УНИВЕРЗИТЕТ ЦРНЕ ГОРЕ

Природно-математички факултет Подгорица

Анђела Јовановић

Прости бројеви око нас

СПЕЦИЈАЛИСТИЧКИ РАД

Подгорица, 2018.

УНИВЕРЗИТЕТ ЦРНЕ ГОРЕ

Природно-математички факултет Подгорица

Прости бројеви око нас

СПЕЦИЈАЛИСТИЧКИ РАД

Математика

Ментор: Владимир Божовић

Анђела Јовановић

Студијски програм: Математика и рачунарске науке

Подгорица, јул 2018.

Посвета

Захваљујем се мојим најмилијима

Апстракт

Разлог због кога сам жељели да обрадимо ову тему је велико интересовање за расподјелу простих бројева. Привукла нас је мистерија непредвидивости која описује распрострањеност простих бројева. Наравно, овим рад је темељен на изучавању теорија које су поставили највећи савремени математичари. Прости бројеви су можда највише истраживана тема којом се највећа наука бави, а одговори још увијек нису дати. Трагајући за њима, слушали смо предавања највећих математичара данашњице, чија разматрања смо обрадили и покушали да приближимо.

На самом почетку, дефинисаћемо и објаснити неопходне појмове, а затим доказати теореме које ће нас увести у причу о простим бројевима. Објаснићемо њихов приказ, а затим се осврнути на карактристичне бројеве, који су у великом помогли да дођемо до важних резултата. Покушаћемо да уђемо у срж проблематике и објаснимо проблем растојања између простих бројева.

Дакле, од једноставности до врло компликованих закључака које доносимо, улазимо у свијет простих бројева.

Abstract

The reason I wanted to deal with this topic is huge interest in distributing prime numbers. I was attracted by a mystery of unpredictability that describes the prevalence of primes. Of course, this work is based on studying the theories set by the greatest mathematician today. Primes are perhaps the most explored topic with which the biggest science deals, and the answers are still not given. Looking for them, we listened to the lectures of the greatest mathematicians of today, whose considerations we have processed and tried to get closer.

At the very beginning, we will define and explain the necessary concepts, and then prove the theorems that will introduce us into the story of primes. We will explain their presentation, and then look at the characteristic numbers, which greatly helped us to get important results. We will try to get at the core of the problem and explain the problem of distance between primes.

So, from simplicity to very complicated conclusions we bring, we enter the world of free numbers.

Садржај

Глава 1

Увод

Када је Бекам прешао у Реал Мадрид фасцинантан је био одабир броја на његовом дресу. Сви су били у чуду зашто је баш изабрао број 23. Велики Раул имао је 7 на леђима. Роналдо, најбољи играч данашњице 11, док и у кошарци М. Џордан је освајао титуле са 23ом. Ови играчи били су круцијални састав својих тимова и сви су играли са простим бројевима на дресевима. Прости бројеви су дјељиви са собом и са јединицом. Тимови, чију су част браниили су били свјесни ових спортских величина и тога да побједе без њих нема. Зато они постају недјељив дио екипе, а ови бројеви крију тајну успјеха. Прости бројеви представљају једну од највећих мистерија математике. Њиховим множењем добијамо све бројеве, док они граде само себе. Због њихове недјељивости називамо их атомима аритметике.

Направите звучни талас, он је гласан кад је број прост, тих кад није. Посматрајмо функцију математички. Слушајући талас узимамо одговарајући функцију. Међутим, ноте нам дају повезаност, али не одговор.

У раду ћемо видјети најбитније, али и најзанимљивије чињенице о простим бројевима.

Глава 2

Теорија простих бројева

Прости бројеви представљају једну од највећих мистерија математике. Да би приближили њихов свијет, прво ћемо објаснити основне појмове и навести најважније теореме.

Дефиниција 1. *Нека су a и b цијели бројеви, гдје је $b \neq 0$. Кажемо да број a дијели број b ако постоји природан број t такав да важи: $b = t \cdot a$. Записујемо: $a \mid b$.*

Дефиниција 2. *Број $a > 1$ је прост уколико је дјељив само са собом и са јединицом. Број који није прост је сложен.*

Дефиниција 3. *Број k је највећи заједнички дјелилац бројева a и b, са ознаком* **нзд**(a, b)*, ако $k|b$ и $k|a$ и не постоји $k' > k$ тако да $k'|a$ и $k'|b$.*

Дефиниција 4. *Бројеви a и b су релативно прости ако је највећи заједнички дјелитељ бројева a и b једнак 1, тј. бројеви a и b немају заједничких фактора или нзд(a,b)=1.*

Дефиниција 5. *Прави дјелитељ природног броја a је број b који дијели тај број различит од 1 и од њега самога.*

Теорема 1. *Сваки природни број је дјељив са бар једним простим бројем.*

Доказ.

Ако је n прост број, дјељив је самим собом, а ако је сложен онда има праве дјелитеље. Међу њима постоји најмањи. Означимо га са p. Он мора бити прост број, јер ако би био сложен, постојао би његов прави дјелитељ, а то би био уједно и дјелитељ од n, мањи од p. То нас доводи до контадикције. □

Теорема 2. *Сваки сложен број можемо написати као производ простих бројева.*

Доказ.

Нека је p_1 најмањи прост број, прави дјелилац сложеног броја n. Тада постоји q_1, тако да $q_1 = \frac{n}{p_1}$ имамо

$$n = p_1 \cdot q_1.$$

Ако је q_1 сложен, онда постоји најмањи прости број p_2 такав да $n = p_1 \cdot p_2 \cdot q_2$. Настављамо понављање овог поступка. У једном тренутку сваки сложен дјелилалац броја n ће бити представљен у облику производа простих, а број n као производ свих:

$$n = p_1 \cdot p_2 \cdots p_n$$

, гдје је $n > q_1 > q_2 > q_3 ...$ □

Дефиниција 6. *Представљање броја n у облику производа простих бројева називамо канонски облик броја n.*

Теорема 3. *Сваки цијели број $n > 1$ се може представити у канонском облику.*

Доказ.

