Математичка гимназија

Матурски рад

из математике

Аритметичка статистика

Ученик: Владимир Ђурица, IVd

Ментор: Др Стеван Гајовић

Београд, 2026.

Садржај

1 Увод **2**

2 Основе и дефиниције **3**
2.1 Зета функција 3
2.2 Основе 4

3 Вероватноће са простим бројевима **5**
3.1 Густина простих бројева 5
3.2 Густине простих бројева по модулу 8

4 Делиоци и вероватноће **10**
4.1 Која је вероватноћа да су два насумично изабрана природна броја узајамно проста? 10
4.2 Која је вероватноћа да је насумично изабран природан број бесквадратан? 10
4.3 Уопштење на произвољан број чланова 12
4.4 Која је вероватноћа да је број у $\mathbb{Z}_p$ квадрат? 14
4.5 Која је вероватноћа да се природан број може представити као збир k квадрата? 16

5 Вероватноће и полиноми **18**
5.1 Која је вероватноћа да насумично изабран полином другог степена има решење у пољу $\mathbb{F}_p$? 18
5.2 Која је вероватноћа да полином има нулу у $\mathbb{F}_p$? 20
5.3 Која је вероватноћа да је бинарна квадратна форма растављива? 22

6 Закључак **26**

1 Увод

Аритметичка статистика је област математике која се бави проучавањем вероватноћа разних аритметичких својстава у теорији бројева. Пример би били прости бројеви, квадрати, делиоци и многи други. С обзиром на то да веома често радимо са бесконачним скуповима вероватноћу није увек лако израчунати. У овом раду ћемо се бавити неким занимљивим проблемима аритметичке статистике попут:
1) Која је вероватноћа да су два (и више) насумично изабрана природна броја узајамно прости? Која је вероватноћа да једначина: $ax + by = c$ има решење у целим бројевима? Која је вероватноћа да је природан број бесквадратан и $\mathbb{N}$ у $\mathbb{Z}_p$? Која је вероватноћа да број може да се представи као збир квадрата?
2) Која је вероватноћа да је неки полином растављив и да има нулу у $\mathbb{F}_p$?
3) Која је густина простих бројева? Која је вероватноћа да прост број даје остатак r по модулу m?

Неке ознаке које се појављују у раду:

(a, b) - највећи заједнички делилац за a и b.
$\mathbb{P}$ - скуп простих бројева
$\mathbb{F}_p$ - $\{0,\ 1, \ldots,\ p-1\}$
$\mathbb{Z}_p$ - p-адски цели
$\#\{A\}$ - број елемената скупа A
$Re(z)$, $Im(z)$ - реалан и имагинаран део комплексног броја
$A(n) \sim B(n)$ - $\lim_{n\to\infty} \frac{A(n)}{B(n)} = 1$
$A(n) = O(B(n))$ - $\exists\ (n_0, c) \in \mathbb{N} \times \{\mathbb{R} \setminus \{0\}\}\ \ \forall n \geq n_0\ A(n) \leq cB(n)$
$A(n) \lesssim B(n)$ - $\exists c \in \mathbb{R} \setminus \{0\}\ A(n) \leq cB(n)$
$P(A)$ - вероватноћа да се деси догађај A
$v_p(n)$ - највећи степен p који дели n
$\mathbb{Z}/n\mathbb{Z}$ - скуп остатака по модулу n
$\lfloor x \rfloor$ - цео део од x

2 Основе и дефиниције

2.1 Зета функција

[5] У комплексној анализи, један од најпознатијих отворених проблема јесте Риманова хипотеза. Она подразумева налажење свих комплексних нула зета функције. За сврху рада ће нам бити потребно само да дефинишемо и покажемо лему која повезује комплексну анализу и просте бројеве.

Дефиниција 1. *Функцију* $\zeta : \mathbb{C} \to \mathbb{C}$ *дефинишемо на следећи начин за* $Re(s) > 1$*:*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Лема 1.

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}$$

Доказ. По основном ставу теорије бројева знамо да се сваки природан број, осим 1, може на јединствен начин приказати као производ простих бројева (Канонска факторизација). Посматрајмо следећи производ:

$$\left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \dots\right) \dots \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) \dots$$

Из сваке заграде узимамо тачно један сабирак $\frac{1}{p^{\alpha s}}$, при чему ће се сваки природан број $n = p_1^{\alpha_1} p_2^{\alpha 2} \dots p_k^{\alpha_k}$ појавити тачно једном. Самим тим, можемо тврдити да је

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(\sum_{n=0}^{\infty} \frac{1}{p^{ns}} \right)$$

Приметимо геометријске редове, који због услова $Re(s) > 1$ конвергирају:

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

Овим је доказ леме завршен.
*Напомена: Степеновање на комплексан степен се дефинише за $a > 0$ на следећи начин:

$$a^z = a^{Re(z)} e^{Im(z) i \ln a} = a^{Re(z)} cis(Im(z) \ln a).$$

2.2 Основе

У овом раду ћемо се бавити вероватноћама на бесконачним скуповима. Вероватноћу дефинишемо као лимес:

Дефиниција 2. *За* $\mathbb{S} \subset \mathbb{N}$*:*

$$P(x \in \mathbb{S}) = \lim_{n\to\infty} \frac{\#\{\ m \in \mathbb{S};\ m \leq n\ \}}{n}.$$

Дефиниција 3. *За* $\mathbb{S} \subset \mathbb{Z}$*:*

$$P(x \in \mathbb{S}) = \lim_{n\to\infty} \frac{\#\{\ m \in \mathbb{S};\ m \leq n\ \}}{2n+1}.$$

Пример 1. *Која је вероватноћа да је природан/цео број паран?*

Решење. Приметимо да ако је позитиван цео број паран, онда је и његова негација такође парна, при чему је вероватноћа да је цео број једнак нули 0. Тиме добијамо да су та два проблема еквивалентна. За природан број n у скупу $\{1, 2, ..., n\}$ има тачно $\lfloor \frac{n}{2} \rfloor$ парних природних бројева. Тј:

$$\#\{m|m \in \mathbb{N};\ \ 2|m;\ \ m \leq n\ \} = \lfloor \frac{n}{2} \rfloor$$

$$\lim_{n\to\infty} \frac{\#\{2|m;\ \ m \leq n\}}{n} = \lim_{n\to\infty} \frac{\lfloor \frac{n}{2} \rfloor}{n} = \frac{1}{2}.$$

.

Пример 2. *Вероватноћа да је природан/цео број дељив са* $z \in \mathbb{Z} \setminus \{0\}$ *је* $\frac{1}{|z|}$.

Пример 3. *Вероватноћа да природан број даје остатак* a *по модулу* n *је* $\frac{1}{|n|}$.

