

Faktorizacija s pomočjo stožnic

Osnutek diplomske naloge

Nik Mrhar

Mentor: izr. prof. dr. Aleš Vavpetič

februar 2022

1 Uvod

S faktorizacijo celih števil so se ukvarjali že v Antični Grčiji, kjer so poznali in tudi dokazali osnovni izrek aritmetike. Ta pravi, da lahko vsako naravno število zapišemo kot enoličen produkt praštevilskih faktorjev do vrstnega natančno. Do danes se je faktorizacija števil razširila na različna področja in pojavila se je potreba po čim bolj učinkovitih algoritmih faktorizacije. Z enostavnimi algoritmi, kot je na primer zaporedno deljenje, smo se srečali tudi tekom študija. Med klasičnimi algoritmi pa obstajata dva, ki temeljita na zapisu števila v obliki kvadratne forme. V diplomski nalogi se bomo posvetili opisu Fermatove ter Eulerjeve faktorizacije celih števil ter posplošitvi le-te.

2 Fermatov razcep

Prvi izmed teh algoritmov je Fermatov razcep števila, kjer celo število N zapišemo v obliki:

$$N = x^2 - y^2 = (x - y) \cdot (x + y).$$

Ta razcep je pomemben, saj je kot prvi predstavil število v obliki kvadratne forme. Pomemben pa je tudi zato, ker je zamenjal do takrat glavno metodo faktorizacije, in sicer deljenje števila N s praštevili $\leq \sqrt{N}$.

Fermatov razcep vedno obstaja, saj velja

$$N = \left[\frac{(N+1)}{2} \right]^2 - \left[\frac{(N-1)}{2} \right]^2.$$

Opomba: Ta reprezentacija pokaže samo obstoj razcepa, saj poda trivialno faktorizacijo $N = 1 \cdot N$. Ostane nam še določitev pogojev za x , da faktorizacija ne bo trivialna:

Naj bo $N = a \cdot b$, kjer je $1 < a < \sqrt{N}$. Ker velja $x - y = a$ in $x + y = b$, vidimo, da je $x = \frac{a+b}{2} = \frac{a+(\frac{N}{a})}{2}$. Iz tega hitro sledi, da mora veljati $\sqrt{N} < x < \frac{N+1}{2}$.

3 Eulerjeva faktorizacija

Druga metoda se imenuje Eulerjeva faktorizacija, s katero se je približno sto let po Fermatu začel ukvarjati švicarski matematik Leonhard Euler. Metoda temelji na zapisu lihega celega števila v obliki vsote kvadratov na dva različna načina. Euler je za ta problem podal enostavno rešitev, predstavljeno v naslednjem izreku.

Izrek 1: Naj bo N liho celo število, ki ga lahko na dva različna načina predstavimo kot

$$N = a^2 + b^2 = c^2 + d^2,$$

kjer so $a, b, c, d \in \mathbb{Z}^+$. Potem velja:

$$N = \frac{1}{4(d-b)^2} [(a-c)^2 + (d-b)^2] \cdot [(a+c)^2 + (d-b)^2].$$

Nekoliko kasneje je Euler podal tudi izboljšano verzijo metode, v kateri so dobljeni faktorji netrivialni, vendar bomo to formulacijo za zdaj izpustili.

4 Lucas-Mathewsova formula

Ko enkrat poznamo Eulerjevo faktorizacijo, se hitro pojavi vprašanje, ali lahko to metodo tudi posplošimo. V ta namen si pogledjmo dve posplošitvi.

4.1 Faktorizacija s pomočjo elipse

Prva posplošitev, ki takoj sledi iz Eulerjeve formule, je posplošitev zapisa števila v obliki splošne enačbe elipse na dva različna načina. Za to faktorizacijo velja naslednji izrek.

Izrek 2: Lucas-Mathewsova formula za elipso

Naj bo N liho celo število, ki ga lahko na dva načina predstavimo kot

$$N = ma^2 + nb^2 = mc^2 + nd^2,$$

kjer so $a, b, c, d, m, n \in \mathbb{Z}^+$ in velja $(ma, nb) = (mc, nd) = 1$. Potem je

$$N = (N, ad - bc)(N, ad + bc).$$

Opomba: Za $a, b \in \mathbb{Z}$ z (a, b) označimo največji skupni delitelj teh dveh števil.

