Секція: Фізико-математичні науки

Танчук Микола Олександрович
пенсіонер
м. Київ, Україна

РОЗГАДКА ТАЄМНИЦІ ДОВЕДЕННЯ ВЕЛИКОЇ ТЕОРЕМИ ФЕРМА

В роботі розміщено матеріал, що торкається розгляду нелінійних діофантових рівнянь (велика теорема Ферма) у виді: 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 $n > 2$.

Зроблено короткий історичний огляд відносно доведення цієї теореми багатьма математиками світу протягом майже 400 років.

Залишений запис П'єром де Ферма на полях перекладу «Арифметики» Діофанта: «Я знайшов цьому воістину дивовижне доведення, але поля тут досить вузькі, щоб умістити його», завжди магічно впливав на тих, хто старався відшукати алгоритм розв'язку цієї трудної задачі, хоча жодному із них так і не вдалось відшукати, окрім часткових випадків, повного її розв'язку. Врешті, в 2015 році, мені вдалося розгадати таємницю алгоритму доведення Великої теореми П'єра де Ферма і вперше приведено 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. Вся текстова інформація підготовлена з використанням **Microsoft Word 2010.**

До 350-ї річниці від дня смерті великого французького математика

П'єра де Ферма (17.08.1601 – 12.01.1665)

В 2015 році (12.01) виповнилося 350 років з 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 із них так і не вдалося знайти загальний розв'язок цієї задачі .

Ось деякі дані, взяті в інтернеті щодо результатів доведення великої теореми Ферма на протязі 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 доказана Гауссом. Доведення теореми Ферма для випадку, коли $n = 5$, запропонували в 1825 році майже одночасно Лежен Діріхле і Лежандр. Своє доведення Діріхле опублікував в 1828 році, але воно було досить складним і, в 1912 році, його упростив Племель.

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

Метод Ламе уявляв собою надто віддалений розвиток ідей Ейлера і базувався на арифметичних властивостях чисел.

Проте зразу ж Ліувіль віднайшов в міркуваннях 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». Вона довела, що рівняння Ферма не має вирішення, коли n = p-1, де p – просте число виду 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».

Притягальна сила цієї теореми Ферма очевидна: не має іншого математичного твердження з таким простим формулюванням і уявною доступністю доведення, а також привабливістю суспільного престижу.

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

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

Вважається, що остаточний розв'язок великої теореми Ферма в 1994 році отримав англійський математик, професор Принстонського університету Эндрю Уайлс, який своєму доведенні опирався на відносно слабо використовувану на практиці теорію арифметичної алгебраїчної геометрії і ряд 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.

Для отримання більш повної інформації про доведення великої теореми Ферма Ендрю Уайлсом можна в інтернеті, в роботах: Дмитра Абрарова «Теорема Ферма: феномен доказательств Уайлса», Фелікса

Кірсанова «История великой теоремы Ферма», А. М. Белова «О доказательстве большой теоремы Ферма элементарными методами известными во время жизни Пьера де Ферма».

В моїй брошурі [4], надрукованій в 2015 році, в м. Києві, хоча стисло, але послідовно приведено 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 відносно 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 в 1665 році.

Далі приведено детальніше моє доведення великої теореми Ферма, розраховане на широке коло читачів і любителів серйозної математики.

Розглянемо нелінійні діофантові рівняння виду:

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

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:

$$(X, Y, Z) = 1 \tag{2}$$

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 із рівнянь (3) або (4):

$$X^n + Y^n = Z^n \tag{3}$$

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

$$X^n - Y^n = Z^n \tag{4}$$

де $X > 0$, $Y > 0$ – непарні, $X > Y$, $n \geq 2$ - цілі числа, в яких зліва присутні 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 виді:

$$X = 2 \cdot k + 1,\ Y = 2 \cdot m + 1,\ Z = 2^s \cdot q \tag{5}$$

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:

$$n = 2^{s0} \cdot p1^{s1} \cdot p2^{s2} \cdot \ldots \cdot pl^{sl} \tag{5*}$$

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

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

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:

$$X^n + Y^n \equiv 0 \pmod{2^n} \tag{7}$$

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

$$X^n - Y^n \equiv 0 \pmod{2^n} \tag{8}$$

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, $n \geq 2$ – ціле число)», P_3 (X, Y, Z, n) : «$X^n + Y^n = Z^n$, X, Y, Z – числа типу(5), $n \geq 2$ – ціле число)», P_4 (X, Y, Z, n) : «$X^n - Y^n = Z^n$, X, Y, Z – числа типу(5), $n \geq 2$ – ціле число)», P_7 (X, Y, n) : «$X^n + Y^n \equiv 0(\mathrm{mod}\ 2^n)$, X, Y – числа типу(5), $n \geq 2$ – ціле число)», P_8 (X, Y, n) : «$X^n - Y^n \equiv 0(\mathrm{mod}\ 2^n)$, X, Y – числа типу(5), $n \geq 2$ – 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 (Таблиця 1) і діз'юнкції (Таблиця 2), покажемо у виді 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 $n \geq 2$ рівняння (1) не має розв'язку при X = Y. Порівняння (7) в цьому випадку має вид: $X^n + Y^n = 2 \cdot X^n \equiv 0(\mathrm{mod}\ 2^n)$, що неможливо при $n \geq 2$. 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 $n \geq 2$ 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 $n \geq 2$, 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 $n = 2 \cdot h$, $h > 1$ – ціле, маємо: $X^{2 \cdot h} + Y^{2 \cdot h} = (X^h)^2 + (Y^h)^2 \equiv 2 \pmod{2^2} \not\equiv 0 \pmod{2^{2 \cdot h}}$, отже, P_7 (X, Y, 2h) = 0.

Отже, для всіх степенів $n = 2 \cdot h$, $h > 0$ - ціле, порівняння (7) , а також рівняння (3) не маюь 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, $h \geq 1$.

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

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

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

$X^2 - Y^2 = 4 \cdot (k^2 - m^2) + 4 \cdot (k - m) = 4 \cdot (k - m) \cdot (k + m + 1) \equiv 0 \pmod{2^2}$, 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) V P_4 (X, Y, Z, 2) = 0 V 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 в 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:

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

$$X^{h} - Y^{h} \equiv 0 \ (\mathrm{mod}\ 2^{h}). \qquad (10)$$

Якщо порівняння (9) і (10) виконуються одночасно, то їх сума і різниця також порівняні з нулем по (mod 2^h), тобто, $2 \cdot X^h \equiv 0$ (mod 2^h),

$2 \cdot Y^h \equiv 0$(mod 2^h), так як X і Y непарні, $2 \equiv 0$ (mod 2^h), що неможливо при $h \geq 2$, отже:

$P_8(X, Y, 2h) = ((P_7(X, Y, h) = 0) \wedge (P_8(X, Y, h) = 1)) \vee ((P_7(X, Y, h) = 1) \wedge (P_8(X, Y, h) = 0)) \vee ((P_7(X, Y, h) = 0) \wedge (P_8(X, Y, h) = 0)) = 0 \vee 0 \vee 0 = 0$, $h \geq 2$, 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) V P_4 (X, Y, Z, 2h) = 0 V 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 на протязі майже 4 - х століть, безперечно, вражає така простота *отриманих результатів дослідження справедливості твердження цієї теореми відразу для всієї множини парних чисел натурального ряду.*

Залишається дослідити на 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, ... і т. д.

Розглянемо (3) і (4) у виді:

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

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, s, p): « $X \pm Y = (2^{s})^{p}$, де X, Y - числа типу (5), $s \geq 1$- 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:

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

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

Враховуючи (5), для існування розв'язку рівнянь(3) і (4) необхідно, щоб

$$R = X \pm Y = (2^s)^p,$$

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

$$q = (2w+1)^p,\ w \geq 1 \text{ – ціле число} \qquad (12^*)$$

Враховуючи це: $(2w+1)^p \equiv 2w+1 \pmod p$, (мала теорема Ферма).

