Микола Танчук

РОЗГАДКА ТАЄМНИЦІ ДОВЕДЕННЯ ВЕЛИКОЇ ТЕОРЕМИ П'ЄРА де ФЕРМА. ТРИСЕКЦІЯ ДОВІЛЬНИХ ПЛОСКИХ КУТІВ І КВАДРАТУРА КРУГА

шукаємо, знаходимо, порівнюємо, пізнаємо…

Україна

м. Київ 2016

УДК 519.64
ББК 22.1я9

Танчук Микола. Розгадка таємниці доведення великої теореми П'єра де Ферма. Трисекція довільних плоских кутів і квадратура круга. – К.: ДЕТУТ, 2016. – 36 с.

У брошурі розміщений матеріал, що стосується розгляду нелінійних діофантових рівнянь (велика теорема Ферма), також доведено, що рівняння $X^n + Y^n = Z^n$ не має розв'язку в цілих числах $X > 0$, $Y > 0$, $Z > 0$ для всіх натуральних $n > 2$.

Зроблений короткий історичний огляд щодо доведення цієї теореми багатьма математиками світу упродовж майже 400 років.

Залишений запис П'єром де Ферма на полях перекладу «Арифметики» Діофанта: «Я знайшов цьому воістину дивовижне доведення, але поля тут занадто вузькі, щоб умістити його», завжди магічно впливав на тих, хто намагався відшукати алгоритм розв'язку цієї складної задачі, хоча жодному з них так і не вдалося відшукати, окрім часткових випадків, повного її розв'язку. Зрештою, 2015 року, мені пощастило розгадати таємницю алгоритму доведення великої теореми П'єра де Ферма і вперше, в брошурі, наводиться моє повне доведення цього твердження лише за допомогою властивостей порівнянь і малої теореми Ферма, якими на той час досконало володів П'єр де Ферма.

Більше того, справедливість великої теореми Ферма розширена на множини цілих і раціональних чисел.

Описується розв'язок двох древніх задач на побудову за допомогою циркуля і лінійки – трисекцію плоских кутів і розв'язання задачі квадратури круга. В результаті візуального аналізу побудованої конструкції квадрата, рівновеликого одиничному кругу, отримано нове фундаментальне значення для **числа $\pi = 3.2$.**

До цих двох задач наведені відповідні рисунки, виконані за допомогою **Paint**.

Вся текстова інформація підготовлена з використанням **Microsoft Word 2010**.

ISBN 978-966-2197-92-1

Зміст

До 350-ї річниці від дня смерті великого французького математика П'єра де Ферма (17.08.1601 – 12.01.1665)

У 2015 році (12.01) виповнилося 350 років від дня смерті видатного французького математика П'єра де Ферма, одного із творців аналітичної геометрії, математичного аналізу, теорії імовірностей, теорії чисел.

Найбільше він відомий своєю знаменитою великою теоремою Ферма: доказати, що рівняння $X^n + Y^n = Z^n$ не має розв'язку в цілих числах: $X > 0$, $Y > 0$, $Z > 0$ для всіх натуральних значень $n > 2$, яка була ним сформульована ще в 1637 році.

Розв'язком цієї задачі займалися досить відомі математики, а саме: Л. Ейлер, А. Лежандр, Ж. Л. Лагранж, К. Ф. Гаусс, П. Л. Чебишев, Е. Куммер та багато інших, але нікому з них так і не пощастило знайти загальний розв'язок цієї задачі.

Ось деякі дані, взяті в інтернеті щодо результатів доведення великої теореми Ферма упродовж майже 400 років:

«Випадок, коли $n = 3$, було доказано Ейлером ще в 1768 році. І потрібно було ще багато років, щоб теорія, якою необґрунтовано користувався Ейлер при своєму доведенні, була доведена Гауссом. Доведення теореми Ферма для випадку, коли $n = 5$, запропонували в 1825 році майже одночасно Лежен Діріхле і Лежандр. Своє доведення Діріхле опублікував у 1828 році, однак воно було досить складним і, в 1912 році, його упростив Племель.

Для наступного простого показника $n = 7$ теорема Ферма була доведена лише в 1839 році Ламе. Доведення Ламе було удосконалене, майже зразу ж, Лебегом. У 1847 році Ламе сповістив, що йому вдалося знайти доведення теореми Ферма для всіх простих показників $n \geq 3$.

Метод Ламе був надто віддаленим від розвитку ідей Ейлера і базувався на арифметичних властивостях чисел. Проте зразу ж Ліувіль віднайшов у дослідженнях Ламе серйозну прогалину, чим і спростував це доведення. Ламе був змушений визнати свою помилку. Софі Жермен довела так званий «перший випадок» великої теореми для «простих чисел Софі Жермен«, довівши, що рівняння Ферма не має вирішення, коли $n = p-1$, де p – просте число вигляду $8k+7$. Наприклад, якщо $k = 2$, то p – просте число, а саме 23, і $n = 22$.

На ЕОМ, користуючись ідеями Куммера і Вандивера, доказали справедливість теореми Ферма для всіх простих показників $n < 100\,000$».

Привабливість теореми Ферма очевидна: немає іншого математичного твердження з таким простим формулюванням і уявною доступністю доведення, який би викликав такий ажіотаж.

Окрім того, завжди приваблювала ймовірність елементарного доведення, тому що сам Ферма, очевидно, знав доведення, написавши на полях перекладу «Арифметики» Діофанта: «Я знайшов цьому воістину дивовижне доведення, але поля тут занадто вузькі, щоб умістити його».

Додатковим стимулом слугувала ще й солідна премія в 100 000 марок, заснована німцем Вольфскелем у 1908 році, яка призначалась тому, хто першим подасть правильний розв'язок цієї задачі.

Є інформація про те, що розв'язок великої теореми Ферма в 1994 році отримав англійський математик Ендрю Уайлс за допомогою сучасних, спеціально розроблених ним методів, які не могли бути доступними для Ферма.

Після появи доведення великої теореми Ферма Уайлсом постало питання його доступного викладу, оскільки більшість математиків у світі знають про це, але говорити про усвідомлення цього доведення можуть лише деякі з них.

Ось деякі витяги з книги Саймона Сінгха «Великая теорема Ферма», що характеризують проблему Ферма в усіх ракурсах:

«Помітка на полях «Арифметики» Діофанта, написана рукою П'єра де Ферма, породила одну з найскладніших головоломок в історії математики.

Незважаючи на триста років блискучих провалів і припущення Геделя про те, що полювання, можливо, іде за неіснуючим доведенням, проблема Ферма й досі нестримно приваблює деяких математиків. Велика теорема Ферма була математичною сиреною, яка вабила геніїв лише для того, щоб ущент розбити їхні надії. Кожен математик, що вирішив зайнятися великою теоремою Ферма, ризикував даремно витратити свої найактивніші роки.

Одначе той, кому вдалося б зробити рішучий прорив, ввійшов би в історію, як людина, що знайшла розв'язок найскладнішої задачі у світі. Велика теорема Ферма – задача неймовірно трудна, і все ж таки її можна сформулювати так, що вона стане зрозумілою навіть школяру. Ні у фізиці, ні в хімії, ні в біології немає жодної проблеми, яка формулюється так просто і зрозуміло й залишається нерозв'язаною так довго.

У своїй книзі «Велика проблема» Е.Т. Белл висловив припущення, що, можливо, наша цивілізація підійде до кінця раніше, ніж пощастить довести велику теорему Ферма. Доведення великої теореми Ферма стало найціннішим призом у теорії чисел, і тому не дивно, що пошуки його привели до деяких найбільш захоплюючих епізодів в історії математики. До таких пошуків були залучені видатні уми нашої планети, за доведення виділялись величезні премії. Через велику теорему Ферма люди бились на дуелі, а декотрі, зневірившись знайти доведення, навіть заподіювали собі смерть. Статус «великої головоломки» вийшов за рамки замкнутого світу математики.

У 1958 році велика теорема Ферма проникла навіть у легенду про Фауста. У збірнику «Як мати справу з дияволом» була опублікована новела Артура Порджеса «Саймон Флегг і Диявол». В ній диявол звертається до професора математики Саймона Флегга з пропозицією задати йому, дияволу, яке-небудь запитання. Якщо дияволу вдасться знайти відповідь за двадцать чотири години, то він отримає душу Саймона. У випадку невдачі диявол зобов'язаний виплатити Саймону 100 000 доларів. Саймон задає дияволу запитання: «Чи справедлива велика теорема Ферма?». Диявол зникає і носиться світами, збираючи по крихті всі досягнення математики. Наступного дня він

повертається і визнає свою поразку: «Ви виграли, Саймон, – сказав диявол, шанобливо дивлячись на професора. – Навіть мені не посилі вивчити всю математику, яка необхідна для розв'язку настільки трудної задачі за такий короткий час. Чим глибше я занурююсь у цю проблему, тим стає вона труднішою. Неєдиний розклад на множники, ідеальні числа… Та що даремно говорити! Знаєте, – зізнався диявол, – навіть найкращі математики на інших планетах, а вони, маю вам сказати, набагато випередили ваших, не розв'язали її. Узяти хоча б того хлопця на Сатурні, що дуже схожий на гриба на ходулях. Він усно розв'язує диференціальні рівняння в частинних похідних. Однак навіть він не зміг упоратися з цією задачею».

Велика теорема Ферма заволоділа думками поколінь математиків через дві причини. По-перше, ними рухало нестримне бажання продемонструвати свою перевагу. Велика теорема Ферма була незаперечним критерієм, і кожен, хто зумів би її довести, мав би успіх там, де зазнали поразки Коші, Ейлер, Куммер і багато інших математиків. Подібно до того, як сам Ферма отримував величезне задоволення від розв'язку задач, що ставили в глухий кут його сучасників, той, кому пощастило б знайти доведення великої теореми Ферма, зміг би радіти тому, що зумів розв'язати проблему, яка декілька віків височіла неприступною фортецею перед математичною спільнотою. По-друге, кожен, хто зміг би відповісти на виклик Ферма, пізнав би почуття нечуваного задоволення від того, що зумів розв'язати найскладнішу головоломку. Захоплення, отримане від розв'язку найскладнішої проблеми теорії чисел, доступної лише тим, хто на цьому розуміється.

Щодо цього можна навести окремі витяги з роботи Дмитра Абрарова «Теорема Ферма: феномен доказательств Уайлса»: «Уся довга історія загадкової теореми супроводжувалась постійними оголошеннями про її доведення, починаючи з самого Ферма. Наявні помилки в нескінченному потоці доказів охоплювали не тільки математиків-любителів, а й математиків-професіоналів. Це призвело до того, що термін «ферматист», який стосувався тих, хто доказував теорему Ферма, став негативним. Інтрига, що постійно зберігалася з її доведенням, приводила, іноді, до смішних казусів. Так, коли в першому варіанті її широко розрекламованого доведення Уайлса знайшлася неточність, на одній із станцій метро з'явився єхидний напис: «Я знайшов, справді, чудове доведення великої теореми Ферма, але підійшов мій поїзд і я не встигаю його записати».

Задача роз'яснення такого супердоведення є абсолютно самостійною і зовсім непростою, хоча й перспективною проблемою. Отже, якщо говорити коротко, то на сьогодні факт доведення Уайлса є просто фактом доведення теореми Ферма із статусом першого правильного доведення і використання в ньому «надпотужної математики». І все ж таки, поставимо тепер запитання: чи можливо в достатньо доступних термінах описати доведення Уайлса для широкої аудиторії? З точки зору спеціалістів – це абсолютна утопія». Щодо

інформації про велику теорему Ферма, можна навести витяг із роботи Фелікса Кірсанова «История великой теоремы Ферма»:

«Доведення великої теореми Ферма можна поставити в один ряд із такими досягненнями XX ст., як винахід комп'ютера, ядерної бомби і політ у космос. Хоча про нього і не так широко відомо, тому що не стосується сфери наших безпосередніх потреб, як наприклад, телевізор або електрична лампочка, але воно стало спалахом нової зірки, яка, як і всі непорушні Істини, завжди буде світити людству… А тепер повернімося до початку нашої історії, пригадаємо запис П'єра Ферма на полях книги Діофанта і ще раз поставимо запитання: чи дійсно Ферма довів свою теорему? Цього ми, звичайно, не можемо знати насправді, і як у будь-якій справі тут виникають різні версії.

Версія 1: Ферма довів свою теорему (На запитання: «Чи мав Ферма точно таке ж доведення своєї теореми?», Ендрю Уайлс зауважив: «Ферма не міг володіти таким доведенням. Це доведення XX століття». Ми з вами розуміємо, що в XVII ст. математика, звичайно ж, була не та, що в кінці XX ст., в ту епоху д'Артаньяна, «цариця наук» ще не володіла тими відкриттями (модулярні форми, теореми Таніями, Фрея та інші), завдяки яким можна було довести велику теорему Ферма. Звичайно, можна припустити: чим чорт не жартує – а раптом Ферма здогадався іншим шляхом? Ця версія хоча й вірогідна, але, за оцінками більшості математиків, практично неможлива).

Версія 2: П'єру Ферма здалося, що він довів свою теорему, але в його доведенні були помилки (Тобто, сам Ферма був також і першим фермистом).

