Математички факултет у Београду

Мастер рад

О ТЕСТОВИМА ПРИМАЛНОСТИ

СТУДЕНТ
Марко Радовановић
1007/2008

МЕНТОР
др Жарко Мијајловић

Београд 2009.

Садржај

Увод

Посебну улогу у теорији бројева заузимају тзв. прости бројеви, тј. они природни бројеви већи од један који су дељиви само са 1 и самим собом. Иако се дефиниција чини доста једноставна, сам процес утврђивања да ли је неки број прост или не то свакако није. И дан данас остали су отворени многи класични проблеми везани за просте бројеве, као што је нпр. проналажење било какве формуле којом би могао да се срачуна n-ти прост број. У овом тексту даћемо неке од најпознатијих и најефикаснијих алгортитама за утврђивање да ли број прост или не, тзв. *тестове прмалности*.

Сигуран и једноставан начин да проверимо да ли је број n прост је да испитамо да ли је дељив бројевима од 2 до $n-1$ и уколико није можемо тврдити да је n прост. Уз примедбу да сложен број n мора имати простог делиоца мањег од $\sqrt{n}$, претходни алгоритам можемо побољшати провером дељивости бројевима од 2 до $[\sqrt{n}]$. Овако задат алгоритам без проблема можемо користити за мале бројеве, чак и без употребе рачунара. Међутим, због велике примене простих бројева пре свега у криптографији, потребни су нам тестови прималности који могу радити са бројевима који имају и преко 1000 цифара[1], па овакав тест није примењив.

Други класнични начин за тестирање прималности је тзв. Ератостеново[2] сито. Овим ситом прималност броја n испитујемо на следећи начин: запишемо све бројеве од 2 до n у низ. Затим прецртавамо све бројеве који су дељиви са 2. После тога бирамо најмањи непрецртани број и прецртавамо све бројеве који су дељиви тим бројем. Овај процес настављамо све док не остане само n - тада је n прост, или док n не прецртамо - тада је n сложен. Овако задат тест такође је врло неефикасан. Међутим, он нам даје више, јер њиме можемо да одредимо све просте бројеве не веће од n.

За претходна два алгоритма кажемо да су *експоненцијалне сложености*, јер време потребно да се они изврше полиномијално зависи од n. Нама од интереса неће бити овакви алгоритми, него тзв. алгоритми *полиномијалне сложености*, тј. они који се извршавају у времену које полиномијално зависи од $\ln n$. Скоро сви тестови које ћемо дати у овом тексту биће управо полиномијалне сложености.

У тексти ће бити разматрани детерминистички и пробабилистички тестови прималности. Дефиницију ових појмова ћемо дати касније. Треба

[1] овакви бројеви називају се *титански*

[2] *Ερατσθένης* - грчки математичар 276-195 п.н.е.

напоменути да је тек 2002. године дат први полиномијални детерминистички алгоритам и тиме је доказано да су прости бројеви у класи $\mathcal{P}$ проблема.

Осим теоријског осврта на сложеност алгоритма, тј. разматрања асимптотске сложености, за сваки алгоритам биће разматрана и његова практична примена, тј. „реална" ефикасност.

У тексту ће бити коришћене стандардне ознаке сложености $O(n)$ и $\Omega(n)$, где $O(n)$ означава да је за довољно велико n за извршење алгоритма потребно не више од $k \cdot n$ операција (k је нека константа), док $\Omega(n)$ означава да је за довољно велико n за извршење алгоритма потребно не мање од $k \cdot n$ операција.

Већина алгоритама ће бити дата и у псеудо-коду који потсећа на код програмског језика C.

Део 1

Основне теореме и алгоритми теорије бројева

У овом поглављу даћемо преглед теорема и алгоритама који ће бити саставни део готово свих наредних алгоритама. Компликованије и значајније теореме биће дате са доказом, док ће оне опште познате и једноставне бити или подразумеване или дате без доказа.

1.1 Еуклидов алгоритам

Често ће за природне бројеве m и n бити потребно одредити њихов највећи заједнички делилац, у ознаци НЗД (a, b) или само (a, b). Један од најпознатијих, а уједно и веома ефикасан начин за одређивање НЗД-а два броја је Еуклидов алгоритам, који у псеудо-коду можемо дати са:

Алгоритам 1.1. (Еуклидов[1] алгоритам)
`while` $(y > 0)$ $(x, y) = (y, x$ `mod` $y)$;
`vrati` x;

Пажљивијим увидом у Еуклидов алгоритам закључујемо да он даје и решење линеарне Диофантове једначине

$$ax + by = (x, y).$$

Овај алгоритам називаћемо продужени Еуклидов алгоритам, а у псеудо-коду га можемо записати као:

Алгоритам 1.2. (Продужени Еуклидов алгоритам)
$(a, b, g, u, v, w) = (1, 0, x, 0, 1, y)$;
`while` $(w > 0)\{$
$q = [g/w]$;

[1] $Ευκλειδης$ - грчки математичар 323-283 п.н.е.

$(a, b, u, v, w) = (u, v, w, a - qa, b - qv, g - qw)$;
}
`vrati` (a, b, g);

Специјално, уколико је $(x, y) = 1$, овим алгоритмом одређујемо број a такав да је $ax \equiv 1 \pmod{y}$.

Време рада алгоритма је $O(\ln x \ln y)$, тј. сразмерно је производу цифара бројева чији НЗД одређујемо. Постоје разне варијанте Еуклидовог алгоритма које у пракси дају боље резултате. Међутим, сви ови алгоритми имају исто асимптотско време рада, које је за „мале" бројеве прихватљиво. За „велике" бројеве ипак постоје ефикаснији алгоритми са асимптотски краћим временом рада. Овакви алгоритми су засновани на идејама које су дате у другом поглављу.

1.2 Мала Фермаова и Ојлерова теорема

Нека је за природан број n са $\varphi(n)$ означен број природних бројева мањих од n који су узајамно прости са n. Ову функцију називамо Ојлерова[2] функција и она представља једну од најзначајнијих функција теорије бројева. Уколико је $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$ канонско представљање броја n, важи

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Значај функције φ даје чувена Ојлерова теорема:

Теорема 1. За природне бројеве a и n, такве да је $(a, n) = 1$, важи

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Доказ. Посматрајмо скуп $A = \{x \mid (x, n) = 1\}$ и скуп $B = \{ax \mid (x, n) = 1\}$. Јасно је да у скупу B не постоје два елемента која дају исти остатак по модулу n и да су сви елементи из B узајамно прости са n. Самим тим скуп A и скуп B су једнаки по модулу n, па важи

$$\prod_{x \in A} x \equiv \prod_{x \in A} ax \pmod{n}.$$

Како је $|A| = |B| = \varphi(n)$, то скраћивањем једнаких чланова са леве и десне стране конгруенције добијамо жељену конгруенцију. □

У случају да је n прост број добијамо Малу Фермаову[3] теорему (МФТ):

[2] Leonhard Paul Euler - швајцарски математичар 1707-1783.
[3] Pierre de Fermat - француски математичар 1601-1665.

Последица 1. За прост број p и природан број a важи

$$a^p \equiv a \pmod{p}.$$

Претходна теорема даје потребан услов да број буде прост. Можемо приметити да се приликом ове провере јавља потреба за израчунавање остатка степена неког броја. Један од алгоритама којим се ово може ефикасно извршити је:

Алгоритам 1.3. (Степен по модулу)
$pow(x, n)\{$
`if` $(n = 1)$ `vrati` x`;`
`if` $(2 \mid n)$ `vrati` $pow(x^2, n/2)$`;`
`else vrati` $x \cdot pow(x^2, (n-1)/2)$`;`
$\}$

Треба напоменути да се готово сви тестови прималности заснивају на теоремама које су инспирисане Малом Фермаовом теоремом.

1.3 Кинеска теорема о остацима

Кинеска теорема о остацима даје начин за решавање система конгруенција:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\dots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

где су n_1, n_2, $\dots$, n_k у паровима узајамно прости бројеви.

Теорема 1. Нека је $N = \prod_{i=1}^{k} n_k$, $N_i = N/n_i$ и $v_i N_i \equiv 1 \pmod{n_i}$, за $1 \leqslant i \leqslant k$. Тада је

$$x \equiv \sum_{i=1}^{k} a_i v_i N_i \pmod{N}.$$

□

Како из продуженог Еуклидовог алгоритма можемо одредити бројеве v_i претходне теореме, то можемо дати и алгоритам заснован на Кинеској теореми о остацима:

Алгоритам 1.4. (Кинеска теорема о остацима (КТО))
`for` $(1 \leqslant i \leqslant k)\{$
$\quad \nu_i = \prod_{j=1}^{i-1} m_j$;
$\quad c_i\nu_i \equiv 1 \pmod{n_i}$;
}
$M = \nu_k m_k$;
$x = a_1$;
`for` $(1 \leqslant i \leqslant k)\{$
$\quad u = ((a_i - x)c_i)$ `mod` n_i;
$\quad x = x + u\nu_i$;
}
$x = x$ `mod` N;
`vrati` x;

Претходни алгоритам није директно изведен из Кинеске теореме о остацима, али није тешко приметити да даје истоветан резултат. При томе овај алгоритам је далеко ефикаснији.

1.4 Група $U(\mathbb{Z}/n\mathbb{Z})$

Нека је са $U(\mathbb{Z}/n\mathbb{Z})$ означен скуп сви инвертибилних елемената прстена $\mathbb{Z}/n\mathbb{Z}$. Јасно је да је ова структура група. У овом поглављу испитаћемо особине ове групе.

Наредна теорема даје одговор у случају простих бројева:

Теорема 1. Уколико је p прост број $\mathbb{Z}/p\mathbb{Z}$ је поље, а $U(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$ је циклична група.
Доказ. За први део тврђења довољно је показати да сваки ненула елемент $a \in \mathbb{Z}/p\mathbb{Z}$ има инверз. Ово следи из чињенице да међу бројевима ax, $x \in \mathbb{Z}/p\mathbb{Z}$, нема једнаких, па мора постојати један који је једнак 1.

Из претходног закључујемо да је $U(\mathbb{Z}/p\mathbb{Z})$ група, а њен ред је $p-1$. Да бисмо доказали да је она циклична, довољно је показати да у њој постоји елемент реда $p-1$. Означимо зато за $d \mid p-1$ са $\psi(d)$ број елемената чији је ред d. Јасно је $\sum_{d|n} \psi(d) = n$. Нека је a неки број чији је d. Тада су a^0, a^1, $\ldots$, a^{d-1} решења конгруенције $x^d \equiv 1 \pmod{p}$, па су ово и једина решења. Међутим, ред броја a^k је d само ако је $(k,d) = 1$. Самим тим, закључујемо да је $\varphi(d) \geqslant \psi(d)$. Како је по познатом Ојлеровом идентитету

$$\sum_{d|p-1} \varphi(d) = p - 1,$$

то је $\varphi(d) = \psi(d)$, за све $d \mid p-1$. Специјално $\psi(p-1) = \varphi(p-1) > 0$. □

Генераторе групе $U(\mathbb{Z}/p\mathbb{Z})$ називаћемо *примитивни корени* по модулу p. Општије:

Дефиниција 1. Цео број a је *примитивни корен* по модулу n уколико генерише групу $U(\mathbb{Z}/n\mathbb{Z})$.

У наставку ћемо доказати да примитивни корени постоје само за потенције простих бројева различитих од 2, као и за 2 и 4. При доказу овог тврђења биће нам од користи следеће теореме:

Теорема 2. Уколико је $l \geqslant 1$ и $a \equiv b \pmod{p^l}$, тада је и $a^p \equiv b^p \pmod{p^{l+1}}$.
Доказ. Из датог услова је $a = b + p^l \cdot k$, за неки природан број k, па применом биномног образца добијамо

$$a^p = \sum_{i=0}^{p} \binom{p}{i} b^{p-i} \cdot p^{li} k^i.$$

Јасно је да су за $i \geqslant 1$ чланови претходног развоја дељиви са p^{l+1}, па је $a^p \equiv b^p \pmod{p^{l+1}}$, што је и требало доказати. □

Теорема 3. Уколико је $l \geqslant 2$ и $p > 2$, тада $(1 + ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \pmod{p^l}$ за све целе бројеве a.
Доказ. Доказ изводимо индукцијом по l. За $l = 2$ тврђење је очигледно тачно. Претпоставимо зато да је $(1+ap)^{p^{l-2}} \equiv 1+ap^{l-1} \pmod{p^l}$ и докажимо да је $(1 + ap)^{p^{l-1}} \equiv 1 + ap^l \pmod{p^{l+1}}$. Из претходне теореме је

$$(1 + ap)^{p^{l-1}} = \left((1 + ap)^{p^{l-2}}\right)^p \equiv (1 + ap^{l-1})^p \pmod{p^{l+1}}. \qquad (*)$$

Из биномног образца је $(1 + ap^{l-1})^p = \sum_{i=0}^{p} a^i \cdot p^{(l-1)i}$, па како $p \mid \binom{p}{2}$ то су за $i \geqslant 2$ сви чланови овог развоја дељиви са p^{l+1}. Самим тим $(1+ap^{l-1})^p \equiv 1+ap^l \pmod{p^{l+1}}$, што заједно са $(*)$ даје тражени резултат. □

Кометар. На сличан нажин доказује се да је за $p = 2$ и $l \geqslant 3$ испуњено $(1 + 4a)^{2^{l-3}} \equiv 1 + a2^{l-1} \pmod{2^l}$.

Теорема 4. Нека је $a \in U(\mathbb{Z}/p^l\mathbb{Z})$ и $p > 2$. Поредак $1+ap \in U(\mathbb{Z}/p^l\mathbb{Z})$ једнак је p^{l-1}.
Доказ. Из претходне теореме је $(1 + ap)^{p^{l-1}} \equiv 1 \pmod{p^l}$, па поредак броја $1 + ap$ дели p^{l-1}. Међутим, поредак не може бити делилац p^{l-2}, јер по претходној теореми $(1 + ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \not\equiv 1 \pmod{p^l}$. □

Теорема 5. Уколико је l природан број група $U(\mathbb{Z}/p^l\mathbb{Z})$ $(p > 2)$ је циклична. Еквивалентно, постоји примитиван корен по модулу p^l.

Доказ. Према Теореми 1 постоји примитивни корен по модулу p. Уколико је то g, тада је и $g+p$ такође примитивни корен по истом модулу. Докажимо да је један од њих примитивни корен по модулу p^2. У супротном је $g^{p-1} \equiv 1 \pmod{p^2}$ и $(g+p)^{p-1} \equiv 1 \pmod{p^2}$. Међутим, из биномног развоја је $(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2}$, што је очигледна контрадикција.

Овим је тврђење доказано у случају $l = 2$. Докажимо да је примитивни корен g по модулу p^2 уједно и примитивни корен по модулу p^l, за све $l \geqslant 2$. Нека је зато $g^n \equiv 1 \pmod{p^l}$ и докажимо да $p^{l-1}(p-1) \mid n$. Како је g примитивни корен по модулу p^2, то $p(p-1) \mid n$, и при томе $g^{p-1} = 1 + ap$, где $p \nmid a$. Међутим, по Теореми 4 поредак броја $1+ap$ по модулу p^l једнак је p^{l-1}, чиме је теорема у потпуности доказана. □

Изглед групе $U(\mathbb{Z}/2^l\mathbb{Z})$ даје следећа теорема:

Теорема 6. Примитивни корени по модулу 2^l постоје уколико је $l = 1$ или $l = 2$, док за $l \geqslant 3$ не постоје. За $l \geqslant 3$ група $U(\mathbb{Z}/2^l\mathbb{Z})$ је директан производ цикличне групе реда 2 и цикличне групе реда 2^{l-2}.
Доказ. 1 је примитини корен по модулу 2, а 3 по модулу 4. Нека је даље $l \geqslant 3$.

На основу коментара после Теореме 3 закључујемо да је $5^{2^{l-3}} \equiv 1 + 2^{l-1} \pmod{2^l}$. Сада је $5^{2^{l-2}} \equiv 1 \pmod{2^l}$, па 5 није примитивни корен по модулу 2^l. Даље, међу бројевима $\{(-1)^a 5^b \mid 0 \leqslant a \leqslant 1,\ 0 \leqslant b < 2^{l-2}\}$ нема конгруентних по модулу 2^l, па су то управо сви непарни остаци по модулу 2^l. Како ниједан од њих није примитивни корен, то по модулу 2^l нема примитивних корена. Претходно представљање доказује и да је група $U(\mathbb{Z}/2^l\mathbb{Z})$ директан производ цикличне групе реда 2 и цикличне групе реда 2^{l-2}. □

Из Теорема 5 и 6 и Кинеске теореме о остацима добијамо опис групе $U(\mathbb{Z}/n\mathbb{Z})$, за произвољан природан број n:

Теорема 7. Нека је $n = 2^a \cdot p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ канонско представљање броја n. Тада је

$$U(\mathbb{Z}/n\mathbb{Z}) \cong U(\mathbb{Z}/2^a\mathbb{Z}) \oplus U(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \oplus \ldots \oplus U(\mathbb{Z}/p_k^{a_k}\mathbb{Z}),$$

где је $U(\mathbb{Z}/p_i^{a_i}\mathbb{Z})$ циклична група реда $p_i^{a_i-1}(p_i-1)$. Група $U(\mathbb{Z}/2^a\mathbb{Z})$ је циклична група реда 2^{a-1} за $a \leqslant 2$, а за $a > 2$ је директан производ цикличне групе реда 2 и цикличне групе реда 2^{a-2}. □

На крају овог поглавља дајемо и теорему која даје списак свих модула по којима постоји примитивни корен:

Теорема 8. Једини модули по којима постоје примитивни корени су 1, 2, 4, p^k и $2 \cdot p^k$, за $p > 2$ прост број и k природан број.
Доказ. Теореме 5 и 6 дају одговор за које од бројева облика p^k, где је p прост број, постоји примитиван корен.

Претпоставимо зато да је $n = n_1 n_2$, где је $n_1, n_2 > 2$ и $(n_1, n_2) = 1$. Из Теореме 7 је $U(\mathbb{Z}/n\mathbb{Z}) \cong U(\mathbb{Z}/n_1\mathbb{Z}) \oplus U(\mathbb{Z}/n_2\mathbb{Z})$ и при томе свака од група $U(\mathbb{Z}/n_1\mathbb{Z})$ и $U(\mathbb{Z}/n_2\mathbb{Z})$ има елемент реда 2. Како циклична група не може имати више од једног елемента реда 2, то $U(\mathbb{Z}/n\mathbb{Z})$ није циклична.

Остаје још да испитамо случај $n = 2p^k$, где је $p > 2$ прост број. Како је $U(\mathbb{Z}/2p^k\mathbb{Z}) \cong U(\mathbb{Z}/2\mathbb{Z}) \oplus U(\mathbb{Z}/p^k\mathbb{Z}) \cong U(\mathbb{Z}/p^k\mathbb{Z})$, то је $U(\mathbb{Z}/2p^k\mathbb{Z})$ циклична, па постоји примитивни корен по модулу $2p^k$. □

Како је примитивни корен генератор одговарајуће групе, од великог значаја нам је проналажење оваквог елемента. Уколико су нам познати прости делиоци броја $p-1$ (p је прост број), следећом једноставном теоремом можемо тестирати да ли је број примитивни корен по модулу p:

Теорема 9. Број g је примитивни корен по модулу p уколико

$$g^{(p-1)/q} \not\equiv 1 \pmod{p}$$

за све просте делиоце q броја $p-1$. □

У псеудо-коду овај тест може записати као:

Алгоритам 1.5. (Да ли је елемент примитивни корен?)
`for (`q `prost i` $q \mid p-1$`)`
  `if` $(g^{(p-1)/q} \equiv 1 \pmod{p})$ `ispiši NE;`
`ispiši DA;`

На крају поглавља даћемо задатак чији је аутор потписник овог текста:

Задатак 1. Одредити све природне бројеве a и b такве да

$$a^b \mid b^a - 1.$$

Решење. Очигледно је пар $(a, 1)$ решење. Зато претпоставимо да је $b > 1$.

Нека је прво a непаран број. Представимо број a као $a = \prod_{i=1}^{n} p_i^{k_i}$, где су p_i различити прости бројеви. Нека је без умањења општости p_1 најмањи прост број који дели a. Сада је јасно да

$$p_1^{k_1 b} \mid b^a - 1,$$

па ако је t_1 највећа потенција броја p_1 која дели $b^a - 1$, то је $t_1 \geqslant k_1 b$. Даље, ако ставимо да је $c_1 = a/p_1^{k_1}$, из Теореме 3 добијамо да

$$p_1^{t_1 - k_1} \parallel b^{c_1} - 1.$$[4]

[4] $p^k \parallel a$ ако и само ако $p^k \mid a$ и $p^{k+1} \nmid a$

Нека је s_1 поредак број a по модулу p_1. Тада $s_1 \mid p_1 - 1$ и $s_1 \mid c_1$, па како је p_1 минималан прост делилац броја a, то је $s_1 = 1$. Сада мора бити

$$p_1^{t_1-k_1} \parallel b - 1.$$

Даље, добијамо је

$$p_1^{b-1} \leqslant p_1^{k_1 b - k_1} \leqslant p_1^{t_1-k_1} \leqslant b - 1.$$

Међутим, за сваки природан x број већи од 1 и ненегативан цео број t је $x^t > t$, па добијамо очигледну контрадикцију. Значи не постоји решење код кога је $b > 1$ и a непаран.

Нека је сада a паран и то $a = 2^k t$, где је t непаран број. Јасно је да је број b непаран. Сада

$$2^{kb} \mid b^{2^k t} - 1,$$

па према коментару после Теореме 3 важи $2^{kb-k+1} \mid b^2 - 1$. Зато мора бити $2^b \leqslant 2^{kb-k+1} < b^2$, што једноставном индукцијом добијамо да не важи за $b > 3$. Једина могућност је $b = 3$. Такође, једино је могуће $k = 1$.

Сада $t^3 \mid 9^t - 1$. Слично као у случају да је a непаран добијамо да најмањи непаран прост делилац броја t мора да дели $9 - 1 = 8$, што је немогуће за $t > 1$. За $t = 1$ решење је $a = 2,\ b = 3$.

Сва решења датог проблема су парови $(a, 1)$ и $(2, 3)$. □

1.5 Коначна поља

У прошлом делу поглавља доказали смо да је за просте бројеве p скуп $\mathbb{Z}/p\mathbb{Z}$ поље. Ово је дат пример једног коначног поља.

У овом делу поглавља детаљније ћемо испитати коначна поља, јер ће нам она бити од великог значаја у даљем делу текста. Основне особине дајемо у следећој теореми:

Теорема 1. (а) Свако коначно поље мора имати p^k елемената, где је p прост, а k природан број.
(б) Мултипликативна група коначног поља је циклична.
(в) За све просте бројеве p и природне бројеве k постоји поље са p^k елемената и сва оваква поља су изоморфна. Поље са p^k елемената означавамо са $\mathbb{F}_{p^k}$.
(г) Поље $\mathbb{F}_{p^k}$ је потпоље поља $\mathbb{F}_{p^l}$ ако и само ако $k \mid l$.

Доказ. (а) Јасно је да свако коначно поље мора имати ненула карактеристику и она мора бити прост број p. Међутим, тада се ово поље може схватити као векторски простор над $\mathbb{Z}_p$. Уколико његова база има k елемената, то дато поље има p^k елемената.

(б) Нека је $\mathbb{E}^*$ мултипликативна група датог поља. Свака коначна група је производ цикличних група. Претпоставимо да у том производу постоје неке групе $\mathbb{C}_m$ и $\mathbb{C}_n$, такве да је $(m,n) > 1$. Ако $p \mid m,n$, то постоје елемнти $a \in \mathbb{C}_m$ и $b \in \mathbb{C}_n$ реда p. Како је $\mathbb{C}_m \cap \mathbb{C}_n = \{1\}$, то у скупу $1, a, a^2, \ldots, a^{p-1}, b, b^2, \ldots, b^{p-1}$ нема једнаких. Међутим, тако добијамо $2p-1$ нула полинома $x^p - 1$, што је очигледна контрадикција. Значи, $\mathbb{E}^*$ се записује као производ цикличних група са узајамно простим редовима. Како за $(m,n) = 1$ важи $\mathbb{C}_m\mathbb{C}_n = \mathbb{C}_{mn}$, то је $\mathbb{E}^*$ заиста циклична група.

