Универзитет Унион

Рачунарски факултет

дипломски рад

Факторизација бројева коришћењем решета бројног поља

Аутор:
Алекса Станковић

Ментор:
др Драган Урошевић

Београд, 22. август 2015.

Апстракт

Факторизација бројева је, као један од фундаменталних проблема математике, одувек био предмет интересовања математичара. Из античког периода нам је познат метод Ератостеновог решета. Методе за решавање овог проблема доживљавају процват у 20. и 21. веку кроз алгоритме који користе идеју *разлике квадрата*. У овом раду је изложен најнапреднији од ових алгоритама, који захваљујући континуираном усавршавању у последњих 25 година постиже спетакуларне резултате. Биће обрађене све фазе алгоритма, уз осврт на евентуалне могућности за даља истраживања и усавршавања. Уз то, биће споменут и практичан значај алгоритма у испитивању безбедности криптографских система који се ослањају на *RSA* криптосистем, као и на системе који се уздају у сложеност тражења дискретног логаритма(*Diffie-Hellman, ElGamal*).

Садржај

1 Увод

Проблем тражења оптималног алгоритма за факторизацију бројева још увек чека на решење. Иако је сам појам факторизације тривијалан, математика чак уз сву модерну апаратуру још увек не поседује одговоре на многа питања везана за овај проблем. Пре свега, у трагању за савршеним алгоритмом било би корисно знати које су теоријске границе за перформансе. Ова граница није позната, али већина математичара се слаже да вероватно није могуће постићи сложеност бољу од експоненцијалне. Ову сложеност има већина савремених алгоритама. Али чак и мале разлике у експоненту се могу снажно одразити на брзину, поготово за велике улазне податке, те итекако има смисла радити на унапређиавњу постојећих и конструкцији нових алгоритама. У овом раду је представљен најсавршенији алгоритам данашњице, чија је веома оптимизована верзија заслужна за највећи практичан успех до сада, а то је факторизација RSA-768 броја који се састоји од 232 децималне цифре. Вршене су факторизације и већих бројева, али су се обично заснивале на специфичности броја којег факторишемо[1]. За њих је коришћена специјална верзија алгоритма решета бројног поља, која је погодна за бројеве облика $r^e + s$, при чему су r и s мали. Генерална верзија којом се овде бавимо може да разлаже произвољне бројеве, па и оне чија је факторизација најсложенија, облика $n = pq$ где су p и q прости бројеви.

Осим теоријских разлога за изучавање оваквих алгоритама, факторизација има и практичну примену у испитивању безбедности криптографских система. Мноштво популарних криптосистема своју безбедност заснива на чињеници да је факторизација тешка операција за рачунање, те свако веће откриће у домену факторизације бројева има директан утицај на поверљивост савремене заштићене комуникације. Осим тога, овај алгоритам се уз мање модификације може начинити подесним и за решавање проблема тражења дискретног логаритма, на коме је утемељена још једна већа класа криптосистема. У овом раду ће пажња бити усмерена на факторизацију, док се читаоцу који је заинтересован за примену алгоритма решета бројног поља за тражење дискретног алгоритма препоручују радови [22],[23]. У раду ће бити дат детаљан опис свих корака за извршавање алгоритма.

Циљ је да се читаоцу упознатом са основним математичким појмовима из области алгебре и теорије бројева објасни начин функционисања алгоритма. Математика неопходна за читање овог рада изложена је у [5],[6].

Асимптотска сложеност овог алгоритма је, уз неке хеуристичке претпоставке, $L_n[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}]$, где је $L_n[u, v]$ ознака за $e^{(v+o(1))(\log n)^u(\log\log n)^{1-u}}$. За проучавање сложености овог алгоритма неопходно је темељно познавање разноврсних области математике, као што је алгебарска теорија бројева, теорија графова, реална и комплексна анализа, што је изван домета овог рада. Детаљније информације о овој проблематици се могу наћи у радовима [2],[3].

[1] На пример, највећи до сада факторисани број је $2^{1061} - 1$

2 Алгоритми разлике квадрата

Већина модерних метода факторизације се заснива на истој идеји. Уколико се тражи факторизација броја n, они покушавају да нађу два броја x и y, такве да је $x^2 \equiv y^2 \pmod{n}$. Одатле је:

$$(x+y)(x-y) \equiv 0 \pmod{n}$$

тј., $n \mid (x+y)(x-y)$. Ово је завршна тачка свих алгоритама разлике квадрата. Уз претпоставку да још важи $x \not\equiv \pm y \pmod{n}$ факторе можемо извући налажењем највећег заједничког делиоца $(x+y, n)$. Заиста, број $(x+y, n)$ ће делити n, па треба показати и да ће бити прави делилац. Уколико то не би био случај било би или $(x+y, n) = n$ или $(x+y, n) = 1$. У случају да је $(x+y, n) = n$, имамо да је $x \equiv -y \pmod{n}$, што је контрадикција. Уколико је $(x+y, n) = 1$, онда би из $((x-y)(x+y), n) = n$ морало да важи $(x-y, n) = n$ што је контрадикција са $x \not\equiv \pm y \pmod{n}$. Због тога је $1 < (x+y, n) < n$, па је $(x+y, n)$ прави делилац n, кога можемо наћи веома брзо Еуклидовим алгоритмом.

Дакле, за успешну факторизацију неопходни су нам парови бројева x и y који задовољавају $x^2 \equiv y^2 \pmod{n}$ и $x \not\equiv \pm y \pmod{n}$. Алгоритми се обично брину само о генерисању пара за који важи први услов, док се за други услов рачуна да постоји велика вероватноћа да ће бити задовољен. Уколико други услов није задовољен, тражи се нови пар (x, y) и опет врши провера. Након налажења неколико парова готово је сигурно да ћемо наћи један одговарајући.

Покушајмо да дамо доњу оцену вероватноће да за случајно изабрани пар (x,y) за који важи $x^2 \equiv y^2 \pmod{n}$, важи и $x \not\equiv \pm y \pmod{n}$. Довољно је посматрати само оне парове за које је $(xy, n) = 1$, јер у супротном можемо лако извући делиоца из (x, n) и (y, n). Због $(xy, n) = 1$ важи $(y, n) = 1$, па y има инверз у прстену $\mathbb{Z}/n\mathbb{Z}$. Зато је еквивалентно посматрати вероватноћу да x које задовољава $x^2 \equiv 1 \pmod{n}$ не задовољава $x \not\equiv \pm 1 \pmod{n}$. Ако је $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ факторизација n, то једначину по кинеској теореми о остацима можемо посматрати и као систем једначина:

$$x^2 \equiv 1 \pmod{p_1^{a_1}}$$

$$x^2 \equiv 1 \pmod{p_2^{a_2}}$$

$$\vdots$$

$$x^2 \equiv 1 \pmod{p_k^{a_k}}$$

Свака од ових једначина има најмање два решења ($x \equiv \pm 1$), па ако са m означимо број решења једначине $x^2 \equiv 1 \pmod{n}$ имамо да је $m \geq 2^k$. За $k > 1$ (тј. у случају да n није степен простог броја) важиће $m \geq 4$. Пошто од свих решења само два задовољавају $x \equiv \pm 1 \pmod{n}$, оцену можемо дати као:

$$\Pr(x \not\equiv \pm y \pmod{n} \mid x^2 \equiv y^2 \pmod{n}) = \frac{m-2}{m} = 1 - \frac{2}{m} \geq 0.5$$

.

Сматра се да је први математичар који је користио идеју разлике квадрата у сврху факторизације математичар Пјер де Ферма. Он је узимао целе бројеве x такве да је $x \approx \sqrt{n}$, и испитивао да ли је је број $z = x^2 - n$ потпуни квадрат, тј. решавао $y^2 = x^2 - n$, што би му давало одгаварјуће квадрате.

2.1 Диксонов алгоритам

Проблем код Фермаовог приступа је у томе што су кандидати за разлику квадрата (x, y) бирани директно. Овакав приступ је скоро сличан простом погађању делиоца n. Са друге стране, Диксонов[1] алгоритам [7] уводи решето које у себи садржи информације о обрађеним бројевима, временом сакупља све више и више корисних информација на основу којих формира пар (x, y) који ће дати факторизацију n.

Алгоритам прво фиксира базу фактора $F = \{p_1, p_2, p_3, ...p_k\}$, коју чине прости бројеви. Обично се поставља нека граница B, и у F се убацују бројеви мањи од B. За број x кажемо да је гладак у односу на базу F ако су сви његови прости фактори из F,тј. ако га можемо представити као $x = \prod_{i=1}^{k} p_i^{e_i}$. Идеја је да нађемо m brojeva $x_1, x_2, ..., x_m$ за које је $x_i^2 \pmod n$ глатко. За свако од тих x_i можемо писати $x_i^2 \equiv \prod_{j=1}^{k} p_j^{e_{ji}} \pmod n$. За $y = \prod_{i=1}^{m} x_i$ биће

$$y^2 \equiv (\prod_{i=1}^{m} x_i)^2 \equiv \prod_{i=1}^{m} x_i^2 \equiv \prod_{i=1}^{m}\prod_{j=1}^{k} p_j^{e_{ji}} \equiv \prod_{j=1}^{k}\prod_{i=1}^{m} p_j^{e_{ji}} \equiv \prod_{j=1}^{k} p_j^{e_{j1}+e_{j2}+...+e_{jm}} \pmod n$$

Са леве стране лако можемо прочитати једну вредност корена. Другу вредност можемо лако наћи из десне стране у случају да су за p_j експоненти $e_{j1} + e_{j2} + ... + e_{jm}$ парни , тј. да је $e_{j1} + e_{j2} + ... + e_{jm} = 2e_j$ за неко $e_j \in \mathbb{N}$. Узимамо да је

$$x = \prod_{i=1}^{k} p_i^{e_i} \pmod n$$

За овако x важи

$$x^2 \equiv \left(\prod_{j=1}^{k} p_j^{e_j}\right)^2 \equiv \prod_{j=1}^{k} p_j^{2e_j} \equiv \prod_{j=1}^{k} p_j^{e_{j1}+e_{j2}+...+e_{jm}} \equiv y^2 \pmod n$$

па имамо да је $x^2 \equiv y^2 \pmod n$, и пошто су корени бирани на различите начине можемо се надати да ће бити $x \not\equiv \pm y \pmod n$, што би нам могло дати факторизацију.

Дакле, наш циљ да кроз паметан одабир x_i добијемо да су експоненти r_i у факторизацији $y^2 \equiv \prod_{i=1}^{k} p_i^{r_i}$ парни. Зато ћемо посматрати подскупове од m пронађених бројева и y тражити као њихов производ. Формално, y записујемо као $y = \prod_{i=1}^{m} (x_i)^{c_i}$, при чему $c_i = 1$ означава да је број x_i укључен у факторизацију, а $c_i = 0$ да није. Тада је

$$y^2 = \left(\prod_{i=1}^{m} x_i^{c_i}\right)^2 \equiv \prod_{i=1}^{m} (x_i)^{2c_i} \equiv \prod_{i=1}^{m} (x_i^2)^{c_i} \equiv \prod_{i=1}^{m} \left(\prod_{j=1}^{k} p_j^{e_{ij}}\right)^{c_i} \equiv \prod_{i=1}^{m} \left(\prod_{j=1}^{k} p_j^{c_i e_{ij}}\right) \equiv$$
$$\prod_{j=1}^{k} \left(\prod_{i=1}^{m} p_j^{c_i e_{ij}}\right) \equiv \prod_{j=1}^{k} p_j^{c_1 e_{j1} + c_2 e_{j2} + ... + c_m e_{jm}}$$

[1] J.D.Dixon, професор на универзитету Carleton у Отави, у пензији од 2003. године

Сви експоненти у овој факторизацији ће бити парни ако и само ако задовољавају следећи систем једначина у пољу $\mathbb{Z}/2\mathbb{Z}$:

$$c_1e_{11} + c_2e_{12} + \ldots + c_me_{1m} \equiv 0 \pmod 2$$

$$c_1e_{21} + c_2e_{22} + \ldots + c_me_{2m} \equiv 0 \pmod 2$$

$$\vdots$$

$$c_1e_{k1} + c_2e_{k2} + \ldots + c_me_{km} \equiv 0 \pmod 2$$

при чему c_i посматрамо као непознате. Када нађемо више од k глатких бројева, тј. кад је $m > k$ овај систем има нетривијално решење, тј. решење у коме нису сви c_i нуле. Било које такво решење нам даје конструкцију бројева x и y, којима можемо покушати факторизацију.

Најједноставнија верзија Диксоновог алгоритма тражи глатке бројеве тако што бира произвољне $x < n$ и затим проверава да ли се $x^2 \pmod n$ разлаже у бази фактора. Након неког времена надамо се да ћемо наћи више од k глатких бројева, након чега сигурно можемо формирати разлику квадрата и уз мало среће добити факторе. Уколико факторизација не буде успешна настављамо претрагу, и комбинујемо нове бројеве са старим да би добили нова разлагања. Углавном је довољно само неколико нових бројева чији су квадрати глатки да би добили успешну факторизацију.

Већа база у Диксоновом алгоритму нам даје и већу шансу да је $x^2 \pmod n$ гладак. Ипак, бирање веће базе значи и да је неопходно да нађемо више бројева. Када n постане велико, постаје просто неопходно да имамо и већу базу, јер би уз малу базу било потребно доста среће и много времена за проналазак макар једног глатког броја.

2.2 Алгоритам квадратног решета

Алгоритам квадратног решета [8] је увео 1981. године Карл Померанс[1]. Овај алгоритам је дуго важио за најбржи метод факторизације произвољног броја, све до појаве алгоритма решета бројног поља. Данас је и даље метод избора за факторизацију бројева са мање од 100 декадних цифара. Поступак факторизације је готово исти као и код Диксоновог алгоритма. Суштинска разлика је у начину тражења глатких бројева. Ово ипак доноси значајно побољшање перформанси, с обзиром да је већину времена Диксонов алгоритам проводио у покушајима да нађе глатке бројеве(поступак формирања квадрата је прилично ефикасан).

Уместо захтева да бројеви $x_i^2 \pmod n$ буду глатки, алгоритам квадратног решета то захтева од бројева $x_i^2 - n$. Када нађемо k оваквих бројева, слично Диксоновом алгоритму важиће за $y = \prod_{i=1}^{m} x_i$:

$$y^2 = \prod_{i=1}^{m} x_i^2 \equiv \prod_{i=1}^{m} (x_i^2 - n) \equiv \prod_{i=1}^{m}\prod_{j=1}^{k} p_j^{e_{ji}} \equiv \prod_{j=1}^{k} p_j^{e_{j1}+e_{j2}+\ldots+e_{jm}} \pmod n$$

Када генеришемо довољно бројева x_i можемо приступити факторизацији на већ описан начин. На почетку фазе прикупљања x_i, алгоритам бира неку границу u за коју очекујемо да је довољно велика да се у скупу $\{x^2 - n | [\sqrt{n}] - u < x < [\sqrt{n}] + u\}$ нађе k глатких бројева. Овде смо транслирали x за $[\sqrt{n}]$ да би добили мање бројеве, који ће због тога вероватно имати и мале факторе. У меморији се прво иницијализује низ који репрезентује скуп $\{y = x^2 - n | [\sqrt{n}] - u < x < [\sqrt{n}] + u\}$ (приметимо да ово можемо урадити ефикасно, тако да операцију квадрирања применимо само једном). Након

[1] Carl Pomerance(1944-), амерички математичар

тога, за свако $p_i \in F$ решавамо квадратну[1] конгруенцију $x^2 \equiv n \pmod{p_i}$. Пошто је $\mathbb{Z}/p_i\mathbb{Z}$ поље, ова конгруенција има или два или ниједно решење. Базу F на почетку алгоритма бирамо тако да је n квадратни остатак за свако p_i, тако да ће свака од ових једначина имати два решења, x_1^i и x_2^i. Зато у генерисаном низу проверавамо дељивост са p_i само за $x = x_1^i + lp_i$ и $x = x_2^i + lp_i$, $l \in \mathbb{Z}$. Када сваки од бројева у низу изделимо одговарајућим факторима из базе, оне позиције код којих је $y = \pm 1$ ће означавати позиције глатких бројева. Пошто су бројеви глатки у $\mathbb{Z}$, они ће бити и глатки у $\mathbb{Z}/n\mathbb{Z}$, па даље можемо поступати као у Диксоновом алгоритму, само што овом приликом сваком x_i додељујемо знак($+$ или $-$) који третирамо као још један коефицијент и водимо рачуна да је $\prod_{i=1}^{m}(x_i^2 - n)$ позитивног знака.