Версія 3: Ферма свою теорему не довів, а на полях просто збрехав. Якщо правдива одна з двох останніх версій, що найбільше ймовірно, то тоді можна зробити простий висновок: видатні люди, вони хоча й видатні, але також можуть помилятися або інколи, навіть, прибрехати (в основному цей висновок буде корисним тим, хто схильний безмежно довіряти своїм кумирам та іншим володарям думок). Тому, читаючи твори авторитетних синів людства або слухаючи їхні пафосні виступи, ви маєте повне право сумніватися в їхніх твердженнях (Прошу взяти до уваги, що сумніватися – не означає заперечувати)».

Тут слід навести ще витяг із роботи А. М. Бєлова: «О доказательстве большой теоремы Ферма элементарыми методами, известными во время жизни Пьера де Ферма»: «Очевидно, в даний час існує лише єдине таке доведення, що вважається достовірним. Це доведення великої теореми Ферма, виконане 19-го вересня 1994 року професором Принстонського університету Эндрю Уайлсом. Але необхідно враховувати, що Уайлс у своєму доведенні опирався на відносно слабо використовувану на практиці теорію арифметичної алгебраїчної геометрії і низку сучасних математичних інструментів, створених великою кількістю математиків за останні сто років, які були відсутніми за життя П'єра де Ферма. В результаті він отримав доведення досить об'ємне (в журнальному варіанті займає 120 сторінок) і складне для розуміння навіть професіональними математиками, виконане методами, недоступними за життя П'єра де Ферма.

Як наслідок цього, реакція на представлене Эндрю Уайлсом доведення була досить нейтральною навіть серед математичної спільноти. Окрім того, що доведення було надзвичайно складним, а це означає, що перевірити його на надійність досить важко, усі очікували зовсім іншого доведення, в усякому разі, отриманого не будь-якою ціною.

Вся справа в тому, що велика теорема Ферма набула надзвичайної популярності, в основному, завдяки зробленому П'єром де Ферма на полях перекладу «Арифметики» Діофанта запису: «Я знайшов цьому воістину дивовижне доведення, але поля тут занадто вузькі, щоб умістити його». І, звичайно, очікувалось доведення, виконане елементарними методами, доступними за життя П'єра де Ферма. Очевидно, прихильники доведення Уайлса намагаються усіх переконати в тому, що методологічна складність властива всім сучасним великим доведенням і в майбутньому буде тільки зростати, що П'єр де Ферма помилявся, стверджуючи, що знайшов доведення своєї теореми, тому що довести її методами, які відрізняються від методів Уайлса, нібито, неможливо у зв'язку з мінімальністю математичних інструментів Уайлса. Але якщо врахувати, що через складність і об'ємність доведення Уайлса все ще зберігає імовірність наявності в ньому помилок, а також уточнення формулювання теореми в цій статті, то й подібні висловлювання, скоріше за все, є черговою помилкою».

До речі, цей же А. М. Бєлов у своїй роботі намагається обґрунтувати існування розв'язку великої теореми Ферма на безмежності, а також можливий варіант розв'язку цієї задачі за допомогою нумерології (чистий абсурд). (Детальніше про це читайте в інтернеті: Саймон Сингх: «Великая теорема Ферма»; Дмитрий Абраров: «Теорема Ферма: феномен доказательств Уайлса»; Феликс Кирсанов: «История великой теоремы Ферма»; А. М. Бєлов: «О доказательстве большой теоремы Ферма элементарными методами, известными во время жизни Пьера де Ферма»).

Мати у своєму розпорядженні потрібні математичні інструменти – замало, треба ще вміти ними розумно користуватися.

У Ендрю Уайлса були такі інструменти: теорія порівнянь з усіма її властивостями, серед яких і мала теорема Ферма, тобто все те, що потрібно для роботи з цілими числами й елементарними арифметичними операціями в співвідношеннях між ними. Але цього, очевидно, було недостатньо, тому що бажання за будь-яку ціну довести велику теорему Ферма змусило його шукати і створювати нові математичні інструменти. Врешті, знайдено, доведено, але досить складно і сумнівно.

Якщо не сучасники, то нащадки розберуться, що до чого. Головне – результат є і вперше повністю доведена велика теорема Ферма.

Сумніви щодо доведення Ендрю Уайлсом великої теореми Ферма існують не тільки з точки зору мінімального набору інструментів для виконуваних розрахунків (яких саме?), а й сумнівна єдина функція Фрея для тестування.

Невже це достатня інформація для того, щоб робити логічний висновок щодо справедливості великої теореми Ферма?

Я, врешті, знайшов розв'язок великої теореми Ферма доступними йому методами, а це означає, що він володів алгоритмом розв'язку цієї задачі.

Вперше, майже після 400 років, знайдене доведення на підставі відомих за часів Ферма методів і знань із теорії чисел, по-перше, дає довгоочікувану відповідь тим сучасним математикам, які продовжують наполягати, що «велика теорема Ферма не має доведення відомими за часів Ферма засобами і тому знайдене Ферма доведення було невірним (бо якби воно було вірним, то, мовляв, було б віднайдене протягом майже 400 (!) років наполегливих пошуків математиками всього світу)».

По-друге, моїм доведенням підтверджується відомий у світі високий рейтинг української математики. На мою думку, знайдений і наведений у моїй роботі алгоритм доведення великої теореми Ферма настільки простий, прозорий, логічний і зрозумілий, що його сміливо можна назвати перлиною мистецького витвору в математиці, в теорії чисел.

У моїй брошурі [4], надрукованій 2015 року в м. Києві, хоча й стисло, але послідовно наведено алгоритм доведення великої теореми Ферма спочатку для всіх парних степенів за допомогою властивостей порівнянь, потім і для всіх непарних степенів із застосуванням малої теореми Ферма, саме так, його теореми, що спростовує всілякі сумніви щодо того: знав чи ні він доведення своєї теореми.

Маю надію, що моя робота знайде серед математиків тих, які спроможні оцінити це, знайдене в Україні, важливе для світової математики, перше повне доведення цієї теореми методами, добре відомими Ферма, за ці рівно 350 років (12. 01. 2015 р.), що проминули від дня його відходу в інший світ у 1665 році.

Читачам, які недостатньо володіють необхідними знаннями з теорії порівнянь і алгебри логіки, для того, щоб краще зрозуміти алгоритм доведення великої теореми Ферма, нижче, на допомогу їм, наводяться, частково, короткі теоретичні відомості з цих предметів.

Порівняння

Візьмемо довільне фіксоване натуральне число m і будемо розглядати лишки при діленні на m різних цілих чисел. При розгляді цих лишків і виконання операцій над ними зручно ввести поняття порівняння за модулем.

Означення 01. Цілі числа a і b називаються порівнянні між собою за модулем m, якщо їхня різниця $a - b$ ділиться на m, тобто $mIa - b$.

Таким чином, порівняння є співвідношенням між трьома числами a, b і m, причому m відіграє роль своєрідного еталона порівняння, який ми називаємо модулем. Коротко таке співвідношення між a, b, m запишемо у вигляді:

$$a \equiv b(\mathrm{mod}\ m),$$

a і b будемо називати відповідно лівою і правою частинами порівняння.

Число m, що стоїть під знаком модуля, будемо завжди вважати додатнім, тобто запис mod m означає, що $m \geq 1$. Якщо різниця $a - b$ не ділиться на m, то це записуємо так: $a \not\equiv b (\mathrm{mod}\, m)$.

Згідно з означенням, $a \equiv 0 \,(\mathrm{mod}\, m)$ означає, що a ділиться на m.

Приклади: $10 \equiv 1(\mathrm{mod}\ 3)$, $10 \equiv 1(\mathrm{mod}\ 9)$, $10 \equiv -1(\mathrm{mod}\ 11)$, $2 \equiv 0(\mathrm{mod}\ 2)$,
$2 \equiv 2(\mathrm{mod}\ 4)$, $10 \equiv 0(\mathrm{mod}\ 5)$, $10 \equiv 2(\mathrm{mod}\ 4)$, $-5 \equiv 17(\mathrm{mod}\ 11)$.

Порівняння чисел a і b за модулем m рівнозначне:

a) Можливість представити a у вигляді $a = b + m \cdot t$, де t – ціле.

b) Подільності $a - b$ на m.

Дійсно, із $a \equiv b(\mathrm{mod}\ m)$ випливає $a = m \cdot q + r$, $b = m \cdot q_1 + r$, $0 \leq r < m$,
звідси $a - b = m\,(q - q_1)$, $a = b + m \cdot t$, $t = q - q_1$.
Навпаки, із $a = b + m \cdot t$, представляючи b у вигляді $b = m \cdot q_1 + r$, $0 \leq r < m$,
знаходимо $a = m \cdot q + r$, $q = q_1 + \mathrm{t}$, тобто $a \equiv b(\mathrm{mod}\ m)$.

Властивості порівнянь

a) Два числа, порівнянні з третім, порівнянні між собою.

b) Порівняння можна почленно додавати.

Дійсно, нехай
$a_1 \equiv b_1(\mathrm{mod}\ m)$, $a_2 \equiv b_2(\mathrm{mod}\ m)$, . . . , $a_k \equiv b_k(\mathrm{mod}\ m)$.
Тоді
$a_1 = b_1 + m \cdot t_1$, $a_2 = b_2 + m \cdot t_2$, . . . , $a_k = b_k + m \cdot t_k$,
звідси
$a_1 + a_2 + \ldots + a_k = b_1 + b_2 + \ldots + b_k + m\,(t_1 + t_2 + \ldots + t_k)$,
або
$a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k\,(\mathrm{mod}\ m)$.

Доданок, який знаходиться в будь-якій частині порівняння, можна переносити в іншу частину, змінивши знак на протилежний.

Дійсно, додаючи порівняння $a + b \equiv c(\mathrm{mod}\ m)$ до очевидного порівняння
$-b \equiv -b(\mathrm{mod}\ m)$, маємо $a \equiv c - b(\mathrm{mod}\ m)$.

До кожної частини порівняння можна додати (або відняти від неї) довільне число, кратне модулю.

Дійсно, додаючи порівняння $a \equiv b(\mathrm{mod}\ m)$ до очевидного порівняння
$m \cdot k \equiv 0(\mathrm{mod}\ m)$, маємо: $a + m \cdot k \equiv b\ (\mathrm{mod}\ m)$.

c) Порівняння можна перемножувати між собою.

Дійсно, нехай
$a_1 \equiv b_1\,(\mathrm{mod}\ m)$, $a_2 \equiv b_2(\mathrm{mod}\ m)$, . . . , $a_k \equiv b_k(\mathrm{mod}\ m)$.
Тоді
$a_1 = b_1 + m \cdot t_1$, $a_2 = b_2 + m \cdot t_2$, . . . , $a_k = b_k + m \cdot t_k$,
звідси, перемножуючи між собою ці рівності, маємо:
$a_1 \cdot a_2 \cdot \ldots \cdot a_k \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_k + m \cdot N$, *де* N *– ціле.*
Згідно з означенням 01, маємо:
$a_1 \cdot a_2 \cdot \ldots \cdot a_k \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_k\,(\mathrm{mod}\ m)$.

Обидві частини порівняння можна піднести до одного степеня.

Це випливає із попереднього розгляду операції множення.

Обидві частини порівняння можна помножити на однакове число.

Дійсно, помноживши порівняння $a \equiv b(mod\ m)$ на очевидне порівняння $k \equiv k(mod\ m)$, маємо $a \cdot k \equiv b \cdot k(mod\ m)$.

d) Обидві частини порівняння можна поділити на їхній спільний дільник, якщо цей дільник взаємно простий з модулем.

Дійсно, із $a \equiv b(mod\ m)$, $a = a_1 \cdot d$, $b = b_1 \cdot d$, $(d, m) = 1$ випливає, що різниця $a - b$, рівна $(a_1 - b_1) \cdot d$, ділиться на m. Тому $a_1 - b_1$ ділиться на m, тобто, $a_1 \equiv b_1\ (mod\ m)$.

e) Обидві частини порівняння і модуль можна помножити на однакове ціле число.

Дійсно, із $a \equiv b(mod\ m)$ випливає $a = b + m \cdot t$, $a \cdot k = b \cdot k + m \cdot k \cdot t$, маємо: $a \cdot k \equiv b \cdot k\ (mod\ m \cdot k)$.

f) Обидві частини порівняння і модуль можна поділити на довільний їхній спільний дільник.

Дійсно, нехай: $a \equiv b(mod\ m)$, $a = a_1 \cdot d$, $b = b_1 \cdot d$, $m = m_1 \cdot d$.

Маємо: $a = b + m \cdot t$, $a_1 \cdot d = b_1 \cdot d + m_1 \cdot d \cdot t$, $a_1 = b_1 + m_1 \cdot t$, отже, $a_1 \equiv b_1(mod\ m_1)$.

g) Якщо порівняння $a \equiv b$ виконується для декількох різних модулів, то воно справедливе і для модуля, який є найменшим спільним кратним цих модулів.

Дійсно, із $a \equiv b(m_1)$, $a \equiv b(m_2)$, . . . , $a \equiv b(m_k)$ випливає, що різниця $a - b$ ділиться на всі модулі m_1 , m_2 ,. . . , m_k. Тому вона ділиться і на найменше спільне кратне цих модулів, тобто $a \equiv b(mod\ m)$, де $m = [m_1, m_2, . . ., m_k]$.

h) Якщо порівняння $a \equiv b$ виконується для модуля m, то воно справедливе і для всякого модуля d, який є будь-яким дільником числа m.

