И.М. Титенко

Полное обнуление Большой теоремы Ферма

Аннотация

В статье без привлечения «новых сущностей» доказывается Большая теорема Ферма.

Введение

В 1637 г. Пьер Ферма (1601 – 1665) выдвинул предположение, что уравнение $x^k+y^k=z^k$ не имеет решения среди ненулевых целых чисел, если $k\geq 3$. Со временем данное предположение стало именоваться Большой (Великой, Последней) теоремой Ферма.

В течение 350 лет теорему для нечётных k не удавалось доказать, для чётных k теорема была доказана ещё Л. Эйлером. За отмеченный промежуток времени теорема обросла многими мифами. Вот один из мифов недавнего прошлого: коль скоро теорема не доказана до данного момента времени, то для её доказательства необходимы математические методы, более мощные по сравнению с существующими.

В 1995 г. англичанин Э. Уайлс представил [1] на ~110 страницах доказательство теоремы, в основе которого – идеи и методы, разработанные математиками во второй половине XX в. Но это доказательство мало созвучно простоте формулировки теоремы. Ведь ещё в XIV в. монах-францисканец У. Оккам выдвинул принцип, согласно которому при исследовании проблем «*не следует умножать сущности сверх необходимого*». Этот принцип в определённой степени соблюдался в науке в последующие века. Возможность реализации данного принципа для некоторых частных случаев рассматриваемой теоремы была продемонстрирована в [2].

Ниже, следуя данному принципу, доказывается Большая теорема Ферма.

I. Допущения и обозначения

Согласно Ферма уравнение

$$x^k + y^k = z^k, \quad k \geq 3, \tag{1}$$

не имеет целочисленных решений.

При доказательстве теоремы принимается следующее.

Считается, что $x < y < z$; Ξ, Ω - множества чётных и нечётных чисел, $x, z, k \in \Omega$, $y \in \Xi$;

$\overset{п}{=}$, $\overset{п}{\equiv}$ ($\overset{дб}{=}, \overset{дб}{\equiv}$) - обозначения равенства и сравнения, которые имеют место по предположению или должны иметь место быть при условии выполнения (1).

Обычно отдельно рассматривают случай I, когда $x \wedge y \wedge z \neq 0(\mathrm{mod}k)$, и случай II, когда $x \vee y \vee z \equiv 0(\mathrm{mod}k)$. Ниже при доказательстве случая I принимается, что x, y, z и k взаимно

простые, т.е. $(x,y,z,k)=1$, а при доказательстве случая II принимается, что $(x,y,z)=1$, $(x,y,k)=1$, но $z\equiv 0(\mathrm{mod}k^i,\ i\geq 1)$.

II. Доказательство случая I теоремы

Случай I теоремы был доказан в [2]. Чтобы соблюсти единство изложения, доказательство этого случая, правда с минимальными изменениями, приводится и в настоящей статье.

2.1. Некоторые соотношения

1. Если (1) имеет место быть, то согласно Абелю [3]

$$\begin{array}{lll} x\overset{\text{дб}}{=}uG, & u^k\overset{\text{дб}}{=}z-y, & G^k\overset{\text{дб}}{=}\sum_{i=0}^{k-1}z^{k-1-i}y^i, \\ y\overset{\text{дб}}{=}vP, & v^k\overset{\text{дб}}{=}z-x, & P^k\overset{\text{дб}}{=}\sum_{i=0}^{k-1}z^{k-1-i}x^i, \\ z\overset{\text{дб}}{=}wF, & w^k\overset{\text{дб}}{=}x+y, & F^k\overset{\text{дб}}{=}\sum_{i=0}^{k-1}(-1)^i y^{k-1-i}x^i, \end{array} \tag{2}$$

где $(u,G,v,P,w,F,k)=1;\ \ u,w,G,P,F\in\Omega$, а $v\in\Xi$.

