Селбергова асимптотска формула

др Горан Ђанковић, **Београд**

Драгици Стојановић и успомени на Николу Муца,
мојим наставницима и мојим херојима,
са најдубљом захвалношћу

1. Увод

1.1. Колико има простих бројева? Сви ученици 5. разреда основне школе знају шта су прости бројеви. На пример, 5, 17, 97 и 229 су прости. Свако је научио како да провери да ли је неки (не претерано велики) број прост или не. Ја се и данас сећам часова, на којима нам је мој наставник Никола Муц показивао како то да урадимо и сећам се табле прекривене његовим ситним уредним цифрама. Сећам се свог узбуђења, што сад знам поступак како то да урадим за *било који* број и свог узбуђења што за само неке, ретке, бројеве „испадне" да су прости, док већини брзо нађемо неки делиоц већи од 1. Дакле, прости бројеви су један од најранијих математичких концепата. Најранијих, и по узрасту кад их деца сусрећу, и по томе што су за њих знали и о њима размишљали људи још у античком добу. Сви читаоци „Тангенте" знају да је још Еуклид, око 300. године пре нове ере, доказао да простих бројева има *бесконачно много.* То је један од најчувенијих и најефектнијих доказа свођењем на контрадикцију. Претпоставимо да простих бројева има само коначно много, означимо их све са $p_1, p_2, \dots, p_k$, па онда посматрајмо број $p_1 p_2 \cdots p_k + 1$. И он мора имати бар један прост делиоц, а одмах видимо да тај делиоц не може бити на нашем списку.

Прости бројеви су веома интригантни. Толико су једноставни, да и деца раде задатке о њима, а са друге стране проучавали су их и највећи математичари у историји, па и после свих њих и даље имамо много хипотеза о простим бројевима, које су недоказане. Тај наизглед једноставан подниз у скупу природних бројева је непресушан извор изузетно дубоке и занимљиве математике.

Које је најједноставније питање о простим бројевима, ако већ знамо да их има бескочачно много? Па, прво прецизније питање је колико су „чести" прости бројеви, да ли се они у низу природних бројева појављују на потпуно случајан начин, или можда постоји нека законитост коју они следе? На пример у интервалу $[1, 100]$ има тачно 25 простих бројева. Ако читалац не зна шта ће од дуга дана, може да провери и да у интервалу $[1, 100\,000\,000]$ има тачно 5 761 455 простих бројева. И уопште, ако са $\pi(x)$ означимо број простих бројева у интервалу $[1, x]$, колико је $\pi(x)$? За појединачне вредности x, видели смо да је $\pi(x)$ неки бизаран број, али можемо да се запитамо: како (колико брзо) $\pi(x)$ расте са x?

То се запитао и један петнаестогодишњи дечак у 18. веку. Почео је да проучава и прави таблице простих бројева и да их броји у све већим и већим интервалима. Приметио је да се прости бројеви око x срећу са вероватноћом $\frac{1}{\log x}$, где (и свуда надаље) са $\log x$ означавамо природни логаритам. Дакле, како се x повећава, прости бројеви су све „ређи" и „ређи", али се још увек појављују, са поприличном правилношћу. Дакле, дечак је претпоставио да је $\pi(x)$ отприлике једнако

$$\int_2^x \frac{dt}{\log t}. \tag{1}$$

Наравно, $\pi(x)$ скоро никад није баш једнако вредности овог интеграла (која се *непрекидно* повећава са x, док $\pi(x)$ има *скок* за 1 у сваком простом броју), али дечак је претпоставио да је $\int_2^x \frac{dt}{\log t}$ *увек* јако близу $\pi(x)$. На пример, за $x = 100\,000\,000$, овај интеграл има вредност која је за око 753 већа од тачне вредности $\pi(x) = 5\,761\,455$. Видимо да је грешка јако мала, у поређењу са величином $\pi(x)$. И уопште, кад $x \to \infty$, дечак је претпоставио да

$$\lim_{x\to\infty} \frac{\pi(x)}{\int_2^x \frac{dt}{\log t}}$$

постоји и да је једнак 1. Ето, то је најједноставније и најосновније питање о простим бројевима и њиховој *расподели* унутар скупа свих природних бројева. То је прва хипотеза да потпуно „непредвидив" низ простих бројева, ипак није сасвим непредвидив: функција $\pi(x)$ која броји просте бројеве расте по тачно одређеном асимптотском закону!

На овом месту се можда многи читаоци, чак и они који су преспремни такмичари и освајачи награда на државним и међународним такмичењима и који знају све што се има знати у средњошколској математици, питају како то да ја не знам доказ овог тврђења? У ствари, доказ ове хипотезе није знао ни петнаестогодишњи дечак који ју је формулисао (чак ни када је порастао). Она је доказана тек око 100 година касније, 1896. године. Од тада то је теорема, и зове се *Теорема о простим бројевима*. Дечак из наше приче се звао Карл Фридрих Гаус...

Доказ Теореме о простим бројевима је био спектакуларан! Методе које су коришћене у доказу припадају области математике која се зове *комплексна анализа*[1] и која проучава комплексне функције! Доказ ове теореме је практично круна математике 19. века. То је био један од првих дубоких доказа математике у коме се, да би се доказала хипотеза у једној области (бројевима), користила сасвим друга и наизглед тотално неповезана област (комплексна анализа). На српском језику, овај доказ је изложен у књигама [2] и [1].