Пример 4. ***део решења ELMO 2021*** *Скуп природних бројева је партиционисан на* n *дисјунктних аритметичких прогресија* $S_1, S_2, \ldots, S_n$*, чије су разлике редом* $d_1, d_2, \ldots, d_n$*. Доказати да је:* $\sum_{k=1}^{n} \frac{1}{d_k} = 1$.

Решење. Приметимо да приликом одабира произвољног природног броја, вероватноћа да се он налази у S_i једнака $\frac{1}{d_i}$. С обзиром на то да $S_1, S_2, \ldots, S_n$ партиционишу $\mathbb{N}$ важиће:

$$1 = P(x \in \mathbb{N}|x \in \mathbb{N}) = \sum_{k=1}^{n} P(x \in S_k) = \sum_{k=1}^{n} \frac{1}{d_k}$$

што је и требало показати.

3 Вероватноће са простим бројевима

3.1 Густина простих бројева

[1] Постоји пуно доказа егзистенције бесконачно много простих бројева. Најпознатији је Еуклидов доказ који посматра производ првих n простих бројева и додаје на њих 1, чиме се гарантује да тај израз није дељив ниједним мањим простим бројем.

Дефиниција 4. *Функција $\pi : \mathbb{N} \to \mathbb{N}$ за дати природан број даје број простих природних бројева који нису већи од n.*

Теорема о простим бројевима нам каже да се $\pi(n)$ асимптотски понаша као $\frac{n}{\ln n}$. Доказ исте користи комплексну анализу, што је напредније од средњошколског градива, па ћемо доказати мало слабије тврђење. Докажимо прво $\pi(n) \geq C \cdot \frac{n}{\ln n}$ за неко реално C. За сврху доказа ћемо дефинисати Чебишевљеву пси функцију.

Дефиниција 5.

$$\psi : \mathbb{N} \to \mathbb{R}; \quad \psi(n) = \sum_{p \in \mathbb{P} \quad p^\alpha \leq n} \ln p$$

Она се такође може и посматрати као ln од најмањег заједничког садржаоца првих n природних бројева, јер је број степена простих који су $\leq n$ баш $\log_p n$.

Лема 2.

$$\psi(n) \geq (n-2)\ln 2$$

Доказ. Јасно је да за свако $x \in \mathbb{R}$ важи $x(1-x) \leq \frac{1}{4}$. Такође, важи $\forall (x,n) \in (0,1) \times \mathbb{N} \;\; x^n(1-x)^n \leq \frac{1}{4^n}$ односно:

$$\int_0^1 x^n(1-x)^n dx \leq \frac{1}{4^n}.$$

Сада посматрајмо израз $e^{\psi(2n+1)}(\int_0^1 x^n(1-x)^n dx)$. Јасно је да је позитиван. Такође знамо да је у питању цео број с обзиром на то да је вредност одређеног интеграла кад се сведе на заједнички делилац заправо рационалан број који у имениоцу има вредност која дели НЗС првих $2n+1$ бројева што је баш једнако овом $e^{\psi(2n+1)}$. Дакле можемо тврдити да је:

$$e^{\psi(2n+1)} \int_0^1 x^n(1-x)^n dx \geq 1 \Leftrightarrow \frac{e^{\psi(2n+1)}}{4^n} \geq 1 \Leftrightarrow \psi(2n+1) \geq 2n \ln 2.$$

Како је пси функција неопадујаћа знамо да је

$$\psi(2n) \geq \psi(2n-1) \geq 2(n-1)\ln 2.$$

Овим је доказ леме завршен. Сада треба да пси функцију повежемо са пи функцијом. Запишимо је на следећи начин:

$$\psi(n) = \ln\left(\prod_{k=1}^{\pi(n)} p_i^{\alpha_i}\right)$$

Овде је $p_i^{\alpha_i}$ i-ти прост број са највећим експонентом тако да је $p_i^{\alpha_i} \leq n$. И када ову неједнакост убацимо у производ добићемо:

$$\psi(n) = \ln\left(\prod_{k=1}^{\pi(n)} p_i^{\alpha_i}\right) \leq \ln\left(\prod_{k=1}^{\pi(n)} n\right) = \ln(n^{\pi(n))}) = \pi(n)\ln(n)$$

$$\Rightarrow \pi(n) \geq \frac{\psi(n)}{\ln(n)} \geq \frac{(n-2)\ln 2}{\ln(n)} \sim \frac{n\ln 2}{\ln n}$$

Заиста, ово је добра процена с обзиром на то да је $\ln 2 \approx 0.7$ па нам је грешка 30% за довољно велико n. Сада ћемо ограничити $\pi(n)$ са друге стране. Наиме, показаћемо да је $\pi(n) \leq C \cdot \frac{n}{\ln n}$ за неку константу $C \in \mathbb{R}$. Посматрајмо биномни коефицијент $\binom{2n}{n}$ и очигледну чињеницу:

$$\prod_{p\in\mathbb{P};n<p<2n} p | \binom{2n}{n}$$

Приметимо да је производ на левој страни дељивости $\geq n^{\pi(2n)-\pi(n)}$, јер је сваки број у том интервалу бар n. Са друге стране коришћењем Стирлингове апроксимације за факторијел $n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$, па је $\binom{2n}{n} \lesssim 4^n$. Другим речима, добили смо:

$$n^{\pi(2n)-\pi(n)} \lesssim 4^n \Leftrightarrow \pi(2n) - \pi(n) \lesssim \frac{2n\ln 2}{\ln n}$$

Знамо да је $\pi(n)$ неопадајућа функција, па је $\pi(n) \leq \pi(2^{\lceil \log_2(n)\rceil})$. Можемо само да докажемо ограничење за степен двојке $n = 2^a;\ \ a \in \mathbb{N}$.

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

$$\sum_{k=2}^{a} \pi(2^k) - \pi(2^{k-1}) \lesssim \sum_{k=2}^{a} \frac{2^k \ln 2}{\ln(2^{k-1})} = \sum_{k=1}^{a-1} \frac{2^{k+1}\ln 2}{k\ln 2} = 2\sum_{k=1}^{a-1} \frac{2^k}{k}$$

Лема 3.

$$\sum_{k=1}^{a} \frac{2^k}{k} \sim \frac{2^{n+1}}{n}$$

Доказ. Применимо Штолцову теорему на следећи лимес:

$$\lim_{n\to\infty} \frac{\sum_{k=1}^{a} \frac{2^k}{k}}{\frac{2^n}{n}} = \lim_{n\to\infty} \frac{a_n}{b_n}$$

Јасно је да је низ $b_n = \frac{2^n}{n}$ монотоно растући и тежи бесконачно за $n \to \infty$. Заиста, пошто је $\frac{d}{dx}\frac{2^x}{x} = \frac{2^x(x\ln 2-1)}{x^2}$, што је очигледно позитивно добијамо монотоност, која је критеријум примене Штолцове теореме.

