ФЕРМАОВА ВЕЛИКА ТЕОРЕМА

Ратко Тошић, Нови Сад

Пример проблема из најраније фазе теорије бројева је *Питагорин проблем*. Као што знамо, за дужине страница правоуглог троугла важи једнакост $x^2 + y^2 = z^2$, где су x и y дужине катета, а z дужина хипотенузе. То нам омогућава да одредимо дужину једне странице правоуглог троугла ако су познате друге две. Ова чињеница била је позната Вавилонцима скоро 2000 година пре Питагоре, иако нису знали доказ. Грци су са посебним интересом изучавали правоугле троуглове код којих су све три дужине страница цели бројеви. Такви троуглови називају се Питагорини троуглови а одговарајуће тројке бројева (x, y, z) су Питагорине тројке. На пример, $(3, 4, 5)$ и $(5, 12, 13)$ су Питагорине тројке бројева.

Да ли је број Питагориних тројки бесконачан?

Одговор на ово питање је, очигледно, потврдан. Наиме, лако се види да ако је (x, y, z) Питагорина тројка, онда је за сваки природан број k, тројка (kx, ky, kz), такође, Питагорина. Заиста, ако је $x^2 + y^2 = z^2$, тада је

$$(kx)^2 + (ky)^2 = k^2x^2 + k^2y^2 = k^2(x^2 + y^2) = k^2z^2 = (kz)^2,$$

тј. (kx, ky, kz) је Питагорина тројка. Тако, на пример, из Питагорине тројке (3, 4, 5), стављајући $k = 2, 3, \ldots$, добијамо бесконачан низ Питагориних тројки (6, 8, 10), (9, 12, 15),...

Још су Питагорини следбеници пронашли да је $\left(m, \frac{m^2-1}{2}, \frac{m^2+1}{2}\right)$ Питагорина тројка за сваки природан непаран број m. Кронекер је у 19. веку доказао да су сва целобројна решења једначине

$$x^2 + y^2 = z^2$$

облика

$$x = m(a^2 - b^2),\ y = 2mab,\ z = m(a^2 + b^2),$$

где су m, a и b цели бројеви, a и b узајамно прости, један од њих паран, а други непаран.

Питагорин проблем припада типу Диофантових проблема. Таквим проблемима се бавио грчки математичар Диофант, који је живео у Александрији у 3. веку наше ере. Његово велико дело је ”Аритметика”. У суштини, то је колекција примера једначина различитих степена, где је основни проблем да се нађу целобројна или рационална решења. Диофантова дела су представљала полазну тачку за истраживања Фермаа, Ојлера, Гауса и других математичара у области теорије бројева.

Интересантна је судбина Диофантове ”Аритметике”. Написана је у 3. веку нове ере, али је ишчезла и више од једног миленијума сматрала се изгубљеном. Тек 1464. године је немачки математичар Региомонтанус случајно пронашао 6 од 13 књига ”Аритметике”. У латинском преводу први пут је објављена 1575. године. Издање из 1621. године, упоредо на латинском и грчком, приредио је Фермаов пријатељ Баше де Мезирјак. Један примерак је поклонио Фермау. Та књига је постала обавезна лектира за све европске математичаре, између осталих за Фермаа и Декарта. Ни после хиљаду година књига није изгубила ништа од своје актуелности; њен садржај је био далеко изнад нивоа европске алгебре 16. века.

Француски математичар и правник Пјер Ферма (1601-1665) практиковао је да на маргинама свог примерка Диофантове ”Аритметике” записује белешке ко је су се односиле на проблеме из теорије бројева којима се бавио. Те белешке су често имале облик тврђења без доказа. Сва та тврђења су касније, од стране других математичара потврђена као коректна, уз малобројне изузетке.

У Диофантовој књизи наведен је и следећи проблем:

За сваки позитиван цео број а, једначина $x^2 + y^2 = a^2$ *има бесконачно много рационалних решења.*

Другим речима, квадрат целог броја може се представити као збир два квадрата рационалних бројева на бесконачно много начина. Одатле лако следи да има бесконачно много Питагориних тројки бројева.