Введемо предикати:

$P_9(X, Y, p)$: «$R = X \pm Y \equiv 0 \pmod{2^p}$, X, Y – числа типу (5), p > 2 – просте число», $P_{10}(X, Y, q, p)$: «$(S = X^{p-1} + (\mp 1)^{p-2} X^{p-2} Y + \ldots + (\mp 1) X \cdot Y^{p-2} + Y^{p-1}) \equiv q^p \pmod p$, 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].

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

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

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

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

Відповідні значення k і m, що задовольняють таке порівняння, визначаємо з умови: $2\cdot(k \pm m + (1\pm1)/2) \equiv 0 \pmod{2^p}$; звідси $k \pm m + (1\pm1)/2 = 2^{p-1} \cdot t$, $t \geq 1$ – ціле ($t = 2^{p\cdot j}$, $j = 0, 1, 2, 3, \ldots$).

При таких значеннях k і m отримуємо відповідні взаємно прості значення X і Y, що забезпечують необхідну умову існування розв'язку для правих частин рівнянь (3) і (4), а саме, їх парної складової, для усіх простих степенів $p \geq 3$, при цьому предикати: $P_9(X, Y, p) = 1$ і $P_{12}(X, Y, s, p) = 1$.

Наведені нижче приклади для простих модулів *p = 3, 5, 7,* можливо краще, при уважному розгляді, допоможуть зрозуміти суть описаного тут алгоритму доведення великої теореми Ферма, а саме: використання малої теореми Ферма і ту дивовижність розв’язку, згадану в запису Ферма на сторінках «Арифметики» Діофанта.

Враховуючи (11) і (12), маємо:

$(S = (X^p \pm Y^p)/(X \pm Y)) \equiv 1 \pmod{p}$, (використана мала теорема Ферма ([1] , b , § 6 , гл. III)).

Візьмемо $p = 3$, $k \pm m + (1\pm1)/2 = 2^{3-1} \cdot t$,

$t \geq 1$ – ціле ($t = 2^{3\cdot j}$, $j = 0, 1, 2, \ldots$).

$J = 0$; $k \pm m + (1\pm1)/2 = 4$;

Приклад 1, k = 3, m = 0.

$X = 2\cdot3 + 1 = 7$, $Y = 1$, $X^3 + Y^3 = 7^3 + 1^3 = 343 + 1 = 344 = 2^3\cdot 43$,

$R = X + Y = 7 + 1 = 8 \equiv 0 \pmod{2^3}$,

$(S = (7^3 + 1^3)/ (7 + 1) = 43) \equiv 1 \pmod{3}$, (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 2, k = 4, m = 0.

$X = 2\cdot4 + 1 = 9$, $Y = 1$, $X^3 – Y^3 = 9^3 – 1^3 = 729 - 1 = 728 = 2^3\cdot 91 = 2^3\cdot7\cdot13$,

$R = X - Y = 9 - 1 = 8 \equiv 0 \pmod{2^3}$,

$(S = (9^3 - 1^3)/ (9 - 1) = 91) \equiv 1 \pmod 3$, (використана мала теорема Ферма ([1], b, § 6, гл. III));

$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;

$Z^3 = 2^3 \cdot (7 \cdot 13^{1/3})^3$;

$J = 1$; $k \pm m + (1 \pm 1)/2 = 32$;

Приклад 3, k = 31, m = 0.

$X = 2 \cdot 31 + 1 = 63$, $Y = 1$, $X^3 + Y^3 = 63^3 + 1^3 = 250047 + 1 = 250048 = 2^{3 \cdot} 43$,

$R = X + Y = 63 + 1 = 64 = 2^{3 \cdot 2} \equiv 0 \pmod{2^3}$,

$(S = (63^3 + 1^3)/ (63 + 1) = 3907) \equiv 1 \pmod 3$, (використана мала теорема Ферма ([1], b, § 6, гл. III));

$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;

$Z^3 = 2^{3 \cdot 2} (3907^{1/3})^3$;

Приклад 4, k = 32, m = 0.

