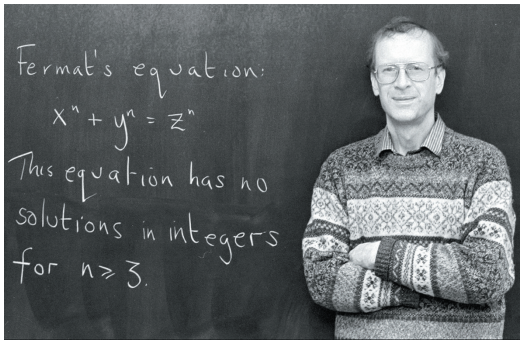
Andrew Wiles dobio Abelovu nagradu

Ivica Gusić[1]

Uvod

Britanski matematičar Andrew Wiles (rođen 1953.) dobio je Abelovu nagradu iz matematike za 2016. godinu, kako je odbor za nagradu istakao "for his stunning proof of Fermat's Last Theorem by way of the modularity conjecture for semistable elliptic curves, opening a new era in number theory" (za njegov zadivljujući dokaz Fermatova posljednjeg teorema preko slutnje o modularnosti polustabilnih eliptičkih krivulja, otvarajući tako novo poglavlje teorije brojeva).



[1] Autor je profesor matematike na Fakultetu kemijskog inženjerstva i tehnologije Sveučilišta u Zagrebu; e-pošta: igusic@fkit.hr

Wiles je 1994., nakon osam godina upornog rada, dokazao Fermatov posljednji teorem: *ne postoje prirodni brojevi X, Y, Z i prirodni broj n veći od 2 tako da bude*

$$X^n + Y^n = Z^n. \tag{1}$$

Dokaz je proizašao kao posljedica dokaza slutnje o modularnosti jedne klase eliptičkih krivulja. Tako je nakon više od 350 godina riješen problem kojeg je postavio francuski matematičar Fermat 1637. (vidi [5], [6]). Wiles je bio prestar da bi mogao dobiti Fieldsovu medalju koja se dodjeljuje matematičarima mlađim od 40 godina za izvanredne doprinose u matematici.

