Математичка гимназија

Матурски рад
из математике

О бесконачности простих бројева

Ученик
Никола Лазић, IVд

Ментор
др Соња Чукић

Београд, 25. мај 2023.

Садржај

1

Предговор

Теорија бројева ми је увек била једна од омиљених области математике, а у њеном средишту су се одувек налазили управо прости бројеви. Зато сам њима и хтео да посветим свој матурски рад. Желео сам и да тема коју одаберем обухвати што више грана математике, а када сам чуо да се постојање бесконачно много простих бројева може показати не само преко теорије бројева, већ и преко теорије група, редова, комбинаторике или чак топологије, избор је био очигледан. Током писања овог рада научио сам много о областима које су ми биле познате, упознао се са некима које нису (топологија) и сазнао безброј занимљивости од којих неке нису чак ни директно повезане са радом (да ли сте знали да се оптималном игром Ханојска кула са n дискова може решити у $2^n - 1$ потеза?), а између осталог сам научио и да користим LaTeX.

Намера ми је била да рад буде лак за читање и приступачан и оним људима којима су коришћене области мање познате. Из тог разлога сам, у уводима у поглавља, наводио основне дефиниције и теореме које су потребне за саме доказе.

За крај, желим да се захвалим свом ментору на стрпљењу и помоћи и надам се да ће у овом раду уживати ко год га буде читао.

2

Увод

Чињеница да простих бројева има бесконачно много позната је математичарима преко 2300 година. Упркос томе, како су се развијале нове гране математике, тако су настајали нови докази овог тврђења. У овом раду ће бити приказани неки од њих, али имајте на уму да их има много више.

Налажење нових простих бројева је увек била занимација математичара. Када је ручно проверавање дељењем постало превише временски захтевно, тражени су ефикаснији алгоритми, од којих већина проистиче директно из различитих доказа ове чињенице. Дуго није постојао практичан разлог да се налазе нови прости бројеви, али је 1970-их пронађена примена у криптографији.

Управо чињеница да простих бројева има бесконачно много отвара многа питања, а на велик део њих нисмо нашли одговор. Најпознатија међу њима су Голдбахова хипотеза, која претпоставља да се сваки паран природан број већи од 2 може представити као збир два проста броја (проверено важи до $4 \cdot 10^{18}$) и хипотеза о простим близанцима, која тврди да постоји бесконачно много простих бројева p за које је $p + 2$ такође прост број (највећи пронађен је $2996863034895 \cdot 2^{1290000} - 1$). Трагање за доказима ових хипотеза је довело до многих открића у различитим гранама теорије бројева.

Дефиниција 2.1. Функција пребројавања простих бројева[1] је функција која реалан број x слика у број простих бројева p за које $p \leqslant x$, а означава се са $\pi(x)$.

Дуго се није много знало о понашању ове функције, али је крајем 19. века доказана следећа теорема.

[1] *Prime counting function* на енглеском језику, у српској литератури нема опште прихваћено име.

Теорема 2.1. (*Теорема о простим бројевима*)

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

Теорема о простим бројевима нам заправо говори да је функција $f(x) = \frac{x}{\ln(x)}$ добра апроксимација функције бројања простих бројева за велике вредности x. Доказ ове теореме је врло сложен и нећемо се њиме бавити, али сам је навео да бих дао уопштену слику о понашању броја простих бројева у бесконачности. За крај, доказаћемо једну очигледну тврдњу која ће нам бити од користи за велик број доказа у овом раду.

Лема 2.1. Сваки природан број већи од 1 има простог делиоца.

Доказ. Ову тврдњу ћемо доказати преко јаке индукције.
База. $n = 2$ има простог делиоца, број 2.
Индуктивни корак. Ако сви бројеви мањи од n имају простог делиоца, онда и n има простог делиоца.

1° Ако је n прост број, тада $n \mid n$ па n има простог делиоца.

2° Ако је n сложен број, тада се n може раставити као $n = ab$, где $1 < a, b < n,\ a, b \in \mathbb{N}$. На основу индуктивне хипотезе, знамо да a има неког простог делиоца, на пример p, па онда важи $p \mid n$. Дакле, број n има простог делиоца.

□

Напомена. Скуп простих бројева ће даље у раду бити обележаван са $\mathbb{P}$.

3

Докази преко теорије бројева

Сваки доказ који је изнет у овом раду користи теорију бројева, али ће касније докази залазити и у друге области математике. За разлику од њих, прва два доказа ће се ослањати само на теорију бројева.

3.1 Еуклидов доказ

Теорема 3.1. Постоји бесконачно много простих бројева.

Доказ. Претпоставимо да скуп простих бројева $\mathbb{P}$ има коначно много елемената, $\mathbb{P} = \{p_1, p_2, ..., p_n\}$. Показаћемо да постоји прост број који не припада овом скупу. Посматрајмо број

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

Због леме 2.1, број X мора имати прост делилац p. Међутим, број X даје остатак један при дељењу са сваким елементом скупа $\mathbb{P}$. Дакле, p је прост број који не припада скупу $\mathbb{P}$, па смо дошли до контрадикције са почетном претпоставком. Према томе, скуп простих бројева не може бити коначан. □

Еуклид[1] је у деветој књизи *Елемената*[2] изнео овај доказ, што га чини најстаријим записаним доказом ове чињенице. На основу овог доказа, Алберт

[1]Еуклид је био старогрчки математичар који је живео око 300. године п. н. е. Највише се бавио геометријом и логиком, али је допринео и многим другим гранама математике попут теорије бројева. Сматра се оцем геометрије.