2. По Малой теореме Ферма $h^{k-1}\equiv 1(\mathrm{mod}k)\ \ \forall(k,h)=1$. Поэтому, если имеет место (1), [3]

$$x+y-z\overset{\text{дб}}{\equiv}0(\mathrm{mod}k). \tag{3}$$

3. Пусть

$$x+y-z\overset{\text{п}}{=}\Phi. \tag{4}$$

Из (3) и (4) следует $\Phi\overset{\text{дб}}{\equiv}0(\mathrm{mod}k)$, а из (4) и (2) имеем: $x\overset{\text{дб}}{=}u^k+\Phi,\ \Phi\overset{\text{дб}}{\equiv}0(\mathrm{mod}u);\ y\overset{\text{дб}}{=}v^k+\Phi,$ $\Phi\overset{\text{дб}}{\equiv}0(\mathrm{mod}v);\ z\overset{\text{дб}}{=}w^k-\Phi,\ \Phi\overset{\text{дб}}{\equiv}0(\mathrm{mod}w)$. Поэтому, если имеет место (1),

$$\begin{array}{l} x\overset{\text{дб}}{=}u^k+\Phi, \\ y\overset{\text{дб}}{=}v^k+\Phi, \quad \Phi\overset{\text{дб}}{=}uvwk\psi, \quad \psi\in\Omega. \\ z\overset{\text{дб}}{=}w^k-\Phi, \end{array} \tag{5}$$

4. Из (2) и (5), учитывая Малую теорему Ферма, имеем: $G\overset{\text{дб}}{=}(u^{k-1}+\Phi/u)\overset{\text{дб}}{\equiv}1(\mathrm{mod}k)$, $P\overset{\text{дб}}{=}(v^{k-1}+\Phi/v)\overset{\text{дб}}{\equiv}1(\mathrm{mod}k)$, а $F\overset{\text{дб}}{=}(w^{k-1}-\Phi/w)\overset{\text{дб}}{\equiv}1(\mathrm{mod}k)$. Отсюда

$$G^k,P^k,F^k\overset{\text{дб}}{\equiv}1(\mathrm{mod}k^2). \tag{6}$$

5. Учитывая (2), (1) может быть записано в виде $u^kG^k+v^kP^k\overset{\text{п}}{=}w^kF^k$ или, учитывая, что по (2) и (5) $w^k=x+y=u^k+v^k+2\Phi$, в виде

$$u^k(G^k - F^k) + v^k(P^k - F^k) \overset{\text{дб}}{=} 2\Phi F^k. \tag{7}$$

Так как по (6) $G^k, P^k, F^k \overset{\text{дб}}{\equiv} 1 (\mathrm{mod} k^2)$, то в (7) $\Phi \overset{\text{дб}}{\equiv} 0 (\mathrm{mod} k^2)$, а в (5) $\psi = k\varphi$. Поэтому

$$\Phi \overset{\text{дб}}{=} uvwk^2\varphi, \quad \varphi \in \Omega, \ (u, v, w, k, \varphi) = 1. \tag{8}$$

2.2. Соотносительное числовое кольцо *R*

Ниже потребуется знание некоторых свойств алгебраических операций, проводимых в рамках соотносительного числового кольца *R*.

Данное кольцо определяется следующим образом.

Пусть $A \in \Xi$, а $B \in \Omega$. Введём следующие операции:

операции, соотносимые со сложением: $A + A \sim A; \ A + B \sim B; \ B + B \sim A;$

операции, соотносимые с умножением: $AA \sim A, \ AB \sim A, \ BB \sim B;$

операции, соотносимые с вычитанием: $A - A \sim A; \ A - B \sim B; \ B - B \sim A.$

Введённые операции в определённой мере отвечают требованиям системы, определяемой как числовое кольцо. Однако следует отметить, что в предложенной системе для любых двух чисел из $\Xi \cup \Omega$ нельзя, например, определить сумму или разность этих чисел. Можно лишь соотнести сумму или разность этих чисел с чётным или нечётным множествами или с некоторыми их подмножествами. Отсюда название введённого кольца R - соотносительное.

