П. М. Орлов

Великая теорема Ферма

Арифметическое решение

Платон мне друг,
но истина дороже
Аристотель

URSS

П. М. Орлов

ВЕЛИКАЯ ТЕОРЕМА ФЕРМА

Арифметическое решение

URSS
МОСКВА

ББК 22.131г

Орлов Петр Макарович

Великая теорема Ферма: Арифметическое решение. — М.: Книжный дом «ЛИБРОКОМ», 2009. — 32 с. (Relata Refero.)

Размышления над решением равенства $A^n = X^n + Y^n$ в целых числах всегда выступали для автора в качестве своеобразного отдыха и вдохновения, поскольку были свободным полетом мысли. В научной литературе приходилось читать об алгебраическом доказательстве большой теоремы Ферма. Но это доказательство всегда было оторвано от теоремы Пифагора — «родной сестры» теоремы Ферма. Автору всегда хотелось найти общее решение равенства $A^n = X^n + Y^n$ в целых числах, где теорема Пифагора и большая теорема Ферма решались бы по единой методике. И такое арифметическое решение найти удалось.

Работа предназначается специалистам-математикам, преподавателям и студентам физико-математических вузов, а также любителям математики.

Издательство «Книжный дом "ЛИБРОКОМ"».
117312, Москва, пр-т Шестидесятилетия Октября, 9.
Формат 60×90/16. Печ. л. 2. Зак. № 2014.

Отпечатано в ООО «ЛЕНАНД»
117312, Москва, пр-т Шестидесятилетия Октября, 11А, стр. 11.

ISBN 978-5-397-00303-2

6502 ID 83310
9 785397 003032

Оглавление

От издательства

Эта книга продолжает серию «Relata Refero» (дословный перевод — рассказываю рассказанное).

Под этим грифом издательство предоставляет трибуну авторам, чтобы высказать публично новые идеи в науке, обосновать новую точку зрения, донести до общества новую интерпретацию известных экспериментальных данных, etc.

В споре разных точек зрения только решение Великого судьи — Времени — может стать решающим и окончательным. Сам же процесс поиска Истины хорошо характеризуется известным высказыванием Аристотеля, вынесенным на обложку настоящей серии: авторитет учителя не должен довлеть над учеником и препятствовать поиску новых путей.

Мы надеемся, что публикуемые в этой серии тексты внесут, несмотря на свое отклонение от установившихся канонов, свой вклад в познание Истины.

О чем книга?

В ней решена задача: «Подобрать три целых числа A, X и Y таких, чтобы выполнялось равенство

$$A^n = X^n + Y^n$$

при $n \geqslant 2$». Задача решена при $n = 2$, $n = 4$ и $n = p$, где p — простое нечетное число. Для решения задачи была разработана новая арифметическая методика из десяти теорем, фундаментом которых является основная теорема арифметики натуральных чисел. По этой методике интенсивно используются числа попарно взаимно простые и числа попарно делящиеся на одни и те же простые делители.

Благодаря разработанной методике и удачной постановке задачи, при каждом показателе степени $2, 4$ и p удалось найти общее решение, где числа X, Y и A выражены через число

$$C = X + Y - A$$

и его взаимно простые делители E_x и E_y. Для всех показателей степени *общее решение имеет одну форму, в которой решения отличаются величиной параметра, роль которого выполняет показатель степени.* По общему решению были сделаны соответствующие выводы.

Для равенства

$$A^2 = X^2 + Y^2$$

найдено новое решение в целых числах. Доказано, что равенства

$$A^4 = X^4 + Y^4 \quad \text{и} \quad A^p = X^p + Y^p$$

не могут иметь решения в целых числах. Поэтому все равенства

$$A^n = X^n + Y^n,$$

где n делится на 4 или на простое нечетное число p, не могут иметь решения в целых числах.

Постановка задачи

Задача. Подобрать три целых числа A, X и Y — таких, чтобы выполнялось равенство:

$$A^n = X^n + Y^n \quad \text{при } n \geqslant 2. \tag{1}$$

В равенстве (1) все три числа должны быть целыми числами одновременно. Задача объединяет целочисленную часть теоремы Пифагора и большую теорему Ферма. Поскольку эта задача арифметическая, и она тесно связана с основной теоремой арифметики натуральных чисел, то для решения задачи разработана новая арифметическая методика, состоящая из десяти теорем.

В решение задачи введем числа B и C, где:

$$B = X + Y, \tag{2}$$

$$C = X + Y - A. \tag{3}$$

Число B может быть представлено несколькими парами $(X+Y)$, а число C вообще может быть представлено неограниченным количеством троек

$$(X + Y - A).$$

Поэтому числа B и C слабо связаны с показателем степени n. Из этих соображений числа B и C надо считать заданными, а их особенности надо выяснять в ходе решения задачи.

Если B и C будут заданы, то число A из равенства (1) найдется сразу:

$$A = B - C. \tag{4}$$

Для чисел X и Y найдем другие зависимости через подстановки:

$$A = B - C, \quad X = X, \qquad Y = B - C, \tag{5}$$

$$A = B - C, \quad X = B - Y, \quad Y = Y. \tag{6}$$

Тогда получим:

$$(B - C)^n = X^n + (B - X)^n, \tag{7}$$

$$(B - C)^n = (B - Y)^n + Y^n. \tag{8}$$

Трудно воспринимаемое равенство (1) заменено на два равенства, которые подобны между собой и значительно проще равенства (1). Начальные условия, при которых решается задача:

а) при попарно взаимно простых A, X и Y,

б) при показателях степени $n = 2$, $n = 4$ и $n = p$, где p — простое число,

в) при условии, что одно из чисел A, X или Y может делиться на показатель степени n,

г) при предположении (допущении), что при каждом показателе степени n обязательно есть тройка целых чисел A, X и Y, которая обеспечивает равенство $A^n = X^n + Y^n$.

Решив задачу при этих условиях, потом можно будет сделать выводы и обобщения на всю область целых чисел и на все целые показатели степени n.

Следствие из условия (а). *В этом случае в равенстве* (1) *обязательно будут два числа нечетных и одно четное. Тогда число*

$$C = X + Y - A$$

всегда будет четным числом, делящимся на 2. *Так как числа* X *и* Y *взаимно простые, то в равенстве*

$$B = X + Y$$

числа B, X *и* Y *попарно взаимно простые.*

Следствие из условия (б). *В этом случае* (7) *и* (8) *надо решать в виде:*

$$X^2 = (X - C) \cdot (2B - (X + C)), \tag{9}$$

$$Y^2 = 2 \cdot (Y - C) \cdot \left(B - \frac{1}{2} \cdot (Y + C)\right), \tag{10}$$

$$X^4 = (X - C) \cdot M_x, \tag{11}$$

$$Y^4 = 4 \cdot (Y - C) \cdot M_y, \tag{12}$$

$$C^p = p \cdot B \cdot (X - C) \cdot M'_x, \tag{13}$$

$$C^p = p \cdot B \cdot (Y - C) \cdot M'_y. \tag{14}$$

Следствие из условия (в). *Так как в равенстве* (1) *числа* X *и* Y *занимают равноправные положения по отношению к показателю степени, то принято решение, что* X *не будет делиться на показатель* n, *а число* Y *может делиться на* n, *но может и не делиться.*

Следствия из условия (г):

- *правые части равенств* (9) *и* (10) *должны быть полными квадратами,*
- *правые части равенств* (11) *и* (12) *должны быть полными степенями* $n = 4$,
- *правые части равенств* (13) *и* (14) *должны быть полными степенями* $n = p$.

1. Основные теоремы

Основная теорема арифметики натуральных чисел:

Для каждого натурального числа $A > 1$ существует единственное разложение на простые множители:

$$A = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \; \ldots \; p_k^{\alpha_k} \; \ldots \; p_s^{\alpha_s}, \tag{1.1}$$

$$A^n = (p_1^{\alpha_1})^n \cdot (p_2^{\alpha_2})^n \cdot (p_3^{\alpha_3})^n \cdot \ldots \cdot (p_k^{\alpha_k})^n \cdot \ldots \cdot (p_s^{\alpha_s})^n, \tag{1.2}$$

где p_i — попарно различные простые числа, $\alpha_i \geqslant 1$, а правые части называются каноническими разложениями A и A^n на простые множители.

К формулам (1.1) и (1.2) будем обращаться во всех теоремах.

В научной литературе известна

Лемма. *Если в равенстве*

$$A^n = B \cdot C$$

числа A, B и C целые, а B и C взаимно простые, то B и C будут полными степенями показателя n, т.е. $B = B_1^n$, $C = C_1^n$.

Теоремы от автора

Во всех теоремах будем иметь ввиду только целые положительные числа.

