SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Dario Maltarski

SITO POLJA BROJEVA

Diplomski rad

Voditelj rada:
Doc. dr. sc. Filip Najman

Zagreb, rujan 2014.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Prosti brojevi su osnovni blokovi iz kojih možemo koristeći operaciju množenja dobit bilo koji prirodan broj. Otkad postoji želja za proučavanjem prirodnih brojeva postoji i želja da se složeni brojevi "razbiju" na proste. Postupak reduciranja nekog broja na proste zovemo faktorizacija. U ovom radu bavit ćemo se problemom netrivijalne faktorizacije velikih prirodnih brojeva. Osim što se radi o važnom problemu u teoriji brojeva, također se radi o zahtjevnom problemu iz pozicije složenosti algoritama.

Usprkos tome što postoje algoritmi koji brzo, tj. u polinomnom vremenu mogu provjeriti prostost nekog broja (AKS test prostosti), problem netrivijalne faktorizacije cijelih brojeva je NP problem, tj. trenutno nisu poznati algoritmi koji mogu u polinomnom vremenu netrivijalno faktorizirati velike cijele brojeve na konkretnom računalu ili više njih. Najteže je faktorizirati velike cijele brojeve koji imaju velike proste faktore. Sigurnost nekih kriptosustava temelji se upravo na toj činjenici, te bi pronalaskom brzog algoritma za faktorizaciju prirodnih brojeva oni postali nesigurni.

U 1. poglavlju navest ćemo definicije osnovnih pojmova te iskazati neke važne teoreme iz teorije brojeva koje ćemo kasnije koristiti, od kojih je najvažniji osnovni teorem aritmetike koji nam garantira postojanje i jedinstvenost faktorizacije složenog broja na proste brojeve. Nakon toga ćemo pogledati kako je tekao napredak u razumijevanju složenih i prostih brojeva te faktorizaciji kroz povijest, uz naglasak na razvoj algoritama iz teorije brojeva. Spomenut ćemo trenutne značajne faktorizacijske rekorde i detaljnije se upoznati s važnošću problema faktorizacije za sigurnost kriptosustava s javnim ključem, poput RSA kriptosustava.

U 2., 3. i 4. poglavlju opisat ćemo redom algoritme racionalnog, kvadratnog i specijalnog sita. Najprije ćemo opisati algoritam Fermatove faktorizacije. Svi prethodno navedeni algoritmi temelje se na tom algoritmu, samo što koriste metodu faktorske baze te pokušavaju množenjem relacija kongruencije modulo n, gdje je n broj koji želimo faktorizirati, dobiti kongruenciju kvadrata $a^2 \equiv b^2 \pmod{n}$, koja je zapravo poopćenje uvjeta $a^2 - b^2 = n$ iz Fermatove faktorizacije. Nakon što se dobije kongruencija kvadrata to često dovodi do netrivijalne faktorizacije broja n.

Racionalno sito nije efikasno i ne koristi se u praksi za faktorizaciju brojeva, ali je dobar uvod u razumijevanje kvadratnog i specijalnog sita. Kvadratno sito je najefikasniji

algoritam za faktorizaciju brojeva koji imaju 50 do 100 znamenki. Radi se o poboljšanju Dixonovog algoritma koji pokušava množenjem relacija oblika $a^2 \equiv a^2 - n \pmod{n}$ dobiti kvadrat s desne strane novonastale kongruencije čime bi se dobila kongruenciju kvadrata. Specijalno sito je najefikasniji faktorizacijski algoritam za brojeve specijalnog oblika poput primjerice Mersennovih i Fermatovih brojeva. Algoritam je sličan racionalnom, ali je postupak dobivanja relacija kongruencije efikasniji jer se za jednu stranu kongruencije koristi faktorska baza u proširenju prstena $\mathbb{Z}$.

Poglavlje 1

Faktorizacija prirodnih brojeva

Definicija 1.1. *Faktorizacija matematičkog objekta* A *je postupak pronalaženja matematičkih objekata* $A_1, A_2, \ldots, A_n$ *i operacija množenja* $\odot_1, \odot_2, \ldots, \odot_{n-1}$*, gdje je* $n \in \mathbb{N}$*, takvih da vrijedi*

$$A = A_1 \odot_1 A_2 \odot_2 \ldots \odot_{n-1} A_n.$$

Kažemo da je A *produkt faktora* $A_1, A_2, \ldots, A_n$*.*

Napomena 1.2. *U ovom radu ćemo pretpostaviti da vrijedi* $0 \notin \mathbb{N}$*, a sa* $\mathbb{N}_0$ *ćemo označavati skup* $\mathbb{N} \cup \{0\}$*.*

Napomena 1.3. *Primjetimo, za* $n = 1$ *i* $A_1 = A$ *imamo trivijalnu faktorizaciju* $A = A$*.*

Faktorizirati možemo različite matematičke objekte: brojeve, polinome, matrice itd. U nastavku ćemo se baviti isključivo faktorizacijom prirodnih brojeva na proste faktore. Ako je operacija množenja neasocijativna, npr. vektorski umnožak, potrebno je kod zapisa faktorizacije zagradama istaknuti redoslijed operacija. Mi ćemo se baviti množenjem cijelih brojeva koje je asocijativno, pa nećemo zagradama istaknuti redoslijed operacija. Sada ćemo navesti niz definicija, propozicija i teorema iz teorije brojeva koje ćemo koristiti u ovom, ali i kasnijim poglavljima.

Definicija 1.4. *Neka su* a *i* b *cijeli brojevi. Kažemo da* a *dijeli* b *(u oznaci* $a \mid b$*) ako postoji* $k \in \mathbb{Z}$ *takav da je* $b = ak$*. Broj* a *zovemo djeliteljem broja* b*, a broj* b *višekratnikom broja* a*. U suprotnom kažemo da* a *ne dijeli* b *i to označavamo sa* $a \nmid b$*.*

Relacija djeljivosti je relacija parcijalnog uređaja (refleksivna je, tranzitivna i antisimetrična) na skupu $\mathbb{N}$, ali nije na skupu $\mathbb{Z}$ (ne vrijedi antisimetričnost).

Teorem 1.5 (Teorem o dijeljenju s ostatkom)**.** *Za proizvoljne cijele brojeve* a *i* $b \neq 0$ *postoje jedinstveni cijeli brojevi* q *i* r *takvi da je* $a = qb + r, 0 \leq r < |b|$*.*

Broj r iz prethodnog teorema zovemo ostatak pri dijeljenju broja a brojem b i to možemo zapisati na sljedeći način $r = a \bmod b$. U slučaju da je $r = 0$ vrijedi $b \mid a$.

Definicija 1.6. *Neka su a i b cijeli brojevi. Cijeli broj v nazivamo zajednički višekratnik od a i b ako $a \mid v$ i $b \mid v$. Najmanji nenegativni među njima nazivamo najmanji zajednički višekratnik od a i b, u oznaci $V(a, b)$.*

Definicija 1.7. *Neka su a i b cijeli brojevi. Cijeli broj d nazivamo zajednički djelitelj od a i b ako $d \mid a$ i $d \mid b$. Ako je barem jedan od brojeva a i b različit od nule onda postoji samo konačno mnogo zajedničkih djelitelja od a i b. Najveći među njima nazivamo najveći zajednički djelitelj od a i b (ili mjera od a i b), u oznaci (a, b) ili $M(a, b)$.*

Teorem 1.8 (Bezoutova lema)**.** *Za cijele brojeve a i b vrijedi*

$$(b, c) = \min(\{bx + cy \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}).$$

Propozicija 1.9. *Ako $d \mid a$ i $d \mid b$, onda $d \mid (ax + by)$ za sve $x, y \in \mathbb{Z}$*

Budući da se ostatak dijeljenja dva broja može prikazati kao njihova linearna kombinacija, vrijedi sljedeći korolar.

Korolar 1.10. *Za sve $n, m \in \mathbb{N}$ vrijedi $(n, m) = (m, n \bmod m)$.*

Definicija 1.11. *Za cijele brojeve a i b kažemo da su relativno prosti ako vrijedi $(a, b) = 1$.*

Definicija 1.12. *Prirodan broj $p > 1$ je prost ako za svaki $d \in \{2, 3, \ldots, p - 1\}$ vrijedi $d \nmid p$. Ako prirodan broj $p > 1$ nije prost, onda kažemo da je složen. Broj 1 nije ni prost ni složen.*

Propozicija 1.13 (Euklidova lema)**.** *Ako je p prost broj i $p \mid ab$, onda $p \mid a$ ili $p \mid b$. Općenitije, ako $p \mid a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.*

Dokaze prethodnih teorema i propozicija možete naći u [8].

Teorem 1.14 (Osnovni teorem aritmetike)**.** *Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.*

Dokaz. Postojanje faktorizacije dokazujemo indukcijom. Broj 2 je prost i ima trivijalnu faktorizaciju. Pretpostavimo da postoji faktorizacija na proste faktore za sve brojeve manje od n. Ako je n prost broj, on ima primitivnu faktorizaciju. Ako je n složen tada postoje $1 < n_1, n_2 < n$ takvi da vrijedi $n = n_1 n_2$. Po pretpostavci indukcije postoje prosti brojevi $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ takvi da vrijedi

$$n_1 = p_1 p_2 \ldots p_k,$$

$$n_2 = q_1 q_2 \dots q_l.$$

Tada postoji i faktorizacija na proste faktore broja n:

$$n = n_1 n_2 = p_1 p_2 \dots p_k q_1 q_2 \dots q_l.$$

Sada ćemo dokazati da je faktoriizacija broja na proste faktore jedinstvena do na poredak faktora. Pretpostavimo da n ima dvije različite faktorizacije na proste faktore, takve da se jedna faktorizacija ne može dobiti iz druge zamjenom poretka faktora. Dijelimo te reprezentacije s prostim brojevima koji su zajednički objema reprezentacijama. Budući da su reprezentacije različite, dobit ćemo jednakost oblika

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s, \qquad (*)$$

gdje su p_i, q_j prosti brojevi takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve i, j. Medutim, to je nemoguće jer iz $p_1 \mid q_1 q_2 \cdots q_s$, po prethodnoj propoziciji (Euklidova lema), slijedi da p_1 dijeli barem jedan q_j . No, to znači da je $p_1 = q_j$, čime smo dobili kontradikciju s činjenicom da se niti jedan prost broj s lijeve strane jednakosti $(*)$ ne pojavljuje na desnoj strani. □

Ako sa p_i označimo i-ti prost broj, onda iz osnovnog teorema aritmetike slijedi da za svaki prirodan broj n vrijedi

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

gdje su $\alpha_1, \alpha_2, \dots, \alpha_k$ nenegativni cijeli brojevi, a p_k najveći prost broj koji dijeli n. Ovakav prikaz broja n zovemo kanonski rastav broja n na proste faktore. Budući da za svaki $l > k$ i $\alpha_{k+1}, \alpha_{k+2}, \dots, \alpha_l = 0$ vrijedi

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{l} p_i^{\alpha_i},$$

kanonski rastav broja n na proste faktore možemo označiti sa

$$n = \prod_{i} p_i^{\alpha_i}.$$

Neka prirodni brojevi a i b imaju sljedeće kanonske rastave na proste brojeve

$$a = \prod_{i} p_i^{\alpha_i}, \; b = \prod_{i} p_i^{\beta_i}.$$

Iz definicije najmanjeg zajedničkog višekratnika slijedi da on očito mora imati sljedeći kanonski rastav na proste brojeve

$$V(a, b) = \prod_{i} p_i^{\max\{\alpha_i, \beta_i\}}.$$

Analogno, najveći zajednički djelitelj mora imati sljedeći kanonski rastav na proste brojeve

$$(a, b) = \prod_i p_i^{\min\{\alpha_i, \beta_i\}}.$$

Propozicija 1.15. *Neka su* a, b, c *i* d *neki cijeli brojevi. Ako vrijedi* $a \mid b$ *i* $c \mid d$*, onda vrijedi i* $ac \mid bd$.

Dokaz. Pretpostavimo da vrijedi $a \mid b$ i $c \mid d$. Tada postoje cijeli brojevi k_1 i k_2 takvi da vrijedi $b = k_1 a$ i $d = k_2 b$. Množenjem prethodnih jednakosti dobivamo $bd = (k_1 k_2)ac$. □

Propozicija 1.16. *Neka su* a, b *i* n *neki prirodni brojevi. Ako* $a \mid n$ *i* $b \mid n$*, onda vrijedi* $V(a, b) \mid n$.

Dokaz. Pretpostavimo da brojevi a, b i n imaju sljedeće kanonske rastave na proste faktore

$$a = \prod_i p_i^{a_i},\ b = \prod_i p_i^{b_i},\ n = \prod_i p_i^{n_i}.$$

Iz $a \mid n$ slijedi da za svaki i vrijedi $n_i \geq a_i$, a iz $b \mid n$ slijedi da za svaki i vrijedi $n_i \geq b_i$, stoga očito za svaki i vrijedi $n_i \geq \max\{a_i, b_i\}$. Zaključujemo da za svaki i vrijedi $p^{\max\{a_i, b_i\}} \mid p^{n_i}$ Konačno, po prethodnoj propoziciji slijedi

$$V(a, b) = \prod_i p^{\max\{a_i, b_i\}} \mid \prod_i p^{n_i} = n.$$

□

Propozicija 1.17. *Neka su* a, b *i* n *neki prirodni brojevi. Ako* $n \mid ab$*, onda vrijedi* $n \mid (a, n)(b, n)$

Dokaz. Dajemo kanonske rastave na proste faktore brojeva a, b i n

$$a = \prod_i p_i^{a_i},\ b = \prod_i p_i^{b_i},\ n = \prod_i p_i^{n_i}.$$

Zbog tranzitivnosti relacije djeljivosti za proizvoljan prirodan broj j vrijedi $p_j^{n_j} \mid ab$, odnosno $p_j^{n_j} \mid p_j^{a_j} p_j^{b_j}$, iz čega zaključujemo $n_j \leq a_j + b_j$, što dalje povlači $n_j \leq \min\{a_j, n_j\} + \min\{b_j, n_j\}$ Dakle vrijedi

$$p_j^{n_j} \mid p_j^{\min\{a_j, n_j\}} p_j^{\min\{b_j, n_j\}}.$$

Budući da očito $p_j^{\min\{a_j,n_j\}}$ dijeli (a,n), te $p_j^{\min\{b_j,n_j\}}$ dijeli (b,n), koristeći Propoziciju 1.15 i tranzitivnost relacije dijeljenja zaključujemo da vrijedi

$$p_j^{n_j} \mid (a,n)(b,n).$$

Kako je n najmanji zajednički višekratnik brojeva $p_i^{n_i}$, iz prethodne propozicije slijedi $n \mid (a,n)(b,n)$. □

Osnovni teorem aritmetike govori da su prosti brojevi osnovni gradivni blokovi pomoću kojih možemo izgraditi bilo koji prirodni broj njihovim množenjem. Postavlja se logično pitanje: Koliko ima tih blokova?

Teorem 1.18 (Euklidov teorem)**.** *Prostih brojeva ima beskonačno mnogo.*

Dokaz. Pretpostavimo da ima n prostih brojeva, gdje je $n \in \mathbb{N}$. Sa p_i ćemo označavati i-ti prost broj, za $i \in \{1,2,\ldots,n\}$. Sada definiramo prirodan broj m na sljedeći način

$$m := 1 + \prod_{i=1}^{n} p_i.$$

Broj m je očito složen jer vrijedi $m > p_n$, a p_n je najveći prost broj. Budući da je m složen, postoji $k \in \{1,2,\ldots,n\}$ takav da vrijedi $p_k \mid m$. Očito vrijedi i $p_k \mid \prod_{i=1}^{n} p_i$ pa po Propoziciji (1.9) p_k dijeli i razliku

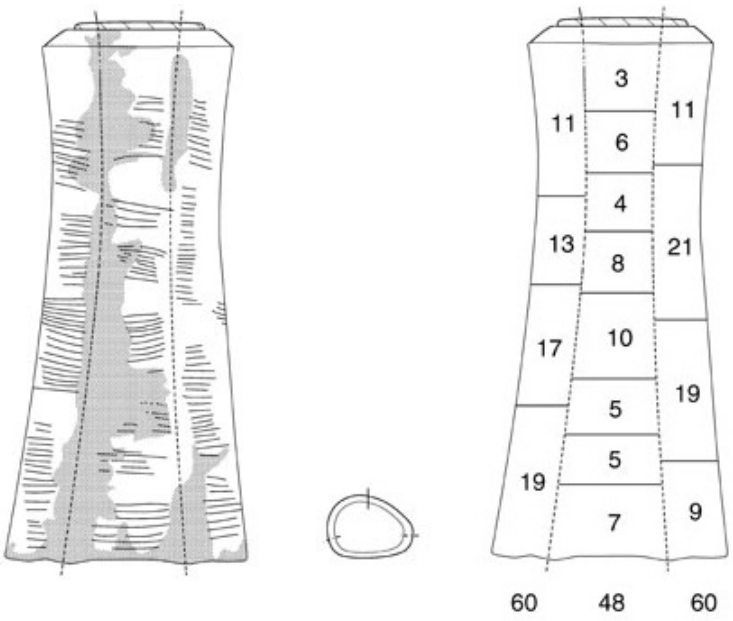
$$(1 + \prod_{i=1}^{n} p_i) - (\prod_{i=1}^{n} p_i).$$

Zaključujemo $p_k \mid 1$ što je kontradikcija. Dakle prostih brojeva ima beskonačno mnogo. □

1.1 Povijest

1960 godine belgijski geolog Jean de Heinzelin de Braucourt na području Ishanga (u središnjoj Africi između Konga i Ugande) pronašao je kost (fibula pavijana) staru 25000 godina koja je imala tri retka grupiranih ureza koji bi mogli predstavljati brojeve. Ukoliko urezi na kosti predstavljaju brojeve, to bi moglo značiti da su ljudi razlikovali proste i složene brojeve pred 25000 godine, jer se u jednom retku nalaze samo prosti brojevi između 10 i 20, tj. 11, 13, 17 i 19.