1.2. Може ли то мало елементарније? Мора ли та комплексна анализа? Најпре, људи су се, као вероватно и читаоци сада, осећали доста нелагодно. Нас су интересовали (прелепи, чисти и невини) прости бројеви, а доказ у коме се рачунају разни комплексни интеграли и доказује гомила оцена и неједнакости, делује перверзно.

Одмах се појавила жеља да се нађе и *елементаран* доказ Теореме о простим бројевима. Дуго година то никоме није пошло за руком: теорема је заста *тешка*. Тек 1948. године, тада тридесетједногодишњи норвешки математичар, Атл Селберг, који се тада већ налазио на *Институту за напредне студије* у Принстону, САД, доказао је

[1] коју ће читаоци упознати на факултету

елементарним средствима следећу асимптотску формулу:

$$\sum_{\substack{p \text{ прост} \\ p \leqslant x}} \log^2 p + \sum_{\substack{p \neq q \text{ прости} \\ pq \leqslant x}} \log p \log q = 2x \log x + O(x). \tag{2}$$

Овде је симбол $O(\cdot)$ такозвана „велико O" асимптотска нотација: за две реалне функције f и g ћемо писати $f(x) = O(g(x))$ и читати *f је велико O од g*, ако постоји нека константа $C > 0$, таква да важи неједнакост $|f(x)| \leqslant Cg(x)$, за све $x \geqslant 1$. Често нам тачна вредност константе C није битна, па се онда користи O-нотација.[2] У једнакости (2), $2x \log x$ је *главни члан*, док $O(x)$ означава неку функцију која расте највише линеарно по x. Кад $x \to \infty$, овај други члан је много мањи од главног члана тј. кажемо да је *мањег асимптотског реда величине*.

Селберг је формулу (2) доказао потпуно *независно* од Теореме о простим бројевима. Пробајмо да урадимо следеће *хеуристичко* разматрање. Претпоставимо да имамо Теорему о простим бројевима. Леву страну Селберговог асимптотског идентитета (2) напишимо као

$$\sum_{\substack{p \text{ прост} \\ p \leqslant x}} \log^2 p + 2 \sum_{\substack{p \text{ прост} \\ p \leqslant \sqrt{x}}} \log p \sum_{\substack{q \text{ прост} \\ p < q \leqslant x/p}} \log q,$$

где је двострука сума расписана за случај $p < q$, па због симетричног случаја $p > q$, имамо и фактор 2.

Сада суме заменимо интегралима (то је оно што је и петнаестогодишњи Гаус претпоставио да важи). У првој суми, за просте бројеве величине око t, вредност сваког суманда је око $(\log t)^2$, а према Теореми о простим бројевима, густина простих бројева око t је $\frac{1}{\log t}$, па прву суму хеуристички можемо заменити интегралом

$$\int_1^x (\log t)^2 \frac{1}{\log t} dt = x \log x - x + 1 = x \log x + O(x).$$

Слично, унутрашњу суму по простим бројевима q можемо хеуристички заменити интегралом

$$\int_p^{x/p} \log t \cdot \frac{1}{\log t} dt = \frac{x}{p} - p,$$

па укупно двострука сума по p, q доприноси (поново, заменом сума по простим бројевима, интегралима са „густином" $\frac{1}{\log t}$)

$$\begin{aligned} 2 \sum_{\substack{p \text{ прост} \\ p \leqslant \sqrt{x}}} \log p \left(\frac{x}{p} - p\right) &= 2x \sum_{\substack{p \text{ прост} \\ p \leqslant \sqrt{x}}} \frac{\log p}{p} - 2 \sum_{\substack{p \text{ прост} \\ p \leqslant \sqrt{x}}} p \log p \\ &\approx 2x \int_1^{\sqrt{x}} \frac{\log t}{t} \cdot \frac{1}{\log t} dt - 2 \int_1^{\sqrt{x}} t \log t \cdot \frac{1}{\log t} dt \\ &= 2x \log \sqrt{x} - x + 1 = x \log x + O(x). \end{aligned}$$

[2] Многи докази у *анализи* и *аналитичкој теорији бројева* користе и по неколико десетина неједнакости и оцена и у свакој од њих би се појављивале неке константе, које би било компликовано и означавати, а и све теже и прецизно израчунавати. У таквим доказима долази до изражаја корисност O-нотације.

Дакле, укупно, лева страна (2) је једнака $x\log x + O(x) + x\log x + O(x) = 2x\log x + O(x)$, што јесте десна страна Селберговог идентитета. Ово хеуристичко разматрање се у ствари може лако претворити у прави доказ, тј. Селбергов идентитет (2) је лака последица Теореме о простим бројевима.

Велики мађарски математичар Пал Ердош, који се у то време налазио у Принстону, чим је видео Селбергов идентитет, схватио је да је тај идентитет *јако близу* Теореми о простим бројевима, и да се мост од (2) до целе теореме може урадити *елементарно*. Ердош је то и успео, а кад је Селберг чуо да је Ердош успео, успео је и Селберг да докаже Теорему о простим бројевима елементарно, независно од Ердоша.

Математичка јавност је била одушевљена и Атл Селберг је 1950. године добио *Филдсову медаљу*, између осталог и за свој елементарни доказ Теореме о простим бројевима.

