# NEKAJ O TEORIJI ŠTEVIL

Sodobna matematika obsega precej vej, katerih poimenovanje, utrjeno skozi stoletja, ne pove vedno njihove dejanske vsebine. To velja tudi za teorijo števil, eno najstarejših vej matematike, ki je privlačevala pozornost mnogih velikih matematikov skozi preteklih 2300 let. Z njo so se ukvarjali stari Grki, Indijci in Kitajci, hiter razvoj pa je doživela predvsem po Fermatu (1601-1665), enem od največjih francoskih matematikov.

Ime "teorija števil" bi nas lahko privedlo na misel, da je to neke vrste splošna teorija, ki se ukvarja s pojmom števila, teorija torej, ki iz naravnih števil izvede cela, racionalna, realna in kompleksna števila in ki gradi teorijo operacij nad temi števili. Pričakovali bi, da sta npr. znana zakona

$a+b = b+a$ $\qquad a.b = b.a$ komutativnostni zakon

$(a+b)+c = a+(b+c)$ $\qquad (a.b).c = a.(b.c)$ asociativnostni zakon,

ki veljata za seštevanje in množenje vseh naštetih vrst števil, produkta teorije števil. Toda to ni tako. Teorija števil se zanima za lastnosti celih števil

$$\ldots -3, -2, -1, 0, 1, 2, 3, \ldots$$

Pri tem privzame pojem celega števila in teorijo operacij nad temi števili za znana. Pri svojih raziskovanjih lastnosti celih števil pa s pridom uporablja tudi realna in kompleksna števila in nemalokrat poseže v druge veje matematike, kot sta npr. analiza in algebra.

Najlaže opišemo teorijo števil tako, da navedemo več problemov, ki sodijo v teorijo. Da je naštevanje problemov čim bolj urejeno, jih razdelimo glede na njihovo naravo v štiri skupine. Ti ne zajamejo vsega, kar teorija števil obravnava, vtis o njej pa bomo vendarle dobili.

Najprej so tu multiplikativni problemi, ki obravnavajo deljivost celih števil. V to skupino spada eden najosnovnejših in najpomembnejših izrekov v teoriji števil, včasih imenovan "osnovni izrek teorije števil", ki pravi:

Vsako pozitivno celo število n, ki je večje od 1, se da enolično zapisati kot produkt praštevil, če se ne oziramo na vrstni red faktorjev. Pri tem je praštevilo vsako celo število večje od

1, ki je deljivo samo z 1 in s samim seboj, če upoštevamo samo pozitivne delitelje.

Uporabnost tega izreka v teoriji števil je izredno velika. Iz razstavitve števila n na produkt praštevil lahko določimo število pozitivnih deliteljev števila n. To število označimo z $d(n)$. Različna števila imajo v splošnem seveda različno mnogo deliteljev in zato z oznako $d(n)$ nakažemo, da je število deliteljev d odvisno od n. Pravimo, da je število d funkcija števila n. Zdaj si lahko zastavimo razna vprašanja o vrednosti $d(n)$. Ali z večanjem števila n tudi $d(n)$ ves čas narašča, ali doseže poljubno velike vrednosti, ali zavzame kakšno vrednost večkrat in podobno. Na našteta vprašanja je kaj lahko odgovoriti, a preden se lotimo odgovorov, podajmo s tabelo prvih nekaj vrednosti funkcije $d(n)$:

| $n$ | $d(n)$ | $n$ | $d(n)$ |
|---|---|---|---|
| 1 | 1 | 13 | 2 |
| 2 | 2 | 14 | 4 |
| 3 | 2 | 15 | 4 |
| 4 | 3 | 16 | 5 |
| 5 | 2 | 17 | 2 |
| 6 | 4 | 18 | 6 |
| 7 | 2 | 19 | 2 |
| 8 | 4 | 20 | 6 |
| 9 | 3 | 21 | 4 |
| 10 | 4 | 22 | 4 |
| 11 | 2 | 23 | 2 |
| 12 | 6 | 24 | 8 |

Že na prvi pogled je očitno, da je vedenje funkcije $d(n)$ zelo neurejeno. Če je $n = 2^m$, delijo n števila $1,2,2^2,\ldots,2^m$ tako, da je $d(2^m) = m+1$. Če pa je $n$ praštevilo, je seveda $d(n) = 2$. Ker je, kot bomo spoznali, praštevil neskončno, uvidimo, da doseže $d(n)$ poljubno velike vrednosti in obenem vrednost 2 za neskončno mnogo n. S tem smo odgovorili na zastavljena vprašanja, toda ob nadaljnem študiranju tabele se hitro zastavijo nova:

a) Ali je zares $d(n)$ liho samo takrat, kadar je n kvadrat?
b) Ali velja $d(m).d(n) = d(m.n)$, če m in n nimata skupnega faktorja?
c) Kolikšna je povprečna vrednost $d(n)$, se pravi, kaj lahko pove-

mo o $(d(1) + d(2) + \ldots + d(N))/N$, ko $N$ narašča čez vsako mejo?

d) Ali zavzame $d(n)$ največje vrednosti pri $n$ z obliko $2^m$ ?

e) Približno koliko je praštevil med $1,2,\ldots,N$ ?

