PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **21** (1993/1994)
Številka 1
Strani 23–26

Ian Stewart, prevod Marija Vencelj:

# DOKAZ, DOLG TISOČ STRANI, POTRJUJE FERMATA

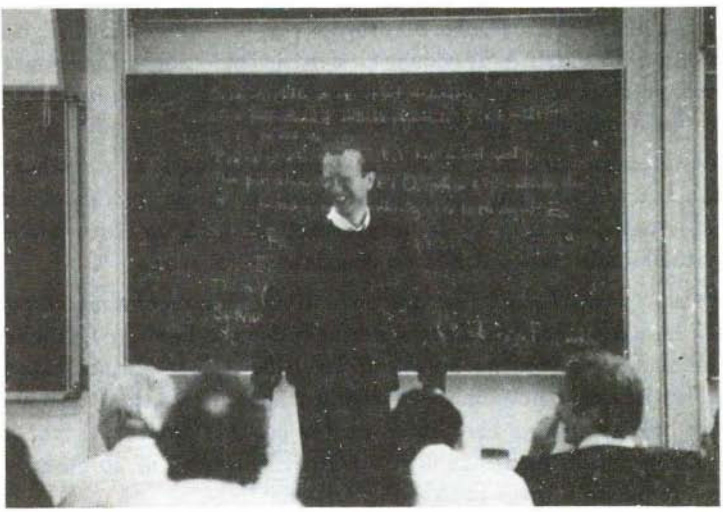
Ključne besede: novice, matematika, teorija števil, Fermatov izrek, eliptične krivulje, Andrew Wiles.

Elektronska verzija:
http://www.presek.si/21/1160-Stewart-Vencelj.pdf

# DOKAZ, DOLG TISOČ STRANI, POTRJUJE FERMATA

Ena največjih poslastic za matematika je odgovoriti na katerega od velikih problemov, ki so zaposlovali in begali največje učenjake več stoletij. Številni problemi te vrste se imenujejo po njihovih avtorjih, npr.: Riemannova hipoteza, Poincaréjeva domneva, Keplerjev problem. Eden najtrdovratnejših je gotovo Fermatov zadnji izrek, ki se je upiral največjim matematikom več kot 350 let.

Zadnji ponedeljek letošnjega junija pa je na konferenci v Angliji Andrew Wiles z univerze Princeton najavil svoj 1000 strani dolg dokaz o veljavnosti Fermatovega izreka. To se je zgodilo ob koncu njegovega predavanja z naslovom Modulske forme, eliptične krivulje in Galoisove reprezentacije. Toda nabito polna predavalnica na matematičnem inštitutu Isaaca Newtona v Cambridgu je kazala, da poslušalci slutijo, da se za naslovom skriva več, da ima Wiles skritega Fermata v rokavu. Imeli so prav.



Andrew Wiles je napravil na poslušalce izjemen vtis, toda dokaz je treba še preveriti.

Pierre de Fermat (1601-1665) je bil francoski odvetnik, katerega konjiček je bila matematika. Stoletje pred Newtonom je izdelal številne osnovne ideje infinitezimalnega računa. Najpomembnejši pa so njegovi dosežki v teoriji števil, matematični veji, ki se ukvarja z lastnostmi celih števil. To je eno najzahtevnejših matematičnih področij, kjer se do domnev in številnih vzorcev zlahka dokopljemo, dokazi pa so pogosto težko razumljivi.

Fermatov zadnji izrek – tako se imenuje zato, ker je bila to dolga leta edina njegova trditev, ki je nihče ni uspel niti dokazati niti ovreči – je ena takih domnev. Že stari Grki so vedeli, da obstaja neskončno mnogo takih trojic celih števil, da daljice ustreznih dolžin tvorijo stranice pravokotnega trikotnika. Pitagorov izrek nam pove, da morajo taka števila $x$, $y$, $z$ ustrezati enačbi $x^2 + y^2 = z^2$. Splošno znana sta primera $3^2 + 4^2 = 5^2$ in $5^2 + 12^2 = 13^2$. Fermat se je vprašal, ali lahko slična zveza velja za kube, četrte potence itd. Bil je prepričan, da ne. Na rob svoje kopije Diofantove knjige *Arithmetica* je zapisal: 'Ni mogoče razstaviti kuba v vsoto dveh kubov ali bikvadrata v vsoto dveh bikvadratov. Sploh ni mogoče razstaviti nobene potence, večje od kvadrata, v vsoto dveh potenc iste stopnje. Za to sem našel res čudovit dokaz. Rob knjige je preozek, da bi ga zapisal."

Fermat je trdil, da enačba $x^n + y^n = z^n$ za $n \geq 3$ nima celih rešitev razen trivialne, v kateri je eno od števil $x$, $y$, $z$ enako nič. Dolgo časa je bila ta domneva videti le zgodovinska zanimivost – zunaj čiste matematike nima nobene direktne uporabe – toda vprašanje je bilo tako preprosto, da je matematike neustavljivo privlačevalo.

Fermatovega 'čudovitega' dokaza niso nikdar našli in v splošnem velja prepričanje, da je v tistem, kar je imel Fermat za dokaz, morala biti napaka. Težko si je tudi predstavljati, da bi matematična sredstva, ki so bila na voljo v Fermatovih časih, lahko vodila do dokaza.