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{a_{n+1}-a_n}{b_{n+1}-b_n} = \lim_{n\to\infty} \frac{\frac{2^{n+1}}{n+1}}{\frac{2^{n+1}}{n+1}-\frac{2^n}{n}} = \lim_{n\to\infty} \frac{\frac{2^{n+1}}{n+1}}{\frac{2^n(2n-(n+1))}{n(n+1)}} =$$

$$\lim_{n\to\infty} \frac{2n}{n-1} = 2$$

Овим смо комплетирали доказ леме.
Сада када применимо лему на $\pi(n) \leq \pi(2^{\lceil \log_2(n)\rceil})$ и $\pi(2^a) \lesssim 2\sum_{k=1}^{a-1} \frac{2^k}{k}$ добијамо:

$$\pi(n) \lesssim \frac{2^{\lceil \log_2 n\rceil+2}}{\lceil \log_2 n\rceil} \sim \frac{4n\ln 2}{\ln n}$$

Дакле, елементарно смо добили:

$$\frac{n\ln 2}{\ln n} \lesssim \pi(n) \lesssim \frac{4n\ln 2}{\ln n}$$

Ово нам јасно показује да је вероватноћа да је насумично одабран природан број прост једнака нули. Међутим, можемо добити и мало бољу оцену. Наиме, добили смо да је број простих бројева заправо $O(\frac{n}{\ln n})$, са пристојном константом, што је веома корисно у теорији бројева.

3.2 Густине простих бројева по модулу

[3] У претходном делу смо показали да има бесконачно много простих бројева, али и много боље да је њихова густина $O(\frac{N}{\ln N})$ када $N \to \infty$. Са друге стране, једна од најпознатијих теорема у теорији бројева јесте Дирихлеова:

Теорема 1. *У свакој аритметичкој прогресији, у којој постоје два узајамно проста члана, постоји бесконачно много простих.*

Другим речима, Дирихлеова теорема каже да за сваки остатак по модулу m који је узајамно прост са m постоји бесконачно много простих бројева. Њен доказ се заснива на доказивању да густина простих бројева $\equiv a \ (mod\ m)$ асимптотски тежи $\frac{n}{\ln n \cdot \varphi(m)}$, где је φ Ојлерова функција која броји узајамно просте бројеве са n који нису већи од n. Приметимо да ова густина не зависи од a (осим што је потребно $(a, m) = 1$).
У претходном делу смо разматрали густину простих бројева и закључили да је она $\frac{n}{\ln n}$. Као последицу ове две густине добијамо да се сви остаци по модулу m, који су узајамно прости са m, појављују са једнаким вероватноћама. Доказ је компликован и користи напредну теорију Дирихлеових карактера и L-функције. За илустрацију ћемо само урадити прост случај $m = 4$. Прво ћемо показати да постоји бесконачно много простих бројева $\equiv 3 \ (mod\ 4)$. Мотивација нам је Еуклидов доказ бесконачности скупа простих бројева. Претпоставимо да их је коначно много и нека су они редом једнаки $p_1, p_2, \dots p_k$. Посматрајмо израз:

$$P = 4(\prod_{n=1}^{k} p_n) - 1 = 4p_1p_2 \dots p_k - 1 \equiv -1 \ (mod\ 4)$$

Лако је приметити да је $(P, p_i) = 1$ за свако i, што значи да је или P прост који даје остатак 3 при дељењу са 4 или има делилац који је $\equiv -1 \ (mod\ 4)$ који није једнак ниједном од p-ова. Ово нам директно даје контрадикцију и крај доказа.
На сличан начин ћемо доказати да постоји бесконачно много простих који дају остатак 1 при дељењу са 4, само што ћемо овај пут посматрати израз:

$$P = 4(\prod_{n=1}^{k} p_i)^2 + 1 = (2p_1 ... p_k)^2 + 1 \equiv 1 \ (mod\ 4)$$

На идентичан начин закључујемо да је $(P, p_i) = 1$ за свако i. Једина разлика је што овде користимо познато тврђење да $n^2 + 1$ нема непарних делилаца $\equiv -1 \ (mod\ 4)$ (биће доказано у каснијим главама). Заиста закључујемо да су делиоци броја P сви $\equiv 1 \ (mod\ 4)$ и различити од p-ова.

4 Делиоци и вероватноће

У овом поглављу ћемо се бавити вероватноћама везаним за Канонску факторизацију природног броја. Осврнућемо се и на решивост линеарних Диофантових једначина. Дискутоваћемо мало и о томе кад је број квадрат у $\mathbb{Z}_p$. На крају ћемо гледати када се природан број може записати као сума квадрата.

4.1 Која је вероватноћа да су два насумично изабрана природна броја узајамно проста?

[4]

Главна идеја ће нам бити да ако су два броја узајамно проста, онда за сваки прост број p важи да неће делити бар један од та два броја. Посматрајмо неки прост број p и нека су a и b два узајамно проста природна броја. Сада знамо да p не дели (a, b). Вероватноћу да бар један број није дељив са p ћемо рачунати тако што од укупне вероватноће одузимамо вероватноћу да су оба дељива са p. Односно:

$$P(p \nmid a \vee p \nmid b) = 1 - P(p \mid a)P(p \mid b) = 1 - \frac{1}{p^2}$$

Дакле, наша коначна вероватноћа ће бити:

$$P((a, b) = 1) = \prod_{p \in \mathbb{P}} (1 - \frac{1}{p^2}) = P((a, b) = 1) = \frac{1}{\zeta(2)}$$

Фокус овог рада није Баселов проблем (рачунање $\zeta(2)$), те ћу се само позвати на познат резултат $\zeta(2) = \frac{\pi^2}{6}$. Доказ би био посматрање Вијетових формула на Тејлоров развој функције $\sin(x)$. Решење нашег задатка ће бити $P((a, b) = 1) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.61 = 61\%$.

4.2 Која је вероватноћа да је насумично изабран природан број бесквадратан?