Nema jednostavnog dokaza Fermatova teorema

Abelove lekcije sastavni su dio svečanosti dodjele Abelove nagrade. Godine 2016. uvodnu lekciju, *Fermatov posljednji teorem: abelovi i neabelovi pristupi*, držao je dobitnik Andrew Wiles. Slijedili su ga Henri Darmon s McGill Sveučilišta, Manjul Bhargava s Princetona, a popularnu lekciju *Od Fermatova posljednjeg teorema do Homerova posljednjeg teorema*, održao je britanski popularizator znanosti indijskog podrijetla Simon Singh. Tu nije riječ o starogrčkom slijepom pjesniku, autoru Ilijade i Odiseje, već o liku iz kultne animirane TV-serije *Simpsoni (The Simpsons)*. U jednoj epizodi iz 1995. Homer demonstrira 'jednakost' $1782^{12} + 1841^{12} = 1922^{12}$ u svijetu *Homer na treću*. Naravno, ako bi ta jednakost bila istinita, onda bi Fermatov posljednji teorem bio neistinit, pa tako i Wilesov dokaz. Navodna istinitost potkrijepljuje se vađenjem dvanaestog korijena: $\sqrt[12]{1782^{12} + 1841^{12}} = 1921.99999996$ (na osam decimala). To se od 1922 razlikuje tek za 0.00000004, što se može pripisati greški pri računanju. Danas, nakon više od 20 godina, mogućnosti točnog računanja bitno su napredovale. Tako se online kalkulatorom ([1]) lako dobije $1782^{12} + 1841^{12} - 1922^{12} = -700212234530608691501223040959$: neznatna razlika kod vađenja dvanaestog korijena ovako sagledana postaje ogromna, mjeri se milijardama milijarda milijarda. Tobožnja jednakost može se oboriti bez ikakva računanja, uz malo znanja o parnim i neparnim brojevima, na razini petog razreda osnovne škole. Broj 1782 je paran pa je i njegova dvanaesta potencija paran broj. Nasuprot tome, 1841 je neparan pa je i njegova dvanaesta potencija neparan broj. Zbroj parnog i neparnog broja je neparan pa je lijeva strana jednakosti neparna. Desna strana je parna jer je 1922 paran broj. Kako neparan broj ne može biti jednak parnom, Homerova jednakost je neistinita. Tri godine poslije Homer je izašao s drugim 'protuprimjerom' koji se ne da oboriti ovakvim jednostavnim razmatranjem parnih i neparnih brojeva: $3987^{12} + 4365^{12} = 4472^{12}$. Tu je razlika nakon korjenovanja još neznatnija, 0.000000007, međutim stvarna razlika još je veća. Ni tu nije potrebno računanje da se pokaže kako je jednakost neistinita, već samo razmatranje djeljivosti s 3. Poznato je da je za to dovoljno gledati djeljivost zbroja znamenaka s 3. Kako je $3+9+8+7 = 27$ što je djeljivo s 3, broj 3987 djeljiv je s 3 pa i njegova dvanaesta potencija. Slično vrijedi i za 4365. Zbroj brojeva djeljivih s 3 opet je djeljiv s 3, pa je lijeva strana djeljiva s 3. S druge strane $4+4+7+2 = 17$, što nije djeljivo s 3, pa desna strana nije djeljiva s 3. Kako ne može biti da isti broj i bude i ne bude djeljiv s 3, jednakost je neistinita. Ovi primjeri zorno pokazuju važnost izgradnje i razumijevanja matematičkih pojmova, i kako vrlo jednostavno matematičko rezoniranje može zamijeniti mukotrpno računanje. Govoreći suvremenijim matematičkim jezikom, prva Homerova jednakost razmatrala se modulo 2, a druga modulo 3. Jednakosti modulo 2, odnosno modulo 3 nisu bile istinite pa se zaključilo da su izvorne jednakosti neistinite. Općenito se može, kako za jednakosti cijelih brojeva, tako i za jednadžbe s cijelim

brojevima (diofantske jednadžbe), razmatrati pripadne jednakosti odnosno jednadžbe modulo m, za bilo koji prirodni broj m (vidi, na primjer [2]). Pokazat će se da će taj pristup (istina, u puno složenijim okolnostima) biti važan u Wilesovom dokazu.

Simon Singh naslovom svoje lekcije aludirao je na višestoljetne neuspješne amaterske pokušaje da se Fermatov teorem dokaže ili opovrgne elementarnim metodama. Formulacija problema je jednostavna, mogu je razumjeti svi koji su završili osnovnu školu, pa mnogi s pravom očekuju da se i rješenje može izreći jednostavnim jezikom. Možda se jednom to i ostvari, ali izgledi za to nisu veliki. Navest ćemo neke razloge koji na to upućuju.

Fermatov teorem i algebarska teorija brojeva. Izvorno, Fermatova se tvrdnja odnosi na pozitivne brojeve. U matematici je prirodno uključivanje i negativnih brojeva, odnosno razmatranje jednadžbe $X^n + Y^n = Z^n$ za cijele brojeve X, Y, Z (dok n i dalje ostaje prirodan broj veći od 2). Lako se vidi da su onda za parne n očita rješenja $(0, \pm 1, \pm 1), (\pm 1, 0, \pm 1)$, a za neparne n, još i $(\pm 1, \mp 1, 0)$. Takva se rješenja nazivaju trivijalnim. Sad Fermatov posljednji teorem tvrdi da jednadžba $X^n + Y^n = Z^n$ za $n > 2$ nema drugih cjelobrojnih rješenja osim trivijalnih. Makar negativni brojevi donose i probleme za čas će se vidjeti opravdanost njihova uvođenja. Radi jednostavnosti, započnimo s $n = 3$, kada se jednadžba može zapisati u obliku

$$X^3 = (Z - Y)(Z - \omega Y)(Z - \overline{\omega} Y) = (Z - Y)(Z - \omega Y)(Z - \omega^2 Y). \tag{2}$$