(в) Нека је $\mathbb{E}$ коренско поље полинома $f(x) = x^{p^k} - x \in \mathbb{Z}_p[X]$. Јасно је $\mathbb{E}$ карактеристике p, јер је $\mathbb{Z}_p \subset \mathbb{E}$ (по МФТ), па је самим тим према (а) $|\mathbb{E}| = p^l$. Нека је $H = \{a \in E \mid a^{p^k} = a\}$. Како је H скуп свих корена полинома f, то је $|H| = p^k$. Даље, $H \setminus \{0\}$ је јасно подгрупа мултипликативне групе $\mathbb{E}^*$. Докажимо и да је H група у односу на сабирање. Из биномног развоја је $(x+y)^p = x^p + y^p$, па индукцијом добијамо $(x+y)^{p^k} = x^{p^k} + y^{p^k}$. Последње даје да је H затворено у односу на сабирање, односно да је H и адитивна група. Значи H је потпоље поља $\mathbb{E}$, па како оно садржи све корене полинома f, то је $\mathbb{E} = H$.

Докажимо и да су сва поља са p^k елемената међусобно изоморфна, тј. да су сва коренска поља полинома f. Уколико је $\mathbb{F}$ коначно поље, према (б) је $\mathbb{F}^*$ циклична група, односно $\mathbb{F}^* =< b >$. Међутим, тада важи $b^{p^k-1} = 1$, па за све $a = b^i$ важи $a^{p^k} = a$, а како ово важи и за 0, то је $\mathbb{F}$ потпоље поља $\mathbb{E}$. Ово значи да је $\mathbb{F} = \mathbb{E}$.

(г) Уколико је $\mathbb{F}_{p^k}$ потпоље поља $\mathbb{F}_{p^l}$, то је $\mathbb{F}^*_{p^k}$ подгрупа групе $\mathbb{F}^*_{p^l}$. Како су обе ове групе према (б) цикличне, то број елемената једне дели број елемената друге, односно $p^k - 1 \mid p^l - 1$. Није тешко доказати да је последње еквивалентно са $k \mid l$. □

Из претходне теореме закључујемо да су мултипликативне групе коначних поља цикличне. Следећа теорема, аналогна Теореми 9 из претходног дела, тестира да ли је неки елемент поља генератор његове мултипликативне групе:

Теорема 2. Елемент $g \in \mathbb{F}^*_{p^k}$ је генератор уколико

$$g^{(p^k-1)/q} \neq 1$$

за све просте делиоце q броја $p^k - 1$. □

1.6 Аритметика над полиномима

У овом поглављу обратићемо пажњу на полиноме. За прстене полинома $\mathbb{F}[X]$, где је $\mathbb{F}$ поље, важи теорема о дељењу са остатком, која тврди да за

све ненула полиноме $f, g \in \mathbb{F}[X]$ постоје јединствени полиноми $q, r \in \mathbb{F}[X]$ тако да је

$$f = gq + r, \quad \deg r < \deg g.$$

Ова теорема, као и у случају прстена $\mathbb{Z}$, омогућује да НЗД полинома одређујемо Еуклидовим алгоритмом.

Уколико посматрамо полиноме над $\mathbb{F}[X]$, где $\mathbb{F}$ није поље, ствар се значајно компликује. Ипак од користи ће нам бити случај $\mathbb{F} = \mathbb{Z}$. Нека од својстава $\mathbb{Z}[X]$ која ћемо често користити дајемо у следећој теореми:

Теорема 1. Нека су p и r различити прости бројеви. Тада важи:

(а) Уколико је $f(x) \in \mathbb{Z}[X]$ тада је

$$f(x^p) \equiv f(x)^p \pmod{p}.$$

(б) Нека је $h(x)$ било који фактор полинома $x^r - 1$ и $m \equiv m_r \pmod{r}$. Тада је

$$x^m \equiv x^{m_r} \pmod{h(x)}.$$

(в) Нека је $o_r(p)$ поредак броја p у групи $\mathbb{F}_r$. У пољу $\mathbb{F}_p[X]$ полином $\dfrac{x^r - 1}{x - 1}$ факторише се на полиноме степена $o_r(p)$.

Доказ. (а) Из биномног развоја је $(a+b)^p \equiv a^p + b^p \pmod{p}$, па је индукцијом $(a_1 + a_2 + \ldots + a_n)^p \equiv a_1^p + a_2^p + \ldots + a_n^p \pmod{p}$, за произвољан природан број n. Из овога директно следи тврђење овог дела теореме.

(б) Јасно је да за свако d дељиво са r важи $x^r - 1 \mid x^d - 1$, па самим тим $x^r - 1 \mid x^{m - m_r} - 1$. Одавде је јасно $x^m \equiv x^{m_r} \pmod{h(x)}$, јер $h(x) \mid x^r - 1$.

(в) Нека је $h(x)$ иредуцибилни фактор степена k полинома $\dfrac{x^r - 1}{x - 1}$. Тада је $\mathbb{F}_p[X]/h(x)$ поље са p^k елемената чија је мултипликативна група циклична са генератором $g(x)$. Према делу (а) ове теореме имамо

$$g(x)^{p^d} \equiv g(x^{p^d}) \pmod{g(x)},$$

па самим тим $p^d - 1$ дели ред $g(x)$. Значи $p^k - 1 \mid p^d - 1$, тј. $k \mid d$.
Приметимо да у $\mathbb{F}_p[X]/h(x)$ важи $x^r \equiv 1$, па и $r \mid p^k - 1$. Како је $o_r(p) = d$, то $d \mid k$. Значи $k = d$, што је и требало доказати. □

Први покушаји да се одреди формула за n-ти прост број били су у облику полинома. Један такав занимљив пример је и полином $x^2 + x + 31$, који је прост за све бројеве $0 \leqslant x \leqslant 29$. Следећи задатак ипак гарантује да је тражење формуле у овом облику на неки начин бесмислено:

Задатак 1. За сваки неконстантни полином $f(x) \in \mathbb{Z}[X]$, постоји бесконачно много природних бројева n тако да број $|f(n)|$ није прост.

Решење. Претпоставимо супротно. Нека $2 \mid \deg f$ (аналогно разматрамо и случај $2 \nmid \deg f$). Тада постоји природан број n такав да је $P(n) > 0$ и низ $\{P(m)\}_{m \geqslant n}$ растући. Сваки од чланова овог низа је прост, односно $P(m) = p_m$, и нека је $p_n = p$. Тада из

$$n + p - n \mid P(n + p) - P(n) = p_{n+p} - p,$$

па $p \mid p_{n+p}$. Међутим, то мора значити да је $p = p_{n+p}$, што је очигледна контрадикција. □

1.7 Дистрибуција простих бројева

Једно од класичних питања везаних за просте бројеве је како су они распоређени, тј. колико има простих бројева не већих од датог природног броја n. Ову функцију означићемо са $\pi(n)$. Следећа теорема даје једну лепу оцену за $\pi(n)$:

Теорема 1. За сваки природан број $n \geqslant 2$ важи

$$\frac{1}{6} \cdot \frac{n}{\log n} < \pi(n) < 6 \cdot \frac{n}{\log n}.$$

Доказ. Докажимо прво неједнакост

$$2^n \leqslant \binom{2n}{n} < 4^n. \qquad (*)$$

Десна неједнакост следи из биномног развоја $(1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} > \binom{2n}{n}$, док леву доказујемо математичком индукцијом. Како је $\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!}$, то је логаритмовањем лева стана неједнакости $(*)$ еквивалентна са

$$n \log 2 \leqslant \log(2n)! - 2 \log n!. \qquad (**)$$

Највећи степен броја p који дели $n!$ је $\alpha(p) = \sum_{k=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^k}\right]$, па је

$$\log n! = \sum_{p \leqslant n} \alpha(p) \cdot \log p.$$

Самим тим је $\log(2n)! - \log n! = \sum_{p\leqslant 2n} \sum_{k=1}^{\left[\frac{\log n}{\log p}\right]} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right) \cdot \log p$, па како је $[2x] - 2[x] \leqslant 1$, то је из неједнакости $(**)$ и претходне једнакости

$$n \log 2 \leqslant \sum_{p\leqslant 2n} \left(\sum_{k=1}^{\left[\frac{\log n}{\log p}\right]} 1 \right) \cdot \log p \leqslant \sum_{p\leqslant 2n} \log 2n = \pi(2n) \cdot \log 2n.$$

Последња неједнакост даје $\pi(2n) \geqslant \dfrac{2n}{\log 2n} \cdot \dfrac{\log 2}{2} > \dfrac{1}{4} \cdot \dfrac{2n}{\log 2n}$. Даље,

$$\pi(2n+1) \geqslant \pi(2n) > \frac{1}{4} \cdot \frac{2n}{\log 2n} > \frac{1}{6} \cdot \frac{2n+1}{\log(2n+1)},$$

где последња неједнакост важи јер је $\dfrac{2n}{2n+1} > \dfrac{2}{3}$, за $n \geqslant 2$. Овим неједнакостима доказана је лева страна почетне неједнакости.

Докажимо и десну страну неједнакости. Важи

$$\log(2n)! - \log n! = \sum_{p\leqslant 2n} \sum_{k=1}^{\left[\frac{\log n}{\log p}\right]} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right) \cdot \log p \geqslant \sum_{p\leqslant 2n} \left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right) \cdot \log p.$$

Како за сваки прост број $n < p < 2n$ важи $\left[\dfrac{2n}{p}\right] - 2\left[\dfrac{n}{p}\right] = 1$, то из претходне неједнакости добијамо

$$\log(2n)! - \log n! \geqslant \sum_{n<p\leqslant 2n} \log p.$$

Означимо са $\Lambda(n) = \sum_{p\leqslant n} \log p$. Претходна неједнакост заједно са $(*)$ даје

$$\Lambda(2n) - \Lambda(n) < n \log 4.$$

Специјално, уколико претходну теорему применимо за $n = 2^r$, добијамо $\Lambda(2^{r+1}) - \Lambda(2^r) < 2^r \log 4$. Сабирањем оваквих неједнакости за $r = 0, 1, \ldots, k$ добијамо неједнакост $\Lambda(2^{k+1}) < 2^{k+2} \log 2$. Самим тим за $2^k \leqslant n < 2^{k+1}$ важи

$$\Lambda(n) \leqslant \Lambda(2^{k+1}) < 2^{k+2} \log 2 < 4n \log 2.$$

Нека је $0 < \alpha < 1$. Како за сваки прост број $p > n^\alpha$ тривијално важи $\log p > \log n^\alpha$, то је

$$(\pi(n) - \pi(n^\alpha)) \cdot \log n^\alpha < \sum_{n^\alpha<p<n} \log p \leqslant \Lambda(n) < 4n \log 2,$$

односно

$$\pi(n) < \frac{4n\log 2}{\alpha \log n} + \pi(n^\alpha) < \frac{4n\log 2}{\alpha \log n} + n^\alpha = \frac{n}{\log n}\left(\frac{4\log 2}{\alpha} + \frac{\log n}{n^{1-\alpha}}\right).$$

Није тешко видети да функција $f(x) = \dfrac{\log x}{x^{1-\alpha}}$ достиже максимум за $x = e^{1/(1-\alpha)}$ и тај максимум је $\dfrac{1}{e(1-\alpha)}$. Одабиром $\alpha = \dfrac{2}{3}$ добијамо тражену неједнакост, тј.

$$\pi(n) < \frac{n}{\log n}\left(6\log 2 + \frac{3}{e}\right) < 6 \cdot \frac{n}{\log n}.$$

□

Претходна теорема даје нам горњу и доњу границу за $\pi(n)$. Следећа теорема даје тачно асимптотско понашање функције $\pi(n)$:

Теорема 2.

$$\lim_{n\to+\infty} \frac{\pi(n)\log n}{n} = 1.$$

Део 2

Брзи алгоритми за велике бројеве

Основни алгоритми за множење бројева са N цифара раде у времену $O(N^2)$. Иако су ови алгоритми довољно добри за „мале" бројеве, они нису погодни за рачунање са „великим" бројевима. У овом поглављу дајемо асимптотски значајно брже алгоритме за ова израчунавања.

2.1 Дискретна Фуријеова трансформација

Под „сигналом" подразумеваћемо коначан низ елемената из неког скупа, тј. сигнал је $x = (x_0, \ldots, x_{D-1})$, где је D дужина сигнала. Претпоставимо да су елементи сигнала x из неког алгебарског домена у коме постоји D^{-1} и нека је g примитивни D-ти корен у том домену (тј. $g^k = 1$ ако и само ако $D \mid k$). Тада можемо дефинисати дискретну Фуријеову[1] трансформацију ДФТ[2]:

Дефиниција 1. Дискретна Фуријеова трансформација сигнала x је сигнал $X = DFT(x)$ дат са

$$X_k = \sum_{j=0}^{D-1} x_j g^{-jk},$$

са инверзном трансформацијом $DFT^{-1}(X) = x$

$$x_k = \frac{1}{D} \sum_{j=0}^{D-1} X_j g^{jk}.$$

Познати примери ДФТ су:

(1) Комплексна ДФТ: $x, X \in \mathbb{C}^D$, g је D-ти корен из јединице, односно $g = e^{2\pi i/D}$;

[1] Jean Baptiste Joseph Fourier - француски математичар и физичар, 1768-1830

[2] discrete Fourier transformation

(2) ДФТ на коначним полима: $x, X \in \mathbb{F}_{p^k}^D$, g је D-ти корен из јединице у пољу;

Алгоритме који се заснивају на ДФТ називаћемо брзе Фуријеове трансформације, скраћено ФФТ[3]. Сама ФФТ базира се на следећем једноставном идентитету, уколико је D паран број:

$$DFT(x) = \sum_{j=0}^{D/2-1} x_{2j}(g^2)^{-jk} + g^{-k} \sum_{j=0}^{D/2-1} x_{2j+1}(g^2)^{-jk}.$$

Сада можемо дати рекурзивни ФФТ за сигнал x дужине $D = 2^d$:

Алгоритам 2.1 (ФФТ алгоритам)

$FFT(x)\{$
    $n = duzina(x)$;
    `if` $(n = 1)$ `vrati` x;
    $m = n/2$;
    $X = (x_{2j})_{j=0}^{m-1}$;
    $Y = (x_{2j+1})_{j=0}^{m-1}$;
    $X = FFT(X)$;
    $Y = FFT(Y)$;
    $U = (X_{k \bmod m})_{k=0}^{n-1}$;
    $V = (g^{-k} Y_{k \bmod m})_{k=0}^{n-1}$;
    `vrati` $U + V$;
}

Комплексност овог алгоритма је јасно $O(D \ln D)$.

2.2 Теорија конволуција

Нека су дата два сигнала x и y дужине D. Дефинишимо основне облике конволуција за њих:

Дефиниција 1. Циклична конволуција, у ознаци $z = x \times y$, дужине D дата је са

$$z_n = \sum_{i+j \equiv n \pmod D} x_i y_j.$$

Негациклична конволуција, у ознаци $v = x \times_- y$, дужине D дата је са

$$v_n = \sum_{i+j=n} x_i y_j - \sum_{i+j=n+D} x_i y_j.$$

[3]fast Fourier transformation

Ациклична конволуција, у ознаци $u = x \times_A y$, дужине $2D$ дата је са

$$u_n = \sum_{i+j=n} x_i y_j,$$

за $n \in \{0, 1, \ldots, 2D-2\}$ при чему је $u_{2D-1} = 0$.
Полу-циклична конволуција, у ознаци $x \times_H y$, дужине D састављена је од првих D елемената ацикличне конволуције u.

Одмах примећујмо да је производ два броја, који су дужине D у бази са основом B, једна ациклична конволуција дужине $2D$. Зато у наставку дајемо теореме које ће омогућити брзо рачунање конволуција. Нека је за два сигнала x и y дужине D са $z = x * y$ дат сигнал дужине D такав да је $z_n = x_n \cdot y_n$.

Теорема 1. Нека су x и y сигнали дужине D. Циклична конволуција ових сигнала задовољава једнакост

$$x \times y = DFT^{-1}(DFT(x) * DFT(y)),$$

тј.

$$(x \times y)_n = \frac{1}{D} \sum_{k=0}^{D-1} X_k Y_k g^{kn}.$$

Доказ. Из дефиниције ДФТ је

$$\frac{1}{D} \sum_{k=0}^{D-1} X_k Y_k g^{kn} = \frac{1}{D} \sum_{k=0}^{D-1} g^{kn} \sum_{i=0}^{D-1} x_i g^{-ik} \sum_{j=0}^{D-1} y_j g^{-jk} = \frac{1}{D} \sum_{i=0}^{D-1} \sum_{j=0}^{D-1} x_i y_j \sum_{k=0}^{D-1} g^{k(n-i-j)}.$$

Како је вредност $\sum_{k=0}^{D-1} g^{k(n-i-j)}$ једнака 0 када је $n \not\equiv i + j \pmod{D}$, а D када је $n \equiv i + j \pmod{D}$, то је

$$\frac{1}{D} \sum_{k=0}^{D-1} X_k Y_k g^{kn} = \sum_{i+j \equiv n} x_i y_j = (x \times y)_n.$$

□

Применом ФФТ алгоритама, ова теорема омогућује брзо рачунање цикличне конволуције. Следећом теоремом даћемо везу између различитих врста конволуција, што ће нам дати и брз алгоритам за множење бројева. При томе $z = x \pm y$ је сигнал такав да је $z_n = x_n \pm y_n$, док је $u = qx$, за константу q, сигнал такав да је $z_n = qx_n$. Такође, нека је $v = x \cup y$ спајање два сигнала од левог ка десном.

Теорема 2. Нека су x и y сигнали дужине D. Уколико у одговарајућем домену постоји 2^{-1} важе следеће везе између конволуција:

(а) $x \times_H y = \frac{1}{2}((x \times y) + (x \times_- y))$.

(б) $x \times_A y = (x \times_H y) \cup \frac{1}{2}((x \times y) - (x \times_- y))$.

Доказ. (а) Из дефиниција конволуција и основних операција над сигналима добијамо

$$\begin{aligned}\left(\frac{1}{2}((x \times y) + (x \times_- y))\right)_n &= \frac{1}{2}\left(\sum_{i+j=n} x_i y_j + \sum_{i+j=n+D} x_i x_j + \sum_{i+j=n} x_i y_j - \sum_{i+j=n+D} x_i y_j\right) \\ &= \sum_{i+j=n} x_i y_j,\end{aligned}$$

што је управо n-ти елемент конволуције $x \times_H y$.

(б) По дефиницији, првих D елемената сигнала $x \times_A y$ и $x \times_H y$ су једнаки, док за остале важи

$$\begin{aligned}\left(\frac{1}{2}((x \times y) - (x \times_- y))\right)_n &= \frac{1}{2}\left(\sum_{i+j=n} x_i y_j + \sum_{i+j=n+D} x_i x_j - \sum_{i+j=n} x_i y_j + \sum_{i+j=n+D} x_i y_j\right) \\ &= \sum_{i+j=n+D} x_i y_j = (x \times_A y)_{n+D},\end{aligned}$$

што је и требало доказати. □

Алгоритам 2.2. (ФФТ множење)

1. [Inicijalizacija]
   Dopuniti x i y nulama tako da su dužine $2D$, tako da ciklična konvolucija novih brojeva sadrži acikličnu prethodnih;
2. [Transformacije]
   $X = DFT(x)$;
   $Y = DFT(y)$;
   $Z = X * Y$;
   $z = DFT^{-1}(Z)$;
   $z = zaokruzhi(z)$; // Zaokružujemo elemente do najbližeg celog broja
3. [Prenos u bazi B]
   $prenos = 0$;
   for($0 \leqslant n < 2D$){
   $v = z_n + prenos$;
   $z_n = v \bmod B$;
   $prenos = [v/B]$;
   }
4. [Korekcije]
   Ako je $prenos > 0$ dodavanje te cifre kao vodeće;

```
Izbrisati vodeće nule;
vrati z;
```

Због заокруживања бројева, овај алгоритам може дати погрешан резултат, али је он од великог значаја, јер се изведени облици ФФТ множења базирају на њему.

Из комплексности ФФТ алгоритма закључујемо и да је комплексност овог алгоритма $O(D \ln D)$. Међутим, нас занима сложеност у односу на број цифара бројева које множимо. Показује се да је комплексност алгоритма, уколико множимо бројеве са n цифара

$$O(n(C \ln n)(C \ln \ln n) \cdots),$$

где је C константа, а множимо са $\ln \ln \ldots n$ све док је тај број већи од 1. Иако постоје алгоритми којима се множење може извршити у времену $O(n \ln n \ln \ln n)$, због спорог раста функција $\ln \ln \ln n$ комплексност овог алгоритма није много лошија. Овај (основни) облик ФФТ множења коришћен је приликом доказивања прималности неких од највећих познатих простих бројева.

Део 3

Брзи пробабилистички тестови прималности

Једна од основних подела тестови прималност је на *детерминистичке* и *пробабилистичке*. Код првих резултат теста је увек тачна вредност, док код других знамо само да је резултат тачан са неком вероватноћом. Иако су предности детерминистичких алгоритама јасне, у пракси се често примењују и пробабилистички алгоритми, јер је време њиховог извршавања често краће од времена извршавања детерминистичких алгоритама.

Постоји више типова пробабилистичких алгоритама. Алгоритми које ћемо користити у овом поглављу заснивају се на *проблему одлуке*, тј. резултат који ће давати може бити *да* или *не* (тј. PROST или SLOŽEN). Посебно, користићемо Монте-Карло алгоритме, чију дефиницију можемо дати са:

Дефиниција 2. „ДА-усмерен" Монте - Карло алгоритам је алгоритам за проблем одлуке код кога је одговор „да" увек тачан, али одговор „не" не мора бити. Кажемо да ДА-усмерен Монте - Карло алгоритам има вероватноћу грешке ϵ, ако за сваки улаз за који је одговор „да", алгоритам враћа вредност „не" са вероватноћом највише ϵ.

Коментар. Слично можемо дефинисати и „НЕ-усмерене" Монте-Карло алгоритме.

3.1 Соловеј - Штрасенов тест прималности

Први у низу пробабилистичких алгоритама које ћемо изложити у овом поглављу је алгоритам Соловеј[1] - Штрасена[2]. Он је базиран на Лежандровом[3] и Јакобијевом[4] симболу чије дефиниције и својства дајемо у првом делу овог потпоглавља.

[1]Robert Martin Solovay - амерички математичар 1938-
[2]Volker Strassen - немачки математичар 1936-
[3]Adrien-Marie Legendre - француски математичар 1752-1833
[4]Carl Gustav Jacob Jacobi - немачки математичар 1804-1851

3.1.1 Лежандров и Јакобијев симбол

Дефиниција 1. Нека је $n \in \mathbb{Z}$. За број a који није дељив са n кажемо да је квадратни остатак по модулу n ако конгурнција $x^2 \equiv a \pmod{n}$ има решења, а иначе кажемо да је квадратни неостатак.

Следећа теорема говори о броју квадратних остатака и неостатака по простим модулима:

Теорема 1. Нека је p непаран прост број. Број квадратних остатака и неостатака по модулу p једнак је $\frac{p-1}{2}$.

