PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **21** (1993/1994)
Številka 5
Strani 264–271

Ivan Vidav:

# TEORIJA ŠTEVIL IN VERJETNOSTNI RAČUN

Ključne besede: matematika, verjetnostni račun, naravna števila.

Elektronska verzija: http://www.presek.si/21/1186-Vidav.pdf

# TEORIJA ŠTEVIL IN VERJETNOSTNI RAČUN

Teorija števil je veja matematike, ki proučuje lastnosti naravnih števil. Na prvi pogled se zdi, da ne more imeti nobene zveze z verjetnostnim računom, ki določa verjetnosti raznim slučajnim dogodkom. Povezavo najdemo, če nekatere trditve teorije števil izrazimo v jeziku verjetnostnega računa. Namen tega članka je, da si ogledamo nekaj takih primerov.

Najprej si zastavimo vprašanje: Na slepo izberemo naravno število $n$. Kolikšna je verjetnost, da je liho? Pri tem seveda privzamemo, da ima vsako naravno število, naj bo majhno ali veliko, isto verjetnost, da ga izberemo. Ker je polovica števil lihih in polovica sodih, bo vsakdo takoj odgovoril, da je iskana verjetnost $\frac{1}{2}$. Težava je v tem, da je naravnih števil neskončno. Na loteriji žrebajo številke iz neke končne množice številk. Verjetnost, da bo izbrana številka liha, izračunamo tako, da delimo število lihih številk s številom vseh številk iz množice številk, ki pridejo v poštev za žrebanje.

Naj bo $L$ lastnost, ki jo nekatera naravna števila imajo, druga ne. Lihost, deljivost s 5, biti praštevilo so primeri takih lastnosti. Poskušajmo opredeliti verjetnost, da ima na slepo izbrano naravno število lastnost $L$. V ta namen vzemimo poljubno naravno število $N$ in preštejmo, koliko je od 1 do $N$ števil z lastnostjo $L$. Denimo, da jih je $M$. Potem je kvocient med številom $M$ ugodnih možnosti in številom $N$ vseh možnosti enak verjetnosti $v_N$, da ima lastnost $L$ število, ki ga na slepo izberemo izmed števil od 1 od $N$. Torej

$$v_N = \frac{M}{N}. \tag{1}$$

Za različne $N$ je verjetnost $v_N$ tudi pri isti lastnosti $L$ v splošnem različna. Večajmo zdaj $N$ čez vse meje! Lahko se zgodi, da obstaja tako število $v$, da se $v$ in $v_N$ razlikujeta za tako malo, kakor želimo, brž ko je $N$ dovolj velik. V tem primeru pravimo, da zaporedje s členi $v_N$ konvergira proti $v$, ko gre $N$ čez vse meje; število $v$ pa imenujemo limita našega zaporedja. Z limito $v$ opredelimo verjetnost, da ima na slepo izbrano naravno število lastnost $L$, če ne postavimo nobene omejitve glede velikosti izbranega števila.

Oglejmo si zdaj nekaj zgledov:

**1. Kolikšna je verjetnost, da je na slepo izbrano naravno število deljivo z $a$, kjer je $a$ dano naravno število?**

Izberimo poljuben $N$ in ga delimo z $a$. Delitev se v splošnem ne izide, tako da dobimo kvocient $q$ in še ostanek $o$, ki je manjši od delitelja $a$. Če smo prav delili, velja enakost

$$N = qa + o, \quad 0 \leq o < a. \tag{2}$$

Do $N$ je $q$ števil deljivih z $a$, namreč $a, 2a, \ldots, qa$. Naslednji večkratnik $(q+1)a$ je večji od $N$, ker je $(q+1)a = qa + a > qa + o = N$. Zato je v našem primeru $M = q$. Kvocient $v_N = \frac{M}{N} = \frac{q}{N}$ zapišimo v obliki

