Ana Petrović i Milica Maksimović

Verovatnoća pogotka pri pogrešnoj primeni teoreme

Ideja projekta bazirana je na ispitivanju verovatnoće tačnosti neke teoreme ako izostavimo jedan od uslova ili iskoristimo obrnutu implikaciju. Sve teoreme koje smo proučavali bave se granom matematike koja se naziva teorija brojeva. U prvom delu rada upoznali smo se sa pojmovima, tvrđenjima i asimptotskim ponašanjima nekih funkcija koje su nam bile potrebne. Takođe, objašnjen je i pojam verovatnoće koji se primenjuje na skupove sa beskonačno mnogo elemenata kao što su skupovi celih, racionalnih i prirodnih brojeva. U drugom delu rada bazirali smo se na posmatranje određenih netrivijalnih teorema iz teorije brojeva i došli do zaključka da će u svakoj od posmatranih teorema tražena verovatnoća biti jednaka nuli. U trećem delu smo prikazali nedovršena izračunavanja traženih verovatnoća, kao i ideje i smernice o daljem toku istraživanja.

Uvod

Inspiracija za projekat pronađena je u radu australijskog matematičara Adriana Dudeka (Dudek 2016). On je primetio da studenti često greše izostavljajući neki od uslova pri primeni teoreme, te je odlučio da izračuna kolika je verovatnoća da oni pogode tačan rezultat, iako su pogrešno primenili teoremu. U svom radu Dudek se bazirao na Euklidovu lemu koja glasi:

Lema 1. Za prost broj p i cele brojeve a i b važi sledeća implikacija

$$p \mid ab \Rightarrow p \mid a \vee p \mid b$$

Zanimalo ga je koja je verovatnoća tačnosti leme ako se izostavi uslov da je p prost broj, te je izračunao da je za „slučajno izabrane brojeve" p, a i b ta verovatnoća jednaka nuli.

U ovom projektu radićemo nešto slično. Ispitivaćemo verovatnoću tačnosti teorema iz teorije brojeva, ako izostavimo neki od uslova ili primenimo obrnutu implikaciju.

Ana Petrović (2000), Čačak, Nemanjina 6, učenica 3. razreda Gimnazije u Čačku

Milica Maksimović (2001), Bačka Palanka, Drvarska 6, učenica 2. razreda Gimnazije „20. oktobar" u Bačkoj Palanci

MENTOR: Branislav Šobot, student Prirodno-matematičkog fakulteta Univerziteta u Novom Sadu

Sam rad se sastoji iz tri dela. Prvi deo će nam pomoći da se upoznamo sa funkcijama, teoremama i asimptotskim ponašanjima koje ćemo koristiti u nastavku rada. Drugi deo rada predstavljen je kroz više podsekcija. Svaka od njih obuhvata teoremu čiju smo verovatnoću tačnosti računali prilikom izostavljenog ili izmenjenog uslova, ili ukoliko smo teoremu primenili u suprotnom smeru. Izostavljeni uslovi su uglavnom da li su brojevi prosti, uzajamno prosti, kongruentni, deljivi itd. Na kraju se nalazi odeljak u kome se nalaze nedovršena izračunavanja traženih verovatnoća, kao i ideje i smernice o daljem toku istraživanja.

Metoda

U ovoj sekciji upoznaćemo se sa metodom koju smo koristili pri radu, tačnije verovatnoćom. Takođe uvešćemo i osnovne teoreme, funkcije, asimptotska ponašanja, kao i ostale pojmove neophodne za razumevanje ostalih odeljaka ovog rada. Teoreme su navedene bez dokaza, a uz svaku je priloženo gde se njen dokaz nalazi.

Verovatnoća

U ovoj sekciji objasnićemo kako se računa verovatnoća koja nas zanima. Još u XVII veku, pomažući svom prijatelju kockaru, francuski matematičari Pjer de Ferma i Blez Paskal uspeli su da reše jedan problem sa kartama. Baš te 1654. godine začeli su novu granu matematike koja se naziva *verovatnoća*.

Klasična verovatnoća nam govori koje su šanse da odaberemo određeni elemenat nekog konačnog skupa. U našem slučaju, najčešće se radi o skupovima celih ($\mathbb{Z}$) i prirodnih brojeva ($\mathbb{N}$), čijih elemenata ima beskonačno mnogo. Iz tog razloga verovatnoća koju ćemo koristiti u ovom radu razlikuje se od ove gore pomenute. Da bismo našli verovatnoću koja nas je zanimala koristili smo sledeći izraz:

$$\lim_{n\to\infty} \frac{A(n)}{B(n)}$$

pri čemu nam funkcija $A(n)$ broji sve uređene k-torke čije su sve koordinate manje od n i koje ispunjavaju uslove početne teoreme, dok je $B(n)$ funkcija koja broji sve uređene k-torke čije su sve koordinate manje od n i za koje ne mora da važi zanemareni uslov, gde je k broj promenljivih koji se pominje u nekoj konkretnoj teoremi.

Teoreme i funkcije

Krajem 18. veka Gaus i Ležandr definisali su funkciju $\pi(n)$, kao funkciju koja broji proste brojeve manje ili jednake n. Za nju važi sledeća teorema.

