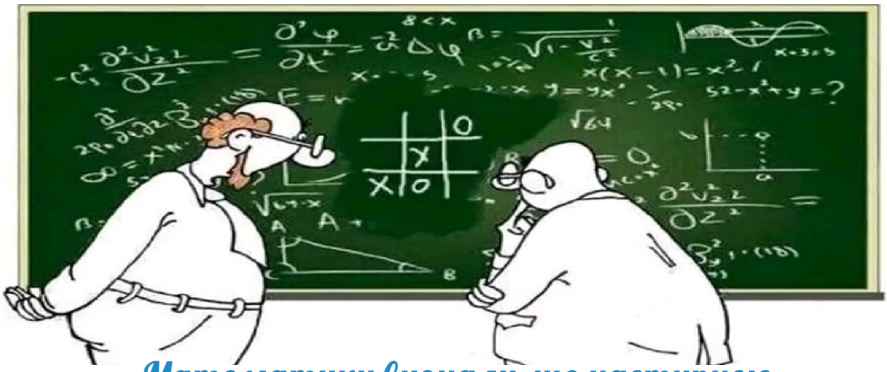
Маленькі кроки до Великої теореми Ферма: 358 років від примітки на полях до еліптичних кривих і модулярних форм.



Математики визнали, що наступною за складністю після Великої теореми Ферма стоїть формула нарахування пенсій)

***

До відомого професора, спеціаліста з теорії чисел, прийшов черговий дивний суб'єкт, який приніс чергове доведення Великої теореми Ферма. Зітхнувши, професор почав читати рукопис ферматиста.

— Але дозвольте, — вигукнув він через хвилину, — у вас тут на другій сторінці елементарна помилка!

Ображений ферматист зарозуміло відповів:

— Справа мислителів висувати глобальні ідеї, а ваша — виправляти дрібні неточності.

1.1 Велика теорема Ферма і маленькі кроки.

Уявіть собі тихий вечір 1637 року в Тулузі. Французький юрист та математик-любитель П'єр де Ферма гортає переклад давньогрецької "Арифметики" Діофанта (рис. 2 нижче). У цій античній праці було зібрано понад сотню задач на розв'язання визначених та невизначених рівнянь у цілих числах — тих самих, що сьогодні ми називаємо діофантовими.

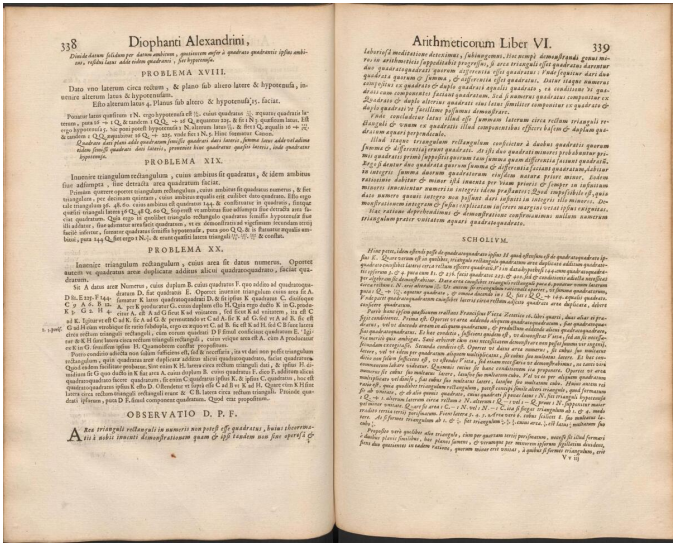
На вузьких полях сторінки, де ледь залишалося місце для короткої нотатки, Ферма поспіхом виводить латиною слова, що згодом стануть найвідомішим викликом в історії науки: *«Cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet»*.

Рис. 1. П'єр Ферма.

У перекладі це звучить як іронічне пророцтво: «Я знайшов по істині дивовижне доведення цього твердження, проте поля книги занадто вузькі, щоб його вмістити».

Так народилася Велика теорема Ферма: для будь-якого натурального $n > 2$ рівняння $x^n + y^n = z^n$ не має розв'язків у додатних цілих числах x, y, z. Проста формула, яка стала однією з найдовших математичних авантюр в історії – 358 років пошуків!

Імовірно, Ферма не лукавив: принаймні для випадку $n = 4$ він дійсно мав доведення, побудоване на методі «нескінченного спуску» — елегантному способі доведення від супротивного, який він сам і винайшов. Але чи мав він рішення для загального випадку?


338 Diophanti Alexandrini,

PROBLEMA XVIII.

PROBLEMA XIX.

PROBLEMA XX.

OBSERVATIO D. P. F.

Arithmeticorum Liber VI. 339

SCHOLIVM.

Рис. 2. Сторінки «Арифметики» Діофанта.

П'єр де Ферма пішов із життя у 1665 році, не залишивши нащадкам жодного рядка розгортки свого «дивовижного доведення» для довільного степеня. Відтоді теорема перетворилася на математичну легенду, на справжній «Священний Ґрааль» науки. Найкращі математики світу, немов середньовічні лицарі, один за одним кидалися в цей інтелектуальний бій, навіть не підозрюючи, що облога цієї фортеці затягнеться на три століття.

- **1738 рік**: Леонард Ейлер публікує перше повне доведення для випадку $n = 4$, систематизуючи та надаючи елегантності методу нескінченного спуску Ферма.
- **1770 рік**: Ейлер підкорює випадок $n = 3$, вперше застосувавши розклад на множники в кільці комплексних чисел (зараз відомих як цілі числа Ейзенштейна). Це стало фундаментальним кроком до виникнення абстрактної алгебри.
- **1825 рік**: Петер Діріхле та Адрієн-Марі Лежандр незалежно доводять теорему для $n = 5$, використовуючи розвиток теорії числових полів та узагальнюючи методи своїх попередників.

Кожен такий "маленький крок" – це цеглинка стіни Колізею Великої теореми Ферма, яка руйнується лише для окремих n, але залишається непохитною для всіх інших.

До середини XIX століття справедливість теореми була підтверджена лише для окремих випадків: $n = 3, 4, 5, 7$. Згодом, у XX столітті, комп'ютерні обчислення дозволять перевірити її для мільйонів значень, але загальне доведення продовжувало вислизати, як невловима тінь.

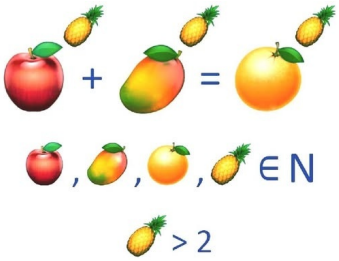


Рис. 3. Велика теорема Ферма у вигляді мема.

У березні 1847 року Габріель Ламе та Огюстен-Луї Коші оголосили про перемогу, представивши Паризькій академії свої варіанти доведення. Проте їхній тріумф був недовгим. Ернст Куммер продемонстрував, що їхні аргументи спираються на хибне припущення про однозначність факторизації в кільцях циклотомічних чисел. Ця поразка стала народженням нової ери: Куммер ввів поняття «ідеальних чисел», заклавши фундамент сучасної алгебраїчної теорії чисел.

Теорема перетворилася на справжнє «прокляття математики». Найвидатніші розуми століття – Ламе, Коші, Куммер, а згодом і Еміль Борель – витрачали роки життя, натикаючись на все ту ж непохитну стіну. Проте у 1908 році ситуація набула нового оберту: німецький промисловець

Пауль Вольфскель, чиє життя, за легендою, було врятоване завдяки цій задачі, заповів 100 000 марок тому, хто знайде доведення. Премія Вольфскеля перетворила академічну загадку на світову сенсацію, залучивши до її вирішення не лише вчених, а й тисячі аматорів.

- **Кінець XIX – початок XX століття**: Завдяки працям Карла Вейєрштрасса та Давида Гільберта формалізується теорія еліптичних кривих (рис. 4 нижче) – рівнянь виду $y^2 = x^3 + ax + b$. Ці криві описують складні геометричні об'єкти, які спочатку здавалися далекими від теореми Ферма, проте згодом стали ключовим інструментом для її розв'язання.

- **1950-ті роки**: Ясутака Таніяма та Горо Шімура висувають революційну гіпотезу (нині – теорема Таніями-Шімури-Вейля): кожна еліптична крива над раціональними числами є модулярною. Тобто вона пов'язана з модулярною формою – функцією, що володіє неймовірною симетрією під дією групи $SL(2, \mathbb{Z})$. Це стало мостом між алгебраїчною геометрією та комплексним аналізом.

- **1984–1986 роки**: Герхард Фрей пропонує ідею, що якщо рівняння Ферма має розв'язок, то йому відповідає надзвичайно дивна еліптична крива ("крива Фрея"): $y^2 = x(x-a^n)(x+b^n)$. Фрей припустив, що ця крива настільки аномальна, що вона не може бути модулярною.

- **1987 рік**: Кен Рібет доводить "Епсилон-гіпотезу" Серра, завершуючи логічну конструкцію: якщо гіпотеза Таніями-Шімури справджується для напівстабільних еліптичних кривих, то Велика теорема Ферма мусить бути істинною. Таким чином, доведення теореми Ферма звелося до доведення гіпотези про модулярність.

Ці кроки – уже навіть не по прямій лінії, а лабіринтом: від класичної геометрії до абстрактних груп та функцій!

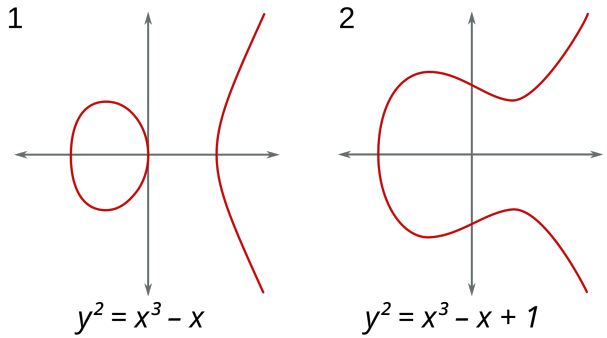


Рис. 4. Приклад графіків двох еліптичних кривих.

Модулярна форма – це зовсім інший тип об'єкта. Це складна функція, що має неймовірну симетрію. Уявіть собі візерунок, який можна зсувати, повертати та відображати, і при цьому він виглядатиме незмінним (рис. 5). Модулярна форма поводиться подібним чином, але в більш абстрактному просторі.

Ось основні її риси:

- Вона визначена на верхній комплексній півплощині, тобто множині чисел виду $z = x + iy$, де $x, y \in \mathbb{R}$ та $y > 0$. Цей простір зазвичай позначається як $\mathbb{H}$.

- Високий ступінь симетрії: Вона перетворюється певним, дуже передбачуваним чином під дією групи матриць, які відомі як спеціальна лінійна група $\mathrm{SL}(2, \mathbb{Z})$. Ця група складається з матриць 2x2 з цілочисельними елементами та визначником, рівним 1:

$$\mathrm{SL}(2, \mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

  Ці перетворення можна уявити як своєрідне «перетасовування» верхньої півплощини, але модулярна форма при цьому зберігає свою структуру.

