АБХАЗСКИЙ НАУЧНЫЙ ЦЕНТР
РОССИЙСКОЙ АКАДЕМИИ КОСМОНАВТИКИ
им. К.Э. ЦИОЛКОВСКОГО
Р. А. КАМЛИЯ

ТЕОРЕМА ФЕРМА И РАЗЛОЖИМОСТЬ СТЕПЕННЫХ ВЫЧЕТОВ

Сухум-2008

ББК 22.131

К 18

Абхазский научный центр
Российской академии космонавтики
им. К.Э. Циолковского

Р.А.Камлия. ***Теорема Ферма и разложимость степенных вычетов. Абхазский научный центр Российской академии космонавтики им. К.Э.Циолковского.***

Работа посвящена теореме Ферма, Рассмотрены различные свойства и соотношения чисел, которые могли бы удовлетворять уравнению Ферма. Рассмотрены вопросы разложимости степенных вычетов в сумму двух степенных вычетов и показаны свойства Пифагоровых чисел. Доказаны ряд новых теорем, с использованием которых доказывается теорема Ферма пользуясь исключительно методами элементарной теории чисел. Предназначена для специалистов и студентов занимающихся теорией чисел.

ПРЕДИСЛОВИЕ

Данная работа является результатом многолетней работы. Различные подходы к доказательству теоремы Ферма дали ряд результатов, не все из которых в конечном счете используются при доказательстве теоремы. Они могут иметь самостоятельный интерес.

Среди математиков существует спор – ошибался или нет Пьер Ферма утверждая, что нашел оригинальный способ доказательства теоремы.

Формулировка теоремы, которую дал сам Пьер Ферма, приведена в книге П. Рибенбойма “Последняя теорема Ферма”. Она гласит: невозможно разложить куб на два куба, биквадрат - на два биквадрата, в общем случае, любую степень, большую двух, в сумму двух таких же степеней.

Как увидим в данной работе, доказательство теоремы Ферма осуществляется через разложимость степенных вычетов в сумму двух степенных вычетов.

Если имеет место разложимость степенного вычета по модулю простого числа, то разложим любой степенной вычет, но это не означает, что любая сумма двух степенных вычетов есть степенной вычет.

Есть основание полагать, что Ферма анализируя вопросы разложимости степенных вычетов пришел к своему выводу и поэтому дал именно такую формулировку теоремы.

В данной работе через разложимость квадратичных вычетов показано, что любая тройка Пифагоровых чисел содержит число кратное 3 и число кратное 5.

Свойства и соотношения чисел, удовлетворяющих уравнению Ферма, если оно вообще выполнимо, посвящен **§**1. Используя Теорему1 и Теорему1А можно получить известные формулы Абеля.

Замеченные свойства сравнений Эйлера и Ферма выделены в отдельный параграф **§2.**

Некоторые свойства степенных вычетов получены с использованием матрицы вычетов. Они изложены в §3.

Далее в §4, §5 рассмотрены свойства степенных вычетов и разложимость степенных вычетов в сумму двух степенных вычетов.

Доказательство теоремы Ферма приведено в §6. Два подхода к доказательству согласуются между собой.

Различные попытки доказать теорему Ферма сформировали содержание работы.

При написании работы не ставилось целью систематическое изложение каких то вопросов, в том числе и вопросов разложимости степенных вычетов.

§1 ОСНОВНЫЕ ТЕОРЕМЫ И СООТНОШЕНИЯ

1.1.Теорема1. ***Пусть p-простое число, b и c взаимно простые и не сравнимы по модулю p. Тогда в равенстве*** $c^p - b^p = (c-b)(c^{p-1} + \ldots + b^{p-1})$ ***множители правой части*** $a_1 = c-b$ ***и*** $a_2 = c^{p-1} + \ldots + b^{p-1}$ ***не имеют общего делителя.***

Доказательство. Пусть p_1 - простое число и делит a_1. Это значит, что $a_1 \equiv 0 (mod p_1)$ или $c-b \equiv 0 (mod p_1)$ или $c \equiv b (mod p_1)$.