Дійсно, із $a \equiv b(mod\ m)$, випливає, що різниця $a - b$ ділиться на m, тому вона ділиться на будь-який дільник d числа m, тобто $a \equiv b(mod\ d)$.

i) Якщо одна частина порівняння $a \equiv b$ і модуль m діляться на яке-небудь ціле число, то й інша частина порівняння має ділитися на те ж саме число.

Дійсно, із $a \equiv b(mod\ m)$, випливає, що $a = b + m \cdot t$. Якщо a і m кратні d, то і b має бути кратним d.

j) Якщо $a \equiv b(mod\ m)$, то $(a, m) = (b, m)$.

Це безпосередньо випливає із рівності $a = b + m \cdot t$.

k) Якщо $a_0 \equiv b_0(mod\ m)$, $a_1 \equiv b_1(mod\ m)$, . . . , $a_k \equiv b_k(mod\ m)$, $x \equiv y\ (mod\ m)$, то $a_0 + a_1 \cdot x + a_2 \cdot x^2 + . . . + a_k \cdot x^k \equiv b_0 + b_1 \cdot y + b_2 \cdot y^2 + . . . + b_k \cdot y^k\ (mod\ m)$.

Це безпосередньо випливає із властивостей **b)** і **c).**

Класи чисел за заданим модулем

Означення 02. Класом за даним модулем m називається множина всіх цілих чисел, які порівнянні з деяким даним числом a.

Такий клас будемо позначати $\bar{a}$. Таким чином, $\bar{a}$ позначає множину всіх тих x, які задовольняють умову $x \equiv a\ (mod\ m)$. Наприклад, за модулем $(mod\ 3)$

$10 \in \bar{1},\ 8 \in \bar{2}, 12 \in \bar{0}$. В силу транзитивності порівнянь усі числа одного класу порівнянні між собою, тобто мають однакові лишки при діленні на модуль.

Клас чисел $\bar{a}$ за модулем m співпадає зі значеннями лінійної функції $a + m \cdot t$ при цілих значеннях t.

Оскільки модуль m – число обмежене, то і кількість класів також є обмеженим і рівне m, а саме: це будуть класи, в яких найменшими невід'ємними лишками є цілі числа $r \in \{0, 1, 2, \ldots, m-2, m-1\}$.

Для $m = p$, де p – просте число, є рівно $p - 1$ класів, що містять числа взаємно прості з модулем p. Для таких чисел a справедлива так звана **мала теорема Ферма:** $\boldsymbol{a^{p-1} \equiv 1 \pmod p}$.

В записі $\boldsymbol{a^{p} \equiv a \pmod p}$ теорема Ферма справедлива для всіх натуральних значень a.

Нагадаємо, що прості числа – це такі, які діляться тільки на 1 і самі на себе: 2, 3, 5, 7, 11, 13, 17, 19, 23, . . .

Множина простих чисел необмежена.

Натуральне число $N > 1$ називається складним, якщо N має хоча б один додатній дільник, відмінний від 1 і N. Усі парні числа, крім 2, складні і можуть бути записані у вигляді $N = 2k$, $k > 1$ – ціле число. Таким чином, множина натуральних чисел складається із трьох підмножин:

1) прості числа, 2) складні числа і 3) число 1, котре не належить ні до простих, ні до складних чисел.

Такий поділ натуральних чисел на три множини прийнятий в сучасній літературі, хоча число 1 розумно і справедливо було б віднести до множини простих чисел, а саме число 1 назвати найпростішим серед них зі своїм статусом. Якщо скористатись четвірковою системою числення, то за допомогою чотирьох цифр 0, 1, 2, 3 можна записати кожне натуральне число і, враховуючи, що 1, 2, 3 – прості числа, то матимемо зображення усіх натуральних чисел за допомогою трьох простих чисел.

Таким чином, не треба придумувати універсальну формулу для простих чисел, а досить віднайти критерії для їх виділення в четвірковому запису для всіх натуральних чисел, подібно решету Ератосфена.

Просте парне число 2 можна записати як 2 = 1 + 1, просте непарне число 3 можна записати як 3 = 2 + 1 або 3 = 1 + 1 + 1, тобто парне число 2 подане сумою двох простих чисел, непарне число 3 подане один раз сумою двох простих чисел і другий раз – сумою трьох простих чисел; запишемо такі подання для інших послідовних натуральних чисел n не більше 20 (серед них випишемо перші пари простих чисел- близнюків:

(1, 3), (3, 5), (5, 7), (11,13), (17,19)):

4 = (3 + 1, 2 + 2),

5 = (2 + 3, 2 + 2 + 1, 3 + 1 + 1),

6 = (5 + 1, 3 + 3),

7 = (5 + 2, 5 + 1 + 1, 3 + 3 + 1, 2 + 2 + 3),

8 = (7 +1, 5 + 3),

9 = (7 + 2, 7 + 1 + 1, 5 + 2 + 2, 5 + 3 + 1, 3 + 3 + 3),
10 = (7 + 3, 5 + 5),
11 = (7 + 2 + 2, 7 + 3 + 1, 5 + 3 + 3),
12 = (11 + 1, 7 + 5),
13 = (11 +2, 11 + 1 + 1, 7 + 5 + 1, 7 + 3 + 3, 5 + 5 + 3),
14 = (13 + 1, 11 + 3, 7 + 7),
15 = (13 + 2, 13 +1+1,11 + 2 + 2, 7 + 5 + 3, 5 + 5 + 5),
16 = (13 + 3, 11 + 5),
17 = (13 + 2 + 2, 13 + 3 + 1, 11 + 5 + 1, 11 + 3 + 3, 7 + 5 + 5),
18 = (17 + 1,13 + 5, 11 + 7),
19 = (17 + 2, 17 + 1 + 1, 13 + 3 + 3, 13 + 5 + 1, 11 + 7 + 1, 11 + 5 + 3, 7 + 7 + 5),
20 = (19 + 1, 17 + 3, 13 +7), . . .

Як бачимо із наведених прикладів, перші парні числа натурального ряду можуть бути записані у вигляді мінімальної кількості доданків, а саме: суми двох простих чисел; це стосується усіх парних чисел $2k\ (k \geq 1)$, а непарні числа натурального ряду можуть бути записані у вигляді мінімальної кількості доданків, а саме: суми не більше ніж двох або трьох простих чисел; це стосується усіх непарних чисел $n \geq 3$. Звичайно, виписати для всіх чисел натурального ряду такі суми неможливо.

Чи поширюється це правило на всі числа натурального ряду? Це питання залишається відкритим і вимагає свого доведення. Це є однією з нерозв'язаних проблем в теорії чисел.

Сильна проблема Гольдбаха. Кожне парне число, більше 2, можна подати у вигляді суми двох простих чисел.

Слабка проблема Гольдбаха. Кожне непарне число, більше 5, можна подати у вигляді суми трьох простих чисел (доведена для всіх досить великих непарних чисел Виноградовим І. М.).

Якщо вважати 1 простим числом (а не сиротою серед натуральних чисел, як це є тепер), що цілком справедливо, то можна проблеми Гольдбаха записати таким чином.

Сильна проблема Гольдбаха.

Кожне парне число $n \geq 2$, можна подати у вигляді суми двох простих чисел.

Слабка проблема Гольдбаха. Кожне непарне число $n \geq 3$, можна подати у вигляді суми не більше двох або трьох простих чисел (доведена для всіх досить великих непарних чисел Виноградовим І. М.).

Якби була розв'язана **с**ильна проблема Гольдбаха, то тоді досить легко довести слабку проблему Гольдбаха. Дійсно, відомо, що між двома числами натурального ряду n і $2n$ існує просте число $n < p_n < 2n$ (теорема Бертрана – Чебишева). В цьому легко переконатись розглянувши числа на початку ряду: таких простих чисел на кожному з інтервалів $(n, 2n)$ може бути і більше одного. Візьмемо в якості n довільне просте число $p_k \geq 2$ і розглянемо інтервал $(p_k, 2p_k)$. Згідно із сказаним вище, на цьому інтервалі є прості числа (хоча б одне !). Усі

непарні числа на цьому інтервалі, в тому числі й прості, можуть бути записані у вигляді $p_k + 2s$, *де* $1 \le s \le (p_k - 1)/2$ і, оскільки, $2s$ може бути подане сумою двох простих чисел, то слабка проблема Гольдбаха справедлива для всіх непарних чисел на цьому інтервалі. Далі все можна довести послідовно, рухаючись у бік зростання простих чисел і без теореми Виноградова І. М. Залишається тільки знайти обґрунтування сильної проблеми Гольдбаха. Дерзайте! Можливо вам пощастить розв'язати сильну проблему Гольдбаха.

2) Кожне натуральне число, відмінне від самих простих чисел, можна представити у вигляді добутку простих чисел і їх степенів. Такий розклад називається **канонічним** і записується у вигляді:

$N = 2^{s0} \cdot p1^{s1} \cdot p2^{s2} \cdot \ldots \cdot pl^{sl}$, *де* $s0, s1, s2, \ldots, sl$ – цілі числа ≥ 0 ;

при $s0 \ge 1$, $si \ge 0$ ($i = 1, 2, \ldots, l$) маємо парні числа ; при $s0 = 0$ і хоча б одне із $si \ne 0$ ($i = 1, 2, \ldots, l$) маємо непарні числа;

тут $p1 < p2 < \ldots < pl$ – прості числа > 2 .

Для кожного натурального числа N такий розклад існує і є єдиним.

Числа натурального ряду за *(mod 2)* поділяються на два класи $\overline{0}$ і $\overline{1}$, тобто парні, що при діленні на 2 дають остачу 0 і непарні, що при діленні на 2 дають остачу 1; парні числа можна записати у вигляді $m = 2k$, $k \ge 1$ – ціле число або $n = 2^s q$, *де* $s \ge 1$ – ціле число, $q = 2w + 1$ – ціле непарне число, де $w \ge 1$ – ціле число; непарні числа можна записати у вигляді $n = 2m + 1$, де $m \ge 0$ – ціле число. Такий запис парних і непарних чисел інколи зручніший для практичного користування, ніж запис натуральних чисел у канонічній формі.

Розв'язування деяких задач за допомогою теорії порівнянь

Задача 1. У двох коробках є олівці. Якщо з першої коробки перекласти в другу один олівець, то в другій коробці стане у двічі олівців більше, ніж у першій, і навпаки, коли один олівець з другої коробки перекласти в першу, то в коробках олівців стане порівну. Скільки олівців є в кожній коробці?

Розв'язання. Задача з двома невідомими. Все просто: позначаємо через X і Y відповідно кількості олівців е першій і другій коробках, згідно з умовами задачі складаємо систему двох рівнянь з двома невідомими:

$2(X - 1) = Y + 1$, $X + 1 = Y - 1$. Розв'язуємо систему двох рівнянь з двома невідомими і отримуємо розв'язок $X = 5$, $Y = 7$.

А якщо ми не вивчали рівнянь, як бути? Ось тут і допомагають методи теорії чисел, а саме, теорії порівнянь. Від перекладання олівців із коробки в коробку їхня сума не змінюється, а за умовою задачі це число кратне 2(двом) і 3(трьом); на мові порівнянь $a \equiv 0 (mod\ 2)$, $a \equiv 0 (mod\ 3)$ і, згідно з властивостями порівнянь, $a \equiv 0 (mod\ 6)$, тобто число a кратне 6.

Першим таким числом у натуральному ряді є число 6, другим число 12, третім число 18 і т. д. Безпосередньою перевіркою умов задачі отримуємо $a = 12$, а число олівців у коробках, відповідно, 5 і 7. Як бачимо, звичайні

міркуванння мовою порівнянь дають можливість отримати розв'язок без застосування алгебраїчних методів.

Задача 2. На плацу прапорщик займається стройовою підготовкою з певною кількістю солдатів. У результаті такого навчання він помітив, якщо поставити солдат у шеренгу по 2, то 1 солдат зайвий, по 3 – 1 зайвий, по 4 – 1 зайвий, по 5 – 1 зайвий , по 6 – 1 зайвий , і тільки коли поставити в шеренгу по 7, все буде гаразд; зайвих солдатів не буде. Яка мінімальна кількість солдатів займалась стройовою підготовкою на плацу?

Розв'язання. Маємо задачу з одним невідомим X. Мовою порівнянь умову задачі можна записати у вигляді:

$X \equiv 1(mod\ 2), X \equiv 1(mod\ 3), X \equiv 1(mod\ 4), X \equiv 1(mod\ 5), X \equiv 1(mod\ 6), X \equiv 0(mod\ 7).$

Перші 5 порівнянь, згідно з властивостями порівнянь, можна замінити одним порівнянням $X \equiv 1(mod\ 60), 60 = [2, 3, 4, 5, 6]$ – найменше спільне кратне.

Отже, маємо систему двох порівнянь $X \equiv 1(mod\ 60), X \equiv 0(mod\ 7).$

Розв'язки цих двох порівнянь можна записати у вигляді:

$X_1 = 60\,v + 1, X_2 = 7\,u,$

де v, u – цілі числа.

Залишається знайти мінімальні значення $v, u,$ за яких $X_1 = X_2.$ Безпосередньою перевіркою знаходимо $v = 5, u = 43, X = 301$, тобто, найменша кількість солдатів, що займалася на плацу стройовою підготовкою і задовольняє умовам задачі, дорівнює 301. Попробуйте розв'язати цю задачу іншими методами.

