РОЗГАДКА ТАЄМНИЦІ ДОВЕДЕННЯ ВЕЛИКОЇ ТЕОРЕМИ ФЕРМА

М. О. Танчук, м. Київ

У статті розміщено матеріал, що торкається розгляду нелінійних діофантових рівнянь (велика теорема Ферма) у вигляді: довести, що рівняння $x^n + y^n = z^n$ не має розв'язків у цілих числах $x > 0$, $y > 0$, $z > 0$ для всіх натуральних $n > 2$.

Зроблено короткий історичний огляд щодо доведення цієї теореми багатьма математиками світу впродовж майже 400 років.

Залишений запис П'єром де Ферма на берегах перекладу «Арифметики» Діофанта: «Я знайшов цьому воістину дивовижне доведення, але берега тут досить вузькі, щоб умістити його», завжди магічно впливав на тих, хто намагався відшукати алгоритм розв'язання цієї складної задачі, хоча жодному з них так і не вдалось відшукати, окрім часткових випадків, повного її розв'язання. Урешті, 2015 року, мені вдалося розгадати таємницю алгоритму доведення Великої теореми П'єра де Ферма і вперше наведено 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. Уся 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)

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

Найбільше він відомий своєю знаменитою великою теоремою Ферма: довести, що рівняння $x^n + y^n = z^n$ не має розв'язків у цілих числах: $x > 0$, $y > 0$, $z > 0$ для всіх натуральних значень $n > 2$,— яку він сформулював ще 1637 року.

Розв'язанням 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, узяті в інтернеті щодо результатів доведення великої теореми Ферма впродовж 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 під час свого доведення, 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 1828 року, але воно було досить складним і 1912 року його спростив Племель.

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

Метод Ламе — це надто віддалений розвиток ідей Ейлера, який базувався на арифметичних властивостях чисел. Проте відразу Ліувіль віднайшов у 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 розв'язків, 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, довели справедливість теореми Ферма для всіх простих показників $n<100000$.

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

Окрім того, завжди вражала ймовірність елементарного доведення, оскільки сам Ферма, вочевидь, знав доведення, написавши на берегах перекладу «Арифметики» Діофанта: «Я знайшов цьому справді дивовижне доведення, але берега тут досить вузькі, щоб помістити його».

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

Уважається, що остаточне розв'язання великої теореми Ферма отримав (1994 рік) англійський математик, професор Принстонського університету Эндрю Уайлс, який у своєму доведенні спирався на відносно слабко використовувану на практиці теорію арифметичної алгебраїчної геометрії й низку сучасних математичних інструментів, створених великою кількістю математиків за останні сто років, що були відсутніми за життя П'єра де Ферма. У результаті він отримав доведення досить об'ємне (у журнальному варіанті займає 120 сторінок) і складне для розуміння навіть професійними математиками.

Більш повну інформацію про доведення великої теореми Ферма Ендрю Уайлсом можна знайти в інтернет, у таких роботах: Дмитро Абраров «Теорема Ферма: феномен доказательств Уайлса», Фелікс Кірсанов «История великой теоремы Ферма», А. М. Белов «О доказательстве большой теоремы Ферма элементарными методами известными во время жизни Пьера де Ферма».

У моїй брошурі [4], надрукованій у 2015 році, хоча 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.

Маю надію, що моя робота знайде серед математиків тих, хто спроможний оцінити знайдене в Україні, важливе для світової математики, перше повне доведення цієї теореми методами, добре відомими Ферма, за ці рівно 350 років (12.01.2015), що минули від дня його відходу в інший світ 1665 року.

Далі наведено 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: $x>0$, $y>0$, $z>0$.

Уважаємо, що три числа $x>0$, $y>0$, $z>0$, якщо вони є розв'язками рівняння (1), задовольняють умову:

$$(x,y,z)=1. \tag{2}$$

Трійка чисел, що задовольняє умову (2) має найбільший спільний дільник 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):

$$x^n+y^n=z^n, \tag{3}$$

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, у яких ліворуч присутні сума або різниця тільки двох непарних чисел степеня n $\left(x^n,y^n\right)$, а праворуч — парне число в степені n $\left(z^n\right)$.