Ради једноставности записа нека је $\mathbb{S} = \{n \in \mathbb{N} | \forall p \in \mathbb{P}; p \mid n \Rightarrow v_p(n) = 1\}$ скуп свих бесквадратних природних бројева. Нас интересује $P(x \in \mathbb{S})$. За сваки елемент скупа $\mathbb{S}$ важи $p^2 \nmid n$. Када посматрамо $\mathbb{Z}/p^2\mathbb{Z}$ знамо да постоји јединствен остатак који задовољава $p^2 \mid n$ (то је 0), па је

вероватноћа $P(p^2 \nmid n) = 1 - \frac{1}{p^2}$.
Коначно решење ће бити:

$$P(n \in \mathbb{S}) = \prod_{p \text{ prost}} (1 - \frac{1}{p^2}) = \frac{6}{\pi^2}$$

Можемо приметити да је решење исто као и код узајмно простих бројева. Испоставља се да није случајност у питању! Како бисмо интуитивно објаснили зашто су те две вероватноће једнаке, пробаћемо да нађемо неки вид бијекције између ова два проблема. Међутим, налажење бијекције није довољан услов; на пример вероватноћа да је природан број паран је $\frac{1}{2}$, а вероватноћа да је природан број дељив са 4 је $\frac{1}{4}$, иако између та два скупа постоји бијекција $f(n) = 2n$.
За сврху тога, дефинишимо функцију $rad : \mathbb{N} \to \mathbb{N}$ која нам враћа производ свих простих делилаца (без вишеструкости). Приметимо тривијално својство функције:

$$(a, b) = 1 \Leftrightarrow (rad(a), rad(b)) = 1$$

То значи да је:

$$P((a, b) = 1) = P((rad(a), rad(b)) = 1)$$

Међутим, услов да је $(rad(a), rad(b)) = 1$ је еквивалентан са тиме да производ $rad(a)rad(b) \in \mathbb{S}$. Нека је $rad(a) = \prod_{k=1}^{n} p_k$ и $rad(a) = \prod_{k=1}^{m} q_k$. $rad(a)rad(b)$ ће бити производ $m + n$ различитих простих бројева само ако је $(rad(a), rad(b)) = 1$ (биће бесквадратан). У супротном ће се неки прости делиоци поновити, што имплицира да је $(rad(a), rad(b)) \neq 1$. Иако ово није формалан доказ, даје нам добру интуицију зашто одговор има смисла. Кључни разлог зашто се вероватноће поклапају јесте то што се у оба бесконачна производа појављују исти фактори $1 - \frac{1}{p^2}$.

4.3 Уопштење на произвољан број чланова

Сада ћемо се бавити случајем када је $(a, b) = c$, где је c фиксиран природан број. За сврху решења ћемо користити тривијално својство највећег заједничког делиоца $(ax, bx) = x(a, b)$ за свако $(a, b, x) \in \mathbb{N}^3$. Заиста, ако је $(a, b) = c$ за $(a, b, c) \in \mathbb{N}^3$, тада $\exists (x, y) \in \mathbb{N}^2; (x, y) = 1$, при чему је $a = cx$ $b = cy$.

Овако добијамо (пошто су догађаји независни):

$$P((a, b) = c) = P(c \mid a)P(c \mid b)P((x, y) = 1) = \frac{1}{c} \cdot \frac{1}{c} \cdot \frac{6}{\pi^2}$$

Генерално је добра пракса проверити смисленост решења. Заиста кад просумирамо по свим c-овима добијамо 1:

$$\sum_{c=1}^{\infty} P((a, b) = c) = \sum_{c=1}^{\infty} \frac{6}{\pi^2 c^2} = \frac{6}{\pi^2} \sum_{c=1}^{\infty} \frac{1}{c^2} = 1$$

Овај приступ нам је такође одговор и на питање: „Која је вероватноћа да једначина $ax+by = c$ има целобројна решења?". Заиста, из Еуклидовог алгоритма знамо да та једначина има целобројна решења ако и само ако $(a, b) \mid c$. Идеја је да фиксирамо (a, b) и да потом наметнемо услов $(a, b) \mid c$. Означимо са P ту вероватноћу. Тражена вероватноћа ће бити:

$$P = \sum_{k=1}^{\infty} P((a, b) = k)P(k \mid c) = \sum_{k=1}^{\infty} \frac{6}{\pi^2 k^3} = \frac{6}{\pi^2}\zeta(3) \approx 0.73 = 73\%$$

За почетак, позабавићемо се вероватноћом да приликом насумичног одабира $n \in \mathbb{N}$ природних бројева, одаберемо узајамно просте, тј. $(a_1, a_2, \ldots, a_n) = 1$. Идеја ће бити слична као и за случај $n = 2$. Од укупне вероватноће одузимамо случај кад су сви дељиви са простим бројем p:

$$P((a_1, a_2, \ldots, a_n) = 1) = \prod_{p \in \mathbb{P}} (1 - \prod_{i=1}^{n} P(p \mid a_i)) = \prod_{p \in \mathbb{P}} (1 - \frac{1}{p^n}) = \frac{1}{\zeta(n)}$$

Показаћемо да како n тежи бесконачности наша вероватноћа тежи ка 1. Другим речима да:

$$\lim_{n \to \infty} \zeta(n) = 1$$

Користићемо познату идеју Риманових сума, тј. да је површина испод графика функције $f(x) = \frac{1}{x^n}$ већа од $\zeta(n)$, за $n \in \mathbb{N}; n > 1$:

$$\lim_{n \to \infty} \zeta(n) = 1 + \lim_{n \to \infty} \sum_{k=2}^{\infty} \frac{1}{k^n} \leq \lim_{n \to \infty} (1 + \int_1^{\infty} \frac{1}{x^n} dx) = \lim_{n \to \infty} (1 + \frac{1}{n+1}) = 1$$

Са друге стране јасно је да је $1 \leq \zeta(n)$ за све $n \in \mathbb{N}$. Сада по теореми о два полицајца знамо да низ $\zeta(n)$ конвергира ка 1.

Вероватноћа да је $(a_1, a_2, \ldots, a_n) = k$ за неко $k \in \mathbb{N}$ се рачуна:

$$P((a_1, a_2, \ldots, a_n) = k) = P((x_1, x_2, \ldots, x_n) = 1)P(k \mid a_1)P(k \mid a_2) \ldots P(k \mid a_n) =$$

$$= \frac{1}{\zeta(n)k^n}$$

Посматрајмо сада једначину $a_1x_1+a_2x_2+\ldots+a_nx_n = m$. Она има решења само када $(a_1, a_2, \ldots, a_n) \mid m$. Вероватноћа да се то деси је:

$$P(a_1x_1+a_2x_2+\ldots+a_nx_n = m) = \sum_{k=1}^{\infty} P((a_1, a_2, \ldots, a_n) = k)P(k \mid m) = \frac{\zeta(n+1)}{\zeta(n)}$$

Занимљиво је да већ за $n = 6$ вероватноћа већа од 99%.

4.4 Која је вероватноћа да је број у $\mathbb{Z}_p$ квадрат?