Задача 3. Встановити правила подільності натуральних десяткових чисел на 3, на 9, на 11.

Розв'язання. Будемо вважати, що натуральні десяткові числа записані у вигляді суми ряду:

$N = \sum_0^n 10^k c_k = 10^0 c_0 + 10^1 c_1 + \ldots + 10^n c_n$, *де* $c_k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ – десяткові цифри числа N. Маємо порівняння: $10^k \equiv 1(mod\ 3)$,

$10^k \equiv 1(mod\ 9), k \geq 0$ – *ціле,* $10^k \equiv 1(mod\ 11)$, k – ціле, парне число,

$10^k \equiv -1(mod\ 11)$, k – ціле, непарне число. Число N буде кратне 3 і 9, коли $N \equiv 0(mod\ 3), N \equiv 0\ (mod\ 9)$, отже, в силу властивостей порівнянь, маємо:

$N \equiv \sum_0^n 10^k c_k = 10^0 c_0 + 10^1 c_1 + \ldots + 10^n c_n \equiv 0(mod\ 3) \equiv$

$\equiv c_0 + c_1 + \ldots + c_n \equiv 0(mod\ 3).$

$N \equiv \sum_0^n 10^k c_k = 10^0 c_0 + 10^1 c_1 + \ldots + 10^n c_n \equiv 0\ (mod\ 9) \equiv$

$\equiv c_0 + c_1 + \ldots + c_n \equiv 0(mod\ 9).$

Тобто, число N ділиться на 3 і на 9, коли сума цифр цього числа ділиться відповідно на 3 і на 9. Встановимо правило ділення натуральних чисел на 11, користуючись властивостями порівнянь.

$N \equiv \sum_0^n 10^k c_k = 10^0 c_0 + 10^1 c_1 + \ldots + 10^n c_n\ (mod\ 11) \equiv 0(mod\ 11),$

$c_0 - c_1 + \ldots + (-1)^n c_n \equiv 0(mod\ 11).$

Тобто, число N ділиться на 11, коли алгебраїчна сума цифр цього числа ділиться на 11, нумерація цифр числа N починається зліва направо:
0, 1, 2, 3, . . .; цифри з парними номерами: 0, 2, 4, . . . беруть зі знаком «+»,
цифри з непарними номерами: 1, 3, 5, . . . беруть зі знаком «–».

На цих простих прикладах було показано, як застосування знань із теорії порівнянь допомагає розв'язувати різні за змістом практичні задачі.

Тріумфом застосування теорії порівнянь для розв'язання досить складних нелінійних задач в теорії чисел може служити **доведення справедливості великої теореми Ферма,** що буде показано згодом.

Недостатність логіки висловлювань. Поняття предиката.

В алгебрі логіки висловлювання розглядаються як нероздільні цілі і тільки з точки зору їх істинності або хибності, неправдивості.

Ні структура висловлювань, ні, тим паче, їхній зміст не беруться до уваги. У той же час і в науці, і на практиці використовують висновки, які істотно залежать як від структури, так і від змісту використовуваних у них висловлювань.

Наприклад, у твердженні, що «Всякий ромб – паралелограм; ABCD – ромб; отже, ABCD – паралелограм» посилання і висновки є елементарними висловлюваннями логіки висловлювань, і, з точки зору цієї логіки, розглядаються як цілі, неділимі, без урахування їхньої внутрішньої структури.

Отже, алгебра логіки, як важлива частина логіки, є недостатньою при аналізі багатьох досліджень.

У зв'язку з цим виникає необхідність у розширенні логіки висловлювань, у побудові такої логічної системи, засобами якої можна було б досліджувати структуру тих висловлювань, котрі, в рамках логіки висловлювань, розглядаються як елементарні.

Такою логічною системою є логіка предикатів, що містить усю логіку висловлювань як свою частину.

Логіка предикатів, як і традиційна формальна логіка, поділяє елементарне висловлювання на суб'єкт (буквально – підмет, хоча воно виконує і роль додатку) і предикат (буквально – присудок, хоча воно може грати і роль означення).

Суб'єкт – це те, про що стверджується у висловлюванні;

предикат – це те, що стверджується про суб'єкт.

Наприклад, у висловлюванні «7 – просте число», «7» – суб'єкт, «просте число» – предикат. Це висловлювання стверджує, що «7» має властивість «бути простим числом».

Якщо в цьому прикладі замінити конкретне число 7 змінною x із множини натуральних чисел, то отримаємо висловлювальну форму «x – просте число». За одних значеннях x (наприклад, $x=13,\ x=17$) ця форма дає істинне

висловлювання, а за інших значеннях x (наприклад, $x=10$, $x=18$) ця форма дає хибне висловлювання.

Зрозуміло, що ця висловлювальна форма визначає функцію однієї змінної x, яка визначена на множині N, і набирає значення із множини {1;0}. Тут предикат набуває значення функції суб'єкта і виражає властивість суб'єкта.

Дамо декілька означень, що стосуються предикатів.

Означення 1

Одномісним предикатом $P(x)$ називається довільна функція змінної x, визначена на множині M і яка набирає значення із множини $\{1; 0\}$.

Множина M, на якій визначено предикат $P(x)$, називається областю визначення предиката $P(x)$.

Множина всіх елементів $x \in M$, за яких предикат набирає значення «істина» (1), називається множиною (областю) істинності предиката $P(x)$. Так, наприклад, предикат $P(x)$ – «x – просте число» визначений на множині N, а множина істинності I_P для нього є множина усіх простих чисел.

Предикат $Q(x)$ – «$\sin(x) = 0$» визначено на множині R, а його множиною істинності є $I_Q = \{k\pi, k \in Z\}$.

Предикат $F(x)$ – «діагоналі паралелограма x взаємно перпендикулярні» визначено на множині усіх паралелограмів, а його множиною істинності є множина всіх ромбів.

Із наведених прикладів бачимо, що одномісні предикати виражають властивості предметів (суб'єктів).

Означення 2

Предикат $P(x)$, визначений на множині M, називається тотожньо істинним, якщо його множина істинності співпадає з областю визначення, тобто $Ip=M$.

Означення 3

Предикат $P(x)$, визначений на множині M, називається тотожньо хибним, якщо його множина істинності є пустою множиною, тобто $Ip=0$.

Природнім узагальненням поняття одномісного предиката є поняття багатомісного предиката, за допомогою якого виражаються відношення між предметами.

Прикладом бінарного відношення, тобто, відношення між двома предметами, є відношення «менше». Нехай це відношення введено на множині Z цілих чисел. Воно може бути охарактеризоване висловлювальною формою «$x < y$», де x, $y \in Z$, тобто, є функцією двох змінних $P(x, y)$, визначеній на множині упорядкованних пар цілих чисел $ZxZ=Z^2$ з множиною значень $\{1;0\}$.

Означення 4

Двомісним предикатом $P(x, y)$ називається функція двох змінних x і y, визначена на множині $M=M1xM2$ і яка набирає значення із множини $\{1;0\}$.

У числі прикладів двомісних предикатів можна назвати такі предикати:
Q(x, y) – «x=y» – предикат рівності, визначеної на множині $RxR=R^2$;
F(x, y) – «*x* паралельну», «пряма *x* паралельна прямій *y*», визначеній на множині прямих, що лежать на даній площині.

Цілком аналогічно вводиться поняття тримісного предиката.

Наведемо приклад тримісного предиката (функції трьох змінних):

S(x,y,z) – «x+y=z».

Підстановка в нього *x=3* приводить його в двомісний предикат:

S(y,z) – «3+y=z»,

а підстановка *x=3, z=2* – в одномісний предикат *S(y) – «3+y=2».*

Підстановка *S(2, 3, 5)* приводить його в істинне висловлювання,

а *S(1, 7, 4)* – в хибне.

Аналогічно визначається і *n*-місний предикат (функція *n* змінних).

Приклад *n*-місного предиката:

$R(x_1, x_2, \ldots, x_n)$: $a_1 x_1 + \ldots + a_n x_n = 0$,

котрий, як бачимо, є алгебраїчним рівнянням з *n* невідомими.

При *n=0* будемо мати нульмісний предикат – це логічна (пропозиціональна) змінна, що набирає значення із множини *{1; 0}.*

Предикати, які використані в цій роботі, будуть безпосередньо виписані при розгляді алгоритму доведення великої теореми Ферма.

Доведення великої теореми Ферма

Далі наведемо детальніше доведення великої теореми Ферма, розраховане на широке коло читачів і поціновувачів серйозної математики.

Розглянемо нелінійні діофантові рівняння вигляду:

$$X^n + Y^n = Z^n, \quad (1)$$

де $X > 0$, $Y > 0$, $Z > 0$, $n \geq 2$ – цілі числа.

Дослідимо, чи мають розв'язок такі рівняння в цілих числах: $X>0$, $Y>0$, $Z>0$.

Вважаємо, що три числа $X > 0$, $Y > 0$, $Z > 0$, якщо вони є розв'язком рівняння (1), задовольняють умову:

$$(X, Y, Z) = 1 \quad (2)$$

Трійка чисел, що задовольняє умову (2) має найбільший спільний дільник (НСД) = 1 і складається із двох непарних, нехай це будуть X, Y і парного Z чисел. Якщо така трійка чисел задовольняє рівняння (1), то вона задовольняє хоча б одне з рівнянь (3) або (4):

$$X^n + Y^n = Z^n, \quad (3)$$

де $X > 0$, $Y > 0$ – непарні, $n \geq 2$ – цілі числа,

$$X^n - Y^n = Z^n, \quad (4)$$

де $X > 0$, $Y > 0$ – непарні, $X > Y$, $n \geq 2$ – цілі числа, в яких зліва присутня сума або різниця тільки двох непарних чисел степеня n (X^n, Y^n), а справа – парне число в степені n (Z^n).

Цілі числа X, Y, Z будемо розглядати у вигляді:

$$X = 2\cdot k + 1,\ Y = 2\cdot m + 1,\ Z = 2^s \cdot q, \quad (5)$$

де k, m, q, s – цілі числа, $k \geq 0$, $m \geq 0$, $s \geq 1$, $q \geq 1$ – непарне число;

$q= 2\cdot w +1$, $w \geq 0$ – ціле число.

При розгляді степенів n рівняння (1) числа натурального ряду будемо розглядати в канонічній формі:

$$n = 2^{s0}\cdot p1^{s1}\cdot p2^{s2}\cdot \ldots \cdot pl^{sl}, \quad (5^*)$$

де s0,s1,s2,…,sl – цілі числа ≥ 0; при $s0 \geq 1$, $si \geq 0$ (i=1, 2, …, l) маємо парні числа; при $s0 = 0$ і, хоча б одне із $si \neq 0$, (i=1, 2, …, l) маємо непарні числа;

тут $p1 < p2 < \ldots < pl$ – прості числа > 2.

Зразу зауважимо, що праві частини рівнянь (3) і (4) задовольняють порівняння:

$$Z^n = (2^s\cdot q)^n \equiv 0 \pmod{2^n}, \quad (6)$$

де $s \geq 1$, $n \geq 2$ – цілі числа, $q \geq 1$ – непарне.Без особливих втрат для подальшого розгляду будемо вважати s =1.Враховуючи (6), розглянемо питання існування розв'язку порівнянь:

$$X^n + Y^n \equiv 0 \pmod{2^n}, \quad (7)$$

де X, Y – непарні типу (5), $n \geq 2$ – ціле число,

$$X^n - Y^n \equiv 0 \pmod{2^n}, \quad (8)$$

де X, Y – непарні типу (5), $X > Y$, $n \geq 2$ –ціле число.

Розглянемо предикати, що відповідають рівнянням і порівнянням, виписаним вище:

P_1 (X, Y, Z, n): «$X^n + Y^n = Z^n$, X > 0, Y > 0, Z > 0 – цілі, n ≥ 2 – ціле число»,
P_3 (X, Y, Z, n): «$X^n + Y^n = Z^n$, X, Y, Z – числа типу (5), n ≥ 2 – ціле число»,
P_4 (X, Y, Z, n): «$X^n – Y^n = Z^n$, X, Y, Z – числа типу (5), n ≥ 2 – ціле число»,
P_7 (X, Y, n): «$X^n + Y^n \equiv 0(\mathrm{mod}\ 2^n)$, X, Y – числа типу (5), n ≥ 2 – ціле число»,
P_8 (X, Y, n): «$X^n – Y^n \equiv 0(\mathrm{mod}\ 2^n)$, X, Y – числа типу (5), n ≥ 2 – ціле число».

Значення ці предикати приймають на множині M = {1; 0}, тобто «істина» = 1, коли рівність або порівняння справедливі або «хибність» = 0, коли рівність або порівняння не виконуються. Операції над предикатами P_3 і P_4 типу кон'юнкції (табл. 1) і диз'юнкції (табл. 2), покажемо у вигляді таблиць істинності:

Таблиця 1

P_3	P_4	$P_3 \wedge P_4$
1	1	1
1	0	0
0	1	0
0	0	0

Таблиця 2

P_3	P_4	$P_3 \vee P_4$
1	1	1
1	0	1
0	1	1
0	0	0

Тривіальний розв'язок X=0, Y=0, Z=0 не розглядаємо. Покажемо, що для n ≥2 рівняння (1) не має розв'язку при X = Y. Порівняння (7) в цьому випадку має вигляд: $X^n + Y^n = 2 \cdot X^n \equiv 0(\mathrm{mod}\ 2^n)$, що неможливо при n ≥ 2.