Drevni Egipćani su imali običaj sve razlomke pisati u obliku sume jediničnih razlomaka, tj. razlomaka kojima je brojnik 1. Na Rhindovom papirusu, nastalim oko 1650.



Slika 1.1: Matematička interpretacija ureza na Ishanga kosti

godine pr.Kr., nalaze se raspisi brojeva oblika $2/n$ kao sume jediničnih razlomaka, pri čemu se zapisi razlikuju ovisno o tome je li n složen ili prost broj, što pokazuje da su Egipćani razlikovali proste i složene brojeve.

Oko 300. god. pr. Kr. grčki matematičar Euklid objavio je djelo Elementi, u kojem je u 13 knjiga sustavno prikazao sva dotadašnja znanja iz geometrije, ali i drugih dijelova matematike. Za nas su zanimljive 7., 8. i 9. knjiga koje se bave Teorijom brojeva.

U njima je dokazan specijalan slučaj Euklidove leme za produkt dva broja (vidi [13, Propozicija VII.30]). Također Euklid je dokazao da je svaki prirodan broj ili prost ili je djeljiv prostim brojem (vidi [13, Propozicije VII.31, VII.32]) iz čega lako induktivnim korakom možemo dokazati egzistencijalni dio osnovnog teorema aritmetike (Teorem 1.14). Euklidov dokaz Euklidovog teorema (vidi [13, Propozicija IX.20]) jednak je našem (vidi Teorem 1.18). Kad kažemo da su Euklidovi dokazi jednaki našima, to ne valja shvatiti doslovno, jer Euklid ne koristi suvremenu matematičku notaciju, a način razmišljanja mu je "geometrijski" (prirodne brojeve poistovjećuje s duljinama dužina, a dijeljenje s mjerenjem, tj. nanošenjem jedne dužine na drugu). Euklid je proučavao Mersennove brojeve.

Definicija 1.19. *Brojevi oblika* $2^p - 1$*, gdje je* p *prost broj, zovu se Mersennovi brojevi.*

Propozicija 1.20. *Ako je* n *složen broj, tada je* $2^n - 1$ *složen broj.*

Dokaz. Dokažimo obrat po kontrapoziciji, tj. da je n prost broj, ako je $2^n - 1$ prost. Pretpostavimo da je n složen, tj. $n = ab, a > 1, b > 1$. Tada je

$$2^{ab} - 1 = 2^{ab} + \left(\sum_{k=1}^{b-1} 2^{ka} - \sum_{k=1}^{b-1} 2^{ka}\right) - 1 = 2^a\left(2^{(b-1)a} + \sum_{k=0}^{b-2} 2^{ka}\right) - \left(\sum_{k=1}^{b-1} 2^{ka} + 1\right)$$
$$= (2^a - 1)\sum_{k=0}^{b-1} 2^{ka}$$

složen, što je kontradikcija jer broj ne može biti i prost i složen. Dakle, ako je $2^n - 1$ prost, onda je n prost, odnosno ako je n složen, onda je $2^n - 1$ složen. □

Obrat prethodne propozicije ne vrijedi. Neki Mersennovi brojevi su prosti, dok su neki složeni, kao npr. $2^{11} - 1 = 23 \cdot 89$. Smatra se da ima beskonačno mnogo prostih Mersennovih brojeva (Lenstra-Pomerance-Wagstaff slutnja). Do siječnja 2013. godine poznato je 48 prostih Mersennovih brojeva. 10 najvećih poznatih prostih brojeva su Mersennovi brojevi. Najveći poznati prost broj je Mersennov broj $2^{57,885,161} - 1$.

Jedno od bitnijih pitanja u mnogim granama matematike poput teorije brojeva, teorije složenosti, kriptografije i drugih grana je kako efikasno izračunati faktorizaciju velikih brojeva na proste faktore. Euklid je dao algoritam za pronalaženje najvećeg zajedničkog djelitelja (vidi [13, Propozicije VII.1, VII.2, X.2, X.3]), koji se koristi u mnogim faktorizacijskim algoritmima, poput Pollardove ρ metode, Dixonove metode ili Shorovog algoritma. Euklidov algoritam jedan je od najstarijih poznatih algoritama.

Ulaz: nenegativni cijeli brojevi a i b
Izlaz: najveći zajednički djelitelj brojeva a i b

sve dok $b \neq 0$ **radi**
  $t \leftarrow b$;
  $b \leftarrow a \bmod t$;
  $a \leftarrow t$;
vrati a;

Algoritam 1.1.1: Euklidov algoritam

Ako u i-tu iteraciju petlje algoritma ulaze brojevi a_i i a_{i+1}, onda u $(i+1)$-u iteraciju ulaze brojevi a_{i+1} i $a_i \bmod a_{i+1}$, pa iz Korolara 1.10 slijedi korektnost algoritma.

Kako je vremenska složenost osnovnih aritmetičkih operacija polinomna, Euklidov algoritam je polinomne vremenske složenosti (dokaz pogledajte u [29, Propozicija 2.18]), za razliku od izvornog Euklidovog algoritma, tj. algoritma kakvog ga je opisao Euklid u Elementima, koji nije polinomne složenosti jer je se u njemu do ostatka dijeljenja dolazilo na složeniji način.

Ukoliko nas ne zanima faktorizacija broja, već samo odgovor na pitanje je li broj prost ili nije, umjesto faktorizacijskih algoritama koristimo testove prostosti, tj. algoritme koji odlučuju je li zadani broj prost. Svaki faktorizacijski algoritam je ujedno i test prostosti, dok obaratno ne vrijedi. Budući da testovi prostosti ne trebaju pronaći sve faktore zadanog broja, oni su vremenski efikasniji od faktorizacijskih algoritama.

U 3. st. pr. Kr. grčki matematičar Eratosten osmislio je algoritam Eratostenovo sito i to je prvi poznati test prostosti. Algoritam pronalazi sve proste brojeve manje ili jednake zadanom broju. Prije analize složenosti dajemo pseudokod Eratostenovog sita.

Ulaz: prirodan broj $n > 1$
Izlaz: lista svih prostih brojeva manjih ili jednakih n

```
Brojevi ← novo polje(n + 1);
Brojevi[0] ← 0;
Brojevi[1] ← 0;
za i ← 2 do n radi
    Brojevi[i] ← 1;
i ← 2;
n_0 ← √n;
sve dok i < n_0 radi
    ako Brojevi[i] = 1 onda
        j ← i^2;
        sve dok j < n radi
            Brojevi[j] ← 0;
            j ← j + i;
    i = i + 1;
Prosti ← ∅;
za i ← 2 do n radi
    ako Brojevi[i] = 1 onda
        dodaj(Prosti,i);
vrati Prosti;
```

Algoritam 1.1.2: Eratostenovo sito

Algoritam redom "precrtava" sve višekratnike prostih ("neprecrtanih") brojeva manjih od $\sqrt{n}$. Za neki prost broj $p < \sqrt{n}$, postoji najviše n/p njegovih višekratnika koji su manji od n, pa će algoritam ukupno precrtati

$$\sum_{p_i \leq \sqrt{n}} \frac{n}{p_i}$$

brojeva, gdje su p_i prosti brojevi.

Sada iskazujemo teorem koji će nam pomoći da damo "lijepe" ocjene za prethodnu sumu. Dokaz teorema je podosta složen i možete ga naći u [30, str. 26].

Teorem 1.21 (Mertensov teorem)**.** *Neka je* n *neki prirodan broj i* S *skup prostih brojeva. Tada postoji* $c > 0$ *takav da vrijedi*

$$\sum_{\substack{p \in S \\ p \leq n}} \frac{1}{p} = \ln(\ln(n)) + c + O\left(\frac{1}{\ln(n)}\right).$$

Pod pretpostavkom da je vremenska složenost aritmetičkih operacija $\Theta(\log_2(n))$, iz prethodnog teorema slijedi da je složenost algoritma $\Theta(n \log_2(n) \log_2(\log_2(n)))$. Eratostenov algoritam je primjer pseudopolinomnog algoritma.

Definicija 1.22. *Algoritme koji su vremenski polinomni s obzirom na ulaz* n*, a eksponencijalni s obzirom na duljinu ulaza* $\lfloor \log_2(n) \rfloor + 1$ *zovemo pseudopolinomni algoritmi.*

Kod većine algoritama vremenska složenost predstavlja veći problem, ali kod Eratostenovog sita ni prostorna složenost nije polinomna budući da je duljina izlaza

$$\prod_{p_i \leq \sqrt{n}} \log_2(p_i) = \Theta(n),$$

(dokaz pogledajte u [25, Teorem 9])

Najstariji zapis algoritma dao je u 1. stoljeću Nikomah u djelu "Uvod u aritmetiku" (vidi [20, Poglavlje I.XIII]). Najvažnija razlika u odnosu na "naš" algoritam je ta da je izvorni algoritam prilikom svakog precrtavanja broja "zapamtio" njegovog djelitelja, pa je na kraju za svaki složeni broj manji od n vratio sve njegove djelitelje.

1.2 Faktorizacijski rekordi

Trenutna granica do koje se uspješno mogu faktorizirati proizvoljni dekadski brojevi je oko 170 znamenki, dok je granica za test prostosti (ili složenosti) 15000 znamenki. Za teoriju kompleksnosti je od velikog interesa pronaći brzi algoritam za faktorizaciju prostih brojeva, budući da ne postoji algoritam koji bi faktorizirao cijeli broj n u polinomnom vremenu u odnosu na $\log n$. Može se pokazati je li broj prost testovima prostosti u polinomnom vremenu, međutim ti testovi ne generiraju faktore promatranog broja. Trenutno asimptotski najbrži algoritam za faktorizaciju cijelih brojeva je opće sito polja brojeva, čije vrijeme izvršavanja za cijeli broj n se procjenjuje na

$$\exp\left[(\log n)^{1/3}\left(\left(\frac{64}{9} + o(1)\right)\log\log n\right)^{2/3}\right]$$

1.3 Primjena u kriptografiji

U današnje doba zbog sve veće ekspanzije modernih tehnologija i potrebe za elektronskom komunikacijom, sigurnost podataka jedan je od najbitnijih izazova današnjice. Grana matematike koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati je kriptografija. Osnovni zadatak kriptografije je omogućiti dvjema osobama (zvat ćemo ih pošiljalac i primalac) komuniciranje preko nesigurnog komunikacijskog kanala (telefonska linija, računalna mreža, ...) na način da treća osoba, koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke.

Definicija 1.23. *Kriptosustav je uređena petorka* $(\mathcal{P}, C, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elementa otvorenog teksta;*
2. C *je konačan skup svih mogućih osnovnih elemenata šifrata;*
3. $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva;*
4. *Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$. *Pritom su* $e_K : \mathcal{P} \to C$ *i* $d_K : C \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$.

Kriptosustave možemo podijeliti na kriptosustave s tajnim ključem (simetrični kriptosustavi) i kriptosustave s javnim ključem (asimetrični kriptosustavi). Kod simetričnih kriptosustava pošiljalac i primalac bi tajno izabrali ključ K, koji bi onda generirao funkcije za šifriranje e_K i dešifriranje d_K. Pritom je d_K ili isti kao e_K ili se iz njega lako dobije. Za sigurnost ovih kriptosustava nužna je tajnost ključa. No, to je i njihov veliki nedostatak, budući da prije šifriranja pošiljalac i primalac moraju biti u mogućnosti razmjeniti tajni ključ preko nekog sigurnog komunikacijskog kanala (ili se osobno susresti). Štoviše, oni bi morali često mijenjati ključeve, budući da šifriranje više poruka istim ključem znatno smanjuje sigurnost.

Definicija 1.24. *Kriptosustav s javnim ključem se sastoji od dviju familija* $\{e_K\}$ *i* $\{d_K\}$ *funkcija za šifriranje i dešifriranje (ovdje* K *prolazi skupom svih mogućih korisnika) sa svojstvom:*

1. *Za svaki* K *je* d_K *inverz* e_K.
2. *Za svaki* K *je* e_K *javan, ali je* d_K *poznat samo osobi* K.
3. *Za svaki* K *je* e_K *osobna jednosmjerna funkcija.*

e_K *se zove javni ključ, a* d_K *privatni (ili osobni ili tajni) ključ.*

Uspješnost kriptosustava najviše ovisi o nemogućnosti treće osobe da dešifrira šifrat koji se šalje kroz komunikacijski kanal. Kod kriptosustava s javnim ključem možemo uspješnom faktorizacijom komponente javnog ključa dobiti dvije od tri komponente privatnog ključa. Zadnju komponentu će nakon toga biti lako otkriti, a poznavajući privatni ključ moći ćemo dešifrirati poruku. Za sigurnost kriptosustava s javnim ključem je dakle važno da se odabere javni ključ koji je teško faktorizirati. Obično se stoga za javni ključ najčešće uzimaju veliki poluprosti brojevi ili općenito brojevi koji su produkt više velikih prostih brojeva.

Definicija 1.25. *Broj* $n \in \mathbb{N}$ *je poluprost ili biprost ako je produkt točno dva, ne nužno različita, prosta broja, tj. ako postoje prosti brojevi* $p_1, p_2 \in \mathbb{N}$ *takvi da vrijedi* $n = p_1 p_2$.

Tvrtka "RSA Laboratories", koju su osnovali tvorci jednog od najpoznatijih i najkorištenijih kriptosustava s javnim ključem, RSA kriptosustava, objavila je 1991. god. nagradni natječaj "RSA Factoring Challenge", u kojem su dali listu poluprostih brojeva zajedno sa novčanim iznosom koji se dobije za uspješnu faktorizaciju pripadnog broja. Ti brojevi su poznati kao RSA brojevi. 1999. god. 155 znamenkasti, 512 bitni broj RSA-155 je korištenjem nekoliko stotina računala faktoriziran, što je značilo da se moralo polako preći s korištenja 512 bitnih na 1024 bitne ključeve. RSA-155, kao i svi RSA brojevi koji su faktorizirani poslije njega, su faktorizirani korištenjem algoritma općeg sita. U međuvremenu je "RSA Laboratories" 2007. godine ukinuo "RSA Factoring Challenge". Trenutno najveći faktorizirani RSA broj je 232 znamenkasti, 768 bitni broj RSA-768, koji je faktoriziran 2009. god. Dakle, 1024 bitni RSA kriptosustav se trenutno još uvijek može smatrati sigurnim.

Poglavlje 2

Racionalno sito

Prije nego opišemo algoritam racionalnog sita, opisat ćemo algoritam Fermatove faktorizacije. Racionalno sito, ali i mnogi drugi algoritmi koriste kongruenciju kvadrata za faktorizaciju, a ona je zapravo poopćenje Fermatove metode. Sada dajemo pseudokod algoritma Fermatove faktorizacije.

Ulaz: prirodan broj n
Izlaz: brojevi a i b, takvi da vrijedi $n = ab$

ako $n \bmod 2 == 0$ **onda**
  vrati $\left(\frac{n}{2}, 2\right)$;
$x \leftarrow \left\lceil \sqrt{n} \right\rceil$;
$y2 \leftarrow x^2 - n$;
sve dok $y2$ *nije potpuni kvadrat* **radi**
  $x \leftarrow x + 1$;
  $y2 \leftarrow x^2 - n$;
vrati $\left(x + \sqrt{y2}, x - \sqrt{y2}\right)$;

Algoritam 2.0.1: Fermatova faktorizacija

Propozicija 2.1. *Za svaki neparan broj* $n \in \mathbb{N}$ *i brojeve* $a, b \in \mathbb{N}$ *takve da vrijedi* $n = ab$ *postoje brojevi* $x, y \in \mathbb{N}_0$ *takvi da vrijedi* $n = x^2 - y^2$.

Dokaz. Možemo pretpostaviti bez smanjenja općenitosti da vrijedi $a \geq b$. Uzmimo sljedeće vrijednosti x i y

$$x = \frac{a+b}{2}, y = \frac{a-b}{2}.$$

Brojevi a i b su oba neparni jer je n neparan, pa očito vrijedi $x, y \in \mathbb{N}_0$. Preostaje nam provjeriti je li zadovoljeno $n = x^2 - y^2$

$$x^2 - y^2 = (x+y)(x-y) = \left(\frac{a+b}{2} + \frac{a-b}{2}\right)\left(\frac{a+b}{2} - \frac{a-b}{2}\right) = ab = n.$$

□

Opišimo rad algoritma. Pretpostavimo da želimo faktorizirati $n \in \mathbb{N}$. Ukoliko je n paran broj imamo netrivijalnu faktorizaciju i algoritam završava. Budući da se svaki neparni broj po prethodnoj propoziciji može napisati kao razlika kvadrata, postoje $x, y \in \mathbb{N}$ takvi da vrijedi $n = x^2 - y^2 = (x+y)(x-y)$. Sada je samo potrebno naći brojeve x i y takve da to vrijedi. Budući da vrijedi $x^2 - n = y^2 \geq 0$, mora vrijediti i $x^2 \geq n$. Na početku uzimamo $x = \left\lceil \sqrt{n} \right\rceil$, a potom inkrementiramo vrijednost od x sve dok ne dobijemo da je $x^2 - n$ potpuni kvadrat. Ukoliko n ima netrivijalnu faktorizaciju algoritam će ju naći. U najgorem slučaju n nema netrivijalnu faktorizaciju, te će algoritam stati za $x = (n+1)/2$ i dati trivijalnu faktorizaciju. Algoritam će najbrže raditi kada je n umnožak dva bliska broja, a najduže kada je n prost broj. Budući da je broj potpunih kvadrata manjih od n relativno mali ($\sqrt{n}$), možemo zaključiti da je u najvećem broju slučaja algoritam ipak neefikasan.