- Як і в еліптичної кривої, у модулярної форми є свій «паспорт» – послідовність чисел, відома як коефіцієнти її ряду Фур'є. Для модулярної форми $f(z)$ її ряд Фур'є має вигляд:

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \quad \text{де } q = e^{2\pi i z}$$

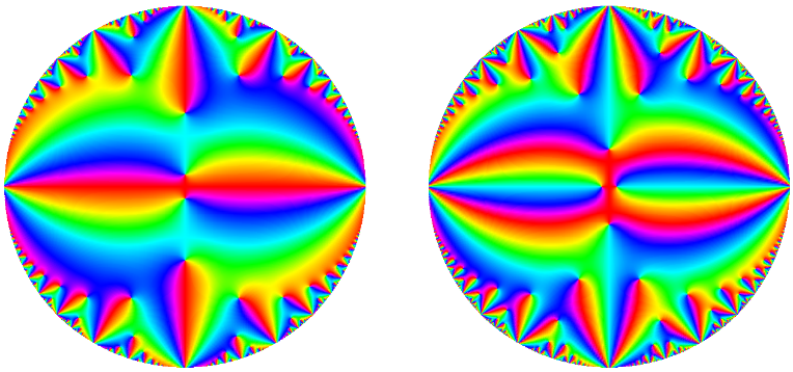


Рис. 5. Модель «квазімодулярної» форми.

У 1963 році десятирічний Ендрю Вайлс читає про Велику теорему Ферма в книзі Еріка Темпла Бела, а в 1986 році вирішує (спираючись на відкриття колег, які вказують шлях до розв'язку): "Це моя гора". Він ставить на паузу кар'єру в Прінстоні та усамітнюється з сім'єю. Сім років таємної роботи – 200 сторінок рукопису.

Стратегія Вайлса: довести, що напівстабільні еліптичні криві модулярні (частина гіпотези Таніями–Шімури). Якщо так, то крива Фрея не існує, отже, розв'язку Великої теореми Ферма немає.

- **23 червня 1993**: Вайлс оголошує доведення наприкінці серії з трьох лекцій під назвою "Модулярні форми, еліптичні криві та представлення Галуа" в Інституті математичних наук Ісаака Ньютона (Isaac Newton Institute for Mathematical Sciences) в Кембриджі, Англія. Світ затамував подих.
- **Серпень – вересень 1993**: Під час рецензування виявлено серйозну помилку. Вайлс у відчаї: "Я думав, що все зруйнувалося".
- **Вересень 1994**: Допомога Річарда Тейлора – колишнього студента Вайлса. Вони знаходять обхід через теорію Івасави та представлення Галуа.
- **1995**: Нове, виправлене доведення опубліковано в двох статтях у журналі *Annals of Mathematics*.

За свій науковий подвиг Ендрю Вайлс отримав численні нагороди. Оскільки на момент завершення доведення йому вже виповнилося 40 років (граничний вік для медалі Філдса), у 1998 році Міжнародний математичний союз вручив йому унікальну відзнаку — Срібну пластину Міжнародного конгресу математиків, що стала єдиним подібним винятком в історії. У 2000 році за свої заслуги він був удостоєний лицарського звання від королеви Англії.

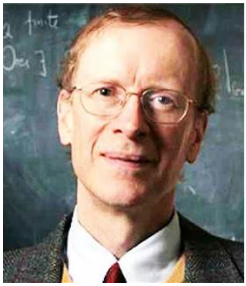


Рис. 6. Сер Ендрю Джон Вайлс.

Фінальну ж крапку в теорії модулярності було поставлено у 1999 році: Крістоф Брейль, Браян Конрад, Фред Даймонд та Річард Тейлор, спираючись на методи Вайлса, довели повну теорему модулярності для всіх еліптичних кривих над раціональними числами.

358 років – не просто час, а еволюція математики: від інтуїції Ферма до симфонії алгебри, геометрії та аналізу. Еліптичні криві тепер у криптографії Біткоїна, модулярні форми – у фізиці струн. Теорема Ферма нагадує: великі відкриття – це ланцюжок маленьких кроків, де помилки ведуть до великих просвітлень!

1.2 Метод нескінченного спуску Ферма для $n = 4$.

Метод нескінченного спуску – це техніка доведення від супротивного, винайдена П'єром де Ферма (хоча найдавніше застосування методу нескінченного спуску є в «Началах» Евкліда, згадайте наше доведення ірраціональності $\sqrt{2}$ в «П'яти постулатах геометрії Всесвіту Евкліда»).

Ідея полягає в наступному:

1. Припускаємо, що існує розв'язок (x, y, z) у додатних цілих числах.
2. Показуємо, що тоді повинен існувати інший розв'язок (x', y', z'), де $z' < z$.
3. Оскільки процес можна повторювати нескінченно, отримуємо нескінченну спадну послідовність додатних цілих чисел, що неможливо.
4. Тому початкове припущення хибне – розв'язків не існує.

Розглядаючи доведення того, що рівняння $x^4+y^4 = z^4$ не має розв'язків у додатних цілих числах, достатньо довести більш сильне твердження: рівняння $x^4 + y^4 = z^2$ не має розв'язків у додатних цілих числах. Якщо $x^4 + y^4 = z^4$, то для $(z^2)^2 = z^4$ це буде частковим випадком.

Рис. 7 демонструє два прямокутні трикутники, катети верхнього з яких дорівнюють катету та гіпотенузі нижнього.

Схожу на цю побудову ми розглянули для спіралі Феодора-Ейнштейна-Піфагора тільки без обмеження бути додатним цілим числом у статті «Піфагор - архітектор числового порядку».

Згідно з теоремою Піфагора, ця конфігурація описується системою рівнянь:

1. Для синього трикутника: $b^2+d^2 = c^2$
2. Для жовтого: $a^2 + d^2 = b^2$

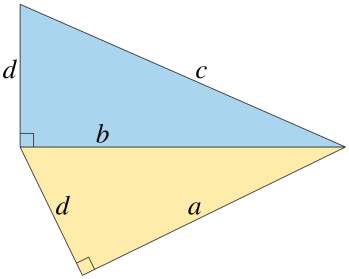


Рис. 7. Система з двох прямокутних трикутників зі спільним катетом.

З цих рівнянь випливає, що різниця між квадратами гіпотенуз та катетів є однаковою:

$$b^2 - a^2 = d^2 \quad \text{та} \quad c^2 - b^2 = d^2$$

Це означає, що числа a^2, b^2, c^2 утворюють **арифметичну прогресію** з різницею d^2, яка також є квадратом цілого числа.

Ферма довів, що не існує трьох квадратів цілих чисел, які б утворювали арифметичну прогресію, різниця якої сама є квадратом. Це твердження еквівалентне доведенню того, що площа прямокутного трикутника з цілими сторонами не може бути квадратом цілого числа, що в свою чергу є ключем до розв'язання рівняння $x^4 \pm y^4 = z^2$.

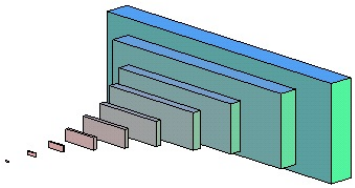


Рис. 8. Схематичне зображення методу нескінченного спуску.

Розглянемо метод Ферма детальніше.

Крок 1: Початкові припущення.

Припустимо, що існує розв'язок (a, b, c) рівняння

$$a^4 + b^4 = c^2$$

у додатних цілих числах. Можемо припустити, що $\gcd(a, b, c) = 1$ (інакше можна скоротити на спільний дільник). Також можемо припустити, що a і b не обидва парні.

Крок 2: Перетворення до піфагорового трійки. Перепишемо рівняння як:

$$(a^2)^2 + (b^2)^2 = c^2$$

Це піфагорова трійка з катетами a^2, b^2 та гіпотенузою c.

За теорією піфагорових трійок, якщо $\gcd(a^2, b^2) = 1$, то існують взаємно прості числа $m > n > 0$ протилежної парності такі, що:

$$a^2 = m^2 - n^2, \quad b^2 = 2mn, \quad c = m^2 + n^2$$

(або навпаки для a^2 і b^2).

Крок 3: Аналіз рівняння $b^2 = 2mn$. Оскільки $b^2 = 2mn$ і $\gcd(m, n) = 1$, то m і n не можуть бути обидва парними або обидва непарними. Отже, одне з них парне.

Нехай m парне, n непарне (або навпаки). Тоді $m = 2m_1$ для деякого цілого m_1.

Маємо:

$$b^2 = 2mn = 2 \cdot 2m_1 \cdot n = 4m_1 n$$

Отже:

$$\left(\frac{b}{2}\right)^2 = m_1 n$$

Оскільки $\gcd(m_1, n) = 1$ і їх добуток є повним квадратом, кожне з m_1 і n повинно бути повним квадратом:

$$m_1 = r^2, \quad n = s^2$$

для деяких додатних цілих r і s з $\gcd(r, s) = 1$.

Крок 4: Аналіз рівняння $a^2 = m^2 - n^2$.

Підставляємо $m = 2m_1 = 2r^2$ і $n = s^2$:

$$a^2 = (2r^2)^2 - (s^2)^2 = 4r^4 - s^4$$

Перепишемо:

$$a^2 + s^4 = 4r^4$$

Ділимо на 4:

$$\frac{a^2}{4} + \frac{s^4}{4} = r^4$$

Але оскільки a непарне (бо b парне), $a^2 \equiv 1 \pmod 4$, що суперечить діленню на 4.

Крок 5: Альтернативний випадок.

Розглянемо випадок, коли $a^2 = 2mn$ і $b^2 = m^2 - n^2$.

Тоді аналогічно отримуємо $m = p^2$, $n = q^2$, і:

$$b^2 = p^4 - q^4$$

Це дає:

$$q^4 + b^2 = p^4$$

або перепишемо як піфагорову трійку:

$$(q^2)^2 + b^2 = (p^2)^2$$

Знову застосовуючи параметризацію піфагорових трійок:

$$q^2 = u^2 - v^2, \quad b = 2uv, \quad p^2 = u^2 + v^2$$

де $\gcd(u, v) = 1$ та u, v протилежної парності.

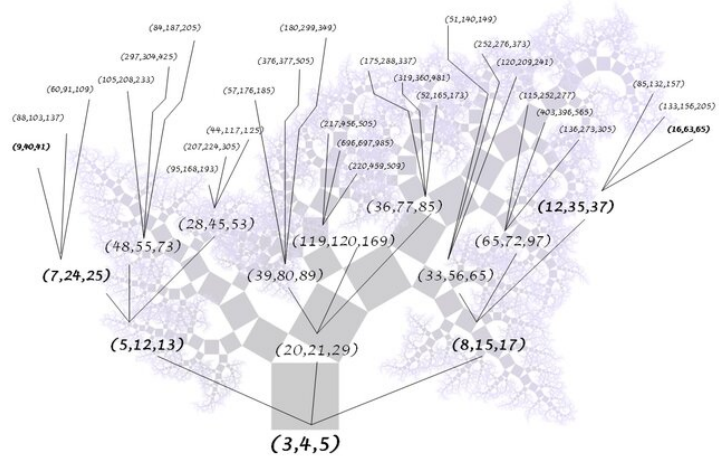


Рис. 9. Дерево взаємно простих піфагорових трійок.

Така послідовна параметризація розкриває внутрішню ієрархію піфагорових трійок. Кожен крок спуску фактично є рухом по дереву взаємно простих трійок, структуру якого наочно представлено на рис. 9.

Крок 6: Нескінченний спуск.

З $p^2 = u^2+v^2$ і $\gcd(u, v) = 1$ отримуємо, що u і v є повними квадратами (за властивостями сум квадратів):

$$u = \alpha^2, \quad v = \beta^2$$

Тоді:

$$p^2 = \alpha^4 + \beta^4$$

Але $p^2 < m^2 + n^2 = c$, оскільки $p < m$.