Ако је n прост број, тврђење очигледно важи.

Претпоставимо да тврђење важи за сваки сложен број мањи од n. Ако је n сложен број, тада постоји цијели број d такав да је $1 < d < n$ и $d|n$. Означимо са m најмањи такав број. Број m не може бити сложен, јер би у том случају постојао цијели број k, такав да је $1 < k < m$ и $k|m$, што повлачи да је $k|n$. То је, међутим, у контрадикцији са претпоставком да је m најмањи цијели број већи од 1 који је дјелитељ од n. Дакле, m је прост број. Означимо га са p_1. Слиједи да је $n = p_1 \cdot n_1$, гдје је $1 < n_1 < n$. По претпоставци индукције број n_1 се може представити у облику простих фактора, према томе, онда може и n. Групишући једнаке преостале факторе броја n, закључујемо да се сваки цио број већи од 1 може представити у облику производа

$$\prod_{i=1}^{n} p_i^{\alpha_i} \quad i = 1, 2, .., n.$$

□

Дефинишући основне појмове и теореме неопходне за наш рад, потребно је формулисати и доказати теорему која је врло значајна како за саму ариметику , тако и за Теорију бројева. Ријеч је о Основној Теореми Аритметике, коју наводимо у даљем тексту.

Теорема 4. *Сваки цијели број $n \geq 1$ има јединствен канонски облик.*

Доказ.

Канонско представљање постоји на основу Теореме 4. Преостаје да докажемо да је то представљање јединствено. Претпоставимо да постоји позитиван сложен број већи од 1 који се може на два различита начина представити у канонском

облику. Нека је n најмањи такав број са представљањима:

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k \qquad n = q_1 \cdot q_2 \cdot ... \cdot q_m.$$

Не постоји прост број p који се појављује у обје канонске репрезентације броја n, јер би у том случају и број $n' = \frac{n}{p}$ који је мањи од n, имао двије различите канонске репрезентације, што је у контрадикцији са претпоставком о минималности броја n. Можемо претпоставити да је

$$p_1 \leq p_2 \leq \ldots \leq p_k \qquad q_1 \leq q_2 \leq \ldots \leq q_m$$

. За просте факторе p_1 и q_1 важи $p_1 \neq q_1$, па можемо узети $p_1 < q_1$.

Нека је $N = p_1 \cdot q_2 \cdot \ldots \cdot q_m$. Како је $p_1|n$ и $p_1|N$, слиједи да је $p_1|(n - N)$, гдје је

$$n - N = (q_1 - p_1) \cdot q_2 \cdot ... \cdot q_m > 1.$$

Слиједи да се број $n - N$ може написати у облику $p_1 \cdot t_1 \cdot ... \cdot t_h$, гдје су ти прости бројеви за $i = 1, 2, \ldots, h$. Са друге стране, ако је $q_1 - p_1 > 1$, онда се $q_1 - p_1$ може написати као производ простих фактора, на примјер $(q_1 - p_1) = r_1 \cdot r_2 \cdot r_3 ... \cdot r_s$, па добијамо, на други начин, у облику производа простих фактора:

$$N - n = r_1 \cdot r_2 \cdot ... \cdot r_s \cdot q_2 \cdot q_3 ... \cdot q_m.$$

Ова последња факторизација не садржи прост фактор p_1. Знамо да је $p_1 \neq 1$, за $i = 1, 2, \ldots, m$; са друге стране $p_1 \neq r_j$, за $j = 1, 2, \ldots, s$, јер p_1 није дјелитељ од $p_1 - q_1$. Дакле, број $n - N$ има двије различите факторизације, јер само једна од њих садржи прост фактор p_1. То важи и у случају када је $p_1 - q_1 = 1$. Међутим,

$1 < n - N < n$ што је у контрадикцији са претпоставком о минималности броја n да не постоји цио број већи од 1, који се може представити на два начина у канонском облику. □

Теорема 5. ***(Еуклид)*** *Скуп свих простих бројева је бесконачан.*

Доказ.

Претпоставимо супротно тј. да их има коначно много. Ако их означимо са $p_1, p_2, \ldots, p_n$ тада дефинишемо

$$P = p_1 \cdots p_n + 1.$$

Тада P није дјељив са нити једним простим бројем, а из прве теореме закључујемо да је P или прост или има простог дјелитеља који је тада различит од свих $p_i, i = 1, ..., n$. То је у контрадикцији са претпоставком те смо доказали тврђење. □

Знајући претходно формулисане теореме, постављамо питање приказати просте бројеве? Наводимо примјер како то изгледа у $c++$ коду.

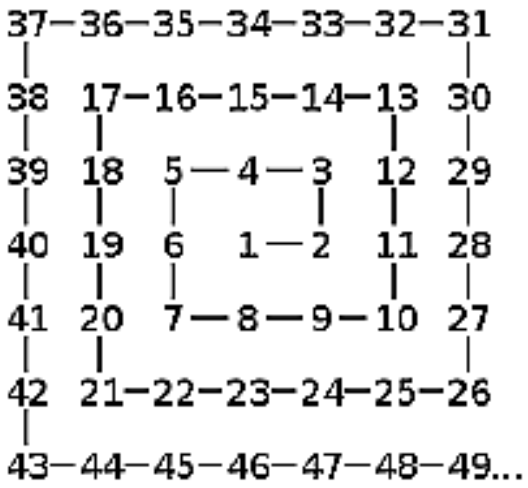
```
int main ()
{
    for (int i=2; i<100; i++)
        for (int j=2; j*j<=i; j++)
        {
            if (i % j == 0)
                break;
            else if (j+1 > sqrt(i)) {
                cout << i << " ";

            }

        }

    return 0;
}
```

Један од начина да прикажемо просте бројеве је да нацртамо правоуглу спиралу и посматрамо дијагонале. На тим дијагоналама видјећемо само просте бројеве. Поменута спирала, о којој ћемо говорити, назива се Уламова спирала.