Tu je $\omega = \dfrac{-1 + \sqrt{3}i}{2} = \cos\dfrac{2\pi}{3} + \sin\dfrac{2\pi}{3} i$ kompleksni treći korijen iz 1, a $\overline{w}$ je njegova kompleksno-konjugirana vrijednost (koja je ujedno jednaka ω^2 odnosno $-\omega - 1$). Jednakost (2) uspoređuje dva rastava na faktore u prstenu

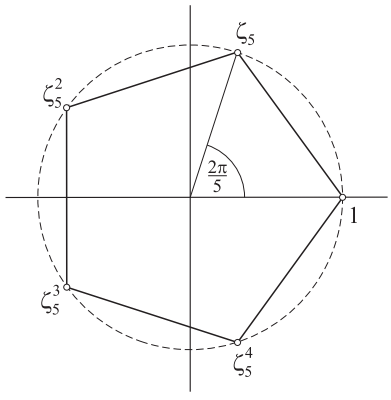
$$\mathbf{Z}[\omega] = \{u + v\omega | u, v \in \mathbf{Z}\} \tag{3}$$

a to je najmanji prsten koji sadrži prsten cijelih brojeva $\mathbf{Z}$ i broj ω. U $\mathbf{Z}[\omega]$ nema smisla govoriti koji je broj pozitivan, a koji negativan, ali, kao i kod prstena cijelih brojeva, ima smisla govoriti o djeljivosti, prostim brojevima i rastavu na proste faktore. Može se pokazati da svi obični prosti brojevi koji pri dijeljenju s 3 imaju ostatak 2 (tj. 2, 5, 11, 17 itd.), ostaju prosti i u ovom prstenu. Oni obični prosti brojevi koji pri dijeljenju s 3 imaju ostatak 1 nisu više prosti u $\mathbf{Z}[\omega]$ već su umnožak od po dvaju prostih. Na primjer, $7 = (2 - \omega)(3 + \omega)$. Nadalje, u ovom je prstenu rastav na proste faktore jednoznačan (do na množenje s ± 1, $\pm\omega$, $\pm\overline{\omega}$), a korištenjem te činjenice može se dokazati Fermatov teorem za $n = 3$. Prvi je to dokazao Euler, ali je u početku napravio pogrešku s prstenom $\mathbf{Z}[\sqrt{-3}] = \{u + v\sqrt{-3} | u, v \in \mathbf{Z}\}$. Njemu je bilo samorazumljivo da je rastav na proste faktore u tome prstenu jednoznačan, što nije istinito.

Na primjer, $4 = 2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$. Jednoznačnost vrijedi tek u nešto većem prstenu $\mathbf{Z}[\omega]$ (što se u ovom primjeru vidi ako se stavi $\sqrt{-3} = 2\omega + 1$). Slično kao za $n = 3$, jednakost $X^n + Y^n = Z^n$, za bilo koji n, može se zapisati kao

$$X^n = (Z - Y)(Z - \zeta_n Y)(Z - \zeta_n^2 Y) \cdot \ldots \cdot (Z - \zeta_n^{n-1} Y), \tag{4}$$

gdje je $\zeta_n = \cos\dfrac{2\pi}{n} + \sin\dfrac{2\pi}{n} i$ (primitivni) kompleksni n-ti korijen iz 1 (slika 1). Već je rečeno da je u prstenu $\mathbf{Z}[\zeta_3]$ rastav na proste faktore jednoznačan (naime $\zeta_3 = \omega$). To vrijedi i u $\mathbf{Z}[\zeta_4]$ (tu je $\zeta_4 = i$). Prsten $\mathbf{Z}[i]$ naziva se, prema njemačkom matematičaru Gaussu, prstenom



