УДК:511.521

Сражидинов Адил, к.ф-м.н., доцент,
Кызыл-Кийский педагогический институт,
Баткенский государственный университет,
г. Кызыл-Кия, Кыргызская Республика

ЭЛЕМЕНТАРНОЕ ДОКАЗАТЕЛЬСТВО ВЕЛИКОЙ ТЕОРЕМЫ ФЕРМА, АДАПТИРОВАННОЕ ДЛЯ ФАКУЛЬТАТИВНОГО КУРСА ШКОЛЬНИКОВ

Великая теорема Ферма носит имя талантливого математика, впервые заметившего в 1637 году всю её глубину, и красоту да и простоту формулировки, требующие не одинарных подходов мысли того времени. В течение более 350 лет доказать её не удавалось никому. Наконец-то, в 1997 году Гёттингенским Королевским обществом официально признанно, что известный математик Эндрю Уайса доказал Великую теорему Ферма. Несмотря, на публикацию доказательства (в объеме страниц 100), требующего специальных знаний из теории чисел, представляет интерес найти насколько упрощённое доказательство, о которых упоминал родоначальник проблемы. К такому классу доказательств, наверное, можно отнести предлагаемый нами способ. И вкратце можно описать его следующим образом, исходя из уравнения $x^n+y^n+z^n=0$, любая из целочисленных переменных x,y,z представляется в виде произведения двух взаимно простых чисел, которые в свою очередь взаимно простые с остальными множителями подобных произведений. Рассматривая каждый из двух логически возможных случаев, т.е. либо произведение xyz кратно числу простому показателю n, либо это произведение не кратно числу n, далее показывается невозможность указанных случаев.

Ключевые слова: Великая теорема Ферма, «Арифметика» Диофанта, метод от противного, теория чисел, взаимно простые числа, доказательства частных случаев и общего: П. Ферма (n=4) Л. Эйлер (n=3), Л. Дирихле, А. Лежандр (n=5), Г, Ламе, А. Лебег (n=7), Э. Куммер (n≤100), Э. Уайлс (для всех n ≥3).

Сражидинов Адил, ф-м.и.н., доцент, Кызыл-Кыя
педагогикалык институту, Баткен мамлекеттик
университети, Кызыл-Кия ш., Кыргыз Республикасы

МЕКТЕП ОКУУЧУЛАРЫНЫН ФАКУЛЬТАТИВДИК КУРСУНА ЫНГАЙЛАШТЫРЫЛГАН ФЕРМАНЫН УЛУУ ТЕОРЕМАСЫНЫН ЭЛЕМЕНТАРДЫК ДАЛИЛДӨӨСҮ

Ферманын улуу теоремасынын аталышы теореманы эң алгачкы болуп 1637-жылы байкаган таланттуу математиктин ысмы менен байланыштуу. П. Ферма теореманын мазмунунун жөнөкөйлүгүн, айтылышынын кооздугун жана анын логикалык тереңдигин түшүнгөн. 350 жыл бою далилденбей келишинин өзү эле ага өзгөчөлөнгөн жол-жолбонун керек экендигинен кабар берет. Жүрүп олтуруп, 1995-жылы белгилүү математик Э. Уайлс Ферманын улуу теоремасын далилдеп, кубануу бактысына туш келди. 1997-жылы математиктердин Гёттинген коому Ферманын улуу теоремасын далилдегендигин жана далилдөөнүн Э.Уайлсга таандык экендигин жар салды. Басмадан (колому 100 беттей) чыккан менен тушунууго сандар теориясынын акыркы жетишкендиктерин пайдалануу талап кылынат. Ошондуктан проблеманын баштоочусу П.Ферманын оюндагыдай жөнөкөй далилдөө көпчулукту сөзсуз кызыктырат. Биз сунуштаган ыкма ушул багыттагы далилдөөлөрдүн алгачкыларынан болот деген ойдобуз. Далилдөөгө кыскача токтоло кетсек:

$x^n+y^n+z^n=0$ теңдемесине катышкан бүтүнсандык маанилерге ээ болгон өзгөрмөлөрдүн ар бирин өз ара жөнөкөй болгон эки сандын көбөйтүндүсү түрүндө көргөзөбүз жана көйбөтүүчүлөрдүн ар бири башка өзгөрмөлөдүн көбөйтүүчүлөрү менен өз ара жөнөкөй сандар болот. Андан ары, логикалык жактан мүмкүн болгон эки учурдун, б.а. xyz көбөйтүндүсү жөнөкөй көрсөткуч n ге эселүү, же xyz тин n санына эселүү эмес болгон учурлардын ар биринин мүмкүн эместигине алып келет.