Отже, ми знайшли новий розв'язок рівняння $x^4 + y^4 = z^2$ з меншим значенням z, а саме (α, β, p) замість (a, b, c).

Цей процес можна повторювати нескінченно, отримуючи нескінченну спадну послідовність додатних цілих чисел:

$$c > p > p' > p'' > \dots$$

Це неможливо, оскільки не існує нескінченної спадної послідовності додатних цілих чисел.

Тому наше початкове припущення хибне, і рівняння $a^4 + b^4 = c^2$, а значить, і $x^4 + y^4 = z^4$ не має розв'язків у додатних цілих числах.

Рис. 10. Абстрактне зображення методу нескінченного спуску.

1.3 Елегантніший підхід Ейлера для $n = 4$.

Леонард Ейлер у 1738 році переформулював доведення П'єра де Ферма, зробивши його більш систематичним і зрозумілим (Рис. 11).

Його підхід базувався на тій же ідеї нескінченного спуску, але з кращою структурою.

Ключова лема Ейлера.

Якщо $x^2 + y^2 = z^2$ з $\gcd(x, y) = 1$ і x непарне, то існують взаємно прості числа $m > n > 0$ протилежної парності такі, що:

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2$$

Ейлер застосував цю лему послідовно двічі до рівняння $(a^2)^2 + (b^2)^2 = c^2$, що дозволило йому більш чітко відстежити структуру розв'язків.

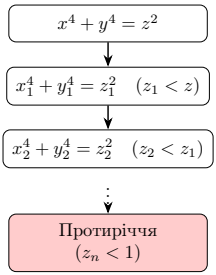


Рис. 11. Нескінченний спуск Ейлера.

Алгоритм Ейлера:

1. Розглядаємо $a^4 + b^4 = c^2$ як $(a^2)^2 + (b^2)^2 = c^2$
2. За лемою: $a^2 = m^2 - n^2$, $b^2 = 2mn$, $c = m^2 + n^2$
3. З $b^2 = 2mn$ випливає, що $m = 2u^2$, $n = v^2$ (оскільки $\gcd(m, n) = 1$)
4. Підставляємо в $a^2 = m^2 - n^2$:

$$a^2 = (2u^2)^2 - (v^2)^2 = 4u^4 - v^4$$

5. Це дає $v^4 + a^2 = 4u^4$, або еквівалентно:

$$v^4 + a^2 = (2u^2)^2$$

6. Знову застосовуємо лему до $(v^2)^2 + a^2 = (2u^2)^2$
7. Отримуємо новий розв'язок з меншим z

Ейлер систематизував доведення і показав, як можна використовувати параметризацію піфагорових трійок як стандартний інструмент.

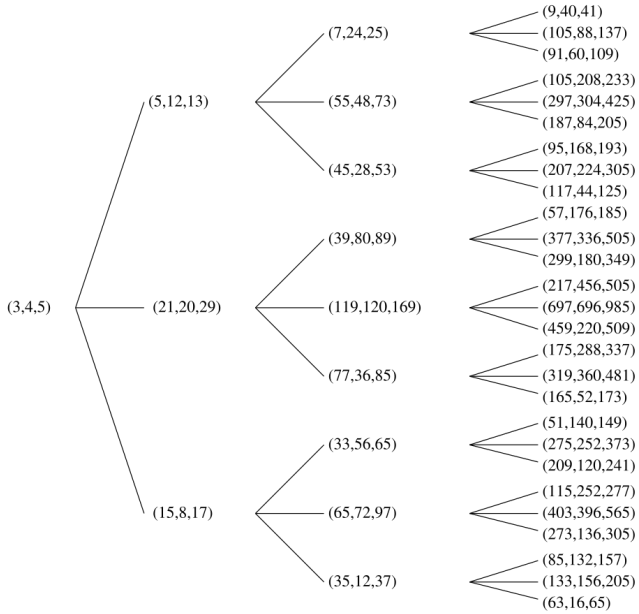


Рис. 12. Класичне дерево примітивних піфагорових трійок.

1.4 Випадок $n = 3$: комплексні числа та тріумф Ейлера (1770).

Для доведення випадку $x^3 + y^3 = z^3$ Ейлер використав революційну ідею – факторизацію в кільці цілих чисел $\mathbb{Z}[\omega]$, де $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$ – примітивний кубічний корінь з одиниці.

На рис. 13 нижче показані всі цілі числа решітки Ейзенштейна, також відомі як числа Ейлера (сірі точки) та виділено прості числа: червоні на осях та сині поза ними. Точки на зелених прямих відповідають натуральним простим числам виду $3k - 1$. Квадрат модуля всіх інших точок дає натуральне просте число. На відміну від звичайної цілочисельної прямої, ці числа утворюють гексагональну структуру на комплексній площині, що дозволяє розкласти суму кубів на три лінійні множники.

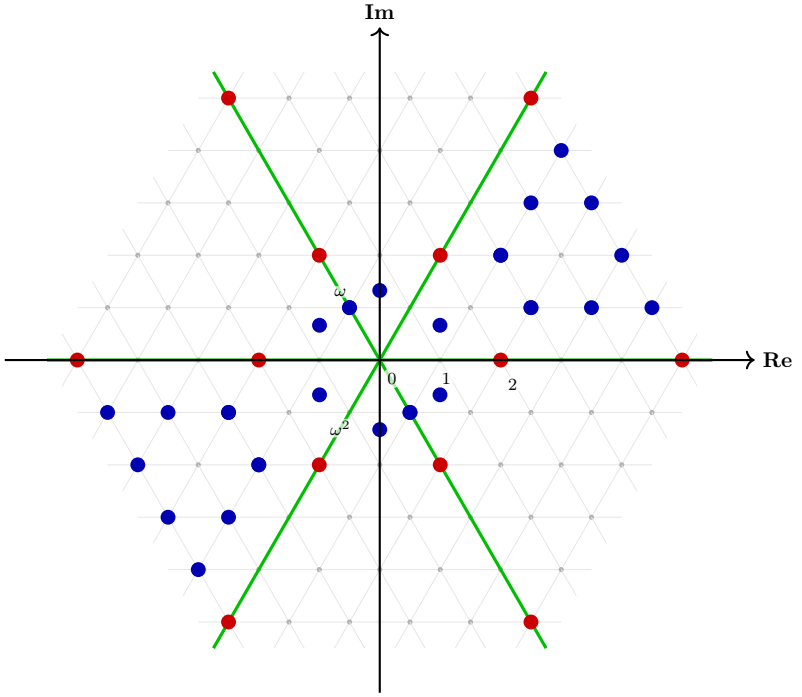


Рис. 13. Решітка чисел Ейзенштейна $\mathbb{Z}[\omega]$.

Число ω задовольняє рівностям:

$$\omega^3 = 1, \quad \omega^2 + \omega + 1 = 0$$

Кільце $\mathbb{Z}[\omega]$ складається з чисел виду $a + b\omega$, де $a, b \in \mathbb{Z}$.

Факторизація суми кубів.

Рівняння $x^3 + y^3 = z^3$ можна переписати через факторизацію:

$$x^3 + y^3 = (x + y)(x + \omega y)(x + \omega^2 y)$$

У своєму дослідженні Ейлер спирався на фундаментальну **властивість факторизації** кільця $\mathbb{Z}[\omega]$. Це означає, що будь-який його елемент розкладається на прості множники єдиним чином (з точністю до порядку та множення на одиниці кільця). Хоча пізніше Ернст Едуард Куммер встановив, що для складніших алгебраїчних розширень однозначність факторизації втрачається, для випадку $n = 3$ інтуїція Ейлера була цілком коректною.

Саме ця властивість дозволяє стверджувати: оскільки права частина рівняння $x^3 + y^3 = z^3$ є третім степенем, то за умови взаємної простоти x та y кожен із лінійних множників $(x + y)$, $(x + \omega y)$ та $(x + \omega^2 y)$ також має бути «майже» кубом. У математичному сенсі це означає, що кожна дужка дорівнює кубу деякого числа з $\mathbb{Z}[\omega]$, помноженому на один із шести **оборотних елементів**: $\{\pm 1, \pm\omega, \pm\omega^2\}$ (рис. 14). Ретельний аналіз усіх варіантів поєднання цих множників дозволив Ейлеру виявити суперечність і завершити доведення методом нескінченного спуску, продемонструвавши відсутність ненульових розв'язків для суми кубів.

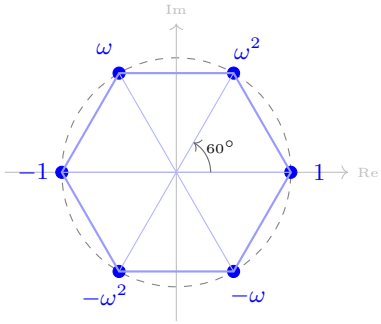


Рис. 14. Шість одиниць (оборотних елементів) кільця $\mathbb{Z}[\omega]$.

Схема доведення:

1. **Припущення**: Припускаємо, що існує розв'язок $x^3+y^3 = z^3$ у цілих взаємно простих числах.

2. **Факторизація**: Використовуємо комплексні числа для розкладу суми кубів у кільці $\mathbb{Z}[\omega]$:

$$(x + y)(x + \omega y)(x + \omega^2 y) = z^3$$

3. **Умова куба**: Оскільки множники попарно взаємно прості в $\mathbb{Z}[\omega]$, кожен із них (з точністю до одиниць) має бути кубом:

$$x + \omega y = (a + b\omega)^3$$

4. **Перехід до цілих параметрів**: Розкриття куба $(a + b\omega)^3$ та прирівнювання частин дозволяє виразити x та y через цілі числа a та b. Це веде до заміни $x + y = 2u$ та $x - y = 2v$.

5. **Аналіз структури**: Рівняння набуває вигляду $2u(u^2 + 3v^2) = z^3$. На основі властивостей $\mathbb{Z}[\omega]$ доводимо, що це можливо лише тоді, коли $u = a(a^2 - 3b^2)$.

6. **Виділення множників**: Підставляємо значення u і отримуємо, що число $2u$ повинно бути повним кубом:

$$2u = (2a) \cdot (a - 3b) \cdot (a + 3b) = \text{куб}$$

7. **Поява нових кубів**: Оскільки ці три множники взаємно прості, кожен із них окремо є кубом:

$$2a = A^3, \quad a + 3b = B^3, \quad a - 3b = C^3$$

8. **Нескінченний спуск**: Складання нових кубів $B^3 + C^3 = (a + 3b) + (a - 3b) = 2a = A^3$ дає нове рівняння того ж виду, але з меншими значеннями, що створює нескінченне спадання, неможливе для натуральних чисел (рис. 15).

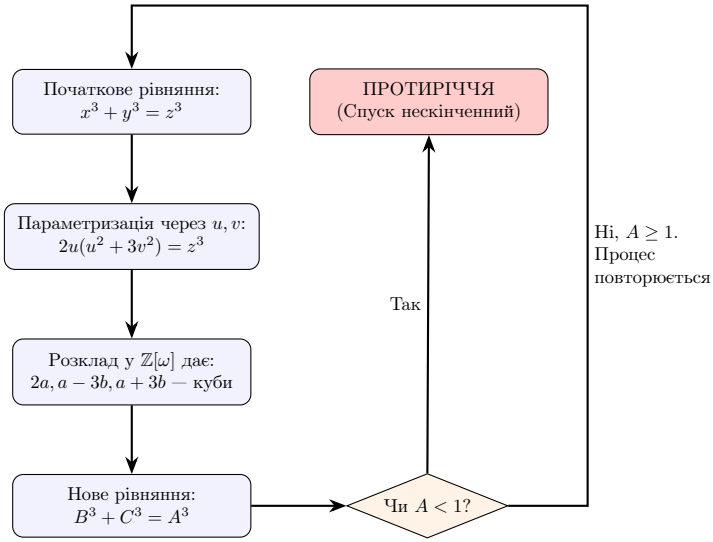


Рис. 15. Логічна схема методу нескінченного спуску Ейлера.