Vsa gornja vprašanja so značilna za multiplikativno teorijo števil. Formulirana so kratko in jasno in marsikdo bi pričakoval, da odgovori nanje niso preveč trd oreh. Toda za matematiko je značilno, da je pogosto težko dokazati ravno preprosto postavljene probleme. Razlog je verjetno delno ta, da tak izrek s svojim besedilom ne da nobenega namiga o pripomočkih, ki naj bi jih rabili pri dokazovanju, deloma pa ta, da ustreznih pripomočkov ne poznamo. V teoriji števil je veliko izrekov takšne vrste in prav to jo dela še posebej privlačno. Na prvo izmed vprašanj je zelo lahko odgovoriti. Naslednja vprašanja so težja, na zadnje vprašanje pa nista uspela popolnoma odgovoriti niti tako velika matematika, kot sta bila C.F. Gauss in A. Legendre, čeprav sta oba slutila rešitev.

Vprašanju dokazov v teoriji števil bomo malo kasneje posvetili še nekaj pozornosti, zdaj pa nadaljujmo z razdelitvijo teorije števil.

V drugo skupino sodijo problemi aditivne teorije števil. Sem spadajo vprašanja predstavljivosti pozitivnih celih števil kot vsote celih števil določenega tipa. Pokaže se, da nekatera cela števila, npr. $5 = 2^2 + 1^2$ in $13 = 2^2 + 3^2$, lahko zapišemo kot vsoto dveh kvadratov, drugih, npr. 3 ali 12, pa ne moremo. Katera cela števila se dajo zapisati kot vsota k-tih potenc in koliko je takšnih zapisov in ali obstaja pri danem $k$ neko takšno število $g(k)$, da vsako celo število lahko zapišemo kot vsoto kvečjemu $g(k)$ k-tih potenc. Ti vprašanji sta tipični za aditivno teorijo števil.

V tretjo skupino bi lahko šteli diofantske enačbe, imenovane po grškem matematiku Diophantu, ki jih je prvi študiral. To so enačbe z eno ali več neznankami, njihove rešitve iščemo med celimi števili. Znano je npr., da je $3^2 + 4^2 = 5^2$, kar nam da rešitev diofantske enačbe $x^2 + y^2 = z^2$. Vendar pa nas pri reševanju manj zanima posamezna (partikularna) rešitev, bolj pa splošna formula za vse rešitve. Zelo znana diofantska enačba je Fermatova enačba: $x^n + y^n = z^n$. Fermat je trdil, da ta enačba nima rešitve, pri kateri bi bili $x$, $y$ in $z$ vsi različni od nič, če je $n \geq 3$; trditev

nikoli ni bila dokazana ali ovržena za vse n. Danes pravzaprav ne moremo govoriti o neki splošni teoriji diofantskih enačb, čeprav obstaja precej specialnih metod, ki so bile večinoma razvite za reševanje določenih enačb.

Diofantske aproksimacije sestavljajo zadnjo skupino. Ta veja teorije števil si najbrž največ izposoja iz drugih vej matematike in jim največ vrača. Zato tukaj o njej ne bomo govorili. Za radovedneže omenimo samo, da spadata v to skupino dokaza o transcendentnosti* števil e in $\pi$.

Teorijo števil bi lahko razdelili tudi drugače, npr. po metodah, ki jih rabimo pri dokazovanju izrekov. Toda bodi dovolj o delitvah, rajši posvetimo še nekaj besed dokazom.

Denimo, da imamo opraviti z večjim številom izrekov, ki govore o istem predmetu, a se njihovi dokazi v bistvu zelo razlikujejo. V tem primeru imamo tehnike pri različnih dokazih za posebne trike, od katerih je vsak uporaben samo pri dokazu tistih izrekov, s katerimi je povezan. Tehnika preneha biti trik in postane metoda šele takrat, ko je uporabljena tolikokrat, da se zdi naravna. Določen predmet imamo lahko za "vrečo trikov", če je število tehnik v primerjavi s številom izrekov preveliko. Žal so elementarno teorijo števil včasih imeli za tak predmet. Z nadaljnim delom na tem področju pa so mnogo trikov združili v metodo: teorija števil je pokazala več enotnosti, kot je sprva kazalo.