Primjer 2.2. *Želimo faktorizirati* $n = 1147$. *Uzimamo* $x = \left\lceil \sqrt{1147} \right\rceil = 34$. *Tada je* $34^2 - 1147 = 9$ *što je potpuni kvadrat, pa je* $y = \sqrt{9} = 3$. *Dakle tražena faktorizacija je* $n = (34+3)(34-3) = 37 \cdot 31$.

Osim u slučajevima gdje je n umnožak dva bliska broja, Fermatova faktorizacija je spor algoritam, jer je najčešće potrebno dugo tražiti brojeve x i y koji zadovoljavaju $n = x^2 - y^2$. Međutim, do netrivijalnih faktora broja n možemo doći tako da tražimo brojeve x i y koji zadovoljavaju slabiji uvjet, točnije takve da $x^2 - y^2$ ne mora biti jednak n, već samo mora biti djeljiv sa n uz uvjet da $x+y$ i $x-y$ nisu djeljivi s n (u suprotnom će faktorizacija biti trivijalna). Prije iskaza teorema o kongruenciji kvadrata i opisa algoritma racionalnog sita dajemo definicije nekih pojmova koje ćemo koristiti.

Definicija 2.3. *Za prirodan broj* n *kažemo da su cijeli brojevi* a *i* b *kongruentni modulo* n*, u oznaci* $a \equiv b \pmod{n}$ *ako vrijedi* $n \mid a - b$. *U protivnom, kažemo da* a *i* b *nisu kongruentni modulo* n *i pišemo* $a \not\equiv b \pmod{n}$.

Propozicija 2.4. *Za prirodan broj* n *i cijele brojeve* a *i* b *vrijedi* $a \equiv b \pmod{n}$ *ako i samo ako* a *i* b *imaju isti ostatak pri dijeljenju s* n*, tj.* $a \bmod n = b \bmod n$.

Dokaz. Pretpostavimo prvo da vrijedi $a \equiv b \pmod{n}$. Po teoremu o dijeljenju s ostatkom (Teorem 1.5) postoje jedinstveni cijeli brojevi q_1, q_2, r_1 i r_2 takvi da vrijedi $a = q_1 n + r_1, 0 \leq r_1 < n$ i $b = q_2 n + r_2, 0 \leq r_2 < n$. Tada vrijedi

$$a - b = q_1 n + r_1 - (q_2 n + r_2) = (q_1 - q_2)n + (r_1 - r_2).$$

Budući da po definiciji kongruentnosti vrijedi $n \mid a - b$, očito mora vrijediti $n \mid r_1 - r_2$, što je moguće samo ako je $r_1 = r_2$.

Pretpostavimo sada da vrijedi $r := a \bmod n = b \bmod n$. Tada postoje jedinstveni cijeli brojevi q_1 i q_2 takvi da vrijedi $a = q_1 n + r$ i $b = q_2 n + r$, pa oduzimanjem tih jednakosti dobivamo $a - b = (q_1 - q_2)n$. Dakle vrijedi $n \mid a - b$. □

Propozicija 2.5. *Relacija "biti kongruentan modulo n" je relacija ekvivalencije na skupu $\mathbb{Z}$.*

Dokaz prethodne propozicije možete naći u [8, Propozicija 2.1].

Propozicija 2.6. *Neka je n prirodan, te a, b, c i d cijeli brojevi. Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, onda je $a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$ i $ac \equiv bd \pmod{n}$.*

Dokaz. Neka je $a - b = nk$ i $c - d = nl$. Tada je $(a + c) - (b + d) = n(k + l)$ i $(a - c) - (b - d) = n(k - l)$, pa je $a + c \equiv b + d \pmod{n}$ i $a - c \equiv b - d \pmod{n}$. Zbog $ac - bd = a(c - d) + d(a - b) = n(al + dk)$ slijedi da je $ac \equiv bd \pmod{n}$. □

Propozicija 2.7. *Neka je n prirodan, te a, b i k cijeli brojevi takvi da su k i n relativno prosti. Ako je $ka \equiv kb \pmod{n}$, onda vrijedi $a \equiv b \pmod{n}$.*

Dokaz. Iz $ka \equiv kb \pmod{n}$ zaključujemo da vrijedi $ka - kb = k(a - b) \equiv 0 \pmod{n}$. Zaključujemo da n dijeli $k(a - b)$, no kako su k i n relativno prosti, nijedan prost faktor od n ne dijeli k. Dakle vrijedi $n \mid a - b$ iz čega dalje slijedi $a - b \equiv 0 \pmod{n}$ i konačno $a \equiv b \pmod{n}$. □

Teorem 2.8 (Teorem o kongruencija kvadrata)**.** *Ako za prirodan broj n te za cijele brojeve x i y takve da je $x \not\equiv \pm y \pmod{n}$ vrijedi kongruencija $x^2 \equiv y^2 \pmod{n}$, onda vrijedi $n \mid (x + y, n)\,(x - y, n)$, gdje su $(x + y, n)$ i $(x - y, n)$ različiti od 1 i n.*

Dokaz. Za x^2 i y^2 postoje k_1, k_2 i $l < n$ takvi da vrijedi

$$x^2 = k_1 n + l \quad \text{i} \quad y^2 = k_2 n + l,$$

pa oduzimanjem prethodnih jednakosti i primjenom formule za razliku kvadrata dobivamo

$$(x + y)\,(x - y) = (k_1 - k_2)\,n.$$

Zaključujemo da vrijedi $n \mid (x + y)(x - y)$, pa onda po Propoziciji 1.17 vrijedi i

$$n \mid (x + y, n)\,(x - y, n)\,.$$

Iz $x \not\equiv \pm y \pmod{n}$ slijedi $n \nmid (x+y)$ i $n \nmid (x-y)$, pa je stoga $(x+y, n) \neq n$ i $(x-y, n) \neq n$. Zbog $n \mid (x+y)(x-y)$ i $n \nmid (x-y)$ postoji prost broj p takav da $p \mid n$ i $p \mid x+y$, tj. $(x+y, n) \neq 1$. Analogno, postoji prost broj p takav da $p \mid n$ i $p \mid x-y$, pa vrijedi $(x-y, n) \neq 1$. Dakle, pokazali smo da su $(x+y, n)$ i $(x-y, n)$ netrivijalni djelitelji od n. □

Primjer 2.9. *Prvo valja primjetiti da postoje brojevi n za koje ne možemo naći brojeve x i y takve da vrijede pretpostavke teorema (npr. za $n = 10$).*

Uzmimo $n = 12$. Za $x = 5$ i $y = 1$ vrijede pretpostavke teorema $5 \not\equiv \pm 1 \pmod{12}$, te $5^2 = 25 \equiv 1^2 = 1 \pmod{12}$. Budući da je $(5+1, 12) = 6$ i $(5-1, 12) = 4$ vidimo da vrijedi $12 \mid 6 \cdot 4$.

Osim za $x = 5$ i $y = 1$ pretpostavke teorema vrijede i za brojeve $x = 4$ i $y = 2$. Provjerimo; $4 \not\equiv \pm 2 \pmod{12}$ i $4^2 = 16 \equiv 2^2 = 4 \pmod{12}$. Vidimo da će u ovom slučaju osim $n \mid (x+y, n)\,(x-y, n)$ vrijediti i $n = (x+y, n)\,(x-y, n)$, naime $12 = (4+2, 12) \cdot (4-2, 12) = 6 \cdot 2$.

Prethodni teorem koristi u mnogim faktorizacijskim algoritmima poput racionalnog sita, kvadratnog sita, algoritma faktorske baze, Dixonovog algoritma, CFRAC algoritma i drugih. Glavana razlika između tih algoritama je način na koji se dolazi do brojeva x i y. Problem pronalaženja brojeva x i y za koje vrijede pretpostavke prethodnog teorema je vremenski pseudopolinoman problem. Brojeve x i y možemo pokušati naći isprobavanjem za mali n, budući da nema mnogo kandidata, ali za veći n trebamo bolje metode.

Jedan od jednostavnijih, ali ne i efikasan način za velike n, je uzeti neki slučajan broj $x \in \mathbb{N}$, $x > \sqrt{n}$, kvadrirati ga i vidjeti je li $x^2 \bmod n$ kvadrat nekog prirodnog broja. Ova metoda je zapravo poboljšanje onoga što radimo u Fermatovoj faktorizaciji. Jednom kada nađemo brojeve x i y Euklidovim algoritmom u polinomnom vremenu možemo izračunati $(x+y, n)$ i $(x-y, n)$.

Primjer 2.10. *Sada ćemo uzeti nešto veći broj $n = 1711$. Uzmimo $x = 44$. Vidimo da je $44^2 \bmod 1711 = 1936 \bmod 1711 = 225$ kvadrat broja $y = 15$. Budući da vrijedi $44 \not\equiv \pm 15 \pmod{1711}$, možemo primjeniti teorem o kongruenciji kvadrata. Po teoremu dobivamo da vrijedi $n = (44+15, 1711) \cdot (44-15, 1711) = 59 \cdot 29$.*

Sada ćemo definirati još neke pojmove koje ćemo koristiti, a potom ćemo opisati algoritam racionalnog sita.

Definicija 2.11. *Za proizvoljan broj $x \in \mathbb{R}$ sa $\pi(x)$ ćemo označavati funkciju brojanja prostih brojeva, koja vraća broj prostih brojeva koji su manji ili jednaki x.*

Definicija 2.12. *Za prirodne brojeve n i B kažemo da je broj n B-gladak ukoliko nijedan prost faktor broja n nije veći od B.*

Propozicija 2.13. *Ako za prirodan broj* n *te cijele brojeve* x *i* y *takve da je* $x \not\equiv \pm y \pmod{n}$ *vrijedi kongruencija* $x^2 \equiv y^2 \pmod{n}$*,a za svaki prost broj* $q \leq p$*, gdje je* p *najveći prost broj koji dijeli* x *ili* y*, vrijedi* $q \nmid n$*, onda vrijedi* $n = (x+y, n)\,(x-y, n)$*, gdje su* $(x+y, n)$ *i* $(x-y, n)$ *različiti od* 1 *i* n*.*

Pretpostavimo da želimo faktorizirati broj $n \in \mathbb{N}$. Odaberemo neki broj $B \in \mathbb{N}$, a sa p_i označimo i-ti prost broj. Ukoliko neki od brojeva $p_i, i = 1, 2, \ldots, \pi(B)$ dijeli n, imamo netrivijalnu faktorizaciju broja n i algoritam može stati. U suprotnom tražimo prirodne brojeve z takve da su z i $z + n$ B-glatki. Ako pronađemo takve brojeve, onda imamo sljedeći rastav na proste faktore brojeva z i $z + n$

$$z = \prod_{i=1}^{\pi(B)} p_i^{a_i},\ z + n = \prod_{i=1}^{\pi(B)} p_i^{b_i}.$$

Budući da je z kongruentan $z + n$ modulo n vrijedi

$$\prod_{i=1}^{\pi(B)} p_i^{a_i} \equiv \prod_{i=1}^{\pi(B)} p_i^{b_i} \pmod{n}.$$

Nakon što pronađemo dovoljno ovakvih relacija (obično je dovoljno naći nešto više od $\pi(B)$ relacija), ukoliko ne postoji relacija u kojoj su svi eksponenti a_i i b_i parni, potrebno je množenjem dobivenih relacija (Propozicija 2.6) i dijeljenjem zajedničkim faktorima p_i (Propozicija 2.7), što smijemo jer $p_i \nmid n$, dobiti novu relaciju u kojoj su eksponenti prostih brojeva parni, te ju zapisati kao kongruencija kvadrata $x^2 \equiv y^2 \pmod{n}$. Sada ćemo po prethodnoj propoziciji dobiti netrivijalnu faktorizaciju broja n. Bitno je da uvjet $x \not\equiv \pm y \pmod{n}$ iz teorema bude zadovoljen, u suprotnom će faktorizacija biti trivijalna, tj. $n = n \cdot 1$.

Prilikom odabira broja B, treba voditi računa da je bolje uzeti malo veći B, nego manji. Ako odaberemo preveliki B, složenost algoritma će se povećati. S druge strane, ako uzmemo premali B moguće je da nećemo pronaći dovoljno relacija z takvih da su z i $z+n$ B-glatki, ili da iz dobivenih relacija nećemo moći dobiti netrivijalnu faktorizaciju.

Primjer 2.14. *Želimo faktorizirati* $n = 893$*. Uzet ćemo* $B = 11$*. Budući da nijedan od prostih brojeva manjih ili jednakih* B *ne dijeli* n*, nastavljamo s algoritmom. Prva* 3 *broja* z *takva da su* z *i* $z + n$ 11*-glatki su* 3*,* 7 *i* 75*. Sada dajemo pripadne relacije kongruencije*

$$2^0 3^1 5^0 7^0 11^0 = 3 \equiv 896 = 2^7 3^0 5^0 7^1 11^0 \pmod{893}$$
$$2^2 3^2 5^2 7^0 11^0 = 900 \equiv 7 = 2^0 3^0 5^0 7^1 11^0 \pmod{893}$$
$$2^0 3^1 5^2 7^0 11^0 = 75 \equiv 968 = 2^3 3^0 5^0 7^0 11^2 \pmod{893}$$

Množenjem prethodnih relacija dobivamo sljedeću relaciju

$$2^2 3^4 5^4 7^0 11^0 \equiv 2^{10} 3^0 5^0 7^2 11^2 \pmod{893}.$$

Budući da su svi eksponenti parni možemo prethodnu relaciju zapisati kao kongruenciju kvadrata, a možemo, ako želimo, podijeliti sa zajedničkim faktorima kako bismo dobili manje brojeve.

Podijelimo prethodnu relaciju sa 2^2*, što smijemo jer* $2 \nmid n$*. Sada imamo kongruenciju kvadrata*

$$3^4 5^4 = \left(3^2 5^2\right)^2 = 225^2 \equiv 1232^2 = \left(2^4 \cdot 7 \cdot 11\right)^2 = 2^8 7^2 11^2.$$

Budući da je zadovoljeno $1232 \not\equiv \pm 225 \pmod{893}$ *imamo netrivijalnu faktorizaciju broja* 893

$$893 = (1232 + 225, 893)\,(1232 - 225, 893) = (1457, 893)\,(1007, 893) = 47 \cdot 19.$$

Racionalno sito, kao i opće sito polja brojeva, ne može faktorizirati brojeve oblika $n = p^k$, gdje je p prost broj, međutim to nije problem jer postoje algoritmi koji, ako vrijedi $n = m^k$, pronalaze brojeve m i k u polinomnom vremenu (vidi [1]). Već smo pokazali u Primjeru 2.9 da postoje brojevi koji imaju netrivijalnu faktorizaciju, ali ne zadovoljavaju uvjete teorema o kongruenciji kvadrata, što znači da racionalno sito ne može dati netrivijalnu faktorizaciju svih složenih brojeva.

Također, najveći problem je pronaći dovoljno brojeva z takvih da su z i $z + n$ B-glatki. Što je n veći to je teže, ponekad i nemoguće, naći dovoljno takvih brojeva jer im se učestalost pojavljivanja smanjuje kako rastu (vidi [12]). Racionalno sito se u praksi ne koristi kao faktorizacijski algoritam zbog prevelike vremenske složenosti, ali nam koristi kako bismo bolj razumjeli rad općeg sita polja brojeva.

Poglavlje 3

Kvadratno sito

Prije nego opišemo algoritam kvadratnog sita, opisat ćemo jednostavniji Dixonov algoritam na kojem se algoritam kvadratnog sita temelji. Nakon toga objasnit ćemo razlike u odnosu na Dixonov algoritam te posebnosti i moguća poboljšanja algoritma kvadratnog sita.

Dixonov algoritam je 1981. god. objavio John D. Dixon, matematičar sa sveučilišta Carleton. Kao i algoritam racionalnog sita, Dixonov algoritam za dani broj n pronalazi brojeve x i y takve da vrijede pretpostavke teorema o kongruenciji kvadrata, te time dolazimo do netrivijalnih faktora $(x+y, n)$ i $(x-y, n)$ od n. Prije nego što smo opisali racionalno sito spomenuli smo metodu sličnu Fermatovom algoritmu, gdje za dani n tražimo brojeve a takve da je $a^2 \bmod n$ potpuni kvadrat, što bi značilo da za $b = \sqrt{a^2 \bmod n}$ odmah imamo kongruenciju kvadrata $a^2 \equiv b^2 \pmod{n}$ i možemo krenuti na faktorizaciju broja n(vidi Primjer 2.10).

Broj potpunih kvadrata manjih ili jednakih n je $\sqrt{n}$, što znači da su brojevi a takvi da je $a^2 \bmod n$ potpuni kvadrat rijetki te je ova metoda, baš kao i Fermatova faktorizacija, dosta spora. Dixonov algoritam stoga umjesto traženja potpunih kvadrata, traži brojeve a takve da $a^2 \bmod n$ ima samo male proste faktore, odnosno da je B-gladak, gdje je B neki mali broj koji odabiremo na početku algoritma. U sljedećem primjeru vidimo da za svaki malo veći B postoji više brojeva koji su B-glatki, nego brojeva koji su potpuni kvadrati. Kasnije ćemo vidjeti da se uzimanjem prevelikog B nepotrebno povećava složenost algoritma, te ćemo pojasniti kako odabrati idealan B.