Teorema 1. (Teorema o prostim brojevima; preuzeto iz Gehring i Halmos 1976). Za funkciju $\pi(n)$ važi:

$$\pi(n) \sim \frac{n}{\log n}$$

odnosno da je:

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

Ojlerova funkcija $\varphi(n)$, definisana za pozitivne cele brojeve n, predstavlja broj pozitivnih, celih brojeva manjih ili jednakih n, koji su uzajamno prosti sa n. Uveo ju je Leonard Ojler 1763. godine.

Teorema 2 (preuzeto iz Đanković 2013). Za funkciju $\varphi(n)$, za $n \in \mathbb{N}$, važi sledeća jednakost:

$$\sum_{d|n} \varphi(n) = n$$

gde suma prolazi kroz sve pozitivne delioce broja n.

Teorema 3 (Dirihle; preuzeto iz Selberg 1949). Ako su a i d uzajamno prosti prirodni brojevi, onda aritmetička progresija

$$a, a + d, a + 2d, a + 3d \ldots$$

sadrži beskonačno mnogo prostih brojeva.

Landauovi simboli

Landauovi simboli u matematici se koriste za opisivanje asimptotskih tendencija, tačnije brzine rasta funkcija i redova. Ukoliko posmatramo aritmetičke funkcije, oni su definisani na sledeći način.

Definicija 1. Neka je n celobrojna promenljiva koja teži beskonačnosti, i neka je $f(n)$ neka funkcija, a $\phi(n)$ neka pozitivna funkcija. Tada je Landau simbol $O(n)$, poznatiji kao „veliko O" definisan kao:

$$f = O(\phi) \Leftrightarrow |f(n)| < A\phi(n)$$

za neku konstantu $A > 0$ i sve prirodne vrednosti za n.

Iako po definiciji O predstavlja skup funkcija, mi ćemo ga posmatrati kao izraz koji je proizvoljna funkcija iz tog skupa. Iz ovog razloga smemo koristiti sledeće operacije.

Teorema 4 (preuzeto iz Knuth 1997). Prilikom posmatranja aritmetičkih funkcija, za notaciju O važe sledeće operacije:

- $c \cdot f = O(c \cdot f) = c \cdot O(f) = O(f)$ za svako $c \geq 0$
- $O(f_1) + O(f_2) + \ldots + O(f_k) = O(\max\{f_1, \ldots, f_k\})$ za neku konstantu $k \in \mathrm{N}$, pri čemu funkcija max traži najveću od ponuđenih funkcija $f_1, \ldots, f_k$
- $O(f) \cdot O(g) = O(f \cdot g)$

Asimptotska ponašanja

Teorema 5 (preuzeto iz Gehring i Halmos 1976). Ako imamo pozitivan ceo broj x, takav da on teži beskonačnosti, važi sledeća jednakost:

$$\sum_{n=1}^{x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$$

pri čemu je $C > 0$ konstanta.

Konstanta koju smo pominjali u prethodnoj teoremi naziva se Ojlerova konstanta i približno je jednaka $C \approx 0.5772$.

Neka je $\zeta(s)$ Rimanova zeta funkcija koja se definiše kao:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots$$

za sve $s > 1$. Neke od vrednosti za Rimanovu zeta funkciju su sledeće: $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, … Dalje imamo da važi sledeća teorema:

Teorema 6 (preuzeto iz Broughan 2001). Neka je:

$$g(a) = a\sum_{d|a} \frac{\varphi(d)}{d} \text{ i } G_{\alpha}(x) = \sum_{n=1}^{x} \frac{g(n)}{n^{\alpha}}$$

gde $\alpha \in \mathbb{N}$. Tada je asimptotsko ponašanje funkcije $G_2(x)$ sledeće:

$$G_2(x) = \frac{\log^2 x}{2\,\zeta(2)} + O(\log x)$$

Nemački matematičar Mebijus je 1832. godine definisao funkciju $\mu(n)$ na sledeći način.

Definicija 2. Za $n = 1$ Mebijusova funkcija $\mu(n)$ definisana je kao:

$$\mu(1) = 1$$

Ako je $n > 1$, zapisano kao $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ gde su p_i prosti brojevi, a a_i prirodni brojevi, onda je:

$$\mu(n) = \begin{cases} (-1)^k, & \text{ako je } a_1 = a_2 = \ldots = a_k = 1 \\ 0, & \text{inače.} \end{cases}$$

Sa T ćemo obeležiti konstantu $T = \sum_{n=1}^{\infty} \frac{\mu(n)\log n}{n^2}$, za čiji red nećemo pokazivati da konvergira.

Teorema 7 (preuzeto iz Đanković 2013). Ukoliko imamo neki broj n, takav da n teži beskonačnosti, važe sledeće jednakosti:

$$\sum_{p=1}^{n} \varphi(p) = \frac{n^2}{2\,\zeta(2)} + O(n \log n)$$

$$\sum_{p=1}^{n} \frac{\varphi(p)}{p^2} = \frac{1}{\zeta(2)} \log n + \frac{C}{\zeta(2)} - T + O\left(\frac{\log n}{n}\right)$$

Rezultati

U ovom odeljku upoznaćemo se sa razultatima rada i posvetiti pažnju samim teoremama kao i računanju traženih verovatnoća.

1. Da li je broj oblika $6k \pm 1$ je prost?

U ovoj podsekciji ćemo razmatrati suprotan smer sledeće teoreme.

