Számítógépes prímtesztelés

Előadás

Járai Antal

$16869987339975 \cdot 2^{171960} \pm 1$ ikerprímek.

1991 *Mathematics Subject Classification*. Primary: 11-04. Secondary: 11A41.

Typeset by $\mathcal{AMS}$-TEX

A számelmélet két legrégebbi algoritmikus problémája:

- Döntsük el egy számról, hogy prím vagy összetett.
- Ha összetett, bontsuk prímtényezőkre.

Az első problémáról fogok beszélni.

Néhány napja találtuk (Csajbók Tímea, Farkas Gábor, Járai Antal, Járai Zoltán, Kasza János) a fenti ikerprimet, amely a jelenleg ismert legnagyobb.

A híres ikerprím sejtés szerint végtelen sok ikerprím van. Bateman és Horn alábbi, sokkal általánosabb sejtése még a prím s-esek asszimptotikus sűrűségét is megadja egy sokkal általánosabb esetben.

Sejtés. *Legyenek $f_1, f_2, \dots, f_s$ irreducibilis polinomok, egész együtthatókkal és pozitív főegyütthatókkal. Ha*

$$\pi_{f_1,\dots,f_s}(N)$$

jelöli azon $0 < n \le N$ egészek számát, amelyekre

$$f_1(n), \dots, f_s(n)$$

mind prímek, akkor

$$\pi_{f_1,\dots,f_s}(N) \sim C_{f_1,\dots,f_s} \frac{1}{\deg(f_1)\cdots\deg(f_s)} \sum_2^N \frac{1}{(\ln(n))^s},$$

ahol

$$C_{f_1,\dots,f_s} = \prod_p \Big(1 - \frac{w(p)}{p}\Big)\Big(1 - \frac{1}{p}\Big)^{-s};$$

itt $w(p)$ jelöli az

$$f_1(x)\cdots f_s(x) = 0 \pmod p$$

kongruencia x megoldásainak számát.

Megmutatható, hogy a végtelen szorzat mindig konvergens, és pozitív, ha minden p prímre $w(p) < p$.

Az egyszerű gondolat a sejtés mögött az, hogy a prímszámtétel szerint annak valószínűsége, hogy egy nagy n szám prím, $1/\ln(n)$. Így annak valószínűsége, hogy az

$$f_1(n), \ldots, f_s(n)$$

számok mind prímek, ha ezek az események függetlenek volnának,

$$\frac{1}{\ln f_1(n) \cdots \ln f_s(n)}$$

lenne. Azonban, az $(f_1(n), \ldots, f_s(n))$ szám s-es nem véletlenszerű. $C_{f_1,\ldots,f_s}$ definíciójában az $1 - w(p)/p$ szám annak az esélye, hogy az $f_1(n), \ldots, f_s(n)$ egészek egyike sem osztható p-vel, $(1 - 1/p)^s$ pedig annak az esélye, hogy egy véletlen szám s-es egészei közül egyik sem osztható p-vel, így logikus azt várni, hogy annak esélye, hogy $f_1(n), \ldots, f_s(n)$ mindegyike prím legyen,

$$\frac{C_{f_1,\ldots,f_s}}{\ln f_1(n) \cdots \ln f_s(n)}.$$

Így a $\pi_{f_1,\ldots,f_s}(a, b)$ várható száma azon n-eknek $(a, b]$-ben, amelyekre $f_1(n), \ldots, f_s(n)$ egyszerre prímek,

$$\pi_{f_1,\ldots,f_s}(a, b) \sim C_{f_1,\ldots,f_s} \int_a^b \frac{du}{\ln f_1(u) \cdots \ln f_s(u)}.$$

Például, ha $f_1(X) = X$ és $f_2(X) = X + 2$ akkor az ikerprímek számára nyerünk egy asszimptotikus formulát. A kostans ebben az esetben $2C_2$ ahol $C_2 = 0.66016\ldots$ az ikerprím konstans.