Због чега ово доноси побољшање? Код Диксоновог алгоритма дељивост бројем p_i је проверавана за сваког кандидата, док је овде паметнијим приступом дељивост конкретним p_i проверавана само за $\frac{2}{p_i}$ кандидата. Приметимо да се ово лепо скалира и са растом броја p_i, тако да како је p_i већи број, а тиме и операција дељења скупља, биће мања вероватноћа да ће наш алгоритам покушавати да тај број дели тим фактором.

[1] Квадратним конгруенцијама ћемо се детаљније бавити када будемо говорили о квадратној бази фактора, у поглављу 3.3.3

3 Алгоритам решета бројног поља

1988. године Џон Полард[1] у папиру [10] презентује нову идеју за факторисање бројева. Са појавом папира [3] у коме су разјашњени детаљи неопходни за имплементацију алгоритам постаје познат под називом решето бројног поља. Иако је предложени метод био веома ефикасан, он је могао да се примењује само на бројеве облика $n = b^c + 1$ где је b веома мало. И поред овог ограничења, представљен алгоритам је сматран спектакуларним и омогућио је факторизације неких интересантних бројева, од којих је нарочито занимљива факторизација деветог Фермаовог броја $F_9 = 2^{2^9} + 1$.

Још у време стварања овог алгоритма се претпостављало да се може генерализовати за произвољне n. Ово се заиста испоставило тачним захваљујући раду [2]. Стари алгоритам је од тада познат као специјално решето бројног поља. У то време овај алгоритам је био првенствено значајан јер је давао најбољу сложеност за факторизацију[2]. Компликованост имплементације га је чинила неподесним за ондашње рачунаре. Овај алгоритам је најбржи тек за бројеве са преко 100 цифара, што је било изван домета ондашњих рачунарских машина, када су вршене факторизације бројева са до 80 цифара. Напретком рачунарске технологије овај алгоритам преузима примат од алгоритма квадратног решета, и захваљујући њему су познате неке факторизације општих 140-цифрених бројева. Алгоритам је и даље предмет екстензивног проучавања научне заједнице, која успева да пронађе нове начине да учини алгоритам ефикаснијим.

3.1 Идеја бројног поља

Сваки од алгоритама факторизације преко разлике квадрата се може апстраховати на следећи начин. Нека је дата група (довољно је и моноид) G, и хомоморфизам

$$\psi : G \mapsto \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Поред овога, неопходан је и поступак за генерисање елемената $g \in G$ за које је $\psi(g) \in \{(x, x)|x \in (\mathbb{Z}/n\mathbb{Z})^*\}$[3]. Тада сваки од алгоритама покушава да комбинацијом таквих елемената добије квадратан елемент, нађе корен h тог квадратног елелемента тако да важи $\psi(h) \notin \{(x, \pm x)|x \in \mathbb{Z}/n\mathbb{Z}\}$. На известан начин, структуру $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ преносимо на G у којој покушавамо да генеришемо квадратни елемент. У случају Диксоновог алгоритма имали смо $G = (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, а у алгоритму квадратног решета $G = (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z})^*$. Када n постане веома велико, решето уведено овим алгоритмима постаје исувише грубо. Ова грубоћа сита пре свега значи да је тражење корена у оваквој групи могуће само под јаким условима, које је тешко задовољити за велико n. Тада се опет морамо надати да ћемо случајним избором баш наћи одговарајуће елементе, што је био и проблем који је начинио Фермаов алгоритам неадекватним.

Како ово превазићи? Идеја је да се користи шира структура G у којој је лакше наћи корен. Поред групе G неопходно је осмислити и хомоморфизам ψ. Зато је логично посматрати структуре блиске $\mathbb{Z}$. Нека је $f \in \mathbb{Z}[X]$ иредуцибилан моничан полином степена d и нека је $\mathbb{Z}[\alpha]$ прстен генерисан неким његовим кореном[4] α. Тада сваки елемент $x \in \mathbb{Z}[\alpha]$ можемо представити у бази као $x = \sum_{i=0}^{d-1} a_i\alpha^i$ при чему је $a_0, a_1, ..., a_{d-1} \in \mathbb{Z}$.

[1] John Pollard(1941-), британски математичар

[2] Не постоји формалан математички доказ ове сложености. Израчуната сложеност је резултат хеуристичке анализе засноване на неким хипотезама, каква је рецимо генералисана Риманова хипотеза. Иако ова оцена није у потпуности формална, она нам ипак може помоћи да оценимо разлику у ефикасности различитих алгоритама.

[3] R^* означава мултипликативни моноид прстена R.

[4] Можемо узети било који корен, јер су сви прстени генерисани њима међусобно изоморфни.

Збир ових елемената је очигледно садржан у $\mathbb{Z}[\alpha]$, док за производ два елемента можемо користити релацију $f(\alpha) = 0$ да би га свели на базну репрезентацију. Поред тога, за потребе конструкције ψ биће нам неопходан број $m \in \mathbb{Z}$ за који је $f(m) \equiv 0 \pmod{n}$. Тада постоји природан хомоморфизам између прстена $\varphi : \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z}$ генерисан са $\varphi(1) = 1$ и $\varphi(\alpha) = m \pmod{n}$. Алгоритам решета бројног поља узима за $G = \mathbb{Z}^* \times \mathbb{Z}[\alpha]^*$, и користи хомоморфизам $\psi(a, x) = (a \pmod{n}, \varphi(x))$. Да би описали целокупан алгоритам, неопходно је одговорити још и на следећа питања:

1. Како бирати елементе $g \in G$ за које је $\psi(g) = (x, x)$?
2. Како наћи иредуцибилни полином $f \in \mathbb{Z}[X]$ и $m \in \mathbb{Z}$ тако да је $f(m) \equiv 0 \pmod{n}$?
3. Како наћи елементе $g_1, g_2, ..., g_n$ за које је $\prod_{i=1}^{n} g_i$ квадратан у G?
4. Уколико нам је познато да је $g \in G$ квадратан, како наћи $\psi(\sqrt{g})$[1]?

У нашем алгоритму генерисаћемо узајамно просте парове $(a, b) \in \mathbb{Z}^2$, и за тражене елементе g из питања (1) узимати $g = (a + bm, a + b\alpha)$. Остала питања су нешто компликованија и на њих дајемо одговор у наредним одељцима.

3.2 Избор полинома

Први корак у одабиру полинома јесте избор његовог степена. Већи степен полинома обично значи финију структуру решета, али и скупље операције. За бројеве између 50 и 80 цифара узима се степен $d = 3$, за бројеве са више од 80 а мање од 110 цифара $d = 4$, а за бројеве са више од 110 цифара $d = 5$. Најједноставнији начин за формирање полинома узима $m = \lceil n^{\frac{1}{d}} \rceil$, и затим број n расписује у бројевном систему са основом m, тако да је

$$n = a_d m^d + a_{d-1} m^{d-1} + ... + a_1 m + a_0$$

Није тешко доказати да ће овде бити $a_d = 1$. За полином узимамо

$$f(x) = x^d + a_{d-1} x^{d-1} + ... + a_1 x + a_0$$

Такав полином задовољава $f(m) = n \equiv 0 \pmod{n}$. Неопходно је још проверити његову иредуцибилност. Тест за несводљивост износимо у наредном одељку, а овде се бавимо алтернативном стратегијом коју примењујемо у случају да утврдимо да полином није несводљив. Тада се он може представити као производ $f(x) = g(x)h(x)$, и из ове факторизације веома вероватно можемо наћи факторизацију броја n, јер из $n = f(m) = g(m)h(m)$ можемо извући делиоце $g(m)$ и $h(m)$. У супротном, можемо узети неки други број близак првобитном m и на њега применити исти поступак.

3.2.1 Несводљивост полинома

Пре него што развијемо ефикасан алгоритам за тестирање иредуцибилности полинома, присетићемо се неких теоријских резултата о структури коначних поља, која се доказују у основним курсевима алгебре.

***Теорема* 1.** *Коначно поље $\mathbb{F}_q$ са q елемената задовољава следеће:*

1. $q = p^d$ за неко просто p

[1] Приметимо да корен у групи(прстену) није јединствено одређен. У овом тренутку за $\sqrt{g}$ сматрамо било које $h \in G$ за који је $h^2 = g$.

2. *Коначно поље са $q = p^d$ елемената постоји за произвољно изабрано просто p као и за произвољно d.*

3. *Сва коначна поља са истим бројем елемената су међусобно изоморфна.*

4. *У пољу $\mathbb{F}_q$ важи следеће разлагање полинома $x^q - x$:*

$$x^q - x = x(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_{q-1})$$

где су α_i сви елементи $\mathbb{F}_q^*$

Следећа теорема даје згодан начин за представљање поља преко иредуцибилног полинома:

Теорема 2. *Нека је $f(x)$ моничан иредуцибилан полином над пољем $\mathbb{F}_p$ степена d и нека је α корен[1] полинома f(x). Тада:*

- $\mathbb{F}_p[X]/f(x) \cong \mathbb{F}_{p^d}$
- *$f(x)$ дели полином $g(x)$ са коефицијентима у $\mathbb{Z}/p\mathbb{Z}$ ако и само ако је $g(\alpha) = 0 \pmod p$.*
- *Сваки елемент $x \in \mathbb{F}_{p^d}$ се може изразити као $\mathbb{F}_p$-линеарна комбинација елемената $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$*

Од значаја су и следеће теореме:

Теорема 3. *Нека су $a, b \in \mathbb{N}$ такви да $a|b$. Тада и $x^a - 1|x^b - 1$.*

Доказ. Пошто $a|b$, постоји k тако да је $b = ak$. Тада је:

$$(x^a - 1)(x^{a(k-1)} + x^{a(k-2)} + x^{a(k-3)} + \dots + x^a + 1) = x^{ak} + x^{a(k-1)} + x^{a(k-2)} + x^{a(k-3)}$$
$$+ \dots + x^{2a} + x^a - x^{a(k-1)} - x^{a(k-2)} - x^{a(k-3)} - \dots - x^a - 1 = x^{ak} - 1 = x^b - 1$$

□

Теорема 4. *Поље $\mathbb{F}_{q^e}$ се може видети као потпоље поља $\mathbb{F}_{p^d}$ ако и само ако је $p = q$ и $e|d$. Овакво потпоље је јединствено.*

Доказ. Претпоставимо да је $\mathbb{F}_{q^e}$ потпоље $\mathbb{F}_{p^d}$. Поље $\mathbb{F}_{q^e}$ садржи 1 и затворено је у односу на сабирање, па је зато $\mathbb{F}_p \subseteq \mathbb{F}_{q^e}$. Одатле видимо да морају имати исту карактеристику, па је $p = q$. Ако је $k = [\mathbb{F}_{p^d} : \mathbb{F}_{p^e}]$, онда из $p^d = |\mathbb{F}_{p^d}| = |\mathbb{F}_{p^e}|^k = (p^e)^k = p^{ek}$ видимо да $e|d$.

Обрнуто, нека је $q = p$ и $e|d$. Онда из теореме 3 имамо $x^e - 1|x^d - 1$, па и $p^e - 1|p^d - 1$. Зато опет применом теореме 3 имамо и да је $x^{p^e-1} - 1|x^{p^d-1} - 1$ и одатле $x^{p^e} - x|x^{p^d} - x$. Посматрајмо све елементе који задовољавају $x^{p^e} - x = 0$ у пољу $\mathbb{F}_{p^d}$. Није тешко доказати је овај скуп затворен у односу на сабирање и множење, а пошто садржи неутрале за сабирање и множење он је и поље, а самим тим и потпоље $\mathbb{F}_{p^d}$. Обзиром да има p^e елемената он мора бити изоморфан пољу $\mathbb{F}_{p^e}$. Уколико би још неко поље са p^e елемената било садржано у $\mathbb{F}_{p^d}$, онда би за сваки њен елемент морало да важи $x^{p^e} - x = 0$, па би се оно управо поклапало са пољем $\mathbb{F}_{p^e}$, јер полином $x^{p^e} - x$ има тачно p^e корена. □

[1] *За произвољно поље можемо конструисати натпоље које ће садржати све корене произвољних полинома у том пољу. Овакво поље се назива коренско поље, и можемо узети да је α елемент тог поља. Нама неће бити неопходно да знамо ишта о овом пољу, и α углавном третирамо као симбол који анулира полином f(x).*

Сада, када смо се упознали са структуром коначних поља, можемо размотрити проблем иредуцибилности полинома у њима.

***Теорема* 5.** *Нека је $f(x) \in \mathbb{F}_p[X]$ моничан и иредуцибилан полином степена e. Тада $f(x)|x^{p^d} - x$ ако и само ако $e|d$.*

Доказ. Претпоставимо да $f(x)|x^{p^d} - x$. Нека је α корен полинома $f(x)$ и нека је поље генерисано њиме $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^e}$. Тада, пошто је $f(\alpha) = 0$, мора бити и $\alpha^{p^d} - \alpha = 0$. Зато $\alpha \in \mathbb{F}_{p^d}$, и $\mathbb{F}(\alpha)$ је потпоље поља $\mathbb{F}_{p^d}$, па зато $e|d$ по теореми 4.

Обрнуто, ако $e|d$, поље $\mathbb{F}_{p^e}$ је потпоље поља $\mathbb{F}_{p^d}$. А пошто је $\mathbb{F}_{p^e} = \mathbb{F}_p(\alpha)$, то је и $\alpha \in \mathbb{F}_{p^d}$, и $\alpha^{p^d} - \alpha = 0$. Због тога, по теореми 2, $f(x)$ дели $x^{p^d} - x$. □

***Теорема* 6.** *Полином $x^{p^d} - x \in \mathbb{F}_p[X]$ је производ свих иредуцибилних, моничних полинома чији степен дели d над $\mathbb{F}_p$ међу којима нема идентичних.*

Доказ. Полином $x^{p^d} - x$ се може представити као производ иредуцибилних моничних полинома. Из претходне теореме закључујемо да степен сваког од њих мора делити d. Такође из претходне теореме видимо да се сваки иредуцибилан полином чији степен дели број d појављује као чинилац у факторизацији полинома. Први извод полинома $f(x)$ је $p^d x^{p^d-1} - 1 \equiv -1 \not\equiv 0 \pmod{p}$, па је он сепарабилан[1]. Зато се у његовој факторизацији не могу појавити вишеструки чиниоци. □

Следећа теорема ће нам омогућити изградњу жељеног алгоритма.

***Теорема* 7.** *Монични полином степена d је иредуцибилан у $\mathbb{F}_p[X]$ ако и само ако $f(x)$ дели $x^{p^d} - x$ и $(x^{p^{d/q}} - x, f(x)) = 1$ за све просте бројеве q који деле d.*

Доказ. Претпоставимо да је $f(x)$ иредуцибилан. Тада $f(x)$ мора делити $x^{p^d} - x$ по теореми 5. Обзиром да је $f(x)$ иредуцибилан, вредност $(x^{p^{d/q}} - x, f(x))$ може бити или 1 или $f(x)$. Али у случају да је $(x^{p^{d/q}} - x, f(x)) = f(x)$, по теореми 5 мора бити $d|(d/q)$ што није могуће, па за свако q важи $(x^{p^{d/q}} - x, f(x)) = 1$.