Доказ. Посматрајмо бројеве $1^2, 2^2, \ldots, (p-1)^2$. Јасно је да је сваки од њих квадратни остатак, па је довољно одредити колико међу овим бројевима има различитих. Нека је зато $x^2 \equiv y^2 \pmod{p}$, за неке $x, y \in \mathbb{F}_p$. Тада је $(x-y)(x+y) \equiv 0 \pmod{p}$, па је $x \equiv y \pmod{p}$ или $x \equiv -y \pmod{p}$. Значи, у скупу $\{x^2 \mid 1 \leqslant x \leqslant p-1\}$ по модулу p имамо парове једнаких, тј. укупан број квадратних остатака је $\frac{p-1}{2}$. Број квадратних неостатака је $p-1-\frac{p-1}{2} = \frac{p-1}{2}$. Овим је теорема у потпуности доказана. □

Уведимо сада и Лежандров симбол:

Дефиниција 2. Нека је p непаран прост број, а a цео број. Лежандров симбол $\left(\frac{a}{p}\right)$ дефинисан је са:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p \mid a \\ 1, & a \text{ је квадратни остатак} \\ -1, & a \text{ није квадратни остатак} \end{cases}$$

Следећа теорема, позната и као Ојлеров критеријум, биће нам од велике важности у наставку текста:

Теорема 2. (Ојлеров критеријум) За непаран прост број p важи

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

Доказ. Нека је g примитивни корен модула p и k број такав да је $g^k \equiv a \pmod{p}$. Тада је a квадратни остатак акко је k паран, па је $\left(\frac{a}{p}\right) = (-1)^k$. Са друге стране је $a^{\frac{p-1}{2}} \equiv g^{k \cdot \frac{p-1}{2}} \equiv (g^{\frac{p-1}{2}})^k \equiv (-1)^k \pmod{p}$, чиме је тврђење доказано. □

Основна својства Лежандровог симбола дајемо у следећој теореми:

Теорема 3. Нека је p непаран прост број. Тада важи:

(а) $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ и $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}$;

(б) Ако је $m_1 \equiv m_2 \pmod{p}$, тада $\left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right)$;

(в) $\left(\frac{m_1 m_2}{p}\right) = \left(\frac{m_1}{p}\right) \cdot \left(\frac{m_2}{p}\right)$;

Доказ.

(а) Прво тврђење следе из чињеница да је $1^2 = 1$, док је друго директна последица Ојлеровог критеријума. Треће тврђење доказаћемо нешто касније, у склопу доказа Гаусовог закона реципроцитета.

(б) Ово тврђење директно следи из дефиниције.

(в) Искористимо Ојлеров критеријум. Наиме,

$$\left(\frac{m_1 m_2}{p}\right) \equiv (m_1 m_2)^{\frac{p-1}{2}} = m_1^{\frac{p-1}{2}} m_2^{\frac{p-1}{2}} \equiv \left(\frac{m_1}{p}\right) \cdot \left(\frac{m_2}{p}\right) \pmod{p}.$$

□

Следећи задатак илуструје употребу квадратних остатака. Аутор је потписник овог текста.

Задатак 1. Одредити све парове x и n природних бројева такве да је

$$x^3 + 2x + 1 = 2^n.$$

Решење. Доказаћемо да је једино решење ове једначине пар $(1, 2)$. За $n = 1$ нема решење, па је довољно испитати случај $n \geqslant 3$.

Како је $x \cdot (x^2+2)$ увек дељиво са 3 то број n мора бити паран. Докажимо да за $n \geqslant 3$ број n не може бити ни паран.

Нека је n паран. Додавањем обема странама једнакости број 2 и растављањем добијамо $(x+1)(x^2-x+3) = 2^n+2$. Како десна страна једнакости за $n \geqslant 3$ није дељива са 4 то није ни лева, па је x облика $8k+1$ или $8k+5$. Уколико је x облика $8k+1$, добијамо да је лева страна једнакости конгруентна са 6 по модулу 8, што је очигледна контрадикција. Значи $x = 8k+5$, за неки цео број k. Како је n паран, то је и $2^n + 2 = 2(2y^2 + 1)$, па је -2 квадратни остатак по сваком простом непарном делиоцу броја $2^n + 2$, посебно по сваком непарном простом делиоцу броју $x^2 - x + 3$. Како је

$x = 8k + 5$, то је $x^2 - x + 3 \equiv_8 7$, па мора имати простог делиоца p облика $8s + 5$ или $8s + 7$. Међутим, тада је

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8} = (-1)^{(p-1)(p+5)/8} = -1,$$

одакле -2 није квадратни остатак по модулу p. Контрадикција. □

У наставку овог дела поглавља циљ нам је доказ Гаусовог[5] закона реципроцитета. Докажимо зато прво следећу теорему:

Теорема 4. (**Гаусова лема**) Нека је μ број остатака у скупу ak, $1 \leqslant k \leqslant \frac{p-1}{2}$, чија је вредност већа од $\frac{p-1}{2}$. Тада је

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

Доказ. Нека је $la \equiv \pm m_l \pmod p$, где је $1 \leqslant m_l \leqslant \frac{p-1}{2}$. Како $k \pm l \not\equiv 0 \pmod p$, за $1 \leqslant k < l \leqslant \frac{p-1}{2}$, то је $m_l \neq m_k$, за све $1 \leqslant k < l \leqslant \frac{p-1}{2}$. Значи $\left\{1, 2, \ldots, \frac{p-1}{2}\right\} = \{m_1, m_2, \ldots, m_{(p-1)/2}\}$, па множењем конгруенција $la \equiv m_l \pmod p$ добијамо

$$\left(\frac{p-1}{2}\right)! \cdot a^{(p-1)/2} \equiv \left(\frac{p-1}{2}\right)! \cdot (-1)^{\mu} \pmod p.$$

Тврђење сада следи на основу Ојлеровог критеријума. □

Следеће класично тврђење, можда и једно од најпознатијих тврђења теорије бројева, познато је као Гаусов закон реципроцитета:

Теорема 5. **(Гаусов закон реципроцитета)** За непарне просте бројеве p и q важи

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Доказ. Докажимо да за свака два броја x и y и непаран природан број n важи једнакост

$$x^n - y^n = \prod_{k=0}^{n-1}(\varsigma^k x - \varsigma^{-k} y), \qquad (*)$$

[5]Carl Friedrich Gauss - немачки математичар 1777-1855

где је $\varsigma = e^{2\pi i/n}$. Наиме, скуп $-2k$, за $0 \leqslant k \leqslant n-1$, чини потпун систем остатка по модулу n, па је $x^n - y^n = \prod_{k=0}^{n-1}(x - \varsigma^{-2k}y)$. Како је $\varsigma^{-(1+2+\ldots+n-1)} = \varsigma^{-n(n-1)/2} = 1$, то је

$$x^n - y^n = \prod_{k=0}^{n-1}(x - \varsigma^{-2k}y) = \prod_{k=0}^{n-1}(\varsigma^k x - \varsigma^{-k}y).$$

Нека је сада $f(z) = e^{2\pi iz} - e^{-2\pi iz}$. Докажимо да је

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) \cdot f\left(z - \frac{k}{n}\right). \qquad (**)$$

Према $(*)$ имамо да је

$$f(nz) = \prod_{k=0}^{n-1} f\left(z + \frac{k}{n}\right).$$

Како је $f(z + k/n) = f(z + k/n - 1) = f(z - (n-k)/n)$, то је

$$\begin{aligned}
\frac{f(nz)}{f(z)} &= \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) \cdot \prod_{k=(n+1)/2}^{n-1} f\left(z + \frac{k}{n}\right) \\
&= \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) \cdot \prod_{k=(n+1)/2}^{n-1} f\left(z - \frac{n-k}{n}\right) \\
&= \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right).
\end{aligned}$$

На крају докажимо да је

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right). \qquad (***)$$

Нека је $la \equiv \pm m_l \pmod p$, где је $1 \leqslant m_l \leqslant \dfrac{p-1}{2}$. Како се $\dfrac{la}{p}$ и $\pm\dfrac{m_l}{p}$ разликују за цео број, то је $f\left(\dfrac{la}{p}\right) = f\left(\pm\dfrac{m_l}{p}\right)$, па једнакост $(***)$ следи на основу Гаусове леме. Специјално, важи

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{lq}{p}\right) = \left(\frac{q}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Такође, према $(**)$ важи

$$\frac{f(ql/p)}{f(l/p)} = \prod_{k=1}^{(q-1)/2} f\left(\frac{l}{p}+\frac{m}{q}\right)\cdot f\left(\frac{l}{p}-\frac{m}{q}\right),$$

па је

$$\left(\frac{q}{p}\right) = \prod_{m=1}^{(q-1)/2}\prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}+\frac{m}{q}\right)\cdot f\left(\frac{l}{p}-\frac{m}{q}\right).$$

Слично је

$$\left(\frac{p}{q}\right) = \prod_{m=1}^{(q-1)/2}\prod_{l=1}^{(p-1)/2} f\left(\frac{m}{q}+\frac{l}{p}\right)\cdot f\left(\frac{m}{q}-\frac{l}{p}\right),$$

па како је $f(m/q-l/p) = -f(l/p-m/q)$, то је заиста

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Докажимо и последњи део Теореме 3(а). Користићемо Гаусову лему. Број μ једнак је броју елемената скупа $2\cdot 1, 2\cdot 2, \ldots, 2\cdot\dfrac{p-1}{2}$, који су већи од $\dfrac{p-1}{2}$. Јасно је:

(1) $\mu = 2k$ за $p = 8k+1$;
(2) $\mu = 2k+2$ за $p = 8k+7$;
(3) $\mu = 2k+1$ за $p = 8k+3$;
(4) $\mu = 2k+1$ за $p = 8k+5$.

Из претходног тврђење теореме је очигледно. □

Следећи задатак илуструје примену претходне теореме. Аутор задатка је потписник овог текста:

Задатак 2. Доказати да за просте бројеве p и q, такве да $4 \nmid p-q$ бројеви

$$p^q - 1 \quad \text{и} \quad q^p - 1,$$

не могу имати све исте просте делиоце.

Решење. Претпоставимо супротно.

Приметимо да бројеви p и q не могу бити једнаки 2, јер би тада један од p^q-1 и q^p-1 био паран, а други непаран, па не би имали све исте просте делиоце. Такође, по услову задатка p и q не могу давати исти остатак по модулу 4, па је један од њих нпр. q облика $4t+3$, а други облика $4u+1$.

Нека је r било који прост број који дели и q^p-1 и p^q-1. Претпоставимо да $r \mid q-1$ и да је h поредак броја p по модулу r. Тада $r \mid p^h-1$, па како $r \mid p^q-1$, то $h \mid q$. Значи или је $h=1$ или је $h=q$. Ако је $h=q$ из $h \mid r-1$

имамо да $q \mid r-1$, међутим ово је немогуће јер $r \mid q-1$. Значи $h=1$, тј. $r \mid p-1$. Претпоставимо још и да $r^\alpha \parallel p-1$. Како је $(r,q)=1$, то је и $r^\alpha \parallel p^q-1$. Разматрајући и све делиоце броја $q-1$ налазимо да се бројеви p^q-1 и q^p-1 могу записати као

$$p^q-1 = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}q_1^{\beta_1}q_2^{\beta_2}\dots q_l^{\beta_l}, \quad q^p-1 = p_1^{\gamma_1}p_2^{\gamma_2}\dots p_k^{\gamma_k}q_1^{\delta_1}q_2^{\delta_2}\dots q_l^{\delta_l},$$

где су p_i сви делиоци $p-1$ и при томе је и $p_i^{\alpha_i} \parallel p-1$, $p_i^{\gamma_i} \parallel q-1$, $p_i \neq q_j$. Посматрајмо сада делиоце q_i. Нека је поредак броја p по модулу q_i једнак s. Тада $q_i \mid p^q-1$ и $q_i \mid p^s-1$, па $s \mid q$. Како q_i није неки од делиоца броја $p-1$, то $h \neq 1$, тј. $h=q$. Значи $q \mid q_i-1$ и слично $p \mid q_i-1$, па како је $(p,q)=1$, то $pq \mid q_i-1$. Посматрајмо сада $q_i \mid q^p-1 \mid q^{p+1}-q$. Како је $p+1$ паран, то је број q квадратни остатак по модулу q_i, тј. $\left(\frac{q}{q_i}\right)=1$. Применом Гаусовог закона реципроцитета добијамо

$$\left(\frac{q}{q_i}\right) = \left(\frac{q_i}{q}\right)(-1)^{\frac{q-1}{2}\frac{q_i-1}{2}} = (-1)^{\frac{q_i-1}{2}},$$

јер је $q=4t+3$ и $q \mid q_i-1$. Значи сваки од бројева q_i мора бити облика $4v+1$. Сада је

$$\frac{p^q-1}{p-1} = q_1^{\beta_1}q_2^{\beta_2}\dots q_l^{\beta_l} \equiv_4 1.$$

Међутим, са друге стране имамо

$$\frac{p^q-1}{p-1} = p^{q-1}+p^{q-2}+\ldots+1 \equiv_4 q\cdot 1 \equiv_4 3,$$

што доводи до очигледне контрадикције. □

На неки начин уопштење Лежандровог симбола на све непарне бројеве је Јакобијев симбол:

Дефиниција 3. Нека су n и m природни бројеви, при чему је m непаран и $m = p_1^{a_1}p_2^{a_2}\cdot\ldots\cdot p_k^{a_k}$ његова канонска репрезентација. Тада је

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

Из дефиниције и Теорема 3 и 5, директно се изводи следећа теорема која даје основна својства Јакобијевог симбола:

Теорема 6. Нека су n и m природни бројеви, где је m непаран. Тада важи:

(а) $\left(\frac{1}{m}\right) = 1$, $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ и $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{2}}$;

(б) Ако је $n_1 \equiv n_2 \pmod{m}$, тада $\left(\frac{n_1}{m}\right) = \left(\frac{n_2}{m}\right)$;

(в) $\left(\frac{n_1 n_2}{m}\right) = \left(\frac{n_1}{m}\right) \cdot \left(\frac{n_2}{m}\right)$;

(г) Ако је и n непарни број важи

$$\left(\frac{n}{m}\right) \cdot \left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}.$$

□

На основу претходне теореме можемо дати и алгоритам за рачунање Јакобијевог симбола $\left(\frac{n}{m}\right)$:

Алгоритам 3.1. (Одређивање Јакобијевог симбола)

`if` $(n = 0)$ `vrati 0;`
`if` $(n = 1)$ `vrati 1;`
`if` $(n = -1)\{$
  `if` $(m \equiv 1 \pmod 4)$ `vrati 1;`
  `else vrati` -1`;`
$\}$
`if` $(n = 2)\{$
  `if` $(m \equiv 1 \pmod 8)$ `ili` $m \equiv 7 \pmod 8)$ `vrati 1;`
  `else vrati` -1`;`
$\}$
`if` $(n > m)$ `vrati` $\left(\frac{n \bmod m}{m}\right)$`;`
`if` $(2 \mid n)\{$
  `Zapiši` $n = 2^t \cdot k$`, gde` $2 \nmid t$`;`
  `vrati` $\left(\frac{k}{m}\right) \cdot \left(\frac{2}{m}\right)^t$`;`
$\}$
`if` $(n \equiv 3 \pmod 4$ `i` $m \equiv 3 \pmod 4)$ `vrati` $-\left(\frac{m}{n}\right)$`;`
`else vrati` $\left(\frac{m}{n}\right)$`;`

Теорема 7. Сложеност алгоритма за одређивање Јакобијевог симбола је $O(\ln^{2+\epsilon} m)$, за свако $\epsilon > 0$.

Доказ. Јасно је да се алгоритам извршава у највише $O(\ln m)$ корака. У сваком кораку одговарајућа операција се, коришћењем алгоритама из

претходног поглавља, може извршити у времену $O(\ln m \ln \ln m)$. Самим тим алгоритам се може извршити у времену $O(\ln^{2+\epsilon} m)$. □

3.1.2 Алгоритам и сложеност

У псеудо-коду Соловеј - Штрасенов тест прималности може се записати као:

Алгоритам 3.2. (Соловеј - Штрасенов тест прималности)
`Izabrati slučajan broj` a, $2 \leqslant a \leqslant n-1$;
$x = \left(\frac{a}{n}\right)$;
`if` $(x = 0)$ `ispiši SLOŽEN;`
$y = a^{\frac{n-1}{2}}$ `mod` n;
`if` $(x \equiv y \pmod{n})$ `ispiši PROST;`
`else ispiši SLOŽEN;`

Теорема 8. Соловеј - Штрасенов тест прималности је за сложене бројеве „ДА-усмерен" Монте-Карло алгоритам. Вероватноћа грешке је највише 0,5.
Доказ. Први део теореме је директна последица Ојлеровог критеријума, док други део теореме следи из чињенице да постоји највише пола квадратних остатака.

Следећа теорема показује да је овај алгоритам полиномијане сложености:

Теорема 9. Алгоритам Соловеј - Штрасена се може извршити у времену $O(\ln^{2+\epsilon} n)$, за све $\epsilon > 0$.
Доказ. Ова теорема је директна последица Теореме 7. □

Као и код већине пробабилистичких алгоритама, тестирање треба вршити више од једном, па је од интереса оценити вероватноћу да за неки (довољно велики) сложен број n алгоритам m пута узастопно испише PROST, тј. да m пута узастопно погреши. Ову оцену дајемо у следећој теореми:

Теорема 10. Вероватноћа да за непаран број n алгоритам m пута узастопно погреши је највише

$$\frac{\ln n}{\ln -2 + 2^{m+1}}.$$

Доказ. Нека је X догађај да је број сложен, а Y догађај да је алгоритам m пута узастопно исписао PROST. Према Теореми 8 је јасно $P\{Y \mid X\} \leqslant 2^{-m}$,

па је по формули за условну вероватноћи и Бајесовој формули

$$P\{X \mid Y\} = \frac{P\{Y \mid X\} \cdot P\{X\}}{P\{Y\}} = \frac{P\{Y \mid X\} \cdot P\{X\}}{P\{Y \mid X\} \cdot P\{X\} + P\{Y \mid \overline{X}\} \cdot P\{\overline{X}\}}. \qquad (*)$$

Одредимо $P\{X\}$. Нека је $N \leqslant n \leqslant 2N$. Према Теореми 1 из 1.7, број простих бројева између N и $2N$ се може апроксимирати са

$$\frac{2N}{\ln 2N} - \frac{N}{\ln N},$$

па како непарних бројева између N и $2N$ има $N/2$ то је

$$P\{X\} = 1 - 2\left(\frac{2}{\ln 2N} - \frac{1}{\ln N}\right) \approx 1 - \frac{2}{\ln N}.$$

Како је $P\{Y \mid \overline{X}\} \leqslant 1$, то је из једнакости $(*)$

$$P\{X \mid Y\} \approx \frac{P\{Y \mid X\}\left(1 - \frac{2}{\ln N}\right)}{P\{Y \mid X\}\left(1 - \frac{2}{\ln N}\right) + \frac{2}{\ln N}} \leqslant \frac{2^{-m}(\ln N - 2)}{2^{-m}(\ln N - 2) + 2} = \frac{\ln N - 2}{\ln N - 2 + 2^{m+1}}.$$

□

Из датог алгоритма јасно је да је за $m = 100$ вероватноћа грешке готово једнака нули, па је време потребно да би се овим алгоритмом утврдило да ли је неки број прост или не по Теореми 9 једнако $O(\ln^{2+\epsilon} n)$.

3.1.3 „Детерминистичка" верзија алгоритма

На крају овог поглавља показаћемо како се уз претпоставку Продужене Риманове[6] хипотезе Соловеј - Штрасенов алгоритам алгоритам може допунити до полиномиланог детерминистичког алгоритма. За почетак даћемо формулацију Риманове хипотезе:

Продужена Риманова хипотеза. Нека су n и a уазајмно прости природни бројеви. За свако ϵ важи

$$\pi(x, n, a) = \frac{\mathrm{li(x)}}{\varphi(n)} + O(x^{1/2+\epsilon}),$$

где је $\pi(x, n, a)$ број простих бројева не већих од x и $\equiv a \pmod{n}$, а $\mathrm{li}(x) = \int_2^x \frac{\mathrm{d}\, t}{\log t}$.

Под претпоставком Продужене Риманове хипотезе важе следеће теореме:

[6]Georg Friedrich Bernhard Riemann - немачки математичар 1826-1866

Теорема 11. Нека је

$$G(n) = \min\{x \mid \mathbb{Z}_n^* \text{ је генерисана простим бројевима } \leqslant x\}.$$

Тада је $G(n) = O((\log n)^2)$.

Теорема 12. Нека је G нетривијална подгрупа групе $\mathbb{Z}_n^*$. Тада постоји $m > 0$ и $m \notin G$, тако да је $m \leqslant 2(\log_2 n)^2$.

Следећа теорема, која такође важи под претпоставком Продужене Риманове хипотезе, биће основа детерминистичког алгоритма:

Теорема 13. Ако је n непаран сложен број, тада постоји природан број $a < n$ такав да је $a \leqslant 2(\log_2 n)^2$, за који је тачно барем једно од:
(1) $(a, n) \neq 1$;
(2) $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$.
Доказ. Нека је

$$E(n) = \left\{a \in \mathbb{Z}_n^* \mid \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}\right\}.$$

Докажимо да је $E(n)$ права подгрупа групе $\mathbb{Z}_n^*$. Претпоставимо супротно, тј. да је $E(n) = \mathbb{Z}_n^*$. Тада за свако $a \in \mathbb{Z}_n^*$ важи $1 = \left(\frac{a}{n}\right)^2 \equiv a^{n-1} \pmod{n}$. Претпоставимо да постоји непаран прост број тако да $p^2 \mid n$. Како је $\mathbb{Z}_{p^2}^*$ циклична то за њен генератор g важи $g^{p(p-1)} \equiv 1 \pmod{p^2}$, а из дате претпоставке $p(p-1) \mid n-1$. Међутим, $p \nmid n-1$, што доводи до очигледне контрадикције. Значи $n = pr$, где је p прост и $p \nmid r$. Сада ако g није квадрат у $\mathbb{Z}_p^*$, то према КТО постоји a тако да је $a \equiv g \pmod{p}$ и $a \equiv 1 \pmod{r}$. Међутим, за овако одабрано a важи

$$\left(\frac{a}{n}\right) = \left(\frac{g}{p}\right) \cdot \left(\frac{1}{r}\right) = -1,$$

па би морало да буде $a^{(n-1)/2} \equiv -1 \pmod{r}$, што је у контрадикцији са одабиром броја a. Овим је доказано да $E(n)$ мора бити права подгрупа групе $\mathbb{Z}_n^*$.

Сада, према Теореми 11, постоји $a \in \mathbb{Z}_n^* \setminus E(n)$ и $a = O((\log n)^2)$. Самим тим или $a \notin \mathbb{Z}_n^*$ (тј. $(a, n) \neq 1$) или $a \notin E(n)$. Према Теореми 12 важи $a \leqslant 2(\log_2 n)^2$, чиме је теорема у потпуности доказана. □

На основу претхоне теореме добијамо и детерминистички облик Соловеј - Штрасеновог алгоритма:

Алгоритам 3.3. (Детерминистички Соловеј - Штрасенов алгоритам)
`while` $(2 \leqslant a \leqslant \min\{n-1, 2(\log_2 n)^2\})\{$

$x = \left(\frac{a}{n}\right)$;
if ($x = 0$) ispiši SLOŽEN;
$y = a^{\frac{n-1}{2}} \bmod n$;
if ($x \not\equiv y \pmod n$) ispiši SLOŽEN;
}
ispiši PROST;

На основу Теореме 13 јасно је да је сложеност детерминистичког Соловеј - Штрасеновог алгоритма $O(\ln^{4+\epsilon} n)$.

3.2 Рабин-Милеров тест прималности

Пођимо од самог алгоритма:

Алгоритам 3.4. (Рабин[7] - Милеров[8] тест прималности)
Zapisati $n - 1 = 2^m \cdot t$, gde $2 \nmid t$;
Izabrati slučajan broj a, $2 \leqslant a \leqslant n - 1$;
$b = a^t \bmod n$;
if ($b = 1$) ispiši PROST;
for ($0 \leqslant i \leqslant m - 1$){
if ($b \equiv -1 \pmod n$) ispiši PROST;
else $b = b^2 \bmod n$;
}
ispiši SLOŽEN;

Теорема 1. Рабин-Милеров тест прималности је за сложене бројеве „ДА-усмерен" Монте-Карло алгоритам. Вероватноћа грешке је највише 0,25.
Доказ. Довољно је доказати да алгоритам не може исписати SLOŽEN за прост број n. У супротном, из алгоритма закључујемо да $a^t \not\equiv 1 \pmod n$ и да нити један од бројева a^t, $a^{2\cdot t}$, ..., $a^{2^{m-1}\cdot t}$ није конгруентан са -1 по модулу n. Са друге стране, из Мале Фермаове теореме је $a^{2^m \cdot t} \equiv 1 \pmod n$, па је $a^{2^m \cdot t} - 1 = (a^{2^{m-1}t} - 1)(a^{2^{m-1}t} + 1) \equiv 0 \pmod n$, односно

$$a^{2^{m-1}t} \equiv 1 \pmod n \qquad \text{или} \qquad a^{2^{m-1}t} \equiv -1 \pmod n.$$

Како друга конгруенција по претпоставци не важи, то мора бити $a^{2^{m-1}\cdot t} \equiv 1 \pmod n$. Настављајући овај поступак добијамо да је $a^{2^i \cdot t} \equiv 1 \pmod n$, за све $0 \leqslant i \leqslant m$. Међутим, ово је немогуће јер је по претпоставци $a^t \not\equiv 1 \pmod n$. Овим је први део тврђења доказан.