$X = 2 \cdot 32 + 1 = 65$, $Y = 1$, $X^3 - Y^3 = 65^3 - 1^3 = 274625 - 1 = 274624 = 2^{3 \cdot 2} \cdot 4291 = \ = 2^{3 \cdot 2} ((7 \cdot 613)^{1/3})^3$,

$R = X - Y = 65 - 1 = 64 \equiv 0 \pmod{2^3}$,

$(S = (65^3 - 1^3)/ (65 - 1) = 4391) \equiv 1 \pmod 3$, (використана мала теорема Ферма ([1], b, § 6, гл. III));

$S \not\equiv q^3 \pmod 3$, тобто, для будь-яких допустимих значень q маємо: $q^3 \neq S$;

$Z^3 = 2^{3 \cdot 2} ((7 \cdot 613)^{1/3})^3$;

Візьмемо $p = 5$, $k \pm m + (1 \pm 1)/2 = 2^{5-1} \cdot t$,

$t \geq 1$ – ціле ($t = 2^{5 \cdot j}$, $j = 0, 1, 2, \ \ldots$).

$J = 0$; $k \pm m + (1 \pm 1)/2 = 16$;

Приклад 5, k = 15, m = 0.

$X = 2\cdot 15 + 1$, $Y = 1$, $X^5 + Y^5 = 31^5 + 1^5 = 28629151 + 1 = 28629152$,

$R = X + Y = 31 + 1 = 32 = 2^5$, $R \equiv 0 \pmod{2^5}$,

($S = (31^5 + 1^5)/ (31 + 1) = 894661) \equiv 1 \pmod 5$, (використана мала теорема Ферма ([1], b, § 6, гл. III));

$S \not\equiv q^5 \pmod 5$, тобто, для будь-яких допустимих значень q маємо: $q^5 \neq S$;

$Z^5 = 2^5\cdot (894661^{1/5})^5$;

Приклад 6, k = 16, m = 0.

$X = 2\cdot 16 + 1 = 33$, $Y = 1$, $X^5 - Y^5 = 33^5 - 1^5 = 39135393 - 1 = 39135392 =$

$= 2^5\cdot 1222981$,

$R = 2^5$, $S = 1222981$,

$R \equiv 0 \pmod{2^5}$, ($S = (33^5 - 1^5)/ (33 - 1) = 1222981) \equiv 1 \pmod 5$,(використана мала теорема Ферма ([1], b, § 6, гл. III));

$S \not\equiv q^5 \pmod 5$, тобто, для будь-яких допустимих значень q маємо: $q^5 \neq S$;

$Z^5 = 2^5\cdot (1222081^{1/5})^5$;

Візьмемо $p = 7$, $k \pm m + (1\pm 1)/2 = 2^{7-1} \cdot t$,

$t \geq 1$ – ціле ($t = 2^{7\cdot j}$, $j = 0, 1, 2, \ldots$).

$J = 0$; $k \pm m + (1\pm 1)/2 = 64$;

Приклад 7, k = 63, m = 0.

$X = 2\cdot 63 + 1$, $Y = 1$, $X^7 + Y^7 = 127^7 + 1^7 = 532875860165503 + 1 =$

$= 532875860165504$,

$R = X + Y = 127 + 1 = 128 = 2^7$, $R \equiv 0 \pmod{2^7}$,

($S = (127^7 + 1^7)/ (127 + 1) = 4163092657543) \equiv 1 \pmod 7$, (використана мала теорема Ферма ([1], b, § 6, гл. III));

$S \not\equiv q^7 \pmod 7$, тобто, для будь-яких допустимих значень q маємо: $q^7 \neq S$;

$Z^7 = 2^7\cdot (4163092657543^{1/7})^7$;

Приклад 8, k = 64, m = 0.

$X = 2{\cdot}64 + 1$, $Y = 1$, $X^7 - Y^7 = 129^7 - 1^7 = 594467302491009 - 1 =$

$= 594467302491008 = 2^7 \cdot 4644275800711$,

$R = 2^7$, $S = 4644275800711$,

$R \equiv 0 (\mathrm{mod}\ 2^7)$, $(S = (129^7 - 1^7)/(129 - 1) = 4644275800711) \equiv 1 (\mathrm{mod} 7)$, (використана мала теорема Ферма ([1], b, § 6, гл. III));

$S \not\equiv q^7\ (\mathrm{mod}\ 7)$, тобто, для будь-яких допустимих значень q маємо: $q^7 \neq S$;

$Z^7 = 2^7 \cdot (4644275800711^{1/7})^7$.