1.3. Циљ овог чланка. Цео елементарни доказ Теореме о простим бројевима је у ствари, релативно дугачак и толико компликован, да се уместо да је елементаран, може рећи и да је „елементаран". У сваком случају превазилази оквире овог часописа. Додатно, тај доказ се није показао бољим од доказа комплексном анализом, који за разлику од „елементарног", може да се уопшти на огромну класу аритметичких објеката (и њима придружених низова), који су (разна) уопштења простих бројева.

Али Селбергова асимптотска формула (2), која је *кључна компонента* „елементарног" доказа нам је на дохват руке. Циљ нам је да изложимо доказ формуле (2), како би се и ученици средње школе упознали са неким од основних идеја и концепата *теорије простих бројева* и како би читаоци можда успели да наслуте њену дубину и лепоту. Дакле, само ћемо да отшкринемо врата у овај нови, узбудљиви, тајанствени свет...

За читање овог чланка је потребно да читаоци знају Риманов одређени интеграл и да умеју да интеграле неколико једноставнијих функција. Дакле, надам се да је чланак доступан ученицима 4. разреда средњих школа. Додатно, сви одељци, осим 4. су и потпуно елементарни.

2. Аритметичке функције и прости бројеви

Аритметичка функција је свака функција $f : \mathbb{N} \to \mathbb{C}$ дефинисана на скупу природних бројева.

2.1. Мебијусова и фон Манголтова функција. *Мебијусову функцију* $\mu : \mathbb{N} \to \{-1, 0, 1\}$ дефинишемо на следећи начин: ако је n дељив квадратом неког простог броја, онда је $\mu(n) = 0$, а ако је n производ k *различитих* простих бројева, онда је $\mu(n) = (-1)^k$. Додатно дефинишемо $\mu(1) = 1$. На пример, $\mu(2) = -1$, $\mu(4) = 0$, $\mu(6) = 1$, $\mu(10) = 1$, $\mu(12) = 0$, $\mu(30) = -1$, $\mu(36) = 0$, $\mu(37) = -1$, $\mu(38) = 1$, $\mu(39) = 1$, $\mu(40) = 0, \ldots$.

Друга функција која ће нас занимати је *фон Манголтова функција* Λ дефинисана са

$$\Lambda(n) = \begin{cases} \log p, & \text{ако је } n = p^{\alpha}, \text{ за неки прост број } p \text{ и неко } \alpha \geqslant 1, \\ 0, & \text{иначе.} \end{cases}$$

На пример, $\Lambda(1) = 0$, $\Lambda(5) = \log 5$, $\Lambda(9) = \log 3$, $\Lambda(10) = 0$, $\Lambda(25) = \log 5$, $\Lambda(26) = 0$, $\Lambda(27) = \log 3$, $\Lambda(28) = 0$, $\Lambda(29) = \log 29$, $\Lambda(30) = 0$, $\Lambda(125) = \log 5, \ldots$.

Функције μ и Λ су практично две најважније аритметичке функције, иако се то можда на први поглед не може наслутити. Једино што нам одмах упада у очи је да је функција Λ уско повезана са простим бројевима: она *детектује* просте бројеве p (и њихове степене) „тежином" $\log p$, док је на свим осталим природним бројевима, који имају бар два различита проста фактора, једнака 0.

Дефинисаћемо и константну аритметичку функцију $\mathbf{1} : \mathbb{N} \to \mathbb{C}$, $\mathbf{1}(n) = 1$, за све $n \in \mathbb{N}$.

2.2. Дирихлеова конволуција. За две аритметичке функције $f, g : \mathbb{N} \to \mathbb{C}$ дефинишемо њихову *Дирихлеову конволуцију* $f * g : \mathbb{N} \to \mathbb{C}$ са

$$f * g(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{dm=n} f(d) g(m).$$

Овде је сумирање по свим различитим природним делиоцима природног броја n. Дакле, на пример

$$f * g(49) = f(1)g(49) + f(7)g(7) + f(49)g(1),$$

док је

$$f * g(50) = f(1)g(50) + f(2)g(25) + f(5)g(10) + f(10)g(5) + f(25)g(2) + f(50)g(1).$$

Из дефиниције се одмах види да је Дирихлеова конволуција комутативна, односно да је $f * g = g * f$.

Дирихлеова конволуција је изузетно природна операција. Она нам даје начин да „помножимо" две аритметичке функције, али на начин који респектује мултипликативну структуру природних бројева, а то је управо оно што желимо да разумемо.

Пример 2.1. Одредимо шта је Дирихлеова конволуција фон Манголтове функције Λ и константне функције $\mathbf{1}$.

На основу *Основне теореме аритметике*, сваки природан број n можемо на јединствен начин факторисати као $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, где су p_j прости бројеви и $\alpha_j \geqslant 1$. Сада имамо $\Lambda * \mathbf{1}(n) = \sum\limits_{d|n} \Lambda(d) \mathbf{1}\left(\frac{n}{d}\right) = \sum\limits_{d|n} \Lambda(d)$, а због дефиниције фон Манголтове функције, $\Lambda(d) \neq 0$ само за делиоце d који су степени једног простог броја, тј. за d облика p_j^{β}, за неко $1 \leqslant \beta \leqslant \alpha_j$. Дакле, добијамо да је

$$\Lambda * \mathbf{1}(n) = \sum_{j=1}^{k} \sum_{\beta=1}^{\alpha_j} \Lambda(p_j^{\beta}) = \sum_{j=1}^{k} \sum_{\beta=1}^{\alpha_j} \log p_j = \sum_{j=1}^{k} \alpha_j \log p_j = \sum_{j=1}^{k} \log p_j^{\alpha_j} = \log n,$$

односно конволуција $\Lambda * \mathbf{1}$ није ништа друго него логаритам. $\square$

2.3. Формула Мебијусове инверзије. Значај и корисност Мебијусове функције μ можемо да наслутимо из следећег тврђења.