Teorema 8. Svaki prost broj $p > 3$ je oblika $p = 6k \pm 1$, za neki prirodan broj k.

Pitamo se koja je verovatnoća da smo u pravu ako za neki broj tog oblika kažemo da je prost. U ovom slučaju $A(n)$ predstavlja funkciju koja broji proste brojeve manje ili jednake od n i nju ćemo predstaviti funkcijom $\pi(n)$ koju smo definisali u prethodnoj sekciji, a $B(n)$ predstavlja funkciju koja broji brojeve oblika $6k \pm 1$ manje ili jednake od n. Nju možemo zapisati na sledeći način:

$$B(n) = \frac{n}{3} + \alpha(n)$$

jer se na svakih 6 uzastopnih brojeva pojavljuju po dva broja sa traženim osobinama. U prethodnoj formuli funkcija $\alpha(n)$ predstavlja grešku koju možemo napraviti pri deljenju bilo kog broja $n \in \mathbb{N}$ sa 3. Kako funkcija $\alpha(n)$ može imati vrednosti $0, \frac{1}{3}$ i $\frac{2}{3}$ što je uvek manje ili jednako od 1, možemo je zameniti oznakom $O(1)$. Dakle:

$$B(n) = \frac{n}{3} + O(1).$$

Uvođenjem asimptotskih vrednosti funkcija $A(n)$ i $B(n)$ u sledeću formulu možemo izračunati traženu verovatnoću:

$$\lim_{n\to\infty} \frac{A(n)}{B(n)} = \lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{3} + O(n)} = 3 \lim_{n\to\infty} \frac{\pi(n)}{n + O(1)}$$

Kako znamo da za funkciju $\pi(n)$ važi teorema 1 možemo zaključiti da je:

$$\lim_{n\to\infty} \frac{A(n)}{B(n)} = 3 \lim_{n\to\infty} \frac{\pi(n)\log n}{n + O(1)} \cdot \frac{1}{\log n} = 3 \lim_{n\to\infty} \frac{1}{\log n} = 0$$

i da važi sledeća teorema:

Teorema 9. Ako za neki broj oblika $6k \pm 1$ kažemo da je prost, verovatnoća da smo u pravu jednaka je 0.

Sada ćemo dokazati da teorema 9 važi i u nešto opštijem slučaju. Posmatrajmo ostatke pri deljenju prostih brojeva p sa nekim prirodnim brojem $2 \le d < p$. Kada bi ti ostaci imali zajedničke delioce sa d, broj p bi bio deljiv sa tim zajedničkim faktorom i sa samim sobom, što znači da ne bi bio prost. Posmatrajmo sada aritmetičke progresije oblika:

$$\begin{array}{c} d+a_1, 2d+a_1, \ldots, xd+a_1 \\ d+a_2, 2d+a_2, \ldots, xd+a_2 \\ \vdots \\ d+a_m, 2d+a_m, \ldots, xd+a_m \end{array}$$

pri čemu $d \in \mathbb{N}$, a $a_1, a_2, \ldots, a_m$ su svi prirodni brojevi uzajamno prosti sa d, i manji od d. Na osnovu teoreme 3 znamo da svaka od ovih progresija sadrži beskonačno mnogo prostih brojeva, što znači da su u pomenutim progresijama sadržani svi prosti brojevi veći od d. Odnosno, svi prosti brojevi veći od d mogu se zapisati u nekom od oblika $dk + a_1$, $dk + a_2$, …, $dk + a_m$, pri čemu je k bilo koji prirodan broj. Kako znamo da d i a_i moraju biti uzajamno prosti, vidimo da za neko d postoji tačno $m = \varphi(d)$ različitih a.

Sada se pitamo koja je verovatnoća da smo u pravu ako za neki broj pomenutog oblika kažemo da je prost. U ovom slučaju funkcija $A(n)$ broji proste brojeve manje od n i nju možemo predstaviti funkcijom $\pi(n)$. Funkcija $B(n)$ broji sve brojeve oblika $dk + a_1$, $dk + a_2$, …, $dk + a_m$ manje od n, gde su a_i uzajamno prosti sa d. Kako na svakih d uzastopnih brojeva postoji $\varphi(d)$ brojeva tog oblika funkcija $B(n)$ može se predstaviti kao:

$$B(n) = \varphi(d)\left\lfloor \frac{n}{d} \right\rfloor + O(1) = \varphi(d)\frac{n}{d} + O(1)$$

Dakle, tražena verovatnoća jednaka je:

$$\lim_{n\to\infty} \frac{A(n)}{B(n)} = \lim_{n\to\infty} \frac{\pi(n)}{\varphi(d)\frac{n}{d} + O(1)}$$

Kako smo d definisali kao konstantu, onda je i $\varphi(d)$ takođe konstanta. Limes ne utiče na konstante, pa one mogu da izađu ispred njega. Prema tome:

$$\lim_{n\to\infty} \frac{A(n)}{B(n)} = \frac{d}{\varphi(d)} \lim_{n\to\infty} \frac{\pi(n)}{n + O(1)}$$

Ranije smo dokazali da je limes iz ove formule jednak nuli, pa možemo zaključiti da je i tražena verovatnoća jendaka nuli, čime smo dokazali da teorema 9 važi i u opštijem slučaju. Dakle, važi sledeća teorema.