В дальнейшем некоторые свойства частных случаев введённых выше операций будут рассмотрены по мере необходимости.

2.3. Доказательство

Покажем, что $\forall x, y, z$ соотношения (2) – (8), полученные при условии, что $x^k + y^k = z^k$, не могут быть выполнены. Соответственно, не может иметь место и равенство (1).

Если (1) имеет место, то по (2) $w^k \overset{\text{дб}}{=} x + y$. Отсюда, учитывая (2), (5) и (8), значение w должно удовлетворять следующему целочисленному уравнению:

$$w^k = 2uvwk^2\varphi + (u^k + v^k). \tag{9}$$

Известно [4], что если уравнение типа (9) имеет целочисленные корни, то они являются делителями свободного члена. Так как $k \in \Omega$, то $u^k + v^k = (u + v)\sum_{i=0}^{k-1}(-1)^i u^{k-1-i} v^i$. Поэтому искомое значение числа w может быть, по предположению, равно либо

$$w_1 \overset{\text{п}}{=} u + v, \tag{10}$$

либо

$$w_2 \overset{\text{п}}{=} \sum_{i=0}^{k-1}(-1)^i u^{k-1-i} v^i. \tag{11}$$

Случай $w = w_1$

Рассмотрим $w_1^k = (u+v)^k = u^k + \sum_{i=1}^{k-1}\binom{k}{i}u^{k-i}v^i + v^k = u^k + uvk\rho + v^k$, $\rho \in \Omega$. Видно, что w_1^k $\forall \rho \in \Omega$ не сводится к (9). Поэтому, если по (10) $w = w_1$, то $x^k + y^k \neq z^k \ \ \forall x, y, z, k$.

Случай $w = w_2$

Приводимый ниже пример объясняет некоторые операции, используемые ниже.

Пример. Рассмотрим уравнение $x^3 - 6x^2 + 11x - 6 = 0$. Предполагая, например, что $x = x_3 = 3$ является одним из корней приведённого уравнения, уменьшим на единицу степени у неизвестного x, а свободный член разделим на 3. Наше предположение, что $x = x_3 = 3$ является корнем приведённого уравнения, подтвердится, если $x_3^2 - 6x_3 + 11 - 2 = 0$. И действительно, при $x_3 = 3$ последнее соотношение выполняется; очевидно, выполняется и первое соотношение примера.

Пример показывает, что иногда при оценке, является или нет то или иное значение неизвестного корнем некоторого уравнения, можно воспользоваться уравнением, порядок которого на единицу меньше рассматриваемого уравнения.

Так как $w_2 \in (u^k + v^k)$, то, учитывая рассмотренный пример, чтобы при $w = w_2$ выполнялось (9), должно иметь место следующее соотношение:

$$w_2^{k-1} \overset{\text{дб}}{=} u + v + 2uvk^2\varphi. \tag{12}$$

Учитывая (2) – (8), покажем невозможность (9) или (12), если по (11) $w = w_2$.

Введём подмножества Ω_A и Ω_B нечётных чисел: $\Omega_A = \{2A+1,\ A \in \Xi\}$, $\Omega_B = \{2B+1,\ B \in \Omega\}$. Очевидно, $\Omega = \Omega_A \cup \Omega_B$, $\Omega_A \cap \Omega_B = \varnothing$.

***Утверждение* 1.** Если $x \in \Omega_A$, а $z \in \Omega_B$ или наоборот, то $x^k + y^k \neq z^k \quad \forall k \geq 3$.

Пусть $x \sim 2A+1$, $z \sim 2B+1$. Тогда $z - x \sim 2B - 2A \sim 2B \neq v^k$, так как по (2) $v^k \overset{\text{дб}}{\sim} 2^{rk}B, r \geq 1$. Отсюда $x^k + y^k \neq z^k \ \ \forall k \geq 3$ для принятых z и x. При $x \in \Omega_B$ и $z \in \Omega_A$ получим подобное.