Definicija 3.1. *Za proizvoljne brojeve $x, y \in \mathbb{N}$ sa $\Psi(x, y)$ ćemo označavati funkciju brojanja glatkih brojeva, koja vraća broj y-glatkih brojeva koji su manji ili jednaki x. Funkcija Ψ zove se de Bruijnova funkcija.*

Primjer 3.2. *Uzmimo $n = 37523$. Postoji 193 potpunih kvadrata manjih od 37523. U sljedećoj tablici dane su vrijednosti funkcije Ψ za različite B.*

B	2	3	5	10	15	25	50	150	500	2000	10000
$\Psi(n, B)$	16	86	248	520	1269	2703	5497	11895	19687	26927	33604

Za svaki B-glatki broj $b_i = a_i^2 \bmod n$, gdje je $i \in \mathbb{N}$, kojeg algoritam pronađe očito imamo sljedeću relaciju kongruencije $a_i^2 \equiv b_i \pmod n$. Cilj Dixonovog algoritma je međusobnim množenjem ovakvih relacija dobiti kongruenciju kvadrata (sličnu tehniku smo koristili i kod racionalnog sita). Međusobnim množenjem relacija $a_i^2 \equiv b_i \pmod n$ i $a_j^2 \equiv b_j \pmod n$ dobijemo relaciju $(a_i a_j)^2 \equiv b_i b_j \pmod n$. Očito je da za sve $a, b \in \mathbb{Z}$ vrijedi $(ab) \equiv ((ab) \bmod n) \pmod n$, pa množenjem ove relacije sa samom sobom dobivamo $(ab)^2 \equiv ((ab) \bmod n)^2 \pmod n$. Kako je "biti kongruentan modulo n" relacija ekvivalencije vrijedi $(a_i a_j \bmod n)^2 \equiv b_i b_j \pmod n$. Sada smo na lijevoj strani relacije dobili potpuni kvadrat koji je manji od $(a_i a_j)^2$, pa će s njim biti lakše računati.

Pokazali smo da množenjem relacija na lijevoj strani novodobivene relacije uvijek dobijemo potpuni kvadrat, pa jedino što preostaje je pronaći koji od brojeva b_i međusobnim množenjem daju potpuni kvadrat.

Primjer 3.3. *Neka je* $n = 2461$. *Brojevi* $52^2 \bmod 2461 = 243$ *i* $56^2 \bmod 2461 = 675$ *nisu potpuni kvadrati, ali njihov umnožak* $243 \cdot 675 = 164025 = 405^2$ *jest. Dakle množenjem relacija* $52^2 \equiv 243 \pmod{2461}$ *i* $56^2 \equiv 675 \pmod{2461}$ *dobijemo kongruenciju kvadrata* $(52 \cdot 56 \bmod 2461)^2 = (2912 \bmod 2461)^2 = 451^2 \equiv 405^2 \pmod{2461}$. *Budući da vrijedi* $451 \not\equiv \pm 405 \pmod{2461}$, *po teoremu o kongruenciji kvadrata dobijemo* $2461 = (451 + 405, 2461)(451 - 405, 2461) = 107 \cdot 23$.

Kako bi provjerili umnožak kojih brojeva b_i daje potpuni kvadrat koristimo isti postupak kao i kod racionalnog sita. Sada ćemo malo detaljnije objasniti taj postupak. Pretpostavimo da smo pronašli k B-glatkih brojeva b_i. Za svaki b_i, $i \in \{1, 2, \ldots, k\}$ imamo sljedeći kanonski rastav tog broja na proste faktore

$$b_i = \prod_{j=1}^{\pi(B)} p_j^{e_{i,j}},$$

gdje je svaki $e_{i,j} \in \mathbb{N}_0$. Cilj je pronaći brojeve $b_{r_1}, b_{r_2}, \ldots, b_{r_l}$, $1 < r_1 < r_2 < \ldots < r_l \leq k$, takve da množenjem pripadnih relacija kongruencije na desnoj strani dobijemo potpuni kvadrat, tj. da svi eksponenti u kanonskom rastavu umnoška budu parni

$$\prod_{i=1}^{l} b_{r_i} = \prod_{j=1}^{\pi(B)} p_j^{\sum_{i=1}^{l} e_{i,j}}, \ \sum_{i=1}^{l} e_{i,j} \equiv 0 \pmod 2 \text{ za svaki } j \in \{1, 2, \ldots, \pi(B)\}.$$

Za svaki b_i stoga možemo definirati pripadni vektor eksponenata $v_{b_i} = (e_{i,1}, e_{i,2}, \ldots, e_{i,\pi(B)})$. Budući da se potencije istih baza množe tako da se eksponenti zbroje, vektor eksponenata

umnoška proizvoljnih brojeva b_i i b_j bit će jednak zbroju vektora eksponenata tih brojeva, odnosno $v_{b_i b_j} = (e_{i,1} + e_{j,1}, e_{i,2} + e_{j,2}, \ldots, e_{i,\pi(B)} + e_{j,\pi(B)})$. Također očito je da će neki broj $x \in \mathbb{N}$ biti potpuni kvadrat ako i samo ako su sve koordinate vektora eksponenata v_x tog broja parni brojevi. Dakle problem pronalaženja brojeva b_i takvih da je njihov umnožak potpuni kvadrat svodi se na problem pronalaženja vektora eksponenata v_{b_i} tih brojeva takvih da je njihov zbroj vektor kojem su sve koordinate parni brojevi.

Kako znamo da je zbroj dva broja paran ako i samo ako su oba pribrojnika ili parni ili neparni brojevi, zaključujemo prema tome da nam nisu bitne same koordinate vektora već isključivo njihova parnost, pa možemo tražiti vektore oblika $w_{b_i} = (e_{i,1} \bmod 2, e_{i,2} \bmod 2, \ldots, e_{i,\pi(B)} \bmod 2)$ čiji je zbroj modulo 2 nul-vektor.

Primjer 3.4. *Primjenimo opisani postupak kako bismo provjerili je li umnožak brojeva* 243 *i* 675 *potpuni kvadrat. Možemo uzeti* $B = 5$*. Brojevi* 243 *i* 675 *tada imaju sljedeće kanonske rastave na proste faktore* $243 = 2^0 3^5 5^0$ *i* $675 = 2^0 3^3 5^2$*, pa su pripadni vektori eksponenata* $(0, 5, 0)$ *i* $(0, 3, 2)$ *koje možemo reducirati modulo* 2 *na vektore* $(0, 1, 0)$ *i* $(0, 1, 0)$*. Njihovim zbrajanjem modulo* 2 *dobivamo nul-vektor. Zaključujemo da je umnožak vektora* 243 *i* 675 *potpuni kvadrat.*

Ovakav postupak se može efikasno primjenjivati na računalima jer oni mogu kompaktno pohraniti te vektore kao nizove bitova, te obavljati zbrajanje modulo 2 koja je zapravo logička operacija XOR. Budući da se vektori w_{b_i} nalaze u vektorskom prostoru $\mathbb{Z}_2^{\pi(B)}$, zapravo treba provjeriti je li skup vektora w_{b_i} linearno ovisan.

Definicija 3.5. *Neka je* V *vektorski prostor nad poljem* $\mathbb{F}$*. Kažemo da je skup* $S \subseteq V$ *linearno ovisan ako se* $0 \in V$ *može prikazati kao netrivijalna linearna kombinacija konačnog broja elemenata iz* S*. U suprotnom kažemo da je* S *linearno neovisan.*

Sljedeća propozicija nam garantira da će skup vektora w_{b_i} biti linearno ovisan ako imamo više od $\pi(B)$ vektora w_{b_i}, tj. ako smo pronašli više od $\pi(B)$ brojeva b_i.

Propozicija 3.6. *Neka je* V *vektorski prostor nad poljem* $\mathbb{F}$*. Ako neki skup* $S \subseteq V$ *ima više od* $\dim_{\mathbb{F}} V$ *elemenata, onda je* S *linearno ovisan.*

Dokaz. Pretpostavimo da je S linearno neovisan. Iz $S \subseteq V$ slijedi da je vektorski prostor kojeg S razapinje podskup od V pa ima dimenziju manju od $\dim_{\mathbb{F}} V$. Budući da S ima više od $\dim_{\mathbb{F}} V$ elemenata i S je linearno neovisan, vektorski prostor kojeg S razapinje ima dimenziju veću od $\dim_{\mathbb{F}} V$, čime smo dobili kontradikciju. □

Kombinaciju vektora koji u zbroju daju nul-vektor možemo pronaći koristeći algoritam Gaussovih eliminacija na matrici $e_{k \times \pi(B)} \bmod 2$, gdje je $k \in \mathbb{N}$ broj vektora w_{b_i}, odnosno brojeva b_i koje smo pronašli. Očito je da ćemo Gaussovim eliminacijama sigurno pronaći kombinaciju vektora koji u zbroju daju nul-vektor ukoliko vrijedi $k > \pi(B)$.

U Primjeru 3.2 možemo vidjeti da sigurno postoji više od $\pi(B)$ B-glatkih brojeva b_i, čak i za male B, no mi bismo htjeli odabrati dovoljno veliki B da ih ne trebamo predugo tražiti. S druge strane u navedenom primjeru možemo primjetiti da funkcija $f(B)$, odnosno broj B-glatkih brojeva manjih od n, raste sve sporije kako se B povećava (to možemo lijepo vidjeti donjom tablicom za $n = 37523$), što znači da ćemo odabirom prevelikog B dobiti relativno malo novih relacija, a složenost će se nepotrebno povećati jer će se matrica $e_{k\times\pi(B)} \bmod 2$ povećati.

p_k	2	3	5	7	13	23	47	149	1999	9973
$\Psi(n,p_k)-\Psi(n,p_{k-1})$	15	70	162	272	414	498	447	232	18	3

Neka je $b \in \mathbb{N}$, $b \leq n$ slučajno odabrani broj. Vjerojatnost da je b B-gladak je tada $\Psi(n,B)/n$, što znači da se u prosjeku među $n/\Psi(n,B)$ brojeva nalazi jedan B-gladak broj. S obzirom da moramo pronaći oko $\pi(B)$ B-glatkih brojeva, prosječno ćemo morati provjeriti $\pi(B)n/\Psi(n,B)$ brojeva. Također kako bismo provjerili je li neki broj B-gladak potrebno nam je približno $\pi(B)$ koraka, pa će ukupni broj koraka algoritma za pronalazak brojeva b_i biti približno $(\pi(B))^2 n/\Psi(n,B)$. Može se pokazati kako je ta vrijednost minimalna za $B = e^{2\sqrt{\ln(n)\ln(\ln(n))}}$.

Osim dobrim odabirom broja B, Dixonov algoritam možemo optimizirati na način da odaberemo bolji algoritam za rješavanje matrične jednadžbe. Sada iskazujemo jedan važan teorem u teoriji brojeva, koji će nam dati dobru predodžbu o veličini vektora v_i. Dokaz teorema možete pronaći u [21, str. 151].

Teorem 3.7 (Teorem o prostim brojevima)**.** *Funkcija $\pi(x)$ može se aproksimirati na sljedeći način*

$$\pi(x) \sim \frac{x}{\ln(x)}, \text{ za } x \to \infty.$$

Budući da brojevi b_i sigurno imaju manje od $\log_2(b_i) < \log_2(n)$ prostih faktora, zaključujemo da vektori v_i sadržavaju $\Omega\left(n\Big/\left((\log(n))^2\right)\right)$ nul koordinata više nego nenul koordinata. Isti zaključak očito tada vrijedi i za vektore w_i. Matrica $e_{k\times\pi(B)} \bmod 2$ je dakle "rijetka" matrica, tj. ima mnogo nula, te se mogu koristiti brži algoritmi od Gaussovih eliminacija kako bismo rješili pripadnu matričnu jednadžbu. Jedan od često korištenih algoritama koji pronalazi linearne ovisnosti velikih rijetkih matrica nad Z_2 je blok Lanczosov algoritam (vidi [19]). Uz navedena poboljšanja vremenska složenost Dixonovog algoritma je $O(e^{2\sqrt{2}\sqrt{\log(n)\log(\log(n))}})$ Vrijeme izvođenja možemo dodatno smanjiti paralelizacijom na više računala. Primjerice, računala mogu tražiti brojeve b_i u disjunktnim intervalima. Također za rješavanje matrične jednadžbe može se koristiti blok Wiedemannov algoritam (vidi [15]), pri čemu svako računalo mora imati pohranjenu matricu $e_{k\times\pi(B)} \bmod 2$.

Algoritam kvadratnog sita je vrlo sličan Dixonovom algoritmu, možemo reći da se zapravo radi o poboljšanju Dixonovog algoritma, stoga nema smisla opisivati cijeli algoritam,

već ćemo opisati ćemo samo bitne modifikacije u odnosu na Dixonov algoritam i prikazati rad algoritma na konkretnom primjeru. Najprije ćemo definirati što je to faktorska baza.

Definicija 3.8. *Faktorska baza je neprazni skup različitih prostih brojeva. Kažemo da se* $x \in \mathbb{N}$ *faktorizira nad faktorskom bazom* S *ili da je* x *gladak s obzirom na faktorsku bazu* S *ako postoji* $k \in \mathbb{N}_0$ *i* $r_1, r_2, \ldots, r_k \in S$ *takvi da vrijedi*

$$x = \prod_{j=1}^{k} {r_j}^{a_j},$$

gdje su $a_j \in \mathbb{N}$.

Napomena 3.9. *Očito je da je za sve* $x, B \in \mathbb{N}$ *vrijedi da je* x B*-gladak ako i samo ako je* x *gladak s obzirom na faktorsku bazu* $\{p_1, p_2, \ldots, p_{\pi(B)}\}$.

Na početku algoritma odlučimo koliko elemenata će imati naša faktorska baza. Želimo odabrati faktorsku bazu S takvu da ćemo moći pronaći brojeve a_i takve da se ${a_i}^2 - n$ faktorizira nad S. Neka je funkcija f definirana na sljedeći način $f(x) = x^2 - n$ za svaki $x \in \mathbb{N}$ i neka je p neki prost broj. Tada za svaki $x \in \mathbb{N}$ i $k \in \mathbb{Z}$ vrijedi $f(x + kp) = (x + kp)^2 - n = f(x) + p(2kx + k^2p)$ iz čega slijedi $f(x + kp) \equiv f(x) \pmod{p}$. Dakle, ako za neki broj $x \in \mathbb{N}$ vrijedi $f(x) \equiv 0 \pmod{p}$, onda za svaki $y = x + kp$ vrijedi $f(y) \equiv 0 \pmod{p}$. Jednadžbu $f(x) \equiv 0 \pmod{p}$ možemo alternativno napisati u obliku $x^2 \equiv n \pmod{p}$ pa kažemo da tražimo korijen broja n modulo p.

Postoje efikasni algoritmi poput Shanks–Tonelli algoritma (vidi [17]) koji pronalaze korijen broja modulo prost broj. Mogu se desiti dvije mogućnosti, da jednadžba ima beskonačno mnogo rješenja i da jednadžba nema rješenja. Ako jednadžba ima rješenja onda postoje dva rješenja x_1 i $x_2 = p - x_1$, ili jedno rješenje za $p = 2$ kada je $x_1 = x_2 = 1$, takva da vrijedi $0 \leq x_1, x_2 < p$. Osim ta dva, zvat ćemo ih osnovna rješenja, kao što smo već spomenuli, svaki broj koji ima isti ostatak kao neki od ova dva osnovna rješenja je također rješenje jednadžbe $x^2 - n \equiv 0 \pmod{p}$. Drugim rječima za osnovna rješenja x_1 i $p - x_1$, svi brojevi $x_1 + kp$ i $p - x_1 + kp$, gdje je $k \in \mathbb{Z}$, su također rješenja jednadžbe $x^2 \equiv n \pmod{p}$. Ako jednadžba nema rješenje, onda ne postoji $x \in \mathbb{N}$ takav da $p \mid x^2 - n$. Sada znamo kako napuniti faktorsku bazu S. Uzimamo redom proste brojeve p_i i provjeravamo ima li jednadžba $x^2 - n \equiv 0 \pmod{p_i}$ rješenja, ako ima ubacujemo p_i u S, ako nema uzimamo broj p_{i+1} i ponovimo postupak. Postupak ponavljamo sve dok S ne napunimo do zadane veličine.

Za male brojeve $x \in \mathbb{N}_0$ će $\left(\left\lceil \sqrt{n} \right\rceil + x\right)^2 - n$ također biti mali broj te će stoga biti veća vjerojatnost da je gladak. Pretragu za brojevima a_i zato počinjemo od broja $\left\lceil \sqrt{n} \right\rceil$. Na taj način dobijemo relacije kongruencije oblika ${a_i}^2 \equiv {a_i}^2 - n \pmod{n}$. Daljnji postupak je potpuno isti kao kod Dixonovog algoritma, međusobnim množenjem relacija na lijevoj

strani sigurno ćemo dobiti potpuni kvadrat, pa je jedino bitno da dobijemo potpuni kvadrat i na desnoj strani kako bi imali kongruenciju kvadrata. Za svaki $b_i = a_i{}^2 - n$ možemo definirati vektor eksponenata čija duljina je jednaka veličini faktorske baze, reducirati vektor modulo n, napraviti matricu i pronaći linearnu ovisnost Gaussovim eliminacijama ili nekim drugim efikasnijim algoritmom za rijetke matrice.

Najbitnija razlika kvadratnog sita u odnosu na Dixonov algoritam je način na koji se traže glatki brojevi. Najprije uzmemo niz brojeva oblika $x^2 - n$, počevši od $x = \left\lceil \sqrt{n} \right\rceil$ koji predstavljaju kandidate za brojeve b_i i spremimo ih u niz A, tj. vrijedi $A[i] = \left(\left\lceil \sqrt{n} \right\rceil + i\right)^2 - n$. Duljinu niza A sami odredimo. Sa većom duljinom niza imamo i veću vjerojatnost da ćemo pronaći dovoljno relacija i time veću vjerojatnost faktorizacije. S druge strane uzimanjem većeg niza povećava se složenost algoritma. Algoritam je dobio ime kvadratno sito jer je $x^2 - n$ kvadratni polinom, a do brojeva b_i ćemo doći metodom sita, tj. procesom eliminacije.

