 = 2^{2^1} + 1 = 5$
3. $F_2 = 2^{2^2} + 1 = 17$
4. $F_3 = 2^{2^3} + 1 = 257$
5. $F_4 = 2^{2^4} + 1 = 65537.$

Fermat azt sejtette, hogy az összes ilyen alakú szám prím, azonban Euler 1732-ben bebizonyította, hogy $F_5 = 2^{2^5} + 1 = 2^{32} + 1$ nem prím, mert osztója a 641. További előrelépést jelentett az a megállapítás, hogy F_n biztosan összetett, ha $5 \leq n \leq 23$. Sejtjük, de nem bizonyított, hogy az ismert 5 darab Fermat-prímen kívűl nincs több prím. Használhatók még a sokszög szerkesztésnél is. Gauss erre vonatkozó tétele kimondja, hogy a szabályos n-szög pontosan akkor szerkeszthető euklideszi szerkesztéssel, ha n ($n \geq 3$) páratlan prímtényezői különböző Fermat-prímek és mindegyik csak az első hatványon szerepel.
Általában a modern matematikában a legnagyobb ismert prímszámok Mersenne-prímek. Ezt igazolja az is, hogy 2008-ban találták meg a jelenlegi legnagyobb konkrétan ismert prímet, ami a $2^{43112609} - 1$, amely 12 978 189 jegyű.

Továbbá a tökéletes számok előállításában van még nagy szerepe a Mersenne-prímeknek. Tökéletes számok, azok amelyek egyenlőek a náluk kisebb osztóik összegével. Euklidesz bizonyította, hogy ha p és q prímek, ahol $q = 2^p - 1$, akkor az $n = 2^{p-1}q$ szám tökéletes lesz és minden páros tökéletes szám így áll elő.

3.1.1. Tétel.

F_n bármely (pozitív) osztója $k2^{n+1} + 1$, sőt $n \geq 2$ esetén $r2^{n+2} + 1$ alakú.

Bizonyítás: Először azt vizsgáljuk, hogy ha ez az osztó egy p prímszám. Ekkor az, hogy $p \mid F_n$ átírható a következőképpen:

$$2^{2^n} \equiv -1 \pmod{p}. \tag{4}$$

Négyzetre emelve kapjuk, hogy

$$2^{2^{n+1}} \equiv 1 \pmod{p}. \tag{5}$$

A következő lépésnél egy tételt fogunk használni, miszerint:

$$2^j \equiv 1 \pmod{p} \iff o_p(2) \mid j. \tag{6}$$

Ezt alkalmazva az (5)-ös kongruenciára kapjuk, hogy

$$o_p(2) \mid 2^{n+1},$$

azonban a (4)-es kongruencia alapján

$$o_p(2) \nmid 2^n,$$

mivel feltettük, hogy $p > 2$, ezért $1 \not\equiv -1 \pmod{p}$. Ezekből az következik, hogy

$$o_p(2) = 2^{n+1}$$

mivel $o_p(2) \mid 2^{n+1}$ miatt csak 2^{n+1} osztói jöhetnek szóba, amelyek 2^i $(0 \leq i \leq n+1)$ alakúak. Ezek közül, ha $o_p(2) = 2^j$ $(j \leq n)$, akkor fenn kell, hogy álljon a

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

kongruencia. Így 2^n felírható $2^j 2^k$ alakban, miszerint

$$(2^{2^j})^{2^k} \equiv 2^{2^n} \pmod{p}$$

vagyis

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

Azonban (4) miatt ez nem lehet. Továbbá tudjuk egy korábbi tételből, hogy az $o_m(a) \mid \varphi(m)$, amely egy $m = p$ prím esetén $p-1$-gyel egyenlő, tehát

$$o_p(a) \mid p-1, \text{ vagyis itt } 2^{n+1} \mid p-1.$$

Ezt átírva, egy alkalmas k egésszel $p = k2^{n+1} + 1$, amely pont a tételben szereplő állítás első fele. Ha $n \geq 2$, akkor p felírható $8s+1$ alakban, így az 1.2.2 tétel alapján

$$\left(\frac{2}{p}\right) = 1, \quad \text{azaz} \quad 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Ezt az előzőekben megállapított renddel összevetve kapjuk, hogy:

$$o_p(2) = 2^{n+1} \mid \frac{p-1}{2},$$

vagyis egy alkalmas r egésszel $p = r2^{n+2} + 1$, ami az állítás második felével egyezik meg. Továbbá ez az egyenlőség átírható $p \equiv 1 \pmod{2^{n+1}}$, illetve $n \geq 2$ esetén $p \equiv 1 \pmod{2^{n+2}}$ alakba is. Ezzel a tételt bizonyítottuk abban az esetben, ha az osztó egy prím.

Az általános esetre rátérve legyen $d \mid F_n$ tetszőleges. Bontsuk fel d-t (nem feltétlenül különböző) prímszámok szorzatára, ha $d > 1$, $d = p_1 \cdots p_s$. Mivel beláttuk, hogy minden i-re $p_i \equiv 1 \pmod{2^{n+1}}$, ezért ezeket a kongruenciákat összeszorozva kapjuk, hogy $d \equiv 1 \pmod{2^{n+1}}$, és ez nyilván $d = 1$ esetén is érvényes. Ugyanígy bizonyítható a tétel második fele. ■

3.1.2. Tétel (Pepin-teszt).

Az $n \geq 1$ esetben F_n akkor és csak akkor prím, ha

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \tag{7}$$

Bizonyítás: Először feltesszük, hogy F_n prím, ekkor

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

vagyis a 3 kvadratikus nemmaradék modulo F_n az 1.1.2 tétel szerint. Mivel feltettük, hogy $n \geq 1$, ezért $2^{2^n} = 4^t$ alakú, (tehát $F_n = 4^t + 1$) és így

$$F_n \equiv 1 \pmod 4, \qquad \text{továbbá} \qquad F_n = 4^t + 1 \equiv 1 + 1 \equiv -1 \pmod 3.$$

Itt ismét a kvadratikus reciprocitási tételt használva kapjuk

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

A másik irány bizonyításához feltesszük, hogy (7) fennáll, ezt négyzetre emelve

$$3^{F_n - 1} \equiv 1 \pmod{F_n}. \tag{8}$$

Az (7)-es, illetve (8)-as kongruenciákból kapjuk az alábbiakat

$$o_{F_n}(3) \nmid \frac{F_n - 1}{2}, \qquad \text{illetve} \qquad o_{F_n}(3) \mid F_n - 1.$$

Tudjuk, továbbá, hogy $F_n - 1$ kettőhatvány, így

$$o_{F_n}(3) = F_n - 1.$$

Ismét felhasználva, hogy a rend osztója $\varphi(m)$-nek, vagyis itt $F_n - 1 \mid \varphi(F_n)$, amiből az adódik, hogy

$$F_n - 1 \leq \varphi(F_n).$$

Mivel $\varphi(m)$ az m-nél nem nagyobb, m-hez relatív prímek számát jelöli, ami egy prím esetén is csak legfeljebb $m - 1$ darab lehet, ezért $\varphi(m) \leq m - 1$ bármely m szám esetén. Ezért itt

$$F_n - 1 \geq \varphi(F_n).$$

A két egyenlőtlenséget összevetve arra jutunk, hogy csak $F_n - 1 = \varphi(F_n)$ lehetséges, ami pedig pont azt jelenti, hogy F_n prím. Ezzel a tételt bebizonyítottuk. ■

3.1.3. Tétel.

Legyen $p > 2$ prím. Ekkor M_p bármely pozitív osztója $2kp+1$ alakú. Továbbá az is igaz, hogy 8-cal osztva $+1$ vagy -1 maradékot ad.