$$v_N = \frac{qa}{Na} = \frac{N-o}{Na} = \frac{1}{a} - \frac{o}{Na}.$$

Po enačbi (2) je namreč $qa = N - o$. Ker je $o < a$, je člen $\frac{o}{Na}$ na desni manjši od $\frac{1}{N}$. Toda $\frac{1}{N}$ je tako majhno število, kakor želimo, če je le $N$ dovolj velik. Zato se kvocient $v_N = \frac{M}{N}$ v našem primeru približuje vrednosti $\frac{1}{a}$, ko gre $N$ v neskončnost, to se pravi, da ima limito $\frac{1}{a}$. Torej je verjetnost, da je na slepo izbrano naravno število deljivo z $a$, enaka $\frac{1}{a}$.

Verjetnost, da na slepo izbrano naravno število ni deljivo z $a$, pa je seveda enaka $1 - \frac{1}{a}$.

Navedena naloga je preprosta. Rešitev lahko takoj uganemo, če pomislimo, da je v zaporedju naravnih števil vsako $a$-to število deljivo z $a$. Oglejmo si zdaj primer, pri katerem rešitve ne moremo kar tako uganiti.

### 2. Kolikšna je verjetnost, da je na slepo izbrano naravno število praštevilo?

Vemo, da je praštevil neskončno. Odgovor na zastavljeno vprašanje je odvisen od tega, kako na gosto so med naravnimi števili posejana praštevila. Naj bo spet $N$ poljuben. Ponavadi označimo s $\pi(N)$ število praštevil, ki so manjša ali enaka $N$. Torej $M = \pi(N)$. Iz teorije števil je znan izrek, da je kvocient $\frac{\pi(N)}{N}$ tako majhen, kakor želimo, če je le $N$ dovolj velik, to se pravi, da konvergira proti nič. Čeprav dokaz tega dejstva ni zelo zahteven, pa ga vseeno tu ne moremo navesti. Ker je limita kvocienta $\frac{M}{N} = \frac{\pi(N)}{N}$ enaka nič, je verjetnost, da izberemo praštevilo, enaka nič. To pomeni, da so praštevila razmeroma redko posejana med naravnimi števili.

Dogodek, da je izbrano število praštevilo, ima verjetnost nič. Kljub temu to ni nemogoč dogodek, saj praštevila obstajajo in celo neskončno jih je. Če je lastnost $L$ taka, da se z njo odlikuje le končno mnogo naravnih števil, je seveda verjetnost, da ima po naključju izbrano število to lastnost, enaka nič.

**3. Naj bosta $a$ in $b$ dani naravni števili. Kolikšna je verjetnost, da na slepo izbrano naravno število ni deljivo niti z $a$ niti z $b$?**

Zgoraj smo ugotovili, da je verjetnost, da izbrano naravno število ni deljivo z $a$, enaka $1 - \frac{1}{a}$. Verjetnost, da ni deljivo z $b$, pa je $1 - \frac{1}{b}$.

Zaznamujmo z $V$ najmanjši skupni večkratnik števil $a$ in $b$. Spomnimo se, da je vsako naravno število, ki je deljivo z $a$ in z $b$, deljivo tudi z najmanjšim skupnim večkratnikom $V$. Izberimo si spet poljuben $N$ in ga delimo z $a$, z $b$ in z $V$. Naj bo pri delitvi z $a$ kvocient $q$ in ostanek $o$, pri delitvi z $b$ kvocient $q'$ in ostanek $o'$, pri delitvi z $V$ pa kvocient $q''$ in ostanek $o''$. Potem veljajo enačbe

$$N = qa + o, \quad N = q'b + o', \quad N = q''V + o''. \tag{3}$$

Vsi ostanki so nenegativni in manjši od ustreznega delitelja, torej $o < a$, $o' < b$, $o'' < V$.