2.1 Уламова спирала

Уламова спирала је једноставан начин визуализације простих бројева. Потребно је написати бројеве од 1 па надаље у облику правоугле спирале, те након тога побрисати све бројеве осим простих, на тај начин се добију занимљиви облици. Открио ју је Станислав Улам 1963. године док се досађивао на састанку црткарајући по папиру, примјетивши да се прости бројеви налазе на дијагоналама. Убрзо након тога је са сарадницима Мајроном Стејном и Марком Велсом користећи МАНИАК II (Mathematical Analyzer Numerical Integrator Computer

Model II) у истраживачкој лабораторији у Лос Аламосу, генерисао слику спирале која је обухватала бројеве до 65,000.

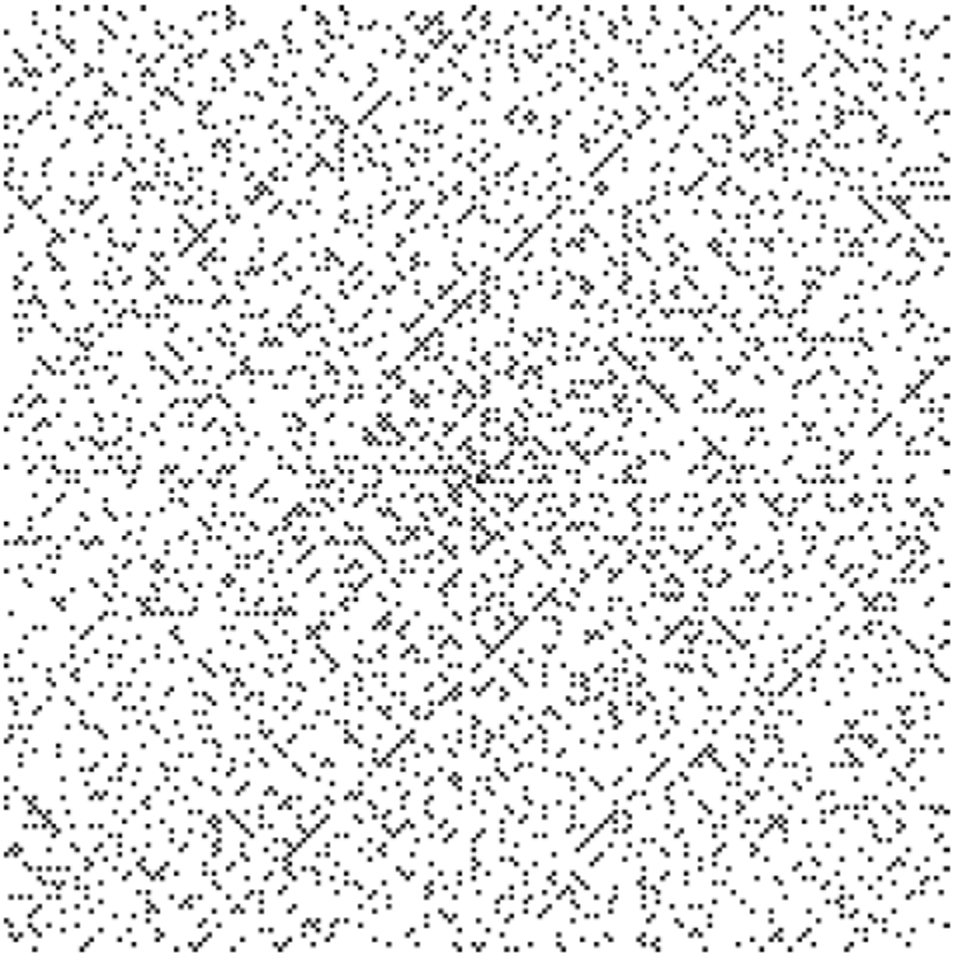


Након што смо одговорили на питање које се односи на кардиналност скупа простих бројева, те утврдили да их има бесконачно, занима нас да ли постоји шаблон по ком можемо ефикасно издвојити просте бројеве? Овим питањем, међу првима, бавио се старогрчки математичар Ератостен. Та метода коју је установио је препозната као *Ератостеново сито.*

2.2 Ератостеново сито

Прије описивања Ератостеновог поступка истичемо теорему на којој се то заснива.

Теорема 6. *Природан број n је сложен ако и само ако је дјељив простим бројем p за који важи $p \leq \sqrt{n}$.*



Слика 2.1: Уламова спирала која обухвата бројеве до 65,000.

Доказ.

Ако n има прост фактор $p \leq \sqrt{n}$, тада је n, очигледно, сложен број. Обратно, ако је p најмањи прост фактор сложеног броја n, тада је