Теорема I. *Если степень A^n делится на $(A - B) = P$, то числа A, P и B имеют наибольший общий делитель E такой, что E делится на каждый простой делитель числа P, а число P делится на каждый простой делитель числа E.*

Доказательство. Пусть A и A^n будут представлены каноническими разложениями (1.1) и (1.2). Тогда число P, как делитель A^n, должно иметь вид:

$$P = p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdot \ldots \cdot p_k^{q_k} \cdot \ldots \cdot p_s^{q_s}, \tag{1.3}$$

где $q_i = 0$, если делитель p_i не делит числа P, $1 \leqslant q_j \leqslant \alpha_j \cdot n$, если делитель p_j делит число P.

Так как $B = (A - P)$, то имеем:

$$B = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \ldots \cdot p_s^{\alpha_s} - p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdot \ldots \cdot p_k^{q_k} \cdot \ldots \cdot p_s^{q_s} =$$
$$= (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot \ldots \cdot p_k^{\beta_k} \cdot \ldots \cdot p_s^{\beta_s}) \cdot K, \tag{1.4}$$

где K — целое число, взаимно простое с A и P, а показатели β определяются по правилу: $\beta_i = q_i = 0$, если p_i не делит числа P. Если p_j делит P, то $\beta_j = q_j \geqslant 1$, если $q_j \leqslant \alpha_j$; $\beta_j = \alpha_j \geqslant 1$, если $\alpha_j \leqslant q_j$.

Произведение сомножителей p^β в (1.4) есть наибольший общий делитель A и P, т.е. число E:

$$E = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot \ldots \cdot p_k^{\beta_k} \cdot \ldots \cdot p_s^{\beta_s}, \tag{1.5}$$

так как показатели $\beta_j \geqslant 1$ соответствуют наибольшей степени делителей p_j или в числе A, или в числе P. Из (1.4) видно, что E делит B.

Из зависимости показателей степени β и q видно, что число E делится на каждый простой делитель числа P, а число P делится на каждый простой делитель числа E. Теорема доказана. □

Теорема II. *Если A^n делится на $(B - A) = P$, то числа A, P и B имеют наибольший общий делитель E такой, что E делится на каждый простой делитель числа P, а число P делится на каждый простой делитель числа E.*

Доказательство. Теорема доказывается аналогично теореме I. Отличие состоит в том, что в данном случае $B = A + P$. □

Теорема III. *Если в равенстве*

$$A^n = (A - B) \cdot C$$

разность $(A - B) = P$, *а* P *и* C *взаимно простые, то*

$$(A - B) = P = E^n,$$

где E *есть наибольший общий делитель чисел* A, P *и* B, *и* E *делится на каждый простой делитель числа* P, *а число* P *делится на каждый простой делитель числа* E.

Доказательство. Пусть число A имеет вид (1.1), а степень A^n — вид (1.2). Числа P и C взаимно простые, и, согласно Лемме, должно быть $P = P_1^n$, $C = C_1^n$. Число $P = P_1^n$ и оно делит степень A^n, поэтому должно быть:

$$P = P_1^n = (p_1^{q_1})^n \cdot (p_2^{q_2})^n \cdot (p_3^{q_3})^n \cdot \ldots \cdot (p_k^{q_k})^n \cdot \ldots \cdot (p_s^{q_s})^n, \tag{1.6}$$

где: $q_i = 0$, если делитель вида $(p_i^{q_i})^n$ не делит числа $P = P_1^n$, $q_j = \alpha_j$, если делитель вида $(p_j^{q_j})^n$ делит число $P = P_1^n$.

Так как $(A - P) = B$, то $B = (A - P)$, или в разложениях это будет так:

$$B = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \ldots p_k^{\alpha_k} \cdot p_s^{\alpha_s} - (p_1^{q_1})^n \cdot (p_2^{q_2})^n \cdot (p_3^{q_3})^n \cdot \ldots \cdot (p_k^{q_k})^n \cdot \ldots \cdot (p_s^{q_s})^n =$$

$$= (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot \ldots \cdot p_k^{\beta_k} \cdot \ldots \cdot p_s^{\beta_s}) \cdot K, \tag{1.7}$$

где K — целое число, взаимно простое с A и P, а показатели β определяются по правилу: $\beta_i = q_i = 0$, если делитель p_i не делит числа $P = P_1^n$, $\beta_j = q_j = \alpha_j$, если делитель p_j делит число $P = P_1^n$.

Произведение сомножителей p^β в (1.7) есть наибольший общий делитель E чисел A и P, так как $\beta_i = q_i = 0$ или $\beta_j = q_j = \alpha_j$, что для числа A будет наибольшим показателем степени у простого p_j. Итак, имеем:

$$E = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot \ldots \cdot p_k^{\beta_k} \cdot \ldots \cdot p_s^{\beta_s}. \tag{1.8}$$

Из (1.7) видно, что число B делится на E. Поэтому E есть наибольший общий делитель чисел A, P и B. В (1.8) показатели β можно заменить на показатели q:

$$E = p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdot \ldots \cdot p_k^{q_k} \cdot \ldots \cdot p_s^{q_s}. \tag{1.9}$$

Общий делитель E в (1.9) возведем в степень n, сравним с (1.6) и запишем:

$$(A - B) = P = E^n = (p_1^{q_1})^n \cdot (p_2^{q_2})^n \cdot (p_3^{q_3})^n \cdot \ldots \cdot (p_k^{q_k})^n \cdot \ldots \cdot (p_s^{q_s})^n. \tag{1.10}$$

Из (1.10) видно, что у чисел P и E одни и те же простые делители. Теорема доказана. □

Теорема IV. *Если в равенстве*

$$A^n = (B - A) \cdot C$$

разность $(B - A) = P$, а числа P и C взаимно простые, то

$$(B - A) = P = E^n,$$

где E есть наибольший общий делитель чисел A, P и B, и E делится на каждый простой делитель числа P, а число P делится на каждый простой делитель числа E.

Доказательство. Теорема доказывается по аналогии с теоремой III. Отличие состоит в том, что в данном случае $B = A+P$, а было $B = A-P$. □

Теорема V. *Пусть имеем:*

а) $A^n = p_k^\gamma \cdot (A - B) \cdot C$,

б) $A - B = P$ *и* P *делится на* p_k,

в) P *и* C *взаимно простые*,

г) $\alpha_k \cdot n - \gamma \geqslant \alpha_k$,

тогда

$$A - B = P = p^{-\gamma} \cdot E^n,$$

где E есть наибольший общий делитель чисел A, P и B, и E делится на каждый простой делитель числа P, а число P делится на каждый простой делитель числа E.

Доказательство. Пусть A имеет вид (1.1), а A^n — вид (1.2). Числа P и C взаимно простые, а P делится на p_k. Поэтому $(p_k^\gamma \cdot P)$ и C должны быть взаимно простыми и, согласно Лемме, в равенстве $A^n = (p_k^\gamma \cdot P) \cdot C$ они должны быть полными степенями показателя n. И тогда число P должно содержать делитель p_k^e, где $e = \alpha_k \cdot n - \gamma$. В свою очередь число P, как делитель степени A^n, должно иметь вид:

$$P = (p_1^{q_1})^n \cdot (p_2^{q_2})^n \cdot (p_3^{q_3})^n \cdot \ldots \cdot (p_k^e) \cdot \ldots \cdot (p_s^{q_s})^n, \tag{1.11}$$

где $q_i = 0$, если P не делится на p_i, $q_j = \alpha_j$, если P делится на p_j, $e = \alpha_k \cdot n - \gamma \geqslant \alpha_k$. Найдем число $B = (A - P)$, что в каноническом разложении будет так:

$$\begin{aligned} B &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \ldots \cdot p_s^{\alpha_s} - \\ &\quad - (p_1^{q_1})^n \cdot (p_2^{q_2})^n \cdot (p_3^{q_3})^n \cdot \ldots \cdot (p_k^e) \cdot \ldots \cdot (p_s^{q_s})^n = \\ &= (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot \ldots \cdot p_k^{\beta_k} \cdot \ldots \cdot p_s^{\beta_s}) \cdot K, \end{aligned} \tag{1.12}$$

где K — целое число, взаимно простое с A и P, а показатели β равны: $\beta_i = q_i = 0$, если P не делится на p_i, $\beta_j = q_j = \alpha_j$, если P делится на p_j, $\beta_k = \alpha_k$, так как $e = \alpha_k \cdot n - \gamma \geqslant \alpha_k$.