Негизги сөздөр: Ферманын улуу теоремасы, Диофанттын «Арифметикасы», каршысынан далилдөө методу, сандар теориясы, өз ара жөнөкөй сандар, жеке жана жалпы учурлардын далилдениши: П. Ферма (n=4), Л.Эйлер (n=3), Л.Дирихле, А.Лежандр (n=5), А.Лебег, Г. Ламе (n=7), Э.Куммер (n ≤ 100), Э.Уайлс (бардык n≥3).

Srazhidinov Adil, candidate of physical and mathematical sciences, associate professor,
Kyzyl-Kiya pedagogical Institute, Batken state university,
Kyzyl- Kiya c., Kyrgyz Republic

AN ELEMENTARY PROOF OF THE GREAT FARM'S THEOREM, ADAPTED FOR THE OPTIONAL COURSE OF PUPILS

Fermat's great theorem bears the name of a talented mathematician who first noticed in 1637 all its depth, beauty and simplicity non-uniform approaches to the thought. For over 350 years no one has been able to prove it. Finally, in 1997 the Great Fermat Theory was proved by famous mathematician Andrew Wiles officially recognized by the Royal Society of Gottingen. Despite the publication of evidence (about 100 pages) that requires special knowledge from Number Theory, it is of interest to find how simplified the evidence mentioned by the originator of the problem. To this class of evidence, probably, we can refer the method proposed by us. And we can be briefly described as follows from the equation $x^n+y^n+z^n=0$ any of the integer variables x, y, z is represented as the product of two mutually prime numbers, which in turn are mutually simple with other factors of similar products. Further, looking through each of the two logically possible cases, i.e., either the product xyz is a multiple of the number of prime exponent's n, or this product is not a multiple of the number n, the impossibility of any of these cases in shown.

Key words: Great Fermat`s Theorem, «Arithmetic» of Diophantus, Method on the contrary, Number Theory, Mutually prime numbers, Proof of particular cases and general: P.Fermat (n=4), L.Euler (n=3), L.Dirichlet, A.Legendre (n=5), A.Lebesgue, G.Lame (n=7), E.Kummer (n≤100), E.Wiles (for all n ≥ 3)

Введение. Значение и история Великой теоремы Ферма довольно в популярной форме приведены в книге Сайман Сингх [1].

Начнем с формулировки предположения великого математика П. Ферма, записавшего в 1637 году в форме тезисов на краях страниц "Арифметики" Диофанта.

Теорема. При любом натуральном числе n≥3 уравнение

$$x^n+y^n+z^n = 0 \qquad (1)$$

не может иметь решений в целых числах (отличных от нуля).

Ферма к удивлению добавил, что он «нашел поистине удивительное доказательство этого предположения, но здесь слишком мало место , чтобы его поместить». Из-за простоты к пониманию и красоты формулировки, да и отсутствия доказательства теоремы, захватило многих, начиная с математиков кончая до школьников, увлеченных кажущейся простой головоломкой. Даже 1908 году Геттингенским математическим обществом была объявлена

премия в размере 100 тысяч марок тому, кто даст полное доказательство теоремы. Элементарного доказательства Великой теоремы Ферма нет ни одного показателя n≠4, если же не считать элементарным доказательство автора [4] при n=3.