Bizonyítás: A 2.1.1-es tétel bizonyításánál láthattuk, hogy elég az állítást prímosztókra igazolni, mert minden osztó néhány prímosztó szorzata és ha

$$a \equiv 1 \pmod{2kp} \text{ és } b \equiv 1 \pmod{2kp} \Longrightarrow ab \equiv 1 \pmod{2kp}$$

ami esetünkben:

$$a \equiv \pm 1 \pmod{8} \text{ és } b \equiv \pm 1 \pmod{8} \Longrightarrow ab \equiv \pm 1 \pmod{8}.$$

Tehát tegyük fel, hogy a q prímre igaz, hogy

$$q \mid 2^p - 1, \quad \text{azaz} \quad 2^p \equiv 1 \pmod{q}.$$

Ekkor $o_q(2) \mid p$, továbbá nyilvánvaló, hogy $o_q(2) \neq 1$, ezért $o_q(2) = p$.
Ismét felhasználva, hogy $o_m(a) \mid \varphi(m)$, ami a mi esetünkben azt jelenti, hogy $p \mid q - 1$ (mivel q prím), azt kapjuk, hogy

$$q - 1 = tp \Longrightarrow q = tp + 1 \text{ alakú.}$$

Mivel q és p páratlanok, ezért a t-nek párosnak kell lennie ($t = 2k$ alakú), vagyis $q = 2kp + 1$ alakú.
Az 1.2.2 tétel szerint ahhoz, hogy $q = 8r \pm 1$ alakú, elegendő , hogy belássuk a 2 kvadratikus maradék modulo q. Ehhez felhasználjuk a $2^p \equiv 1 \pmod{q}$ kongruenciát, p páratlan voltát (ha akár $+1$-et, akár -1-et páratlan hatványra emeljük, akkor az eredmény is $+1$, illetve -1 marad) és a Legendre-szimbólum tulajdonságait.

$$\left(\frac{2}{q}\right) = \left(\frac{2}{q}\right)^p = \left(\frac{2^p}{q}\right) = \left(\frac{1}{q}\right) = 1.$$

■

3.1.4. Tétel (Lucas-Lehmer-teszt).

Legyen $p > 2$ prím, továbbá $a_1 = 4$ és $a_{i+1} = {a_i}^2 - 2$, ha $i \geq 1$. Ekkor M_p pontosan akkor prím, ha

$$M_p \mid a_{p-1}. \tag{9}$$

Bizonyítás: Jelöljük H-val az $a + b\sqrt{3}$ (a, b egész) alakú számok gyűrűjét, amely a szokásos műveletekre nézve kommutatív, egységelemes, és nullosztómentes. Így valóban gyűrűt kapunk minden a, b, c, d egészre, mivel:

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3}$$

$$(a + b\sqrt{3}) - (c + d\sqrt{3}) = (a - c) + (b - d)\sqrt{3}$$

$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = ac + (ad + bc)\sqrt{3} + 3bd = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

Tehát az $+, -, \cdot$ műveletek nem vezetnek ki a gyűrűből, azok is $a + b\sqrt{3}$ alakúak maradnak.

A bizonyításban a H-beli oszthatóság, kongruencia és rendfogalom elemi tulajdonságait használjuk fel, melyek H-ban is ugyanúgy érvényesek, mint az egész számoknál.

I. lépés: Teljes indukcióval könnyen igazolható, hogy bármely k-ra

$$a_k = (2 + \sqrt{3})^{2^{k-1}} + (2 - \sqrt{3})^{2^{k-1}}.$$

$a_1 = 4$-re igaz: $a_1 = (2 + \sqrt{3})^{2^{1-1}} + (2 - \sqrt{3})^{2^{1-1}} = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4$

Tegyük fel a_i-re igaz, belátjuk a_{i+1}-re.

$$a_{i+1} = {a_i}^2 - 2 = (2 + \sqrt{3})^{2^{i+1-1}} + (2 - \sqrt{3})^{2^{i+1-1}}$$

$$((2 + \sqrt{3})^{2^{i-1}} + (2 - \sqrt{3})^{2^{i-1}})^2 - 2 =$$

$$= (2 + \sqrt{3})^{2^i} + (2 - \sqrt{3})^{2^i} + 2(2 + \sqrt{3})^{2^{i-1}}(2 - \sqrt{3})^{2^{i-1}} - 2$$

$$= (2 + \sqrt{3})^{2^i} + (2 - \sqrt{3})^{2^i}, \text{ hiszen}$$

$$2(2 + \sqrt{3})^{2^{i-1}}(2 - \sqrt{3})^{2^{i-1}} - 2 = 2((2 + \sqrt{3})(2 - \sqrt{3}))^{2^{i-1}} - 2$$

$$2 \cdot 1 - 2 = 0.$$

Ekkor a (9) átírható az

$$M_p \mid (2+\sqrt{3})^{2^{p-2}} + (2-\sqrt{3})^{2^{p-2}} \tag{10}$$

oszthatóságra. A jobb oldalon, ha kiemeljük $(2-\sqrt{3})^{2^{p-2}}$-t, akkor kapjuk

$$M_p \mid (2-\sqrt{3})^{2^{p-2}}((2+\sqrt{3})^{2^{p-1}} + 1). \tag{11}$$

Mivel $(2-\sqrt{3})(2+\sqrt{3}) = 1$, ezért a $2 \pm \sqrt{3}$ számok egész kitevős hatványai egységek H-ban. Továbbá felhasználjuk, hogy a (11)-beli oszthatóság pontosan akkor teljesül az egész számok körében, mint amikor H-ban. Így a (9) és (11) ekvivalens azzal, hogy $M_p \mid (2+\sqrt{3})^{2^{p-1}} + 1$, vagyis

$$(2+\sqrt{3})^{2^{p-1}} \equiv -1 \pmod{M_p}. \tag{12}$$

Így a tételt átfogalmazva azt mondhatjuk, hogy M_p akkor és csak akkor prím, ha (12) teljesül.

II. lépés: Ennek igazolásához egy lemmát használunk fel.

Lemma: Ha $q > 3$ tetszőleges prímszám, akkor

$$(a+\sqrt{3})^q \equiv a + \left(\frac{3}{q}\right) b\sqrt{3} \pmod{q}. \tag{13}$$

Bizonyítás: A binomiális tételt használva

$$(a+\sqrt{3})^q = a^q + \binom{q}{1} a^{q-1} b\sqrt{3} + \binom{q}{2} a^{q-2} 3b^2 + \cdots + b^q 3^{(q-1)/2}\sqrt{3}. \tag{14}$$

A kis Fermat-tétel szerint

$$a^q \equiv a \pmod{q} \quad \text{és} \quad b^q \equiv b \pmod{q},$$

továbbá

$$\binom{q}{1}, \binom{q}{2}, \ldots, \binom{q}{q-1}$$

mindegyike osztható q-val, illetve (1) alapján

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

Ezeket beírva (14)-be (13)-at kapjuk. ■

III. lépés: Megmutatni, ha (12) fennáll, akkor M_p prím.

Négyzetre emeljük a (12)-es kongruenciát

$$(2+\sqrt{3})^{2^p} \equiv 1 \pmod{M_p}. \tag{15}$$

Vegyük M_p-nek egy q prímosztóját, amelyre $q > 3$ könnyen látható, mivel $M_p = 2^p - 1$, ahol p páratlan, mivel feltettük, hogy $p > 2$ prím. Ha

$$2 \nmid p \Longrightarrow 2^p \equiv 2 \pmod{3}$$

$$M_p = 2^p - 1 \equiv 1 \pmod{3} \Longrightarrow 3 \nmid M_p.$$

Erre a q modulusra ugyanúgy teljesül a (12)-es és (15)-ös kongruencia:

$$(2+\sqrt{3})^{2^{p-1}} \equiv -1 \pmod{q}$$

$$(2+\sqrt{3})^{2^p} \equiv 1 \pmod{q}.$$

Ekkor hasonlóan a korábbi bizonyításokhoz

$$o_q(2+\sqrt{3}) \mid 2^p \quad \text{és} \quad o_q(2+\sqrt{3}) \nmid 2^{p-1}.$$

Tehát $o_q(2+\sqrt{3}) = 2^p$, ahol a rend fogalmát most a H gyűrűben értjük. A rend szokásos tulajdonságai itt is érvényesek.