$$n = p \cdot m,$$

за неки цио број m и при томе је $m \geq p$. Слиједи да је $p \leq \sqrt{n}$. □

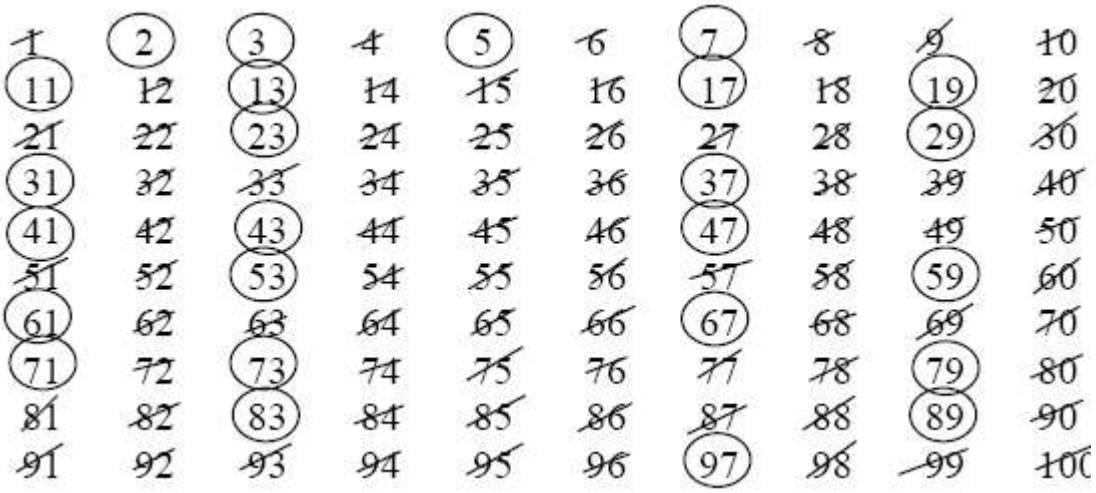
На овом критеријуму се и заснива алгоритам, познат под називом Ерастотеново сито, примјењен у3. вијеку пре нове ере. Ерастотенов алгоритам састоји се од следећих корака:

1. Исписати у низ све природне бројеве од 2 до n.

2. Уочити у низу први број који није ни подвучен ни прецртан и подвући га, а затим прецртати све његове садржиоце у низу.

3. Ако су сви бројеви у низу означени (подвучени или прецртани) поступак је завршен; у противном, примјенити корак 2.

По завршетку поступка добијамо све просте бројеве не веће од n. То су, на наредној слици, заокружени бројеви:



Попут Ерастотеновог алгоритма, генерације математичара су покушавале да дођу до јендноставног поступка селекције простих бројева у скупу природних. Пар тих покушаја је предтсављен и у наредном поглављу.

Глава 3

Фермаови и Мерсенови бројеви

Велики математичари Пјер де Ферма и Мерсен бавили су се дуго питањем постојања неке једноставне формуле којом се генеришу прости бројеви. Иако нису успјели, из тих покушаја су рођене двије класе бројева које су назване по њиховим ауторима.

3.1 Фермаови бројеви

Као што смо рекли, француски математичар Пјер де Ферма је, као и многи, тражио "свети грал" за генерисање простих бројева. Наиме, он је претпоставио да су сви бројеви облика

$$F_n = 2^{2^n} + 1$$

прости. Дуго нисмо имали дефинитиван одговор да ли је тачна Фермаова хипотеза, све док је Ојлер доказао да за Фермаов број F_5 ово тврђење не важи. Неки од њих јесу прости:

$$F_0 = 3$$

$$F_1 = 5$$

$$F_2 = 17$$

$$F_3 = 257$$

$$F_4 = 65537$$

До данас није пронађен ни један Фермаов прости број за $n > 4$ прост број. Па су следећи проблеми још увијек отворени :

1. Је ли F_n сложен за све $n > 4$?

2. Постоји ли бесконачно много Фермаових простих бројева?

3. Постоји ли бесконачно много сложених Фермаових бројева?

До 2010. познато је да је F_n сложен за $5 \leq n \leq 32$, али до 2012. само су бројеви од F_0 и до F_{11} и у потпуности факторизовани, а бројеви од F_{20} и до F_{24} и немају познатих фактора. Највећи Фермаов број за који се зна да је сложен је $F_{2543548}$ и , а његов прости фактор откривен је помоћу Prime Greed Proth Prime-ове потраге 2011-те године.

Кад је ријеч о Фермаовом научном доприносу, не можемо да не наведемо једну од најважнијих теорема за Теорију бројева коју је овај великан поставио и доказао.

Теорема 7. ***(Мала Фермаова теорема)*** *Нека је a природан, а p прост број. Тада a^p даје исти остатак као a при дијељењу са p. Пишемо:*

$$a^p = a \quad (mod p)$$

Доказ.

Нека p представља дужину неког низа који се добије користећи (понављање је допуштено) a различитих знакова. На примјер нека је $p = 5$ и $a = 2$, значи да можемо користити 2 знака (нека то буду слова A и B) и укупан број низова које можемо направити дужине 5 је $2^5 = 32$. То су следећи низови:

AAAAA, AAAAB, AAABA, AAABB, AABAA, AABAB, AABBA, AABBB,
ABAAA, ABAAB, ABABA, ABABB, ABBAA, ABBAB, ABBBA, ABBBB,
BAAAA, BAAAB, BAABA, BAABB, BABAA, BABAB, BABBA, BABBB,
BBAAA, BBAAB, BBABA, BBABB, BBBAA, BBBAB, BBBBA, BBBBB.

Посматраћемо случај када уклонимо низове који се састоји од само једног симбола и показати да преосталих $a^p - a$ низова могу бити сложени у групе од којих свака има тачно p низова. Из чега слиједи да је $a^p - a$ дјељиво са p . Наведено ћемо доказати корстећи следећи примјер.

Примјер Фермаове теореме: Огрлице и пријатељи:

Нека сваки низ представља огрлицу када му се крај споји с почетком : Ова огрлица представља 7 различитих низова:

(ABCBAAC

BCBAACA

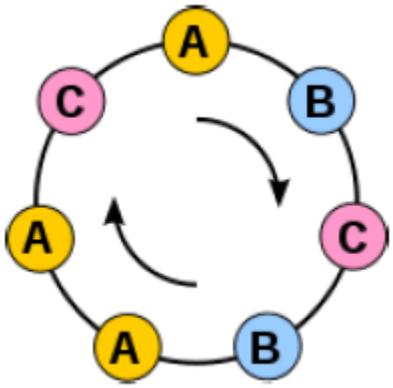
CBAACAB

BAACABC

AACABCB

ACABCBA

CABCBAA) зависно од тога што сматрамо почетком односно крајем.Ако можемо добити 2 низа користећи исту огрлицу назваћемо такве низове пријатељима.