Эйлером в 1768 году доказан случай n=3, а случай n=5 в 1825 году почти одновременно доказали Дирихле и Лежандр. Доказательство Лежандра упростил Племель в 1912 году. Для n=7 теорема Ферма доказана Ламе в 1839 году. Доказательство последнего почти сразу было усовершенствовано Лебегом. Самые серьезные исследования Великой теоремы Ферма связаны с именем известного математика Куммера, доказавшего ее разом для всех n≤100, исключая нерегулярные простые числа n=32, 59,67. Однако, и с этими исключениями скоро удалось ему справиться "по одиночке ". В 1934 году математик Г. Вандивер упростил условия Куммера, и в этом варианте при помощи ЭВМ доказал теорему для всех n≤100 000.

В 1900 году выдающийся математик Гильберт в историческом докладе на II Международном конгрессе математиков в Париже сформулировал двадцать три проблемы, среди них – Великая теорема Ферма. По мнению Гильберта эти проблемы имеют наиболее значение для развития математики.

Наконец-то, в 1995 году известным математиком Эндрю Уайлсом [2,3]. доказана Великая теорема Ферма. Последствии 27 июня 1997 года Э. Уайлсу вручена вышеназванная премия Вольфскеля и Великая теорема Ферма официально признана доказанной. О своем достижении Уайлс оценил скромна, что ему выпало счастье осуществить в взрослой жизни то, что было его мечтой в детстве [1].

''Несмотря на публикацию доказательства (в объеме страниц 100) Уайлса, существует много математиков, которые уверены в том, что им удастся открыть первоначальное доказательство Ферма [1]''. Мы считаем, что любая публикация в данном направление, в том числе и наша, представляет определенный научный, да и исторический интерес.

Теорема при n=4 впервые доказана радоначальником проблемы знаменитым математиком Ферма [5]. В последствии этот случай рассмотрен и другими математиками [1,6,7]. Поэтому будем считать n≠4 и n≥3. Тогда теорема сводится к случаю, что n- простое число и n≥3.

Доказательство проводим методом от противного. Предположим, что (1) имеет некоторое решение x,y и z в целых числах, отличных от нуля, поэтому в равенстве (1) можем считать, что числа x,y и z взаимно просто

$$D(x,y)=1,\ D(x,z)=1,\ D(y,z)=1. \qquad (2)$$

Пользуемся обозначениями, т.е. будем писать:

1) $a \equiv b$, если целое число a делится на целое число b без остатка ;
2) $a \not\equiv c$, если целое число a не делится на целое число c;
3) $\omega(a)$ = p,если для целого числа a выполняются соотношения $a \equiv n^p$, $a \not\equiv n^{p+1}$ при некотором натуральном числе p;
4) $\omega_m(a)= p$, если целое число a при данном натуральном числе m, удовлетворяет условию: $a \equiv m^p$, $a \not\equiv m^{p+1}$.

А так же докажем две леммы.

Лемма 1. При любом простом числе n≥3 сумма $C_{n-1}^{k}+(-1)^{k-1}$ кратна числу n, где k=1,2, …,(n-1)/2, $C_{n-1}^{k}=(n-1)!/[k!(n-1-k)!]$.

Доказательство. При k=1, очевидно, что $C_{n-1}^{1}+1=n$, отсюда , $C_{n-1}^{1}+1 \equiv n$.

Пусть теперь k=2. Тогда $C_{n-1}^{2}-1=(n-1)(n-2)/2! -1 = (n^2-3n+2-2)/2 =n(n-3)/2$, т.е

$$. C_{n-1}^{2} -1= n(n-3)/2. \qquad (3)$$

Так как n - простое число и n≥3, то n - нечетное, следовательно , (n-3) – четное число, значит в равенстве (3) заключаем, что $C_{n-1}^{2}-1 \equiv n$.

Пусть теперь k ≤ (n-1)/2 и k=2m, т.е. k – четное число. Тогда непосредственно получаем, что

C_{n-1}^{2m} -1 =(n-1)(n-2)…(n-2m)/(2m)! -1=(n^{2m}+a_1 n^{2m-1}+…+a_{2m-1}n+(2m)!)/(2m)! -

-1= n(n^{2m-1}+$a_1 n^{2m-2}$+… +a_{2m-1})/(2m)!, т.е.

$$C_{n-1}^{2m} -1 = n(n^{2m-1}+a_1 n^{-2}+\dots +a_{2m-1})/(2m)!, \quad (4)$$

где $a_1, a_2, \dots, a_{2m-1}$, a_{2m}- определяются формулами Виета:

$n_1+n_2+\dots+n_{2m}= - a_1$,

$n_1n_2+n_1n_3+\dots+n_{2m-1}n_{2m} = a_2, \dots$,

$n_1n_2\dots n_{2m}= a_{2m}$

при $n_1=1$, $n_2=2,\dots,n_{2m} = 2m$. Поэтому числа, a_1, a_2 , …, a_{2m}- целые числа. Так как n - простое число и n>2m, что из равенства (4) следует, что число внутри квадратной скобки в правой части (4) кратно (2m)!, следовательно, имеет место

$C_{n-1}^{2m} \equiv$ n. (5) Очевидно, что получаем

$$[C_{n-1}^{2m} -1]+ [C_{n-1}^{2m-1} +1]= [C_{n-1}^{2m} +C_{n-1}^{2m-1}], \quad (6)$$

$C_{n-1}^{2m} +C_{n-1}^{2m-1}$=(n-1)(n-2)…(n-2m)/(2m)! + (n-1)(n-2)…(n-2m+1)/(2m-1)!=[(n--1)(n-2)…(n-2m+1)/(2m-1)!] [(n-2m)+ 2m], т.е.

$$C_{n-1}^{2m} +C_{n-1}^{2m-1}= nC_{n-1}^{2m-1}. \quad (7)$$

Поэтому из (6) с учетом соотношений (5) и (7) следует, что $C_{n-1}^{2m-1}+1 \equiv$ n.

Лемма доказана. Рассмотрим разложение :

$t^{n-1}–t^{n-2}v+t^{n-3}v^2\dots-tv^{n-2}+v^{n-1}=(t+v)^{n-1}+\alpha_1 tv(t+v)^{n-3}+\alpha_2(tv)^2(t+v)^{n-5}+\dots+ \alpha_p(tv)^p$, (8)

где p=(n-1)/2, относительно которого справедлива

Лемма 2. Пусть 3≤n – простое число. Тогда равенством (8) однозначно определяются коэффициенты α_1 , α_2 ,…, α_p и все они целые, причем кратные простому числу n .

Доказательство. Приравнивая коэффициенты при t^{n-1} , $t^{n-2}v$,…, tv^{n-2} обоих частей (8), получаем при t^{n-1} равенство 1=1, а при других :

$$-1= C_{n-1}^{1} + \alpha_1 , \ 1= C_{n-1}^{2} + \alpha_1 C_{n-2}^{1} + \alpha_2 , \ -1= C_{n-1}^{3} + \alpha_1 C_{n-2}^{2} + \alpha_2 C_{n-3}^{1} + \alpha_3 , \dots ,$$

$$(-1)^p = C_{n-1}^{p} + \alpha_1 C_{n-2}^{p-1} + \alpha_2 C_{n-3}^{p-2} + \alpha_3 C_{n-4}^{p-3} +\dots+ \alpha_p \ , \quad (9)$$

где p=(n-1)/2. Из первого уравнения системы (9) имеем α_1= -n, отсюда, $\alpha_1 \equiv$ n .

Аналогично из второго уравнения системы (9) получаем:

$$\alpha_2 = - (C_{n-1}^{2}-1) + n C_{n-2}^{1}. \quad (10)$$

Согласно лемме 1 $C_{n-1}^{2}-1 \equiv$ n, поэтому $\alpha_2 \equiv$ n. В равенстве (10) замечаем, что $\alpha_2 = C_n^2$, в частности , $\alpha_2 >0$.

Записав третье уравнение из (9) в виде

$$- [1+C_{n-1}^{3}] = \alpha_1 C_{n-2}^{2} + \alpha_2 C_{n-3}^{1} + \alpha_3 \quad (11)$$

и учитывая, что левая часть (11) согласно лемме1 кратна числу n и $\alpha_1 \equiv$ n, $\alpha_2 \equiv$ n, заключаем $\alpha_3 \equiv$ n. Аналогично для остальных, $\alpha_i \equiv$ n, i=1,2,...,(n-1)/2. Лемма 2 доказана. Полагая в тождестве (8) v= - t, имеем n $t^{n-1}= \alpha_p(-t^2)^p$, откуда $\alpha_p = (-1)^p$ n, p=(n-1)/2 Значит нами, в частности, получены, что α_1= -n, $\alpha_2= C_n^2$, α_p= = $(-1)^p$ n, и, следовательно, $\alpha_1<0$, $\alpha_2>0$. По желанию можно было бы определить знаки и других коэффициентов, но нам это не понадобится.