Redom uzimamo brojeve $p \in S$ i pronalazimo rješenja jednadžbi $x^2 - n \equiv 0 \pmod{p}$. Primjetimo kako jednadžba $x^2 - n \equiv 0 \pmod{p}$ sigurno ima rješenja jer je $p \in S$, no onda očito i jednadžba $A[i] = \left(\left\lceil \sqrt{n} \right\rceil + i\right)^2 - n \equiv 0 \pmod{p}$ ima rješenja. Točnije, ako je x' neko rješenje jednadžbe $x^2 - n \equiv 0 \pmod{p}$ onda je $i' = x' - \left\lceil \sqrt{n} \right\rceil$ rješenje jednadžbe $A[i] = \left(\left\lceil \sqrt{n} \right\rceil + i\right)^2 - n \equiv 0 \pmod{p}$. Budući da za svako rješenje x' jednadžbe $x^2 - n \equiv 0 \pmod{p}$ vrijedi $x' \equiv x_1 \pmod{p}$ ili $x' \equiv x_2 \pmod{p}$, gdje su x_1 i $x_2 = p - x_1$ osnovna rješenja navedene jednadžbe, zaključujemo da za $i' = x' - \left\lceil \sqrt{n} \right\rceil$ vrijedi $i' \equiv x_1 - \left\lceil \sqrt{n} \right\rceil \pmod{p}$ ili $x' \equiv x_2 - \left\lceil \sqrt{n} \right\rceil \pmod{p}$. Osnovna rješenja jednadžbe $A[i] = \left(\left\lceil \sqrt{n} \right\rceil + i\right)^2 - n \equiv 0 \pmod{p}$ će dakle biti $i_1 = x_1 - \left\lceil \sqrt{n} \right\rceil \bmod p$ i $i_2 = x_2 - \left\lceil \sqrt{n} \right\rceil \bmod p$ (primjetimo da ovdje ne vrijedi $i_1 = p - i_2$). Sva ostala rješenja navedene jednadžbe moraju imati isti ostatak pri dijeljenju s p, pa su oblika $i_1 + kp$ ili $i_2 + kp$. Algoritam dakle redom za svako $p \in S$ izračuna osnovna rješenja x_1 i x_2 jednadžbe $x^2 - n \equiv 0 \pmod{n}$ i iz njih dobije $i_1 = x_1 - \left\lceil \sqrt{n} \right\rceil \bmod p$ i $i_2 = x_2 - \left\lceil \sqrt{n} \right\rceil \bmod p$ takva da vrijedi $A[i] \equiv 0 \pmod{p}$ te svim elementima $A[i_1 + kp]$ i $A[i_2 + kp]$ pridruži nove vrijednosti dobivene dijeljenjem starih vrijednosti brojem p.

Na kraju ovog postupka će vrijediti $A[x] = 1$ ako i samo ako je

$$x^2 - n = \prod_{p \in S} p^{a_i},$$

gdje su $a_i \in \{0, 1\}$. Međutim kako postoje brojevi koji su glatki s obzirom na S, a nisu navedenog oblika, tj. djeljivi su i sa p^k, za neke $p \in S$ i $k \geq 2$, ukoliko nemamo dovoljno glatkih brojeva nove glatke brojeve dobit ćemo novim krugom eliminacija, tj. rješavanjem jednadžbi $x^2 - n \equiv 0 \pmod{p^k}$. Na ovaj način dobijemo brojeve a_i za koje je $b_i = a_i{}^2 \bmod n$ gladak s obzirom na S. Još je samo preostalo naći kanonski rastav tih brojeva

kako bismo mogli dobiti vektore eksponenata v_{b_i}. Budući brojevi b_i imaju samo male proste faktore, tj. glatki su s obzirom na S, imamo efikasne algoritme poput Shanksove faktorizacije s kvadratnim formama, Pollardove ρ metode, algoritma eliptičkih krivulja ili jednostavno naivnim pristupom provjerom djeljivosti unaprijed pripremljenim prostim brojevima.

Primjer 3.10. *Želimo faktorizirati broj* $n = 19667$. *Uzet ćemo da faktorska baza ima* 5 *prostih faktora. Prvih* 5 *prostih brojeva* p *takvih da jednadžba* $\left(x + \left\lceil \sqrt{19667} \right\rceil\right)^2 - 19667 = (x + 141)^2 - 19667 \equiv 0 \pmod{p}$ *ima rješenja su brojevi* 2, 7, 17, 23 *i* 29. *Dakle naša faktorska baza je skup* $S = \{2, 7, 17, 23, 29\}$.

Neka je A *niz od* 100 *brojeva oblika* $A[i] = (i+141)^2 - 19667$, *za* $i \in \{0, 1, 2, \ldots, 99\}$. *Sljedeća tablica prikazuje osnovna rješenja* $x \in \mathbb{N}$ *jednadžbe* $x^2 - 19667 \equiv 0 \pmod{p}$, *za* $p \in S$ *te osnovna rješenja* $i = x - 141 \bmod p$ *jednadžbe* $A[i] \equiv 0 \pmod{p}$. *Algoritam*

p	2	7	7	17	17	23	23	29	29
x	1	2	5	7	10	5	18	11	18
i	0	1	4	2	5	2	15	15	22

dakle sve elemente $A[2k]$ *podijeli sa* 2, *sve elemente* $A[1 + 7k]$ *i sve elemente* $A[4 + 7k]$ *podijeli sa* 7, *sve elemente* $A[2+17k]$ *i sve elemente* $A[5+17k]$ *podijeli sa* 17, *sve elemente* $A[2 + 23k]$ *i sve elemente* $A[15 + 23k]$ *podijeli sa* 23 *te sve elemente* $A[15 + 29k]$ *i sve elemente* $A[22+29k]$ *podijeli sa* 29. *Pogledajmo sada što se dogodilo nakon ovog postupka sa elementima* $A[2]$, $A[15]$ *i* $A[22]$.

Na početku je $A[2] = (2 + 141)^2 - 19667 = 782$, *no kako za* $k_1 = 1$ *i* $k_2 = k_3 = 0$ *vrijedi* $2 = 2k_1 = 2 + 17k_2 = 2 + 23k_3$, *element* $A[2]$ *bit će redom podijeljen brojevima* 2, 17 *i* 23, *te će na kraju imati vrijednost* $A[2] = 782/(2 \cdot 17 \cdot 23) = 1$.

Na početku je $A[15] = (15 + 141)^2 - 19667 = 4669$, *no kako za* $k_1 = 2$ *i* $k_2 = k_3 = 0$ *vrijedi* $15 = 1 + 7k_1 = 15 + 23k_2 = 15 + 29k_3$, *element* $A[15]$ *bit će redom podijeljen brojevima* 7, 23 *i* 29, *te će na kraju imati vrijednost* $A[15] = 4669/(7 \cdot 23 \cdot 29) = 1$.

Na početku je $A[22] = (22 + 141)^2 - 19667 = 6902$, *no kako za* $k_1 = 11$, $k_2 = 3$, $k_3 = 1$ *i* $k_4 = 0$ *vrijedi* $22 = 2k_1 = 1 + 7k_2 = 5 + 17k_3 = 22 + 29k_4$, *element* $A[22]$ *bit će redom podijeljen brojevima* 2, 7, 17 *i* 29, *te će na kraju imati vrijednost* $A[22] = 6902/(2 \cdot 7 \cdot 17 \cdot 29) = 1$.

Brojevi 782, 4669 *i* 6902 *su dakle glatki s obzirom na faktorsku bazu* S. *Budući da broj glatkih brojeva nije veći od broja elemenata faktorske baze, uobičajeno je da nastavimo tražiti brojeve koji su glatki s obzirom na* S *rješavanjem jednadžbe*

$$A[i] \equiv 0 \pmod{p^k},$$

sve dok ne pronađemo više glatkih brojeva nego što S *ima elemenata, jer bi nam to garantiralo postojanje linearne ovisnosti vektora eksponenata tih brojeva i samim time dobivanje*

kongruencije kvadrata. Mi ćemo pokušati doći do toga samo sa ova tri broja koja smo pronašli.

Budući da su elementi $A[2]$, $A[15]$ *i* $A[22]$ *postavljeni svi na vrijednost* 1, *njihove prvotne vrijednosti možemo izračunati na sljedeći način* $b_1 = (3+141)^2 - 19667$, $b_2 = (15+141)^2 - 19667$ *i* $b_3 = (22+141)^2 - 19667$. *Nakon toga možemo relativno brzo dobiti kanonski rastav na proste faktore brojeva* b_i *jer imaju samo male faktore budući da su glatki s obzirom na* S. *Sada konstruiramo matricu* $\boldsymbol{E}_{3\times 5}$ *kojoj su retci vektori eksponenata* $w_{b_i} = v_{b_i} \bmod 2$ *te rješavamo sustav* $\boldsymbol{xE} = \boldsymbol{0} \pmod 2$ *odnosno*

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}^T \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}^T \pmod 2$$

Jedino netrivijalno rješenje sustava je

$$\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Dakle množenjem relacija

$$(2+141)^2 = 143^2 \equiv (2+141)^2 - 19667 = 782 = 2^1 7^0 17^1 23^1 29^0 \pmod{19667}$$
$$(15+141)^2 = 156^2 \equiv (15+141)^2 - 19667 = 4669 = 2^0 7^1 17^0 23^1 29^1 \pmod{19667}$$
$$(22+141)^2 = 163^2 \equiv (22+141)^2 - 19667 = 6902 = 2^1 7^1 17^1 23^0 29^1 \pmod{19667}$$

dobijemo kongruenciju kvadrata

$$(143 \cdot 156 \cdot 163)^2 \equiv (2 \cdot 7 \cdot 17 \cdot 23 \cdot 29)^2 \pmod{19667}.$$

Budući da vrijedi

$$(143 \cdot 156 \cdot 163)^2 \equiv (143 \cdot 156 \cdot 163 \bmod 19667)^2 = 17476^2 \pmod{19667}$$
$$(2 \cdot 7 \cdot 17 \cdot 23 \cdot 29)^2 \equiv (158746 \bmod 19667)^2 = 1410^2 \pmod{19667}$$

dobijemo kongruenciju kvadrata sa manjim brojevima $17476^2 \equiv 1410^2 \pmod{19667}$. *Konačno dobivamo faktorizaciju* $n = (17476 + 1410, 19667)(17476 - 1410, 19667) = 71 \cdot 277$

Kvadratno sito moguće je optimizirati traženjem tzv. ciklusa. Ako postoje brojevi oblika $x^2 - n$ koji imaju isti prost faktor p izvan faktorske baze, onda međusobnim množenjem

parcijalnih relacija oblika $x^2 \equiv x^2 - n \pmod{n}$ na desnoj strani relacije dobijemo umnožak spomenutih brojeva koji je sigurno djeljiv s p^2, pa dobivenu relaciju možemo pomnožiti brojem $(p^{-1})^2$, gdje je p^{-1} multiplikativni inverz modulo n broja p, tj. vrijedi $p^{-1}p \equiv pp^{-1} \equiv 1 \pmod{n}$. Na taj način na desnoj strani relacije će ostati broj gladak s obzirom na faktorsku bazu. Takvu punu relaciju dobivenu množenjem parcijalnih relacija i modularnog inverza p^{-1} zovemo ciklus.

Primjer 3.11. *Neka je* $n = 187$ *i faktorska baza* $S = \{2, 3\}$. *Imamo sljedeće parcijalne relacije*

$$15^2 \equiv 2^1 3^0 19^1 \pmod{187} \quad i \quad 23^2 \equiv 2^1 3^2 19^1 \pmod{187}$$

Njihovim množenjem dobivamo relaciju

$$(15 \cdot 23)^2 \equiv 2^2 3^2 19^2 \pmod{187}.$$

U ovom primjeru se desilo da smo na desnoj strani dobili potpuni kvadrat pa imamo kongruenciju kvadrata i možemo faktorizirati broj 187. *Općenito na desnoj strani nećemo dobiti potpuni kvadrat, stoga ćemo nastaviti s postupkom dobivanja ciklusa. Množenjem dobivene relacije sa modularnim inverzom* $19^{-1} \equiv 128 \pmod{187}$ *broja* 19 *modulo* 187 *dobijemo sljedeću relaciju*

$$(128 \cdot 15 \cdot 23)^2 \equiv 2^2 3^2 \pmod{187} \Leftrightarrow 28^2 \equiv 6^2 \pmod{187}.$$

Na desnoj strani samo dobili broj gladak s obzirom na S*, koji je u našem primjeru i potpuni kvadrat pa je dobivena relacija kongruencije kvadrata. Faktorizacija broja* n *je stoga* $n = (28 + 6, 187)(28 - 6, 187) = 17 \cdot 11$.

Budući da osim jednadžbi oblika $x^2 = n \pmod{p}$, znamo rješavati i općenitije jednadžbe $(Ax + B)^2 = n \pmod{p}$, gdje su $A, B \in \mathbb{Z}$, možemo tražiti a_i takve da se $f(a_i) = (Aa_i + B)^2 - n$ faktorizira nad faktorskom bazom. To je vrlo pogodno kod paralelizacije rada na više računala, gdje svako računalo ima svoju kolekciju kvadratnih polinoma $f(x)$ i traži brojeve a_i takve da je $f(a_i)$ gladak s obzirom na faktorsku bazu koju je to računalo odredilo. Ovu metodu zovemo multipolinomno kvadratno sito (engl. MPQS - Multiple Polynomial Quadratic Sieve).

Algoritam kvadratnog sita je osmislio Carl Pomerance 1981. god. i bio je jedan od najefektivnijih algoritama 80-ih i ranih 90-ih godina te je još uvijek najbolji izbor za faktorizaciju brojeva do oko 100 znamenki. Danas se smatra da je nakon općeg sita polja brojeva drugi najbrži faktorizacijski algoritam te je konceptualno mnogo jednostavniji od općeg sita. Vremenska složenost kvadratnog sita je $O\left(e^{\sqrt{\log(n)\log(\log(n))}}\right)$. Metodom multipolinomnog kvadratnog sita 1994. god. faktoriziran je 129-znamenkasti poluprost broj

RSA-129. Korištena je faktorska baza sa 524339 prostih brojeva. To je do tada bio najveći RSA broj koji je faktoriziran, sve dok 1996. god. nije faktoriziran RSA-130 algoritmom općeg sita brojeva u približno 15% vremena koje bi bilo potrebno kvadratnom situ. Trenutni rekord za kvadratno sito je 135 znamenkasti broj, inače faktor broja $2^{803} - 2^{402} + 1$, koji je 2001. god. faktoriziran na umnožak 66 i 69 znamenkastog broja.

Poglavlje 4

Specijalno sito

Racionalno i kvadratno sito će pod pretpostavkom da koriste dovoljno veliku faktorsku bazu i da nema vremenskih ograničanja na trajanje njihovog rada, pronaći netrivijalnu faktorizaciju bilo kojeg broja $n \in \mathbb{N}$, ukoliko ona postoji. Kod specijalnog sita to nije slučaj, jer ono može pronaći netrivijalnu faktorizaciju samo onih prirodnih brojeva n koji su blizu potenciji nekog drugog prirodnog broja, odnosno koji su oblika $n = r^e \pm s$ gdje su $r, e, s \in \mathbb{N}$ te su r i s mali brojevi. S druge strane prednost specijalnog sita je da faktorizaciju tih brojeva radi brže od bilo kojeg drugog algoritma uključujući i opće sito. Točnije, vremenska složenost specijalnog sita je

$$O\left(e^{(32/9)^{1/3}(\log(n))^{1/3}(\log(\log(n)))^{2/3}}\right).$$

Faktorizaciju brojeva oblika $n = r^e \pm s$ gdje su r i s mali brojevi, ćemo kao i u slučaju RSA brojeva smatrati velikom ako je n produkt velikih prostih brojeva. Tada najvećom faktorizacijom uopće, a ne samo brojeva specijalnog oblika, možemo smatrati onu 320 znamenkastog Mersennovog broja $2^{1061} - 1$, koji je 2012. god. faktoriziran na produkt 143 i 177 znamenkastih prostih brojeva algoritmom specijalnog sita. Algoritam specijalnog sita osmislio je 1988. god. britanski matematičar John Pollard, a prva značajnija faktorizacija koja je navijestila uspjeh algoritma bila je faktorizacija 9. Fermatovog broja $2^{2^9} + 1$, što u to vrijeme, 1990. god., nije uspjelo kvadratnom situ, ali ni drugim algoritmima poput algoritma eliptičkih krivulja.

Definicija 4.1. *Brojevi oblika* $2^{2^n} + 1$ *zovu se Fermatovi brojevi.*

Prije nego krenemo s opisom algoritma specijalnog sita, potrebno je prisjetiti se nekih definicija koje ćemo koristiti. Pretpostavljamo da su pojmovi kao što su prsten, polje, polinom, linearni operator i njegova matrična reprezentacija, determinanta, svojstvene vrijednosti i sl. poznati.

Definicija 4.2. *Neka je* R *prsten. Skup svih polinoma oblika*

$$\sum_{k=0}^{n} a_k X^k, n \in \mathbb{N}_0, a_k \in R, a_n \neq 0$$

zovemo prsten polinoma u varijabli X *nad prstenom* R*, u oznaci* $R[X]$.

Lako se može pokazati da $R[X]$ zajedno s operacijama zbrajanja i množenja (vidi [14, str. 82]) čini prsten.