[7] Gary Miller - амерички информатичар
[8] Michael Oser Rabin - израелски информатичар 1931-

Доказимо и други део тврђења. Нека је n непаран сложен број, $n-1 = 2^m t$ где $2 \nmid t$ и

$$S(n) = \{a \in \mathbb{Z}_n^* \mid a^t \equiv 1 \pmod{n} \text{ или } a^{2^r \cdot t} \equiv -1 \pmod{n}, \text{ за неко } 0 \leqslant r < m\}.$$

Довољно је доказати да је $|S(n)| \leqslant \dfrac{n-1}{4}$.

Нека је k највећи број такав да постоји b тако да је $b^{2^k} \equiv -1 \pmod{n}$ (k је добро дефинисано, јер је $(-1)^{2^0} = -1$) и нека је $n' = 2^k \cdot t$. Такође, нека је $n = p_1^{a_1} p_2^{a_2} \dots p_j^{a_j}$. Како је $p_i \equiv 1 \pmod{2^{k+1}}$, то је $n \equiv 1 \pmod{2^{k+1}}$ и самим тим $2n' \mid n-1$.

Посматрајмо скупове $J = \{a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \pmod{n}\}$, $K = \{a \in \mathbb{Z}_n^* \mid a^{n'} \equiv \pm 1 \pmod{p_i^{a_i}} \text{ за све } i\}$, $L = \{a \in \mathbb{Z}_n^* \mid a^{n'} \equiv \pm 1 \pmod{n}\}$, $M = \{a \in \mathbb{Z}_n^* \mid a^{n'} \equiv 1 \pmod{n}\}$. Јасно су J, K, L, M подгрупе групе $\mathbb{Z}_n^*$ и важи $M \subset L \subset K \subset J \subset \mathbb{Z}_n^*$. Како је $S(n) \subset L$, довољно је доказати да је индекс групе L у $\mathbb{Z}_n^*$ барем 4.

Како је $[K : M] = 2^j$ и $[L : M] = 2$, то је $[K : L] = 2^{j-1}$. Размотримо следећа три случаја:
(1) $j \geqslant 3$. Како је $[\mathbb{Z}_n^* : L] \geqslant [\mathbb{Z}_n^* : J] \cdot [K : L] \geqslant 4$, то је у овом случају тврђење доказано.
(2) $j = 2$. Докажимо да је J права подгрупа групе $\mathbb{Z}_n^*$. Уколико је супротно томе $\mathbb{Z}_n^* = J$ из доказа Теореме 13 закључујемо да n није дељив квадратом, па је $n = pq$, где су $p > q$ неки прости бројеви. Међутим, ако је g генератор $\mathbb{Z}_p^*$ и $g^{n-1} \equiv 1 \pmod{p}$, то $p-1 \mid n-1$, односно $p-1 \mid q-1$. Ово је немогуће, јер је $p-1 > q-1$. Значи $[\mathbb{Z}_n^* : J] \geqslant 2$, па $[\mathbb{Z}_n^* : L] \geqslant [\mathbb{Z}_n^* : J] \cdot [K : L] \geqslant 4$, што је и требало доказати.
(3) $j = 1$. У овом случају је $n = p^a$, за $a \geqslant 2$. Међутим, како је $a^{n-1} \equiv a^{p-1} \pmod{p^2}$, то је $|J| = p-1$, а самим тим $[\mathbb{Z}_n^* : J] = p^{a-1} \geqslant 2$, односно $[\mathbb{Z}_n^* : L] \geqslant 4$. □

Следећа теорема показује да је Рабин - ов тест исте сложености као и Соловеј - Штрасенов:

Теорема 2. Алгоритам Рабин - Милеров се може извршити у времену $O(\ln^{2+\epsilon} n)$. □

Слично као у претходном поглављу можемо доказати да важи:

Теорема 3. Вероватноћа да за непаран број n алгоритам m пута узастопно погреши је највише

$$\frac{\ln n}{\ln -2 + 2 \cdot 4^m}.$$

□

Из доказа Теореме 1 закључујемо да је L права подгупа групе $\mathbb{Z}_n^*$. Самим тим, уз претпоставку Продужене Риманове хипотезе, коришћењем Теореме 13 из претходног поглавља, Рабин-Милеров тест се на сличан начин као и Соловеј-Штрасенов тест може допунити до детерминистичког.

Како због мање вероватноће грешке, лакшег кода, а и из других разлога, у пракси се Рабин - Милеров тест показује као бољи него тест Соловеј - Штрасена.

Део 4

Тест прималности помоћу Гаусових сума

У овом поглављу представићемо детерминистички тест који је 1981. године открио Ленстра[1]. Време рада овог алгоритма је ограничено одозго са $(\ln n)^{c \ln\ln\ln n}$ за неку константу c, па с обзиром на спори раст функције $\ln\ln\ln n$ може се рећи да је време рада $(\ln n)^{O(1)}$, односно да је алгоритам „скоро" полиномијалне сложености.

4.1 Карактери и Гаусове суме

Мултипликативни карактер на $\mathbb{F}_p^*$ је пресликавање $\chi : \mathbb{F}_p^* \to \mathbb{C}\backslash\{0\}$ које задовољава услов

$$\chi(ab) = \chi(a) \cdot \chi(b), \qquad \text{за све } a, b \in \mathbb{F}_p^*.$$

Некада је згодно проширити χ на $\mathbb{F}_p$ узимањем да је $\chi(0) = 0$.

Један од класичних примера карактера је Лежандров симбол $\chi(a) = \left(\frac{a}{p}\right)$.

Други (тривијални) пример карактера је $\varepsilon(a) = 1$ за све $a \in \mathbb{F}_p^*$. Није тешко доказати да сваки карактер има следећа својства:

Теорема 1. Нека је χ мултипликативни карактер и $a \in \mathbb{F}_p^*$. Тада важи:

(а) $\chi(1) = 1$;

(б) $\chi(a)$ је $(p-1)$-ви корен јединице;

(в) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

(г) ако је $\chi \neq \varepsilon$, тада $\sum_{t \in \mathbb{F}_p} \chi(t) = 0$.

[1]Hendrik Willem Lenstra - холандски математичар 1949-

Доказ. (а) Из дефиниције је $\chi(1)\cdot\chi(1)=\chi(1)$, па је јасно $\chi(1)=1$.
(б) Нека је g примитивни корен по модулу p. Како је $g^{p-1}=1$, из мултипликативности χ добијамо $1=\chi(1)=\chi(g^{p-1})=\chi(g)^{p-1}$, па је $\chi(g)$ јасно $(p-1)$-ви корен из јединице. Како за свако $a\in\mathbb{F}_p^*$ постоји природан број k тако да је $a=g^k$, то је $\chi(a)=\chi(g^k)=\chi(g)^k$, па је и $\chi(a)$ $(p-1)$-ви корен из јединице.
(в) Имамо $\chi(a^{-1})=\chi(a^{p-1-1})=\chi(a)^{p-2}=\chi(a)^{-1}$, а како је $|\chi(a)|=1$, јер је $\chi(a)$ корен јединице, то је и $\chi(a)^{-1}=\overline{\chi(a)}$.
(г) Из доказа дела под (б) закључујемо да је

$$\sum_{t\in\mathbb{F}_p}\chi(t)=\sum_{k=0}^{p-1}\chi(g^k)=\sum_{k=0}^{p-2}\chi(g)^k=\frac{\chi(g)^{p-1}-1}{\chi(g)-1}=0.$$

□

Уведимо на скупу свих карактера множење: за карактере χ и λ карактер $\chi\lambda$ дефинишимо са $(\chi\lambda)(a)=\chi(a)\cdot\lambda(a)$. Такође, можемо увести и инверз карактера χ^{-1} са $\chi^{-1}(a)=\chi(a)^{-1}$, за $a\in\mathbb{F}_p^*$. Овако дефинисана структура је група, тачније:

Теорема 2. Група карактера је циклична група реда $p-1$. За сваки броја $a\in\mathbb{F}_p^*$, $a\neq 1$, постоји карактер χ тако да је $\chi(a)\neq 1$.
Доказ. Посматрајмо функцију $\chi(g^k)=\varsigma_{p-1}^k$, где је $\varsigma_{p-1}=e^{2\pi i/(p-1)}$, а g примитивни корен по модулу p. Јасно је да је χ мултипликативни карактер и да је $\chi(a)\neq 1$, за све $a\neq 1$, па је други део теореме доказан. Такође, из доказа Теореме 1 закључујемо да је $\lambda(g)=\varsigma_{p-1}^l$, за сваки карактер λ и неки природан број l, па је јасно $\lambda=\chi^l$. Овим је доказано да је група карактера циклична са генератором χ, а како је $\chi(g)^{p-1}=\chi(g^{p-1})=1$, то је њен ред $p-1$. □

Уведимо и појам Гаусове суме:

Дефиниција. Нека је p прост број, $a\in\mathbb{F}_p$ и χ карактер на $\mathbb{F}_p$. Израз

$$G_a(\chi)=\sum_{t\in\mathbb{F}_p}\chi(t)\varsigma_p^{at},$$

где је $\varsigma_p=e^{2\pi i/p}$ назива се Гаусова сума на $\mathbb{F}_p$ која одговара карактеру χ.

Следећа теорема показује како се свака Гаусова сума $G_a(\chi)$ може представити преко Гаусове суме $G_1(\chi)$:

Теорема 3. За карактер χ и $a\in\mathbb{F}_p$ важи

$$G_a(\chi)=\begin{cases}\chi(a^{-1})\cdot G_1(\chi), & \text{ако је } a\neq 0 \text{ и } \chi\neq\varepsilon;\\ 0, & \text{ако је } a\neq 0 \text{ и } \chi=\varepsilon;\\ 0, & \text{ако је } a=0 \text{ и } \chi\neq\varepsilon;\\ p, & \text{ако је } a=0 \text{ и } \chi=\varepsilon\end{cases}.$$

Доказ. Уколико је $\chi = \varepsilon$ имамо $G_a(\chi) = \sum_{t\in\mathbb{F}_p} \varsigma_p^{at}$, а ова сума је 0 када је $a \neq 0$, односно p када је $a = 0$. Уколико је $a = 0$ и $\chi \neq \varepsilon$ по делу (г) Теореме 1 важи $G_a(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t) = 0$.
Испитајмо и случај $a \neq 0$ и $\chi \neq \varepsilon$. Тада је

$$G_a(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t)\cdot\varsigma_p^{at} = \sum_{t\in\mathbb{F}_p} \chi(a^{-1})\chi(at)\cdot\varsigma_p^{at} = \chi(a^{-1})\cdot G_1(\chi),$$

где последња једнакост важи јер бројеви at, за $0 \leqslant t \leqslant p-1$, чине потпун систем остатака по модулу p. □

Због претходне теореме уводимо ознаку $G_1(\chi) = G(\chi)$. Следећа теорема показује да је у нетривијалним случајевима вредност $|G(\chi)|$ (па самим тим и $|G_a(\chi)|$) једнака $\sqrt{p}$, односно:

Теорема 4. За $\chi \neq \varepsilon$ важи $|G(\chi)| = \sqrt{p}$.
Доказ. Израчунаћемо вредност израза $S = \sum_{a\in\mathbb{F}_p} G_a(\chi)\overline{G_a(\chi)}$ на два начина.
Према претходној теореми за $a \neq 0$ важи $\overline{G_a(\chi)} = \overline{\chi(a^{-1})G(\chi)} = \chi(a)\overline{G(\chi)}$ и $G_a(\chi) = \chi(a^{-1})G(\chi)$. Самим тим је $G_a(\chi)\overline{G_a(\chi)} = |G(\chi)|^2$ и како је $G_0(\chi) = 0$ закључујемо да је

$$\sum_{a\in\mathbb{F}_p} G_a(\chi)\overline{G_a(\chi)} = (p-1)\cdot|G(\chi)|^2.$$

Са друге стране, из дефиниције $G_a(\chi)$ закључујемо да је

$$\begin{aligned} S &= \sum_{a\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_p^*}\sum_{y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\varsigma_p^{ax-ay} = \sum_{x\in\mathbb{F}_p^*}\sum_{y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\sum_{a\in\mathbb{F}_p}\varsigma_p^{ax-ay} \\ &= \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\delta(x,y)p = p(p-1), \end{aligned}$$

где претпоследњу једнакост важи, јер скуп $\{a(x-y)\,|\,0 \leqslant a \leqslant p-1\}$ чини потпун систем остатака по модулу p ако и само ако је $x \neq y$. Овде је δ Кронекерова функција ($\delta(x,x) = 1$ и $\delta(x,y) = 0$ за $x \neq y$).
Из два представљања дате суме лако налазимо да је $|G(\chi)| = \sqrt{p}$. □

У алгоритму који ће овде бити изложен од великог значаја биће карактери $\chi_{p,q}$ на $\mathbb{F}_q$ дефинисани са $\chi_{p,q}(g_q) = \varsigma_p$, где су p и q прости бројеви такви да $p \mid q-1$, g_q примитивни корен по модулу q и $\varsigma_p = e^{2\pi i/p}$. Одговарајућу Гаусову суму означаваћемо са $G(p,q)$, односно $G(p,q) = \sum_{t\in\mathbb{F}_q} \chi_{p,q}(t)\cdot\varsigma_q^t$.
Доказаћемо и следећу теорему која ће представљати основу алгоритма:

Теорема 5. Нека су p, q и n прости бројеви, такви да $p \mid q-1$ и $(pq, n) = 1$. Тада је

$$G(p,q)^{n^{p-1}-1} \equiv \chi_{p,q}(n) \pmod{n}.$$

Доказ. Приметимо прво да уколико је $k \equiv l \pmod{p}$, да је и $\chi(m)^k = \chi(m)^l$, јер је $\chi(m)$ степен p-тог корена из јединице. Такође, важи $(a+b)^n \equiv a^n + b^n \pmod{n}$, а из Мале Фермаове теореме и $n^{p-1} \equiv 1 \pmod{p}$, па добијамо следећи низ конгруенција и једнакости

$$\begin{aligned} G(p,q)^{n^{p-1}} &= \left(\sum_{t\in\mathbb{F}_q} \chi(t)\varsigma_q^t\right)^{n^{p-1}} \equiv \sum_{t\in\mathbb{F}_q} \chi(t)^{n^{p-1}} \varsigma_q^{t\cdot n^{p-1}} = \sum_{t\in\mathbb{F}_q} \chi(t)\varsigma_q^{t\cdot n^{p-1}} \\ &= \chi(n^{-(p-1)}) \sum_{t\in\mathbb{F}_q} \chi(t\cdot n^{p-1}) \cdot \varsigma_q^{t\cdot n^{p-1}} = \chi(n)\cdot G(p,q) \pmod{n}, \end{aligned}$$

где последња једнакост следи из $\chi(n^{-(p-1)}) = \chi(n)$ и чињенице да бројеви $t \cdot n^{p-1}$, за $0 \leqslant t \leqslant q-1$, чине потпун систем остатака по модулу q, јер је $(p,n) = 1$. Дељењем добијамо тражену конгруенцију. □

На крају наведимо и једну теорему која није директно повезана са карактерима и Гаусовим сумама, али која ће нам бити корисна у доказу исправности алгоритма:

Теорема 6. Ако су m и n природни бројеви при чему $n \nmid m$, тада из $\varsigma_m^j \equiv \varsigma_m^k \pmod{n}$ следи $\varsigma_m^j = \varsigma_m^k$.

Доказ. Уколико поделимо конгруенцију и дату једнакост са ς_m^k, јасно је да је дати проблем довољно решити у случају $k = 0$. Претпоставимо да тада тврђење не важи, тј. да је $\varsigma_m^j \equiv 1 \pmod{n}$ и да $\varsigma_m^j \neq 1$. Посматрајмо полином $P(x) = \dfrac{x^m-1}{x-1} = \prod_{i=1}^{m-1}(x-\varsigma_m^i)$. Како $\varsigma_m^j \neq 1$, то постоји $1 \leqslant i \leqslant m-1$, тако да је $\varsigma_m^j = \varsigma_m^i$, па из дате конгрунције важи $n \mid P(1) = m$, што је супротно претпоставци да n не дели m. □

4.2 Алгоритам, доказ исправности и сложеност

Детерминистички тест преко Гаусових сума може се описати на следећи начин:

Алгоритам 4.1. (Тест прималности Гаусовим сумама)

1. `[Priprema]`
   $I = 0$; $F = 1$;

while($F^2 \leqslant n$){
$I = I + 2$;
Isprobavanjem predstaviti I kao proizvod različitih
prostih delioca;
F je proizvod svih prostih q takvih da $q-1 \mid I$;
}
if (n je prost delilac od IF) ispiši PROST;
if ((n,IF)>1) ispiši SLOŽEN;
for (prost $q \mid F$) naći najmanji primitivni koren g_q od q;

2. [Određivanje stepena]
for (prost $p \mid I$) predstaviti $n^{p-1} - 1 = p^{s_p} u_p$ gde $p \nmid u_p$;
for (prosti p, q takvi da $p \mid I$, $q \mid F$, $p \mid q-1$){
Odrediti najmanji broj $\omega(p,q) \leqslant s_p$ tako da

$$G(p,q)^{p^{\omega(p,q)} u_p} \equiv \varsigma_p^j \pmod{n} \quad \text{za neki ceo broj } j;$$

if (broj $\omega(p,q)$ ne postoji) ispiši SLOŽEN;
}

3. [Traženje najvećeg stepena]
for (prost $p \mid I$) neka je $\omega(p)$ maksimum od svih $w(p,q)$ za sve $q \mid F$,
gde $p \mid q-1$ i neka je $q_0(p)$ minimalno q za koje je $\omega(p) = \omega(p,q)$;
for (prosti p, q takvi da $p \mid I$, $q \mid F$, $p \mid q-1$) odrediti ceo
broj $l(p,q) \in [0, p-1]$ tako da je

$$G(p,q)^{p^{\omega(p)} u_p} \equiv \varsigma_p^{l(p,q)} \pmod{n};$$

4. [Test uzajamne prostosti sa n]
for (prost $p \mid I$, $\omega(p) \geqslant 2$ i $l(p,q) = 0$ uvek kada $q \mid F$, $p \mid q-1$){
for ($0 \leqslant j < p$){
if ($(G(p, q_0(p))^{p^{\omega(p)-1} u_p} - \varsigma_p^j, n) \neq 1$) ispiši SLOŽEN;
}
}

5. [Traženje delioca]
for (prost $q \mid F$) pomoću Kineske teoreme o ostacima odrediti ceo broj
$l(q)$ tako da je

$$l(q) \equiv l(p,q) \pmod{p} \quad \text{za sve } p \mid q-1;$$

Pomoću Kineske teoreme o ostacima odrediti ceo broj l tako da je

$$l \equiv g_q^{l(q)} \pmod{q} \quad \text{za sve proste } q \mid F;$$

for ($1 \leqslant j < I$)
if (l^j mod F netrivijalni delilac od n) ispiši SLOŽEN;

```
ispiši PROST;
```

Следеће две теореме доказују да је алгоритам заиста детерминистички:

Теорема 1. Уколико је број n прост алгоритам исписује PROST.
Доказ. Нека је n прост број. Јасно је да у делу Припрема не може доћи до исписа SLOŽEN, јер је тада $(n, IF) > 1$, а $I, F < n$. Такође, до исписа SLOŽEN не може доћи ни у делу Одређивање степена, што следи из Теореме 5 претходног дела поглавља. Даље, у делу Тест узајамне простости са n не може доћи до исписа SLOŽEN, јер би тада постојао делилац броја n који би због начина одабира бројева $\omega(p)$ и $\omega(p, q)$ био мањи од n. Коначно, како је јасно да ни у делу Тражење делиоца не може доћи до исписа SLOŽEN (тада би n имао нетривијалног делиоца), за прост број n алгоритам исписује PROST. □

Теорема 2. Уколико је број n сложен алгоритам исписује SLOŽEN.
Доказ. Претпоставимо супротно, тј. да је за сложен број n алгоритам исписао PROST. Нека је r најмањи прост делилац броја n. Докажимо да

$$p^{\omega(p)} \mid r^{p-1} - 1.$$

Према Малој Фермаовој теореми тврђење је тачно за $\omega(p) = 1$, па можемо да претпоставимо да је $\omega(p) \geqslant 2$. Нека је прво $l(p, q) \neq 0$. Како $r \mid n$, то је

$$G(p, q)^{p^{\omega(p)} u_p} \equiv \varsigma_p^{l(p,q)} \not\equiv 1 \pmod{r},$$

па степеновањем на p добијамо да је поредак броја $G(p, q)$ по модулу r дељив са $p^{\omega(p)+1}$. Са друге стране, према Теореми 5 претходног дела поглавља, поредак дели $p \cdot (r^{p-1} - 1)$, чиме је тврђење у случају $l(p, q) \neq 0$ доказано. Уколико је $l(p, q) = 0$, то из делова Одређивање степена и Тест узајамне простости са n добијамо да поредак броја $G(p, q)$ по модулу r дели $p^{\omega(p)} u_p$ и да није једнак $p^{\omega(p)-1} u_p$, па самим тим мора бити дељив са $p^{\omega(p)}$. Поновним коришћењем Теореме 5 претходног дела поглавља и из дела Тест узајамне простости са n закључујемо да поредак дели $r^{p-1} - 1$, па је тврђење и у овом случају доказано.

Доказана дељивост показује да за сваки прост број $p \mid I$ постоје бројеви a_p и b_p такви да је

$$\frac{r^{p-1} - 1}{p^{\omega(p)} u_p} = \frac{a_p}{b_p}, \qquad b_p \equiv 1 \pmod{p}.$$

Из Кинеске теореме о остацима, одредимо a тако да је $a \equiv a_p \pmod{p}$, за све $p \mid I$ и докажимо да је

$$r \equiv l^a \pmod{F}.$$

Из конструкције бројева $l(q)$ и l у делу Тражење делиоца, добијамо низ конгруенција

$$G(p,q)^{p^{\omega(p)}u_p} \equiv \varsigma_p^{l(p,q)} \equiv \varsigma_p^{l(q)} \equiv \chi_{p,q}(g_q^{l(q)}) \equiv \chi_{p,q}(l) \pmod{n}.$$

Даље, према Теореми 5 претходног дела поглавља и конструкцији броја b_p добијамо

$$\chi_{p,q}(r) = \chi_{p,q}(r)^{b_p} \equiv G(p,q)^{(r^{p-1}-1)\cdot b_p} \equiv G(p,q)^{p^{\omega(p)}u_p a_p} \equiv \chi_{p,q}(l)^{a_p} = \chi_{p,q}(l^a) \pmod{r},$$

па на основу Теореме 6 важи $\chi_{p,q}(r) = \chi_{p,q}(l^a)$ за све $q \mid F$ и $p \mid q-1$. Самим тим, ако је $r \equiv g_q^{\rho_q} \pmod{q}$ и $l \equiv g_q^{l(q)} \pmod{q}$, то је $\rho_q \equiv l(q)a \pmod{p}$. Међутим, ово важи за све просте делиоце p броја $q-1$, па како је $q-1$ делилац бесквадратног броја I, то је и $q-1$ бесквадратан и самим тим $\rho_q \equiv l(q)a \pmod{q-1}$. Сада је јасно и $g_q^{\rho_q} \equiv g_q^{l(q)a} \pmod{q}$, па је $r \equiv l^a \pmod{q}$. Како је F бесквадратан, то је и $r \equiv l^a \pmod{F}$.