[2] [6] За почетак приметимо да је вероватноћа да је цео број потпун квадрат једнака нули. Доказаћемо дефиницијом:

$$P(\exists m \in \mathbb{Z};\ \ n = m^2) = \lim_{a\to\infty} \frac{\#(\ k \in \mathbb{S};\ k \leq a\ )}{2a} = \lim_{a\to\infty} \frac{\lceil\sqrt{a}\rceil}{2a} \sim \frac{1}{2\sqrt{a}} \to 0$$

Занимљивији проблем би свакако био да проблем посматрамо у пољу p-адских бројева.

Лема 4. *За непаран прост p, a је потпун квадрат у $\mathbb{Z}_p$ ако и само ако је облика $a = up^k$ $((u,p) = 1)$ где је u је квадратни остатак и k је паран.*

Доказ. Доказ ћемо изоставити пошто није главна тема овог рада.

Дефиниција 6. *Лежандров симбол за $a \in \mathbb{F}_p$ се дефинише на следећи начин:*

$$(\frac{a}{p}) = \begin{cases} -1, & a \not\equiv m^2 \quad \forall m \in \mathbb{F}_{\text{ı}} \\ 0, & a = 0 \\ 1, & a \equiv m^2 \quad \exists m \in \mathbb{F}_p \end{cases}$$

У овом раду ћемо, конвенције ради, претпостављати да је 0 такође квадратни остатак по модулу p. За почетак, лако је приметити да је вероватноћа да је $v_p(a) \equiv 0 \pmod 2$ за неки цео број a на основу принципа укључења-искључења једнака:

$$\sum_{k=0}^{\infty} \frac{(-1)^k}{p^k} = \frac{1}{1+\frac{1}{p}} = \frac{p}{p+1}$$

Остаје нам само да израчунамо вероватноћу да је $(\frac{u}{p}) = 1$.

Лема 5. *За сваки непаран прост број p постоји тачно $\frac{p-1}{2}$ ненултих квадратних остатака и тачно $\frac{p-1}{2}$ ненултих квадратних неостатака.*

Доказ. За сврху доказа, користићемо да чињеницу да постоји примитивни корен по простом модулу. Нека је $g \in \mathbb{F}_p$ примитивни корен по модулу p. Сада знамо да ће скуп $\mathbb{K} = \{g^0, g^1, \ldots, g^{p-2}\}$ чинити потпун систем остатака, јер би у супротном постојали a и b такви да је: $0 \leq a < b \leq p-2$ и $g^a \equiv_p g^b$. То је еквивалентно са $g^{a-b} \equiv_p 1$, што по дефиницији примитивног корена значи да $p-1 \mid a-b$ што значи да је $a = b$ што је контрадикција. Приметимо да у скупу $\mathbb{K}$ тачно $\frac{p-1}{2}$ ће имати паран експонент уз g.

За g^{2k} знамо постоји елемент из $x \in \mathbb{F}_p$, ткд. $x^2 \equiv_p g^{2k}$ ($x \equiv_p \pm g^k$). За g^{2k+1} знамо да једначина $x^2 \equiv_p g^{2k+1}$ нема решења, јер ако је $x \equiv_p g^t$ онда је $x^2 \equiv_p g^{2t}$, односно $p-1 \mid 2t-2k-1$, али ово не може због парности.

Сада на основу леме знамо да је $P((\frac{u}{p}) = 1) = \frac{1}{2}$. Пошто су та два догађаја независна, коначан одговор ће бити $\frac{p}{2(p+1)}$.

4.5 Koja je vероватноћа да се природан број може представити као збир k квадрата?

За сада смо у раду показали да је вероватноћа да је природан потпун квадрат једнака 0. За почетак докажимо да се сваки природан број може представити као збир 4 квадрата (самим тим и више).

Теорема 2. *Сваки природан број се може представити као збир 4 квадрата.*

Доказ. Сматраћемо да је познато тврђење да се сваки прост број може приказати као збир 4 квадрата. Доказивање тог тврђења се заснива на чињеници да конгруенција има решење за сваки прост број $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ (због Дирихлеовог принципа) и на Фермаовом принципу бесконачног спуста. Докажимо да је тврђење мултипликативно, односно да ако се a и b могу приказати као збир 4 квадрата, онда се и ab може приказати. Заиста, уочимо Лагранжов идентитет:

$$(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)^2 +$$

$$+(a_1b_2+a_1b_2+c_1d_2-c_2d_1)^2+(a_1c_2+a_2c_1+b_2d_1-b_1d_2)^2+(a_1d_2+a_2d_1+b_1c_2-c_1b_2)^2$$

Овај идентитет се лако може проверити множењем чинилаца у заградама. Сада је јасно да се сваки природан број може приказати као збир 4 квадрата, индукцијом по простим делиоцима природног броја (ако може n онда може и np где је p прост).
Другим речима доказали смо да је вероватноћа да се природан број може приказати као збир $k \geq 4$ квадрата једнака 1. Остају нам само случајеви $k = 2, 3$. За случај $k = 2$ ће стратегија бити слична.

Теорема 3. *Природан број се може приказати као збир 2 квадрата ако и само ако је вишеструкост сваког његовог простог делиоца који је* $\equiv 3 \pmod{4}$ *парна.*

Доказ. Докажимо прво да конгруенција $x^2 \equiv -1 \pmod{p}$ нема решења за просте $p \equiv -1 \pmod{4}$. Заиста, ако би такво решење постојало претпоставимо да је оно $\equiv g^\alpha \pmod{p}$, где је g примитивни корен по модулу p и нека је без умањења општости α паран број који није већи од $\frac{p-1}{2}$. Јасно је да је:

$$g^{2\alpha} \equiv 1(mod\ p) \Rightarrow p - 1 \mid 2\alpha \Rightarrow p - 1 = 2\alpha$$

Међутим, ово имплицира да је $p \equiv 1 \pmod{4}$. Са друге стране, из Гаусових целих је познато да се сваки прост број $\equiv 1 \pmod{4}$ може представити као збир два квадрата. На основу идентитета $(a - b)^2 + (a + b)^2 = 2(a^2 + b^2)$ можемо закључити да $v_2(n)$ не утиче на резултат, па можемо претпоставити да баратамо само са непарним бројевима.

