SZÁMÍTÓGÉPES SZÁMELMÉLET

Járai Antal

SZÁMÍTÓGÉPES SZÁMELMÉLET

A könyv bírálója

ISBN 000 00 0000 0

TARTALOMJEGYZÉK

I. ELŐSZÓ

Ez a könyvecske azokra a tapasztalatokra épül, amelyeket a szerző Paderbornban, Németországban, Karl-Heinz Indlekofer munkacsoportjában szerzett, ahol öt évig (1992–1997) dolgozott projektmenedzserként. A számítógépes számelméleti projektjeink keretében tíznél több új „világrekord" született. A legismertebb ezek közül talán a legnagyobb ismert ikerprím megtalálása. Az eredmények közös dolgozatokban kerültek publikálásra, és a kutatás jelenleg is tovább folyik. Ezen könyvecskének, illetve a speciálkollégiumnak, amelynek anyagát tárgyalja, az a célja, hogy az érdeklődőket felkészítse a közös munkában hallgatóként, szakdolgozóként, PhD hallgatóként vagy kollégaként való részvételre. Remélem azonban, hogy mindenki, aki a számítógépes számelmélet iránt érdeklődik, haszonnal forgathatja. Ugyancsak számítok azok érdeklődésére, akiket a nagy hatékonyságú számítások érdekelnek, mert rekordjaink hátterében mindenütt a modern algoritmusok lehetőségeinek és a modern mikroprocesszorok képességeinek végsőkig történő kihasználása áll. A mikroelektronika fantasztikus fejlődése mellett is csak ez tette lehetővé, hogy mára ezen a területen a szuperszámítógépek korábbi egyeduralma megszünjön. Természetesen a rekordok elképzelhetetlenek megfelelő számítógépes háttér nélkül. Paderborn-ban a Matematikai és Informatikai Intézetben 6–800 SUN munkállomás és három nagy párhuzamos gép — a legnagyobb 1024 processszorral — állt rendelkezésre. Természetesen ilyen háttérrel itthon nem rendelkezünk, mégis számos világrekordot sikerült munkacsoportunknak itt is elérni.

Általános bevezetésként Bressoud [9] elemi könyvét javaslom. Kezdetben, a régebbi módszerek ismertetésénél ezt követjük. Magasabb szintű Cohen [11] kitűnő könyve; a hangsúlyt inkább a számelméletre, és nem az algoritmusok sebességére helyezi. Az elméleti informatika kitűnő összefoglalásában, amelyet van Leeuwen [31] szerkesztett, a számítógépes számelmélet két kiválósága, A. K. Lenstra és H. W. Lenstra Jr. írta a számítógépes számelméleti részt; ez kiváló tömör összefoglalása az akkori helyzetnek.

A számelméleti alapismeretek megtalálhatók Niven és Zuckerman [37] könyvében. Magasabb szintű Serre [45] kis könyve.

Az elméleti informatika kitűnő tankönyve Cormen, Leiserson és Rivest [12] könyve; ebben megtalálhatók a szükséges informatikai alapismeretek. Régebbi, de nagyon jól használható könyv Aho, Hopcroft és Ullman [4] könyve. Az algoritmusok sokkal részletesebb analízise található D. E. Knuth: The art of computer programming című könyvének három kötetében (magyarul is megjelent), amely a programozási gyakorlatra helyezi a hangsúlyt [20,21,22,23,24,25,26,27]. Én úgy érzem, hogy ebből a könyvből tanultam a programozásról a legtöbbet.

A rejtjelzéssel való kapcsolatot részletesen tárgyalja Kranakis [30] könyve. Prímtesztek és a faktorizálás számítógépes módszereivel foglalkozik Riesel [44] könyve igen részletesen. Feltétlenül érdemes megnézni Ribenboim [42, 43] könyvét, különösen az új kiadást. Mivel az egész terület nagyon gyorsan fejlődik, számos itt tárgyalt módszer csak eredeti dolgozatokban található meg. Ezekre a megfelelő helyen fogunk hivatkozni. Néhány még publikálatlan eredmény is szerepelni fog. Bár a jegyzetet az utóbbi 10 évben to"bbszo"r javítottam, kiegészítettem, még a jelenlegi formája sem tekinthető véglegesnek, az oktatási és kutatási tapasztalatok alapján folyamatosan bővítem, és igyekszem a hibákat kijavítani. A legfontosabb új bővítés számos algoritmus Maple[1] megvalósítása; ez a honlapomon elérhető.

Budapest, 2011.02.25

Járai Antal

[1]Maple a Maple Inc. bejegyzett védjegye

II. ALAPVETŐ ALGORITMUSOK

1995 októberének első napjaiban Harvey Dubner megtalálta az akkor ismert legnagyobb, 5129 jegyű ikerprímet. A mi korábbi ikerprím rekordunk $697053813 \cdot 2^{16352} \pm 1$ volt, 4932 decimális jeggyel. Néhány nappal előbb találta Dubner a legnagyobb ismert, 5089 jegyű Sophie Germain prímet (azaz olyan p prímet, amelyre $2p+1$ is prím), megdöntve 4931 illetve 4932 jegyű, $157324389 \cdot 2^{16352} - 1$ és $470943129 \cdot 2^{16352} - 1$ rekordjainkat, amelyeket 1995 februárjában találtunk. Ekkor már futott ikerprímkereső programunk javított változata, és 11700 jegy körül keresett ikerprímeket. Mivel a teljes várható futásidő 1500–2000 CPU nap volt a Texas Instruments SuperSPARC[2] processzorát tartalmazó Sun[3] munkaállomásokon, (33 MHz és 60 MHz közötti órajellel), úgy döntöttünk, hogy leállítjuk a keresést egy időre, és új, kombinált teszt programunkat fogjuk futtatni, amely egyszerre képes ikerprímeket és Sophie Germain prímeket keresni, megfelezve ezzel a keresés idejét. A két teszt kombinálásának ötlete Dubner-től eredt. Mivel az új teszt futásidejét ≈ 5850 jegy körül 100 CPU napnál kevesebbre becsültük, úgy gondoltuk, jóval reálisabb lesz ebben a tartományban keresgélni, és csak később folytatni a kombinált teszttel a ≈ 11700 jegy körüli tartományban. A kombinált teszt programjának próbáihoz még szükség volt néhány napra, és addig hagytuk futni a régi programot. A leállítás előtti napon a régi program a $242206083 \cdot 2^{38880} \pm 1$ (11713 jegyű) ikerprímet találta. Ezután leállítottuk a régi programot, és elindítottuk az új, kombinált tesztet. Ez találta a jelenleg ismert legnagyobb Sophie Germain prímet: $p = 2375063906985 \cdot 2^{19380} - 1$ (5847 jegyű). Nagy p Sophie Germain prím segítségével, ha kongruens $3 \bmod 4$, nagy összetett Mersenne számok adhatók meg. Így $2^p - 1$, ahol $p = 2375063906985 \cdot 2^{19380} - 1$ a legnagyobb ismert összetett Mersenne szám.

Egyik e-mail-ében Harvey Dubner olyan p prímek keresését javasolta, amelyekre $p+2$ és $2p+1$ is prímek. Kombinált teszt programunk minden további nélkül képes volt erre. Elindítottunk egy keresést, és a $p = 4610194180515 \cdot 2^{5056} - 1$ (1535 jegyű) prímet találtuk, amelyre $p+2$ és $2p+1$ is prímek.

Mi áll ezeknek a rekordoknak a hátterében? Hogyan becsülhető egyáltalán a futásidő? Milyen algoritmusokat kell használnunk? Hogyan írhatunk elég gyors programot? Mire jók a nagy prímek? Mire használhatók még az elkészült programok? Mi a kapcsolat a faktorizálással? Milyen más számelméleti keresésekre,

[2]SPARC a SPARC International bejegyzett védjegye

[3]Sun a Sun Microsystem Inc. bejegyzett védjegye

tesztekre használhatók még programjaink? Ezekre és hasonló kérdésekre keressük a választ ebben az első részben.

1. A prímek eloszlása, szitálás

1.1. A prímszámtétel. Mint tudjuk, Euklidész már bizonyította, hogy végtelen sok prím van: ha véges sok prím lenne, a szorzatukhoz egyet hozzáadva, a kapott számnak a prímosztói nem szerepelhetnek a listában. A matematikusokat már régen izgatta a prímek eloszlása, vagy olyan képletek keresése, amelyek csak prímeket adnak. *Marin Mersenne* (1588–1648) például 1644-ben azt állította, hogy $2^p - 1$ alakú, ma Mersenne-számoknak nevezett számok közül $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ prímet ad, de más, 257-nél kisebb érték nem (nem igaz), Fermat pedig azt gondolta, hogy $2^{2^n} + 1$ prím, ha $n = 0, 1, 2, \ldots$ (ez sem igaz).

15 évesen, 1792-ben *Karl Friedrich Gauss* (1777–1855) azt sejtette, hogy az x-nél nem nagyobb prímek $\pi(x)$ számát

$$\int_2^x \frac{dt}{\ln t}$$

közelíti. Gauss sejtése pontosabban

$$\pi(x) \sim \int_2^x \frac{dt}{\ln t}$$

alakba írható. Ennek a jelölésnek a pontos jelentése, hogy a két függvény hányadosa 1-hez tart, amint x tart végtelenhez. Ez a híres *prímszámtétel*. 1896-ban bizonyította be egymástól függetlenül *Charles Jean de la Vallée Poussin* (1866–1962) és *Jacues Hadamard* (1865–1963). Pontosabban, ma azt tudjuk, hogy alkalmas $A > 0$-val

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + O\left(xe^{-A(\ln x)^{3/5}/(\ln\ln x)^{1/5}}\right).$$

Az itt szereplő O jelölést lépten-nyomon használni fogjuk: $O(f(x))$ egy olyan függvényt jelent, amelynek abszolút értéke elég nagy x-ekre korlátos az f pozitív függvény egy konstansszorosával. A hasonló $o(f(x))$ jelölés egy olyan függvényt jelent, amely f-el osztva nullához tart.

Parciális integrálással átalakítva az integrált, azt kapjuk, hogy

$$\pi(x) = \frac{x}{\ln x} + \frac{x}{(\ln x)^2} + \frac{2!x}{(\ln x)^3} + \cdots + \frac{r!x}{(\ln x)^{r+1}} + O\left(\frac{x}{(\ln x)^{r+2}}\right)$$

bármely $r \geq 0$-ra.

A nevezetes Riemann-sejtésből, mely szerint a Riemann-féle ζ függvény nem triviális gyökeinek valós része $1/2$, az következik, hogy

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + O\left(\sqrt{x}\ln x\right).$$

További hivatkozásokat lásd Knuth [24] könyvében, 373–374. o.

Egy sokkal általánosabb kérdést is felvethetünk. Megkérdezhetjük, hány prím van az $a + dn$, $n = 0, 1, 2, \ldots$ számtani sorozatban, amely x-nél kisebb. Természetesen, ha $a \geq 0$ és $d > 1$ legnagyobb közös osztója nagyobb mint egy, akkor legfeljebb 1. Ha azonban nem ez a helyzet, akkor mint *Peter Gustav Lejeune Dirichlet* (1805–1859) bebizonyította 1837-ben, végtelen sok prím van a sorozatban, és megint csak de la Vallée Poussin bebizonyította, hogy a prímek egy rögzített d-re „egyenlően oszlanak el” a különböző a-khoz tartozó sorozatok között.

1.2. Kérdés: ζ gyökei. Megmutatták, hogy a ζ függvény 0 és 32585736.4 közé eső képzetes részű 75 000 000 gyökének a valós része 1/2, és a gyökök egyszeresek. Vajon hogyan? (Lásd Crandall [13] könyvének 2.3 pontját és az ott megadott hivatkozásokat.)

1.3. Kérdés: $\pi(x)$. Hogyan határozhatjuk meg $\pi(x)$ értékét nagy x-re?

1.4. Ikerprímek. Még ha ismerjük is $\pi(x)$ közelítését, ennek a függvénynek a viselkedése távolról sem jól ismert. Néha a függvény egy hosszabb szakaszon nem nő, azaz nagy rés van a prímek között, máskor csak egy páros szám van két prím között, a két prím *ikerprím*. Nagyon régi kérdés, hogy vajon van-e végtelen sok ikerprím? A válasz nem ismert. Érdekes módon, annak ellenére, hogy még ezt sem tudjuk, Hardy és Littlewood híres „Partitio Numerorum” című dolgozatukban az összes $p, p + 2$, $p \leq x$ ikerprímek $\pi_2(x)$-el jelölt számára egy formulát javasoltak. Közelítésük, amely a számítógépes kísérletek szerint nagyon jó,

$$\pi_2(x) \sim 2C_2 \frac{x}{(\ln x)^2}.$$

Itt C_2 az úgynevezett ikerprím konstans, $C_2 = 0.66016\ldots$. Hasonló formulát sejtenek a $p, 2p + 1$, $p \leq x$ Sophie Germain prímek számára.

Hogyan jutott Hardy és Littlewood ehhez a sejtéshez? Durván szólva, a gondolat a következő: A prímszámtétel szerint, annak a „valószínűsége”, hogy egy x-nél nem nagyobb szám prím, durván $1/\ln x$. Ha az ikerprímpár két tagjára független esemény lenne az hogy prímek, akkor ennek valószínűsége $1/(\ln x)^2$ lenne, és így az ikerprímek várható száma $x/(\ln x)^2$ lenne. Azonban, természetesen, ezek az „események” nem függetlenek, például ha p páratlan, akkor $p + 2$ is. Ez a függőség eredményezi a $2C_2$ konstanst. Az alábbiakban egy sokkal általánosabb esetben mutatjuk meg, hogyan kapjuk a konstanst.

1.5. Kérdés: $\pi_2(x)$. Hogyan határozhatjuk meg $\pi_2(x)$ értékét nagy x-ekre?

1.6. Kérdés: $\sum_{p,p+2\in P} 1/p$. Megmutatták, hogy ez a sor konvergens. Hogyan számíthatjuk ki az összeg egy jó közelítését?

1.7. Sejtés [Bateman és Horn, 1962]. *Legyenek $f_1(x), f_2(x), \ldots, f_s(x)$ egész együtthatós irreducibilis polinomok (azaz nem állíthatók elő nem triviális módon két egész együtthatós polinom szorzataként). Jelölje $d_i > 0$ az f_i polinom* *fokát, és tegyük fel, hogy x^{d_i} együtthatója f_i-ben pozitív. Minden $x \geq 0$-ra, jelölje $\pi_{f_1,\dots,f_s}(x)$ azon $1 \leq n \leq x$ egészek számát, amelyekre $f_1(n), f_2(n), \dots, f_s(n)$ prímek. Ekkor*

$$\pi_{f_1,\dots,f_s}(x) \sim C_{f_1,\dots,f_s} \frac{1}{d_1 \cdots d_s} \sum_{2 \leq n \leq x} \frac{1}{(\ln(n))^s},$$

ahol

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

itt $w(p)$ az

$$f_1(z) \cdots f_s(z) \equiv 0 \pmod p$$

kongruencia megoldásainak számát jelöli.

Megmutatható, hogy a végtelen szorzat mindig konvergens, és ha egyik tényezője sem nulla, akkor nem nulla. Az egyszerű gondolat, ami a sejtéshez vezet, a következő: A prímszámtétel szerint annak valószínűsége, hogy egy nagy véletlen n szám prím, $1/\ln(n)$. Így annak valószínűsége, hogy az $f_1(n), \dots, f_s(n)$ számok egyszerre prímek, ha ezek független események lennének,

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

lenne. Azonban az $(f_1(n), \dots, f_s(n))$ vektorok nem véletlenek. A $C_{f_1,\dots,f_s}$ konstans definíciójában, $1 - w(p)/p$ annak az esélye, hogy az $f_1(n), \dots, f_s(n)$ egészek egyike sem osztható p-vel, $(1-1/p)^s$ pedig annak az esélye, hogy egy véletlen s-dimenziós egész koordinátáju vektor egyik kordinátája sem osztható p-vel. Így ésszerű azt feltételezni, hogy annak esélye, hogy az $f_1(n), \dots, f_s(n)$ számok mind prímek,

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

Ebből kapjuk a sejtést, ha a nagy n-re érvényes $\ln f_i(n) \approx d_i \ln n$ közelítést alkalmazzuk.

Az összeget közelíthetjük integrállal is. Például azon, $[a, b[$-beli n-ek $\pi_{f_1,\dots,f_s}(a, b)$ várható száma, amelyekre $f_1(n), \dots, f_s(n)$ egyszerre prímek,

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

Megjegyezzük, hogy $C_{f_1,f_2,\dots,f_s}$ kiszámítása néha visszavezethető a

$$C_s = \prod_{s<p\in\mathbb{P}} \frac{1 - s/p}{(1-1/p)^s},$$

$s = 1, 2, 3, \dots$ konstansok kiszámítására. Nyilván $C_1 = 1$, a C_2 konstans pedig az ikerprím konstans.

1.8. Példa. Tekintsük a legnagyobb ikerprím utáni hajszát. Itt $f_1(x) = (3 + 30x)2^{38880} - 1$ és $f_2(x) = (3 + 30x)2^{38880} + 1$. Ha az $[a, b[= [0, 2^{27}[$ intervallumban tervezünk keresést, hány ikerprímet várhatunk? Ekkor

$$\begin{aligned}\pi_{f_1,f_2}(a,b) &\approx C_{f_1,f_2} \int_0^{2^{27}} \frac{du}{\ln f_1(u) \cdot \ln f_2(u)} \\ &\approx C_{f_1,f_2} \frac{2^{27}}{6} (0{,}1376769251 + 4 \cdot 0{,}1374695060 + 0{,}1374624404) \cdot 10^{-8} \\ &\approx C_{f_1,f_2} \cdot 0{,}1845532660.\end{aligned}$$

Itt

$$C_{f_1,f_2} = \left(1 - \frac{1}{2}\right)^{-2} \cdot \left(1 - \frac{1}{3}\right)^{-2} \cdot \left(1 - \frac{1}{5}\right)^{-2} \prod_{5<p\in\mathbb{P}} \frac{1 - 2/p}{(1 - 1/p)^2} = 20C_2,$$

ahol C_2 az ikerprím konstans. Így $\pi_{f_1,f_2}(0, 2^{27}) \approx 13{,}2032 \cdot 0{,}18455 \approx 2{,}4367$.

1.9. Kérdés. Hogyan ellenőriznénk Bateman és Horn sejtését számítógéppel?

1.10. Eratosztenesz szitája. Ha tömegével akarunk prímeket találni, a legjobb módszer a szitálás. Az alábbi algoritmus megkeresi a $N \geq 3$-nál nem nagyobb páratlan prímeket.

(1) [Inicializálás.] Legyen $n \leftarrow \lfloor (N-1)/2 \rfloor$ és $0 \leq j < n$-re legyen $B[j] = 1$. (Itt B egy bittábla, $B[j] = 1$ azt fogja jelenteni, hogy $2j + 3$ prím.) Legyen $j \leftarrow 0$.

(2) [Következő prím.] Amíg $B[j] = 0$, legyen $j \leftarrow j + 1$.

(3) [Túl nagy?] $i \leftarrow 2j^2 + 6j + 3$. (Ez az első kiszitálandó szám indexe.) Ha $i \geq n$, akkor menjünk (5)-re.

(4) [Szita.] Legyen $B[i] \leftarrow 0$ majd $i \leftarrow i + 2j + 3$. Ha $i \geq n$, legyen $j \leftarrow j + 1$ és menjünk (2)-re, egyébként ismételjük meg (4)-et.

(5) [Eredmény.] $0 \leq j < n$-re, ha $B[j] = 1$, akkor $2j + 3$ prím.

Annak, hogy a p prímmel való szitálást p^2-től kezdjük, nincs nagy jelentősége, mert a szitálási munka zöme a kis prímekre esik.

1.11. Feladat. Irjunk programot Erathoszthenesz szitájára.

Hasonlóan szitálhatunk egy $a + dx$, $x = 0, 1, \ldots$ számtani sorozatban. Nyilván csak azokkal a p prímekkel kell szitálnunk, amelyekre $p \nmid d$. A gyakorlatban d mindig páros, a pedig páratlan. Az első probléma az legkisebb olyan $x \geq 0$ meghatározása, amelyre $p \mid a+dx$, azaz $x = -a/d \bmod p$. Ez a (kiterjesztett) euklidészi algoritmussal oldható meg.

1.12. Moduláris inverz euklidészi algoritmussal. Adott $0 \leq a < m$ egészekhez meghatározza az a és m legnagyobb közös osztóját, d-t, és egy olyan $0 \leq x < m$ számot, amelyre $ax - d$ többszöröse m-nek. Az algoritmus során végig $ax_i - d_i$ többszöröse m-nek, $i = 1, 2, 3$.

(1) [Inicializálás.] Legyen $x_1 \leftarrow 1$, $d_1 \leftarrow a$, $x_2 \leftarrow 0$, $d_2 \leftarrow m$.

(2) [Vége?] Ha $d_2 = 0$, készen vagyunk, az eredmény $x_1 \bmod m$ és d_1.

(3) [Osztás, kivonás.] Legyen $q \leftarrow \lfloor d_1/d_2 \rfloor$, $d_3 \leftarrow d_1 - qd_2$, $x_3 \leftarrow x_1 - qx_2$, és ezután legyen $(x_1, d_1) \leftarrow (x_2, d_2)$, $(x_2, d_2) \leftarrow (x_3, d_3)$. Térjünk vissza a (2) lépésre.

Az algoritmust most nem vizsgáljuk, csak annyit jegyzünk meg, hogy q gyakran kicsi, és így az osztás esetleg eltolásokkal és kivonásokkal is megoldható. Belátható, hogy az x_i-k előjele minden lépésben ellenkezőjére változik, így ha a lépéseket számoljuk, nemnegatív egészekkel is dolgozhatunk. Az is belátható, hogy $|x_1| < m$ marad. (Lásd Knuth [könyvét.)

1.13. Feladat. Irjunk egy Maple demo programot a moduláris inverz számolására euklidészi algoritmussal.

1.14. Moduláris inverz bináris lnko algoritmussal. A bináris lnko algoritmus ötlete, hogy amíg a két természetes szám páros, 2-t kiemelhetünk belőlük, majd amíg az egyik páros és nem nulla, a másik páratlan, a párost oszthatjuk 2-vel. Ha már mindkét szám páratlan, akkor kivonjuk a nagyobbikból a kisebbet: a különbség páros lesz, stb. Az alábbi, erre az ötletre épülő algoritmus adott $m > 2$ páratlan modulus és $0 \leq a < m$ esetén meghatározza az a és m számok d legnagyobb közös osztóját és egy olyan $0 \leq x < m$ számot, amelyre $ax - d$ osztható m-el. Az algoritmus során végig $ax_i - d_i$ osztható m-el.

(1) [Inicializálás.] Legyen $x_1 \leftarrow 1$, $d_1 \leftarrow a$, $x_2 \leftarrow m$, $d_2 \leftarrow m$. Ha a páratlan, legyen $x_3 \leftarrow 0$, $d_3 \leftarrow -m$, és menjünk (4)-re. Egyébként legyen $x_3 \leftarrow 1$ és $d_3 \leftarrow a$.

(2) [d_3 felezése.] Ha x_3 páros, legyen $x_3 \leftarrow x_3/2$ és $d_3 \leftarrow d_3/2$; egyébként legyen $x_3 \leftarrow (x_3 + m)/2$ és $d_3 \leftarrow d_3/2$.

(3) [d_3 páros?] Ha d_3 páros, menjünk vissza (2)-re.

(4) [$\max(d_1, d_2)$ módosítása.] Ha d_3 pozitív, legyen $x_1 \leftarrow x_3$ és $d_1 \leftarrow d_3$, egyébként legyen $x_2 \leftarrow m - x_3$ és $d_2 \leftarrow -d_3$.

(5) [Kivonás.] Legyen $x_3 \leftarrow x_1 - x_2$ és $d_3 \leftarrow d_1 - d_2$. Ha most $x_3 < 0$, legyen $x_3 \leftarrow x_3 + m$. Ha $d_3 \neq 0$, menjünk vissza (2)-re. Egyébként az algoritmus véget ér, az eredmény x_1 és d_1.

Itt is megoldható, hogy csak nemnegatív számokkal számoljunk.

1.15. Feladat. Irjunk egy Maple demo programot moduláris inverz számolására bináris algoritmussal.

1.16. Általános szita. Mint a Bateman–Horn sejtésnél, az $f_1, f_2, \ldots, f_s$ polinomok adottak. Az alábbi algoritmus a $0 \leq x < n$ számokból csak azokat hagyja meg, amelyekre egyik $f_i(x)$-nek sincs prímosztója a $P[j]$, $0 \leq j < m$ prímsorozatban.

(1) [Inicializálás.] Legyen $0 \leq j < n$-re $B[j] = 1$. Itt B egy bittábla, $B[x] = 1$ azt fogja jelenteni, hogy $f_1(x), \ldots, f_s(x)$-nek nincs prímosztója az adott prímek között. Jelölje $w(p)$ az $f_1(z) \cdots f_s(z) \equiv 0 \pmod p$ egyenlet gyökeinek számát. Ha $0 \leq j < m$, legyen $W[j] \leftarrow w(P[j])$ és $R[j,i] \leftarrow r_i$ ha $0 \leq r_i < P[j]$ az egyenlet i-edik gyöke moduló $P[j]$. Itt $0 \leq i < w(P[j])$. Legyen $j \leftarrow 0$.

(2) [Vége?] Ha $j \geq m$, készen vagyunk. Az eredményt a B tábla reprezentálja. Egyébként $p \leftarrow P[j]$, $w \leftarrow W[j]$ és $i \leftarrow 0$.

(3) [Kész egy prím?] Ha $i \geq w$, akkor legyen $j \leftarrow j+1$ és menjünk (2)-re. Egyébként $k \leftarrow R[j,i]$.

(4) [Túl nagy?] Ha $k \geq n$, akkor menjünk (6)-ra.