Таким образом, для того, чтобы выполнялось (1), $x, z \overset{\text{дб}}{\in} \Omega_A$ или $x, z \overset{\text{дб}}{\in} \Omega_B$.

***Утверждение* 2.** Если $x, z \in \Omega_B$, то $x^k + y^k \neq z^k \quad \forall k \geq 3$.

1. Пусть $r = 1$. Отсюда $y \sim 2^r B_y \sim 2B_y$, а $v \sim 2B_v$, $B_v \leq B_y$. Учитывая (2) и (5), получим:

$$u^k = z - y \overset{\text{п}}{\sim} 2B + 1 - 2B_y \sim 2A + 1, \tag{13}$$

$$w^k = x + y \overset{\text{п}}{\sim} 2B+1+2B_y \sim 2A+1. \qquad (14)$$

Нетрудно показать, что если $\chi^k \sim 2A+1$, то $\chi \sim 2A+1$, если же $\chi^k \sim 2B+1$, то $\chi \sim 2B+1$. Учитывая это, оценим левую и правую части (12). Очевидно, $w^{k-1} \sim (2A+1)^{k-1} \sim 2A+1$, тогда как, учитывая (13), (14) и то, что $uk^2\varphi \in \Omega$, $u+v+2uvk^2\varphi \sim 2A+1+2B_v+2A \sim 2B+1$. Как видно, левая и правая части (12) принадлежат непересекающимся подмножествам Ω_A и Ω_B множества Ω. Отсюда равенство (12) невозможно. Это и доказывает Утверждение 2 при $r=1$.

2. Пусть теперь $r \geq 2$, т.е. $y \sim 2^{\geq 2}B_y$, а $v \sim 2^{\geq 2}B_v$, $B_y, B_v \in \Omega$. Учитывая (2) и (5), имеем:

$$u^k = z - y \overset{\text{п}}{\sim} 2B+1-2^{r\geq 2}B_y \sim 2B+1-2A \sim 2B+1, \qquad (15)$$

$$w^k = x + y \overset{\text{п}}{\sim} 2B+1+2^{r\geq 2}B_y \sim 2B+1+2A \sim 2B+1. \qquad (16)$$

Так как $k-1 \in \Xi$, то из (16) имеем: $w^{k-1} \sim (2B+1)^{k-1} \sim 2A+1$. С другой стороны, учитывая (15), $u+v+2\cdot 2^{r\geq 2}B_v uk^2\varphi \sim 2B+1+2A+2A \sim 2B+1$. Как видно, левая и правая части (12) принадлежат непересекающимся подмножествам Ω_A и Ω_B. Это и доказывает Утверждение 2 при $r \geq 2$, так как равенство (12) невозможно.

Таким образом, показано, что если $x, z \in \Omega_B$, т.е. x и z принимают значения 3, 7, 11, 15, 19…, то $\forall k \geq 3$ и $\forall y$ $x^k + y^k \neq z^k$. Утверждение 2 доказано.

***Утверждение* 3.** Если $x, z \in \Omega_A$, то $x^k + y^k \neq z^k \quad \forall k \geq 3$.

Очевидно, $\Omega_A = \{\Omega_{A_i},\ i \geq 2,\ \Omega_{A_i} = \{2^i B+1, B \in \Omega\}\}$, при этом $\Omega_{A_i} \cap \Omega_{A_j} = \varnothing \ \forall i \neq j$.

Ввиду $\Omega_{A_i} \cap \Omega_{A_j} = \varnothing \ \forall i \neq j$ (1) может иметь место быть лишь при $x, z \in \Omega_{A_i}$, $i \geq 2$. Докажем справедливость утверждения 3 для каждого подмножества Ω_{A_i}, $i \geq 2$.

1. Предварительно определим некоторые свойства соотносительного кольца *R*.