[2]Елементи су Еуклидов најпознатији математички рад. Састоје се од 13 књига. У њима се налазе постулати Еуклидове геометрије, а уз њих се помиње још и елементарна теорија бројева и ирационални бројеви.

Мулин[3] је конструисао алгоритам за налажење простих бројева. Кренувши од скупа $S = \{2\}$, следећи број који је додавао је био најмањи прост делилац броја

$$X = 1 + \prod_{p \in S} p.$$

Као и у претходном доказу, знамо да овај број неће бити члан скупа S. Након додавања броја у скуп настављамо процес. Првих пет корака изгледа овако:

(1) $S = \{2\},\ 2 + 1 = 3$, 3 је прост, додајемо 3.

(2) $S = \{2, 3\},\ 2 \cdot 3 + 1 = 7$, 7 је прост, додајемо 7.

(3) $S = \{2, 3, 7\},\ 2 \cdot 3 \cdot 7 + 1 = 43$, 43 је прост, додајемо 43.

(4) $S = \{2, 3, 7, 43\},\ 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \cdot 139$, додајемо 13.

(5) $S = \{2, 3, 7, 43, 13\}, 2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 + 1 = 23479 = 53 \cdot 443$, додајемо 53.

Низ елемената које добијамо овим алгоритмом (тим редом) се зове **Еуклид-Мулин секвенца**. Мулин се питао да ли ће се сваки прост број појавити у овом низу, али овај проблем још није решен. Првих 10 чланова низа су: 2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139.

Последица. За $x \geqslant 2, \pi(x) > \log_2(\log_2(x))$.

Доказ. Нека су $p_1, p_2, \ldots, p_n$ првих n простих бројева, а X_n њихов производ. На основу Еуклидовог доказа знамо да постоји прост број p који није међу првих n простих бројева, а јесте фактор броја X_n. Одавде следи да је $p_{n+1} \leqslant X_n$. Користећи ову неједнакост и јаку индукцију, показаћемо да важи $p_n \leqslant 2^{2^{n-1}}$ за свако $n \geqslant 1$.
База. $n = 1,\ p_1 = 2 \leqslant 2 = 2^{2^{1-1}}$.
Индуктивни корак. Ако за свако k мање од n важи $p_k \leqslant 2^{2^{k-1}}$, онда важи и $p_n \leqslant 2^{2^{n-1}}$. Наиме,

$$\begin{aligned} p_n \leqslant X_{n-1} &= p_1 p_2 \cdots p_{n-1} + 1 \leqslant 2 \cdot 2^2 \cdots 2^{2^{n-2}} + 1 \\ &= 2^{1+2+\ldots+2^{n-2}} + 1 = 2^{2^{n-1}-1} + 1 \leqslant 2^{2^{n-1}}. \end{aligned}$$

Сада, пошто знамо да важи $p_n \leqslant 2^{2^{n-1}}$, знамо и да до $2^{2^{n-1}}$ има барем n простих бројева, односно да је $\pi(2^{2^{n-1}}) \geqslant n$ за свако $n \geqslant 1$. За произвољно $x \geqslant 2$, можемо одабрати неки природан број n тако да $2^{n-1} \leqslant \log_2(x) < 2^n$. За овакво n је $x \geqslant 2^{2^{n-1}}$, па онда важи $\pi(x) \geqslant \pi(2^{2^{n-1}}) \geqslant n > \log_2(\log_2(x))$ (прва неједнакост важи јер је $\pi(x)$ очигледно неопадајућа функција). □

[3] *Albert Mullin* (25. август 1933 – 16. мај 2017) је био амерички математичар и инжењер.

3.2 Голдбахов доказ

Дефиниција 3.1. Бројеви облика $2^{2^n}+1$ се зову **Фермаови**[4] **бројеви** и обележавају се са F_n.

Лема 3.1. За Фермаове бројеве важи релација $\prod_{k=0}^{n-1} F_k = F_n - 2$.

Доказ. Ову тврдњу ћемо доказати преко индукције.
База. $F_0 = 3,\ F_1 = 5,\ F_1 = F_0 + 2$.
Индуктивни корак. Ако важи релација $\prod_{k=0}^{n-1} F_k = F_n - 2$, онда важи и $\prod_{k=0}^{n} F_k = F_{n+1} - 2$.

$$\prod_{k=0}^{n} F_k = F_n \cdot \prod_{k=0}^{n-1} F_k = F_n \cdot (F_n - 2) = F_n^2 - 2F_n + 1 - 1$$
$$= (F_n - 1)^2 - 1 = (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1 = F_{n+1} - 2. \qquad \square$$

Теорема 3.2. (*Голдбахова*[5] *теорема*) Свака два Фермаова броја су узајамно проста.