(5) [Szita.] Legyen $B[k] \leftarrow 0$ majd $k \leftarrow k + p$, és menjünk (4)-re.

(6) [Következő.] Legyen $i \leftarrow i + 1$ és menjünk (3)-ra.

Természetesen, ha $w(p)$ konstans, vagy könnyen számolható, akkor felesleges nyilvántartani. A $w(p)$ átlagértéke s. Rendszerint vagy a P, W és R, vagy a B tábla nem fér be az operatív tárba. Az első esetben a P tábla következő részletének előállítása után egy új W és R táblát inicializálva, folytatjuk a szitálást. A második esetben rendszerint érdemes a (3) lépésben egy $R[j, i-1] \leftarrow k - n$ utasítással visszaírni az R táblába. A B tábla kivitele után B-t újra inicializáljuk, és R már készen áll a következő szitára.

Tegyük fel, hogy a fenti két eset valamelyike áll fenn, a $0 \leq x < N$ értékekre szitálunk, olyan p prímekkel, amelyek nem nagyobbak, mint M, a polinomok pedig rögzítettek. Az R tábla vagy táblák inicializálásához $\approx C_1 M$ idő szükséges, ha lineárisak a polinomok. (Az általános esetet csak később tudjuk vizsgálni.) A P, W és R táblák olvasásához és az R tábla írásához$\approx C_2(N/n)M/\lg M$ idő szükséges. Végül maga a szitálás $\approx C_3 N \sum_{p \in \mathbb{P}, p \leq M} 1/p$ időt igényel. Mivel az M-nél nem nagyobb prímek reciprokainak összege $\approx C + \ln\ln M$, az $]A, B]$ intervallumba eső prímekkel történő szitálás időigénye $\approx C_3 N \ln(\ln B / \ln A)$.

1.17. Programozási problémák. Csak a szitálás időigényét vizsgálva, tekintsünk egy példát. Ha 2^{20} prímmel akarunk szitálni, akkor a legnagyobb prím kb. 14 000 000 lesz. Ezek közül a 2^{10}-edik kb. 7 000. Egyszerű szitálásnál a 3 és $2^6 = 64$ közötti, a 64 és 7 000 közötti, és a többi prímre jutó munka aránya kb. $1,33 : 0,76 : 0,62$. Lényeges sebességnövekedést érhetünk tehát el, ha a kis prímekkel való szitálást a tábla inicializálásával együtt, regiszterekben végezzük. A közepes prímekkel való szitálás is gyorsítható, ha úgy szervezzük, hogy a gyorsítótár (chache) kihasználása jó legyen. Egy konkrét esetben kb. 2, 5-szeres gyorsítást lehetett így elérni.

1.18. A szitálás dúsító hatása. Ugyanaz a heurisztika, amit Bateman és Horn sejtésénél használtunk, azt sugallja, hogy ha az összes $A \leq p < B$ prímmel szitálunk, akkor egy

$$q^{A,B}_{f_1,\ldots,f_s} = \prod_{A \leq p < B, p \in \mathbb{P}} 1 - \frac{w(p)}{p}$$

faktorszor kevesebb szám marad. Ez a faktor gyakran redukálható az

$$q_s^{A,B} = \prod_{A \le p < B, p \in \mathbb{P}} 1 - \frac{s}{p}$$

faktorra. Ez utóbbinál, ha A, B nagyok, akkor az $(\ln A / \ln B)^s$ közelítés használható.

1.19. Példa. Tekintsük ismét az ikerprímkeresést. Minden prímmel szitálva 7-től $44\,000 \cdot 2^{25}$-ig, az eredeti 2^{27} számból csak egy

$$\begin{aligned} q_{f_1,f_2}^{7,44\,000 \cdot 2^{25}} &= \prod_{7 \le p < 44\,000 \cdot 2^{25}, p \in \mathbb{P}} 1 - \frac{2}{p} = q_2^{7,44\,000 \cdot 2^{25}} \\ &\approx q_2^{7,1\,000\,000} \left(\frac{\ln 1\,000\,000}{\ln 44\,000 \cdot 2^{25}} \right)^2 \\ &\approx 0,021\,804\,674 \cdot 0,243\,096\,25 \approx 0,005\,300\,634 \end{aligned}$$

faktorszor kevesebb, $\approx 711\,439$ marad. Ezzel a szitálás előtti $\approx 2.4367/2^{27} \approx 1,815\,482\,974 \cdot 10^{-8}$ „ikerprím sűrűség” $\approx 188,656\,665\,36$-szeresre, $\approx 3,425\,029\,425 \cdot 10^{-6}$-ra nőtt. Összesen 55 440 számot teszteltünk, így $\approx 55\,440 \cdot 3,425\,029\,425 \cdot 10^{-6} \approx 0,1899$ ikerprímet várhattunk.

Tulajdonképpen három szitálás történt. Az első szita egy kis prímtáblát állított elő. A második ezekkel a prímekkel szitálva, sok részletben, előállított minden prímet $44\,000 \cdot 2^{25}$-ig. Ezekkel történt az ikerprímjelöltek szitálása.

1.20. Kérdés. Mekkorák a rések a prímek között?

1.21. Kérdés. Hogyan érdemes tárolni egy prímtáblát?

1.22. Kérdés. Mi jobb: tárolni a prímeket és beolvasni, vagy szitálással előállítani?

1.23. Kérdés. A Goldbach-sejtés szerint minden kettőnél nagyobb páros szám előáll két prímszám összegeként. Hogyan ellenőriznénk ezt minden $n \le x$ páros számra?

1.24. Kérdés. Milyen hosszú számtani sorozatokat tudunk a prímszámok között találni?

1.25. Kérdés. Hogyan szerveznénk egy általános szitaprogramot?

2. Egyszerű faktorizálási módszerek

2.1. Próbaosztás. A legegyszerűbb faktorizálási módszer a próbaosztás. Az alábbi algoritmus adott N egészhez megkeresi N-nek a $p_1 \le p_2 \le p_3 \le \ldots \le p_t$ prímtényezőit. Az algoritmushoz szükség van a $2 = d_0 < d_1 < d_2 < \ldots$ próbaosztók sorozatára, amelynek minden $\le \sqrt{N}$ prímszámot tartalmaznia kell, és legalább egy $d_k \ge \sqrt{N}$ értéket is.

(1) [Inicializálás.] Legyen $t \leftarrow 0$, $k \leftarrow 0$, $n \leftarrow N$. Az algoritmus során $n = N/(p_1 p_2 \cdots p_t)$ és n-nek nincsen d_k-nál kisebb prímosztója.

(2) [$n = 1$?] Ha $n = 1$, az algoritmus véget ér.

(3) [Osztás.] Legyen $q \leftarrow \lfloor n/d_k \rfloor$, $r \leftarrow n \bmod d_k$.

(4) [Nulla maradék?] Ha $r \ne 0$, menjünk (6)-ra.

(5) [Osztót találtunk.] $t \leftarrow t+1$, majd $p_t \leftarrow d_k$, $n \leftarrow q$. Térjünk vissza (2)-re.

(6) [Kicsi a hányados?] Ha $q > d_k$, akkor $k \leftarrow k+1$ és menjünk vissza (3)-ra.

(7) [n prím.] $t \leftarrow t+1$ majd $p_t \leftarrow n$, és vége az algoritmusnak.

Ha elfogadjuk a $p_0 = 1$ konvenciót, az algoritmus futásideje $O(\max(p_{t-1}, \sqrt{p_t})$. Szokás a próbaosztók sorozatát a $2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, \ldots$ sorozatnak választani. Az algoritmus futásidejének vizsgálatához a legnagyobb és a második legnagyobb prímosztó eloszlását kell megvizsgálni.

2.2. Feladat. Irjunk programot a próbaosztásra.

2.3. Feladat. Hogyan működik a Maple 'ifactor' eljárása 'easy' opcióval?

2.4. A prímosztók eloszlásáról. Vizsgáljuk annak valószínűséget, hogy egy 1 és x közötti véletlen egész legnagyobb prímosztója $\le x^\alpha$. Ha feltesszük, hogy $x \to \infty$ esetén ez a valószínűség egy $F(\alpha)$ határeloszláshoz tart, akkor F-et az alábbi függvényegyenletből határozhatjuk meg:

$$F(\alpha) = \int_0^\alpha F\left(\frac{t}{1-t}\right)\frac{dt}{t}, \qquad \text{ha } 0 \le \alpha \le 1;\ F(\alpha) = 1, \text{ ha } \alpha \ge 1.$$

A heurisztika, amely a fügvényegyenlethez vezet, a következő: Adott $0 < t < 1$-re, azoknak az x egészeknek a száma, amelyek legnagyobb prímosztója x^t és x^{t+dt} közé esik, $xF'(t)\,dt$. A prímek száma ebben a tartományban $\pi(x^{t+dt}) - \pi(x^t) \approx \pi(x^t + (\ln x)x^t\,dt) - \pi(x^t) \approx x^t\,dt/t$. Minden ilyen p-re azoknak az n-eknek a száma, amelyekre $np \le x$ és n legnagyobb prímosztója $\le p$ nem más, mint azon $n \le x^{1-t}$ értékeknek a száma, amelyeknek a legnagyobb prímosztója $\le (x^{1-t})^{t/(1-t)}$, vagyis $x^{1-t}F(t/(1-t))$. Így $xF'(t)\,dt = (x^t\,dt/t)\cdot(x^{1-t}F(t/(1-t)))$, és innen integrálással adódik a függvényegyenlet.

Az egyenletet a számolásra alkalmasabb

$$F(\alpha) = 1 - \int_\alpha^1 F\left(\frac{t}{1-t}\right)\frac{dt}{t}, \qquad \text{ha } 0 \le \alpha \le 1$$

alakra hozhatjuk, ha figyelembe vesszük, hogy $F(1) = 1$.

Hasonlóan, ha annak $G(\alpha)$ valószínűségét vizsgáljuk, hogy egy 1 és x közötti véletlen egész második legnagyobb prímosztója $\le x^\alpha$, a

$$G(\alpha) = \int_0^\alpha \left(G\left(\frac{t}{1-t}\right) - F\left(\frac{t}{1-t}\right)\right) \frac{dt}{t} \qquad \text{ha } 0 \le \alpha \le 1/2$$

függvényegyenletet kapjuk, és $G(\alpha) = 1$ ha $\alpha \ge 1/2$. Valóban, annak valószínűsége, hogy az 1 és x közötti véletlen egész legnagyobb prímosztója $> x^\alpha$, második legnagyobb prímosztója pedig $\le x^\alpha$, $(G(\alpha) - F(\alpha))$. Most számoljuk össze azon $\le x$ egészeket amelyekre a második legnagyobb prímosztó x^t és x^{t+dt} közé esik. Ezek száma egyrészt $xG'(t)\,dt$. Másrészt, minden x^t és x^{t+dt} közötti p prímre, azon n-ek száma, amelyekre $np \le x$ és n legnagyobb prímosztója $> x^t$, második legnagyobb prímosztója pedig $\le x^{t+dt}$, $x^{1-t}(G(t/(1-t)) - F(t/(1-t)))$. Emiatt

$$xG'(t)\,dt = (\pi(x^{t+dt}) - \pi(x^t)) \cdot x^{1-t}(G(t/(1-t)) - F(t/(1-t))),$$

amiből kapjuk a függvényegyenletet.

Itt is az egyenletet számolásra alkalmasabb

$$G(\alpha) = 1 - \int_\alpha^{1/2} \left(G\left(\frac{t}{1-t}\right) - F\left(\frac{t}{1-t}\right)\right) \frac{dt}{t} \qquad \text{ha } \alpha \le 1/2$$

alakra hozhatjuk, ha figyelembe vesszük, hogy $G(1/2) = 1$.

A hivatkozásokat illetően lásd Knuth [24] könyvének 4.5.4 pontját.

2.5. A prímosztók számának határeloszlása. A valószínűségi számelméletben vizsgálták a prímosztók t számának határeloszlását is. Nyilván az n egész prímosztóinak száma 1 és $\lg n$ között van, de ezeket a határokat ritkán éri el. Megmutatható, hogy ha n-et véletlenszerűen választjuk 1 és x között, akkor bármely rögzített c-re annak valószínűsége, hogy $t \le \ln\ln x + c\sqrt{\ln\ln x}$, az

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^c e^{u^2/2}\,du$$

értékhez tart, ha $x \to \infty$. Azaz t határeloszlása normális $\ln\ln x$ várható értékkel és szórásnégyzettel. A hivatkozásokat illetően lásd Knuth [24] könyvének 4.5.4 pontját.

2.6. Fermat módszere. Fermat észrevette, hogy elég egy olyan $0 \le y < x \le n$ párt találni, amelyre $n = x^2 - y^2$, mert ekkor $n = (x-y)(x+y)$. Ha $n > 1$ páratlan és összetett, mindig vannak ilyen egészek, és $x = \lceil\sqrt{n}\rceil$-szel és $y = 0$-val indulva, és szükség szerint x-et illetve y-t növelve, meg is találhatók. Fermat az $x = \lceil\sqrt{n}\rceil$ kezdőértékkel kezdve, minden x-re kiszámította $x^2 - n$ értékét. Rápillantott a két utolsó jegyre, és abból állapította meg, hogy lehet-e négyzetszám: négyzetszámok két utolsó jegye 00, $e1$, $e4$, 25, $o6$ vagy $e9$ lehet, ahol e páros, o páratlan jegy. E helyett különböző modulusokra kiszámolhatjuk $x^2 - n$ maradékát, hogy lehet-e négyzetszám maradéka. Mivel adott n-re ez csak x maradékától függ, az alábbi algoritmust kapjuk, amely adott n páratlan számhoz meghatározza az n legnagyobb olyan osztóját, amely kisebb vagy egyenlő $\sqrt{n}$. Az eljárás olyan $m_1, m_2, \ldots, m_r$ modulusokat használ, amelyek páronként relatív prímek, és n-hez is relatív prímek. Feltesszük, hogy elkészült r darab $S[i,j]$, szitatáblázat, ahol $0 \leq j < m_i$, $1 \leq i \leq r$ és $S[i,j] = 1$ ha van olyan y, amelyre $j^2 - n \equiv y^2 \pmod{m_i}$, egyébként nulla.

(1) [Inicializálás.] Legyen $x \leftarrow \lceil\sqrt{n}\rceil$ és legyen $k_i \leftarrow (-x) \bmod m_i$, $1 \leq i \leq r$. (Az algoritmus során a k_i változóra mindig $k_i = (-x) \bmod m_i$ teljesül.)

(2) [Szitálás.] Ha $S[i, k_i] = 1$ minden $1 \leq i \leq r$-re, akkor menjünk (4)-re.

(3) [x léptetése.] Legyen $x \leftarrow x + 1$, és legyen $k_i \leftarrow (k_i - 1) \bmod m_i$, $1 \leq i \leq r$. Menjünk vissza (2)-re.

(4) [$x^2 - n$ ellenőrzése.] Legyen $y \leftarrow \lfloor\sqrt{x^2 - n}\rfloor$. Ha $y^2 = x^2 - n$, akkor $x - y$ a keresett osztó, és az algoritmus véget ér. Egyébként menjünk vissza (3)-ra.

Az eljárás bitműveletekkel gyorsítható, de még így sem elég gyors. Alapgondolata azonban sok mai eljárásban felbukkan. A módszerrel már 1965-ben 1 000 000 próba másodpercenkénti sebességet értek el. Mechanikus (fogaskerék, biciklilánc, stb.) és elektronikus (késleltetővonalas, shift regiszteres, stb.) gépeket szerkesztettek szitálásra.

2.7. Feladat. Irjunk programot, amely csak összeadással és kivonással faktorizál.

2.8. Feladat. Irjunk programot Fermat módszerére.

2.9. Pollard ϱ módszere. Legyen f tetszőleges egész együtthatós polinom, és tekintsük az $x_{m+1} = f(x_m)$ iterációt valamilyen x_0 kezdőértékkel. Ha n egy pozitív egész szám, könnyen kiszámíthatjuk az $x_m \bmod n$ értékeket. A sorozat előbb-utóbb ciklikus lesz. Ha p az n egy prímfaktora, és $x_m \bmod p$-t tekintjük, akkor várhatóan sokkal hamarabb lesz ciklikus. Ezt használjuk fel faktorizálásra: ha ez utóbbi ciklus hossza t, akkor $x_{m+t} - x_m \bmod p = 0$, de nagy valószínűséggel $x_{m+t} - x_m \bmod n \neq 0$, azaz $x_{m+t} - x_m \bmod n$ faktorai között megjelenik p, és lnko-számítással onnan kinyerhető. Nem tudjuk, mennyi t, de rendre kiszámoljuk n és

$$x_1 - x_0, x_2 - x_1, x_3 - x_1, x_4 - x_3, x_5 - x_3, x_6 - x_3, x_7 - x_3, x_8 - x_7, x_9 - x_7, \ldots$$

legnagyobb közös osztóját.

A gyakorlatban az $f(x) = x^2 + c$ polinomokat használjuk $x_0 = 1$ kezdőértékkel, a $c \geq 1$ egész szabadon választható paraméter.

(1) [Inicializálás.] Legyen $x \leftarrow 1 + c \bmod n$, $x' \leftarrow 1$, $k \leftarrow 1$, $l \leftarrow 1$. Az algoritmus során x és x' az $x_{2l-k} \bmod n$ illetve az $x_{l-1} \bmod n$ mennyiségeket jelölik.

(2) [Osztót találtunk?] Legyen $d \leftarrow \mathrm{lnko}(x' - x, n)$. Ha $d = 1$, menjünk (3)-ra. Egyébként az algoritmus véget ér, eredménye d. (Lehet, hogy $d = n$, ekkor az algoritmus sikertelen.)

(3) [Továbblépés.] Legyen $k \leftarrow k-1$. Ha $k=0$, legyen $x' \leftarrow x$, $k \leftarrow l$, $l \leftarrow 2l$. Legyen $x \leftarrow x^2 + c \bmod n$, és menjünk vissza (2)-re.

Az algoritmus futásideje heurisztikusan $\sqrt{p_1}$ nagyságrendű. Ha az lnko művelet lassú, akkor megtehetjük, hogy mondjuk s darab $x' - x$ különbség szorzatát összegyűjtjük moduló n, és csak a szorzat és n lnko-ját számoljuk ki. Ezzel majdnem semmit sem vesztünk, ha s nem túl nagy. Ha még ennyit sem szeretünk veszíteni, vagy s-et szeretnénk nagyra választani, akkor ha a legnagyobb közös osztó n, használjunk visszalépést. Megmutatható az is, hogy kihagyhatjuk a (2) lépés, ha $k > l/2$.

2.10. Feladat. Irjunk programot Pollard ϱ módszerére.

2.11. Fermat tétele. *Ha p prím, és $\mathrm{lnko}(a,p) = 1$, akkor $a^{p-1} \bmod p = 1$.*

A tétel egy sokkal általánosabb tétel speciális esete. Jelölje $\phi(m)$az m pozitív egészre azon 0 és m közötti egészek számát, amelyek relatív prímek m-hez: ϕ az *Euler-függvény.*

2.12. Euler tétele. *Ha $\mathrm{lnko}(a,m) = 1$, akkor $a^{\phi(m)} \bmod m = 1$.*

Bizonyítás. Legyen a_i, $i = 1, \dots \phi(m)$ egy redukált maradékrendszer. Ekkor aa_i, $i = 1, \dots \phi(m)$ is egy redukált maradékrendszer. Innen

$$\prod_i (aa_i) \equiv \prod_i a_i \pmod{m},$$

és kapjuk a tételt, mivel a jobb oldalon álló szorzat relatív prím m-hez.

2.13. Kínai maradéktétel. *Ha $n, m > 0$ relatív prímek, akkor $0 \le a < n$, $0 \le b < m$ esetén egyetlen olyan $0 \le c < nm$ létezik, amelyre $c \bmod n = a$ és $c \bmod m = b$.*

Bizonyítás. Legfeljebb egy ilyen c létezhet, mert bármely kettő különbsége osztható lenne nm-el. Az euklideszi algoritmus segítségével kaphatunk olyan $0 \le x < m$ és $0 \le y < n$ számokat, amelyekre $nx - my = 1$. Legyen $c = nxb - mya \bmod nm$.

2.14. Feladat. Általánosítsuk a kínai maradéktételt több modulus esetére.

2.15. Tétel. *Az Euler-féle φ függvény multiplikatív, azaz ha $n, m > 0$ relatív prímek, akkor $\varphi(nm) = \varphi(n)\varphi(m)$.*

Bizonyítás. A kínai maradéktételből következik.

2.16. Gyors hatványozás. A balról-jobbra bináris módszerrel a^e-t $O(\lg e)$ szorzással számolhatjuk ki ($e \in \mathbb{N}^+$). Az általánosabb 2^m alapú módszert adjuk meg. Tetszőleges félcsoportban használható. Jelölje $b_i(x)$ az 2^i együtthatóját x bináris kifejtésében.

(1) [Inicializálás.] Legyen $n \leftarrow \lfloor \lg(e) \rfloor - 1$ és $P[i] \leftarrow a^{2i+1}$, ha $0 \le i < 2^{m-1}$. Legyen $x \leftarrow a$.

(2) [Vége?] Ha $n < 0$, az eljárás véget ért, az eredmény x.

(3) [Nulla bit?] Ha $b_n(e) = 0$, legyen $x \leftarrow x^2$, $n \leftarrow n - 1$, és menjünk (2)-re.

(4) [Egyest találtunk.] Legyen $i \leftarrow 0$, $j \leftarrow 1$, $k \leftarrow 0$, $x \leftarrow x^2$ és $n \leftarrow n - 1$. (Itt i azt mutatja, hogy $P[i]$-vel kell majd szoroznunk, j, hogy milyen hosszú bitsorozatot találtunk, amely 1-el kezdődik és 1-re végződik, k pedig, hogy ez után hány nulla bit áll.)

(5) [Elég bit?] Ha $n < 0$, vagy $k + j = m$, menjünk (10)-re.

(6) [Nulla bit?] Ha $b_n(e) = 0$, legyen $k \leftarrow k + 1$, $n \leftarrow n - 1$ és menjünk (5)-re.

(7) [Egyes bit.] Legyen $k \leftarrow k + 1$ majd $j \leftarrow k + j$ és $i \leftarrow (2i + 1)2^{k-1}$.

(8) [Elmaradt négyzetreemelések.] Amíg $k > 0$ legyen $x \leftarrow x^2$ és $k \leftarrow k - 1$.

(9) [Vissza.] Legyen $n \leftarrow n - 1$, és menjünk (5)-re.

(10) [Elég bit.] Legyen $x \leftarrow xP[i]$.

(11) [Elmaradt négyzetreemelések.] Amíg $k > 0$ legyen $x \leftarrow x^2$ és $k \leftarrow k - 1$.

(12) [Főciklus vége.] Menjünk (2)-re.

Az eljárás az átlagos esetekre közel optimális számú szorzást (ideértve a négyzetreemeléseket is) használ, ha $m \approx \lg\lg e - 2\lg\lg\lg e$. Speciális esetekre kevesebb művelet is elég lehet. A gyakorlatban m-et jóval kisebbre választjuk, mivel 2^{m-1} méretű táblát kell tárolnunk.

2.17. Feladat. Irjunk programot hatványozásra.

2.18. Pollard $p - 1$ módszere. Az alapgondolat a következő: Tegyük fel, hogy az n összetett szám valamelyik p prímfaktorára $p - 1$ „sima”, azaz csupa kis prímtényezői vannak. Ekkor egy nem túl nagy k-ra $p - 1 | k!$. Valamely $1 < a < n$ alapra, amely relatív prím n-hez, $a^{k!} - 1$ osztható p-vel, de remélhetjük, hogy n-el nem. Így egy lnko művelettel p kinyerhető. A $k!$-nál valamivel kisebb kitevő is elegendő.

Az alábbi algoritmus egy $P[i]$, $0 \leq i < m$ táblát használ, amely egy szigorúan monoton növekedő, 1-nél nagyobb természetes számokból álló sorozatot tartalmaz. Nagy valószínűséggel megtalálja az n szám egy p prím faktorát, amelyre $p - 1$ minden prímtényezője benne van a táblában, és egyetlen prímhatvány tényezője sem nagyobb, mint a B korlát. Az $1 < a < n$ alapot használja.

(1) [Inicializálás.] Legyen $i \leftarrow 0$ és $b \leftarrow \lg B$.

(2) [Kész?] Ha $i \geq m$ vagy $\mathrm{lnko}(a - 1, n) > 1$, készen vagyunk, az eredmény $\mathrm{lnko}(a - 1, n)$.

(3) [Következő prím.] Legyen $p \leftarrow P[i]$, $e \leftarrow \lfloor b/\lg p \rfloor$, majd $q \leftarrow p^e$, $i \leftarrow i + 1$.

(4) [Hatványozás.] Legyen $a \leftarrow a^q \bmod n$, és menjünk (2)-re.

2.19. Feladat. Irjunk programot Pollard $p - 1$ módszerére.

2.20. Pollard $p-1$ módszere, második lépcső. Ha az előző algoritmusban nem csak lnko$(a-1,n)$-et, hanem a-t is visszaadjuk, folytathatjuk az eljárást a $P[i]$, $m \le i < M$ részére a táblázatnak. Feltesszük, hogy a keresett p prímfaktorra $p-1$ prímtényezői között csak egy szerepel a táblázat ezen részéből, és első hatványon. Feltehetjük, hogy a $P[i]$, $m \le i < M$ számok mind páratlanok. Az algoritmus a következő:

(1) [Inicializálás.] Legyen $i \leftarrow m+1$ és $x \leftarrow a^{P[m]} \bmod n$. Legyen minden $1 \le j \le N$-re $E[j] \leftarrow a^{2j} \bmod n$.

(2) [Kész?] Ha $i \ge M$ vagy lnko$(x-1,n) > 1$, készen vagyunk, az eredmény lnko$(x-1,n)$.

(3) [Következő differencia.] Legyen $d \leftarrow P[i]-P[i-1]$.

(4) [Megvan?] Ha $d/2 \le N$, legyen $x \leftarrow xE[d/2]$, $i \leftarrow i+1$, és menjünk (2)-re.