Слично као и код $k = 4$ доказаћемо да је тврђење мултипликативно. За то нам је довољан Брамагуптин идентитет:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ac + bd)^2$$

који се лако може проверити простим множењем. Тиме смо завршили доказ.
Сада нам треба да докажемо да је вероватноћа 0. Вероватноћу да се природан број може представити као збир два квадрата ћемо рачунати тако што фиксирамо прост број $p \equiv -1 \ (mod\ 4)$. На основу претходног дела и на основу неједнакости $\ln(1 - x) \leq -x$ добити:

$$P = \prod_{p \in \mathbb{P};\ p \equiv -1 (mod 4)} (1 - \frac{1}{p+1})$$

$$\Rightarrow \ln(P) \leq \sum_{p \in \mathbb{P};\ p \equiv -1 (mod 4)} -\frac{1}{p+1}$$

За десну страну је познато да дивергира ка $-\infty$, самим тим $P \to 0$ (у глави 3.2 смо показали да има бесконачно много простих бројева $\equiv -1 \ (mod\ 4)$ и да се појављују са вероватноћом $\frac{1}{2}$). Раманујан је доказао да ова вероватноћа асимтотски тежи $O(\frac{1}{\sqrt{\ln(n)}})$.
Остаје нам само случај $k = 3$.

Теорема 4. *Природан број n се може не може приказати као збир 3 квадрата ако и само ако је $n = 4^a(8b + 7); \quad (a, b) \in \mathbb{N}_0^2$.*

Означимо са p вероватноћу вероватноћу да не може да се представи као збир три квадрата. Међу осам остатака по модулу 8 само 2 ће бити дељиви са 4, на њих радимо рекурзију, тј. када их поделимо са 4 добијемо исти проблем, а од других 6 остатака нас интересује само $\equiv 7 (mod\ 8)$:

$$p = \frac{p}{4} + \frac{3}{4} \cdot \frac{1}{6}$$

$$\Rightarrow p = \frac{1}{6}$$

Дакле, коначно решење је $\frac{5}{6}$.

5 Вероватноће и полиноми

У овом поглављу ћемо се бавити вероватноћама везане за решивост једначина у неким скуповима као што су $\mathbb{F}_p$, $\mathbb{Z}_p$, $\mathbb{Z}\ldots$ Конкретно, бавићемо се полиномима и њиховим коренима.

5.1 Која је вероватноћа да насумично изабран полином другог степена има решење у пољу $\mathbb{F}_p$?

Можемо без умањења општости претпоставити да су коефицијенти нашег полинома из $\mathbb{F}_p$.
Ако је водећи коефицијент $0(modp)$ онда наша једначина постаје линеарна. Линеарна конгруенција облика $ax+b \equiv_p 0$ има решење у свим случајевима осим када $p \mid a$ и $p \nmid b$. Дакле вероватноћа у том случају ће бити:

$$P(\exists x \in \mathbb{F}_p; p \mid ax^2+bx+c; p \mid a) = P(p \mid a)(1 - P(p \mid c)P(p \nmid b)) =$$

$$= \frac{1}{p}(1 - \frac{p-1}{p^2}) = \frac{p^2-p+1}{p^3}$$

У случају $p \nmid a$ можемо без умањења општости претпоставити да је наш полином моничан, јер кад помножимо ax^2+bx+c са модуларним инверзом a^{-1} (који постоји за $a \neq 0$) добијамо моничан полином по x.
Прво посматрамо случај $p = 2$. Дељивост $2 \mid x^2+bx+c$ је еквивалентна са $2 \mid (b-1)x+c$, јер $2 \mid x^2+x$ за све целе x (x и $x+1$ су различите парности). Наша једанчина нема решење само ако су b и c непарни. Вероватноћа да се то деси је $\frac{1}{4}$. Дакле, случај $p = 2$ има решење:

$$P(\exists x \in \mathbb{F}_2; 2 \mid ax^2+bx+c) = P(\exists x \in \mathbb{F}_2; 2 \mid ax^2+bx+c; 2 \mid a)$$

$$+P(\exists x \in \mathbb{F}_2; 2 \mid ax^2+bx+c; 2 \nmid a) = \frac{2^2-2+1}{2^3} + \frac{3}{8} = \frac{3}{4}$$

Надаље претпоставимо да је $p > 2$. Сада ћемо наћи све α и β за које конгруенција $x^2 + \alpha x + \beta \equiv_p 0$ има решење у $\mathbb{F}_p$.

$$p \mid x^2+\alpha x+\beta \Leftrightarrow p \mid 4x^2+4\alpha x+4\beta \Leftrightarrow p \mid (2x+\alpha)^2+4\beta-\alpha^2 \Leftrightarrow \left(\frac{4\beta-\alpha^2}{p}\right) = 1$$

Вероватноћа да је $4\beta-\alpha^2$ квадратни остатак је $\frac{p+1}{2p}$, јер је 4β сурјективно на $\mathbb{F}_p$, тј. за фиксирано α израз $4\beta - \alpha^2$ пролази кроз све остатке по модулу p. Дакле, проћи ће кроз све квадратне остатке који нису 0 и кроз 0 (која је исто квадратни остатак), па је то укупно $\frac{p+1}{2}$ остатака.
Сада можемо коначно одговорити на питање која је вероватноћа да произвољан квадратни полином са коефицијентима из $\mathbb{F}_p$ има нулу у $\mathbb{F}_p$:

$$P(\exists x \in \mathbb{F}_p; p \mid ax^2 + bx + c) = P(\exists x \in \mathbb{F}_p; p \mid ax^2 + bx + c; p \mid a)+$$

$$P(\exists x \in \mathbb{F}_p; p \mid x^2+\alpha x+\beta)P(p \nmid a) = \frac{p^2-p+1}{p^3}+\frac{p+1}{2p}\cdot\frac{p-1}{p} = \frac{p^3+2p^2-3p+2}{2p^3}$$

Заиста, када у ову формулу убацимо $p = 2$ добијемо исто решење $\frac{3}{4}$, што значи да је формула тачна за све просте.

5.2 Која је вероватноћа да полином има нулу у $\mathbb{F}_p$?

У претходном делу смо се бавили конкретно квадратним полиномом. Међутим, како бисмо генерализовали морамо паметније приступити. Као што смо и у прошлом делу можемо без умањења општости да претпоставимо да радимо са моничним полиномима степена n. Нека је x_n вероватноћа да полином n-тог степена има нулу у $\mathbb{F}_p$. Јасно је да је $x_1 = 1$ и $x_0 = 0$. Идеја нам је да пребројимо колико има полинома који немају корен и да њих одузмемо од укупног броја полинома (којих је тачно p^n).