Gaussovih brojeva. Sredinom 19. st. pojavio se 'dokaz' Fermatova teorema koji se zasnivao na neistinitoj pretpostavci da je u prstenu $\mathbf{Z}[\zeta_n]$ rastav na proste faktore jednoznačan za svaki n. Iako je rastav jednoznačan za početne vrijednosti n, to općenito nije istina. Prvi takav n je 23, a ima ih beskonačno mnogo. Probleme koje je donijela nejednoznačnost djelomično je otklonio Kummer zamijenivši je jednoznačnošću rastava na proste ideale. Usprkos razvoju teorije algebarskih brojeva u drugoj polovici 19. i u 20. stoljeću, ti problemi nisu nikada u potpunosti otklonjeni. Ne postoji sigurna metoda zasnovana na aritmetici u ciklotomskim poljima (najmanje polje koje sadrži sve racionalne brojeve i ζ_n) kojom bi se potvrdila (ili opovrgla) Fermatova tvrdnja za svaki konkretan n, a pogotovo onda nema metode kojom bi se zaključak proveo odjednom za sve n. Tako je (bar zasad) propao pokušaj da se takvim pristupom dokaže Fermatov teorem, iako je 1993, koristeći se računalima i aritmetikom ciklotomskih polja, tim autora provjerio da Fermatov teorem vrijedi za sve eksponente n manje od 4 000 000.

Fermatov teorem i algebarska geometrija. Jednadžba $X^n + Y^n = Z^n$ dijeljenjem sa Z^n i zamjenom $x = \dfrac{X}{Z}$, $y = \dfrac{Y}{Z}$ može se zapisati kao

$$x^n + y^n = 1 \tag{5}$$

gdje su x, y sad racionalni, a ne više cijeli brojevi. Trivijalna rješenja te jednadžbe su $(\pm 1, 0)$, $(0, \pm 1)$ za parne n, a $(1, 0)$, $(0, 1)$ za neparne n. Sad Fermatov teorem postaje tvrdnja da jednadžba (5) ima samo trivijalna racionalna rješenja. Jednadžbom (5) zadana je algebarska krivulja (tu se pretpostavlja da x, y ne moraju primati samo racionalne, već i realne, čak i kompleksne vrijednosti). Svako rješenje jednadžbe određuje točku krivulje, a ako je rješenje racionalno, kaže se da je točka racionalna. Fermatov teorem postaje tvrdnja: krivulja zadana s (5) ima samo trivijalne racionalne točke. Algebarske krivulje proučavaju se unutar matematičke discipline algebarske geometrije, a ako je težište na racionalnim točkama, onda je riječ o aritmetičkoj algebarskoj geometriji. To znači da se gledaju samo krivulje koje se mogu zadati jednadžbom kojoj su koeficijenti racionalni brojevi. Složenost algebarske krivulje ovisi o njenom genusu (rodu): što je rod veći, krivulja je složenija. Genus g krivulje može biti bilo koji prirodni broj uključujući i nulu. Najjednostavnije su krivulje pravci i konike (krivulje drugog reda – zadane su jednadžbama drugog stupnja), one imaju genus $g = 0$. Krivulje zadane kubnom jednadžbom koje se ne mogu svesti na konike imaju genus 1 i tako redom. Složenija algebarska krivulja u pravilu ima složeniju aritmetiku, tj. teže joj je odrediti racionalne točke. Krivulje genusa 0 ili nemaju racionalnih točaka ili ih imaju beskonačno mnogo. Postoji algoritam koji odlučuje:

(i) ima li ili nema konkretna krivulja genusa 0 racionalnu točku,

(ii) kako se može doći do racionalne točke (ako postoji),

(iii) kako se iz poznate racionalne točke mogu odrediti sve ostale (njih beskonačno mnogo).