Произведение сомножителей p^β есть наибольший общий делитель E чисел A и P, так как $\beta_i = 0$ или $\beta_j = \alpha_j$, что соответствует наибольшей степени p_j в A. Из (1.12) видно, что E делит B. Итак, имеем:

$$E = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot \ldots \cdot p_k^{\beta_k} \cdot \ldots \cdot p_s^{\beta_s}. \tag{1.13}$$

В (1.13) показатели β можно заменить на показатели q:

$$E = p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdot \ldots \cdot p_k^{q_k} \cdot \ldots \cdot p_s^{q_s}. \tag{1.14}$$

Из зависимости показателей α, q и β видно, что E и P делятся на одни и те же простые делители. Число E в (1.14) возведем в степень n:

$$E^n = (p_1^{q_1})^n \cdot (p_2^{q_2})^n \cdot (p_3^{q_3})^n \cdot \ldots \cdot (p_k^{q_k})^n \cdot \ldots \cdot (p_s^{q_s})^n. \tag{1.15}$$

Степень E^n сравним с числом P в (1.11). В этих числах есть отличие только в двух сомножителях: p_k^c из (1.11) и $(p_k^{q_k})^n$ в (1.15). Имеем:

$$e = \alpha_k \cdot n - \gamma, \ \beta_k = q_k = \alpha_k, \ q_k \cdot n = \alpha_k \cdot n. \tag{1.16}$$

Находим разность: $(q_k \cdot n - e) = \gamma$. Из этого видно, что E^n больше P в p_k^γ раз, или:

$$(A - B) = P = p_k^{-\gamma} \cdot E^n. \tag{1.17}$$

Теорема доказана. □

Теорема VI. *Пусть имеем:*

а) $A^n = p_k^\gamma \cdot (B - A) \cdot C$,

б) $B - A = P$ *и* P *делится на* p_k,

в) P *и* C *взаимно простые,*

г) $\alpha_k \cdot n - \gamma \geqslant \alpha_k$,

тогда

$$(B - A) = P = p_k^{-\gamma} \cdot E^n,$$

где E есть наибольший общий делитель чисел A, P и B, и E делится на каждый простой делитель числа P, а P делится на каждый простой делитель числа E.

Доказательство. Доказывается теорема аналогично теореме V. □

Теорема VII. *Пусть $A = 2^\alpha \cdot X$ и $B = 2^\beta \cdot Y$, где $\alpha \geqslant 1$, $\beta \geqslant 1$, а X и Y нечетные числа, тогда $(A + B)$ и $(A - B)$ одновременно будут делиться на 2^e, где $e = 1$, если в степенях 2^α и 2^β будет неравенство $\alpha \neq \beta$ и одно из чисел α или β будет равно 1, во всех остальных случаях $(A + B)$ и $(A - B)$ одновременно будут делиться на 2^γ, где $\gamma \geqslant 2$.*

Доказательство. Итак, имеем:

$$A \pm B = 2^\beta \cdot \left(2^{\alpha-\beta} \cdot X \pm Y\right), \quad \text{если} \quad \alpha > \beta, \tag{1.18}$$

$$A \pm B = 2^\alpha \cdot \left(X \pm 2^{\beta-\alpha} \cdot Y\right), \quad \text{если} \quad \beta > \alpha, \tag{1.19}$$

$$A \pm B = 2^\alpha \cdot \left(X \pm Y\right), \quad \text{если} \quad \alpha = \beta. \tag{1.20}$$

Так как X и Y числа нечетные, то числа $\left(2^{\beta-\alpha} \cdot X \pm Y\right)$ и $\left(X \pm 2^{\beta-\alpha} \cdot Y\right)$ всегда будут нечетными, а числа $\left(X \pm Y\right)$ всегда будут четными. Поэтому в (1.20) и сумма, и разность одновременно будут делиться на 2^γ, где $\gamma \geqslant 2$. В равенствах (1.18) и (1.19) в правой части наибольший общий делитель по простому числу 2 равен 2^β или 2^α. Наименьшее его значение будет при $\beta = 1$ или при $\alpha = 1$, если $\alpha \neq \beta$, и в этом случае $(A+B)$ и $(A-B)$ одновременно будут делиться на 2^e, где $e = 1$. □

Теорема VIII. *Пусть числа A и B делятся на одни и те же простые делители. Тогда с некоторым числом C числа A и B будут одновременно взаимно простыми или каждое из них будет иметь с C свой общий делитель.*

Доказательство. Если число C не делится на простые делители числа A, то C не будет делиться на простые делители числа B. Если число C будет делиться хотя бы на один простой делитель числа A, то C будет делиться на этот же делитель числа B. □

2. Подбор целых чисел к равенству $A^2 = X^2 + Y^2$

Предполагаем, что есть тройка целых чисел A, X и Y, попарно взаимно простых и обеспечивающих равенство:

$$A^2 = X^2 + Y^2, \tag{2.1}$$

которое заменим на два равенства:

$$(B-C)^2 = X^2 + (B-X)^2, \tag{2.2}$$

$$(B-C)^2 = (B-Y)^2 + Y^2, \tag{2.3}$$

где $B = X+Y$, $C = X+Y-A$, числа B, X и Y попарно взаимно простые, а число C всегда четное. Равенства (2.2) и (2.3) раскроем и преобразуем:

$$X^2 = 2B(X-C) - (X^2 - C^2), \tag{2.4}$$

$$Y^2 = 2B(Y-C) - (Y^2 - C^2). \tag{2.5}$$

Теорема 2.1. *Если при заданных числах C и B нечетное число X будет обеспечивать равенство* (2.4), *то*

$$X = C + \mathrm{E}_x^2,$$

где E_x есть наибольший общий делитель чисел X и C.

Доказательство. В правой части равенства (2.4) вынесем за скобку разность $(X-C)$:

$$X^2 = (X-C) \cdot \big(2B - (X+C)\big). \tag{2.6}$$

Обозначим:

$$P = X - C, \tag{2.7}$$

$$\Pi = 2B - (X+C). \tag{2.8}$$

В (2.6) X^2 должен делиться на $(X-C) = P$. Тогда по Основной Теореме I числа X, C и P должны иметь наибольший общий делитель E_x такой, что E_x и P будут делиться на одни и те же простые делители. Так как X и C будут иметь общий делитель E_x, то $(X - C)$ и $(X + C)$ будут делиться на E_x, а число $2B$, как взаимно простое с X, будет взаимно простым с E_x. Поэтому число П в (2.8) будет взаимно простым с E_x и с $P = (X - C)$ в (2.7) и в (2.6). Следовательно, в правой части (2.6) будут два взаимно простых числа: $\big(2B-(X+C)\big)$ и $(X-C)$, произведение которых по нашему предположению должно быть полным квадратом, и согласно Основной Теореме III должно быть равенство:

$$X - C = P = E_x^2, \tag{2.9}$$

или

$$X = C + E_x^2, \tag{2.10}$$

где число C — заданное четное число, а E_x есть нечетный делитель C, в том числе и $E_x = 1$. □

Теорема 2.2. *Если при заданных числах C и B четное число Y будет обеспечивать равенство* (2.3), *то*

$$Y = C + \frac{1}{2}E_y^2,$$

где E_y есть наибольший общий делитель Y и C.

Доказательство. Число Y делится на показатель степени $n = 2$. В правой части равенства (2.3) вынесем за скобку число $2 \cdot (Y - C)$:

$$Y^2 = 2 \cdot (Y - C) \cdot \left(B - \frac{1}{2} \cdot \big(Y + C\big)\right). \tag{2.11}$$

Обозначим:

$$P = Y - C, \tag{2.12}$$

$$\Pi = B - \frac{1}{2} \cdot \big(Y + V\big). \tag{2.13}$$

Согласно принятому предположению левая и правая части (2.11) должны быть полными квадратами, и степень Y^2 должна делиться на $P = Y - C$. Тогда согласно Основной Теореме I числа Y, P и C должны иметь наибольший общий делитель E_y такой, что E_y и P будут делиться на одни и те же простые делители в том числе и на 2, так как Y и C делятся на 2. Так как Y и C имеют общий делитель E_y, то $(Y - C)$ и $(Y + C)$ будут делиться на E_y, а число B будет взаимно простым с E_y, потому что B и Y взаимно простые. Дальнейшее решение разделим на два варианта в зависимости от деления $(Y + C)$ на 2^γ: а) когда $\gamma \geqslant 2$, б) когда $\gamma = 1$.

Вариант а). Если $(Y + C)$ делится на 2^γ, где $\gamma \geqslant 2$, то $1/2 \cdot (Y + C)$ делится на каждый простой делитель числа E_y, в том числе и на 2. Но число B не делится на простые делители числа E_y, поэтому число П в (2.13) не будет делиться на простые делители E_y и будет взаимно простым с $P = (Y - C)$ и с $2P = 2 \cdot (Y - C)$. Тогда в (2.11) будут два взаимно простых числа: $2 \cdot (Y - C)$ и $\left(B - 1/2 \cdot (Y + C)\right)$. Это дает возможность воспользоваться Основной Теоремой V и записать:

$$(Y - C) = \frac{1}{2} \cdot E_y^2, \tag{2.14}$$

или

$$Y = C + \frac{1}{2} \cdot E_y^2. \tag{2.15}$$

Вариант б). Если $(Y + C)$ делится на 2^γ, где $\gamma = 1$, то число $1/2 \cdot (Y + C)$ не делится на 2. Число П будет четным, так как в правой части (2.13) находятся два нечетных числа: B и $1/2 \cdot (Y + C)$. Однако число $1/2 \cdot (Y + C)$ делится на каждый нечетный простой делитель числа E_y, а число B взаимно простое с E_y. Поэтому число П и число E_y будут взаимно простыми по всем простым нечетным делителям числа E_y. По этим же простым нечетным делителям будут взаимно простыми число П и число $P = Y - C$. Из этого следует, что в (2.11) числа $(Y - C)$ и $(B - 1/2 \cdot (Y + C))$ будут взаимно простыми по всем делителям $(Y - C)$, кроме делителя 2.