Међутим, ово је немогуће, јер би у кораку Тражење делиоца због $F > \sqrt{n} \geqslant r$ (r је најмањи прост делилац од n) дошло до исписа SLOŽEN. Овим је тврђење у потпуности доказано. □

Теорема 3. Време рада алгоритма ограничено је одозго са $(\ln n)^{c \ln\ln\ln n}$ за неку константу c.

Доказ. Како је време рада алгоритма ограничено са неким степеном броја I, то је ово тврђење директна последица следеће теореме из аналитичке теорије бројева:

Теорема 4. Нека је $I(x)$ најмањи бесквадратан природан број I, тако да је производ свих простих бројева p са $p-1 \mid I$ већи од x. Тада постоји број c такав да је $I(x) < (\ln x)^{c \ln\ln\ln x}$, за све $x > 16$.

4.3 Јакобијеве суме и могућност побољшања алгоритма

У претходном делу овог поглавља дат је асимптотски веома брз алгоритам, али је он далеко од практичног. Највећи проблем је што се све операције врше у прстену $\mathbb{Z}[\varsigma_{p^k}, \varsigma_q]$. Ово се може поправити коришћењем Јакобијевих сума:

Дефиниција 1. Ако су χ и λ карактери на $\mathbb{F}_p$ израз

$$J(\chi,\lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$$

називамо Јакобијева сума.

Одмах можемо приметити да је $J(\chi,\lambda) \in \mathbb{Z}_p[\varsigma_n]$, где $n \mid \varphi(p)$. Ово ће бити кључно за побољшање алгоритма, јер је рачунање у прстену $\mathbb{Z}[\varsigma_n]$ знатно лакше него у прстену $\mathbb{Z}[\varsigma_n, \varsigma_m]$.

Следећа теорема даје основна својства Јакобијевих сума:

Теорема 1. Нека су χ и λ нетривијални карактери на $\mathbb{F}_p$. Тада важи:

(а) $J(\varepsilon,\varepsilon) = p$;

(б) $J(\varepsilon,\chi) = 0$;

(в) $J(\chi,\chi^{-1}) = -\chi(-1)$;

(г) $J(\chi,\lambda) = \dfrac{G(\chi)G(\lambda)}{G(\chi\lambda)}$.

Доказ. Део под (а) је тривијалан, док део (б) следи из Теореме 1(а). Докажимо преостале делове.
(в) Из дефиниције добијамо

$$J(\chi,\chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{a\neq 0} \chi\left(\frac{a}{1-a}\right).$$

Ако је $c = \dfrac{a}{1-a}$ и $c \neq -1$, то је $a = \dfrac{c}{1+c}$, па самим тим када a пролази скупом $\mathbb{F}_p \setminus \{0\}$, тада c пролази скупом $\mathbb{F}_p \setminus \{-1\}$. Сада, на основу Теореме 1(а)

$$J(\chi,\chi^{-1}) = \sum_{c\neq -1} \chi(c) = -\chi(-1).$$

(г) Приметимо да је

$$\begin{aligned} G(\chi)G(\lambda) &= \left(\sum_x \chi(x)\varsigma^x\right)\left(\sum_y \lambda(y)\varsigma^y\right) = \sum_{x,y} \chi(x)\lambda(y)\varsigma^{x+y} \\ &= \sum_t \left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\varsigma^t. \end{aligned}$$

Ако је $t = 0$ имамо $\sum_{x+y=0} \chi(x)\lambda(y) = \sum_x \chi(x)\lambda(-x) = \lambda(-1)\sum_x \chi\lambda(x) = 0$ $(\chi\lambda \neq \varepsilon)$. Ако $t \neq 0$ сменом $x = tx'$ и $y = ty'$ добијамо

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi\lambda(t)J(\chi,\lambda).$$

Сумирањем по t добијамо тражену формулу. □

Директно из Теореме 4 следи и следеће тврђење:

Теорема 2. Ако су χ, λ и $\chi\lambda$ различити од ε важи $|J(\chi,\lambda)| = \sqrt{p}$. □

Нека је G Галоаова група раширења $\mathbb{Q}(\varsigma_n)$ поља $\mathbb{Q}$. Тада је

$$G = \{\sigma_a \,|\, (a,n) = 1,\ \sigma_a(\varsigma_n) = \varsigma_n^a\}.$$

Како је $\mathbb{Q}(\varsigma_n) \cong \mathbb{Q}[X]/\Phi_n(x)$, где је $\Phi_n(X)$ минимални полином за ς_n над $\mathbb{Q}$ (ово је циклотомични полином), то $\sigma_a \in G$ можемо записати као $\sigma_a(X) = X^a$ у $\mathbb{Q}[X]/\Phi_n(x)$. Сада можемо увести група прстен:

Дефиниција 2. Група прстен $\mathbb{Z}[G]$ дефинисан је као скуп свих $f = \sum_{\sigma\in G} f_\sigma\sigma$, где су f_σ неки цели бројеви, са операцијама

$$\begin{aligned} f \pm g &= \sum_{\sigma\in G}(f_\sigma + g_\sigma)\sigma \\ f \cdot g &= \sum_{\sigma,\tau\in G}(f_\sigma g_\tau)(\sigma\tau) \end{aligned}$$

Дефинишимо и дејство $\mathbb{Z}(G)$ на $\mathbb{Q}(\varsigma_n)$:

Дефиниција 3. За $x \in \mathbb{Q}(\varsigma_n)$ и $f \in \mathbb{Z}[G]$ дејство f на x дефинишемо са

$$x^f = \prod_{\sigma\in G}\sigma(x)^{f_\sigma},$$

за $x \neq 0$ и $0^f = 0$.

Заиста, није тешко проверити да важи следећа теорема, чиме је оправдана претходна дефиниција:

Теорема 3. Уколико је $x_1, x_2 \in \mathbb{Q}(\varsigma_n)$ и $f_1, f_2 \in \mathbb{Z}[G]$ важи:

(а) $x^{f_1+f_2} = x^{f_1}\cdot x^{f_2}$;

(б) $x^{f_1 f_2} = (x^{f_1})^{f_2} = (x^{f_2})^{f_1}$;

(в) $(x_1 + x_2)^f = x_1^f + x_2^f$;

(г) $(x_1x_2)^f = x_1^f x_2^f$. □

Нама је од интереса случај $n = p^k$, где је p неки прост број. Како је G комутативна, то је и $\mathbb{Z}[G]$ комутативни прстен. Нека је

$$\mathcal{P} = \{f \in \mathbb{Z}[G] \,|\, \varsigma_p^f = 1\}.$$

Посматрајмо $f = \sum_{\sigma \in G} f_\sigma \sigma \in \mathcal{P}$. Јасно је $\sum_{a \in (\mathbb{Z}/n\mathbb{Z})^*} a f_{\sigma_a} \equiv_p 0$, па је $\mathcal{P}$ идеал у $\mathbb{Z}[G]$. Овај идеал је и прост и генерисан је са $p \cdot 1$ и $a \cdot 1 - \sigma_a$, где је 1 јединично пресликавање. У наставку ћемо $k \cdot 1 \in \mathbb{Z}[G]$ означавати само са k.

Кључ теста чини следећа теорема, која представља аналог Теореме 5 из поглавља 4.2:

Теорема 4. Нека је χ карактер на $\mathbb{F}_q$ реда p^k, нека су a и b цели бројеви такви да $p \nmid ab(a+b)$ и нека је $E = (\mathbb{Z}/p^k\mathbb{Z})^*$. Такође, нека је

$$\alpha = \sum_{x \in E} \left\lfloor \frac{Nx}{p^k} \right\rfloor \sigma_x^{-1}$$

и

$$\beta = -\sum_{x \in E} \left(\left\lfloor \frac{xa}{p^k} \right\rfloor + \left\lfloor \frac{xb}{p^k} \right\rfloor - \left\lfloor \frac{x(a+b)}{p^k} \right\rfloor \right) \sigma_x^{-1}.$$

Тада је

$$G(\chi)^{\beta(N-\sigma_N)} = J(\chi^a, \chi^b)^\lambda.$$

Доказ. Нека је $\Theta = \sum_{x \in E} x\sigma_x^{-1}$ и нека $p \nmid r$. Тада је

$$\Theta(\sigma_r - r) = \sum_{x \in E} x\sigma_{x^{-1}r} - \sum_{x \in E} xr\sigma_{x^{-1}} = \sum_{x \in E} (xr)_{p^k} \sigma_{x^{-1}} - \sum_{x \in E} xr\sigma_{x^{-1}},$$

где је $(xr)_{p^k}$ остатак xr при дељењу са p^k. Сада је јасно

$$\Theta(\sigma_r - r) = -p^k \sum_{x \in E} \left\lfloor \frac{xr}{p^k} \right\rfloor \sigma_x^{-1}.$$

Специјално, за $r = N$ добијамо $\Theta(\sigma_r - r) = p^k \alpha$, односно

$$\Theta(\sigma_a + \sigma_b - \sigma_{a+b}) = \Theta(\sigma_a - a + \sigma_b - b - (\sigma_{a+b} - (a+b))) = p^k \beta,$$

тј. $\beta(N - \sigma_N) = \alpha(\sigma_a + \sigma_b - \sigma_{a+b})$. По Теореми 1(г) из 4.1 је

$$J(\chi^a, \chi^b) = G(\chi)^{\sigma_a + \sigma_b - \sigma_{a+b}},$$

па тврђење заиста важи. □

Да бисмо искористили ову теорему потребно је одредити погодне a и b тако да $\beta \notin \mathcal{P}$. Јасно је да сам услов $p \nmid ab(a+b)$ не може бити задовољен за $p = 2$, па ћемо за почетак претпоставити да је $p \geqslant 3$. Уз ознаке из претходне теореме, важи:

Теорема 5. Потребан и довољан услов да $\beta \notin \mathcal{P}$ је

$$a^p + b^p \not\equiv (a+b)^p \pmod{p^2}.$$

Доказ. Нека је

$$K = -\sum_{x\in E}\left(\left\lfloor\frac{xa}{p^k}\right\rfloor + \left\lfloor\frac{xb}{p^k}\right\rfloor - \left\lfloor\frac{x(a+b)}{p^k}\right\rfloor\right)x^{-1}.$$

Јасно је да је $\beta\notin\mathcal{P}$ еквивалентно са $p\nmid K$. Како $p\nmid a$, то је скуп остатака бројева ax, $x\in E$, једнак скупу E. Докажимо да је

$$\sum_{x\in E}\left\lfloor\frac{xa}{p^k}\right\rfloor x^{-1} \equiv a\frac{a^{(p-1)p^{k-1}}-1}{p^k} \pmod{p^k}. \qquad (*)$$

Посматрајамо производ бројева ax, за $x\in E$, по модулу p^{2k}. Тада је

$$\prod_{x\in E} xa = \prod_{x\in E}\left(\left\lfloor\frac{xa}{p^k}\right\rfloor p^k + (ax)_{p^k}\right) \equiv p^k\sum_{x\in E}\left\lfloor\frac{xa}{p^k}\right\rfloor\prod_{y\neq x} ay + \prod_{x\in E}(ax)_{p^k} \pmod{p^{2k}},$$

где је $(ax)_{p^k}$ остатак при дељењу ax са p^{2k}. Како је $\prod_{y\in E} y\equiv 1 \pmod{p^k}$, то је $\prod_{y\neq x,\ y\in E} ay \equiv a^{-1}x^{-1} \pmod{p^k}$. Даље, како је $\prod_{x\in E}(ax)_{p^k} = \prod_{x\in E} x$, то је из претходне конгруенције

$$\frac{a^{(p-1)p^{k-1}}-1}{p^k}\prod_{x\in E} x \equiv \sum_{x\in E}\left\lfloor\frac{xa}{p^k}\right\rfloor a^{-1}x^{-1} \pmod{p^k}.$$

Како је $\prod_{x\in E} x\equiv 1 \pmod{p^k}$, то је $(*)$ доказано.

Докажимо и да је

$$\frac{a^{(p-1)p^{k-1}}-1}{p^k} \equiv \frac{a^{p-1}-1}{p} \pmod{p}. \qquad (**)$$

Нека је $a^{p-1} = Ap+1$. Из биномне формуле и $p^{k+1}\mid\binom{p^{k-1}}{m}(Ap)^m$, за $m\geqslant 2$, закључујемо да је $a^{(p-1)p^{k-1}}\equiv Ap^k+1 \pmod{p^k}$, што доказује $(**)$.

Дато тврђење сада директно следи из $(*)$ и $(**)$. □

Из претходне теореме добијамо и наредно тврђење, које се директно користи у тесту:

Теорема 6. Ако је $3\leqslant p<6\cdot 10^9$ и $p\neq 1093, 3511$ и ако у Теореми 3 узмемо $a=b=1$ важи $\beta\notin\mathcal{P}$. Тачније за

$$\beta = \sum_{p^k/2<x<p^k,\, p\nmid x}\sigma_x^{-1}$$

важи $\beta\notin\mathcal{P}$ и

$$J(\chi,\chi)^\alpha \equiv \chi(N)^{-cN} \pmod{N},$$

где је

$$\alpha = \sum_{x \in E} \left\lfloor \frac{Nx}{p^k} \right\rfloor \sigma_x^{-1}$$

и

$$c = 2 \cdot \frac{2^{(p-1)p^{k-1}} - 1}{p^k}.$$

Доказ. У претходној теореми доказано је да $\beta \notin \mathcal{P}$ ако и само ако важи $2^p \not\equiv 2 \pmod{p^2}$. Ова конгруеција је детаљно испитивана и добијено је да су њена једина решења мања од $6 \cdot 10^9$ баш $p = 1093, 3511$. Остатак теореме следи на основу релације $(*)$. □

Иако се чини да претходну теорему можемо ограничено примењивати, њена ограничења су у пракси небитна. Наиме, још увек нисмо ни близу могућности да факторишемо бројеве са 10^9 декадних цифара, а и уколико бисмо то могли не би нам били потребни прости бројеви већи или једнаки од 1093.

Вратимо се на случај $p = 2$. Већ смо напоменули да овај случај не можемо решити на исти начин као $p \neq 2$. У овој ситуацији од користи ће нам бити трострука Јакобијева сума, тј.

$$J(\chi_1, \chi_2, \chi_3) = \sum_{x+y+z=1} \chi_1(x)\chi_2(y)\chi_3(z).$$

Слично као у доказу Теореме 1 може се показати да је

$$J(\chi_1, \chi_2, \chi_3) = \frac{G(\chi_1)G(\chi_2)G(\chi_3)}{G(\chi_1\chi_2\chi_3)}$$

и специјално за $\chi_1 = \chi_2 = \chi_3 = \chi$

$$J(\chi, \chi, \chi) = G(\chi)^{3-\sigma_3}.$$

Следећа теорема је аналог Теореме 4:

Теорема 7. Нека је χ карактер модула q чији је ред 2^k, где је $k \geqslant 3$. Нека је са E означен скуп свих бројева x таквих да је $1 \leqslant x < 2^k$ и x конгруентно са 1 или 3 по модулу 8. Такође, нека је

$$\alpha = \sum_{x \in E} \left\lfloor \frac{Nx}{2^k} \right\rfloor \sigma_x^{-1}$$

и

$$\beta = \sum_{x \in E} \left\lfloor \frac{3x}{2^k} \right\rfloor \sigma_x^{-1}.$$

Тада, уколико N даје остатак 1 или 3 по модулу 8 важи

$$G(\chi)^{\beta(N-\sigma_N)} = J(\chi,\chi,\chi)^{\alpha}.$$

Такође, $\beta \notin \mathcal{P}$.
Доказ. Доказ је сличан као доказ Теореме 4. Основна разлика је што $(\mathbb{Z}/2^k\mathbb{Z})^*$ није циклична, него има цикличну групу индекса 2, па је услов за N неопходан. □

Уколико је N конгруентно са 3 или 7 по модулу 8, идеја је да N заменимо са $-N$ ($-N$ је конгруентно са 1 или 3 по модулу 8). Важи

$$G(\chi)^{\sigma_{-N}+N} = G(\chi)^{N-\sigma_N}G(\chi^N)G(\chi^{-N}) = (\text{Према Теореми 1(в)}) = -G(\chi)^{N-\sigma_N}q.$$

Сада можемо дати „допуну" Теореме 7:

Теорема 8. Нека је χ карактер модула q чији је ред 2^k, где је $k \geqslant 3$. Нека је са E означен скуп свих бројева x таквих да је $1 \leqslant x < 2^k$ и x конгруентно са 1 или 3 по модулу 8. Такође, нека је

$$\alpha = \sum_{x\in E}\left(\left\lfloor \frac{Nx}{2^k}\right\rfloor + 1\right)\sigma_x^{-1}$$

и

$$\beta = \sum_{x\in E}\left\lfloor \frac{3x}{2^k}\right\rfloor \sigma_x^{-1}.$$

Тада, уколико N даје остатак 5 или 7 по модулу 8 важи

$$G(\chi)^{\beta(N-\sigma_N)} = J(\chi,\chi,\chi)^{\alpha}(-q)^{-\beta}.$$

Такође, $\beta \notin \mathcal{P}$. □

Из дефиниције троструке Гаусове суме и њених основних особина добијамо да је

$$J(\chi,\chi,\chi) = J(\chi,\chi)\cdot J(\chi,\chi^2),$$

што нам даје ефикаснији начин за рачунање $J(\chi,\chi,\chi)$. Даћемо и следеће две теореме:

Теорема 9. Нека је ψ произвољни карактер и χ_1 карактер реда m. Тада важи

$$\prod_{0\leqslant x<m} G(\psi\chi_1^x) = -G(\psi^m)\psi^{-m}(m)\prod_{0\leqslant x<m} G(\chi_1^x).$$

На основу ове теореме доказујемо и:

Теорема 10. Уколико је $\gamma = \sum_{x \in E} \sigma_x^{-1}$ и $d = 2^{k-2} - 1$, тада

$$J(\chi, \chi, \chi)^\gamma = q^d J^2(\chi^{2^{k-3}}, \chi^{3 \cdot 2^{2^{k-3}}}).$$

Доказ. Из формуле за представљање троструке Јакобијеве суме преко Гаусових сума добијамо

$$J(\chi, \chi, \chi)^\gamma = \prod_{x \in E} G^2(\chi^x).$$

Применимо сада претходну теорему за $\psi = \chi^a$ и $\chi_1 = \chi^{2^{k-l}}$. Индукцијом по l доказујемо да је

$$\prod_{0 \leqslant n < 2^l} G^2(\chi^{a+n2^{k-l}}) = q^{2^{l-1}} G^2(\chi^{2^l a}) \chi(2)^{-al2^{l+1}}.$$

Помножимо ли дате идентите за $l = k - 3$ у случајевма $a = 1$ и $a = 3$, применом Теореме 1 добијамо дато тврђење. □

Сада можемо доказати и теорему која представља аналог Теореме 5 из 4.2 поглавља за $p = 2$. Ознаке су као у Теоремама 7 и 8:

Теорема 11. Нека је $\delta_N = 0$ ако је N конгруентно са 1 или 3 по модулу 8 и $\delta_N = 1$ ако је N конгруентно са 5 или 7 по модулу 8. Важи

$$(J(\chi, \chi) \cdot J(\chi, \chi^2))^\alpha \cdot J^{2\delta_N}(\chi^{2^{k-3}}, \chi^{3 \cdot 2^{k-3}}) \equiv (-1)^{\delta_N} \chi(N)^{-cN} \pmod{N},$$

где је

$$\alpha = \sum_{x \in E} \left\lfloor \frac{Nx}{2^k} \right\rfloor \sigma_x^{-1}$$

и

$$c = 3 \cdot \frac{3^{2^{k-2}} - 1}{2^k}.$$

Доказ. Прво $J(\chi, \chi, \chi) = J(\chi, \chi) \cdot J(\chi, \chi^2)$, где је израз са десне стране дат (као што је већ и напоменуто) јер је овакав начин израчунавања ефикаснији.

Уколико је N конгруентно са 1 или 3 по модулу 8, теорема следи на основу Теореме 7 и конгруенције $(*)$ за $a = 3$. Из Теореме 8, конгруенције $(*)$ и идентитета

$$\sum_{x \in E} \left\lfloor \frac{3x}{2^k} \right\rfloor = 2^{k-2} - 1$$

добијамо

$$J(\chi, \chi, \chi)^{\alpha_1} \equiv \chi(N)^{-cN} (-q)^d \pmod{N},$$

где је $d = 2^{k-2} - 1$ и $\alpha_1 = \sum_{x \in E} \left(\left\lfloor \frac{Nx}{2^k} \right\rfloor + 1 \right) \sigma_x^{-1}$. Тврђење сада следи на основу претходне теореме. □

Доказом Теореме 4 и Теореме 11 преостају још случајеви p^k, за $p = 2$ и $k \leqslant 2$. Њих разрешава следећа теорема, која је последица Теореме 1:

Теорема 12. За $p = 2$ и $k = 1$ важи

$$q^{(N-1)/2} \equiv \chi(N) \pmod{N}.$$

За $p = 2$ и $k = 2$, уколико је $N \equiv 1 \pmod 4$ важи

$$J(\chi, \chi)^{(N-1)/2} q^{(N-1)/4} \equiv \chi(N)^{-1} \pmod{N},$$

а уколико је $N \equiv 3 \pmod 4$ важи

$$J(\chi, \chi)^{(N+1)/2} q^{(N-3)/4} \equiv -\chi(N) \pmod{N}.$$

□

Теоремама 4, 11 и 12 дат је потпун аналог Теореме 5 из 4.2. Тест Јакобијевим сумама изводимо аналогно као и тест Гаусовим, само што примену Теореме 5 претходног дела поглавља замењујемо одговарајућом од Теорема 4, 11 или 12 овог поглавља.

Заједно са тестовима елиптичким кривама (који су дати у последњем поглављу) тест Јакобијевим сумама се најчешће примењује приликом доказа прималности великих бројева. Овим тестом се може доказивати прималност бројева са више од 1000 цифара.

Део 5

Тестови прималности са делимичном факторизацијом

У пракси се најчешће не користе основни облици тестова прималности, него се међусобно комбинују како би дали што боље резултате. У овом поглављу даћемо могућа побољшања алгоритама уколико је позната делимична факторизација броја $n-1$ или $n+1$.

5.1 Пепинов тест прималности

Као што је напоменуто у уводу, још од давнина људи су трагали за формулом за просте бројеве или за формулом која даје неке просте бројеве. Тако су настали и Фермаови бројеви $F_k = 2^{2^k}+1$, за које је Ферма мислио да су прости. Међутим, иако његова претпоставка није тачна (F_5 није прост), од велике је важости испитати да ли је неки Фермаов број прост. Прво ћемо дати Лукасову[1] теорему:

Теорема 1. Ако су a и $n>1$ природни бројеви такви да је

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{и} \quad a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \text{ за све просте бројеве } q \mid n-1,$$

онда је n прост број.

Доказ. Други услов гарантује да ред елемента a у $\mathbb{Z}_n^*$ није прави делилац броја $n-1$, што нам заједно са првим условом даје да је тај ред једнак $n-1$. Међутим, како је $n-1 \leqslant \varphi(n)$ једино уколико је n прост број (тада важи једнакост), то је јасно n прост број. □

Сада можемо дати и тест прималности за Фермаове бројеве:

[1] Francois Édouard Anatole Lucas - француски математичар 1841-1891

Теорема 2. Нека је $k \geqslant 1$. Број $F_k = 2^{2^k} + 1$ је прост ако и само ако је $3^{(F_k-1)/2} \equiv -1 \pmod{F_k}$.
Доказ. Претпоставимо прво да је F_k прост број. Из Ојлеровог критеријума и Гаусовог закона реципроцитета је

$$3^{(F_k-1)/2} \equiv \left(\frac{3}{F_k}\right) = (-1)^{\frac{F_k-1}{2}\cdot\frac{3-1}{2}} \left(\frac{F_k}{3}\right) = \left(\frac{2}{3}\right) = -1 \pmod{F_k},$$

где претпоследња једнакост важи из чињенице да је $2^{2^k} \equiv 1 \pmod 3$.
Обрат теореме је директна последица Теореме 1. □

Овај тест познат је као Пепинов тест. Највећи број за који је овим тестом одређено да ли је прост је F_{24}. Тај број је сложен, а интересантно је да су такви и сви бројеви F_k, за $5 \leqslant k \leqslant 24$, за које је одређено да ли су прости или сложени.