Definicija 4.3. *Neka je* $A[X]$ *prsten polinoma. Kažemo da je polinom* $f \in A[X]$ *normirani, ako mu je vodeći koeficijent* 1.

Definicija 4.4. *Neka je* $A[X]$ *prsten polinoma i* B *neki natprsten od* A*. Kažemo da je polinom* $f \in A[X]$ *ireducibilan nad* B*, ako ne postoje polinomi* $f_1, f_2 \in B[X]$ *svaki stupnja barem* 1 *takvi da vrijedi* $f = f_1 \cdot f_2$.

Definicija 4.5. *Kompleksan broj* $\alpha \in \mathbb{C}$ *zove se algebarski broj ako postoji polinom* $0 \neq f \in \mathbb{Q}[X]$*, takav da je* $f(\alpha) = 0$*. Kompleksan broj se zove transcendentan ako nije algebarski.*

Definicija 4.6. *Neka je* R *prsten. Podskup* $S \subseteq R$ *koji je i sam prsten zovemo potprsten od* R*. Kažemo da je* R *proširenje od* S.

Propozicija 4.7. *Ako je* S *prsten,* R *neki njegov potprsten i* $a \in S$*, onda je skup* $R[a] := \{f(a) \mid f \in R[X]\}$ *proširenje prstena* R.

Dokaz. Neka je S neki prsten, R neki njegov potprsten i $a \in S$. Budući da je očito $R \subseteq R[a]$, jedino preostaje pokazati da je $R[a]$ prsten, dokaz čega ide analogno kao i dokaz da je $R[X]$ prsten. □

Definicija 4.8. *Ako su* $\mathbb{K} = (\mathbb{K}, +_{\mathbb{K}}, \cdot_{\mathbb{K}})$ *i* $\mathbb{L} = (\mathbb{L}, +_{\mathbb{L}}, \cdot_{\mathbb{L}})$ *polja takva da vrijedi* $\mathbb{K} \subseteq \mathbb{L}$*,* $+_{\mathbb{K}} = +_{\mathbb{L}}|_{\mathbb{K}\times\mathbb{K}}$ *i* $\cdot_{\mathbb{K}} = \cdot_{\mathbb{L}}|_{\mathbb{K}\times\mathbb{K}}$*, onda kažemo da je* $\mathbb{K}$ *potpolje od* $\mathbb{L}$*, odnosno da je* $\mathbb{L}$ *natpolje od* $\mathbb{K}$*. Uobičajeno je reći da je* $\mathbb{L}|\mathbb{K}$ *(čitaj "*$\mathbb{L}$ *nad* $\mathbb{K}$*") proširenje polja, što znači da je polje* $\mathbb{L}$ *natpolje od* $\mathbb{K}$*. Ako vrijedi* $\mathbb{L}|\mathbb{K}$ *i* $\mathbb{K} \subsetneq \mathbb{L}$ *onda kažemo da je* $\mathbb{K}$ *pravo potpolje od* $\mathbb{L}$*, odnosno da je* $\mathbb{L}|\mathbb{K}$ *pravo proširenje.*

Propozicija 4.9. *Svako polje* $\mathbb{L}$ *je vektorski prostor nad svojim proizvoljnim potpoljem.*

Dokaz. Neka je $\mathbb{L}$ neko polje i $\mathbb{K}$ neko njegovo potpolje. Iz definicije polja slijedi da je $(\mathbb{L}, +)$ komutativna grupa. Također iz definicije polja slijedi distributivnost množenja prema zbrajanju pa budući da je $\mathbb{K} \subseteq \mathbb{L}$, za sve $v, w \in \mathbb{L}$ i $\lambda, \mu \in \mathbb{K}$ vrijedi $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$ i $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$. Kako je $\mathbb{L}$ polje, po definiciji operacija množenja mora biti asocijativna pa za sve $v \in \mathbb{L}$ i $\lambda, \mu \in \mathbb{K}$ vrijedi $(\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$. Budući da je svako polje prsten s jedinicom, za svaki $v \in \mathbb{L}$ vrijedi $1 \cdot v = v$. □

Definicija 4.10. *Neka je $\mathbb{L}|\mathbb{K}$ neko proširenje polja. Dimenziju vektorskog prostora $\mathbb{L}$ nad $\mathbb{K}$ zovemo stupanj proširenja od $\mathbb{L}|\mathbb{K}$, u oznaci $[\mathbb{L} : \mathbb{K}]$. Ako je $[\mathbb{L} : \mathbb{K}] \in \mathbb{N}$ kažemo da je $\mathbb{L}|\mathbb{K}$ konačno proširenje.*

Definicija 4.11. *Neka je $\mathbb{K}$ polje i S neki skup. Tada ćemo sa $\mathbb{K}(S)$ označavati najmanje polje koje sadrži i polje $\mathbb{K}$ i skup S, odnosno*

$$\mathbb{K}(S) := \bigcap_{\substack{\mathbb{E}|\mathbb{K} \\ S\subseteq\mathbb{E}}} \mathbb{E}.$$

Polje $\mathbb{K}(S)$ zovemo proširenje od $\mathbb{K}$ generirano sa S. Ako je skup $S = \{a\}$ jednočlan umjesto $\mathbb{K}(\{a\})$ pišemo $\mathbb{K}(a)$.

Definicija 4.12. *Neka je $\alpha \in \mathbb{C}$ algebarski broj. Normirani polinom $g \in \mathbb{Q}[X]$ minimalnog stupnja, takav da vrijedi $g(\alpha) = 0$, zovemo minimalni polinom od α.*

Definicija 4.13. *Neka su R i S dva prstena. Preslikavanje $f : R \to S$ je homomorfizam prstena ukoliko je aditivno i multiplikativno, tj. ako za sve $x, y \in R$ vrijedi*

$$f(x + y) = f(x) + f(y) \text{ i } f(xy) = f(x)f(y),$$

te f preslikava jedinicu u jedinicu ($f(1_R) = 1_S$).

Definicija 4.14. *Neka je R prsten. Ako za sve $x, y \in R$, takve da je $xy = 0$, vrijedi $x = 0$ ili $y = 0$, onda kažemo da je R integralna domena.*

Definicija 4.15. *Neka je R prsten s jedinicom. Kažemo da je element $x \in R$ invertibilan ako postoji element $x^{-1} \in R$ takav da vrijedi $x \cdot x^{-1} = x^{-1} \cdot x = 1$. Skup svih invertibilnih elemenata od R označavamo sa $R^\times$.*

Definicija 4.16. *Neka je R prsten s jedninicom. Kažemo da je element $x \in R$ ireducibilan u R ako vrijedi*

- *x je neinvertibilan nenul element, tj. $0 \neq x \notin R^\times$.*
- *Za sve $a, b \in R$ takve da je $x = ab$ vrijedi ili $a \in R^\times$ ili $b \in R^\times$.*

Definicija 4.17. *Integralna domena R je faktorijalan prsten ako vrijedi*

- *Za svaki $x \in R$ takav da je $0 \neq x \notin R^\times$ postoji $n \in \mathbb{N}$ i ireducibilni elementi $p_i \in R, i \in \{1, 2, \ldots, n\}$ takvi da vrijedi*

$$x = \prod_{i=1}^{n} p_i.$$

- *Ako za neki* $x \in R$ *vrijedi*

$$x = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} r_i,$$

gdje su $p_i, r_i \in R$ *ireducibilni elementi, onda je* $n = m$ *i postoji permutacija* $\sigma \in \mathcal{S}_n$ *takva da za svaki* $i \in \{1, 2, \dots n\}$ *vrijedi* $p_i = r_{\sigma(i)}$.

Definicija 4.18. *Kažemo da je neinvertibilan nenul element* p *komutativnog prstena* R *prost u* R *ako za sve* $a, b \in R$ *takve da* $p \mid ab$ *vrijedi* $p \mid a$ *ili* $p \mid b$.

Definicija 4.19. *Neka je* $\mathbb{L}|\mathbb{K}$ *neko proširenje polja. Budući da je* $\mathbb{L}$ *po Propoziciji 4.9 vektorski prostor nad* $\mathbb{K}$*, za* $\alpha \in \mathbb{L}$ *definiramo* $\mathbb{K}$*-linearni operator* $m_\alpha : \mathbb{L} \to \mathbb{L}$ *na sljedeći način* $m_\alpha(x) := \alpha x$*. Funkciju* $N_{\mathbb{L}|\mathbb{K}} : \mathbb{L} \to \mathbb{K}$ *koja svakom elementu* $\alpha \in \mathbb{L}$ *pridružuje determinantu operatora* m_α *zovemo norma elementa* α *u proširenju* $\mathbb{L}|\mathbb{K}$.

Definicija 4.20. *Neka je* $\mathbb{L}|\mathbb{K}$ *neko proširenje polja. Karakteristični polinom* $\mathbb{K}$*-linearnog operatora* $m_\alpha : \mathbb{L} \to \mathbb{L}$*,* $m_\alpha(x) := \alpha x$*, u oznaci* χ_{m_α}*, definiramo na sljedeći način* $\chi_{m_\alpha}(X) := \det(XI - M_\alpha) \in \mathbb{K}[X]$*, gdje je* M_α *neka matrična reprezentacija operatora* m_α.

Definicija 4.21. *Neka je* $\mathbb{L}|\mathbb{K}$ *neko proširenje polja. Karakteristični polinom nekog algebarskog broja* $\alpha \in \mathbb{L}$*, u oznaci* χ_α*, jednak je karakterističnom polinomu od* m_α.

Propozicija 4.22. *Neka je* $\mathbb{L}|\mathbb{K}$ *neko proširenje polja. Slobodni koeficijent karakterističnog polinoma algebarskog broja* $\alpha \in \mathbb{L}$ *je* $\pm N_{\mathbb{L}|\mathbb{K}}(\alpha)$.

Dokaz. Neka je $\alpha \in \mathbb{L}$ algebarski broj. Slobodni koeficijent karakterističnog polinoma od α je $\chi_\alpha(0) = \chi_{m_\alpha}(0) = \det((-1)(M_\alpha)) = \det(-I)\det(m_\alpha) = (-1)^{[\mathbb{L}:\mathbb{K}]} N_{\mathbb{L}|\mathbb{K}}(\alpha)$. □

Definicija 4.23. *Kažemo da je algebarski broj* $x \in \mathbb{C}$ *cijeli ako postoji normirani polinom* $f \in \mathbb{Z}[X]$ *takav da vrijedi* $f(x) = 0$.

Propozicija 4.24. *Neka je* $\mathbb{L}|\mathbb{K}$ *neko proširenje polja. Ako je* $x \in \mathbb{L}$ *algebarski cijeli broj, onda vrijedi* $N_{\mathbb{L}|\mathbb{K}}(x) \in \mathbb{Z}$.

Dokaz. Neka je $x \in \mathbb{L}$ algebarski cijeli broj. Iz definiciji algebarski cijelih brojeva slijedi da postoji normirani polinom $f \in \mathbb{Z}[X]$ takav da je $f(x) = 0$. Budući da je polinom f normiran, on je minimalni polinom od x. Svi koeficijenti minimalnog polinoma od x su dakle elementi iz $\mathbb{Z}$.

Neka je $\alpha \in \mathbb{L}$. Iz definicije operatora m_α slijedi da je α svojstvena vrijednost tog operatora, tj. za svaki $\beta \in \mathbb{L}$ vrijedi $m_\alpha(\beta) = \alpha\beta$ iz čega redom dobivamo

$$m_\alpha(\beta) - \alpha\beta = 0 \Rightarrow M_\alpha\beta - \alpha I\beta = 0 \Rightarrow (M_\alpha - \alpha I)\beta = 0 \Rightarrow \det(\alpha I - m_\alpha) = 0.$$

Zaključujemo da svaki karakteristični polinom nekog broja poništava taj broj, posebno vrijedi $\chi_x(x) = 0$.

Minimalni polinom od x mora po definiciji dijeliti svaki drugi polinom koji poništava x, pa posebno mora dijeliti karakteristični polinomom od x, što povlači da koeficijenti karakterističnog polinoma od x moraju biti iz $\mathbb{Z}$. Kako po prethodnoj propoziciji vrijedi $\chi_x(0) = \pm N_{\mathbb{L}|\mathbb{K}}(x)$, a $\chi_x(0)$ je iz $\mathbb{Z}$ jer je slobodni koeficijent karakterističnog polinoma od x, tvrdnja propozicije je dokazana. □

Propozicija 4.25. *Neka je $\mathbb{L}|\mathbb{K}$ neko proširenje polja. Norma $N_{\mathbb{L}|\mathbb{K}}$ je multiplikativna funkcija.*

Dokaz. Neka su $\alpha, \beta \in \mathbb{L}$. Tada za $x \in \mathbb{L}$ vrijedi $(m_\alpha \circ m_\beta)(x) = m_\alpha(m_\beta(x)) = m_\alpha(\beta x) = \alpha(\beta x) = (\alpha\beta)x = m_{\alpha\beta}(x)$. Budući da je determinanta kompozicije linearnih operatora jednaka umnošku determinanti tih operatora dobivamo $N_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = \det(m_{\alpha\beta}) = \det(m_\alpha \circ m_\beta) = \det(m_\alpha)\det(m_\beta) = N_{\mathbb{L}|\mathbb{K}}(\alpha)N_{\mathbb{L}|\mathbb{K}}(\beta)$ □

Propozicija 4.26. *Neka je R faktorijalan prsten. Element $p \in R$ je prost u R ako i samo ako je ireducibilan u R.*

Dokaz. Pretpostavimo da je p prost element u R te $x, y \in R$ takvi da vrijedi $p = xy$. Najprije ćemo pretpostaviti da su i x i y neinvertibilni. Tada za sve $a, b \in R$ takve da $p \mid ab$ mora vrijediti $p = xy \mid a$ ili $p = xy \mid b$. Posebno za $a = x$ i $b = y$ mora vrijediti $xy \mid x$ ili $xy \mid y$. Pretpostavimo, bez smanjenja općenitosti da vrijedi $xy \mid x$. To znači da postoji $k \in R$ takav da je $xyk = x$, odnosno $yk = 1$, što je u kontrdikciji s pretpostavkom da je y neinvertibilan. Sada pretpostavimo da su i x i y invertibilni. Očito je tada i p invertibilan jer je njegov inverz umnožak inverza elemenata x i y, pa nije prost element po definiciji, što znači da smo došli do kontradikcije. Ovime smo dokazali da nijedan prost element u R nije umnožak dva invertibilna ili dva neinvertibilna elementa iz R, odnosno da uvijek jedan element mora biti invertibilan, a drugi neinvertibilan što znači da je p ireducibilan element. Time smo dokazali jedan smjer.

Pretpostavimo da je p ireducibilan element u R i neka su $a, b \in R$ takvi da vrijedi $p \mid ab$. Ako je a invertibilan, onda očito $p \mid b$. Analogno, ako je b invertibilan, onda $p \mid a$. Pretpostavimo stoga da ni a ni b nisu invertibilni. Kako je R faktorijalan prsten, a a i b neinvertibilni nenul elementi, postoje $n_1, n_2 \in \mathbb{N}$ i ireducibilni elementi $p_i \in R, i \in \{1, 2, \ldots, n_1\}$ te $r_i \in R, i \in \{1, 2, \ldots, n_2\}$ takvi da vrijedi

$$a = \prod_{i=1}^{n_1} p_i \quad \text{i} \quad b = \prod_{i=1}^{n_2} r_i.$$

Množenjem prethodnih faktorizacija na ireducibilne elemente od a i b dobivamo faktorizaciju na ireducibilne elemente od ab

$$ab = \left(\prod_{i=1}^{n_1} p_i\right)\left(\prod_{i=1}^{n_2} r_i\right).$$

Kako $p \mid ab$ te je ireducibilan, zaključujemo da je jednak nekom od elemenata p_i ili r_i. Dakle $p \mid a$ ili $p \mid b$, pa je p prost element. □

Definicija 4.27. *Polje algebarskih brojeva je proširenje konačnog stupnja polja* $\mathbb{Q}$.

Definicija 4.28. *Neka je* B *komutativni prsten i* $A \subseteq B$ *neki njegov potprsten. Kažemo da je element* $x \in B$ *cijeli nad* A *ako postoji* $n \in \mathbb{N}$ *i* $a_j \in A$*, za svaki* $j \in \{1, 2, \ldots n\}$*, takvi da vrijedi*

$$\left(\sum_{i=0}^{n-1} a_i b^i\right) + b^n = 0.$$

Definicija 4.29. *Neka je* A *integralna domena i* L *polje koje sadrži* A*. Skup elemenata iz* L *koji su cijeli nad* A *tvori prsten. Taj prsten zovemo cijelo zatvorenje od* A *u* L.

Definicija 4.30. *Cijelo zatvorenje prstena* $\mathbb{Z}$ *u polju algebarskih brojeva* $\mathbb{F}$ *zovemo prsten cijelih brojeva u* $\mathbb{F}$ *i označavamo s* $\mathcal{O}_{\mathbb{F}}$.

Propozicija 4.31. *Neka je* $\mathbb{F}$ *polje algebarskih brojeva. Algebarski cijeli broj* $x \in \mathcal{O}_{\mathbb{F}}$ *je invertibilan u* $\mathcal{O}_{\mathbb{F}}$ *ako i samo ako vrijedi* $N_{\mathbb{F}|\mathbb{Q}}(x) = \pm 1$.

Dokaz prethodne propozicije možete pogledati u [22, Korolar 1.11].

