Математичка гимназија

# МАТУРСКИ РАД

**- из математике -**

## Специјални случајеви Михајлескуове теореме

Ученик:
Милош Милићев IVд

Ментор:
Стеван Гајовић

Београд, јун 2021.

# Садржај

# 1

# Увод

Посматрајмо низ природних бројева који су потупни степени: $1, 4, 8, 9, 16, 25, 27, ...$
Овај низ нема неку посебну правилност - наравно, квадрати су у њему најзаступљенији, па затим кубови, и тако даље. Интересантно је уочити да су бројеви 8 и 9 суседни степени, али да ли постоји још таквих парова?
Белгијски математичар Ежен Шарл Каталан је 1844. године објавио претпоставку да су 8 и 9 једини суседни степени. Овај проблем заинтересовао је многе математичаре који су допринели његовом решавању, све док румунски математичар Преда Михајлеску није коначно ставио тачку на њега 2002. године.
У свом доказу, Михајлеску је користио разне резултате који су раније откривени, али и успео да их повеже са својим закључцима и тиме реши овај захтеван проблем.
У овом раду бавићемо се једначином $x^p - y^q = 1$, где су све непознате природни бројеви већи од 1, а $p$ и $q$ бројеви већи од 1.
Приметимо да можемо претпоставити да су $p$ и $q$ прости бројеви. Надаље ћемо користити тај услов.
Анализираћемо решење и њему повезане случајеве. Главни део рада је доказ да је број 9 једини потпун квадрат суседан природном степену, односно решићемо једначину када је неки од $p$ и $q$ једнак 2.

# Catalan's conjecture

$$a^n - b^m = 1 \quad a, b, m, n > 1$$

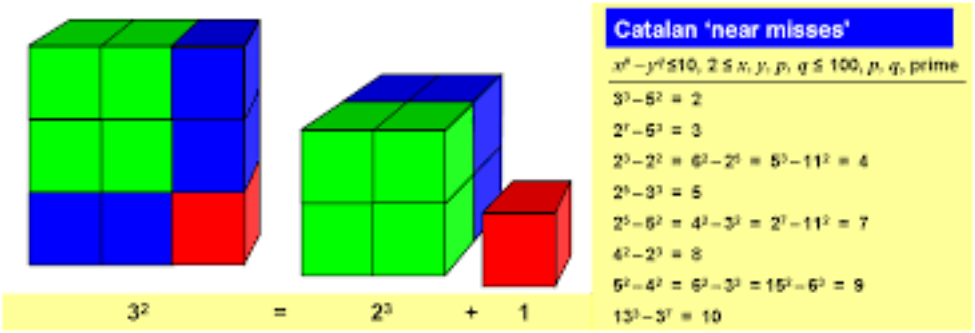
has only one integer solution:

$$3^2 - 2^3 = 1$$

Proposed by Eugene Catalan, 1844

Proved by Preda Mihailescu, 2002

Слика 1: Тврђење хипотезе




Слика 2: Сликовит приказ и степени који су ,,близу"

# 2

# О решењу

Познато нам је решење $(x, y, p, q) = (3, 2, 2, 3)$. Неколико ствари можемо уочити. На пример, да су $x$ и $y$ прости. Пада нам на памет да генерализујемо доказ да је то једино решење кад је неки од $x$ и $y$ прост, или степен простог броја.

## 2.1 Решење уз услов да је $y$ степен простог броја

Нека је $y = r^k$, где је $r$ прост, а $k$ природан број. Сменом $kq = l$ наша једначина се своди на:

$$x^p - r^l = 1$$

Ова једначина може се решити рутинском применом Жигмондијеве теореме. Међутим, нема смисла користити „тешку артиљерију", с обзиром на то да постоји једноставно решење које наводимо испод.

Раздвајамо два случаја:

1° $r = 2$. Знамо да је:

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + ... + x + 1) = 2^l$$

Одавде је јасно да је $x$ непарно. Међутим, уколико је $p$ непаран прост број, други чинилац је непаран јер је он збир $p$ непарних сабирака. Он је очито већи од 1, па не може бити степен двојке, односно делилац броја $2^l$. Дакле, мора бити $p = 2$. Сада је:

$$(x - 1)(x + 1) = 2^l,$$

па су $x-1$ и $x+1$ степени двојке који се разликују за 2, одакле је јасно да је $x=3$. Дакле, овде долазимо до решења почетне једначине: $3^2-2^3=1$.

2° $r>2$. Поново ћемо записати:

$$x^p-1=(x-1)(x^{p-1}+x^{p-2}+...+x+1)=r^l,$$

одакле су оба чиниоца степени броја $r$. Приметимо да за сваки њихов заједнички делилац $d$ важи:
$x\equiv 1\ (mod\ d)\Rightarrow x^{p-1}+...+x+1\equiv p\ (mod\ d)$, па ако они нису узајамно прости мора важити $d=p$.

Ако су чиниоци узајамно прости, мора бити $x-1=1$ и $x^{p-1}+...+1=r^l$. Одавде је $x=2$ и $2^p-1=r^l$. Ово је специјални случај за ,,случај кад је $x$ степен двојке", који више одговара делу 2.2 и биће наведен ту.