На примјер у нашем случају пријатељи су : AAAAB, AAABA, AABAA, ABAAA, BAAAA. Овдје сваки ред представља једну огрлицу за наш примјер:

AAABB, AABBA, ABBAA, BBAAA, BAAAB,

AABAB, ABABA, BABAA, ABAAB, BAABA,

AABBB, ABBBA, BBBAA, BBAAB, BAABB,

ABABB, BABBA, ABBAB, BBABA, BABAB,

ABBBB, BBBBA, BBBAB, BBABB, BABBB,

AAAAA,

BBBBB.

Неке огрлице горе се састоје од $p = 5$ низова, а двије ($a = 2$) од једног. Лако се види да је 32 - 2 дјељиво са 5.

Колико огрлица може имати пријатеља?

Докле год се огрлица не може раставити на мање дијелове који се понављају ротацијом огрлице се неће добити исти низ. На примјер низ ABBABBABBABB се састоји од узастопних ABB низова те се зато ротацијом почетка огрлице за 3 мјеста опет добија исти низ. Ако се не може разбити огрлица на мање понављајуће

дијелове колико онда има пријатеља? Има их тачно p јер се сваким помјерањем почетка у огрлици добија нови низ. Како је дужина нашег низа прост број он се сигурно не може разбити на дијелове који се понављају. Зато можемо све од ap низова подијелити у 2 скупа :

1.Они низови који се састоји од само једног симбола, њих има колико и различитих слова, а то је a.

2. Остали низови које све можемо преставити са n огрлица од којих свака представља p пријатеља. Број таквих низова $a^p - a$ је дјељив са p јер смо их подијелили у групе од којих свака има p чланова. Одавде,

$$a^p - a = 0 \pmod{p} \quad a^p = a \pmod{p}$$

□

Занимљиво је да Фермаови бројеви задовољавају рекурзивне релације. Навешћемо неколико њих:

$$F_n = (F_{n-1} - 1)^2 + 1$$

$$F_n = F_{n-1} + 2^{2 \cdot n-1} \cdot F_0 \cdot F_1 \cdot .... \cdot F_{n-2}$$

$$F_n = {F_{n-1}}^2 - (F_{n-2} - 1)^2$$

$$F_n = F_0 \cdot F_1 \cdot .... \cdot F_{n-1} + 2$$

Теорема 8. *Свака два Фермаова броја су узајамно проста.*

Доказ.

Нека су F_n и F_{n+k}, $k > 0$ два различита Фермаова броја. Претпоставимо да је m цијели позитиван број, такав да је $m|F_n$ и $m|F_{n+k}$. Нека је $x = 2^{2^n}$, тада је:

$$x^{2^k} = (2^{2^n})^{2^k} = 2^{2^n \cdot 2^k} = 2^{2^{n+k}} = F_{n+k} - 1$$

Ако посматрамо количник:

$$\frac{F_{n+k} - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 1} + ... - 1$$

Видимо да F_n дијели $(F_{n+k} - 2)$. Одавде слиједи да $m|F_{n+k}$ и $m|2$. Како су сви Фермаови бројеви непарни , па је $m = 1$ и слиједи да је највећи заједнички дјелилац за F_{n+k} и F_k једнак 1, тј бројеви F_{n+k} и F_k су узајамно прости. □

3.2 Мерсенови бројеви

Слично као и Ферма, Мерсен је сматрао да се међу бројевима облика $M_n = 2^n - 1$, гдје је n ненегативан цијели број налази одређен број простих бројева. Наиме, тврђење је да када је год n прост број M_n је такође прост. Доказати можемо супротно. Ако је n сложен онда ће и M_n бити сложен. Рецимо да је $n = a \cdot b$.

$$(2^{a \cdot b} - 1) = (2^a - 1) \cdot (1 + \cdots + 2^{a \cdot (b-1)})$$

$$(2^{a \cdot b} - 1) = (2^b - 1) \cdot (1 + \cdots + 2^{b \cdot (a-1)})$$

Идентитет показује да ће M_p моћи бити прост само ако је и $n = p$ прост, што много олакшава потрагу за Мерсеновим простим бројевима. Обрнуто тврђење које је било наведено на почетку није тачно. M_p не мора бити прост ако је p прост. Најмањи контрапримјер је $2^{11} - 1 = 2047$, док је $2047 = 23 \cdot 89$, сложен број. Мерсенови бројеви повезани су са простим бројевима. Још увијек није доказана теорема да Мерсенових бројева који су прости има бесконачно много, а тренутно их је пронађено само 47. Највећи прости број је Мерсенов број

$$2^{43112609} - 1$$

, а да би га могли приказати требало би 3461 страница за приказ свих цифара у бази 10.

Глава 4

Густина простих бројева

Питање да ли је неки Фермаов број прост или сложен повезано је проблемом конструкције правилних многоуглова помоћу лењира и шестара. Одговор даје Гаусова теорема, чију формулацију наводимо.