Sada opisujemo rad algoritma. Neka je n broj kojeg želimo faktorizirati. Na početku algoritma odabiremo neki normirani polinom $f \in \mathbb{Z}[X]$ koji je ireducibilan nad $\mathbb{Z}$ i broj $m \in \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ takav da je $f(m) \equiv 0 \pmod{n}$. Neka je $\alpha \in \mathbb{C}$ takav da vrijedi $f(\alpha) = 0$. Iz definicije algebarskih brojeva slijedi da je α algebarski broj, a svi algebarski brojevi zajedno s operacijama naslijeđenim iz $\mathbb{C}$ čine polje (vidi [27, Korolar 1.3]). Zaključujemo po Propoziciji 4.7 da je $\mathbb{Z}[\alpha]$ prsten. Također po Propoziciji 4.9 znamo da je polje $\mathbb{Q}(\alpha)$ vektorski prostor nad $\mathbb{Q}$. Sljedeća propozicija dat će nam dimenziju tog vektorskog prostora.

Propozicija 4.32. $\mathbb{Q}(\alpha)$ *je* d*-dimenzionalni vektorski prostor nad* $\mathbb{Q}$ *ako i samo ako je stupanj minimalnog polinoma od* α *jednak* d*. U tom slučaju baza vektorskog prostora* $\mathbb{Q}(\alpha)$ *nad* $\mathbb{Q}$ *je skup* $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.

Polinom $f \in \mathbb{Z}[X]$ je očito minimalni polinom od α budući da je ireducibilan. Pretpostavimo da je njegov stupanj d. Iz prethodne propozicije možemo zaključiti da se svaki element iz $\mathbb{Q}[\alpha]$ može napisati u obliku

$$\sum_{i=0}^{d-1} q_i \alpha^i,$$

gdje su $q_i \in \mathbb{Q}$. Očito se tada elementi potprstena $\mathbb{Z}[\alpha]$ od $\mathbb{Q}(\alpha)$ mogu napisati u obliku

$$\sum_{i=0}^{d-1} s_i \alpha^i,$$

gdje su $s_i \in \mathbb{Z}$. Definirajmo funkciju $\varphi : \mathbb{Z}[\alpha] \to \mathbb{Z}_n$ na sljedeći način

$$\varphi\left(\sum_{i=0}^{d-1} s_i \alpha^i\right) := \left(\sum_{i=0}^{d-1} s_i m^i \bmod n\right).$$

Lako se pokaže da je tako definirana funkcija surjektivni homomorfizam prstena.

Sada bismo htjeli konstruirati dvije faktorske baze, jednu u $\mathbb{Z}$, a drugu u $\mathbb{Z}[\alpha]$. Kako bismo to mogli najprije ćemo proširiti definicija pojma faktorske baze. Pretpostavit ćemo da je $\mathbb{Z}[\alpha]$ faktorijalan prsten. Algoritam je moguće modificirati da radi i kad $\mathbb{Z}[\alpha]$ nije faktorijalan prsten, ali uz dodatne komplikacije.

Definicija 4.33. *Neka je R faktorijalan prsten. Faktorska baza u R je neprazni skup različitih prostih elemenata iz R. Kažemo da se $x \in R$ faktorizira nad faktorskom bazom S ili da je x gladak s obzirom na faktorsku bazu S ako postoji $k \in \mathbb{N}_0$ i $r_1, r_2, \ldots, r_k \in S$ takvi da vrijedi*

$$x = \prod_{j=1}^{k} {r_j}^{a_j},$$

gdje su $a_j \in \mathbb{N}$.

Sada možemo konstruirati faktorske baze $P_1 \subseteq \mathbb{Z}[\alpha]$ i $P_2 \subseteq \mathbb{Z}$. Elementi od P_1 će biti (ne nužno svi) prosti elementi iz $\mathbb{Z}[\alpha]$ čija norma u $\mathbb{Q}(\alpha)|\mathbb{Q}$ nije veća od zadanog $B_1 \in \mathbb{N}$. Kako smo pretpostavili da je $\mathbb{Z}[\alpha]$ faktorijalan prsten, a polinom $f \in \mathbb{Z}[x]$ je normiran, što znači da je α algebarski cijeli broj po definiciji, sljedeća nam propozicija može pomoći u traženju prostih elemenata u $\mathbb{Z}[\alpha]$.

Propozicija 4.34. *Neka je $\alpha \in \mathbb{C}$ algebarski cijeli broj i $\mathbb{Z}[\alpha]$ faktorijalan prsten. Ako je za neki element $x \in \mathbb{Z}[\alpha]$ njegova norma $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x)$ prost element u $\mathbb{Z}$, onda je element x prost u $\mathbb{Z}[\alpha]$.*

Dokaz. Najprije primjetimo da je svaki element iz $\mathbb{Z}[\alpha]$ algebarski cijeli broj te je njegova norma u $\mathbb{Q}(\alpha)|\mathbb{Q}$ po Propoziciji 4.24 cijeli broj. Neka je $x \in \mathbb{Z}[\alpha]$ takav da je $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x)$ prost u $\mathbb{Z}$. Odaberimo proizvoljne $a, b \in \mathbb{Z}[\alpha]$ takvi da je $x = ab$. Tada zbog multiplikativnosti norme (vidi Propoziciju 4.25) vrijedi $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x) = N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(ab) = N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(a)N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(b)$. Kako je $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x)$ prost u $\mathbb{Z}$, točno jedan od brojeva $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(a)$ ili $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(b)$ mora po Propoziciji 4.26 biti invertibilan u $\mathbb{Z}$, odnosno element skupa $\mathbb{Z}^\times = \{-1, 1\}$. Pretpostavimo, bez smanjenja općenitosti da je $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(a)$ invertibilan. Tada je po Propoziciji 4.31 i $a \in \mathbb{Z}[\alpha]$ invertibilan. Kako je odabir $a, b \in \mathbb{Z}[\alpha]$ takvi da je $x = ab$ bio proizvoljan, zaključujemo da $x \in \mathbb{Z}[\alpha]$ nikako nemože biti umnožak dva neinvertibilna elementa iz $\mathbb{Z}[\alpha]$, pa je po Propoziciji 4.26 x prost broj. □

U faktorskoj bazi P_2 će kao i kod racionalnog sita biti svi prosti brojevi koji nisu veći od zadanog $B_2 \in \mathbb{N}$.

Propozicija 4.35. *Neka je* B *neki prirodni broj,* α *neki algebarski broj i* P *faktorska baza koja sadrži sve proste elemente iz* $\mathbb{Z}[\alpha]$ *čija norma u* $\mathbb{Q}(\alpha)|\mathbb{Q}$ *nije veća od* B. *Broj* $x \in \mathbb{Z}[\alpha]$ *je gladak s obzirom na faktorsku bazu* P *ako i samo ako je njegova norma* $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x)$ B*-gladak broj.*

Dokaz. Pretpostavimo da je $x \in \mathbb{Z}[\alpha]$ gladak s obzirom na faktorsku bazu $P = \{p \mid p \text{ je prost u } \mathbb{Z}[\alpha], N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(p) \leq B\}$. Dakle vrijedi

$$x = \prod_{p \in P} p^{k_p},$$

gdje su $k_p \in \mathbb{N}_0$. Iz svojstva multiplikativnosti norme (vidi Propoziciju 4.25) slijedi

$$N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x) = N_{\mathbb{Q}(\alpha)|\mathbb{Q}}\left(\prod_{p \in P} p^{k_p}\right) = \prod_{p \in P} \left(N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(p)\right)^{k_p}.$$

Kako je svaki $p \in P$ B-gladak, tj. vrijedi $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(p) \leq B$, očito je da su $p \in P$ jedini prosti elementi koji dijele $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x)$.

Pretpostavimo sada da je $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x)$ B-gladak broj i da se x ne faktorizira isključivo nad P. To znači da postoji $k \in \mathbb{N}$ i prosti elementi $q_i \in \mathbb{Z}[\alpha]$, $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(q_i) > B$, $i \in \{1, 2, \ldots, k\}$ takvi da vrijedi

$$x = \left(\prod_{p \in P} p^{k_p}\right)\left(\prod_{i=1}^{k} {q_i}^{l_i}\right),$$

gdje su $l_i \in \mathbb{N}$. Dalje imamo

$$N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x) = N_{\mathbb{Q}(\alpha)|\mathbb{Q}}\left(\left(\prod_{p \in P} p^{k_p}\right)\left(\prod_{i=1}^{k} {q_i}^{l_i}\right)\right) = \left(\prod_{p \in P} \left(N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(p)\right)^{k_p}\right)\left(\prod_{i=1}^{k} \left(N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(q_i)\right)^{l_i}\right),$$

pa očito $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x)$ nije B-gladak broj zbog $N_{\mathbb{Q}(\alpha)|\mathbb{Q}}(q_i) > B$. Time je dobivena kontradikcija, pa zaključujemo da se x faktorizira nad P. □

Definicija 4.36. *Elemente iz* $\mathbb{Z}[\alpha]$ *čija norma je* B*-gladak broj, za neki* $B \in \mathbb{Z}$*, zvat ćemo* B*-glatki elementi.*

Nakon što smo konstruirali faktorske baze tražimo relativno proste parove brojeva $a, b \in \mathbb{Z}$ takve da vrijedi

- $a + b\alpha$ je B_1-gladak element, tj. gladak je s obzirom na faktorsku bazu P_1
- $a + bm$ je B_2-gladak broj, tj. gladak je s obzirom na faktorsku bazu P_2

Do parova brojeva a i b dolazimo kao i kod kvadratnog sita metodom sijanja. Pretpostavimo da je S skup svih parova brojeva a i b takvih da su

$$\prod_{(a,b)\in S} a + b\alpha \quad \text{i} \quad \prod_{(a,b)\in S} a + bm$$

potpuni kvadrati u $\mathbb{Z}[\alpha]$, odnosno $\mathbb{Z}$. Kako je $\varphi : \mathbb{Z}[\alpha] \to \mathbb{Z}_n$ homomorfizam zaključujemo da vrijedi

$$\varphi\left(\prod_{(a,b)\in S} a + b\alpha\right) \equiv \prod_{(a,b)\in S} \varphi(a + b\alpha) \pmod{n}.$$

Na desnoj strani prethodne kongruencije imamo potpuni kvadrat u $\mathbb{Z}$ budući da vrijedi $\varphi(a + b\alpha) = a + bm \pmod{n}$. Budući da φ potpuni kvadrat iz $\mathbb{Z}[\alpha]$ šalje u potpuni kvadrat iz $\mathbb{Z}_n$, tj. za svaki $x \in \mathbb{Z}[\alpha]$ vrijedi $\varphi(x^2) = \varphi(x)^2 \pmod{n}$ na lijevoj strani prethodne relacije kongruencije imamo potpuni kvadrat u $\mathbb{Z}_n$, no mi bismo htjeli imati potpuni kvadrat u $\mathbb{Z}$, tj. mi još uvijek nismo formalno gledano dobili kongruenciju kvadrata već relaciju oblika $a^2 \bmod n \equiv b^2 \pmod{n}$. Budući da za svaki $x \in \mathbb{Z}$ vrijedi $(x \bmod n) \bmod n$, očito se iz prethodne kongruencije može dobiti kongruencija kvadrata $a^2 \equiv b^2 \pmod{n}$, što obično dovodi do netrivijalne faktorizacije broja n.

Ukoliko je faktorizacija trivijalna, tj. uvjet $a \not\equiv \pm b \pmod{n}$ nije zadovoljen, treba pokušati dobiti novu kongruenciju kvadrata drugačijom kombinacijom množenja relacija. Problem pronalaska skupa S, odnosno relacija koje u umnošku daju kongruenciju kvadrata se kao i kod kvadratnog sita svodi na problem traženja linearne ovisnosti vektora eksponenata koje dobijemo iz relacija. Budući da je duljina tih vektora $B_1 + B_2$, preporuča se da pronađemo nešto više od $B_1 + B_2$ relacija kako bismo bili sigurni da možemo dobiti kongruenciju kvadrata.

Za uspješan rad algoritma polinom $f \in \mathbb{Z}[X]$ kojeg odabiremo na početku algoritma mora imati male koeficijente i biti stupnja približno $(3\ln(n)/\ln(\ln(n)))^{1/3}$, što znači da se za velike brojeve n koji se uspješno faktoriziraju koriste polinomi stupnja 4, 5 i 6. Takvi

polinomi postoje za tzv. Cunninghamove brojeve, među kojima su najpoznatiji Mersennovi brojevi koje smo već spominjali (vidi Definicija 1.19) i Fermatovi brojevi (vidi Definicija 4.1).

Definicija 4.37. *Brojevi oblika* $b^n \pm 1$*, gdje je* $b \in \mathbb{Z}$ *prost broj, zovu se Cunninghamovi brojevi.*

Primjer 4.38. *Pokušajmo naći ireducibilni polinom* $f \in \mathbb{Z}[X]$ *i broj* m *takav da je* $f(m) \equiv 0 \pmod{n}$ *za Cunninghamov broj* $3^{479}+1$*. Očito vrijedi*

$$3^{480}+3 = 3\left(3^{479}+1\right) \equiv 0 \pmod{3^{479}+1}.$$

Kako je $3^{480}+3 = (3^{80})^6+3$*, možemo uzeti polinom* $f(x) = x^6+3$ *i* $m = 3^{80}$*.*

Za brojeve definirane pomoću linearnih rekurzija polinome je teže naći te su složeniji. Primjerice za faktorizaciju 709. Fibonaccijevog broja F_{709} korišten je polinom $f(x) = x^5+10x^3+10x^2+10x+3$. Broj m takav da je $f(m) \equiv 0 \pmod{n}$ mora zadovoljavati dodatni uvjet $a+bm \equiv 0 \pmod{n}$ za neke $a, b \leq n^{1/d}$, gdje je d stupanj polinoma f, kako bi algoritam radio. Primjerice m (ne pišemo konkretan broj jer je predugačak) takav da je $f(m) = m^5+10m^3+10m^2+10m+3 \equiv 0 \pmod{F_{709}}$ zadovoljava navedeni uvjet jer vrijedi $F_{142}m - F_{141} \equiv 0 \pmod{F_{709}}$.

Algoritam specijalnog sita je posebno efikasan za brojeve oblika $n = r^e \pm s$ gdje su $r, e, s \in \mathbb{N}$ te su r i s mali brojevi, ali i druge brojeve koji se mogu prikazati u obliku polinoma s malim koeficijentima. Naime, kod faktorizacije takvih brojeva u usporedbi s općenitim cijelim brojevima norme elemenata iz $\mathbb{Z}[\alpha]$ su manje, a to znači da je veća vjerojatnost da su te norme B_1-glatki brojevi, što pak po Propoziciji 4.35 znači da je veća vjerojatnost da su elementi iz $\mathbb{Z}[\alpha]$, uključujući i brojeve $a+b\alpha$ koje mi tražimo, glatki s obzirom na faktorsku bazu $P_1 \subseteq \mathbb{Z}[\alpha]$.

Na kraju dajemo primjer faktorizacije broja pomoću specijalnog sita.

Primjer 4.39. *Pokušajmo faktorizirati broj* $n = 510^2+1 = 260101$*. Polinom* $f(x) = x^2+1$ *je ireducibilan i za* $m = 510$ *očito vrijedi* $f(510) \equiv 0 \pmod{260101}$*. Također za* $\alpha = i \in \mathbb{C}$ *vrijedi* $f(i) = i^2+1 = -1+1 = 0$*. Sada želimo konstruirati faktorsku bazu* $P_1 \subseteq \mathbb{Z}[i]$ *(primjetimo da je* $\mathbb{Z}[i]$ *faktorijalan prsten) i* $P_2 \subseteq \mathbb{Z}$*. Neka su gornje ograde na te baze brojevi* $B_1 = 55$ *i* $B_2 = 40$*.*

Za $x = x_1+x_2i \in \mathbb{Z}[i]$*, gdje su* $x_1, x_2 \in \mathbb{Z}$*, možemo lako provjeriti je li norma* $N_{\mathbb{Q}(i)|\mathbb{Q}}(x) = {x_1}^2+{x_2}^2$ *prost broj. Iz Propozicije 4.34 slijedi da je za* $x_1, x_2 \in \mathbb{Z}$*, takve da je* ${x_1}^2+{x_2}^2$ *prost element u* $\mathbb{Z}$*,* x_1+x_2i *prosti element u* $\mathbb{Z}[i]$*. Primjerice* $5+2i$ *je prost u* $\mathbb{Z}[i]$ *jer je* $5^2+2^2 = 25+4 = 29$ *prost u* $\mathbb{Z}$*.*

Neka je x *prost element u* $\mathbb{Z}[i]$ *takav da je* $N_{\mathbb{Q}(i)|\mathbb{Q}}(x)$ *prost element u* $\mathbb{Z}$ *i* y *invertibilan u* $\mathbb{Z}[i]$*. Budući da je* y *invertibilan u* $\mathbb{Z}[i]$*, po Propoziciji 4.31 mora vrijediti* $N_{\mathbb{Q}(i)|\mathbb{Q}}(y) = \pm 1$*.*

Kako je $N_{\mathbb{Q}(i)|\mathbb{Q}}(x)$ *prost u* $\mathbb{Z}$ *i vrijedi* $N_{\mathbb{Q}(i)|\mathbb{Q}}(xy) = N_{\mathbb{Q}(i)|\mathbb{Q}}(x)N_{\mathbb{Q}(i)|\mathbb{Q}}(y) = \pm N_{\mathbb{Q}(i)|\mathbb{Q}}(x)$ *zaključujemo da je i* $N_{\mathbb{Q}(i)|\mathbb{Q}}(xy)$ *prost u* $\mathbb{Z}$*, odnosno da je* xy *prost u* $\mathbb{Z}[i]$*. Budući da je skup svih invertibilnih elemenata u* $\mathbb{Z}[i]$ *jednak* $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$*, za svaki prost element* x *iz* $\mathbb{Z}[i]$ *postoje još tri prosta elementa iz* $\mathbb{Z}[i]$*, dobivena množenjem elementa* x *sa* -1*,* i *te* $-i$*, koji imaju istu normu kao* x*. Uzmimo npr.* $y = -i$ *i* $x = 5 + 2i$*, tada je* $N_{\mathbb{Q}(i)|\mathbb{Q}}((-i)(5 + 2i)) = N_{\mathbb{Q}(i)|\mathbb{Q}}(2 + (-5)i) = 2^2 + (-5)^2 = 4 + 25 = 29$ *prost u* Z *te je* $(-i)(5 + 2i)$ *prost u* $\mathbb{Z}[i]$*.*