Отже, P_7(X, X, 2) = 0, P_3(X, X, Z, 2) = 0.

Оскільки при X = Y для рівняння (4) Z = 0, то P_4(X, Y, 0, n) = 0.

І тоді P_1 (X, Y, Z, 2) = P_3 (X, X, Z, 2) V P_4 (X, X, 0, 2) = 0V0 = 0, тобто розв'язку для рівняння (1) не існує при n ≥ 2 в цілих числах:
X > 0, Y > 0, Z > 0 типу (5).

Дослідимо рівняння (3) на існування розв'язку в цілих числах:
X > 0, Y > 0, Z > 0 типу (5) для цілих n ≥ 2, використовуючи порівняння (7). Розглянемо: $X^2 + Y^2 = Z^2$. Враховуючи (5), маємо:

$(2 \cdot k + 1)^2 + (2 \cdot m + 1)^2 = 4 (k^2 + m^2) + 4 (k + m) + 2 \equiv 2(\mathrm{mod}\ 2^2)$;

з цього випливає, що умова (7) не виконується для всіх цілих значень:
X >0, Y > 0 типу (5), отже, P_7 (X, Y, 2) = 0.

Розглянемо випадки, коли n = 2 · h , h > 1 – ціле, маємо:

$X^{2 \cdot h} + Y^{2 \cdot h} = (X^h)^2 + (Y^h)^2 \equiv 2 (\mathrm{mod}\ 2^2) \not\equiv 0 (\mathrm{mod}\ 2^{2 \cdot h})$, отже, P_7 (X, Y, 2h) = 0.

Отже, для всіх степенів n = 2· h, h > 0 – ціле, порівняння (7), а також рівняння (3) не мають розв'язку в цілих числах: X >0, Y > 0, Z > 0 типу (5),

тобто, P_7 (X, Y, 2h) = 0, P_3 (X, Y, Z, 2h) = 0, h ≥ 1.

Дослідимо рівняння (4) на існування розв'язку в цілих числах:

X > 0 , Y > 0 , Z > 0 для цілих n ≥ 2, використовуючи порівняння (8).

Розглянемо порівняння (8), для n=2, маємо:

$X^2 – Y^2 = 4 \cdot (k^2 – m^2) + 4 \cdot (k – m) = 4 \cdot (k – m) \cdot (k + m + 1) \equiv 0 (\mathrm{mod}\ 2^2)$, отже, розв'язок існує і при k = 2, m = 1 (k > m), маємо: X=5, Y=3, Z=4; $5^2-3^2=4^2$;
для відшукання інших чисел X , Y , Z можна скористатись формулами [2]
$X = u^2 + v^2$, $Y = u^2 – v^2$, $Z = 2 \cdot u \cdot v$, де u > v – два послідовних числа натурального ряду, наприклад: u = 8, v = 7, $X=8^2+7^2=113$, $Y = 8^2 – 7^2=15$,

$Z = 2\cdot 8\cdot 7 = 112$; $113^2 - 15^2 = 112^2$, ... і т.д.,
тобто, $P_8(X, Y, 2) = 1$, $P_4(X, Y, Z, 2) = 1$.

Отже, для рівняння (1), маємо:

$P_1(X, Y, Z, 2) = P_3(X, Y, Z, 2) \vee P_4(X, Y, Z, 2) = 0 \vee 1 = 1$, тобто, розв'язок рівняння (1) існує для $n = 2$ в цілих числах: $X > 0$, $Y > 0$, $Z > 0$ типу (5).

Прості три числа – і тільки знаменитий Піфагор першим розгледів у них довжини відповідних сторін прямокутних трикутників!

Розглянемо випадки, коли $n = 2\cdot h$, де $h \geq 2$ – ціле число, маємо:

$X^{2\cdot h} - Y^{2\cdot h} = (X^h + Y^h) \cdot (X^h - Y^h)$.

Враховуючи це, порівняння (8) розпадається на систему двох порівнянь:

$$X^h + Y^h \equiv 0 \pmod{2^h}, \quad (9)$$

$$X^h - Y^h \equiv 0 \pmod{2^h}. \quad (10)$$

Якщо порівняння (9) і (10) виконуються одночасно, то їхня сума і різниця також порівнянні з нулем за $(\mathrm{mod}\ 2^h)$, тобто, $2\cdot X^h \equiv 0 \pmod{2^h}$, $2\cdot Y^h \equiv 0 \pmod{2^h}$, оскільки X і Y непарні, $2 \equiv 0 \pmod{2^h}$, що неможливо при $h \geq 2$, отже: $P_8(X, Y, 2h) = (P_7(X, Y, h) = 0) \wedge (P_8(X, Y, h) = 1) \vee (P_7(X, Y, h) = 1) \wedge (P_8(X, Y, h) = 0) \vee (P_7(X, Y, h) = 0) \wedge (P_8(X, Y, h) = 0) = 0$, $h \geq 2$, отже, $P_4(X, Y, Z, 2h) = 0$, $h \geq 2$.

Враховуючи ці результати, маємо:

$P_1(X, Y, Z, 2h) = P_3(X, Y, Z, 2h) \vee P_4(X, Y, Z, 2h) = 0 \vee 0 = 0$, тобто розв'язку для рівняння (1) не існує при $h \geq 2$ в цілих числах: $X > 0$, $Y > 0$, $Z > 0$ типу (5).

З погляду на відомі історичні дані про труднощі доведення великої теореми Ферма упродовж майже чотирьох століть, безперечно, вражає така простота отриманих результатів дослідження справедливості твердження цієї теореми відразу для всієї множини парних чисел натурального ряду.

Залишається дослідити існування розв'язку рівнянь (3) і (4), використовуючи відповідно порівняння (7) і (8), для непарних значень

$n = 2\cdot h + 1$, h – ціле ≥ 1.

Спочатку розглянемо для простих чисел $n = p = 3, 5, 7, 11, \ldots$ і т. д.

Розглянемо (3) і (4) у вигляді :

$$X^p \pm Y^p = (X \pm Y) \cdot (X^{p-1} + (\mp 1)^{p-2} X^{p-2} Y + \ldots + (\mp 1) X \cdot Y^{p-2} + Y^{p-1}) = Z^p \quad (11)$$

Введемо предикати:

$P_{11}(X, Y, Z, p)$: «$X^p \pm Y^p = (X \pm Y) \cdot (X^{p-1} + (\mp 1)^{p-2} X^{p-2} Y + \ldots + (\mp 1) X \cdot Y^{p-2} + Y^{p-1}) = Z^p$, X, Y, Z – числа типу (5), $p > 2$ – просте число».

$P_{12}(X, Y, r, p)$: «$X \pm Y = (2\cdot r)^p$, де X, Y – числа типу (5), $r \geq 1$ – ціле число, $p > 2$ – просте число».

Значення предикати P_{11} і P_{12} приймають на множині $M = \{1; 0\}$, тобто, «істина» = 1, коли рівність справедлива або «хибність» = 0, коли рівність не виконується.

Враховуючи (11), введемо позначення:

$R = X \pm Y$, $S = (X^{p-1} + (\mp 1)^{p-2} X^{p-2} Y + \ldots + (\mp 1) X \cdot Y^{p-2} + Y^{p-1})$,

$$R \equiv 0 \pmod 2, \ S \equiv 1 \pmod 2 \quad (12)$$

Введемо предикати:

$P_9(X, Y, p)$: «$R = X \pm Y \equiv 0(\text{mod } 2^p)$, X, Y – числа типу (5), $p > 2$ – просте число»,

$P_{10}(X, Y, q, p)$: «$(S = X^{p-1} + (\mp 1)^{p-2} X^{p-2} Y + \ldots + (\mp 1) X \cdot Y^{p-2} + Y^{p-1}) \equiv q^p (\text{mod } p)$, X, Y, q – числа типу (5), $p > 2$ – просте число».

Значення предикати P_9, P_{10} приймають на множині $M = \{1; 0\}$, тобто «істина» = 1, коли порівняння справедливі або «хибність» = 0, коли порівняння не виконуються.

Враховуючи (5), маємо: $R=2\cdot k + 1 \pm (2\cdot m +1) = 2\cdot(k \pm m + (1\pm 1)/2)$ – парне число; $S >1$ – симетричний многочлен відносно X, Y і за величиною є непарним числом [3].

Якщо R не порівнянне з нулем по $\text{mod}(2^p)$, то рівняння (3) і (4), очевидно, розв'язку не мають, тобто, $P_9(X , Y, p) = 0$, $P_{12}(X , Y, r, p) = 0$, $P_3(X , Y, Z, p) = 0$, $P_4 (X , Y, Z, p) = 0$.

$P_1(X, Y, Z, p) = P_3 (X, Y, Z, p) \vee P_4 (X, Y, Z, p) = 0 \vee 0 = 0$, тобто розв'язку не існує в цілих числах: $X > 0$, $Y > 0$, $Z > 0$ типу (5).

Враховуючи (6), (11), (12) розглянемо порівняння: $R \equiv 0(\text{mod } 2^p)$.

Така умова є необхідною для існування розв'язку рівнянь (3) і (4).

Відповідні значення k і m, що задовольняють таке порівняння, визначаємо з умови: $2\cdot(k \pm m + (1\pm 1)/2) \equiv 0 (\text{mod } 2^p)$; звідси $k \pm m + (1\pm 1)/2 = 2^{p-1} \cdot t$, $t \geq 1$ – ціле, тобто при таких значеннях k і m предикат $P_9(X , Y, p) = 1$.

Наведені нижче приклади для простого модуля *p = 3*, можливо, за уважного розгляду, допоможуть краще зрозуміти суть алгоритму доведення великої теореми Ферма, а саме: використання малої теореми Ферма і ту дивовижність розв'язку, згадану в запису Ферма на сторінках «Арифметики» Діофанта. В загальному вигляді маємо: $X^3 \pm Y^3 = Z^3$, $X^3 \pm Y^3 = (X \pm Y) \cdot (X^2 \mp X\cdot Y + Y^2) = Z^3$, $R = X – Y$, $S = (X^3 \pm Y^3)/(X \pm Y) = X^2 \mp X\cdot Y + Y^2$, $R \equiv 0 (\text{mod } 2)$, $S > 1$,
$S \equiv 1(\text{mod } 2)$, $(S = (X^3 \pm Y^3)/(X \pm Y)) \equiv 1 (\text{mod } (p = 3))$,

(використана мала теорема Ферма ([1] , b , § 6 , гл. III)).

$q = (2\cdot w + 1)^3$, $w \geq 1$ – ціле число, ***$q \equiv (2\cdot w + 1)^3 (\text{mod } 3) \equiv 2\cdot w + 1 (\text{mod } 3) > 1$,***

(використана мала теорема Ферма ([1], b, § 6, гл. III));

при $w = (t\cdot p – 1)/2$, $(t=1,2,3, \ldots)$; $2\cdot w + 1 \equiv 0 (\text{mod } (p=3))$.

Візьмемо $k = 2^2\cdot 3^2$, $m = 0$.

Приклад 1.

$X = 2k + 1= 2\cdot 2^2\cdot 3^2 + 1= 73$, $Y = 1$, $X^3 – Y^3 = 73^3 – 1^3 = 389017 – 1 = 389016$,

$R = X – Y = 73 – 1 = 72 = 2^3\cdot 3^2$, $R \equiv 0 (\text{mod } 2^3)$,

$(S = (73^3 – 1^3)/ (73 – 1)) \equiv 1(\text{mod } 3)$,

(використана мала теорема Ферма ([1], b, § 6, гл. III));

$S = 389016/72 = 5403 = 3\cdot 1801$, $S \not\equiv q^3 (\text{mod } 3)$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;

$Z^3 = (2\cdot 3^{2/3})^3\cdot ((3\cdot 1801)^{1/3})^3$;

Приклад 2.