Обрнуто, нека $f(x)$ дели $x^{p^d} - x$ и нека је испуњено $(x^{p^{d/q}} - x, f(x)) = 1$ за сваки прост $q|d$. Доказ изводимо свођењем на апсурд. У том циљу, претпоставимо да $f(x)$ има нетривијалан фактор $g(x)$ чији је степен e строго мањи од d. Пошто $g(x)|f(x)$ и $f(x)|x^{p^d} - x$ онда и $g(x)|x^{p^d} - x$. Даље, $e|d$ по теореми 5. Пошто је e прави делилац d то мора постојати прост број q такав да $e|(d/q)$. Али онда, опет по теореми 5 имамо да $g(x)|x^{p^{d/q}} - x$, и пошто $g(x)|f(x)$ биће $(f(x), x^{p^{d/q}} - x) \neq 1$, што је контрадикција. □

Ово нам даје тест иредуцибилности полинома над коначним пољима. С обзиром да ће за наше потребе d бити мало, видимо да је овај тест прилично ефикасан. Али нама је неопходна иредуцибилност у прстену $\mathbb{Z}[X]$. Како осигурати овај услов? За ту сврху је згодна следећа теорема:

***Теорема* 8.** *Уколико је моничан полином $f(x) \in \mathbb{Z}[X]$ иредуцибилан у $\mathbb{F}_p[X]$, онда је он иредуцибилан и у $\mathbb{Z}[X]$.*

Доказ. Претпоставимо супротно. Тада је $f(x) = g(x)h(x)$, при чему су полиноми g(x) и h(x) монични. Али онда редукцијом коефицијената по модулу p добијамо факторизацију полинома $f(x) = g(x)h(x)$ у $\mathbb{F}_p[X]$, при чему водећи коефицијенти полинома $f(x), g(x)$ и $h(x)$ нису нула, па је ово права факторизација. Због тога $f(x)$ није иредуцибилан ни у $\mathbb{F}_p[X]$, што је контрадикција. □

[1] *Нема вишеструке корене*

Зато је за тестирање иредуцибилности полинома $f(x)$ довољно наћи неко p тако да $f(x)$ буде иредуцибилан у $\mathbb{F}_p[X]$. Ова метода нам даје генерални поступак. Ипак, проверу иредуцибилности у неким случајевима можемо вршити и директно. На пример, у случају да је $d = 3$, полином $f(x)$ је растављив ако и само ако има корен у $\mathbb{Z}$, и тај корен мора делити његов последњи коефицијент (који стоји уз $x^0 = 1$).

3.3 Решета

Овај део текста се бави проблемом комбиновања $g_1, g_2, ..., g_n$ за које је $\prod_{i=1}^{n} g_i$ квадратан у G. Пошто је $G = \mathbb{Z}^* \times \mathbb{Z}[\alpha]^*$ довољно је проверити да ли је $\alpha \in G$ корен у $\mathbb{Z}^*$ и у $\mathbb{Z}[\alpha]^*$. За тражење квадрата у $\mathbb{Z}^*$ користимо рационално решето, док се квадрати у $\mathbb{Z}[\alpha]^*$ траже преко алгебарског и квадратног решета. Суштина је у томе да ова решета раде заједно, тако да $\prod_{i=1}^{n} g_i$ задовољава свако од решета, чиме је он квадрат и у G. Сам овај поступак постаће јасан када се објасни начин рада решета у наредним одељцима.

3.3.1 Рационално решето

Рационално решето је заправо исто оно решето које смо користили код Диксоновог алгоритма. У првом кораку се поставља граница B, након чега формирамо базу k фактора $F = \{p_1, p_2, \ldots, p_k\}$ коју називамо рационална база фактора. За узајамно просте (a, b) тражимо да се $a + bm$ факторише у бази. Уколико је то случај, пару (a, b) можемо придружити за сваки фактор рационалног решета p_i коефицијенте e_i. Нека $\mathbb{F}$ чине сви елементи $\mathbb{Z}$ глатки у F. Коефицијенте e_i можемо видети и као хомоморфизме, $e_i : \mathbb{F} \to \mathbb{N}$, дефинисане са $e_i(\prod_{j=1}^{k} p_j^{e_j}) = e_i$. Слично алгоритму квадратног решета, тражићемо m парова (a_i, b_i) тако да је $e_i(\prod_{j=1}^{m}(a_j + b_j m))$ парно, односно у пољу $\mathbb{Z}/2\mathbb{Z}$ да је

$$\sum_{j=1}^{m} e_i(a_j + b_j m) \equiv 0 \pmod 2$$

Након налажења довољно глатких (a, b) алгоритам бира одговарајуће парове да би добио квадратни број на исти начин као у алгоритму квадратног решета, па ћемо опис тог поступка овде прескочити.

Како тражити парове (a, b)? Насумичним бирањем парова након којег би вршили проверу глаткости у F не можемо добити алгоритам ефикаснији од Диксоновог, с обзиром да је тражење глатких парова управо и било уско грло Диксоновог алгоритма. Видимо да је неопходно осмислити нарочиту процедуру за тражење бројева облика $a + bm$ који су глатки у F. Примењујемо поступак сличан оном из квадратног решета. Алгоритам у почетку сваког корака фиксира b (већина алгоритама креће од $b = 1$ и инкрементира га док не нађе довољно парова), и затим узима бројеве a_i у границi $-u < a_i < u$, за неко $u > 0$. Од одговарајућих a_i правимо низ у меморији који чине бројеви облика $a_i + bm$. У овом низу тражимо глатке бројеве, и то тако што сваки од бројева делимо са $p_j \in F$ докле год је то могуће. Након што смо дељење покушали за сваки $a_i + bm$ у низу са сваким p_j из F, у низу тражимо места где је резултат свих дељења ± 1, што означава да пар на датом месту даје гладак број. Циљ је да избегнемо неуспешна дељења бројевима $p_j \in F$. Приметимо да $p_j | a_i + bm \Leftrightarrow a_i + bm \equiv 0 \pmod{p_j}$, па је довољно проверити дељивост са p_j на бројевима $a + bm$ такве да је $a = -bm + p_j k, k \in \mathbb{Z}$.

Јасно је да је овакав начин решетања бржи од оног из Диксоновог алгоритма. Ипак, на први поглед делује да је оваква процедура готово иста оној у квадратном решету. Па зашто је онда овај алгоритам ефикаснији? Суштинска разлика је у томе што ће сада бројеви $a + bm$ генерисани узајамно простим паровима (a, b) покривати сваки могући број, за разлику од бројева $y = x^2 - n$ алгоритма квадратног решета који су знатно ређе распоређени. Због тога очекујемо да ће кандидати за глатке бројеве који се појављују у рационалном решету бити доста мањи, па самим тим и имати већу шансу да се факторишу у бази F.

Са друге стране, овакав формат нам не даје јасан начин за генерисање квадрата у $\mathbb{Z}[\alpha]$, што је било могуће на директан начин у алгоритму квадратног решета из $x^2 - n$ у $\mathbb{Z}/n\mathbb{Z}$. Зато је неопходно увођење решета у $\mathbb{Z}[\alpha]$, којем називамо алгебарским.

3.3.2 Алгебарско решето

Покушајмо да при стварању овог решета имитирамо стратегију рационалног решета. Природно би било да онда у алгебарску базу убацујемо просте или иредуцибилне елементе прстена $\mathbb{Z}[\alpha]$, и елементе $a+b\alpha$ факторишемо по њима. Нажалост, овај приступ није могућ. Покажимо зашто је то тако на примеру прстена $\mathbb{Z}[\sqrt{6}]$. Посматрајмо две факторизације броја 6, наиме $6 = 2 \cdot 3$ и $6 = \sqrt{6} \cdot \sqrt{6}$. Није тешко проверити да су 2,3 и $\sqrt{6}$ сви иредуцибилни у овом прстену, па су ово две различите факторизације. Због тога не постоји јединствен начин да се дефинише коефицијент уз базни фактор. Како превазићи овај проблем? Једно решење је да се посматрају само прстени $\mathbb{Z}[\alpha]$ са јединственом факторизацијом[1]. Ово је заиста и био приступ код раних имплементација алгоритма специјалног квадратног решета. Испоставља се да је овај захтев исувише рестриктиван у већини случајева, па је неопходно генералније решење, које се неће ослањати на специјалне особине $\mathbb{Z}[\alpha]$.

Пракса у теорији бројева је да се у оваквим случајевима пређе са факторизације елемената прстена на факторизацију идеала. Тада би идеја била да се уместо простих елемената у алгебарску базу убацују прости идеали $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$, и да онда за елемент $\beta \in \mathbb{Z}[\alpha]$ факторишемо идеал $\langle\beta\rangle$ у бази тако да буде $\langle\beta\rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_k^{e_k}$. Ово све можемо да урадимо уз претпоставку да је факторизација идеала добро дефинисана. Природно окружење за ово представљају Дедекиндови домени, што и видимо из једног начина за њихово дефинисање:

***Дефиниција* 1.** *Дедекиндов домен $\mathfrak{D}$ је домен целих[2] у коме се сваки ненула идеал може преставити на јединствен начин као производ простих идеала.*

И прстен $\mathbb{Z}$ је домен целих, у коме су сви идеали главни (облика $\langle n\rangle, n \in \mathbb{Z}$). Додатно, сви прости идеали су $\mathfrak{p}_i = \langle p_i\rangle$ за просте p_i, и ако је $n = \prod_{i=1}^{k} p_i^{e_i}$ онда ће бити $\langle n\rangle = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$, па је $\mathbb{Z}$ један од примера Дедекиндових домена. У овом случају факторизација идеала се поклапа са факторизацијом бројева, па је ово природно проширење појма факторизације. За наше потребе би било згодно да је $\mathbb{Z}[\alpha]$ Дедекиндов домен. Ово у већини случајева није тачно, па опет имамо проблем при дефинисању коефицијената. Ипак, ако посматрамо скуп $\{x \in \mathbb{Q}(\alpha) | g(x) = 0 \text{ за неко } g \in \mathbb{Z}[X]\}$, онда ће овај скуп бити Дедекиндов домен, који називамо интегралним затворењем $\mathbb{Z}$ у $\mathbb{Q}(\alpha)$, и означавамо са $\mathcal{O}_{\mathbb{Q}(\alpha)}$. Није тешко показати да је $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_{\mathbb{Q}(\alpha)}$

[1] Тј прстени у којима су сваке две факторизације на просте елементе еквивалентне. Такав је рецимо прстен Гаусових целих $\mathbb{Z}[i]$.

[2] *комутативни прстен са јединицом без делитеља нуле*

Наша жеља је да помоћу алгебарског решета нађемо m парова (a_i, b_i) тако да је

$$\prod_{i=1}^{m}(a_i + b_i\alpha) = \gamma^2 \tag{3.3.1}$$

за неко $\gamma \in \mathbb{Z}[\alpha]$, при чему се (a_i, b_i) факторишу у алгебарској бази. Означимо са $e_{\mathfrak{p}_i}$ хомоморфизам који елементу $\theta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ додељује степен идеала $\mathfrak{p}_i$ из факторизације $\langle\theta\rangle$. Рецимо ако је $\langle\theta\rangle = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$, онда је $e_{\mathfrak{p}_i}(\theta) = e_i$. Пошто је $\mathcal{O}_{\mathbb{Q}(\alpha)}$ Дедекиндов домен овај хомоморфизам је коректно дефинисан за све елементе $\mathcal{O}_{\mathbb{Q}(\alpha)}$ и све просте идеале $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{Q}(\alpha)}$. Применом хомоморфизма на једнакост 3.3.1 добијамо

$$e_{\mathfrak{p}_j}(\prod_{i=1}^{m}(a_i + b_i\alpha)) = e_{\mathfrak{p}_j}(\gamma^2) = 2e_{\mathfrak{p}_j}(\gamma)$$

Са друге стране је

$$e_{\mathfrak{p}_j}(\prod_{i=1}^{m}(a_i + b_i\alpha)) = \sum_{i=1}^{m} e_{\mathfrak{p}_j}(a_i + b\alpha)$$

па је зато

$$\sum_{i=1}^{m} e_{\mathfrak{p}_j}(a_i + b\alpha) \equiv 0 \pmod 2$$

Одатле можемо да наслутимо механизам за развој алгебарског решета: прво тражимо парове који се факторишу у алгебарској бази, и за алгебарска база од k елемената тражимо $m = k + 1$ или више глатких парова за које формирамо систем једначина:

$$\sum_{i=1}^{m} c_i e_{\mathfrak{p}_1}(a_i + b\alpha) \equiv 0 \pmod 2$$

$$\sum_{i=1}^{m} c_i e_{\mathfrak{p}_2}(a_i + b\alpha) \equiv 0 \pmod 2$$

$$\vdots$$

$$\sum_{i=1}^{m} c_i e_{\mathfrak{p}_k}(a_i + b\alpha) \equiv 0 \pmod 2$$

у коме $c_i \in \{0, 1\}$ третирамо као непознате. Обзиром да смо изабрали $m > k$ постоји неко решење такво да нису сви коефицијенти c_i нуле. За њега дефинишемо $A = \{0 < i \leq k | c_i = 1\}$, и онда можемо посматрати $\theta = \prod_{i\in A}(a_i + b_i\alpha)$. Да ли је ово довољно да нађемо корен од θ? За два различита елемента $\gamma_1, \gamma_2 \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ може важити $e_{\mathfrak{p}_i}(\gamma_1) = e_{\mathfrak{p}_i}(\gamma_2)$ за све просте идеале $\mathfrak{p}_i$, па само на основу вредности пресликавања $e_{\mathfrak{p}_i}$ не можемо наћи корен како смо то радили код рационалног решета. Осим тога, чак и ако ако бисмо успели да нађемо неко γ тако да је $2e_{\mathfrak{p}_i}(\gamma) = e_{\mathfrak{p}_i}(\theta)$ $(0 < i \leq k)$, то не би обавезно значило да је $\gamma^2 = \theta$, јер из $\langle\gamma^2\rangle = \langle\gamma\rangle^2 = \prod_{i=1}^{k} \mathfrak{p}_i{}^{2e_{\mathfrak{p}_i}(\gamma)} = \prod_{i=1}^{k} \mathfrak{p}_i{}^{e_{\mathfrak{p}_i}(\theta)} = \langle\theta\rangle$ тј. $\langle\gamma^2\rangle = \langle\theta\rangle$ не следи да је $\gamma^2 = \theta$. Ипак, уколико је неко θ заиста квадратно, онда оно мора задовољавати горњи систем једначина, тако да се у неким случајевима можемо надати да ћемо погодити одговарајући број. У наредном одељку ћемо видети да, уз сарадњу са пажљиво изабраним квадратним решетом, постоји велика шанса да алгебарско сито нађе баш квадратан број.

Да би могли да применимо овај поступак морамо да имамо начин за представљање елемената и идеала $\mathcal{O}_{\mathbb{Q}(\alpha)}$, као и ефикасан начин за рад са њима. Кључно је да операције попут факторизације идеала на просте (тј. пресликавања $e_{\mathfrak{p}_i}$) буду довољно брзе. У раду [25] је објашњено како се све ово може одрадити. Због обимности те теме ми се њоме овде нећемо бавити, али ћемо зато представити алтернативан, једноставнији начин који не жртвује превише перформанси.

У ту сврху биће нам неопходан појам норме елемента. Норму дефинишемо у пољу $\mathbb{Q}(\alpha)$. Пошто је α нула иредуцибилног и моничног полинома $f(x)$, то је он и сепарабилан и важи факторизација

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$$

при чему су сви α_i различити (и можемо претпоставити да је $\alpha_1 = \alpha$). Даље, важи следећа теорема:

***Теорема* 9.** *Нека је $f(x) \in \mathbb{Z}[X]$ моничан, иредуцибилан полином степена d и α нека његова нула. Тада постоји тачно d различитих хомоморфизама $\sigma_i : \mathbb{Q}(\alpha) \to \mathbb{C}$.*

Доказ. Дефинишемо за σ_i да је $\sigma_i(1) = 1$ и $\sigma_i(\alpha) = \alpha_i$. Ако је α нула полинома $f(x) = x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \ldots + a_0$, онда сваки елемент $\mathbb{Q}(\alpha)$ можемо написати као $a_{d-1}\alpha^{d-1} + a_{d-2}\alpha^{d-2} + \ldots + a_0$. Пошто захтевамо да су σ_i хомоморфизми, онда мора бити и $\sigma_i(a_{d-1}\alpha^{d-1} + a_{d-2}\alpha^{d-2} + \ldots + a_0) = a_{d-1}\alpha_i^{d-1} + a_{d-2}\alpha_i^{d-2} + \ldots + a_0$, чиме је задато пресликавање σ_i на целом домену $\mathbb{Q}(\alpha)$, и очигледно су сва прелсикавања различита. Директном провером се показује да су ово и хомоморфизми поља.