Продолжим доказательство теоремы. Из равенства (1) непосредственно получаем

$$-x^n=(y+z)L(y,z),\ y^n=(x+z)L(x,z),\ -z^n=(x+y)L(x,y), \quad (12)$$

где L(t,v) – двумерная функция, определяемая правой частью (8), т.е.

$$L(t,v)= (t+v)^{n-1}+\alpha_1 tv(t+v)^{n-3}+ \alpha_2(tv)^2(t+v)^{n-5}+\dots+ \alpha_p(tv)^p, \quad (13)$$

где p=(n-1)/2. В первом из равенств (12) замечаем, что все простые множители суммы y+z так же являются множителями числа x. Аналогично, из других равенств (12) следует, что все простые множители сумм x+z и x+y так же являются простыми множителями чисел y и z соответственно. Поэтому согласно соотношениям (2) числа x+y , x+z, y+z являются взаимно простыми:

$D(x+y,x+z) =1$, $D(x+y,y+z)=1$, $D(x+z,y+z)=1$. (14)

Покажем, что сумма y+z и число L(y,z) из (12) взаимно простые. Действительно, если l – какой-либо их общий делитель и $l \neq 1$, то на l делится без остатка произведение yz (его коэффициент равен ± n). Прежде всего заметим, что y+z некратно числу n согласно соотношению (12). Поэтому любой общий делитель чисел y+z и L(y,z) отличен от l. Далее, если предположить, что $D(y+z,L(y,z))=l$ и $l \neq 1$, то на число l делится без остатка произведения yz. Тогда приходим к противоречию тому , что $D(y,z)=1$. Поэтому числа y+z и L(y,z) взаимно простые и , следовательно, $D(x_1, x_2)=1$. Аналогично получаем $D(z_1,z_2)=1$, $D(y_1, y_2)=1$, $D(x_1, x_2)=1$. (15)

Теперь покажем , что из равенства (1) следует равенство $u^n = n(x+y)(x+z)(y+z)\, r$, где $u = x+y+z$, r – некоторое целое число, которое определяется ниже.

Сначала покажем, что

$(x+y+z)^n \equiv (x+y)$, $(x+y+z)^n \equiv (x+z)$, $(x+y+z)^n \equiv (y+z)$. (16)

Очевидно, имеем

$(x+y+z)^n=(x+y)^n+z^n+ \sum_{i=1}^{n-1} C_n^i (x+y)^i z^{n-I}$, (17)

$(x+y)^n + z^n + \sum_{i=1}^{n-1} C_n^i (x+y)^i z^{n-I} = x^n +y^n +z^n +\sum_{i=1}^{n-1} C_n^i [(x+y)^i z^{n-1} + x^i\, y^{n-i}]$. (18)

Из равенств (12) и (17) заметим, что число u^n кратно сумме x+y ,т.е. имеет место первое из (16). Аналогично получаем остальные равенства (16). Согласно (15) имеем

$u^n \equiv (x+y)(x+z)(y+z)$. (19)

Очевидно , что из равенств(1) и (18) имеем

$(x+y+z)^n =\sum_{i=1}^{n-1} C_n^i [(x+y)^i z^{n-1} + x^i\, y^{n-i}]$. (20)

Так как C_n^i, i=1,2,…., n-1, кратен числу n , то из равенства (20) получаем

$u^n \equiv n$. (21)

Логически возможны только два случая:

Случай 1. Ни одно из чисел x,y и z не кратно числу n , т.е.