Доказ. Претпоставимо да неки број m дели нека два Фермаова броја F_i и F_j $(0 \leqslant i < j)$. На основу леме 3.1, знамо да је $\prod_{k=0}^{j-1} F_k + 2 = F_j$. Пошто m дели F_j, а и производ са леве стране (јер је F_i један од његових чинилаца), m мора делити и њихову разлику, односно $m \mid 2$. На основу овога закључујемо да је $m = 1$ или $m = 2$, али, пошто су сви Фермаови бројеви непарни, мора бити $m = 1$. $\square$

До следећег доказа дошао је Голдбах 1930. године.

Теорема 3.3. Постоји бесконачно много простих бројева.

Доказ. На основу Голдбахове теореме знамо да су свака два Фермаова броја узајамно проста. Фермаових бројева има бесконачно много, а на основу леме 2.1 сваки од њих има бар једног простог делиоца. Пошто су узајамно прости, ниједна два Фермаова броја немају истог делиоца, па простих бројева мора бити бесконачно много. $\square$

[4] *Pierre de Fermat* (1607 - 12. јануар 1665) је био француски математичар. Најпознатији је по својим доприносима гранама математике попут диференцијалног рачуна, инфинитезималног рачуна и теорије бројева, али се бавио још и аналитичком геометријом, вероватноћом и оптиком.

[5] *Christian Goldbach* (18. март 1690 - 20. новембар 1764) је био пруски математичар који се пре свега бавио теоријом бројева.

Ферма је сматрао да су сви Фермаови бројеви прости. Заиста, тако делује за првих пет Фермаових бројева (3, 5, 17, 257, 65537), међутим F_5 није прост, већ се може записати као $641 \cdot 6700417$. Ово је показао Ојлер 1732. године и тиме је оборио Фермаову претпоставку. Упркос напретку компјутера, постоје бројна отворена питања о већим Фермаовим бројевима. Нека од њих су:

(1) Постоји ли прост Фермаов број за $n > 4$? Ако да, постоји ли их бесконачно много? (За $4 < n < 33$ сви су сложени.)

(2) Постоји ли бесконачно много сложених Фермаових бројева?

(3) Постоји ли Фермаов број дељив квадратом природног броја већег од 1?

4

Доказ преко теорије група

За следећи доказ ћемо користити теорију група, па ћемо се прво подсетити основних дефиниција и теорема које ће нам бити потребне.

4.1 Основе теорије група

Подсетник. Бинарна операција на скупу G је пресликавање $G \times G \to G$.

Дефиниција 4.1. Нека је G скуп и $*$ бинарна операција на том скупу.

(1) Ако $(\forall x, y, z \in G)((x * y) * z = x * (y * z))$, операција $*$ је **асоцијативна** на скупу G.

(2) Ако $(\exists e \in G)(\forall x \in G)(x * e = e * x = x)$, операција $*$ има **неутрал** у скупу G.

(3) Ако $(\forall x \in G)(\exists x^{-1} \in G)(x * x^{-1} = x^{-1} * x = e)$, где је e неутрал, сваки елемент скупа G има **инверз** за операцију $*$.

(4) Ако $(\forall x, y \in G)(x * y = y * x)$, операција $*$ је **комутативна** на скупу G.

Дефиниција 4.2. Нека је G скуп и $*$ бинарна операција на G која је асоцијативна, има неутрал у скупу G и нека сваки елемент скупа G има инверз за опрацију $*$. Структура $(G, *)$ се зове **група**.

Дефиниција 4.3. Абелова група је група у којој важи и комутативност.

Теорема 4.1. Неутрал је јединствен у свакој групи.

Теорема 4.2. Сваки елемент групе има тачно један инверз.

Теорема 4.3. Ако су a и b елементи групе, тада је $(ab)^{-1} = b^{-1}a^{-1}$.

Дефиниција 4.4. Број елемената коначне групе, у ознаци $|G|$, зове се **ред групе** G.

Дефиниција 4.5. Најмањи природан број k уколико такав постоји, за који важи $x^k = e$, где је x елемент групе G, а e неутрал те групе, зове се **ред елемента** x у групи G и означава се са $\mathrm{ord}(x)$.
Napomena. Svaki element u konačnoj grupi ima red.

Теорема 4.4. Нека је k природан број за који важи $x^k = e$, где је x елемент групе G, а e неутрал те групе, а r ред елемента x у групи G. Тада је број k дељив бројем r.

Доказ. Ако је x неутрал, његов ред је 1 па тврђење теореме очигледно важи. Ако није, претпоставимо да k није дељиво са r. Онда k можемо записати као $k = ar + t, 0 < t < r$ (због $x \neq e$ имамо $r > 1$). Имамо да је $e = x^k = x^{ar+t} = (x^r)^a x^t = e^a x^t = x^t$. Међутим, ово је у контрадикцији са претпоставком да је r ред елемента x, па r мора делити k. □

Последица. Ако је k прост број, а x није неутрал, онда важи $\mathrm{ord}(x) = k$.

Дефиниција 4.6. Нека је $(G, *)$ група и $H \subset G$. Ако је $(H, *)$ такође група, онда се ова структура назива **подгрупом** групе $(G, *)$.

Теорема 4.5. Свака подгрупа мора да садржи неутрал групе.

Теорема 4.6. Нека је a елемент групе G и $\mathrm{ord}(a) = n$. Tada je $\{1, a, a^2, \ldots, a^{n-1}\}$ podrgrupa grupe G. Inače, grupe ovog oblika se zovu **ciklične grupe**.