Последнее означает, что $c = p_1 q + r$, $b = p_1 q_1 + r$, $0 < r < p_1$

где: q, q_1, r-целые числа.

Тогда

$$a_1 = c - b = p_1 q + r - p_1 q_1 - r = p_1 (q-q_1) \qquad (1)$$

$$a_2 = (p_1 q + r)^{p-1} + \ldots + (p_1 q_1 + r)^{p-1} = k p_1 + p r^{p-1} \qquad (2)$$

где: k-какое то целое число.

Так как c и b по условиям теоремы не сравнимы по модулю p, а любое число p_1, по модулю которого сравнимы c и b не может быть равным p.

Как следует из (1), число p_1 делит a_1, но он не делит a_2 потому, что для этого p_1 должен делить второе слагаемое в (2), т.е. $p r^{p-1}$, а это не возможно поскольку p простое, а $r < p_1$ -простого. В качестве p_1 мы можем взять любой простой делитель a_1 больший единицы. Если любой простой делитель a_1 не делит a_2, то a_1 и a_2 взаимно простые числа. Теорема доказана.

1.2Теорема1А. ***Пусть p-простое, b и c взаимно простые числа и c+b не кратно p. Тогда в равенстве***

$$c^p + b^p = (c+b)(c^{p-1} - c^{p-2}b + \cdots + b_{p-1})$$ ***множители правой части*** $a_1 = c+b$ ***и*** $a_2 = c^{p-1} - \cdots + b^{p-1}$ ***не имеют общего делителя.***

Доказательство. Пусть ***m***-простое число и делит a_1. Это значит, что $a_1 \equiv 0(\mathrm{mod}\, m)$ или $c+b \equiv 0(\mathrm{mod}\, m)$. Последнее означает, что $c = mq + r$, $b = mq_1 - r$**,** где: q_1, q, r - целые числа.

$$a_1 = c + b = mq + r + q_1 m - r = m(q_1 + q) \qquad (1)$$

$$a_2 = (mq + r)^{p-1} - \cdots + (mq_1 - r)^{p-1} = km + pr^{p-1} \qquad (2)$$

где:***k***-целое число.

Число a_1 не кратно ***p*** по условию теоремы, но кратно ***m,*** как следует из (1). Поэтому ***m*** не равно ***p*** и не кратно ***p*** поскольку ***m*** простое.

Число a_2 не делится на ***m*** так как для этого должно делится второе слагаемое в (2) $\boldsymbol{p}\, r^{p-1}$, где ***p***-простое и не равно ***m***, а ***r<m***-простого. Аналогично доказывается для любого простого делителя a_1. Если для всех простых делителей a_1 это выполняется, значит a_1 и a_2 взаимно простые числа. Теорема доказана.

Возможно, доказательства этих теорем где то существуют, но их не удалось найти. С использованием Теоремы1 и Теоремы1А можно получить известные в литературе [1] формулы Абеля. Мы их приведем здесь с использованием тех же обозначений, которые будут использованы далее

$$\boldsymbol{c-b=a}_1^{\,p} \qquad (3)$$

$$\boldsymbol{c-a = b}_1^{\,p} \qquad (4)$$

$$\boldsymbol{a+b= c}_1^{\,p} \qquad (5)$$

где: $\boldsymbol{a}_1, \boldsymbol{b}_1, \boldsymbol{c}_1$ - делители чисел ***a,b,c***, соответственно.