Претпоставимо сада да чиниоци имају неки заједнички прост делилац. По претходном, он мора бити $p$, а оба су степени броја $r$, одакле је $p=r$. Наша једначина се своди на:

$$x^p-1=(x-1)(x^{p-1}+...+x+1)=p^l$$

Из Мале Фермаове теореме јасно је да је $x^p-1\equiv x-1\ (mod\ p)$, одакле је $x\equiv 1\ (mod\ p)$.

Како су оба чиниоца степени броја $p$ и нису 1, а други очигледно већи од првог, други чинилац мора бити дељив са $p^2$. Међутим, показаћемо да ово није могуће.
Нека је $x=sp+1$. Израчунаћемо $\sum_{i=0}^{p-1}x^i=\sum_{i=0}^{p-1}(sp+1)^i$ по модулу $p^2$ уз помоћ следеће леме:

**Лема 2.1.** $(sp+1)^i\equiv isp+1\ (mod\ p^2)$

*Доказ:* По биномној формули је:

$$(sp+1)^i=\sum_{j=0}^{i}\binom{i}{j}(sp)^j=1+isp+\binom{i}{2}s^2p^2+...\equiv 1+isp\ (mod\ p^2),$$

јер су сви чланови суме надаље дељиви са $p^2$. □

Сада је по Леми:

$\sum_{i=0}^{p-1} x^i = \sum_{i=0}^{p-1}(sp+1)^i \equiv \sum_{i=0}^{p-1}(1+isp) = p+\sum_{i=0}^{p-1} isp = p+sp\sum_{i=0}^{p-1} i = p+sp\frac{p(p-1)}{2} = p+sp^2\frac{p-1}{2} \equiv p \ (mod\ p^2)$,

јер $2 \mid p-1$ (ово не би важило у 1°, па смо зато и направили овакву поделу случајева).

Дакле, осим $(3,2,2,3)$ не постоји друго решење $(x,y,p,q)$ наше једначине $x^p - y^q = 1$ ако је $y$ степен простог броја. □

## 2.2 Решење уз услов да је $x$ степен простог броја

Слично као у претходном случају, наша једначина се своди на $r^l - y^q = 1$, где је $r$ прост, а $l \geq 2$ природан број. Слично као у претходном, издвојићемо посебно случај кад је $r = 2$.

1° $r = 2$, важи $2^l - 1 = y^q$.

Приметимо да је $q \neq 2$, јер $4 \mid 2^l$ и $4 \nmid y^2 + 1$ ни за један природан број $y$. Дакле, $q$ је непарно.

Слично претходном делу, записаћемо нашу једначину у следећем облику:

$$2^l = y^q + 1 = (y+1)(y^{q-1} - y^{q-2} + ... - y + 1)$$

Из једначине је очито $y$ непарно, па је овде други чинилац непаран, јер он представља збир $q$ непарних бројева. Како он дели $2^l$ и очито је позитиван, он мора бити 1. Међутим, $y > 1$ и $q \geq 3$, одакле је

$$(y^{q-1} - y^{q-2} + ... - y + 1) = 1 + (y^2 - y) + ... + (y^{q-1} - y^{q-2}) > 1,$$

па у овом случају нема решења.

2° $r$ је непаран прост број.

Приметимо да за непарно $q$ можемо раставити $y^q + 1$ на просте чиниоце и мање-више поступати на исти начин као у другом случају дела 2.1. (посматрањем највећег заједничког делиоца, ако је већи од 1 онда је $q = r$, па су оба чиниоца степени броја $r$, други чинилац већи сем за $y = 2$ које је већ анализирано у 2.1, а никад није дељив са $r^2$ - доказ исти као у 2.1).

Сада се поставља питање: шта ако је $q = 2$?

Наша једначина се тада записује као $r^l - 1 = y^2$.

Израз $r^l - 1$ можемо раставити на чиниоце, али то што је $r$ прост број нам ништа додатно не говори о највећем заједничком делиоцу чинилаца. Самим тим, овај услов нам не делује нимало јачи од једначине $x^p - y^2 = 1$ за било који природан број $x$ (небитно да ли је степен простог броја).

Дакле, растављање $r^l - 1$ не помаже нам пуно. С друге стране, $y^2 + 1$ не можемо раставити, бар не у скупу природних бројева.

Сама чињеница да се једначина $x^p - y^2 = 1$ не може решити елементарном теоријом бројева нам говори колико је Каталанов проблем захтеван.

У наставку рада, решаваћемо сложеније случајеве и изводити закључке за $x$ и $y$ у зависности од $p$ и $q$.

# 3

# Случај $q = 2$

У овом поглављу анализираћемо случај када је $q = 2$, односно мањи степен квадрат. Овом једначином бавио се француски математичар Виктор-Амеде Лебег и решио је 1850. године.

Пођимо од једначине $x^p = y^2 + 1$. Како је $p \geq 2$, лева страна је дељива са 4 уколико је $x$ паран број, а лако се проверава да десна страна не може бити дељива са 4 ни за један цео број $y$. Дакле, $x$ мора бити непарно, а самим тим $y$ парно.