Розглянуті вище приклади тільки на множині допустимих пар непарних чисел (X, Y), що гарантують істинність предикатів P_9 і P_{12} , а інші пари непарних чисел (X, Y), які цього не гарантують можна зовсім не розглядати.

Як бачимо із наведених прикладів, для любого простого $p \geq 3$ можна чітко вказати всю множину таких пар взаємно простих непарних чисел (X, Y), для яких $R \equiv 0 (\mathrm{mod}\ 2^p)$, і завжди представлене у вигляді: $R = (2^s)^p$, $s \geq 1$ – ціле число, як це вимагається за змістом задачі і гарантує істинність предикатів P_9 і P_{12}. Подібні приклади можна навести для будь-якого простого модуля $p > 2$.

Але, як бачимо із прикладів, навіть істинність предиката P_9 і P_{12} ще не гарантує істинності предиката P_{10}, 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 $R = (2^s)^p$, $s \geq 1$ – ціле число, $S = q^p$.

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

Чи існує q, щоб $S = q^p$?

Згідно з (13) , $q^p \equiv 2{\cdot}w{+}1\ (\mathrm{mod}\ p)$ – непарне > 1; (використана мала теорема Ферма ([1], b, § 6, гл. III));

згідно з (11) $(S = (X^p \pm Y^p)/(X \pm Y)) \equiv 1\ (\mathrm{mod}\ p)$ (використана мала теорема Ферма ([1] , b , § 6 , гл. III)).

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

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

$P_3(X, Y, Z, p) = 0$, $P_4(X, Y, Z, p) = 0$.

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 представлене у вигляді добутку двох або більше простих чисел і їх степенів; для переконливості досить розглянути випадок, коли $n = p1 \cdot p2$, (p1 , p2 - прості числа > 2), маємо:

$$X^{p1 \cdot p2} \pm Y^{p1 \cdot p2} = Z^{p1 \cdot p2} \tag{14}$$

Рівняння (14) можна представити у виді:

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

Як бачимо (15) є рівнянням виду (11), а тому для нього справедливі висновки, приведені 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 в 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 в рівняннях (3) і (4) зміна знаку чисел X, Y, Z не впливає на результати дослідження.

В Табл. 3 показана зміна ситуації залежно від того, які значення приймають змінні X, Y, Z в множині цілих чисел при непарних степенях в рівняннях (3) і (4).

Таблиця 3

№ варіанту	**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 із Таблиці 3, Велика теорема Ферма справедлива в множині цілих чисел з точністю до знаку.

Припустимо, що рівняння (1) має розв'язок в 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 виді: $(x_1/x_2)^n + (y_1/y_2)^n = (z_1/z_2)^n$, 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 вважати новинкою в сучасній теорії чисел, як самий простий, 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 і не має геометричної наочності.

У підтвердження зробленому П'єром де Ферма на полях перекладу "Арифметики" Діофанта запису: "Я знайшов цьому справді дивовижне доведення, але поля тут досить вузькі, щоб розмістити 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 із трьох значень: парне, просте, складне непарне, а для таких чисел правдивість великої теореми Ферма доведена формально.

Переконатися в цьому можна за допомогою додаткових тестових розрахунків на ЕОМ для різних простих чисел, як це показано вище приведеними прикладами.

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

Література

1. Виноградов И. М. Основы теории чисел. М.: 1965 г. Изд. "Наука".
2. Бухштаб А. А. Теория чисел. М.: 1966 г. Изд. "Просвещение".
3. Курош А. Г. Курс высшей алгебры. М.: 1975 г. Изд. "Просвещение"
4. Танчук М.О. Доведення великої теореми П. Ферма. Київ. – 2015 р. RMprint.
5. Танчук М.О. Розгадка таємниці доведення великої теореми Ферма // Математика в школах України. – 2018. - №30. – С. 27-34.