Дефиниција 4.7. Десни косет групе G је $Ga = \{xa | x \in G\}$. **Леви косет** се дефинише аналогно.

Теорема 4.7. Ред косета групе је једнак реду групе.

Дефиниција 4.8. Нека је $\sim$ релација еквиваленције. Сви елементи скупа који су по њој међусобно еквивалентни чине једну **класу еквиваленције**.
Коментар: Сваки елемент групе припада тачно једној класи еквиваленције јер, ако би био еквивалентан свим елементиме две различите класе, тада би, због симетричности и транзитивности, сви елементи једне групе били еквивалентни свим елементима друге, па би ове две групе морале бити део исте класе.

Теорема 4.8. (*Лагранжова теорема*) Ако је G коначна група, а H њена подгрупа, тада $|H|$ дели $|G|$.

Доказ. Нека је $\sim$ бинарна релација дефинисана као $a \sim b \iff ba^{-1} \in H$. Покажимо прво да је $\sim$ релација еквиваленције.

(1) (*Рефлексивност*) $a \sim a \iff aa^{-1} \in H \iff e \in H \iff \top$

(2) (*Симетричност*) $a \sim b \iff ba^{-1} \in H \iff (ba^{-1})^{-1} \in H$
$\iff ab^{-1} \in H \iff b \sim a.$

(3) (*Транзитивност*) $a \sim b \iff ba^{-1} \in H$; $b \sim c \iff cb^{-1} \in H$;
$(cb^{-1})(ba^{-1}) \in H \iff ca^{-1} \in H \iff a \sim c.$

Дакле, пошто је $\sim$ релација еквиваленције, можемо посматрати класе еквиваленције. Класа еквиваленције која садржи елемент a је управо косет Сада, пошто се група G може разбити у неки број класа еквиваленције са по $|H|$ елемената, а између њих нема пресека, јасно је да $|H|$ мора да дели $|G|$. □

Последица. На основу сваког елемента групе можемо формирати цикличну подргрупу, па самим тим ред сваког елемента мора делити ред групе.

Пример. Посматрајмо скуп $S = \{1, 2, \ldots, p-1\}$, где је p прост број и операцију множења по модулу p. Покажимо да је $(S, \cdot_p)$ група.

(1) (*Затвореност*) У скупу S имамо све могуће остатке по модулу p осим 0, а пошто множењем два броја која нису дељива са p не можемо добити број дељив са p (због тога што је p прост), затвореност важи.

(2) (*Асоцијативност*) Очигледно важи због особина множења по модулу.

(3) (*Неутрал*) Неутрал за множење по модулу је број 1, а он се налази у скупу S.

(4) (*Инверзи*) Последица **Еуклидовог алгоритма** нам говори да једначина $ax + by = 1$ у природним бројевима има решења ако и само ако је $(a, b) = 1$. Једначину можемо записати у другачијем облику као $ax \equiv_b 1$. Ако узмемо $a \in S$ и $b = p$, $(a, b) = 1$ ће заиста важити. Сада знамо да постоји x за које је $ax \equiv_p 1$, а пошто одавде $p \nmid x$, постоји елемент скупа који је конгруентан x по модулу p и управо он ће бити инверз за a.

4.2 Доказ преко Мерсеновог броја

Дефиниција 4.9. Бројеви облика $2^n - 1$ се зову **Мерсенови**[1] **бројеви** и обележавају се са M_n.

За разлику од претходних доказа, није познато ко је први дошао до овог.

Теорема 4.9. Постоји бесконачно много простих бројева.

[1] *Marin Mersenne* (8. септембар 1588 - 1. септембар 1648) је био Француз који се бавио бројним наукама, укључујући математику, физику и филозофију. У математици је био најпознатији по Мерсеновим бројевима.

Доказ. Претпоставимо да је скуп $\mathbb{P}$ коначан и да је највећи прост број p. Посматраћемо Мерсенов број M_p и показати да је сваки његов прост фактор већи од p. Знамо да M_p има неки прости фактор q по леми 2.1. За q онда важи $2^p \equiv_q 1$. Пошто је p прост број, на основу последице теореме 4.4 знамо да је ред елемента 2 у групи $(\{1, 2, \ldots, q-1\}, \cdot_q)$ управо p. Ова група има $q-1$ елемената. Сада, по последици Лагранжове теореме, знамо да $p \mid q-1$, па је самим тим $p < q$. Добили смо контрадикцију са почетном претпоставком, па простих бројева мора бити бесконачно много. □

