PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **12** (1984/1985)
Številka 5
Strani 229–232

Joso Vukman:

O NEKATERIH NEREŠENIH PROBLEMIH IZ TEORIJE ŠTEVIL

Ključne besede: matematika, teorija števil.

Elektronska verzija: http://www.presek.si/12/763-Vukman.pdf

O NEKATERIH NEREŠENIH PROBLEMIH IZ TEORIJE ŠTEVIL

Znanost se izredno hitro razvija, saj skoraj ne mine dan, da ne bi zvedeli za kako pomembno znanstveno odkritje. Ali bo znanost sčasoma našla odgovore na vse probleme, ki jih danes še ne znamo rešiti? Težko si je predstavljati, da se bomo kdaj dokopali do dokončnih spoznanj, saj se nam z razširitvijo enega problema običajno pojavi vrsta novih. Tudi matematika je v zadnjih stoletjih napredovala z velikimi koraki, njen razvoj v zadnjih desetletjih pa je tak, da danes ni več matematika, ki bi se lahko pohvalil, da obvlada vso matematiko. Toda kljub neslutenemu razvoju obstajajo več sto in celo več tisoč let stari matematični problemi, ki še vedno čakajo na rešitev. Na tovrstve probleme naletimo pogosto v teoriji števil, veji matematike, ki proučuje lastnosti naravnih oziroma celih števil. V tem sestavku si bomo ogledali nekatere nerešene probleme iz teorije števil, ki so po svoji formulaciji preprosti in lahko razumljivi, njihove rešitve pa so tako zahtevne, da jim največji matematiki niso kos.

GOLDBACHOVA DOMNEVA

Goldbach (1690 – 1764) je leta 1742 izrekel naslednjo domnevo:

Vsako sodo število, ki je večje od dva, je vsota dveh praštevil.

Matematiki se že dobrih dvesto let ubadajo s tem problemom, vendar doslej te domneve še nihče ni dokazal ne ovrgel.

MERSENNOVA PRAŠTEVILA

Dokažimo naslednjo trditev:

Naj bo p naravno število. Če je $2^p - 1$ praštevilo, potem je tudi p praštevilo.

Pišimo p v obliki $p = mn$, kjer je n praštevilo. Trditev bo dokazana, če dokažemo, da je $m = 1$. Oglejmo si vsoto $1 + 2^m + 2^{2m} + \ldots + 2^{(n-1)m}$. To je v bistvu vsota prvih n členov geometrijskega zaporedja. Prvi člen tega zaporedja je 1, kvocient zaporedja pa 2^m. Z uporabo formule za vsoto členov geometrijskega zaporedja dobimo $1 + 2^m + 2^{2m} + \ldots + 2^{(n-1)m} = ((2^m)^n - 1)/(2^m - 1)$. Z upoštevanjem $mn = p$ dobimo $2^p - 1 = (2^m - 1)(1 + 2^m + 2^{2m} + \ldots +$

$2^{(n-1)m}$). Število $2^p - 1$ smo torej zapisali v obliki produkta dveh naravnih števil. Ker je $2^p - 1$ praštevilo in je očitno, da je drugi faktor večji od ena, mora biti prvi faktor ena, to pa pomeni, da je $m = 1$.

Dokazali smo torej, da je p praštevilo, če je $2^p - 1$ praštevilo. Samo po sebi se vsiljuje naslednje vprašanje: ali velja ta trditev tudi v nasprotni smeri? Natančneje povedano, ali je vedno $2^p - 1$ praštevilo, če je p praštevilo? Če za p vstavimo zapovrstjo 2, 3 in 5, dobimo 3, 7 in 31, torej praštevila, vendar to še nič česar ne dokazuje. Praštevila oblike $2^p - 1$ imenujemo po matematiku *Mersennu* (1588 – 1648) Mersennova praštevila. Mersenne je vedel, da $2^p - 1$ ni vedno praštevilo, če je p praštevilo, saj je poznal primer $2^{11} - 1 = 2048 - 1 = 23.89$ in še mnogo drugih. S tem pa vsi problemi v zvezi z Mersennovimi praštevili še niso rešeni. Do današnjih dni je namreč ostal odprt problem, ali je Mersennovih praštevil neskončno ali pa samo končno mnogo.