Посматрајмо једначину у прстену $\mathbb{Z}[i]$ Гаусових целих бројева:

$$(yi + 1)(1 - yi) = x^p$$

Познато је да Дељење са остатком (ДСО) и Основна теорема аритметике (ОТА, односно јединственсот растављања на просте чиниоце до на јединичне елементе) важе у $\mathbb{Z}[i]$ (видети [4]). Такође, лако је проверити да су $\pm 1, \pm i$ једини јединични елементи овог прстена. Сада рачунамо највећи заједнички делилац чинилаца са леве стране:

$$d = (yi + 1, 1 - yi) \implies d \mid 2$$

па уколико они нису узајамно прости, због ОТА морају бити дељиви неким простим делиоцем броја 2 у $\mathbb{Z}[i]$. У $\mathbb{Z}[i]$ се 2 растаља као $(1 + i)(1 - i)$. Пошто знамо да је $y$ парно од раније, самим тим дељиво са 2 у $\mathbb{Z}[i]$, закључујемо да

$yi + 1$ није дељиво ниједним од ових чинилаца, јер они деле $yi$, а очито не јединични број 1. Самим тим, $yi + 1$ и $1 - yi$ су узајамно прости, односно они су еквиваленти $p-$тим степенима из $\mathbb{Z}[i]$.

Приметимо да $p$ није 2, јер разлика два квадрата не може бити 1. Због тога важи: $(\pm 1)^p = \pm 1$, $(\pm i)^p = \pm i$ или $(\pm i)^p = \mp i$, у зависности од остатка броја $p$ при дељењу са 4. Зато су еквиваленти $p-$тим степенима у $\mathbb{Z}[i]$ уједно и $p-$ти степени.

Како су $yi+1$ и $1-yi$ конјугати у $\mathbb{Z}[i]$, они су $p-$ти степени међусобно конјугованих бројева. То значи да за неке целе бројеве $a$ и $b$ важе следеће две једначине:

$$(a + bi)^p = yi + 1$$

$$(a - bi)^p = 1 - yi$$

Јасно је да је $b \neq 0$, јер је $y$ природан број. Сабирањем једначина закључујемо:

$$(a + bi)^p + (a - bi)^p = 2$$

Знамо да $2a = (a+bi)+(a-bi) \mid (a+bi)^p+(a-bi)^p = 2$, јер је $p$ непарно, одакле је $a = \pm 1$.

Сада се наша једначина своди на $(1 + bi)^p + (1 - bi)^p = \pm 2$.

Сетимо се да $a+bi$ није дељиво ниједним од $1+i$ и $1-i$, а знамо да је $a$ непаран број. Самим тим је $b$ паран (у супротном $1+i \mid 2 \mid (a+bi)-(1+i)$, па $1+i \mid a+bi$).

Дефинишимо низ $a_j = (1 + bi)^{2j+1} + (1 - bi)^{2j+1}$.

Докажимо да за парно $b$ важи $8 \mid a_j - 2$ за сваки ненегативан цео број $j$. Заиста, $a_0 = 2$, $a_1 = 2 - 6b^2$, а из теорије рекурентних једначина знамо да овај низ испуњава релацију:

$$a_{n+2} = ((1+bi)^2 + (1-bi)^2)a_{n+1} - (1+bi)^2(1-bi)^2 a_n = (2-2b^2)a_{n+1} - (1+b^2)^2 a_n,$$

одакле тврђење следи једноставном индукцијом по $j$.

Одавде је јасно да је $(1+bi)^p + (1-bi)^p = 2$, јер је $p$ непаран број.

Распишимо једначину по биномној формули: $2\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j}(bi)^{2j} = 2$, односно

$$\sum_{j=1}^{\frac{p-1}{2}} (-1)^j \binom{p}{2j} b^{2j} = 0.$$

Доказаћемо да је ово немогуће преко аргумента дељивости степеном двојке.

Заиста, ако са $v_2(m)$ означимо највећи степен двојке који дели цео број $m$ различит од нуле, први сабирак у суми имаће строго мањи експонент од свих осталих, па збир свих сабирака не може бити 0, уколико постоји више од једног сабирка. Једноставно се проверава да за $p = 3$ мора бити $b = 0$, што је немогуће по претходном, па можемо сматрати $p \geq 5$.

Како фактор $(-1)^j$ не утиче на $v_2$, можемо увести низ:

$$x_j = \binom{p}{2j} b^{2j},$$

у циљу доказивања $v_2(x_1) < v_2(x_j)$ за $j > 1$.

Ово тврђење еквивалентно је са:

$$0 < v_2\left(\frac{x_j}{x_1}\right) = v_2\left(\frac{\binom{p}{2j}}{\binom{p}{2}} b^{2j-2}\right) = v_2\left(\binom{p-2}{2j-2}\frac{b^{2j-2}}{j(2j-1)}\right)$$

Како је $j \geq 2$, $\binom{p-2}{2j-2}$ природан број, $2j-1$ непаран, а $b$ паран број, знамо:

$$v_2\left(\binom{p-2}{2j-2}\frac{b^{2j-2}}{j(2j-1)}\right) \geq v_2\left(\frac{b^{2j-2}}{j}\right) = v_2(b^{2j-2}) - v_2(j) \geq$$
$$\geq 2j - 2 - v_2(j) \geq j - v_2(j) \geq j - \log_2 j \geq 1,$$

па је доказ завршен. Дакле, једначина $x^p - y^2 = 1$ нема решења. $\square$

# 4

# Случај $p = 2$

У овом поглављу бавићемо се једначином $x^2 - y^q = 1$. Ову једначину први је решио корејски математичар Ке Цао 1965. године.