Hasonló heurisztika alkalmazható, hogy megbecsüljük egy kis prímekkel való szitálás után visszamaradó s-esek számát.

A sejtés által adott becslések nagyon jó egyezésben vannak a számítógépes kísérletek eredményeivel.

Egyszerű prímtesztek

Miller-Rabin valószínűségi teszt. Egy m páratlan egészre, ez az algorimus megpróbálja eldönteni, hogy m prím vagy nem. Legyen $m = 1 + 2^k q$ ahol q páratlan, és a egy egész az $1 < a < m$ intervallumban. Az ötlet az, hogy ha $m = 1 + 2^k q$ prím, és $a^q \bmod m \neq 1$, akkor az

$$a^q \bmod m, \quad a^{2q} \bmod m, \quad a^{4q} \bmod m, \ldots, a^{2^k q} \bmod m$$

sorozat 1-re végződik, és az első 1 előtt a sorozatban $m - 1$ áll, mivel $b^2 \bmod m = 1$ megoldásai csak $b = \pm 1$ ha m prím, ugyanis $(b-1)(b+1)$ osztható m-el.

A legfontosabb tény az algoritmussal kapcsolatban, hogy ha egy véletlen a-t választunk, akkor az algoritmus kisebb mint $1/4$ valószínűséggel hibázik. Ismételt alkalmazással tetszőlegesen kis valószínűséget elérhetünk.

A valószínűségi teszt igen ritkán hibázik. $25 \cdot 10^9$-ig csak 13 olyan összetett szám van, amely átcsúszik a teszten $a = 2, 3, 5$ alapokkal.

Lucas teszt. *Egy m pozitív egész szám akkor és csak akkor prím, ha van olyan a amelyre $(a, m) = 1$ és*

$$a^{m-1} \bmod m = 1$$

de minden $p | m - 1$ prímre $a^{(m-1)/p} \bmod m \neq 1$.

Riesel teszt. *Tegyük fel, hogy h egy páratlan egész és hogy $2^n > h$. Ekkor $N = h2^n - 1$ akkor és csak akkor prím, ha $v_{n-2} \equiv 0 \bmod N$, ahol $v_s = v_{s-1}^2 - 2$ és $v_0 = a^h + a^{-h}$. Ebben a kifejezésben a egy*

$$a = \frac{(k + l\sqrt{D})^2}{r}$$

alakú egység $\mathbf{Q}(\sqrt{D})$-ben, ahol

$$\left(\frac{D}{N}\right) = -1$$

és

$$\frac{k^2 - l^2 D}{r}\left(\frac{r}{N}\right) = -1.$$

Itt k, l és r egészek. Megjegyezzük, hogy $|r| = |k^2 - l^2 D|$.

A kritikus pont: a szorzás

Szorzás és polinomszorzás. Számok szorzása polinomszorzásra vezethető vissza:

$$\left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{k=0}^{\infty} b_k x^k\right) = \sum_{k=0}^{\infty} c_k x^k, \quad c_k = \sum_{i+j=k} a_i b_j.$$

Megfordítva, a polinomszorzás is visszavezethető nagy számok szorzására. Ha a B alapszám valamivel hosszabb, mint a jegyek hosszának kétszerese, akkor $\sum_k a_k B^k$ és $\sum_k b_k B^k$ szorzatának jegyei a c_k-k. Mindkét trükk hasznos.

Szorzás gyors Fourier transzformációval. Egy *valós* $2n$ tagú $f_0, f_1, \dots, f_{2n-1}$ sorozat diszkrét Fourier transzformáltját használjuk. Definíció szerint ez

$$\hat{f}_k = \sum_{j=0}^{2n-1} f_j \omega^{-jk}$$

$j = 0, 1, \dots, 2n-1$-re, ahol $\omega = e^{-\pi i/n} = e^{-2\pi i/(2n)}$ egy $2n$-edik egységgyök. Egyszerűbb jelöléseket kapunk, ha ezt a sorozatot, és az eredeti sorozatot is kiterjesztjük egy $2n$ szerint periódikus, mindkét irányban végtelen sorozattá.

