Debreceni Egyetem
Természettudományi és Technológiai Kar
Matematikai Intézet

Szakdolgozat

Faktorizációs eljárások

készítette:

Zsidai Emese

témavezető: Dr. Tengely Szabolcs

Debrecen, 2017

Tartalomjegyzék

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani mindazoknak, akik bármilyen formában hozzájárultak szakdolgozatom elkészítéséhez. Legfőképp a szüleimnek, az egyetemi éveim alatt nyújtott támogatásukért, türelmükért és a tanulmányaim elvégzéséhez szükséges anyagi háttér biztosításáért.

1. Speciális célú faktorizációs algoritmusok

Faktorizációs eljárásokkal egész számok prímtényezős felbontását adhatjuk meg. Kisebb számok esetén ezek az algoritmusok könnyen elvégezhetőek, viszont ha egy szám elegendően nagy, nem ismerünk olyan eljárást, amely a felbontást gyorsan elvégezné. Ezt használják fel a titkosításban. A speciális és az általános célú algoritmusok a faktorizációs eljárások két nagy típusa [10] .

Speciális célú algoritmusok olyan összetett egész számokra alkalmazhatóak, melyek elég kicsik vagy kis osztókkal rendelkeznek. Ekkor az algoritmusok gyorsan végrehajthatóak.

1.1. Próbaosztás

Kis számok esetén alkalmazhatjuk, legkönnyebben megérthető algoritmus. A [7] forrást követve haladtunk.
Az n összetett számot szeretnénk faktorizálni. Osszuk el n az első p_1 prímmel, ha az osztás maradék nélküli, írjuk le p_1-t, és folytassuk a vizsgálatot $\frac{n}{p_1}$-el. Ha az osztás maradékos volt, akkor osszuk n-t a következő prímmel, amíg $\frac{n}{p_i}$ nem lesz egyenlő 1-el, maradék nélkül. Az n szám osztói a $[1, \sqrt{n}]$ intervallumból kerülnek ki, ezért elegendő a vizsgálatot $\sqrt{n}$-ig elvégezni.

Példa

$n = 114$, $p_1 := 2$, k_1 osztja 114-et, folytassuk a vizsgálatot $\frac{n}{p_1}$ -el, 57 legkisebb prímosztója $p_2 = 3$, $\frac{n}{p_2} = 19$, 19 prím, tehát $114 = 2 * 3 * 19$.

1.2. Fermat-féle faktorizáció

A Fermat-féle faktorizáció esetén a [3] irodalomra támaszkodtunk.

Olyan n számokra alkalmazhatjuk a Fermat-féle faktorizációt, mely felírható két négyzetszám különbségeként.

1.2.1. Tétel. *Legyen n páratlan egész szám. Ekkor létezik n $a*b$ alakú felbontása és $t^2 - s^2$ alakú felírása között egy egyértelmű hozzárendelés.*

Bizonyítás. A tétel következik n felírásából: $n = a * b = (\frac{a+b}{2})^2 - (\frac{a-b}{2})^2$ ahol $t = (\frac{a+b}{2})^2$ $s = (\frac{a-b}{2})^2$ □

A Fermat faktorizáció Sage kódja:

```
@interact
def _(n=('$N$',141467)):
    a=ceil(sqrt(n))
    b=a^2-n
    while not is_square(b):
        a += 1
        b=a^2-n
    pretty_print(html('$%s$ felírható $t^2-s^2=%s^2-%s^2$ alakban.
    '%(latex(n),latex(a),latex(sqrt(b)))))
    pretty_print(html('$t^2-s^2=(t-s)*(t+s)=a*b.$'))
    pretty_print(html('Tehát $N$ két osztója: $a=%s$ és $b=%s$
    '%(latex(a-sqrt(b)),latex(a+sqrt(b)))))
    return a-sqrt(b),a+sqrt(b)
```

Példák az előző kód futási képére:

N 141467

141467 felírható $t^2 - s^2 = 414^2 - 173^2$ alakban.
$t^2 - s^2 = (t - s) * (t + s) = a * b.$
Tehát N két osztója: $a = 241$ és $b = 587$

N 601847

601847 felírható $t^2 - s^2 = 816^2 - 253^2$ alakban.
$t^2 - s^2 = (t - s) * (t + s) = a * b.$
Tehát N két osztója: $a = 563$ és $b = 1069$

1.3. Rho módszer

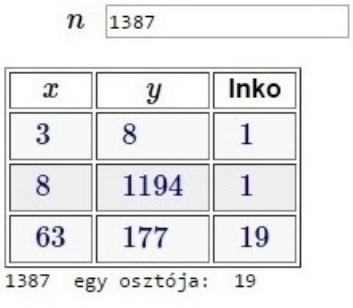
A Rho módszer esetén szintén [3] forrást használtuk fel.
Az $n \in \mathbb{N}$ szám prímosztóit úgy kaphatjuk meg, hogy választunk egy egész együtthatós egyszerű polinomot, például: $f(x) = x^2+1$. Választunk egy x_0 kezdőpontot $(i = 1, 2 \ldots)$ és elvégezzük a következőket:
$x_1 = f(x_0) \bmod n$
$x_2 = f(x_1) \bmod n$
$\vdots$
$x_{i+1} = f(x_i) \bmod n.$