Введём обозначения: $B_A \in \Omega_A$ и $B_B \in \Omega_B$. Тогда $\forall B \in \Omega$ имеем:

$$2^{\geq 2}B - B_\chi \sim \begin{cases} B_A, & \text{если } B_\chi \sim B_B, \\ B_B, & \text{если } B_\chi \sim B_A, \end{cases} \qquad (17)$$

$$2^{\geq 2}B + B_\chi \sim \begin{cases} B_B, & \text{если } B_\chi \sim B_B, \\ B_A, & \text{если } B_\chi \sim B_A. \end{cases} \qquad (18)$$

Докажем первое соотношение (17). Так как $B_\chi \sim B_B$, то $B_\chi \sim 2B+1$. Отсюда $2^{\geq 2}B - B_\chi \sim 2A-2B-1 \sim 2A-2B-2+1 \sim 2B-2B+1 \sim 2A+1 \sim B_A$. Аналогично доказываются другие соотношения (17) и (18).

Также очевидным образом доказывается справедливость следующих соотношений:

$$2B - B_\chi \sim \begin{cases} B_B, & \text{если } B_\chi \sim B_B, \\ B_A, & \text{если } B_\chi \sim B_A, \end{cases} \tag{19}$$

$$2B + B_\chi \sim \begin{cases} B_A, & \text{если } B_\chi \sim B_B, \\ B_B, & \text{если } B_\chi \sim B_A. \end{cases} \tag{20}$$

2. Произвольным образом выберем $i \geq 2$. Соответственно, $x, z \overset{\text{дб}}{\sim} 2^i B + 1$.

2.1. Предположим сначала, что $y \sim 2^l B_y, 1 \leq l < i-1$. Соответственно, $\nu \sim 2^{1 \leq l < i-1} B_\nu$. При принятых условиях, учитывая (17) и (18), получим:

$$u^k = z - y \sim 1 + 2^l (2^{i-l} B - B_y) \sim 1 + 2^l \begin{cases} B_A, & \text{если } B_y \sim B_B, \\ B_B, & \text{если } B_y \sim B_A, \end{cases} \tag{21}$$

$$w^k = x + y \sim 1 + 2^l (2^{i-l} B + B_y) \sim 1 + 2^l \begin{cases} B_B, & \text{если } B_y \sim B_B, \\ B_A, & \text{если } B_y \sim B_A. \end{cases} \tag{22}$$

Учитывая допущения и (21), оценим правую часть (9): $u^k + v^k + 2\Phi \sim 1 + 2^l \begin{cases} B_A \\ B_B \end{cases} + 2^{lk} B_\nu^k + 2 \cdot 2^l B \sim 1 + 2^l \begin{cases} B_A \\ B_B \end{cases} + 2^l A + 2^l A \sim 1 + 2^l \begin{cases} B_A \\ B_B \end{cases}$. Сравнивая полученную величину с w^k (22) и учитывая применявшиеся выше методы, нетрудно заметить, что они принадлежат непересекающимся подмножествам множества Ω. Вследствие этого равенство (9) для рассматриваемого случая не может иметь место и, соответственно, не может иметь место (1).

2.2. Пусть $l = i-1$, т.е. $y \sim 2^{i-1} B_y$, а $\nu \sim 2^{i-1} B_\nu$. Учитывая (19) и (20), имеем:

$$u^k = z - y \sim 1 + 2^{i-1} (2B - B_y) \sim 1 + 2^{i-1} \begin{cases} B_B, & \text{если } B_y \sim B_B, \\ B_A, & \text{если } B_y \sim B_A, \end{cases} \tag{23}$$

$$w^k = x + y \sim 1 + 2^{i-1} (2B + B_y) \sim 1 + 2^{i-1} \begin{cases} B_A, & \text{если } B_y \sim B_B, \\ B_B, & \text{если } B_y \sim B_A. \end{cases} \tag{24}$$

С учётом (23) оценим правую часть (9): $u^k + v^k + 2\Phi \sim 1 + 2^{i-1} \begin{cases} B_B \\ B_A \end{cases}$. Но, как видно из (24), $w^k \sim 1 + 2^{i-1} \begin{cases} B_A \\ B_B \end{cases}$ соответственно, т.е. левая и правая части (9) принадлежат непересекающимся подмножествам множества Ω. Поэтому равенство (9) и, соответственно, (1) невозможны.