Preštejmo zdaj, koliko je do $N$ števil, ki niso deljiva niti z $a$ niti z $b$. Najprej prečrtajmo v zaporedju $1, 2, 3, \ldots, N$ tista števila, ki so deljiva z $a$. Teh je $q$ (glej dokazovanje pri prvi nalogi). Nato še tista, ki so deljiva z $b$. Ker je $N = q'b + o'$, je teh $q'$. Pri tem smo nekatera števila dvakrat prečrtali, namreč vsa, ki so deljiva z $a$ in z $b$. Števila deljiva z $a$ in z $b$ pa so natanko tista, ki so deljiva z najmanjšim skupnim večkratnikom $V$. Ker je $N = q''V + o''$, jih je $q''$, tako da smo $q''$ števil dvakrat prečrtali. Torej $q + q' - q''$ števil med 1 in $N$ smo vsaj enkrat prečrtali. Ta so tista, ki so deljiva z $a$ ali z $b$. Števila, ki jih nismo prečrtali, pa niso deljiva niti z $a$ niti z $b$. Le-teh je potemtakem

$$N - q - q' + q'' = M.$$

Izračunajmo zdaj iz enačb (3) kvociente $q, q'$ in $q''$. Verjetnost $v_N = \frac{M}{N}$ lahko izrazimo takole:

$$v_N = \frac{M}{N} = 1 - \frac{1}{a} - \frac{1}{b} + \frac{1}{V} + \frac{1}{N}\left(\frac{o}{a} + \frac{o'}{b} - \frac{o''}{V}\right). \tag{4}$$

Ker velja $0 \leq o < a, 0 \leq o' < b, 0 \leq o'' < V$, so kvocienti $\frac{o}{a}$, $\frac{o'}{b}$ in $\frac{o''}{V}$ nenegativni in vsi manjši od 1. Zato je zadnji člen na desni v (4) po absolutni vrednosti manjši od $\frac{2}{N}$, prvi štirje pa so neodvisni od $N$. Ko narašča $N$ čez vse meje, postane zadnji člen tako majhen, kakor želimo; gre torej proti nič.

Zato zaporedje $v_N$ konvergira, in sicer proti limiti

$$v = 1 - \frac{1}{a} - \frac{1}{b} + \frac{1}{V}. \tag{5}$$

Limita $v$ je verjetnost, da po naključju izbrano naravno število ni deljivo niti z $a$ niti z $b$. Pri tem pomeni $V$ najmanjši skupni večkratnik števil $a$ in $b$.

Oglejmo si posebni primer, ko sta $a$ in $b$ tuji si števili. Tedaj je najmanjši skupni večkratnik $V$ kar produkt $ab$. Formula (5) se v tem primeru glasi

$$v = 1 - \frac{1}{a} - \frac{1}{b} + \frac{1}{ab}.$$

Zapišemo jo lahko v obliki

$$v = (1 - \frac{1}{a})(1 - \frac{1}{b}). \tag{6}$$

Na desni je prvi faktor $1 - \frac{1}{a}$ verjetnost, da izbrano število ni deljivo z $a$, drugi $1 - \frac{1}{b}$ pa verjetnost, da ni deljivo z $b$. Torej pri tujih si $a$ in $b$ izračunamo verjetnost, da izbrano število ni deljivo niti z $a$ niti z $b$ tako, da enostavno pomnožimo verjetnost, da ni deljivo z $a$, z verjetnostjo, da ni deljivo z $b$.

V verjetnostnem računu velja pravilo o množenju verjetnosti tedaj, kadar so dogodki med seboj neodvisni. Če igramo na primer na dve loteriji, je seveda dogodek, da zadenemo glavni dobitek na prvi, neodvisen od dogodka, da ga zadenemo na drugi. Zato je verjetnost, da zadenemo glavni dobitek na obeh loterijah, enaka produktu $v_1 v_2$, kjer je $v_1$ verjetnost, da zadenemo glavni dobitek na prvi loteriji, in $v_2$ verjetnost, da ga zadenemo na drugi. Tudi v zgornjem primeru smo množili verjetnosti. Dogodek, da izbrano število ni deljivo z $a$, se vede potemtakem, kakor da je neodvisen od dogodka, da število ni deljivo z $b$. To velja pri tujih si $a$ in $b$.