1.5 Випадок $n = 5$: Діріхле та Лежандр (1825).

Для випадку $x^5 + y^5 = z^5$ Петер Густав Лежен Діріхле та Адрієн-Марі Лежандр незалежно розробили доведення, яке поєднувало:

- Алгебраїчну теорію чисел (як у Ейлера),
- Геометричні властивості простих чисел,
- Квадратичні форми.

Кільце $\mathbb{Z}[\zeta_5]$.
Аналогічно до випадку $n = 3$, розглядається кільце цілих чисел $\mathbb{Z}[\zeta_5]$, де $\zeta_5 = e^{2\pi i/5}$ – примітивний корінь п'ятого степеня з одиниці.
Властивості ζ_5:

$$\zeta_5^5 = 1, \quad 1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$$

Мінімальний поліном: $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
Факторизація:
Рівняння $x^5 + y^5 = z^5$ факторизується як:

$$x^5 + y^5 = (x + y)(x + \zeta_5 y)(x + \zeta_5^2 y)(x + \zeta_5^3 y)(x + \zeta_5^4 y)$$

На відміну від $\mathbb{Z}[\omega]$, кільце $\mathbb{Z}[\zeta_5]$ завжди має однозначну факторизацію.
Діріхле та Лежандр використовували попередні версії ідей, які пізніше Ернст Куммер формалізував як теорію ідеальних чисел. На рис. 16 нижче позначені п'ять симетричних векторів, які є основою для факторизації рівняння $x^5 + y^5 = z^5$ у кільці цілих чисел $\mathbb{Z}[\zeta_5]$

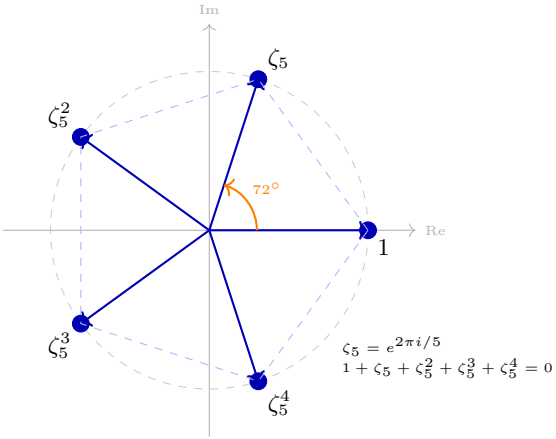


Рис. 16. Корені п'ятого степеня з одиниці в комплексній площині.

Ключові інструменти

1. **Норма елемента:** Для $\alpha = a_0 + a_1\zeta_5 + \ldots + a_4\zeta_5^4$ норма:

$$N(\alpha) = \alpha \cdot \bar{\alpha} \cdot \overline{\overline{\alpha}} \cdot \ldots$$

(добуток усіх спряжених).

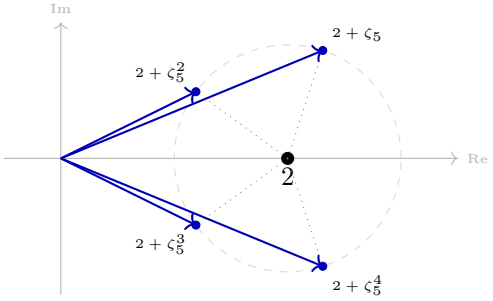
2. **Одиниці в кільці:** Елементи з нормою ± 1. Для $\mathbb{Z}[\zeta_5]$ існує нескінченно багато одиниць, що ускладнює аналіз.

3. **Квадратичні лишки:** Діріхле використав теорію квадратичних лишків по модулю 5:

$$1^2 \equiv 1 \pmod 5, \quad 2^2 \equiv 4 \pmod 5, \quad 3^2 \equiv 4 \pmod 5, \quad 4^2 \equiv 1 \pmod 5$$

Схема доведення Діріхле:

1. Розглядається $x^5 + y^5 = z^5$ з умовою $5 \nmid xyz$ (випадок I Куммера);
2. Факторизація в $\mathbb{Z}[\zeta_5]$ дає п'ять множників;
3. Показується, що ці множники попарно взаємно прості;
4. Кожен множник повинен бути п'ятим степенем (з точністю до одиниць);
5. Аналіз одиниць кільця приводить до суперечності;
6. Використовується нескінченний спуск через норми елементів.



$$N(2+\zeta_5) = |2+\zeta_5| \cdot |2+\zeta_5^2| \cdot |2+\zeta_5^3| \cdot |2+\zeta_5^4| = 31$$

Рис. 17. Геометрична інтерпретація норми елемента $2 + \zeta_5$.

На рис. 17 показано геометричну інтерпретацію норми елемента $2+\zeta_5$. Чотири сині вектори представляють спряжені множники в $\mathbb{Z}[\zeta_5]$. Добуток їхніх значень (норм) дорівнює цілому числу 31.

Нехай $\alpha = 2 + \zeta_5$. Обчислимо норму:

$$N(\alpha) = (2+\zeta_5)(2+\zeta_5^2)(2+\zeta_5^3)(2+\zeta_5^4) = \prod_{k=1}^{4}(2+\zeta_5^k)$$

Використовуючи $\prod_{k=1}^{4}(x+\zeta_5^k) = x^4+x^3+x^2+x+1$ при $x=2$:

$$N(2+\zeta_5) = 2^4+2^3+2^2+2+1 = 16+8+4+2+1 = 31$$

Оскільки 31 – просте число, $2+\zeta_5$ є простим елементом у $\mathbb{Z}[\zeta_5]$.

Лежандр додав геометричний підхід через квадратичні форми:

$$Q(x,y) = ax^2 + bxy + cy^2$$

Він показав, що якщо $x^5 + y^5 = z^5$ має розв'язок, то існують певні квадратичні форми з неможливими властивостями (наприклад, негативним дискримінантом там, де він має бути додатним).

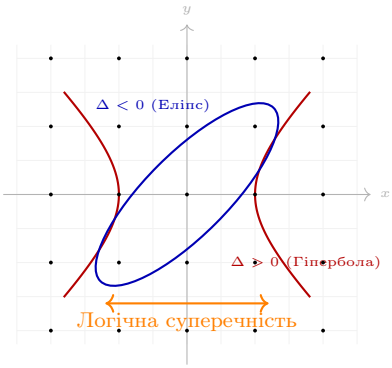


Рис. 18. Геометрична ілюстрація суперечності за Лежандром.

Перетин еліпса (обмеженість) та гіперболи (нескінченність) візуалізує (рис. 18) конфлікт арифметичних умов, що виникає при припущенні існування розв'язку рівняння Ферма для $n = 5$.

Доведення для $n = 5$ стало поворотним моментом: воно показало необхідність розвитку абстрактної алгебри, привело до теорії алгебраїчних чисел, мотивувало Куммера створити теорію ідеалів, підкреслило різницю між простими числами та простими елементами в кільцях.

Випадки для $n = 4$ (Ферма/Ейлер), $n = 3$ (Ейлер) та $n = 5$ (Діріхле і Лежандр) продемонстрували еволюцію математичних методів:

1. $n = 4$: елементарні методи, піфагорові трійки, нескінченний спуск,
2. $n = 3$: комплексні числа, факторизація в алгебраїчних кільцях,
3. $n = 5$: поєднання алгебри, геометрії, теорії ідеалів.

Кожен наступний випадок вимагав глибших математичних теорій, і це передбачало, що загальне доведення потребуватиме революційних ідей – що і сталося з роботою Ендрю Вайлса в 1995 році.

1.6 Підхід Ламе-Коші, ідеали Куммера та проблема однозначної факторизації.

У 1847 році французький математик Габрієль Ламе оголосив на засіданні Паризької академії наук, що він знайшов повне доведення Великої теореми Ферма. Його підхід базувався на факторизації рівняння $x^n + y^n = z^n$ у кільці циклотомічних цілих чисел (комплексні числа особливого виду).

Огюстен-Луї Коші незалежно працював над схожим методом. Однак незабаром Ернст Куммер вказав на критичну помилку в їхніх міркуваннях: припущення про однозначну факторизацію в циклотомічних кільцях.

На рис. 19 показано структуру коренів 7-го степеня з одиниці. Велика кількість внутрішніх зв'язків (діагоналей) символізує складну структуру одиниць циклотомічного кільця. Для $p < 23$ однозначність факторизації зберігається, проте на $p = 23$ виникає «арифметична аномалія» (число класів $h = 3$), яка спростувала підхід Ламе.

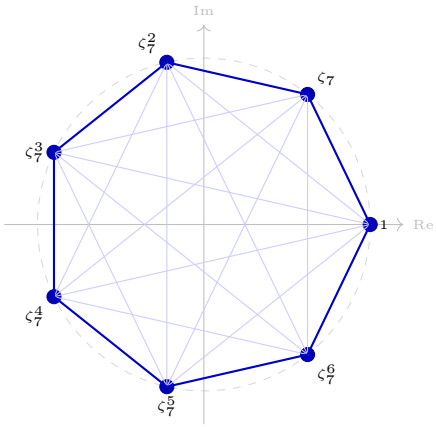


Рис. 19. Структура коренів 7-го степеня з одиниці.

Метод Ламе: факторизація в циклотомічному полі. Розглянемо рівняння Ферма для простого показника p:

$$x^p + y^p = z^p$$

Нехай $\zeta = e^{2\pi i/p}$ — примітивний корінь p-го степеня з одиниці. Тоді рівняння можна факторизувати в кільці $\mathbb{Z}[\zeta]$:

$$z^p = x^p + y^p = \prod_{j=0}^{p-1} (x + \zeta^j y)$$

Ламе припустив, що множники $(x + \zeta^j y)$ попарно взаємно прості в $\mathbb{Z}[\zeta]$, і якщо їхній добуток є p-м степенем, то кожен з них (з точністю до одиниць) також має бути p-м степенем:

$$x + \zeta^j y = u_j \cdot \alpha_j^p$$

де u_j — одиниці кільця $\mathbb{Z}[\zeta]$, а $\alpha_j \in \mathbb{Z}[\zeta]$.

З умови $x + \zeta^j y = \alpha_j^p$ можна отримати систему рівнянь. Ламе намагався показати, що ця система призводить до суперечності, використовуючи властивості одиниць та норм у $\mathbb{Z}[\zeta]$.

Формально, якщо $\alpha = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$, то:

$$\alpha^p = (a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1})^p$$

Порівнюючи коефіцієнти при різних степенях ζ, Ламе сподівався отримати суперечність.

Заперечення Куммера та проблема однозначної факторизації.

Жозеф Ліувілль одразу ж висловив сумніви щодо доведення Ламе, зауваживши, що метод залежить від унікальності факторизації в $\mathbb{Z}[\zeta]$. Куммер підтвердив це побоювання, показавши контрприклад:

У кільці $\mathbb{Z}[\zeta_{23}]$, де $\zeta_{23} = e^{2\pi i/23}$, однозначна факторизація на прості елементи не виконується.