Ha $\left(\frac{3}{q}\right) = 1$, akkor (13) miatt

$$(2+\sqrt{3})^q \equiv (2+\sqrt{3}) \pmod{q}.$$

Ezt felhasználva kapjuk, hogy

$$(2+\sqrt{3})^{q-1} = (2-\sqrt{3})(2+\sqrt{3})^q \equiv (2-\sqrt{3})(2+\sqrt{3}) = 1 \pmod{q},$$

és így

$$o_q(2+\sqrt{3}) = 2^p \mid q-1,$$

ami azt jelenti, hogy $2^p \leq q-1$, ami lehetetlen, mert $q \leq M_p$ (mert q az M_p osztója) $= 2^p - 1$, vagyis $q \leq 2^p - 1$.

Ha $\left(\frac{3}{q}\right) = -1$, akkor hasonlóan adódik, hogy

$$(2+\sqrt{3})^{q+1} = (2+\sqrt{3})^q(2+\sqrt{3}) \equiv (2-\sqrt{3})(2+\sqrt{3}) = 1 \pmod{q},$$

és emiatt

$$o_q(2+\sqrt{3}) = 2^p \leq q+1.$$

Ezt összevetve a $q \leq M_p = 2^p - 1$ egyenlőtlenséggel

$$2^p \leq q+1 \text{ és } 2^p \geq q+1,$$

ami csak úgy lehetséges, ha $2^p = q+1$, vagyis $q = M_p$, tehát M_p valóban prím.

IV. lépés: Utolsó lépésként belátjuk, hogy ha M_p prím, akkor (12) teljesül. Mivel $M_p = 2^p - 1$ és $p > 2$, ezért $M_p \equiv -1 \pmod 8$ és ezért az 1.3.2 tétel miatt

$$\left(\frac{2}{M_p}\right) = 1, \tag{16}$$

mint Legendre-szimbólum (mivel M_p prím), továbbá $M_p \equiv 1 \pmod 3$ (fentebb beláttuk) és $M_p \equiv -1 \pmod 4$, így a reciprocitási tétel segítségével látható, hogy

$$\left(\frac{3}{M_p}\right) = -\left(\frac{M_p}{3}\right) = -\left(\frac{1}{3}\right) = -1. \tag{17}$$

A továbbiakban a $2(2+\sqrt{3}) = (1+\sqrt{3})^2$ egyenlőséget használjuk. Mindkét oldalt $(M_p+1)/2 = 2^p/2 = 2^{p-1}$-edik hatványra emeljük:

$$2^{(M_p+1)/2} \cdot (2+\sqrt{3})^{2^{p-1}} = (1+\sqrt{3})^{M_p+1}. \tag{18}$$

A bal oldalon, felhsználva (16)-ot azt kapjuk, hogy

$$2^{(M_p+1)/2} = 2 \cdot 2^{(M_p-1)/2} \equiv 2\left(\frac{2}{M_p}\right) = 2 \pmod{M_p}. \tag{19}$$

A jobb oldalon pedig a (17)-et és (13)-at használjuk, az utóbbit úgy, hogy $a + b\sqrt{3} = 1+\sqrt{3}$ és $q = M_p$, ekkor

$$(1+\sqrt{3})^{M_p+1} = (1+\sqrt{3})(1+\sqrt{3})^{M_p} \equiv (1+\sqrt{3})(1+\left(\frac{3}{M_p}\right)\sqrt{3}) =$$

$$= (1+\sqrt{3})(1-\sqrt{3}) = -2 \pmod{M_p}.$$

Ezeket visszahelyettesítve (18)-ba jutunk el a

$$2(2+\sqrt{3})^{2^{p-1}} \equiv -2 \pmod{M_p} \tag{20}$$

kongruenciához. Ekkor már csak meg kell (20)-at szorzni 2^{p-1}-nel

$$2^p(2+\sqrt{3})^{2^{p-1}} \equiv -2^p \pmod{M_p - 1}.$$

Mivel $2^p \equiv 1 \pmod{M_p}$, ezért

$$(2+\sqrt{3})^{2^{p-1}} \equiv -1 \pmod{M_p}$$

és pont ezt (12) akartuk bizonyítani.
Ugyanezt könnyebben is megkaphattuk volna, ha a (20) kongruenciát 2-vel leosztjuk. Hogy ez H-ban valóban megtehető, az külön meggondolást igényelne. ■

3.2. Prímtesztek

Prímtesztnek nevezzük az olyan algoritmusokat, eljárásokat, amelyek segítségével véges sok lépésben el tudjuk dönteni bármely adott (nagy) egész számról, hogy az prím-e vagy összetett. A további problémát a prímtényezős felbontás jelenti, összetett szám esetén, amely egy nagyon bonyolult és hosszadalmas feladat például egy 100 jegyű szám esetén. Ekkor már nem működik a próbaosztogatás, amelyet egy 1-2-3 vagy esetleg 4 jegyű szám esetén még érdemes elvégezni. Ez a legegyszerűbb, naív módszer: az adott egész számot sorra elosztjuk a nála kisebb pozitív egész számokkal. Ha van ezek között olyan, 1-től különböző szám, ami az adott egész számnak osztója, akkor a szám nem prím, de ha nincs ilyen akkor az. Úgy gyorsítható a módszer, hogy természetesen nem kell az összes, a számnál kisebb pozitív számot megvizsgálni, elég csak a prímeket. Ehhez használhatók prímtáblázatok vagy például az eratoszthenészi szita módszere. Egy több száz jegyű szám esetén azonban már annyira sok próbálkozást kéne elvégezni, hogy még számítógéppel is hosszú évekbe telne. Ezek a tesztek azonban nem osztókat keresnek, hanem olyan feltételeket jelentenek, amelyek gyorsan elvégezhetőek és igazak egy prímszámra, de egy összetett szám már nem elégíti ki őket.
A speciális alakú számokkal könnyebb a dolgunk, ezekről jóval egyszerűbben eldönthető prím mivoltuk. Ilyenek voltak a 2.1 fejezetben tárgyalt Fermat-,

Mersenne-számok.
Gyors algoritmus létezik alapvető számelméleti feladatok kiszámítására, ezeket egy tételben összefoglaljuk, majd konkrét prímteszteket vizsgálunk meg.