Если $(Y + C)$ делится на 2^γ, где $\gamma = 1$, то согласно Основной Теореме VII разность $(Y - C)$ тоже будет делиться на 2^γ, где $\gamma = 1$. И поэтому число $2 \cdot (Y - C)$ будет делиться на 2^2. Числа Y и C делятся на 2, поэтому примем:

$$Y_1 = \frac{1}{2} \cdot Y, \quad C_1 = \frac{1}{2} \cdot C, \quad E_{y1} = \frac{1}{2} \cdot E_y,$$

а равенство (2.11) разделим на 2^2 и получим:

$$Y_1^2 = (Y_1 - C_1)\left(B - \frac{1}{2} \cdot (Y + C)\right). \tag{2.16}$$

Теперь число $(Y_1 - C_1)$ будет нечетным и взаимно простым с числом $(B - 1/2 \cdot (Y + C))$. А по Основной Теореме III можно записать:

$$(Y_1 - C_1) = E_{y1}^2. \tag{2.17}$$

Умножим (2.17) на 2 и получим:

$$Y - C = 2 \cdot E_{y1}^2 = \frac{1}{2} \cdot E_y^2, \tag{2.18}$$

или

$$Y = C + \frac{1}{2} \cdot E_y^2. \tag{2.19}$$

Формула (2.19) повторяет формулу (2.15), где четное число C задается, а E_y есть четный делитель числа C, в том числе $E_y = C$.

Теперь находим число

$$A = B - C = X + Y - C = C + E_x^2 + \frac{1}{2} \cdot E_y^2.$$

Найденные решения для чисел X, Y и A надо подставить в исходное равенство $A^2 = X^2 + Y^2$ и проверить эти решения на истинность. Для упрощения операций примем замену:

$$M = E_x^2, \quad T = \frac{1}{2} \cdot E_y^2 \tag{2.20}$$

и

$$X = C + M, \quad Y = C + T, \quad A = C + M + T. \tag{2.21}$$

Теперь равенство $A^2 = X^2 + Y^2$ будет таким:

$$\big(C + (M + T)\big)^2 = (C + M)^2 + (C + T)^2. \quad \square \tag{2.22}$$

Теорема 2.3. *Пусть задано четкое число $C \geqslant 2$ и его два взаимно простых делителя E_x и E_y, тогда числа*

$$X = C + E_x^2, \quad Y = C + \frac{1}{2} \cdot E_y^2 \quad \text{и} \quad A = C + E_x^2 + \frac{1}{2} \cdot E_y^2$$

могут обеспечить равенство $A^2 = X^2 + Y^2$ при условии, что $E_x \cdot E_y = C$.

Доказательство. В (2.22) раскроем скобки и упростим:

$$2 \cdot MT = C^2, \tag{2.23}$$

или

$$E_x^2 \cdot E_y^2 = C^2, \tag{2.24}$$

или

$$E_x \cdot E_y = C. \tag{2.25}$$

Итак, если задано четное число $C \geqslant 2$ и его два взаимно простых делителя E_x и E_y таких, что $E_x \cdot E_y = C$, то равенство $A^2 = X^2 + Y^2$ будет обеспечиваться числами:

$$X = C + E_x^2, \quad Y = C + \frac{1}{2} \cdot E_y^2, \quad A = C + E_x^2 + \frac{1}{2} \cdot E_y^2. \tag{2.26}$$

Это новое целочисленное решение для $A^2 = X^2 + Y^2$. $\square$

3. Подбор целых чисел к равенству $A^4 = X^4 + Y^4$

Предполагаем, что есть тройка целых чисел A, X и Y попарно взаимно простых и обеспечивавших равенство:

$$A^4 = X^4 + Y^4, \tag{3.1}$$

которое заменим на два равенства:

$$(B - C)^4 = X^4 + (B - X)^4, \tag{3.2}$$

$$(B - C)^4 = (B - Y)^4 + Y^4, \tag{3.3}$$

где $B = X + Y$, $C = X + Y - A$, $A = B - C$, и числа B, X и Y попарно взаимно простые, а число C всегда четное. Равенства (3.2) и (3.3) раскроем и преобразуем:

$$X^4 = 4B^3 \cdot (X - C) - 6B^2 \cdot (X^2 - C^2) + \\ + 4B \cdot (X^3 - C^3) - (X^4 - C^4), \tag{3.4}$$

$$Y^4 = 4B^3 \cdot (Y - C) - 6B^2 \cdot (Y^2 - C^2) + \\ + 4B \cdot (Y^3 - C^3) - (Y^4 - C^4). \tag{3.5}$$

На основании принятого ранее предположения в правых и левых частях равенств (3.4) и (3.5) должны быть полные степени показателя $n = 4$.

Теорема 3.1. *Если при заданных числах C и B нечетное число X будет обеспечивать равенство* (3.4), *то $X = C + E_x^4$, где E_x есть наибольший общий делитель чисел C и X.*

Доказательство. Нечетное число X является взаимно простым с показателем степени $n = 4$. В правой части (3.4) вынесем за скобку число $(X - C)$ и получим:

$$X^4 = (X - C) \cdot M_x, \tag{3.6}$$

где M_x — многочлен от деления правой части (3.4) на $(X - C)$. Обозначим:

$$P = X - C. \tag{3.7}$$

В (3.6) степень X^4 должна делиться на $(X - C) = P$. Тогда согласно Основной Теореме I числа X, P и C должны иметь наибольший общий делитель E_x такой, что E_x и P будут делиться на одни и те же простые делители. Так как у X и C будет общий делитель E_x, то в (3.4) каждая разность $(X^k - C^k)$, где $k = 1, 2, 3$ и 4, будет делиться на E_x^k, т. е. на E_x, E_x^2, E_x^3 и E_x^4 соответственно, а число $4B^3$ будет взаимно простым с E_x, так как E_x делит X, с которым число $4B^3$ взаимно простое. При вынесении разности $(X - C)$ за скобку надо было разделить каждую разность $(X^k - C^k)$ на $(X - C)$. После такого деления получатся частные, каждое из которых будет делиться на E_x^0, E_x, E_x^2 и E_x^3 соответственно.

Многочлен M_x будет содержать свободный член $4B^3$ и члены, каждый из которых будет делиться на E_x. Так как в многочлене M_x есть только один член $4B^3$, который взаимно простой с E_x, то и сам M_x будет взаимно простым с E_x и потом с $P = (X - C)$. Поэтому в (3.6) числа $(X - C)$ и M_x будут взаимно простыми, и согласно Основной Теореме III должно быть:

$$X - C = E_x^4, \tag{3.8}$$

или

$$X = C + E_x^4. \tag{3.9}$$

Условия теоремы будут выполнены, когда при заданном четном числе C и выбранном его нечетном делителе E_x число X будет определяться по формуле (3.9), в том числе и при $E_x = 1$, когда X и C будут взаимно простыми. □

Теорема 3.2. *Если при заданных числах C и B четное число Y будет обеспечивать равенство* (3.5), *то Y должен определяться по формулам*

$$Y = C + 2^{-2} \cdot E_y^4 \quad \textit{или} \quad Y = C + 2^{-3} \cdot E_y^4,$$

где E_y есть наибольший общий делитель чисел C и Y.

Доказательство. Четное число Y имеет общий делитель с показателем степени $n = 4$. В правой части (3.5) вынесем за скобку число $4 \cdot (Y - C)$:

$$Y^4 = 4 \cdot (Y - C) \cdot M_y, \tag{3.10}$$

где M_y — многочлен от деления правой части (3.5) на $4 \cdot (Y - C)$.

Обозначим:

$$P = (Y - C), \tag{3.11}$$

$$\Pi = B^3 - 3B^2 \cdot \frac{1}{2} \cdot (Y + C), \tag{3.12}$$

где $(B^3 - 3B^2 \cdot 1/2 \cdot (Y + C))$ — это выделенные из M_y первые два члена. В (3.10) степень Y^4 должна делиться на $(Y - C) = P$, а правая часть должна быть полной степенью показателя $n = 4$ по предположению. Тогда согласно Основной Теореме I числа Y, C и P должны иметь наибольший общий делитель E_y такой, что E_y и P будут делиться на одни и те же простые делители. Так как Y и C имеют общий делитель E_y, то в (3.5) каждая разность $(X^k - C^k)$, где $k = 1, 2, 3$ и 4, будет делиться на E_y^k, т. е. на E_y, E_y^2, E_y^3 и E_y^4 соответственно, а число B^3 будет взаимно простым с E_y, так как E_y делит Y, с которым число B взаимно простое. При вынесении числа $4 \cdot (Y - C)$ за скобку надо было делить каждый член правой части (3.5) на $4 \cdot (Y - C)$. Поэтому при делении $(Y^k - C^k)$ на $(Y - C)$ получатся частные, каждое из которых будет делиться на E_y^0, E_y, E_y^2 и E_y^3 соответственно. Но член

$$6B^2 \cdot (Y + C)$$

не всегда будет делиться на 2^γ, где $\gamma \geqslant 3$, и тогда число

$$3B^2 \cdot 2^{-1} \cdot (Y + C)$$

в (3.12) будет определять условия делимости многочлена M_y на простые делители числа E_y, главным образом на число 2. Те члены многочлена M_y, которые отсутствуют в (3.12), делятся на E_y, без всяких условий.