Če vzamemo namesto dveh tri naravna števila $a$, $b$ in $c$, izračunamo na podoben način verjetnost, da naključno izbrano naravno število ni deljivo niti z $a$ niti z $b$ niti s $c$. Račun je precej dolgovezen in formula za verjetnost zapletena, zato je ne bomo navajali. Oglejmo si samo primer, ko so števila $a, b, c$ paroma tuja. V tem primeru verjetnosti spet množimo: Verjetnost $v$, da izbrano število ni deljivo niti z $a$ niti z $b$ niti s $c$, je enaka produktu verjetnosti, da ni deljivo s posameznimi števili, torej

$$v = (1 - \frac{1}{a})(1 - \frac{1}{b})(1 - \frac{1}{c}).$$

Za zgled vzemimo za $a, b, c$ prva tri praštevila 2, 3 in 5. Verjetnost, da po naključju izbrano naravno število ni deljivo niti z 2 niti s 3 niti s 5, je enaka

$$v = (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = \frac{4}{15}.$$

Če se spomnimo, kako smo opredelili verjetnost, lahko rečemo, da štiri petnajstine naravnih števil ni deljivih niti z 2 niti s 3 niti s 5.

Pravilo, da pri dveh in treh tujih deliteljih verjetnosti množimo, velja tudi za poljubno končno množico paroma tujih si števil $a, b, \ldots, k$. Verjetnost, da naključno izbrano naravno število ni deljivo z nobenim številom iz navedene množice, je enako produktu verjetnosti, da ni deljivo s posameznimi števili te množice.

\- - -

Oglejmo si na koncu še dve zahtevnejši nalogi. Preden navedemo prvo, povejmo tole: Naravno število je brez kvadratnih deliteljev ali faktorjev, kadar ni deljivo z nobenim kvadratom večjim od 1. Tako so npr. števila 6, 10, 15 brez kvadratnih faktorjev. Število 6 ima delitelje 1, 2, 3, in 6; nobeden izmed njih ni kvadrat, večji od 1. Pač pa imajo 8, 12 in 18 kvadratne faktorje. Prvi dve števili sta namreč deljivi s $4 = 2^2$, tretje pa z $9 = 3^2$. Število $n$ je brez kvadratnih faktorjev natanko takrat, kadar je produkt samih različnih praštevil (oziroma je praštevilo ali 1). Če nastopa namreč v razcepitvi števila $n$ na prafaktorje kakšno praštevilo $p$ večkrat kot faktor, je $n$ deljiv s $p^2$, torej ima kvadratni faktor. Obratno je tudi res: Naj bo $n$ deljiv s kvadratom $k^2$, kjer je naravno število $k$ večje od 1. Ker je $k$ deljiv vsaj z enim praštevilom $p$, je potem $n$ deljiv s $p^2$ in v razcepitvi števila $n$ nastopa prafaktor $p$ najmanj dvakrat.

Zdaj pa k nalogi!

### 4. Kolikšna je verjetnost, da je na slepo izbrano naravno število brez kvadratnih deliteljev?

Pravkar smo ugotovili, da je naravno število brez kvadratnih faktorjev natanko takrat, kadar ni deljivo s kvadratom nobenega praštevila, torej kadar ni deljivo niti z $2^2$ niti s $3^2$ niti s $5^2$ itd. Verjetnost, da izbrano število $n$ ni deljivo z $a$, je $1 - \frac{1}{a}$. Kvadrati med seboj različnih praštevil so paroma tuja si števila. Zato dobimo verjetnost, da $n$ ni deljiv niti z $2^2$ niti s $3^2$ itd. tako, da pomnožimo verjetnost, da ni deljiv z $2^2$, z verjetnostjo, da ni deljiv s $3^2$, itd. Verjetnost $v$, da je izbrano število $n$ brez kvadratnih faktorjev, se

potemtakem izraža takole

$$v = (1 - \frac{1}{2^2})(1 - \frac{1}{3^2})(1 - \frac{1}{5^2})\ldots \qquad (7)$$

Na desni teče produkt po vseh praštevilih. Toda, ojoj, praštevil je neskončno in je zato v tem produktu neskončno faktorjev. Neskončno faktorjev pa ne moremo zmnožiti, niti z najhitrejšim računalnikom ne. Kakšen pomen ima potem izraz na desni v (7)?