(5) [Nincs meg.] Legyen $x \leftarrow xa^d$, $i \leftarrow i+1$, és menjünk (2)-re.

Ennek a módszernek egy lehetséges másik változata a következő: Válasszunk egy S „sima” számot, amely $< P[m]$, és tekintsük a modulo S vett legkisebb pozitív $r_1, r_2, \dots, r_s$ redukált maradékokat. A $\prod_{j=1}^{s}(x-a^{-r_j}) \bmod n$ polinom a^{iS} helyen vett helyettesítési értéke, ahol a az első lépcső kimenete, rendre minden olyan p prímmel osztható, amelyre $p-1$-nek egy prímfaktora van iS és $(i+1)S$ között, a többi pedig kisebb mint $P[m]$ (és nem túl sokszor szerepel). Így egy lnko művelettel van remény, hogy p-t megkapjuk. Az eljárást megismételve $i = 1, 2, \dots, \lfloor P[M]/S \rfloor$-re, a második lépcső egy újabb változatát kapjuk. Ez akkor gazdaságos, ha a polinom helyettesítési értékeit *egyszerre* tudjuk kiszámolni, ami Fourier-transzformációval lehetséges. Később erre még visszatérünk. A második lépcső más gyorsításai is ismeretesek, lásd Crandall [13] könyvét, 3. fejezet, és az ott található hivatkozásokat.

2.21. Feladat. Irjunk programot Pollard $p-1$ módszerének második lépcsőjére.

3. Egyszerű prímtesztelési módszerek

Egy jól ismert kritérium arra, hogy egy szám prím legyen, *Wilson tétele:* n akkor és csak akkor prím, ha $n \mid 1+(n-1)!$. Sajnos, ez a kritérium a gyakorlatban teljesen használhatatlan, mert a faktoriális függvény nem számítható elég gyorsan.

3.1. Kérdés. A p prímet *Wilson-prím*nek nevezzük, ha nem csak $p|1+(p-1)!$ de $p^2|1+(p-1)!$. Hány Wilson prím van?

3.2. Feladat. Irjunk egy egyszerű programot Wilson-prímek keresésére. ($12 \cdot 10^6$-ig csak három Wilson-prím van.)

3.3. Probléma. Irjunk egy hatékony programot Wilson-prímek keresésére. Vegyük figyelembe a Crandall [13] könyvben leírtakat.

Nézzük a legegyszerűbb *használható* prímtesztelési módszert.

3.4. Fermat-teszt. Fermat tétele a következő tesztet adja: ha $1 < a < m$ és $a^{m-1} \bmod m \neq 1$, akkor m összetett. Bár a teszt elég jól működik, még akkor is, ha csak egyszer, mondjuk a 3 alappal próbáljuk ki, ma már alig használjuk, mert ugyanilyen gyors, de még jobb teszt is van. A Fermat-teszttel nem tudjuk bebizonyítani, hogy m prím. Például, $(2^{28} - 9)/7$ összetett, de átmegy a teszten az $a = 3$ alappal. Egy m összetett számot, amely átmegy a teszten az a alappal, szokás *az a alapra nézve álprím*nek nevezni. Még olyan összetett számok, úgynevezett *Carmichel-szám*ok is vannak, amelyek minden olyan alapra nézve álprímek, amely relatív prím hozzájuk. A legkisebb ilyen szám 561.

3.5. Feladat. Irjunk programot a Fermat-tesztre. Az alap legyen bemenő paraméter.

3.6. Feladat. Irjunk programot, amely egy vagy több adott alaphoz álprímeket keres.

3.7. Feladat. Irjunk programot, amely Carmichael-számokat keres.

3.8. Lemma. *Ha n egy pozitív egész szám, akkor $n = \sum_{d|n} \phi(d)$.*

Bizonyítás. Vegyük észre, hogy egy $1 \leq x \leq d$ egész képe pontosan akkor generálja $\mathbb{Z}/d\mathbb{Z}$-t, ha relatív prím d-hez. Ha d osztja n-et, akkor legyen C_d az egyetlen d rendű részcsoportja $\mathbb{Z}/n\mathbb{Z}$-nek, és legyen Φ_d a C_d generátorainak halmaza. Mivel $\mathbb{Z}/n\mathbb{Z}$ minden eleme valamelyik C_d-t generálja, a $\mathbb{Z}/n\mathbb{Z}$ csoport diszjunkt uniója a Φ_d halmazoknak, és így

$$n = \mathrm{card}(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \mathrm{card}(\Phi_d) = \sum_{d|n} \phi(d).$$

3.9. Lemma. *Legyen H egy véges csoport, a rendje legyen n. Tegyük fel, hogy minden d osztójára n-nek, azon $x \in H$-k halmaza, amelyekre $x^d = 1$, legfeljebb d elemű. Ekkor H ciklikus.*

Bizonyítás. Legyen d egy osztója n-nek. Ha van $x \in H$, amelynek a rendje d, az x által generált $(x) = \{1, x, \ldots, x^{d-1}\}$ részcsoport ciklikus d renddel; a feltevésünk szerint minden $y \in H$ amelyre $y^d = 1$, az (x) részcsoportban van. Speciálisan, minden d rendű eleme H-nak generátora (x)-nek, és $\phi(d)$ ilyen van. Így d rendű eleme H-nak 0 vagy $\phi(d)$ van. Ha valamely d-re nulla lenne, az $n = \sum_{d|n} \phi(d)$ összefüggésből az következne, hogy H elemeinek száma $< n$, ellentmondásban a feltételünkkel. Speciálisan, létezik olyan $x \in H$, amelynek rendje n és H megegyezik a (x) ciklikus csoporttal.

3.10. Tétel. *Ha p prím, akkor $\mathbb{Z}/p\mathbb{Z}$ nem nulla elemeinek multiplikatív csoportja $p - 1$ rendű ciklikus csoport.*

Bizonyítás. Az $x^d = 1$ egyenletnek, amelynek foka d, legfeljebb d gyöke van a $\mathbb{Z}/p\mathbb{Z}$ testben, így a tétel következik az előző lemmából.

3.11. Definíció. Ha $a \in Z$, $m > 1$, $\mathrm{lnko}(a, m) = 1$, és az $x^2 \equiv a \pmod{m}$ kongruenciának van megoldása, akkor azt mondjuk, hogy *a kvadratikus maradék modulo m*, egyébként azt mondjuk, hogy *a kvadratikus nemmaradék modulo m*. Legyen p páratlan prím. Az $(a|p)$ vagy $\left(\dfrac{a}{p}\right)$ *Legendre-szimbólum*ot a következőképpen definiáljuk: $(a|p) = 0$, ha $p|a$, egyébként $(a|p) = 1$, ha a kvadratikus maradék modulo p és $(a|p) = -1$, ha a kvadratikus nemmaradék modulo m.

3.12. Euler tétele. *Minden $p > 2$ prímre és $0 < x < p$-re*

$$x^{(p-1)/2} \equiv (x|p) \pmod{p}.$$

Bizonyítás. Legyen g egy generátora $(\mathbb{Z}/n\mathbb{Z})^*$-nek. Mindkét oldal $\equiv 1$, ha x a g páros hatványa, és $\equiv -1$, ha x a g páratlan hatványa.

3.13. Gauss lemmája. *Legyen $p > 2$ egy prímszám, és $a \in \mathbb{Z}$ úgy hogy $p \nmid a$. Ekkor*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2} \lfloor 2ai/p \rfloor},$$

továbbá $(2|p) = (-1)^{(p^2-1)/8}$, és ha $2 \nmid a$, akkor

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2} \lfloor ai/p \rfloor}.$$

Bizonyítás. A $p_1 = (p-1)/2$ jelöléssel, ha $1 \le i \le p_1$, akkor $ia \equiv \varepsilon_i r_i \pmod{p}$, ahol $\varepsilon_i = \pm 1$ és $1 \le r_i \le p_1$. Az $r_1, \ldots, r_{p_1}$ számok páronként különbözőek, és

$$\varepsilon_i = \begin{cases} 1, & \text{ha } ia/p \bmod 1 < 1/2, \\ -1, & \text{ha } ia/p \bmod 1 > 1/2. \end{cases}$$

Minden $x \in \mathbb{R}$-re $x = \lfloor x \rfloor + (x \bmod 1)$, ahonnan $2x = 2\lfloor x \rfloor + 2(x \bmod 1)$. Innen $\lfloor 2x \rfloor = 2\lfloor x \rfloor + \lfloor 2(x \bmod 1) \rfloor$. Ezt alkalmazva $x = ai/p$-re,

$$(-1)^{\sum_{i=1}^{p_1} \lfloor 2ai/p \rfloor} = (-1)^{\sum_{i=1}^{p_1} \left\lfloor 2(ai \bmod p) \right\rfloor} = (-1)^{\mu},$$

ahol μ azon i indexek száma, amelyekre $\varepsilon_i = -1$. Összeszorozva az $a, 2a, \ldots, p_1 a$ számokat,

$$p_1! a^{p_1} \equiv (-1)^{\mu} p_1! \pmod{p},$$

ahonnan

$$a^{p_1} \equiv (-1)^{\mu} \pmod{p},$$

azaz kapjuk az első állítást.

Alkalmazva az első állítást egy páratlan a-ra,

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4(a+p)/2}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{(a+p)/2}{p}\right) = \left(\frac{(a+p)/2}{p}\right)$$
$$= (-1)^{\sum_{i=1}^{p_1}\lfloor (a+p)i/p\rfloor} = (-1)^{\sum_{i=1}^{p_1}\lfloor ai/p\rfloor}(-1)^{\sum_{i=1}^{p_1} i}$$
$$= (-1)^{\sum_{i=1}^{p_1}\lfloor ai/p\rfloor}(-1)^{(p^2-1)/8}.$$

Innen egyrészt $a = 1$ helyettesítéssel $(2|p) = (-1)^{(p^2-1)/8}$, mert ekkor $\lfloor ai/p\rfloor = \lfloor i/p\rfloor = 0$ minden i-re, másrészt, mivel ezt felhasználva, minden $a \in \mathbb{Z}$ esetén $(2a|p) = (2|p)(a|p) = (-1)^{(p^2-1)/8}(a|p)$, következik páratlan a-ra, hogy

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2}\lfloor ai/p\rfloor}.$$

3.14. Gauss kvadratikus reciprocitási törvénye. *Ha $p, q > 2$ páratlan prímszámok, akkor*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Bizonyítás. A $p_1 = (p-1)/2$, $q_1 = (q-1)/2$ jelölésekkel tekintsük az azon (pi, qj) párok P halmazát, amelyekre $1 \le i \le q_1$ és $1 \le j \le p_1$. Nyilván $\natural(P) = p_1q_1$. Mivel $pi = qj$ lehetetlen, azon párok $P_<$, illetve $P_>$ halmaza, amelyekre $pi < qj$, illetve $pi > qj$, diszjunkt halmazokra való felbontása P-nek. Rögzítsük j-t. Ekkor $\lfloor qj/p\rfloor$ darab i létezik, amelyre $1 \le i \le qj/p$. Mivel $1 \le j \le p_1$ és $\lfloor qp_1/p\rfloor < q/2$, azt kapjuk, hogy $\natural(P_<) = \sum_{j=1}^{q_1}\lfloor pj/q\rfloor$. Hasonlóan $\natural(P_>) = \sum_{i=1}^{p_1}\lfloor qi/p\rfloor$. A Gauss-lemmát felhasználva,

$$\left(\frac{p}{q}\right) = (-1)^{\natural(P_<)}, \quad \left(\frac{q}{p}\right) = (-1)^{\natural(P_>)},$$

így

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\natural(P_<)+\natural(P_>)} = (-1)^{\natural(P)} = (-1)^{p_1q_1}. \quad \square$$

3.15. Definíció. Az Euler-tétel prímtesztként történő használatához ki kell terjesztenünk az $(x|m)$ Legendre-szimbólumot arra az esetre, amikor m tetszőleges páratlan természetes szám. Ez a kiterjesztés a Jacobi-szimbólum. Definíciója: ha m prímfelbontása $p_1p_2\cdots p_n$, és $x \in \mathbb{Z}$, akkor legyen

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

3.16. Tétel. *Legyen $m, n > 2$ páratlan szám. Ekkor*

(1) ha $x \equiv y \pmod m$ akkor $(x|m) = (y|m)$;

(2) $(x|m) \cdot (y|m) = (xy|m)$;

(3) $(-1|m) = (-1)^{(m-1)/2}$;

(4) $(2|m) = (-1)^{(m^2-1)/8}$;

(5) $(n|m) \cdot (m|n) = (-1)^{(m-1)(n-1)/4}$.

Bizonyítás. (1) és (2) bizonyítása könnyű. Ha m prím, akkor (3) közvetlenül következik az Euler-kritériumból. Az általános eset következik ebből és a könnyen belátható

$$\frac{s-1}{2} + \frac{t-1}{2} \equiv \frac{st-1}{2} \bmod 2, \quad \text{ha } t, s \text{ páratlanok}$$

összefüggésből. (4)-et már beláttuk, ha m prím. Az általános eset erre redukálható a könnyen bizonyítható

$$\frac{s^2-1}{8} + \frac{t^2-1}{8} \equiv \frac{s^2t^2-1}{8} \bmod 2 \quad \text{ha } t, s \text{ páratlanok}$$

összefüggés segítségével. Végül ha $m, n > 2$ prímek, akkor (5) Gauss tétele. Az általános eset ugyanúgy redukálható erre az esetre, mint (3).

3.17. Példa.

$$\begin{aligned}(76|131) &= (2|131) \cdot (2|131) \cdot (19|131) = (19|131)\\ &= (131|19) \cdot (-1)^{(131-1)(19-1)/4} = -(17|19)\\ &= -(19|17) \cdot (-1)^{(19-1)(17-1)/4} = -(19|17)\\ &= -(2|17) = -(-1)^{(17^2-1)/8} = -1.\end{aligned}$$

3.18. A Jacobi-szimbólum kiszámítása. Az alábbi algoritmus kiszámítja az $(n|m)$ Jacobi szimbólum értékét. Itt $m > 1$ páratlan szám, $n \geq 0$ egész, és $b_i(x)$ a 2^i együtthatója x bináris alakjában.

(1) [Inicializálás.] Legyen $p \leftarrow 0$. (Az algoritmus során p az előjelváltások párossága.)

(2) [Moduláris redukció.] Legyen $n \leftarrow n \bmod m$.

(3) [Nulla?] Ha $n = 0$, akkor az algoritmus véget ért, az eredmény nulla.

(4) [n páros?] Ha $b_0(n) = 1$, menjünk (6)-ra.

(5) [Osztás kettővel.] Legyen $p \leftarrow p \oplus b_1(m) \oplus b_2(m)$ és $n \leftarrow n/2$, majd menjünk (4)-re.

(6) [$n = 1$?] Ha $n = 1$, az algoritmus véget ért, az eredmény $1 - 2p$.

(7) [Reciprocitás.] Legyen $p \leftarrow p \oplus (b_1(n) \wedge b_1(m))$, $m \leftrightarrow n$, és menjünk (2)-re.

A Jacobi szimbólum kiterjeszthető minden $n, m \in \mathbb{Z}$ esetére. Az ezt számoló általánosabb rutinnak a programja a fenti algoritmusra támaszkodhat.

3.19. Feladat. Irjunk Maple demo programot $(x|m)$ kiszámolására, ahol x tetszőleges, m pedig pozitív páratlan egész.

3.20. Feladat. Hogyan működik a Maple 'jacobi' nevű eljárása?

3.21. Feladat. Hogyan működik a Maple 'legendre' nevű eljárása?

3.22. Soloway–Strassen-teszt. Az n szám prím voltát Euler tétele alapján teszteljük: egy $1 < a < n$ számra ellenőrizzük, hogy

$$a^{(n-1)/2} \equiv (a|n) \pmod{n}$$

teljesül-e. Soloway és Strassen megmutatták, hogy ha n összetett, akkor azon $1 < a < n$ alapok száma, amelyekre a feltétel teljesül, legfeljebb $(n-1)/2$. Véletlen a-kat választva, a teszt ismétlésével a hiba valószínűségét tetszőleges kicsire csökkenthetjük.

3.23. Feladat. Irjunk programot a Soloway–Strassen-tesztre.

3.24. Miller–Rabin-teszt. Egy adott $n > 1$ páratlan egészre, az algoritmus megpróbálja eldönteni, hogy n prím-e. Legyen $n = 1 + 2^k q$ ahol q páratlan, és a egy egész, amelyre $1 < a < n$.

(1) [Inicializálás.] Legyen $j \leftarrow k$ és $b \leftarrow a^q \bmod n$.

(2) [Kész?] Ha $j = k$ és $b = 1$, vagy ha $b = n - 1$, akkor mondjuk azt hogy „n valószínű prím", és az algoritmus véget ért. Ha $j < k$ és $b = 1$, akkor n összetett, és az algoritmus véget ért.

(3) [j csökkentése.] Legyen $j \leftarrow j - 1$. Ha $j > 0$, legyen $b \leftarrow b^2 \bmod n$ és menjünk vissza (2)-re.

(4) [Nem prím.] Az algoritmus véget ért, n összetett.

Az ötlet az, hogy ha $n = 1 + 2^k q$ prím, és $a^q \bmod n \neq 1$, akkor az

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

sorozatnak 1-re kell végződnie, és az első 1 előtti tagnak $n-1$-nek kell lenni, mivel $b^2 \equiv 1 \pmod{n}$ megoldásai csak $b = \pm 1$ ha n prím, ugyanis $(b-1)(b+1)$ az n többszöröse kell legyen.

A legfontosabb tény ezzel az algoritmussal kapcsolatban, hogy ha $n \geq 9$ és véletlen $1 < a < n$ alapot választunk, akkor az algoritmus kisebb mint $1/4$ valószínűséggel téved. (A bizonyítást lásd például Knuth [24], 4.5.4, 22. feladat.) Ismételt alkalmazásával tetszőlegesen kis valószínűséget elérhetünk. Az is megmutatható, hogy soha nem téved, ha a Soloway–Strassen-algoritmus nem hibázik, így annál erősebb. (Lásd Knuth [24], 4.5.4, 23. feladat.)

A valószínűségi teszt nagyon ritkán hibázik. Az első összetett szám, amely (hibásan) a 2 alappal átmegy a teszten 2 047; amely még a 3 alappal is 1 373 653; amely még az 5 alappal is 25 326 001; amely még a 7 alappal is 118 670 087 467; amely még a 11 alappal is 2 152 302 898 747; amely még a 13 alappal is 3 474 789 660 383; és amely még a 17 alappal is 341 550 071 728 321.

3.25. Feladat. Irjunk programot a Miller-Rabin tesztre.

3.26. Feladat. Irjunk programot, amely a Miller–Rabin teszttel jó ikerprím jelölteket keres.

3.27. Miller tétele. *Ha az általánosított Riemann sejtés igaz, és n összetett, de nem prímhatvány, akkor van olyan $a < 2(\ln n)^2$ alap, amellyel a Miller–Rabin teszt felfedezi, hogy n összetett.*

3.28. Feladat. Miller tétele alapján irjunk egy determinisztikus prímteszt programot, feltételezve, hogy az általánosított Riemann-sejtés igaz.

3.29. Lucas-teszt. *Az $n > 1$ egész szám akkor és csak akkor prím, ha van olyan a egész, amelyre $a^{n-1} \bmod n = 1$ de minden p prímre, amelyre p osztója $n-1$-nek, $a^{(n-1)/p} \bmod n \neq 1$.*

Bizonyítás. Ha n prím, akkor a redukált maradékosztályok egy $n-1$ rendű ciklikus csoportot alkotnak, és ennek bármely a generátora rendelkezik a fenti tulajdonsággal. Másrészt, ez a tulajdonság azt jelenti, hogy a egy $n-1$ rendű eleme a redukált maradékosztályok multiplikatív csoportjának, ami lehetetlen, ha n összetett, és a csoport rendje $\varphi(n) < n-1$.

A teszthez szükségünk van $n-1$ prímfelbontására, amit általában nehéz megtalálni. Az a alap megtalálása általában nem okoz gondot, mert ha n prím, akkor $\varphi(n-1)$ ilyen a van, és $\varphi(m)/m$ átlagértéke $6/\pi^2$. Ez ugyan túl optimista becslés páros számokra, de jelzi, hogy a megtalálása nem jelent nagy gondot. Kicsit gyorsíthatunk, ha csak olyan a számokat használunk, amelyekre $(a|n) = -1$, először azt ellenőrizzük, hogy $a^{(n-1)/2} \bmod n = n-1$, majd a többi p prímtényezőjére $n-1$-nek azt, hogy $a^{(n-1)/(2p)} \bmod n \neq n-1$.

3.30. Feladat. Irjunk programot a Lucas-tesztre.

A Lucas-teszt különösen hasznos, ha $n-1$ prímtényezős felbontása triviális. Például ez a helyzet a Fermat-számoknál.

3.31. Pépin-teszt. *Jelölje F_m a $2^{2^m}+1$ Fermat számot. Ha $m > 0$, akkor F_m akkor és csak akkor prím, ha $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$.*

Bizonyítás. Mivel az egyetlen prím, ami F_m-1-et osztja a 2, ha az egyenlőség teljesül, akkor F_m prím. Csak azt kell megmutatnunk, hogy ha F_m prím, akkor az egyenlőség teljesül. Tudjuk, hogy 2^2 kongruens 1 modulo 3. Mivel 2^m többszöröse 2-nek, $F_m \equiv 2 \pmod 3$. A $(3|F_m)$ Legendre-szimbólumot a kvadratikus reciprocitás tétele segítségével számíthatjuk ki: $(3|F_m) = (F_m|3) = (2|3) = -1$, így Euler tételéből következik az állítás.

3.32. Feladat. Irjunk programot a Pepin-tesztre.

A Lucas-teszt két irányban is továbbfejleszthető. A egyik, hogy nem szükséges $n-1$ teljes felbontását ismernünk (Pocklington), a másik, hogy az a alap függhet p-től (Lehmer).

3.33. Pocklington–Lehmer-teszt. *Legyen $n > 1$ egy egész szám és $n - 1 = fu$, ahol $\mathrm{lnko}(f, u) = 1$. Tegyük fel, hogy minden p prímosztójához f-nek van olyan a_p egész, amelyre $a_p^{n-1} \bmod n = 1$ és $\mathrm{lnko}(a_p^{(n-1)/p} - 1, n) = 1$. Ekkor minden d osztójára n-nek $d \bmod f = 1$ és ha $f \geq \sqrt{n}$, akkor n prím.*

Bizonyítás. Legyen q egy prímosztója d-nek. Ekkor $a_p^{q-1} \equiv 1 \pmod{q}$, mivel a_p relatív prím n-hez, így q-hoz is. Másrészt, mivel $\mathrm{lnko}(a_p^{(n-1)/p} - 1, n) = 1$, azt kapjuk, hogy $a_p^{(n-1)/p} \not\equiv 1 \pmod{q}$. Ha e a pontos rendje a_p-nek modulo q, ez azt jelenti, hogy $e|q-1$, $e \nmid (n-1)/p$ de $e|n-1$. Ha most p^α a legmagasabb hatványa p-nek, amely osztja $n-1$-et, akkor $p^\alpha|e|q-1$, mutatva, hogy $q \equiv 1 \pmod{p^\alpha}$. Mivel ez f minden prímosztójára teljesül, a kínai maradéktétel alapján azt kapjuk, hogy $q \equiv 1 \pmod{f}$. Most, mivel ez d minden q prímosztójára teljesül, azt kapjuk, hogy d-re is teljesül. Végül, ha $f \geq \sqrt{n}$, akkor ez azt jelenti, hogy n-nek nincs prímosztója, amely $\leq \sqrt{n}$, azaz n prím.

3.34. Feladat. Irjunk programot a Pocklington–Lehmer tesztre.

3.35. Feladat. Irjunk programot $hk^m + 1$ alakú számok prímtesztelésére, ahol h, k, m „kicsik”.

3.36. Proth-teszt. *Ha $n = h2^m + 1$, ahol h páratlan természetes szám, $h < 2^m$, és létezik olyan $a \in \mathbb{Z}$, hogy $a^{(n-1)/2} \equiv -1 \pmod{n}$, akkor n prím.*

Bizonyítás. Alkalmazzuk a Pocklington–Lehmer-tesztet $f = 2^m$-el. Ha $2^m \leq \sqrt{n}$ lenne, akkor $h2^m + 1 \leq 2^m(2^m - 1) + 1 < 2^{2m} \leq n$, ellentmondást kapnánk.

3.37. Feladat. Irjunk programot a Proth-tesztre.

Ha $n - 1$ prímosztóit próbaosztással kerestük, akkor melléktermékként egy b korlátot kapunk, amelynél az $n - 1$ még faktorizálatlan részének csak nagyobb prímosztói vannak. Ez lehetővé teszi az előbbi állítás élesítését.

3.38. Tétel. *Legyen $n > 1$ egy egész szám és $n-1 = fu$, ahol $\mathrm{lnko}(f, u) = 1$ és u minden prímosztója nagyobb mint b, továbbá $bf \geq \sqrt{n}$. Tegyük fel, hogy minden p prímosztójához f-nek van olyan a_p egész, amelyre $a_p^{n-1} \bmod n = 1$ és $\mathrm{lnko}(a_p^{(n-1)/p} - 1, n) = 1$, továbbá van olyan a_u amelyre $a_u^{n-1} \bmod n = 1$ és $\mathrm{lnko}(a_u^f - 1, n) = 1$. Ekkor n prím.*

Bizonyítás. Legyen q egy prímosztója n-nek. Ugyanúgy, mint az előző bizonyításban, kapjuk, hogy $q \equiv 1 \pmod{f}$. Ha e az a_u pontos rendje modulo q, akkor $e|q-1$, $e \nmid f = (n-1)/u$ de $e|n-1$. Most $g = \mathrm{lnko}(e, u)$-ra $g = 1$ nem teljesülhet, mivel ekkor $e|n-1 = fu$ miatt azt kapnánk, hogy $e|f$, ellentmondásban feltevésünkkel. Innen $g > 1$, és mivel u minden prímfaktora nagyobb, mint b, azt kapjuk, hogy $g > b$. Végül, mivel $\mathrm{lnko}(f, u) = 1$, a $q \equiv 1 \pmod{e}$ és $q \equiv 1 \pmod{f}$ feltételekből azt kapjuk, hogy $q \equiv 1 \pmod{fg}$. Innen $q > bf \geq \sqrt{n}$, mutatva, hogy n prím.