Теорема 5. ***(Лагранжова теорема)*** *Полином n-тог степена може имати највише n корена у $\mathbb{F}_p$.*

На основу Лагранжове теореме можемо моничан полином n-тог степена са тачно $1 \leq k \leq n$ корена у $\mathbb{F}_p$ записати на следећи начин:

$$P(x) \equiv (x - \alpha_1) \dots (x - \alpha_k) Q(x) (mod \ \ p)$$

Овде су α_i елементи $\mathbb{F}_p$, а Q је моничан полином степена $(n - k)$, који нема корен у $\mathbb{F}_p$. Са $\#P_n$, $\#\alpha$, $\#Q_n$ означавамо број моничних полинома степена n који имају корен, број алфи и број моничних полинома степена n који немају корен тим редом. Полинома P имамо $\sum_{k<n} (\#Q_{n-k})(\#\alpha)$. За почетак пребројимо прво алфе. Нека је се међу њима налази n_0 оних који су 0, n_1 оних који су 1 ... n_{p-1} оних који су $p - 1$. За њих је јасно да важи

$$\sum_{i=0}^{p-1} n_i = k$$

Познато је да је број решења ове једначине у скупу ненегативних бројева баш $\binom{k+p-1}{p-1}$. Дакле: $\#\alpha = \binom{p+k-1}{p-1}$. Сада бројимо колико има полинома Q. Јасно је да је њихов број баш $p^{n-k} - \#P_{n-k}$. Са друге стране имамо $\#P_i = x_i p^i$, тј. $\#Q = p^{n-k}(1 - x_{n-k})$. Коначно:

$$x_n = \frac{\sum_{k=1}^{n} \binom{p+k-1}{p-1} p^{n-k}(1 - x_{n-k})}{p^n} = \sum_{i=0}^{n-1} \frac{(1 - x_i)\binom{p+n-i-1}{p-1}}{p^{n-i}}$$

Ова рекурентна је јако компликована и не постоји затворен облик њеног решења. Иако није лако формулисати решење без рекурзије можемо одговорити на питање колико је нерастављивих моничних полинома степена n у $\mathbb{F}_p$. За почетак дефинишимо омега и Мебијусову функцију:

Дефиниција 7. *Функцију* $\omega : \mathbb{N} \to \mathbb{N}$ *дефинишемо као број различитих простих делилаца.*

Дефиниција 8. *Мебијусова функција се дефинише на следећи начин:*

$$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^{\omega(n)}, & n \in \mathbb{S} \\ 0, & n \notin \mathbb{S} \cup \{1\} \end{cases}$$

Постоји напредна теорија о раширењима $\mathbb{F}_{p^n}$ која нам говори да је број иредуцибилних полинома у $\mathbb{F}_p$ једнак:

$$\frac{\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d}{n}.$$

Оквирно објашњење би било да се делиоци појављују због чињенице да је $\mathbb{F}_{p^a} \supseteq \mathbb{F}_{p^b} \Leftrightarrow b \mid a$, а Мебијусова функција се појављује због принципа укључења и искључења.
*Напомена: Важно је нагласити да иредуцибилан полином и полином који нема корен нису исто. Контрапример би био $x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1)$. Како бисмо пребројали колико има растављивих полинома радили бисмо сличну рекурзију само што по свим партицијама природног броја n.

5.3 Која је вероватноћа да је бинарна квадратна форма растављива?

Дефиниција 9. ***Квадратна форма*** *је полином степена* 2 *по више променљивих, који нема слобних чланова.*

Дефиниција 10. ***Бинарна квадратна форма*** *је полином по две променљиве облика* $ax^2 + bxy + cy^2$.

Дефиниција 11. *Бинарна форма је растављива над* $\mathbb{Z}$ *ако може да се прикаже као производ два линеарна полинома по две променљиве са целобројним коефицијентима. Другим речима:*

$$\exists(a, b, c, d) \in \mathbb{Z}^4; \alpha x^2 + \beta xy + \gamma y^2 = (ax + by)(cx + dy)$$

Лема 6. *Бинарна квадратна форма облика* $\alpha x^2+\beta xy+\gamma y^2$ *је растављива ако и само ако је дискриминанта* $\beta^2 - 4\alpha\gamma$ *потпун квадрат.*

Доказ. Докажимо прво $\Rightarrow$ смер. Нека је $\alpha x^2 + \beta xy + \gamma y^2 = (ax + by)(cx + dy)$. Тада је: $\alpha = ac$; $\gamma = bd$; $\beta = bc + ad$. Приметимо:

$$4\alpha\gamma = 4abcd = (bc + ad)^2 - (bc - ad)^2 \Leftrightarrow \beta^2 - 4\alpha\gamma = (bc - ad)^2$$

За други смер ћемо увести смену $t = \frac{x}{y}$ и хоћемо да је полином $\alpha t^2+\beta t+\gamma$ растављив над $\mathbb{Q}$. Решење квадратне једначине ће бити:

$$t = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}$$

Међутим, овај израз је рационалан само када је $\beta^2-4\alpha\gamma$ потпун квадрат, чиме је доказ завршен.
Сада нас занима која је вероватноћа да насумичним одабиром 3 цела броја, α, β и γ, израз $\beta^2 - 4\alpha\gamma$ буде потпун квадрат. Нажалост, ова вероватноћа је 0 (што нам није занимљиво), али ћемо посматрати понашање у бесконачности.
Претпоставимо да важи $-n \leq \alpha, \beta, \gamma \leq n$ за неко $n \in \mathbb{N}$. Једанчина $n^2 = \beta^2-4\alpha\gamma$ је еквивалентна са $(\beta-n)(\beta+n) = 4\alpha\gamma$, што нас наводи да бирамо α и γ и бројимо колико $4\alpha\gamma$ има парова делилаца $d_1d_2 = 4\alpha\gamma$, који су исте парности (због $\beta = \frac{d_1+d_2}{2}$) и $|d_1 + d_2| \leq 2n$. Да би били исте парности претпоставимо $d_1 = 2d_1'$; $d_2 = 2d_2'$; $d_1'd_2' = \alpha\gamma$; $|d_1' + d_2'| \leq n$. Такође, јако је тешко (можда чак и немогуће) контролисати број делилаца и генерално понашање простих бројева помоћу елементарних функција, те ћемо у овом раду само покушати да то оквирно проценимо. Ради

једноставности претпоставимо да су у питању само природни бројеви, па ћемо на крају „поправити" константу тако што је помножимо са 4. Коначно решење ће нам бити:

$$P = \frac{\sum_{\alpha,\gamma \leq n} \#(d_1', d_2')}{n^3}$$

Дефиниција 12. *Број природних делилаца природног броја* $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ *се означава са* τ *и рачуна се по формули:*

$$\tau(n) = \prod_{i=1}^{k} (\alpha_i + 1)$$

Лема 7.

$$\forall (a, b) \in \mathbb{N}^2 \quad \tau(ab) \leq \tau(a)\tau(b)$$

При чему једнакост важи за $(a, b) = 1$.