Тврђење 2.2. *Ако су $f, g : \mathbb{N} \to \mathbb{C}$ две аритметичке функције, важи следећа еквиваленција:*

$$f = g * \mathbf{1} \iff g = f * \mu.$$

Дакле, ако је f конволуцијски производ функције g и константне функције $\mathbf{1}$ (а што се често среће у пракси), онда g можемо да реконструишемо као конволуцијски производ функције f и Мебијусове функције μ.

Доказ. Доказ тривијално следи из следеће основне формуле

$$\mu * \mathbf{1}(n) = \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{ако је } n = 1, \\ 0, & \text{ако је } n > 1. \end{cases} \tag{3}$$

Да бисмо њу доказали, означимо $1 < n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Како је Мебијусова функција једнака 0 на свим бројевима d дељивим квадратом неког простог броја, одмах закључујемо да је

$$\sum_{d|n} \mu(d) = \sum_{d|(p_1 p_2 \dots p_k)} \mu(d) = \sum_{r=0}^{k} \binom{k}{r} (-1)^r = (1-1)^k = 0,$$

јер за свако $0 \leqslant r \leqslant k$, број $p_1 p_2 \dots p_k$ има укупно $\binom{k}{r}$ делиоца d који имају тачно r простих фактора и за које је $\mu(d) = (-1)^r$.

Претпоставимо сада да је $f = g * \mathbf{1}$. Онда за свако $n \in \mathbb{N}$ имамо да је

$$\begin{aligned} f * \mu(n) &= \sum_{md=n} f(m)\mu(d) = \sum_{md=n} g * \mathbf{1}(m)\mu(d) = \sum_{md=n} \mu(d) \sum_{ab=m} g(a)\mathbf{1}(b) \\ &= \sum_{abd=n} g(a)\mu(d) = \sum_{a|n} g(a) \sum_{d|\frac{n}{a}} \mu(d) = \sum_{a|n} g(a)\ \mu * \mathbf{1}\left(\frac{n}{a}\right) = g(n), \end{aligned}$$

где смо последњу једнакост добили директном применом формуле (3). Ово значи да је $f * \mu = g$, чиме смо доказали један смер тврђења. Супротан смер остављамо читаоцима за вежбу. $\square$

Последица 2.3. *Ако су T и G две реалне функције на $(0, \infty)$ које за свако реално $x > 0$ задовољавају једнакост*

$$T(x) = \sum_{m \leqslant x} G\left(\frac{x}{m}\right),$$

онда за све $x > 0$ важи и једнакост

$$G(x) = \sum_{n \leqslant x} \mu(n) T\left(\frac{x}{n}\right).$$

Доказ. Пођимо од десне стране:

$$\sum_{n\leqslant x}\mu(n)T\left(\frac{x}{n}\right)=\sum_{n\leqslant x}\mu(n)\sum_{m\leqslant x/n}G\left(\frac{x/n}{m}\right)=\sum_{mn\leqslant x}\mu(n)G\left(\frac{x}{mn}\right)$$
$$=\sum_{k\leqslant x}G\left(\frac{x}{k}\right)\cdot\sum_{mn=k}\mu(n)=G(x),$$

где смо у другом реду увели смену променљивих $k=mn$ и због формуле (3) је „преживео" само сабирак за $k=1$. □

Задатак 2.4. Доказати да важи и обрнути смер из претходне последице.

2.4. Фон Манголтова функција реда 2. Ову функцију ћемо означити са Λ_2 и дефинисати на следећи начин:

$$\Lambda_2(n)=\Lambda(n)\log n+\sum_{lm=n}\Lambda(l)\Lambda(m).$$

Ова дефиниција делује компликованије него претходне, па погледајмо на примерима шта су њене вредности. Ако је $n=p^\alpha$, степен простог броја, имамо да је

$$\Lambda_2(p^\alpha)=\Lambda(p^\alpha)\log p^\alpha+\sum_{lm=p^\alpha}\Lambda(l)\Lambda(m)=\log p\cdot\alpha\log p+\sum_{j=0}^{\alpha}\Lambda(p^j)\Lambda(p^{\alpha-j})$$
$$=\alpha(\log p)^2+(\alpha-1)(\log p)^2=(2\alpha-1)(\log p)^2.$$

Ако је $n=p^\alpha q^\beta$, где су p и q различити прости бројеви и $\alpha,\beta\geqslant 1$, имамо да је $\Lambda_2(p^\alpha q^\beta)=\Lambda(p^\alpha q^\beta)\log(p^\alpha q^\beta)+\sum_{lm=p^\alpha q^\beta}\Lambda(l)\Lambda(m)=\sum_{lm=p^\alpha q^\beta}\Lambda(l)\Lambda(m)$. Међутим, због дефиниције Λ, сви сабирци у последњој суми су 0, осим за $l=p^\alpha$ и $l=q^\beta$, па, дакле, добијамо да је

$$\Lambda_2(p^\alpha q^\beta)=\Lambda(p^\alpha)\Lambda(q^\beta)+\Lambda(q^\beta)\Lambda(p^\alpha)=2\log p\log q.$$

Сада одмах видимо и да ако n има *бар три* различита проста фактора, $\Lambda_2(n)$ ће бити 0, јер у сваком члану $\Lambda(l)\Lambda(m)$ у суми која дефинише Λ_2, или l или m морају имати бар два различита проста фактора, па одговарајући члан мора бити 0.