5.2 Тестови са делимичном факторизацијом броја $n-1$

Нека за природан број n који испитујемо знамо да је $n - 1 = FR$, где је факторизација броја F позната. Следећа теорема нам даје основу теста:

Теорема 1. (**Поклингтонова**[2] **теорема**) Нека је a природан број такав да је

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{и} \quad (a^{(n-1)/q} - 1, n) = 1 \text{ за све просте } q \mid F. \tag{1}$$

Тада је сваки прост делилац броја n конгурентан са 1 по модулу F.
Доказ. Нека је r неки делилац броја n. Посматрајмо број a^R. Како је из прве конгруенције $(a^R)^F \equiv 1 \pmod r$, то је поредак броја a^R делилац броја F. Из другог услова закључујемо да поредак не може бити нити један прави делилац од F, па је поредак једнак F. Самим тим $F \mid r - 1$, што је и требало доказати. □

Уколико је $F \geqslant \sqrt{n}$ из претходне теореме можемо закључити да је n прост број. Из наредне теореме сличан резултат имамо и за мање вредности F:

Теорема 2. Нека важи (1), $\sqrt[3]{n} \leqslant F < \sqrt{n}$ и нека је $n = c_2F^2 + c_1F + 1$, где су $c_1, c_2 \in [0, F-1]$. Тада је n прост ако и само ако $c_1^2 - 4c_2$ није квадрат.
Доказ. Како су сви прости делиоци броја n облика $aF+1$, то n заиста има дату презентацију у бази F, а како је $F \geqslant \sqrt[3]{n}$, то n може имати највише два проста фактора.

[2]Henry Cabourn Pocklington - енглески математичар 1870-1952

Претпоставимо да n није прост, тј. да је $n = pq$, где је $p = aF + 1$ и $q = bF + 1$. Самим тим

$$c_2F^2 + c_1F + 1 = abF^2 + (a + b)F + 1.$$

Доказаћемо да је $c_2 = ab$ и $c_1 = a+b$, одакле можемо закључити да је $c_1^2-4c_2$ квадрат.

Прво, како је $F^3 \geqslant pq > abF^2$, то је $ab < F$, а како је $ab \geqslant a + b - 1$, то је јасно $a + b \leqslant F$, при чему једнакост може важити једино уколико је $a = 1$ и $b = F-1$ (или обрнуто). Међутим, тада је $n = (F+1)(F^2-F+1) = F^3+1 > n$, па мора бити $a + b < F$, што доказује нашу тврдњу.

Нека је сада $c_1^2 - 4c_2 = u^2$ за неки природан број u. Тада је јасно

$$n = \left(\frac{c_1 + u}{2} \cdot F + 1\right) \cdot \left(\frac{c_1 - u}{2} \cdot F + 1\right),$$

па је n сложен. Овим је доказ у потпуности завршен. □

Последње две теореме дају једноставан тест прималности:

Алгоритам 5.1. (Тест са делимичном факторизацијом $n-1$)

1. [Pocklington test]
Izabrati proizvoljan broj $a \in [2, n-1]$;
if ($a^{n-1} \not\equiv 1 \pmod{n}$) ispiši SLOŽEN;
for (prost $q \mid F$){
$d = (a^{(n-1)/q} - 1, n)$;
if ($1 < d < n$) ispiši d;
if ($d = n$) goto [Pocklington test];
}
2. [Test prve veličine]
if ($F \geqslant \sqrt{n}$) ispiši PROST;
3. [Test druge veličine]
if ($\sqrt[3]{n} \leqslant F < \sqrt{n}$){
Predstaviti $n = c_2F^2 + c_1F + 1$;
if ($c_1^2 - 4c_2$ nije kvadrat) ispiši PROST;
else ispiši SLOŽEN;
}

5.3 Мерсенови бројеви

Слично као и у случају Фермаових бројеви настао је и низ бројева који се називају Мерсенови[3]. Овај низ задат је формулом $M_n = 2^n - 1$. Јасно је

[3]Marin Mersenne - француски математичар 1588-1648

да уколико је M_n прост да и n мора бити прост. Следећа теорема даје довољан услов да је Мерсенов број прост, а самим тим и тест прималности за Мерсенове бројеве. Ова теорема позната је као Лукас - Лемерова[4] теорема:

Теорема 1. Нека је n непаран број и низ $\{L_m\}$ дефинисан са $L_1 = 4$ и

$$L_{m+1} = L_m^2 - 2.$$

Број M_n је прост ако и само ако је $L_{n-1} \equiv 0 \pmod{M_n}$.
Доказ. Нека је q прост делилац броја M_n и $\alpha, \beta \in \mathbb{F}_{q^2}$ нуле полинома

$$f(x) = x^2 - 2^{(n+1)/2}x - 1$$

над $\mathbb{F}_q$. Из Виетових[5] формула је $\alpha + \beta = 2^{(n+1)/2}$ и $\alpha\beta = -1$.

Нека је $\overline{L_m}$ остатак броја L_m по модулу q и $V_m = \alpha^m + \beta^m$. Докажимо индукцијом да је $\overline{L_m} = V_{2^m}$.

За $m = 1$ добијамо

$$V_2 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = 2^{n+1} + 2 \equiv 4 = L_1 \pmod{q},$$

што је и требало доказати. Претпоставимо даље да је $\overline{L_m} = V_{2^m} = \alpha^{2^m} + \beta^{2^m}$. Тада је

$$\overline{L_{m+1}} = (\alpha^{2^m} + \beta^{2^m})^2 - 2 = \alpha^{2^{m+1}} + \beta^{2^{m+1}} + 2\alpha^{2^m}\beta^{2^m} - 2 = \alpha^{2^{m+1}} + \beta^{2^{m+1}} = V_{2^{m+1}}.$$

Пређимо на доказ датог тврђења. Претпоставимо прво да је M_n прост. Докажимо да је $f(x)$ иредуцибилан у $\mathbb{F}_{M_n}$, односно да дискриминанта $\Delta = 2^{p+1} + 4 \equiv 6 \pmod{M)_n}$ није квадрат у F_{M_n}. Како је $\left(\frac{2}{M_n}\right) = 1$ и $\left(\frac{3}{M_n}\right) = -1$, то је $\left(\frac{\Delta}{M_n}\right) = \left(\frac{2}{M_n}\right)\left(\frac{3}{M_n}\right) = -1$, па Δ заиста није квадрат. Како је $f(x)$ иредуцибилан, то је $\mathbb{Z}_{M_n}/(f(x)) \cong \mathbb{F}_{M_n^2}$, па је са x^{M_n} дат један аутоморфизам овог поља. Аутоморфизми пермутују нуле полинома $f(x)$, па како су оне x и $2^{(n+1)/2} - x$, то је $x^{M_n} = 2^{(n+1)/2} - x$. Специјално, уколико претходну једнакост записану за α помножимо са α добијамо $\alpha^{M_n+1} = -1$ (у $\mathbb{F}_{M_n^2}$) и слично $\beta^{M_n+1} = -1$.

Сада је $\overline{L_n} = \alpha^{M_n+1} + \beta^{M_n+1} = -2$. Како је $L_n = L_{n-1}^2 - 2$, то мора бити $L_{n-1} \equiv 0 \pmod{M_n}$.

Докажимо и други део тврђења, тако што ћемо претпоставити супротно. Нека је $L_{n-1} \equiv 0 \pmod{M_n}$ и нека је q најмањи прост делилац броја M_n. Тада је $L_{n-1} \equiv 0 \pmod{q}$ и $q^2 \leqslant n$. Такође $\alpha^{2^{n-1}} + \beta^{2^{n-1}} = 0$, па множењем

[4]Derrick Henry Lehmer - амерички математичар 1905-1991
[5]Francois Viète - француски математичар 1540-1603

са $\alpha^{2^{n-1}}$ добијамо $\alpha^{2^n} = -1$. Значи ред елемента α у $\mathbb{F}_{q^2}$ је 2^{n+1}, па је $2^{n+1} \leqslant q^2 - 1 < 2^n$, што је очигледна контрадикција. □

Из претходне теореме можемо закључити да је време потребно за тестирање прималности броја M_n једнако $O(n^{2+\epsilon})$.

Највећи познати Мерсенови прости бројеви су $M_{43112609}$ и $M_{37156667}$, са 12978189, односно 11185272 цифара. Ово су и највећи познати прости бројеви.

5.4 Тестови са делимичном факторизацијом броја $n+1$

Слично као у случају да нам је позната делимична факторизација броја $n-1$, од користи нам може бити и познавање делимичне факторизације броја $n+1$. У овом поглављу даћемо један овакав тест.

Нека су a и b бројеви такви да број $\Delta = a^2 - 4b$ није квадрат у $\mathbb{Z}_n$. Тада корени једначине $x^2 - ax + b = 0$ морају бити различити и један од њих је $r = \dfrac{a + \sqrt{\Delta}}{2}$. Следећа теорема даје једно интересантно својство бројева r^k:

Теорема 1. Важи $r^k = \dfrac{V_k + U_k\sqrt{\Delta}}{2}$, где су $\{U_m\}$ и $\{V_m\}$ низови задати са

$$U_0 = 0, \quad U_1 = 1, \quad U_{k+2} = aU_{k+1} - bU_k$$

$$V_0 = 2, \quad V_1 = a, \quad V_{k+2} = aV_{k+1} - bV_k, \quad k \geqslant 0.$$

Доказ. Општи чланови ових низова дати су са

$$U_k = \frac{r^k - r'^k}{\sqrt{\Delta}}, \quad V_k = r^k + r'^k,$$

где је $r' = \dfrac{a - \sqrt{\Delta}}{2}$, одакле следи дато тврђење. □

Овако дефинисани низови $\{U_m\}$ и $\{V_m\}$ имају и следеће својство које ће нам бити од велике користи за брзо рачунање U_k:

Теорема 2. За свако $k \geqslant 0$ важи

$$U_{2k} = U_k V_k, \quad V_{2k} = V_k^2 - 2q^k.$$

Доказ. Ово тврђене директно добијамо заменом општих чланова низова U_k и V_k. □

Уведимо бројеве $r(m)$ следећом дефиницијом:

Дефиниција 1. За природан број m, такав да је $(m, 2b\Delta) = 1$, са $r(m)$ означавамо минималан број r такав да је U_r дељиво са m.

Из општег члана низа закључујемо да уколико $k \mid l$ тада и $U_k \mid U_l$. Самим тим, узимајући у обзир претходну дефиницију, закључујемо да је U_k дељиво са m ако и само ако је k дељиво са $r(m)$.

Следећа теорема даје аналог Мале Фермаове теореме:

Теорема 3. Ако је p прост број и $\delta = \left(\frac{\Delta}{p}\right)$, тада је $U_{p-\delta} \equiv 0 \pmod{p}$, а самим тим $r(p) \mid p - \delta$.
Доказ. Из биномног развоја $r^{p-\delta}$ и $r'^{p-\delta}$ добијамо

$$U_{p-\delta} = \sum_{k=0}^{p-\delta} \binom{p-\delta}{k} a^{p-\delta-k} \Delta^{(k-1)/2} (1 - (-1)^k). \qquad (*)$$

Размотримо два случаја:
1° $\delta = 1$. Можемо претпоставити да $p \nmid a$, јер је у супротном очигледно U_{p-1} дељиво са p. Даље, како је из Вилсонове[6] теореме $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$, и како су у развоју $(*)$ једини ненула чланови за непарне k, то је

$$U_{p-\delta} \equiv -2 \sum_{k=0}^{(p-3)/2} a^{p-1-2k-1} \cdot \Delta^k \equiv -2a^{-1} \sum_{k=0}^{(p-3)/2} b'^k \pmod{p},$$

где је $b' = a^{-2}(a^2 - 4b)$. Самим тим, из $\sum_{k=0}^{(p-3)/2} b'^k = \frac{b'^{(p-1)/2} - 1}{b' - 1}$, добијамо $U_{p-1} \equiv 0 \pmod{p}$, јер је по Ојлеровом критеријуму $b'^{(p-1)/2} \equiv 1 \pmod{p}$.
2° $\delta = -1$. Како је $\binom{p+1}{k} \equiv 0 \pmod{p}$, за $2 \leqslant k \leqslant p-1$, и како су у развоју $(*)$ једини ненула чланови за непарне k, то је

$$U_{p-\delta} \equiv 2(a^p + a \cdot \Delta^{(p-1)/2}) \equiv 0 \pmod{p}.$$

Последња конгуренција следи из Мале Фермаове теореме и Ојлеровог критеријума, јер Δ није квадратни остатак. □

Нека су ознаке као у претходном делу поглавља. Тест се базира на следећем аналогу Поклингтонове теореме:

Теорема 4. Нека је n природан број, $(n, 2b) = 1$ и нека Δ није квадрат у $\mathbb{Z}_n$. Ако је F делилац броја $n + 1$ и ако важи

$$U_{n+1} \equiv 0 \pmod{n}, \quad (U_{(n+1)/r}, n) = 1 \quad \text{за сваки прост } r \mid F,$$

[6] John Wilson - енглески математичар 1741-1793

тада сваки прост делилац p од n задовољава $p \equiv \left(\frac{\Delta}{p}\right) \pmod F$. Специјално, уколико је $F > \sqrt{n}+1$, тада је n прост.

Доказ. Нека је p најмањи прост делилац броја n и $\delta = \left(\frac{\Delta}{p}\right)$. Према Теореми 3 $r(p) \mid p - \delta$. Такође, према другом услову теореме, број $r(p)$ мора бити дељив са F. У супротном постојао би прост број q који дели F, а не дели $r(p)$, што је немогуће, јер тада p дели $U_{(n+1)/q}$. Из претходног закључујемо да $F \mid p - \delta$, што је и требало доказати. Такође, ако је $F > \sqrt{n}+1$, тада је и $p > \sqrt{n}$, па како је p најмањи прост делилац од n, то мора бити $n = p$. □

Слични тестови се могу дати и за бројеве облика $n^2 \pm n - 1$, $n^2 + 1$, итд. У следећим задацима дајемо тестове за два специфична скупа бројева:

Задатак 1. Наћи детерминистички полиномијални алгоритам за тестирање бројева из скупа $\{n \mid \varphi(n)$ је степен броја $2\}$.

Решење. Нека је $n = \prod_{i=1}^{k} p_i^{a_i}$ канонска факторизација неког броја из датог скупа. Како је $2^t = \varphi(n)$, то из формуле за $\varphi(n)$ добијамо

$$2^t = \prod_{i=1}^{k} p_i^{a_i}(p_i - 1).$$

Како 2^t није дељив нити једним простим бројем различитим од 2, то је $a_i - 1 = 0$ и $p_i - 1 = 2^{n_i}$, за све $1 \leqslant i \leqslant k$. Из последњег закључујемо да су сви p_i неки Фермаови прости бројеви, тј. $p_i = 2^{2^{m_i}} + 1$. Самим тим, број n је прост ако и само ако је Фермаов прост. Дакле, довољно је n тестирати Пепиновим тестом. □

Задатак 2. Наћи детерминистички полиномијални алгоритам за тестирање бројева из скупа $\{n \mid \sigma(n)$ је степен броја $2\}$, где је са $\sigma(n)$ означен збир позитивних делилаца природног броја n.

Решење. Нека је $n = \prod_{i=1}^{k} p_i^{a_i}$ канонска факторизација неког броја из датог скупа. Како је $2^t = \sigma(n)$, то из формуле за $\sigma(n)$ добијамо

$$2^t = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}. \qquad (*)$$

Докажимо да $a_i + 1$ не може имати непарног делиоца већег од 1. У супро-

тном, ако је $a_i + 1 = s_i t_i$, где $2 \nmid s_i$, то је

$$\begin{aligned}\frac{p_i^{a_i+1} - 1}{p_i - 1} &= \frac{(p_i^{s_i} - 1)(p_i^{s_i(t_i-1)} + p_i^{s_i(t_i-2)} + \ldots + 1)}{p_i - 1} \\ &= (p_i^{s_i-1} + p_i^{s_i-2} + \ldots + 1)(p_i^{s_i(t_i-1)} + p_i^{s_i(t_i-2)} + \ldots + 1).\end{aligned}$$

Међутим, тада је $p_i^{s_i-1} + p_i^{s_i-2} + \ldots + 1$ непаран број већи од 1, што је немогуће.

Закључујемо да је $a_i + 1 = 2^{n_i}$, за све $1 \leqslant i \leqslant k$. Сада је $p_i^{a_i+1} - 1 = (p_i - 1)\prod_{j=0}^{n_i-1}(p_i^{2^j} + 1)$, па како $p_i^{2^j} + 1$ није дељиво са 4 за $j \geqslant 1$, то је $n_i = 1$, за све $1 \leqslant i \leqslant k$. Сада се $(*)$ своди на

$$2^t = \prod_{i=1}^{k}(p_i + 1),$$

па је сваки p_i неки Мерсенов прост број. Значи, n је прост број ако и само ако је Мерсенов прост број. Самим тим, број n је довољно тестирати Лукас-Лемеровим тестом. □

Део 6

Тест прималности помоћу коначних поља

У претходном поглављу дали смо неке тестове који су се базирали на претпоставци да знамо факторизацију броја $n-1$ (односно $n+1$). У овом поглављу даћемо једно уопште, тј. тест прималности уколико број n^I-1 има „велики" фактор, за неки „не превише велики" број I.

6.1 Иредуцибилни полиноми над коначним пољима

Нека је p прост број. Приметимо да је за произвољан број k поље $\mathbb{F}_{p^k}$ изоморфно пољу $\mathbb{Z}_p[X]/(f)$, где је $f \in \mathbb{Z}_p[X]$ произвољан иредуцибилан полином степена k. Самим тим, коришћењем познатих особина поља $\mathbb{F}_{p^k}$ добићемо и неке особине прстена $\mathbb{Z}_p[X]$, које ће нам бити од велике користи у наставку поглавља.

Основно питање на које ћемо дати одговор у овом потпоглављу је колико има и како одредити иредуцибилне полиноме у $\mathbb{Z}_p[X]$. Поље $\mathbb{F}_{p^k}$ је коренско поље полинома $x^{p^k}-x$. Самим тим сви иредуцибилни полиноми у $\mathbb{Z}_p[X]$ морају бити делиоци полинома $x^{p^k}-x$. Уз то њихов степен мора делити k, јер је $\mathbb{F}_{p^d}$ потпоље поља $\mathbb{F}_{p^k}$ ако и само ако $d \mid k$. Ако је са $N_d(p)$ означен број моничних иредуцибилних полинома из $\mathbb{Z}_p[X]$ степена d, претходно нам даје

$$\sum_{k|d} dN_d(p) = p^k.$$

Према Мебијусовој[1] формули инверзије добијамо формулу за $N_k(p)$, тј.

$$N_k(p) = \frac{1}{k}\sum_{d|k} p^d \mu(k/d).$$

Како је $|\mu(m)| \leqslant 1$, за све $m \in \mathbb{N}$, то је за довољно велике p вредност $N_k(p)$ приближно $\frac{p^k}{k}$. Самим тим потребно је испробати $O(k)$ случајно изабраних

[1] August Ferdinand Möbius - немачки математичар 1790-1868

полинома да бисмо добили иредуцибилан полином. Наравно, поставља се и питање како препознати иредуцибилан полином. Одговор даје следећа теорема:

Теорема 1. Полином $f \in \mathbb{Z}_p[X]$ степена k је иредуцибилан ако и само ако је

$$(f(x), x^{p^j} - x) = 1, \qquad \text{за} \qquad j = 1, 2, \ldots, \lfloor k/2 \rfloor.$$

Доказ. Полином f има иредуцибилан фактор g степена d ако и само ако $g \mid x^{p^d} - x$ и $d \mid k$.

Претпоставимо сада да је f иредуцибилан. Уколико би за неко $1 \leqslant j \leqslant \lfloor k/2 \rfloor$ важило $g(x) \mid (f(x), x^{p^j} - x)$, како је f иредуцибилан, то мора бити $f(x) = g(x)$, па самим тим и $j = d$. Овим добијамо очигледну контрадикцију.

Претпоставимо да важи услов из теореме и нека је $g(x)$ иредуцибилни фактор од $f(x)$ степена $d < k$. Како $d \mid k$, то је $d \leqslant \lfloor k/2 \rfloor$, што је у супротности са датим условом. □

Сада можемо дати алгоритам за утврђивање иредуцибилности у $\mathbb{Z}_p[X]$ полинома f степена k:

Алгоритам 6.1. (Иредуцибилност полинома)
$g(x) = x$;
`for` $(1 \leqslant j \leqslant \lfloor k/2 \rfloor)$`{`
    $g(x) = g(x)^p \pmod{f(x)}$;
    $d(x) = (g(x), f(x))$;
    `if` $(d(x) \neq 1)$ `vrati NE;`
`}`
`vrati DA;`

6.2 Тест прималности

Основу теста чини следећа теорема:

Теорема 1. Нека су дати бројеви n, I, $F \in \mathbb{N}$ такви да је $n > 1$ и $F \mid n^I - 1$. Нека су $f, g \in \mathbb{Z}_n[x]$ такви да је:

(1) f дели $g^{n^I-1} - 1$ у $\mathbb{Z}_n[x]$;

(2) f и $g^{(n^I-1)/q} - 1$ су узајамно прости за све просте $q \mid F$;

(3) сваки од I елементарних симетричних полинома од g, g^2, $\ldots$, g^{n^I-1} конгруентан је по модулу f неком елементу из $\mathbb{Z}_n$.

Тада је сваки прост делилац од n конгруентан са n^j по модулу F, за неко $j \in [0, I-1]$.

Доказ. Нека је r неки прост делилац броја n. Нека је f_1 неки иредуцибилни фактор полинома f над $\mathbb{F}_r$. Тада је $\mathbb{Z}_r[x]/(f_1) = \mathbb{F}$ поље. Нека је $\overline{g}$ елемент поља $\mathbb{F}$ који одговара g. По (1) је $\overline{g}^{n^I-1} = 1$, а по (2) $\overline{g}^{(n^I-1)/q} \neq 1$ за сваки прост $q \mid F$. Самим тим ред броја $\overline{g}$ у групи $\mathbb{F}^*$ је дељив са F.

Посматрајмо полином $p(T) = (T-\overline{g})(T-\overline{g}^n)\cdot\ldots\cdot(T-\overline{g}^{n^{I-1}}) \in \mathbb{F}[T]$. Према (3) је $p \in \mathbb{Z}_r[T]$, па је за сваку нулу α полинома p и α^r нула тог полинома. Самим тим $\overline{g}^r = \overline{g}^{n^j}$ за неко $j \in [0, I-1]$, па је јасно $r \equiv n^j \pmod F$, што је и требало доказати. □

Наравно, поставља се питање како ефикасно одредити полиноме f и g и да ли је то уопште могуће. Следећа теорема даје одговор на ово питање:

Теорема 2. За сваки иредуцибилни полином $f \in \mathbb{Z}_n[X]$ степена $\deg f = I$ и полином $g \in \mathbb{Z}_n[X]$ тако да је $(f, g) = 1$ задовољени су услови (1) и (3) претходне теореме.