В зависимости от делимости $(Y + C)$ на 2^γ рассмотрим два варианта решения: а) когда $\gamma \geqslant 2$ и б) когда $\gamma = 1$.

Вариант а). Если $(Y + C)$ делится на 2^γ, где $\gamma \geqslant 2$, то число

$$3B^2 \cdot 2^{-1} \cdot (Y + C)$$

в (3.12) будет делиться на каждый простой делитель числа E_y, в том числе и на 2. Число B^3 — единственное число в многочлене M_y, которое не будет делиться на простые делители числа E_y. Поэтому M_y будет взаимно простым с E_y, а значит, и с $P = (Y - C)$, и с $2^2 \cdot (Y - C)$. Итак, в правой части (3.10) будут два взаимно простых числа: $2^2 \cdot (Y - C)$ и M_y, и в соответствии с Основной Теоремой V должно быть:

$$(Y - C) = 2^{-2} \cdot E_y^4, \tag{3.13}$$

или

$$Y = C + 2^{-2} \cdot E_y^4. \tag{3.14}$$

Вариант б). Если $(Y + C)$ будет делиться на 2^γ, где $\gamma = 1$, то число

$$3B^2 \cdot 2^{-1} \cdot (Y + C)$$

будет нечетным и не будет делиться на простой делитель 2 числа E_y, но будет делиться на каждый простой нечетный делитель числа E_y. В этом варианте число П в (3.12) будет четным, но не будет делиться на простые нечетные делители числа E_y, так как число B взаимно простое с E_y. Поэтому многочлен M_y будет взаимно простым с числом E_y и с числом $P = Y - C$ по всем простым нечетным делителям чисел E_y и $(Y - C)$.

Если $(Y + C)$ будет делиться на 2^γ, где $\gamma = 1$, то по Основной Теореме VII разность $(Y - C)$ тоже будет делиться на 2^γ, где $\gamma = 1$. Так как Y и C делятся на 2, то можно записать:

$$Y = 2Y_1, \quad C = 2C_1, \quad E_y = 2E_{y1}. \tag{3.15}$$

Равенство (3.10) разделим на 2^2 и получим:

$$Y_1^4 = (Y_1 - C_1) \cdot \left(\frac{1}{2} \cdot M_y\right). \tag{3.16}$$

Многочлен M_y будет четным и взаимно простым с нечетным числом $(Y_1 - C_1)$. По Основной Теореме III запишем:

$$Y_1 - C_1 = E_{y1}^4 = 2^{-4} \cdot E_y^4. \tag{3.17}$$

Равенство (3.17) умножим на 2 и получим:

$$Y - C = 2^{-3} \cdot E_y^4, \tag{3.18}$$

или

$$Y = C + 2^{-3} \cdot E_y^4. \tag{3.19}$$

Итак, число Y должно определяться формулой (3.14) или (3.19). Число

$$A = X + Y - C,$$

или

$$A = C + E_x^4 + 2^{-2} \cdot E_y^4 \tag{3.20}$$

и

$$A = C + E_x^4 + 2^{-3} \cdot E_y^4. \tag{3.21}$$

Решения для A, X и Y подставим в $A^4 = X^4 + Y^4$ и проверим их истинность. Для упрощения операций примем временную замену:

$$M = E_x^4, \quad T = 2^{-2} \cdot E_y^4 \quad \text{или} \quad T = 2^{-3} \cdot E_y^4, \tag{3.22}$$

$$A = C + M + T, \quad X = C + M, \quad Y = C + T. \tag{3.23}$$

Тогда имеем:

$$\left(C + (M + T)\right)^4 = (C + M)^4 + (C + T)^4. \quad \square \tag{3.24}$$

Теорема 3.3. *Если равенство* (3.24) *возможно при целых числах* C, M *и* T, *то оно возможно только при неравенстве*

$$12 \cdot M \cdot T < C^2.$$

Доказательство. Равенство (3.24) раскроем и упростим;

$$C^2 \cdot 12 \cdot MT + C \cdot 12 \cdot MT \cdot (M + T) +$$
$$+ 2 \cdot MT \cdot (2M^2 + 3 \cdot MT + 2T^2) = C^4. \tag{3.25}$$

Если в (3.25) окажется, что $12 \cdot MT \geqslant C^2$, то левая часть в (3.25) будет больше правой части, т. е. больше C^4. Для обеспечения равенства необходимо иметь неравенство:

$$12 \cdot MT < C^2. \tag{3.26}$$

Это и есть требование теоремы. $\square$

Следствие из неравенства (3.26). *Воспользуемся условиями замены* (3.22) *и получим два неравенства*:

$$3 \cdot E_x^4 \cdot E_y^4 < C^2, \tag{3.27}$$

$$\frac{3}{2} \cdot E_x^4 \cdot E_y^4 < C^2. \tag{3.28}$$

Или

$$E_x \cdot E_y < \left(\frac{1}{3} \cdot C^2\right)^{\frac{1}{4}}, \tag{3.29}$$

$$E_x \cdot E_y < \left(\frac{2}{3} \cdot C^2\right)^{\frac{1}{4}}. \tag{3.30}$$

Числа E_x и E_y взаимно простые и являются делителями числа C, но достаточна малыми делителями, как это видно из неравенств (3.29) и (3.30). Так как E_x, и E_y являются взаимно простыми малыми делителями числа C, то можно записать так:

$$C = H \cdot E_x \cdot E_y, \tag{3.31}$$

где H — некоторое целое число, взаимно простое с $(E_x \cdot E_y)$. Равенство (3.25) не определяет соотношение между C и произведением $(E_x \cdot E_y)$ или между C и числом H. Поэтому при заданном числе C нельзя указать точную величину произведения $(E_x \cdot E_y)$, которая соответствовала бы показателю степени $n = 4$. Для равенства $A^2 = X^2 + Y^2$ потребовалось равенство $E_x \cdot E_y = C$ при любом четном $C \geqslant 2$. Неравенства (3.29) и (3.30) исключили из решения большие делители числа C. Но оказывается, что и самые наименьшие делители числа C тоже не могут использоваться в решении.

Теорема 3.4. *Равенство $A^4 = X^4 + Y^4$ не имеет решения в целых числах при наименьших делителях числа C.*

Доказательство. Число C должно быть четным числом. Для всякого четного числа наименьшими делителями будут $E_x = 1$ и $E_y = 2$, что соответствует Теореме 3.1, Теореме 3.2 и ограничениям (3.29) и (3.30). Для решения воспользуемся равенством (3.31) и получим:

$$C = H \cdot 1 \cdot 2 = 2H.$$

По наименьшим делителям $E_x = 1$ и $E_y = 2$ надо найти наименьшее целое число $C = 2H$. Теперь надо найти наименьшее число H.

В теореме 3.2 было установлено, что Y может иметь две формы:

$$Y = 2^{-2} \cdot E_y^4 \quad \text{и} \quad Y = 2^{-3} \cdot E_y^4.$$

Поэтому в равенство (3.25) надо подставить два варианта C, M, T:

$$C = H \cdot 1 \cdot 2, \quad M = E_x^4 = 1, \quad T = 2^{-2} \cdot E_y^4 = 2^2;$$

$$C = H \cdot 1 \cdot 2, \quad M = E_x^4 = 1, \quad T = 2^{-3} \cdot E_y^4 = 2.$$

Эти условия подставим в (3.25) и получим два уравнения:

$$H^4 - H^2 \cdot 12 - H \cdot 30 - 23 = 0, \tag{3.32}$$

$$H^4 - H^2 \cdot 6 - H \cdot 9 - 4 = 0. \tag{3.33}$$

В уравнениях надо найти целое число H. Тогда его значения должны равняться хотя бы одному целому делителю свободного члена уравнения. Однако целых делителей свободного члена уравнения для числа H нет ни в одном из уравнении. Поэтому число H не может быть целым числом в указанных уравнениях. Отсюда следует, что при наименьших делителях $E_x = 1$ и $E_y = 2$ нет наименьшего числа C для обеспечения равенства

$$A^4 = X^4 + Y^4.$$

По Теореме 3.1 и Теореме 3.2 были доказаны две формы решения:

Форма 1: $X = C + E_x^4, \quad Y = C + 2^{-2} \cdot E_y^4, \quad A = C + E_x^4 + 2^{-2} \cdot E_y^4.$

Форма 2: $X = C + E_x^4, \quad Y = C + 2^{-3} \cdot E_y^4, \quad A = C + E_x^4 + 2^{-3} \cdot E_y^4.$ □

Нами установлено, что равенство $A^4 = X^4 + Y^4$ не обеспечивается ни при больших делителях E_x и E_y, ни при их наименьших значениях. Поэтому равенство

$$A^4 = X^4 + Y^4$$

не может быть обеспечено ни при каких значениях E_x и E_y в целых числах, следовательно, целочисленные решения по Форме 1 и 2 являются ошибочными и не подходят для целочисленного решения равенства

$$A^4 = X^4 + Y^4.$$

Так как в методике решения ошибок нет, то ошибка должна быть в начальных условиях. Ошибочным является условие, что при каждом показателе степени n обязательно есть тройка целых чисел A, X и Y, которая обеспечивает равенство

$$A^n = X^n + Y^n.$$

При $n = 4$ такой тройки целых чисел нет, т. е. нет целочисленного решения

$$A^4 = X^4 + Y^4,$$

когда числа A, X и Y являются целыми числами одновременно.