Oglejmo si dva primera uporabe te formule.

Zgled 1: Mersennovo število $M_{11} = 2^{11} - 1 = 2047$ lahko na dva različna načina napišemo kot:

$$\begin{aligned} 2047 &= 6 \cdot 2^2 + 7 \cdot 17^2 = 6 \cdot 12^2 + 7 \cdot 13^2 \\ 2047 &= (2047, -178)(2047, 230) = 89 \cdot 23 \end{aligned}$$

Zgled 2: Fermatovo število $F_5 = 2^{32} + 1 = 4394967297$ zapišemo kot:

$$\begin{aligned} F_5 &= (F_5, 7389 \cdot 3983 - 2618 \cdot 6674)(F_5, 7389 \cdot 3983 + 2618 \cdot 6674) \\ F_5 &= (F_5, 11957855)(F_5, 46902919) = 641 \cdot 6700417 \end{aligned}$$

Kot vidimo, z uporabo Lucas-Matthewsove formule za elipso, dobimo netrivialen razcep v obeh primerih. Da je razcep netrivialen ni naključje, saj velja naslednji izrek, katerega dokaz za zdaj izpuščamo.

Izrek 3: Faktorizacija z elipso je vedno netrivialna.

Opomba: Za dokaz Lucas-Matthewsovega izreka uporabimo naslednji dve formuli:

$$(d^2 - b^2)N = m(ad - bc)(ad + bc) \quad (1)$$

in

$$(mac \mp nbd)^2 + mn(ad \pm bc)^2 = N^2. \quad (2)$$

Iz enačbe (1) lahko dokažemo, da N deli $(ad - bc)(ad + bc)$, enačbo (2) pa lahko uporabimo za dokaz netrivialnosti razcepa.

4.2 Faktorizacija s pomočjo hiperbole

Druga posplošitev Eulerjeve metode je zapis števila v obliki enačbe hiperbole. Poseben primer tega razcepa je tudi Fermatov razcep. Vse kar moramo narediti, da pridemo iz enačbe elipse $E : mx^2 + ny^2 = N$ do enačbe hiperbole $H : mx^2 - ny^2 = N$, je nadomestiti n z $-n$. Tako lahko za primer dvojne reprezentacije s hiperbolo hitro izpeljemo, da velja ista faktorizacija kot v primeru elipse. Ostane pa vprašanje, ali je ta razcep netrivialen. V ta namen si ponovno pogledjmo primer razcepa Mersennovega števila M_{11} .

Zgled 3:

$$1. \quad M_{11} = 2^{11} - 1 = 2047 = 1 \cdot 63^2 - 2 \cdot 31^2 = 1 \cdot 47^2 - 2 \cdot 9^2$$

$$\begin{aligned} M_{11} &= (M_{11}, ad - bc)(M_{11}, ad + bc) \\ &= (2047, 63 \cdot 9 - 31 \cdot 47)(2047, 63 \cdot 9 + 31 \cdot 47) \\ &= (2047, -890)(2047, 2024) = 89 \cdot 23. \end{aligned}$$

$$2. \quad M_{11} = 2^{11} - 1 = 1 \cdot 63^2 - 2 \cdot 31^2 = 1 \cdot 65^2 - 2 \cdot 33^2$$

$$\begin{aligned} (M_{11}, ad - bc) &= (2047, 63 \cdot 33 - 65 \cdot 31) = (2047, 64) = 1, \\ (M_{11}, ad + bc) &= (2047, 4094) = (M_{11}, 2M_{11}) = M_{11}. \end{aligned}$$

Kot vidimo v zgledu, za faktorizacijo s hiperbolo ne velja netrivialnost razcepa. V primeru 2 nam izbor števil v zapisu enačb hiperbole porodi trivialen razcep $M_{11} \cdot 1$.

Propozicija: Če je $N = ma^2 - nb^2 = mc^2 - nd^2$, potem velja

$$(mac \pm nbd)^2 - mn(ad \pm bc)^2 = N^2 \quad (3)$$

Iz enačbe (3), katere analog je enačba (2), ne moremo sklepati nič o relativni velikosti $ad \pm bc$ in N , zato nam ne koristi pri dokazovanju netrivialnosti razcepa.