Мерсен се највише бавио простим Мерсеновим бројевима. Они су значајни из више разлога. За почетак, корисни су за проналажење нових простих бројева. Јасно се види да је индекс сваког Мерсеновог простог броја прост. У супротном, ако би индекс био облика ab, где су a и b већи од 1, могли бисмо раставити Мерсенов број као $M_{ab} = 2^{ab} - 1 = (2^a - 1)(1 + 2^a + \ldots + 2^{(b-1)a})$. Дуго није постојао добар алгоритам за проверавање сложености Мерсенових бројева, а они расту јако брзо, па су стандардне методе биле врло споре. Тест сложености за Мерсенове бројеве је развијен 1876. од стране Едуарда Лукаса[2] а касније (1930-те) дорађен од стране Дерика Хенрија Лемера[3]. Доказ тачности овог алгоритма је сложен и нећемо се њиме бавити, али је сам алгоритам једноставан. Писан у *C#*, он изгледа овако, са условом да је p непаран прост број:

```
bool prime(int p)
{
    long s = 4;
    long M = (long)Math.Pow(2, p)-1;
    for (int i = 0; i < p - 2; i++)
    {
        s = ((s * s) - 2) % M;
        Console.WriteLine(s);
    }
    if (s == 0) return true;
    return false;
}
```

Највећи пронађен прост број је нађен управо коришћењем овог алгоритма. У питању је $M_{82,589,933}$. Још једна занимљивост у вези Мерсенових простих бројева је њихова повезаност са Еуклидовим савршеним бројевима (бројевима који су једнаки суми својих делилаца, не рачунајући самог себе). У четвртом

[2] *François Édouard Anatole Lucas* (4. април 1842 – 3. октобар 1891) је био француски математичар. Највише се бавио Фибоначијевим бројевима.

[3] *Derrick Henry Lehmer* (23. фебруар 1905 – 22. мај 1991) је био амерички математичар најпознатији по свом доприносу рачунарској теорији бројева.

веку пре нове ере, Еуклид је показао да је број $2^{p-1}(2^p - 1)$ савршен ако је M_p прост број, а касније је утврђено да сви парни савршени бројеви морају бити овог облика. Није познат ниједан непаран савршен број.

Као и за Фермаове бројеве, није познато да ли постоји бесконачно много сложених Мерсенових бројева, нити да ли постоји бесконачно много простих. Индекси првих 11 простих Мерсенових бројева су 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.

5

Доказ преко редова

За овај доказ, који је први изнео Ојлер[1] 1737. године, биће нам потребне основне особине неких редова, конкретно геометријског и хармонијског.

Дефиниција 5.1. $\sum_{k=0}^{\infty} a \cdot r^k,\ ar \neq 0$ зове се **геометријски** ред са почетним чланом a и количником r.

Теорема 5.1. Геометријски ред конвергира ако и само ако је апсолутна вредност количника мања од 1.

Доказ. Дефинишимо S_n као суму првих n чланова реда. За $|r| \neq 1$,

$$S_n = a + ar + \ldots + ar^{n-1} = a \cdot \frac{1 - r^n}{1 - r} \tag{5.1}$$

Ако постоји лимес S_n када n тежи бесконачно, тада ред конвергира. За $|r| < 1$,

$$\lim_{n\to\infty} S_n = \lim_{n\to\infty} a \cdot \frac{1 - r^n}{1 - r} = \frac{a}{1 - r}. \tag{5.2}$$

(1) За $r = 1$, не можемо сумирати S_n као у једначини (5.1), већ је $S_n = na$, што очигледно дивергира.

(2) За $r = -1$, $S_{2k} = 0$, а $S_{2k+1} = a$, па ред не конвергира.

(3) За $|r| > 1$, не постоји лимес у једначини (5.2) због тога што $|r^n| \to \infty$ када $n \to \infty$.

□

[1] *Leonhard Euler* (15. април 1707 – 18. септембар 1783) је био швајцарски математичар, физичар, астроном, географ, логичар и инжењер. У математици је основао области топологије и теорије графова, а имао је и велике доприносе аналтичкој теорији бројева, комплексној анализи и инфинитезималном рачуну. Сматра се једним од највећих математичара икада.

Дефиниција 5.2. $\sum_{k=1}^{\infty} \frac{1}{k}$ зове се **хармонијски** ред.[2]

Теорема 5.2. Хармонијски ред дивергира.

Доказ. Показаћемо да хармонијски ред дивергира тако што ћемо показати да други ред, који је мањи од хармонијског, тежи бесконачности. Дефинишимо ред чији је $n-$ти члан једнак $1/2^k$, где је 2^k најмањи степен двојке за који важи $n \leqslant 2^k$.

$$\begin{aligned}\sum_{k=1}^{\infty} \frac{1}{k} &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \dots \\ &> 1 + \frac{1}{2} + (\frac{1}{4} + \frac{1}{4}) + (\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}) + \dots \\ &= 1 + \frac{1}{2} + \frac{1}{2} + \dots\end{aligned}$$

Одавде видимо да хармонијски ред мора да дивергира. □

До сада смо у доказима користили то што сваки природан број већи од јединице има простог делиоца. Сада нам то неће бити довољно, него ће нам бити потребна чињеница да се сваки број већи од један може јединствено раставити на просте факторе.

Теорема 5.3. (*Основна теорема аритметике*) Сваки природан број већи од један има јединствену факторизацију преко простих чиниоца.

Доказ. Прво треба да покажемо да се сваки природан број већи од један може представити као производ простих бројева, а потом ћемо доказати јединственост. Постојање ћемо показати јаком индукцијом.
База. $n = 2$ је прост, једини фактор му је управо 2.
Индуктивни корак. Ако се сваки број мањи од n може представити као производ простих бројева, онда се може представити и n.
Ако је n прост, његов једини фактор је управо n. Ако није, онда постоје бројеви a и b такви да $n = ab$ и $1 < a \leqslant b < n$. Како се по индуктивној хипотези и a и b могу представити као производи простих бројева, n се може представити као производ њихових факторизација.