3.2.1. Tétel.

Legyenek a, b, c és m egészek, ahol $b > 1$ és $m > 0$. Ekkor

1. a^b maradéka modulo m;
2. az a és b legnagyobb közös osztója;
3. (páratlan b és $(a, b) = 1$ esetén) az $\left(\frac{a}{b}\right)$ Jacobi-szimbólum
4. az $ax + by = c$ lineáris diofantikus egyenlet megoldásai és
5. az $ax \equiv c \pmod{b}$ kongruencia megoldásai

kiszámíthatóak legfeljebb $5 \log_2 b$ lépésben, ahol egy lépés két egész szám összeadását, kivonását, szorzását vagy maradékos osztását jelenti.

Bizonyítás: 1. kiszámításának lépései az ismételt négyzetre emelések, majd minden lépés után az eredmény modulo m redukálása. Példa: $17^{27} \pmod{41}$

$$17^2 = 289 \equiv 2 \pmod{41}$$

$$17^4 \equiv 2^2 \equiv 4 \pmod{41}$$

$$17^8 \equiv 4^2 \equiv 16 \pmod{41}$$

$$17^{16} \equiv 16^2 \equiv 10 \pmod{41}$$

és így

$$17^{27} = 17^{16} \cdot 17^8 \cdot 17^2 \cdot 17 \equiv 10 \cdot 16 \cdot 2 \cdot 17 = 160 \cdot 34 \equiv (-4) \cdot (-7) = 28 \equiv$$

$$\equiv -13 \pmod{41}.$$

Legyen $t = \lfloor \log_2 b \rfloor$ és felírjuk a b kitevőt kettes számrendszerben. Mivel a számítógép kettes számrendszerre épül, ezért a b szám eleve így van tárolva.

Más alapú számrendszerből történő átszámítás esetén pedig legfeljebb $\log_2 b$ darab lépés, mivel a számjegyeket a 2-vel történő maradékos osztások szorzatával kapjuk meg.

$$b = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_s}, \quad \text{ahol} \quad 0 \leq i_1 < i_2 < \cdots < i_s \leq t.$$

Ezután ismételt négyzetre emelésekkel és mindig modulo m redukálva kiszámoljuk

$$a^2, a^4, a^8, \ldots, a^{2^t}$$

maradékait modulo m. Végül az

$$a^b = a^{2^{i_1}} a^{2^{i_2}} \ldots a^{2^{i_s}}$$

alapján kapjuk meg a keresett maradékot.
Tehát t darab négyzetre emelést és legfeljebb t darab további szorzást, illetve modulo m redukciót végzünk el. Vagyis összesen legfeljebb $2t \leq 2\log_2 b$ ilyen szorzásra és redukcióra van szükség. Ehhez már csak azt kell hozzávennünk, hogy b-t átírjuk 2-es számrendszerbe, ami megint csak $\log_2 b$ darab lépés. Ezt összegezve a^b modulo m maradékát legfeljebb $5\log_2 b$ lépésben kaphatjuk meg. 2.-t a legkisebb abszolút értékű maradékokkal végzett euklideszi algoritmussal számoljuk:

$$\begin{aligned}
a &= bq_1 + r_1, && \text{ahol} \quad |\, r_1 \,| \leq \frac{b}{2},\\
b &= r_1 q_2 + r_2, && \text{ahol} \quad |\, r_2 \,| \leq |\, \frac{r_1}{2} \,| \leq \frac{b}{4},\\
r_1 &= r_2 q_3 + r_3, && \text{ahol} \quad |\, r_3 \,| \leq |\, \frac{r_2}{2} \,| \leq \frac{b}{8},\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n, && \text{ahol} \quad |\, r_n \,| \leq |\, \frac{r_{n-1}}{2} \,| \leq \frac{b}{2^n},\\
r_{n-1} &= r_n q_{n+1}, && \text{vagyis} \quad r_{n+1} = 0.
\end{aligned}$$

ami $n+1$ lépésből áll. Mivel

$$1 \leq \mid r_n \mid \leq \frac{b}{2^n},$$

amely egyenlőtlenséget 2^n-nel beszorozva kapjuk, hogy:

$$2^n \leq b, \qquad \text{azaz} \qquad n \leq \log_2 b.$$

Tehát az összes lépés száma legfeljebb $1 + \log_2 b$.

A 3. pontban a Jacobi-szimbólumot az a-ban szereplő kettőhatványok leválasztásával és a reciprocitási tétel ismételt alkalmazásával számolhatjuk ki.

Számoláskor az a-t b-vel osztjuk maradékosan, mint az euklideszi algoritmusnál:

$$\left(\frac{a}{b}\right) = \left(\frac{r}{b}\right), \qquad \text{ahol} \qquad \mid r \mid < \frac{b}{2}.$$

Felhasználhatjuk $\left(\frac{-1}{b}\right)$-t (mert bármikor kiemelhető az 1.1.4-es tétel szerint), és ekkor $r > 0$.

Ha r páros, akkor a második lépésben kiemelhetünk $\left(\frac{2}{b}\right)$-t és így a "számláló" feleződik. Ha r páratlan, akkor a reciprocitási tétel miatt r lesz a "nevezőben" és fentre a b modulo r szerinti maradéka kerül, legyen s. $\mid s \mid < r/2$ ugyanúgy és ismét elérhető, hogy $s > 0$. Vagyis minden ilyen lépésnél a "számláló" legalább feleződik, így legfeljebb $\log_2 b$ lépést igényel. Továbbá, $\left(\frac{-1}{v}\right)$ és $\left(\frac{2}{v}\right)$ kiszámításához ki kell számolnunk v-nek modulo 4 és modulo 8 szerinti maradékait az 1.1.4 és 1.2.2 tételek szerint. Ezek egy-egy maradékos osztást jelentenek. Hasonlóan megkaphatjuk a "számlálót" is.

Az 1.3.1 definíció szerint a Jacobi-szimbólum csak akkor értelmes, ha $b > 1$ páratlan szám és $(a, b) = 1$. Utóbbi ellenőrzésére azért nincs szükség, mert ha a-nak és b-nek lenne közös osztója, akkor eljutnánk egy olyan lépésbe, hogy a számláló d lenne és a nevező pedig d többszöröse, vagyis nem létezne az $\left(\frac{a}{b}\right)$ Jacobi-szimbólum. Ha viszont a és b relatív prímek, akkor ilyen nem fordulhat elő, tehát csak egy $\left(\frac{\pm 1}{v}\right)$ vagy $\left(\frac{\pm 2}{v}\right)$ kiszámítása lehet az utolsó lépés.

A tétel 4. és 5. pontja ekvivalens egymással. Az $ax \equiv c \pmod{b}$ kongruencia megoldása egy olyan t egész szám, melyre $at \equiv c \pmod{b}$. Ez pedig

azt is jelenti, hogy $at + bs = c$ egy megfelelő s egész számmal. Ami megfelel az $ax + by = c$ diofantikus egyenletnek, aminek megoldásait az euklideszi algoritmussal kapjuk.

■

A továbbiakban konkrét prímtesztekről lesz szó. A legáltalánosabb ezek közül a kis Fermat-tételből következik:

Ha egy $n > 2$ számra $2^{n-1} \not\equiv 1 \pmod{n}$, akkor n összetett.

3.2.2. Tétel.

Legyen $n > 2$. Ha $2^{n-1} \not\equiv 1 \pmod{n}$, akkor n biztosan összetett. Ha $2^{n-1} \equiv 1 \pmod{n}$, akkor n "majdnem biztosan" prím. A feltétel gyorsan ellenőrizhető, ha a hatványozást ismételt négyzetre emelések segítségével végezzük.