Приметимо да решењу почетне једначине $(x, y, p, q)$ одговара решење ове једначине $(x, y, q)$. Јасно је да је $q > 2$, јер разлика два природна квадрата никад не може бити 1. Доказ ћемо раздвојити на два случаја: специјално за $q = 3$ и $q > 3$.

## 4.1 Случај $q = 3$ - Ојлеров доказ

Наша једначина се своди на $x^2 - y^3 = 1$. Интересантно је да се Ојлер бавио решавањем ове једначине, и то у скупу ненула рационалних бројева, где је једино решење $(x, y) = (\pm 3, 2)$ (приметимо да то значи да не постоје рационални бројеви који нису цели и задовољавају ову једначину). Свој доказ објавио је 1738. године (подсетимо се да је Каталанова претпоставка објављена тек 1844. године).

У овом делу демонстрираћемо Ојлерово решење једначине $x^2 - y^3 = 1$ у скупу позитивних рационалних бројева. Иако наизглед прилично неинтуитивно, ово ремек-дело засновано је на познатој идеји: пару $(x, y)$ из ове једначине који није $(3, 2)$ придружићемо пар природних бројева који задовољава еквивалентну једначину, па тиме почетну једнакост свести на одговарајућу у скупу природних бројева. Онда ћемо пару природних бројева који испуњава нову једначину придружити још ,,мањи пар" (под овим подразумевамо пар са мањим збиром) који задовољава исту једначину. Овим процесом смањујемо решења, а то не може вечно трајати (ова техника позната је као метод бесконачног спуста). Дакле, ако успемо да спроведемо ову идеју, лако ће следити да почетна јед-

начина нема других решења у скупу рационалних бројева. Овај доказ можемо наћи у оригиналу на латинском језику у [1].

Нека је $x$ позитивно и $x = \frac{a}{b}$ нескратив разломак за неке природне бројеве $a$ и $b$.

Како је $\frac{a^3}{b^3} + 1$ квадрат рационалног броја, множењем са $b^4$ (који је квадрат) закључујемо да број $b(a^3 + b^3)$ квадрат природног броја. Доказаћемо да ово не може важити осим за $a = 2$ и $b = 1$.

Нека је $c = a + b > b$. Растављањем збира кубова на чиниоце, закључујемо да је следећи израз потпун квадрат:

$$f(b, c) = bc(3b^2 - 3bc + c^2)$$

Овде постоји очигледно решење $(1, 1)$, али оно не испуњава $c > b$, па га занемарујемо.

Нека постоји најмањи такав пар $(b, c)$ у ком је $(b, c) \neq (1, 3)$, а $(b, c) = 1$. Изградићемо још мањи такав пар и доћи до контрадикције.

Приметимо да из $(b, c) = 1$ следи $(b, (3b^2 - 3bc + c^2)) = 1$ и $(c, (3b^2 - 3bc + c^2)) \mid 3$.

Ако је други највећи заједнички делилац једнак 3, онда $3 \mid c$ и $c = 3c_1$. Међутим, уврштавањем у $f(b, c)$ и дељењем са 9 добијамо мање решење $(c_1, b)$ за које је $f(c_1, b)$ потпун квадрат. Очито је $(c_1, b) \neq (1, 3)$, јер би било $(b, c) = (3, 3)$, па они не би били узајамно прости. Такође, јасно је да су $b$ и $c_1$ узајамно прости, одакле смо добили мањи пар, па је ово немогуће.

Одавде су бројеви $b, c$ и $(3b^2 - 3bc + c^2)$ узајамно прости по паровима, а производ им је потпун квадрат. Следи да су сви они потпуни квадрати ($b > 0, c > 0$, па и трећи чинилац мора бити позитиван).

Како је $3b^2 - 3bc + c^2 < c^2$ и није 0 (јер $3 \nmid c$), то је он квадрат неког броја мањег од $c$, односно постоје узајамно прости природни бројеви $m$ и $n$ за које је:

$$(3b^2 - 3bc + c^2) = (c - \frac{m}{n}b)^2$$

Сређивањем ове једначине и скраћивањем са $b \neq 0$ можемо закључити да је:

$$\frac{b}{c} = \frac{2mn - 3n^2}{m^2 - 3n^2}$$

Леви разломак је по претходном нескратив. Израчунајмо највећи заједнички делилац бројиоца и имениоца десног разломка, знајући да је $(m, n) = 1$.

Нека неки прост број $r$ дели $2mn - 3n^2 = n(2m - 3n)$ и $m^2 - 3n^2$.

Ако $r \mid n$, онда $r \mid m^2 \Rightarrow r \mid m$, што је немогуће јер $(m, n) = 1$.

Дакле, $r \mid 2m - 3n$. Јасно је да је $r \neq 2$, јер би тада и $m$ и $n$ били парни.

Из $2m \equiv 3n \ (mod\ r)$ је $4m^2 \equiv 9n^2 \ (mod\ r)$ и $3m^2 \equiv 9n^2 \ (mod\ r)$ важи из другог услова, одакле добијамо $r \mid m$, па $r \mid 3n$, односно $r \mid 3$.

Јасно је да не могу оба броја бити дељиви са 9, јер би $m$ и $n$ били дељиви са 3. Дакле, овде имамо два случаја:

1° НЗД $(2mn - 3n^2, m^2 - 3n^2) = 3$. Тада $3 \mid m$ по претходном, па је $m = 3k$ и $(k, n) = 1$. Сада је:

$$\frac{b}{c} = \frac{2nk - n^2}{3k^2 - n^2},$$

при чему је сада и десни разломак нескратив.