На маргини, поред овог Диофантовог текста, Ферма је записао следећи коментар: *Међутим, немогуће је представити куб као збир два куба, четврти степен као збир два четврта степена, и уопште, било који степен већи од другог као збир два таква степена. Нашао сам заиста леп доказ овог тврдђња, али на маргини нема довољно места да га запишем.*
(*Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.*)

Другим речима, Ферма тврди да Диофантова једначина

$$x^n + y^n = z^n,$$

где је n цео број већи од 2, нема решења у скупу природних бројева. У Фермаовој заоставштини није пронађен доказ о коме је говорио. Заувек је остала загонетка да ли је и каквим доказом располагао Ферма.

Кад је Фермаов син Самуел 1670. године објавио Башеов превод Диофантове Аритметике заједно са очевим белешкама, ова белешка је постала чувена.

Најбољи математичари су током више од 300 година безуспешно покушавали да докажу Фермаово тврђење, примењујући разне приступе. У тим покушајима добијени су многи важни и интересантни резултати из теорије бројева. За $n = 3$ и $n = 4$, тврдђње је доказао Ојлер (1707-1783), а за $n = 5$, Дирихле (1805-1859). Ојлер је 1742. године, скоро читав век после Фермаове смрти, тражио од свог пријатеља, француског математичара Клероа, да претражи Фермаову кућу у нади да ће се пронаћи неки папир са бар делом доказа. Није постојала никаква идеја о томе како би могао изгледати Фермаов доказ, ако га је уопште било. Гаус је био мишљења да доказ није ни постојао, или је био погрешан. У писму Олберсу, Гаус каже: "Признајем да је Фермаова теорема, као изоловано тврђење, од малог интереса за мене, јер бих могао лако формулисати мноштво сличних тврђења, која се не могу ни доказати ни оповргнути." Велики немачки математичар Давид Хилберт (1862-1943) овако је објаснио разлоге зашто никад није покушао да докаже Фермаову велику теорему: "Пре него што почнем, морао бих да посветим три године интензивном проучавању, а ја немам толико времена да бих га страћио на вероватан неуспех."

Поред аксиома (тврђења чија се тачност прихвата без доказа) и теорема (доказаних тврђења), у математици постоје и хипотезе (тврђења за која се претпоставља да су тачна, али за која немамо доказ). У историји математике познате су многе хипотезе, које су изрекли разни математичари. Неке од њих су касније доказане и самим тим су постале теореме, а неке су оповргнуте, тј. доказано је да не важе. И у једном и у другом случају, значај хипотеза изречених од стране великих математичара је велики. И у једном и у другом случају, напори да се хипотеза докаже или оповргне обично резултирају често неочекиваним открићима и развојем нових математичких дисциплина. Фермаова велика теорема је преко 350 година имала статус хипотезе.

Велики напредак у правцу решења Фермаовог проблема направио је познати немачки математичар Кумер (1810-1893). Доказао је да Фермаово тврђење важи за све природне бројеве $n < 100$; за тај резултат добио је награду Париске академије наука. Кумер је, 1843. године чак саопштио решење комплетног проблема, али је Дирихле указао на грешку у његовом доказу. Без обзира на то, може се рећи да је велики прогрес у правцу решења Фермаовог проблема, који су постизали разни математичари, текао у складу са Кумеровим идејама. Од почетка рачунарске ере, упоредо са покушајима решења Фермаовог проблема, вршена су и проверавања помоћу рачунара. На тај начин је Фермаово тврђење било проверено за све природне бројеве $n \leq 150000$.

Фермаов проблем привукао је у 20. веку пажњу и многих нематематичара, делом захваљујући и чињеници да је 1908. године Немац Волфскел завештао награду од 100 000 марака ономе ко први реши проблем. Последица тога била је поплава "решења" од стране аматера, од којих многи нису ни схватили суштину проблема. Интересовање аматера је спласнуло након што је поменута сума обезвређена хиперинфлацијом која је у Немачкој наступила после Првог светског рата. Коначно је, 1994. године, енглески математичар Ендрју Вајлс доказао Фермаову велику теорему. Неки пропусти и нејасна места у доказу отклоњени су ускоро уз сарадњу других математичара.