4. Подбор целых чисел к равенству $A^p = X^p + Y^p$

Предполагаем, что есть тройка целых чисел A, X и Y, попарно взаимно простых и обеспечивающих равенство:

$$A^p = X^p + Y^p, \tag{4.1}$$

которое заменим на два равенства:

$$(B - C)^p = X^p + (B - X)^p, \tag{4.2}$$

$$(B - C)^p = (B - Y)^p + Y^p, \tag{4.3}$$

где p — простое нечетное число,

$$B = X + Y, \quad C = X + Y - A, \quad A = B - C$$

и числа B, X и Y попарно взаимно простые, а число C всегда четное.

Равенства (4.2) и (4.3) раскроем и преобразуем:

$$\begin{aligned}C^p &= pB^{p-1} \cdot (X - C) - \\ &- C_p^2 B^{p-2} \cdot (X^2 - C^2) + \ldots + C_p^2 B^2 \cdot (X^{p-2} - C^{p-2}) - \\ &- pB \cdot (X^{p-1} - C^{p-1});\end{aligned} \tag{4.4}$$

$$\begin{aligned}C^p &= pB^{p-1} \cdot (Y - C) - \\ &- C_p^2 B^{p-2} \cdot (Y^2 - C^2) + \ldots + C_p^2 B^2 \cdot (Y^{p-2} - C^{p-2}) - \\ &- pB \cdot (Y^{p-1} - C^{p-1}),\end{aligned} \tag{4.5}$$

где C_p^i — биномиальные коэффициенты, каждый из которых делится на показатель степени p, так как p — простое нечетное число.

Теорема 4.1. *Правые части равенств* (4.4) *и* (4.5) *делятся на* B, *а частные от деления правых частей на* B *будут взаимно простыми с* B.

Доказательство. Каждый член правой части равенств (4.4) и (4.5) делится на B, поэтому и сами правые части делятся на B. Тогда и левые части, т. е. степень C^p, должны делиться на B, а число C должно делиться на каждый простой делитель числа B. Число X примем не делящимся на показатель p, а для Y примем два варианта: а) Y делится на p, б) Y не делится на p.

В каждом члене правой части равенств (4.4) и (4.5) содержится биномиальный коэффициент C_p^i, который делится на p. Поэтому правые и левые части (4.4) и (4.5) будут делиться на p. Следовательно, степень C^p и само C будут делиться на показатель p.

Рассмотрим **вариант (а)**, когда Y делится на p, а число B, как взаимно простое с Y, не будет делиться на p. Разделим правую часть (4.4) и (4.5) на B и после этого рассмотрим получившиеся члены слева направо. Окажется, что B не содержится в единственном члене

$$p \cdot (X^{p-i} - C^{p-i})$$

из (4.4) и в единственном члене

$$p \cdot (Y^{p-i} - C^{p-i})$$

из (4.5), которые будут взаимно простыми с B, так как число C делится на каждый простой делитель числа B, а числа p, X и Y — взаимно простые с B. Поэтому частные от деления правых частей (4.4) и (4.5) на число B будут взаимно простыми с числом B.

Вариант (б), когда ни X, ни Y не делятся на p, а число B может делиться на p, но может и не делиться на p. Разделим правые части (4.4) и (4.5) на $p \cdot B$ и потом рассмотрим получившиеся члены слева направо. Окажется, что $p \cdot B$ не содержится в единственном члене

$$(X^{p-1} - C^{p-1})$$

из (4.4) и в единственном члене

$$(Y^{p-1} - C^{p-1})$$

из (4.5), каждый из которых будет взаимно простым с $p \cdot B$. Поэтому частные от деления правых частей (4.4) и (4.5) на число B будут взаимно простыми с B. Утверждение теоремы получено. □

Следствие из Теоремы 4.1. *Число B может иметь вид*

$$B = B_1^p \quad \textit{или} \quad B = p^{p-1}B_1^p,$$

где B_1^p есть полная степень показателя p.

Доказательство. Левые части равенств (4.4) и (4.5) равны между собой. Поэтому и правые части должны быть равны между собой. Тогда при делении правых частей на $p \cdot B$ получим равные частные, которые обозначим буквой M. Теперь запишем:

$$C^p = p \cdot B \cdot M. \tag{4.6}$$

Частное M по Теореме 4.1 взаимно простое с B. Если B не делится на p, то в правой части (4.6) будут два взаимно простых числа: B и $(p \cdot M)$. По Лемме оба этих числа должны быть полными степенями показателя p. В частности $B = B_1^p$. Если B будет делиться на p, то будут взаимно простыми $(p \cdot B)$ и M. В этом случае должно быть: $(p \cdot B) = E^p$. Число E должно делиться на p, т. е.

$$E^p = p^p \cdot B_1^p.$$

Теперь имеем

$$(p \cdot B) = p^p \cdot B_1^p, \quad \text{или} \quad B = p^{p-i} \cdot B_1^p.$$

В итоге получаем:

$$B = B_1^p, \quad \textit{или} \quad B = p^{p-1} \cdot B_1^p. \tag{4.7}$$

Число C будет иметь вид:

$$C = 2 \cdot p \cdot B_1 C_1, \tag{4.8}$$

где C_1 — целое число. □

Теорема 4.2. *Если при заданных числах C и B целое число X, не делящееся на показатель степени p, обеспечивает равенство* (4.4), *то*

$$X = C + E_x^p,$$

где E_x есть наибольший общий делитель чисел X и C.

Доказательство. В правой части (4.4) каждый член делится на

$$p \cdot B \cdot (X - C),$$

и это число вынесем за скобку:

$$C^p = p \cdot B \cdot (X - C) \cdot M_x, \tag{4.9}$$

где M_x — многочлен от деления правой части (4.4) на $p \cdot B \cdot (X - C)$. Обозначим:

$$P = (X - C). \tag{4.10}$$

Из (4.9) видно, что C^p должно делиться на $(X - C) = P$. А согласно Основной Теореме II в этом случае числа C, P и X должны иметь общий делитель E_x такой, что E_x и P будут делиться на одни и те же простые делители.

Так как X и C будут иметь общий делитель E_x, то число B, как взаимно простое с X, будет взаимно простым с E_x, а каждая разность $(X^k - C^k)$, где $1 \leqslant k \leqslant p - 1$, будет делиться на E_x^k. При делении каждой разности $(X^k - C^k)$ на $(X - C)$ получится многочлен H_k, который будет делиться на E_x^{k-1}. Поэтому многочлен M_x можно записать с выделением E_x:

$$M_x = B^{p-2} - E_x \cdot B^{p-3} \cdot H_3 + \\ + E_x^2 \cdot B^{p-4} \cdot H_4 - \ldots + E_x^{p-3} \cdot B \cdot H_{p-3} - E_x^{p-2} \cdot H_{p-2}, \tag{4.11}$$

где H_i — целочисленные многочлены.

В правой части (4.11) число B^{p-2} взаимно простое с E_x, а каждый последующий член делится на E_x. Поэтому M_x будет взаимно простым с E_x, а потом с $P = (X - C)$.

Число X не делится на p, а число C делится на p, поэтому в (4.10) число $P = (X - C)$ не делится на p. Тогда в равенстве (4.9) будут взаимно простыми два числа: $(X - C)$ и $(p \cdot B \cdot M)$. Согласно Основной Теореме IV должно быть:

$$X - C = E_x^p, \tag{4.12}$$

или

$$X = C + E_x^p. \tag{4.13}$$

Теорема доказана. □

Теорема 4.3. *Если при заданных числах C и B целое число Y, делящееся на показатель степени p, обеспечивает равенство (4.5), то*

$$Y = C + \frac{1}{p} \cdot E_y^p,$$

где E_y есть наибольший общий делитель Y и C.

Доказательство. В правой части (4.5) каждый член делится на

$$p \cdot B \cdot (Y - C),$$

и это число вынесем за скобку:

$$C^p = p \cdot B \cdot (Y - C) \cdot M_y, \tag{4.14}$$

где M_y — многочлен от деления правой части на $p \cdot B \cdot (Y - C)$. Обозначим:

$$P = (Y - C). \tag{4.15}$$

В (4.14) степень C^p должна делиться на $(Y - C) = P$, и согласно Основной Теореме II числа C, P и Y должны иметь наибольший общий делитель E_y такой, что E_y и P будут делиться на одни и те же простые делители.