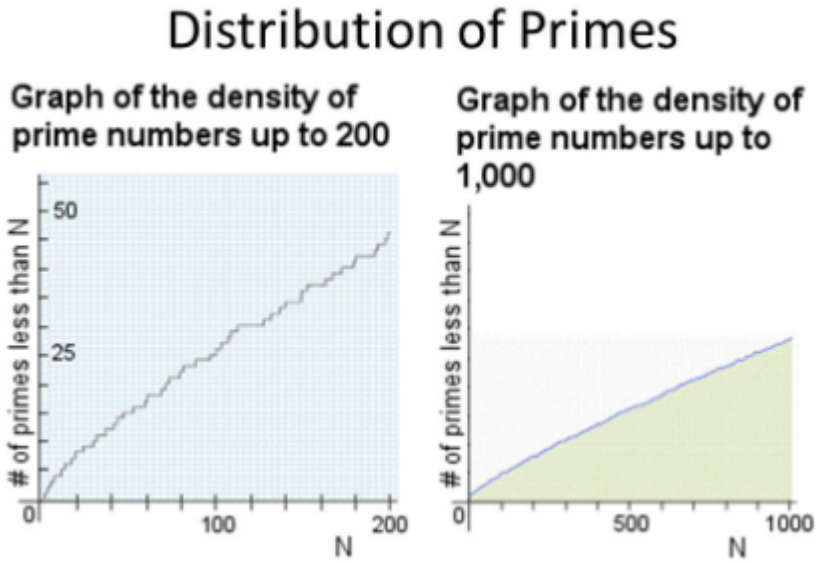
Теорема 9. ***(Гаус)*** *Правилан многоугао са n страница може се конструисати шестаром и лењиром ако и само ако је n природан број облика* $n = 2^s \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k$ *, где је s ненегативан цио број, а* $p_1, p_2, \ldots, p_k$ *различити Фермаови прости бројеви* $(k > 0)$ *или је* $n = 2^s$ *, где је s цио број већи од 1.*

Дефиниција 7. *Функција* $\pi(x)$ *представља броје простих бројева* $\leq x$*.*

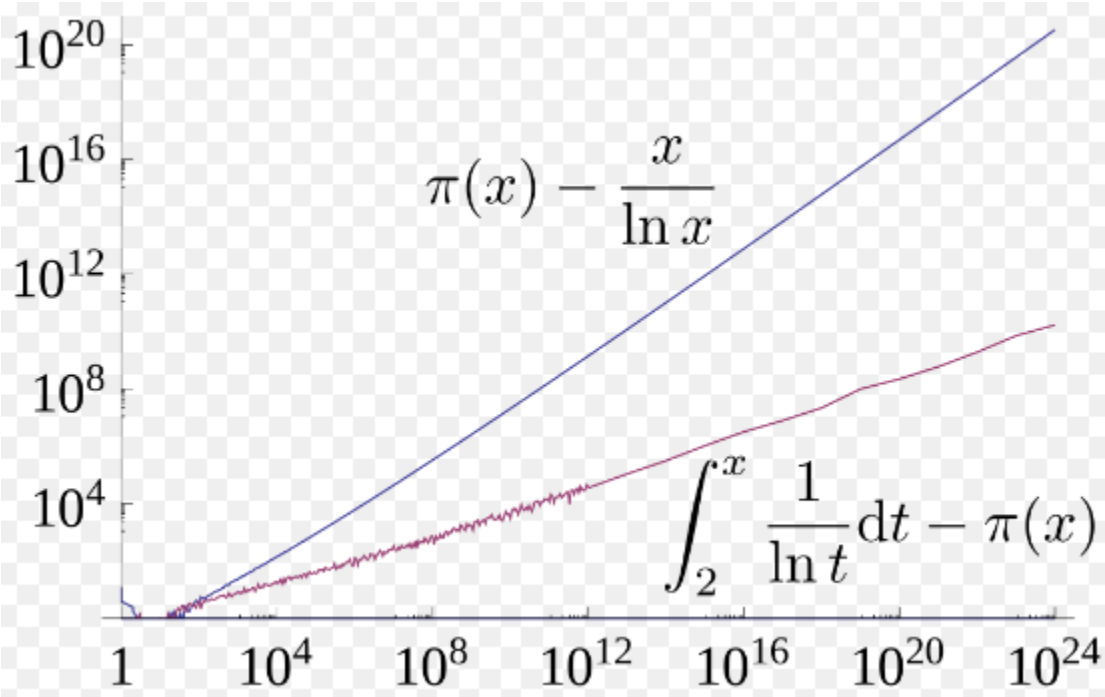
Гаус је у једном свом писму рекао како је он још као шеснаестогодишњак примјетио да густина простих бројева опада апроксимативно као $\frac{1}{ln(x)}$. Дошао је до претпоставке да би се функција $\pi(x)$ могла приказати помоћу логоритамског интеграла

$$\int_2^x \frac{dt}{\ln t}$$

.



1896. је доказана је независност горњег интеграла од густине простих бројева.



Теорема о простим бројевима даје одговоре. Она даје асимптотску расподјелу простих бројева међу природним бројевима, формализује интуитивну идеју брзине којом налазимо следећи прост број. Теорему су независно доказали Хадамард и Пуасон 1896. године користећи идеје које је увео Риман.

Теорема 10. *Нека је $\pi(x)$ број простих бројева мањих од x, $x \leq R$, R је велики реалан број, тада важи:*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$$

или $\pi(x) \sim x/ln(x)$.

Питање којим ћемо се даље бавити је растојање између простих бројева.

Prime number theorem
(illustrated by selected values n from 10^2 to 10^{14})

n	$\pi(n)$ = number of primes less than or equal to n	$\frac{\pi(n)}{n}$ = proportion of primes among the first n numbers	$\frac{1}{\log n}$ = predicted proportion of primes among the first n numbers
10^2	25	0.2500	0.2172
10^4	1,229	0.1229	0.1086
10^6	78,498	0.0785	0.0724
10^8	5,761,455	0.0570	0.0543
10^{10}	455,052,511	0.0455	0.0434
10^{12}	37,607,912,018	0.0377	0.0362
10^{14}	3,204,941,750,802	0.0320	0.0310

Дефиниција 8. *Прости бројеви се називају близанцима ако се разликују се за 2, док се називају рођацима, ако се разликују за 4. Неки примјери близанаца су:*

$(3,5),(5,7),$

$(11,13),(17,19),(29,31),(41,43),(59,61),(71,73),$

$(101,103),(107,109),(137,139),(149,151),(179,181),(191,193),(197,199)\ldots$

Највећи до сада откривени пар близанаца има 58,711 цифара. То су бројеви

$$2\,003\,663\,613 \cdot 2^{195,000} - 1 \text{ и } 2,003,663,613 \cdot 2^{195,000} + 1.$$

Дакле, најмања разлика између два сусједна проста броја је 2. Питање је да ли постоји максимална разлика између 2 сусједна проста броја? Овим изазовом, у 21. вијеку, баве се велики математичари данашњице - Грин и Тао.