1.3Теорема 2. ***Если уравнение $a^p + b^p = c^p$ имеет решение при p-простом и числа a,b,c попарно взаимно просты и не делятся на p, то справедливо сравнение $a + b \equiv c \pmod{p^2}$.***

Эта теорема устанавливает для первого случая теоремы Ферма более жесткую связь между числами ***a ,b, c*** чем известное ранее соотношение

$$a + b = c \pmod{p} \qquad (1)$$

Доказательство. Введем параметр $e = a + b - c$. Из (1) перенося c в левую часть получим

$$e = 0 \pmod{p} \qquad (2)$$

Используя формулы Абеля (3), (4),(5) из 1.2 и учитывая, что

$e = a + b - c$ можно написать

$$\begin{aligned} e &= a - a_1^p \\ e &= b - b_1^p \qquad (3) \\ e &= c_1^p - c \end{aligned}$$

или

$$\begin{aligned} a &= e + a_1^p \\ b &= e + b_1^p \qquad (4) \\ c &= c_1^p - e \end{aligned}$$

Используя последние равенства можно уравнение $a^p + b^p = c^p$ записать в виде

$$(e + a_1^p)^p + (e + b_1^p)^p = (c_1^p - e)^p \qquad (5)$$

Если последнее равенство выполнимо, то левая и правая его части сравнимы по модулю любого числа, в частности по модулю p^2. Тогда

$$(e + a_1^p)^p + (e + b_1^p)^p = (c_1^p - e)^p \pmod{p^2} \qquad (6)$$

После возведения в степень и отбрасывания членов кратных p^2 с учетом (2) получим

$$(a_1^p)^p + (b_1^p)^p \equiv (c_1^p)^p \pmod{p^2} \qquad (7)$$

или $(a_1^{p-1})^p a_1^p + (b_1^{p-1})^p b_1^p \equiv (c_1^{p-1})^p c_1^p \pmod{p^2}$ (8)

В силу малой теоремы Ферма $a_1^{p-1} \equiv 1(\mathrm{mod} p)$, $b_1^{p-1} \equiv 1(\mathrm{mod}\ p)$, $c_1^{p-1} \equiv 1(\mathrm{mod}\ p)$. Тогда $(a_1^{p-1})^p \equiv 1(\mathrm{mod} p^2)$ $(b_1^{p-1})^p \equiv 1(\mathrm{mod} p^2)$, $(c_1^{p-1})^p \equiv 1(\mathrm{mod}\ p^2)$. С учетом последних сравнений из (8) получим

$$a_1^p + b_1^p \equiv c_1^p (mod\ p^2) \quad (9)$$

Теперь сложим два последних равенства из (3)

$$2e = c_1^p - c + b - b_1^p$$

или $2e = c_1^p - a_1^p - b_1^p$ (10)

С учетом (9) из последнего равенства получим

$$\boldsymbol{2e \equiv 0\ (mod\ p^2)}$$

Поскольку $\boldsymbol{p}^2$ нечетное число, последнее сравнение можно сократить на 2. Тогда

$$\boldsymbol{e} \equiv \mathbf{0} (\mathrm{mod}\ p^2) \quad (11)$$

Подставляя значение $\boldsymbol{e}$ в (11) получим $\boldsymbol{a+b-c \equiv 0 (mod\ p^2)}$

или $\boldsymbol{a+b \equiv c\ (mod\ p^2)}$ (12)

Теорема доказана.

Интересную форму записи уравнения Ферма для первого случая можно получить после несложных преобразований.

Как следует из (10)

$$\boldsymbol{e} = \frac{c_1^p - a_1^p - b_1^p}{2} \quad (13)$$

Теперь подставляя полученное значение e в левую часть уравнения (5) можно записать уравнение Ферма в виде

$$(e + a_1^p)^p + (e + b_1^p)^p = (e + a_1^p + b_1^p)^p \quad (14)$$

Вводя функцию $f(x) = (e + x)^p$ можно это же уравнение записать в другой форме

$$f(x_1) + f(x_2) = f(x_1 + x_2) \quad (15)$$

где: $x_1 = a_1^p$; $x_2 = b_1^p$;

Удобно записать это уравнение как

$$f(x_1 + x_2) = f(x_1) + f(x_2) \quad (16)$$

1.4. Свойства чисел уравнения Ферма

С помощью сравнений левой и правой частей уравнения Ферма по модулям различных чисел можно выявлять различные свойства и соотношения чисел, которые могли бы удовлетворять уравнению Ферма, если вообще оно имеет решение для каких то простых степеней ***p***.