$X = 73$, $Y = 1$, $X^3 + Y^3 = 73^3 + 1^3 = 389017 + 1 = 389018$, $R = X + Y = 73 + 1 = 74 = 2\cdot 37$, $R \not\equiv 0 (\text{mod } 2^3)$, $(S = (73^3 + 1^3)/ (73 + 1)) \equiv 1(\text{mod } 3)$,

(використана мала теорема Ферма ([1], b, § 6, гл. III));
$S = 389018/74 = 5257 = 7\cdot751$,
$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;
$Z^3 = ((2\cdot37)^{1/3})^3\cdot ((7\cdot751)^{1/3})^3$;
Приклад 3.
$X = 17, Y = 1, X^3 - Y^3 = Z^3 = 17^3 - 1^3 = 4913 - 1 = 4912 = 2^4\cdot 307$,
$R = 2^4, S = 307$,
$R \equiv 0(\mathrm{mod}\ 2^3), (S = (17^3 - 1^3)/ (17 - 1)) \equiv 1(\mathrm{mod}\ 3)$,
(використана мала теорема Ферма ([1], b, § 6, гл. III));
$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;
$Z^3 = (2^{4/3})^3\cdot (307^{1/3})^3$;
Приклад 4.
$X^3 + Y^3 = Z^3 = 17^3 + 1^3 = 4913 + 1 = 4914 = 2\cdot3^3\cdot7\cdot13$, $R = 18 = 2\cdot3^2$, $S = 273 = 3\cdot7\cdot13$,
$R \not\equiv 0(\mathrm{mod}\ 2^3), (S = (17^3 + 1^3)/ (17 + 1)) \equiv 1(\mathrm{mod}\ 3)$,
(використана мала теорема Ферма ([1], b, § 6, гл. III));
$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;
$Z^3 = (2^{1/3}\cdot3^{2/3})^3\cdot ((3\cdot7\cdot13)^{1/3})^3$;
Приклад 5.
$X=15, Y = 1, X^3 + Y^3 = Z^3 = 15^3 + 1^3 = 3375 + 1 = 3376 = 2^4\cdot 211, R = 2^4, S=211$,
$R \equiv 0(\mathrm{mod}\ 2^3), (S = (15^3 + 1^3)/ (15 + 1)) \equiv 1(\mathrm{mod}\ 3)$,
(використана мала теорема Ферма ([1], b, § 6, гл. III));
$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;
$Z^3 = (2^{4/3})^3\cdot (211^{1/3})^3$;
Приклад 6.
$X^3 - Y^3 = Z^3 = 15^3 - 1^3 = 3375 - 1 = 3374 = 2\cdot7\cdot241$, $R = 14 = 2\cdot7$, $S = 241$,
$R \not\equiv 0(\mathrm{mod}\ 2^3), (S = (17^3 + 1^3)/ (17 + 1)) \equiv 1(\mathrm{mod}\ 3)$,
(використана мала теорема Ферма ([1], b, § 6, гл. III));
$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;
$Z^3 = ((2\cdot7)^{1/3})^3\cdot (241^{1/3})^3$;
Приклад 7.
$X = 7, Y = 1, X^3 + Y^3 = Z^3 = 7^3 + 1^3 = 343 + 1 = 344 = 2^3\cdot 43$, $R = 2^3$, $S = 43$,
$R \equiv 0(\mathrm{mod}\ 2^3), (S = (7^3 + 1^3)/ (7 + 1)) \equiv 1(\mathrm{mod}\ 3)$,
(використана мала теорема Ферма ([1], b, § 6, гл. III));
$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;
$Z^3 = 2^3\cdot (43^{1/3})^3$;
Приклад 8.
$X^3 - Y^3 = Z^3 = 7^3 - 1^3 = 343 - 1 = 342 = 2\cdot3^2\cdot19$, $R = 6 = 2\cdot3$, $S = 57 = 3\cdot19$,
$R \not\equiv 0(\mathrm{mod}\ 2^3), (S = (7^3 - 1^3)/ (7 - 1)) \equiv 1(\mathrm{mod}\ 3)$,
(використана мала теорема Ферма ([1], b, § 6, гл. III));
$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;
$Z^3 = ((2\cdot3)^{1/3})^3\cdot ((3\cdot19)^{1/3})^3$;
Приклад 9.

$X = 9, Y = 1, X^3 + Y^3 = Z^3 = 9^3 + 1^3 = 729 + 1 = 730 = 2\cdot3\cdot1217, R = 2\cdot5, S = 73,$
$R \not\equiv 0(\text{mod } 2^3), (S = (9^3 + 1^3)/ (9 + 1)) \equiv 1(\text{mod } 3),$
(використана мала теорема Ферма ([1], b, § 6, гл. III));
$S \not\equiv q^3 \text{ (mod 3)}$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;
$Z^3 = ((2\cdot 5)^{1/3})^3 \cdot (73^{1/3})^3$;

Приклад 10.

$X^3 - Y^3 = Z^3 = 9^3 - 1^3 = 729 - 1 = 728 = 2^3\cdot7\cdot13, R = 2^3, S = 91 = 7\cdot13,$
$R \equiv 0(\text{mod } 2^3), (S = (9^3 - 1^3)/ (9 - 1)) \equiv 1(\text{mod } 3),$
(використана мала теорема Ферма ([1], b, § 6, гл. III));
$S \not\equiv q^3 \text{ (mod 3)}$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;
$Z^3 = 2^3\cdot ((7\cdot13)^{1/3})^3$.

Як бачимо з наведених прикладів, навіть тоді, коли $R \equiv 0(\text{mod } 2^{(p=3)})$, R не завжди може бути представленим у вигляді: $R = (2\cdot k)^3$, $k \geq 1$ – ціле раціональне число, як це вимагається за змістом задачі. Такі ж приклади можна навести для будь-якого простого модуля $p > 2$.

Як бачимо, навіть істинність предиката P_9 ще не гарантує істинності предиката P_{12}, від якого залежить істинність предикатів P_3, P_4, P_{11}. Будемо вважати, що $P_9 = 1$ і $P_{12} = 1$.

Розглянемо рівність $R\cdot S = R\cdot q^p$, де $R = (2\cdot r)^p$, $r \geq 1$ – ціле число, $S = q^p$.

$$q^p = (2\cdot w + 1)^p, (w > 0 \text{, ціле число}). \qquad (13)$$

Чи існує q, щоб $S = q^p$? Згідно з (13) , $q^p \equiv 2\cdot w+1 \text{ (mod p)}$ – непарне > 1 ;
при $w = (t\cdot p - 1)/2$,(t=1,2,3, . . .); $2\cdot w + 1 \equiv 0 \text{ (mod p)}$;
згідно з (11) $(S = (X^p \pm Y^p)/(X \pm Y)) \equiv 1 \text{ (mod p)}$
(використана мала теорема Ферма ([1] , b , § 6 , гл. III)).

Оскільки $S \equiv 1 \text{ (mod p)}$, а $2\cdot w + 1$ непарне > 1, або порівнянне з нулем за (mod p), то S і q^p не порівнянні за (mod p), тобто, предикат $P_{10}(X, Y, q, p) = 0$, а це означає, що:

$P_{11} (X, Y, Z, p) = P_9 (X, Y, p) \wedge P_{12} (X, Y, r, p) \wedge P_{10} (X, Y, q, p) = 1 \wedge 1 \wedge 0 = 0;$
$P_3 (X, Y, Z, p) = 0, P_4 (X, Y, Z, p) = 0.$

При $P_9 = 1$ і $P_{12} = 0$ предикат P_{10} можна не розглядати, хоча і в цьому випадку $P_{10} = 0, P_{11} = 0, P_3 = 0, P_4 = 0$.

Отже, рівняння (3) і (4) для простих значень $n = p > 2$ не мають розв'язку в цілих числах : $X > 0$, $Y > 0$, $Z > 0$ типу (5), отже:

$P_1 (X, Y, Z, p) = P_3 (X, Y, Z, p) \vee P_4 (X, Y, Z, p) = 0 \vee 0 = 0$, тобто, для рівняння (1) розв'язку не існує в цілих числах: $X > 0, Y > 0, Z > 0$ типу (5) для всіх простих чисел $p > 2$.

Розглянемо випадки, коли степені n – складні непарні числа, тобто n подане у вигляді добутку двох або більше простих чисел і їхніх степенів; для переконливості досить розглянути випадок, коли $n = p1\cdot p2$, (p1 , p2 – прості числа > 2), маємо:

$$X^{p1\cdot p2} \pm Y^{p1\cdot p2} = Z^{p1\cdot p2}. \qquad (14)$$

Рівняння (14) можна подати у вигляді:

$X^{p1\cdot p2} \pm Y^{p1\cdot p2} = (X^{p1})^{p2} \pm (Y^{p1})^{p2} = (X^{p1} \pm Y^{p1}) \cdot ((X^{p1})^{p2-1} +$

$+ (\mp 1)^{p-2} (X^{p1})^{p2-2} \cdot Y^{p1} + ... + (\mp 1) X^{p1} \cdot (Y^{p1})^{p2-2} + (Y^{p1})^{p2-1}) = Z^{p1} \cdot (Z^{p1})^{p2-1}$. (15)

Як бачимо (15) є рівнянням вигляду (11), а тому для нього справедливі висновки, наведені вище. Більше того, якщо враховувати канонічну форму (5*) числа n, то p1 можна вважати складним, а p2 – простим і в такий спосіб показати, що розв'язку не існує і для інших умовно простих степенів рівнянь (3) і (4) в цілих числах : X >0, Y > 0, Z > 0 типу (5), звичайно також і рівняння (1). Отже, велика теорема Ферма доведена.

Таємниця алгоритму розв'язку великої теореми Ферма розгадана.

Тепер легко переконатись у її справедливості і для всіх цілих чисел X, Y, Z, відмінних від нуля, окрім того, вона буде справедлива і в множині раціональних чисел. Покажемо це. Для парних степенів у рівняннях (3) і (4) зміна знаку чисел X, Y, Z не впливає на результати дослідження. У табл. 3 показана зміна ситуації залежно від того, яких значень набувають змінні X, Y, Z у множині цілих чисел при непарних степенях у рівняннях (3) і (4).

Таблиця 3

№ варіанта	змінні (+, –)			тип рівняння (3) V (4)	
	X	Y	Z	тип 1	тип 2
1	+	+	+	(3)	(4)
2	+	–	+	(4)	(3)
3	–	+	–	– (3)	– (4)
4	–	–	–	– (4)	– (3)

Як видно з табл. 3, велика теорема Ферма справедлива в множині цілих чисел з точністю до знака.

Припустимо, що рівняння (1) має розв'язок у раціональних числах: $X = x_1/x_2$, $Y = y_1/y_2$, $Z = z_1/z_2$, де x_1 , x_2 , y_1 , y_2 , z_1 , z_2 – цілі числа $\neq 0$ і $(x_1 , x_2) = 1$, $(y_1 , y_2) = 1$, $(z_1 , z_2) = 1$.

Тоді рівняння (1) можна записати у вигляді: $(x_1/x_2)^n + (y_1/y_2)^n = (z_1/z_2)^n$, або $x_1^n/x_2^n + y_1^n/y_2^n = z_1^n/z_2^n$, або, помноживши ліву і праву частини цієї рівності на $x_2^n y_2^n z_2^n$, одержимо:
$x_1^n y_2^n z_2^n + y_1^n x_2^n z_2^n = z_1^n x_2^n y_2^n$, або $(x_1 y_2 z_2)^n + (y_1 x_2 z_2)^n = (z_1 x_2 y_2)^n$.

Позначимо $U = x_1 y_2 z_2$, $V = y_1 x_2 z_2$, $Q = z_1 x_2 y_2$, маємо: $U^n + V^n = Q^n$, а це і є рівняння (1), для якого справедлива велика теорема Ферма.

Алгоритм проведення дослідження на існування розв'язку рівняння (1) може служити прикладом для ствердження відомого філософського вислову: «Все пізнається в порівнянні». Шукаємо, знаходимо, порівнюємо, пізнаємо. . .

Так, завдяки очевидній простоті і послідовності логічних кроків дослідження на існування розв'язку нелінійних діофантових рівнянь (великої теореми Ферма) з використанням теорії порівнянь і їх властивостей, а також малої теореми Ферма, описаних вище, можна стверджувати:

Ферма володів алгоритмом розв'язку цієї задачі.

Розроблений мною алгоритм доведення великої теореми Ферма, можна назвати перлиною мистецького витвору в математиці, в теорії чисел, як найпростіший, послідовний, логічний, зрозумілий.

Тут використані лише відомі доступні методи кожному математику, незалежно від його спеціалізації. Цей алгоритм можна вважати цілком зрозумілим, як і доведення теореми Піфагора, хоча й немає геометричної наочності.

У підтвердження, зробленому П'єром де Ферма на полях перекладу «Арифметики» Діофанта запису: «Я знайшов цьому воістину дивовижне доведення, але поля тут занадто вузькі, щоб умістити його», я тепер можу впевнено заявити: «Знайомтесь, вивчайте! Я знайшов це, воістину надзвичайно дивовижне доведення великої теореми Ферма, доведення, котре науковий світ очікував майже 400 років!».

Тепер відпадають всілякі розмови про те, що велика теорема Ферма сформульована не зовсім точно і на безмежності існує розв'язок. Схаменіться! Довільне, взяте на числовій осі актуальної безмежності натуральне число, завжди матиме одне з трьох значень: парне, просте, складне непарне, а для таких чисел правдивість великої теореми Ферма доведена формально.

Тим, хто розробляє алгоритми і пише програми для розрахунків на ЕОМ, з метою перевірки справедливості великої теореми Ферма, як математик-програміст, хочу порадити: не шукайте того, чого не існує, і не витрачайте на це свою фізичну і духовну енергію, час і матеріальні ресурси.

Доведення великої теореми Ферма тепер стане доступним не тільки математикам-професіоналам, а й усім бажаючим, хто цікавиться теорією чисел, особливо студентам навчальних закладів і учням середніх шкіл.

Використана література

1. Виноградов И. М. Основы теории чисел. – М.: Наука, 1965.
2. Бухштаб А. А. Теория чисел. – М.: Просвещение, 1966.
3. Курош А. Г. Курс высшей алгебры.– М.: Просвещение, 1975.
4. Танчук М. О. Доведення великої теореми П.Ферма. – К.: RMprint, 2015.

Поділ плоских кутів на n ≥ 2 рівних частин за допомогою циркуля і лінійки

Розглянемо довільний гострий кут $<$ BOA і покажемо, як його можна розділити на *n* рівних частин за допомогою циркуля і лінійки, незважаючи на ті догми, які на сьогодні існують у математичній літературі з геометрії, що таку побудову виконати неможливо для деяких значень числа n > 2.