Természetesen számítógéppel gyorsan elvégezhető a^{n-1} maradékának kiszámítása modulo n, nem csak $a = 2$-re, hanem bármely más a-ra. Ha ezek közül csak egy a-ra is nem 1 a maradék, akkor n a kis Fermat-tétel szerint biztosan összetett.
Ha minden a-ra 1 a maradék, akkor még biztosabb, hogy n prím, de persze még így sem biztos teljesen.
További gondot okoznak az *álprím*ek, melynek fogalmát az alábbiakban vezetem be.

3.2.3. Definíció.

Ha egy n összetett számra $a^{n-1} \equiv 1 \pmod{n}$ teljesül, akkor az n-et *a alapú álprím*nek nevezzük.
Ha az n összetett számra a fenti kongruencia minden $(a, n) = 1$ esetén teljesül, akkor az *n univerzális álprím* vagy *Carmichael-szám*.

Bizonyítottan minden $a > 1$ esetén végtelen sok mind az a alapú álprímek, mind az univerzális álprímek száma.
Most két olyan prímtesztet fogunk tárgyalni, amelyeknél olyan feltételeket

keresünk, amikre nézve már nem fordulhatnak elő álprímek.
Mindkét tétel esetén véletlen választjuk a számokat, bármely szám kiválasztásának ugyanannyi az esélye. A számítógép ekkor valamilyen véletlenszámgenerátort használ.

3.2.4. Tétel (Solovay-Strassen-prímteszt).

1. Legyen $n > 1$ páratlan szám, és tekintsük az

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \tag{21}$$

kongruenciát, ahol $\left(\frac{a}{n}\right)$ a Jacobi-szimbólum.
Ha n prím, akkor (21) minden $a \not\equiv 0 \pmod{n}$ esetén teljesül.
Ha n összetett, akkor (21) egy modulo n teljes maradékrendszer elemeinek kevesebb, mint a felére teljesül.

2. Az 1. kritérium alapján a következőképpen dönthetjük el egy nagy páratlan n-ről, hogy prím-e vagy összetett. Válasszunk mondjuk 1000 véletlen $a \not\equiv 0 \pmod{n}$ értéket, és mindegyikre vizsgáljuk meg, hogy a (21) feltétel teljesül-e. Ha legalább egy esetben nem teljesül, akkor az n biztosan összetett. Ha mind az 1000 esetben teljesül, akkor 2^{-1000}-nél kisebb annak a valószínűsége, hogy az n összetett.

Néhány megjegyzés a tételhez:

1. Ha $(a, n) > 1$, akkor a Jacobi-szimbólum nem értelmes, tehát (21) eleve nem teljesülhet.

2. Előfordulhat természetesen, hogy a tétellel egy összetett számot tévesen prímnek ítélünk, de a 2.2.2 tételhez képest ez nagy előrelépést jelent.

3. Elég sok a érték kipróbálásával tetszőlegesen kicsi lehet a tévedés valószínűsége.

Bizonyítás: Elég a tétel első felét igazolni, mert a második fele ennek következménye.

Ha n prím, akkor (21) teljesül (1) miatt.
Ha n összetett, akkor eleve csak olyan a számok jöhetnek szóba, amelyekre $(a, n) = 1$. Vagyis elegendő azt megmutatni, hogy (21)-et egy modulo n redukált maradékrendszer elemeinek legfeljebb a fele elégíti ki.
A továbbiakban egy n-hez relatív prím a számot *tanú*nak nevezünk, ha (21) nem teljesül rá és *cinkos*nak, ha igen. Így átfogalmazva, azt fogjuk belátni, hogy egy modulo n redukált maradékrendszer elemeinek legalább a fele tanú.

I. Először azt mutatjuk meg, hogy minden páratlan összetett n-hez létezik tanú. Ehhez egy definícióra lesz szükségünk.

3.2.5. Definíció.

Egy g számot *primitív gyök*nek nevezünk modulo m, ha $o_m(g) = \varphi(m)$.

Két esetet fogunk vizsgálni. Az egyik, hogy létezik egy olyan q prímszám, melyre $q^2 \mid n$. Továbbá $q = q_1, q_2, \cdots, q_s$ legyenek n különböző prímosztói. Ismeretes, hogy minden q prímre létezik primitív gyök modulo q^2. Legyen g primitív gyök modulo q^2. Nézzük az

$$x \equiv g \pmod{q^2}, \qquad x \equiv 1 \pmod{q_i}, \qquad 2 \leq i \leq s$$

szimultán kongruenciarendszert. Legyen ennek egy megoldása v, vagyis

$$v \equiv g \pmod{q^2}, \qquad v \equiv 1 \pmod{q_i}, \qquad 2 \leq i \leq s. \tag{22}$$

Ha $s = 1$, akkor legyen $v = g$.
Azt fogjuk megmutatni, hogy v tanú.
Mivel q_i mindegyike prímszám, ezért $(v, q_i) = 1$ minden i-re. Emiatt pedig $(v, n) = 1$. Indirekt feltesszük, hogy

$$v^{\frac{n-1}{2}} \equiv \left(\frac{v}{n}\right) \pmod{n}. \tag{23}$$

Ezt négyzetre emelve:

$$v^{n-1} \equiv \left(\frac{v}{n}\right)^2 = 1 \pmod{n}. \tag{24}$$

Mivel n-nek osztója q^2, ezért a (24)-es kongruencia teljesül modulo q^2 is:

$$v^{n-1} \equiv 1 \pmod{q^2}.$$

Felhasználva (22)-őt

$$g^{n-1} \equiv 1 \pmod{q^2}. \tag{25}$$

Itt g primitív gyök modulo q^2 azaz a rendje $\varphi(q^2) = q^2 - q^1 = q(q-1)$, így (6)-ot felhasználva azt kapjuk, hogy $q(q-1) \mid n-1$. Viszont $q^2 \mid n$, vagyis q osztója n-nek és $n-1$-nek is, ami lehetetlen, mert a ± 1-en kívül semmi nem lehet osztója két egymást követő számnak. Így ellentmondáshoz jutottunk, vagyis v tanú.

Most nézzük azt az esetet, amikor $q^2 \mid n$ nem teljesül semmilyen q prímosztóra. Az ilyen n számokat négyzetmentesnek hívjuk. Tehát legyen $n = q_1 \cdots q_s$, ahol q_i-k különböző prímek és $s \geq 2$. Itt két (al)esetet fogunk vizsgálni. Az egyik, hogy

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n} \tag{26}$$

kongruencia teljesül minden $(a, n) = 1$ esetén, illetve, hogy nem.
Ha teljesül, akkor legyen h kvadratikus nemmaradék modulo q_1 és w egy megoldása a

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

szimultán kongruenciarendszernek. Vagyis

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

Ekkor $(w, n) = 1$, mert q_i mindegyike prím, és w-t q_i-vel osztva mindig 1 maradékot ad, ha $2 \leq i \leq s$. Modulo q_1 pedig w kongruens egy h kvadratikus nemmaradékkal, vagyis $q_1 \nmid w$. S mivel fennáll, hogy w és n relatív prímek, ezért w-re alkalmazva (26)-ot $w^{\frac{n-1}{2}} \equiv 1 \pmod{n}$. Viszont $\left(\frac{w}{n}\right)$, mint Jacobi-szimbólum

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

Tehát w tanú.
A másik aleset, hogy (26) nem teljesül valamilyen n-hez relatív prím a számra. Ekkor n prímosztói között van legalább egy olyan - legyen ez q_1 -, amelyikre:

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

Vegyük ekkor z-t, ami egy megoldása az

$$x \equiv a \pmod{q_1}, \qquad x \equiv 1 \pmod{q_i}, \qquad 2 \leq i \leq s \tag{27}$$

szimultán kongruenciarendszernek. Tehát

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

Továbbra is azt akarjuk belátni, hogy z tanú.
Mivel ebben az esetben (26) nem teljesül, ezért

$$z^{\frac{n-1}{2}} \equiv a^{\frac{n-1}{2}} \not\equiv 1 \pmod{q_1}, \quad \text{és így} \quad z^{\frac{n-1}{2}} \not\equiv 1 \pmod{n},$$

mivel korábban tanultuk, hogy ha $d \mid m$, akkor $a \equiv b \pmod{m} \implies a \equiv b \pmod{d}$. Mivel $A \implies B$ tagadása esetén $\neg B \implies \neg A$, ezért $a \not\equiv b \pmod{d} \implies a \not\equiv b \pmod{m}$. Másrészt $z \equiv 1 \pmod{q_i}$, $2 \leq i \leq s$ miatt

$$z^{\frac{n-1}{2}} \equiv 1 \not\equiv -1 \pmod{q_2}, \quad \text{és így} \quad z^{\frac{n-1}{2}} \not\equiv -1 \pmod{n}.$$

Tehát

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

vagyis nem teljesül (21), tehát z valóban tanú.

II. Most már csak azt kell belátni, hogy egy redukált maradékrendszer elemeinek legalább a fele tanú. Legyen t tetszőleges tanú. Továbbá legyenek $c_1, c_2, \ldots, c_k$ páronként inkongruens cinkosok. Azt fogjuk belátni, hogy ekkor $tc_1, tc_2, \ldots, tc_k$ páronként inkongruens tanúk. A tanúk száma tehát legalább akkora, mint a cinkosoké.
Felhasználjuk, hogy $(t, n) = (c_i, n) = 1$, mivel eleve feltettük, hogy a tanúk és

cinkosok csak n-hez relatív prímek lehetnek. Ez esetben viszont $(tc_i, n) = 1$ is igaz, mert ha olyan számokat tekintünk, amelyeknek nincsenek n-nel közös osztóik, akkor az azt jelenti, hogy prímtényezős felbontásukban nem szerepelnek azok a prímszámok, amelyek n felbontásában igen. Tehát, ha ezeket az n-hez relatív prímeket összeszorozzuk, akkor továbbra is relatív prímek maradnak n-hez.
Most belátjuk, hogy a tc_i elemek is páronként inkongruensek modulo n. Tehát tudjuk, hogy a c_i cinkosok páronként inkongruensek, vagyis

$$c_i \not\equiv c_j \pmod{n} \text{ ha } i \neq j.$$

Tegyük fel indirekt, hogy:

$$tc_i \equiv tc_j \pmod{n}.$$

Ekkor, mivel $(t, n) = 1$, ezért leoszthatunk t-vel, így

$$c_i \equiv c_j \pmod{n},$$

ami ellentmondás.
Most indirekt feltesszük, hogy valamelyik i-re tc_i cinkos, azaz

$$(tc_i)^{\frac{n-1}{2}} \equiv \left(\frac{tc_i}{n}\right) \pmod{n} \tag{28}$$

teljesül. Mivel c_i is cinkos, ezért teljesül rá a

$$c_i{}^{\frac{n-1}{2}} \equiv \left(\frac{c_i}{n}\right) \pmod{n} \tag{29}$$

kongruencia. Ha (28) és (29)-et összeszorozzuk, akkor kapjuk, hogy

$$t^{\frac{n-1}{2}} c_i{}^{n-1} \equiv \left(\frac{t}{n}\right)\left(\frac{c_i}{n}\right)^2 \pmod{n}. \tag{30}$$

Továbbá (29)-et négyzetre emelve

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

adódik, amit beírva (30)-ba kapjuk, hogy

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

ami azt jelenti, hogy t is cinkos, ami ellentmondás.
Így beláttuk, hogy ha veszünk páronként inkongruens cinkosokat és végigszorozzuk egy tanúval, akkor páronként inkongruens tanúkat kapunk, vagyis így legalább annyi tanút kapunk, mint cinkost. Tehát egy redukált maradékrendszer elemeinek legalább a fele tanú. ■

A következő prímteszt alapja egyrészt a kis Fermat-tétel, illetve a következő állítás.
Állítás: Ha p prím és $u^2 \equiv 1 \pmod{p}$, akkor csak $u \equiv \pm 1 \pmod{p}$ lehetséges, ahogy azt a modulo p gyökvonásról tanultuk. Például modulo 8 esetén a ± 1 mellett ± 3 is kijöhetne. A kis Fermat-tétel miatt $(a, p) = 1$, vagyis $p \nmid a$. Ekkor az

$$a^{p-1}, a^{\frac{p-1}{2}}, a^{\frac{p-1}{4}}, \ldots$$

számok modulo p vett legkisebb abszolút értékű maradékainak sorozata mindenképpen 1-gyel kezdődik (a kis Fermat-tétel miatt) és vagy végig 1 vagy valahányadik lépésnél -1-et kapunk.
Ha viszont p helyett egy tetszőleges n összetett számot veszünk, akkor sok a esetén már nem ilyen sorozatot kapunk.

3.2.6. Tétel (Miller-Lenstra-Rabin-prímteszt).

Legyen $n > 1$ páratlan szám, $n - 1 = 2^k r$, ahol r páratlan. Az

$$a^r, a^{2r}, a^{4r}, \cdots, a^{2^{k-2}r} = a^{\frac{n-1}{4}}, a^{2^{k-1}r} = a^{\frac{n-1}{2}} \tag{31}$$

számokat jó sorozatnak nevezzük, ha ezek modulo n vett legkisebb abszolút értékű maradékai között előfordul -1 vagy pedig a^r maradéka 1.
Ha n prím, akkor (31) minden $a \not\equiv 0 \pmod{n}$ esetén jó sorozat.
Ha n összetett, akkor (31) egy modulo n teljes maradékrendszer elemeinek kevesebb, mint a felére alkot jó sorozatot.

A feltételt gyorsan tudjuk ellenőrizni. Először kiszámoljuk a^r maradékát modulo n, ezt ismételt négyzetre emelésekkel tehetjük meg. Utána $a^{2r}, a^{4r}, \ldots$ sorozat elemei egy-egy további négyzetre emelést igényelnek.

Tekintsünk erre egy példát: a 221-ről szeretnénk megállapítani, hogy vajon prím vagy összetett. Ekkor $n-1 = 220 = 2^2 \cdot 55$. Ebből kapjuk, hogy $k = 2$ és $r = 55$. Vegyünk véletlen egy 221-nél kisebb számot, például a 174-et, ez lesz az a.

$$174^{55} \equiv 47 \not\equiv \pm 1 \pmod{221}$$

$$174^{110} \equiv 220 = n - 1 \equiv -1 \pmod{221}$$

Mivel $220 \equiv -1 \pmod{221}$, ezért vagy a 221 prím vagy a 174 cinkos.
Próbáljunk meg egy másik véletlen számot, legyen ez a 137.

$$137^{55} \equiv 188 \not\equiv \pm 1 \pmod{221}$$

$$137^{110} \equiv 205 \neq n - 1 \not\equiv -1 \pmod{221}.$$

Bizonyítás:
Ha n prím és p nem osztója a-nak, akkor a 2.2.6 tétel előtti állítás miatt jó sorozatot kapunk.
Ha n összetett, akkor tanúnak fogjuk nevezni azokat, amelyek n összetettsége mellett nem adnak jó sorozatot, vagyis tanusítják n összetettségét. Azok lesznek a cinkosok, amelyekkel jó sorozatot kapunk, de n mégis összetett. Ebben az értelemben, a fent említett példában a 137 egy tanú a 221 összetettségét tekintve, vagyis azt tanúsítja, hogy a 221 nem prím. Ennélfogva a 174 valójában cinkos. Természetesen ez még semmit nem mond a 221 felbontásáról, ami $13 \cdot 17$.