$xyz \not\equiv n$. (22)

В случае 1, как показано выше , тем более

$(x+y)(x+z)(y+z) \not\equiv n$. (23)

Поэтому из соотношений (19) и (23) вытекает, что

$u^n \equiv n(x+y)(x+z)(y+z)$. (24)

Обозначим r число $u^n / [n(x+y)(x+z)(y+z)]$, т.е. $r=(x+y+z)^n/[(x+y)(x+z)(y+z)]$.

Из соотношения (24) следует, что число r - целое число, и, следовательно

$(x+y+z)^n= n\,(x+y)(x+z)(y+z)r$. (25)

Теперь хотим показать, что число r взаимно простое с числами x, y и z. Из равенств (12) замечаем, что

$y+z=x_1^n$, $x+z=y_1^n$, $x+y=z_1^n$, (26)

$x_2=x/x_1$, $y_2=y/y_1$, $z_2=z/z_1$, (27)

где целые числа x_2, y_2 , z_2 определяются в соответствии с равенствами (12)):

$-x_2^n = L(y,z)$, $-y_2^n = L(x,z)$, $-z_2^n = L(x,y)$. (28)

Из равенства (26) непосредственно получим: $x+x_1^n = u$, $y+y_1^n = u$, $z+z_1^n = u$

$-x_2+x_1^{n-1} = u/x_1$, $y_2+y_1^{n-1} = u/y_1$, $z_2+z_1^{n-1} = u/z_1$. (29)

В левых частях равенств (29) стоят целые числа, поэтому в их правых частях так же должны стоять целые числа, т.е. числа u/x_1 , u/y_1, u/z_1 – целые числа . Тогда равенство (25) принимает вид:

$$u^n=nx_1^n y_1^n z_1^n \ r. \qquad (30)$$

Так как $D(x_1,y_1)=1$, $D(x_1,z_1)=1$, $D(y_1,z_1)=1$, то число $u/(x_1y_1z_1)$ так же целое. Поэтому из (30) следует, что $nr=[u/x_1y_1z_1]^n$, или обозначив $l_1= u/(x_1y_1z_1)$, имеем

$n\ r = l_1^n$, где l_1, как показано только что , целое число . Следовательно, из равенства (30) имеем $u^n= l_1^n x_1^n y_1^n z_1^n$, откуда

$$u=l_1x_1y_1z_1,\ l_1 \equiv n. \qquad (31)$$

Теперь покажем, что число l_1 взаимно простое с x,y и z. В соответствии с равенствами (25), (27) и (31) имеем

$$x_2+x_1^{n-1}= l_1y_1z_1,\ y_2+y_1^{n-1}= l_1x_1z_1,\ z_2+z_1^{n-1}= l_1x_1y_1. \qquad (32)$$

Из первого из равенств (32) следует, что если x_1 и l_1 имеют общий простой делитель l, то на l делится без остатка и число x_2; тогда $D(x_1,x_2)=l$. Это противоречит тому, что числа x_1 и x_2 – взаимно простые. Поэтому

$$D(l_1,x_1)=1 . \qquad (33)$$

Аналогичным рассуждением из первого равенства (32) получаем

$$D (l_1,x_2)=1. \qquad (34)$$

Объединив соотношения (33) и (34) , имеем $D (l_1,x)=1$. Аналогично получаем

$D (l_1,z)=1$, $D (l_1,y)=1$, $D (l_1,x_1)=1$. (35)

Из (42) очевидным образом получаем $[(u^n – x^n) + x^n]/(y+z)=n(x+y)(x+z)r$.

Так как $x^n= x_1^n x_2^n$, $x_1^n= y+z$, $u - x = y+z$, то последовательно получаем, что

$(u^n–x^n)=(y+z)L(u,-x)$, где $p=(n-1)/2$, $-x^n=(y+z)L(y,z)$, $n(x+y)(x+z)r=L(u,-x) - L(y,z)$,

$L(u,-x)=(y+z)^{n-1}-\alpha_1ux(y+z)^{n-3}+\alpha_2(ux)^2(y+z)^{n-5}+\ldots+ (-1)^p\ \alpha_p\ (ux)^p$,

Последнее равенство с учетом $u - x = y+z$ принимает вид

$n(x+y)(x+z)r=\alpha_1(yz-ux)(y+z)^{n-3}+\alpha_2(y^2z^2+u^2x^2)(y+z)^{n-5}+\ldots+ \alpha_p[(yz)^p-(-1)^p(ux)^p]$, (36)

где $p=(n-1)/2$, $\alpha_1= -n$, $\alpha_2= n(n-1)/2$, … , $\alpha_p=(-1)^p n$.