Как известно из [2], соотношение $c \equiv a+b \pmod{p}$ получаем из сравнения левой и правой частей уравнения по модулю ***p***. Точно также можно получить соотношение $c \equiv a+b \pmod{3}$ поскольку для любого нечетного ***p*** выполняются сравнения $a^n \equiv a \pmod{3}$, $b^n \equiv b \pmod{3}$, $c^n \equiv c \pmod{3}$, для любых ***a,b,c*** в том числе, когда какое то число делится на ***p*** или на 3.

Если выполняются сравнения $c \equiv a+b \pmod{p}$ и $c \equiv a+b \pmod{3}$, то справедливо сравнение по модулю произведения модулей $c \equiv a+b \pmod{3p}$.

Если еще учесть, что $a^p \equiv a \pmod{2}$, $b^p \equiv b \pmod{2}$, $c^p \equiv c \pmod{2}$, то получим

$$c \equiv a+b \pmod{6p} \quad (1)$$

Обычно доказательства теоремы Ферма разделяются на первый и второй случаи. Для первого случая ни одно из чисел ***a, b, c*** не делится на ***p***, а для второго случая – одно из чисел делится на ***p***. Два числа не могут делится на ***p*** потому, что в этом случае и третье число должно делиться на ***p*** и тогда уравнение можно сократить на p^p.

Рассмотрим некоторые свойства чисел ***a,b,c*** не разделяя первый и второй случаи теоремы Ферма.

Если какое то число делится на p, то это число c, либо какое-то из чисел a или b. Для определенности будем полагать, что a не делится на p.

Соотношения, используемые в дальнейшем, справедливы не зависимо от того делится какое то из чисел b или c на p или ни одно число не делится на p. С учетом свойств, которые удастся выяснить в процессе анализа, числа a и b в уравнении будем считать заданными, а c неизвестным.

$$c^p = b^p + a^p \qquad (2)$$

Перенесем b^p в левую часть и разложим на множители

$$(c-b)(c^{p-1}+\ldots+b^{p-1}) = a^p \qquad (3)$$

Один из множителей левой части

$$c-b=a_1^p \qquad (4)$$

что следует из формул Абеля. Это соотношение справедливо не зависимо от того c либо b кратно p или нет, а a как условились не кратно p. Число a_1 является делителем a. Второй множитель левой части (3) явно больше единицы. Поэтому a содержит кроме a_1 хотя бы еще один делитель больше единицы, причем на основании Теоремы**1**, не имеющий общего делителя с a_1.

Обозначим через a_2 один из простых делителей a, но не являющийся делителем a_1. Если уравнение (2) имеет целочисленное решение то левая и правая его части сравнимы по модулю любого числа, в частности по модулю a_2. Рассмотрим сравнение левой и правой части (2) по модулю a_2.

$$c^p \equiv b^p + a^p \pmod{a_2} \qquad (5)$$

Поскольку a_2 делит a, последнее сравнение примет вид

$$c^p \equiv b^p \pmod{a_2} \qquad (6)$$

Сравнение такого вида, как известно [2], Гл.IV,§5,если имеет решения, то количество решений равно $d=(p,\varphi(a_2))$, а индекс правой части должен быть кратен d.

Поскольку **p**-простое, количество решений у нас определяется величиной $\varphi(a_2)$. Если $\varphi(a_2)$ кратен p, то $d = p$, в противном случае $d = 1$. Индекс правой части в (6) кратен p, а потому он всегда кратен d. Следовательно сравнение (6) имеет решения. Рассмотрим два случая для d.