Тиме је Фермаова хипотеза (тврђење за које није оставио доказ) добила статус теореме и позната је под именом Фермаова велика теорема (за разлику од тзв. Фермаове мале теореме која је, иако по називу ”мала”, веома значајна).

За читаоца ће бити интересантно да види како је врло једноставно доказати ”велики део” ФВТ (Фермаове велике теореме). Такви докази у математици често доприносе оптем утиску о приступачности неког проблема и наводе аматере без великог математичког знања да се упуштају у решавање озбиљних математичких проблема. Слична ситуација је карактеристична и за друге тешке математичке проблеме као што су квадратура круга, трисекција угла и дуплирање (удвајање) коцке.

Задатак 1. *Доказати да не постоје природни бројеви* x, y, z, n, *где је* $n \geq z$, *такви да је* $x^n + y^n = z^n$.

Решење. Претпоставимо супротно, тј. да за неке природне бројеве x, y, z, n, где је $n \geq z$, важи $x^n + y^n = z^n$. Лако се види да мора бити $x < z$, $y < z$, па на основу симетрије израза $x^n + y^n$ можемо претпоставити да је $x \leq y$. Користићемо идентитет

$$z^n - y^n = (z - y)(z^{n-1} + yz^{n-2} + \ldots + y^{n-2}z + y^{n-1})$$

који се лако доказује множењем израза на десној страни. Како у другој загради на десној страни има n сабирака, сваки је, на основу $x \leq y < z$, већи од x^{n-1} и како је $z - y \geq 1$, то је

$$(z - y)(z^{n-1} + yz^{n-2} + \ldots + y^{n-2}z + y^{n-1}) > nx^{n-1} > x^n.$$

Следи $z^n - y^n > x^n$, односно $x^n + y^n < z^n$, што је супротно претпоставци $x^n + y^n = z^n$. Из добијене контрадикције следи тачност тврђења формулисаног у задатку.

□

У уобичајеним задацима који се односе на диофантске једначина, најчешће се подразумева да није дозвољено коришћење ФВТ (Фермаова велика теорема), уколико није друкчије наглашено. Ипак, у следећем задатку демонстрираћемо пример доказа коришћењем ФВТ.

Задатак 2. *Нека су* m *и* n *два природна броја који су седми степени и при томе је* m 2009*-цифрен, а* n 2016*-цифрен. Да ли* 4025*-цифрен број који се добија исписивањем броја* n *иза броја* m *може бити седми степен*?

Решење. Не може. Нека је $m = x^7$ и $n = y^7$. Тада је број који се из њих добија надовезивањем једнак

$$10^{2016}x^7 + y^7 = (10^{288}x)^7 + y^7.$$

Међутим, на основу ФВТ, овај број не може бити седми степен.

Теорија бројева је непресушни извор добрих проблема. За математичаре добар проблем је онај чија је формулација једноставна, а решење је сложено. Што је већа диспропорција између једноставности формулације и сложености решења, проблем је бољи. ФВТ је најбољи пример за то. Њену формулацију разуме сваки ученик 7. разреда основне школе, иако су у решавању коришћене методе из разних области математике, које се изучавају само на постдипломским студијама.

ФВТ је била само једна од многобројних хипотеза из теорије бројева, које дуго нису биле ни доказане ни оповргнуте.

И у другим областима математике су постојале и постоје сличне хипотезе, али оно по чему се разликују од хипотеза у теорији бројева је чињеница да само математичари специјализовани у тој области могу да схвате суштину проблема и да се евентуално упусте у његово решавање.

Ради поређења, наводимо један од такозваних миленијумских проблема – Поенкареову хипотезу, коју је 2003. године доказао руски математичар Григориј Перељман. При томе наводимо само њену специјалну (тродимензионалну) варијанту:

Свака неограничена једноструко повезана компактна тродимензионална многострукост хомеоморфна је тродимензионалној сфери.