Ha veszünk egy másik $g_0, g_1, \dots, g_{2n-1}$ sorozatot, és $f_k = g_k = 0$ ha $n \le k < 2n$, akkor felhasználhatjuk a $\hat{f}_k$ és $\hat{g}_k$ sorozatokat, hogy kiszámoljuk a

$$h_k = \sum_{j=0}^{k} f_j g_{k-j}$$

számokat $k = 0, 1, \dots, 2n-2$-re. Ezek a számok a $\sum_{j=0}^{2n-2} h_j x^j$ polinom együtthatói, amely a $\sum_{j=0}^{n-1} f_j x^j$ és $\sum_{j=0}^{n-1} g_j x^j$ polinomok szorzata. Ezért nagyon hasznosak, ha két hosszú szám szorzatát akarjuk kiszámolni, amelyeket $f_0, f_1, \dots, f_{n-1}$ illetve $g_0, g_1, \dots, g_{n-1}$ reprezentál x alapú számrendszerben. Mivel a h_k sorozat az f_k és a g_k sorozatok göngyölt konvolúciója, h_k mint $\hat{h}_k = \hat{f}_k \hat{g}_k$ inverz diszkrét Fourier transzformáltja számolható.

Diszkrét Fourier transzformáltnak és inverzének a számítása $n \log_2 n$ művelettel megoldható az FFT algoritmust használva.

Mivel f_k valós, azt kapjuk, hogy

$$\bar{\hat{f}}_{2n-k} = \sum_{j=0}^{2n-1} f_j \omega^{(2n-k)j} = \hat{f}_k$$

minden $k \in \mathbf{Z}$-re. Az n független komplex $\hat{f}_k$ kiszámítása a komplex $F_k = f_{2k} + i f_{2k+1}$, $k = 0, 1, \ldots, n-1$ sorozat Fourier transzformáltjának kiszámítására redukálható.

Nézzünk egy példát. Osszuk a 2^{19} bites számot 16 bites darabokra. 2^{15} komplex koordinátával rendelkező vektorok Fourier és inverz Fourier transzformáltját kell kiszámítani. Az eredményvektor tagjai legfeljebb 2^{15} darab 32 bites szorzat összegei. Így legalább 47 bit pontosságot kell elérnünk. Elég nagy valószínűséggel rekonstruálni tudjuk a szorzatot.

A Schönhage–Strassen-féle gyorsszorzó algoritmus. Ez a nevezetes algoritmus két n-bites szám szorzásához szükséges bit műveletek számát $n \log n \log\log n$ rendig képes redukálni. A fő gondolat FFT-IFFT használata, de minden műveletet moduló egy $2^{2^k}+1$ Fermat-szám végzünk egy alkalmas k-val amelyre $2^k \approx \sqrt{n}$. Az egységgyökök kettőhatványok, így az FFT-IFFT alatt csak összeadásra, kivonásra és eltolásra van szükség. A jegyenkénti szorzás rekurzív módon történik. Egy finom trükk az eredményt csak moduló 2^n+1 kiszámolni, ez rekurzív hívások esetén további nyereséget hoz. Például egy $16 * 32768$ bites számot 2^{10} részre oszthatunk, amelyek mindegyike 17 darab 32 bites szóból áll, és az FFT-IFFT 2^{11} taggal történik $\bmod(2^{1024}+1)$.

Az Agrawal–Kayal–Saxena-algoritmus

Az AKS-algoritmus ötlete. *Ha* $\operatorname{lnko}(s,n)=1$, *akkor* $(x+s)^n \equiv x^n + s \pmod{n}$ *pontosan akkor teljesül, ha* n *prím.*

Valóban, ha n prím, a kongruencia teljesül. Egyébként $p^k \| n$ esetén p^k nem osztója $\binom{n}{p}$-nek és relatív prím s^{n-p}-hez, így x^p együtthatója nem nulla.