2.3. Пусть теперь $l = i$, т.е. $y \sim 2^i B_y$, а $\nu \sim 2^i B_\nu$. Очевидно, $u^k = z - y \sim 2^i B + 1 - 2^i B_y \sim \sim 2^i A + 1$, а $w^k = x + y \sim 2^i A + 1$. Выше отмечалось, что если $\chi^k \sim 2^i A + 1$, то $\chi \sim 2^i A + 1$. Поэтому в рассматриваемом случае $w^{k-1} \sim 2^i A + 1$. Однако правая часть (12) $u + v + 2\Phi / w \sim \sim 2^i A + 1 + 2^i B_\nu + 2 \cdot 2^i B \sim 2^i B + 1$ принадлежит подмножеству, которое не пересекается с подмножеством, включающим w^{k-1}. Поэтому (12) невозможно, невозможно и (1).

2.4. Наконец, пусть $l = i + s,\ s \geq 1$, т.е. $y = 2^{i+s} B_y$, а $\nu = 2^{i+s} B_\nu$. Очевидно, $u^k = z - y \sim$ $\sim 2^i B + 1 - 2^{i+s} B_y \sim 2^i B + 1$, $w^k = x + y \sim 2^i B + 1$. Отсюда $u + v + 2\Phi / w \sim 2^i B + 1 + 2^{i+s} B_\nu + 2 \cdot 2^{i+s} B \sim$ $\sim 2^i B + 1$, а $w^{k-1} \sim (k-1) 2^i B + 1 \sim 2^i A + 1$. Как видно, левая и правая части (12) находятся в непересекающихся подмножествах множества Ω. Поэтому (12) невозможно, невозможно и (1).

Утверждение 3 доказано.

Таким образом, показано, что какие бы значения не принимали x и z, находясь в подмножестве $\Omega_B = \{2B+1,\ B \in \Omega\}$ или в $\Omega_{A_i} = \{2^i B + 1,\ B \in \Omega, i \geq 2\}$, равенство (1) оказывается невозможным. Но так как $\Omega = \Omega_B \cup \sum_{i \geq 2} \Omega_{A_i}$, то вывод о невозможности (1) при $(x, y, z, k) = 1$ справедлив $\forall x, y, z, k$.

III. Доказательство случая II теоремы

Введение дополнительного условия иногда усложняет решение исследуемой задачи, но порой существенно упрощает. В данном случае введение условия $z \equiv 0 (\mathrm{mod} k)$ упрощает доказательство рассматриваемой теоремы.

3.1. Некоторые предварительные результаты

3.1.1. Отметим сначала возможную причину, которая привела многих исследователей к необходимости доказательства теоремы для случая I, когда $x \wedge y \wedge z \neq 0 (\mathrm{mod} k)$, и случая II, когда $x \vee y \vee z \equiv 0 (\mathrm{mod} k)$.

Известно, что если (1) имеет место быть, то, учитывая приведённую в [3] лемму, из $x^k \overset{\text{п}}{=} z^k - y^k$, как было отмечено в (2), можно получить следующие соотношения:

$$x \overset{\text{дб}}{=} uG, \quad u^k \overset{\text{дб}}{=} z - y, \qquad G^k \overset{\text{дб}}{=} \sum_{i=0}^{k-1} z^{k-1-i} y^i, \tag{25}$$

а из $y^k \overset{\text{п}}{=} z^k - x^k$ - следующие:

$$y \overset{\text{дб}}{=} vP, \quad v^k \overset{\text{дб}}{=} z - x, \qquad P^k \overset{\text{дб}}{=} \sum_{i=0}^{k-1} z^{k-1-i} x^i . \tag{26}$$

Согласно лемме, справедливость (25) и (26) следует в силу $(u, G) = 1$ и $(v, P) = 1$.