Цілі числа x, y, z розглядатимемо у вигляді:

$$z=2k+1,\ \ y=2m+1,\ \ z=2^s\cdot q, \tag{5}$$

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

$$q=2w+1,\ \ w\geq 0 \text{ — ціле число.}$$

Під час розгляду степенів n рівняння (1) числа натурального ряду розглядатимемо в канонічній формі:

$$n = 2^{s_0} \cdot p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_l^{s_l \ 1}, \tag{5*}$$

де s_0, s_1, s_2, ..., s_l — цілі числа, які більші або дорівнюють нулю; при $s_0 \geq 1$, $s_i \geq 0$ $(i = 1, 2, \ldots, l)$ маємо парні числа; при $s_0 = 0$ і, хоча б одне із $s_i \neq 0$, $(i = 1, 2, \ldots, l)$ маємо непарні числа; тут $p_1 < p_2 < \ldots < p_l$ — прості числа, більші за 2.

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

$$z^n = \left(2^s \cdot q\right)^n \equiv 0\left(\operatorname{mod} 2^n\right), \tag{6}$$

де $s \geq 1$, $n \geq 2$ — цілі числа, $q \geq 1$ — непарне.

Без особливих втрат для подальшого розгляду вважатимемо $s = 1$. Ураховуючи (6), розглянемо питання існування розв'язку порівнянь:

$$x^n + y^n \equiv 0\left(\operatorname{mod} 2^n\right), \tag{7}$$

де x, y — непарні числа виду (5), $n \geq 2$ — ціле число,

$$x^n - y^n \equiv 0\left(\operatorname{mod} 2^n\right), \tag{8}$$

де x, y — непарні числа виду (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 виду (5), $n \geq 2$ — ціле число,
- ✓ $P_4(x, y, z, n)$: $x^n - y^n = z^n$, x, y, z — числа виду (5), $n \geq 2$ — ціле число,
- ✓ $P_7(x, y, n)$: $x^n + y^n \equiv 0\left(\operatorname{mod} 2^n\right)$, x, y — числа виду (5), $n \geq 2$ — ціле число,
- ✓ $P_8(x, y, n)$: $x^n - y^n \equiv 0\left(\operatorname{mod} 2^n\right)$, x, y — числа виду (5), $n \geq 2$ — ціле число.

Ці предикати набувають значення 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 виду кон'юнкції (таблиця 1) і диз'юнкції (*таблиця 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 $n \geq 2$ рівняння (1) не має розв'язків при $x = y$. Порівняння (7) в цьому випадку має вигляд: $x^n + y^n = 2 \cdot x^n \equiv 0\left(\operatorname{mod} 2^n\right)$, 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

$$P_1(x, y, z, 2) = P_3(x, x, y, 2) \vee P_4(x, x, 0, 2) = 0 \vee 0 = 0,$$

тобто розв'язку для рівняння (1) не існує при $n \geq 2$ у цілих числах: $x > 0$, $y > 0$, $z > 0$ виду (5).

Дослідимо рівняння (3) на існування розв'язків у цілих числах:

$x > 0$, $y > 0$, $z > 0$ виду (5) для цілих $n \geq 2$, використовуючи порівняння (7).

Розглянемо: $x^2 + y^2 = z^2$.

Ураховуючи (5), маємо:

$$(2k + 1)^2 + (2m + 1)^2 =$$

$$= 4\left(k^2 + m^2\right) + 4(k + m) + 2 \equiv 2\left(\operatorname{mod} 2^2\right).$$

Із цього випливає, що умова (7) не виконується для всіх цілих значень:

$x > 0$, $y > 0$ виду (5), отже, $P_7(x, y, 2) = 0$.

Розглянемо випадки, коли $n = 2 \cdot h$, $h > 1$ — ціле, маємо:

$$x^{2h} + y^{2h} = \left(x^h\right)^2 + \left(y^h\right)^2 \equiv 2\left(\operatorname{mod} 2^2\right) \not\equiv 0\left(\operatorname{mod} 2^{2h}\right),$$

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 мають розв'язків у цілих числах:

$x>0$, $y>0$, $z>0$ виду (5), тобто, $P_7(x,y,2h)=0$, $P_3=(x,y,z,2h)=0$, $h\geq 1$.

Дослідимо рівняння (4) на існування розв'язків у цілих числах: $x>0$, $y>0$, $z>0$ для цілих $n\geq 2$, використовуючи порівняння (8).