Посматрајму сада произвољан хомоморфизам $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$. Нека је $\sigma(\alpha) = \theta$. Тада је

$$\begin{aligned} f(\theta) &= \theta^d + a_{d-1}\theta^{d-1} + a_{d-2}x^{d-2} + \ldots + a_0 = \sigma(\alpha)^d + a_{d-1}\sigma(\alpha)^{d-1} + a_{d-2}x^{d-2} + \ldots + a_0 \\ &= \sigma(\alpha^d) + a_{d-1}\sigma(\alpha^{d-1}) + a_{d-2}x^{d-2} + \ldots + a_0 = \sigma(\alpha^d + a_{d-1}\alpha^{d-1} + a_{d-2}\alpha^{d-2} + \ldots + a_0) \\ &= \sigma(0) = 0. \end{aligned}$$

па је θ нула полинома f и због тога је $\sigma(\alpha) = \alpha_i$ за неко i. Уз то, сваки ненула хомоморфизам поља чува јединице, па због тога је и $\sigma(1) = 1$, те је $\sigma = \sigma_i$. □

Сада можемо дефинисати норму.

***Дефиниција* 2.** *Нека је $f(x) \in \mathbb{Z}[X]$ моничан, иредуцибилан полином степена d и α нека његова нула, и нека су $\sigma_1, \sigma_2, \ldots, \sigma_d$ хомоморфизми из теореме 9. Тада норму елемента $\theta \in \mathbb{Q}(\alpha)$, дефинишемо изразом:*

$$N(\theta) = \sigma_1(\theta)\sigma_2(\theta) \cdots \sigma_d(\theta)$$

Норма елемената је и сама хомоморфизам као производ таквих. Поред тога, изузетно је значајна и следећа особина норме:

***Теорема* 10.** *Нека је $f(x) \in \mathbb{Z}[X]$ моничан, иредуцибилан полином степена d и α нека његова нула. Тада норма слика елементе $\mathbb{Q}(\alpha)$ у $\mathbb{Q}$ као и елементе $\mathcal{O}_{\mathbb{Q}(\alpha)}$ у $\mathbb{Z}$. Самим тим, $N(\mathbb{Z}[\alpha]) \subseteq \mathbb{Z}$.*

Појам норме можемемо увести и на идеалима:

***Дефиниција* 3.** *Нека је дат прстен R и у њему идеал I. Тада се норма идеала дефинише као $N(I) = [R : I]$.*

Појам норме на идеалима и елементима прстена се донекле слажу, о чему и говори следећа теорема.

***Теорема* 11.** *Нека је $f(x) \in \mathbb{Z}[X]$ моничан, иредуцибилан полином степена d и нека је α нека његова нула. Тада је норма идеала у Дедекиндовом домену $\mathcal{O}_{\mathbb{Q}(\alpha)}$ коначан број. Уз то, за произвољно $\theta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ важи $|N(\theta)| = N(\langle\theta\rangle)$.*

Пошто у Дедекиндовим доменима важи јединственост факторизације идеала, за произвољни идеал $\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{Q}(\alpha)}$ важи факторизација

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_k^{e_k}$$

па узимајући за $\mathfrak{a} = \langle\theta\rangle$, видимо да важи и

$$\begin{aligned}|N(\theta)| = N(\langle\theta\rangle) = N(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_k^{e_k}) = N(\mathfrak{p}_1^{e_1})N(\mathfrak{p}_2^{e_2})\cdots N(\mathfrak{p}_k^{e_k}) \\ = N(\mathfrak{p}_1)^{e_1}N(\mathfrak{p}_2)^{e_2}\cdots N(\mathfrak{p}_k)^{e_k}\end{aligned}$$

За пресликавања e_i којим смо дефинисали коефицијенте на Дедекиндовом домену ће важити следећа теорема која нам и омогућава конструкцију решета на Дедекиндовом домену:

***Теорема* 12.** *За сваки прост идеал $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{Q}(\alpha)}$ постоји хомоморфизам $e_\mathfrak{p} : \mathcal{O}_{\mathbb{Q}(\alpha)} \to \mathbb{Z}$ са следећим својствима:*

- $e_\mathfrak{p}(\theta) \geq 0$
- $e_\mathfrak{p}(\theta) > 0 \iff \mathfrak{p}|\langle\theta\rangle$[1]
- *За свако $\theta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ постоји коначно много простих идеала идеала $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_k$ таквих да је $e_{\mathfrak{p}_i}(\theta) > 0$ и уз ознаке $e_i = e_{\mathfrak{p}_i}(\theta)$ важи $N(\langle\theta\rangle) = N(\mathfrak{p}_1)^{e_1}N(\mathfrak{p}_2)^{e_2}\cdots N(\mathfrak{p}_k)^{e_k}$*

Трећа тачка теореме је нарочито занимљива јер се из ње може наслутити веза између коефицијената у факторизацији и норме. Наша је жеља да уместо $\mathcal{O}_{\mathbb{Q}(\alpha)}$ радимо са $\mathbb{Z}[\alpha]$ на којој идеали имају згоднију репрезентацију. Преласком на $\mathbb{Z}[\alpha]$ губимо могућност факторизације идеала, али нам се појам норме очувава. Интересантно је да теорема аналогна теореми 12 важи и у $\mathbb{Z}[\alpha]$, иако је доказ ових теорема фундаментално другачији:

***Теорема* 13.** *За сваки прост идеал $\mathfrak{p} \subseteq \mathbb{Z}[\alpha]$ постоји хомоморфизам $e_\mathfrak{p} : \mathbb{Z}[\alpha] \to \mathbb{Z}$ са следећим својствима:*

- $e_\mathfrak{p}(\theta) \geq 0$
- $e_\mathfrak{p}(\theta) > 0 \iff \mathfrak{p}|\langle\theta\rangle$
- *За свако $\theta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ постоји коначно много простих идеала идеала $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_k$ таквих да је $e_{\mathfrak{p}_i}(\theta) > 0$ и уз ознаке $e_i = e_{\mathfrak{p}_i}(\theta)$ важи $N(\langle\theta\rangle) = N(\mathfrak{p}_1)^{e_1}N(\mathfrak{p}_2)^{e_2}\cdots N(\mathfrak{p}_k)^{e_k}$*

За наш алгоритам је неопходно да знамо вредности $e_\mathfrak{p}$ само за $\theta = a + b\alpha$. Видећемо да је због овога вредности $e_\mathfrak{p}(a + b\alpha)$ лако израчунавати. У том циљу ћемо прво истражити какви све идеали могу да деле $\langle a + b\alpha\rangle$.

***Дефиниција* 4.** *Идеал $\mathfrak{a}$ називамо првостепеним ако и само ако је $N(\mathfrak{a}) = p$, при чему је p прост број.*

Важи следећа теорема:

***Теорема* 14.** *Сваки првостепени идеал I у прстену R је прост.*

[1] *Еквивалентно $\langle\theta\rangle \subseteq \mathfrak{p}$*

Доказ. Обзиром да је $|R/I| = [R : I] = p$, то је прстен R/I карактеристике p, те мора бити $R/I \cong \mathbb{F}_p$. Зато је R/I поље, те је I максималан идеал у R а самим тим је и прост. □

Посматрајмо неки идеал $\mathfrak{a} \subseteq \mathbb{Z}[\alpha]$ и неко $a \in \mathfrak{a}$. Тада је $\langle a \rangle \subseteq \mathfrak{a}$, па је и $|\mathbb{Z}[\alpha] : \langle a \rangle| > |\mathbb{Z}[\alpha] : \mathfrak{a}|$, тј. $N(\langle a \rangle) > N(\mathfrak{a})$. Имамо да је $N(\langle a \rangle) = |N(a)| < \infty$, па је зато $N(\mathfrak{a}) < +\infty$, те је норма $N(\mathfrak{a})$ добро дефинисана за све идеале прстена $\mathbb{Z}[\alpha]$. Следећа теорема значајно сужава класу простих идеала са којима радимо:

***Теорема* 15.** *Ако прост идеал $\mathfrak{p} \subseteq \mathbb{Z}[\alpha]$ дели $\langle a + b\alpha \rangle$, онда је $N(\mathfrak{p}) = p$, при чему је p прост број.*

Доказ. $\mathbb{Z}[\alpha]/\mathfrak{p}$ је коначан домен, па он има коначну карактеристику p. Поред тога, по малој Ведербурновој[1] теореми $\mathbb{Z}[\alpha]/\mathfrak{p}$ је поље, па по теореми 1 важи $\mathbb{Z}[\alpha]/\mathfrak{p} \cong \mathbb{F}_{p^e}$, за неко $e \in \mathbb{N}$. Посматрајмо канонски епиморфизам $\pi_\mathfrak{p} : \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/\mathfrak{p}$. Докажимо да је $Im(\pi_\mathfrak{p}) \cong \mathbb{Z}/p\mathbb{Z}$. Пошто је $\pi_\mathfrak{p}$ хомоморфизам прстена, биће $\pi_\mathfrak{p}(1) = 1$. Обзиром да је p карактеристика поља $\mathbb{Z}/\mathfrak{p}$, то ће за $m \in \mathbb{Z}$ бити $\pi_\mathfrak{p}(m) \equiv m \pmod p$, па имамо да је $\mathbb{Z}/p\mathbb{Z} \cong \pi_\mathfrak{p}(\mathbb{Z}) \subseteq Im(\pi_\mathfrak{p})$. Треба доказати и да је $Im(\pi_\mathfrak{p}) \subseteq \mathbb{Z}/p\mathbb{Z}$

Претпоставимо да $p|b$. Пошто је $\langle a + b\alpha \rangle \subseteq \mathfrak{p}$, имамо да је $a + b\alpha \in \mathfrak{p}$, и зато је $\pi_\mathfrak{p}(a + b\alpha) = 0$. Са друге стране је $\pi_\mathfrak{p}(a + b\alpha) = a + b\pi_\mathfrak{p}(\alpha)$, па је $\pi_\mathfrak{p}(a) = 0$, што значи и да је $a \equiv 0 \pmod p$, те $p|a$, што је контрадикција са $(a, b) = 1$. Дакле, $p \nmid b$, па можемо наћи инверз од b у $\mathbb{Z}/p\mathbb{Z}$, тј. у $\mathbb{Z}/\mathfrak{p}$. Зато из $\pi_\mathfrak{p}(a+b\alpha) \equiv a+b\pi_\mathfrak{p}(\alpha) \pmod \mathfrak{p}$ важи $\pi_\mathfrak{p}(\alpha) \equiv -b^{-1}a \pmod \mathfrak{p}$, па и $\pi_\mathfrak{p}(\alpha) \in \mathbb{Z}/p\mathbb{Z}$, и зато је и $Im(\pi_\mathfrak{p}) \subseteq \mathbb{Z}/p\mathbb{Z}$.

Из прве теореме о изоморфизмима имамо да је $\mathbb{Z}[\alpha]/ker\pi \cong Im(\pi)$, тј. $\mathbb{Z}[\alpha]/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$, одакле је $N(\mathfrak{p}) = p$, чиме је доказ завршен. □

Дакле, у алгебарску базу има смисла само убацивати првостепене идеале. Следећа теорема нам даје погодан начин за њихову репрезентацију:

***Теорема* 16.** *Скуп S свих првостепених идеала прстена $\mathbb{Z}[\alpha]$ генерисаног кореном α моничног иредуцибилног полинома $f \in \mathbb{Z}[X]$ је у бијективној коресподенцији са скупом $S' = \{(r, p) \mid p$ је прост, $r \in \mathbb{Z}/p\mathbb{Z}$ и $f(r) \equiv 0 \pmod p\}$.*

Доказ. Нека је $\mathfrak{p}$ произвољни првостепени идеал. Дефинишимо са $p = N(\mathfrak{p})$ и $r = \pi_\mathfrak{p}(\alpha)$, где је $\pi_\mathfrak{p}$ природни хомоморфизам $\pi_\mathfrak{p} : \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/\mathfrak{p}$. Пошто је $\mathfrak{p}$ првостепени идеал биће $\mathbb{Z}[\alpha]/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$, па је и $r \in \mathbb{Z}/p\mathbb{Z}$. Такође важи и

$$\begin{aligned} 0 = \pi_\mathfrak{p}(f(\alpha)) = \pi_\mathfrak{p}(\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = \pi_\mathfrak{p}(\alpha)^d + a_{d-1}\pi_\mathfrak{p}(\alpha)^{d-1} + \ldots + a_0 \\ \equiv r^d + a_{d-1}r^{d-1} + \ldots + a_0 = f(r) \pmod p \end{aligned}$$

чиме смо конструисали пресликавање $\phi : S \to S'$. Конструишимо сада и хомоморфизам $\psi : S' \to S$. Нека $(r, p) \in S'$. Постоји природан хомоморфизам $\pi_p : \mathbb{Z}[\alpha] \to \mathbb{Z}/p\mathbb{Z}$ генерисан са $\pi_\mathfrak{p}(1) = 1$ и $\pi_\mathfrak{p}(\alpha) = r$ (коректно је дефинисан јер је $f(r) \equiv 0 \pmod p$). Ово је епиморфизам, па је $\mathbb{Z}[\alpha]/ker(\pi_p) \cong Im(\pi_p) = \mathbb{Z}/p\mathbb{Z}$. Означимо са $\mathfrak{p} = ker(\pi_p)$. Тада је $\mathfrak{p}$ првостепени идеал. Овиме је дата конструкција пресликавања ψ.

Из конструкција се види да је $\psi \circ \phi = \phi \circ \psi = id$, па су ψ и ϕ бијекције, које дају бијективну коресподенцију између скупова S и S'. □

Од сада ћемо увек када радимо са првостепеним идеалима поистовећивати скуп $\mathbb{Z}[\alpha]/\mathfrak{p}$ са $\mathbb{Z}/p\mathbb{Z}$. Докажимо теорему која ће нам омогућити рачунање конкретних вредности $e_\mathfrak{p}$.