Teorema 10. Ako za neki broj oblika $dk + a$, pri čemu su d i a uzajamno prosti prirodni brojevi i $k \in \mathbb{N}$, kažemo da je prost, verovatnoća da smo u pravu jednaka je 0.

2. Proizvod dva broja je potpun kvadrat?

U ovom delu izračunaćemo verovatnoću tačnosti sledeće teoreme ako zanemarimo jedan od uslova.

Teorema 11. Ako su a i b uzajamno prosti brojevi i važi $ab = c^2$ onda je a potpun kvadrat i b potpun kvadrat.

Ako u formulaciji prethodne teoreme zanemarimo činjenicu da su a i b uzajamno prosti, koja je verovatnoća da su oni zaista potpuni kvadrati?

Funkcija $A(n)$ predstavlja broj uređenih trojki (a, b, c) takvih da su $a, b, c \le n$, važi $ab = c^2$ i da su a i b potpuni kvadrati, dok funkcija $B(n)$ predstavlja broj uređnih trojki (a, b, c) takvih da su $a, b, c \le n$ i da važi $ab = c^2$. U narednoj lemi daćemo asimptotsko ponašanje funkcije $A(n)$.

Lema 2. Kada n teži beskonačnosti, za funkciju $A(n)$ važi sledeća jednakost:

$$A(n) = n + O(\sqrt{n}).$$

Dokaz. Ako predstavimo a i b kao potpune kvadrate brojeva x i y, funkciju $A(n)$ možemo zapisati kao:

$$A(n) = \sum_{\substack{a \le n \\ a = x^2}} \sum_{\substack{b \le n \\ b = y^2}} 1$$

Dalje, sumu po brojevima b koji se nalaze u intervalu od 1 do n, uzimajući u obzir već pomenuti uslov da je $b = y^2$, možemo zapisati i kao sumiranje brojeva po y koji idu od 1 do $\sqrt{n}$, to jest:

$$A(n) = \sum_{\substack{a \le n \\ a = x^2}} \sum_{y=1}^{\sqrt{n}} 1 = \sum_{\substack{a \le n \\ a = x^2}} \left(\sqrt{n} + O(1) \right)$$

Analogno ćemo transformisati sumu koja sumira po svim a takvim da je $a = x^2$ i koji idu od 1 do $\sqrt{n}$. Dakle:

$$\sum_{\substack{a \le n \\ a = x^2}} \left(\sqrt{n} + O(1) \right) = \sum_{x=1}^{\sqrt{n}} \left(\sqrt{n} + O(1) \right) =$$

$$= \sum_{x=1}^{\sqrt{n}} \sqrt{n} + \sum_{x=1}^{\sqrt{n}} O(1) =$$

$$= \sqrt{n} \sum_{x=1}^{\sqrt{n}} 1 + O(\sqrt{n}) =$$

$$= \sqrt{n} \left(\sqrt{n} + O(1) \right) + O(\sqrt{n}) =$$

$$= n + 2O(\sqrt{n}) = n + O(\sqrt{n}) \quad \square$$

Ako uvedemo funkciju $C(n)$ takvu da je $C(n) \le \mathrm{B}(n)$ i pokažemo da je prilikom posmatranja funkcija $A(n)$ i $C(n)$ tražena verovatnoća jednaka 0, lako možemo zaključti da će isto važiti za svaku funkciju veću od $C(n)$, pa i za $B(n)$. Dokažimo sada da važi sledeća lema.

Lema 3. Za funkciju $C(n)$ oblika:

$$C(n) = \frac{1}{2} \cdot \frac{1}{\zeta(2)} n \log n + O(n) = \frac{3}{\pi^2} n \log n + O(n)$$

kada n teži bekonačnosti važi $C(n) \le B(n)$.

Dokaz. Broj uređenih trojki (a, b, c), za koje važi da je $ab = c^2$, predstavićemo kao broj uređenih trojki oblika (m, mq^2, mq). Na ovaj način dobili smo da je $m = a$, $q = \frac{c}{a}$, pri čemu je b jednoznačno određeno i $q \in \mathrm{Q}$.

Ovim je zadovoljen uslov da a i b mogu, a i ne moraju biti uzajamno prosti. Dalje ćemo q prikazati kao količnik brojeva p i r koji su uzajamno prosti. Ako bismo posmatrali parove brojeva p i r koji nisu uzajamno prosti, istu vrednost njihovog količnika, odnosno parametra q, dobili bismo na više načina zbog različitih koeficijenata koji bi množili p i r. Kako su a, b i c celi brojevi, iz toga sledi da i mq^2 mora biti ceo broj koji se može predstaviti kao $\frac{mp^2}{r^2}$. Pošto su p i r uzajamno prosti mora da važi uslov da $r^2 \mid m$. Kako smo trojku (a, b, c) predstavili kao (m, mq^2, mq), zaključujemo da m, mq^2, mq moraju biti manji od n. Dakle:

$$mq \le n \Rightarrow m\frac{p}{r} \le n \Rightarrow p \le \frac{nr}{m}$$

$$mq^2 \le n \Rightarrow m\frac{p^2}{r^2} \le n \Rightarrow p \le \sqrt{\frac{n\,r^2}{m}}$$