Nakažimo na primeru eno od metod dokazovanja, tipičnih za teorijo števil. Poskusimo dokazati trditev, da je $d(n)$ sodo število, če $n$ ni kvadrat kakega celega števila. Dokaz teče takole: če $d$ deli $n$, tudi $n/d$ deli $n$. Če $n$ ni kvadrat, $d \neq n/d$, ker je sicer $n = d^2$. Se pravi, če $n$ ni kvadrat, lahko njegove delitelje združimo v pare $(d, n/d)$ tako, da vsak delitelj števila $n$ nastopa natanko enkrat kot element enega od teh parov. Število deliteljev je torej dvakrat število parov in zato sodo. Bistven element tega dokaza je grupiranje deliteljev števila $n$ v pare. Metoda grupiranja števil v določene skupine je zelo uporabna, kadar hočemo prešteti cela števila z določeno lastnostjo. Seveda pa te skupine niso vedno pari, temveč je treba za posamezen problem te vrste šele odkriti ustrezen način grupiranja.

Veliko je v teoriji števil negativnih trditev, npr. "vsakega

* Število je transcendentno, če pri nobenem naravnem številu $n$ ni rešitev enačbe $x^n + a_1 x^{n-1} + \ldots + a_n = 0$; $a_i$ so cela števila.

pozitivnega celega števila ne moremo izraziti kot vsoto treh kvadratov". Takšne trditve zahtevajo od nas samo to, da najdemo en sam primer. Za navedeno trditev je to npr. število 7. Na drugi strani pa pozitivne trditve, kot je "vsako pozitivno celo število se da izraziti kot vsota štirih kvadratov", ne moremo dokazati s primeri, naj bodo ti še tako številni.

Poleg specialnih metod se v teoriji števil velikokrat srečamo z dvema zelo splošnima tipoma dokazov: dokaz s protislovjem in dokaz z indukcijo. O dokazih z indukcijo je bralec že slišal v šoli ali pa še bo ali pa je prebral kakšen članek, ki govori samo o tem. Zato tukaj o indukciji ne bomo govorili. Pač pa na primeru ilustrirajmo dokaz s protislovjem.

Pravimo, da smo trditev $P$ dokazali s protislovjem, če smo iz predpostavke, da je $P$ napačna, izpeljali trditev $Q$, za katero vemo, da je napačna ali da $Q$ nasprotuje predpostavki o nepravilnosti $P$. Za primer dokažimo trditev, da je praštevil neskončno mnogo. Poskusimo torej iz nasprotne trditve priti do protislovja. Predpostavimo, da je praštevil končno. Naj bodo to $p_1, p_2, \ldots, p_k$. Tvorimo število $N = p_1 p_2 \cdots p_k + 1$. Število $N$ je ali praštevilo ali sestavljeno število. Če je $N$ praštevilo, smo že prišli do protislovja, saj je $N$ večje od vseh praštevil med $p_1, p_2, \ldots, p_k$. Če pa je $N$ sestavljeno število, je gotovo deljivo z nekim praštevilom $p$. Vendar $N$ ni deljivo z nobenim od praštevil $p_1, p_2, \ldots, p_k$, saj je ostanek pri deljenju s temi praštevili vedno enak 1. Praštevilo $p$ torej ne more biti enako nobenemu praštevilu med $p_1, p_2, \ldots, p_k$. Zopet smo prišli do protislovja in tako dokazali, da je praštevil neskončno.

Omenimo na koncu še tri lastnosti naravnih ali pozitivnih celih števil, ki jih v teoriji števil večkrat uporabljamo:

1. Vsaka neprazna množica naravnih števil ima najmanjši element.
2. Če sta $a$ in $b$ naravni števili, obstaja naravno število $n$ tako, da je $na > b$.
3. Naj bo $n$ naravno število. Če razdelimo množico iz $n+1$ elementov v $n$ ali manj podmnožic tako, da vsak element spada v natanko eno podmnožico, vsaj ena podmnožica vsebuje več kot en element.

Vse tri lastnosti so posledice aksiomov, ki jih je za naravna števila postavil Peano in jih v teoriji števil privzamemo brez dokaza.

NALOGE:

1. Pokaži, da je $d(n)$ liho, če je $n$ kvadrat!
2. Ali je 2 edina vrednost, ki jo $d(n)$ zavzame neskončno mnogokrat?
3. Koliko členov je najmanj potrebnih za zapis števila $2^k-1$ kot vsote $k$-tih potenc?
4. Pokažemo lahko, da se da vsako celo število zapisati v obliki $6k+r$, kjer je $k$ neko celo število, $r$ pa eno od števil 0,1,2, 3,4,5. Pokaži
   a) če je $p= 6k+r$ praštevilo različno od 2 in 3, potem je $r=1$ ali 5;
   b) da je produkt števil oblike $6k+1$ spet število take oblike;
   c) da obstaja praštevilo oblike $6k-1 = 6(k-1)+5$;
   d) da obstaja neskončno mnogo praštevil oblike $6k-1$.

*Janez Stare*