Vizsgáljuk $(x+s)^n \equiv x^n + s$-et $\pmod{x^r-1, p}$.

AKS-tétel. *Ha* $n \in \mathbf{N}^+$, $q, r \in \mathbf{P}$, $S \subset \mathbf{Z}$ *véges,* $q | r-1$ *és* $n^{(r-1)/q} \bmod r \notin \{0,1\}$, *továbbá* $\operatorname{lnko}(n, s-s') = 0$, *ha* $s, s' \in S$, $s \neq s'$ *és*

$$\binom{\natural S + q - 1}{\natural S} \geq n^{2\lfloor\sqrt{r}\rfloor}, \qquad (x+s)^n \equiv x^n + s \pmod{x^r - 1, n}$$

minden $s \in S$*-re, akkor* n *prímhatvány.*

Megjegyzések. (1) Megmutatják, hogy van olyan c, hogy $c\lg^6 n$-ig van olyan r, amelyre van olyan q prímosztója $r-1$-nek, hogy $q \geq 4\sqrt{r}\lg n$ és q osztja az n moduló r vett rendjét. (Ez azzal ekvivalens, hogy $n^{(r-1)/q} \bmod r \neq 1$, mert $q > \sqrt{r-1}$.) Az elég nagy Sophie Germain prímek közül nagyon sok jó, ekkor $q \approx 32\lg^2 n$.

(2) Nyilván

$$\frac{(\natural S+q-1)(\natural S+q-2)\cdots(\natural S+1)}{1\cdot 2\cdot\dots\cdot(q-1)} \geq \left(\frac{\natural S+1}{q-1}\right)^{q-1},$$

és ha

$$\left(\frac{\natural S+1}{q-1}\right)^{q-1} \approx n^{2\sqrt{r}},$$

akkor

$$\natural S \approx \frac{1}{\sqrt{2}}r.$$

(3) Prímhatványteszt: még bináris kereséssel is elég gyors.

(4) Tovább élesítették, $r \approx 0.01\lg^2 n$ elérhető, $\natural S$ is csökkenthető, így ≈ 2000000-szor gyorsabb, $(\lg n)^{6+o(1)}$ sebességű. A valségi változat $(\lg n)^{4+o(1)}$ sebességű.

(5) Nem fér el a tárban.

Prímteszt elliptikus görbékkel

Elliptikus görbék. Egy *elliptikus görbe* $\mathbf{R}$ *felett* azon síkbeli (x, y) párok halmaza, amelyek kielégítik az

$$y^2 = x^3 + ax + b$$

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

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

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

ahol

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

λ az egyenes meredeksége.

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

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

akkor megmutatható, hogy egy Abel csoportot kapunk.

Még ha csak egy egységelemes kommutatív gyűrű adott, például $\mathbf{Z}/n\mathbf{Z}$, $\mathrm{lnko}(n, 6) = 1$, akkor is definiálhatjuk a fenti műveleteket *parciálisan*, azaz ha az osztás elvégezhető; természetesen ekkor nem kapunk csoportot. Fontos azonban észrevennünk, hogy ha $\mathrm{lnko}(n, 4a^3 + 27b^2) = 1$, akkor bármely p prímosztójára n-nek modulo p is egy elliptikus görbét kapunk, és ha $\mathbf{Z}/n\mathbf{Z}$ felett el tudunk végezni egy összeadást, akkor bármely p prímosztójára n-nek, az eredmény modulo p redukálva, az ugyanaz, mint ha előbb elvégezzük a modulo p redukálást, és aztán végezzük el a műveletet modulo p. (Az ∞ szimbólum redukálva saját maga.)

Prímteszteléshez és faktorizáláshoz csak ilyen, modulo n vett „elliptikus görbékre” lesz szükségünk.