To je znao francuski matematičar Legendre koncem 18. stoljeća. Najteži je dio (i) algoritma. Ipak, i on se zasniva na jednostavnoj ideji već opisanoj: gleda se ima li jednadžba rješenje modulo m za različite cijele brojeve m (a pokaže se da je to dovoljno gledati samo za konačno mnogo m). Usput slijedi i dio (ii) algoritma, a najjednostavniji je dio (iii). Sve ćemo ilustrirati na dva primjera koji dobro ocrtavaju opću situaciju.

Krivulja $x^2 + y^2 = 3$ nema racionalnih točaka. Naime, svaka racionalna točka (x, y) vodila bi do cjelobrojnog rješenja (X, Y, Z) jednadžbe $X^2 + Y^2 = 3Z^2$ u kojoj se može pretpostaviti da X, Y, Z nemaju zajedničkih faktora (da su relativno prosti). Ako sad ovu jednadžbu pogledamo modulo 3 (tj. gledamo samo ostatke 0, 1, 2 pri dijeljenju s

3), dobijemo $X^2+Y^2=0$ modulo 3. Lako se vidi da to znači da je $X=Y=0$ modulo 3, pa su X, Y djeljivi s 3, a onda je i Z djeljiv s 3, a to je nemoguće.

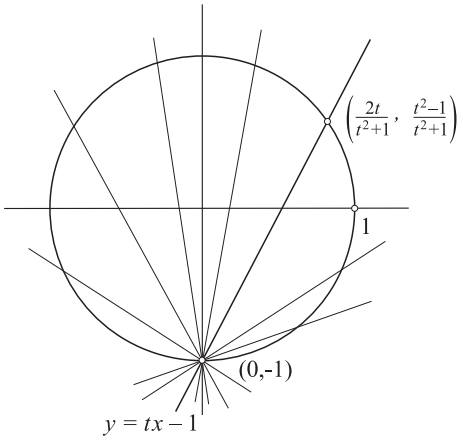
Krivulja $x^2+y^2=1$, kružnica, ima beskonačno mnogo racionalnih točaka. Naime, odmah vidimo trivijalnu točku $(0,-1)$ (ima ih još). Tom točkom provlačimo pravce, beskonačno mnogo njih, parametriziranih racionalnim parametrom t:

$$y=tx-1. \tag{6}$$

Druga točka presjeka tog pravca s kružnicom jednaka je

$$(x,y)=\Big(\frac{2t}{t^2+1},\frac{t^2-1}{t^2+1}\Big). \tag{7}$$

Mijenjanjem racionalnog parametra t dobiju se sve ostale racionalne točke (slika 2).



Za krivulje genusa 1 nema kriterija za postojanje racionalne točke. Ako krivulja genusa 1 ima bar jednu racionalnu točku, onda je ona eliptička krivulja, i tada se pokazuje da se ona može zadati kubnom jednadžbom oblika

$$y^2=x^3+Ax^2+Bx+C \tag{8}$$

gdje su A, B, C racionalni brojevi (vidi [3]). O racionalnim točkama eliptičkih krivulja puno se zna, ali još uvijek nedovoljno. Može se dogoditi da eliptička krivulja ima samo konačno mnogo racionalnih točaka (i tada se sve one mogu pronaći), ali može ih biti i beskonačno mnogo, a tada nema postupka poput onog s konikama koji bi funkcionirao u svim situacijama. Dugo se nije znalo što je s krivuljama genusa većeg od 1 iako se vjerovalo da svaka takva krivulja ima konačno mnogo racionalnih točaka. To vjerovanje bilo je poznato kao Mordellova slutnja (prema britansko-američkom matematičaru Mordellu koji je slutnju formulirao 1922.), makar se nije znala njena istinitost ni za jednu konkretnu krivulju sve do 1983. kada je slutnju dokazao njemački matematičar Faltings (i za to dobio Fieldsovu medalju). Ipak, do današnjih dana nema algoritma za određivanje tog konačnog skupa, čak ni za sve krivulje genusa 2. Vratimo se na krivulje (5) povezane s Fermatovim teoremom. Općenito nije jednostavno iz jednadžbe izračunati genus, ali ovdje se može pokazati da je