Međutim, imamo da je:

$$\frac{nr}{m} < \sqrt{\frac{nr^2}{m}} \Rightarrow n < m$$

što je u kontradikciji sa uslovom da je $m \le n$. Dakle dovoljno je da uzmemo u obzir uslov $p \le \sqrt{\frac{nr^2}{m}}$, a iz njega možemo zaključiti da je $p \le \sqrt{n}$, što će nam kasnije biti potrebno. Na osnovu prethodnih uslova, prikazaćemo funkciju $B(n)$ u obliku:

$$B(n) = \sum_{m=1}^{n} \sum_{r^2 \mid m} \sum_{\substack{(p,r)=1 \\ p \le \sqrt{\frac{nr^2}{m}}}} 1$$

Sada ćemo naći donje ograničenje za funkciju $B(n)$, tako što ćemo ubaciti uslov $p \ge r$ među ostale uslove za brojače i dobiti da važi:

$$B(n) \ge \sum_{p=1}^{\sqrt{n}} \sum_{\substack{(p,r)=1 \\ r \le p}} \sum_{\substack{m \le \frac{nr^2}{p^2} \\ r^2 \mid m}} 1 =$$

$$= \sum_{p=1}^{\sqrt{n}} \sum_{\substack{(p,r)=1 \\ r \le p}} \left(\frac{n}{p^2} + O(1) \right) =$$

$$= \sum_{p=1}^{\sqrt{n}} \left(\frac{n}{p^2} \sum_{\substack{(p,r)=1 \\ r \le p}} 1 + O\left(\sum_{\substack{(p,r)=1 \\ r \le p}} 1 \right) \right)$$

Sređivanjem dobijenog izraza dolazimo do ograničenja tražene funkcije:

$$B(n) \geq n\sum_{p=1}^{\sqrt{n}} \frac{\varphi(p)}{p^2} + O\left(\sum_{p=1}^{\sqrt{n}} \varphi(p)\right)$$

Ako uporedimo funkcije $B(n)$ i $C(n)$ možemo zaključiti da je:

$$C(n) = \frac{3}{\pi^2} n \log n + O(n) \leq n\sum_{p=1}^{\sqrt{n}} \frac{\varphi(p)}{p^2} + O\left(\sum_{p=1}^{\sqrt{n}} \varphi(p)\right)$$

što sledi iz teoreme 7. Ovim smo dokazali da je $C(n) \leq B(n)$ kada n teži beskonačnosti. □

Verovatnoću, ako posmatramo funkcije $A(n)$ i $C(n)$, računamo na sledeći način:

$$\lim_{n\to\infty} \frac{A(n)}{C(n)} = \lim_{n\to\infty} \frac{n + O(n)}{\frac{3}{\pi^2} n \log n + O(n)} = 0$$

Kako je $C(n) \leq B(n)$ sledi da je verovatoća u ovom slučaju takođe jednaka 0, odnosno da važi sledeća teorema.

Teorema 12. Ako posmatramo brojeve a, b i c takve da važi da je $ab = c^2$ i kažemo da su a i b potpuni kvadrati, verovatnoća da smo u pravu jednaka je 0, to jest:

$$\lim_{n\to\infty} \frac{A(n)}{B(n)} = 0$$

3. Deljenje kongruencije

U narednoj podsekciji razmatraćemo tačnost sledeće teoreme prilikom zanemarivanja jednog od uslova.

Teorema 13. Ako znamo da su brojevi a i m uzajamno prosti i da važi $ab \equiv ac \pmod{m}$ onda je $b \equiv c \pmod{m}$.

Pitamo se šta se dešava ako u formulaciji prethodne teoreme izostavimo uslov da su a i m uzajamno prosti. Funkcija $A(n)$ predstavlja broj uređenih četvorki (a, b, c, m) takvih da su $a, b, c, m \leq n$ i da važi $b \equiv c \pmod{m}$, a funkcija $B(n)$ je broj uređenih četvorki (a, b, c, m) takvih da su $a, b, c, m \leq n$ i da važi $ab \equiv ac \pmod{m}$. Prvo ćemo dokazati da se funkcija $A(n)$ može prikazati na sledeći način.

Lema 4. Kada n teži beskonačnosti funkcija $A(n)$ je:

$$A(n) = n^3 \log n + O(n^3)$$

Dokaz. Najpre ćemo fiksirati broj m koji može biti u intervalu od 1 do n, i za njega ćemo ispitati broj kombinacija b i c takvih da važi $b \equiv c \pmod{m}$. Ostaci pri deljenju broja b (odnosno c) sa m mogu biti $\{0, 1, 2, 3, \ldots, m-1\}$ iz čega zaključujemo da postoji tačno m različitih ostataka. Svaki od tih ostataka možemo izabrati na $\frac{n}{m} + O(1)$ načina, jer b mora biti manje od n. S obzirom da posmatramo uređene parove brojeva b i c, u obzir moramo uzeti ostatke za oba broja. Iz svega ovoga, zaključujemo da je broj traženih

kombinacija jednak $m\left(\frac{n}{m}+O(1)\right)^2$. Kako a može biti bilo koji broj manji od n imamo da je funkcija $A(n)$ jednaka:

$$A(n)=\sum_{m=1}^{n}\sum_{a=1}^{n}m\left(\frac{n}{m}+O(1)\right)^2=$$
$$=n\sum_{m=1}^{n}m\left(\frac{n}{m}+O(1)\right)^2=$$
$$=n\sum_{m=1}^{n}m\left(\frac{n^2}{m^2}+2O\left(\frac{n}{m}\right)+O(1)\right)=$$
$$=n\sum_{m=1}^{n}\left(\frac{n^2}{m}+O(n)\right)=$$
$$=n\sum_{m=1}^{n}\frac{n^2}{m}+O(n^3)=$$
$$=n^3\sum_{m=1}^{n}\frac{1}{m}+O(n^3)$$