Разделив обе части (49) на n , имеем

$(x+y)(x+z)r = -[yz-ux](y+z)^{n-3}+ [(n-1)/2][(y^2z^2+u^2x^2)](y+z)^{n-5}+\ldots+$

$+(-1)^p[(yz)^p-(-1)^p(ux)^p]$. (37)

В силу леммы 2 следует заметить, что все коэффициенты вида α_1 /n, α_2 /n, α_3 /n, … , α_p /n в правой части (37) целые числа. Оценим первую квадратную скобку правой части (37): $ux-yz = x(x+y) + xz-yz = x(x+y)+z(x-y)$, т.е.

$$ux-yz = x(x+y)+z(x-y). \qquad (38)$$

Не ограничивая общности, можно считать , что $x+y>0$.

Действительно, если $x+y<0$, то в уравнении (1) достаточно производить замену x, y и z на –x, -y и –z соответственно. Так как $x+y=z_1^n$, $z=z_1z_2$,$D(z_1,z_2)= 1$, то $(x-y) \not\equiv z_1$ и с учётом обозначений 3) и 4) $\omega(z) = \omega(z_1)$, $\omega_{z1}(x+y) = n$. Поэтому из равенства (38) следует, что $\omega_{z1}(ux-yz)= \omega_{z1}(z)= \omega_{z1}(z_1) = 1$, т.е.

$\omega_{z1}(ux-yz) = 1$. Так как $u=(x+y)+z$,то

$$\omega_z,(u)= \omega_{z1}(z)=1. \qquad (39)$$

Далее $u^2x^2+y^2z^2=(ux+yz)^2-2xyzu=[x^2+xy+zx+yz]^2-2xyzu=[x(x+z)+y(x+z)]^2-$ $-2xyzu=(x+y)^2(x+z)^2-2xyzu$, т.е.

$$u^2x^2+y^2z^2=(x+y)^2-2xyzu. \qquad (40)$$

Отсюда в силу соотношения (40) получим $\omega_{z1}[(y^2z^2+u^2x^2)]=2$. Здесь мы считали , что $z_1\neq2$. Невозможность случая $z_1\neq2$ рассмотрена в конце работы. В силу равенства (39) имеем

$\omega_{z1} (u^3x^3-y^3z^3) \geq 3$, $\omega_{z1} (u^4x^4+y^4z^4) \geq 4$, … , $\omega_{z1} [(ux)^p - (-1)^p(yz)^p] \geq p$.

Поэтому правая часть (37) имеет порядок $\omega_{z1} = 1$, а левая часть - $\omega_{z1}(x+y)=n$.

Это противоречие показывает невозможность случая 1.

Теперь рассмотрим **случай** 2. В этом случае одно и только одно из чисел x, y и z кратно n . Без ограничения общности, будем считать $z \equiv n$.

Обозначим $\omega(z) = q$, $q \geq 1$. Откуда

$$\omega(z^n) = nq . \quad (41)$$

Третье равенство из (12) представимо в виде

$$-z^n = n(x+y)[L(x,y)/n]. \quad (42)$$

Тогда в равенстве (42) следует заметить, что числа в квадратной скобке правой части (42) не кратно числу n. Поэтому из равенств (41) и (42) имеем $\omega(n(x+y)) = nq$ и отсюда , $\omega(x+y) = nq-1$. А так же заметим, что числа $n(x+y)$ и $L(x,y)/n$ взаимно простые. В самом деле, прежде всего заметим, что в силу $x+y \equiv n$, следует, что $y+z$ n, $x \not\equiv n$. Поэтому, как показано в случае 1, получаем $D(x_1,x_2) = 1$, $D(y_1,y_2) = 1$.