Сада остаје да покажемо да је факторизација јединствена. Претпоставимо да је n најмањи број чија факторизација није јединствена, односно да $n = p_1 \cdots p_n = q_1 \cdots q_k$. Одавде закључујемо да $p_1 \mid q_1 \cdots q_k$ па, пошто су у питању прости бројеви, мора бити $p_1 = q_i$ за неко $1 \leqslant i \leqslant k$. Нека је то, без умањења општости, q_1. Након што скратимо p_1 односно q_1 из израза, остаје

[2] Редови дефинисани као $\sum_{k=1}^{\infty} \frac{1}{k^a}, a \neq 1$ зову се **уопштени** хармонијски редови. За све вредности $a > 1$ конвергирају, док за $a < 1$ дивергирају.

нам једнакост $p_2 \cdots p_n = q_2 \cdots q_k$ па и број $\frac{n}{p_1}$, који је мањи од n, нема јединствену факторизацију што је у контрадикцији са почетном претпоставком. То значи да не постоји број чија факторизација није јединствена. □

5.1 Ојлеров доказ

Теорема 5.4. Постоји бесконачно много простих бројева.

Доказ. Посматрајмо број облика $\frac{1}{1-\frac{1}{p}}, p \in \mathbb{P}$. Приметимо да је управо то сума геометријског реда са почетним чланом 1 и количником $\frac{1}{p}$, односно да

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \dots$$

Шта се деси када помножимо више оваквих редова? Узмимо геометријске редове са количницима $\frac{1}{2}$, $\frac{1}{3}$ и $\frac{1}{5}$, где је почетни члан сва три јединица.

$$\begin{aligned}\frac{1}{1-\frac{1}{2}} \cdot \frac{1}{1-\frac{1}{3}} \cdot \frac{1}{1-\frac{1}{5}} &= (1 + \frac{1}{2} + \frac{1}{4} + \dots)(1 + \frac{1}{3} + \frac{1}{9} + \dots)(1 + \frac{1}{5} + \frac{1}{25} + \dots) \\ &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{12} + \frac{1}{15} \dots\end{aligned}$$

У овој једнакости користимо дистрибутивност при множењу редова. То смемо да урадимо због тога што посматрамо производ три конвергентна реда чији су сви чланови позитивни.[3] Ова сума личи на хармонијски ред, али се у њој појављују само реципрочне вредности бројева у чијој факторизацији учествују једино 2, 3 и 5. Приметимо да бисмо додавањем нових чланова облика $\frac{1}{1-\frac{1}{p}}$ у десној суми добили реципрочне вредности бројева у чијој факторизацији учествује ново p, а сви остали фактори су степени претходно урачунатих простих бројева. Сада знамо да

$$\prod_{p \in \mathbb{P}} \frac{1}{1-\frac{1}{p}} = \sum_{n=1} \frac{1}{n},$$

а основна теорема аритметике нам обезбеђује да се сваки $\frac{1}{n}$ појављује тачно једном. Пошто на основу теореме 5.2 знамо да хармонијски низ дивергира, производ са леве стране не може садржати коначно много елемената, одакле закључујемо да простих бројева мора имати бесконачно много. □

[3] Мертенсова теорема тврди да, ако су $\sum_{n=0}^{\infty} a_n$ и $\sum_{n=0}^{\infty} b_n$ конвергентни редови, њихове суме бројеви A и B и бар један од ових редова апсолутно конвергира, тада њихов Кошијев производ конвергира управо у AB.

6

Доказ преко топологије

За овај доказ, који је Фурстенберг[1] објавио 1955. године, биће нам потребно неколико основних појмова из топологије. Зато ћемо прво проћи кроз њих, затим кроз сам доказ, а на крају показати како је овај доказ заправо идејно врло сличан Еуклидовом.

6.1 Основе топологије

Дефиниција 6.1. Нека је X скуп а τ неки скуп подскупова X. Скуп τ је **топологија** ако важе следећи услови:

(1) $\emptyset, X \in \tau$.

(2) Било која унија елемената из τ је такође члан скупа τ.

(3) Пресек коначно много елемената из τ је такође члан скупа τ.

Структура (X, τ) зове се **тополошки простор**.

Дефиниција 6.2. Нека је (X, τ) тополошки простор. За скуп кажемо да је **отворен** ако припада τ, односно **затворен** ако његов комплемент припада τ.

Коментар. Скуп може бити у исто време и отворен и затворен као што су празан скуп и сам скуп X. Такође, скуп не мора бити ни отворен ни затворен.

Лема 6.1. Унија коначно много затворених скупова је затворен скуп.

[1] *Hillel Furstenberg*, рођен 29. септембра 1935. године у Немачкој, је америчко-израелски математичар најпознатији по својим доприносима теорији бројева и теорији група.