3.39. Feladat. Irjunk programot, amely n prím voltát teszteli, ha $n-1=fu$, az f faktorai adottak, és adott egy b korlát úgy, hogy u-nak nincs b-nél kisebb prímtényezője, valamint $fb > \sqrt{n}$.

4. Lucas-sorozatok

4.1. Definíció. Legyenek a és b az egész együtthatós

$$\lambda^2 - P\lambda + Q = 0$$

úgynevezett *karakterisztikus egyenlet* gyökei, $a \neq b$, és az U_n, V_n sorozatokat definiáljuk az

$$U_n = \frac{a^n - b^n}{a-b}, \qquad V_n = a^n + b^n, \qquad n \geq 0.$$

összefüggésekkel. Ezek az úgynevezett *Lucas-sorozat*ok. Vegyük észre, hogy ha a-t és b-t felcseréljük, akkor U_n, V_n nem változnak.

4.2. Megjegyzés. A fenti jelölésekkel, $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$, és ha $m \geq n$, akkor

$$U_{m+n} = U_m V_n - Q^n U_{m-n},$$
$$V_{m+n} = V_m V_n - Q^n V_{m-n}.$$

Ha $n = 1$, egy *rekurziós formulá*t kapunk, amiből látszik, hogy U_m, V_m egészek. Továbbá $D = P^2 - 4Q$ jelöléssel

$$2U_{n+m} = U_n V_m + U_m V_n,$$
$$2V_{n+m} = V_n V_m + D U_n U_m,$$
$$V_n + U_n\sqrt{D} = 2^{1-n}(P + \sqrt{D})^n.$$

4.3. Példa. $\lambda^2 - \lambda - 1 = 0$, $a, b = (1 \pm \sqrt{5})/2$, az aranymetszés aránya. $P = 1$, $Q = -1$, U_n a Fibonacci-sorozat.

4.4. Rekurzió számoláshoz. Az

$$U_{2n} = U_n V_n,$$
$$V_{2n} = V_n^2 - 2Q^n,$$
$$U_{2n+1} = U_{n+1} V_n - Q^n,$$
$$V_{2n+1} = V_{n+1} V_n - PQ^n,$$

összefüggéseket felhasználva, U_n, V_n kiszámítása nagy n indexekre is gyors. Példa: F_{100} a Fibonacci-sorozatból. Kiszámítandó U_{100}, U_{50}, V_{50}, U_{25}, V_{25}, U_{13}, V_{13}, U_{12}, V_{12}, U_7, V_7, U_6, V_6, U_4, V_4, U_3, V_3, U_2, V_2. Más megfogalmazás: a

$$\begin{pmatrix} U_{m+1} & V_{m+1} \\ U_m & V_m \end{pmatrix} = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} U_m & V_m \\ U_{m-1} & V_{m-1} \end{pmatrix}$$

összefüggésből azt kapjuk, hogy

$$\begin{pmatrix} U_{m+1} & V_{m+1} \\ U_m & V_m \end{pmatrix} = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}^m \begin{pmatrix} U_1 & V_1 \\ U_0 & V_0 \end{pmatrix}.$$

4.5. Feladat. Irjunk programot, amely nagy n-re kiszámolja egy Lucas-sorozat U_n, V_n tagjait.

4.6. Megjegyzés. A Lucas-sorozatok tagjainak oszthatóságát tanulmányozva prímtesztekhez juthatunk. Az általános eset tanulmányozása sok könyvben megtalálható, lásd például Bressoud könyvét. Számunkra elegendő lesz a $Q = 1$ speciális esethez tartozó Lucas-sorozatok tanulmányozása.

4.7. Definíció. Tegyük fel, hogy $D \bmod 4$ vagy 0, vagy 1, az n pozitív egész szám, amely relatív prím $2D$-hez, és tekintsük az összes (a, b), $0 \le a, b < n$ párok $L(D, n)$ halmazát, amelyekre $a^2 - b^2 D \equiv 4 \pmod{n}$. Ha $(a', b'), (a'', b'') \in L(D, n)$, definiáljuk az $(a, b) = (a', b')(a'', b'')$ *szorzat*ukat az

$$a = \frac{n+1}{2}(a'a'' + b'b''D) \bmod n,$$
$$b = \frac{n+1}{2}(a'b'' + b'a'') \bmod n,$$

összefüggéssel. Nem nehéz belátni, hogy az így definiált szorzás nem vezet ki $L(D, n)$-ből, kommutatív, asszociatív, a $(2, 0)$ pár egységelem, és az (a, b) pár inverze az $(a, -b)$ pár. Így $L(D, n)$ Abel-csoport. Könnyű kiszámolni, hogy az $(n - 2, 0)$ pár négyzete az egységelem. Ha n prím, akkor csak ennek és az egységelemnek a négyzete az egységelem. Hasonlóan, ha $a = 0$, akkor az (a, b) pár négyzete $(n-2, 0)$. Ha n prím, akkor az $a = 0$ feltétel szükséges is ahhoz, hogy az (a, b) pár négyzete $(n - 2, 0)$ legyen.

Vegyük észre, hogy szoros kapcsolat van a P és $Q = 1$ paraméterekhez tartozó Lucas-sorozattal: Teljes indukcióval azonnal következik, hogy az (a_k, b_k), $a_k = V_k \bmod n$, $b_k = U_k \bmod n$ párok $L(D, n)$-ben vannak, és az (a_k, b_k) párnak az (a_l, b_l) párral vett szorzata az (a_{k+l}, b_{k+l}) pár.

4.8. Tétel. *Az előző definíció jelöléseivel, ha n páratlan prím, $D > 1$, $n \nmid D$, akkor $L(D, n)$ elemeinek száma $n - (D|n)$.*

Az is megmutatható, hogy a tétel feltételei mellett $L(D, n)$ ciklikus.

Bizonyítás. Azon (a, b) párok számát keressük, amelyekre $a^2 - b^2 D \bmod n = 4$. Ha $b = 0$, akkor két megoldás van, $a \equiv \pm 2$. Ha $b \ne 0$, akkor a kongruencia a

$$D \equiv (ab^{-1} - 2b^{-1})(ab^{-1} + 2b^{-1})$$

kongruenciával ekvivalens. Ez azt mutatja, hogy kölcsönösen egyértelmű megfeleltetés van az (a, b), $b \ne 0$ megoldáspárok és az olyan (r, s), $0 < r, s < n$, $r \ne s$ párok között, amelyekre $rs \equiv D$. Így ha $(D|n) = -1$, akkor minden $0 < r < n$-hez van egy s, amellyel megoldást kapunk, egyébként kettőhöz nincs.

4.9. Feladat. Irjunk programot az n szám prím voltának bizonyítására, ha ismerjük $n+1$ prímfelbontását. Próbáljunk ki minden Lucas-sorozatot, amelynek P paramétere egy adott határ alatt van, Q paramétere pedig 1.

4.10. Lucas-típusú teszt. *Legyen $n > 1$ egy páratlan egész szám és $n+1 = fu$, $\mathrm{lnko}(f,u) = 1$. Tegyük fel, hogy van olyan P és $Q = 1$ paraméterekkel generált Lucas-sorozat, amelyre $\mathrm{lnko}(D,n) = 1$, $(D|n) = -1$,*

$$V_{n+1} \equiv 2, \quad U_{n+1} \equiv 0 \pmod{n},$$

és minden p prímosztójához f-nek

$$\mathrm{lnko}(V_{(n+1)/p} - 2, U_{(n+1)/p}, n) = 1.$$

Ekkor minden d osztójára n-nek $d \equiv \pm 1 \pmod{f}$ és ha $f \geq \sqrt{n} + 2$, akkor n prím.

Bizonyítás. Legyen q egy prímosztója d-nek. Legyen e a pontos rendje a $(P \bmod n, 1)$ párnak az $L(D,q)$ csoportban. Tudjuk, hogy $e|q-(D|q)$. Feltételeinkből a $(P,1)$ pár $n+1$-edik hatványa $L(D,q)$-ban $(2,0)$, azaz $e|n+1$, de az $(n+1)/p$-edik hatvány $L(D,q)$-ban nem $(2,0)$, azaz $e \not| (n+1)/p$. Ebből ha p^α a legmagasabb hatványa p-nek, amely osztja f-et, azt kapjuk, hogy $p^\alpha | e | q - (D|q)$, mutatva, hogy $q \equiv (D|q) \pmod{p^\alpha}$. Mivel ez f minden prímosztójára teljesül, a kínai maradéktétel alapján azt kapjuk, hogy $q \equiv (D|q) \pmod{f}$. Most, mivel ez n minden q prímosztójára teljesül, azt kapjuk, hogy egy tetszőleges d osztójára n-nek $d \equiv \pm 1 \pmod{f}$. Végül, ha $f \geq \sqrt{n} + 2$, akkor ez azt jelenti, hogy $d > \sqrt{n}$, azaz n-nek nincs prímosztója, amely $\leq \sqrt{n}$, tehát n prím.

4.11. Feladat. Irjunk programot az n szám prím voltának bizonyítására, ha ismerjük $n+1$ prímfelbontásának egy részét. Próbáljunk ki minden Lucas-sorozatot, amelyre $|P|$ egy adott határ alatt van, és $Q = 1$.

4.12. Feladat. Irjunk programot az $n = h2^m - 1$ szám prím voltának bizonyítására, ha h páratlan és $h < 2^m$. Próbáljunk ki minden Lucas sorozatot, amelynek P paramétere egy adott határ alatt van, Q paramétere pedig 1.

4.13. Számtestek. *Algebrai szám* alatt olyan komplex számot értünk, amely gyöke valamely racionális együtthatós nem nulla polinomnak. A polinomot mindig választhatjuk *normált*, azaz 1 főegyütthatós polinomnak, vagy egész együtthatós polinomnak. Ha α egy algebrai szám, akkor megmutatható, hogy azon normált racionális együtthatós polinomok között, amelyeknek gyöke, pontosan egy irreducibilis létezik. Ezt nevezzük az α *minimálpolinom*jának, és ennek fokszámát az α *fok*ának. Ha α minimálpolinomja egész együtthatós, akkor α-t *algebrai egész*nek nevezzük. Könnyű látni, hogy az elsőfokú algebrai számok pontosan a racionális számok, az elsőfokú algebrai egészek pedig a racionális egészek. Megmutatható, hogy az algebrai számok testet alkotnak, az algebrai egészek pedig gyűrűt. Az algebrai számok testének egy résztestét *algebrai számtest*nek nevezzük. Például ha α algebrai szám, az összes $f(\alpha)/g(\alpha)$ alakú számok, ahol f és g racionális együtthatós polinomok, $g(\alpha) \neq 0$ egy algebrai számtestet alkotnak. Könnyű látni, hogy ez a komplex számok legszűkebb részteste, amely tartalmazza $\mathbb{Q}$-t és α. Szokásos jelölése $\mathbb{Q}(\alpha)$. Megmutatható, hogy $\mathbb{Q}(\alpha)$ elemei egyértelműen állíthatók elő $r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}$ alakban, ahol n az α foka, az $r_0, \ldots, r_{n-1}$ együtthatók pedig racionálisak. Ha p az α minimálpolinomja, akkor p többi gyökeit az α konjugáltjainak nevezzük. Ezek nem feltétlenül vannak $\mathbb{Q}(\alpha)$-ban, például $x^3 - 2$ esetén ez nem teljesül. A minimálpolinom összes gyökeinek szorzatát $N(\alpha)$-val jelöljük, és α *normá*jának nevezzük. Nem nehéz megmutatni, hogy ha α, β algebrai számok, akkor $N(\alpha\beta) = N(\alpha)N(\beta)$.

Bármely algebrai számtest algebrai egészei gyűrűt alkotnak. Oszthatósági kérdések, kongruenciák ebben a gyűrűben értendők. Megmutatható, hogy egy α algebrai egész pontosan akkor egység, ha $N(\alpha) = \pm 1$. A $\mathbb{Q}(\sqrt{D})$ alakú számtesteket, ahol $D \neq 0, 1$ egy négyzetmentes egész, *kvadratikus számtest*eknek nevezzük. Bármely α másodrendű algebrai számra $\mathbb{Q}(\alpha)$ egy kvadratikus számtest.

4.14. Tétel. *Az $r + s\sqrt{D}$, $r, s \in \mathbb{Q}$ másodrendű algebrai szám normája $r^2 - Ds^2$. A $\mathbb{Q}(\sqrt{D})$ egészei, ahol $D \neq 0, 1$ négyzetmentes,*

$$\begin{aligned} r + s\sqrt{D} \quad &\text{ha } D \equiv 2 \text{ vagy } D \equiv 3 \pmod 4, \\ r + s\frac{-1+\sqrt{D}}{2} \quad &\text{ha } D \equiv 1 \pmod 4, \end{aligned}$$

ahol r és s racionális egészek.

4.15. Riesel-teszt. *Tegyük fel, hogy $n = h2^m - 1$, ahol h egy páratlan természetes szám, $m \geq 2$ és $h < 2^m$. Legyen a egy egység $\mathbb{Q}(\sqrt{D})$-ben, amelyre valamely $k, l, r \in \mathbb{Z}$ egészekkel*

$$a = \frac{(k + l\sqrt{D})^2}{r}, \quad \text{ahol} \quad r = |k^2 - l^2D|, \quad \left(\frac{D}{n}\right) = -1 \quad \text{és} \quad \frac{k^2 - l^2D}{r}\left(\frac{r}{n}\right) = -1.$$

Ekkor n akkor és csak akkor prím, ha $v_{m-2} \bmod n = 0$, ahol $v_s = v_{s-1}^2 - 2$ és $v_0 = a^h + a^{-h}$.

Bizonyítás. Nyilván $N(a) = 1$. Tegyük fel, hogy n prím. Tekintsük a $P = a + a^{-1}$, $Q = aa^{-1} = 1$ paraméterekhez tartozó Lucas sorozatot. (D nem a (P, Q) párhoz tartozó diszkrimináns!) Ekkor $v_{m-2} = V_{(n+1)/4}$. Számoljuk ki $V_{(n+1)/2} \bmod n$-et. Mivel

$$\begin{aligned} V_{(n+1)/2} &= \frac{(k + l\sqrt{D})^{n+1}}{r^{(n+1)/2}} + \frac{r^{(n+1)/2}}{(k + l\sqrt{D})^{n+1}} \\ &= \frac{(k + l\sqrt{D})^{n+1}}{r^{(n+1)/2}} + \frac{(k - l\sqrt{D})^{n+1}}{r^{(n+1)/2}}, \end{aligned}$$

azt kapjuk, hogy

$$r^{(n+1)/2}V_{(n+1)/2} = 2\sum_{j=0}^{(n+1)/2} \binom{n+1}{2j} l^{2j}D^jk^{n+1-2j} \equiv 2(k^2 - l^2D) \pmod n.$$

Mivel $r^{(n+1)/2} = r^{(n-1)/2}r \equiv r(r|n) \pmod n$, a tétel feltételei miatt kapjuk, hogy $V_{(n+1)/2} \equiv -2 \pmod n$. Innen az $L(P^2-4,n)$ csoport tulajdonságai miatt következik, hogy csak $V_{(n+1)/4} \bmod n = 0$ lehetséges.

A másik irányhoz vegyük észre, hogy az $L(P^2-4,n)$ csoport tulajdonságaiból ha $V_{(n+1)/4} \bmod n = 0$, akkor $V_{(n+1)/2} \equiv -2 \pmod n$ és $V_{n+1} \equiv 2 \pmod n$, így a Lucas típusú teszt alapján következik, hogy n bármely d osztójára $d \equiv \pm 1 \pmod{2^m}$. Így n legkisebb lehetséges prímfaktora 2^m-1. Mivel n nem négyzetszám, hiszen $n \bmod 4 = 3$, ha n összetett lenne, azt kapnánk, hogy $n \geq (2^m-1)(2^m+1) = 2^{2m}-1 > h2^m-1 = n$, ellentmondás.

4.16. Következmény. *Ha h páratlan, $m \geq 2$ és $h < 2^m$, továbbá sem $n = h2^m-1$, sem h nem osztható 3-mal, akkor n pontosan akkor prím, ha $v_{m-2} \bmod n = 0$ ahol $v_s = v_{s-1}^2 - 2$ és $v_0 = (2+\sqrt{3})^h + (2-\sqrt{3})^h$.*

Bizonyítás. Az

$$a = 2+\sqrt{3} = \frac{(1+\sqrt{3})^2}{2} \in \mathbb{Q}(\sqrt{3})$$

egységet használhatjuk a tételben, mivel

$$\left(\frac{D}{n}\right) = \left(\frac{3}{n}\right) = -1 \quad \text{és} \quad \frac{k^2-l^2D}{r}\left(\frac{r}{n}\right) = \frac{-2}{2}\left(\frac{2}{n}\right) = -1.$$

4.17. Feladat. Irjunk programot, amely Lucas-sorozatok segítségével kiszámolja $a^h + a^{-h}$ értékét, ahol $a \in \mathbb{Q}(\sqrt{D})$ egy egység, amelynek normája 1.

4.18. Feladat. Irjunk programot, amely $n = h2^m - 1$ prímtesztelését végzi, ahol h páratlan és nem osztható 3-mal. Használható-e ez a teszt ikerprímek keresésére?

4.19. Feladat. Irjunk programot a Riesel-tesztre, ha az a egység $\mathbb{Q}(\sqrt{D})$-ben a szükséges tulajdonságokkal adott.

4.20. Feladat. Irjunk programot, amely $(k+l\sqrt{D})^2/r$ alakú egységeket keres $\mathbb{Q}(\sqrt{D})$-ben, ahol k, l és r kis egészek úgy, hogy $|r| = |k^2 - l^2D|$.

4.21. Lucas–Lehmer-teszt a Mersenne-számokra. *Ha $m > 2$ páratlan, akkor $M_m = 2^m - 1$ akkor és csak akkor prím, ha $v_{m-2} \bmod M_m = 0$, ahol $v_s = v_{s-1}^2 - 2$ és $v_0 = 4$.*

Bizonyítás. Az előző tesztből $h = 1$ esetén kapjuk a Lucas–Lehmer-tesztet, mert ekkor $v_0 = (2+\sqrt{3}) + (2-\sqrt{3}) = 4$.

4.22. Feladat. Irjunk programot a Lucas–Lehmer-tesztre.

4.23. Valószínűségi teszt. Tekintsük a P és a $Q = 1$ paraméterekhez tartozó Lucas-sorozatot, ahol $D = P^2 - 4$. Legyen $n > 0$ természetes szám, és tegyük fel, hogy $\mathrm{lnko}(n, 2D) = 1$. Ha $n - (D|n) = q2^m$, és n prím, akkor a

$$V_q \bmod n, \quad V_{2q} \bmod n, \quad \ldots \quad V_{2^m q} \bmod n$$

sorozat 2-re végződik, és hátulról az első nem kettes $n - 2$ kell legyen. Erre egy valószínűségi teszt alapozható.

4.24. Feladat. Hogyan dolgozik a Maple 'isprime' eljárása?

4.25. Williams $p + 1$-módszere. Lucas-sorozatokat használva, egy, Pollard $p - 1$ módszerével analóg faktorizálási módszert adhatunk, amely akkor hasznos, ha $p + 1$ „sima". Ez Williams $p + 1$-módszere, amely azon alapul, hogy ha V_i egy Lucas-sorozat $Q = 1$ és P paraméterekkel, p egy prím, amelyre $(D|p) = -1$ és m egy pozitív szám, akkor

$$V_{m(p+1)} \equiv 2 \pmod p.$$

Legyen n egy faktorizálandó egész, és számoljuk ki $Q = 1$-re és valamely P-re a $V_{k!} \bmod n$ értéket. Ha valamely p prímfaktorára n-nek $(D|p) = -1$ és $p+1|k!$, akkor $V_{k!} - 2$ osztható p-vel. Jó esélyünk van rá, hogy $V_{k!} - 2$ nem osztható n-el, így $\mathrm{lnko}(V_{k!} - 2, n)$ egy nem triviális osztója n-nek. A gyakorlatban nem tudjuk, hogy $(D|p) = -1$ teljesül-e, de 50% esélyünk van erre, így jobb több különböző P értéket kipróbálni.

Ha ki tudjuk $V_{k!}$-t $V_{(k-1)!}$-ból számolni, akkor a fenti módszert még egyszerűbb alkalmazni. Ez lehetséges, az alábbi lemma szerint:

4.26. Lemma. *Legyenek $U_k(P)$ és $V_k(P)$ a $Q = 1$ és $P \neq \pm 2$ paraméterekhez tartozó Lucas sorozat tagjai. Ekkor*

$$\begin{aligned} U_{mk}(P) &= U_k(P)U_m(V_k(P)), \\ V_{mk}(P) &= V_m(V_k(P)). \end{aligned}$$

Bizonyítás. Legyen $P' = V_k(P)$ és $Q' = 1$, ekkor a $D = P^2 - 4$ és $D' = P'^2 - 4$ jelölésekkel

$$D' = DU_k(P)^2.$$

Ebből

$$\begin{aligned} V_{mk}(P) + U_{mk}(P)\sqrt{D} &= 2^{1-mk}(P + \sqrt{D})^{mk} \\ &= 2^{1-m}(2^{1-k}(P + \sqrt{D})^k)^m \\ &= 2^{1-m}(V_k(P) + U_k(P)\sqrt{D})^m \\ &= 2^{1-m}(P' + \sqrt{D'})^m \\ &= V_m(P') + U_m(P')\sqrt{D'} \\ &= V_m(P') + U_m(P')U_k(P)\sqrt{D}. \end{aligned}$$

Mivel D nem lehet teljes négyzet, kapjuk a lemma állítását.

4.27. Feladat. Írjunk programot Williams $p + 1$-módszerére.

5. Alkalmazások

5.1. Fermat-számok. Ha 2^n+1 prím, akkor $n=2^m$, mert

$$2^{q2^m}+1=\left(2^{2^m}+1\right)\left(2^{2^m(q-1)}-2^{2^m(q-2)}+\cdots+2^0\right).$$

Ha $m\geq 2$, akkor $F_m=2^{2^m}+1$ minden q prímosztója $k2^{m+2}+1$ alakú, mert $2^{2^m}\equiv -1 \pmod q$, valamint $2^{q-1}\equiv 1 \pmod q$, így $2^{m+1}\mid q-1$, tehát $q=h2^{m+1}+1$, de

$$2^{(q-1)/2}\equiv\left(\frac{2}{q}\right)=(-1)^{(q^2-1)/8}=1 \pmod q,\quad \text{ha } m\geq 2,$$

innen $2^{m+1}\mid (q-1)/2$, azaz $q=k2^{m+2}+1$.

Ennek az észrevételnek az alapján kereshetjük Fermat-számok osztóit, kis k értékekre ismételt négyzetreemeléssel kiszámolva $2^{2^m} \bmod q$ értékét. Nagyon sok Fermat-számnak ismert osztója. Ha nem találunk kis k-t, amelyre q osztója F_m-nek, akkor prímtesztelést a Pépin-teszttel végezhetünk. A teszt futásideje a modulo F_m végzett négyzetreemelés sebességén múlik.

Ha $m=0,1,2,3,4$, akkor F_m prím. Ha $m=5,6,7,8,9,10,11$, akkor F_m teljes prímfelbontását ismerjük. Ha $m=20,22$, akkor tudjuk, hogy F_m összetett, de nem ismerjük osztóját. F_{33} a legkisebb Fermat-szám, amelyről nem tudjuk, hogy összetett-e?

5.2. Feladat. Írjunk programot Fermat-számok osztóinak keresésére.

5.3. Feladat. Hogyan működik a Maple 'fermat' nevű eljárása?

5.4. Mersenne-számok. Legyen $M_p=2^p-1$. Ha p összetett, akkor M_p összetett, mert

$$2^{uv}-1=\left(2^u-1\right)\left(2^{u(v-1)}+2^{u(v-2)}+\cdots+2^0\right).$$

Ha q prím, és $q\mid 2^p-1$, akkor q páratlan, és mivel $2^p\equiv 1 \pmod q$, a 2 rendje moduló q megegyezik p-vel, így $2^{q-1}\equiv 1 \pmod q$ miatt $p\mid q-1$, de $q-1$ páros, így $p|(q-1)/2$, azaz $q=2kp+1$. Mivel

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

azt kapjuk, hogy $q\equiv\pm 1 \pmod 8$. Innen $k\equiv 0$ vagy $k\equiv -p \pmod 4$.

Mersenne-prímek kereséséhez adott p-re szitálással a $2kp+1$ alakú számok közül kiszűrjük azokat, amelyeknek van kis prímosztójuk. A maradék $q=2kp+1$ értékekre kiszámoljuk $2^p \bmod q$ értékét. Ha így nem találunk osztóját M_p-nek, akkor a Lucas–Lehmer-teszttel teszteljük. A teszt futásideje a modulo M_p végzett négyzetreemelés sebességén múlik.

A legnagyobb ismert prím egy rövid időszakot kivéve mindig Mersenne-prím volt. Tudjuk, hogy M_p prím, ha

$$\begin{aligned} p = & 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, \\ & 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, \\ & 86243, 110503, 132049, 216091, 756839, 859433, 1257787, \\ & 1398269, 2976221, 3021377, 6972593, 13466917, \end{aligned}$$

és eddig a határig más kitevőre M_p nem prím. A jelenleg ismert legnagyobb prím $2^{43112609} - 1$. A keresés PC számítógépekkel folyik, több tízezer résztvevővel.