Наводимо неке од најзначајнијих теорема њиховог рада, али без доказа, првенствено због изузетне комплексности.

Теорема 11. *Низ простих бројева садржи произвољно много аритметичких низова произвољне дужине.*

За било који низ простих бројева постоји много аритметичких низова $\{a_1,...,a_k\}$, гдје је k било који велики природан број.

Дефиниција 9. *За одређени низ различитих бројева $\{a_1,...,a_k\}$ за који $a_1 < a_2 < ... < a_k$, $0 < k < n+1$, кажемо да постоји прости број p који је опструкција ако p дијели најмање један од $\{n+a_1,...,n+a_k\}$, за сваки цијели број n, другим ријечима, p дијели $P(n) = (n+a_1)\cdot(n+a_2)...\cdot(n+a_k)$ за сваки цијели број n, под условом да низ $\{a_1,...,a_k\}$ укључује све остатке по* $(\mathrm{mod}\ p)$.

Дефиниција 10. *Ако не постоји таква опструкција, онда кажемо да је за природан број k, $0 < k < n+1$, за сваки цијели број n, $\{a_1,...,a_k\}$ $(\mathrm{mod}\ p)$ допустљив низ.*

Примјетимо да

$$a_1, ..., a_k \quad (mod p)$$

могу заузимати више од k остатака класе по $(mod p)$ и тако ако $p > k$, тада p не може бити опструкција. Дакле, провјерити је ли одређени скуп A од k цијелих бројева допустљив, потребно је пронаћи само једну класу остатака по $(mod p)$, за сваки прост број $p \leq k$ што не припада скупу A.

Грин и Тао су свој рад засновали на резултатима Јитланда Занга. Он је формулисао теорију као добар путоказ младим математичарима.

Теорема 12. ***(Занг)*** *Постоји природан број k, такав да* $\{x + a_1, ..., x + a_k\}$ *је допустљив скуп , онда је бесконачно много природних бројева n тако да у скупу* $\{n + a_1, ..., n + a_k\}$ *постоје најмање два броја проста, гдје је n природан број и замјена за x .*

Таова претпоставка је да постоји ограничење B такав да било који пар простих бројева p и q у Занговој к-торци и вриједи $p < q < p + B$. Проналажење овакве k-торке је изазовно питање. Теорема о простим бројевима заједно са овом конструкцијом имплицира да

$$B < k(\log k + C)$$

за неку константу C, али је интересантно да нађемо боље ограничење. За 50-орку ширина је 246:

0, 4, 6, 16, 30, 34, 36, 46, 48, 58, 60, 64, 70, 78, 84, 88, 90, 94, 100, 106, 108, 114, 118, 126, 130, 136, 144, 148, 150, 156, 160, 168, 174, 178, 184, 190, 196, 198, 204, 210, 214, 216, 220, 226, 228, 234, 238, 240, 244, 246

Циљ је да поставимо ограничење B тако да постоји бесконачно много парова узастопних простих бројева p_n, p_{n+1} чија разлика $p_{n+1} - p_n$ износи највише константу B, еквивалнтно са

$$p_{n+1} - p_n \leq B;$$

Питање је колико велико или мало може бити B?

На прво питање одговор даје теорема о близанцима: $p_{n+1} - p_n = 2$

Такође, поставља се питање како наћи ограничења за разлике

$$p_{n+2} - p_n, p_{n+3} - p_n, ...$$

Наравно, уколико дођемо до конктретног и непромјењивог резултата горње разлике, друга ограничења ћемо одатле израчунати.

4.1 Велике разлике између простих бројева:

Разлика између простих бројева може бити врло велика

Примјер 1.

Посматрајмо низ од $n-1$ *узастопних сложених цијелих бројева и мора припадати размаку између простих бројева дужине најмање* n.

$n! + 2, n! + 3, \ldots n! + n$.

Из тога слиједи да постоје празнине између простих бројева који су произвољно велики, односно, за било који цијели број n, постоји цио број m са $g_m \geq n$,

g_m је m -та разлика између простих бројева по реду. Можемо узети n велико.

Теорема простих бројева каже

$$\pi(x) = (1 + o(1)) \cdot \frac{x}{\log(x)},$$

o(1) је бесконачно мала функција. Ово повлачи:

$$p_{n+1} - p_n \leq (1 + o(1)) \cdot \frac{x}{\log(x)},$$

за било коју разлику простих бројева из $[x, 2x]$, x је велики цијели број, важи израз изнад. Поменути принцип се назива принципом голубова. Ова разлика може бити велика колико и $(1 - o(1)) \log(x)$. Не знамо колика је конкретна разлика, али знамо да је много мања ($<<$) од $p_n^{0.55}$.

$$p_{n+1} - p_n << p_n^{0.55}$$

Директна последица теореме о простим бројевима.

Ако користимо Риманову хипотезу (

$$\sum_{n=1}^{\infty} n^{-s}$$

s је комплексан број = Риманова зета функција, код које све комплексне нуле имају особину да им је реални дио 1/2):

$$p_{n+1} - p_n << p_n \cdot \log p_n$$

Ово је најбољи могући резултат добијен помоћу Риманове хипотезе.