Доказ. Обележимо посматране затворене скупове са $U_1, \ldots, U_n$, а њихове отворене комплементе са $\overline{U_1}, \ldots, \overline{U_n}$.

$$\overline{(\bigcup_{i=1}^{n} U_i)} = \bigcap_{i=1}^{n} \overline{U_i}$$

Пошто је пресек коначно много отворених скупова отворен, то значи да је комплемент уније посматраних скупова отворен, односно да је унија посматраних скупова затворена. □

Због потреба доказа, бавићемо се конкретно топологијама на скупу целих бројева. Изабраћемо прво другачију дефиницију отвореног скупа, а онда показати да овако дефинисани отворени скупови формирају топологију.

Дефиниција 6.3. За скуп $U \subset \mathbb{Z}$ кажемо да је **отворен** ако је он или празан или ако за свако $a \in U$ постоји аритметички низ облика $a + m\mathbb{Z}$ за неко $m \geqslant 1$ таква да је $a + m\mathbb{Z} \subset U$.

Доказ. Покажимо да ови отворени скупови задовољавају услове топологије.

(1) Празан скуп је по дефиницији отворен, а $\mathbb{Z} = 0 + 1 \cdot \mathbb{Z}$ је такође отворен.

(2) Узмимо произвољан скуп ових подскупова $\{U_i\}$. Њихова унија такође мора бити отворена јер, пошто свако a које припада унији мора припадати и неком конкретном подскупу, рецимо U_i, имамо да је $a + m\mathbb{Z} \subset U_i$ за неко $m \geqslant 1$, па самим тим тај низ мора бити и подскуп уније.

(3) Узмимо коначно много ових подскупова, на пример $U_1, \ldots, U_n$. Ако је њихов пресек празан скуп, он је по дефиницији отворен. Ако није, узмимо неко $a \in \bigcap_{i=1}^{n} U_i$. За такво a, за сваки U_i мора постојати аритметички низ такав да је $a + m_i\mathbb{Z} \subset U_i, m_i \geqslant 1$. То значи да ће аритметички низ $a + m_1 \cdots m_n\mathbb{Z}$ бити подскуп сваког од ових подскупова, па ће бити и подскуп њиховог пресека. Дакле, показали смо да за сваки елемент посматраног пресека постоји аритметички низ који је подскуп пресека која садржи тај елемент, чиме је доказ завршен.

□

Коментар. Овако дефинисана топологија има два битна својства.

(1) Пошто сваки непразан отворени подскуп скупа $\mathbb{Z}$ по дефиницији садржи неки аритметички низ, ниједан од њих није коначан.

(2) Сваки аритметички низ (посматран као скуп) је уједно и отворен и затворен.

Доказ. За сваки елемент $a + mb$ из $a + m\mathbb{Z}$ имамо да је $a + mb + m\mathbb{Z} = a + m\mathbb{Z}$, чиме смо показали отвореност. Комплемент скупа вредности аритметичог низа $a + mb$ је унија аритметичких низова облика $r + m\mathbb{Z}$ за $0 \leqslant r \leqslant m - 1, r \not\equiv_m a$. Показали смо да је сваки аритметички низ отворен, као и да је унија отворених скупова отворена, па онда, пошто је комплемент сваког аритметичког низа отворен, сваки аритметички низ мора бити затворен. □

6.2 Фурстенбергов доказ

Теорема 6.1. Постоји бесконачно много простих бројева.

Доказ. Посматрајмо (као скупове) аритметичке низове облика $p\mathbb{Z}, p \in \mathbb{P}$. Унија свих ових скупова је управо $\mathbb{Z}\setminus\{\pm 1\}$, јер на основу леме 2.1 сви остали цели бројеви имају неког простог делиоца. Пошто скуп $\{\pm 1\}$ није празан, а нема ни бесконачно много елемената, он није отворен. Уније посматраних скупова је комплемент овог скупа, па она онда није затворена. Сваки од посматраних скупова је затворен, па би њихова унија, ако би их било коначно много, такође била затворена на основу леме 6.1. Ово није случај, па посматраних скупова, а самим тим и простих бројева, мора бити бесконачно много. □

Овај доказ користи само основне тополошке појмове. Сваку од тврдњи које су нам потребне за доказ можемо извести и без увођења било каквих нових појмова. Показаћемо да је сваки низ $p\mathbb{Z}$ затворен и да је унија коначно много оваквих низова такође затворена без помињања топологија.

Покажимо да је сваки низ $p\mathbb{Z}$ (посматран као скуп) затворен. Његов комплемент је $\mathbb{Z}\setminus(p\mathbb{Z}) = \{a \in \mathbb{Z} \mid p \nmid a\}$, односно скуп свих целих бројева који нису дељиви са p. За произвољан елемент овог скупа a, аритметички низ $a + p\mathbb{Z}$ је у целини садржан у овом скупу јер, пошто a није дељиво са p, неће бити ни било који број облика $a + pk$. Пошто смо овиме показали да је комплемент од $p\mathbb{Z}$ отворен, он сам мора бити затворен.