Щоб зрозуміти як це відбувається в кільці $\mathbb{Z}[\zeta_{23}]$, розглянемо простіший приклад у кільці $\mathbb{Z}[\sqrt{-5}]$:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Тут числа 2, 3, $(1+\sqrt{-5})$, $(1-\sqrt{-5})$ — усі є незвідними, але не простими елементами.

Куммер ввів поняття **класового числа** h циклотомічного поля $\mathbb{Q}(\zeta_p)$, яке вимірює "ступінь неунікальності" факторизації:

Класове число h — це порядок групи класів ідеалів кільця цілих алгебраїчних чисел. Якщо $h = 1$, то виконується однозначна факторизація (область однозначності позначена пунктиром на рис. 20 нижче).

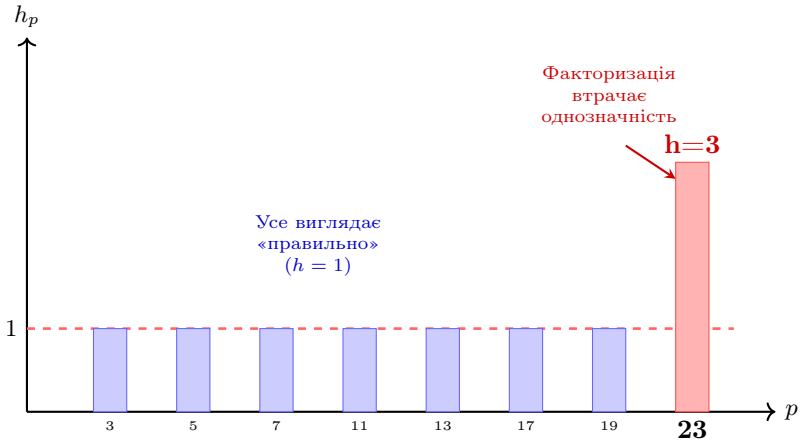


Рис. 20. Діаграма класових чисел h_p для циклотомічних полів.

Виправлення Куммера: теорія ідеалів

Щоб врятувати підхід Ламе, Куммер розробив революційну теорію **ідеальних чисел** (пізніше названих просто **ідеалами** Дедекіндом).

Ідеал I кільця R — це підмножина $I \subseteq R$ така, що:

1. I — адитивна підгрупа,
2. Для будь-яких $a \in I$ та $r \in R$: $ra \in I$.

У кільці цілих $\mathbb{Z}[\zeta_p]$ кожен ненульовий ідеал однозначно (з точністю до порядку) розкладається на добуток простих ідеалів.

Це означає, що хоча елементи можуть не мати однозначної факторизації, ідеали завжди факторизуються єдиним чином.

Просте число p називається **регулярним**, якщо p не ділить класове число h поля $\mathbb{Q}(\zeta_p)$. В іншому випадку p називається **нерегулярним**.

- Регулярні прості: $3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$
- Перше нерегулярне просте: 37 (позначено на рис. 21)
- Інші нерегулярні: $59, 67, 101, 103, 131, 149, \ldots$

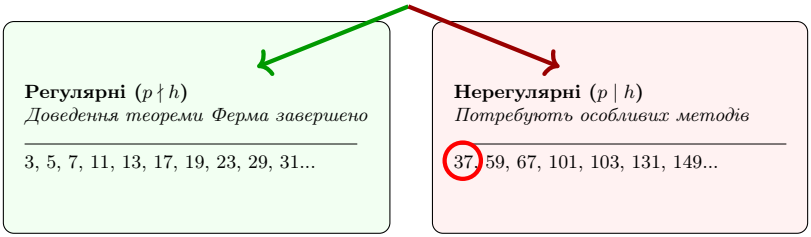


Рис. 21. Класифікація простих чисел за Куммером.

Теорема Куммера, 1850

Якщо p — регулярне просте число, то рівняння Ферма

$$x^p + y^p = z^p$$

не має розв'язків у ненульових цілих числах.

Крок 1: Факторизація ідеалів

Розглянемо ідеали, породжені множниками:

$$I_j = (x + \zeta^j y) \subseteq \mathbb{Z}[\zeta_p]$$

Крок 2: Взаємна простота ідеалів

Ідеали I_j є попарно взаємно простими, тобто $I_j + I_k = \mathbb{Z}[\zeta_p]$ при $j \neq k$.

Крок 3: Використання однозначної факторизації ідеалів

Оскільки $I_0 \cdot I_1 \cdots I_{p-1} = (z^p)$ та ідеали є взаємно простими, кожен I_j має бути p-м степенем ідеалу:

$$I_j = J_j^p$$

Крок 4: Перехід до головних ідеалів

Для регулярних простих, використовуючи властивості групи класів, можна показати, що J_j — головний ідеал:

$$J_j = (\alpha_j)$$

Отже:

$$(x + \zeta^j y) = u_j(\alpha_j)^p$$

де u_j — одиниця.

Крок 5: Аналіз одиниць та суперечність

Куммер використав глибокі властивості одиниць у $\mathbb{Z}[\zeta_p]$ (включаючи теорему Діріхле про одиниці) і показав, що система рівнянь, отримана з умови $(x + \zeta^j y) = u_j \alpha_j^p$, призводить до суперечності.

Для нерегулярних простих Куммер розробив додаткові критерії. Пізніше було доведено, що ВТФ (велика теорема Ферма) є правильною і для багатьох нерегулярних простих за виконання певних умов.

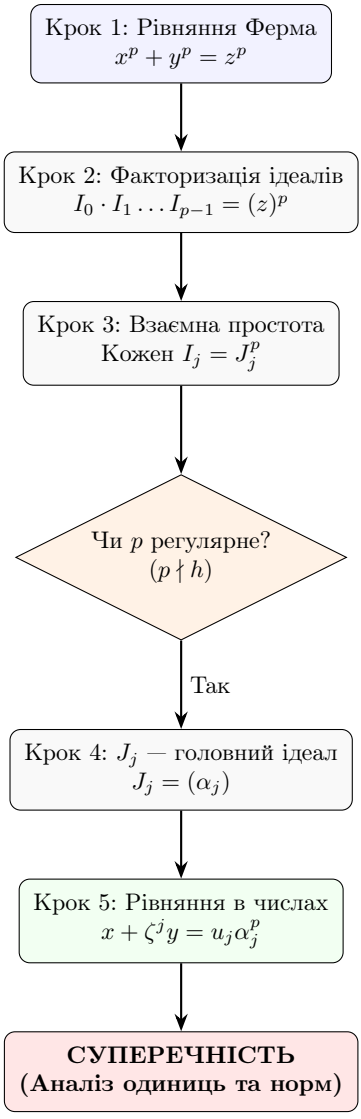


Рис. 22. Логічний алгоритм доведення Куммера.

До кінця XIX століття було доведено, що ВТФ є правильною для всіх простих $p < 100$, завдяки роботам Куммера та його послідовників. Ці ідеї лягли в основу сучасної алгебраїчної теорії чисел і, зрештою, призвели до доведення Ендрю Вайлса через модулярні форми та еліптичні криві.

1.7 Мала теорема Ферма.

1.7.1 Формулювання

Якщо p — просте число, а a — ціле число, що не ділиться на p, то $a^{p-1} - 1$ ділиться на p.

Мовою теорії конгруенцій: a^{p-1} є конгруентним 1 за простим модулем p. Формальний запис:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Наприклад, якщо $a = 2$, $p = 7$, то $2^6 = 64$, і $64 - 1 = 63 = 7 \cdot 9$.

Мала теорема Ферма є окремим випадком теореми Ейлера, яка, в свою чергу, є окремим випадком теореми Кармайкла і теореми Лагранжа для скінченних циклічних груп. Теорему висловив без доведення П'єр Ферма у 1640 році; перше доведення дали Леонард Ейлер та Готфрід Вільгельм Лейбніц.

Одним із найбільш елегантних способів доведення Малої теореми Ферма є комбінаторний підхід (рис. 23). Уявіть, що ми виготовляємо намисто, яке складається з p намистин і маємо у розпорядженні a різних кольорів.

Якщо ми розкладемо намистини в ряд, то загальна кількість можливих розфарбувань становитиме a^p. Серед них рівно a варіантів будуть одноколірними (наприклад, усі намистини тільки сині або тільки червоні). Якщо ми виключимо ці випадки, у нас залишиться $a^p - a$ багатоколірних комбінацій.

Оскільки це намисто, його можна повертати по колу. Для будь-якого багатоколірного намиста існує рівно p можливих поворотів. Оскільки p є простим числом, усі ці p поворотів виглядатимуть по-різному (вони не можуть повторитися раніше, ніж ми зробимо повне коло). Таким чином, всі багатоколірні розфарбування можна згрупувати в набори по p штук у кожному. Це безпосередньо доводить, що число $a^p - a$ обов'язково ділиться на p.

Рис. 23. Комбінаторне доведення Малої теореми Ферма через розфарбовування намиста.

1.7.2 Альтернативне формулювання

Наступне формулювання відрізняється відсутністю вимоги, щоб число a не ділилося на p: Якщо p — просте число, а a — будь-яке ціле число, то a^p є конгруентним a за модулем p, тобто

$$a^p \equiv a \pmod{p}.$$

Наприклад, якщо $a = 7$, $p = 5$, то $7^5 = 16807 = 5 \cdot 3361 + 2$, і $7 = 5 \cdot 1 + 2$.

Легко показати, що це формулювання зводиться до початкового. Так, якщо a ділиться на p, то $a \equiv 0 \pmod{p}$ і $a^p \equiv 0 \pmod{p}$, тобто $a^p \equiv a \pmod{p}$. Якщо ж a не ділиться на p, то вираз $a^p \equiv a \pmod{p}$ є еквівалентним виразу $a^{p-1} \equiv 1 \pmod{p}$.

Як основне, так і альтернативне формулювання можуть бути використані для перевірки, чи є задане число простим; однак основне формулювання є надійнішим у тому сенсі, що відсіює більше складених чисел. Приклад: перевіримо, чи є 6 простим числом. Нехай $a = 4$. В альтернативному формулюванні отримуємо $4^6 = 4096 = 682 \times 6 + 4$, а це є конгруентним 4 (mod 6). Тобто число 6 не відсіяно, його простота не спростована. Якщо ж повернутися до оригінальної теореми: $a^{p-1} \equiv 1 \pmod{p}$, то $4^{6-1} = 4^5 = 1024 = 170 \times 6 + 4$, а це не є конгруентним 1 (mod 6), як мало б бути у випадку, якщо p — просте число. Таким чином, основне формулювання є більш ефективним при відсіюванні складених чисел (рис. 24).

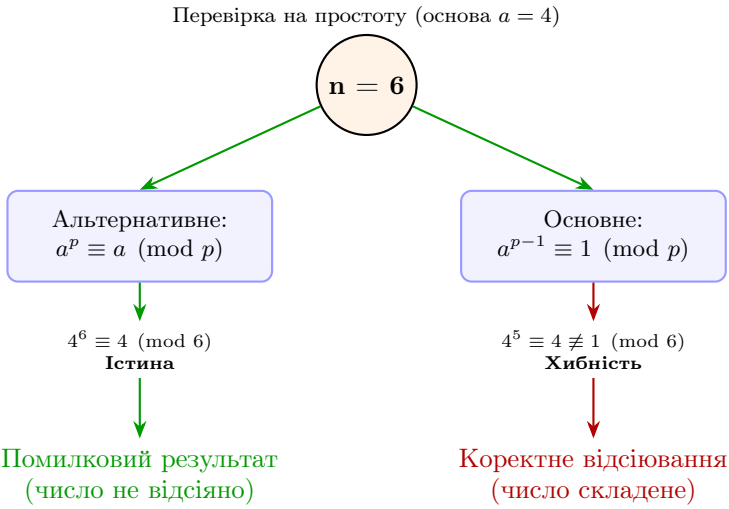


Рис. 24. Порівняння ефективності формулювань Малої теореми Ферма.