5 Pellove družine in netrivialnost

Čeprav za faktorizacijo s hiperbolo ne velja, da je razcep vedno netrivialen, bomo v tem razdelku videli, da obstajajo določene družine točk, ki ležijo na hiperboli $H : mx^2 - ny^2 = N$, za katere velja, da vedno porodijo trivialen razcep.

Definicija 1: Naj bosta (a, b) in (c, d) celoštevilski točki na hiperboli $H : mx^2 - ny^2 = N$. Naj bosta (α^+, β^+) in (α^-, β^-) definirani kot

$$\begin{bmatrix} \alpha^\pm \\ \beta^\pm \end{bmatrix} = \frac{1}{N} \begin{bmatrix} mac \pm nbd \\ ad \pm bc \end{bmatrix}, \quad (4)$$

Potem pravimo, da sta točki (a, b) in (c, d) Pellovo povezani natanko tedaj, ko sta (α^+, β^+) ali (α^-, β^-) , ki zadoščata Pellovi enačbi $x^2 - mny^2 = 1$, celoštevilski točki.

Opomba: Po enačbi (3), točki, definirani kot v (4), zadoščata Pellovi enačbi.

Zgled 4: Če vzamemo za $(a, b) = (63, 31)$ in za $(c, d) = (47, 9)$, kot v *Zgledu 3.1*, kjer smo imeli netrivialno faktorizacijo, sta dve racionalni točki, definirani v (4), enaki $(\alpha^-, \beta^-) = (\frac{27}{23}, -\frac{10}{23})$ ter $(\alpha^+, \beta^+) = (\frac{153}{89}, \frac{88}{89})$. Vidimo, da nobena od teh dveh točk ni celoštevilski rešitev Pellove enačbe $x^2 - 2y^2 = 1$. Torej točki nista Pellovo povezani.

Zgled 5: Po drugi strani, če za (a, b) in (c, d) vzamemo točki iz *Zgleda 3.2*, dobimo

$$\begin{bmatrix} \alpha^+ \\ \beta^+ \end{bmatrix} = \frac{1}{2047} \begin{bmatrix} 63 \cdot 65 + 2 \cdot 31 \cdot 33 \\ 63 \cdot 33 + 31 \cdot 65 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}.$$

Torej je (α^+, β^+) celoštevilski rešitev Pellove enačbe $x^2 - 2y^2 = 1$. Tako smo pokazali, da sta točki (a, b) in (c, d) Pellovo povezani.

Opomba: Če imamo dano celoštevilsko točko (a, b) na hiperboli in Pellovo rešitev $\alpha^2 - mn\beta^2 = 1$, lahko zapišemo

$$N \cdot 1 = (ma^2 - nb^2)(\alpha^2 - mn\beta^2) = m(\alpha a + n\beta b)^2 - n(m\beta a + \alpha b)^2$$

in drugo Pellovo povezano točko (c, d) lahko dobimo kot

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} \alpha & n\beta \\ m\beta & \alpha \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}. \quad (5)$$

Tako lahko iz ene točke (a, b) na hiperboli $mx^2 - ny^2 = N$ dobimo celo družino Pellovo povezanih točk z množenjem prvotne točke s potencami matrike iz (5). Domnevamo, da dve Pellovo povezani točki vedno porodita trivialen razcep, kar potrdi tudi naslednji izrek.

Izrek 4: Če lahko liho, pozitivno celo število N zapišemo na dva načina kot $N = ma^2 - nb^2 = mc^2 - nd^2$, kjer so $a, b, c, d, m, n \in \mathbb{Z}^+$ in velja $(ma, nb) = (mc, nd) = 1$, potem je faktorizacija

$$N = (N, ad - bc)(N, ad + bc)$$

trivialna natanko tedaj, ko sta (a, b) in (c, d) Pellovo povezani.

Literatura

- [1] Richard Blecksmith, John Brillhart and Michael Decaro: Using Conic Sections to Factor Integers,
<https://www.jstor.org/stable/10.4169/amer.math.monthly.123.2.168>
- [2] John Brillhart: A Note on Euler's Factoring Problem,
<https://www.jstor.org/stable/40391253>
- [3] Richard Blecksmith, John Brillhart and Michael Decaro: The Completion of Euler's Factoring Formula,
<https://www.jstor.org/stable/44240179>