Но при $z \overset{\text{п}}{\equiv} 0 (\mathrm{mod} k^{i \geq 1})$ подобные выражения для числа z невозможно получить, так как в выражении $z^k \overset{\text{дб}}{=} (x+y) \sum_{i=0}^{k-1} (-1)^i x^{k-1-i} y^i$ числа $(x+y)$ и $\sum_{i=0}^{k-1} (-1)^i x^{k-1-i} y^i$ - не взаимно простые.

Последнее следует из следующего: если числа S и T взаимно простые, то

$$S^k + T^k \equiv \begin{cases} 0(\mathrm{mod}\, k^{j+1}), \text{ если } (S+T) \equiv 0(\mathrm{mod}\, k^j),\ j \geq 1; \\ 0(\mathrm{mod}\, k^0), \text{ если } (S+T) \equiv 0(\mathrm{mod}\, k^0). \end{cases} \quad (27)$$

Действительно, ввиду $k \in \Omega$ имеем:

$$(S+T-T)^k + T^k = \sum_{i=0}^{k-1} (-1)^i \binom{k}{i} (S+T)^{k-i} T^i =,$$
$$= (S+T) \sum_{i=0}^{k-1} (-1)^i \binom{k}{i} (S+T)^{k-1-i} T^i.$$

В последнем выражении каждый из $(k-1)$ первых членов суммы включает множитель $(S+T)$, а последний член суммы – множитель $\binom{k}{k-1} = k$. Отсюда следует справедливость утверждения (27) и, как следствие, вывод, что $((x+y), \sum_{i=0}^{k-1} (-1)^i x^{k-1-i} y^i) \neq 1$, если $z \overset{\text{п}}{\equiv} 0(\mathrm{mod}\, k^{i \geq 1})$.

3.1.2. ***Утверждение* 4.** Если $z \overset{\text{п}}{\equiv} 0(\mathrm{mod}\, k^{i \geq 1})$, то (1) может иметь место лишь при $i \geq 2$.

Действительно, из (25) и (26) имеем:

$$\begin{array}{l} z = x + V,\ V = v^k; \\ z = y + U,\ U = u^k. \end{array} \quad (28)$$

Отсюда

$$2z = (x+y) + (U+V) \quad (29)$$

Учитывая (27), $x + y \overset{\text{дб}}{\equiv} 0(\mathrm{mod}\, k^{ik-1})$, $U + V \equiv 0(\mathrm{mod}\, k^{0 \vee \geq 2})$, поэтому $z \overset{\text{дб}}{\equiv} 0(\mathrm{mod}\, k^{i \geq 2})$.

3.2. Доказательство

Возведём левую и правую части первого равенства (28) в степень k. Ввиду $k \in \Omega$ получим:

$$z^k = x^k + \sum_{i=1}^{k-1} \binom{k}{i} x^{k-i} V^i + V^k = x^k + kzxVH(x,V,k) + V^k,$$

где $H(x,V,k)$ - некоторая целочисленная функция от параметров x, V и k.

Аналогично, из второго равенства (28) можно получить следующее соотношение:

$$z^k = y^k + \sum_{i=1}^{k-1} \binom{k}{i} y^{k-i} U^i + U^k = y^k + kzyUH(y,U,k) + U^k.$$

Из двух последних соотношений следует, что

$$2z^k = (x^k + y^k) + kz[xVH(x,V,k) + yUH(y,U,k)] + (U^k + V^k), \quad (30)$$

Отсюда, если предположить, что справедливо (1), должно иметь место соотношение:

$$z^k \overset{\text{дб}}{=} kz[xVH(x,V,k) + yUH(y,U,k)] + (U^k + V^k), \quad (31)$$

Однако найти число z, которое удовлетворяло бы и (29), и (31), невозможно.