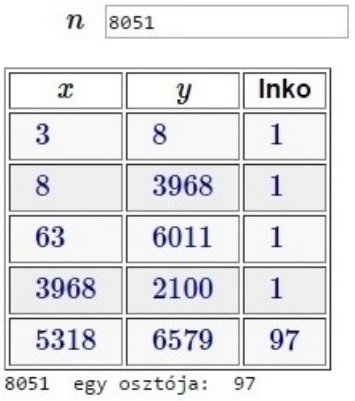
Összehasonlítjuk x_j azon értékeit, amelyek különböző osztályokban vannak $(\bmod n)$, de ugyanabban $(\bmod t)$. Ekkor t egy osztója n-nek.
Tehát $(x_j - x_i, n)$ értékeit teszteljük, amíg n valódi osztóját meg nem kapjuk.

Az alábbiakban megtalálható egy Sage kód, amely egy tetszőleges szám faktorizációját adja meg, Rho-módszer segítségével:

```
def fv(x,n):
    return mod(x^2-1,n)
@interact
def _(n=('$n$',1387)):
    a=2
    b=2
    d=1
    rows = []
    while d == 1:
        a=fv(a,n)
        b=fv(fv(b,n),n)
        d=gcd(a-b,n)
        rows.append([a,b,d])
    pretty_print(table(rows,header_row=["$x$","$y$","lnko"],frame=True))
    if d == n:
        print "faktorizáció triviális eredményt adott: ",d
        return -1
    else:
        print n," egy osztója: ",d
```

Néhány példa:





1.4. Euler faktorizáció

Az Euler-féle faktorizáció felhasználja Brahmagupta–Fibonacci azonosságot, mely segítségével megadhatjuk n szám osztóit.

1.4.1. Tétel (Brahmagupta–Fibonacci-féle azonosság)**.** *Tetszőleges a, b, c, d egész számok esetén:* $(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2 = (ac+bd)^2+(ad-bc)^2$.

Az azonosságról bővebben a [8]-ban olvashatunk.

Az n számot szeretnénk faktorizálni. Felírjuk n-t két különböző négyzetszám összegeként: $n = a^2 + b^2 = c^2 + d^2$.
Ekkor $a^2 - c^2 = d^2 - b^2$ ebből következik, hogy $(a - c)(a + c) = (d - b)(d + b)$.
Jelöljük $a-c$ és $d-b$ legnagyobb közös osztóját k-val,az $a+c$ és $d+b$ legnagyobb közös osztóját pedig h-val. Az l, m, l', m' kostansokkal kielégítjük a következő egyenleteket:
$(a - c) = kl$
$(d - b) = km$
$(a + c) = hm'$
$(d + b) = hl'$
Az l, m és l', m' relatív prímek lesznek. Behelyettesítve az $(a - c)(a + c) = (d - b)(d + b)$ egyenletbe kapjuk, hogy $klhm' = kmhl'$. Ekkor k-val és h-val egyszerűsítve kapjuk, hogy $lm' = l'm$. Mivel $(l, m) = 1$ és $(l', m') = 1$, ezért $l = l'$ illetve $m = m'$. Tehát
$(a - c) = kl$
$(d - b) = km$
$(a + c) = hm$
$(d + b) = hl$
Láthatjuk, hogy $a + c$ és $d - b$ legnagyobb közös osztója m,
$a - c$ és $d + b$ legnagyobb közös osztója pedig l lesz.

Alkalmazva Brahmagupta–Fibonacci-féle azonosságot azt kapjuk, hogy
$(k^2+h^2)(l^2+m^2) = (kl-hm)^2+(km+hl)^2 = ((a-c)-(a+c))^2+((d-b)+(d+b))^2 = (2c)^2+(2d)^2 = 4n$,
$(k^2+h^2)(l^2+m^2) = (kl+hm)^2+(km-hl)^2 = ((a-c)+(a+c))^2+((d-b)-(d+b))^2 = (2a)^2+(2b)^2 = 4n$.
Mivel minden tényező összege két négyzetszám, ezért (k,h) vagy (l,m) páros számok. Az általánosság elvesztése nélkül, tegyük fel, hogy (k,l) páros.
Ekkor n felbontása egyenlő lesz

$$\left(\left(\frac{k}{2}\right)^2+\left(\frac{h}{2}\right)^2\right)\left(l^2+m^2\right).$$

Az Euler faktorizációhoz [9] irodalmat használtuk fel.