Dobijeni izraz transformisaćemo pomoću teoreme 5:

$$n^3\sum_{m=1}^{n}\frac{1}{m}+O(n^3)=n^3\left(\log n+C+O\left(\frac{1}{n}\right)\right)+O(n^3)=$$
$$=n^3\log n+n^3C+O(n^2)+O(n^3)=$$
$$=n^3\log n+n^3C+O(n^3)=$$
$$=n^3\log n+O(n^3)\ \square$$

Sledeći korak je izračunavanje funkcije $B(n)$.

Lema 5. Kada n teži beskonačnosti imamo da je:

$$B(n)=\frac{n^3\log^2 n}{2\zeta(2)}+O(n^3\log n)$$

Dokaz. Znamo da važi:

$$ab\equiv ac\,(\mathrm{mod}\,m)\Rightarrow m\mid(ab-ac)\Rightarrow m\mid a(b-c)$$

Uvešćemo smenu $x=b-c$ i primetiti da se svako $x\geq 0$ može predstaviti na tačno $n-x$ načina i svako $x<0$ na $n+x$ načina, kao razlika $b-c$ gde su b i c manji ili jednaki od n. Dakle:

$$B(n)=\sum_{m=1}^{n}\sum_{a=1}^{n}\left(\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x\geq 0\\ x\leq n}}(n-x)+\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x<0\\ x\geq -n}}(n+x)\right)$$

Kako pomenuta suma po x, kada je x negativan ima jednaku vrednost kao i kada je pozitivan sledi da je:

$$\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x\geq 0\\ x\leq n}}(n-x)+\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x<0\\ x\geq -n}}(n+x)=2\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x>0\\ x\leq n}}(n-x)=2\left(n\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x>0\\ x\leq n}}1-\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x>0\\ x\leq n}}x\right)$$

Ove sume možemo predstaviti i na sledeći način:

$$2n\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x>0\\ x\leq n}}1=2n\left\lfloor\frac{n}{\frac{m}{(a,m)}}\right\rfloor=2\frac{n^2(a,m)}{m}+O(n)$$

$$2\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x>0\\ x\leq n}}x=2\left(\frac{m}{(a,m)}+\frac{2m}{(a,m)}+\ldots+\left\lfloor\frac{n}{\frac{m}{(a,m)}}\right\rfloor\cdot\frac{m}{(a,m)}\right)=$$

$$=2\cdot\frac{m}{(a,m)}\left(1+2+\cdots+\left\lfloor\frac{n}{\frac{m}{(a,m)}}\right\rfloor\right)=$$

$$=2\cdot\frac{m}{(a,m)}\cdot\frac{\left\lfloor\frac{(a,m)n}{m}\right\rfloor\left(\left\lfloor\frac{(a,m)n}{m}\right\rfloor+1\right)}{2}=$$

$$=\frac{m}{(a,m)}\left(\frac{(a,m)n}{m}+O(1)\right)\left(\frac{(a,m)n}{m}+O(1)+1\right)=$$

$$=\frac{m}{(a,m)}\left(\frac{(a,m)^2n^2}{m^2}+\frac{(a,m)n}{m}+O\left(\frac{(a,m)n}{m}\right)\right)=$$

$$=\frac{n^2(a,m)}{m}+n+O(n)=\frac{n^2(a,m)}{m}+O(n)$$

pa je traženi izraz jednak:

$$\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x\geq 0\\ x\leq n}}(n-x)+\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x<0\\ x\geq -n}}(n+x)=2\frac{n^2(a,m)}{m}+O(n)-\frac{n^2(a,m)}{m}+O(n)=$$

$$=\frac{n^2(a,m)}{m}+O(n)$$

Dobijenu vrednost uvrstićemo u glavni izraz i dobićemo da je:

$$B(n)=\sum_{m=1}^{n}\sum_{a=1}^{n}\left(\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x>0}}(n-x)+\sum_{\substack{\frac{m}{(a,m)}\mid x\\ x<0}}(n+x)\right)=$$

$$=\sum_{m=1}^{n}\sum_{a=1}^{n}\left(\frac{n^2(a,m)}{m}+O(n)\right)=$$

$$=\sum_{m=1}^{n}\sum_{a=1}^{n}\frac{n^2(a,m)}{m}+O(n^3)=$$

$$=n^2\sum_{m=1}^{n}\frac{1}{m}\sum_{a=1}^{n}(a,m)+O(n^3)$$

Da bismo izračunali $\sum_{a=1}^{n}(a,m)$ koristićemo se teoremom 2 i odatle imamo da je:

$$(a,m)=\sum_{d\mid(a,m)}\varphi(d)$$

prema tome za neko fiksirano m važi:

$$\sum_{a=1}^{n}(a,m)=\sum_{a=1}^{n}\sum_{d\mid(a,m)}\varphi(d)=\sum_{a=1}^{n}\sum_{\substack{d\mid a\\ d\mid m}}\varphi(d)$$