5.5. Feladat. Irjunk egy „előtesztelő" eljárást, amely Mersenne-számok kis osztóit keresi.

5.6. Feladat. Hogyan működik a Maple 'mersenne' nevű eljárása?

5.7. Az $n = h2^m \pm 1$ alakú prímek. Az egyetlen szám, amely a legnagyobb ismert prím volt egy darabig, és nem Mersenne prím, $h2^m - 1$ alakú. Célszerű h-t egy számtani sorozatból választani, szitálással kiszűrni azokat a h értékeket, amelyekre n-nek van kis prímosztója, és a maradékot tesztelni. Keresésre célszerű a Miller–Rabin-tesztet használni. Ha így találunk egy valószínű prímet, akkor az a $+1$ esetben a Proth-teszttel, a -1 esetben a Riesel-teszttel vizsgálható.

5.8. Feladat. Mutassuk meg, hogy $(1 + \sqrt{5})^2/4$ egység $\mathbb{Q}(\sqrt{5})$-ben. Milyen h, m párok esetén teszi ez lehetővé $h2^m - 1$ prímtesztelését?

5.9. Feladat. Irjunk programot, amely az előző feladat eredményei alapján nagy prímeket keres.

5.10. Ikerprímek. Célszerűen $h2^m \pm 1$ alakban keresünk ikerprímet. Itt a szitálás lényegesebb, mint ha csak prímet keresünk. Egyébként úgy járunk el, mint az előző pontban.

5.11. Feladat. Felhasználva, hogy $(1+\sqrt{5})^2/4$ egység $\mathbb{Q}(\sqrt{5})$-ben, milyen h, m párokra használhatjuk a Riesel-tesztet $h2^m \pm 1$ alakú ikerprímek keresésére?

5.12. Feladat. Írjunk programot nagy ikerprímek keresésére az előző feladat eredményeit felhasználva.

5.13. Sophie Germain prímek. Ez definíció szerint azt jelenti, hogy n és $2n + 1$ is prím. Célszerű $n = h2^m - 1$ alakban keresni; n és $2n + 1$ is a Riesel-teszttel tesztelhető.

5.14. Ikerprím, amely Sophie Germain prím is. Célszerű $n = h2^m - 1$ alakban keresni. Az n és $2n + 1$ a Riesel-teszttel, $n + 2$ pedig a Proth-teszttel tesztelhető. Itt a szitálás hatékonysága még fontosabb, mint az előző két problémánál.

5.15. Az n^2+1 és n^4+1 alakú prímek. Legyen $n = h2^m + 1$. A szitáláshoz nem árt tudni, hogy ha q páratlan prím, amely osztja n^2+1-et, akkor $q \equiv 1 \pmod 4$, mert $n^2 \equiv -1 \pmod q$ miatt $1 = (-1|q) = (-1)^{(q-1)/2}$. Hasonlóan, ha q egy páratlan prímosztója n^4+1-nek, akkor $q \equiv 1 \pmod 8$, mert $n^4 \equiv -1 \pmod q$ miatt, ha g egy generátora a $(\mathbb{Z}/q\mathbb{Z})^*$ ciklikus csoportnak, akkor $n = g^k$-ra $g^{4k} \equiv -1$, és így $g^{8k} \equiv 1 \pmod q$, amiből $8k = l(q-1)$, ahol $1 \le l \le 7$, és l nem lehet páros.

5.16. Egyéb speciális prímek. Az eddig tárgyalt tesztekkel megoldható $n! \pm 1$, $n2^n \pm 1$, $(\prod_{p\in\mathbb{P},p<x} p) \pm 1$, és még sok más speciális alakú szám prímtesztelése.

5.17. Kátai egy problémája. Kátai Imre egy problémája az alábbi kérdésre vezet: Igaz-e minden (vagy legalábbis minden elég nagy) p páratlan prímre, hogy $kp-1$ prím valamely $k < p$-re? Az eredeti probléma megoldásához ezt kellene megmutatni $p < 10^{500}$-ra.

Bár, mint a fenti példák mutatják, az eddig tanult algoritmusok speciális alakú számok prím voltának bizonyítására alkalmasak, faktorizálásra és véletlenszerűen választott szám prím voltának bizonyítására csak korlátozottan alkalmazhatók. Az alábbi példa Knuth könyvéből származik.

5.18. Példa. Tegyük fel, hogy a $2^{214}+1$ számot szeretnénk faktorizálni. Egy polinom azonosságból

$$2^{214}+1 = (2^{107}-2^{54}+1)(2^{107}+2^{54}+1).$$

Próbaosztással

$$2^{107}-2^{54}+1 = 5\cdot 857\cdot n_0,$$

ahol n_0 30 jegyű, és $3^{n_0-1} \bmod n_0 = 1$. Próbaosztással

$$n_0 - 1 = 2^2\cdot 19\cdot 107\cdot 353\cdot n_1,$$

ahol n_1 23 jegyű, és $3^{n_1-1} \bmod n_1 \ne 1$. Tovább faktorizálva, $n_1 = 91813 n_2$, ahol n_2 18 jegyű és $3^{n_2-1} \bmod n_2 = 1$. Próbaosztással

$$n_2 - 1 = 2^4\cdot 3^2\cdot 547\cdot n_3,$$

ahol n_3 13 jegyű, és $3^{n_3-1} \bmod n_3 \ne 1$. Tovább faktorizálva, $n_3 = 1103 n_4$, ahol $n_4 = 16537\,01519$, és $3^{n_4-1} \bmod n_4 = 1$. Végül

$$n_4 - 1 = 2\cdot 7\cdot 19\cdot 23\cdot 137\cdot 1973.$$

Most a Lucas-test, vagy Pocklington-Lehmer teszt segítségével bebizonyíthatjuk, hogy n_4, n_2 és n_0 prímek.

A másik faktorral nem ilyen könnyű elbánni. $n_5 = 2^{107}+2^{54}+1$-nek nincs kis prímosztója, de $3^{n_5-1} \bmod n_5 \ne 1$. Pollard ϱ módszerével $n_5 = 843589 n_6$, ahol n_6 27 jegyű, és $3^{n_6-1} \bmod n_6 \ne 1$. Az

$$n_6 = 817\,49124\,77117\cdot 2352\,85691\,04401$$

felbontást például Pollard $p-1$ módszerének második lépcsője képes megtalálni, mert az első faktor $1 + 2^4\cdot 5^2\cdot 67\cdot 107\cdot 199\cdot 41231$.

5.19. Feladat. Végezzük el e fent leírt számításokat: faktorizáljuk $2^{214}+1$-et.

5.20. Prímszámkódolás. Keressünk a valószínűségi teszttel két „nagy" p, q prímet (például 140–160 jegyűeket), és legyen $n = pq$. Ekkor $\varphi(n) = (p-1)(q-1)$. Válasszunk olyan véletlen $1 < e, d < \varphi(n)$ exponenseket, amelyekre $ed \equiv 1 \pmod{\varphi(n)}$. Ha $1 < m < n$ egy üzenet, akkor $c = m^e \bmod n$ használható, mint az üzenet rejtjelzett formája. Ebből az üzenet visszakapható: $m = c^d \bmod n$, hiszen $(m^e)^d \equiv m \pmod p$ és $(m^e)^d \equiv m \pmod q$. Az n és e értékek nyilvánosságra is hozhatók.

A séma felhasználható digitális aláírásra is: Aliz az $m, m^{d_A} \bmod n_A$ párt küldi el Bobnak (a második szám az aláírás), célszerűen Bob kulcsával rejtjelezve.

Az eljárás bizonyítványok kiállítására is felhasználható. Egy hitelt érdemlő szervezettől, akinek nyilvános kulcsát mindenki ismeri, aláírt levélben kaphatjuk meg Aliz nyilvános kulcsát, így ha Aliztól levelet kapunk, biztosak lehetünk benne, hogy nem csalóval állunk szemben, aki Aliznak adja ki magát.

Egy célszerű alkalmazása a prímszámkódolásnak gyorsabb rejtjelző eljárások kulcsainak cseréje.

5.21. Feladat. Irjunk programot ≈ 150 jegyű „biztos" prímek, valamint rejtjelző és fejtő kitevő keresésére az RSA eljáráshoz.

5.22. Feladat. Irjunk egy egyszerű programot az RSA rejtjelzéshez.

III. **ARITMETIKA**

A modern algoritmusok lehetővé teszik „nehéz” számok faktorizálását több mint 200 jegyig, és tetszőleges számok prím voltának bizonyítását több ezer jegyig. De még az előző fejezetben tárgyalt egyszerű algoritmusok több száztól több millió jegyű számokra való alkalmazásához is speciális aritmetikai algoritmusokra van szükség. A modern algoritmusokkal való ismerkedést az aritmetikai algoritmusokkal kezdjük.

6. Számok és polinomok

Szoros kapcsolat van a természetes számokkal végzett és a polinomokkal végzett műveletek között. Mivel ma csak bináris számítógépek léteznek, a számábrázolás alapszámát kettőhatványnak választjuk, a számítógép szóhosszának magfelelő hosszal. Tizes alapú ábrázolás (pl. a Maple régi változatai, 10^4 az alapszám) rendkívül lerontja a hatékonyságot. Néha célszerű negatív jegyeket is megengedni.

6.1. Összehasonlítás, összeadás és kivonás. Az összehasonlítást a legmagasabb helyi értéktől érdemes kezdeni. Számok összeadását és kivonását lehet elölről is kezdeni, bár ez az algoritmos bonyolultabb. Ha hosszú számokkal akarunk moduláris összeadást vagy kivonást végezni, célszerű lehet a műveletet elölről kezdeni, és csak amikor eldőlt hogy a modulus kivonására vagy hozzáadására szükség van, vagy nincs, akkor hátulról befejezni.

6.2. 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.

Ha 2-vel lehet osztani egy kommutatív gyűrűben, akkor a szorzás nem sokkal nehezebb, mint a négyzetreemelés, mert $(a+b)^2 - a^2 - b^2 = 2ab$.

6.3. Klasszikus algoritmusok a szorzásra és az osztásra. Ezeket Knuth [25] könyve részletesen tárgyalja. A szorzás algoritmusa elég nyilvánvaló. Az osztásnál a probléma a hányados becslése. Legyen B az alap, és az a osztandó első jegyei $a_0, a_1, a_2, \ldots$, a b osztóé $b_1, b_2, \ldots$. Tegyük fel, hogy $q = \lfloor a/b \rfloor < B$, és $b_1 \geq \lfloor B/2 \rfloor$. Legyen

$$\hat{q} = \min\Big\{ \big\lfloor (a_0 B + a_1)/b_1 \big\rfloor, B - 1 \Big\}.$$

Ekkor $q \leq \hat{q} \leq q + 2$. Ha

$$\hat{\hat{q}} = \min\Big\{ \big\lfloor (a_0 B^2 + a_1 B + a_2)/(b_1 B + b_2) \big\rfloor, B - 1 \Big\},$$

akkor $q \leq \hat{\hat{q}} \leq q + 1$. (Valójában $\hat{\hat{q}}$ majdnem mindig q.)

A fontos $b_1 \geq \lfloor B/2 \rfloor$ feltétel teljesülése elérhető úgy, hogy az osztandót és az osztót is megszorozzuk egy kettőhatvánnyal, majd az osztás után a maradékot osztjuk ezzel a kettőhatvánnyal. Célszerűbbnek tűnik azonban csak az eltplt osztó első két jegyét előállítani, és minden lépésben előállítani az eltplt osztandó első három jegyét. Ez nagyobb sebességet biztosít, ha a hányados rövid, de az osztó és az osztandó hosszúak, ami nem ritka eset.

Polinomok osztása egyszerűbb.

6.4. Karacuba-szorzás. Az

$$ab = (a_1 B + a_0)(b_1 B + b_0) = (B^2 + B) a_1 b_1 - B(a_1 - a_0)(b_1 - b_0) + (B + 1) a_0 b_0$$

azonosság mutatja, hogy dupla pontos számok szorzását négy helyett három egyszeres pontosságú szorzással is megoldhatjuk. Rekurzívan alkalmazva az ötletet, $k2^m$ bites számok szorzását 4^m darab k bites szorzás helyett 3^m darab k bites szorzással végezhetjük el. Vegyük észre, hogy ha az alap kettőhatvány, akkor ezeken kívül csak összeadásra és kivonásra van szükség, az alappal való szorzás csak eltolás. Ha $a_1 < a_0$ vagy $b_1 < b_0$, célszerű a különbség ellentettjével számolni. Ha a számok hossza nem $k2^m$ bit, három lehetőségünk van: nullákat írunk a szám elé (jó, ha több k-val dolgozhatunk), vagy ha páratlan sok n számjegyből áll a szám, akkor egy jegyet levágva, egy egyszeres pontosságú, két egyszeres pontosságúnak többszörös pontosságúval történő, és egy Karacuba módszerével végezhető szorzásra redukáljuk a feladatot, illetve két $\lceil n/2 \rceil$ és egy $\lfloor n/2 \rfloor$ jegyű szorzásra redukáljuk a feladatot.

Karacuba módszere polinomokra is alkalmazható.

7. Gyors Fourier-transzformáció

7.1. Polinomszorzás gyors Fourier-transzformációval. Test feletti polinomok szorzata könnyen kiszámítható, ha a polinomok az $x_0, x_1, \dots, x_{n-1}$ helyeken felvett értékeikkel adottak, az

$$(x_0, y_0), \dots, (x_{n-1}, y_{n-1})$$

alakban, ahol y_k a polinom x_k helyen felvett értéke. A $p(x) = \sum_{k=0}^{n-1} a_k x^k$ polinom értékei kiszámíthatók a Horner-elrendezés segítségével:

$$p(x) = a_0 + x\Big(a_1 + x\big(a_2 + \cdots + xa_{n-1}\big)\dots\big)\Big)$$

A (legalább) n különböző helyen felvett függvényérték egyértelműen meghatározza a polinom együtthatóit, és az értékekből a polinom Lagrange-interpolációval megkapható:

$$p(x) = \sum_{k=0}^{n-1} y_k l_k(x), \quad \text{ahol} \quad l_k(x) = \prod_{j\neq k} \frac{x - x_j}{x_k - x_j}$$

ezek azonban túl lassú módszerek, és nem vezetnek gyors polinom szorzáshoz.

Komplex együtthatós polinomokra jóval gyorsabb eljárást kapunk, ha $x_j = \omega^j$ választással dolgozunk, ahol $\omega = e^{-2\pi i/n}$ (vagy bármely más primitív n-edik egységgyök). A trükk: ha $k|n$, akkor $y = x^k$ jelöléssel

$$p(x) = \sum_{j=0}^{k-1} x^j p_j(y),$$

ahol

$$p_j(y) = \sum_{l=0}^{n/k-1} a_{kl+j} y^l, \qquad j = 0, 1, \dots, k-1.$$

Ha $x = \omega^j, \omega^{j+n/k}, \dots, \omega^{j+(k-1)n/k}$, akkor y ugyanaz, így minden kiszámított $p_j(y)$ érték többször is felhasználható. Például, ha $k = 2$, akkor a p polinom ω^j és $\omega^{j+n/2}$ helyen felvett értékeit egyszerre számolhatjuk ki (azt is felhasználva, hogy $\omega^{n/2} = -1$) az alábbi pillangó művelettel:

$$\begin{aligned} p(\omega^j) &= p_0(\omega^{2j}) + \omega^j p_1(\omega^{2j}) \\ p(\omega^{j+n/2}) &= p_0(\omega^{2j}) - \omega^j p_1(\omega^{2j}) \end{aligned}$$

Például, ha $n = 8$, $k = 2$, akkor $x = \omega^j$ és $x = \omega^{j+4}$ esetén y értéke ω^{2j}, így az

$$a_0 + a_2 y + a_4 y^2 + a_6 y^3$$

és
$$a_1 + a_3y + a_5y^2 + a_7y^3$$
értékeket kétszer is tudjuk használni, így a munkát nagyjából megfeleztük. Természetesen rekurzívan is alkalmazhatjuk ezt a trükköt. Az alábbi, együtthatóikkal adott polinomok értékeit kell kiszámolnunk a megadott helyeken:

$$\begin{pmatrix} a_0, & a_1, & a_2, & a_3, & a_4, & a_5, & a_6, & a_7 \\ \omega^0, & \omega^1, & \omega^2, & \omega^3, & \omega^4, & \omega^5, & \omega^6, & \omega^7 \end{pmatrix}$$

$$\begin{pmatrix} a_0, & a_2, & a_4, & a_6 \\ \omega^0, & \omega^2, & \omega^4, & \omega^6 \end{pmatrix} \qquad \begin{pmatrix} a_1, & a_3, & a_5, & a_7 \\ \omega^0, & \omega^2, & \omega^4, & \omega^6 \end{pmatrix}$$

$$\begin{pmatrix} a_0, & a_4 \\ \omega^0, & \omega^4 \end{pmatrix} \quad \begin{pmatrix} a_2, & a_6 \\ \omega^0, & \omega^4 \end{pmatrix} \quad \begin{pmatrix} a_1, & a_5 \\ \omega^0, & \omega^4 \end{pmatrix} \quad \begin{pmatrix} a_3, & a_7 \\ \omega^0, & \omega^4 \end{pmatrix}$$

$$\begin{pmatrix} a_0 \\ \omega^0 \end{pmatrix} \begin{pmatrix} a_4 \\ \omega^0 \end{pmatrix} \begin{pmatrix} a_2 \\ \omega^0 \end{pmatrix} \begin{pmatrix} a_6 \\ \omega^0 \end{pmatrix} \begin{pmatrix} a_1 \\ \omega^0 \end{pmatrix} \begin{pmatrix} a_5 \\ \omega^0 \end{pmatrix} \begin{pmatrix} a_3 \\ \omega^0 \end{pmatrix} \begin{pmatrix} a_7 \\ \omega^0 \end{pmatrix}$$

7.2. Gyors Fourier transzformáció (FFT). Az algoritmus az $A[j]$, $0 \le j < n = 2^k$ sorozat Fourier transzformáltját számolja ki. Az eredmény az A tömbben keletkezik, de a Fourier transzformált j-edik eleme $A\big[r_k(j)\big]$, ahol $r_k(j)$ a j természetes szám k bites bináris reprezentációjának megfordításával kapott természetes szám. A számítás használ egy T segédtáblázatot, amely az ω primitív n-edik egységgyök hatványait tartalmazza, alkalmas sorrendben: $T[j] \leftarrow \omega^{r_{k-1}(j)}$, ha $0 \le j < 2^{k-1}$.

(1) [Inicializálás.] Legyen $l \leftarrow 2^{k-1}$.

(2) [Menet kezdete.] Legyen $i \leftarrow 0$ és $t \leftarrow 0$.

(3) [Pillangósorozat kezdete.] Legyen $j \leftarrow i + l$ és $w \leftarrow T[t]$.

(4) [Pillangó.] Legyen $x \leftarrow A[i]$ és $y \leftarrow wA[i+l]$, majd legyen $A[i] \leftarrow x + y$ és $A[i+l] \leftarrow x - y$, végül legyen $i \leftarrow i + 1$.

(5) [Pillangósorozat vége?] Ha $i < j$, menjünk vissza (4)-re.

(6) [Menet vége?] Ha $j + l < 2^k$, legyen $i \leftarrow j + l$, $t \leftarrow t + 1$ és menjünk vissza (3)-ra.

(7) [Vége?] Legyen $l \leftarrow \lfloor l/2 \rfloor$. Ha $l > 0$, menjünk vissza (2)-re, egyébként az algoritmus véget ért.

Az r_k függvény számítása, a „bitfordítás” eltolásokkal történhet: a függvény változóját balra tolva, egyenként megkapjuk bitjeit, és azokat jobbra tolással összerakjuk fordított sorrendben. Még egyszerűbb $r_k(j+1)$ értékét $r_k(j)$-ből számítani, a *legnagyobb helyiértékű bithez* 1-et hozzáadva, és az átvitelt az *alacsonyabb helyiértékek* felé végezve.

Vegyük észre, hogy ugyanaz a T táblázat különböző k értékekre is megfelel, ha a maximális k értékre számoljuk ki.

Az algoritmus helyességét úgy bizonyíthatjuk, hogy belátjuk, ha az eredeti sorozat a_j, $j = 0, 1, \dots, n-1$, akkor a (2) lépésnél, ha $l = 2^{k-1-q}$ (azaz q menet után vagyunk) egy k-bites j szám bináris számot $[j_{k-1}j_{k-2}\dots j_1j_0]$-vel jelölve, ahol $j_i \in \{0,1\}$ a bináris jegyek,

$$A[s_{k-1}s_{k-2}\dots s_{k-q}t_{k-q-1}t_{k-q-2}\dots t_1t_0] = \sum_{t_{k-1},\dots,t_{k-q}\in\{0,1\}} \omega^{[s_0\dots s_{k-1}][t_{k-1}\dots t_{k-q}0\dots 0]} a_{[t_{k-1}\dots t_0]}.$$

7.3. Inverz FFT. A fenti algoritmus megfordítható: ha a meneteket fordított sorrendben hajtjuk végre, $l = 1, 2, \dots, 2^{k-1}$-re, és a (4) pillangó műveletet invertáljuk, akkor a transzformáció inverzét kapjuk:

(4') [Inverz pillangó.] Legyen $x \leftarrow A[i]$, $y \leftarrow A[i+l]$, majd $A[i] \leftarrow (x+y)/2$, $A[i+l] \leftarrow (x-y)/(2w)$, végül $i \leftarrow i+1$.

A felhasznált T táblázat ugyanaz. A kettővel való osztásokat elhagyhatjuk, ha az egész algoritmus elején vagy végén az A tömb minden elemét osztjuk 2^k-val. Vegyük észre azt is, hogy $1/w = \overline{w}$, így nincs szükség osztásra, szorzással is dolgozhatunk.

7.4. Szorzás komplex FFT-vel. Az $(a_0, a_1, \dots, a_{n-1})$ és $(b_0, b_1, \dots, b_{n-1})$ sorozatok Fourier-transzformáltjaira azt kapjuk, hogy $\hat{a}_k\hat{b}_k = \hat{c}_k$, $0 \le k < n$, ahol

$$c_k = \sum_{j=0}^{k} a_j b_{k-j} + \sum_{j=k+1}^{n-1} a_j b_{n+k-j} = \sum_{j=0}^{n-1} a_j b_{k-j \bmod n}.$$

Valóban, a megfelelő $\sum_{k=0}^{n-1} a_k x^k$ és $\sum_{k=0}^{n-1} b_k x^k$ polinomok szorzata minden ω^j helyen ugyanazt az értéket veszi fel, mint a $\sum_{k=0}^{n-1} c_k x^k$ polinom. Ha az $\sum_{k=0}^{n-1} a_k x^k$ és $\sum_{k=0}^{n-1} b_k x^k$ polinomok szorzatának foka kisebb, mint n, akkor éppen a $\sum_{k=0}^{n-1} c_k x^k$ polinom. Így két Fourier-transzformáció és egy inverz Fourier transzformáció segítségével megkaphatjuk a szorzatpolinom együtthatóit, így hosszú számok szorzatát.

Természetesen számításainkat nem tudjuk tökéletes pontossággal végezni. Knuth [24], 4.3.3 megggondolásai mutatják, hogy ha $n = 2^k$ és a számot l bites darabokra bontjuk, akkor $m \ge 3k + 2l + \lg k + 7/2$ bites pontossággal elég dolgozni, ha mindenütt nulla felé történő csonkolást használunk. A feltétel teljesül, ha $k \ge 7$ és $m \ge 4k + 2l$, így l bites gépen mindig elegendő $6l$ bites pontossággal dolgozni. Lehet például úgynevezett „tömblebegőpontos" aritmetikát is használni: ennél a számok mantisszait fixpontosan ábrázoljuk, és egy közös exponens van az összes számra. Ha valamelyik számnál túlcsordulás lépne fel, az egész tömböt egyszerre normalizáljuk.

7.5. Valós FFT. Egy $(a_0, a_1, \dots, a_{2n-1})$ valós számsorozat diszkrét Fourier transzformáltjára $\omega = e^{-\pi i/n}$ jelöléssel

$$\overline{\hat{a}_k} = \sum_{j=0}^{n-1} a_j \bar{\omega}^{jk} = \sum_{j=0}^{n-1} a_j \omega^{(2n-k)j} = \hat{a}_{(2n-k) \bmod 2n}.$$

A $2n$ független valós koordináta kiszámítása redukálható a komplex

$$A_k = a_{2k} + ia_{2k+1}, \qquad k = 0, 1, \dots, n-1$$

sorozat Fourier transzformáltjának kiszámítására:

$$\left(\hat{A}_k + \overline{\hat{A}}_{n-k}\right) - i\omega^k\left(\hat{A}_k - \overline{\hat{A}}_{n-k}\right) = 2\hat{a}_k,$$

ahol az A-k indexei modulo n értendők.

7.6. Szorzás komplex FFT-vel a gyakorlatban. A gyakorlatban praktikusabbnak bizonyul nem túlságosan nagy számok szorzására a processzor beépített lebegőpontos, úgynevezett duplapontosságú aritmetikáját használni, mert ezzel a lebegőpontos szorzások végrehajtása igen gyors. Elég sok bitet teszünk egy jegybe, így az eredmény nem biztos hogy helyes, de a szorzatot modulo $2^m \pm 1$ is kiszámolva, ellenőrizzük, hogy valószínűleg helyes-e? Célszerű negatív jegyeket is megengedni, ekkor a konvolúciós összeg tagjainak előjele vegyes, és csökken a kerekítési hiba esélye.

A bitfordítást elkerülhetjük, ha külön FFT és inverz FFT programot használunk. Természetesen érdemes kihasználni, hogy valós sorozatról van szó. A menetek összevonása lehetséges, két, három vagy négy menet összevonása gazdaságos, a processzortól függően. Az inicializálást összevonhatjuk az első 1–4 menettel, és a végső átvitel számítását is az utolsó 1–4 menettel az inverz FFT-ből.

7.7. Példa. 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.

7.8. FFT véges testek felett. Ha biztos eredményt akarunk, véges testeket használhatunk. Például $n = h2^k + 1$ alakú prím modulust, ekkor van $(\mathbb{Z}/n\mathbb{Z})^*$-ban 2^k-adik primitív egységgyök.