С л у ч а й 1. Пусть d=1.Сравнение (6) имеет одно решение. Это единственное решение легко найти проиндексировав (6).

Тогда $p\cdot indc \equiv p\cdot indb \pmod{\varphi(a_2)}$ и разделив на p получим

$$ind\ c \equiv ind\ b \pmod{\varphi(a_2)}$$

Единственным решением является

$$c \equiv b \pmod{a_2}$$

или $$c-b \equiv 0 \pmod{a_2} \qquad (8)$$

С учетом известного соотношения (4) сравнение (8) примет вид

$$a_1^p = 0 \pmod{a_2} \qquad (9)$$

Поскольку a_1 не кратно a_2, последнее сравнение не выполнимо. Следовательно сравнение (6) для случая $d=1$ не имеет решения, а следовательно не имеет решения и уравнение (2).

С л у ч а й 2. Пусть $d= p$.Сравнение (6)имеет p решений.

Найдем их пользуясь известной методикой [2],Гл.IV,§5.Проиндексируем сравнение (6)

$$p\cdot indc \equiv p\cdot indb \pmod{\varphi(a_2)} \qquad (10)$$

Сократим на p с учетом, что $\varphi(a_2)$ кратен p. Тогда

$$indc \equiv indb \ (mod \ \frac{\varphi(a_2)}{p}) \qquad (11)$$

p различных значений **indc** найдем как

$$indc \equiv indb + \frac{\varphi(a_2)}{p} k \qquad (12)$$

где: **k=0,1,…,p-1**.

Пусть $\alpha = \frac{\varphi(a_2)}{p}$. Тогда из (12) будем иметь

$$indc \equiv indb + \alpha k \ (mod \ \tfrac{\varphi(a_2)}{p}) \qquad (13)$$

или $$indc \equiv indb + indg^{\alpha k} \ (mod \tfrac{\varphi(a_2)}{p}) \qquad (14)$$

где: ***g***- первообразный корень по модулю a_2.

Решения для *c* в общем виде получатся как

$$c \equiv bg^{\alpha k} \ (mod \ a_2) \qquad (15)$$

При различных значениях ***k*** мы получим ***p*** не сравнимых по модулю a_2 числа. Решениями для ***c*** являются ***p*** классов чисел, в каждом из которых числа сравнимы по модулю a_2.

Если a_2 не простое число, то все делители a_2 имеют форму ***kp+1***. Если бы это было не так, то рассмотрев сравнение (6) по модулю этого числа получили бы ***d=1*** и пришли бы к ***С л у ч а ю 1*** не имеющего решения.

§2. ДАЛЬНЕЙШИЕ СВОЙСТВА СРАВНЕНИЙ ЭЙЛЕРА И ФЕРМА.

Известная теорема Эйлера гласит, что при ***m>1*** и ***(a,m)=1*** справедливо сравнение

$$a^{\varphi(m)} = 1 \ (mod \ m) \qquad (1)$$

В этом случае можно вместо модуля ***m*** написать модуль ***3m*** при том же $\varphi(m)$ и условии, что ***a*** не кратно трем т.е. (*a*,*3*)=1. Это возможно в связи с тем, что $a^2 \equiv 1 \pmod 3$ при (*a*,*3*)=1. Поскольку $\varphi(m)$ всегда четное число при ***m***>2 то сравнение (1) можно написать в виде

$$(a^2)^{\frac{\varphi(m)}{2}} \equiv 1 \pmod m \qquad (2)$$

$$\text{или} \quad (3k+1)^{\frac{\varphi(m)}{2}} \equiv 1 \pmod m$$

Из последнего видно, что левая часть сравнима с 1 по модулю 3, а следовательно справедливо сравнение по модулю произведения модулей

$$a^{\varphi(m)} \equiv 1 \pmod{3m} \qquad (3)$$

Даже при простом ***m*** представляет интерес по модулю какого еще числа выполняется сравнение (1). Это зависит от делителей $\varphi(m)$. Допустим, что $\varphi(m) = p_1 \cdot p_2 \cdots p_n$. Если произведение каких либо делителей $\varphi(m)$ (любое сочетание) плюс 1 есть простое число , то по модулю этого простого числа выполняется сравнение (1) при условии, что ***a*** не кратно этому простому числу.