Крамер је приказао просте бројеве као случајан низ иако у суштини није насумичан, него експонецијално насумичан, што значи да се елементи тог низа бирају случајно из експоненцијалне расподјеле . Рачунањем се поставља претпоставка да је разлика

$$p_{n+1} - p_n << c \cdot \log^2 \cdot p_n$$

ако узмемо $c > 0$ које је бесконачно често и мало. Док ако узмемо C велико коначно често разлика

$$p_{n+1} - p_n << C \cdot \log^2 p_n$$

Ово није близу рјешења и врло је тешко пронаћи овакве просте бројеве. Низ резултата у дали велики математичари. Хронолошки су добијени следећи резултати:

1.Њетинзис је дошао до резултата :

$$p_{n+1} - p_n >> \frac{\log(p_n) \cdot (\log(\log(\log p_n)))}{(\log(\log(\log(\log(p_n)))))}$$

2.Ердос 1935. :

$$p_{n+1} - p_n >> \frac{\log(p_n) \cdot (\log(\log(p_n))}{(\log(\log(\log(p_n)))))}$$

3.Ранхин 1938. :

$$p_{n+1} - p_n >> \frac{c \cdot \log(p_n) \cdot (\log(\log(p_n))) \cdot (\log(\log(\log(\log(p_n))))))}{\log(\log(\log(p_n)^2)))}$$

Израчутно је касније да је $c = 1/3$.

Најбољи резултат данашњице је :

$$p_{n+1} - p_n >> \frac{\log(p_n) \cdot (\log(\log(p_n \cdot (\log(\log(\log(\log(p_n))))))))}{\log(\log(\log(p_n)))}$$

4.2 Мале разлике између простих бројева

Нека је интервал $[x, 2x]$, гдје је x довољно велики број, интервал на ком посматрамо просте бројеве. Циљ је да ограничимо разлику између узастопних бројева на овом интервалу. Тао тврди да је на $[x, 2x]$ постоје p_{n+1} и p_n тако да важи:

$$p_{n+1} - p_n << \log(x)$$

Покушавајући да на било ком интервалу са горње стране ограниче разлику константом B:

$$\liminf_{n\to\infty}(p_{n+1} - p_n) < B$$

Савремени математичари су различитим методама дошли до следећих резултата:

Јитланд Занг је користећи методе математичке анализе одредио да тражено горње ограничење разлике два узастопна проста броја на интевалу је $A = 70000000$.

Даљим истраживањем поменуте горње границе бавили су се велики математичари који су радили на Полимат пројекту, спустили границу на $A = 4,680$.

Мајнард је пронашао у новембру 2013. да је ту разлику могуће смањити на $A = 600$.

Док је Полимат пројекат је у априлу 2014. године смањио на $A = 246$ уз помоћ

рачунара.

Говорећи о великим разликама између узастопних простих бројева, конструишемо низ $n! + 2, ..., n! + n$ добијамо велику раздаљину:

$$p_{n+1} - p_n >> \frac{\log(p_n)}{\log(\log p_n)}$$

што нам не одговара, па посматрамо $n\#$ (n прајморијал), он представља производ само простих бројева мањих или једнаких од n. Наново конструишемо низ $n\# + 1, ..., n\# + n(*)$. Ако користимо овакву конструкцију посматрамо скуп бројева 2,...,n и радимо $n\#$ мод сваки од ових бројева. Битна чињеница је да та да ми овим покривамо цијели интервал, тј (*) је дјељива са свим бројевима до n. Можемо посматрати и веће интервале. Сад се поставља питање са почетка како покрити цијели интервал простих бројева? У комбинаторној литератури ефикасан алгоритам покривања су развили Пипингер и Спенсер 1989, користећи метод познат као полу-случајни метод или Родл нибл. За све $p < n$ посматрамо скуп

$$1, ..., \frac{\log\log\log(n) \cdot n}{log(n)}.$$

Овај интервал требамо бројевима до n. Оваквим поступком покрићемо све просте бројеве до $n/2$, а преживјеће прости бројеви од $n/2$ до поседњег броја у посматраном скупу. Груба идеја је одабрати мали број остатака класе $C_p \pmod{p}$ случајно. За сваки прост број из интервала формирамо класу C_p. Формирамо низ:

$$C_p, C_p + p, C_p + 2 \cdot p, C_p + 3 \cdot p...$$

Треба уклонити из разматрања све додатне класе остатака које пресијецају класе остатака које су изабране. Затим узмимо још неколико класа остатака насумично у преосталом базену расположивих класа. Узастопним понављањем овог процеса елиминишемо готово све губитке који долазе од преклапања класе остатака. Суштина цијеле приче је да овим поступком ми покривамо много простих бројева, али не све.

Глава 5

Закључак:

Осврнимо се још једном на већ речено. На самом почетку дефиницијама и уводним теоремама описали смо просте бројеве, а затим дошли смо лаганим корацима до највећих проблема у математици данас. Највећи познати прост број, који се састоји од више од 17 милиона цифара, открили су амерички научници. Број, који се изражава са

$$2^{57885161} - 1$$

, може да се дијели једино сам са собом и са 1, што га чини највећим основним бројем икад идентификованим.

Наћи следећи прост број је тежак задатак, док наћи образац за њихово тражење је веома дуг и исцрпан пут којим ћемо корачати и даље, и наравно никад нећемо престати да тражимо боље и више. Али, још увијек прости бројеви су неоткривена тајна једне краљице. Познато је да је математика краљица међу наукама, а нама математичарима да је Теорија бројева њена краљица. Настављамо ово истраживање на још већем нивоу али наравно темељено на досадашњим чињеницама.

Библиографија

[1] David Burton Eelementary number theory

[2] Edwin Clark Elementary Number Theory

[3] Bounded gaps between primes

[4] Small and large gaps in the primes