$$g=\frac{(n-1)(n-2)}{2}.$$

Na primjer, za redom $n=2$, 3, 4, 5, 6, 7 dobije se $g=0$, 1, 3, 6, 10, 15 pa se vidi da se genus sve brže povećava. Za $n=2$ dobije se $g=0$. To objašnjava zašto se slučaj Pitagorinih trojki $X^2+Y^2=Z^2$ izdvaja i jednostavan je u usporedbi s Fermatovim teoremom u kojemu je $n>2$. Štoviše, za $n>3$ genus je veći od 1 čime se sve još više usložnjava.

Fermatov teorem i *abc* slutnja. Možda je najprirodniji kontekst za Fermatov teorem još uvijek nedokazana tvrdnja o jednadžbi $a+b=c$, poznata kao *abc*-slutnja ([4]). Za njeno razumijevanje potreban je pojam radikala prirodnog broja – to je umnožak svih njegovih različitih prostih djelitelja. Na primjer, $12=2^2\cdot 3$ pa je $\mathrm{rad}(12)=2\cdot 3=6$. Slično, $720=2^4\cdot 3^2\cdot 5$ pa je $\mathrm{rad}(720)=2\cdot 3\cdot 5=30$. Slutnja ima više različitih formulacija, prva se pojavila 1985, a ovdje će biti navedena jedna pojednostavnjena koja zorno ilustrira vezu s Fermatovim teoremom.

Ako za relativno proste prirodne brojeve a, b, c vrijedi $a+b=c$, onda je

$$c < \operatorname{rad}(abc)^2. \tag{9}$$

Na primjer, za $3+125=128$, $c=128$, a $\operatorname{rad}(abc)=\operatorname{rad}(3\cdot 125\cdot 128)=30$ i zaista vrijedi $128<30^2$. Bitno je da su brojevi a, b, c relativno prosti. Na primjer, u $48+16=64$, $\operatorname{rad}(48\cdot 16\cdot 64)=6$ i nije istina da je 64 manje od 6^2. Ako se prihvati da (9) vrijedi, onda se lako pokaže Fermatov teorem. Naime, u $X^n+Y^n=Z^n$ može se pretpostaviti da su X, Y, Z relativno prosti, pa se može primijeniti (9) uz $a=X^n$, $b=Y^n$, $c=Z^n$. Dobije se $Z^n<(\operatorname{rad}(X^nY^nZ^n)^2=(\operatorname{rad}(XYZ))^2<(Z^3)^2=Z^6$, odakle slijedi $n<6$, pa Fermatovu tvrdnju treba dokazati još samo za $n=3$, 4, 5. Kako je ovo posljednje odavno poznato, Fermatov teorem bio bi dokazan. Japanski matematičar Shinichi Mochizuki najavio je 2012. dokaz vrlo stroge verzije *abc*-slutnje, zasnovan na novoj matematičkoj teoriji. Nažalost, do danas matematičari nisu uspjeli provjeriti ispravnost rezultata u člancima koje je postavio na svojoj stranici. Vidjeli smo kako Fermatov teorem slijedi iz slutnje (9) koja je provjerena na velikom broju primjera. Međutim, Fermatov teorem bi proizlazio i iz puno slabije verzije te relacije. Na primjer, ako bi bila istinita tvrdnja koja se dobije ako se (9) zamijeni s $c<\operatorname{rad}(abc)^{1\,000\,000}$, u koju teško tko može posumnjati (makar ni ona nije dokazana), gornjim postupkom bi se lako pokazalo da bi onda Fermatov teorem trebalo provjeravati samo za $n<3\,000\,000$. Podsjetimo da je prije više od 20 godina provjerena istinitost Fermatova teorema za sve n manje od $4\,000\,000$.