[1] *Joseph Henry Maclagan Wedderburn (1882-1948) - шкотски математичар*

***Теорема* 17.** *Нека је* $\mathfrak{p}$ *првостепени идеал коме одговара пар* (r, p)*, и нека је дато* $a + b\alpha$ *(* a *и* b *су међусобно прости). Тада је*

$$e_{\mathfrak{p}}(a+b\alpha) = \begin{cases} ord_p(N(a+b\alpha)) & \text{ако } a+br \equiv 0 \pmod p \\ 0 & \text{иначе} \end{cases}$$

при чему је $ord_p(x)$ *степен* p *у факторизацији броја* x*.*

Доказ. $e_{\mathfrak{p}}(a+b\alpha) > 0$ *ако и само ако* $\mathfrak{p}|\langle a+b\alpha\rangle$*. Посматрајмо канонски епиморфизам* $\pi_{\mathfrak{p}} : \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/\mathfrak{p}$*. Пошто* $\langle a+b\alpha\rangle \subseteq \mathfrak{p}$ *имамо да је* $\pi_{\mathfrak{p}}(a+b\alpha) = 0$*, тј.* $a + b\pi_{\mathfrak{p}}(\alpha) \equiv 0 \pmod p$*. Пошто смо дефинисали са* $r = \pi_{\mathfrak{p}}(\alpha)$*, имаћемо да је управо* $a + br \equiv 0 \pmod p$*. Из треће особине хомоморфизма* $e_{\mathfrak{p}}$ *имамо да је* $N(\langle\theta\rangle) = N(\mathfrak{p}_1)^{e_1}N(\mathfrak{p}_2)^{e_2}\cdots N(\mathfrak{p}_k)^{e_k}$*. Пошто је* $\mathfrak{p}$ *једини међу идеалима норме* p *који ће имати ненула степен у овој факторизацији (јер је једино* r *дато формулом* $r = -ab^{-1} \pmod p$*), важи* $e_{\mathfrak{p}}(a+b\alpha) = ord_p(N(a+b\alpha))$*.* □

Факторизацијом норме елемента $a + b\alpha$, можемо наћи све идеале који деле $\langle a + b\alpha\rangle$. Уколико су сви ови идеали у алгебарској бази, тада $a + b\alpha$ сматрамо глатким. Ишчитавањем степена у факторизацији норме можемо наћи и коефицијенте за сваки од фактора у бази. Остаје још показати како се може израчунати норма. Имамо да је:

$$N(a+b\alpha) = \sigma_1(a+b\alpha)\sigma_2(a+b\alpha)\ldots\sigma_d(a+b\alpha) = (a+b\alpha_1)(a+b\alpha_2)\ldots(a+b\alpha_d) =$$
$$b^d(\frac{a}{b}+\alpha_1)(\frac{a}{b}+\alpha_2)\ldots(\frac{a}{b}+\alpha_d) = (-1)^d b^d(-\frac{a}{b}-\alpha_1)(-\frac{a}{b}-\alpha_2)\ldots(-\frac{a}{b}-\alpha_d) = (-b)^d f(-\frac{a}{b}) =$$
$$a^d - a_{d-1}a^{d-1}b + a_{d-2}a^{d-2}b^2 - a_{d-3}a^{d-3}b^3 + \ldots + (-1)^d a_0 b^d$$

3.3.3 Квадратно решето

Задатак алгебарског решета је да пронађе елементе $a_i + b_i\alpha$ такве да је $\prod_{i=1}^{m}\langle a_i + b_i\alpha\rangle = \mathfrak{a}^2$. То ће заиста и бити остварено у случају да радимо у Дедекиндовом домену. Уколико радимо у $\mathbb{Z}[\alpha]$, немамо никакве гаранције да ће ово важити. Ипак, ово није једини проблем на нашем путу. У случају да смо успели да нађемо идеал $\mathfrak{a}$, ми се надамо да ће бити главноидеалски, облика $\theta\mathbb{Z}[\alpha]$. Одатле имамо да је $\prod_{i=1}^{m}(a_i+b_i\alpha)\mathbb{Z}[\alpha] = \theta^2\mathbb{Z}[\alpha]$. Али и када је ово остварено, не мора бити $\theta^2 = \prod_{i=1}^{m}(a_i+b_i\alpha)$. Алгебарско решето ће нам давати кандидате за квадратне бројеве. Квадратно решето можемо видети као својеврстан тест за извучене кандидате.

Прво ћемо посматрати проблем у $\mathbb{Z}$, након чега развијене идеје преносимо у $\mathbb{Z}[\alpha]$. Један од најелегантнијих метода испитивања квадратности неких бројева је метод Лагранжевог остатка. Лагранжев метод се бави провером квадратности елемената у $\mathbb{Z}/p\mathbb{Z}$. Еквивалентно томе је решавати једначину

$$x^2 \equiv a \pmod p$$

Ове једначине зовемо квадратне конгруенције. Посматрајмо на пример квадратне конгруенције

$$x^2 \equiv 3 \pmod 7$$
$$x^2 \equiv 2 \pmod 7$$

Директном провером можемо видети да прва од једначина нема ниједно решење, док друга има два решења, и то $x \equiv 3 \pmod 7$ и $x \equiv 4 \pmod 7$. Ово ће бити и једини могући исходи решавања једначине. Уколико једначина има макар једно решење,

нека то буде x_1 тада ће и $x_2 = -x_1$ бити решење. Пошто је $\mathbb{Z}/p\mathbb{Z}$ поље, из алгебре је познато да је онда $\mathbb{Z}/p\mathbb{Z}[X]$ домен са јединственом факторизацијом. Зато је једина факторизација $x^2 - a$ управо $(x - x_1)(x - x_2)$, па закључујемо да су то једина решења.

***Дефиниција* 5.** *Нека је p непаран прост број и нека $p \nmid a$. Ако конгруенција $x^2 \equiv a \pmod{p}$ има решења, онда a зовемо квадратни остатак модуло p и то означавамо са*

$$\left(\frac{a}{p}\right) = 1$$

Уколико дата конгруенција нема решења у $\mathbb{Z}/p\mathbb{Z}$, a називамо квадратни неостатак модуло p и то означавамо са

$$\left(\frac{a}{p}\right) = -1$$

Додатно, у случају да $p|a$, дефинишемо:

$$\left(\frac{a}{p}\right) = 0$$

Овако дефинисан симбол $\left(\frac{a}{p}\right)$ дефинише пресликавање из $\mathbb{Z}$ у $\{-1, 0, 1\}$ које називамо Лежандров симбол.

У следећој теореми су енкапсулиране све неопходне особине Лежандровог симбола:

***Теорема* 18.** *Нека је p прост број и нека $a, b \in \mathbb{Z}$. Тада важи:*

1. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$
2. $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$
3. *ако је* $a \equiv b \pmod{p}$ *онда је* $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \pmod{p}$.

Доказ. Докажимо прво тачку 1. У случају да $p|a$ исказ је очигледно тачан, па можемо претпоставити да $a \not\equiv 0 \pmod{p}$. Уколико је a квадратни остатак, имаћемо да је $a \equiv x^2 \pmod{p}$ за неко x, па је зато $x^{p-1} \equiv 1 \pmod{p}$ по малој Фермаовој теореми, и зато је

$$\left(\frac{a}{p}\right) \equiv 1 \equiv x^{p-1} \equiv (x^2)^{(p-1)/2} \equiv a^{(p-1)/2}$$

Остаје да се обради случај када је a неквадратни остатак. Опет по малој Фермаовој теореми имамо $a^{p-1} \equiv 1 \pmod{p}$, па пошто је p непаран можемо записати претходну једначину и као

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}$$

тј. као

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

Група $(\mathbb{Z}/p\mathbb{Z})^*$ је циклична, па постоји елемент g такав да је $\langle g \rangle = (\mathbb{Z}/p\mathbb{Z})^*$. Тада постоји неко $1 \leq \nu \leq p - 1$, тако да је $a \equiv g^\nu \pmod{p}$, па је

$$g^{\nu(p-1)/2} \equiv \pm 1 \pmod{p}$$

У случају да је $g^{\nu(p-1)/2} \equiv 1 \pmod{p}$, пошто је g генератор групе реда $p-1$ важи $p-1|\nu(p-1)/2$, па је ν паран, тј. облика $\nu = 2\nu'$. Али тада је и $a \equiv (g^{\nu'})^2 \pmod{p}$, па је a квадратни остатак, што је контрадикција. Зато мора бити $g^{\nu(p-1)/2} \equiv -1 \pmod{p}$, тј. $a^{(p-1)/2} \equiv -1 \pmod{p}$, чиме је доказ тачке 1 завршен. Тачке 2 и 3 су директна последице тачке 1. □

Уколико је x квадратан у $\mathbb{Z}$, тј. постоји y , тако да је $y^2 = x$, онда ће x бити квадратан и у сваком пољу $\mathbb{Z}/p\mathbb{Z}$ за непарно p, јер ће важити $y^2 \equiv x \pmod{p}$. Из претходне теореме видимо да је испитивање квадратности у пољу $\mathbb{Z}/p\mathbb{Z}$ веома ефикасно, јер је довољно рачунати степен, што можемо радити у логаритамској сложености. Зато је наша идеја да, уместо да тестирамо да ли је неко x квадратно у $\mathbb{Z}$, то тестирамо у $\mathbb{Z}/p\mathbb{Z}$ за неколико простих p-ова. Уколико неки од ових тестова падне, онда x неће бити квадратан у $\mathbb{Z}$. Ипак, уколико покушамо тест за доста простих бројева, биће веома вероватно да је x квадратан.

Пребацимо се сада у прстен $\mathbb{Z}[\alpha]$. Идеја у овом случају је да уместо провере да ли је неки број квадратан у $\mathbb{Z}[\alpha]$, то проверавамо у $\mathbb{Z}[\alpha]/\mathfrak{p}$. Пошто имамо згодну репрезентацију првостепених идеала овде ћемо користити искључиво њих. Следећа теорема је еквивалент провере квадратности у $\mathbb{Z}$ преласком у $\mathbb{Z}/p\mathbb{Z}$, само што сада прелазимо са $\mathbb{Z}[\alpha]$ у $\mathbb{Z}[\alpha]/\mathfrak{p}$.

***Теорема* 19.** *Нека је $\theta \in \mathbb{Z}[\alpha]$ квадратан у $\mathbb{Z}[\alpha]$, тј. нека постоји неко $\gamma \in \mathbb{Z}[\alpha]$ за које је $\gamma^2 = \theta$. Нека је $\mathfrak{p}$ првостепени идеал одређен паром (r,p) такав да $\theta \notin \mathfrak{p}$. Уколико је $\pi_\mathfrak{p} : \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/\mathfrak{p}$ природни епиморфизам, биће*

$$\left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = 1$$

Доказ. Кад би $\gamma \in \mathfrak{p}$ онда би и $\gamma^2 \in \mathfrak{p}$, тј. $\theta \in \mathfrak{p}$, што је контрадикција. Зато је $\gamma \notin \mathfrak{p}$. За канонски епиморфизам $\pi_\mathfrak{p}$ важи да је $ker(\pi_\mathfrak{p}) = \mathfrak{p}$ па је $\left(\frac{\pi_\mathfrak{p}(\gamma)}{p}\right) \neq 0$. Зато имамо да је

$$\left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = \left(\frac{\pi_\mathfrak{p}(\gamma^2)}{p}\right) = \left(\frac{\pi_\mathfrak{p}(\gamma)^2}{p}\right) = \left(\frac{\pi_\mathfrak{p}(\gamma)}{p}\right)^2 = 1$$

□

Дакле, ако за неко $\mathfrak{p}$ детектујемо да је $\left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = -1$ онда са сигурношћу можемо тврдити да θ није квадратан у $\mathbb{Z}[\alpha]$. Али у случају да је $\left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = 1$ не можемо тврдити да је θ квадратан у $\mathbb{Z}[\alpha]$. Ипак, овај тест можемо да применимо узимајући за основу разне првостепене идеале $\mathfrak{p}$. Што више идеала испробамо то ћемо бити сигурнији да ће тест боље детектовати квадратне бројеве. Да ли је ово довољно? У [2], у првом делу осме главе је дата хеуристичка анализа која показује да уколико радимо са доста првостепених идеала $\mathfrak{p}$ овај тест детектује квадрате са великом сигурношћу. У [11] је изложена анализа у којој је изнета претпоставка да ће тест са 50-100 идеала бити довољан у готово свим случајевима. Све ове претпоставке важе под условом да је $\langle\theta\rangle$ делив само са коначно много идеала. Приметимо да ће такви бити управо θ који су глатки у алгебарском решету. Комбинација сва три решета ће радити са (a,b) тако да је $(a+b\alpha)$ глатко и у алгебарској и у квадратној бази, те ће овај услов бити испуњен.

Вратимо се сада конструкцији решета. Ми желимо да нађемо $\prod_{i=1}^{m}(a_i + b_i\alpha)$ који је квадратан у $\mathbb{Z}[\alpha]$. Из следеће теореме можемо наслутити како се то може учинити:

***Теорема* 20.** *Нека је дато m узајамно простих парова (a_i, b_i) таквих да је*

$$\prod_{i=1}^{m}(a_i + b_i\alpha) = \gamma^2$$

за неко $\gamma \in \mathbb{Z}(\alpha)$*. Нека је првостепени идеал* $\mathfrak{p}$ *одређен паром* (r,p)*, и нека* $\mathfrak{p}$ *не дели ниједно* $\langle a_i + b_i\alpha\rangle$*. Тада је*

$$\prod_{i=1}^{m}\left(\frac{a_i+b_ir}{p}\right)=1$$

Доказ. Посматрајмо природни епиморфизам $\pi_{\mathfrak{p}}$*. Сваки од* $(a_i+b_i\alpha)$ *не припадају* $\mathfrak{p}$*, па је зато* $\pi_{\mathfrak{p}}(a_i+b_i\alpha)\neq 0$*. Обзиром да је* $\mathbb{Z}/\mathfrak{p}$ *поље, биће и*

$$0\neq\prod_{i=1}^{m}\pi_{\mathfrak{p}}(a_i+b_i\alpha)=\pi_{\mathfrak{p}}\left(\prod_{i=1}^{m}(a_i+b_i\alpha)\right)=\pi_{\mathfrak{p}}(\gamma^2)=\pi_{\mathfrak{p}}(\gamma)^2$$

па је $\pi_{\mathfrak{p}}(\gamma)\neq 0$*, па зато не може ни* $\gamma\in\mathfrak{p}$*. Одатле* $\left(\frac{\pi_{\mathfrak{p}}(\gamma)}{p}\right)=\pm 1$*, па можемо рачунати*

$$1 \;=\; \left(\frac{\pi_{\mathfrak{p}}(\gamma)}{p}\right)^2 \;=\; \left(\frac{\pi_{\mathfrak{p}}(\gamma^2)}{p}\right) \;=\; \left(\frac{\pi_{\mathfrak{p}}\left(\prod_{i=1}^{m}(a_i+b_i\alpha)\right)}{p}\right) \;=\; \prod_{i=1}^{m}\left(\frac{\pi_{\mathfrak{p}}(a_i+b_i\alpha)}{p}\right)$$

Обзиром да смо дефинисали r *као* $r=\pi_{\mathfrak{p}}(\alpha)$ *имамо и да је* $1=\prod_{i=1}^{m}\left(\frac{\pi_{\mathfrak{p}}(a_i+b_ir)}{p}\right)=\prod_{i=1}^{m}\left(\frac{a_i+b_ir}{p}\right)$ *што је и требало доказати.* □

У алгебарској бази ћемо имати k идеала, $\mathfrak{p}_1,\mathfrak{p}_2,\ldots,\mathfrak{p}_k$. Тест тражи $(a_j+b_j\alpha)$, тако да ниједан од $\mathfrak{p}_i$ не дели $(a_j+b_j\alpha)$, и за које је :

$$\prod_{i=1}^{m}\left(\frac{a_i+b_ir_1}{p_1}\right)=1$$

$$\prod_{i=1}^{m}\left(\frac{a_i+b_ir_2}{p_2}\right)=1$$

$$\vdots$$

$$\prod_{i=1}^{m}\left(\frac{a_i+b_ir_k}{p_k}\right)=1$$

при чему су (r_j,p_j) парови који репрезентују идеал $\mathfrak{p}_j$. Мултипликативна група $\{-1,1\}$ је изоморфна адитивној $\{0,1\}$ кроз изоморфизам $\eta:\{-1,1\}\to\{0,1\}$ дат са

$$\eta(x)=\begin{cases}0 & x=1\\ 1 & x=-1\end{cases}$$

Уколико дефинишемо хомоморфизме $\chi_{\mathfrak{p}_j}(\theta)=\eta\circ\left(\frac{\pi_{\mathfrak{p}_j}(\theta)}{p}\right)$, имаћемо да је систем еквивалентан горњем дат са

$$\sum_{i=1}^{m}\chi_{\mathfrak{p}_1}(a_i+b_ir_1)=0 \pmod 2$$

$$\sum_{i=1}^{m}\chi_{\mathfrak{p}_2}(a_i+b_ir_2)=0 \pmod 2$$

$$\vdots$$

$$\sum_{i=1}^{m} \chi_{\mathfrak{p}_k}(a_i + b_i r_k) = 0 \pmod 2$$

па слично као и код рационалног и алгебарског решета можемо наћи одговарајуће $(a_i + b_i\alpha)$.