Vagyis, ha a tanú, akkor

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

így két eset lehetséges:

$$a^{\frac{n-1}{2}} \equiv 1, \quad \text{de} \quad \left(\frac{a}{n}\right) = -1$$

vagy

$$a^{\frac{n-1}{2}} \equiv -1, \quad \text{de} \quad \left(\frac{a}{n}\right) = 1.$$

Ha n összetett és nem négyzetmentes, akkor ugyanúgy történik a bizonyítás, mint a 2.2.4-es tételnél. Tehát ugyanúgy gyártunk egy szimultán kongruenciarendszert, amelynek egy megoldása v. Be akarjuk látni, hogy v tanú és ismét feltesszük indirekt, hogy v cinkos, vagyis

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

Ha ezt négyzetre emeljük akkor biztosan 1-et kapunk. Itt két eset lehetséges. Az egyik, hogy a sorozatunk végig $+1$ és ekkor a négyzete is annyi. A másik esetben, ha a sorozat utolsó tagja -1, annak a négyzete is $+1$. A bizonyítás innentől ugyanúgy folytatódik, tehát ugyanúgy ellentmondásra jutunk.

Ha n összetett és négyzetmentes, akkor vegyük azt a legnagyobb j számot, amelyre $0 \leq j \leq k-1$ és amihez van olyan $(a, n) = 1$, hogy

$$a^{2^j r} \not\equiv 1 \pmod{n}. \tag{32}$$

Például a $j = 0$ és $a = -1$ választással biztosak lehetünk benne, hogy van ilyen j és a számpár, mivel:

$$(-1)^{2^0 r} \not\equiv 1 \pmod{n}$$

$$(-1)^r \not\equiv 1 \pmod{n}.$$

Ez biztosan igaz, mert r páratlan. Ha pedig van ilyen j, akkor van köztük egy maximális, amely még $k-1$-nél kisebb.
Most vegyük az n egy prímosztóját, q_1-et. Erre is fennáll a (32)-es kongruencia:

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

Ekkor hasonlóan a 2.2.4 tétel bizonyításához vegyük z-t, ami egy megoldása az

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

szimultán kongruenciarendszernek, ahol q_i-k továbbra is az n prímosztói. Tehát

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

Emiatt:

$$z^{2^j r} \equiv a^{2^j r} \not\equiv 1 \pmod{q_1}, \quad \text{és így} \quad z^{2^j r} \not\equiv 1 \pmod{n},$$

másrészt $z \equiv 1 \pmod{q_i}$, $2 \leq i \leq s$ miatt

$$z^{2^j r} \equiv 1 \not\equiv -1 \pmod{q_2}, \quad \text{és így} \quad z^{2^j r} \not\equiv -1 \pmod{n}.$$

Vagyis azt mondhatjuk, hogy

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

viszont j definíciója szerint ($j < k - 1$ esetén)

$$z^{2^{j+1} r} \equiv 1 \pmod{n},$$

mivel j maximális olyan szám, amire (32) fennáll, vagyis ha azt négyzetre emeljük, akkor biztosan 1-et kapunk.

Az utolsó lépés megegyezik a 2.2.4-es tételével. Ha az első esetben kapott v-t, illetve a második esetben kapott z-t megszorozzuk páronként inkongruens cinkosokkal, akkor ugyanolyan módon belátható, hogy páronként inkongruens tanúkat kapunk. Erre a speciálisan előállított z-re biztosan igaz, azonban, ha tetszőleges tanút veszünk, akkor nem feltétlenül. Tehát beláttuk, hogy összetett n esetén egy redukált maradékrendszer elemeinek legalább a fele tanú. ■

A két prímtesztet összehasonlítva azt kapjuk, hogy a Miller-Lenstra-Rabin teszt hatékonyabb, mint a Solovay-Strassen a következő értelemben.

Ha egy adott n-re az a tanú a Solovay-Strassen tesztnél, akkor az tanú lesz a másiknál is. Vagyis, ha egy a-ra nem teljesül, hogy $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$, akkor ugyanerre az a-ra a Miller-Lenstra-Rabin tesztnél előállított sorozat nem alkothat jó sorozatot, vagyis nem teljesül a tagjaira, hogy modulo n vett legkisebb abszolút értékű maradékai között előfordul a -1 vagy pedig a^r maradéka 1.

Bizonyítás: Legyen az $n > 1$ páratlan szám kanonikus alakja $n = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, és $n - 1 = 2^k r$, ahol r páratlan. Azt akarjuk tehát belátni, hogy ha egy a-ra a 2.2.6 tétel alapján definiált jó sorozatot kapunk, akkor $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ is fennáll.
Ha $a^r \equiv 1 \pmod{n}$, akkor ezt 2^{k-1} hatványra emelve (mivel a 2.2.6 tétel alapján $a^{2^{k-1}r} = a^{\frac{n-1}{2}}$) azt kapjuk, hogy $a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$. Továbbá

$$1 = \left(\frac{1}{n}\right) = \left(\frac{a^r}{n}\right) = \left(\frac{a}{n}\right)^r,$$

és mivel feltettük, hogy r páratlan, ezért $\left(\frac{a}{n}\right) = 1$ biztosan, mivel -1 páratlan hatványon -1 lenne.
Vagyis $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ teljesül.
Most feltesszük, hogy

$$a^{2^j r} \equiv -1 \pmod{n}, \text{ ahol } 0 \leq j \leq k-2. \tag{33}$$

Ezt négyzetre emelve, a jobb oldalon 1-et, a bal oldalon a legnagyobb j megválasztása esetén is legfeljebb $a^{2^{k-1}r}$-t kapunk, mivel $j < k - 1$. Mivel $a^{2^{k-1}r} = a^{\frac{n-1}{2}}$, ezért $a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$. Azt kell még igazolni, hogy $\left(\frac{a}{n}\right) = 1$ is teljesül. A (33)-as kongruenciát modulo q_i-re nézve

$$a^{2^j r} \equiv -1 \pmod{q_i}$$

majd négyzetre emelve azt kapjuk, hogy

$$a^{2^{j+1} r} \equiv 1 \pmod{q_i}.$$

Ekkor ismét használjuk a rend tulajdonságait, vagyis

$$o_{q_i}(a) \not| \ 2^j r \quad \text{és} \quad o_{q_i}(a) \mid 2^{j+1} r,$$

és így

$$o_{q_i}(a) = 2^{j+1} r_i, \quad \text{ahol} \quad r_i \mid r.$$

Mivel q_i prím, ezért a fentiből

$$a^{2^j r_i} \equiv -1 \pmod{q_i}$$

adódik. Továbbáb $o_{q_i}(a) \mid \varphi(q_i) = q - 1$, ezért egy alkalmas h_i-vel

$$q_i = 1 + 2^{j+1} r_i h_i. \tag{34}$$

Az utóbbi két összefüggést felhasználva

$$\left(\frac{a}{q_i}\right) \equiv a^{(q_i-1)/2} = a^{2^j r_i h_i} = (a^{2^j r_i})^{h_i} \equiv (-1)^{h_i} \pmod{q_i}.$$