Dokaz

Wilesov dokaz Fermatova teorema je neizravan. To znači da se polazi od pretpostavke da tvrdnja teorema nije istinita, a onda se pokaže da bi to vodilo do zaključka da nije istinita neka druga tvrdnja za koju se zna da je istinita. Iako mu je shema jednostavna, dokaz je praktično nedostupan i velikoj većini matematičara. Za njegovo razumijevanje potrebno je predznanje koje imaju samo specijalisti. Zato su mnogi pokušali popularnim izdanjima koliko-toliko dokaz približiti široj čitalačkoj publici. Spomenimo tek [8] od Simona Singha (poznata i kao *Fermatova enigma*), ili nešto stručniju i zahtjevniju [7]. Autor druge, Yves Hellegouarch i sam je sudjelovao u posljednjem dijelu ove napete priče. On je početkom druge polovice 20. stoljeća došao na ideju da uz hipotetsko netrivijalno rješenje Fermatove jednadžbe, tj. uz prirodne brojeve a, b, c i prirodni broj n veći od 2 koji zadovoljavaju uvjet $a^n+b^n=c^n$, poveže eliptičku krivulju

$$y^2=x(x-a^n)(x+b^n)=x^3-(a^n-b^n)x^2-a^nb^nx. \tag{10}$$

Ta je krivulja isto hipotetska, postoji samo ako ne vrijedi Fermatov posljednji teorem. Hellegouarch je naveo neka njezina neobična svojstva i iznio pretpostavku da bi se moglo dokazati da takva krivulja ne može nikako postojati, pa ni brojevi pomoću koje je konstruirana, čime bi Fermatov teorem bio dokazan. Dvadesetak godina poslije, njemački matematičar Gerhard Frey, iznio je puno određeniju tvrdnju o kojim neobičnim svojstvima krivulje (10) bi moglo biti riječ (od tada se svaka hipotetska krivulja (10) naziva Freyovom krivuljom). Naime, on je iznio argumente koji su upućivali na to da takva eliptička krivulja ne bi bila modularna. O modularnosti ćemo nešto reći poslije, a sad recimo samo to da su se u ono doba većina teoretskih matematičara dijelila u dvije skupine: jedni su vjerovali da su sve eliptičke krivulje (s jednadžbom kojoj su koeficijenti racionalni brojevi) modularne, a drugi su vjerovali u suprotno. Ubrzo, nastavljajući rad koji je započeo francuski matematičar Jean Pierre Serre, Ken Ribet je dokazao da Freyova krivulja nije modularna. To je značilo da ili Freyova krivulja ne postoji (tada je istinita tvrdnja Fermatova teorema) ili je Freyova krivulja primjer eliptičke krivulje koja nije modularna (tada ne bi bili istiniti ni Fermatov teorem niti

slutnja o modularnosti). U tom je trenutku Andrew Wiles, koji je i do tada pokušavao dokazati Fermatov teorem drugim metodama, odlučio svoju matematičku karijeru staviti na kocku. Zanemario je sve druge obaveze i započeo dokazivati slutnju o modularnosti. Napravio je redukciju, tako da nije dokazivao slutnju za sve eliptičke krivulje već za jednu užu klasu polustabilnih eliptičkih krivulja u kojoj su bile i hipotetske Freyove krivulje. Nakon nekoliko godina, izgledalo je sve uzaludno, jer je u dokazu koji je predložio otkrivena pogreška. Uz pomoć mladog britanskog matematičara Rićarda Taylora uspio je otkloniti pogrešku. Poslije je Taylor bio u timu koji je dokazao slutnju o modularnosti za sve eliptičke krivulje.