Одавде је $b = 2nk - n^2$ и $c = 3k^2 - n^2$, или $b = n^2 - 2nk$ и $c = n^2 - 3k^2$.

Међутим, по претходном је $c$ потпун квадрат, а $3k^2 - n^2$ то не може бити (једначина $u^2 + v^2 = 3w^2$ нема решења у скупу природних бројева: њено најмање решење $(u, v, w)$ би имало све компоненте дељиве са 3 (показати!), па би $(\frac{u}{3}, \frac{v}{3}, \frac{w}{3})$ било мање решење).

Одавде следи да је $b = n^2 - 2nk$ и $c = n^2 - 3k^2$. Очито је $c$ квадрат мањи од $n^2$, па је за неке узајамно просте бројеве $l$ и $s$ испуњено $n^2 - 3k^2 = (n - \frac{l}{s}k)^2$, па је:

$$\frac{k}{n} = \frac{2ls}{3s^2 + l^2}$$

Пошто је $b$ потпун квадрат по претходном, $\frac{b}{n^2} = 1 - \frac{2k}{n} = \frac{3s^2-4ls+l^2}{3s^2+l^2} = \frac{(l-s)(l-3s)}{3s^2+l^2}$ мора бити квадрат рационалног броја.

Дакле, $(l-3s)(l-s)(3s^2+l^2)$ мора бити квадрат природног броја.

Одавде су $l-3s$ и $l-s$ истог знака (ако је неки од њих 0, можемо проверити да се добија почетно решење $(b,c) = (1,1)$). Уз смену $u = |l-s|$ и $v = |l-3s|$ добијамо да је израз $f(u,v)$ потпун квадрат. Лако анализирамо њихов највећи заједнички делилац и скраћујемо их по потреби. Дакле, од пара $(b,c)$ у овом случају смо изградили мањи пар $(\frac{u}{(u,v)}, \frac{v}{(u,v)})$. Рутинском провером закључујемо да је овај пар заиста мањи.

2° НЗД $(2mn-3n^2, m^2-3n^2) = 1$. Одавде је $(b,c) = (2mn-3n^2, m^2-3n^2)$ или $(b,c) = (3n^2-2mn, 3n^2-m^2)$, при чему други случај одбацујемо из истог разлога као у 1°.

Дакле, имамо $b = 2mn-3n^2$ и $c = m^2-3n^2$. Слично као пре, сменом $c = (m-\frac{l}{s}n)^2$ налазимо:

$$\frac{m}{n} = \frac{3s^2+l^2}{2ls}$$

Сада је $\frac{b}{n^2} = \frac{2m}{n} - 3 = \frac{3s^2-3ls+l^2}{ls}$ квадрат рационалног броја, па је и број $ls(3s^2-3ls+l^2) = f(s,l)$ квадрат природног броја.

Међутим, није тешко уверити се да је пар $(s,l)$ мањи од пара $(b,c)$. Тако смо и у овом случају изградили нови и мањи пар узајамно простих бројева који испуњавају задату особину.

Дакле, једначина $x^2 - y^3 = 1$ у скупу позитивних рационалних бројева има јединствено решење $(x,y) = (3,2)$. □

## 4.2 Случај $q > 3$ - Чејнов доказ

Овде ћемо доказати да једначина $x^2 - y^q = 1$ нема решења у скупу природних бројева ако је $q$ прост број већи од 3. Доказ који наводимо дело је математичара Јозефа Е. З. Чејна.

Ако би $x$ било парно, $x-1$ и $x+1$ би били узајамно прости, па би оба била $q-$ти степени природних бројева. Међутим, разлика два $q-$та степена не може бити 2 за $q > 1$. Одавде је $x$ непарно и $y$ парно.

Ако је $y = 2y'$, имамо $(x-1)(x+1) = 2^q y'^q$, при чему је највећи заједнички делилац чинилаца са леве стране 2. Одавде је један од чинилаца облика $2^{q-1}m^q$, а други $2n^q$.

Доказ ће бити директна последица следеће две леме:

**Лема 4.1.** Мора важити $q \mid x$.

*Доказ:* Претпоставимо супротно, то јест да $q \nmid x$. Запишимо једначину као:

$$x^2 = y^q + 1 = (y+1)(y^{q-1} - y^{q-2} + ... - y + 1)$$

Слично као пре, можемо закључити да ако $q \nmid x$, онда два чиниоца морају бити узајамно прости, па зато оба морају бити потпуни квадрати.

Дакле, за неки природан број $t$ је $y = t^2 - 1$.

Из једначине видимо да је пар $(x, y^{\frac{q-1}{2}})$ решење Пелове једначине $a^2 - yb^2 = 1$.

Јасно је да је $(t, 1)$ њено минимално решење. Како најмање решење класичне Пелове једначине генерише сва њена решења (видети [5]), знамо да за неки природан број $m$ важи:

$$x + y^{\frac{q-1}{2}}\sqrt{y} = (t + \sqrt{y})^m$$

(јасно је да $y = t^2 - 1$ није квадрат, па је представљање $u + v\sqrt{y}$ јединствено за целе бројеве $u$ и $v$).