Чак и математичари којима топологија није специјалност имају тешкоћа да у потпуности схвате формулацију Поенкареове хипотезе, чак и у специјалном тродимензионалном случају.

Да бисмо објаснили смисао Поенкареове хипотезе, претходно морамо рашчистити са појмовима једноструке повезаности, n-димензионалне многострукости, компактности, хомеоморфизма, а при дефинисању сваког од тих појмова појављују се нове чудне речи које се односе на нове појмове, које поново треба објашњавати.

Рад на решавању тешких математичких проблема, као и уопште истраживања у математици, најбоље је окарактерисао сам Ендрју Вајлс, у интервјуу за ББЦ, кад су га питали како се осећа после таквог величанственог открића:

Можда бих најбоље могао описати своје бављење математиком тако да га упоредим с боравком у мрачној и неистраженој кући. Уђете у прву собу и уверите се да у њој влада потпун мрак. Ходајући по соби стално се спотичете о намештај, али мало помало учите где је који комад намештаја. Напокон, после шест месеци или више, пронађете прекидач и упалите светло. И тада све постаје видљиво. Напокон, можете видети где се налазите. А онда улазите у следећу мрачну собу.

Следећих неколико задатака ће помоћи читаоцу да схвати суштину Фермаове велике теореме и с њом повезане проблематике.

Задатак 3. *Јоца је погрешно разумео формулацију Фермаове велике теореме и зачудио се како је лако успео да је докаже. Наиме, он је решавао следећи задатак:*

Доказати да једначина

$$n^x + n^y = n^z$$

има бесконачно много решења за $n = 2$, *а нема решења за* $n > 2$ *у скупу природних бројева. Како изгледа Јоцино решење*?

Решење. Очигледно је $n \geq 2$ и $x, y < z$. Због симетрије леве стране можемо узети да је $x \leq y$. Након деобе леве и десне стране са n^x, једначину можемо написати у облику

$$n^{z-x} - n^{y-x} = 1. \qquad (1)$$

Ако претпоставимо да је $y > x$, тада је $y - x \geq 1$. Како је $z > y$ и $y > x$, то је $z - x \geq 2$. То повлачи да је лева страна (1) је дељива са n. Таква мора бити и десна страна, тј. 1 је дељиво са n. Но, то је немогуће, јер је $n \geq 2$. Стога је $y = x$, па је $n^{y-x} = n^0 = 1$. Када то уврстимо у (1), добијамо да је $n^{z-x} = 2$. Како су у питању природни бројеви, следи $n = 2$ и $z - x = 1$.

Дакле, за $n = 1$ и $n > 2$ једначина $n^x + n^y = n^z$ нема решења у скупу природних бројева. За $n = 2$ има бесконачно много решења. То су све уређене четворке (x, y, z, n), где је x произвољан природан број, $y = x$, $z = x + 1$ и $n = 2$.

□

Задатак 4. *Доказати да једначина*

$$x^n + y^n = z^{n+1}$$

има бесконачно много решења у скупу природних бројева, за сваки природан број n.

Решење. Једначина се може написати у облику

$$\left(\frac{x}{z}\right)^n + \left(\frac{y}{z}\right)^n = z.$$

Сад се лако проверава да је за свака два природна броја a и b, тројка $x = a(a^n + b^n)$, $y = b(a^n + b^n)$, $z = a^n + b^n$ решење дате једначине.

□

На пример, једно од решења једначине

$$x^3 + y^3 = z^4$$

добијамо за $a = 5$ и $b = 7$. Тада је $x = 5(5^3 + 7^3) = 2340$, $y = 7(5^3 + 7^3) = 3276$, $z = 5^3 + 7^3 = 468$.

Задатак 5. *Нека су x, y, z, n природни бројеви такви да је*

$$x^n + y^n = z^n ,$$

где је $x \leq y$. Доказати да је $n \leq x$.