Egy tetszőleges egész szám faktorizációjának Sage kódja, Euler faktorizációval:

```
@interact
def _(n=('$N$',2020)):
    var('x,y')
    N=solve_diophantine(x^2+y^2==n)
    l=len(N)
    i=0
    v=[]
    while i < l :
        if (N[i][0] > 0 and N[i][1] > 0):
            v.append(N[i])
        i=i+1
    if len(v) == 2 :
        a, b, c, d = v[0][0], v[0][1], v[1][0], v[1][1]
        if  (a-c)%2==1:
            c1=d
            d=c
            c=c1
        k=gcd(a-c,d-b)
        l=(a-c)//k
        m=(d-b)//k
        n=(a+c)//m
        N=a^2+b^2
        ac=(a-c)
        db=(d-b)
```

```
            pretty_print(html('$N$ felírható két négyzetszámpár
            különbségeként, azaz :$a^2+b^2=c^2+d^2=%s$'%latex(N)))
            pretty_print(html('$a=%s$'%latex(a)))
            pretty_print(html('$b=%s$'%latex(b)))
            pretty_print(html('$c=%s$'%latex(c)))
            pretty_print(html('$d=%s$'%latex(d)))
            pretty_print(html(r'$(a-c)=%s$ és $(d-b)=%s$
            legnagyobb közös osztója:
            $k=%s$'%(latex(ac),latex(db),latex(k))))
            pretty_print(html(r"$l=\displaystyle\frac{(a-c)}{k}=%s$"
            %latex(l)))
            pretty_print(html(r"$m=\displaystyle\frac{(d-b)}{k}=%s$"
            %latex(m)))
            pretty_print(html(r"$n=\displaystyle\frac{(a+c)}{m}=%s$"
            %latex(n)))
            oszto1=(k//2)^2+(n//2)^2
            oszto2=m^2+l^2
            pretty_print(html(r"az egyik osztó:
            $\left(\displaystyle\frac{k}{2}\right)
            ^2+\left(\displaystyle\frac{n}{2}\right)^2=%s$"%latex(oszto1)))
            pretty_print(html(r"a másik osztó: $m^2+l^2=%s$"%latex(oszto2)))
            pretty_print(html(r'Tehát $N$ felírható a következő módon:
             $%s\times %s$'%(latex(oszto1),latex(oszto2))))
        else:
            pretty_print(html('$Nem\ megoldható.$'))
```

Példa olyan számra, ami nem írható fel kétféleképpen két négyzetszám összegeként:

N 9452979572975

Nem megoldható.

Néhány példa olyan n egészekre, melyekre alkalmazható az Euler faktorizáció. Azaz n felírható $a^2 + b^2 = c^2 + d^2$ alakban:

N 265889879757

N felírható két négyzetszámpár különbségeként, azaz: $a^2 + b^2 = c^2 + d^2 = 265889879757$
$a = 445734$
$b = 259251$
$c = 106254$
$d = 504579$
$(a - c) = 339480$ és $(d - b) = 245328$ legnagyobb közös osztója: $k = 24$
$l = \frac{(a-c)}{k} = 14145$
$m = \frac{(d-b)}{k} = 10222$
$n = \frac{(a+c)}{m} = 54$
az egyik osztó: $\left(\frac{k}{2}\right)^2 + \left(\frac{n}{2}\right)^2 = 873$
a másik osztó: $m^2 + l^2 = 304570309$
Tehát N felírható a következő módon: 873×304570309

N 777788453

N felírható két négyzetszámpár különbségeként, azaz: $a^2 + b^2 = c^2 + d^2 = 777788453$
$a = 27887$
$b = 322$
$c = 11023$
$d = 25618$
$(a - c) = 16864$ és $(d - b) = 25296$ legnagyobb közös osztója: $k = 8432$
$l = \frac{(a-c)}{k} = 2$
$m = \frac{(d-b)}{k} = 3$
$n = \frac{(a+c)}{m} = 12970$
az egyik osztó: $\left(\frac{k}{2}\right)^2 + \left(\frac{n}{2}\right)^2 = 59829881$
a másik osztó: $m^2 + l^2 = 13$
Tehát N felírható a következő módon: 59829881×13

N 5468797974789

N felírható két négyzetszámpár különbségeként, azaz :$a^2 + b^2 = c^2 + d^2 = 5468797974789$
$a = 1875633$
$b = 1396710$
$c = 997695$
$d = 2115042$
$(a - c) = 877938$ és $(d - b) = 718332$ legnagyobb közös osztója: $k = 6$
$l = \frac{(a-c)}{k} = 146323$
$m = \frac{(d-b)}{k} = 119722$
$n = \frac{(a+c)}{m} = 24$
az egyik osztó: $\left(\frac{k}{2}\right)^2 + \left(\frac{n}{2}\right)^2 = 153$
a másik osztó: $m^2 + l^2 = 35743777613$
Tehát N felírható a következő módon: 153×35743777613

2. Általános célú faktorizációs algoritmusok

Általános célú algoritmusokat bármelyik összetett szám esetén alkalmazhatunk. Hátránya, hogy a könnyebb számokat is ugyanannyi idő alatt faktorizálják le, mint a nehezebbeket. Az ilyen típusú algoritmusokat használjuk az RSA számok esetén. Az RSA titkosítási rendszerről a [3] forrásban olvashatunk.

2.0.1. Definíció (B sima)**.** Legyen $B = p_1, \ldots, p_k$ egy halmaz, ahol $p_1, p_2, \ldots$ prímek. Ekkor $k \in \mathbb{Z}^+$-t akkor nevezzük B simának, ha k összes prím osztója kisebb, mint B.