Másik lehetőség: Egy M_p Mersenne prímre a Gauss egészek (azaz $\mathbb{Z}+i\mathbb{Z}$ elemei) modulo M_p. Ez egy F véges test, F^* ciklikus csoport, rendje $2^{p+1}(2^{p-1}-1)$.

Harmadik lehetőség: speciális prím modulust választunk, például $2^{64} - 2^{32} + 1$-et.

7.9. Fermat-szám transzformáció. Modulo egy F_m Fermat szám dolgozunk, $\approx 2^m$ bites egészekkel. Ez ugyan csak gyűrű, ha $m > 4$, de a 2 egy primitív 2^{m+1}-edik egységgyök: $2^{2^m} \equiv -1 \bmod F_m$, így $2^{2^{m+1}} \equiv 1 \bmod F_m$, és a 2^k számok és különbségeik mind invertálhatók modulo F_m, mert kettőhatványok illetve 4-el osztva maradékul 3-at adó számok szorzatai.

Ennek a gyűrűnek az előnye, hogy a primitív egységgyök hatványai mind kettőhatványok, és a velük történő szorzás és osztás modulo F_m nagyon egyszerű, összeadás, kivonás és eltolások segítségével felépíthető.

Egyébként még a „$\sqrt{2}$” szerkezete is egyszerű:

$$\left(2^{3\cdot 2^{m-2}} - 2^{2^{m-2}}\right)^2 \equiv 2 \pmod{F_m},$$

ez is használható. Így egy 2^{m+2} fokú szorzat polinom együtthatóit tudjuk kiszámolni, ha azok 0 és F_m közötti egészek. Például egy $15 \cdot 2^{15}$ bites számot 2^{10} részre oszthatunk, amelyek mindegyike 15 darab 32 bites szóból áll, és az FFT és inverz FFT 2^{11} taggal történik $\bmod(2^{1024}+1)$.

7.10. Schönhage-Strassen féle gyorsszorzó algoritmus. A modulo egy Fermat szám történő számolást rekurzívan alkalmazhatjuk. A finom trükk, hogy az eredményt is csak modulo egy Fermat szám számoljuk ki, viszont a jegyeket kissé „túltöltjük”. A modulo F_m maradékgyűrű szerinti Fermat transzformációval kiszámoljuk két $0 \le a, b < F_{2m}$ szám szorzatát $\bmod F_{2m}$, az alábbiak szerint: Az $a = F_{2m} - 1$ vagy $b = F_{2m} - 1$ eseteket külön kezeljük. Egyébként legyenek a és b jegyei $2^{2^{m-1}}$ alapú számrendszerben $a_0, \dots, a_{2^{m+1}-1}$ illetve $b_0, \dots, b_{2^{m+1}-1}$. Képezzük az $a'_j = a_j\omega^j$, $b'_j = b_j\omega^j$ sorozatokat, ahol ω az előző pontban adott „$\sqrt{2}$”. Kiszámolva (a'_j) és (b'_j) konvolúcióját, ω^2-et használva primitív 2^{m+1}-edik egységgyöknek, a

$$\begin{aligned} c'_k &\equiv \sum_{j=0}^{k} a'_j b'_{k-j} + \sum_{j=k+1}^{2^{m+1}-1} a'_j b'_{2^{m+1}+k-j} \\ &\equiv \omega^k \left(\sum_{j=0}^{k} a_j b_{k-j} - \sum_{j=k+1}^{2^{m+1}-1} a_j b_{2^{m+1}+k-j} \right) \end{aligned}$$

értékeket kapjuk, amiből osztással

$$c_k = \left(\sum_{j=0}^{k} a_j b_{k-j} - \sum_{j=k+1}^{2^{m+1}-1} a_j b_{2^{m+1}+k-j} \right)$$

modulo F_m vett $\tilde{c}_k$ maradéka könnyen kiszámítható. Vegyük észre, hogy a c_k számok éppen $ab \bmod F_{2m}$ jegyei (nem normalizált alakban). Sajnos, csak $\bmod F_m$ kaptuk meg őket. Még $m+1$ bit hiányzik. Ez könnyen pótolható, ha $\bmod 2^{m+1}$ is kiszámoljuk c_k maradékát, Fourier-transzformációval, vagy akár szorzásra visszavezetve és a szorzatot Karacuba-módszerrel meghatározva. Az így kapott $\tilde{\tilde{c}}_k$ maradék felhasználásával c_k meghatározható:

$$c_k \equiv F_m(\tilde{\tilde{c}}_k - \tilde{c}_k \bmod 2^{m+1}) + \tilde{c}_k \big(\bmod 2^{m+1} F_m\big),$$

és tudjuk, hogy $-\big(2^{m+1} - (k+1)\big)(F_m - 1) \le c_k \le (k+1)(F_m - 1)$.

Teljesen hasonlóan kapható a $\bmod F_{2m-1}$ számított szorzat, itt $\omega = 2$.

7.11. Példa. Modulo F_{24} történő szorzást modulo F_{12} végzett szorzásra, azt pedig modulo F_6 végzett szorzásra vezethetünk vissza. Ez utóbbi lépés kérdéses, hogy megéri-e?

7.12. Ritka polinomok és ritka számok. Ritka polinomról, illetve ritka számról beszélünk, ha az együtthatók, illetve a számjegyek nagy része nulla. Persze, egy számra az, hogy ritka-e, a számrendszertől is függ. Ilyen esetekben más algoritmus lehet optimális. Például ritka számokra a klasszikus osztási algoritmus általában gyorsabb, mint a fentebb tárgyalt egyéb algoritmusok. Ritka polinomokkal kapcsolatban lásd még Aho-Hocroft-Ullman [4] 8.12 elemzését.

7.13. Feladat. Dolgozzunk ki nagy sebességű programot ritka számokkal történő szorzásra és osztásra.

7.14. Osztás, polinomosztás. Az ötlet a Newton-iteráció használata az inverz kiszámítására. Az $f(x) = c - 1/x$ függvény zérushelyét keressük iterációval:

$$x_{n+1} = x_n - \frac{c - 1/x_n}{1/x_n^2} = 2x_n - cx_n^2.$$

Skálázást használunk, az $n+1$ bites c számra $2^{2n}/c$-t közelítjük.

Polinomokra az eljárás hasonló. Ha a $p(x)$ polinom foka n, akkor $x^{2n}/p(x)$-et közelítjük.

7.15. Polinom kiértékelése tetszőleges helyeken. Egy $p(x)$ polinom értéke az a_i helyen a maradék $p(x)$-nek $x - a_i$-vel való osztásánál. Ha sok a_i van, akkor $\prod_{i=1}^{2^k}(x - a_i)$-vel osztunk, majd a maradékot osztjuk tovább 2^{k-1} darab $x - a_i$ szorzatával, stb. Így $O(n \lg^2 n)$ az együtthatókkal végzett numerikus művelet elegendő egy n-nél alacsonyabb fokú polinom n helyen való kiértékeléséhez.

7.16. Interpoláció. Tetszőleges n darab x_i helyen vett értékével adott polinom kiszámítható $O_A(n \lg^2 n)$ művelettel. Az $l(x) = \prod_i (x - x_i)$ Lagrange-féle interpolációs polinomot használjuk. Mivel az (algebrai) deriváltra

$$l'(x) = \left(\prod_{i \neq k}(x - x_i)\right)' \cdot (x - x_k) + \left(\prod_{i \neq k}(x - x_i)\right),$$

az kapjuk, hogy $l'(x_k) = \prod_{i \neq k}(x_k - x_i)$, amiből

$$l_k(x) = \prod_{i \neq k} \frac{x - x_i}{x_k - x_i} = \frac{1}{l'(x_k)} \frac{l(x)}{x - x_k}.$$

Az $l'(x_k)$ értékek kiszámítását az előző pontban tárgyalt módon végezzük, az $l(x)/(x - x_k)$ polinomok kiszámítását pedig $\prod_{i=m}^{m+2^n-1}(x - x_i)$ szorzatok kiszámítására vezetjük vissza.

7.17. Feladat. Adjunk hatékony algoritmust kettes számrendszerről más számrendszerre való átszámításra és az inverzére.

7.18. Feladat. Adjunk hatékony algoritmust kínai maradékolásra és az inverzére sok modulus esetén.

* **7.19. Feladat.** Adjunk hatékony algoritmust legnagyobb közös osztó számolására számoknál és polinomoknál.

IV. **ELLIPTIKUS GÖRBÉK**

Az elliptikus görbék használata lehetővé teszi több ezer jegyű számokra azok prím voltának bizonyítását. Másrész, elliptikus görbék segítségével egy nagyon hasznos faktorizálási eljárást nyerhetünk, amely a jelenleg ismert legjobb mindazon eljárások közül, amelyek futásideje elsősorban a faktor hosszától függ, így igen alkalmas számok 20–30, vagy mégtöbb jegyű faktorainak megtalálására.

8. Elliptikus függvények

8.1. Algebrai görbék. Legyen p egy kétváltozós polinom az F test felett. A $G = \{(x, y) : p(x, y) = 0\}$ halmazt *algebrai görbé*nek nevezzük F felett. A p foka a G *rend*je. A legegyszerűbb algebrai görbék az elsőrendű egyenesek és a másodrendű algebrai görbék, például az $x^2 + y^2 - 1 = 0$, $x, y \in \mathbb{R}$ összefüggéssel definiált kör. A kör (és más első- és másodrendű algebrai görbék) esetében könnyen áttérhetünk egy másik, úgynevezett *paraméteres előállítás*ra: a $(\cos t, \sin t)$, $t \in \mathbb{R}$ párok halmaza a kör. Ennek az előállításnak a segítségével, felhasználva, hogy a cos és sin függvények 2π szerint periódikusak, egy műveletet definiálhatunk a kör pontjai között: egyszerűen átmásoljuk a számegyenes összeadását a körre. Legyen tehát

$$(\cos(t_1), \sin(t_1)) \oplus (\cos(t_2), \sin(t_2)) := (\cos(t_1 + t_2), \sin(t_1 + t_2)).$$

Részletesen kiírva,

$$\begin{aligned}&(\cos(t_1), \sin(t_1)) \oplus (\cos(t_2), \sin(t_2)) \\ &\quad = (\cos(t_1)\cos(t_2) - \sin(t_1)\sin(t_2), \sin(t_1)\cos(t_2) + \sin(t_2)\cos(t_1)).\end{aligned}$$

Észrevehetjük, hogy az „új” művelet megfelel a komplex szorzásnak.

8.2. Elliptikus görbék. A harmadrendű görbék közül a legegyszerűbbek az

$$ay^2 + bxy + cy = dx^3 + ex^2 + fx + g$$

alakúak. Ezeket a legtöbb esetben (ha például lehet kettővel és hárommal osztani az adott testben, stb.) egyszerűbb alakra hozhatjuk. Az a-val osztva, majd lineáris helyettesítéssel új változót vezetve be, az $Y^2 = p(x)$ alakra térhetünk át, ahol p harmadfokú polinom. Most a jobb oldalon alkalmazva egy lineáris helyettesítést, az $Y^2 = X^3 + AX + B$ alakra juthatunk. Ilyen görbékkel fogunk foglalkozni. Műveletet akarunk definiálni ilyen görbék pontjai között. (Megjegyezzük, hogy megfelelő feltételek mellett, projektív transzformációkat is felhasználva, minden harmadrendű görbe ilyen alakra hozható.) Vegyük észre, hogy a körnél a paraméterezésben előforduló függvények közül az egyik a másik deriváltja. Mivel ott sin és cos szerepe felcserélhető volt, kereshetünk olyan $t \mapsto x(t)$ leképezést, amelyre $t \mapsto (x(t), x'(t))$ adja a görbe paraméterezését. Ez azt jelenti, hogy az

$$x'^2 = x^3 + Ax + B$$

differenciálegyenlet megoldását keressük.

8.3. Elliptikus integrálok. Az előző differenciálegyenletben $f(x)$-el jelölve a jobb oldalt, a megoldást a

$$t(x) = \int_{x_0}^{x} \frac{du}{\sqrt{f(u)}}$$

függvény inverz függvénye adja. Ha f egy harmad- vagy magasabbfokú polinom, aminek gyökei mind különbözőek, akkor az integrált elemi módszerekkel nem tudjuk kiszámolni. Harmad- illetve negyedfokú f esetén az ilyen integrálokat *elliptikus integrál*oknak nevezzük. Abel alapvető felfedezése volt, hogy az elliptikus integrálok inverz függvényeit komplex változóra is kiterjesztve, olyan függvényt kapunk, amely két irányban is periódikus. Ezeket a függvényeket szokás elliptikus függvényeknek nevezni.

8.4. Elliptikus függvények. Egy, a komplex síkon meromorf f függvényt *elliptikus függvény*nek nevezünk, ha léteznek olyan ω_1, ω_2 nullától különböző komplex számok, amelyekre $\omega_1/\omega_2 \notin \mathbb{R}$ és $f(z+\omega_1) = f(z+\omega_2) = f(z)$ minden $z \in \mathbb{C}$-re. Ha egy elliptikus függvény nem konstans, akkor kell hogy legyen pólusa az ω_1 és ω_2 által meghatározott $\{t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 < 1\}$ paralelogrammában, mivel egyébként olyan korlátos holomorf függvény lenne, amely nem konstans. Ugyanazon ω_1, ω_2 párhoz tartozó elliptikus függvények lineáris kombinációja, szorzata, és — ha az osztó nem mindenütt nulla — a hányadosa is elliptikus függvény.

8.5. A Weierstrass-féle $\mathcal{P}$-függvény. Legyenek ω_1, ω_2 nullától különböző komplex számok úgy, hogy $\omega_1/\omega_2 \notin \mathbb{R}$. Olyan elliptikus függvényt keresünk, amelynek ω_1 és ω_2 periódusai. Jelölje $\Omega = \{\omega_1 k_1 + \omega_2 k_2 : k_1, k_2 \in \mathbb{Z}\}$ az ω_1 és ω_2 által generált rácsot. Legyen

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in \Omega} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

$\mathcal{P}$ ott van értelmezve, ahol a jobb oldalon álló sor minden tagja értelmezve van, és a sor konvergens. Megmutatjuk, hogy $\mathbb{C} \setminus \Omega$ minden pontjában a sor konvergens, sőt, tetszőleges $C \subset \mathbb{C} \setminus \Omega$ kompakt halmazon a konvergencia egyenletes. Legyen $k(\omega) = \max\{|k_1|, |k_2|\}$, ahol k_1 és k_2 az $\omega \in \Omega$ előállításában szereplő egészek. Mivel

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{-z^2 + 2z\omega}{(z-\omega)^2\omega^2},$$

léteznek olyan c_1 és $K_0 > 0$ konstansok, hogy ha $k(\omega) \geq K_0$, akkor

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \leq \frac{c_1}{|\omega|^3}$$

minden $z \in C$-re. Másrészt van olyan $c_2 > 0$ konstans, hogy minden $\omega \in \Omega$-ra $|\omega| \geq c_2 k(\omega)$. Felhasználva, hogy $k(\omega) = K$ pontosan $8K$ darab ω-ra teljesül, ha $K \in \mathbb{Z}$, $K > 0$, azt kapjuk, hogy $z \in C$ esetén

$$\sum_{k(\omega) \geq K_0} \left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \leq \sum_{k(\omega) \geq K_0} \frac{c_1}{|\omega|^3} = \sum_{K=K_0}^{\infty} \sum_{k(\omega)=K} \frac{c_1}{|\omega|^3}$$
$$\leq \sum_{K=K_0}^{\infty} \frac{8c_1}{c_2^3 K^2} < \infty,$$

és a konvergencia egyenletes. Innen azt kapjuk, hogy $\mathcal{P}$ holomorf a $\mathbb{C} \setminus \Omega$ halmazon. Megmutatjuk, hogy $\mathcal{P}$ duplán periódikus ω_1 és ω_2 periódusokkal. A $\mathcal{P}'$ függvényre

$$\mathcal{P}'(z) = -2 \sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3},$$

és úgy mint fent adódik, hogy a jobb oldalon álló sor konvergens minden $z \in \mathbb{C} \setminus \Omega$-ra. Innen $\mathcal{P}'$ duplán periódikus, amiből ha $\omega = \omega_1$ vagy $\omega = \omega_2$, akkor $\mathcal{P}(z) - \mathcal{P}(z+\omega) \equiv c$ valamely c konstanssal. De $\mathcal{P}$ definíció szerint páros, így $z = -\omega/2$ helyettesítéssel azt kapjuk, hogy $c = 0$.

8.6. A Weierstrass-függvény differenciálegyenlete. Az előző pont jelöléseivel, ha $0 \neq \omega \in \Omega$, akkor

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2} + \frac{2z}{\omega^3} + \frac{3z^2}{\omega^4} + \dots .$$

Innen

$$\mathcal{P}(z) = z^{-2} + 3s_4 z^2 + 5s_6 z^4 + \dots ,$$

ahol $s_j = \sum_{0 \neq \omega \in \Omega} 1/\omega^j$ ha $j = 3, 4, \dots$ (nyilván $s_j = 0$, ha j páratlan). Ezt felhasználva némi számolással

$$\mathcal{P}'(z)^2 - 4\mathcal{P}(z)^3 + 60 s_4 \mathcal{P}(z) = -140 s_6 + \dots ,$$

ahol a jobb oldalon csak z pozitív kitevős hatványai szerepelnek. A konvergencia-problémák hasonlóan kezelhetők, mint az előző pontban. Mivel a jobb oldalon álló függvény holomorf és elliptikus, csak nulla lehet, így

$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - 60 s_4 \mathcal{P}(z) - 140 s_6.$$

A $\mathcal{P}$ függvény tehát egy olyan függvény, amely — a deriváltjával együtt — egy, a komplex számok feletti $Y^2 = 4X^3 + AX + B$ egyenletű görbét paraméterez, igaz, egy „(∞, ∞)" pont is a görbéhez tartozik.

8.7. Addíciós képletek. A $\mathcal{P}$-függvény vizsgálatával az alábbi addíciós képletek vezethetők le:

$$\mathcal{P}(x+y)+\mathcal{P}(x)+\mathcal{P}(y)=\frac{1}{4}\left(\frac{\mathcal{P}'(x)-\mathcal{P}'(y)}{\mathcal{P}(x)-\mathcal{P}(y)}\right)^2,$$

$$\mathcal{P}'(x+y)+\mathcal{P}'(x)=\frac{\mathcal{P}'(x)-\mathcal{P}'(y)}{\mathcal{P}(x)-\mathcal{P}(y)}\left(\mathcal{P}(x)-\mathcal{P}(x+y)\right).$$

Az $y=x$ esetben fennálló összefüggést határátmenettel kapjuk. Ezen összefüggések segítségével definiálható az elliptikus görbén az összeadás. A második egyenletből leolvasható az összeadás geometriai jelentése: a $(\mathcal{P}(x),\mathcal{P}'(x))$ és $(\mathcal{P}(y),\mathcal{P}'(y))$ pontok összegét, a $(\mathcal{P}(x+y),\mathcal{P}'(x+y))$ pontot úgy kapjuk, hogy tekintjük az első két ponton átmenő „egyenest”, és ennek az elliptikus görbével vett metszéspontjának a második koordinátáját ellenkező előjelűre változtatjuk.

9. Számolás elliptikus görbéken

9.1. Elliptikus görbék. Egy *elliptikus görbe* $\mathbb{R}$ *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. Ennek belátásához használjuk az implicit függvény tételt.) 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 megmutatjuk, hogy a harmadik koordinátái

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

ahol

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

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

$$\lambda(y_3+y_1)=x_3^2+x_3x_1+x_1^2+a,$$
$$\lambda(y_3+y_2)=x_3^2+x_3x_2+x_2^2+a,$$

kivonással azt kapjuk, hogy

$$\lambda(y_2 - y_1) = x_3(x_2 - x_1) + x_2^2 - x_1^2.$$

Innen következik, hogy $x_3 = \lambda^2 - x_1 - x_2$.

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

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

akkor megmutatható, hogy egy Abel csoportot kapunk.

Ha a, b racionálisak, tekinthetünk csak racionális koordinátájú pontokat, és egy másik csoportot kapunk. Általánosabban, tekinthetünk elliptikus görbéket egy tetszőleges F test felett, amelynek karakterisztikája különbözik 2-től és 3-tól. Meg lehet mutatni, (nehéz!) hogy mindig egy Abel-csoportot kapunk. Még ha csak egy egységelemes kommutatív gyűrű adott, például $\mathbb{Z}/n\mathbb{Z}$, $\operatorname{lnko}(n, 6) = 1$, akkor is definiálhatjuk a fenti műveleteket *parciálisan*, azaz ha az osztás elvégezhető; természetesen ekkor nem kapunk csoportot. Fontos azonban észrevennünk, hogy ha $\operatorname{lnko}(n, 4a^3 + 27b^2) = 1$, akkor bármely p prímosztójára n-nek modulo p is egy elliptikus görbét kapunk, és ha $\mathbb{Z}/n\mathbb{Z}$ felett el tudunk végezni egy összeadást, akkor bármely p prímosztójára n-nek, az eredmény 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.

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

A bizonyítás nehéz.

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

9.3. Gyakorlat. Rajzoltassuk ki az $y^2 = x^3 - 10x + 10$ elliptikus görbét a Maple segítségével.

9.4. Gyakorlat. Irjunk programot $\mathbb{Z}/n\mathbb{Z}$ feletti elliptikus görbén történő parciális műveletvégzésre. A pontokat reprezentálják számhármasok. Az utolsó koordináta ∞ esetén legyen 0, egyébként legyen 1.

10. Faktorizálás elliptikus görbékkel

Az alapgondolat egyszerű: választunk egy véletlen „elliptikus görbét” $\mathbb{Z}/n\mathbb{Z}$ felett egy P véletlen ponttal. Ez megtehető úgy, hogy választunk véletlen x, y és a értékeket, kiszámítjuk b-t, és ellenőrizzük az $\mathrm{lnko}(4a^3+27b^2, n) = 1$ feltételt. Ezután megpróbáljuk kiszámolni $k! \cdot P$-t, növekvő k értékekre. Ha nem sikerül, azaz ha egy osztás nem tudunk elvégezni, akkor az n egy osztóját találtuk meg. Ez az osztó rendszerint nem triviális. Ez azért van, mert ha a legkisebb olyan k-ra, amelyre a P rendje $\mathbb{Z}/p\mathbb{Z}$ felett valamely p prímosztójára n-nek osztja $k!$-t, akkor $k! \cdot P$ modulo p tekintve ∞ kell legyen. Ha ki tudtuk számítani $k! \cdot P$-t modulo n, akkor az csak ∞ lehet. Ekkor viszont ∞ kell legyen $\mathbb{Z}/q\mathbb{Z}$ felett is bármely más q prímosztójára n-nek. Ez nem valószínű, hogy modulo p és q is egyszerre következzék be.

Világos, hogy annak esélye, hogy modulo p a P pont rendje sima, azaz csak kis prímosztókat tartalmaz, nem n-től, csak p-től függ, és p növelésével csökken. A módszer a gyakorlatban 20–30 jegyű prímosztók megtalálására képes.

10.1. Kötegelt végrehajtás. Rendszerint 10–40 elliptikus görbét is ki kell próbálnunk, amíg találunk egy olyat, amelyre a véletlen P pont rendje modulo valamely p prímosztójára n-nek sima, azaz csak kis prímtényezőket tartalmaz. Jó ötlet a számításokat egyszerre végezni, ekkor ha valamelyik görbén az adott pont rendje sima, megállhatunk. Egy másik haszna ennek a kötegelt módnak az, hogy a modulo n vett $1/x$ és $1/y$ inverzek kiszámítását egyszerre végezhetjük $x(1/(xy))$ és $y(1/(xy))$ kiszámításával. Ezt a gondolatot több görbére is kiterjeszthetjük, kettes, majd négyes, nyolcas, stb. csoportokat képezve: egyetlen inverzet kiszámítva, a többi megkapható.

10.2. Szorzás egészekkel. A $P = (x, y)$ pont kétszeresének, $2P$-nek az első koordinátája
$$\frac{(3x^2+a)^2}{4y^2} - 2x = \frac{(x^2-a)^2 - 8bx}{4(x^3+ax+b)}.$$
Hasonlóan, $2i \cdot P$ első koordinátáját kiszámíthatjuk $i \cdot P$ első koordinátájából. Továbbá a $(2i+1) \cdot P$ pont első koordinátáját kiszámíthatjuk $i \cdot P$, $(i+1) \cdot P$ és P első koordinátáiból, legalábbis ha $x_i \neq x_{i+1}$ és $\mathrm{lnko}(x, n) = 1$ (ez a nem triviális eset) az alábbi módon: mivel
$$x_{2i+1} = \frac{(y_i - y_{i+1})^2}{(x_i - x_{i+1})^2} - x_{i+1} - x_i,$$
azt kapjuk, hogy
$$\begin{aligned} x_{2i+1}(x_i - x_{i+1})^2 &= (y_i - y_{i+1})^2 - (x_{i+1} + x_i)(x_i - x_{i+1})^2 \\ &= -2y_i y_{i+1} + 2b + (a + x_i x_{i+1})(x_i + x_{i+1}). \end{aligned}$$
Hasonlóan $P = P_{i+1} - P_i$-ből azt kapjuk, hogy
$$x(x_i - x_{i+1})^2 = 2y_i y_{i+1} + 2b + (a + x_i x_{i+1})(x_i + x_{i+1}).$$

Összeszorozva a két egyenletet, azt kapjuk, hogy

$$\begin{aligned} xx_{2i+1}(x_i - x_{i+1})^4 &= (2b + (a + x_i x_{i+1})(x_i + x_{i+1}))^2 \\ &\quad - 4(x_i^3 + ax_i + b)(x_{i+1}^3 + ax_{i+1} + b) \\ &= ((a - x_i x_{i+1})^2 - 4b(x_i + x_{i+1}))(x_i - x_{i+1})^2. \end{aligned}$$

Innen

$$x_{2i+1} = \frac{(a - x_i x_{i+1})^2 - 4b(x_i + x_{i+1})}{x(x_i - x_{i+1})^2}.$$

Ezek az összefüggések lehetővé teszik, hogy csak az első koordinátákkal dolgozzunk egészekkel történő szorzásnál. Ha a k szorzó bal szélső l bitje az i számot reprezentálja, akkor az l-edik lépésben az iP és $(i+1)P$ pontot számoljuk ki.