Решење. Из услова $x \leq y$ и саме једначине следи $y < z$, тј. $y + 1 \leq z$. Тада је

$$x^n = z^n - y^n \geq (y+1)^n - y^n. \qquad (1)$$

Користећи идентитет

$$a^n - b^n = (a-b)(a^{n-1} + ba^{n-2} + \ldots + b^{n-2}a + b^{n-1})$$

(видети решење задатка 1) и стављајући $a = y + 1$ и $b = y$, добијамо

$$(y+1)^n - y^n =$$

$$\big((y+1) - y\big)((y+1)^{n-1} + y(y+1)^{n-2} + \ldots + y^{n-2}(y+1) + y^{n-1}) =$$

$$1 \cdot ((y+1)^{n-1} + y(y+1)^{n-2} + \ldots + y^{n-2}(y+1) + y^{n-1}) .$$

Из тога и (1) следи

$$x^n \geq (y+1)^{n-1} + y(y+1)^{n-2} + \ldots + y^{n-2}(y+1) + y^{n-1} .$$

Како је $y + 1 > y \geq x$, из ове неједнакости добијамо $x^n \geq nx^{n-1}$, одакле је $x \geq n$, што је и требало да се докаже.

□

Задатак 6. *Доказати да за непарне бројеве n, $n > 1$, једначина*

$$x^n + y^n = z^n ,$$

нема решења у скупу природних бројева за које је $x + y$ прост број.

Решење. Ако је n, $n > 1$, непаран број, важи идентитет

$$a^n + b^n = (a+b)(a^{n-1} - ba^{n-2} + \ldots + (-1)^{n-2}b^{n-2}a + (-1)^{n-1}b^{n-1}) .$$

(Доказује се исто као онај из решења задатка 5, множењем израза на десној страни.) Специјално је

$$x^n + y^n = (x+y)(x^{n-1} - yx^{n-2} + \ldots + (-1)^{n-2}y^{n-2}x + (-1)^{n-1}y^{n-1}) ,$$

па је $x^n + y^n$ дељиво са $x + y$. С обзиром да је $x^n + y^n = z^n$, z^n је такође дељиво са $x + y$.

Ако је $x + y$ прост број, тада је и z дељиво са $x + y$, тј. $z \geq x + y$. Међутим, тада је $z \geq (x+y)^n > x^n + y^n$, јер је $n > 1$. (Последња неједнакост непосредно следи из биномне формуле.)

Према томе, ако је $x+y$ прост број и $n>1$, тада не може да важи $x^n+y^n=z^n$, где су x, y, z природни бројеви, тј. једначина $x^n+y^n=z^n$ нема решења.

□

Напомена. Ако се не ограничимо на природне бројеве и не захтевамо да је $n>1$, онда наведена једначина има бесконачно много целобројних решења у којима је $x+y$ прост број. Наиме, за произвољно n, то су све тројке $(p,0,p)$, где је p прост број. А за $n=1$, осим наведених, то су још и тројке $(t,p-t,p)$, где је p прост број, а t цео број.

Задатак 7. *Доказати да једначина* $x^2+y^3=z^2$ *има бесконачно много решења у скупу природних бројева.*

Решење. Једно решење је $(1,2,3)$. С друге стране, ако је (x,y,z) решење, тада је то и $(8x,4y,8z)$. Заиста, важи

$$(8x)^2+(4y)^3=64(x^2+y^3)=64z^2=(8z)^2,$$

одакле следи да дата једначина има бесконачно много решења.

□

Задатак 8. *Користећи Фермаову велику теорему наћи све целе бројеве* n *за које је* $18(n^2+3)$ *куб природног броја.*

Решење. Лако се види да је

$$18(n^2+3)=(n+3)^3-(n-3)^3=(n+3)^3+\left(-(n-3)\right)^3. \qquad (1)$$

По Фермаовој великој теореми, једначина

$$z^3=x^3+y^3$$

нема решења у скупу природних бројева. Зато, ако је $18(n^2+3)$ куб природног броја, онда једначина (1) може да има решења само ако је $n+3=0$ или $n-3=0$, тј. $n=-3$ или $n=3$. У оба случаја је $18(n^2+3)=216=6^3$.

□

Статијата прв пат е објавена во списанието ТАНГЕНТА на ДМ на Србија во 2017/18 година