Французький математик П. Л. Ванцель довів у 1837 р., що трисекція кута α можлива тільки тоді, коли рівняння $x^3 - 3 \cdot x - 2 \cdot \cos\alpha = 0.$ має розв'язок у квадратних радикалах.

Наприклад, трисекція можлива для кутів виду $2\pi/n$, якщо ціле число n не ділиться на 3.

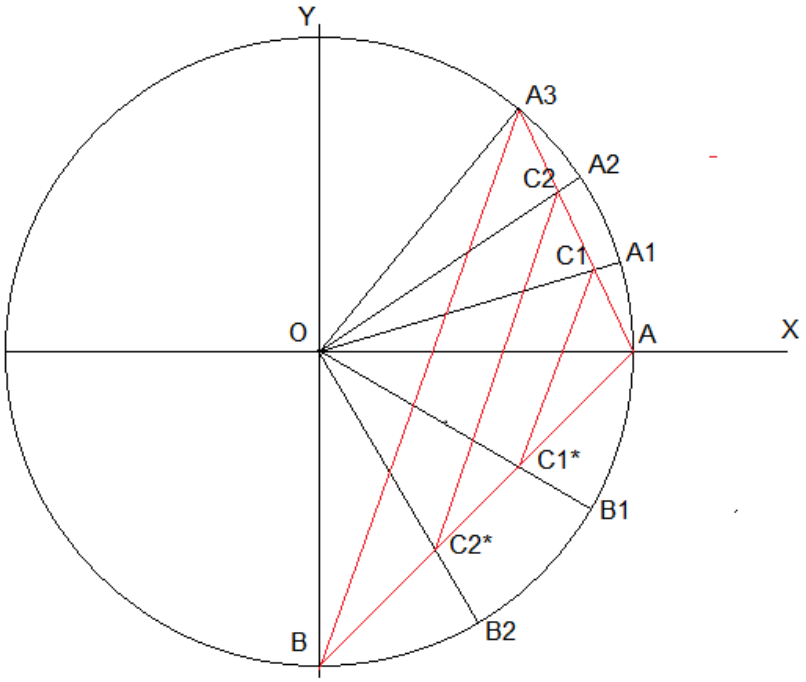
М. М. Постніков у книзі «Теорія Галуа» [1, гл.5] також приводить теоретичні обгрунтування можливих випадків розв'язку задач на побудову за допомогою циркуля і лінійки, підкреслюючи, при цьому, неможливість трисекції кута в загальному випадку циркулем і лінійкою і приводить приклади рівнянь, схожих на рівняння П. Л. Ванцеля.

Вважається, що хоча трисекція кута, в загальному випадку, неможлива за допомогою циркуля і лінійки, практично існують криві, за допомогою яких таку побудову можна виконати: трисектриса, квадратриса, конхоїда Нікомеда, конічні перерізи, спіраль Архімеда, трисекція за допомогою плоского орігамі, трисекція за допомогою невсіса, запропонованого ще Архімедом, хоча така побудова не є класичною.

Тут розглядається модельний метод поділу плоских кутів на n ≥ 2 рівних частин за допомогою циркуля і лінійки, який дозволяє розв'язувати задачу трисекції плоских кутів (і не тільки!) в рамках вимог і умов, викладених в [1, гл.5], без будь-яких обмежень, не застосовуючи допоміжних засобів, окрім циркуля і лінійки [4].

Розглянемо випадок поділу гострого кута на три рівні частини, хоча така схема поділу гострих кутів $\alpha \leq \pi/2$ справедлива і для інших цілих n ≥ 2.

За допомогою лінійки проведемо пряму на стороні OA. З точки O, як з центра, циркулем опишемо коло довільного радіуса R і в точці O проведемо пряму лінію перпендикулярну до OA; таким чином матимемо прямокутну декартову систему координат (див.мал.1).



Мал.1.

Для прикладу візьмемо кут AOB= $\pi/2$, хоча це не істотно (довільний кут AOB може бути меньшим $\frac{\pi}{2}$), який необхідно поділити на три рівних частини. Чому вибрано саме такий кут?

Це позв'язано з тим, що його легко поділити на три рівних частини побудовою кутів в 60 або 30 градусів, а потім виконати такий поділ за допомогою побудови різних моделей, щоб переконатися в правильності розв'язку задачі трисекції кута модельним методом.

Вважаємо, що точки А і В лежать на колі (точка В від точки А за годинниковою стрілкою, тобто справа). На колі проти годинникової стрілки, тобто зліва від точки А, відкладаємо кут $3\alpha \leq \pi/2$, ($\alpha > 0$ – довільний гострий кут). Точки на колі в $\alpha, 2\alpha, 3\alpha$ радіанів, позначимо через A1, A2, A3; проведемо хорду A3A і промені з точки О через точки A1, A2, A3; точки перетину радіусів OA1 і OA2 з хордою A3A позначимо через C1, C2. Таким чином отримали трафарет (модель) поділу дуги A3A (кута AOA3) на 3(три) рівні частини і **“лінійну пам'ять”** цього поділу на хорді A3A. Проведемо хорди AB і A3B; через точки C1, C2, що лежать на хорді A3A, проведемо прямі паралельні до A3B (***пропорціональні відношення, передача інструкції***) і одержимо точки їх перетину з хордою AB: C1*, C2*; з точки О через точки C1*, C2* проведемо промені до перетину з колом і одержимо точки B1, B2;

точки C1*, C2* належать і радіусам OB1, OB2 і відрізки OC1*, OC2* також пропорціональні відповідним відрізкам OC1, OC2; в силу цього дуги: AB1 = B1B2 = B2B, відповідно і кути: B1OA = B2OB1 = BOB2 (див. мал.1). Кут $\alpha =$ A1OA вибраний довільним. Можна вибрати інший кут $\beta \neq \alpha$, побудувати на цьому ж малюнку другу модель, виконати відповідні дії і отримати точки B1, B2. На мал.1 це не показано, але кожен зможе зробити це самостійно.

Зауважимо, що така побудова є можливою завдяки постійній кривизні ліній: прямої (ρ = 0) і кола (ρ = 1/R) і центральної проекції, що і приводить початкову задачу до побудови пропорціональних відрізків [2], спираючись на теорему Фалеса, яка вивчається в шкільному курсі геометрії.

Такий поділ кутів на рівні частини, за допомогою попередньої заготовки (побудови) відповідного трафарету (моделі), можна виконати за допомогою циркуля і лінійки для довільного (в межах розумного) цілого n ≥ 2. Окрім того, таким методом можна ділити кути в заданій пропорції. Кути, які більші за $\frac{\pi}{2}$ (тупі кути), можна спочатку розділити пополам і потім ділити, за схемою, одну половину на n частин. За допомогою одного трафарету (моделі) можна поділити одразу декілька кутів різної величини. Зворотним процесом переконуємось в правильності побудови. Як бачимо, поділ кутів на n рівних частин, схожий з поділом відрізка прямої на n рівних частин, тільки при поділі кутів присутні елементи центральної проекції дуги кола на хорду і навпаки. Поділом кута $\pi/2$ на n рівних частин можна скористатись для вписування в коло правильних n – кутників. Точність результату поділу залежить від того, наскільки точно виконується побудова на всіх етапах. Запропонований метод поділу гострих кутів на n ≥ 2 рівних частин за допомогою циркуля і лінійки легко перевірити при поділі стандартних кутів, що легко діляться на n рівних частин. Такий модельний метод (алгоритм) поділу довільних кутів на довільне число n рівних частин можна легко запрограмувати для розрахунків і виконання креслень на ЕОМ.

Використана література
1. Постников М. М. Теория Галуа. М., 1963 г., Физматгиз.
2. Тесленко І. Ф. Елементарна математика. Геометрія. – К.: Вища школа, 1973.
3. Довідник з елементарної математики для вступників до вузів. За ред. члена-кореспондента АН УРСР П. Ф. Фільчакова. К.: Наук. думка, 1974.
4. Танчук М. О. Поділ плоских кутів на n ≥ 2 рівних частин за допомогою циркуля й лінійки. **XVII Міжнародна наукова конференція ім. акад. Михайла Кравчука, 19—20 травня 2016 р., Київ.** Матеріали конференції. Том 3. Теорія ймовірностей та математична статистика. Історія та методика математики. – С. 317 – 318.

Про квадратуру круга за допомогою циркуля і лінійки

Квадратура круга – задача, яка полягає в знаходженні способів побудови за допомогою циркуля і лінійки квадрата, рівновеликого за площею площі заданого круга, як трисекція кута і подвоєння куба, є однією з найвідоміших нерозв'язаних задач на побудову за допомогою циркуля і лінійки. Якщо позначити R – радіус заданного круга, x – довжину сторони шуканого квадрата, то, в сучасному розумінні, задача зводиться до розв'язку рівняння: $x^2 = \pi R^2$, звідки отримуємо: $x = \sqrt{\pi} R \approx 1{,}77245 R$. Доведено, що за допомогою циркуля і лінійки точно побудувати таку величину неможливо.

Давньогрецькі математики вважали своєю задачею не обчислення, а точну побудову шуканого квадрата («квадратуру»), причому, відповідно тодішнім принципам, тільки за допомогою **циркуля і лінійки.** Цією проблемою займались визначні античні вчені – Анаксагор, Антіфон, Брісон Гераклійський, Архімед та інші.

Гіпократ Хіоський у IV ст. до н. е. один із перших побачив, що деякі криволінійні фігури (гіпократові луночки) допускають точну квадратуру. Розширити клас таких фігур античним математикам не вдалося. Іншим шляхом пішов його сучасник Діностратт, який показав, що квадратуру круга можна чітко виконати за допомогою особливої кривої – квадратриси.

В «Началах» Евкліда (III ст. до н. е.) питання про площу круга не розглядається. Важливим етапом дослідження проблеми площі круга став твір Архімеда «Вимірювання круга», в якому вперше строго доказана теорема: площа круга рівна площі прямокутного трикутника, у якого один катет дорівнює радіусу кола, а другий – довжині кола. Архімед також дав оцінку числа $\pi \approx 22/7$.

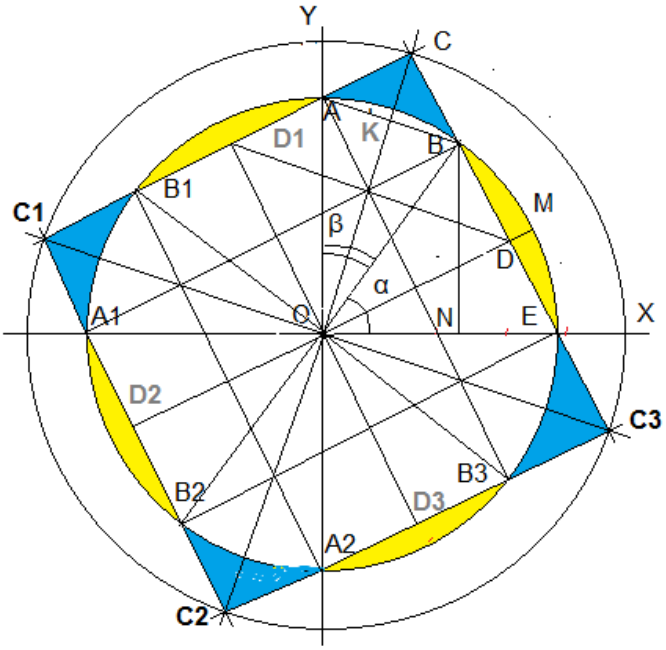
Подальші дослідження індійських, ісламських і європейських математиків на цю тему, довгий час стосувались, в основному, уточнення значення числа π і підбору наближених формул для квадратури круга. В середньовічній Європі цією задачею займались Фібоначі, Микола Кузанський і Леонардо да Вінчі. Пізніше численні дослідження опублікували Кеплер і Гюйгенс. Поступово міцніла впевненність у тому, що число π ірраціональне, тобто, не може бути точно вираженим за допомогою скінченного числа арифметичних операцій (включаючи добування кореня); звідси випливала б неможливість квадратури круга. Ірраціональність числа π була доведена Ламбертом у 1766 р. у роботі «Предварительные сведения для ищущих квадратуру и спрямление круга». Праця Ламберта мала прогалини, які незабаром були виправлені Лежандром (1794). Остаточний розв'язок отримав у 1882 р. Ліндеман. Математики також запропонували велику кількість практично корисних методів наближення квадратури круга. Якщо прийняти за одиницю виміру радіус круга і позначити через *x* довжину сторони шуканого квадрата, то задача зводиться до розв'язку рівняння: $x^2 = \pi$, звідси: $x = \sqrt{\pi}$. За допомогою циркуля і лінійки можна виконати всі 4 арифметичні дії і добування квадратного кореня; звідси випливає, що квадратура круга можлива тоді, і тільки тоді, коли за допомогою скінченного числа таких дій можна побудувати відрізок довжини π. Таким чином, нерозв'язаність цієї задачі випливає з неалгебраїчності (трансцендентності) числа π, яка була доведена в 1882 р. Ліндеманом.

Проте цю нерозв'язаність потрібно розуміти, як нерозв'язанність при використанні тільки **циркуля і лінійки**. Задача про квадратуру круга стає розв'язаною, якщо, крім циркуля і лінійки, використовувати інші засоби (наприклад, квадратрису). Простий механічний спосіб запропонував Леонардо да Вінчі. Виготуємо круговий циліндр із радіусом основи R і висотою R/2, покрасимо чорнилом бічну поверхню цього циліндра і покотимо його по площині. За один повний оберт циліндр залишить на площиі прямокутний слід площею πR^2. Маючи такий прямокутник уже досить просто побудувати рівновеликий йому квадрат.