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

$$x^2-y^2=4\left(k^2-m^2\right)+4(k-m)=$$

$$=4(k-m)(k+m+1)\equiv 0\left(\bmod 2^2\right),$$

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] $x=u^2+v^2$, $y=u^2-v^2$, $z=2uv$, де $u>v$ — два послідовних числа натурального ряду, наприклад:

$$u=8,\ v=7,\ z=8^2+7^2=113,\ y=8^2-7^2=15,$$
$$z=2\cdot 8\cdot 7=112;\ 113^2-15^2=112^2,\ \ldots \text{ тощо},$$

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 $n=2$ у цілих числах: $x>0$, $y>0$, $z>0$ виду (5).

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

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

$$x^{2h}-y^{2h}=\left(x^h+y^h\right)\left(x^h-y^h\right).$$

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

$$x^h+y^h\equiv 0\left(\bmod 2^h\right), \qquad (9)$$

$$x^h-y^h\equiv 0\left(\bmod 2^h\right). \qquad (10)$$

Якщо порівняння (9) і (10) виконуються одночасно, то їхня сума і різниця також порівняні з нулем за $\left(\bmod 2^h\right)$, тобто, $2x^h\equiv 0\left(\bmod 2^h\right),\cdot y^h\equiv 0\left(\bmod 2^h\right)$, оскільки x і y непарні, $2\equiv 0\left(\bmod 2^h\right)$, що неможливо при $h\geq 2$, отже,

$$P_8(x,y,2h)=\left(P_7(x,y,h)\wedge P_8(x,y,h)=1\right)\vee$$
$$\vee\left(P_7(x,y,h)=1\wedge P_8(x,y,h)=0\right)\vee$$
$$\vee\left(P_7(x,y,h)=0\right)\wedge\left(P_8(x,y,h)=0\right)=0,\ \ h\geq 2,$$

отже, $P_4(x,y,z,2h)=0$, $h\geq 2$.

Ураховуючи ці результати, маємо:

$$P_1(x,y,z,2h)=P_3(,y,z,2h)\vee P_4(x,y,z,2h)=0\vee 0=0,$$

тобто, розв'язків для рівняння (1) не існує при $h\geq 2$ у цілих числах: $x>0$, $y>0$, $z>0$ виду (5).

З огляду на відомі історичні дані про труднощі доведення великої теореми Ферма впродовж майже чотирьох 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'язків рівнянь (3) і (4), використовуючи відповідно порівняння (7) і (8), для непарних значень $n=2h+1$, h — ціле ≥ 1.

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

Розглянемо (3) і (4) у вигляді:

$$x^p\pm y^p=(x\pm y)\times$$
$$\times\left(x^{p-1}+(\mp 1)^{p-2}x^{p-2}y+\ldots+(\mp 1)xy^{p-2}+y^{p-1}\right)=z^p. \qquad (11)$$

Уведемо предикати:

$P_{11}(x,y,z,p)$:

$$x^p\pm y^p=(x\pm y)\times$$
$$\times\left(x^{p-1}+(\mp 1)^{p-2}x^{p-2}y+\ldots+(\mp 1)xy^{p-2}+y^{p-1}\right)=z^p,$$

x, y, z — числа виду (5), $p>2$ — просте число.

$P_{12}(x,y,s,p)$: $x\pm y=\left(2^s\right)^p$, де x, y — числа типу (5), $s\geq 1$ — ціле число, $p>2$ — просте число.

Предикати P_{11} і P_{12} набувають значення на множині $M\{1,0\}$, тобто, «істина» = 1, коли рівність справедлива або «хибність» = 0, коли рівність не виконується.

Ураховуючи (11), уведемо позначення:

$$R=x\pm y,$$

$$S=x^{p-1}+(\mp 1)^{p-2}x^{p-2}y+\ldots+(\mp 1)xy^{p-2}+y^{p-1},$$

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

Ураховуючи (5), для існування розв'язків рівнянь (3) і (4) необхідно, щоб

$$R=x\pm y=\left(2^s\right)^p,$$

$$S = x^{p-1} + (\mp 1)^{p-2} x^{p-2} y + \ldots + (\mp 1) x y^{p-2} + y^{p-1} = q^p,$$

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

Ураховуючи це, маємо:

$(2w+1)^p \equiv 2w+1 (\bmod p)$ (мала теорема Ферма).