Дакле, *фон Манголтова функција реда* 2 „детектује" природне бројеве који су дељиви са највише два различита проста броја! Како Λ детектује природне бројеве који су дељиви тачно једним простим бројем, сада видимо зашто су аритметичке функције Λ и Λ_2 рођаци!

Пример 2.5. Аналогно примеру 2.1, одредимо сада шта је Дирихлеова конволуција функција Λ_2 и $\mathbf{1}$.

Користићемо оно што смо већ одредили, тј. да је $\Lambda*\mathbf{1}=\log$. Онда за произвољно

$n \in \mathbb{N}$ имамо

$$\begin{aligned}\Lambda_2 * \mathbf{1}(n) &= \sum_{d|n} \Lambda_2(d)\mathbf{1}\left(\frac{n}{d}\right) = \sum_{d|n} \Lambda_2(d) = \sum_{d|n}\left(\Lambda(d)\log d + \sum_{lm=d} \Lambda(l)\Lambda(m)\right) \\ &= \sum_{d|n} \Lambda(d)\log d + \sum_{lm|n} \Lambda(l)\Lambda(m) = \sum_{l|n} \Lambda(l)\log l + \sum_{lm|n} \Lambda(l)\Lambda(m) \\ &= \sum_{l|n} \Lambda(l)\left(\log l + \sum_{m|(n/l)} \Lambda(m)\right) = \sum_{l|n} \Lambda(l)\left(\log l + \Lambda * \mathbf{1}\left(\frac{n}{l}\right)\right) \\ &= \sum_{l|n} \Lambda(l)\left(\log l + \log\left(\frac{n}{l}\right)\right) = \log n \sum_{l|n} \Lambda(l) = \log n \cdot (\Lambda * \mathbf{1})(n) = (\log n)^2.\end{aligned}$$

Дакле, $\Lambda_2 * \mathbf{1} = \log^2$. $\square$

Применом Мебијусове инверзије сада налазимо и да је $\Lambda_2 = \mu * \log^2$, тј. да за свако $n \in \mathbb{N}$ важи:

$$\Lambda_2(n) = \sum_{d|n} \mu(d)\left(\log \frac{n}{d}\right)^2.$$

Ово је друга формула за фон Манголтову функцију реда 2.

3. Идеја доказа Селбергове формуле

Сада, када смо упознали аритметичку функцију Λ_2, означимо њену суматорну функцију са $S(x) := \sum_{n\leqslant x} \Lambda_2(n)$. Ако упоредимо леву страну Селбергове формуле (2) са сумом $S(x)$, имајући у виду да је $\Lambda_2(p) = (\log p)^2$ и $\Lambda_2(pq) = 2\log p \log q$, закључујемо да је

$$\begin{aligned}&\sum_{n\leqslant x} \Lambda_2(n) - \left(\sum_{\substack{p \text{ прост} \\ p\leqslant x}} \log^2 p + \sum_{\substack{p\neq q \text{ прости} \\ pq\leqslant x}} \log p \log q\right) \\ &= \sum_{n\leqslant x} \Lambda_2(n) - \left(\sum_{\substack{p \text{ прост} \\ p\leqslant x}} \Lambda_2(p) + \sum_{\substack{p< q \text{ прости} \\ pq\leqslant x}} \Lambda_2(pq)\right) \\ &= \sum_{\substack{p \text{ прост, } \alpha\geq 2 \\ p^\alpha\leqslant x}} \Lambda_2(p^\alpha) + \sum_{\substack{n=p^\alpha q^\beta\leqslant x \\ \alpha\geq 2 \text{ или } \beta\geq 2}} \Lambda_2(n) = O\left((\log x)^2 \sum_{p\leqslant\sqrt{x}} 1\right) + O\left(\sum_{\substack{p^\alpha r\leqslant x \\ \alpha\geq 2}} \log p\,\Lambda(r)\right) \\ &= O(\sqrt{x}(\log x)^2) + O\left(\sum_{\substack{p^\alpha\leqslant x \\ \alpha\geq 2}} \log p \sum_{r\leqslant\frac{x}{p^\alpha}} \Lambda(r)\right) = O\left(x\sum_{\substack{p^\alpha\leqslant x \\ \alpha\geq 2}} \frac{\log p}{p^\alpha}\right) = O(x),\end{aligned}$$

где смо у првој суми у трећем реду све сабирке оценили тривијално, а број простих бројева p у интервалу $[1, \sqrt{x}]$ смо тривијално ограничили са $\sqrt{x}$. При оцењивању друге суме у трећем реду смо били пажљивији и искористили класичну (и елементарну) оцену Чебисхева $\sum_{r\leqslant \frac{x}{p^\alpha}} \Lambda(r) = O(\frac{x}{p^\alpha})$. Дакле, како је добијена разлика асимптотски $O(x)$, довољно је да докажемо формулу

$$S(x) = \sum_{n\leqslant x} \Lambda_2(n) = 2x\log x + O(x). \tag{4}$$

Фон Манголтове функције Λ, односно Λ_2, јесу веома лепе са аспекта онога што нам је циљ: пребројавање простих бројева, односно оних који имају највише два различита проста фактора. Међутим, с друге стране, оне су јако *ирегуларне*, што изузетно отежава директан рад са њима.