Теперь покажем, что числа $n(x+y)$ и $L(x,y)/n$ также взаимно простые. Так как $L(x,y)/n \not\equiv n$, то общий простой множитель этих чисел отличен от n. Если обозначить через l их общий простой множитель, то очевидно, $D(x+y, l) = l$ и на l делится без остатка число xy. Но это противоречит соотношению $D(x,y) = 1$. Поэтому $l \neq l$ не может быть. Значит числа $n(x+y)$ и $L(x,y)/n$ взаимно простые и ,следовательно, $D(z_1,z_2) = 1$. Итак, мы установили, что и в случае 2 так же имеют равенства (15). Тогда согласно равенству (42) имеем $z_1^n=n(x+y)$,

$-z_2^n= L(x,y)/n$, где $z_2=z/z_1$. Аналогично $y+z= x_1^n$, $x+z= y_1^n$, $n(x+y)= z_1^n$

$- x_2^n = L(y,z)$, $-y_2^n= L(x,z)$, $-z_2^n= L(x,y)/n$, где $x=x_1x_2$, $y=y_1y_2$, $z= z_1z_2$.

Здесь так же, как и в первом случае, получаем соотношения (35) и $u=l_1x_1y_1z_1$, $l_1^n=r$, $r \equiv n$. Далее, совершенно так же, как в случае 1, завершаем доказательство невозможности случая 2.

В самом деле, записав (1) в виде: $[(u^n – x^n) +x^n]/(y+z)=n(x+y)(x+z)r$, имеем

$$n(x+y)(x+z)r=–n(yz-ux)(y+z)^{n-3}+\alpha_2(y^2z^2+u^2x^2)(y+z)^{n-5}+\ldots+(-1)^p[(yz)^p-(1)^p(ux)^p], \quad (43)$$

или, сокращая обе части (43) на n :

$$(x+y)(x+z)r=–(yz-ux)(y+z)^{n-3}+(\alpha_2/n)(y^2z^2+u^2x^2)(y+z)^{n-5}+\ldots+(-1)^p[(ux)^p-(-yz)^p]. \quad (44)$$

Аналогично находим $\omega_{z1}(ux-yz) = 1$, $\omega_{z1}[(y^2z^2+u^2x^2)]=2$, $\omega_{z1}(u^3x^3-y^3z^3) \geq 3$, $\omega_{z1}(u^4x^4+y^4z^4) \geq 4$, … , $\omega_{z1}[(ux)^p - (-yz)^p] \geq p$, где $p=(n-1)/2$.

Теперь заметим, что левая часть (44) имеет порядок $\omega_{z1} = n-1$, а его правая часть - $\omega_{z1} = 1$. Это противоречие показывает, что и случая 2 быть не может.

Итак, мы получили противоречие в обоих логически возможных случаях из-за предположения, что уравнение (1) имеет решение целых числах, отличных от нуля. Остается доказать, что при любом натуральном числе k не может быть $z_1=2^k$. Действительно, если это так, то имели бы $n(x+y)=2^{nk}$. Тогда как это видно в последнем равенстве была бы сумма x+y нецелой, что вопреки целостности чисел x,y и z . Теорема доказана.

Литература:

1. **Саймон, С.** Великая теорема Ферма [Текст] // - М.:МЦНМО.-2000.-288с
2. **Wiles A.** Modular elliptic curves and Fermat`s Last Theorem [Текст] // Ann. of Math., 1995. Vol. 142, P. 443-551.
3. **Taylor, R.** Wiles A. Ring-theoretic properties of certain Hecke algebras [Текст] // Ann. of Math., 1995. Vol. 142, P. 553-572.
4. **Сражидинов, А.** Элементарное доказательство Великой теоремы Ферма для показателя 3 [Текст] // Изв. вузов Кыргызстана.- №10,2019.-С.6-9.
5. **Ферма П.** Исследования по теории и диофантову анализу. [Текст] // М.: Наука, 1992.
6. **Edwards, H.M.** Fermat`s Last Theorem. A Genetic Introduction to Algebraic Number Theory. - Springer, 1977.
7. **Сражидинов, А.** Об одном подходе к доказательству Великой теоремы Ферма для показателя 4// Изв. вузов Кыргызстана.- № 5,2018. – С.10-12.