Покажимо да је унија скупова вредности коначно много оваквих низова затворена. Обележимо ове низове са $p_1\mathbb{Z}, \ldots, p_n\mathbb{Z}$. Комплемент њихове уније је $\bigcap_{i=1}^{n} \mathbb{Z} \setminus (p_i\mathbb{Z}) = \{a \in \mathbb{Z} \mid p_i \nmid a, i = 1, \ldots, n\}$ односно скуп свих бројева којима ниједан од посматраних простих бројева није фактор. Покажимо да је овај скуп отворен. За произвољан елемент овог скупа a, аритметички низ $a + p_1 \cdots p_n\mathbb{Z}$ је у целини садржан у овом скупу јер, пошто a није дељиво ни са једним од ових простих бројева, неће бити ни било који број облика $a + p_1 \cdots p_n\mathbb{Z}$. Овиме смо показали да је комплемент посматране уније отворен, па је она сама по дефиницији затворена.

Кренимо сад опет корацима Фурстенберговог доказа. По леми 2.1 знамо

да сви остали бројеви осим ± 1 имају просте делиоце, односно да важи

$$\bigcap_{p\in\mathbb{P}} \mathbb{Z} \setminus (p\mathbb{Z}) = \{\pm 1\}$$

Скуп $\{\pm 1\}$ очигледно не садржи ниједан аритметички низ, па самим тим ниједан аритметички низ не постоји ни у скупу са леве стране једначине. Међутим, показали смо да, за коначан број простих бројева, он садржи аритметичке низове, па он не може бити пресек коначно много скупова. Дакле, пошто сваки прост број одређује један од ових скупова, простих бројева мора бити бесконачно много.

Ако овај доказ мало преформулишемо, видимо да је његова суштина да, за коначан број простих бројева, посматрани пресек садржи аритметички низ $1 + p_1 \cdots p_n\mathbb{Z}$. Ово нам говори да ниједан број облика $1 + p_1 \cdots p_n b, b \in \mathbb{Z}$ није дељив било којим од p_i, а управо на томе је, за $b = 1$, заснован Еуклидов доказ.

7

Доказ преко комбинаторике

Последњи, а по мом мишљењу најлепши, доказ који сам одабрао записао је Ердош[1] у фусноти рада који се бавио доказом дивергенције реда $\sum_{p\in\mathbb{P}} \frac{1}{p}$.

Лема 7.1. Сваки природан број се може јединствено записати као производ квадрата природног броја и броја који није дељив ниједним квадратом природног броја већег од један.

Доказ. Основна теорема аритметике нам говори да се сваки природан број n може на јединствен начин раставити на просте чиниоце. Нека је $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Пошто сваки прост чинилац у факторизацији броја b^2 мора бити парног степена, а ниједан прост чинилац у факторизацији броја a не сме имати степен већи од 1, и притом важи $n = b^2a$, јасно је да постоји један начин да распоредимо ове просте факторе. Нека је p_i неки од ових простих чиниоца чији је степен α_i.

1° Ако је α_i парно, тада p_i учествује у факторизацији b^2 степеном α_i, а у факторизацији a не учествује.

2° Ако је α_i непарно, тада p_i учествује у факторизацији b^2 степеном $\alpha_i - 1$, а у факторизацији a учествује степеном један.

□

7.1 Ердошев доказ

Теорема 7.1. Постоји бесконачно много простих бројева.

[1] *Paul Erdős* (26. март 1931 - 20. септембар 1996) био је мађарски математичар који се бавио гранама дискретне математике, теорије бројева, теорије група, анализе, теорије процена и вероватноће. Највише је истраживао отворена питања, а поставио је и велик број хипотеза. Сматра се једним од најзначајнијих математичара 20. века.

Доказ. Претпоставимо да је скуп простих бројева коначан, $\mathbb{P} = \{p_1, \ldots, p_k\}$. Изаберимо неко $N \in \mathbb{N}$. По леми 7.1, сваки природан број до N се може јединствено представити као b^2a, где је b природан број, а a није дељив квадратом природног броја већег од један. Број избора за b може бити највише $\sqrt{N}$, јер би иначе било $b^2a > N$. Пошто се у факторизацији броја a сваки прост број може појавити највише једном, а по претпоставци постоји k простих бројева, број избора за a је 2^k (сваки прост број може или да не учествује у факторизацији или да учествује првим степеном). То значи да бројева мањих од N може бити највише $2^k \cdot \sqrt{N}$. Одавде следи да је $N \leqslant 2^k \cdot \sqrt{N}$ односно да важи $\sqrt{N} \leqslant 2^k$ за свако N. Међутим, ово очигледно не важи за $N > 2^{2k}$, што значи да нам је почетна претпоставка погрешна, па простих бројева мора бити бесконачно много. □

На основу овог доказа можемо наћи још једно доње ограничење за $\pi(x)$.
Последица. За природан број $N \geqslant 2,\ \pi(N) \geqslant \frac{\log_2(N)}{2}$.

Доказ. Нека је N природан број и нека је $\pi(N) = k$. Као и у самом доказу, користећи лему 7.1 долазимо до неједнакости $\sqrt{N} \leqslant 2^k$.

$$\sqrt{N} \leqslant 2^{\pi(N)} \implies \log_2(\sqrt{N}) \leqslant \pi(x) \implies \frac{\log_2(N)}{2} \leqslant \pi(x). \qquad \square$$

Литература

[1] Martin Aigner, Günter M. Ziegler, *Proofs from THE BOOK*, Springer, 3rd ed

[2] Keith Conrad, *The infinitude of primes*

[3] Keith Conrad, *The "topological" proof of the infinitude of primes*

[4] https://www.wikipedia.org