Uvešćemo smenu da je $a=kd$, pa je:

$$\sum_{a=1}^{n}(a,m)=\sum_{d\mid m}\sum_{k\le\frac{n}{d}}\varphi(d)=$$

$$=\sum_{d\mid m}\varphi(d)\left(\frac{n}{d}+O(1)\right)=$$

$$=n\sum_{d\mid m}\frac{\varphi(d)}{d}+O\left(\sum_{d\mid m}\varphi(d)\right)=$$

$$=n\sum_{d\mid m}\frac{\varphi(d)}{d}+O(m)$$

Kada dobijenu vrednost primenimo u glavnom izrazu dobijemo:

$$B(n)=n^2\sum_{m=1}^{n}\frac{1}{m}\sum_{a=1}^{n}(a,m)+O(n^3)=$$

$$=n^2\sum_{m=1}^{n}\frac{1}{m}\left(n\sum_{d\mid m}\frac{\varphi(d)}{d}+O(m)\right)+O(n^3)=$$

$$=n^2\sum_{m=1}^{n}\left(\frac{n}{m}\sum_{d\mid m}\frac{\varphi(d)}{d}+O(1)\right)+O(n^3)=$$

$$=n^3\sum_{m=1}^{n}\frac{1}{m}\sum_{d\mid m}\frac{\varphi(d)}{d}+O(n^3)$$

Iz teoreme 6 sledi da je:

$$\sum_{m=1}^{n} \frac{1}{m} \sum_{d \mid m} \frac{\varphi(d)}{d} = G_2(n) = \frac{\log^2 n}{2\,\zeta(2)} + O(\log n)$$

Kada dobijeni rezultat ubacimo u gore pomenutu jednačinu dobijemo:

$$B(n) = n^3 \left(\frac{\log^2 n}{2\,\zeta(2)} + O(\log n) \right) + O(n^3) =$$

$$= \frac{n^3 \log^2 n}{2\zeta(2)} + O(n^3 \log n) + O(n^3) =$$

$$= \frac{n^3 \log^2 n}{2\zeta(2)} + O(n^3 \log n) \ \square$$

Kako su nam sada poznata asimptotska ponašanja funkcija $A(n)$ i $B(n)$, možemo zaključiti da je tražena verovatnoća jednaka:

$$\lim_{n\to\infty} \frac{A(n)}{B(n)} = \lim_{n\to\infty} \frac{n^3 \log n + O(n^3)}{\frac{n^3 \log^2 n}{2\,\zeta(2)} + O(n^3 \log n)} = 0$$

odnosno da važi naredna teorema.

Teorema 14. Ako za cele brojeve a, b, c i m za koje važi $ab \equiv ac \pmod m$, kažemo da je $b \equiv c \pmod m$, verovatnoća da smo u pravu jednaka je 0.

Dalja istraživanja

U ovom odeljku prikazaćemo neke od teorema za koje smo pokušali da odredimo verovatnoću ali postupak iz određenih razloga nije dovršen. Takođe, navešćemo neke od ideja za dalji rad u ovoj oblasti.

Da li je broj prost?

Posmatrajući sledeću teoremu zanimalo nas je da li je moguće zaključiti da je neki broj a prost ukoliko ne proverimo sve brojeve manje od $\sqrt{a}$ već stanemo posle $f(a)$ koraka, pri čemu nam $f(a)$ predstavlja funkciju koja raste sporije od $\sqrt{a}$.

Teorema 15. Kada proveravamo da li je broj a prost, dovoljno je proveriti da li je deljiv sa svim brojevima manjim ili jednakim od $\sqrt{a}$.

Konkretno, razmatrali smo slučaj u kome nam je $f(a) = \sqrt[3]{a}$ i pitali se kolika bi u tom slučaju bila tražena verovatnoća. Funkcija $A(n)$ tada bi brojala proste brojeve manje ili jednake od n, i možemo je predstaviti funkcijom $\pi(n)$. $B(n)$ bi predstavljala funkciju koja broji sve brojeve a, od 1 do n koji su uzajamno prosti sa svim brojevima od 1 do $\sqrt[3]{a}$. Dakle, koristeći osobine funkcije $\pi(n)$ zaključujemo sledeće:

$$A(n) = \pi(n) \sim \frac{n}{\log n}$$

Funkciju $B(n)$ možemo predstaviti kao $\sum_{a=1}^{n} 1$, pri čemu a nema delioce manje ili jednake od $\sqrt[3]{a}$. Sledeća ideja bila je zapisati funkciju $B(n)$ na lepši način. Kako delioci broja a moraju biti veći od $\sqrt[3]{a}$, možemo zaključiti da broj a sme imati najviše dva delioca. Prema tome, broj a možemo zapisati u obliku $a = pq$, pri čemu su p i q prosti brojevi veći od $\sqrt[3]{a}$. Kako za broj a brojimo neuređene parove $\{p, q\}$, možemo fiksirati da je $p \le q$. Iz uslova $p > \sqrt[3]{pq}$ sledi da je $q < p^2$, a iz uslova $q > \sqrt[3]{pq}$ sledi da je $q > \sqrt{p}$, što možemo zanemariti zbog uslova $p < q$. Dakle, funkciju $B(n)$ možemo zapisati kao sumiranje po prostim p i q tako da važe pomenuti uslovi:

$$B(n) = \sum_{p=1}^{n} \sum_{\substack{q<p^2 \\ q\ge p \\ q\le \frac{n}{p}}} 1 = \sum_{p=1}^{n} \left(\sum_{\substack{q<p^2 \\ q\le \frac{n}{p}}} 1 - \sum_{\substack{q<p \\ q\le \frac{n}{p}}} 1 \right)$$