Пусть $z \overset{\text{п}}{\equiv} 0(\mathrm{mod}\, k^i,\ i \geq 2)$.

Предположим сначала, что $[xVH(x,V,k)+yUH(y,U,k)]\overset{\text{п}}{\neq}0(\mathrm{mod}k)$. Отсюда соотношение (31), учитывая (27), может иметь место лишь при $(U+V)\equiv 0(\mathrm{mod}k^{i})$. Далее, нетрудно заметить, что соотношение (31) можно соотнести с многочленом k-й степени с неизвестным z. Известно [4], что если многочлен типа (31) имеет целочисленные корни, то они являются делителями свободного члена. Поэтому искомое значение числа z может быть равным либо

$$z_1\overset{\text{п}}{=}U+V,$$

либо

$$z_2\overset{\text{п}}{=}\sum_{i=0}^{k-1}(-1)^{i}U^{k-1-i}V^{i}.$$

Однако ни z_1, ни z_2 не могут обеспечить предполагаемое равенство (1).

При $z=z_2$ высказанное предположение очевидно, так как, учитывая (27) и (31), $\sum_{i=0}^{k-1}(-1)^{i}U^{k-1-i}V^{i}\equiv 0(\mathrm{mod}k^{1})$, тогда как $z\overset{\text{дб}}{\equiv}0(\mathrm{mod}k^{\geq 2})$. Предположение справедливо и при $z=z_1$, так как при $z=z_1$ соотношение (29) приведётся к виду $U+V=x+y$, невозможное для x,y и z, при которых возможно (1). Действительно, данные числа можно объединить соотношением $x+y=z+\Phi$, из которого, учитывая (25) и (26), можно получить: $x=U+\Phi$, а $y=V+\Phi$. Видно, что $x>U$, а $y>V$. Поэтому $U+V\neq x+y$, а (1) не может иметь место быть.

При $[xVH(x,V,k)+yUH(y,U,k)]\overset{\text{п}}{\equiv}0(\mathrm{mod}k^{j\geq 1})$ доказательство того, что многочлен (31) не может иметь целочисленных корней, удовлетворяющих (1), осуществляется подобным образом.

Так, при данном предположении, как видно из (31), $(U^{k}+V^{k})\overset{\text{дб}}{\equiv}0(\mathrm{mod}k^{i+j+1})$. Поэтому целочисленным корнем может быть либо $\bar{z}_1\overset{\text{п}}{=}U+V$, либо $\bar{z}_2\overset{\text{п}}{=}\sum_{i=0}^{k-1}(-1)^{i}U^{k-1-i}V^{i}$. Но, учитывая (27), $\bar{z}_1\overset{\text{дб}}{\equiv}0(\mathrm{mod}k^{i+j})$, а $\bar{z}_2\overset{\text{дб}}{\equiv}0(\mathrm{mod}k^{1})$, тогда как выше было принято, что $z\overset{\text{п}}{\equiv}0(\mathrm{mod}k^{i})$. Отсюда ни $\bar{z}_1$, ни $\bar{z}_2$ не могут обеспечить выполнение (1).

Таким образом, доказано, что и случае, когда $z\overset{\text{п}}{\equiv}0(\mathrm{mod}k^{i\geq 1})$, уравнение (1) не имеет целочисленных решений.

Литература

1. *Wiles A.* Modular elliptic curves and Fermat' s last theorem – Annals of Mathematics. 1995, v.141, p.443-551.
2. *Титенко И.М.* Обнуление мифов Большой теоремы Ферма // «Академия Тринитаризма», М., Эл № 77-6567, публ.25198, 18.02.2019.
3. *Постников М.М.* Введение в теорию алгебраических чисел. М.: Наука, 1982. С. 22.
4. *Курош А.Г.* Курс высшей алгебры. М.: Физматгиз, 1962.