1.7.3 Доведення за допомогою індукції

Доведемо, що для будь-якого простого p та цілого невід'ємного a, $a^p - a$ ділиться на p. Доведення проведемо методом математичної індукції за a.

База. Для $a = 0$, $a^p - a = 0^p - 0 = 0$, що ділиться на p.

Перехід. Припустимо, що твердження є правильним для $a = k$, тобто $k^p - k$ ділиться на p. Доведемо, що воно є правильним для $a = k + 1$.

Розглянемо вираз:

$$(k+1)^p - (k+1) = k^p + \sum_{l=1}^{p-1} \binom{p}{l} k^l + 1 - k - 1 = (k^p - k) + \sum_{l=1}^{p-1} \binom{p}{l} k^l.$$

За припущенням індукції, $k^p - k$ ділиться на p. Розглянемо суму, що залишилася:

$$\sum_{l=1}^{p-1} \binom{p}{l} k^l.$$

Кожен доданок у сумі містить множник $\binom{p}{l} = \frac{p!}{l!(p-l)!}$. Для $1 \le l \le p-1$, чисельник цього дробу $(p!)$ ділиться на p, оскільки p — просте число, а знаменник $l!(p-l)!$ є взаємно простим з p, оскільки l та $p-l$ менші за p. Отже, $\binom{p}{l}$ ділиться на p для всіх $1 \le l \le p-1$. Таким чином, кожен доданок $k^l\binom{p}{l}$ ділиться на p, і вся сума $\sum_{l=1}^{p-1} k^l\binom{p}{l}$ також ділиться на p.

Отже, вираз $(k+1)^p - (k+1)$ є сумою двох доданків, кожен з яких ділиться на p, а отже, і сам вираз ділиться на p (рис. 25). Кожен доданок $\binom{p}{l}k^l$ в індукційному переході ділиться на p, оскільки для простого p усі центральні числа ряду є його кратними.

Випадок від'ємних a.

Для від'ємних a та непарних p, теорему легко довести, підставляючи $b = -a$. Тоді $b^p \equiv b \pmod p$, а оскільки p непарне, $(-a)^p = -a^p \equiv -a \pmod p$, що еквівалентно $a^p \equiv a \pmod p$.

Для від'ємних a та $p = 2$, істинність теореми випливає з:

$$a^2 - a = a(a-1).$$

Оскільки a або $a-1$ є парним, добуток $a(a-1)$ ділиться на 2.

Таким чином, для будь-якого цілого a та простого p, $a^p - a$ ділиться на p.

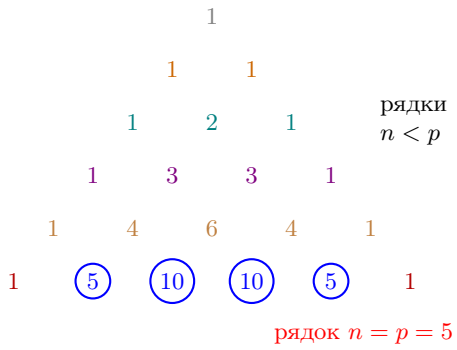


Рис. 25. Властивість біноміальних коефіцієнтів у трикутнику Паскаля.

1.7.4 Доведення за допомогою модульної арифметики

Лема. Для будь-якого простого числа p та цілого числа k, не кратного p, добутки k та чисел $1, 2, 3, \ldots, p-1$ при діленні на p в залишку дають ті ж самі числа $1, 2, 3, \ldots, p-1$, можливо, записані в деякому іншому порядку.

Доведення леми. Розглянемо числа $k, 2k, 3k, \ldots, (p-1)k$. Покажемо, що їхні залишки за модулем p утворюють перестановку чисел $1, 2, 3, \ldots, p-1$. Припустимо, що для деяких i, j (де $1 \le i, j \le p-1$, $i \ne j$) виконується $ik \equiv jk \pmod{p}$. Тоді p ділить $(i-j)k$. Оскільки p — просте число, а k не ділиться на p, то p має ділити $i-j$. Але оскільки $1 \le i, j \le p-1$, то $|i-j| < p$, і єдина можливість — це $i = j$. Таким чином, усі залишки $k, 2k, \ldots, (p-1)k$ за модулем p є різними і належать множині $\{1, 2, \ldots, p-1\}$. Отже, вони утворюють перестановку чисел $1, 2, 3, \ldots, p-1$.

На рис. 26 наведено візуалізацію цієї леми: множення на $a = 3$ за модулем $p = 7$ створює перестановку (бієкцію) множини залишків. Оскільки набори чисел в обох рядах однакові, їхні добутки також рівні.

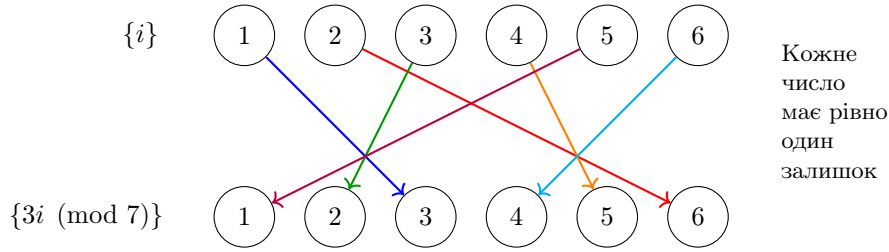


Рис. 26. Візуалізація леми щодо залишків.

Доведення теореми. Оскільки згідно з лемою залишки від ділення чисел $a, 2a, 3a, \ldots, (p-1)a$ за модулем p — це з точністю до перестановки числа $1, 2, 3, \ldots, p-1$, то добуток цих чисел задовольняє конгруенцію:

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Або, в скороченій формі:

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Оскільки $(p-1)!$ є взаємно простим з p (оскільки всі множники $1, 2, \ldots, p-1$ не діляться на p), то можна скоротити $(p-1)!$ з обох боків конгруенції. В результаті отримуємо:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Це і є твердження малої теореми Ферма.

1.8 Числа Ферма: звичайні, прості та узагальнені.

Числа Ферма — це числа виду $F_n = 2^{2^n} + 1$, де $n \geqslant 0$ (послідовність A000215 в OEIS). При $n \in \{0, 1, 2, 3, 4\}$ числа Ферма є простими і дорівнюють $3, 5, 17, 257, 65\,537$.

Поки що інших простих чисел Ферма не виявлено, і невідомо, чи існують вони для інших n, чи всі інші числа Ферма складені.

Вивчення чисел такого виду розпочав Ферма, який висунув гіпотезу, що всі вони є простими. Однак ця гіпотеза була спростована Ейлером у 1732 році, коли той знайшов розклад числа F_5 на прості співмножники:

$$F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

За часів Ферма вважалося правильним твердження, що якщо $2^n \equiv 2 \pmod{n}$, то n — просте. Хоча це твердження виявилося хибним (був знайдений контрприклад: $n = 341$), на думку Тадеуша Банахевича, саме це могло спонукати Ферма висунути свою гіпотезу, оскільки твердження $2^{F_n} \equiv 2 \pmod{F_n}$ є правильним при всіх n.

На січень 2025 року відомо 5 простих чисел Ферма — при $n \in \{0, 1, 2, 3, 4\}$:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3;$$
$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5;$$
$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17;$$
$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257;$$
$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65\,537.$$

Існування інших простих чисел Ферма є відкритою проблемою. Відомо, що F_n є складеними при $5 \leqslant n \leqslant 32$ (рис. 27).

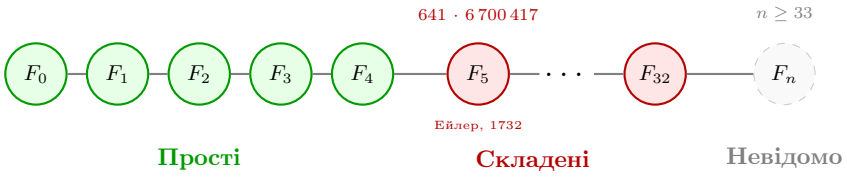


Рис. 27. Поточний статус чисел Ферма.

Властивості чисел Ферма.

- Правильний n-кутник (рис. 28) можна побудувати за допомогою циркуля та лінійки тоді і тільки тоді, коли $n = 2^r \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k$ ($r = 0, 1, 2, \ldots$), де $p_1, \ldots, p_k$ — різні прості числа Ферма (***теорема Гаусса–Ванцеля***).

- Серед чисел виду 2^n+1 простими можуть бути тільки числа Ферма (тобто число n зобов'язане бути степенем 2). Дійсно, якщо n має непарний дільник $d>1$ і $n/d=m$, то

$$2^n+1=(2^m+1)(1-2^m+2^{2m}-\cdots+2^{n-m}),$$

і тому 2^n+1 не є простим.

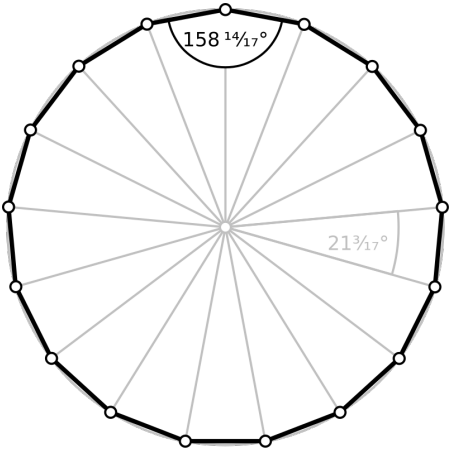


Рис. 28. Правильний сімнадцятикутник.

- Для перевірки чисел Ферма на простоту найефективнішим є **тест Пепіна**. Однак через подвійну експоненціальну швидкість зростання цих чисел тест вимагає колосальних обчислювальних ресурсів. На сьогодні він був успішно завершений лише для невеликої кількості чисел (зокрема до $n=24$ та деяких більших значень), причому у випадках F_{14}, F_{20}, F_{22} та F_{24} він став першим підтвердженням їхньої складеності за відсутності відомих дільників.

- Десятковий запис чисел Ферма, більших за 5, закінчується на 17, 37, 57 або 97.

- Кожен дільник числа F_n при $n>2$ має вигляд $k\cdot 2^{n+2}+1$ (Ейлер, Люка, 1878).

- Числа Ферма зростають дуже швидко: 9-те число більше за гугол, а 334-те число більше за гуголплекс.

Загалом станом на січень 2025 року знайдено 374 простих дільники чисел Ферма. Для 329 чисел Ферма доведено, що вони є складеними, при цьому для двох з них (F_{20} і F_{24}) досі невідомо жодного дільника. Кілька нових дільників чисел Ферма знаходять щороку.