Наш циљ је да сумирамо вредности функције $\Lambda_2(n)$ у интервалу $[1, x]$, где ће x тежити ∞. Дакле, иако су вредности $\Lambda_2(n)$ „незгодне" и делују „случајно", ипак се надамо да ћемо у јако дугачкој суми, *„у средњем"* успети да дођемо до неке правилности.

Формула (4) коју желимо да докажемо се може записати и као

$$\frac{1}{x}\sum_{n\leqslant x} \Lambda_2(n) = 2\log x + O(1),$$

што заиста можемо интерпретирати као да је средња вредност функције Λ_2 на интервалу $[1, x]$ једнака $2\log x$. Дакле, иако је $\Lambda_2(n)$ најчешће једнако 0 и само понегде веће од нуле, нпр. $\Lambda_2(p) = (\log p)^2$, Селбергова формула каже да ипак постоји правилност.

Прву кључну идеју нам даје резултат примера 2.5: Дирихлеова конволуција „незгодне и непредвидиве" функције Λ_2 са константном функцијом $\mathbf{1}$ даје $\log^2$, „лепу и предвидиву" функцију. Функције f које су регуларне и глатке, као што је $n \mapsto \log^2 n$, можемо без проблема сумирати: најчешће се сума $\sum_{n=1}^{x} f(n)$ може добро апроксимирати интегралом $\int_1^x f(t)dt$. Ово се успешно може урадити применом тзв. Ојлер–Маклоренове формуле и ми ћемо у наредном одељку дати најједноставнију верзију ове формуле, која ће свеједно, бити довољна за оно што нам треба.

Поћи ћемо од суме

$$\sum_{n\leqslant x} \Lambda_2 * \mathbf{1}(n) = \sum_{n\leqslant x} (\log n)^2$$

и асимптотски ћемо је израчунати – одредићемо главни члан кад $x \to \infty$ (како сума има $\sim x$ сабирака од којих је сваки величине $\sim (\log x)^2$, већ видимо да ће водећи члан бити $x(\log x)^2$, али ми ћемо бити још прецизнији од овога).

С друге стране, „отворићемо" конволуцију:

$$\begin{aligned}\sum_{n\leqslant x}\sum_{n\leqslant x} \Lambda_2 * \mathbf{1}(n) &= \sum_{n\leqslant x}\sum_{dm=n} \Lambda_2(d)\mathbf{1}(m) = \sum_{n\leqslant x}\sum_{dm=n} \Lambda_2(d)\\ &= \sum_{m\leqslant x}\sum_{d\leqslant \frac{x}{m}} \Lambda_2(d) = \sum_{m\leqslant x} S\left(\frac{x}{m}\right).\end{aligned}$$

Овде су унутрашње суме $S\left(\frac{x}{m}\right)$ управо оне које се налазе на левој страни асимптотске формуле (4) коју желимо да докажемо. Наравно, ми за сада *не знамо* колике су оне, али из хеуристичког разматрања у уводу *очекујемо* да је свака сума $S\left(\frac{x}{m}\right)$ приближно једнака $2\frac{x}{m}\log\frac{x}{m}+O(\frac{x}{m})$. Наравно, ово не можемо да искористимо, али нам нико не брани да претпоставимо да је разлика $\widetilde{S}(y):=S(y)-2y\log y-c_1y-c_2$ асимптотски мала[3], кад $y\to\infty$, за неке две константе $c_1,c_2\in\mathbb{R}$ које ћемо касније погодно одабрати. Ово је „најпрљавији" трик у овој верзији доказа Селбергове формуле[4]. За главни члан $2y\log y$ знамо да немамо избора, а и како смо и хеуристички показали да је $S(y)-2y\log y=O(y)$, разумно је да одузимањем c_1y, за неко c_1 (које, дакле, за сада не знамо колико је), пократимо и овај линеарни раст. Одузимање и константе c_2 заиста у овом тренутку не делује мотивисано, али ћемо у доказу схватити и њену улогу.

Идеја је, дакле, да уместо суме $\sum\limits_{m\leqslant x}S\left(\frac{x}{m}\right)$ посматрамо суму

$$T(x):=\sum_{m\leqslant x}\widetilde{S}\left(\frac{x}{m}\right)$$

и покушамо да погодним избором константи c_1 и c_2, које су нам за сада на располагању, докажемо да је цела ова сума по m асимптотски мала. Ако то успемо, примена последице 2.3 нам даје формулу

$$\widetilde{S}(x)=\sum_{n\leqslant x}\mu(n)T\left(\frac{x}{n}\right),$$

из које ћемо закључити да је заиста и $\widetilde{S}(x)$ асимптотски довољно мало, јер су сви сабирци $T\left(\frac{x}{n}\right)$ у суми мали.

Ако се читалац пита – ко би се овог сетио? – одговор је да је вероватно то и био разлог зашто се на елементаран доказ Теореме о простим бројевима чекало скоро 150 година. Наравно, Селберг је имао своју интуицију засновану на тзв. *теорији решета*, али и свом осталом фундаменталном раду у аналитичкој теорији бројева.

4. Сумација интеграцијом и Ојлерова формула

Само за читање овог одељка је потребно познавање Римановог интеграла.

Тврђење 4.1. *Нека је $N\in\mathbb{N}$ и нека је f произвољна реална функција са непрекидним првим изводом на интервалу $[1,N]$. Онда важи формула:*

$$\sum_{n=1}^{N}f(n)=\int_1^N f(t)dt+\int_1^N\{t\}f'(t)dt+f(1), \tag{5}$$

где је $\{t\}=t-[t]$ разломљени део реалног броја t.