Ako se u P_1 *nalazi prost element* x*, trebamo li onda staviti u* P_1 *i proste elemente* $-x$*,* ix *i* $-ix$*? To možemo učiniti, ali će tada skup* P_1 *biti nepotrebno velik. Budući da se svaki invertibilni element u* $\mathbb{Z}[i]$ *može prikazati kao potencija elementa* i*, elemente* $-x$*,* ix *i* $-ix$ *možemo dobiti množenjem elementa* x *potencijom elementa* i*. Dakle, umjesto da sve proste elemente u* $\mathbb{Z}[i]$ *koji imaju istu normu stavljamo u faktorsku bazu, dovoljno je staviti samo jednog od njih te element* $i \in Z[i]$*. Tako dolazimo do faktorske baze* $P_1 = \{i, 1 + i, 5 + 2i, 1 + 2i, 1 + 6i, 3 + 2i, 5 + 4i, 1 + 4i, 7 + 2i\}$*. Druga, ne toliko bitna, ali zanimljiva posljedica ovog načina je da će faktorizacija nad* P_2 *sada biti jedinstvena do na poredak elemenata iz* P_1*.*

U faktorskoj bazi P_2 *biti će svi prosti elementi iz* $\mathbb{Z}$*, no opet za svaki prost element* $x \in \mathbb{Z}$ *i invertibilni element* $y \in \mathbb{Z}^\times = \{-1, 1\}$ *će element* xy *također biti prost u* $\mathbb{Z}$*. U* P_2 *je dakle dovoljno staviti samo pozitivne proste brojeve i broj* -1*. Tako dolazimo do faktorske baze* $P_2 = \{-1, 2, 3, 5, \ldots, 37\}$*.*

Sada metodom sijanja tražimo parove brojeva $a, b \in \mathbb{Z}$ *takve da su* $a + bi$ *i* $a + 510b$ *faktoriziraju nad faktorskim bazama* P_1 *i* P_2*. Za* $|a| \leq 200$ *i* $b \leq 54$ *pronaći ćemo* 23 *para takvih brojeva što nam daje* 23 *vektora eksponenata duljine* $P_1 + P_2 = 9 + 13 = 22$*. Budući da je broj vektora veći od njihove duljine, Gausovim eliminacijama (ili nekim drugim algoritmom) sigurno ćemo pronaći vektore koji u zbroju modulo* 2 *daju nulvektor. Sljedećom tablicom prikazujemo skup* S *parova brojeva* (a, b) *takvih da su*

$$\prod_{(a,b)\in S} a + bi \quad i \quad \prod_{(a,b)\in S} a + 510b$$

potpuni kvadrati u $\mathbb{Z}[i]$*, odnosno* $\mathbb{Z}$*.*

Množenjem elemenata $a+bi$ *iz prethodne tablice, tj. takvih da su* $(a, b) \in S$ *dobivamo potpuni kvadrat u* $\mathbb{Z}[i]$*.*

$$\begin{aligned}\prod_{(a,b)\in S} a + bi &= i^{10}(1 + i)^2(1 + 2i)^2(3 + 2i)^4(1 + 4i)^2(5 + 2i)^4(1 + 6i)^2(5 + 4i)^2 \\ &= (i(1 + i)(1 + 2i)(3 + 2i)^2(1 + 4i)(5 + 2i)^2(1 + 6i)(5 + 4i))^2 \\ &= (-156017 + 110961i)^2\end{aligned}$$

(a, b)	$a + bi$	$a + 510b$
$(34, 19)$	$i^3(1 + 6i)(5 + 4i)$	$9724 = 2^2 \cdot 11 \cdot 13 \cdot 17$
$(-70, 1)$	$i(3 + 2i)^2(5 + 2i)$	$440 = 2^3 \cdot 5 \cdot 11$
$(-4, 1)$	$i(1 + 4i)$	$506 = 2 \cdot 11 \cdot 23$
$(-2, 5)$	$i(5 + 2i)$	$2548 = 2^2 \cdot 7^2 \cdot 13$
$(3, 1)$	$i^3(1 + i)(1 + 2i)$	$513 = 3^3 \cdot 19$
$(-5, 7)$	$(1 + i)(1 + 6i)$	$3565 = 5 \cdot 23 \cdot 31$
$(3, 2)$	$3 + 2i$	$1023 = 3 \cdot 11 \cdot 31$
$(-59, 2)$	$(1 + 2i)(1 + 4i)(5 + 4i)$	$961 = 31^2$
$(-102, 23)$	$i(3 + 2i)(5 + 2i)^2$	$11628 = 2^2 \cdot 3^2 \cdot 17 \cdot 19$

Množenjem elemenata $a + 510b$ *iz prethodne tablice, tj. takvih da su* $(a, b) \in S$ *dobivamo potpuni kvadrat u* $\mathbb{Z}$*.*

$$\begin{aligned}\prod_{(a,b)\in S} a + 510b &= 2^10 \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 11^4 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 31^4 \\ &= (2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31^2)^2 \\ &= 339597320942880^2\end{aligned}$$

Djelovanjem homomorfizma φ *na potpuni kvadrat u* $\mathbb{Z}[i]$ *dobit ćemo potpuni kvadrat u* $\mathbb{Z}_n$*.*

$$\varphi\left((-156017 + 110961i)^2\right) = (\varphi(-156017 + 110961i))^2 \bmod 260101$$
$$= ((-156017 + 110961 \cdot 510) \bmod 260101)^2 \bmod 260101 = (252277)^2 \bmod 260101$$
$$= (-7824)^2 \bmod 260101 = 7824^2 \bmod 260101$$

Dakle imamo kongruenciju kvadrata

$$7824^2 \equiv 339597320942880^2 \pmod{260101}.$$

Budući da vrijedi $339597320942880 \bmod 260101 = 151328$ *vrijedi sljedeća, jednostavnija, kongruencija kvadrata*

$$7824^2 \equiv 151328^2 \pmod{260101}.$$

Sada imamo netrivijalnu faktorizaciju broja 260101

$$260101 = (151328 + 7824, 260101)(151328 - 7824, 260101) = 29 \cdot 8969.$$

Bibliografija

[1] Daniel Julius Bernstein, *Detecting Perfect Powers in Essentially Linear Time, and Other Studies in Computational Number Theory*, University of California, Berkeley, 1995, http://cr.yp.to/papers/powers.pdf.

[2] Matthew Edward Briggs, *An Introduction to the General Number Field Sieve*, Magistarski rad, 1998, http://www.math.vt.edu/people/brown/doc/briggs_gnfs_thesis.pdf.

[3] Steven Byrnes, *The Number Field Sieve*, http://sjbyrnes.com/math129-finalpaper.pdf, 2005.

[4] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993, https://worldtracker.org/media/library/Science/680mathsbooks/Numbertheory/Acourseincomputationalalgebraicnumbertheory-CohenH..pdf.

[5] Richard E. Crandall i Carl Pomerance, *Prime Numbers - A Computational Perspective*, Springer, 2005, http://thales.doa.fmph.uniba.sk/macaj/skola/teoriapoli/primes.pdf.

[6] Sanjoy Dasgupta, Christos Harilaos Papadimitriou i Umesh Virkumar Vazirani, *Algorithms*, http://www.cs.berkeley.edu/~vazirani/algorithms/, 2006.

[7] Andrej Dujella, *Kriptografija*, http://web.math.pmf.unizg.hr/~duje/kript/kriptografija.html.

[8] _____, *Uvod u teoriju brojeva*, http://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf.

[9] Todd Ebert, *Computational Complexity*, http://www.cecs.csulb.edu/~ebert/teaching/lectures/528/complexity.

[10] Timothy Scott Gegg-Harrison, *Ancient Egyptian Numbers A CS-Complete Example*, ACM SIGCSE Bulletin **33** (2001), br. 3, 268–272, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.4094&rep=rep1&type=pdf.

[11] Linda Gilbert i Jimmie Gilbert, *Elements of Modern Algebra*, Brooks/Cole, 2008, http://ebook-download-now.com/g/download/0495561363/Elements-of-Modern-Algebra,7th-edition/.

[12] Andrew Granville, *Smooth numbers: computational number theory and beyond*, Proc. MSRI Conf. Algorithmic Number Theory: Lattices, University Press, http://math.utoledo.edu/~codenth/Spring_13/3200/NT-books/Smooth_Numbers-Computational_Number_Theory_and_Beyond-Granville.pdf.

[13] Thomas Heath, *The Thirteen Books of Euclid's Elements, Books III - IX*, Cambridge University Press, 1908, http://www.wilbourhall.org/.

[14] Boris Širola, *Algebarske strukture*, http://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf.

[15] Erich Kaltofen, *Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems*, AAECC, Lecture Notes in Computer Science, sv. 673, Springer, 1993, str. 195–212, http://www4.ncsu.edu/~kaltofen/bibliography/95/Ka95_mathcomp.pdf.

[16] Saša Krešić-Jurić, *Algebarske strukture*, http://www.pmfst.hr/~skresic/Algebra/Skripta/Algebarske_strukture_v3.pdf, 2013.

[17] Ramanujachary Kumanduri i Cristina Romero, *Number Theory with Computer Applications*, Featured Titles for Number Theory Series, Prentice Hall, 1998.

[18] Beatrice Lumpkin, *African and African-American Contributions to Mathematics*, http://www.pps.k12.or.us/departments/curriculum/5025.htm, 1987.

[19] Peter L. Montgomery, *A block Lanczos algorithm for finding dependencies over* $GF(2)$, Proc. of Eurocrypt, LNCS, sv. 921, 1995, str. 106–120.

[20] Nicomachus, *Introduction to Arithmetic*, The Macmillan company, 1926, http://archive.org/details/NicomachusIntroToArithmetic.

[21] Robert B. Ash & W. Phil Novinger, *Complex Variables*, Dover Publications, 2007, http://www.math.sc.edu/~girardi/m7034/book/AshComplexVariablesWithHyperlinks.pdf.

[22] Frédérique Oggier, *Introduction to Algebraic Number Theory*, http://www1.spms.ntu.edu.sg/~frederique/ANT10.pdf, 2009.

[23] Carl Pomerance, *A tale of two sieves*, Notices of the American Mathematical Society **43** (1996), br. 12, 1473–1485, http://www.ams.org/notices/199612/pomerance.pdf.

[24] Feng Qi i Bai Ni Guo, *Sharp inequalities for the psi function and harmonic numbers*, http://arxiv.org/abs/0902.2524, 2009.

[25] John Barkley Rosser & Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics **6** (1962), br. 1, 64–94, http://projecteuclid.org/euclid.ijm/1255631807.

[26] Arnold Schonhage, Andreas E W. Grotefeld i Ekkehart Vetter, *Fast Algorithms-A Multitape Turing Machine Implementation*, Bibliographisches Institut Wissenschaftsverlag, 1994.

[27] Jerry Shurman, *Number Theory*, http://people.reed.edu/~jerry/361/lectures/mats.html.

[28] Mladen Vuković, *Izračunljivost*, http://web.math.pmf.unizg.hr/~vukovic/Skripte/IZN-skripta-2009.pdf, 2009.

[29] ———, *Složenost algoritama*, http://web.math.pmf.unizg.hr/~vukovic/Diplomski-kolegiji/SA/SA-skripta-2013-verzija-4.pdf, 2013.

[30] Simon A. Ward, *The divergence of the sum of reciprocals of primes and Mertens*, Magistarski rad, 2009.

[31] Tom Weston, *Algebraic Number Theory*, http://www.math.umass.edu/~weston/cn/notes.pdf, 1999.

Sažetak

Prije razvoja računala složenost algoritama nije bila važna te ni nije postojala kao grana matematike budući da su algoritmi morali biti provedeni ručno, "na papiru". Faktorizacija nije imala nikakvu praktičnu važnost te su se njome obično bavili matematičari iz radoznalosti, a oni malo bolji su pokušavali implementirati nove ideje i pronaći nove algoritme za faktorizaciju, te su tako i nastali algoritmi poput Fermatove faktorizacije ili Eulerovog algoritma. Razvojem računala i teorije složenosti algoritama te zbog važnosti faktorizacije u kriptografiji, složenost algoritama za faktorizaciju velikih brojeva je postala vrlo bitan faktor što je rezultiralo pojavom niza novih brzih algoritama.

Mnogi od tih algoritama imaju temelje u starijim algoritmima. Mi smo pokazali kako se algoritmi racionalnog, kvadratnog i specijalnog sita baziraju na Fermatovoj faktorizaciji. Usprkos tome što su dodavanjem novih ideja navedeni algoritmi otišli korak dalje od Fermatove faktorizacije u smislu vremenske složenosti, još uvijek nije pronađen algoritam koji bi u polinomnom vremenu netrivijalno faktorizirao velike brojeve. U jednom trenutku su neki matematičari smatrali da je vremenska složenost svakog algoritma za faktorizaciju $\Omega(e^{\sqrt{\log(n)\log(\log(n))}})$ budući da su svi najbolji algoritmi imali tu složenost, a nijedan bolju, no tada se pojavio algoritam općeg sita brojeva. Danas se na isti način pitamo je li složenost svakog algoritma za faktorizaciju u najboljem slučaju jednaka složenosti općeg sita, tj. $\Omega(e^{c(\log(n))^{1/3}(\log(\log(n)))^{2/3}})$.

Pojave kvadratnog 1981. god. te specijalnog i općeg sita polja brojeva $1988 - 1990$. god. značile su veliki iskorak u brzini faktorizacije velikih brojeva, no nakon toga svaki napredak u faktorizaciji brojeva možemo zahvaliti isključivo razvoju računala i distribuiranog računanja. Osmisliti brži algoritam za faktorizaciju od općeg sita trenutno nije izgledno, a osmisliti polinoman algoritam izgleda gotovo nemoguće. Pretpostavimo na trenutak da je ipak moguće smisliti brži algoritam od općeg sita. Takav algoritam po mom mišljenju nebi bio rezultat optimizacije algoritama sita brojeva, već bi prije bio rezultat rada s drugim algoritmima i pronalaska novih pristupa i ideja u faktorizaciji brojeva. Osim pronalaženja bržih algoritama za današnja računala problem faktorizacije velikih brojeva moglo bi se rješiti u polinomnom vremenu kvantnim računanjem ukoliko je ono moguće.

Summary

Before computer development algorithm complexity was not important and didn't exist as a branch of mathematics since algorithms had to be carried out "on paper". Factorization had no practical importance, and it was usually practiced by mathematicians out of curiosity, and the better ones tryed to implement new ideas and find new algorithms for factorization, which resulted in algorithms such as Fermat factorization or Euler's algorithm. With the development of computers and algorithm complexity theory, as well as the importance of factorization in cryptography, complexity of factorization algorithms has become a very important factor which resulted in the emergence of a number of new fast algorithms.

Many of these algorithms are based on older algorithms. We have shown how the rational, quadratic and special sieve are based on Fermat factorization. Despite the introduction of new ideas into the aforementioned algorithms, which made a step further in regards to Fermat factorization in terms of time complexity, an algorithm which would factorize large numbers in polynomial time has still not been found. At one point, some mathematicians thought that the time complexity of each algorithm for factorization is $\Omega(e^{\sqrt{\log(n)\log(\log(n))}})$ since all the best algorithms had this complexity, and none had better, but then appeared the general number field sieve algorithm. Today, in the same way we wonder if the complexity of factorization problem is at best equal to the complexity of the general sieve, ie. $\Omega(e^{c(\log(n))^{1/3}(\log(\log(n)))^{2/3}})$.

The appearance of the quadratic in 1981. as well as the special and the general sieve in $1988-1990$ meant a great step forward in improving the speed of factorization of large numbers, but after that, all progress in factorization of numbers can be attributed solely to the development of computers and distributed computing. Developing faster factorization algorithms than the general sieve doesn't seem likely at the moment, and creating a polynomial algorithm seems almost impossible. Let's suppose for a moment that faster algorithm than the general sieve exists. Such an algorithm in my opinion would not have been the result of optimization of sieve algorithms, but would likely be a result of working with other algorithms and finding new approaches and ideas in the factorization of numbers. Besides finding a faster algorithm for today's computers, the problem of factorization of large numbers could be solved in polynomial time with quantum computation if such computation would be possible.

Životopis

Rođen sam 8. studenog 1988. godine u Varaždinu, a živim u Petrijancu, mjestu udaljenom oko 10 km zapadno od Varaždina. Godine 1995. godine upisao sam Osnovnu školu Petrijanec koju sam završio 2003. godine, kada upisujem matematički smjer Prve gimnazije Varaždin u Varaždinu. Srednju školu, odnosno gimnaziju završio sam 2007. godine, te sam iste godine upisao preddiplomski studij matematike na Prirodoslovno - matematičkom fakultetu u Zagrebu. Preddiplomski studij završio sam 2010. godine. Studij sam nastavio na istom fakultetu, te iste godine upisom na smjer "Računarstvo i matematika". Tokom diplomskog studija do sada položio sam upisane programom predviđene i propisane predmete, te mi je ostao još jedan izazov, a to je diplomski rad i diplomski ispit, kako bi uspješno završio upisani diplomski studij.