Уведемо предикати:

$$P_9(x, y, p):\ R = x \pm y \equiv 0 (\bmod 2^p),$$

x, y — числа виду (5), $p > 2$ — просте число,

$P_{10}(x, y, q, p)$:

$$\left(S = x^{p-1} + (\mp 1)^{p-2} x^{p-2} y + \ldots + (\mp 1) x y^{p-2} + y^{p-1}\right) \equiv$$

$$\equiv q^p (\bmod p),$$

x, y, q — числа виду (5), $p > 2$ — просте число.

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

Ураховуючи (5), маємо:

$$R = 2k + 1 \pm (2m+1) = 2\left(k \pm m + \frac{(1 \pm 1)}{2}\right) \text{ —}$$

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 порівнне з нулем за $\bmod (2^p)$, то рівняння (3) і (4), очевидно, розв'язків 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'язків не існує в цілих числах: $x > 0$, $y > 0$, $z > 0$ виду (5).

Ураховуючи (6), (11), (12), розглянемо порівняння $R \equiv 0 (\bmod 2^p)$.

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

Відповідні значення k і m, що задовольняють таке порівняння, визначаємо з умови:

$$2\left(k \pm m + \frac{(1 \pm 1)}{2}\right) \equiv 0 (\bmod 2^p),$$

$$\text{звідси } k \pm m + \frac{(1 \pm 1)}{2} = 2^{p-1} t,$$

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

При таких значеннях k і m отримуємо відповідні взаємно прості значення x і y, що забезпечують необхідну умову існування розв'язків для правих частин рівнянь (3) і (4), а саме, їх парної складової, для всіх 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, за уважного розгляду, допоможуть зрозуміти суть описаного тут алгоритму доведення великої теореми Ферма, а саме: використання малої теореми Ферма і ту дивовижність розв'язання, згадану Ферма на сторінках «Арифметики» Діофанта.

Ураховуючи (11) і (12), маємо:

$S = \dfrac{x^p \pm y^p}{x \pm y} \equiv 1 (\bmod p)$ (використана мала теорема Ферма ([1], b, § 6, гл. III)).

Візьмемо $p = 3$, $k \pm m + \dfrac{1 \pm 1}{2} = 2^{3-1} t$, $t \geq 1$ — ціле ($t = 2^{3j}$, $j = 0, 1, 2, \ldots$).

$$j = 0,\ k \pm m + \frac{1 \pm 1}{2} = 4.$$

Приклад 1. $k = 3$, $m = 0$.

$$x = 2 \cdot 3 + 1 = 7,\ y = 1,$$

$$x^3 + y^3 = 7^3 + 1^3 = 343 + 1 = 344 = 2^3 \cdot 43,$$

$$R = x + y = 7 + 1 = 8 \equiv (\bmod 2^3),$$

- ✓ $S = \dfrac{7^3 + 1^3}{7 + 1} = 43 \equiv 1 (\bmod 3)$ (використана мала теорема Ферма ([1], b, § 6, гл. III));
- ✓ $S \not\equiv q^3 (\bmod 3)$, тобто, для будь-яких допустимих значень q маємо:

$$q^3 \neq S,\ z^3 = 2^3 \cdot \left(43^{\frac{1}{3}}\right)^3.$$

Приклад 2. $k = 4$, $m = 0$.

$$x = 2 \cdot 4 + 1 = 9,\ y = 1,$$

$$x^3 - y^3 = 9^3 - 1^3 = 729 - 1 = 728 = 2^3 \cdot 91 = 2^3 \cdot 7 \cdot 13,$$

$$R = x - y = 9 - 1 = 8 \equiv 0 (\bmod 2^3),$$

✓ $S=\dfrac{9^3-1^3}{9-1}=91\equiv 1(\mathrm{mod}\,3)$ (використана мала теорема Ферма ([1], b, § 6, гл. III));

✓ $S\not\equiv q^3(\mathrm{mod}\,3)$, тобто, для будь-яких допустимих значень q маємо:

$$q^3\ne S,\ z^3=2^3\cdot\left(7\cdot 13^{\frac{1}{3}}\right)^3.$$

$$j=1,\ k\pm m+\frac{1\pm 1}{2}=32.$$

Приклад 3. $k=31,\ m=0.$

$$x=2\cdot 31+1=63,\ y=1,$$

$$x^3+y^3=63^3+1^3=250047+1=250048=2^3\cdot 43,$$

$$R=x+y=63+1=64=2^{3\cdot 2}\equiv 0\left(\mathrm{mod}\,2^3\right),$$

✓ $S=\dfrac{63^3+1^3}{63+1}=3907\equiv 1(\mathrm{mod}\,3)$ (використана мала теорема Ферма ([1], b, § 6, гл. III));