Ez alapján pedig $\left(\frac{a}{n}\right)$ kiszámolható

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{s} \left(\frac{a}{q_i}\right)^{\alpha_i} = (-1)^{\sum_{i=1}^{s} \alpha_i h_i}$$

módon. Ahhoz, hogy a jobb oldalon 1 legyen, azt kell belátnunk, hogy $\sum_{i=1}^{s} \alpha_i h_i$ egy páros szám. Ez azt is jelenti, hogy mivel minden r_i-ről feltettük, hogy páratlan, ezért ha megszorozzuk velük ezt a összeget, akkor a parítás nem változik meg, vagyis, ha eredetileg páros volt, akkor r_i-kel megszorozva is az lesz. (34) alapján:

$$n = \prod_{i=1}^{s} q_i^{\alpha_i} = \prod_{i=1}^{s} (1 + 2^{j+1} r_i h_i)^{\alpha_i}.$$

A binomiális tétel alapján ennek a szorzatnak egy i-edik tagja a következőképpen írható fel:

$$(1 + 2^{j+1} r_i h_i)^{\alpha_i} = 1 + \alpha_i (2^{j+1} r_i h_i) + \binom{\alpha_i}{2} (2^{j+1} r_i h_i)^2 + \ldots =$$

$$= 1 + 2^{j+1} \alpha_i r_i h_i + 2^{j+2} C_i,$$

mivel az összeg harmadik tagjától kezdve minden tagból kiemelhető 2^{j+2}, hiszen onnantól kezdve $(2^{j+1}r_ih_i)$ egyre nagyobb hatványokon szerepel. Így azt kapjuk, hogy

$$n = \prod_{i=1}^{s}(1 + 2^{j+1}\alpha_i r_i h_i + 2^{j+2}C_i).$$

Ezen s darab három tagú összeg összeszorzásával elsőként kapunk 1-et, illetve minden i-re egy $2^{j+1}\alpha_i r_i h_i$ tagot, ha az s darab zárójel közül $s-1$-ből az 1-eseket és egy zárójelből a $2^{j+1}\alpha_i r_i h_i$ tagot szorzzuk össze. A többi tag mindegyikéből pedig kiemelhető 2^{j+2} és így

$$n = 1 + (2^{j+1}\sum_{i=1}^{s}\alpha_i r_i h_i) + 2^{j+2}C.$$

Feltettük, hogy $n-1 = 2^k r$, ezért $n = 2^k r + 1$. Ezt beírva a fenti egyenlőség bal oldalára, majd 1-et kivonva mindkét oldalból kapjuk, hogy

$$2^k r = 2^{j+1}\sum_{i=1}^{s}\alpha_i r_i h_i + 2^{j+2}C.$$

Ezt egyszerűsíthetjük 2^{j+1}-nel:

$$2^{k-j-1}r = \sum_{i=1}^{s}\alpha_i r_i h_i + 2C.$$

Végül 2C-t kivonva a

$$2^{k-j-1}r - 2C = \sum_{i=1}^{s}\alpha_i r_i h_i \tag{35}$$

egyenlőséghez jutunk. Ekkor azt használjuk fel, hogy $j < k-1$, vagyis 2^{k-j-1} egy pozitív egész kitevőjű 2 hatvány, ezt szorozva r-rel továbbra is páros marad, és belőle kivonva a 2C páros számot azt kapjuk, hogy a bal oldal páros. Tehát a jobb oldal is páros, ezzel beláttuk, amit akartunk.
Ha pedig a

$$a^{2^{k-1}r} = a^{\frac{n-1}{2}} \equiv -1 \pmod{q_i}$$

esetet nézzük, akkor azt kell belátni, hogy $\left(\frac{a}{n}\right) = -1$, ami az előzőek alapján azt jelenti, hogy a $\sum_{i=1}^{s} \alpha_i r_i h_i$ összeg páratlan. Ez csak úgy lehetséges, hogy ha $j = k-1$, mert ekkor (35) bal oldalán $2^{k-(k-1)-1}r-2C = 2^0 r-2C = r-2C$-t kapunk és mivel r páratlan, ezért a bal oldal is az, tehát a jobb oldal páratlan, és pont ezt akartuk. ■

A két tesztet összehasonlítva az is belátható, hogy a Miller-Lenstra-Rabin-teszt esetén egy redukált maradékrendszer elemeinek legalább a $\frac{3}{4}$-e tanú.

Végül itt említeném még meg az AKS-algoritmust, ami a jelenlegi "legfrissebb" prímteszt. 2002 augusztusában találta ki három indiai matematikus, Manindra Agrawal, Neeraj Kayal, és Nitin Saxena. Ez egy polinomiális prímteszt, aminek segítségével már teljes biztonsággal tudjuk eldönteni egy számról, hogy az prím-e, köszönhetően annak, hogy itt "cinkos" már nem fordulhat elő. A következő tételre alapszik az AKS-algoritmus.

3.2.7. Tétel.

Legyen $n \geq 2$ természetes szám, r pedig olyan n-nél kisebb természetes szám, hogy n rendje r-rel osztva nagyobb, mint $(\log n)^2$. Ekkor n pontosan akkor prím, ha:

1. n nem teljes hatvány,
2. n-nek nincs olyan p_i prímtényezője, amire $p_i \geq r$,
3. $(x+a)^n \equiv x^n + a \pmod{(n, x^r - 1)}$ teljesül minden $1 \leq a \leq \sqrt{r}\log n$ egész számra.

Az algoritmus segítségével ellenőrizni tudjuk, polinom idő alatt (amennyiben n-et binárisan reprezentáljuk), ezen feltételek teljesülését. Például azt, hogy n teljes hatvány-e legfeljebb $\lceil \log_2 n \rceil^2$ lépésben meg tudjuk mondani, és az egyes lépések számítási igénye sem nagyobb. Ha veszünk mondjuk egy 101 jegyű n számot, akkor első lépésként ellenőrizzük, hogy négyzetszám-e. Ha ez igaz, akkor biztosan egy 51 jegyű szám négyzete, tehát vesszük

a legkisebb és a legnagyobb 51 jegyű számot, és mint ahogy a Barchoba kérdéseknél megtanultuk felező kereséssel $\lceil \log_2 n \rceil$ lépésben meg tudjuk találni. Ha nem négyzetszám, akkor második lépésként ellenőrizzük, hogy köbszáme ugyanezzel a módszerrel, ugyanennyi lépésben és így tovább egészen a $\lfloor \log_2 n \rfloor$-edik hatványig. Ennél nagyobb hatvány nem jöhet szóba, mivel $2^{\log_2 n} = n$. Természetesen ez csak elméleti meggondolás, ezeket a műveleteket a számítógép pillanatok alatt elvégzi helyettünk.

4. Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek, Károlyi Gyulának, aki már a téma kiválasztásában is sokat segített, illetve a dolgozat elkészítése során hasznos tanácsokkal, észrevételekkel, ötletekkel látott el mind formailag, mind tartalmilag. Köszönöm továbbá türelmét és magyarázatait.

Hivatkozások

[1] Freud Róbert - Gyarmati Edit, *Számelmélet*, Nemzeti Tankönyvkiadó, 2000

[2] Agrawal, M, Kayal, N. and Saxena, N.:Primes is in P, *Annals of Math* 160 (2004) 781-793

[3] http://hu.wikipedia.org/wiki/Prímteszt

[4] http://en.wikipedia.org/wiki/Miller-Rabin primality test

[5] http://www.mat.uniroma2.it/ schoof/millerrabinpom.pdf