Нижче наведено розклад чисел Ферма на прості співмножники, при $n \in \{5, 6, 7, 8, 9\}$:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417;$$

$$F_6 = 2^{2^6} + 1 = 2^{64} + 1 = 18\,446\,744\,073\,709\,551\,617 = 274\,177 \cdot 67\,280\,421\,310\,721;$$

$$F_7 = 2^{2^7} + 1 = 2^{128} + 1 = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,457 =$$
$$= 59\,649\,589\,127\,497\,217 \cdot 5\,704\,689\,200\,685\,129\,054\,721;$$

$$F_8 = 2^{2^8} + 1 = 2^{256} + 1 = 115\,792\,089\,237\,316\,195\,423\,570\,985\,008\,687\,907\,853\,269$$
$$984\,665\,640\,564\,039\,457\,584\,007\,913\,129\,639\,937 = 1\,238\,926\,361\,552\,897 \cdot$$
$$\cdot 93\,461\,639\,715\,357\,977\,769\,163\,558\,199\,606\,896\,584\,051\,237\,541\,638\,188\,580\,280\,321;$$

$$F_9 = 2^{2^9} + 1 = 2^{512} + 1 = 13\,407\,807\,929\,942\,597\,099\,574\,024\,998\,205\,846\,127\,479\,365$$
$$820\,592\,393\,377\,723\,561\,443\,721\,764\,030\,073\,546\,976\,801\,874\,298\,166\,903\,427\,690\,031$$
$$858\,186\,486\,050\,853\,753\,882\,811\,946\,569\,946\,433\,649\,006\,084\,097 = 2\,424\,833 \cdot$$
$$\cdot 7\,455\,602\,825\,647\,884\,208\,337\,395\,736\,200\,454\,918\,783\,366\,342\,657 \cdot$$
$$\cdot 741\,640\,062\,627\,530\,801\,524\,787\,141\,901\,937\,474\,059\,940\,781\,097\,519\,023\,905\,821$$
$$316\,144\,415\,759\,504\,705\,008\,092\,818\,711\,693\,940\,737.$$

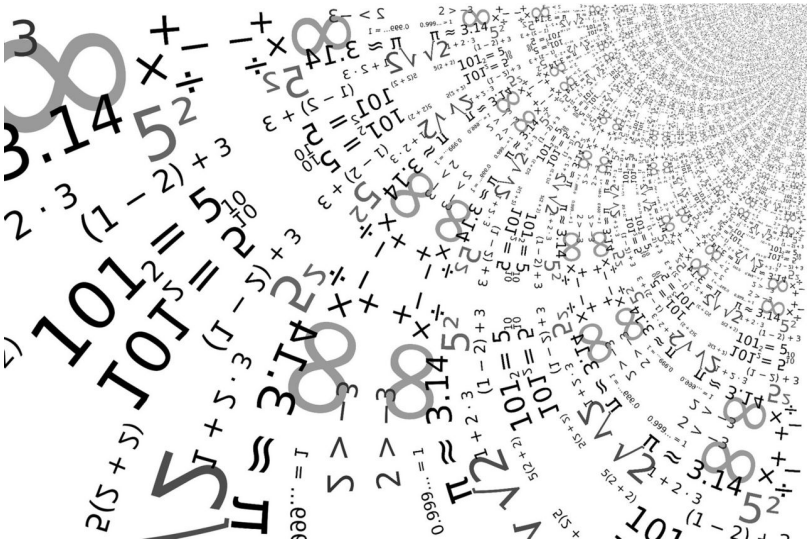


Рис. 29. Символічне зображення «числового вибуху» та складності структури великих чисел Ферма.

Узагальнені числа Ферма.

Числа виду $a^{2^n} + b^{2^n}$, де a, b — будь-які взаємно прості числа, такі що $a > b > 0$, називаються узагальненими числами Ферма. Непарне просте p є узагальненим числом Ферма тоді і тільки тоді, коли $p \equiv 1 \pmod 4$. (Ми розглядаємо лише випадок, коли $n > 0$, тому $3 = 2^{2^0} + 1$ не є контрприкладом.)

За аналогією зі звичайними числами Ферма прийнято записувати узагальнені числа Ферма виду $a^{2^n} + 1$ як $F_n(a)$. У цьому позначенні, наприклад, число 100 000 001 буде записано як $F_3(10)$. Далі ми обмежимося простими числами цього виду, $a^{2^n} + 1$, такі прості числа називаються "прості Ферма за основою a". Звісно, ці прості числа існують лише тоді, коли a є парним.

Через легкість доведення їхньої простоти, в останні роки узагальнені прості числа Ферма стали темою для досліджень у галузі теорії чисел. Багато з найбільших відомих сьогодні простих чисел є узагальненими простими числами Ферма.

Узагальнені числа Ферма можуть бути простими тільки для парних a, оскільки якщо a непарне, то кожне узагальнене число Ферма буде ділитися на 2. Найменше просте число $F_n(a)$ з $n > 4$ — це $F_5(30)$ або $30^{32} + 1$.

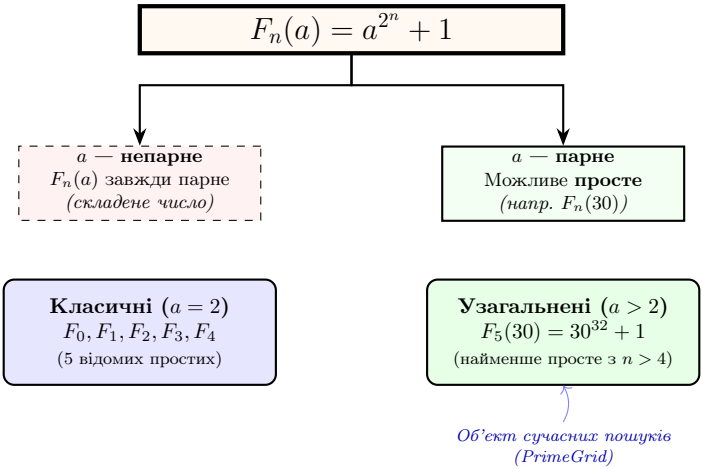


Рис. 30. Класифікація узагальнених чисел Ферма.

1.9 Принцип Ферма.

Принцип Ферма (принцип найменшого часу Ферма) — постулат у геометричній оптиці, згідно з яким світло обирає з множини шляхів між двома точками той шлях, який вимагатиме найменшого часу. Тобто промінь

світла, як показано на рис. 31, рухається з початкової точки в кінцеву точку шляхом, що мінімізує час руху (або, що те ж саме, мінімізує оптичну довжину шляху).

Принцип Ферма математично виражається умовою стаціонарності оптичної довжини шляху:

$$\delta \int_A^B n(s)\, ds = 0$$

де $n(s)$ — показник заломлення середовища в точці на шляху променя, ds — елемент довжини шляху, A та B — початкова і кінцева точки.

Час проходження світла визначається як:

$$t = \frac{1}{c} \int_A^B n(s)\, ds$$

де c — швидкість світла у вакуумі.

Цей принцип, застосований ще в I ст. Героном Александрійським для відбиття світла, в загальному вигляді був сформульований П'єром Ферма у 1662 році як найзагальніший закон геометричної оптики. У різноманітних конкретних випадках з нього випливали вже відомі закони: прямолінійність променя світла в однорідному середовищі, закони відбиття та заломлення світла на межі двох прозорих середовищ.

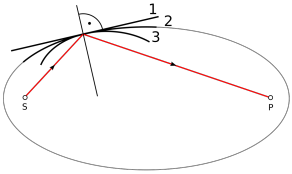


Рис. 31. Принцип Ферма на прикладі еліптичних поверхонь.

Принцип Ферма є граничним випадком принципу Гюйгенса–Френеля у хвильовій оптиці для випадку зникаюче малої довжини хвилі світла і є одним з екстремальних принципів у фізиці.

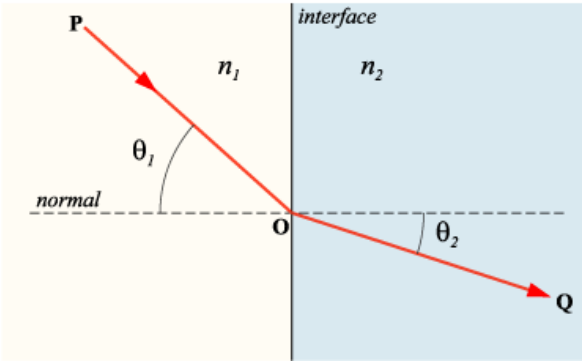


Рис. 32. Пояснення закону Снелла за допомогою принципу Ферма.

1.10 Ферма та народження теорії ймовірностей.

У 1654 році П'єр де Ферма та Блез Паскаль розпочали листування, яке сьогодні вважається моментом народження сучасної теорії ймовірностей. Приводом стала «задача про розподіл ставок» (Problem of Points), яку поставив кавалер де Мере: як чесно розділити призовий фонд у грі, перерваній до її завершення?

Ферма запропонував революційний комбінаторний підхід. Замість того, щоб аналізувати лише минулі ходи, він запропонував розглянути всі можливі варіанти завершення гри.

Приклад: Гравці грають до 3-х перемог. Рахунок 2:1 на користь A. Отже, A треба $r = 1$ перемога, а B треба $s = 2$ перемоги. Максимальна кількість партій $N = 1 + 2 - 1 = 2$. Можливі наслідки двох партій: AA, AB, BA, BB. Гравець A виграє у випадках AA, AB, BA (3 варіанти). Гравець B виграє лише у випадку BB (1 варіант). Розподіл ставок: 3:1 на користь A (рис. 33).

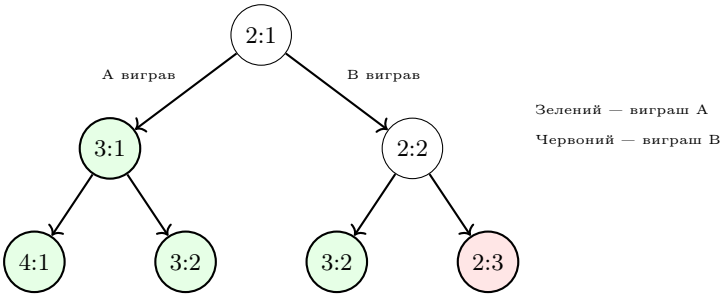


Рис. 33. Дерево можливих фіналів для гри до 3-х перемог (рахунок 2:1).

Математичне формулювання методу Ферма: Нехай гравцеві A бракує r перемог до виграшу, а гравцеві B — s перемог. Тоді гра обов'язково завершиться щонайбільше за $N = r + s - 1$ партій. Ферма припустив, що навіть якщо гра завершиться раніше, ми можемо умовно «дограти» всі N партій, щоб зробити всі результати рівноймовірними.

Загальна кількість можливих фіналів гри становить 2^N. Гравець A виграє призовий фонд, якщо у цих додаткових партіях він здобуде принаймні r перемог. Кількість таких сприятливих випадків обчислюється як сума біноміальних коефіцієнтів:

$$W_A = \sum_{k=r}^{N} \binom{N}{k}$$

Відповідно, ймовірність перемоги гравця A (а отже, і його частка в став-

ках) становить:

$$P(A) = \frac{1}{2^N} \sum_{k=r}^{N} \binom{N}{k}$$

Цей підхід Ферма фактично ввів у науку поняття **математичного сподівання** та став основою для сучасної теорії прийняття рішень у ситуаціях з невизначеністю.

1.11 Факторизація методом Ферма та теорема про суму квадратів.

Метод факторизації Ферма. Ферма запропонував алгоритм розкладу великих чисел на множники, що базується на представленні непарного числа N як різниці двох квадратів:

$$N = x^2 - y^2 = (x - y)(x + y)$$

Алгоритм шукає таке ціле x, щоб значення $x^2 - N$ було повним квадратом y^2. Хоча за часів Ферма це було суто теоретичною розвагою, сьогодні його ідеї лежать в основі найпотужніших методів зламу сучасних криптосистем (наприклад, алгоритму RSA), таких як метод квадратичного решета.