Tétel. *Legyen* $n \in \mathbf{Z}$, $\gcd(6, n) = 1$ *és legyen* $\mathbf{E}_n$ *egy* $\mathbf{Z}/n\mathbf{Z}$ *feletti elliptikus görbe pontjainak a halmaza. Legyenek* m *és* s *egészek, úgy, hogy* $s|m$. *Tegyük fel, hogy találtunk olyan* P *pontot* $\mathbf{E}_n$*-ben, amelyre*

$$m \cdot P = 0 \quad \text{and} \quad \frac{m}{q} \cdot P \neq 0 \quad \text{minden } q \text{ prímfaktorára } s\text{-nek.}$$

Ekkor minden p *prímosztójára* n*-nek* $|\mathbf{E}_p| \equiv 0 \bmod s$. *Továbbá, ha* $s > (\sqrt[4]{n} + 1)^2$ *akkor* n *prím.*

Tétel [Hasse]. *Ha* $p > 3$ *prím, akkor egy* $\mathbf{Z}/p\mathbf{Z}$ *felett vett elliptikus görbe rendje* $p+1-2\sqrt{p}$ *és* $p+1+2\sqrt{p}$ *között van.*

Goldwasser–Kilian teszt. Az n valószínű prím prím voltának bizonyításához, válasszunk egy „elliptikus görbét" $\mathbf{Z}/n\mathbf{Z}$ felett, és egy m számot, amelyre a görbe rendje m, — legalábbis ha n prím. Ha m felírható fn_1 alakban, ahol f faktorait ismerjük, n_1 pedig valószínű prím, és $n_1 > (n^{1/4}+1)^2$, akkor n prím voltát ezen pont első tétele segítségével be tudjuk bizonyítani. Válasszunk ugyanis egy olyan P pontot, amely eleget tesz a tétel feltételeinek $s = n_1$ választással. Ehhez válasszunk egy véletlen P pontot a görbén (x véletlen, y-t kiszámítjuk). Számítsuk ki $(m/n_1)\cdot P = f\cdot P$-t; ha nincs definiálva, akkor megtaláltuk n_1 egy valódi osztóját, ami nagyon valószínűtlen. Annak valószínűsége, hogy $k \cdot P = 0$ legyen, kicsi, ha n prím, ebben az esetben válasszunk új pontot. Ellenőrizzük, hogy $n_1 \cdot (f \cdot P) = m \cdot P = 0$, aminek teljesülnie kell, ha n prím. Így P létezése bizonyítja, hogy n prím, ha n_1 prím. Most alkalmazzuk az eljárást n_1-re, stb.

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

Hatékony faktorizálási algoritmusokat használva, $o(\lg^4 n)$ futásidő érhető el (csak heurisztikusan!).

Részletezve, a teszt a következőképpen működik:

1. Kiválasztjuk D úgynevezett „alapdiszkriminánsoknak” egy elég nagy halmazát. Az alapdiszkriminánsokat növekvő abszolút érték szerint határozhatjuk meg: $D < -1$, $D \equiv 0 \pmod 4$ vagy $D \equiv 1 \pmod 4$ kell teljesüljön, és nem létezhet olyan $k > 1$ egész, amelyre D/k^2 is alapdiszkrimináns. A $D = -3$ és $D = -4$ esetek külön meggondolásokat igényelnek, ezeket itt mellőzzük, tehát feltesszük, hogy $D \leq -7$.

2. $\mathbf{Q}(\sqrt{D})$ algebrai egészei felírhatók $\nu = x + y\omega$ alakban, ahol x, y egészek, és $\omega = (D + \sqrt{D})/2$. Ekkor $|\nu|^2$ a ν normája, így azt akarjuk elérni, hogy

$$n = \left(x + y\frac{D}{2}\right)^2 - y^2\frac{D}{4} \tag{1}$$

teljesüljön. Átrendezve, azt kapjuk, hogy $4n = (2x+yD)^2 - y^2D$. Ha ez a feltétel teljesül, akkor egyrészt $(D|n) = 1$, másrészt minden p páratlan prímre, ami osztja D-t, teljesül, hogy $(n|p) = 1$. Ezek a feltételek szükségesek (de nem elégségesek) (1) teljesüléséhez.