10.3. Projektív reprezentáció. Sokkal elegánsabb egy „elliptikus görbe" pontjait mint az adott egységelemes kommutatív gyűrű elemeiből képzett (X, Y, Z) hármasok osztályait reprezentálni. Azonosítsuk az (X, Y, Z) hármast mindazokkal a hármasokkal, amelyek előállnak (cX, cY, cZ) alakban valamely invertálható c-vel. A ∞ az $(0, 1, 0)$ hármas osztálya. Az elliptikus görbe egyenlete a

$$ZY^2 = X^3 + aXZ^2 + bZ^3$$

homogén egyenlet. A fenti számítások homogén koordinátákban a

$$\begin{aligned} X_{2i} &= (X_i^2 - aZ_i^2)^2 - 8bX_i Z_i^3, \\ Z_{2i} &= 4Z_i(X_i^3 + aX_i Z_i^2 + bZ_i^3), \\ X_{2i+1} &= Z\left((X_i X_{i+1} - aZ_i Z_{i+1})^2 - 4bZ_i Z_{i+1}(X_i Z_{i+1} + X_{i+1} Z_i)\right), \\ Z_{2i+1} &= X(X_{i+1} Z_i - X_i Z_{i+1})^2 \end{aligned}$$

alakba írhatók. Ezek a kifejezések lehetővé teszik, hogy elkerüljük az osztást, azaz a legnagyobb közös osztó számítását. Pontosabban, elég időnként ellenőrizni, hogy Z_i invertálható. Némi hatékonyságvesztés léphet fel, ha közben elérjük a ∞ elemet. Ez elkerülhető, ha visszalépést használunk.

10.4. Második lépcső. Mint a $p-1$ és a $p+1$ módszernél, egy második lépcsőt is beiktathatunk. Ennek során a $Q = k! \cdot P$ pontból indulva, $q_i \cdot Q$-t szamítjuk ki számos $q_i > k$ prímre. Ez megtehető rekurzívan, $(q_i \cdot Q) + (\delta_i \cdot Q)$ kiszámításával, ahol $\delta_i = q_{i+1} - q_i$. A $\delta_i \cdot Q$ pontokat táblázatban tárolhatjuk. Még jobb módszerek is léteznek. Lásd Montgomery [] és Montgomery–Silverman [] dolgozatát.

11. Prímteszt elliptikus görbékkel

Az elliptikus görbékkel történő prímtesztelés az alábbi tételen alapul:

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

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

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

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

$$Q = \frac{m}{s} P_p \in \mathbb{E}_p.$$

Ekkor $sQ = mP_p = (mP)_p = 0$, így Q rendje osztja s-et. Ha q egy prímosztója s-nek, akkor

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

Így Q rendje nem osztója s/q-nak. Mivel q tetszőleges volt, Q rendje s, így $|\mathbb{E}_p| \equiv 0 \pmod s$.

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

Az alábbi tétel elliptikus görbék szerkezetét írja le.

11.2. Tétel. *Legyen $p > 3$ egy prím. Ekkor bármely $\mathbb{E}$ elliptikus görbe $\mathbb{Z}/p\mathbb{Z}$ felett vagy ciklikus, vagy pedig egy m_1 és egy m_2 rendű ciklikus csoport direkt szorzata, ahol $m_1|m_2$ és $m_1|p - 1$.*

A bizonyítást nem tárgyaljuk.

11.3. A prímtesztek vázlata. Az n valószínű prím prím voltának bizonyításához, válasszunk egy „elliptikus görbét" $\mathbb{Z}/n\mathbb{Z}$ felett, és egy m számot, amelyre a görbe rendje m, — legalábbis ha n prím. Ha m felírható 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 egy valódi osztóját, ami nagyon valószínűtlen. Annak valószínűsége, hogy $k \cdot P = 0$ legyen, az előző tétel szerint kisebb, mint 1, ha n prím, mert ha $\mathbb{E}_n$ ciklikus, akkor csak f darab legfeljebb

f rendű elem van (hiszen a d rendű elemek száma egy ciklikus csoportv'ban $\varphi(d)$), ha pedig nem ciklikus, akkor $m_1 m_2 = f n_1$ és $m_1 | m_2$ miatt $m_1 | f$, így $m_1 \leq f$, és legfeljebb f^2 darab f rendű elem van, mert ha a direkt szorzat egy eleme legfeljebb f rendű, akkor mindkét koordinátája legfeljebb f rendű. Ebben az esetben válasszunk új pontot. Egyébként ellenőrizzük, hogy $n_1 \cdot (f \cdot P) = m \cdot P = 0$, aminek teljesülnie kell, ha n prím. Így P létezése bizonyítja, hogy n prím, ha n_1 prím. Most alkalmazzuk az eljárást n_1-re, stb.

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

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

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. $\mathbb{Q}(\sqrt{D})$ 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 $4n = (2x + yD)^2 - y^2 D$. 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 kvadratikus formákat egész a, b, c együtthatókkal. Egy ilyen kvadratikus 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 $c' = c - kb + k^2 a$. Világos, hogy ezen helyettesítések során nem változik meg a forma értékkészlete, azaz a $\{ax^2 + bxy + cy^2 : x, y \in \mathbb{Z}\}$ halmaz és a $\{a'x'^2 + b'x'y' + c'y'^2 : x', y' \in \mathbb{Z}\}$ halmaz megegyeznek. Azt is nyilvánvaló, hogy $b^2 - 4ac = b'^2 - 4a'c'$, azaz ez a mennyiség, a kvadratikus forma *diszkriminánsa* sem változik. Például a (2) jobb oldalán álló forma diszkriminánsa D. Egy kvadratikus formát *pozitív*nak nevezünk, ha $a > 0$, a diszkriminánsa pedig negatív. Világos, hogy ekkor c is pozitív. Egy kvadratikus 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 alakjuk. 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 kvadratikus 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. 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

$$n = n_0, a_0, b_0, m_0, P_0, f_0, n_1, a_1, b_1, m_1, P_1, f_1, n_2, a_2, b_2, m_2, f_2, n_3, \ldots$$

sorozat, ahol $n = n_0, n_1, n_2, n_3, \ldots$ 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

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

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 kiszámíthatók. 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.

12. Polinomfaktorizálás

12.1. Polinomfaktorizálás modulo egy prím. Az Atkin-teszttel kapcsolatban két probléma maradt. Az első D modulo n vett négyzetgyökének meghatározása, a másik pedig a H_D Hilbert polinom egy modulo n vett gyökének meghatározása. Mivel az első probléma speciális esete a másodiknak, csak az utóbbit tárgyaljuk. Általánosabban, legyen n prím, és tekintsük a $\mathbb{Z}/n\mathbb{Z}$ felett vett 1 főegyütthatójú p polinom

$$p(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$$

felbontásának megkeresését, ahol $p_1, \ldots, p_k$ különböző 1 főegyütthatójú, $\mathbb{Z}/n\mathbb{Z}$ felett irreducibilis polinomok, $e_1, \ldots, e_k$ pedig pozitív egész számok.

12.2. Visszavezetés négyzetmentes esetre. Az előző pont jelöléseivel, legyen

$$d(x) = \mathrm{lnko}(p(x), p'(x)).$$

Ha $d(x) = 1$, akkor p négyzetmentes kell legyen, mert $p_j(x)^{e_j-1}$ közös osztója p-nek és p'-nek. Ha $d(x) \neq 1$ és $d(x) \neq p(x)$, akkor d valódi faktora p-nek. Ekkor p faktorizálását $d(x)$ és $p(x)/d(x)$ faktorizálására vezettük vissza. Végül, ha $d(x) = p(x)$, akkor $p'(x) = 0$, így p-ben a p_i együtthatója x^i-nek nulla, ha i nem többszöröse n-nek. Ekkor $p(x) = q(x^n) = q(x)^n$; az utolsó összefüggéshez vegyük észre, hogy a binomiális tétel alapján

$$\big(q_1(x) + q_2(x)\big)^n = q_1(x)^n + q_2(x)^n,$$

továbbá ha

$$q(x) = q_0 + q_1 x + \cdots + q_m x^m,$$

akkor az előző összefüggés és a kis Fermat tétel alapján

$$q(x)^n = q_0^n + (q_1 x)^n + \cdots + (q_m x^m)^n = q(x^n).$$

12.3. Véges testek.

(1) *Egy $\mathbb{F}$ véges test elemeinek száma n^d valamely n prímre és d pozitív egész kitevőre;*

(2) *az $\mathbb{F}^*$ csoport ciklikus;*

(3) *ha p egy d-ed fokú, 1 főegyütthatójú, $\mathbb{Z}/n\mathbb{Z}$ felett irreducibilis polinom, akkor a d-nél alacsonyabb fokú $\mathbb{Z}/n\mathbb{Z}$ feletti polinomok modulo p egy n^d elemű testet alkotnak;*

(4) *egy d-ed fokú, $\mathbb{Z}/n\mathbb{Z}$ felett irreducibilis, 1 főegyütthatójú p polinom akkor és csakis akkor osztja $x^{n^m} - x$-et, ha $d \mid m$.*

Megjegyezzük, hogy megmutatható, minden $d > 0$ egészre létezik d-ed fokú, 1 főegyütthatójú, irreducibilis polinom $\mathbb{Z}/n\mathbb{Z}$ felett, és az összes n^d elemű testek izomorfak.

Bizonyítás. (1)-hez, a legkisebb n, amelyre $n\cdot 1 = 0$, prím, és $\mathbb{F}$ véges dimenziós a $\{0, 1, 2, \dots, n-1\}$ résztest felett. (2) ugyanúgy következik a 3.9 lemmából, mint ahogy a 3.10 tétel következett. (3)-hoz vegyük észre, hogy a d-nél alacsonyabb fokú polinomok modulo p, n egy egységelemes kommutatív gyűrűt alkotnak, amelyben minden nem nulla elem inverze megkereshető az euklidészi algoritmussal. Végül (4) bizonyításához vegyük észre, hogy bármely $q \in \mathbb{F}$-re $q^{n^d} = q$ modulo p, n. Innen ℓ szerinti teljes indukcióval

$$q^{n^{d\ell}} = q^{n^{d(\ell-1)}\cdot n^d} = \left(q^{n^{d(\ell-1)}}\right)^{n^d} = q^{n^d} = q.$$

Így $d|m$ esetén $x^{n^m} = x$. A megfordításhoz, legyen ξ egy generátora $\mathbb{F}^*$-nak. Azok az $\eta \in \mathbb{F}$-ek, amelyekre $\eta^{n^m} = \eta$, az összeadásra és a szorzásra zárt halmazt alkotnak. Így ha $x^{n^m} = x$, akkor ξ-re (amely egész együtthatós polinom x-ben), teljesül, hogy $\xi^{n^m} = \xi$. De ha $m = \ell d + r$, $0 \le r < d$, akkor $\xi^{n^m} = \xi^{n^{\ell d}\cdot n^r} = \xi^{n^r}$, ami ellentmondás, ha $r \neq 0$.

12.4. Faktorizálás különböző fokú faktorokra. Továbbra is $\mathbb{Z}/n\mathbb{Z}$ felett dolgozva, ahol n prím, az 1 főegyütthatós négyzetmentes p polinomra és $d = 1, 2, \dots$-re képezzük az $p_d(x) = \mathrm{lnko}\big(p(x), x^{n^d} - x\big)$ polinomokat. Ez a p összes d-ed fokú irreducibilis faktorainak szorzata lesz. Ezután p-t p/p_d-vel helyettesítjük, és a következő d-vel folytatjuk. Itt x^{n^d}-t csak modulo p, n számítjuk ki, $x^{n^{d-1}}$ modulo p, n felhasználásával. Az eljárás véget ér, ha $2d$ nagyobb, mint p foka.

12.5. Hasítás. Az előző lépés után feladatunk olyan $\mathbb{Z}/n\mathbb{Z}$ feletti, 1 főegyütthatós p_d polinomok faktorizálása, amelynek faktorai d-ed fokúak és különbözők. A p_d-t az alábbi valószínűségi algoritmussal „hasíthatjuk”, ha n páratlan: Legyen t egy véletlen polinom. Ekkor

$$t(x)\left(t(x)^{(n^d-1)/2} - 1\right)\left(t(x)^{(n^d-1)/2} + 1\right) = t(x)^{n^d} - t(x),$$

és a bal oldalon szereplő polinom osztható p_d-vel. Jó esély van arra, hogy a jobb oldalon álló szorzatnak p_d faktorai nem mind ugyanazt a tényezőjét osztják. Így p és a jobb oldalon álló tényezők legnagyobb közös osztóit képezve, p_d nagy valószínűséggel hasítható.

13. Az AKS-teszt

13.1. Az AKS-teszt alapötlete. 2002-ben Agrawal, Kayal és Saxena indiai informatikusok egy olyan algoritmust találtak, amely bármely n természetes számra képes eldönteni, hogy prím-e, és futásideje $O(\lg^{13} n)$. Az alapötlet a következő: ha s és n relatív prímek, akkor $(x+s)^n \equiv x^n + s \pmod{n}$ pontosan akkor teljesül, ha n prím; valóban, ha n prím, akkor nyilván teljesül az összefüggés, másrészt, ha $p^k \mid n$ de $p^{k+1} \nmid n$, akkor

$$p^k \nmid \binom{n}{p} = \frac{n(n-1)\cdots(n-p+1)}{1\cdot 2\cdots p}$$

és relatív prím s^{n-p}-hez, így x^p együtthatója nem nulla. Vizsgáljuk az

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

kongruenciát, de sok különböző s-re.

13.2. AKS-tétel [3]. *Ha $n \in \mathbb{N}^+$, $q, r \in \mathbb{P}$, $S \subset \mathbb{Z}$ véges, $q|r-1$, és $n^{(r-1)/q} \bmod r \notin \{0,1\}$, továbbá* $\operatorname{lnko}(n, s-s') = 1$, *ha $s, s' \in S$, $s \neq s'$ és*

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

akkor n prímhatvány.

13.3. Megjegyzések. (1) Megmutatják, hogy van olyan c, hogy $c\lg^6 n$-ig van olyan r, amelyre $r-1$-nek van olyan q prímosztója, hogy $q \geq 4\sqrt{r}\lg n$ és q osztja az n-nek $\bmod r$ 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) Mivel

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

és ha

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

akkor

$$\frac{r}{2}\lg\frac{2\natural(S)}{r} \approx 2\sqrt{r}\lg n,$$

azt kapjuk, hogy

$$\sqrt{r}\lg\frac{2\natural(S)}{r} \approx 4\lg n, \quad \lg\frac{2\natural(S)}{r} \approx \frac{1}{2} = \lg\sqrt{2}, \quad \natural(S) \approx \frac{1}{\sqrt{2}}r.$$

(3) Hatványteszt: ha $n = m^e$ és $2^k \leq n < 2^{k+1}$, ahol $k \approx \lg n$ és bináris kereséssel könnyű megtalálni, akkor $e \leq k$, $k \leq e\lg m < k+1$, amiből $\lfloor k/e \rfloor \leq \lg m < \lceil (k+1)/e \rceil$, így m-et bináris kereséssel könnyű megtalálni.

(4) A tesztet tovább élesítették $r \approx 0.01\lg^2 n$-ig, és $\natural(S)$ is csökkenthető. Ezzel a tesztet több milliószorosra gyorsították, sebessége $\lg^{6+o(1)} n$.

(5) Rekordokra nem alkalmas, tárkorlátos.

13.4. Bernstein tétele [6]. *Legyenek n, d és e pozitív egészek, c és c_- egészek, legyen $f \in \mathbb{Z}_n[y]$ egy d-ed fokú főpolinom. Legyen R a $\mathbb{Z}_n[y]/(f)$ gyűrű, $r \in R$, $S \subset R$. Tegyük fel, hogy*

(1) $e | n^d - 1$;

(2) $r^{n^d-1} = 1$ *az R-ben;*

(3) $r^{(n^d-1)/q} - 1$ *egység R-ben az e bármely q prímosztójára;*

(4) minden $s \in S$ egység R-ben;

(5) $s^e - s'^e$ *egység R-ben, ha $s, s' \in S$, $s \neq s'$;*

(6) $s^e - r$ *egység R-ben minden $s \in S$-re;*

(7) $e > c \geq c_- \geq 0$;

(8)
$$\binom{e \cdot \natural(S)}{c_-}\binom{c}{c_-}\binom{e \cdot \natural(S) - c_- + e - 1 - c}{e - 1 - c} \geq n^{d\lceil\sqrt{e/3}\rceil};$$

(9) $(x - s)n^d = r^{(n^d-1)/e}x - s$ *az $R[x]/(x^e - r)$ gyűrűben minden $s \in S$-re.*

Ekkor n prímhatvány.

13.5. Megyjegyzések. (1) a d várható értéke nagyon kicsi, gyakorlatilag d mindig 1, és
$$d^2\lceil\lg n\rceil^2 < e < (d+1)d^2\lceil\lg n\rceil^2$$
található, ekkor $\natural(S) = 1$, de már $e \approx 0.01\lg^2 n$-re is $\natural(S)$ elég kicsi.

(2) A c és c_- optimizációs paraméterekre célszerűen $c \approx e/2$ és
$$c_- \approx \frac{\natural(S)}{\natural(S) + 2 + \sqrt{\natural(S)^2 + 1}}e.$$

V. SZITA MÓDSZEREK

A faktorizálás „nagyágyúi” a különböző szita módszerek. Ha a faktorizálandó összetett szám faktorai mind nagyok, akkor ezek a legjobb ismert módszerek. Természetesen előbb egyszerűbb módszerek (próbaosztás, Pollard ϱ és $p-1$ módszere, esetleg Williams módszere, illetve elliptikus görbék) segítségével érdemes leválasztani a „kis” faktorokat, mivel a szita módszerek ugyanannyi idő alatt találnak meg egy kis faktort, mint egy nagyot. Jelenleg a szita módszerek teljesítőképessége 200-nál több jegyű számok faktorizálását is lehető teszi, sőt, nagyobbakét is, ha a szám speciális alakú.

14. A szita módszerek alapjai

14.1. Dixon véletlen négyzet módszere. Ez még nem igazán szita módszer, de az alapgondolatok egy részét megvilágítja. Fermat módszerénél n faktorizálásához olyan x, y egészeket kerestünk, amelyekre $n = x^2 - y^2$. Ezt a feltételt enyhíthetjük: ha véletlen x, y egészekre $n \mid x^2 - y^2 = (x-y)(x+y)$, akkor jó esélyünk van arra, hogy n faktorai megoszlanak $x - y$ és $x + y$ között, így mindkét szám legnagyobb közös osztóját kiszámítva n-el, azt hasíthatjuk. Elég tehát néhány ilyen x, y pár találni. Dixon módszerénél először választunk egy $K > 0$ korlátot. Ezután véletlen m értékekre kiszámítjuk az $r(m) = m^2 \bmod n$ maradékot, és megpróbáljuk azt faktorizálni. Azokat az m értékeket, amelyekre az $r(m)$ maradék K-sima, azaz minden faktora kisebb, mint K, eltároljuk, $r(m)$ prímfelbontásával együtt.

Legyen $r(m_i)$ prímfelbontásában a $p_j < K$ prím kitevője $e_{i,j}$. Az x^2-et *bizonyos* $r(m_i)$-k szorzataként fogjuk keresni. Ha sikerül elérni, hogy ez a szorzat négyzetszám legyen, akkor, mivel tetszőleges m_i^2-k szorzata mindig négyzetszám, a megfelelő m_i-k szorzatát véve y-nak, $x^2 \equiv y^2 \pmod n$ teljesül. Hogy az $r(m_i)$-k szorzata négyzetszám legyen, azt kell elérnünk, hogy $\sum_i e_{i,j}$ páros legyen minden j-re. Jelölje e_i azt a vektort, amelynek j-edik koordinátája $e_{i,j} \bmod 2$. Bizonyos $r(m_i)$ számok szorzata pontosan akkor négyzetszám, ha a megfelelő e_i vektorok modulo 2 vett összege a nullvektor. Tehát a megfelelő $r(m_i)$ maradékok kiválasztásához olyan e_i vektorokat kell keresni, amelyek modulo 2 vett összege nullvektor. Ilyen rendszer mindig létezik, ha az $r(m_i)$-k száma nagyobb, mint a p_j-k száma, mert ekkor az e_i vektorok modulo 2 lineárisan függőek. Minél nagyobb a különbség, annál több ilyen kombinációt találhatunk modulo 2 végzett Gauss-eliminációval, vagy más lineáris algebrai módszerrel.

Természetesen K választása kritikus. Ha K túl kicsi, akkor nagyon kicsi az esélye, hogy az $r(m)$ maradék K-sima legyen. Ha K túl nagy, akkor a p_j prímek száma lesz túl nagy. Legyen $L_n(\beta) = e^{\beta\sqrt{\ln n \ln\ln n}}$. Dixon algoritmusa pontosan analizálható, és megmutatható, hogy ha Gauss-eliminációt használunk, akkor K-t nagyságrendben $L_n(1/2)$-nek érdemes választani, a futásidő nagyságrendben $L_n(3/2)$, a tárigény pedig nagyságrendben $L_n(1)$ lesz. Ha kihasználjuk, hogy az $(e_{i,j})$ mátrix ritka, akkor K-t nagyságrendben $L_n(1/\sqrt{2})$-nek érdemes választani, és nagyságrendben $L_n(\sqrt{2})$ idő és $L_n(1/\sqrt{2})$ tár szükséges.

A módszer további finomításával elérhetjük, hogy az $r(m)$ maradékok nagyságrendje ne az n, hanem csak $n^{2/3}$ nagyságrendjével egyezzen meg, de eloszlásuk még mindig véletlenszerű legyen. Így egy még mindig pontosan analizálható, de gyorsabb módszerhez juthatunk. A gyakorlatban jobb azonban lemondani a pontos analizálhatóságról, és minél kisebbre leszorítani az $r(m)$ maradékok nagyságrendjét. Egy ilyen módszer a lánctörtek felhasználásán alapul.

14.2. Lánctörtek. Legyenek $0 < u_1 < u_0$ egészek, ekkor

$$\begin{aligned} u_1/u_0 &= 1/(u_0/u_1) = 1/(a_1 + u_2/u_1) = 1/(a_1 + 1/(u_1/u_2)) \\ &= 1/(a_1 + 1/a_2 + u_3/u_2)) = \dots, \end{aligned}$$

ahol $a_i = \lfloor u_{i-1}/u_i \rfloor$ és $u_{i+1} = u_{i-1} \bmod u_i$. Vegyük észre a kapcsolatot az euklidészi algoritmussal. Általánosabban, legyen $0 < x < 1$, $x_0 = x$, és ha $x_n \neq 0$, legyen $a_{n+1} = \lfloor 1/x_n \rfloor$ és $x_{n+1} = 1/x_n - a_{n+1}$. Vezessük be a lánctörtekre a

$$//a_1, \dots, a_n// = 1/(a_1 + 1/(a_2 + \dots + 1/a_n)\dots)$$

jelölést. Ekkor

$$x = //a_1, \dots, a_{n-1}, a_n + x_n//.$$

Definiáljuk a k_n polinomokat, az úgynevezett *kontinuáns*okat (a k_n pontosan n változós): legyen $k_n(a_1, \dots, a_n) = 1$, ha $n = 0$, legyen $k_1(a_1, \dots, a_n) = a_1$, ha $n = 1$, és indukcióval legyen $k_n(a_1, a_2, a_3, \dots, a_n) = a_1 k_{n-1}(a_2, a_3, \dots, a_n) + k_{n-2}(a_3, \dots, a_n)$. Teljes indukcióval azonnal adódik az Euler által felfedezett összefüggés, hogy $k_n(a_1, \dots, a_n)$ az összes olyan szorzatok összege, amelyek előállíthatók úgy, hogy az $a_1 a_2 \cdots a_n$ szorzatból néhányszor egymás után törlünk két egymás melletti tényezőt. (Összesen F_n ilyen szorzat van, ahol F_n az n-edik Fibonacci szám). Ebből azonnal következik a $k_n(a_1, \dots, a_n) = k_n(a_n, \dots, a_1)$ szimmetria.

A lánctörtek felírhatók a kontinuánsok segítségével: teljes indukcióval könnyen adódik, hogy

$$//a_1, \dots, a_n// = \frac{k_{n-1}(a_2, a_3, \dots, a_n)}{k_n(a_1, a_2, \dots, a_n)}$$

Az x lánctört kifejtése nyilván akkor és csak akkor véges, ha x racionális. Egyébként x nyilván $//a_1, \dots, a_n//$ és $//a_1, \dots, a_{n-1}, a_n + 1//$ között van. Megmutatjuk, hogy $//a_1, \ldots, a_n//$ igen gyorsan konvergál x-hez, ha $n \to \infty$. Ennek belátásához szükségünk van a kontinuánsokra érvényes

$$k_n(a_1, \ldots, a_n)k_n(a_2, \ldots, a_{n+1}) - k_{n+1}(a_1, \ldots, a_{n+1})k_{n-1}(a_2, \ldots, a_n) = (-1)^n$$

összefüggésre, ami indukcióval könnyen adódik, ha a jobb oldalon az a_1-et tartalmazó kontinuánsokra alkalmazzuk a definíciót. Most

$$\begin{aligned}
|x - //a_1, \ldots, a_n//| &= |//a_1, \ldots, a_{n-1}, a_n + x_n// - //a_1, \ldots, a_n//| \\
&= |//a_1, \ldots, a_n, 1/x_n// - //a_1, \ldots, a_n//| \\
&\le |//a_1, \ldots, a_n, a_{n+1}// - //a_1, \ldots, a_n//| \\
&= \left| \frac{k_n(a_2, \ldots, a_n, a_{n+1})}{k_{n+1}(a_1, a_2, \ldots, a_n, a_{n+1})} - \frac{k_{n-1}(a_2, \ldots, a_n)}{k_n(a_1, \ldots, a_n)} \right| \\
&\le \frac{1}{k_{n+1}(a_1, \ldots, a_{n+1})k_n(a_1, \ldots, a_n)}.
\end{aligned}$$

14.3. Kvadratikus irracionális számok lánctört alakja. Legyen d olyan pozitív egész szám, amely nem teljes négyzet, u pedig egész szám úgy, hogy $x = \sqrt{d} - u$-ra $0 < x < 1$ teljesüljön. Legyen $u_0 = u$, $v_0 = 1$ és indukcióval legyen $v_{n+1} = (d - u_n^2)/v_n$, $a_{n+1} = \lfloor(\sqrt{d} + u_n)/v_{n+1}\rfloor$, $u_{n+1} = a_{n+1}v_{n+1} - u_n$. Teljes indukcióval megmutatjuk, hogy ekkor az a_n egészek az x lánctört kifejtésének jegyei és $x_n = (\sqrt{d} - u_n)/v_n$.