Квадратно решето које смо конструисали ће готово увек прихватати и оне $\theta \in \mathbb{Z}[\alpha]$ који имају корен у $\mathbb{Q}[\alpha]$. То видимо из следеће теореме:

***Теорема* 21.** *Нека је $\theta \in \mathbb{Z}[\alpha]$ квадратан у $\mathbb{Q}(\alpha)$, тј. нека постоји неко $\gamma \in \mathbb{Q}(\alpha)$ за које је $\gamma^2 = \theta$. Нека је $\mathfrak{p}$ првостепени идеал одређен паром (r, p) такав да $f'(r) \not\equiv 0 \pmod p$ и $\theta \notin \mathfrak{p}$. Уколико је $\pi_\mathfrak{p} : \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/\mathfrak{p}$ природни епиморфизам, биће*

$$\left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = 1$$

Доказ. $\theta \in \mathbb{Z}[\alpha]$, па је он интегралан над $\mathbb{Z}$, тј. анулира неки полином $g(X) \in \mathbb{Z}[X]$. Али онда је и γ интегралан у $\mathbb{Z}$, јер ће анулирати полином $g(X^2)$, па $\gamma \in \mathcal{O}_{\mathbb{Q}(\alpha)}$. Из теорије бројева нам је познато ће за такво γ бити $f'(\alpha)\gamma \in \mathbb{Z}[\alpha]$, па је онда и $\pi_\mathfrak{p}(f'(\alpha)\gamma)$ добро дефинисано. Даље можемо рачунати

$$\begin{aligned}\left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) &= 1 \cdot \left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = \left(\frac{f'(r)}{p}\right)^2 \cdot \left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = \left(\frac{f'(r)^2}{p}\right) \cdot \left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) \\ &= \left(\frac{f'(\pi_\mathfrak{p}(\alpha))^2}{p}\right) \cdot \left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = \left(\frac{\pi_\mathfrak{p}(f'(\alpha))^2}{p}\right) \cdot \left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = \left(\frac{\pi_\mathfrak{p}(f'(\alpha)^2) \cdot \pi_\mathfrak{p}(\theta)}{p}\right) \\ &= \left(\frac{\pi_\mathfrak{p}(f'(\alpha)^2 \cdot \gamma^2)}{p}\right) = \left(\frac{\pi_\mathfrak{p}(f'(\alpha)\gamma)}{p}\right)^2\end{aligned}$$

па је $\left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right)$ или 0 или 1. Пошто $\theta \notin \mathfrak{p}$, то је и $\pi_\mathfrak{p}(\theta) \neq 0$, па је и $\left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) \neq 0$. Закључујемо да је:

$$\left(\frac{\pi_\mathfrak{p}(\theta)}{p}\right) = 1$$

□

Дакле, у случају да за сваки од идеала квадратне базе који је репрезентован паром (r, p) важи $f'(r) \not\equiv 0 \pmod p$, квадратно решето ће подједнако видети квадратност у $\mathbb{Z}[\alpha]$ и у $\mathbb{Q}(\alpha)$. Елементи у $\mathbb{Q}(\alpha)$ нам нису употребљиви јер немамо хомоморфизам $\varphi : \mathbb{Q}(\alpha) \to \mathbb{Z}/n\mathbb{Z}$. Ипак, уколико је $\gamma^2 = \theta$ за $\gamma \in \mathbb{Q}(\alpha)$ и $\theta \in \mathbb{Z}[\alpha]$, и уколико $f'(m) \not\equiv 0 \pmod n$, онда је $\gamma f'(\alpha) \in \mathbb{Z}[\alpha]$, и за њега је дефинисано φ. У поглављу 4.2 ћемо видети да је ово довољно да формирамо разлику квадрата. Зато ћемо у квадратно решето стављати само оне идеале $\mathfrak{p}$ за које је $f'(r) \not\equiv 0 \pmod p$, па ћемо на тај начин дозволити и корене у $\mathbb{Q}(\alpha)$.

3.3.4 Спајање свих решета

У претходним поглављима смо дефинисали три различите базе и на свакој од база елементу $(a + bm, a + b\alpha)$ придружили коефицијенте. Да би могли да их разликујемо, специјално у овом поглављу ћемо сматрати да рационалну базу чине прости бројеви $p_1, p_2, \ldots, p_{k_1}$, алгебарску првостепени идеали $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_{k_2}$, и квадратну базу првостепени идеали $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_{k_3}$.

За алгоритам су нам неопходни узајамно прости парови (a_i, b_i) који су глатки у сваком од решета ($a_i + b_i m$ глатки у рационалном, а $a_i + b_i\alpha$ у алгебарском и квадратном). Ове бројеве генеришемо тако по буду глатки у рационалној бази, по алгоритму које

смо описали у 3.3.1, па међу њима бирамо оне елементе који су глатки и у алгебарској и квадратној бази. Од тих m глатких парова (a_i, b_i) тражимо неки подскуп чији ће производ у $\mathbb{Z} \times \mathbb{Z}[\alpha]$ дати квадратни елемент. Зато сваком (a_i, b_i) придружујемо c_i, тако да $c_i = 1$ означава да број треба бити у производу, а $c_i = 0$ да не треба. Пар формално означавамо са $(a_i, b_i)^{c_i}$, што значи да је он у $\mathbb{Z} \times \mathbb{Z}[\alpha]$ заправо $((a_i + b_i m)^{c_i}, (a_i + b_i \alpha)^{c_i})$. Да би производ био квадратан број мора бити:

$$e_i \left(\prod_{j=1}^{m} (a_j + b_j m)^{c_j} \right) \equiv 0 \pmod 2 \quad \text{за} \quad 1 \leq i \leq k_1$$

$$e_{\mathfrak{p}_i} \left(\prod_{j=1}^{m} (a_j + b_j \alpha)^{c_j} \right) \equiv 0 \pmod 2 \quad \text{за} \quad 1 \leq i \leq k_2$$

$$\chi_{\mathfrak{q}_i} \left(\prod_{j=1}^{m} (a_j + b_j \alpha)^{c_j} \right) \equiv 0 \pmod 2 \quad \text{за} \quad 1 \leq i \leq k_3$$

Као и у алгоритму квадратног решета, и овде морамо пазити на знак. Зато дефинишемо хомоморфизам $e_0 : \mathbb{Z}^* \to 0, 1$ са

$$e_0(x) = \begin{cases} 0 & , x > 0 \\ 1 & , x < 0 \end{cases}$$

и као додатан услов захтевамо да је и

$$e_0 \left(\prod_{j=1}^{m} (a_j + b_j m)^{c_j} \right) \equiv 0 \pmod 2$$

Ако дефинишемо са $e_{ij} = e_i(a_j + b_j m), e'_{ij} = e_{\mathfrak{p}_1}(a_j + b_j \alpha)$, и са $e''_{ij} = \chi_{\mathfrak{q}_i}(a_j + b_j \alpha)$, имаћемо да су горњи услови еквивалентни систему линеарних једначина у $\mathbb{Z}/2\mathbb{Z}$:

$$\begin{gathered}
c_1 e_{01} + c_2 e_{02} + \ldots + c_m e_{0m} \equiv 0 \pmod 2 \\
c_1 e_{11} + c_2 e_{12} + \ldots + c_m e_{1m} \equiv 0 \pmod 2 \\
\vdots \\
c_1 e_{k_1 1} + c_2 e_{k_1 2} + \ldots + c_m e_{k_1 m} \equiv 0 \pmod 2 \\
c_1 e'_{11} + c_2 e'_{12} + \ldots + c_m e'_{1m} \equiv 0 \pmod 2 \\
c_1 e'_{21} + c_2 e'_{22} + \ldots + c_m e'_{2m} \equiv 0 \pmod 2 \\
\ldots \\
c_1 e''_{k_3 1} + c_2 e''_{k_3 2} + \ldots + c_m e''_{k_3 m} \equiv 0 \pmod 2
\end{gathered}$$

где коефицијенте c_i третирамо као непознате. Зато, ако нађемо више од $k_1 + k_2 + k_3 + 1$ глатких парова можемо наћи и неко нетривијално решење, на основу кога можемо формирати производ који је вероватно квадратан у $\mathbb{Z} \times \mathbb{Z}[\alpha]$. Коефицијенте c_i можемо тражити решавањем овог система линеарних једначина, рецимо методом Гаусове елиминације. Ипак, с обзиром да ће већина коефицијената e_{ij}, e'_{ij} и e''_{ij} бити једнака нули, и да је нама довољно било које нетривијално решење, логично је потражити неке ефикасније алгоритме који ће се окористити о ове релаксираније услове. Обично се користи или блок Ланцошев[1] алгоритам или блок Видманов[2] алгоритам. За блок Ланцошев алгоритам ваља погледати [31], док се као референца за блок Видманов алгоритам може користити [14, 15].

[1] Cornelius Lanczos(1893-1973), мађарски математичар и физичар јеврејског порекла

[2] D. Wiedemann

4 Расветљавање детаља

4.1 Конструкција првостепених идеала алгебарске и квадратне базе

У претходној глави смо се бавили применом првостепених идеала у тражењу квадратних бројева у $\mathbb{Z}[\alpha]$. У тој глави смо се задовољили практичном карактеризацијом ових идеала, коју смо касније користили да развијемо решета. Подсећања ради, сваки првостепени идеал се може такође видети и као уређени пар (r, p), при чему је p прост број и $r \in \mathbb{Z}/p\mathbb{Z}$ за који је $f(r) \equiv 0 \pmod{p}$.

Да би неки од $a+b\alpha$ био гладак у алгебарском ситу, њега морају делити само идеали из алгебарске базе и ниједни други. Са друге стране, да би био гладак у квадратној бази, $a + b\alpha$ не сме припадати ниједном идеалу из квадратне базе (тј. ниједан од тих идеала не сме да га дели). Зато су алгебарска и квадратна база дисјунктне. Устаљен је начин да се ове базе креирају тако што се одреде неке границе u_1 и u_2, $u_1 < u_2$, и онда се алгебарска база попуњава свим идеалима норме до u_1, док квадратна база садржи идеале који имају вредност норме између u_1 и u_2. Обично алгебарско решето садржи доста више идеала од квадратног. Границе се обично установљавају пре почетка извршавања алгоритма. Уколико у току извршавања приметимо да не добијамо очекивани напредак, можемо их прилагодити уз избегавање понављања већег дела рачуна. Уз те границе налазићемо просте p, за које ће нас интересовати да нађемо све могуће r за које је

$$f(r) \equiv 0 \pmod{p}$$

Видимо да је ово заправо еквивалентно тражењу свих решења алгебарске једначине у $\mathbb{Z}/p\mathbb{Z}$, тј. тражењу линеарних фактора полинома $f(x)$ у $\mathbb{Z}/p\mathbb{Z}[X]$. С обзиром да је то једначина у коначном пољу, скуп свих решења можемо наћи тако што једначину проверавамо за сваки елемент поља. Овај наиван приступ постаје непрактичан за веће p, па морамо пронаћи неко паметније решење. У тачки 4 теореме 1 видели смо да је производ свих могућих фактора $f(x)$ садржан у $x^p - x$, и то тачно једном , тј. да важи

$$x^p - x = x(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_{p-1})$$

Одавде видимо би први корак могао да буде рачунање највећег заједничког делиоца $g(x) = (f(x), x^p - x)$. Полином $g(x)$ ће имати исте линеарне факторе као и $f(x)$, али зато може бити мањег степена. Ово заправо можемо видети као уклањање вишеструкости у факторизацији $f(x)$. Обзиром на ефикасност Еуклидовог алгоритма, ову процедуру би требало увек примењивати.

У нашем методу ћемо покушати да овако изабрани $g(x)$ из корака у корак делимо на све ситније и ситније делове, све док не добијемо линеарне факторе. У ту сврху дефинишемо етапе или фазе. У почетној етапи имамо само полином $g(x)$, док полиноме у свакој од наредних фаза добијамо из полинома етапе која јој претходи. На почетку сваке етапе узимамо неко произвољно c тако да је $0 \leq c < p$. Ово c се може видети и као тачка раздвајања полинома. Да би фаза успешно изделила неки полином неопходно је да ово c буде другачије од оних који су бирани у претходним фазама. Покажимо како се врши разбијање неког полинома $h(x)$ у произвољној етапи. Обзиром да је $h(x)$ настало сукцесивним разбијањима почетног полинома $g(x)$, $h(x)$ неће имати вишеструке чиниоце, те зато $h(x)|x^p - x$. Али онда и $h(x + c)$ нема вишеструке чиниоце, те и $h(x + c)|x^p - x$. Дефинишимо полиноме:

$$h_1(x) = (h(x + c), x^{(p-1)/2} - 1)$$

$$h_2(x) = (h(x + c), x^{(p-1)/2} + 1)$$

$$h_3(x) = (h(x + c), x)$$

Из $x^p - x = x(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1)$ видимо да ће h_1, h_2, h_3 садржати садржати све факторе $h(x + c)$, као и ће сви фактори $h(x + c)$ бити расподељени на h_1, h_2 и h_3. Полином h_3 ће бити или x или 1. У сличају да је $h_3(x) = x$, важиће $x|h(x + c)$, тј. $(x - c)|h(x)$, па је c један од корена $h(x)$, а самим тим и $g(x)$. Уколико је неки $h_1(x)$ или $h_2(x)$ степена 1, и из њих можемо извући још један корен. Ако је рецимо $h_1(x) = x - x_1$, онда ће $h_1(x - c)|h(x)$, тј. $x_1 + c$ је корен $g(x)$. У случају да је $h_1(x)$ степена већег од 1, у следећу фазу преносимо полином $h_1(x - c)$. Преносимо управо $h_1(x - c)$, а не $h_1(x)$, јер је корен од $h_1(x - c)$ корен и од $g(x)$, док то не мора бити случај са $h_1(x)$. Аналогно поступамо и са $h_2(x)$. Наравно, уколико је било који од $h_1(x), h_2(x)$ степена 0, тј. једнак јединици, немамо потребе да их посматрамо у наредним фазама.

У свакој наредној фази ће фигурисати у најгорем случају исти број различитих фактора као у претходној. Након што испробамо сечења на свим местима сигурно смо испитали дељивост свим факторима, те се овај алгоритам мора завршити у коначно много корака. Ипак, ово готово никад неће бити случај, јер ће $g(x)$ имати много мање од p линеарних фактора, и наше дељење не мора да погоди баш корен да би пронашло неки линеаран фактор. Приметимо да овај приступ има предност у перформансама у односу на наиван алгоритам и због тога што ће се укупан број фактора бити смањиван како прелазимо из рунде у рунду, што ће олакшати рачунање, док смо на другој страни стално имали израчунавање на $g(x)$.

4.2 Конструкција $\sqrt{g}$ за квадратно $g \in \mathbb{Z} \times \mathbb{Z}[\alpha]$

Решето развијеног алгоритма даје $g \in \mathbb{Z} \times \mathbb{Z}[\alpha]$ које је веома вероватно квадратно. У овом поглављу ћемо се позабавити испитивањем те квадратности у $\mathbb{Z} \times \mathbb{Z}[\alpha]$ као и конструкцијом корена.

Означимо са (g_1, g_2) елемент g при чему су g_1 и g_2 његове пројекције на $\mathbb{Z}$ и $\mathbb{Z}[\alpha]$. У 3.3.3 видели смо да у случају да g јесте квадратно његов корен h може бити и из $\mathbb{Z} \times \mathbb{Q}(\alpha)$. Али на елементе из $\mathbb{Q}(\alpha)$ не можемо продужити дефинисан хомоморфизам $\psi : \mathbb{Z} \times \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, па корен у оваквом облику не можемо прихватити. Овај проблем се ипак може превазићи. Пошто је $h_2^2 = g_2$ и $g_2 \in \mathbb{Z}[\alpha]$ интегралан над $\mathbb{Z}$, то ће бити и h_2 интегралан над $\mathbb{Z}$. Али онда је из теорије бројева познато да је $f'(\alpha)h_2 \in \mathbb{Z}[\alpha]$ па је за њега дефинисан хомоморфизам φ. Тада, уз $x = \varphi(f'(\alpha)h_2)$ і $y = f'(m)h_1 \pmod n$ имамо да је

$$x^2 \equiv \varphi(f'(\alpha)h_2)^2 \equiv \varphi(f'(\alpha)^2 h_2^2) \equiv \varphi(f'(\alpha)^2)\varphi(g_2) \equiv \varphi(f'(\alpha))^2 g_1 \equiv$$
$$f'(\varphi(\alpha))^2 h_1^2 \equiv f'(m)^2 h_1^2 \equiv (f'(m)h_1)^2 \equiv y^2 \pmod n$$

што даје разлику квадрата. Потребно је показати и да $f'(m) \not\equiv 0 \pmod n$ да не би добили да је $x, y \equiv 0 \pmod n$. Али, због начина одабира полинома f, биће $1 < f'(m) < n$, па је заиста $f'(m) \not\equiv 0 \pmod n$.