Надаље све конгруенције радимо у прстену $\mathbb{Z}[\sqrt{y}]$, у стандардном смислу:

$$s + t\sqrt{y} \equiv u + v\sqrt{y}\ (mod\ j) \iff \exists k, l \in \mathbb{Z},\ j(k + l\sqrt{y}) = (s + t\sqrt{y}) - (u + v\sqrt{y}).$$

Посматрањем наше једначине по модулу $y$ и употребом биномне формуле, јасно је да важи:

$$x \equiv t^m + mt^{m-1}\sqrt{y} \ (mod\ y)$$

Сада се лако закључује (пошто су 1 и $\sqrt{y}$ линеарно независни фактори у $\mathbb{Z}[\sqrt{y}]$) да $y \mid x - t^m$ и $y \mid mt^{m-1}$, а како је $(y, t) = (t^2 - 1, t) = 1$, закључујемо да $y \mid m$.

Сетимо се да из претходног знамо да је $y$ парно, одакле $m$ мора бити парно, $m = 2m'$. Сада наша почетна једначина има облик:

$$x + y^{\frac{q-1}{2}}\sqrt{y} = (t + \sqrt{y})^m = (t + y + 2t\sqrt{y})^{m'},$$

па редукцијом ове једначине по модулу $t$ закључујемо да $t \mid x - y^{m'}$ и $t \mid y^{\frac{q-1}{2}}\sqrt{y}$. Из последњег закључујемо да $t \mid y^q = (t^2 - 1)^q$, па је $t = 1$. Међутим, тада је $y = 0$, што је немогуће.

На овај начин смо дошли до контрадикције претпоставком да $q \mid x$, одакле следи тврђење. □

**Лема 4.2.** $x \equiv \pm 3 \ (mod\ q)$.

*Доказ:* Из наше једначине је $x^2 - 1 = (x - 1)(x + 1) = y^q$.

Претпоставимо да је $x - 1 = 2^{q-1}m^q$ и $x + 1 = 2n^q$. Доказаћемо да је овде $x \equiv 3 \ (mod\ q)$. У другом случају поступа се аналогно и добија сличан резултат $x \equiv -3 \ (mod\ q)$.

Уочимо следећу једнакост:

$$(\frac{x-3}{2})^2 = (\frac{x+1}{2})^2 - 2(x - 1) = n^{2q} - (2m)^q$$

Претпоставимо сада да $q \nmid x - 3$. Сада је $t = \frac{x-3}{2}$ природан број који није дељив са $q$ (јасно је да је $x > 3$ на почетку, јер за мање $x$ нема решења).

Како је $(x - 1, x + 1) = 2$ и $q > 3$, јасно је да је $n$ непарно и $(m, n) = 1$. Сада је јасно да је $(n^2, 2m) = 1$. Закључујемо да је за узајамно просте бројеве $u = n^2$, $v = 2m$ и природан број $t$ испуњена једначина:

$$t^2 = u^q - v^q = (u - v)(u^{q-1} + u^{q-2}v + ... + v^{q-2}u + v^{q-1})$$

Сада ћемо показати да уколико $q \nmid t$, то јест $q \nmid u - v$ мора важити да су чиниоци с десне стране узајамно прости природни бројеви, одакле оба морају бити потпуни квадрати.

Заиста, ако неки прост број $r \neq q$ дели оба чиниоца, имамо да је $u \equiv v \ (mod\ r)$, а пошто дели други чинилац, имамо:

$$0 \equiv (u^{q-1} + u^{q-2}v + ... + v^{q-2}u + v^{q-1}) \equiv qu^{q-1} \ (mod\ r),$$

одакле $r \mid u$, па $r \mid v$, што је немогуће јер су $u$ и $v$ узајамно прости бројеви.

Дакле, $u - v = n^2 - 2m$ је потпут квадрат. Он је очито мањи од $n^2$, па је:

$$n^2 - 2m \leq (n-1)^2 \Rightarrow 2m \geq 2n - 1 \Rightarrow m \geq n$$

Међутим, подсетимо се да је $x - 1 = 2^{q-1}m^q$ и $x + 1 = 2n^q$, одакле је $2^{q-2}m^q + 1 = n^q$, што је сада немогуће јер је $2^{q-2} > 1$ и $m \geq n$.

Дакле, наша претпоставка $q \nmid x - 3$ је погрешна, одакле следи тврђење. □

На основу ове две леме закључујемо да $q \mid 3$, одакле следи да наша једначина $x^2 - y^q = 1$ нема решења у скупу природних бројева за прост број $q > 3$.

# 5

# Један генералан закључак

У досадашњем делу рада позабавили смо се случајевима када је неки од $p$ и $q$ једнак 2. Сада ћемо претпоставити да су оба броја већа од 2.

У овом поглављу доказаћемо да $p \mid y$ или $q \mid x$. Поменућемо још и да је британски математичар Џон В. С. Каслс је 1960. године доказао да обе релације важе.

Јасно је да су $p$ и $q$ различити прости бројеви, јер разлика два $p-$та степена природних бројева не може бити 1. Доказаћемо да ако је $p > q$ онда $q \mid x$, односно да у случају $p < q$ имамо $p \mid y$. Ова два случаја су врло слична, па ћемо доказати први, а други препустити читаоцу.