2.1. Dixon faktorizáció

A Dixon faktorizáció esetében a [1], [6] forrásokat követve haladtunk.
Az $N \in \mathbb{N}$ számot szeretnénk faktorizálni.
Válasszunk egy B korlátot és az ennél kisebb prímek halmazát jelöljük B-vel, ez lesz a fakorbázis. Olyan pozitív egész z-t keresünk, melyre $z^2 \bmod N$ B sima szám lesz, azaz legkisebb abszolút értékű maradéka felírható B-beli számok szorzataként:

$$z_k^2 \equiv \prod_{i=1}^{k} p_j^{a_{j,i}} \pmod{N}.$$

A $a_{j,i}$ kitevőket rögzítsük a

$$\mathbf{v_i} = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{k,i} \end{pmatrix}$$

vektorokban. A vektorokból készítsünk mátrixot:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k1} & a_{2k} & \dots & a_{kk} \end{pmatrix}.$$

Nem triviális lineáris kombináció megtalálásához használhatjuk a Gauss eliminációt (mod 2).

$$z_1^2 z_2^2 \dots z_t^2 \equiv \prod_{p_i \in B} p_i^{a_{i,1}+a_{i,2}+\dots+a_{i,t}} \pmod{N}.$$

Ha találunk ilyen x, y párt, melyre teljesül $x^2 \equiv y^2 \pmod{N}$ és $x \not\equiv \pm y \pmod{N}$ kongruencia, akkor készen vagyunk, ha nem teljesülnek, akkor további B sima számokat keresünk. N két nem triviális osztóját kaphatjuk:

$$lnko\left(\prod_{i=1}^{k} z_i^{e_i} + \sqrt{\prod_{p_i \in B} p_i^{a_{i,j}}}, N\right)$$

és

$$lnko\left(\prod_{i=1}^{k} z_i^{e_i} - \sqrt{\prod_{p_i \in B} p_i^{a_{i,j}}}, N\right).$$

Dixon faktorizáció Sage kódja:

```
@interact
def _(n=('$N$',6216577),B=('$B$',7)):
    w=[]
    for i in [1..B]:
        if is_prime(i):
            w=w + [i]
    x=ceil(sqrt(n))
    a=(x^2)%n
    q=[valuation(a,k) for k in w]
    A=[]
    K=[]
    T=True
    while T:
        p=0
        while p!=1:
            x += 1
            a=(x^2)%n
            p=a/prod([k^valuation(a,k) for k in w])
```

```
            q=[valuation(a,k) for k in w]
        K.append(x)
        A.append(q)
        p=0
        Q=matrix(GF(2),A).transpose()
        if Q.right_kernel().dimension()>0:
            Qv=sum(Q.right_kernel().basis())
            Av=sum([vector(A[k]) for k in [0..len(A)-1] if Qv[k]==1])
            av=prod([w[s]^Av[s] for s in [0..(len(w)-1)]]).nth_root(2)
            Kv=prod([K[k] for k in [0..len(A)-1] if Qv[k]==1])
            d1=gcd(Kv-av,n)
            d2=gcd(Kv+av,n)
            if Set([1,n])!=Set([d1,d2]):
                T=False
            DH=[(k,n//k) for k in [d1,d2] if k!=1 and k!=n]
    pretty_print(html('$B$ faktorbázis elemei: $%s$'%latex(w)))
    pretty_print(html('Egy $p_i$ szám akkor B sima, ha $p_i^2\ (mod\ N)$
    legkisebb abszolút értékű maradéka B faktorbázis szorzataiból áll.'))
    pretty_print(html(r'B sima számok $N$-re nézve: $%s$.'%latex(K)))

    pretty_print(html('Ezen B-beli számok felbontását tároljuk el
    vektorokban. '))
    pretty_print(html('A vektor koordinátái a faktorbázisban lévő
    prímekhez tartozó kitevők a megfelelő sorrendben $%s$ '%latex(A)))
    pretty_print(html('Az összegyűjtött vektorokból készítsünk egy
    mátrixot $(mod\ 2)$ : $%s$, melyre alkalmazzuk a Gauss eliminációt.'
    %latex(Q)))
    pretty_print(html('Az egyenletrendszer megoldása: $%s$ := ${a_{i,j}}$ .'
    %latex(Av)))
    pretty_print(html('$\displaystyle\sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}$ =
    $%s$, ahol $b_i$ a faktorbázis elemei.'%latex(av)))
    pretty_print(html('$\displaystyle\prod_{i=1}^k p_i$ = $%s$'%latex(Kv)))
    pretty_print(html('$N$ osztóit a következőképpen számolhatjuk ki: $lnko
    \displaystyle( \prod_{i=1}^k p_i \pm \sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}
     , N)$'))
    pretty_print(html('$lnko(%s+%s,%s)$ és $lnko(%s-%s,%s)$' %(latex(Kv),
    latex(av),latex(n),latex(Kv),latex(av),latex(n))))
    pretty_print(html('Tehát $N$ nemtriviális osztói: $%s$' %latex(DH)))
```

Néhány példa a Dixon faktorizáció Sage kódjának futási képére:

N 635919259

B 17

B faktorbázis elemei: $[2, 3, 5, 7, 11, 13, 17]$
Egy p_i szám akkor B sima, ha $p_i^2 \ (mod\ N)$ legkisebb abszolút értékű maradéka B faktorbázis szorzataiból áll.
B sima számok N-re nézve: $[25247, 50494, 75741, 80294, 100988, 110036, 111152]$.
Ezen B-beli számok felbontását tároljuk el vektorokban.
A vektor koordinátái a faktorbázisban lévő prímekhez tartozó kitevők a megfelelő sorrendben:
$[[1, 3, 3, 0, 0, 1, 1], [3, 3, 3, 0, 0, 1, 1], [1, 5, 3, 0, 0, 1, 1], [1, 1, 0, 1, 5, 1, 0], [5, 3, 3, 0, 0, 1, 1], [0, 2, 3, 0, 3, 0, 1], [0, 8, 0, 3, 2, 0, 0]]$
Az összegyűjtött vektorokból készítsünk egy mátrixot $(mod\ 2)$: $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$, melyre alkalmazzuk a Gauss eliminációt.
Az egyenletrendszer megoldása: $(6,\ 22,\ 12,\ 4,\ 10,\ 4,\ 4)$:= $a_{i,j}$.
$\sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}$ = 8534692298741734125000, ahol b_i a faktorbázis elemei.
$\prod_{i=1}^{k} p_i$ = 948234517422454843924861155 84
N osztóit a következőképpen számolhatjuk ki: $lnko(\prod_{i=1}^{k} p_i \pm \sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}, N)$
$lnko(948234517422454843924861155 84 + 8534692298741734125000, 635919259)$ és
$lnko(948234517422454843924861155 84 - 8534692298741734125000, 635919259)$
Tehát N nemtriviális osztói: $[(17187007, 37), (37, 17187007)]$

N 17187007

B 11

B faktorbázis elemei: $[2, 3, 5, 7, 11]$
Egy p_i szám akkor B sima, ha $p_i^2 \ (mod\ N)$ legkisebb abszolút értékű maradéka B faktorbázis szorzataiból áll.
B sima számok N-re nézve: $[7211, 14422, 17513, 21542, 21633]$.
Ezen B-beli számok felbontását tároljuk el vektorokban.
A vektor koordinátái a faktorbázisban lévő prímekhez tartozó kitevők a megfelelő sorrendben:
$[[2, 0, 6, 1, 0], [4, 0, 6, 1, 0], [1, 0, 2, 4, 2], [0, 0, 2, 3, 0], [2, 2, 6, 1, 0]]$
Az összegyűjtött vektorokból készítsünk egy mátrixot $(mod\ 2)$: $\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$, melyre alkalmazzuk a Gauss eliminációt.
Az egyenletrendszer megoldása: $(8,\ 2,\ 20,\ 6,\ 0)$:= $a_{i,j}$.
$\sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}$ = 160781250000, ahol b_i a faktorbázis elemei.
$\prod_{i=1}^{k} p_i$ = 48464502462501612
N osztóit a következőképpen számolhatjuk ki: $lnko(\prod_{i=1}^{k} p_i \pm \sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}, N)$
$lnko(48464502462501612 + 160781250000, 17187007)$ és $lnko(48464502462501612 - 160781250000, 17187007)$
Tehát N nemtriviális osztói: $[(503, 34169), (34169, 503)]$

N 24152753

B 40

B faktorbázis elemei: $[2,3,5,7,11,13,17,19,23,29,31,37]$
Egy p_i szám akkor B sima, ha $p_i^2 \ (mod\ N)$ legkisebb abszolút értékű maradéka B faktorbázis szorzataiból áll.
B sima számok N-re nézve: $[4919,4921,4926,4953]$.
Ezen B-beli számok felbontását tároljuk el vektorokban.
A vektor koordinátái a faktorbázisban lévőprímekhez tartozó kitevők a megfelelő sorrendben
$[[5,0,0,0,0,0,0,0,0,0,0,2],[11,0,0,0,0,0,0,0,0,0,1,0],[0,0,0,0,0,2,0,0,1,1,0,0],[6,0,0,2,2,0,0,0,0,0,0,0]]$
Az összegyűjtött vektorokból készítsünk egy mátrixot $(mod\ 2)$: $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, melyre alkalmazzuk a Gauss eliminációt.
Az egyenletrendszer megoldása: $(6,\ 0,\ 0,\ 2,\ 2,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0)$:= $a_{i,j}$.
$\sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}$ =616, ahol b_i a faktorbázis elemei.
$\prod_{i=1}^{k} p_i$ = 4953
N osztóit a következőképpen számolhatjuk ki: $lnko(\prod_{i=1}^{k} p_i \pm \sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}, N)$
$lnko(4953+616, 24152753)$ és $lnko(4953-616, 24152753)$
Tehát N nemtriviális osztói: $[(4337,5569),(5569,4337)]$

N 96304081

B 7

B faktorbázis elemei: $[2,3,5,7]$
B sima számok N-re nézve: $[25964]$.
Egy p szám akkor B sima ha $p^2 \ (mod\ N)$ legkisebb abszolút értékű maradéka B faktorbázis szorzataiból áll
Ezen B-beli számok felbontását tároljuk el vektorokban.
A vektor koordinátái a faktorbázisban lévő prímekhez tartozó kitevők a megfelelő sorrendben $[[0,6,0,0]]$
Az összegyűjtött vektorokból készítsünk egy mátrixot $(mod\ 2)$: $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, melyre alkalmazzuk a Gauss eliminációt.
Az egyenletrendszer megoldása: $(0,\ 6,\ 0,\ 0)$ ami egyenlő 27, ehhez tartozó p= 25964
N osztóit a következőképpen számolhatjuk ki: $lnko(25964-27, 96304081)$ és $lnko(25964+27, 96304081)$
Tehát N nemtriviális osztói: $[(25937,3713),(3713,25937)]$