Доказ. (1) је свакако задовољено, јер поље $\mathbb{F}^* = (\mathbb{Z}_n/(f))^*$ има $n^I - 1$ елемената. За доказ (3) посматрајмо Галоаову[2] групу поља $\mathbb{F}$ над $\mathbb{Z}_n$. Она је реда I и одређена је Фробенијусовим[3] аутоморфизмима α^{n^j}. Самим тим, сваки симетричан израз по g, g^n, g^{n^2}, ..., $g^{n^{I-1}}$ фиксира се аутоморфизмом на $\mathbb{F}$, па мора бити у фиксном пољу, односно у $\mathbb{Z}_n$. □

Остаје још да g изаберемо тако да је задовољено и (2). Јасно је да сваки генереатор поља $\mathbb{F}$ задовољава релацију (2), а како генератор није тешко одредити случајном претрагом то је овај начин и ефикасан. Наиме, постоји $\varphi(n^I - 1)$ генератора групе $\mathbb{F}$, па је вероватноћа да је случајно изабрани полином генератор једнака $\dfrac{\varphi(n^I-1)}{n^I-1}$. Самим тим у $O(\ln\ln(n^I))$ покушаја можемо одредити тражени полином g. Према алгоритму из претходног дела поглавља ни за одређивање иредуцибилног полинома степена I није потребно превише времена, па има смисла направити тест на основу Теореме 1.

Претпоставимо да су дати природни бројеви n, I, F тако да $F \mid n^I - 1$ и $F \geqslant \sqrt[3]{n}$. Тест прималности помоћу коначних поља можемо дати са:

Алгоритам 6.2. (Тест прималности помоћу коначних поља)

1. `[Određivanje ireducibilnog polinoma stepena` I`]`
   `Izabrati proizvoljan polinom moničan` $g \in \mathbb{Z}_n[x]$ `stepena` I`;`
   `Ispitati da li je` g `ireducibilan;`

---

[2] Évariste Galois - француски математичар 1811-1832

[3] Ferdinand Gregor Frobenius - немачки математичар 1849-1917

2. [Određivanje primitivnog korena]
Izabrati prozivoljan moničan $g \in \mathbb{Z}_n[x]$, gde je $\deg g < I$;
if ($g^{n^I-1} \neq 1$) ispiši SLOŽEN;
for (prost $q \mid F$){
if ($(g^{(n^I-1)/q} - 1, f) \neq 1$) goto [Određivanje primitivnog korena]
}
3. [Test simetričnih polinoma]
Zapisati $(T-g)(T-g^n)\cdot\ldots\cdot(T-g^{n^{I-1}}) = T^I + c_{I-1}T^{I-1} + \ldots + c_0$ u $\mathbb{Z}_n[T]/(f)$;
for ($0 \leqslant j < I$)
if ($\deg c_j > 0$) ispiši SLOŽEN;
4. [Traženje delioca]
for ($1 \leqslant j < I$){
Odrediti delilac broja n koji je $\equiv n^j \pmod F$ i ako takav broj
postoji ispiši SLOŽEN;
}
ispiši PROST;

Из претходног није тешко закључити да је време да алгоритам испише PROST једнако $O(I^c + \ln n^c)$, за неку позитивну константу c. Нећемо разматрати време потребно да алгоритам испише SLOŽEN, јер нам овај алгоритам служи само за доказивање да су бројеви за које је (бржим) пробабилистичким алгоритмима из трећег поглавља утврђено да су вероватно прости, заиста прости.

Следеће питање које се јасно поставља је како одабрати I тако да је F довољно велико. Наиме, у алгоритму смо захтевали да је $F \geqslant n^{1/3}$, па треба одредити да ли постоји прихватљиво I које нам може обезбедити фактор од $n^I - 1$ тражене величине. Како сваки прост број p такав да $p - 1 \mid I$ дели $n^I - 1$, Теорема 3 из поглавља 3.3 гарантује да постоји тражени број I мањи $(\ln n)^{c' \ln\ln n}$. Ово нам даје и оцену сложености алгоритма за просте бројеве n:

Теорема 3. Постоји позитивна константа c тако да је време за које алгоритам утврђује да је n прост број мање од $(\ln n)^{c \ln\ln n}$.

Иако овај алгоритам има асимптотски исту сложеност као алгоритми из Дела 4, у пракси се показује да је он доста лошији, и да самим тим није практичан.

У следећем задатку показаћемо како се уз помоћ познавања простих фактора броја $n-1$ до неке границе B у неким случајевима може испитати прималност броја n:

Задатак 1. Нека је $n - 1 = FR$ растављање броја $n - 1$ тако да R није

дељив простим бројем мањим од B. Уколико за природан број a важи

$$a^{n-1} \equiv 1 \pmod{n}, \qquad (a^{(n-1)/q}, n) = 1 \quad \text{за све просте } q \mid F$$

и $(a^F - 1, n) = 1$, тада је сваки прост фактор од n већи од BF. Специјално, уколико је $BF \geqslant n^{1/2}$, тада је n прост.

Решење. Нека је p најмањи прост делилац броја n, и нека је h поредак броја a по модулу p. Јасно $h \mid p-1$. Из другог услова $F \mid h$, док из трећег закључујемо да не може бити $(h, R) = 1$. Самим тим постоји прост број који дели h и R, па како је он барем B и узајамно је прост са F, то је $p \geqslant h + 1 > BF$.

Уколико је $BF \geqslant \sqrt{n}$, то је $p > \sqrt{n}$. Како је p најмањи прост делилац броја n, то мора бити $n = p$, тј. n је заиста прост. □

Део 7

АКС тест прималности

У 2002. години три индијска математичара, Маниндра Агравал[1], Нирај Кајал[2] и Нитин Саксена[3], остварили су циљ њихових претходника. Они су предложили детерминистички алгоритам полиномијалне сложености чија се коректност може доказати коришћењем само факултетских знања из алгебре. Овај алгоритам и доказ његове коректности биће изложени у овом поглављу.

7.1 Идеја алгоритма

Као и код многих претходних тестова, овај алгоритам заснива се на следећем добро познатом идентитету:

Идентитет. Нека су a и p узајамно прости природни бројеви. Тада је број p прост ако и само ако је

$$(x-a)^p \equiv x^p - a \pmod{p}. \tag{1}$$

Доказ. Нека је прво p прост број. Тада из биномног развоја и чињенице да је $\binom{p}{k}$ дељиво са p, за $1 \leqslant k \leqslant p-1$, добијамо $(x-a)^p \equiv x^p - a^p \pmod{p}$. Тражено сада следи на основу Мале Фермаове теореме.

Докажимо и други смер. Претпоставимо супротно, тј. да је p сложен и да $q^k \parallel p$, за неки прост број q. Тада $\binom{p}{q}$ није дељиво са p, па коефицијент уз x^q у биномном развоју леве стране није 0. Овим смо добили жељену контрадикцију, тј. број p је прост. □

[1] Manindra Agrawal - индијски математичар 1981-
[2] Neeraj Kayal - индијски математичар 1966-
[3] Nitin Saxena - индијски математичар 1981-

Према претходној теореми, да бисмо доказали да је p прост број довољно је проверити да ли претходни Идентитет важи. Међутим, у најгорем случају мораћемо да срачунамо p коефицијената леве стране једнакости, па је време алгоритма $\Omega(p)$. Зато ћемо дату једнакост посматрати и по модулу полинома облика $x^r - 1$. Јасно је да из датог идентитета за све a и r мора важити једнакост

$$(x-a)^p \equiv x^p - a \pmod{x^r - 1,\, p}. \tag{2}$$

Међутим, постоје и сложени бројеви p за које (2) важи за неке парове (a, r). Јасно је да се дата конгруенција може проверити у времену $O(r^2 \log^3 p)$, уколико користимо узастопна степеновања, или $O(r \log^2 p)$ коришћењем метода из другог поглавља. Дакле, основни проблем је повољан одабир броја r. У наредном поглављу показаћемо како ћемо то учинити.

Следећа теорема аналитичке теорије бројева биће од велике користи приликом одабира броја r. Напоменимо да ће од сада за базу свих логаритама бити узиман број 2.

Теорема 1. Нека је са $P(n)$ означен највећи прост делилац броја n. Тада постоји константа $c > 0$ и природан број n_0 такав да за све природне бројеве $x \geqslant n_0$ важи

$$\left| \{p \,|\, p \text{ је прост}, p \leqslant x \text{ и } P(p-1) > x^{2/3}\} \right| \geqslant c \cdot \frac{x}{\log x}.$$

7.2 Алгоритам и доказ његове исправности

Прикажимо прво алгоритам:

Алгоритам 7.1. (АКС тест прималности)
if (n oblika a^b, $b > 1$) ispisati SLOŽEN;
r=2;
while ($r < n$) {
    if (NZD$(n, r) \neq 1$) ispisati SLOŽEN;
    if (r je prost)
        q je najveći prost delilac od $r - 1$;
        if ($q \geqslant 4\sqrt{r} \log n$) i ($n^{\frac{n-1}{q}} \not\equiv 1 \pmod{r}$)
            break;
    $r = r + 1$;
}
for $a = 1$ to $2\sqrt{r} \log n$
    if ($(x-a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$) ispisati SLOŽEN;
ispisati PROST;

Циљ овог поглавља је доказ следеће теореме:

ТЕОРЕМА. Алгоритам враћа вредност `PROST` ако и само ако је n прост.

Ову теорему доказаћемо у неколико корака, кроз неколико теорема. Следећа теорема објашњава изглед `while` циклуса и биће од велике користи у следећем поглављу. Са $o_r(n)$ означен је ред броја n по модулу r:

Теорема 1. Постоје позитивне константе c_1 и c_2 за које постоји прост број r у интервалу

$$[c_1(\log n)^6, c_2(\log n)^6]$$

такав да $r-1$ има прост фактор $q \geqslant 4\sqrt{r}\log n$ и $q \mid o_r(n)$.

Доказ. Искористићемо Теорему 1 претходног дела поглавља. Број простих бројева r (звaћемо их *специјални*) између $c_1(\log n)^6$ и $c_2(\log n)^6$ таквих да је $P(r-1) > (c_2(\log n)^6)^{\frac{2}{3}} > r^{\frac{2}{3}}$ за довољно велико r је

$$\begin{aligned}
&\geqslant \text{број специјалних простих у } [1, c_2(\log n)^6] - \text{ број простих у } [1, c_1(\log n)^6] \\
&\geqslant \frac{cc_2(\log n)^6}{7\log\log n} - \frac{6c_1(\log n)^6}{6\log\log n} \quad \text{(по Теореми 1 из 1.7)} \\
&= \frac{(\log n)^6}{\log\log n}\left(\frac{cc_2}{7} - c_1\right).
\end{aligned}$$

Изаберимо c_1 и c_2 тако да је израз у загради, c_3, позитиван. Нека је $x = c_2(\log n)^6$. Посматрајмо производ

$$\Pi = (n-1)(n^2-1)\cdots(n^{x^{\frac{1}{3}}}-1).$$

Како је сваки природан број m дељив са највише $\log m$ различитих простих бројева, то Π садржи највише $\log n + \log n^2 + \ldots + \log n^{x^{\frac{1}{3}}} < x^{\frac{2}{3}}\log n$ простих фактора. Како је

$$x^{\frac{2}{3}}\log n < \frac{c_3(\log n^6)}{\log\log n},$$

то постоји *специјални* прост број r који не дели Π.

Приметимо да уколико изаберемо $c_1 \geqslant 4^6$, то је r управо тражени број. Наиме, $r-1$ има прост фактор $q \geqslant r^{\frac{2}{3}} \geqslant 4\sqrt{r}\log n$, а $q \mid o_r(n)$ јер је иначе $o_r(n) \leqslant \dfrac{r-1}{q} < r^{\frac{1}{3}}$, па би Π било дељиво са r. □

Сада није тешко видети да алгоритам враћа тачну вредност уколико је n прост број:

Теорема 2. Уколико је n прост, алгоритам враћа `PROST`.

Доказ. Како је за све $r \leqslant c_2(\log n)^6$ и n прост заиста $(x, r) = 1$, то се у `while` циклусу не може добити `SLOŽEN`. Према претходној теореми ни у `for` циклусу се не може добити `SLOŽEN`. □

Из Теореме 2 видимо да је потребно још само испитати исправност алгоритма за сложене бројеве n. Обратимо пажњу на r које добијамо из `while` циклуса (ово је управо један од бројева r који се добијају из Теореме 1). Нека је $n = \prod p_i^{\alpha_i}$ факторизација броја n на просте факторе. Како $o_r(n) \mid \text{НЗС}(\{o_r(p_i^{\alpha_i})\}_i)$, то постоји прост делилац p од n за који $q \mid o_r(p^\alpha)$, па самим тим и $p \mid o_r(p)$, јер је $(\alpha, r) = 1$. Нека је у наставку p управо овај прост број.

По завршетку `while` циклуса, `for` циклус узима добијену вредност за r и рачуна биноме $(x-a)^n$, за $1 \leqslant a \leqslant 2\sqrt{r}\log n$. Према делу (в) Теореме 1 из 1.6 постоји фактор полинома $\dfrac{x^r-1}{x-1}$, полином $h(x)$, који је степена $d = o_r(p)$ и иредуцибилан у $\mathbb{F}_p$. Како

$$(x-a)^n \equiv x^n - a \pmod{x^r-1, n} \quad \Rightarrow \quad (x-a)^n \equiv x^n - a \pmod{h(x), p},$$

то идентитети са биномима важе и у пољу $\mathbb{F}_p[X]/h(x)$. Следећа теорема карактерише групу коју чине $l = 2\sqrt{r}\log n$ бинома $x-a$, за $1 \leqslant a \leqslant l$:

Теорема 3. У пољу $\mathbb{F}_p[X]/h(x)$, група генерисана полиномима $(x-a)$, за $1 \leqslant a \leqslant l$, тј.

$$G = \{ \prod_{1 \leqslant a \leqslant l} (x-a)^{\alpha_a} \mid \alpha_a \geqslant 0 \},$$

је циклична и реда већег од $n^{2\sqrt{r}}$.

Доказ. Како је G подгрупа групе $(\mathbb{F}_p[X]/h(x))^*$, она је циклична.

Докажимо да су сви елемнти скупа

$$S = \{ \prod_{1 \leqslant a \leqslant l} (x-a)^{\alpha_a} \mid \sum_{1 \leqslant a \leqslant l} \alpha_a \leqslant d-1,\ \alpha_a \geqslant 0 \},$$

различити у $\mathbb{F}_p[X]/h(x)$. Како је $r > q > 4\sqrt{r}\log n > l$, то не постоје два a која су конгрунтна по модулу p, јер је иначе $p < l < r$, што је немогуће с обзиром да онда у алгоритму мора бити $(p, n) = 1$. Значи, свака два елемента у S су различита по модулу p, па како имају степен мањи од d, то су они различити и у $\mathbb{F}_p[X]/h(x)$. Кардиналност скупа S је

$$\binom{l+d-1}{l} = \frac{(l+d-1)(l+d-2)\cdots d}{l\,!} > \left(\frac{d}{l}\right)^l.$$

Како је $d \geqslant q = 2l$ и како је S подскуп од G, то је доказ у потпуности завршен. □

Нека је надаље $g(x)$ генератор групе G и нека је

$$I_{g(x)} = \{m \mid g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}.$$

Следеће теореме показују особине скупа $I_{g(x)}$:

Теорема 4. Скуп $I_{g(x)}$ затворен је за множење.
Доказ. Нека је $m_1, m_2 \in I_{g(x)}$. Тада је

$$g(x)^{m_1} \equiv g(x^{m_1}) \pmod{x^r - 1, p} \quad \wedge \quad g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p},$$

па заменом x^{m_1} у другу једнакост добијамо

$$g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^{m_1 r} - 1, p} \quad \Rightarrow \quad g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p},$$

јер $r \mid m_1 r$. Сада је јасно и

$$g(x)^{m_1 m_2} \equiv g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p},$$

што завршава наш доказ. □

Теорема 5. Нека је ред елемента $g(x)$ у $\mathbb{F}_p[X]/h(x)$ једнак o_g и $m_1, m_2 \in I_{g(x)}$. Тада

$$m_1 \equiv m_2 \pmod{r} \quad \Rightarrow \quad m_1 \equiv m_2 \pmod{o_g}.$$

Доказ. Како из $m_1 \equiv_r m_2$ следи $x^{m_1} \equiv x^{m_2} \pmod{x^r - 1, p}$, то је

$$g(x)^{m_1} g(x)^{kr} = g(x)^{m_2} \equiv g(x^{m_2}) \equiv g(x^{m_1}) \pmod{x^r - 1, p},$$

где је $m_2 = m_1 + kr$. Како $g(x) \not\equiv 0$ то се $g(x)^{m_1}$ може скратити са обе стране конгруенције, тј.

$$g(x)^{kr} \equiv 1 \pmod{x^r - 1, p}.$$

Значи $o_g \mid kr$, па самим тим $m_1 \equiv m_2 \pmod{o_g}$. □

Претходна теорема биће од великог значају у доказу следеће теореме, којом завршавамо доказ исправности алгоритма:

Теорема 6. Уколико је n сложен, алгоритам враћа `SLOŽEN`.
Доказ. Претпоставимо супротно, тј. да алгоритам враћа `PROST`. Тада у `for` циклусу увек важи једнакост, тј. за све $1 \leqslant a \leqslant 2\sqrt{r}\log n$,

$$(x - a)^n \equiv x^n - a \pmod{x^r - 1, p}.$$

Како је $g(x)$ производ неких бинома $(x - a)$, за $1 \leqslant a \leqslant l$, то је према претпоставци

$$g(x)^n \equiv g(x^n) \pmod{x^r - 1, p}.$$

Значи $n \in I_{g(x)}$. Према делу (а) Теореме 1 из 1.6 је $p \in I_{g(x)}$ и тривијално $1 \in I_{g(x)}$. Докажимо коришћењем Теореме 4 да је ово у супротности са Теоремом 5. Наиме, према овој теореми постоји највише r елемената скупа $I_{g(x)}$ који су мањи од o_g, а ми ћемо доказати да их под датим претпоставкама мора бити више.

Посматрајмо скуп

$$E = \{n^i p^j \mid 0 \leqslant i, j \leqslant [\sqrt{r}]\}.$$

Према Теореми 4 је $E \subset I_{g(x)}$. Како је $|E| = (1 + [\sqrt{r}])^2 > r$, то постоје $n^{i_1}p^{j_1}$ и $n^{i_2}p^{j_2}$, где је $(i_1, j_1) \neq (i_2, j_2)$, такви да је $n^{i_1}p^{j_1} \equiv_r n^{i_2}p^{j_2}$. Тада према Теореми 5 важи и $n^{i_1}p^{j_1} \equiv n^{i_2}p^{j_2} \pmod{o_g}$ односно

$$n^{i_1} \equiv n^{j_2}p^{j_2-j_1} \pmod{o_g},$$

јер је $(p, o_g) = 1$. Међутим, како је $o_g \geqslant n^{2\sqrt{r}}$, а $n^{i_1} < n^{\sqrt{r}}$ и $n^{|i_2|}p^{|j_2-j_1|} \leqslant n^{\sqrt{r}}p^{\sqrt{r}} \leqslant n^{2\sqrt{r}}$, то се претходна конгруенција може записати и као једнакост, па је p једини прост делилац броја n. Међутим, тада је или $n = p$ или $n = p^k$, за $k \geqslant 2$, а у оба случаја добијамо контрадикцију. □

7.3 Анализа сложености алгоритма

Нека је са $\widetilde{O}(t(n))$ означено $O(t(n)poly(\log t(n)))$.

Теорема 1. Сложеност алгоритма је $\widetilde{O}(\log^{12} n)$.

Доказ. Први корак алгоритма, тј. одређивање да ли је n потпун степен захтева време $O(\log^3 n)$. Према Теореми 2 претходног поглавља `while` циклус изврши $O(\log^6 n)$ итерација.

Одредимо колико је време потребно за извршење једне итерације у `while` циклусу. За први корак `while` циклуса потребно је асимптотско време $poly(\log\log r)$. За следећа два корака (испитивање да ли је r прост и одређивање највећег простог делиоца од $r-1$) потребно је време $r^{\frac{1}{2}} \cdot poly(\log\log n)$. За следећа три корака `while` циклуса потребно је време $poly(\log\log n)$, па је укупно време `while` циклуса $\widetilde{O}(\log^6 n \cdot r^{\frac{1}{2}}) = \widetilde{O}(\log^9 n)$.

Одредимо и време `for` циклуса. За једну итерацију, тј. за рачунања коефицијената у $(x-a)^n \equiv x^n - a \pmod{x^r, n}$, коришћењем узастопних квадрирања и брзог Фуријевог множења потребно је асимптотско време $\widetilde{O}(\log n \cdot r \log n)$. Значи, укупно време `for` циклуса је $\widetilde{O}(r^{\frac{3}{2}} \log^3 n) = \widetilde{O}(\log^{12} n)$, што је и време алгоритма. □

Међутим, у пракси овај алгоритам ради много брже. Доказаћемо да под претпоставком следеће хипотезе овај алгоритам ради у времену $\widetilde{O}(\log^6 n)$.

Дефиниција 1. Уколико су r и $\frac{r-1}{2}$ оба прости, број $\frac{r-1}{2}$ називамо Софи-Жерменов[4] прост број. Број r називаћемо ко-Софи-Жерменов прост број.

Хипотеза. Број ко-Софи-Жерменових простих бројева асимптотски се понаша као $\frac{Dx}{\log^2 x}$, где је $D = 0.660\ldots$ константа простих бројева близанаца.

Под претпоставком да је претходна хипотеза тачна, доказаћемо следећу теорему, коју касније користимо уместо слабије Теореме 2 из претходног поглавља:

Теорема 2. Постоји *специјалан* прост број r у интервалу

$$[64\log^2 n, c_2\log^2 n],$$

за све $n > n_0$, где су n_0 и c_2 позитивне константе.

Доказ. Приметимо да уколико је $q = \frac{r-1}{2}$ Софи-Жерменов прост број, тада је $o_r(n) \in \{1, 2, q, r-1\}$. Како n^2-1 може имати највише $2\log n$ различитих простих делилаца, то је и број простих бројева за који је $o_r(n) \in \{1, 2\}$ мањи од $2\log n$. Посматрајмо ко-Софи-Жерменове просте бројеве r који нису међу овим бројевима. Довољно је да

$$\frac{r-1}{2} \geqslant 4\sqrt{r}\log n, \quad \text{тј.} \quad r \geqslant 64\log^2 n.$$

Докажимо зато да за довољно велику константу c_2 постоји барем један ко-Софи-Жерменов прост број у интервалу $[64\log^2 n, c - 2\log^2 n]$. Према претходној хипотези константу c_2 је довољно изабрати тако да је

$$\frac{Dc_2\log^2 n}{\log^2(c_2\log^2 n)} > \frac{D\cdot 64\cdot\log^2 n}{\log^2(64\log^2 n))} + 2\log n.$$

За довољно велико n последња неједнакост сигурно важи за $c_2 > 64 + \frac{8}{D}$.□

Сада је под претпоставком **Хипотезе** време алгоритма једнако

$$\widetilde{O}(r^{\frac{1}{2}}\cdot(\log^2 n))(\text{за } \texttt{while} \text{ циклус}) + \widetilde{O}(r^{\frac{3}{2}}\cdot\log^3 n)(\text{за } \texttt{for} \text{ циклус}) = \widetilde{O}(\log^6 n).$$

[4]Marie-Sophie Germain - француска математичарка 1776-1831

Део 8

Елиптичке криве и тестови прималности

У до сада датим тестовима рачунања смо вршили у пољима $\mathbb{F}_p$, $\mathbb{F}_p[\varsigma_n]$ или $\mathbb{F}_p[X]/(f)$. У овом делу размотрићемо елиптичке криве, те за њих увести одговарајуће групе и те групе користити у даљим рачунањима.

8.1 Елиптичке криве

Пођимо од дефиниције елиптичке криве:

Дефиниција 1. Нека је $\mathbb{K}$ произвољно поље карактеристике различите од 2 и 3. Уколико полином $x^3 + ax + b$ $(a, b \in \mathbb{K})$ нема вишеструких корена, тада под *елиптичком кривом* над пољем $\mathbb{K}$ подразумевамо скуп тачака $(x, y) \in \mathbb{K}$ који задовољавају једначину

$$y^2 = x^3 + ax + b$$

допуњен тачком O коју називамо тачка у бесконачности.