На рис. 34 показано геометричну модель факторизації Ферма. Ми шукаємо такий квадрат x^2, щоб різниця між ним і числом N була ідеальним квадратом y^2. Це дозволяє миттєво знайти дільники через формулу різниці квадратів.

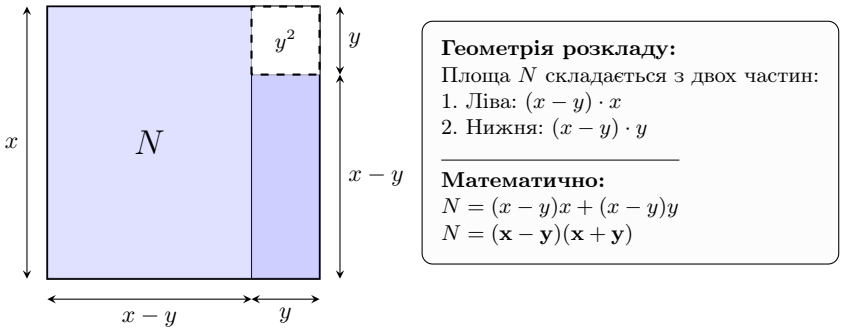


Рис. 34. Геометрична інтерпретація методу Ферма.

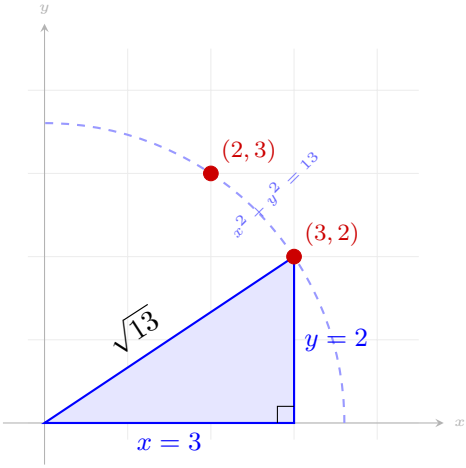
Ефективність цього методу критично залежить від того, наскільки близькими один до одного є множники числа N. Якщо $N = p \cdot q$, а значення p і q знаходяться неподалік від $\sqrt{N}$, то алгоритм знаходить розв'язок за мінімальну кількість ітерацій. Саме через цю особливість у сучасній

криптографії при генерації ключів для алгоритму RSA висувається сувора вимога: прості числа p та q повинні бути різної довжини або суттєво відрізнятися за значенням. В іншому випадку «цифрова фортеця» RSA може бути зруйнована методом Ферма за лічені секунди, що робить теорію XVII століття надзвичайно актуальною для сучасних фахівців із кібербезпеки.

Теорема про суму двох квадратів. Одним із найкрасивіших результатів Ферма є твердження, що будь-яке просте число p вигляду $4k+1$ може бути представлене як сума двох квадратів цілих чисел, причому єдиним способом. Наприклад:

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2$$

Це твердження (відоме як «Різдвяна теорема») було вперше надіслано в листі до Мерсенна у 1640 році і стало відправною точкою для створення теорії квадратичних форм та продемонструвало глибинний зв'язок між структурою простих чисел та їхнім геометричним представленням.



Геометрія теореми:
Число $p = 13$ $(4k + 1)$ — це квадрат відстані від $(0, 0)$ до точки решітки (x, y).

Арифметика:
$13 = 3^2 + 2^2$
$13 = (3 + 2i)(3 - 2i)$

Рис. 35. Геометрична інтерпретація суми двох квадратів.

З точки зору сучасної алгебри, цей результат означає, що прості числа вигляду $4k + 1$ «розщеплюються» у кільці цілих гауссових чисел $\mathbb{Z}[i]$ на добуток двох комплексних множників: $p = (x + iy)(x - iy)$. Теорема стала першим кроком до розуміння того, як звичайні прості числа поводяться в більш широких числових системах. Сьогодні її узагальнення лежать в основі теорії ідеалів та дозволяють класифікувати цілі числа, які можна представити як суму трьох, чотирьох або більшої кількості квадратів, що має глибоке застосування в теорії кодування та криптографії.

1.12 Спадщина Ферма: гіпотези Ейлера та Біла і ABC-гіпотеза.

Гіпотеза Ейлера. У 1769 році Леонард Ейлер запропонував узагальнення Великої теореми Ферма, припустивши, що для того, аби сума n-них степенів дорівнювала n-ному степеню, необхідно щонайменше n доданків. Наприклад, для $n = 4$: $x^4 + y^4 + z^4 = w^4$. Проте у 1986 році Ноам Елкіс знайшов контрприклад, довівши, що інтуїція може підвести навіть генія:

$$268444^4 + 15365639^4 + 18796760^4 = 20615673^4$$

Ця гіпотеза здавалася настільки природною, що ніхто не піддавав її сумніву понад два століття. Проте історія її спростування стала уроком смирення для теоретиків. Перша «тріщина» в теорії з'явилася ще у 1966 році, коли Ландер та Паркін за допомогою одного з перших суперкомп'ютерів знайшли контрприклад для $n = 5$, де сума лише чотирьох п'ятих степенів дала п'ятий степінь ($27^5 + 84^5 + 110^5 + 133^5 = 144^5$). Спростування Елкіса для $n = 4$ у 1986 році було ще більш вражаючим, оскільки він не просто знайшов числа, а використав теорію еліптичних кривих, щоб довести існування нескінченної кількості таких виняткiв. Це відкриття остаточно підтвердило, що Велика теорема Ферма є скоріше унікальною арифметичною аномалією, ніж загальним правилом для вищих степенів.

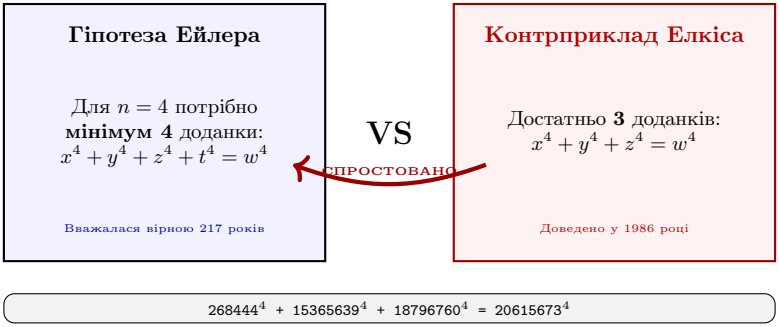


Рис. 36. Гіпотеза Ейлера.

Гіпотеза Біла: «Спадкоємець ВТФ на мільйон доларів». Сформульована у 1993 році техаським банкіром та математиком-самоуком Ендрю Білом, ця гіпотеза є прямим узагальненням Великої теореми Ферма. Вона стверджує:

> *Якщо $A^x + B^y = C^z$, де A, B, C, x, y, z — додатні цілі числа і $x, y, z > 2$, то числа A, B, C повинні мати спільний простий дільник.*

Головна відмінність від задачі Ферма полягає в тому, що показники степенів x, y, z можуть бути різними. Якщо хоча б один із показників дорівнює 2, знайти розв'язки без спільного дільника легко (наприклад, $7^2 + 2^5 = 3^4$, де $\gcd(7, 2, 3) = 1$). Але як тільки всі три степені стають більшими за 2, простір розв'язків різко «стискається».

Сьогодні гіпотеза перевірена за допомогою комп'ютерів для величезних значень чисел, але загальне доведення досі не знайдене. Щоб підігріти інтерес наукового світу, Ендрю Біл заснував премію, сума якої зросла з 5 000 доларів у 1997 році до **1 000 000 доларів** сьогодні. Гіпотеза Біла є значно «сильнішою» за теорему Ферма: якщо вона буде доведена, Велика теорема Ферма автоматично стане її простим наслідком для випадку $x = y = z = n$.

ABC-гіпотеза. Це одна з найглибших проблем сучасної теорії чисел, яка досліджує фундаментальний зв'язок між операціями додавання та множення. Вона стверджує, що якщо три числа пов'язані простим співвідношенням додавання, то вони не можуть одночасно складатися з великої кількості малих простих множників.

Для формулювання гіпотези вводиться поняття **радикалу числа** — добутку всіх його *різних* простих дільників:

$$\mathrm{rad}(n) = \prod_{p \mid n} p$$

Наприклад: $\mathrm{rad}(18) = \mathrm{rad}(2 \cdot 3^2) = 2 \cdot 3 = 6$.

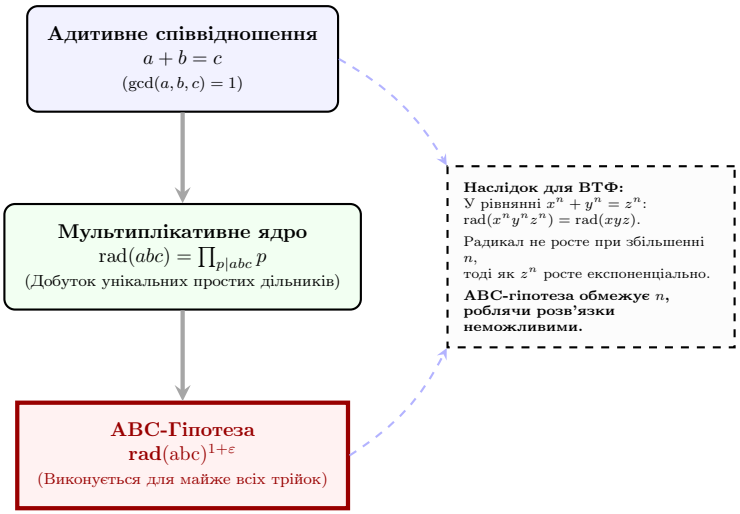


Рис. 37. Логічна структура ABC-гіпотези.

Формулювання гіпотези: Для будь-якого $\varepsilon > 0$ існує лише скінченна кількість трійок взаємно простих додатних цілих чисел (a, b, c), таких що $a + b = c$ та виконується умова:

$$c > \mathrm{rad}(abc)^{1+\varepsilon}$$

Чому це важливо? ABC-гіпотеза фактично стверджує, що «мультиплікативна складність» (радикал) суми трьох чисел зазвичай не набагато менша за сам*е* найбільше число c.

Зв'язок із Великою теоремою Ферма: Якби ABC-гіпотеза була доведена, Велика теорема Ферма стала б її майже миттєвим наслідком. Розглянемо рівняння $x^n + y^n = z^n$. Для великих n значення z^n зростало б значно швидше за радикал добутку $\mathrm{rad}(x^n y^n z^n) = \mathrm{rad}(xyz)$, що прямо суперечило б ABC-гіпотезі. Таким чином, гіпотеза встановлює жорстку межу на те, наскільки «степеневими» можуть бути компоненти суми $a + b = c$. Це підкреслює, що ідеї Ферма, народжені 400 років тому, продовжують формувати передній край сучасної науки.

Покоління, що прийшло за Ферма, втратило інтерес до грецької математики, за винятком хіба що інтересу до робіт Евкліда, праці якого до самого XX століття були прикладом строгості та краси в геометрії, а його *«Начала»* — найбільш часто видавана книга після Біблії.

Зі смертю Ферма у 1665 році грецька математика вже змінилася на сучасну. Після нього жоден великий математик не ставив собі за мету відновити традиції античності.

Рис. 38. Поштова марка Чехії 2000 року, присвячена ВТФ.