2.2. Lánctört faktorizáció

2.2.1. Definíció. Legyen $x \in \mathbb{R}$. Ekkor x lánctörtjegyein a $a_0, a_1 \ldots \in \mathbb{Z}$ számokat értjük.
$x_0 = x; a_0 = \lfloor x_0 \rfloor$
$x_1 = \frac{1}{x_0 - a_0}; a_1 = \lfloor x_1 \rfloor$
$x_2 = \frac{1}{x_1 - a_1}; a_2 = \lfloor x_2 \rfloor$
$\vdots$
$a_i = \lfloor x_i \rfloor; x_{i+1} = \frac{1}{x_i - a_i}$

Megjegyzés. Minden valós számnak létezik lánctört alakja, mely egyértelmű, valamint $a_i > 0$, ha $i \geq 1$.

Megjegyzés. Ha $a_0, a_1, \ldots$ az x valós lánctörtjegyei, akkor az

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\vdots}}}}$$

lánctört alakját a következőképpen jelöljük: $[a_0, a_1, \ldots]$.

2.2.1. Tétel. *Minden $x \in \mathbb{R} \setminus \mathbb{Q}$ esetén megadható x-et legjobban közelítő racionális szám, x lánctört alakjának véges kiértékelésével. A számláló növelésével tudunk közelebbi racionális számot megadni.*
A kiértékelést a következőképpen adhatjuk meg:
$x \approx [a_0, a_1, \ldots a_k] = \frac{p_k}{q_k}, ahol$
$\frac{p_0}{q_0} = a_0$
$\frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}$;
$\frac{p_i}{q_i} = \frac{a_i p_{i-1} + p_{i-2}}{a_i q_{i-1} + a_{i-2}}$

2.2.2. Tétel. *Minden $x \in \mathbb{Q}$ nem négyzetszám esetén $\sqrt{r} = [a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}]$.*

A tételek bizonyítását a [2] , [4] irodalomban találjuk meg.

Az N számot szeretnénk faktorizálni. Konstruáljuk meg a faktorbázist, mely a választott korlátnál kisebb prímeket tartalmazza, jelöljük B-vel.
Írjuk fel $\sqrt{N}$ lánctört alakját. Az $\frac{p_i}{q_i}$ közelítésekre vizsgáljuk meg, hogy p_i B sima szám-e. Azaz $(p_i)^2 \equiv \prod_{b_i \in B} b_i^{a_i} \pmod{N}$ teljesül. A B sima számokhoz tartozó b_i prímek kitevőit rögzítsük egy vektorba, a megfelelő sorrendben. A

kapott vektorokból készítsünk mátrixot, melyre alkalmazzuk a Gauss eliminációt $\mathbb{Z}_2$ felett. Ha találunk olyan x, y számot, melyre igaz, hogy $x^2 \equiv y^2 \pmod{N}$ és $x \not\equiv \pm y \pmod{N}$ is teljesül akkor készen vagyunk, ha nem teljesül, akkor további B sima számokat kell keresnünk.
N két nem triviális osztója lehet:

$$lnko\left(\prod_{i=1}^{k} p_i + \sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}, N\right)$$

és

$$lnko\left(\prod_{i=1}^{k} p_i - \sqrt{\prod_{p_i \in B} b_i^{a_{i,j}}}, N\right).$$

A lánctört faktorizáció esetén a [2] forrást használtuk fel.