**Лема 5.1.** Ако је $p > q$, онда $q \mid x$.

*Доказ:* Претпоставимо да је $p > q$ и $q \nmid x$. Записаћемо почетну једначину у облику:

$$x^p = y^q + 1 = (y+1)(y^{q-1} - y^{q-2} + ... - q + 1),$$

Из истог разлога као пре, ако два чиниоца с десне стране нису дељива с $q$, они морају бити узајамно прости. То значи да су оба потпуни $p-$ти степени, па је за неки природан број $t \geq 2$ испуњено $y = t^p - 1$. Дакле, имамо $x^p = (t^p - 1)^q + 1 < (t^p)^q = t^{pq}$, одакле је $x < t^q$.

Међутим, то значи да је $(t^q - 1)^p \geq x^p = (t^p - 1)^q + 1 > (t^p - 1)^q$, па дизањем ове неједнакости на степен $\frac{1}{pq}$ закључујемо:

$$(t^q - 1)^{\frac{1}{q}} > (t^p - 1)^{\frac{1}{p}}$$

Доказаћемо да је функција $f(x) = (t^x - 1)^{\frac{1}{x}}$ строго растућа за $x > 0$ и $t > 1$, чиме долазимо до контрадикције јер је $p > q$.

Лако рачунамо: $f'(x) = \frac{(t^x-1)^{\frac{1}{x}-1}}{x^2}(t^x \cdot x \cdot \ln t - (t^x - 1) \cdot \ln(t^x - 1)) > 0$, јер је први чинилац очигледно позитиван, а пошто је $t^x > t^x - 1$ и $x \cdot \ln t = \ln(t^x) > \ln(t^x - 1)$, и други је позитиван.

Овиме смо показали да $q \mid x$. □

Доказаћемо још једну лему која говори о томе да $x$ мора бити „велико" у односу на $p$ и $q$ када је $p > q$.

**Лема 5.2.** Ако је $p > q$, онда је $x > q + q^{p-1}$. Слично, за $p < q$ је $y > p + p^{q-1}$.

*Доказ:* Претпоставимо да је $p > q$ и докажимо да је $x > q + q^{p-1}$. Неједнакост у случају $p < q$ се доста слично доказује (приметимо да уз услов да су $x$ и $y$ природни, једначина није скроз симетрична по $p$ и $q$, па не можемо претпоставити њихов поредак без умањења општости. Међутим, ако кажемо да су $x$ и $y$ цели, њиховим негирањем по потреби то можемо урадити, при чему ће наше неједнакости бити $|x| > q + q^{p-1}$, односно $|y| > p + p^{q-1}$), па је препуштамо читаоцу.

По претходној леми, знамо да су $y + 1$ и $\frac{y^q+1}{y+1}$ дељиви са $q$. Из дела 2.1 сећамо се да $\frac{y^q+1}{y+1}$ не може бити дељив са $q^2$.

Пошто је $x^p$ дељиво са $q^p$, $y+1$ мора бити дељиво са $q^{p-1}$. Јасно је да су онда $\frac{y+1}{q^{p-1}}$ и $\frac{\frac{y^q+1}{y+1}}{q}$ узајамно прости природни бројеви чији је производ $(\frac{x}{q})^p$, па они морају бити потпуни $p-$ти степени природних бројева.

Дакле, за неке природне бројеве $a$ и $b$ је:

$$y + 1 = q^{p-1}a^p, \ \frac{y^q + 1}{y + 1} = qb^p \text{ и } x = qab.$$

Одавде је $q^{p-1} \mid y+1 \implies qb^p = y^{q-1}-...-y+1 \equiv (-1)^{q-1}-(-1)^{q-2}+...-(-1)+1 \equiv q \ (mod\ q^{p-1}) \implies q^{p-2} \mid b^p - 1$.

Знамо да је $p > 2$, па између осталог $q \mid b^p - 1$. То значи да је поредак броја $b$ по модулу $q$ делилац броја $p$, па је он 1 или $p$. Последње је немогуће, јер знамо да тај поредак мора делити $q - 1 < p$. Дакле, $q \mid b - 1$.

По Леми о дизању на експонент, знамо да је, због $q \mid b-1$, задовољена једнакост $v_q(b^p - 1) = v_q(b - 1) + v_q(p) = v_q(b - 1)$, одакле закључујемо да $q^{p-2} \mid b - 1$. Алтернативно, због $b \equiv 1 \ (mod\ q)$ и $q^{p-2} \mid (b - 1)(b^{p-1} + b^{p-2} + ... + b + 1)$ знамо да други чинилац даје остатак $p$ при дељењу са $q$, одакле је други чинилац узајамно прост са $q$, па $q^{p-2} \mid b - 1$.

Из последње релације је $b \geq 1 + q^{p-2}$ (не може бити $b = 1$, јер би тада било $q = \frac{y^q+1}{y+1} = 1+y(y-1)+y^3(y-1)+...+y^{q-2}(y-1) \geq 1+\frac{q-1}{2}y(y-1) \geq 1+\frac{q-1}{2}2y = 1+(q-1)y > q$ за $y > 2$ - изузетак $y = 2$ смо анализирали у првом случају дела 2.1).

Из последње неједнакости је сада јасно да је $x = qab \geq qb \geq q(q^{p-2}+1) = q^{p-1}+q$, чиме је лема доказана. $\square$

# 6

# Михајлескуове леме

У овом поглављу ћемо навести без доказа неколико сложенијих резултата које је Михајлеску извео, а који су били кључни за решавање Каталанове претпоставке. Такође, коментарисаћемо зашто су они довољни за сам доказ.