Mivel $x_0 = \sqrt{d} - u$, így

$$\frac{1}{x_0} = \frac{1}{\sqrt{d} - u} = \frac{\sqrt{d} + u}{d - u^2} = \frac{\sqrt{d} + u_0}{v_1},$$

így $n = 1$-re minden állítás teljesül.

Indukcióval,

$$\frac{1}{x_n} = \frac{1}{\sqrt{d} - u_n} = \frac{\sqrt{d} + u_n}{d - u_n^2} = \frac{\sqrt{d} + u_n}{v_{n+1}},$$

amiből $a_{n+1} = \lfloor(\sqrt{d} + u_n)/v_{n+1}\rfloor$ és

$$x_{n+1} = \frac{1}{x_n} - a_{n+1} = \frac{\sqrt{d} + u_n - a_{n+1}v_{n+1}}{v_{n+1}} = \frac{\sqrt{d} - u_{n+1}}{v_{n+1}}.$$

Második lépésként megmutatjuk, hogy $0 < u_n < \sqrt{d}$ és $0 < v_n < 2\sqrt{d}$ egészek és $v_n \mid d - u_n^2$. Ez is nyilván teljesül $n = 1$-re. Indukcióval, mivel $v_n \mid d - u_n^2$, kapjuk, hogy v_{n+1} egész, és mivel $0 < u_n < \sqrt{d}$, azt is kapjuk, hogy $v_{n+1} > 0$. Mivel mint láttuk, $1/x_n = (\sqrt{d} + u_n)/v_{n+1} > 1$, következik, hogy $v_{n+1} < \sqrt{d} + u_n < 2\sqrt{d}$. Hasonlóan, mivel mint láttuk $x_{n+1} = (\sqrt{d} - u_{n+1})/v_{n+1}$, kapjuk, hogy

$0 < u_{n+1} < \sqrt{d}$; valóban $x_{n+1} < 1$ miatt elég a $v_{n+1} > \sqrt{d}$ esettel foglalkozni. Ekkor $u_{n+1} = a_{n+1}v_{n+1} - u_n \geq v_{n+1} - u_n > \sqrt{d} - u_n > 0$. Végül

$$d - u_{n+1}^2 = d - (a_{n+1}v_{n+1} - u_n)^2 = d - u_n^2 + a_{n+1}^2 v_{n+1}^2 + 2u_n a_{n+1} v_{n+1},$$

kapjuk, hogy $v_{n+1} \mid d - u_{n+1}^2$.

Végül megmutatjuk, hogy ha $p_n = k_{n-1}(a_2, \ldots, a_n)$ és $q_n = k_n(a_1, \ldots, a_n)$, akkor

$$(p_n + uq_n)^2 - dq_n^2 = (-1)^{n+1} v_{n+1}.$$

Ez $n = 1$-re könnyen kiszámítható, ha felhasználjuk v_2, majd v_1 és u_1 definícióját. Az indukciós lépéshez azt kell belátni, hogy $y = -\sqrt{d} - u$ jelöléssel

$$-\frac{v_{n+1}}{v_n} = \frac{(q_n x - p_n)(q_n y - p_n)}{(q_{n-1}x - p_{n-1})(q_{n-1}y - p_{n-1})}.$$

Ennek igazolásához először is vegyük észre, hogy az

$$x = //a_1, \ldots, a_n, 1/x_n//$$

összefüggésből

$$x = \frac{k_n(a_2, \ldots, a_n, 1/x_n)}{k_{n+1}(a_1, \ldots, a_n, 1/x_n)} = \frac{p_n/x_n + p_{n-1}}{q_n/x_n + q_{n-1}}.$$

Ebből

$$x_n = -\frac{q_n}{q_{n-1}} \frac{x - p_n/q_n}{x - p_{n-1}/q_{n-1}}.$$

Ha most az $y_0 = y$, $y_n = (-\sqrt{d} - u_n)/v_n$ sorozatot tekintjük, akkor teljes indukcióval könnyen igazolható, hogy

$$y = //a_1, \ldots, a_n, 1/y_n//.$$

Ebből a fentiekhez hasonlóan azt kapjuk, hogy

$$y_n = -\frac{q_n}{q_{n-1}} \frac{y - p_n/q_n}{y - p_{n-1}/q_{n-1}}.$$

Az x_n-re és y_n-re kapott kifejezéseket összeszorozva, kapjuk az indukciós lépés igazolásához szükséges összefüggést.

Végül levezetünk még egy összefüggést, megmutatjuk, hogy

$$v_{n+1} = a_n(u_{n-1} - u_n) + v_{n-1}.$$

Valóban,

$$\begin{aligned} v_{n+1} = \frac{d - u_n^2}{v_n} &= \frac{v_{n-1}(d - (a_n v_n - u_{n-1})^2)}{d - u_{n-1}^2} \\ &= v_{n-1} + a_n \frac{v_{n-1}v_n}{d - u_{n-1}^2}(2u_{n-1} - a_n v_n) = v_{n-1} + a_n(u_{n-1} - u_n). \end{aligned}$$

14.4. Faktorizálás lánctörtekkel. Ez az algoritmus olyan (p, v) párokat „termel”, amelyekre $p^2 \equiv \pm v \pmod{n}$, és v „kicsi”. A természetes $d = n$ választás helyett a $d = kn$ választással élünk, ahol k kis természetes szám; a k paraméter szabad választása több lehetőséget ad. Az algoritmus a következő:

(1) [Inicializálás.] Legyen $d \leftarrow kn$, $r \leftarrow \lfloor\sqrt{d}\rfloor$, $r' \leftarrow 2r$, $u \leftarrow u' \leftarrow r'$, $v \leftarrow 1$, $v' \leftarrow d - r^2$, $p \leftarrow r$, $p' \leftarrow 1$, $a \leftarrow 0$, $s \leftarrow 0$. Az algoritmus során u, u', v, v', p, p', a, s értéke rendre $r+u_i$, $r+u_{i-1}$, v_i, v_{i-1}, $(p_i+rq_i) \bmod n$, $(p_{i-1}+rq_{i-1}) \bmod n$, a_i és $i \bmod 2$, az előző pont jelöléseivel. Mindig $0 < v \le u \le r'$, így u, u', v, v' számjegyeinek száma alig több mint fele n számjegyei számának.

(2) [Új u, v és s.] Legyen $t \leftarrow v$, $v \leftarrow a(u'-u)+v'$, $v' \leftarrow t$, $a \leftarrow \lfloor u/v \rfloor$, $u' \leftarrow u$, $u \leftarrow r' - (u \bmod v)$, $s \leftarrow 1 - s$.

(3) [Próbaosztás.] Most $p^2 - knq^2 = (-1)^s v$ valamely q egészre, azaz $p^2 \equiv (-1)^s v \pmod{n}$. Megpróbáljuk v-t faktorizálni, ha sikerül, eltároljuk.

(4) [Új p.] Ha $v \ne 1$, akkor legyen $t \leftarrow p$, $p \leftarrow (ap+p') \bmod n$, $p' \leftarrow t$, és menjünk (2)-re, egyébként vége.

Megmutatható, hogy az első v érték, ami másodszor fordul elő, csak $v = 1$ lehet. Ha ez hamar bekövetkezik (ami ritka eset), akkor új k-t választva, folytathatjuk a (p, v) párok gyűjtését.

14.5. A kvadratikus szita. Az alapgondolat, hogy az n szám faktorizálásához a $q(x) = (x+b)^2 - n$ polinom értékeit tekintjük, ahol $x \in [-m, m]$ egész szám, és $b = \lceil\sqrt{n}\rceil$, hogy a polinom értékei „kicsik” legyenek: a legnagyobb érték $(m+b)^2 - n \approx 2m\sqrt{n}$. Itt is választunk egy B „simasági határt”, az ennél kisebb prímek tartoznak az F „faktorbázisba”. Pontosabban, mivel $p|(x+b)^2 - n$ azzal ekvivalens, hogy $(x+b)^2 \equiv n \pmod{p}$, elég azokat a $p < B$ prímeket bevenni, amelyekre n kvadratikus maradék. Látszólag gondot okoz, hogy $x < 0$ esetén $q(x)$ negatív. Ezen azonban könnyen segíthetünk: a -1-et is bevesszük a faktorbázisba.

Hogy a faktorbázis minél több elemet tartalmazzon, esetleg érdemes lehet n-et kn-nel helyettesíteni, úgy választva a kis k szorzót, hogy minél több kis prím legyen, amelyre kn kvadratikus maradék. (A továbbiakban ezt az új értéket jelöljük n-nel.) Például 2 pontosan akkor kerül be a faktorbázisba, ha $n \equiv 1 \pmod{8}$.

A kvadratikus szita legfontosabb gondolata, hogy szitálással kiszűrjük azokat az x-eket, amelyekre $q(x)$ (legalábbis nagy valószínűséggel) „sima”, azaz a faktorbázis felett faktorizálható. Ez úgy történik, hogy minden $p \in F$-re egy szitatábla kezdetben kinullázott, x-nek megfelelő helyéhez hozzáadjuk $\log(p)$ értékét, ha $p|q(x)$; a logaritmus alapja tetszőleges. (Még jobbnak tűnik a

$$\frac{p}{p-1}\log p = \log p\Big(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\Big)$$

értéket hozzáadni, abból a meggondolásból, hogy ha $p|q(x)$, akkor $1/p$ valószínűséggel $p^2|q(x)$, és $1/p^2$ valószínűséggel $p^3|q(x)$, stb.) Ezek a helyek két számtani sorozatot alkotnak, mindkettő differenciája p, kezdőértékük pedig $-b \pm \sqrt{n} \bmod p$. Ha egy x-re a logaritmusok összege eléri $\log\big|q(x)\big|$ értékét, akkor $q(x)$ biztosan sima, és nagy valószínűséggel ez a helyzet akkor is, ha csak megközelíti ezt az értéket. (Általában elég a logaritmusok kerekített értékeinek összegét egy, legfeljebb két bájton gyűjteni.) Ezekre az x-ekre próbaosztással vagy más módon fektorizáljuk $q(x)$ értékét. Ha sikerült néhánnyal több, a faktorbázis feletti teljes faktorizálást gyűjteni, mint a faktorbázis elemeinek száma, akkor ugyanúgy eljárva, mint Dixon módszerénél, „hasíthatjuk” n-et.

Egy további finomítás a „nagy prím változat”: ha a próbaosztással nem sikerül teljesen faktorizálni a faktorbázis felett (egy úgynevezett „teljes relációt” kapni), akkor rendszerint $q(x)$-ből egy B-nél nem kisebb nagy prím marad vissza. Az ilyen felbontásokat hívjuk „parciális relációknak”. Ha két vagy több parciális relációban ugyanaz a nagy prím, akkor az egyikkel (célszerűen azzal, amelyikben a második legnagyobb prím a legkisebb) végigszorozva a többit, azokból teljes relációt kaphatunk, mert a nagy prím négyzeten lesz. Hogy több parciális relációt gyűjthessünk, célszerű megnövelni a $\log\lvert q(x)\rvert$ és a logaritmusok összege között megtűrt különbség értékét; persze nem túlságosan, mert ha a „nagy prím” túlságosan nagy, akkor már kicsi a valószínűsége, hogy mégegyszer előfordul. További finomítás, hogy két vagy akár három „nagy prím”-et is megengedünk. Például két nagy prímből az egyiket (összeszorzással) kiküszöbölve olyan parciális relációt kapunk, amiben még két nagy prím lesz, de azok már kisebbek, ha pedig sikerül olyan parciális relációval szorozni, amelyben csak egy nagy prím van, akkor a szorzatokban már csak egy nagy prím lesz. (A megvalósításhoz célszerű verem struktúrát használni.) Mivel így csak az lényeges, hogy a logaritmusok összege és $\log\lvert q(x)\rvert$ között a különbség ne legyen túl nagy, az utóbbit egyszerűen a $\log\max_{x\in[-m,m]}\lvert q(x)\rvert$ konstanssal helyettesítjük, és egyszerűen minden olyan x-re próbaosztunk, amelyre a logaritmusok összege eléri ennek a T-ed részét, ahol a T „treshold” érték 1,5-től 2,6-ig nő, ahogy a decimális jegyek száma nő 24-től 66-ig.

14.6. Többpolinomos kvadratikus szita. A kvadratikus szitának nagy hátránya, hogy ha nem sikerült elég relációt gyűjteni, akkor a $[-m,m]$ intervallum méretét meg kell növelni, és kezdhetjük elölről a szitálást. Célszerűbb több $x\mapsto(ax+b)^2-n$ alakú polinomot használni, különböző a,b értékekkel; a faktorbázis mindig ugyanaz. (Természetesen így a szitálás könnyen párhuzamosítható, és a belső tár igény is jóval kisebb lehet.) Célszerű lesz b értékét úgy választani, hogy b^2-n többszöröse legyen a-nak, azaz $b^2-n=ac$ teljesüljön; a finom ötlet ebben, hogy ekkor a polinom alakja $x\mapsto a(ax^2+2bx+c)$, és ha a-t egy d (valószínű) prím négyzetének választjuk, akkor csak a $q(x)=ax^2+2bx+c$ polinom értékének kell simának lenni. Mint majd látni fogjuk, elérhetjük, hogy $|2b|<|a|$ és $|a|\ll\sqrt{n}$ legyen. Ilyen feltételek mellett $ac\approx -n$ és így ha a pozitív, akkor c negatív. Az a értékének célszerű választásához vegyük észre, hogy a $[-m,m]$ intervallum végpontjaiban q értéke $\approx am^2+c$, a középpontjában pedig $\approx c$. Hogy a q polinom abszolút értéke mindenütt lehetőleg kicsi legyen, célszerű, ha $am^2+c\approx|c|$, azaz $am^2+c\approx -c$, ahonnan $a\approx\sqrt{2n}/m$ és $c\approx m\sqrt{n/2}$.

Egy $d\approx(2n/m^2)^{1/4}$ valószínű prímet választva, amelyre $(d|n)=1$ és $d\equiv 3 \pmod 4$, a következőképpen járhatunk el: Legyen $a=d^2$, és $h_0\equiv n^{(d-3)/4} \pmod d$, továbbá legyen $h_1\equiv nh_0\equiv n^{(d+1)/4} \pmod d$. Ekkor

$$h_1^2\equiv n\cdot n^{(d-1)/2}\equiv n,$$

mivel $(d|n)=1$. Legyen $h_2 \pmod d$ az $(n-h_1^2)/d$ és a $2h_1$ modulo d vett inverzének szorzata; ez utóbbi számolásához vegyük észre, hogy h_0 a h_1 modulo d vett inverze. Végül legyen

$$b \equiv h_1 + h_2 d \pmod{a};$$

erre

$$b^2 \equiv h_1^2 + 2h_1 h_2 d + h_2 d^2 \equiv n \pmod{a}.$$

Megfelelően választva h_1-et és h_2-t az adott maradékosztályból, elérhetjük, hogy $|2b| < a$ legyen. A c is kiszámolható, de nincs is rá szükség: mivel

$$q(x) = \frac{(ax+b)^2 - n}{a}$$

és a relatív prím minden $p \in F$-hez, a $q(x) \equiv 0 \pmod{p}$ egyenlet ekvivalens az $(ax+b)^2 \equiv n \pmod{p}$ egyenlettel, aminek megoldásai $x \equiv (-b \pm \sqrt{n})/a$.

14.7. Példa. A következő példa egy futtatást mutat be. Egy 267 bites összetett számot kívánunk faktorizálni. A szita intervallum 12 darab 32768 hosszú blokkból áll, tehát 393216 egységet tartalmaz. A B „simasági korlát” 1300967, a faktorbázis 50294 prímet tartalmaz. A próbaosztás 27 bitig történik. A nagy prím korlát 128795733 (26 bit). Összesen 25952 „teljes” relációt sikerült közvetlenül találni, 24462 teljes reláció pedig a parciális relációkból adódott, így a teljes mátrix méret 50294×50414, amelyet 35750×35862-re lehetett csökkenteni. 15 nem triviális függőség adódott. Egy polinomra átlag 10 reláció esett. A teljes futásidő egy 1.6 GHz-es UltraSPARC III gépen 35'39” volt, a memóriafelhasználás 8 MB.

IRODALOM

[1] L. M. Adleman, *On Constructing A Molecular Computer*, Draft (1995), 1-20.

[2] L. M. Adleman, M.-D. A. Huang, *Primality Testing and Abelian Varieties Over Finite Fields.* Springer Verlag, LNM 1512 (1992).

[3] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P.* (2002) URL:`http://www.cse.iitk.ac.in /news/primality.html`

[4] A. V. Aho, J. E. Hopcroft, J. D. Ullman, *The Design and Analysis of Computer Algorithms.* Addison-Wesley, 1974. Magyarul: *Számítógép-algoritmusok tervezése és analízise*, Műszaki Könyvkiadó, 1982.

[5] A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. of Computation *61* (1993), 29-68.

[6] D. J. Bernstein, *Proving primality in essentially quartic random time.* Math. Comp. 76 (2007), pp. 389–403.

[7] D. J. Bernstein, A. K. Lenstra, *A general number field sieve implementation*, A. K. Lenstra, H. W. Lenstra, Jr. (Eds.): The development of the number field sieve, Springer-Verlag, LNM 1554, 1993, 103-126.

[8] D. Boneh, R. J. Lipton, *Quantum Cryptanalysis of Hidden Linear Functions*, D. Coppersmith (Ed.): Advances in Cryptology — CRYPTO'95, Springer-Verlag, LNCS 963, 1995.

[9] D. M. Bressoud, *Factorization and Primality Testing.* Springer-Verlag, 1989.

[10] J. Buhler, H. W. Lenstra, Jr., C. Pomerance, *Factoring integers with the number field sieve*, A. K. Lenstra, H. W. Lenstra, Jr. (Eds.): The development of the number field sieve, Springer-Verlag, LNM 1554, 1993, 50-94.

[11] H. Cohen, *A course in computational algebraic number theory*, Springer Verlag, 1993.

[12] T. H. Cormen, C. E. Leiserson, R. L. Rivest, *Algoritmusok*, Műszaki Könyvkiadó, 1997.

[13] R. E. Crandall, *Topics in Advanced Scientific Computations.* Springer TELOS, 1996.

[14] R. Crandall, J. Doenias, C. Norrie, J. Young, *The twenty-second Fermat number is composite*, Math. Comp. *64* (1995), 863–868.

[15] F. Damm, F.-P. Heider, G. Wambach, *MIMD-Factorisation on Hypercubes*, A. De Santis (Ed.): Advances in Cryptology — EUROCRYPT'94, Springer-Verlag, LNCS 950, 1994, 400-409.

[16] B. Dodson, A. K. Lenstra, *NFS with Four Large Primes: An explosive Experiment*, D. Coppersmith (Ed.): Advances in Cryptology — CRYPTO'95, Springer-Verlag, LNCS 963, 1995, 372-385.

[17] K.-H. Indlekofer, *Zahlentheorie. Uni-Taschenbücher 688.* Birkhäuser Verlag, 1978.

[18] K.-H. Indlekofer, A. Járai, *Largest known twin primes*, Math. Comp. *65* (1996), no. 213, 427-428.

[19] K.-H. Indlekofer, A. Járai, *Largest known twin primes and Sophie Germain primes*, Math. Comp. (1998) (to appear).

[20] D. E. Knuth, *Fundamental Algorithms. Vol. 1 of The Art of Computer Programming*, Addison-Wesley, 1968.

[21] D. E. Knuth, *Fundamental Algorithms. Vol. 1 of The Art of Computer Programming. Second edition.* Addison-Wesley, 1981. Magyarul: *A számítógép-programozás művészete 1. Alapvető algoritmusok.* Műszaki Kónyvkiadó, 1987, 1994.

[22] D. E. Knuth, *Fundamental Algorithms. Vol. 1 of The Art of Computer Programming. Third edition.* Addison-Wesley, 1997.

[23] D. E. Knuth, *Seminumerical algorithms. Vol. 2 of The Art of Computer Programming*, Addison-Wesley, 1969.

[24] D. E. Knuth, *Seminumerical algorithms. Vol. 2 of The Art of Computer Programming. Second edition*, Addison-Wesley, 1980. Magyarul: *A számítógép-programozás művészete 2. Szeminumerikus algoritmusok.* Műszaki Könyvkiadó, 1987, 1994.

[25] D. E. Knuth, *Seminumerical algorithms. Vol. 2 of The Art of Computer Programming. Third edition.*, Addison-Wesley, 1997.

[26] D. E. Knuth, *Sorting and searching. Vol. 3 of The Art of Computer Programming*, Addison-Wesley, 1973. Magyarul: *A számítógép-programozás művészete 3. Keresés és rendezés.* Műszaki Kónyvkiadó, 1988, 1994.

[27] D. E. Knuth, *Sorting and searching. Vol. 3 of The Art of Computer Programming. Second edition*, Addison-Wesley, 1997.

[28] P. Kirrinnis, *Zur Berechnung von Partialbruchzerlegungen und Kurvenintegralen rationaler Funktionen, PhD. Thesis*, Rheinischen Friedrich-Wilhelms Universität zu Bonn, 1993.

[29] P. Kirrinnis, *Partial Fraction Decomposition in* $\mathbb{C}(z)$ *and Simultaneous Newton Iteration for Factorization in* $\mathbb{C}[z]$, J. of Complexity (to appear).

[30] E Kranakis [1986], *Primality and Cryptography.* B.G.Teubner–John Wiley & Sohns, 1986.

[31] J. v. Leeuwen (Ed.): Algorithms in Complexity, Vol. A, Elsevier (1990).

[32] A. K. Lenstra, H. W. Lenstra, Jr., *Algorithms in Number Theory*, J. v. Leeuwen (Ed.): Algorithms in Complexity, Vol. A, Elsevier (1990), 673-716.

[33] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard, *The number field sieve*, A. K. Lenstra, H. W. Lenstra, Jr. (Eds.): The development of the number field sieve, Springer-Verlag, LNM 1554, 1993, 11-42.

[34] R. Lipton, *Speeding up computations via molecular biology* , Draft (1994), 1-7.

[35] F. Morain, *Distributed primality proving and the primality of* $(2^{3539}+1)/3$, I. B. Damgąrd (Ed.): Advances in Cryptology - EUROCRYPT'90, 1991, 110-123.

[36] P. L. Montgomery, *A Block Lanczos Algorithm for Finding Dependencies over* $GF(2)$, L. C. Guillou, J.-J. Quisquater (Eds.): Advances in Cryptology — EUROCRYPT'95, Springer-Verlag, LNCS 921, 1995, 95-105.

[37] I. Niven, H. S. Zuckerman, *Bevezetés a számelméletbe*, Műszaki könyvkiadó, 1978.

[38] B. K. Parady, J. F. Smith, S. E. Zarantonello, *Largest known twin primes*, Math. Comp. *55*, 381-382.

[39] J. M. Pollard, *Factoring with cubic integers*, A. K. Lenstra, H. W. Lenstra, Jr. (Eds.): The development of the number field sieve, Springer-Verlag, LNM 1554, 1993, 4-10.

[40] J. M. Pollard, *The lattice sieve*, A. K. Lenstra, H. W. Lenstra, Jr. (Eds.): The development of the number field sieve, Springer-Verlag, LNM 1554, 1993, 43-49.

[41] M. E. Pohst, *Computational Algebraic Number Theory*, Birkhäuser, 1993.

[42] P. Ribenboim, *The Book of Prime Number Records.* Springer-Verlag, 1988.

[43] P. Ribenboim, *The New Book of Prime Number Records.* Springer-Verlag, 1996.

[44] H Riesel [1985], *Prime Numbers and Computer Methods for Factorization.* Birkhüuser, 1985.

[45] J.-P Serre, *A Course in Arithmetic.* Springer-Verlag, 1973.

[46] J.-P. Serre, *Algebraic Groups and Class Fileds. Graduate Text in Mathematics 117,* Springer-Verlag, 1988.

[47] A. Schönhage, *The fundamental theorem of algebra in terms of computational complexity – Preliminary report*, Univ. Tübingen, 1982, 1-74.

[48] A. Schönhage, *Equation Solving in Terms of Computational Complexity*, Proceedings of the International Congress of Mathematicians, Berkeley, California, USA, 1986, 131-154.

[49] A. Schönhage, *Numerik analytischer Funktionen und Komplexität*, Jber. d. Dt. Math.-Verein *92* (1990), 1-20.

[50] A. Schönhage, A. F. W. Grotefeld, E. Vetter, *Fast Algorithms: A Multitape Turing Machine Implementation*, B. I. Wissenschaftverlag, Mannheim, 1994.

[51] D. Weber, *An Implementation of the General Number Field Sieve to Compute Discrete Logarithms mod p*, L. C. Guillou, J.-J. Quisquater (Eds.): Advances in Cryptology — EUROCRYPT'95, Springer-Verlag, LNCS 921, 1995, 95-105.