Доказ. Нека је $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ $b = \prod_{i=1}^{k} p_i^{\beta_i}$, где су $\alpha_i, \beta_i \geq 0$.

$$\tau(ab) = \tau(\prod_{i=1}^{k} p_i^{\alpha_i + \beta_i}) = \prod_{i=1}^{k} (\alpha_i + \beta_i + 1) \leq \prod_{i=1}^{k} (\alpha_i \beta_i + \alpha_i + \beta_i + 1)$$

$$= \prod_{i=1}^{k} (\alpha_i + 1)(\beta_i + 1) = \tau(a)\tau(b)$$

Заиста, једнакост важи ако је за свако i задовољено $\alpha_i \beta_i = 0$, тј. да $(a, b) = 1$.
Приметимо да је парова где је $d_1' + d_2' > n$ релативно мало (јер захтевају да је бар један d (ако не и оба) реда величине n што повлачи и да су α и γ велики, самим тим ће их бити мање него оних који задовољавају $d_1' + d_2' \leq n$) и неће много „кварити" нашу процену. У сваком случају ако их не одузмемо добићемо само лошију константу. Кад применимо лему 7 добићемо:

$$\sum_{\alpha,\gamma \leq n} \#(d_1', d_2') \sim \sum_{\alpha=1}^{n} \sum_{\gamma=1}^{n} \tau(\alpha\gamma) \leq (\sum_{k=1}^{n} \tau(k)\ )^2$$

Лема 8.

$$\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \lfloor \frac{n}{k} \rfloor$$

Доказ. Ради једноставности дефинишимо $l_n = \sum_{k=1}^{n} \tau(k)$ и $r_n = \sum_{k=1}^{n} \lfloor \frac{n}{k} \rfloor$. Докажимо да је $l_n = r_n$ за свако $n \in \mathbb{N}$ математичком индукцијом по n. Базни случај $n = 1$ је тривијалан. Претпоставимо да је $l_n = r_n$. Јасно је да је $l_{n+1} = l_n + \tau(n+1)$. Са друге стране имамо:

$$\lfloor \frac{n+1}{k} \rfloor - \lfloor \frac{n}{k} \rfloor = \begin{cases} 1, & k \mid n+1 \\ 0, & k \nmid n+1 \end{cases}$$

То нам даје да ће се r_{n+1} повећати за 1 за сваки делилац броја $n+1$, тј. $r_{n+1} = r_n + \tau(n+1)$. Како су рекурентне једначине за два низа једнаке и имају једнаке почетне услове можемо тврдити да су та два низа идентички једнака, чиме смо завршили доказ. За сада имамо да је:

$$\sum_{\alpha,\gamma \leq n} \#(d_1', d_2') \leq (\sum_{k=1}^{n} \lfloor \frac{n}{k} \rfloor)^2$$

Користићемо познату неједнакости да је $\lfloor x \rfloor \leq x$ за сваки реалан број x. Нашу процену ћемо завршити доказом да је:

$$\sum_{k=1}^{n} \lfloor \frac{n}{k} \rfloor \leq \sum_{k=1}^{n} \frac{n}{k} = n \sum_{k=1}^{n} \frac{1}{k} \lesssim n \ln n \quad n \to \infty$$

У претходном поглављу смо показали да зета функција конвергира за природне бројеве ≥ 2, али о случају $n = 1$ не можемо рећи исто. Међутим можемо доказати да асимптотски тежи $\ln n$. Заправо, Ојлер је доказао:

$$H_n = \sum_{k=1}^{n} \frac{1}{k}$$

$$\lim_{n \to \infty} (H_n - \ln n) = \lim_{n \to \infty} \left((\sum_{k=1}^{n} \frac{1}{k}) - \ln n \right) = \gamma \approx 0.577$$

Слично као у претходном поглављу, идеја ће нам бити да суму апроксимирамо интегралом и површином испод графика:

$$H_n = 1 + \sum_{k=2}^{n} \frac{1}{k} \leq 1 + \int_1^n \frac{1}{k} = 1 + \ln(n)$$

$$H_n = 1 + \sum_{k=2}^{n} \frac{1}{k} \geq 1 + \int_1^{n-1} \frac{1}{k} = 1 + \ln(n-1)$$

$$\Rightarrow H_n \sim \ln n$$

Коначно имамо:

$$\sum_{\alpha,\gamma\leq n} \#(d_1', d_2') \lesssim (n \ln n)^2$$

Односно наша вероватноћа је:

$$P \lesssim \frac{4n^2 \ln^2 n}{(2n)^3} = \frac{\ln^2 n}{2n} \quad n \to \infty$$

Занимљивост: Један познат отворен проблем је да се испита да ли је Ојлерова константа γ рационалан број.

6 Закључак

Пре свега, хтео бих да се захвалим свом ментору Стевану Гајовићу на корисним саветима и на помоћи око одабира теме и адекватне литературе. Захвалио бих се и осталим професорима Математичке гимназије на несебичној пажњи и залагању, којима су допринели развоју моје љубави према математици.

Јако ми се допала ова тема, јер повезује реалну анализу, комплексну анализу, вероватноћу, аналитичку теорију бројева, алгебарску теорију бројева и још многе друге гране математике. Такође, важно је напоменути да се у овом раду може видети велики део знања које сам стекао у средњој школи.

У свом раду сам се у другој глави бавио неким простим примерима вероватноћа у теорији бројева, са идејом да читаоцу приближим концепт аритметичке статистике. У трећој глави сам елементарно извео слабију верзију теореме о простим бројевима и доказао Дирихлеову теорему о простим бројевима за конкретан случај $m = 4$. У четвртој глави сам се претежно бавио занимљивим примерима вероватноћа везаних за делиоце. У последњој глави сам изводио вероватноће да полином има корен у $\mathbb{F}_p$ као и да је растављив над целим бројевима.

У раду је коришћено доста напредних теорема, које сам морао да наведем без доказа, било да доказ превазилази средњошколско градиво или је доказ дугачак и заморан.

Литература

[1] G. J. O. Jameson. *The Prime Numbers and the Riemann Hypothesis.* 2003.

[2] Uroš Milenković. Maturski rad. `https://www.mg.edu.rs/uploads/files/images/stories/dokumenta/maturski/uros-milenkovic.pdf`, 2020.

[3] M. Ram Murty and Jody Esmonde. *Problems in Algebraic Number Theory.* 2005. Lecture notes, University of Toronto.

[4] Michael Penn. How often (gaussian) integers are relatively prime. `https://www.youtube.com/watch?v=dXdyMeZ7Zmc`, 2025.

[5] E. C. Titchmarsh. *The Theory of the Riemann Zeta-Function.* Oxford University Press, 1986.

[6] Mak Trifković. *Algebraic Theory of Quadratic Numbers.* 2013. Lecture notes (PDF), Cornell University archive.