✓ $S\not\equiv q^3(\mathrm{mod}\,3)$, тобто, для будь-яких допустимих значень q маємо:

$$q^3\ne S,\ z^3=2^{3\cdot 2}\left(3907^{\frac{1}{3}}\right)3.$$

Приклад 4. $k=32,\ m=0.$

$$x=2\cdot 32+1=65,\ y=1,$$

$$x^3-y^3=65^3-1^3=274625-1=274624=$$

$$=2^{3\cdot 2}\cdot 4291=2^{3\cdot 2}\left((7\cdot 613)^{\frac{1}{3}}\right)^3,$$

$$R=x-y=65-1=64\equiv 0\left(\mathrm{mod}\,2^3\right),$$

✓ $S=\dfrac{65^3-1^3}{65-1}=4391\equiv 1(\mathrm{mod}\,3)$ (використана мала теорема Ферма ([1], b, § 6, гл. III));

✓ $S\not\equiv q^3(\mathrm{mod}\,3)$, тобто, для будь-яких допустимих значень q маємо:

$$q^3\ne S,\ z^3=2^{3\cdot 2}\left((7\cdot 613)^{\frac{1}{3}}\right)^3.$$

Візьмемо $p=5,\ k\pm m+\dfrac{1\pm 1}{2}=2^{5-1}t,\ t\ge 1$ — ціле ($t=2^{5j},\ j=0,1,2,\ldots$).

$$j=0,\ k\pm m+\frac{1\pm 1}{2}=16.$$

Приклад 5. $k=15,\ m=0.$

$$x=2\cdot 15+1,\ y=1,$$

$$x^5+y^5=31^5+1^5=28629151+1=28629152,$$

$$R=x+y=31+1=32=2^5,\ R\equiv 0\left(\mathrm{mod}\,2^5\right),$$

✓ $S=\dfrac{31^5+1^5}{31+1}=894661\equiv 1(\mathrm{mod}\,5)$ (використана мала теорема Ферма ([1], b, § 6, гл. III)).

✓ $S\not\equiv q^5(\mathrm{mod}\,5)$, тобто, для будь-яких допустимих значень q маємо:

$$q^5\ne S,\ z^5=2^5\cdot\left(894661^{\frac{1}{5}}\right)^5.$$

Приклад 6. $k=16,\ m=0.$

$$x=2\cdot 16+1=33,\ y=1,$$

$$x^5-y^5=33^5-1^5=$$

$$=39135393-1=39135392=2^5\cdot 1222981,$$

$$R=2^5,\ S=1222981,\ R\equiv 0\left(\mathrm{mod}\,2^5\right),$$

✓ $S=\dfrac{33^5-1^5}{33-1}=1222981\equiv 1(\mathrm{mod}\,5)$ (використана мала теорема Ферма ([1], b, § 6, гл. III)).

✓ $S\not\equiv q^5(\mathrm{mod}\,5)$, тобто, для будь-яких допустимих значень q маємо:

$$q^5\ne S,\ z^5=2^5\cdot\left(1222081^{\frac{1}{5}}\right)^5.$$

Візьмемо $p=7,\ k\pm m+\dfrac{1\pm 1}{2}=2^{7-1}t,\ t\ge 1$ — ціле ($t=2^{7j\ j},\ j=0,1,2,\ldots$).

$$j=0,\ k\pm m+\frac{1\pm 1}{2}=64.$$

Приклад 7. $k=63,\ m=0.$

$$x=2\cdot 63+1,\ y=1,$$

$$x^7+y^7=127^7+1^7=$$

$$=532875860165503+1=532875860165504,$$

$$R=x+y=127+1=128=2^7,\ R\equiv\left(\mathrm{mod}\,2^7\right),$$

✓ $S=\dfrac{127^7+1^7}{127+1}=4163092657543\equiv 1(\mathrm{mod}\,7)$ (використана мала теорема Ферма ([1], b, § 6, гл. III)).