Da bi se izračunala verovatnoća tačnosti pomenute teoreme potrebno je odrediti asimptotsko ponašanje funkcije $B(n)$, što smo sveli na problem izračunavanja datih suma. Kako ne znamo da iskontrolišemo ponašanje ovog izraza, ne znamo ni da izračunamo traženu verovatnoću.

Ojlerova teorema i Mala Fermaova teorema

U datoj teoremi ideja je bila izračunati verovatnoću tačnosti ako se ona primeni u suprotnom smeru.

Teorema 16 (Ojlerova teorema). Ako su a i m uzajamno prosti brojevi, onda je $a^{\varphi(m)} \equiv 1 \pmod{m}$, pri čemu $\varphi(m)$ predstavlja Ojlerovu funkciju.

Tokom rada na ovom delu projekta zaključeno je da Ojlerova teorema važi u oba smera, odnosno da ako važi da je $a^{\varphi(m)} \equiv 1 \pmod{m}$ onda a i m moraju biti uzajamno prosti, što znači da izračunavanje pomenute verovatnoće nema smisla.

Teorema 17 (Mala Fermaova teorema). Ako je p prost broj i $(a, p) = 1$, onda je $a^{p-1} \equiv 1 \pmod{p}$.

Iako ishod istraživanja prethodne teoreme nije bio pozitivan, to nas je inspirisalo da razmislimo o Maloj Fermaovoj teoremi. Došli smo do zaključka da ima smisla posmatrati verovatnoću da je $k = p - 1$, za neki prost broj p koji ne deli a, ukoliko znamo da je $a^k \equiv 1 \pmod{m}$.

Ideje za dalji rad

Jedna od tema o kojoj može da se razmišlja u ovoj oblasti jeste posmatranje funkcija koje govore o broju t takvom da važi $a^t \equiv 1 \pmod{m}$. Na primer, ako kažemo da se Ojlerova i Karmajklova funkcija poklapaju u nekom broju, koja je verovatnoća da smo u pravu? Ili koja je verovatnoća

da smo u pravu ako kažemo da se Karmajklova funkcija u nekom broju poklapa sa redom tog broja?

Takođe može se razmišljati i o multiplikativnim i totalno multiplikativnim funkcijama. Naime, ako uzmemo neku konkretnu multiplikativnu funkciju, što znači da je $f(ab) = f(a)f(b)$ ako su a i b uzajamno prosti, možemo da ispitujemo verovatnoću da smo u pravu ako kažemo da relacija $f(ab) = f(a)f(b)$ važi za proizvoljno uzete brojeve a i b.

Zaključak

Inspirisani radom Adriana Dudeka (Dudek 2016), u ovom radu bavili smo se izračunavanjem verovatnoće tačnosti teoreme ukoliko izostavimo neki od uslova ili je upotrebimo u suprotnom smeru. Bazirali smo se na netrivijalne teoreme iz teorije brojeva i došli do zaključka da će u svakoj od posmatranih teorema tražena verovatnoća biti jednaka nuli. Takođe dali smo ideje i smernice za dalji rad na ovu temu.

Literatura

Abramowitz M., Stegun I. A. 1964. *Handbook of Mathematical Functions*. Dover Publications

Broughan K. A. 2001. The gcd-sum function. *Journal of Integer Sequences*, **4** (2): 01.2.2.

Dudek A. W. 2016. On the success of mishandling Euclid's lemma. Mathematical Sciences Institute The Australian National University. Dostupno na: https://arxiv.org/pdf/1602.03555.pdf

Đanković G. 2013. *Teorija brojeva*. Beograd: Univerzitet u Beogradu – Matematički fakultet

Gehring F. W., Halmos P. R. 1976. *Introduction to analytic number theory*. Springer

Knuth D. E. 1997. *The Art of Computer Programming*. Stanford University

Selberg A. 1949. An elementary proof of Dirichlet's theorem about primes in an arithmetic progression. *Annals of Mathematics*, **50** (2): 297.

Ana Petrović and Milica Maksimović

Probability of Success if We Wrongly Interpret a Theorem

The idea of the project is based on probability testing of the truth of some theorem if we omit one of the conditions or use the opposite implication. All the theorems that we studied were in the area of mathematics called number theory. In the first part of the paper we introduced the necessary terms, claims and asymptotic formulas of some functions. Also, the term probability, which is applied to sets with infinitely many elements like integers, rational and natural numbers, was explained. In the second part of the paper we looked at some non-trivial theorems from number theory and came to the conclusion that in every observed theorem the researched probability will be equal to zero. In the third part we presented unfinished calculations of the researched probabilities as well as ideas and directives for further research.