Коментари. (1) Услов да полином $x^3 + ax + b$ нема вишеструких корена еквивалентан је регуларности криве $F(x, y) = y^2 - x^3 - ax - b$, односно да парцијални изводи $\dfrac{\partial F}{\partial x}$ и $\dfrac{\partial F}{\partial y}$ буду свуда различити од 0 (изводе полинома над произвољним пољем можемо увести на уобичајени начин). Последње је еквивалентно са $4a^3 + 27b^2 \neq 0$. Број $4a^3 + 27b^2$ називамо дискриминанта елиптичке криве.
(2) Елиптичке криве можемо посматрати у пројективној равни, као криву задату једначином

$$Y^2 = X^3 + aXZ^2 + bZ^3.$$

Тачка O одговара тачки $(0 : 1 : 0)$.

Као што смо и навели у уводу овог поглавља, елиптичку криву ћемо снабдети операцијом сабирања, тако да тако добијена структура буде

група.

Дефиниција 2. Нека су дате тачке $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ елиптичке криве E. Уколико је $x_2 = x_1$ и $y_2 = -y_1$ тада је $P + Q = O$. Иначе $P + Q = (x_3, y_3)$, где је

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

и

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1}, & P = Q \end{cases}$$

Коначно $P + O = O + P = P$.

Теорема 1. Структура $(E(\mathbb{Z}_p), +)$ је комутативна група.
Доказ. Из дефиниције сабирања јасно је да је неутрал за сабирање O и да је инверз тачке (x_1, y_1) тачка $(x_1, -y_1)$. Такође, комутативност директно следи из дефиниције сабирања, па је довољно проверити да важи асоцијативни закон. Ово се непосредно проверава коришћењем формула из дефиниције сабирања. □

О броју елемената и структури групе $E(\mathbb{Z}_p)$ говоре следеће теореме:

Теорема 2. (**Хасеова**[1] **теорема**) Ако је $|E(\mathbb{Z}_p)| = p + 1 - t$, тада је

$$|\, t \,| \leqslant 2\sqrt{p}.$$

Теорема 3. Важи

$$E(\mathbb{Z}_p) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2},$$

где $n_1 \mid n_2$ и $n_1 \mid p - 1$.

На следећем примеру показаћемо примену претходних теорема:

Задатак 1. Нека су E и E' елиптичке криве над $\mathbb{F}_{229}$ задате једначинама

$$y^2 = x^3 - 1, \qquad y^2 = x^3 - 8.$$

Одредити $|E|$, $|E'|$ и структуре ових група.
Доказ. Нека је $y^2 = x^3 + ax + b$ произвољна елиптичка крива над $\mathbb{F}_p$. Из дефиниције Лежандровог симбола број тачака на овој кривој можемо дати са

$$1 + \sum_{x=0}^{p-1} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right).$$

[1] Helmut Hasse - немачки математичар 1898-1979

Одредимо прво $|E|$ и структуру групе E. Нека је

$$(x^3-1)^{(229-1)/2} = \sum_{i=0}^{342} a_i x^i.$$

Према претходном, користећи Ојлеров критеријум, број тачака на E је

$$230 + \sum_{x=0}^{228} \left(\frac{x^3-1}{229}\right) \equiv 1 + \sum_{x=0}^{228} (x^3-1)^{114} = 1 + \sum_{i=0}^{342}\sum_{x=0}^{228} a_i x^i \pmod{229}.$$

Како је свако $x \in \mathbb{F}_{229}^*$ облика g^k, где је g примитивни корен по модулу 229, то је

$$\sum_{x=0}^{228} x^i \equiv_{229} \begin{cases} 0, & 228 \nmid i \\ -1, & 228 \mid i \end{cases}.$$

Самим тим важи

$$|E| \equiv 1 - a_{228} = 1 - \binom{114}{76} \pmod{229}.$$

Како је $||E| - 230| \leqslant 2 \cdot \sqrt{229}$, то је $|E| = 252$.

Одредимо и структуру групе E. Прво, свака тачка $P = (x, y)$ из E таква да је $(2) \cdot P = O$ је једнака O или је $y = 0$. Значи, уколико је $P \neq O$ мора важити $0 = x^3 - 1 = (x-1)(x^2+x+1)$. Ова једначина има три решења ако и само ако једначина $x^2 + x + 1 = 0$ има решење у $\mathbb{F}_{229}$. Множењем са 4 добијамо еквивалентну једначину $(2x+1)^2 + 3 = 0$, а она има решења јер је $\left(\frac{-3}{229}\right) = 1$. Самим тим, у E постоје барем три елемента реда 2, па E није циклична. Значи $E \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, где $n_1 \mid n_2$, $n_1 \mid 228$ и $n_1 \cdot n_2 = 252$. Из ових релација је јасно да $n_1 \mid 6$, а из претходног да $2 \mid n_1$.

Одредимо и број елемената реда 3. Нека је $P = (x, y)$ тачка реда 3. Тада је x-координата тачке $2P$ једнака x-координати тачке P, односно $\frac{9x^4}{4y^2} - 2x = x$. Заменом $y^2 = x^3 - 1$ добијамо $x(5x^3 + 4) = 0$. Како се сва четири решења ове једначине налазе на криви, то постоји 8 тачака реда 3. Одавде закључујемо да $3 \mid n_1$, па је јасно

$$E \cong \mathbb{Z}_6 \times \mathbb{Z}_{42}.$$

На сличан начин као и у случају криве E, проналазимо да је

$$|E'| \equiv 1 - 2^{114}\binom{114}{38} \pmod{229},$$

односно због $||E'| - 230| \leqslant 2\sqrt{229}$, да је $|E'| = 252$. Такође, на сличан начин закључујемо и да једначина $0 = x^3 - 8$ има три решења, па на кривој постоје

три тачке реда 2. Самим тим, E' није циклична и уколико је $E' \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, то $2 \mid n_1, n_2$. Такође, закључујемо и да тачка $P = (x, y)$ реда 3 задовољава једначину

$$x(5x^4 + 32) = 0.$$

Међутим, решење $x = 0$ ове једначине се не налази на кривој, јер $\left(\frac{8}{229}\right) = -1$, па постоји највише 6 тачака реда 3. Самим тим $3 \nmid n_1$, па $n_1 \mid 4$. Значи, довољно је одредити да ли је $n_1 = 2$ или $n_1 = 4$. Последње одређујемо посматрањем броја тачака реда 4. За сваку тачку $P = (x, y)$ реда 4 је y-координата тачке $(2) \cdot P$ једнака 0, односно

$$-y + \frac{3x^2}{2y}\left(3x - \frac{9x^4}{4y^2}\right) = 0.$$

Сређивањем добијамо једначину $x^6 - 32x^3 - 64 = 0$, која је еквивалентна са $x^6 - 4x^3 - 1 = 0$. Ова једначина има 6 решења, којима одговарају тачке реда 2 и 4. Самим тим $4 \mid n_1$, односно

$$E' \cong \mathbb{Z}_4 \times \mathbb{Z}_{52}.$$

□

8.2 Одређивање броја тачака на $E(\mathbb{Z}_p)$

У овом поглављу даћемо полиномијани алгоритам за рачунање реда групе $E(\mathbb{F}_p)$.

Приметимо да су координате збира две тачке елиптичке криве рационалне функције координата сабирака. Самим тим, хомоморфизам на $\mathbb{F}_p$ индуковаће природно и хомоморфизам на $E(\mathbb{F}_p)$. Посматрајмо зато Фробенијусов хомоморфизам и одговарајући хомоморфизам Φ на $E(\mathbb{F}_p)$ ($\Phi(x, y) = (x^p, y^p)$ и $\Phi(O) = O$). Уколико са $(n) \cdot P$ означимо збир n тачака P, важи следећа теорема:

Теорема 1. Уколико је $|E(\mathbb{F}_p)| = p + 1 - t$, тада је

$$\Phi^2(P) - (t) \cdot \Phi(P) + (p) \cdot P = 0,$$

за сваку тачку $P \in E(\overline{\mathbb{F}}_p)$, где је $\overline{\mathbb{F}}_p$ алгебарско затворење поља $\mathbb{F}_p$.

Размотримо сада тачке $P \in E(\overline{\mathbb{F}}_p)$ такве да је $(n) \cdot P = O$, за дати природан број n. За овај скуп, у ознаци $E[n]$, важи:

Теорема 2. (1) $E[n]$ је подгрупа групе $E(\overline{\mathbb{F}}_p)$.
(2) Φ слика $E[n]$ у себе.

Доказ. (1) Из комутативности, уколико је $(n)\cdot P = O$ и $(n)\cdot Q = O$ јасно је и $(n)\cdot(P+Q) = O$.
(2) Како је сабирање рационална функција на координатама и Φ хомоморфизам, то из $(n)\cdot P = O$ заиста следи $(n)\cdot\Phi(P) = O$. □

Претходне две теореме дају

$$\Phi^2(P) - (t \bmod n)\cdot\Phi(P) + (p \bmod n)\cdot P = 0, \quad \text{за све} \quad P \in E[n]. \qquad (*)$$

Основна идеја алгоритма је да за разне (мале) вредности одредимо $t \bmod n$ испробавањем. Следећи полиноми помоћи ће у тестирању услова $(*)$:

Дефиниција 1. Елиптичкој кривој $E(\mathbb{F}_p)$ са једначином $Y^2 = X^3 + aX + b$ доделимо полиноме $\Phi_n(x,y) \in \mathbb{F}_p[X,Y]/(Y^2 - X^3 - aX - b)$ на следећи начин:

$$\Phi_{-1} = -1, \quad \Phi_0 = 0, \quad \Phi_1 = 1, \quad \Phi_2 = 2Y,$$

$$\Phi_3 = 3X^4 + 6aX^2 + 12bX - a^2, \quad \Phi_4 = 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4abX - 8b^2 - a^3),$$

односно у осталим случајевима са

$$\begin{aligned} \Phi_{2n} &= \Phi_n(\Phi_{n+2}\Phi_{n-1}^2 - \Phi_{n-2}\Phi_{n+1}^2)/(2Y), \\ \Phi_{2n+1} &= \Phi_{n+2}\Phi_n^3 - \Phi_{n+1}^3\Phi_{n-1}. \end{aligned}$$

Основне особине полинома Φ_n, као и њихову везу са $(n)\cdot P$ даје следећа теорема. Доказ теореме изводи се директно из дефиниције сабирања у $E(\mathbb{F}_p)$ и дате рекурентне релације за полиноме Φ_n.

Теорема 3. За непарно n $\Phi_n(X,Y)$ је полином само по X, а за парно n $\Phi_n(X,Y)$ је Y пута полином само по X. Ако је n непарно и $p \nmid n$ важи $\deg\Phi_n = (n^2-1)/2$, а ако је n парно и $p \nmid n$ степен Φ_n по X је $(n^2-4)/2$. За тачку $(x,y) \in E(\mathbb{F}_p) \setminus E[2]$ важи $(n)\cdot(x,y) = O$ ако и само ако је $\Phi_n(x,y) = 0$. Такође, ако је $(x,y) \in E(\overline{\mathbb{F}}_p) \setminus E[n]$ важи

$$(n)\cdot(x,y) = \left(x - \frac{\Phi_{n-1}\Phi_{n+1}}{\Phi_n^2}, \frac{\Phi_{n+2}\Phi_{n-1}^2 - \Phi_{n-2}\Phi_{n+1}^2}{4y\Phi_n^3}\right).$$

□

Из релације $(*)$ јасно је да постоји јединствен природан број $t \in [0, l-1]$ тако да је

$$(x^{p^2}, y^{p^2}) + (p \bmod l)\cdot(x,y) = (t)\cdot(x^p, y^p). \quad \text{за све} \quad (x,y) \in E[l] \setminus \{O\}. \qquad (*)$$

Уколико бисмо ово јединствено t могли да одредимо, знали бисмо и да је остатак при дељењу $E(\mathbb{F}_p)$ са l једнак $p + 1 - t$.

Сада можемо да поступамо на следећи начин. Тачке на криви представимо као парове полинома по X и Y. Полиноме редукујемо по $Y^2 - X^3 - aX - b$, тако да је степен Y највише 1. Како су све тачке у $E[n]$, полиноме затим редукујемо по Φ_n које израчунавамо из претходне теореме.

На крају дајемо начин на који можемо избећи експлицитно израчунавање инверза полинома (које иначе радимо Еуклидовим алгоритмом). Разматраћемо *рационални* облик елиптичке криве. Тачку ћемо посматрати као $P = (U/V, F/G)$, где су U, V, F и G полиноми по променљивама X и Y. Испоставља се да уз дате редукције, тачке које разматрамо морају бити облика

$$P = (N(X)/D(X), YM(X)/C(X)).$$

Сада можемо дати и сам алгоритам. Алгоритам враћа остатак при дељењу $E(\mathbb{F}_p)$ са l, где је l прост број којим вршимо тестирање (l је много мање од p). Овај алгоритам затим понављамо за разне l, све док $\prod l$ није веће од $4\sqrt{p}$ и затим Кинеском теоремом о остацима одређујемо $E(\mathbb{F}_p)$.

Алгоритам 8.1. (Одређивање $|E(\mathbb{F}_p)|$)

1. [Slučaj $l = 2$]
   if $(l = 2)\{$
   $g(X) = (X^p - X, X^3 + aX + b)$; //NZD polinoma
   if $(g(X) = 1)$ vrati 0;
   vrati 1;
   $\}$
2. [Relacija (**)]
   $\overline{p} = p \bmod l$;
   $u(X) = X^p \bmod (\Phi_l, p)$;
   $v(X) = (X^3 + ax + b)^{(p-1)/2} \bmod (\Phi_l, p)$;
   $P_0 = (u(X), Yv(X))$;
   $P_1 = (u(X)^p \bmod (\Phi_l, p),\ Yv(X)^{p+1} \bmod (\Phi_l, p))$;
   Pomoću Teoreme 3 predstavi $P_2 = (\overline{p}) \cdot (X, Y)$
   u obliku $(N(X)/D(X), YM(X)/C(X))$;
   if $(P_1 + P_2 = O)$ vrati 0;
   $P_3 = P_0$;
   for $(1 \leqslant k \leqslant l/2)\{$
   if (X-koordinate $P_1 + P_2$ i P_3 jednake)$\{$
   if (Y-koordinate jednake) vrati k;
   vrati $l - k$;
   $\}$
   $P_3 = P_3 + P_0$;
   $\}$

Време рада овог алгоритма је $O(\ln^8 n)$. Пажљивијим бирањем бројева l и полинома f_l који деле Φ_l, време рада алгоритма се може спустити на $O(\ln^{5+\epsilon} n)$.

8.3 Тест прималности помоћу елиптичких кривих

Као што је у претходним поглављима напоменуто, за тест прималности је довољно да за дати број, који је скоро сигурно прост, доказује да је он заиста прост. Зато ћемо број који тестирамо третирати као прост број.

Основу теста чини следећи аналог Поклингтонове теореме:

Теорема 1. Нека је $N > 1$ цео број узајамно прост са 6 и E елиптичка крива по модулу N. Уколико цео број m и тачка $P \in E(\mathbb{Z}_N)$ задовољавају услове:
(1) Постоји прост делилац q од m такав да је

$$q > (\sqrt[4]{N} + 1)^2;$$

(2) $(m) \cdot P = O$;
(3) $(m/q) \cdot P = (x : y : t)$ где је $t \in \mathbb{Z}_N^*$;
тада је N прост.
Доказ. Нека је p најмањи прост делилац броја N. Редуковањем по модулу p закључујемо да је ред тачке P у групи $E(\mathbb{Z}_p)$ делилац броја m, али да није делилац броја m/q. Како је q прост залључујемо да је ред тачке P у $E(\mathbb{Z}_p)$ дељив са q, па је $q \leqslant |E(\mathbb{Z}_p)|$. Према Хасеовој теореми закључујемо да је $q < (\sqrt{p} + 1)^2$. Сада, уколико је N сложен важи $\sqrt{N} \geqslant p$, што доводи до очигледне контрадикције. □

Да бисмо ову теорему могли практично да искористимо морамо знати три ствари: како изабрати елиптичку криву, како одредити тачку P и како наћи број m, наравно уколико они уопште постоје. Следећа теорема даје нам одговор на треће, уједно и најтеже питање:

Теорема 2. Нека је N природан број узајамно прост са 6, E елиптичка крива над $\mathbb{Z}_N$ и $m = |E(\mathbb{Z}_N)|$. Уколико је m прост делилац броја q такав да је

$$q > (\sqrt[4]{N} + 1)^2,$$

тада постоји тачка $P \in E(\mathbb{Z}_N)$ тако да је

$$(m) \cdot P = O \quad \text{и} \quad (m/q) \cdot P = (x : y : t) \text{ где је } t \in \mathbb{Z}_N^*.$$

Доказ. Како је m ред групе $E(\mathbb{Z}_N)$, то је први услов задовољен за све тачке $P \in E(\mathbb{Z}_N)$. Како је у алгоритму претпостављено да је N прост, довољно је да P одредимо тако да $(m/q) \cdot P \neq O$.

Претпоставимо да жељена тачка не постоји. Тада ред сваког елемента у групи $E(\mathbb{Z}_N)$ мора бити делилац броја m/q, па је експонент групе $E(\mathbb{Z}_N)$ делилац броја m/q. Даље, према Теореми 3 првог дела овог поглавља, важи

$$E(\mathbb{Z}_N) = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}, \quad d_2 \mid d_1.$$

Према томе експонент групе $E(\mathbb{Z}_N)$ је d_1, па је $m = |E(\mathbb{Z}_N)| = d_1 d_2 \leqslant d_1^2 \leqslant (m/q)^2$, односно $q^2 \leqslant m$. Међутим, на основу Хасеове теореме имамо да је $m < (\sqrt{N}+1)^2$, што даје контрадикцију са одабиром броја q. □

У претходном делу поглавља дали смо ефикасни (полиномијални) алгоритам за рачунање реда групе елиптичке криве $E(\mathbb{Z}_p)$, па сада можемо дати и тест прималности:

Алгоритам 8.2. (Тест прималности помоћу елиптичких кривих)

$i = 0$;
$N_0 = N$;
1. [Test]
while ($N_i > 2^{30}$){
  Proizvoljno izabrati a i b iz $\mathbb{Z}_{N_i}$ tako da je $(4a^3 + 27b^2, N_i) = 1$;
  //E je eliptička kriva sa jedačinom $y^2 = x^3 + ax + b$
  $m = |E(\mathbb{Z}_{N_i})|$;
  $q = m/2$;
  if (q ne prolazi Rabin-Milerov test ili $q \leqslant (\sqrt[4]{N_i}+1)^2$) continue;
  repeat{
    Izabrati proizvoljan $x \in \mathbb{Z}_{N_i}$ tako da je $\left(\dfrac{x^3+ax+b}{N_i}\right)$ 0 ili 1;
    Odrediti y tako da je $y^2 = x^3 + ax + b$;
    if ($(m) \cdot P \neq O$) goto Povratak;
  } until ($(m/q) \cdot P \neq O$)
  $i = i + 1$;
  $N_i = q$;
}
for (p prost, $p \leqslant 2^{15}$)
  if ($p \mid N_i$) goto Povratak;
2. [Povratak]
if ($i = 0$) vrati SLOŽEN;
else {
  $i = i - 1$;
  goto Test;
}
vrati PROST;

Јасно је да је дати алгоритам полиномијални. Испоставља се да је његово време рада $O(\ln^{12} n)$, па он није практичан. У наставку поглавља приказаћемо идеје на којима се заснива практична верзија овог алгоритма.

8.4 Еткин-Моренов тест прималности

У претходном тесту користили смо фиксирану елиптичку криву и затим рачунали ред њене групе. Основна идеја код Аткин[2]-Морен[3]-овог теста је да урадимо обрнуто, тј. да за фиксирани број нађемо елиптичку криву чији ће ред групе бити баш тај број.

Пресудну улогу у проналажењу адекватних редова група имају квадратна представљања, односно, за $D < 0$, $D \equiv 0, 1 \pmod 4$ и p прост број, представљања у облику

$$x^2 + |D|y^2 = 4p.$$

Нека је за једно такво представљање $\pi = \dfrac{x + y\sqrt{D}}{2}$, а самим тим и $\pi\overline{\pi} = p$. Показају се да је за прост број N тада

$$m = |E(\mathbb{Z}/N\mathbb{Z})| = N + 1 - \pi - \overline{\pi} = N + 1 - x,$$

где је E елиптичка крива која једноставно зависи од D. Ипак, иако имамо ред групе $E(\mathbb{Z}/N\mathbb{Z})$, треба испитати је да ли он задовољава услове Теореме 1 из претходног поглавља. Уколико то није случај узимамо нову вредност за D, све док не пронађемо одговарајуће m.

Нека су погодни m и одговарјућа дискриминанта D пронађени. Следеће што је потребно одредити је експлицитну криву над којом ћемо вршити тестирање. Показује се да за $D = -4$ постоје четири изоморфне класе кривих, да за $D = -3$ постоји шест, а за $D \neq -3, -4$ постоје две класе изоморфних кривих чија је то дискриминанта.

Последње што је потребно урадити је за дато D одредити која класа кривих је задовољавајућа. За $D = -3, -4$ директан услов није тешко дати, док је сличан услов готово немогуће дати у трећем случају. Тада за разне (случајне) тачке P са криве одређујемо да ли је $(m) \cdot P = O$ и ако није ту криву одбацујемо. Уколико тај услов јесте задовољен то нам не даје гаранцију да је крива пронађена, али ипак ту криву вероватно можемо користити у Теореми 1 из претходног поглавља.

Овај тест није детерминистички, али је практичан. Његово време рада је $O(\ln^{5+\epsilon} n)$. Уз тест Јакобијевим сумама, овај тест се показује као најбољи за доказивање прималности бројева за које смо претходно утврдили

[2]Arthur Oliver Lonsadale Atkin - енгески математичар 1925-2008

[3]Francois Morain - француски математичар

да су скоро сигурно прости. Овим алгоритмом може се доказивати прималност бројева са више од 1000 цифара у декадном запису. Највећи број чија је прималност доказана овим алгоритмом има 20562 цифре и једнак је:

$$(((((((2^3+3)^3+30)^3+6)^3+12)^3+894)^3+3636)^3+70756)^3+97220.$$

Литература

[1] О. Н. Василенко, *Теоретико-числовые алгоритмы в криптографии*, МЦНМО, 2003.

[2] Душан Ђукић, Зоран Каделбург, Владимир Мићић, *Увод у теорију бројева*, Друштво математичара Србије, 2004.

[3] Гојко Калајџић, *Алгебра*, Математички факултет, 2004.

[4] Жарко Мијајловић, *Алгебра 2*, Скрипта, 2001.

[5] А. Б. Черемушкин, *Лекции по арифметическим алгоритмам в криптографии*, МЦНМО, 2004.

[6] L.M. Adleman, C. Pomerance, R.S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math, 1983.

[7] M. Agrawal, N. Kayan, N. Saxena, *PRIMES is in P*, Preprint, 2003.

[8] Tom Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.

[9] Eric Bach, Jeffrey Shallit, *Algorithmic Number Theory, Volume I: Efficient Algorithms*, The MIT Press, 1996.

[10] Alan Baker, *A Concise Introduction to the Theory of Numbers*, Cambridge University Press, 1986.

[11] Richard Crandall, Carl Pomerance, *Prime numbers: A Computational Perspective*, Springer, 2001.

[12] Henry Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993.

[13] Harold Davenport, *Multiplicative Number Theory*, Springer, 1980.

[14] Martin Dietzfelbinger, *Primality Testing in Polynomial Time*, Springer, 2004.

[15] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford: Clarendon Press, 1960.

[16] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1982.

[17] Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994.

[18] Serge Lang, *Algebra*, Springer, 2002.

[19] H.W. Lentra, *Primality testing algorithms*, Séminaire Bourbaki, 1980-1981.

[20] H. L. Montgomery, I. Niven, H. S. Zucherman, *An Introduction to the Theory of Numbers*, John Wiley and Sons, 1991.

[21] Yuri Ivanovic Manin, Alexei Panchishkin, *Introduction to Modern Number Theory*, Springer, 2005.

[22] Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, book draft, 2003.

[23] Douglas Stinson, *Cryptography: Theory and Practice*, Chapman and Hall/CRC, 2006.