Ось така коротка історія квадратури круга, взята з різних джерел в інтернеті.

Розв'язавши задачу трисекції кута (і не тільки!), я отримав можливість побудови, за допомогою циркуля і лінійки, квадрата рівновеликого заданому кругу [1], звичайно наближено, оскільки ідеальної формули для площі круга, окрім вище згаданої, немає. За основу взята відома формула площі круга $S = \pi R^2$.

Почнемо з аналізу. Оскільки описаний навколо круга квадрат за площею більший за нього, а вписаний – менший, то шуканий квадрат відсікатиме чотири, рівні за площею, сегменти і, в той же час, додаються чотири, рівні за площею криволінійних трикутники, тобто шуканий квадрат має бути таким, щоб площа криволінійного трикутника дорівнювала площі одного сегмента. Розмістимо квадрат таким чином, щоб криволінійний трикутник і сегмент були в одному квадранті прямолінійної системи координат, як це показано на мал. 2.



Мал.2.

Кут в 90° поділений на два гострі кути: BOA і EOB, дуги яких належать відповідно криволінійному трикутнику ACB і сегменту BME. Припустимо, що кут в 90° ($\pi/2$) поділено на дві частини:

$\beta = \text{BOA} = 30^\circ = \pi/6$, $\alpha = \text{EOB} = 60^\circ = \pi/3$. За таких даних легко виконати побудову за допомогою циркуля і лінійки (не описую) і обчислити площі потрібних нам фігур: сегмента і криволінійного трикутника:

$S_{\text{СЕК.EOB}} = (\alpha \cdot R^2)/2$; $S_{\text{ТР.EOB}} = (EB \cdot OD)/2 = (2 \cdot R \cdot \sin\alpha/2 \cdot R \cdot \cos\alpha/2)/2 = (R^2 \cdot \sin\alpha)/2$;

$S_{\text{СЕГ.EBM}} = S_{\text{СЕК.EOB}} - S_{\text{ТР.EOB}} = (\alpha \cdot R^2)/2 - (R^2 \cdot \sin\alpha)/2$;

$S_{\text{СЕК.BOA}} = (\beta \cdot R^2)/2$; $S_{\text{ТР.BOA}} = (AB \cdot OK)/2 = (2 \cdot R \cdot \sin\beta/2 \cdot R \cdot \cos\beta/2)/2 = (R^2 \cdot \sin\beta)/2$;

$S_{\text{СЕГ.AB}} = S_{\text{СЕК.BOA}} - S_{\text{ТР.BOA}} = (\beta \cdot R^2)/2 - (R^2 \cdot \sin\beta)/2$;

у трикутнику ACB: AC = CB; у трикутнику ACK: AK = KC;

$S_{\text{ТР.ACB}} = (AB \cdot KC)/2 = (2 \cdot R \cdot \sin\beta/2 \cdot R \cdot \sin\beta/2)/2 = R^2 \cdot \sin^2\beta/2$;

$S_{\text{КР.ТР.ACB}} = S_{\text{ТР.ACB}} - S_{\text{СЕГ.AB}} = R^2 \cdot \sin^2\beta/2 - (\beta \cdot R^2)/2 + (R^2 \cdot \sin\beta)/2$.

Тепер можна визначити значення параметрів α і β із системи двох рівнянь:

$\alpha + \beta = \frac{\pi}{2}$

$(\alpha \cdot R^2)/2 - (R^2 \cdot \sin\alpha)/2 = R^2 \cdot \sin^2\beta/2 - (\beta \cdot R^2)/2 + (R^2 \cdot \sin\beta)/2$;

Із першого рівняння, маємо: $\alpha = \frac{\pi}{2} - \beta$;

підставивши це значення α в друге рівняння, маємо:

$(\frac{\pi}{2} - \beta)\, R^2/2 - (R^2 \cdot \sin(\frac{\pi}{2} - \beta))/2 = R^2 \cdot \sin^2\beta/2 - (\beta \cdot R^2)/2 + (R^2 \cdot \sin\beta)/2$;

$\pi \cdot R^2/4 - \beta \cdot R^2/2 - (R^2 \cdot \cos\beta)/2 = R^2/2 - (R^2 \cdot \cos\beta)/2 + (R^2 \cdot \sin\beta)/2$;

$\frac{\pi}{2} - 1 = \sin\beta$;

якщо замінити β на $\frac{\pi}{2} - \alpha$, маємо:

$\cdot\frac{\pi}{2} - 1 = \cos\alpha \approx 0.5708$; $\alpha \approx 55^0$; $\beta \approx 35^0$; $\frac{\alpha}{\beta} = \frac{11}{7}$;

За допомогою циркуля і лінійки кут в 90^0 ділимо у відношенні 11/7 і виконуємо побудову квадратури круга, звичайно, наближено (див. мал. 2)

За величину кута $\propto$ можна взяти 1 радіан $\approx \frac{180}{\pi} \approx 57.29577951308$ …

$\propto \approx 57.3$, $\beta \approx 90 - 57.3 = 32.7$, $\alpha/\beta \approx 1.75229$ . . .

Якщо заокруглити до двох знаків, то можна взяти значення цього відношення рівним 1.75, до трьох знаків – 1.752; у першому випадку таке відношення складають числа 7 і 4 – 7/4 = 1.75, у другому – 876 і 500 – 876/500 = 1.752.

При таких відношеннях можна виконати побудову квадратури круга, хоча вона нічим, окрім точності наближення, не відрізняється від побудови на рис. 2. Побудову можна виконати ще простіше і іншим способом. Вважаючи радіус кола OE одиничним, побудуємо відрізок ON, а потім в точці N поставимо перпендикуляр до OE і визначимо точку B. Маючи точку B тепер легко побудувати точки B1, B2, B3 (EB = AB1 =A1B2 = A2B3) і закінчити побудову, провівши прямі через відповідні точки на колі, які в перетині визначають шуканий квадрат (мал. 2).

Можна взяти найкраще раціональное наближення числа π при відношенні двох трьоцифрових чисел 355/113, яке різниться лише сьомим знаком після коми, з точністю до 0.0000001, і виконати розрахунки і побудову, яка нічим (окрім точності наближення) не відрізняється від показаної на мал. 2.

Якщо врахувати, що круг одиничного радіуса обмежений колом $X^2 + Y^2 = 1$, то задача про квадратуру круга зводиться до побудови точки N на одиничному радіусі OE цього кола в першому квадранті (див.мал.2). Обчислюючи більш точніше значення $\cos\alpha$ можна побудувати квадрат із заданою точністю наближення. Слід зауважити, що квадратура круга не залежить від величини радіуса, а залежить тільки від значення $\cos\alpha$.

На мал.2. проведено коло радіусом OK, в яке вписано шуканий квадрат, рівновеликий одиничному кругу. Площа цього квадрата дорівнює:

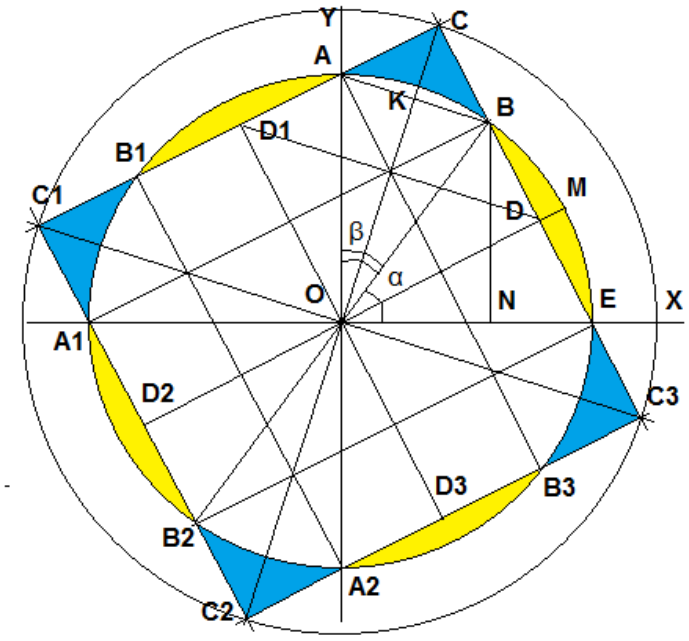
$S_{вп.кв.} = 2\,OC^2 = \pi$ (за умовою), отже:

$OC = (\pi/2)^{1/2} \approx 1.2533141373\ldots$ число трансцендентне, яке за допомогою циркуля і лінійки побудувати неможливо, а класична теорія про неперервність на мові "эпсильон – дельта" в задачах на побудову за допомогою циркуля і лінійки не враховуються, хоча всяка побудова за допомогою циркуля і лінійки, по суті, є наближеною навіть тоді, коли вона обгрунтована теоретично. Якщо не враховувати ці обмеження, то можна вважати задачу про квадратуру круга розв'язаною (наближено).

З описаної побудови випливає, що ідеальний квадрат рівновеликий площі круга існує, хоча при такому значені константи π побудувати його, за

допомогою циркуля і лінійки, неможливо. Будемо вважати, що якимось чином така побудова виконана і проведемо її аналіз.

На мал.2 маємо шуканий квадрат CC1C2C3. Лінії симетрії цього квадрата: D2D, D1D3 ділять його на 4(чотири) рівних квадрати: CD1OD, D1C1D2O, D2C2D3O, D3C3DO. Розглянемо квадрат CD1OD. В ньому проведені 4(чотири) лінії симетрії, включаючи діагоналі. Згідно цьому факту CB = BD, CD = BE, 2·BE = A1B. Із прямокутного трикутника A1BE, маємо: $A1B^2 + BE^2 = A1E^2$. Оскільки OE = 1, маємо: $5 \cdot BE^2 = 4$; звідси $BE = 2/\sqrt{5}$, сторона квадрата $C1C = A1B = 2 \cdot BE = 4/\sqrt{5}$; отже площа шуканого квадрата, рівновеликого площі круга одиничного радіуса $S_{CC1C2C3} = A1B^2 = (4/\sqrt{5})^2 = 3.2 = \pi$, згідно умови задачі. **Згідно умови $\pi/2 - 1 = \cos \alpha = 3.2/2 - 1 = 0.6$, що дозволяє легко виконати побудову рівновеликого квадрата за допомогою циркуля і лінійки (мал.3).**



Мал.3.

Цікаво відмітити і той факт, що координатами точки B є раціональні піфагорові числа (3/5; 4/5).

Таким чином, теоретично отримано нове фундаментальне раціональне значення для числа $\pi = 3.2$, визначення якого опирається на обгрунтовану основу через квадратуру круга одиничного радіуса з використанням властивостей симетрії квадрата. Чи узгоджується цей факт з обчисленнями довжини кола за формулою $C = 2 \cdot \pi \cdot R$? Це досить легко перевірити практично, хоча цей факт, очевидно, вимагає додаткової теоретичної і експериментальної оцінки фахівців. Може статись так, що для обчислень

довжини кола і площі круга, обмеженого цим колом, існують різні значення числа π. При виводі формул для обчислення довжини кола і площі круга, обмеженого цим колом, ми маємо справу з двома різними числовими послідовностями і гіпотетична константа в отриманих формулах: $C = 2\cdot\pi\cdot R$ і $S = \pi \cdot R^2$, можливо, може мати різні, за величиною, значення. Таку можливість не так легко заперечити, опираючись на результати квадратури круга, описані вище і тисячолітню історію розрахунків цього числа, пов'язану з відношенням C/ D (D = 2·R), хоча авторська перевірка цього факту показує на узгодження нового значення числа π з обчисленням довжини кола за формулою $C = 2\cdot\pi \cdot R$.

Нове значення числа π відхиляється від прийнятого, приблизно, лише на 0.06, але для великих значень довжини радіуса кола, обчислювані на практиці величини, що пов'язані з цим числом, наприклад, в астрономії і космонавтиці, матимуть досить значні відхилення, порівняно з попереднім значенням числа π. Ось така істина.

Використана література

1. Танчук М. О. Поділ плоских кутів на n ≥ 2 рівних частин за допомогою циркуля й лінійки. **XVII Міжнародна наукова конференція ім. акад. Михайла Кравчука, 19–20 травня 2016 р., Київ.** Матеріали конференції. Том 3. Теорія ймовірностей та математична статистика. Історія та методика математики. – С. 317 – 318.

Науково-популярне видання

Танчук Микола Олександрович

РОЗГАДКА ТАЄМНИЦІ ДОВЕДЕННЯ ВЕЛИКОЇ ТЕОРЕМИ П'ЄРА де ФЕРМА. ТРИСЕКЦІЯ ДОВІЛЬНИХ ПЛОСКИХ КУТІВ І КВАДРАТУРА КРУГА

шукаємо, знаходимо, порівнюємо, пізнаємо…

Начальник РВВ ДЕТУТ Л. В. Пономаренко
Редактор О. В. Ємець
Макет і верстк а О. В. Ємець

Надруковано в
Редакційно-видавничому відділі ДЕТУТ
(свідоцтво про реєстрацію серія ДК № 3079) від 27.12.07 р.
03049, м. Київ, вул. Миколи Лукашевича, 19.