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

$$q^7 \neq S,\ z^7 = 2^7 \cdot \left(4163092657543^{\frac{1}{7}}\right)^7.$$

Приклад 8. $k = 64,\ m = 0.$

$$x = 2 \cdot 64 + 1,\ y = 1,$$

$$x^7 - y^7 = 129^7 - 1^7 = 594467302491009 - 1 =$$

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

$$R = 2^7,\ S = 4644275800711,\ R \equiv 0\left(\bmod 2^7\right),$$

✓ $S = \dfrac{129^7 - 1^7}{129 - 1} = 4644275800711 \equiv 1 \pmod 7$ (використана мала теорема Ферма ([1], b, § 6, гл. III)).

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

$$q^7 \neq S,\ z^7 = 2^7 \cdot \left(4644275800711^{\frac{1}{7}}\right)^7.$$

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 будь-якого простого $p \geq 3$ можна чітко вказати всю множину таких пар взаємно простих непарних чисел (x, y), для яких $R \equiv 0\left(\bmod 2^p\right)$, і завжди подане у вигляді: $R = \left(2^s\right)^p$, $s \geq 1$ — 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}.

Уважатимемо, що $P_9 = 1$ і $P_{12} = 1$.

Розглянемо рівність $R \cdot S = R \cdot q^p$, де $R = \left(2^s\right)^p$, $s \geq 1$ — ціле число, $S = q^p$.

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

Чи існує q, щоб $S = q^p$?

Згідно з (13), $q^p \equiv 2w + 1 \pmod p$ — непарне, більше за 1 (використана мала теорема Ферма ([1], b, § 6, роз. III)), згідно з (11) $S = \dfrac{x^p \pm y^p}{x \pm y} \equiv 1 \pmod p$ (використана мала теорема Ферма ([1] , b , § 6 , роз. III)).

Оскільки $S \equiv 1 \pmod p$, а $2w + 1$ — непарне, більше за 1, то S і q^p не порівняні за $(\bmod p)$, 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'язків у 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'язків не існує в цілих числах: $x > 0$, $y > 0$, $z > 0$ виду (5) для всіх простих чисел $p > 2$.

Розглянемо випадки, коли степені n складені непарні числа, тобто n подане у вигляді добутку двох або більше простих чисел та їхніх степенів. Для переконливості досить розглянути випадок, коли $n = p_1 \cdot p_2$, (p_1, p_2 — прості числа, більші за 2), маємо:

$$x^{p_1 p_2} \pm y^{p_1 p_2} = z^{p_1 p_2}. \quad (14)$$

Рівняння (14) можна подати у вигляді:

$$x^{p_1 p_2} \pm y^{p_1 p_2} = \left(x^{p_1}\right)^{p_2} \pm \left(y^{p_1}\right)^{p_2} =$$

$$= \left(x^{p_1} \pm y^{p_2}\right)\left(\left(x^{p_1}\right)^{p_2 - 1} + (\mp 1)^{p-2}\left(x^{p_1}\right)^{p_2 - 2} y^{p_1} + \ldots +\right.$$

$$\left. + (\mp 1) x^{p-1}\left(y^{p_1}\right)^{p_2 - 2} + \left(y^{p_1}\right)^{p_2 - 1}\right) = z^{p_1} \cdot \left(z^{p_1}\right)^{p_2 - 1}. \quad (15)$$

Як бачимо, (15) є рівнянням виду (11), а тому для нього справедливі висновки, наведені вище. Більше того, якщо враховувати канонічну форму (5*) числа n, то p_1 можна вважати складеним, а p_2 простим і в такий спосіб показати, що розв'язків не існує і для інших умовно простих степенів рівнянь (3) і (4) у цілих числах: $x>0$, $y>0$, $z>0$ виду (5), звичайно також і рівняння (1).

Отже, **велика теорема Ферма доведена.**

Таємниця алгоритму розв'язання 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 на 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 *таблиці 3* показана зміна ситуації залежно від того, яких значень набувають змінні x, y, z на множині цілих чисел при непарних степенях у 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 на множині цілих чисел із точністю до знака.

Припустимо, що рівняння (1) має розв'язки в раціональних числах: $x=\frac{x_1}{x_2}$, $y=\frac{y_1}{y_2}$, $z=\frac{z_1}{z_2}$, де x_1, x_2, y_1, y_2, z_1, z_2 — цілі числа, відмінні від нуля, і $(x_1;x_2)=1$, $(y_1;y_2)=1$, $(z_1;z_2)=1$.