Так как Y и C будут иметь общий делитель E_y, то E_y будет взаимно простым с числом B, которое взаимно простое с Y, а каждая разность

$$(Y^k - C^k), \quad \text{где} \quad 1 \leqslant k \leqslant p - 1,$$

будет делиться на E_y^k. При делении разности $(Y^k - C^k)$ на $(Y - C)$ получится многочлен H_k, который будет делиться на E_y^{k-1}. Поэтому многочлен M_y можно записать с выделением E_y:

$$\begin{aligned} M_y = B^{p-2} - E_y \cdot B^{p-3} \cdot H_2 + \\ + E_y^2 \cdot B^{p-4} \cdot H_3 - \ldots + E_y^{p-3} \cdot B \cdot H_{p-2} - E_y^{p-2} \cdot H_{p-1}, \end{aligned} \tag{4.16}$$

где H_i — целочисленные многочлены.

Числа Y и C делятся на показатель степени p, поэтому числа P и E_y тоже делятся на p, а число B не будет делиться на p, так как B и Y — взаимно простые. Итак, в правой части (4.16) число B^{p-2} — взаимно простое с E_y и p, а каждый последующий член делится на E_y. Поэтому многочлен M_y будет взаимно простым с E_y (и потом с $P = (Y - C)$) и с показателем p. Из сказанного следует, что в равенстве (4.14) будут взаимно простыми числа

$$(p \cdot (Y - C)) \quad \text{и} \quad (B \cdot M_y),$$

и согласно Основной Теореме VI должно быть:

$$(Y - C) = \frac{1}{p} \cdot E_y^p, \tag{4.17}$$

или

$$Y = C + \frac{1}{p} \cdot E_y^p. \tag{4.18}$$

Если Y не будет делиться на показатель степени p, то Y будет определен по методике нахождения числа X, т. е.

$$Y = C + E_y^p.$$

Так как X и Y — взаимно простые, то E_x и E_y тоже будут взаимно простыми, а их произведение

$$E_x \cdot E_y \leqslant C.$$

В исходном равенстве

$$A^p = X^p + Y^p$$

числа X и Y занимают равноправные положения по отношению к показателю степени p. Но для определенности было принято, что X не делится на p, а Y может делиться на p, но может и не делиться. Если X и Y поменять местами в выборе, то решение останется прежним.

Итак, имеем два варианта подбора чисел X, Y и A к равенству $A^p = X^p + Y^p$:

$$X = C + E_x^p, \quad Y = C + E_y^p, \qquad A = C + E_x^p + E_y^p; \tag{4.19}$$

$$X = C + E_x^p, \quad Y = C + \frac{1}{p} \cdot E_y^p, \quad A = C + E_x^p + \frac{1}{p} \cdot E_y^p. \tag{4.20}$$

Формулы (4.19) соответствуют двум вариантам решения равенства $A^p = X^p + Y^p$:

1) когда ни одно из чисел X, Y и A не делится на показатель p,
2) когда на показатель p делится только число A.

Формулы (4.20) соответствуют варианту решения, когда на p делится Y. Числа E_x и E_y являются делителями числа C, и они взаимно простые, как X и Y, а потому их произведение не может быть больше числа $C \geqslant E_x \cdot E_y$.

Теперь надо выяснить истинность решении (4.19) и (4.20). Для этого надо подставить их в равенство $A^p = X^p + Y^p$ и получить ответ.

Чтобы упростить алгебраические выкладки, примем замену:

$$M = E_x^p, \quad T = E_y^p, \tag{4.21}$$

$$M = E_x^p, \quad T = \frac{1}{p} \cdot E_y^p, \tag{4.22}$$

$$X = C + M, \quad Y = C + T, \quad A = C + M + T. \tag{4.23}$$

Тогда равенство $A^p = X^p + Y^p$ примет вид:

$$[C + (M + T)]^p = (C + M)^p + (C + T)^p. \quad \square \tag{4.24}$$

Теорема 4.4. *Если равенство* (4.24) *возможно при целых числах C, M и T, то оно возможно только при выполнении неравенства*:

$$p \cdot (p - 1) \cdot MT < C^2.$$

Доказательство. В равенстве (4.24) раскроем скобки и произведем перестановку и новую компановку членов, оставив в правой части единственный член C^p:

$$\begin{aligned}
&C^{p-2} \cdot C_p^2 \cdot 2MT + C^{p-3} \cdot C_p^3 \cdot 3MT \cdot (M+T) + \ldots + \\
&\quad + C^2 \cdot C_p^2 \cdot \left[(M+T)^{p-2} - (M^{p-2} + T^{p-2})\right] + \\
&\quad + C \cdot p \cdot \left[(M+T)^{p-1} - (M^{p-1} + T^{p-1})\right] + \\
&\quad + \left[(M+T)^p - (M^p + T^p)\right] = C^p. \qquad (4.25)
\end{aligned}$$

В левой части (4.25) записан многочлен по убывающим степеням числа C, начиная с C^{p-2}, а в правой части стоит степень C^p. Первый член

$$C^{p-2} \cdot C_p^2 \cdot 2MT$$

при определенных значениях M и T может оказаться равным C^p или больше C^p, и тогда левая часть (4.25) окажется больше правой части.

Поэтому надо поставить ограничение:

$$C^{p-2} \cdot C_p^2 \cdot 2MT < C^p, \qquad (4.26)$$

или

$$p \cdot (p-1) \cdot MT < C^2. \qquad (4.27)$$

Это и есть утверждение теоремы. □

Следствие из неравенства (4.27). *Воспользуемся обратным переходом от M и T к E_x и E_y и получим два неравенства:*

$$p \cdot (p-1) \cdot E_x^p \cdot E_y^p < C^2, \qquad \text{если} \quad T = E_y^p, \qquad (4.28)$$

$$(p-1) \cdot E_x^p \cdot E_y^p < C^2, \qquad \text{если} \quad T = \frac{1}{p} \cdot E_y^p. \qquad (4.29)$$

Из этих неравенств получим другие неравенства:

$$E_x \cdot E_y < \left(\frac{C^2}{p \cdot (p-1)}\right)^{1/p}, \qquad (4.30)$$

$$E_x \cdot E_y < \left(\frac{C^2}{p-1}\right)^{1/p}. \qquad (4.31)$$

Итак, делители E_x и E_y должны делить число C, должны быть взаимно простыми и должны быть достаточно малыми, чтобы обеспечить неравенства (4.30) и (4.31). Из сказанного следует, что должно выполняться равенство:

$$C = E_x \cdot E_y \cdot H, \qquad (4.32)$$

где H — целое число, E_x, E_y и H должны быть попарно взаимно простыми.

Равенство (4.25) не определяет соотношение между C и произведением $E_x \cdot E_y$. Поэтому при заданном числе C нельзя указать точную величину произведения $E_x \cdot E_y$, которая соответствовала бы показателю степени $n = p$. Неравенства (4.30) и (4.31) исключили из решения большие делители числа C. Это значит, что из формул (4.19) и (4.20) исключено целое множество решений с большими делителями числа C. Но в числе C все делители равноправны. Однако решения с большими делителями числа C не могут обеспечивать равенство $A^p = X^p + Y^p$ в целых числах, когда числа A, X и Y должны быть целыми числами одновременно. Оказывается, что решения с наименьшими делителями числа C тоже не могут обеспечивать равенство $A^p = X^p + Y^p$ в целых числах.

Теорема 4.5. *Равенство $A^p = X^p + Y^p$ не имеет решения в целых числах при наименьших делителях числа C.*

Доказательство. При наименьших делителях E_x и E_y числа C находим в формулах (4.19) и (4.20) наименьшие числа A, X и Y, которые должны обеспечить равенство $A^p = X^p + Y^p$ в целых числах. Но сперва для наименьших делителей E_x и E_y надо найти наименьшее целое число

$$C = X + Y - A$$

и наименьшее число

$$B = X + Y.$$

По формуле (4.7) находим: $B = B_1^p$ или

$$B = p^{p-1} \cdot B_1^p.$$

А по формуле (4.8) находим:

$$C = 2 \cdot p \cdot B_1 \cdot C_1.$$

В свою очередь $B = X + Y$. Тогда B будет иметь два варианта выражения:

(а) $B = 2C + E_x^p + E_y^p$,

(б) $B = 2C + E_x^p + \dfrac{1}{p} \cdot E_y^p$.

Форма (а) соответствует варианту решения равенства $A^p = X^p + Y^p$, когда ни одно из чисел A, X и Y не делится на показатель степени $n = p$, и варианту, когда на p делится только число A, которое делится на p только в том случае, если на p делится число B.

Форма (б) соответствует варианту решения равенства $A^p = X^p + Y^p$, когда на p делится число Y. В формах (а) и (б) число B выражено через число C и его делители E_x и E_y. Задавая наименьшие значения делителям E_x и E_y, будем искать наименьшие значения чисел B и C.