Pomnožimo najprej prva dva faktorja, nato dobljeni produkt s tretjim faktorjem, potem novi rezultat s četrtim itd. Dobimo zaporedje delnih produktov

$$1 - \frac{1}{2^2},\ (1 - \frac{1}{2^2})(1 - \frac{1}{3^2}),\ (1 - \frac{1}{2^2})(1 - \frac{1}{3^2})(1 - \frac{1}{5^2}),\ldots$$

Vsi faktorji so pozitivni in manjši od 1. Zato so členi v tem zaporedju delnih produktov pozitivni in se manjšajo. Vedno bolj se približujejo nekemu številu, ki je spodnja meja tega zaporedja, in sicer največja spodnja meja. To pomeni, da zaporedje delnih produktov konvergira. Limito $v$ imenujemo vrednost neskončnega produkta (7). Limita $v$, ki je v našem primeru največja spodnja meja, je lahko pozitivna ali nič. Izkaže se, da je za produkt (7) pozitivna. Limita $v$ je verjetnost, da je na slepo izbrano naravno število brez kvadratnih deliteljev.

Kolikšna je vrednost produkta (7)? Izračunal jo je že Euler, in sicer je ugotovil, da znaša $\frac{6}{\pi^2}$. Tu ne moremo razlagati, kako je Euler prišel do rezultata. Povemo lahko samo to, da je njegova pot zelo zanimiva.

Odgovor na četrto vprašanje se potemtakem glasi:

**Verjetnost, da je na slepo izbrano naravno število brez kvadratnih deliteljev, je $\frac{6}{\pi^2}$.**

Naše dokazovanje, da je iskana verjetnost enaka produktu (7), seveda ni povsem neoporečno, saj nismo dokazali pravila o množenju verjetnosti za primer, ko imamo neskončno množico paroma tujih si števil. Vendar v matematiki pogosto pridemo do kakšnega rezultata najprej po poti, ki ni povsem zanesljiva, in potem, ko rezultat že poznamo, poskušamo najti zanj neoporečno utemeljitev. To v našem primeru gre, le neoporečen dokaz, da je iskana verjetnost $\frac{6}{\pi^2}$, je dosti bolj zapleten. Povejmo, da je tudi Euler izračunal vrednost produkta (7) na način, ki z današnjega stališča ni neoporečen.

V produktu (7) nastopajo kvadrati praštevil. Oglejmo si podoben produkt

$$(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})\ldots, \tag{8}$$

ki tudi teče po vseh praštevilih. Faktor $1-\frac{1}{p}$ pomeni verjetnost, da po naključju izbrano naravno število ni deljivo s $p$. Neskončni produkt (8) lahko potem tolmačimo kot verjetnost, da izbrano število ni deljivo z nobenim praštevilom. Toda edino naravno število, ki ni deljivo z nobenim praštevilom, je 1 in verjetnost, da v neskončni množici naravnih števil izberemo ravno število 1, je enaka nič. Res se izkaže, da je vrednost produkta (8) enaka nič: Zaporedni delni produkti postanejo sčasoma poljubno majhni, konvergirajo proti nič.

Na koncu obravnavajmo še eno nalogo, ki pa je za spoznanje različna od dosedanjih.

### 5. Na slepo izberemo dve naravni števili. Kolikšna je verjetnost, da sta si tuji?

Števili $m$ in $n$ sta si tuji natanko tedaj, kadar ni praštevila, ki bi delilo obe. Če si namreč $m$ in $n$ nista tuja, imata kak skupni delitelj $k$, ki je večji od 1. Zato je $k$ deljiv vsaj z enim praštevilom $p$ in s tem $p$ sta deljiva tudi $m$ in $n$. Če pa, obratno, obstaja praštevilo $p$, ki deli $m$ in $n$, potem si $m$ in $n$ nista tuja.