V zvezi z Mersennovimi praštevili povejmo še to, da je Lucas leta 1876 dokazal, da je $2^{127} - 1$ praštevilo. Oglejmo si ta problem podrobneje, da si vsaj približno predočimo, s kakšnimi problemi se srečujejo matematiki, ki rešujejo probleme v teoriji števil. Kako bi ugotovili naravo števila $2^{127} - 1$? Preizkusiti je treba zapovrstjo, ali je to število deljivo s katerim izmed praštevil 3, 5, 7, ... Če ni deljivo z nobenim praštevilom, ki je manjše od $\sqrt{2^{127} - 1}$ (brez posebnih težav se namreč dokaže, da z večjimi praštevili ni potrebno preizkušati), potem je $2^{127} - 1$ praštevilo. V principu je enostavno, praktično pa je ta način neizvedljiv. Število $2^{127} - 1$ ima namreč, zapisano v desetiškem sistemu, 39 mest in opisani postopek bi vzel preveč časa vsakemu računarju, opremljenemu z najsodobnejšim računalnikom. Lucas se je torej moral pri reševanju problema dokopati do ideje, ki je spravila nalogo v okvir računskih zmogljivosti, in v tem je vrednost tega njegovega prispevka v teoriji števil.

PERFEKTNA ŠTEVILA

Obstajajo naravna števila, ki so enaka vsoti vseh svojih deliteljev, manjših od števila samega. Števila s to lastnostjo bomo imenovali perfektna. Perfektni števili sta na primer 6 in 28, saj je $1 + 2 + 3 = 6$, $1 + 2 + 4 + 7 + 14 = 28$. Perfektna števila so poznali že stari Grki. Res je, da so vedeli le za štiri perfektna števila, poleg 6 in 28 še 496 in 8128, vendar je že *Evklid* (3. st. pred. n. št.) dokazal naslednjo trditev:

Naj bo p naravno število. Če je $2^p - 1$ praštevilo, potem je število $2^{p-1}(2^p - 1)$ perfektno.

Euler (1707 – 1783) je Evklidov rezultat dopolnil s tem, da je dokazal verjetnost trditve v nasprotni smeri:

Vsako sodo perfektno število lahko zapišemo v obliki $2^{p-1}(2^p - 1)$, pri čemer je $2^p - 1$ praštevilo.

Obe trditvi skupaj bomo Evklidu in Eulerju na čast imenovali Evklid–Eulerjev izrek. Ker je dokaz tega izreka prezahteven, ga opuščamo. Z Evklid–Eulerjevim izrekom smo torej dobili zvezo med sodimi perfektnimi števili in Mersennovimi praštevili. Kako pa je z lihimi perfektnimi števili? S tem vprašanjem smo spet pri problemu, ki ga doslej še nihče ni rešil. Vsa doslej znana perfektna števila so namreč soda. Ni znano, če liha perfektna števila sploh obstajajo, vendar je matematikom uspelo dokazati naslednje: če obstaja kakšno liho perfektno število, potem je to število zelo veliko. Pa tudi s sodimi perfektnimi števili so še vedno težave. Res je, da jih danes poznamo več, kot so jih poznali Grki, toda še vedno ni znano, če je sodih perfektnih števil neskončno ali samo končno mnogo. Evklid–Eulerjev izrek nam namreč študij sodih perfektnih števil prevede na študij Mersennovih praštevil, zato je problem končnosti oziroma neskončnosti števila sodih perfektnih števil v tesni zvezi s problemom končnosti oziroma neskončnosti Mersennovih praštevil.

PITAGOREJSKE TROJICE IN FERMATOV PROBLEM

Če v pravokotnem trikotniku meri ena kateta 3, druga pa 4 enote, je dolžina hipotenuze 5 enot. O tem nas prepriča Pitagorov izrek, saj je $3^2 + 4^2 = 5^2$. Trikotnik s stranicami 3, 4 in 5 enot so že pred tisočletji uporabljali Egipčani za konstrukcijo pravega kota. Trojici števil 3, 4, 5 pravimo pitagorejska trojica. V splošnem imenujemo pitagorejsko trojico vsako trojico naravnih števil x, y, z, ki ustreza enačbi $x^2 + y^2 = z^2$. Takih pitagorejskih trojic je neskončno mnogo, saj je na dlani, da je pri poljubnem naravnem številu n trojica $3n, 4n, 5n$ tudi pitagorejska. Kaj pa, če vzamemo namesto enačbe $x^2 + y^2 = z^2$ enačbo $x^3 + y^3 = z^3$, ali pa splošno, enačbo $x^n + y^n = z^n$, kjer je eksponent n poljubno naravno število, večje od dva. Ali obstaja tudi v tem primeru trojica naravnih ali pa vsaj trojica od nič različnih celih števil x, y, z, ki reši enačbo? S tem vprašanjem smo že pri slovitem Fermatovem problemu. *Fermat* (1601 – 1665) je namreč trdil, da obstajajo tri od nič različna cela števila x, y, z, ki ustrezajo enačbi $x^n + y^n = z^n$ le v primeru, ko je $n = 2$, za vsa naravna števila, ki so večja od dva, pa takih treh od nič različnih celih števil ni. Na rob neke knjige je Fermat zapisal, da ima dokaz za svojo trditev, vendar ga zaradi premajhnega ro-