Наименьшие делители у четного числа C — это $E_x = 1$ и $E_y = 2$, которые подходят к обоим вариантам решения формы (а).

Наименьшие делители $E_x = 1$ и $E_y = p$ подходят к варианту решения, когда на показатель степени p делится Y, т. е. к форме (б).

Итак, для формы (а) числа B необходимо решить два уравнения:

$$B = B_1^p = 2^2 \cdot p \cdot B_1 \cdot H + 1 + 2^p, \tag{4.33}$$

$$B = p^{p-1} \cdot B_1^p = 2^2 \cdot p \cdot B_1 \cdot H + 1 + 2^p. \tag{4.34}$$

В равенстве (4.33) сумма $(1+2^p)$ должна делиться на B_1. При нечетном p сумма $(1+2^p)$ разлагается в произведение:

$$(1+2^p) = (1+2)(1-2+2^2-2^3+\ldots-2^{p-2}+2^{p-1}). \tag{4.35}$$

Ищется наименьшее число B_1. Поэтому в (4.35) для B_1 надо взять $(1+2)$. Теперь получаем при $B_1 = (1+2)$:

$$(1+2)^p = 2^2 \cdot p \cdot (1+2) \cdot H + 1 + 2^p. \tag{4.36}$$

В (4.36) раскроем скобки, удалим слева и справа равные числа и получим:

$$2p + 2^2 \cdot C_p^2 + 2^3 \cdot C_p^3 + \ldots + 2^{p-2} \cdot C_p^2 + 2^{p-1} \cdot p = 2^2 \cdot p \cdot 3 \cdot H. \tag{4.37}$$

Выражение (4.37) не может быть равенством в целых числах, так как левая его часть делится только на 2, а правая часть делится на 2^2. Поэтому и выражение (4.33) не может быть решено в целых числах B и C.

Рассмотрим равенство (4.34). В правой части этого равенства число $(1+2^p)$ должно делиться на простое число $p \geqslant 3$, являющееся показателем степени. Но при $p \geqslant 3$ остаток от деления числа $(1+2^p)$ на p всегда будет равен числу $(1+2) = 3$. Поэтому число $(1+2^p)$ будет делиться на p без остатка только при $p = 3$. При $p > 3$ равенства в (4.34) в целых числах не может быть. Теперь имеем при $p = 3$:

$$3^2 \cdot B_1^3 = 2^2 \cdot 3 \cdot B_1 \cdot H + 9, \tag{4.38}$$

или

$$3 \cdot B_1^3 = 2^2 \cdot B_1 \cdot H + 3. \tag{4.39}$$

В (4.39) число B_1 может иметь только одно значение $B_1 = 3$. Имеем:

$$27 = 2^2 \cdot H + 1. \tag{4.40}$$

Число H, входящее делителем в число C, в (4.40) не может быть целым числом. Поэтому и число C не может быть целым числом, т. е. выражение (4.34) при наименьших E_x и E_y не может быть решено в целых числах.

Мы искали наименьшие числа B и C, которые должны соответствовать наименьшим делителям $E_x = 1$ и $E_y = 2$. Но целых наименьших чисел B и C не оказалось. Это означает, что в формулах (4.19) возможных решений:

$$X = C + E_x^p, \quad Y = C + E_y^p, \quad A = C + E_x^p + E_y^p$$

не содержится наименьшее решение для чисел X, Y и A, которое могло бы обеспечить равенство $A^p = X^p + Y^p$.

Теперь будем искать наименьшие числа B и C в форме (б). В этом случае необходимо взять наименьшими делителями C числа $E_x = 1$ и $E_y = p$. Числа B и C будут иметь значения: $B = B_1^p$, $C = 2 \cdot p \cdot B_1 \cdot H$. Для формы (б) запишем уравнение:

$$B_1^p = 2^2 \cdot p \cdot B_1 \cdot H + 1 + p^{p-1}, \tag{4.41}$$

которое надо решить в наименьших числах B и H. Число $(1 + p^{p-1})$ является четным числом, т. е. делящимся на 2. Поэтому правая часть (4.41) делится на 2. Следовательно, и левая часть, т. е. B_1^p, должна делиться на 2^p. Число p — нечетное, тогда $(p - 1)$ — четное число. Пусть $(p - 1) = 2k$, а степень $p^k = 2T + 1$. Тогда имеем:

$$p^{2k} = (p^k)^2 = 4 \cdot T^2 + 4 \cdot T + 1. \tag{4.42}$$

Тогда сумма $(1 + p^{2k}) = 4 \cdot T^2 + 4 \cdot T + 2$. Эта сумма может делиться только на 2. Но число $2^2 \cdot p \cdot B_1 \cdot H$ может делиться на 2^3, а степень B_1^p может делиться на 2^p. Поэтому выражение (4.41) не может быть равенством в целых числах. Из сказанного вытекает, что для наименьших делителей $E_x = 1$ и $E_y = p$ нет целых наименьших чисел B и C. Это означает, что в формулах (4.20) возможных решений:

$$X = C + E_x^p, \quad Y = C + \frac{1}{p} \cdot E_y^p, \quad A = C + E_x^p + \frac{1}{p} \cdot E_y^p,$$

при наименьших $E_x = 1$ и $E_y = p$ нет наименьших целых чисел A, X и Y, которые обеспечили бы равенство $A^p = X^p + Y^p$. □

Теперь необходимо подвести итог:

1. В начале решения было сделано предположение, что имеется тройка целых чисел A, X и Y, которая обеспечивает равенство $A^p = X^p + Y^p$. На основе этого предположения проводились все решения.
2. В Теореме 4.2 и Теореме 4.3 на основании п.1 были определены числа X и Y, а потом было определено и число A:

$$X = C + E_x^p, \quad Y = C + E_y^p, \quad A = C + E_x^p + E_y^p, \tag{4.19}$$

$$X = C + E_x^p, \quad Y = C + \frac{1}{p} \cdot E_y^p, \quad A = C + E_x^p + \frac{1}{p} \cdot E_y^p, \tag{4.20}$$

где C — заданное четное число, а E_x и E_y — взаимно простые делители числа C. При доказательстве формул (4.19) и (4.20) на делители E_x и E_y никаких ограничений не было, т. е. при любых целых и взаимно простых делителях формулы (4.19) и (4.20) должны содержать целочисленные решения для обеспечения равенства $A^p = X^p + Y^p$.

3. Однако в Теореме 4.4 были получены ограничения на величину произведения $(E_x \cdot E_y)$: все большие делители числа C были исключены из решения. Это означает, что полученные законным путем решения формул (4.19) и (4.20) не учитывают особенностей исходного равенства $A^p = X^p + Y^p$.
4. В Теореме 4.5 было доказано, что при наименьших делителях E_x и E_y, которые не попали под ограничение, в формулах (4.19) и (4.20) не содержится решение в наименьших целых числах A, X и Y, которые могли бы обеспечить равенство $A^p = X^p + Y^p$.
5. Из сказанного видно, что при любых делителях числа C в формулах (4.19) и (4.20) не содержатся целочисленные решения для чисел A, X и Y, которые могли бы обеспечить равенство $A^p = X^p + Y^p$, хотя формулы (4.19) и (4.20) были получены вполне корректно — на предположении (см. п. 1).
6. Так как формулы (4.19) и (4.20) не учитывают особенностей равенства $A^p = X^p + Y^p$, то это означает, что предположение п. 1 является ошибочным, а равенство $A^p = X^p + Y^p$ не может иметь решения в целых числах, когда все три числа A, X и Y являются целыми числами одновременно.

Остается добавить, что для равенства $A^2 = X^2 + Y^2$ было найдено новое решение и было доказано, что равенства

$$A^4 = X^4 + Y^4 \quad \text{и} \quad A^p = X^p + Y^p$$

не могут иметь решения в целых числах. Поэтому все равенства

$$A^n = X^n + Y^n,$$

где показатель n делится на 4 или на простое нечетное число p, не могут иметь решения в целых числах, так как такие равенства приводятся к равенствам

$$A^4 = X^4 + Y^4 \quad \text{или} \quad A^p = X^p + Y^p,$$

которые не имеют решения в целых числах.

Об авторе Петр Макарович ОРЛОВ

Окончил военно-инженерную академию им. Ф. Э. Дзержинского, где получил высшее военно-техническое образование. Профессиональный военный. В свободное время увлекается теорией чисел.

Размышления над решением равенства $A^n = X^n + Y^n$ в целых числах всегда выступали для автора в качестве своеобразного отдыха и вдохновения, поскольку были свободным полетом мысли. В научной литературе приходилось читать об алгебраическом доказательстве большой теоремы Ферма. Но это доказательство всегда было оторвано от теоремы Пифагора — «родной сестры» теоремы Ферма. Автору всегда хотелось найти общее решение равенства $A^n = X^n + Y^n$ в целых числах, где теорема Пифагора и большая теорема Ферма решались бы по единой методике. И такое арифметическое решение найти удалось.