A lánctört faktorizáció Sage kódja:

```
@interact
def _(n=('$N$',23449),B=('$B$',7)):
    w=[]
    for i in [1..B]:
        if is_prime(i):
            w=w + [i]
    n.is_prime()
    pretty_print(html('$B$ faktorbázis elemei: $%s$'%latex(w)))
    sn=sqrt(n)
    cfn=continued_fraction(sn)
    t=0
    x=cfn.numerator(t)
    pretty_print(html('$%s$ lánctört alakja: $%s$'%(latex(n),
    latex(continued_fraction(sqrt(n))))))
    A=[]
    K=[]
    T=True
    while T:
        x=cfn.numerator(t)
        a=(x^2)%n
        p=a/prod([k^valuation(a,k) for k in w])
        if p==1:
            q=[valuation(a,k) for k in w]
            A.append(q)
```

```
K.append(x)
Q=matrix(GF(2),A).transpose()
if Q.right_kernel().dimension()>0:
    for Qv in Q.right_kernel().
    basis():
        Av=sum([vector(A[k])
        for k in [0..len(A)-1]
        if Qv[k]==1])
        av=prod([w[s]^Av[s] for
        s in [0..(len(w)-1)]])
        .nth_root(2)
        Kv=prod([K[k] for k in
        [0..len(A)-1] if
        Qv[k]==1])
        d1=gcd(Kv-av,n)
        d2=gcd(Kv+av,n)
        if Set([1,n])!=Set([d1,d2])
        and Set([d1,d2])
        !=Set([1]) and Set([d1,d2])
        !=Set([n]):
            pretty_print(html('Egy
            $p$ szám akkor B sima ha
            $p^2\ (mod\ N)$ legkisebb
            abszolút értékű maradéka
            B faktorbázis szorzataiból
             áll.'))
            pretty_print(html('B számok
            $%s$-re nézve: $%s$ '
            %(latex(n),latex(K))))
            pretty_print(html('Ezen
             B-beli számok
            felbontását tároljuk el
            vektorokban. '))
            pretty_print(html('A vektor
             koordinátái a
            faktorbázisban lévő
            prímekhez tartozó kitevők
            a megfelelő sorrendben:'))
            pretty_print(html('$%s$ '
            %latex(A)))
            pretty_print(html('Az összegyűjtött
```

```
                        vektorokból készítsünk egy  mátrixot
                        $(mod\ 2)$ : $%s$, melyre alkalmazzuk
                        a Gauss eliminációt.'%latex(Q)))
                        pretty_print(html('Az
                        egyenletrendszer megoldása:
                        $%s$ := ${a_{i,j}}$ .'
                        %latex(Av)))
                        pretty_print(html('$
                        \displaystyle\sqrt{\prod_
                        {b_i \in B} b_i^{a_{i,j}}}$
                         =  $%s$, ahol $b_i$
                        a faktorbázis elemei.'%latex(av)))
                        pretty_print(html('$\displaystyle
                        \prod_{i=1}^k p_i$ = $%s$'%latex(Kv)))
                        pretty_print(html('$N$ osztóit a
                        következőképpen számolhatjuk ki: $lnko
                        p_i \pm \sqrt{\prod_{b_i \in B} b_i^
                        {a_{i,j}}} , N)$'))
                        pretty_print(html('$lnko(%s+%s,%s)$
                        és $lnko(%s-%s,%s)$' %(latex(Kv),
                        latex(av),latex(n),latex(Kv),latex(av)
                        ,latex(n))))
                        pretty_print(html('Tehát $%s$ nem
                        triviális osztói:
                        $%s,%s$ '%(latex(n),latex(d1),latex(d2))))
                        T=False
            t=t+1
    else:
        t=t+1
```

Példák a Sage kód futási képére:

N 5160847

B 7

B faktorbázis elemei: $[2, 3, 5, 7]$

5160847 lánctört alakja: $2271 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{266 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{16 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\dots}}}}}}}}}}$

Egy p szám akkor B sima ha $p^2 \pmod N$ legkisebb abszolút értékű maradéka B faktorbázis szorzataiból áll.
B számok 5160847-re nézve: $[54701754633003951642102855396149646808268530972981020803417081859477 2]$
Ezen B-beli számok felbontását tároljuk el vektorokban.
A vektor koordinátái a faktorbázisban lévő prímekhez tartozó kitevők a megfelelő sorrendben:
$[[0, 0, 0, 0]]$

Az összegyűjtött vektorokból készítsünk egy mátrixot $\pmod 2$: $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, melyre alkalmazzuk a Gauss eliminációt.

Az egyenletrendszer megoldása: $(0, 0, 0, 0)$:= $a_{i,j}$.

$\sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}} = 1$, ahol b_i a faktorbázis elemei.

$\prod_{i=1}^{k} p_i = 54701754633003951642102855396149646808268530972981020803417081859477 2$

N osztóit a következőképpen számolhatjuk ki: $lnko(\prod_{i=1}^{k} p_i \pm \sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}, N)$

$lnko(54701754633003951642102855396149646808268530972981020803417081859477 2 + 1, 5160847)$ és
$lnko(54701754633003951642102855396149646808268530972981020803417081859477 2 - 1, 5160847)$
Tehát 5160847 nem triviális osztói: $8419, 613$

N 17187007

B 7

B faktorbázis elemei: $[2, 3, 5, 7]$

17187007 lánctört alakja: $4145 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{15 + \cfrac{1}{23 + \cfrac{1}{1 + \cfrac{1}{\dots}}}}}}}}}}$

Egy p szám akkor B sima ha $p^2 \pmod N$ legkisebb abszolút értékű maradéka B faktorbázis szorzataiból áll.
B számok 17187007-re nézve:
$[24262495741529695, 24262495741529695, 7831512150453108991851564837180932472381840657938869534358390517885632]$
Ezen B-beli számok felbontását tároljuk el vektorokban.
A vektor koordinátái a faktorbázisban lévő prímekhez tartozó kitevők a megfelelő sorrendben:
$[[1, 6, 0, 0], [1, 6, 0, 0], [0, 4, 0, 0]]$

Az összegyűjtött vektorokból készítsünk egy mátrixot $\pmod 2$: $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, melyre alkalmazzuk a Gauss eliminációt.

Az egyenletrendszer megoldása: $(0, 4, 0, 0)$:= $a_{i,j}$.

$\sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}} = 9$, ahol b_i a faktorbázis elemei.