3. Keressünk szükséges és elégséges feltételt (1) teljesüléséhez, és módszer arra, hogy az x, y egészeket meghatározzuk. (1) felírható

$$n = x^2 + xyD + y^2\frac{D(D-1)}{4} \tag{2}$$

alakba. A jobb oldal egy bilineáris forma x, y változókkal és egész együtthatókkal.

4. Általánosan, tekinthetünk

$$ax^2 + bxy + cy^2$$

alakú bilineáris formákat egész a, b, c együtthatókkal. Egy ilyen bilineáris formában bevezethetünk új változókat. Például az $x' = -y$, $y' = x$ helyettesítésnél az új forma együtthatói $a' = c$, $b' = -b$ és $c' = a$ lesznek, az $x' = x + ky$, $y' = y$ helyettesítésnél pedig, ahol k egész, az új együtthatók $a' = a$, $b' = b - 2ka$ és $c' = c - kb + k^2a$. Világos, hogy ezen helyettesítések során nem változik meg a forma értékkészlete, azaz a $\{ax^2 + bxy + cy^2 : x, y \in \mathbf{Z}\}$ halmaz és a $\{a'x'^2 + b'x'y' + c'y'^2 : x', y' \in \mathbf{Z}\}$ halmaz megegyeznek. Azt is nyilvánvaló, hogy $b^2 - 4ac = b'^2 - 4a'c'$, azaz ez a mennyiség, a bilineáris forma *diszkriminánsa* sem változik. Például a (2) jobb oldalán álló forma diszkriminánsa D. Egy bilineáris formát *pozitív*nak nevezünk, ha $a > 0$, a diszkriminánsa pedig negatív. Világos, hogy ekkor c is pozitív. Egy bilineáris formát *primitív*nek nevezünk, ha együtthatóinak legnagyobb közös osztója 1. A fenti (invertálható) transzformációk pozitív primitív formát pozitív primitív formába visznek. A fenti két transzformáció ismételt alkalmazásával minden pozitív primitív forma egy *redukált alak*ra hozható: ekkor $|b| \le a \le c$ és $b \ge 0$ ha $|b| = a$ vagy $a = c$. Ez úgy történik, hogy ha $-a < b \le a$ nem teljesül, akkor alkalmazzuk a második lépést ennek elérésére, ha pedig teljesül, és a forma még nem redukált, akkor alkalmazzuk az első lépést. Az algoritmus nagyon hasonlít az euklidészi algoritmushoz. Például a (2) jobb oldalán álló forma nem redukált, de egyetlen lépéssel redukálható: ha D páros, akkor a redukált forma $x^2 - (D/4)y^2$, ha pedig páratlan, akkor $x^2 + xy + y^2(1 - D)/4$. Gauss megmutatta, hogy a redukált alak egyértelmű: minden pozitív primitív formának egy és csak egy redukált alakja létezik. Az adott (negatív) D diszkriminánsú pozitív primitív formákat tehát ekvivalencia-osztályokba sorolhatjuk a szerint, hogy mi a redukált formájuk. Az ekvivalencia-osztályok számát a D diszkriminánshoz tartozó *ideálosztály szám*nak nevezzük, és $h(D)$-vel jelöljük.