За неко $h \in \mathbb{Z} \times \mathbb{Z}[\alpha]$ важи $h^2 = g \Leftrightarrow h_1^2 = g_1$ и $h_2^2 = g_2$. Дакле, проблем тражења корена у $\mathbb{Z} \times \mathbb{Z}[\alpha]$ можемо рашчланити на тражење корена у $\mathbb{Z}$ и $\mathbb{Z}[\alpha]$. Тражење корена у $\mathbb{Z}$ је исто као код алгоритма квадратног решета , па ћемо се овде концентрисати на $\mathbb{Z}[\alpha]$.

Ради лакшег писања означићемо са $x = h_2$ и $y = g_2$, тј. решаваћемо проблем $x^2 = y$ у $\mathbb{Z}[\alpha]$. Такође, претпоставићемо да смо за наш алгоритам узели f непарног степена. За факторизацију n увек можемо бирати овакво f. Ипак, некад је оптималније изабрати f парног степена. У том случају можемо користити алгоритам описан у [27].

Елемент x можемо записати у бази као $x = x_{d-1}\alpha^{d-1} + x_{d-2}\alpha^{d-2} + \ldots + x_0$. Идеја је да проблем рачунања корена пренесемо у коначно поље, у коме имамо ефикасне

алгортиме. За y чији корен тражимо добијено нашим алгоритмом, тј. уколико је $y = \prod_{i=1}^{k}(a_i + b_i)$ у раду [26] је дата оцена:

$$|x_{d-1}m^{d-1} + x_{d-2}m^{d-2} + \ldots + x_0| \leq d^{(d+5)/2} \cdot n \cdot (2u\sqrt{d}n^{1/d})^{k/2}$$

Ово је доста груба оцена, али нам може послужити да стекнемо осећај колики су коефицијенти x_i. Уколико нам је због перформанси неопходна нижа граница, можемо се ослонити на поступак представљен у истом раду ([26]) који даје доста прецизнију оцену за сваки од коефицијената x_i.

Означимо са M израчунату границу. Тада је довољно за сваки x_i знати $x_i \pmod P$, за неки број $P > 2M$. Овде је смо узели $2M$ јер x_i може бити и позитиван и негативан. У случају да је $x_i \pmod P < M$ биће $x_i > 0$, а иначе $x_i < 0$. Идеја је одаберемо $P = \prod_{i=1}^{k} p_i$, при чему су $p_1, p_2, \ldots, p_k$ различити прости бројеви. Претпоставимо да можемо наћи вредности за сваки коефицијент x_i по модулу p, тј. да за свако x_i знамо x_{ij} тако да важи следећи систем:

$$\begin{aligned} x_{i1} &\equiv x_i \pmod{p_1} \\ x_{i2} &\equiv x_i \pmod{p_2} \\ &\vdots \\ x_{ik} &\equiv x_i \pmod{p_k} \end{aligned}$$

Тада по кинеској теореми о остацима можемо једноставно изачунати x_i из вредности x_{ij}. Да би могли да израчунамо бројеве x_{ij} захтеваћемо од простих p_i да је $f(x)$ нерастављив у сваком од $\mathbb{F}_{p_i}[X]$. Покажимо како ћемо израчунати коефицијенте у том случају.

Нека је дато просто p тако да је $f(x)$ нерастављив у $\mathbb{F}_p[X]$. Нека је $\pi_p : \mathbb{Z}[\alpha] \to \mathbb{F}_p(\alpha)$ канонски епиморфизам прстена, који ће заправо бити само редуковање коефицијената по модулу p. Ми желимо да нађемо коефицијенте у базној репрезентацији елемента $\pi_p(x)$. Ради лакшег означавања уведимо ознаке $\pi_p(x) = x_p$ и $\pi_p(y) = y_p$. Уколико је $x^2 = y$ имамо и да је

$$\pi_p(x)^2 = \pi_p(x^2) = \pi_p(y)$$

тј. да је $x_p^2 = y_p$. Пошто смо претпоставили да је f нерастављив у $\mathbb{F}_p[X]$, то ће и $\mathbb{F}_p(\alpha)$ бити поље и важиће $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^d}$ (по теореми 2) . Зато једначина $x_p^2 = y_p$ може да има само два решења, која ће бити облика $\pm r$ за неко $r \in \mathbb{F}_p(\alpha)$. У одељку 4.3 ће бити представљен ефикасан алгоритам који налази ове корене. Ипак, када нађемо ова два корена, морамо се одлучити за један од њих, који ће одговарати елементу x_p. Али како ово урадити?

Овде нам у помоћ долази норма елемента. Испоставља се да се норма може на аналоган начин дефинисати и у коначним пољима :

***Дефиниција* 6.** *Нека је p прост број и $f(x) \in \mathbb{F}_p[X]$ моничан и нерастављив полином степена d. Нека је α нека његов корен у коренском пољу и нека је $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^d}$ коначно поље индуковано овим кореном. Даље, нека су $\sigma_1, \sigma_2, \ldots, \sigma_d$ сви хомоморфизми из $\mathbb{Z}[\alpha]$ који сликају α у неки од корена $f(x)$ у коренском пољу. Тада је норма N_p елемента $\theta \in \mathbb{Z}[\alpha]$ дефинисана са*

$$N_p(\theta) = \sigma_1(\theta)\sigma_2(\theta)\ldots\sigma_d(\theta)$$

Ова дефиниција нам не даје много података о самој норми. Коренско поље може имати веома компликовану структуру, а самим тим није јасно ни како тачно баратати са хомоморфизмима σ_i. Следећа теорема ће нам дати веома једноставан начин за рад са свим овим појмовима:

Теорема 22. *Нека је $q = p^d$ за неки прост број p и нека је $f(x) \in \mathbb{F}_p[X]$ иредуцибилан моничан полином и нека је α једна његова нула. Тада су хомоморфизми σ_i из дефиниције 6 дати формулом $\sigma_i(\theta) = \theta^{p^i}$.*

Доказ. Докажимо прво да су пресликавања σ_i хомоморфизми. За $i > 1$ важи $\sigma_i = \underbrace{\sigma_1 \circ \sigma_1 \circ \ldots \circ \sigma_1}_{i \text{ пута}}$, па је довољно доказати да је σ_1 хомоморфизам. Ако су $a, b \in \mathbb{F}_{p^d}$, имамо да је $\sigma_1(ab) = (ab)^p = a^p b^p = \sigma_1(a)\sigma_1(b)$. Такође, пошто $p \mid \binom{p}{i}$ за $0 < i < p$, имамо да је

$$\sigma_1(a+b) = (a+b)^p = a^p + a^{p-1}b\binom{p}{1} + a^{p-2}b^2\binom{p}{2} + \ldots ab^{p-1}\binom{p}{p-1} + b^p = a^p + b^p$$

при чему смо унутрашње елементе могли да скратимо јер је карактеристика амбијентног поља p. Уколико је α једна од нула, онда ће за сваки од хомоморфизама важити:

$$f(\sigma_i(\alpha)) = \sigma_i(f(\alpha)) = \sigma_i(0)$$

па ће и слика α бити корен полинома. Треба још да покажемо да међу коренима $\sigma_i(\alpha)$ нема истих. Пошто је мултипликативна група $\mathbb{F}^*_{p^d}$ реда $p^d - 1$, имаћемо да је $\theta^{d^p} = \theta^{d^p - 1} \cdot \theta = \theta$, па је $\sigma_d = id$. Зато су $\sigma_i(\alpha)$ заправо вредности $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$. Уколико би међу њима било истих, тј. ако би постојали $i \neq j$ такви да је $\alpha^{p^i} = \alpha^{p^j}$, онда би био $\alpha^{p^{i-j}} = 1$, али онда би било и $f(1) = f(\alpha^{p^{i-j}}) = 0$, па би полином f имао 1 за нулу. Али ово је контрадикција, јер је f нерастављив у $\mathbb{F}_p[X]$, чиме је доказ завршен. □

Из ове теореме лако је извући и аналитички облик функције за норму елемента. Наиме, за неки елемент $\theta \in \mathbb{Z}[\alpha]$ имамо да је

$$N_p(\theta) = \sigma_1(\theta)\sigma_2(\theta)\ldots\sigma_d(\theta) = (\theta)(\theta^p)(\theta^{p^2})(\theta^{p^3})\ldots(\theta^{p^{d-1}}) = \theta^{1+p+p^2+\ldots+p^{d-1}} = \theta^{\frac{p^d-1}{p-1}}$$

Норме N_p и N су повезане следећом теоремом:

Теорема 23. *Нека је дат моничан иредуцибилан полином $f(x) \in \mathbb{Z}[X]$ степена d, и нека је p прост број такав да је $f(x)$ нерастављив и у $\mathbb{F}_p[X]$. Нека је $\mathbb{F}_p[\alpha]$ поље генерисано неком нулом α полинома $f(x)$. Тада је за свако $\theta \in \mathbb{Z}[\alpha]$*

$$N(\theta) \equiv N_p(\theta_p) \pmod{p} \qquad \textit{(4.2.1)}$$

где је θ_p слика елемента θ при канонском епиморфизму $\pi_p : \mathbb{Z}[\alpha] \to \mathbb{F}_p[\alpha]$.

Вратимо се сада једначини $x_p^2 = y_p \pmod{p}$. Ми желимо да нађемо оно решење које ће бити баш слика елемента x при пресликавању π_p. Из мултипликативности норме имамо да је $N(y) = N(x^2) = N(x)^2$, па норму од x можемо наћи иако не знамо x. Тада ће x_p морати да има норму за коју важи $N_p(x_p) \equiv N(x) \pmod{p}$. Пошто смо одабрали полином f непарног степена d, за решења једначине $x_p \equiv \pm r \pmod{p}$ ће важити да је

$$N_p(-r) = \sigma_1(-r)\sigma_2(-r)\ldots\sigma_d(-r) = (-1)^d\sigma_1(r)\sigma_2(r)\ldots\sigma_d(r) = -N_p(r)$$

тј., биће $N_p(-r) = -N_p(r)$. Али даље, пошто је прост p непаран (број 2 не морамо узимати) биће и $N_p(r) \not\equiv N_p(-r) \pmod p$, па не могу оба решења задовољавати конгруенцију $N(x_p) \equiv N(x) \pmod p$, те можемо недвосмислено одабрати одговарајуће решење. Приметимо да се овде може догодити да норма и једног и другог решења не задовољава конгруенцију (4.2.1). У том случају наш кандидат y није квадратан, те се морамо вратити на поступак решетања.

Као што смо већ напоменули, након што нађемо вредности x_{p_i} није тешко конструисати сам број x. Ипак, за велике вредности n имаћемо велики број простих p_i, те ће величине коефицијената за x бити толико велике да време њиховог израчунавања може надмашити све остале фазе алгоритма. Срећом, нас ће занимати само вредности коефицијената x у $\mathbb{Z}/n\mathbb{Z}$, те на сваком кораку можемо посматрати само слику коефицијената у $\mathbb{Z}/n\mathbb{Z}$, и на тај начин избећи баратање са бројевима већим од n. За детаљније објашњење погледати [26] или [13].

4.3 Тражење корена у коначним пољима

За тражење корена у коначним пољима применићемо алгоритам Тонели-Шенкса[1] за цикличне групе. Окружење у коме радимо је коначно поље $\mathbb{F}_{p^d}$, где је p непаран прост број. Алгоритам примењујемо на мултипликативну групу $\mathbb{F}^*_{p^d}$, за коју из алгебре знамо да је циклична. Надаље у овом поглављу ћемо обележити са γ генератор цикличне групе, тј. $\langle\gamma\rangle = \mathbb{F}^*_{p^d}$. Корен ћемо тражити за елемент δ.

Појам квадратних и неквадратних елемената можемо увести и на $\mathbb{F}_{p^d}$. Прецизно, имамо:

***Дефиниција* 7.** *Нека је p непаран прост број, и нека је $\mathbb{F}_{p^d}$ коначно поље кардиналности p^d. Тада за $\theta \in \mathbb{F}^*_{p^d}$ кажемо да је квадратан ако једначина $x^2 = \theta$ има решења у $\mathbb{F}_{p^d}$. Иначе, елемент θ називамо неквадратним остатком.*

Скуп $\mathbb{F}_{p^d}$ има структуру поља, па једначина $x^2 = \theta$ за $\theta \neq 0$ има или два или нема решења. Јасно је да се Лежандров симбол може једноставно проширити и на ово поље. Занимљиво је да и његова аналитичка форма остаје иста, тј. важи следећа теорема:

***Теорема* 24.** *Нека је p непаран прост број, и нека је $\mathbb{F}_{p^d}$ коначно поље кардиналности $q = p^d$. Тада, ако је неко $\theta \in \mathbb{F}^*_{p^d}$ квадратно ако и само ако $\theta^{(q-1)/2} = 1$. У случају да је θ неквадратно важи $\theta^{(q-1)/2} = -1$*

Доказ. У случају да је θ квадратан, постојаће неко ρ такво да је $\rho^2 = \theta$. Зато је и

$$\theta^{(q-1)/2} = \rho^{q-1} = 1$$

где последња једнакост важи јер је ред групе $\mathbb{F}^*_q$ једнак $q - 1$.

Нека је сада $\theta \neq 0$ и $\theta^{(q-1)/2} = 1$. Пошто је $\mathbb{F}^*_q$ циклична, имамо да за неко $k \in \mathbb{N}$ важи $\gamma^k = \theta$, при чему је γ генератор групе. Даље је $1 = \theta^{(q-1)/2} = \gamma^{k(q-1)/2}$. Одатле имамо да $(q-1)|k(q-1)/2$, те је зато и k парно, тј. имамо да је $k = 2k_1$ за неко $k_1 \in \mathbb{N}$. Али онда и

$$(\gamma^{k_1})^2 = \gamma^{2k_1} = \gamma^k = \theta$$

па је θ квадратан.

Други део тврђења се добија директно из првог, јер су једине могуће вредности $\theta^{(q-1)/2}$ за $\theta \neq 0$ управо $+1$ и -1. □

[1] Alberto Tonelli, Daniel Shanks

Број елемената мултипликативне групе p^d-1 можемо факторисати као $p^d-1=2^r s$, тако да је s непарно. Обзиром да је p негативно, важиће $r>0$. Ако узмемо $w=\delta^{(s+1)/2}$ онда је $w^2=\delta^s\delta$, па је $\delta^s=w^2\delta^{-1}$ квадратан. То значи и да постоји неко $\zeta\in\mathbb{F}_{p^d}$ за које је $\zeta^2=\delta^s$. Да би нашли δ прво ћемо тражити ζ. Након што нађемо ζ, дефинишемо $\nu=w\zeta^{-1}$. Имаћемо да је:

$$\nu^2=w^2\zeta^{-2}=\delta^s\delta\delta^{-s}=\delta$$

те одавде видимо како можемо наћи δ ако нам је познато ζ.