Овде последња два члана представљају грешку која је направљена када се сума апроксимира интегралом (и да, наравно да смо $f(1)$ могли да „скратимо", али је овај

[3] Добро је бити оптимиста.

[4] Свака верзија има своје чари...

облик згоднији у применама). За многе функције ова грешка ће бити довољно мала, да је већ ова формула корисна.

Доказ. Уведимо следеће ознаке:

$$I(k) := \int_k^{k+1} (f(k) - f(t))dt = f(k) - \int_k^{k+1} f(t)dt \quad \text{и} \quad S_N := \sum_{k=1}^{N-1} I(k).$$

Интеграл $I(k)$ ћемо трансформисати парцијалном интеграцијом, где ћемо изабрати $u(t) := f(k) - f(t)$ и $v(t) := t - k - 1$:

$$\begin{aligned} I(k) &= \int_k^{k+1} u(t)\, dv(t) = (t-k-1)(f(k)-f(t))\Big|_k^{k+1} - \int_k^{k+1} v(t)\, du(t) \\ &= \int_k^{k+1} (t-k-1)f'(t)dt = \int_k^{k+1} (t-[t]-1)f'(t)dt. \end{aligned}$$

Овде смо у интегранду заменили k са $[t]$, јер t пролази интервалом $[k, k+1]$. Онда добијамо

$$\begin{aligned} &\sum_{k=1}^{N-1} f(k) - \int_1^N f(t)dt = S_N = \sum_{k=1}^{N-1} \int_k^{k+1} (f(k) - f(t))dt \\ &= \sum_{k=1}^{N-1} \int_k^{k+1} (t-[t]-1)f'(t)dt = \sum_{k=1}^{N-1} \int_k^{k+1} \{t\}f'(t)dt - \sum_{k=1}^{N-1} \int_k^{k+1} f'(t)dt \\ &= \int_1^N \{t\}f'(t)dt - \sum_{k=1}^{N-1} (f(k+1) - f(k)) = \int_1^N \{t\}f'(t)dt + f(1) - f(N), \end{aligned}$$

што је управо формула (5).

Доказ је, дакле, сумација $N-1$ појединачних парцијалних интеграција за Риманов интеграл. Они међу читаоцима који знају Стилтјесов интеграл, сигурно су одмах приметили да се формула (5) добија директно, у једном реду, једном применом формуле за *парцијалну интеграцију Стилтјесовог интеграла.* □

ПРИМЕР 4.2. Применимо формулу (5) за функцију $f(t) = (\log t)^2$ и сумацију по целим бројевима у интервалу $[1, x]$, па дакле за N узимамо $[x]$. Налазимо:

$$\begin{aligned} \sum_{m \leqslant x} (\log m)^2 &= \int_1^{[x]} (\log t)^2 dt + \int_1^{[x]} \{t\} \frac{2 \log t}{t} dt \\ &= \int_1^x (\log t)^2 dt + O((\log x)^2) + O\left((\log x) \cdot \int_1^x \frac{1}{t} dt\right) \\ &= x(\log x)^2 - \int_1^x t \frac{2\log t}{t} dt + O((\log x)^2) \\ &= x(\log x)^2 - 2x \log x + 2x + O((\log x)^2), \end{aligned}$$

где смо при преласку из прве у другу линију, у првом интегралу продужили интеграцију $\int_1^{[x]}$ до $\int_1^x$ уз грешку која је највише $O((\log x)^2)$, док смо у дугом интегралу, такође, продужили интеграцију до x и заменили $\{t\}\log t$ са већом вредношћу $\log x$ (фактор 2, као и све остале константе надаље, је „увучен" у O-симбол). Интеграл смо рачунали двоструком применом парцијалне интеграције. □

Пример 4.3. Применимо формулу (5) за функцију $f(t) = 1/t$. Добијамо:

$$\begin{aligned}\sum_{m\leqslant x}\frac{1}{m} &= \int_1^{[x]}\frac{dt}{t} - \int_1^{[x]}\{t\}\frac{dt}{t^2}dt + 1\\ &= \int_1^{x}\frac{dt}{t} + O\left(\frac{1}{x}\right) + 1 - \int_1^{\infty}\{t\}\frac{dt}{t^2}dt + \int_{[x]}^{\infty}\{t\}\frac{dt}{t^2}dt = \log x + \gamma + O\left(\frac{1}{x}\right),\end{aligned}$$

где смо у другом интегралу прошириле интеграцију до ∞, па одузели то што смо додали тј. интеграл $\int_{[x]}^{\infty}$. Константу $1 - \int_1^{\infty}\{t\}\frac{dt}{t^2}dt$ смо означили са γ (то је тзв. *Ојлерова константа*), док је вредност преосталог интеграла $\int_{[x]}^{\infty}\{t\}\frac{dt}{t^2}dt = O\left(\frac{1}{x}\right)$. □