Тоді рівняння (1) можна записати у вигляді: $\left(\frac{x_1}{x_2}\right)^n+\left(\frac{y_1}{y_2}\right)^n=\left(\frac{z_1}{z_2}\right)^n$, або $\frac{x_1^n}{x_2^n}+\frac{y_1^n}{y_2^n}=\frac{z_1^n}{z_2^n}$ або, помноживши ліву і праву частини цієї рівності на $x_2^n y_2^n z_2^n$, дістанемо:

$$x_1^n y_2^n z_2^n + y_1^n x_2^n z_2^n = z_1^n x_2^n y_2^n,$$

$$\text{або } (x_1 y_2 z_2)^n + (y_1 x_2 z_2)^n = (z_1 x_2 y_2)^n.$$

Позначимо $U=x_1y_2z_2$, $V=y_1x_2z_2$, $Q=z_1x_2y_2$, 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'язків рівняння (1) може служити прикладом для ствердження відомого філософського вислову: «Усе пізнається в порівнянні».

Шукаємо, знаходимо, порівнюємо, пізнаємо...

Так, завдяки очевидній простоті і послідовності логічних кроків дослідження на існування розв'язків нелінійних діофантових рівнянь (великої теореми Ферма) із використанням теорії порівнянь і їх властивостей, а також малої теореми Ферма, описаних вище, можна стверджувати, що Ферма володів алгоритмом розв'язання цієї задачі.

Розроблений мною алгоритм доведення великої теореми Ферма, можна назвати одним із кращих у сучасній теорії чисел, як самий простий, послідовний, логічний, зрозумілий.

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

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

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. : 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.

Будьте завжди проінформованими про актуальні освітні новини!

Найкращий спосіб своєчасно ознайомитись із сучасними розробками уроків та останніми тенденціями освіти — передплатити журнал «Математика в школах України»!

У журналі **«Математика в школах України»** ви знайдете орієнтовні календарні планування, актуальні новини МОНУ та безліч корисних практичних матеріалів, які одразу ж можна застосовувати на уроках!

Також до вашої уваги запропоновано інформативні вкладки.
• Повнокольорова вкладка з наочно-дидактичними матеріалами.
• «Фаховий сервер» — усе найнеобхідніше у практичній роботі вчителя щодня. Тематичні збірки матеріалів за актуальними напрямами.
• «Актуальні діалоги» — обговорюємо у формі «запитання-відповідь» усе, що цікавить педагогів незалежно від досвіду та предмета, що викладається.

Журнал можна замовити в одному з двох варіантів: паперовому та електронному. Зміст обох версій однаковий. Обирайте зручніший для себе!

Найвигідніші варіанти передплати

Назва	Індекс	6 міс.	12 міс.
«Математика в школах України» ПІЛЬГОВИЙ	95932	380,00	760,00
«Математика в школах України» ПІЛЬГОВИЙ ПЛЮС книжковий додаток	37055	500,00	1000,00
«Математика в школах України» (електронна версія) на сайті http://journal.osnova.com.ua	00003	294,00	588,00
«Математика в школах України» (електронна версія ПЛЮС книжковий додаток) на сайті http://journal.osnova.com.ua	00057	378,00	756,00

Скористайтеся програмою лояльності «120 балів»!

1. Відскануйте передплатні квитанції.
2. Надішліть їх на електронну адресу: pochta@osnova.com.ua
3. Отримайте на свій рахунок бали.
4. Оформіть наступну передплату зі знижкою.

1 зарахований бал = 10 коп.

Передплативши паперовий журнал, ви можете отримати його електронну версію безкоштовно!

Для цього надсилайте нам квитанцію про оплату та реєструйтеся на сайті http://journal.osnova.com.ua.

Після реєстрації у власному робочому кабінеті ви зможете завантажувати pdf-файли з потрібними статтями.

УВАГА!

Якщо Ви **хочете зекономити 20 %** від ціни, зазначеної за передплату друкованої версії, оформлюйте її за допомогою скретч-картки, за тел. 0-800-505-212 або на сайті http://journal.osnova.com.ua

Передплачуйте журнал просто зараз і забезпечуйте себе найкращими педагогічними матеріалами!

Передплату можна оформити:

за тел.: 0-800-505-212 на сайті: http://journal.osnova.com.ua;

у будь-якому відділенні «Укрпошти» або у регіонального представника вашого міста.

ОСНОВА видавнича група