Због чега је δ^s погоднији за тражење корена? Посматрајмо $(\delta^s)^{2^{r-1}}$. Пошто је δ квадратан, он ће имати неки корен који можемо означити са ρ. Тада имамо да је

$$(\delta^s)^{2^{r-1}}=\delta^{2^{r-1}s}=\rho^{2^r s}=1 \tag{4.3.1}$$

где последња једнакост важи јер ред групе $\mathbb{F}_{p^d}$ износи $p^d-1=2^r s$. Одавде видимо да ред елеменента δ^s дели 2^{r-1}. За корен ρ елемента δ^s, тј. ако је $\rho^2=\delta^s$, важи

$$\rho^{2^r}=(\rho^2)^{2^{r-1}}=\delta^{2^{r-1}s}=1$$

па ред елемента ρ дели 2^r. Дакле, и елемент δ^s и његов корен имају специјална својства која ћемо користити за израду алгоритма. Прва могућа оптимизација би била да корене тражимо само међу онима који су реда 2^k за неко $k<r$, уместо да корен проверавамо на свим елементим мултипликативне групе. За тај поступак је згодна следећа теорема:

***Теорема* 25.** *Нека је p непаран прост број, и некад је $\mathbb{F}_{p^d}$ поље кардиналности $q=p^d$. Нека су r и s природни бројеви такви да је $q-1=2^r s$, при чему је s непаран. Уколико је η неквадратни остатак у пољу $\mathbb{F}_{p^d}$, онда је ред елемента η^s тачно 2^r, а самим тим је и Силовљева[1] 2-подгрупа S_{2^r} групе $\mathbb{F}_{p^d}$ дата са*

$$S_{2^r}=\{1,\eta^s,\eta^{2s},\eta^{3s},\ldots,\eta^{(2^r-1)s}\}$$

Доказ. Означимо са k ред елемента η^s. Пошто је η неквадратан, из теореме 24 имамо да је $\eta^{(q-1)/2}=-1$. Пошто је $q-1=2^r s$, то је и $(q-1)/2=2^{r-1}s$, па је

$$(\eta^s)^{2^{r-1}}=\eta^{s2^{r-1}}=\eta^{(q-1)/2}=-1$$

Одавде имамо да је $(\eta^s)^{2^r}=1$, па због тога ред k елемента η^s дели 2^r. Зато је k неки од бројева $1,2,2^2,\ldots,2^r$. Претпоставимо да $k\neq 2^r$. Тада је $k=2^m$ за неко $m<r$. Али онда је $(\eta^s)^{2^m}=1$ и даље

$$-1=\eta^{s2^{r-1}}=(\eta^{s2^{r-2}})^2=(n^{s2^{r-3}})^{2^2}=\ldots=(n^{s2^m})^{2^{r-1-m}}=1^{2^{r-1-m}}=1$$

што нас доводи до контрадикције, па мора бити $k=2^r$. Пошто је Силовљева 2-подгрупа S_{2^r} кардиналности 2^r то је и η^s генератор те групе, чиме је доказ окончан. □

Дакле, уколико можемо наћи неки неквадратан елемент η, можемо уместо у $2^r s$ наћи корен у 2^r корака. Али овај алгоритам је ефикаснији једино уколико можемо лако наћи неквадратан елемент. У раду [30] је уз претпоставку генералисане Риманове хипотезе показано да је најмањи неквадратни елемент поља $\mathbb{F}_{p^d}$ реда $O(log(p)^2)$. Осим тога, половина елемената $\mathbb{F}_{p^d}$ је неквадратно што видимо из њихове репрезентације преко генератора γ, па можемо узимати разне елементе случајним избором, на њима

[1] *Силовљева q подгрупа групе G је највећа подгрупа чија је кардиналност облика q^r. Оваква група је јединствена. Иначе, ове групе су добиле назив по норвешком математичару Лудвигу Силову(Lydwig Sylow, 1832-1918).*

вршити проверу квадратности Лежандровим симболом, док не нађемо неквадратни. Целокупан алгоритам је сложености $O(2^r)$.

Тонели-Шенксов алгоритам успева да спусти сложеност на $O(r)$. Идеја на којој се алгоритам заснива је да нађемо низ елемената w_i и λ_i у $\mathbb{F}_{p^d}$ за које важи $w_i^2 = \lambda_i\delta$, и да су елементи λ_i такви да су им редови $ord(\lambda_i)$ строго опадајући и да деле 2^{r-1}. Зато ће након највише r бити $\lambda_i = 1$, те је и $w_i^2 = \delta$, тј. w_i је тражени корен. Остаје само да опишемо конструкцију елемената λ_i и w_i, чиме комплетирамо причу о овом алгоритму:

***Теорема* 26.** *Нека је ϑ генератор Силовљеве 2-подгрупе S_{2^r}. Нека је δ квадратни елемент групе $\mathbb{F}^*_{p^d}$, при чему је p негативан прост број, и нека је $p^d - 1 = 2^r s, s \nmid 2$. Дефинишимо рекурзивно низ λ_i који ће имати елементе реда 2^{m_i}:*

$$\lambda_0 = \delta^s, \lambda_{i+1} = \lambda_i\vartheta^{2^{r-m_i}},\ ord(\lambda_i) = 2^{m_i}$$

као и низ w_n:

$$w_0 = \delta^{(s+1)/2}, w_{i+1} = w_i\vartheta^{2^{r-m_i-1}}$$

Тада је $w_i^2 = \lambda_i\delta$ као и $m_{i+1} < m_i$,.

Доказ. Да ред елемента $\lambda_0 = \delta^s$ дели 2^r смо показали већ код једнакости (4.3.1)*. Нека сада λ_i има ред 2_i^m. Тада је $\lambda_i^{2^{m_i-1}} = -1$ јер би иначе било $\lambda_i^{2^{m_i-1}} = 1$, па би $ord(\lambda_i) < 2^{m_i}$. Аналогно и $\vartheta^{2^{r-1}} = -1$. За λ_{i+1} онда имамо:*

$$\lambda_{i+1}^{2^{m_i-1}} = (\lambda_i\vartheta^{2^{r-m_i}})^{2^{m_i-1}} = \lambda_i^{2^{m_i-1}}\vartheta^{2^{r-m_i+m_i-1}} = -1\vartheta^{2^{r-1}} = (-1)(-1) = 1$$

па је $ord(\lambda_{i+1})|2^{m_i-1}$, одакле имамо и да је $m_{i+1} < m_i$. Остаје још да се покаже да је $w_i = \lambda_i^2\delta$. За $i = 0$ ово је очигледно. Даље по индукцији имамо:

$$w_{i+1}^2 = w_i^2\vartheta^{2^{r-m_i}} = \lambda_i\delta\vartheta^{2^{r-m_i}} = \lambda_i\vartheta^{2^{r-m_i}}\delta = \lambda_{i+1}\delta$$

Овиме је доказ завршен. □

5 Закључак

У досадашњем тексту смо дали један од начина за реализацију алгоритма. У овој глави ћемо као закључак на цео текст представити једну врсту криптосистема чија се сигурност заснива на сложености факторизације бројева, те је у природној вези са алгоритмом решета бројног поља. Поред тога, сумираћемо целокупан поступак изложен у раду и прокоментарисати могућа унапређења рада уз неколико коментара на савремене трендове у развоју алгоритма.

5.1 RSA криптосистем и генерално бројно поље

RSA криптосистем је један од први криптосистема јавног кључа настао 1977. година на МИТ универзитету у Бостону. Овај алгоритам је резултат здруженог рада тројице научника: Рона Ривеста,Адија Шамира и Леонарда Адлемана[1], по чијим је презименима и добио назив. Куриозитета ради поменимо и то да је исти систем пројектовао Клифорд Кокс[2] четири године пре ове групе, али с обзиром да је алгоритам био намењен британској тајној служби ова чињеница није била позната све до 1998. године.

RSA криптосистем користи два кључа: јавни и приватни. Јавни кључ дефинише прималац на почетку комуникације и објављује га свима. На основу њега пошиљаоци енкриптују податке. Током процеса стварања јавног кључа прималац ствара и приватни кључ, чију вредност задржава само за себе, и који користи за декриптовање података. У случају да злонамеран корисник пресретне комуникацију, њему ће бити познат јавни кључ и енкриптовани подаци, али не и приватни кључ, без кога он неће моћи да ефикасно дешифрује украдене податке.

RSA криптосистем прво фиксира два велика проста броја p и q, и дефинише $n = pq$. За овако дефинисано n је $\phi(n) = (p-1)(q-1)$. Након тога алгоритам бира b тако да је $(b, \phi(n)) = 1$, и израчунава $a = b^{-1} \pmod{\phi(n)}$. Јавни кључ чине бројеви n и b, док је a приватни кључ. Тада пошиљалац податак $x \in \mathbb{Z}/n\mathbb{Z}$ енкриптује са:

$$x^b \pmod{n}$$

Када примаоца стигне податак $y = x^b$, он може израчунати вредност

$$y^a \equiv (x^b)^a \equiv x^{ab} \pmod{n}$$

и пошто је $a = b^{-1} \pmod{\phi(n)}$, тј. $ab = 1 \pmod{\phi(n)}$ или $1 + ab = k\phi(n)$, важи

$$x^{ab} \equiv x^{k\phi(n)+1} \equiv x \pmod{n}$$

па прималац декриптује све податке тражењем вредности y^a. Све операције степеновања се извршавају у логаритамској сложености алгоритмом за брзо степеновање.

Претпоставимо сада да је малициозни корисник успео да украде неко y из комуникације. Један од начина да дође до вредности x је да рачуна све могуће вредности y^k док не добије смислени податак. Ипак, уколико смо били довољно пажљиви да одаберемо велико a, овај покушај је сигурно осуђен на неуспех. Паметније је покушати да израчунамо a на неки други начин. С обзиром да је нама познато b, можемо израчунати из формуле $a = b^{-1} \pmod{\phi(n)}$, у случају да нам је познат $\phi(n)$. Али у случају да је знамо $\phi(n)$, имаћемо да је

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$$

[1] Ron Rivest, Adi Shamir, Leonard Adleman

[2] Clifford Cocks

па можемо израчунати $p + q = n - \phi(n) + 1$, и по Виетовим формулама знамо да p и q можемо наћи решавањем квадратне једначине

$$x^2 - (p + q)x + pq = 0$$

те је проблем тражења вредности $\phi(n)$ у овом случају еквивалентан факторизацији n.

Поред овог, постоји још неколико начина напада на RSA криптосистем. Такав рецимо Винеров[1] напад који успешан када је одабрано мало a. За RSA није формално показано да не постоји лакши начин пробијања безбедности од факторизације броја n, али научна јавност је чврсто убеђена да је ово случај. За разлику од њега, за Рабинов[2] криптосистем је доказано да је декрипција еквивалентна факторизацији. Ипак, овај криптосистем има извесне проблеме са недвосмисленошћу енкрипције због које он није уведен у масовну употребу.

5.2 Завршна реч

У овом раду смо изложили све фазе алгоритма решета бројног поља уз осврт на математички апарат на коме је утемељен. Рад има за циљ да представи алгоритам на разумљив али и комплетан начин, тако да читаоцу да довољно информација за имплементију целокупног алгоритма. Због овог приступа на многим местима сам избегавао компликације које би допринеле бољим перформансама. Ипак, где год је то могуће, дао сам референце на литературу на основу које елементаран алгоритам може да се надогради. Прво могуће унапређење које може донети значајно побољшање је увођење паралелизације на нивоу решетања. Поред тога, експериментисање са почетним полиномом $f(x)$ може бити од великог значаја. У последње време пажња истраживача је све више оријентисана управо на ову фазу са мањим или већим успехом. Алгоритам је веома осетљив на задате параметре у разним фазама, што га чини веома интересантним за даље проучавање.

У циљу бољег разумењања овог алгоритма, као и даљег истраживања, корисно је експериментисати са разним улазним подацима и параметрима. Такође, може бити корисно и експериментисати изменама самих метода који се користе у алгоритму. У ту сврху могу послужити разне имплементације које постоје на интернету (нпр. *pGNFS*, *GGNFS*, *msieve*). Може послужити и рад [28] у коме је након објашњења свих фаза алгоритма дат код имплементације. Ипак, при раду са овим имплементацијама требамо бити опрезни у оцењивању перформанси јер већина њих због једноставности не користи најефикасније методе.

[1] Michael J. Wiener

[2] Michael Oser Rabin(1931-), израелски информатичар

Литература

[1] A.K. Lenstra, H.W.Lenstra, Jr. (eds.), *The development of the number field sieve*, Lecture Notes in Mathematics, vol. 1554, Berlin, Springer-Verlag,

[2] J.P. Buhler, H.W.Lenstra, Jr., Carl Pomerance, *Factoring integers with the number field sieve*, Lenstra and Lenstra[1] , pp. 50-94

[3] A.K. Lenstra, H.W. Lenstra, M.S. Manasse, J.M. Pollard, *The number field sieve*, Proc. 22nd Annual ACM Symp. on Theory of Computing(STOC) (1900), 564-572, Lenstra and Lenstra[1] , pp. 11-42

[4] Carl Pomerance, *The tale of two sieves*, Notices of the AMS 43 (12). pp. 1473–1485

[5] Gojko Kalajdžič, *Algebra*, Matematički fakultet, Beograd, 1998

[6] Goran Đanković, *Teorija brojeva*, Matematički fakultet, Beograd, 2013

[7] J.D. Dixon, Asymptotically fast factorization of integers, Math. Comp 36 (1981), 255-260

[8] Carl Pomerance, *Analysis and Comparison of Some Integer Factoring Algorithms*, Computational Methods in Number Theory, Part I, H.W. Lenstra, Jr. and R. Tijdeman, eds., Math. Centre Tract 154, Amsterdam, 1982, pp 89-139.

[9] Carl Pomerance, *The number field sieve*, Mathematics of Computation, 1943–1993, Fifty Years of Computational Mathematics, W. Gautschi, ed., Proc. Symp. Appl. Math. 48, American Mathematical Society, Providence, 1994, pp. 465–480.

[10] J.M. Pollard, *Factoring with cubic integers*,Lenstra and Lenstra[1], pp 4-10

[11] Daniel J. Bernstein, A.K.Lenstra, *A general number field sieve implementation*, Lenstra and Lenstra [1], сп. 103-126.

[12] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K.Lenstra, и други, *Factorization of a 768-bit RSA modulus*, Cryptology ePrint Archive, Report 2010/006

[13] Matthew E. Briggs, *An Introduction to the General Nubmer Field Sieve*, master thesis, Virginia Polytechnic Institute and State University, 1998

[14] G. Villard, *A study of Coppersmith's block Wiedemann algorithm using matrix polynomials*, LMC-IMAG, REPORT # 975 IM

[15] D. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Trans. Inform. Theory 32 (1986), 54-62

[16] D. Coppersmith, Modifications to the number field sieve, J. Cryptology, to appear ; IBM Research Report #RC 16264, Yorktown Heights, New York, 1990

[17] Emmanuel Thomeó, *Subquadratic computation of vector generating polynomials and improvement of the block Wiedemann algorithm*, Journal of Symbolic Computation, Elsevier, 2002, 33 (5), pp.757-775

[18] Thorsten Kleinjung,*On polynomial selection for the general number field sieve*, Mathematics of computation Volume 75, Number 256, October 2006, Pages 2037–2047,S 0025-5718(06)01870-9

[19] Shi Bai, Cyril Bouvier, Alexander Kruppa, Paul Zimmerman, *Better polynomials for GNFS*, Mathematics of computation, S 0025-5718(XX)0000-0

[20] Razvan Barbulescu, Cécile Pierrot, *The Multiple Number Field Sieve for Medium and High Characteristic Finite Fields*, IACR Cryptology ePrint Archive 2014: 147 (2014)

[21] Frederick J. Smith, *A brief history of factorization techniques*, CSE590 - Practical Aspects of Modern Cryptography, University of Washington

[22] Daniel M. Gordon, *Discrete Logarithms in GF(p) using the Number Field Sieve*, SIAM J. Discrete Math, vol. 6, 1993, pp. 124--138

[23] Olivier Shirokauer, *The impact of the number field sieve on the discrete logarithm problem in finite fields*, Algorithmic Number Theory, MSRI Publications, Volume 44, 2008

[24] Douglas R. Stinson, *Cryptography: Theory and Practice*, Chapman and Hall/CRC, 2005

[25] J.A.Buchmann, H.W.Lenstra, *Approximating rings of integers in number fields*, Journal de théorie des nombres de Bordeaux 6.2 (1994): 221-260. <http://eudml.org/doc/247529>.

[26] Jean-Marc Couveignes, *Computing a square root for the number sieve*, The development of the number field sieve, 1993.

[27] Phong Nguyen, *A Montgomery-like square root for the number field sieve*,1998

[28] Ruben Grønning Spaans, *Number field sieve*, Master thesis at Norwegian University of Science and Technology

[29] Per Leslie Jensen, *Integer factorization*, Master thesis at University of Copenhagen

[30] Jeremy Booher, *Square roots in finite fields and quadratic nonresidues*, <http://stanford.edu/ jbooher/expos/sqr_qnr.pdf>. Приступљено августа 2015.

[31] Peter Montgomery, *A Block Lanczos Algorithm for Finding Dependencies over GF(2)*. Lecture Notes in Computer Science. EUROCRYPT '95 921. Springer-Verlag. pp 106-120