$\prod_{i=1}^{k} p_i = 7831512150453108991851564837180932472381840657938869534358390517885632$

N osztóit a következőképpen számolhatjuk ki: $lnko(\prod_{i=1}^{k} p_i \pm \sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}, N)$

$lnko(7831512150453108991851564837180932472381840657938869534358390517885632 + 9, 17187007)$ és
$lnko(7831512150453108991851564837180932472381840657938869534358390517885632 - 9, 17187007)$
Tehát 17187007 nem triviális osztói: $503, 34169$

N 6266767

B 7

B faktorbázis elemei: $[2, 3, 5, 7]$

6266767 lánctört alakja: $2503 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{\dots}}}}}}}}}}$

Egy p szám akkor B sima ha $p^2 \ (mod\ N)$ legkisebb abszolút értékű maradéka B faktorbázis szorzataiból áll.
B számok 6266767-re nézve:
$[207995267114957179435406469597077055040181592648054385661143592842843143265965484]$
Ezen B-beli számok felbontását tároljuk el vektorokban.
A vektor koordinátái a faktorbázisban lévő prímekhez tartozó kitevők a megfelelő sorrendben:
$[[0, 4, 0, 0]]$

Az összegyűjtött vektorokból készítsünk egy mátrixot $(mod\ 2)$: $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, melyre alkalmazzuk a Gauss eliminációt.

Az egyenletrendszer megoldása: $(0,\ 4,\ 0,\ 0)$:= $a_{i,j}$.

$\sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}} = 9$, ahol b_i a faktorbázis elemei.

$\prod_{i=1}^{k} p_i = 207995267114957179435406469597077055040181592648054385661143592842843143265965484$

N osztóit a következőképpen számolhatjuk ki: $lnko(\prod_{i=1}^{k} p_i \pm \sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}, N)$
$lnko(207995267114957179435406469597077055040181592648054385661143592842843143265965484 + 9, 6266767)$ és
$lnko(207995267114957179435406469597077055040181592648054385661143592842843143265965484 - 9, 6266767)$
Tehát 6266767 nem triviális osztói: $482059, 13$

N 685726701

B 7

B faktorbázis elemei: $[2, 3, 5, 7]$

685726701 lánctört alakja: $26186 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{7 + \cfrac{1}{2 + \cfrac{1}{30 + \cfrac{1}{5 + \frac{1}{\dots}}}}}}}}}}$

Egy p szám akkor B sima ha $p^2 \ (mod\ N)$ legkisebb abszolút értékű maradéka B faktorbázis szorzataiból áll.
B számok 685726701-re nézve:
$[807598284900899189634789609811452669554725728818606163134407213253009978209729 73]$
Ezen B-beli számok felbontását tároljuk el vektorokban.
A vektor koordinátái a faktorbázisban lévő prímekhez tartozó kitevők a megfelelő sorrendben:
$[[0, 0, 2, 0]]$

Az összegyűjtött vektorokból készítsünk egy mátrixot $(mod\ 2)$: $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, melyre alkalmazzuk a Gauss eliminációt.

Az egyenletrendszer megoldása: $(0,\ 0,\ 2,\ 0)$:= $a_{i,j}$.

$\sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}} = 5$, ahol b_i a faktorbázis elemei.

$\prod_{i=1}^{k} p_i = 807598284900899189634789609811452669554725728818606163134407213253009978209729 73$

N osztóit a következőképpen számolhatjuk ki: $lnko(\prod_{i=1}^{k} p_i \pm \sqrt{\prod_{b_i \in B} b_i^{a_{i,j}}}, N)$
$lnko(807598284900899189634789609811452669554725728818606163134407213253009978209729 73 + 5, 685726701)$ és
$lnko(807598284900899189634789609811452669554725728818606163134407213253009978209729 73 - 5, 685726701)$
Tehát 685726701 nem triviális osztói: $3280989, 209$

Irodalomjegyzék

[1] Dixon's factorization method. http://mathworld.wolfram.com/DixonsFactorizationMethod.html.

[2] Per Leslie Jensen. Integer factorization. http://www.pgnfs.org/DOCS/thesis.pdf, 2005.

[3] Liptai Kálmán. Kriptográfia. http://liptai.ektf.hu/uploads/2011/12/Kriptografia.pdf, 2011.

[4] Niels Lauritzen. Continued fractions and factoring. https://pdfs.semanticscholar.org/a510/fb0836d8741a5ac0f9cb1d2cbbc190637185.pdf.

[5] WA Stein et al. Sagemath software. http://www.sagemath.org/.

[6] Wikipedia. Dixon's factorization method. https://en.wikipedia.org/wiki/Dixon%27s_factorization_method, September 2015.

[7] Wikipedia. Prímfelbontás. https://hu.wikipedia.org/wiki/Pr%C3%ADmfelbont%C3%A1s, 2016.

[8] Wikipedia. Brahmagupta–fibonacci identity. https://en.wikipedia.org/wiki/Brahmagupta%E2%80%93Fibonacci_identity, 2017.

[9] Wikipedia. Euler's factorization method. https://en.wikipedia.org/wiki/Euler%27s_factorization_method, January 2017.

[10] Wikipedia. Integer factorization. https://en.wikipedia.org/wiki/Integer_factorization, April 2017.