Preteklo je več kot 200 let preden je Ernst Kummer[1] napravil prvi večji prodor v teorem. Razvil je idejo o možnem dokazu Fermatovega izreka, pri čemer je uvedel algebraična števila, ki so veliko splošnejša kot cela števila. Potem, ko je razvil povsem novo teorijo tako imenovanih idealov, je bil sposoben dokazati, da je Fermatova trditev pravilna za vsak eksponent $n \leq$ $\leq 100$, razen morda za 37, 59 in 67. Kasnejši matematiki so odstranili tudi te izjeme in potisnili mejo za eksponent tja do 150 000.

[1] V 5. številki lanskega letnika Preseka je izšel prispevek prof. Jožeta Grassellija ob stoletnici smrti tega velikega nemškega matematika.

Vmes je leta 1922 angleški matematik Leo Mordell postavil drugo, veliko abstraktnejšo in splošnejšo domnevo. Ob predpostavki, da je pravilna, bi sledilo, da ima Fermatova enačba za vsak $n \geq 3$ kvečjemu končno mnogo različnih rešitev. Končno število rešitev sicer res ni isto kot nobena rešitev, toda problem je bil s tem zelo zožen. Mordellova ideja je bila v tem, da mora obstajati povezava med celoštevilskimi rešitvami enačbe in rešitvami s kompleksnimi števili. Ker pa je veliko laže obravnavati rešljivost enačb v kompleksnem, je njegova domneva odprla široko pot za globlje raziskave.

Sprva očitnost Mordellove domneve ni bila ravno prepričljiva, toda Mordellova intuicija je bila potrjena, ko je leta 1983 nemški matematik Gerd Faltings Mordellovo domnevo dokazal. V dokazu je uporabil močne nove metode algebraične geometrije. Kmalu za tem je D. R. Heath-Brown dokazal, da Fermatov zadnji teorem velja za 'skoraj vse' eksponente. Če obstajajo kakšni izjemni eksponenti $n$, za katere ima enačba rešitev, potem se take vrednosti izredno redčijo, ko $n$ narašča.

Med letoma 1780 in 1990 so matematiki s področja algebraične geometrije in algebraične teorije števil čedalje bolj stiskali mrežo okoli Fermatovega teorema. Izkazalo se je, da če so pravilne neke druge, močnejše, splošnejše in celo zelo verjetne domneve, potem je veljaven tudi Fermatov izrek. Te domneve so postavile v ospredje zelo zanimivo področje teorije števil, imenovano eliptične krivulje (ki imajo, kljub imenu, le bežno zvezo z elipsami)[2]. Jean-Pierre Serre, vodilni francoski matematik, je bil prepričan, da je dokaz blizu. Leta 1990 je v popravljeni in dopolnjeni izdaji knjige Erica Templa Bella *Zadnji problem* Undervood Dudley zapisal: "Najbrž smo na robu dokaza." Toda kljub številnim silnim napadom algebraične teorije števil je teorem še nekaj časa vzdržal. Sedaj pa je videti, da je Andrew Wiles končno zapečatil njegovo usodo, ko ga je izpeljal kot poseben primer Shimura-Taniyama-Weilove domneve, gradeč na rezultatih Gerharda Freya iz Saarbrückna.

Ob vsaki proglasitvi dokaza kake od velikih domnev, strokovnjaki tistega področja podrobno razčlenijo vsako vrstico dokaza, da bi bili gotovi, da ni prišlo do kakšne pojmovne ali računske napake. To je dolgotrajen posel in dokler ne bo opravljen, ne bomo vedeli, ali je Fermatov izrek res dokazan.

---

[2] Pri Komisiji za tisk DMFA S je leta 1991 izšla knjiga prof. Ivana Vidava: *Eliptične krivulje in eliptične funkcije. Avtor v predgovoru pravi, da sta prvi dve poglavji, ki sta najbolj elementarni, dostopni boljšim dijakom zadnjega razreda srednjih šol, za razumevanje celotne knjige pa zadošča matematična izobrazba diplomanta kakšne od fakultet, kjer se matematika predava kot pomožni predmet.*

Ima pa Wiles sloves skrbnega in previdnega raziskovalca in splošno mnenje strokovnjakov je, da je njegov dokaz najbrž pravilen.

Andrew Granville, angleški strokovnjak s področja teorije števil, ki dela v ZDA, pravi v *The Guardianu*: To utegne biti korektna pot do vrha. Povzemimo še Italijana Enrica Bombierija, ki je leta 1974 prejel Fieldsovo medaljo (matematičen ekvivalent Nobelove nagrade): "Zgradba celotnega dokaza je zelo strnjena in zelo trdna."

Bombieri je opisal Wilesov dokaz kot 'čudovit'. Povedal pa je, da ga še ne razume v vse detajle, kar ni nobeno presenečenje, glede na to, kako dolg je. Fermat bi resnično potreboval zelo zelo širok rob pri knjigi.

*Ian Stewart, prevedla in priredila Marija Vencelj*

## NA ŠPORTNI DAN K VEGI V ZAGORICO

Če se boste odločili, da za športni dan izberete obisk Vegove domačije v Zagorici, vam zagotovo ne bo žal. Z vlakom do Laz ali Jevnice, lahko pa tudi z avtobusom do Dolskega. Severno od ceste Ljubljana - Litija leži ob