Пример 4.4. На крају, применимо формулу (5) и за функцију $f(t) = \frac{\log t}{t}$. Слично као и у претходна два примера, налазимо да је:

$$\begin{aligned}\sum_{m\leqslant x}\frac{\log m}{m} &= \int_1^{[x]}\frac{\log t}{t}dt + \int_1^{[x]}\{t\}\frac{1-\log t}{t^2}dt\\ &= \int_1^{x}\frac{\log t}{t}dt + O\left(\frac{\log x}{x}\right) + \int_1^{\infty}\{t\}\frac{1-\log t}{t^2}dt - \int_{[x]}^{\infty}\{t\}\frac{1-\log t}{t^2}dt\\ &= \frac{1}{2}(\log x)^2 + \eta + O\left(\frac{\log x}{x}\right),\end{aligned}$$

где смо са η означили вредност интеграла $\int_1^{\infty}\{t\}\frac{1-\log t}{t^2}dt$ и искористили да је

$$\int_{[x]}^{\infty}\{t\}\frac{1-\log t}{t^2}dt = O\left(\int_x^{\infty}\frac{\log t}{t^2}dt\right) = O\left(\int_x^{\infty}(\log t)d\left(-\frac{1}{t}\right)\right) = O\left(\frac{\log x}{x}\right). \quad \square$$

Задатак 4.5. Доказати да је $\sum\limits_{m\leqslant x}\log m = x\log x - x + O(\log x)$.

5. Доказ Селбергове формуле

Сада доказ можемо врло брзо да завршимо, реализујући стратегију описану у одељку 3. Дакле, посматрамо суму

$$\begin{aligned}T(x) &= \sum_{m\leqslant x}\widetilde{S}\left(\frac{x}{m}\right) = \sum_{m\leqslant x}\left[S\left(\frac{x}{m}\right) - 2\frac{x}{m}\log\frac{x}{m} - c_1\frac{x}{m} - c_2\right]\\ &= \sum_{m\leqslant x}S\left(\frac{x}{m}\right) - 2x\log x\sum_{m\leqslant x}\frac{1}{m} + 2x\sum_{m\leqslant x}\frac{\log m}{m} - c_1x\sum_{m\leqslant x}\frac{1}{m} - c_2\sum_{m\leqslant x}1\\ &= \sum_{m\leqslant x}(\log m)^2 - (2x\log x + c_1x)\sum_{m\leqslant x}\frac{1}{m} + 2x\sum_{m\leqslant x}\frac{\log m}{m} - c_2[x],\end{aligned}$$

где смо заменили $\sum_{m\leqslant x} S\left(\frac{x}{m}\right)$ са $\sum_{m\leqslant x} \Lambda_2 * \mathbf{1}(m) = \sum_{m\leqslant x}(\log m)^2$.

Сада у добијеној формули, заменимо одговарајуће суме по m асимптотским формулама добијеним у примерима 4.2, 4.3 и 4.4:

$$\begin{aligned} T(x) &= x(\log x)^2 - 2x\log x + 2x + O((\log x)^2) - (2x\log x + c_1 x)\Big[\log x + \gamma + \\ &\quad + O\Big(\frac{1}{x}\Big)\Big] + 2x\left[\frac{1}{2}(\log x)^2 + \eta + O\Big(\frac{\log x}{x}\Big)\right] - c_2 x + O(1) \\ &= (-2 - c_1 - 2\gamma)x\log x + (2 - \gamma c_1 + 2\eta - c_2)x + O((\log x)^2). \end{aligned}$$

Подсетимо се да су нам константе c_1 и c_2 на располагању. Изабримо их на овом месту тако да одговарајући коефицијенти уз $x\log x$ и x буду 0. Дакле, захтевамо да је $-2 - c_1 - 2\gamma = 0$ и $2 - \gamma c_1 + 2\eta - c_2 = 0$, што је испуњено за $c_1 = -2 - 2\gamma$ и $c_2 = 2 + 2\eta + \gamma(2 + 2\gamma)$. Са овим избором константи, главни члан је нестао[5] и остала је само (одлична) горња оцена: $T(x) = O((\log x)^2)$. На основу ове оцене, користећи неједнакост троугла за апсолутну вредност, одмах добијамо да је и

$$\begin{aligned} |\widetilde{S}(x)| &= \left|\sum_{n\leqslant x} \mu(n) T\left(\frac{x}{n}\right)\right| \leqslant \sum_{n\leqslant x}\left|T\left(\frac{x}{n}\right)\right| = O\Big(\sum_{n\leqslant x}\left(\log\frac{x}{n}\right)^2\Big) \\ &= O\Big((\log x)^2\sum_{n\leqslant x} 1 - 2(\log x)\sum_{n\leqslant x}\log n + \sum_{n\leqslant x}(\log n)^2\Big) \\ &= O\left(x(\log x)^2 + (\log x)^2 - 2x(\log x)^2 + 2x\log x + x(\log x)^2 - 2x\log x + 2x\right) \\ &= O(x), \end{aligned}$$

на основу примера 4.2 и задатка 4.5. Ако се подсетимо дефиниције $\widetilde{S}(x)$, ово значи да је

$$\left|\sum_{n\leqslant x}\Lambda_2(n) - 2x\log x - c_1 x - c_2\right| = O(x),$$

одакле следи да је

$$\sum_{n\leqslant x}\Lambda_2(n) = 2x\log x + O(x),$$

што је и требало доказати. □

Литература

[1] Г. Ђанковић, *Теорија бројева*, Математички факултет, Београд, 2013.

[2] А. Ивић, *Увод у аналитичку теорију бројева*, Издавачка књижарница Зорана Стојановића, Нови Сад, 1996.

[5] сада видимо зашто нам је требала и константа c_2

Статијата прв пат е објавена во списанието ТАНГЕНТА на ДМ на Србија во 2013/14 година