Modularnost je određeno svojstvo točaka eliptičke krivulje nad konačnim poljima, tj. kad se njena jednadžba razmatra modulo p za sve proste brojeve p. Zametak ideje je u razmatranju parnosti i neparnosti spomenutoj kod Homerova tobožnjeg protuprimjera Fermatovu teoremu. Sve se može interpretirati jezikom reprezentacija Galoisove grupe. To je grupa koja permutira rješenja algebarskih jednadžba s racionalnim koeficijentima. Na primjer, jednadžba $x^2 - 2 = 0$ ima dva rješenja: $\sqrt{2}$ i $-\sqrt{2}$. Svaki element Galoisove grupe ili ta dva rješenja ostavlja na miru ili zamjenjuje jedan s drugim. Slično, jednadžba $x^5 = 1$ ima pet rješenja: 1, ζ_5, ζ_5^2, ζ_5^3, ζ_5^4. Svaki element Galoisove grupe ostavlja rješenje 1 na miru, a ζ_5 ili ostavlja na miru (tada i sva ostala rješenja ostavlja na miru) ili prebacuje u ζ_5^k, za $k = 2$, 3 ili 4 (a tada rješenje ζ_5^m prebacuje u ζ_5^{mk}). Općenito situacija može biti još složenija. Naziv Galoisova grupa u čast je legendarnog matematičara Galoisa koji je stradao u dvoboju u dvadeset i prvoj godini života, i koji je ostavio rukopis u kojemu je, u terminima grupa, dao kriterij o tome koje jednadžbe jesu, a koje nisu rješive u radikalima. Nešto ranije norveški matematičar Abel, koji je također kratko živio (od 1802. do 1829.), po kojemu se i naziva ova prestižna nagrada, dokazao je da postoje jednadžbe petog stupnja koje nisu rješive u radikalima. On je pokazao da su rješive u radikalima sve jednadžbe na čija rješenja Galoisova grupa (koja se tada još uvijek nije tako ni zvala) djeluje komutativno. To je jedan od glavnih razloga zašto se komutativne grupe nazivaju abelovima. Galoisova grupa ima mnoštvo reprezentacija, a na ciklotomskim poljima djeluje komutativno. Razmatranje abelovih reprezentacija Galoisove grupe isto je kao i razmatranje samo ciklotomskih polja (kako smo vidjeli, ona nisu bila dovoljna za dokaz Fermatova teorema). Svakoj eliptičkoj krivulji pridružena je reprezentacija Galoisove grupe pomoću matrica drugog reda (koje općenito nisu komutativne). Upravo proučavanje takvih reprezentacija dovelo je do dokaza o modularnosti a time i do dokaza Fermatova teorema. Na to je mislio Andrew Wiles kada je u svom nastupnom predavanju spominjao *abelove* i *neabelove pristupe*.

Literatura

[1] `http://web2.0calc.com/`

[2] A. DUJELLA, *Uvod u teoriju brojeva* (skripta), PMF-Matematički odjel Sveučilište u Zagrebu, `https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

[3] A. DUJELLA, *Eliptičke krivulje u kriptografiji* (skripta), PMF-Matematički odjel Sveučilište u Zagrebu, `https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

[4] A. GRANVILLE, T. TUCKER, *It's As Easy As abc*, Notices of the AMS **49** (10), (2002) (1224–1231).

[5] I. GUSIĆ, *Fermatov teorem*, MFL **4** (176), 178–185, Zagreb, 1994.

[6] I. GUSIĆ, *Fermatov teorem*, Život i škola, Zagreb, **5** (1994), 425–434 (English summary).

[7] Y. HELLEGOUARCH, *Invitation to the Mathematics of Fermat-Wiles*, Academic Press 2001.

[8] S. SINGH, *Fermat Last theorem*, Fourth Estate, London, 1997.