5. Térjünk vissza annak vizsgálatához, hogy (2) megoldható-e? Euklidészi algoritmust alkalmazva x-re és y-ra, az derül ki, hogy ha van egy megoldása (2)-nek, akkor van olyan, a (2) jobb oldalával ekvivalens bilineáris forma is, amelyre $x = 1$, $y = 0$ esetén lesz a forma értéke n. Keressünk ilyen formát. Nyilván $a = n$ kell legyen, továbbá $b^2 - D$ osztható kell legyen $4n$-el, különben c nem lehetne egész. Keressünk egy olyan $0 < b' < n$-et, amelyre ${b'}^2 \equiv D \pmod{n}$. (Kell lenni ilyennek, legalább is ha n prím, feltéve, hogy $(D|n) = 1$.) Ha b' és D paritása megegyezik, akkor legyen $b = b'$, egyébként legyen $b = b' + n$. Így $c = (b^2 - D)/(4n)$ egész lesz. Megmutatható, hogy b lehetséges választásai ekvivalens formákat eredményeznek. Így azt kell ellenőriznünk, hogy ennek a formának a redukált alakja megegyezik-

e a (2) jobb oldalán szereplő forma redukált alakjával. Ha igen, akkor nyomon követve a redukció során felhasznált helyettesítéseket, x-et és y-t is megkapjuk, amire (2) fennáll. Ha nem, akkor (2) nem oldható meg. A minden D-re a siker esélye $1/(2h(D))$, mivel $1/2$ eséllyel tudunk gyököt vonni D-ből, és ha sikerül, akkor $1/h(D)$ az esélyünk.

6. Ha sikerült megtalálni ν-t, akkor mindjárt két lehetséges m-et találtunk. Ezeket megpróbáljuk faktorizálni, például próbaosztással. Ha sikerül annyi kis prímfaktort leválasztani, hogy egy valószínű prím marad vissza, akkor tovább léphetünk a rekurzióban. Ha ez nem sikerül, akkor újabb D-vel próbálkozunk.

7. Végül, ha a rekurzió elért egy elég kis számot, amiről már „ránézésre” (pl. próbaosztással) kiderül, hogy prím, felépítjük a „bizonyítékot”. Ez az

$$n, a, b, m, P, f, n_1, a_1, b_1, m_1, P_1, f_1, n_2, a_2, b_2, m_2, f_2, n_3, \ldots$$

sorozat, ahol $n, n_1, n_2, n_3, \ldots$ prímek, a_i, b_i egy modulo n_i elliptikus görbe együtthatói, m_i a rendje, P_i egy pontja, amely eleget tesz ezen pont első tétele feltételeinek, f_i pedig az m_i faktorizált része úgy, hogy $m_i = f_i n_{i+1}$. A „bizonyíték” meghatározása úgy történik, hogy (kellő pontosságú lebegőpontos aritmetikát használva) az adott n-hez talált D diszkrimináns segítségével kiszámítjuk a H_D Hilbert polinomot. Ez egy egész együtthatós polinom $h(D)$ fokszámmal, amelyet a

$$H_D(X) = \prod_{(a,b,c)} \left(X - j\left(\frac{b + \sqrt{D}}{2a} \right) \right)$$

szorzat definiál, ahol a szorzás az összes, a D diszkriminánshoz tartozó pozitív primitív redukált formákra értendő, j pedig egy rögzített komplex függvény, amely a felső félsíkon van definiálva, és

$$j(z) = \frac{\left(1 + 240 \sum_{k=1}^{\infty} \frac{k^3 q^k}{1-q^k}\right)^3}{q \prod_{k=1}^{\infty} (1-q^k)^{24}},$$

ahol $q = e^{2\pi i z}$. Megmutatható, hogy

$$j(z) = \frac{1}{q} + 744 + \sum_{k=1}^{\infty} c_k q^k,$$

ahol a c_k együtthatók pozitív egészek, és j definíciója alapján könnyen kiszámithatók. Az $m = |\nu \pm 1|^2$ rendű elliptikus görbék az

$$y^2 = x^3 + 3kx + 2k,$$
$$y^2 = x^3 + 3kc^2x + 2kc^3$$

görbék, ahol $k \equiv x_0/(1728 - x_0) \pmod{n}$, c egy tetszőleges szám, amire $(c|n) = -1$, x_0 pedig H_D egy tetszőleges gyöke modulo n. Megmutatható, hogy H_D modulo n elsőfokú tényezők szorzatára bomlik.