Kadar na slepo izberemo dve naravni števili $m$ in $n$, je dogodek, da je število $m$ deljivo z $a$, neodvisen od dogodka, da je število $n$ deljivo z $a$. Ker je verjetnost obeh dogodkov $\frac{1}{a}$, je verjetnost, da sta $m$ in $n$ oba deljiva z $a$, enaka produktu obeh verjetnosti, torej $\frac{1}{a}\cdot\frac{1}{a}=\frac{1}{a^2}$. Verjetnost, da nista oba deljiva z $a$, pa je potem $1-\frac{1}{a^2}$. Brez dokaza povejmo, da je verjetnost, da $m$ in $n$ nista oba deljiva niti z $a$ niti z $b$ pri tujih si $a$ in $b$, enaka produktu verjetnosti, da nista oba deljiva z $a$ in verjetnosti, da nista oba deljiva z $b$. (To se pravi, da se dogodek, da $m$ in $n$ nista oba deljiva z $a$, vede, kakor da je neodvisen od dogodka, da nista $m$ in $n$ oba deljiva z $b$.) To pravilo velja tudi v primeru, ko imamo več paroma tujih si števil.

Zgoraj smo ugotovili, da sta si $m$ in $n$ tuja natanko takrat, kadar ni praštevila, s katerim bi bila oba deljiva. Pripadajoča verjetnost $v$ je zato enaka produktu verjetnosti $1-\frac{1}{2^2}$, da nista oba deljiva z 2, z verjetnostjo

$1 - \frac{1}{3^2}$, da nista oba deljiva s 3, itd. po vseh praštevilih. Torej

$$v = (1 - \frac{1}{2^2})(1 - \frac{1}{3^2})(1 - \frac{1}{5^2}) \ldots$$

To je tudi verjetnost, da sta si na slepo izbrani naravni števili $m$ in $n$ tuji. Produkt na desni je isti kakor v (7) in njegovo vrednost poznamo. Tako smo ugotovili:

**Verjetnost, da sta si na slepo izbrani naravni števili tuji, je $\frac{6}{\pi^2}$.**

Morda je prav, da se ob rešitvah zadnjih dveh nalog nekoliko zamislimo. Povejmo, zakaj.

Znani fizik Eugene Wigner pripoveduje v svojem članku Vloga matematike v naravoslovju [1] zgodbo o statistiku, ki je pokazal svojemu nekdanjemu sošolcu separatni odtis svoje razprave o rasti populacije. Sošolec je listal po odtisu in kar ni mogel verjeti, da nastopajo pri teoretičnem obravnavanju rasti populacije tako zapletene matematične formule. Spraševal je o pomenu raznih simbolov in znakov, med drugim tudi črke $\pi$. Statistik je povedal, da je $\pi$ seveda razmerje med obsegom in premerom kroga. Na to mu je sošolec odvrnil: "Razmerje med obsegom in premerom kroga pa prav gotovo nima nobene zveze z rastjo populacije!"

Če bi nam kdo povedal, preden smo se seznanili z zadnjo nalogo in njeno rešitvijo, da je verjetnost, da sta na slepo izbrani naravni števili tuji, enaka $\frac{6}{\pi^2}$, bi tudi mi lahko podobno kakor statistikov sošolec vzkliknili: "Kako je to mogoče? Saj tujost med naravnimi števili vendar nima nobene zveze z razmerjem med obsegom in premerom kroga!"

V članku smo spoznali, da je to mogoče. Število $\pi$ se res pogosto pojavlja v matematiki in uporabi ter včasih tam, kjer bi ga najmanj pričakovali.

*Ivan Vidav*

[1] Prevod tega članka je izšel v časopisu Obzornik za matematiko in fiziko VIII (1961), str. 145 - 154.