Посматрајмо једначину $x^p - y^q = 1$ за непарне $p$ и $q$ (подсетимо се да смо случајеве када је неки од $p$ и $q$ једнак 2 већ дискутовали). Тада важи:

1° (Доказано 2000.) $p^{q-1} \equiv 1 \ (mod\ q^2)$ и $q^{p-1} \equiv 1 \ (mod\ p^2)$;

2° (Доказано 2002.) $p \equiv 1 \ (mod\ q)$ или $q \equiv 1 \ (mod\ p)$;

3° (Доказано 2003.) $p < 4q^2$ и $q < 4p^2$.

Ови услови доказани су уз претпоставку $x^p - y^q = 1$. Сада можемо оставити ту једначину по страни и из три леме закључити да не постоје овакви парови непарних простих бројева.

Без умањења општости, нека у услову 2° важи $p \equiv 1 \ (mod\ q)$.

Доказаћемо да из овога и $p^{q-1} \equiv 1 \ (mod\ q^2)$ следи $p \equiv 1 \ (mod\ q^2)$.

Наше тврђење следи директно из Леме о дизању на експонент (уз стандардне ознаке испод):

$$2 \leq v_q(p^{q-1} - 1) = v_q(p-1) + v_q(q-1) = v_q(p-1),$$

због $p \equiv 1 \ (mod\ q)$, одакле следи тврђење.

За читаоце којима је Лема о дизању на експонент непозната, наводимо још један једноставан доказ.

Нека је $p = kq + 1$. Довољно је показати да $q \mid k$. Израчунаћемо $p^{q-1}$ преко биномне формуле:

$$p^{q-1} = (kq+1)^{q-1} = \sum_{i=0}^{q-1} \binom{q-1}{i} (kq)^i = 1 + (q-1)kq + q^2 \sum_{i=2}^{q-1} \binom{q-1}{i} k^i q^{i-2} \equiv$$
$$\equiv 1 + (q-1)kq \ (mod\ q^2),$$

одакле закључујемо да $q \mid k$ јер је $(q, q-1) = 1$.

Сада из $p \equiv 1 \ (mod\ q^2)$ и $p < 4q^2$ (из $3^\circ$), закључујемо да због $p \neq 1$ број $p$ узима неку од следећих вредности: $q^2+1$, $2q^2+1$ или $3q^2+1$. Како је $q > 2$, оно је непарно, па прва и трећа могућност одмах отпадају јер су то парни бројеви већи од 2, па $p$ не би био прост.

Дакле, мора бити $p = 2q^2 + 1$.

Међутим, како квадрат природног броја који није дељив са 3 даје остатак 1 при дељењу са 3, ако је $q > 3$ број $p = 2q^2 + 1$ био би дељив са 3 и већи од 3, па $p$ не би био прост.

Одавде закључујемо да је $q = 3$ и $p = 2q^2 + 1 = 19$.

Међутим, лако рачунамо: $3^{18} \equiv 729^3 \equiv 7^3 \equiv 343 \neq 1 \ (mod\ 19^2 = 361)$, што противречи услову $1^\circ$.

Дакле, ове леме довољне су за доказ Каталанове претпоставке уколико су $p$ и $q$ непарни бројеви. □

# 7

# Закључак

Током рада смо се бавили решавањем једначине $x^p - y^q = 1$, где су $x$ и $y$ природни бројеви већи од 1, а $p$ и $q$ прости бројеви. У другој глави решили смо случај када је $y$ степен простог броја, затим покушали да решимо случај кад је $x$ степен простог броја. Наишли смо на потенцијалну препреку: када је $q = 2$, не можемо искористити особину степена простог броја на неки посебан начин. Тако смо отворили случај $q = 2$ и решили га за произвољне $x, y \geq 2$ и прост $p$. У четвртом поглављу бавили смо се једначином када је $p = 2$ и приметили да се једино решење $(3, 2, 2, 3)$ налази ту. Даље смо анализирали доња ограничења за $x$ и $y$ и доказали да $q \mid x$ или $p \mid y$. На крају, у шестом поглављу, навели смо леме које је Михајлеску доказао и које су биле довољне за комплетирање доказа Каталанове претпоставке.

Искористио бих прилику да захвалим свом ментору, Стевану Гајовићу, на корисним сугестијама око рада и помоћи у избору литературе. Захваљујем свим професорима Математичке гимназије на несебичној пажњи и залагању, којима су допринели развоју моје љубави према математици. На крају, захваљујем свим својим другарима са којима сам провео незаборавних шест година у Математичкој гимназији.

# Литература


[1] René Schoof, *Catalan's Conjecture*, Springer Universitext, Springer Verlag, London, 2008.

[2] Yuri F. Bilu, Yann Bugeaud, Maurice Mignotte, *The Problem of Catalan*, Springer Universitext, 2014.

[3] Yuri F. Bilu, *Catalan's conjecture (after Mihailescu)*, Sém, Bourbaki Exp. 909, Nov. 2002.

[4] Раширења целих бројева https://imomath.com/srb/dodatne/rasirenja-Q_ddj.pdf

[5] Пелова једначина https://imomath.com/srb/dodatne/Pelovajedn_ddj.pdf