Приведем численный пример. Пусть ***m***=41. Тогда $\varphi(41) = 2 \cdot 2 \cdot 2 \cdot 5$. При различных сочетаниях множителей последнего можем получить делители $\varphi(41)$ 2,4,10, которые равны $2 = \varphi(3)$, $4 = \varphi(5)$, $10 = \varphi(11)$. Следовательно сравнение (1) выполняется по модулю произведения $3 \cdot 5 \cdot 11 \cdot 41 = 6765$ при (***a***,6765)=1.

Ели ***m=p*** имеем теорему Ферма

$$a^{p-1} \equiv 1 (\text{mod} p) \qquad (4)$$

которой в [2] придана более общая форма

$$a^p \equiv a (\text{mod} p) \qquad (5)$$

Числа *a* и a^p совпадают по четности. Следовательно последнее сравнение выполнимо по модулю 2.

Кроме того, если $a \equiv 0(\mathrm{mod}\,3)$ то и $a^p \equiv 0(\mathrm{mod}\,3)$, а если $a \equiv \pm 1(\mathrm{mod}\,3)$, то и $a^p \equiv \pm 1(\mathrm{mod}\,3)$. Таким образом, сравнение выполнимо и по модулю 3.

Если сравнение выполнимо по модулям 2,3,p то это сравнение выполнимо по модулю произведения этих модулей. Следовательно мы можем не теряя общности написать сравнение

$$a^p \equiv a(\mathrm{mod}\,6p) \qquad (6)$$

§3. МАТРИЦА ВЫЧЕТОВ И ИХ СВОЙСТВА

Для большей наглядности при изучении свойств сравнений и степенных вычетов**,** представляется целесообразным рассмотреть матрицу вычетов степени ***p*** по модулю простого числа ***m*** формы ***k****p*+1.

Для построения матрицы рассмотрим сравнение

$K^p = 1 \,(\mathrm{mod}\, m)$

Решение этого сравнения можно найти путем индексирования и записываются как $K_i = g^{\alpha_i}$

где: $\alpha_i = \dfrac{\varphi(m)}{p} i$

i= *0,1,2,....,p-1*

Это такое же решение как в (15), §1,1.4 при ***b=1***.Все эти решения расположим в качестве элементов нулевого столбца матрицы по возрастанию ***i***. Первый столбец матрицы представляет собой произведение $K_i \, g = g^{\frac{\varphi(m)}{p} i+1}$. Если запишем элемент ***j***-того столбца и ***i***-той строки, то это будет $a_{i,j} = K_i \, g^j = g^{\frac{\varphi(m)}{P} i+j}$, то есть номер строки это ***i,*** а номер столбца ***j***. Второй столбец – это произведение чисел нулевого столбца на g^2 и т. д. Самая нижняя строка – это строка

наименьших положительных вычетов степени ***p*** т.е. $a_j = g^{jp} \pmod{m}$. Теперь изобразим саму матрицу.

$$\begin{array}{cccccccc}
K_{p-1} & a_{p-1,1} & a_{p-1,2} & \cdots & a_{p-1,j} & \cdots & a_{p-1,\alpha} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
K_i & a_{i,1} & a_{i,2} & \cdots & a_{i,j} & \cdots & a_{i,\alpha} \\
K_{i-1} & a_{i-1,1} & a_{i-1,2} & \cdots & a_{i-1,j} & \cdots & a_{i-1,\alpha} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\mathrm{K}_1 & a_{1,1} & a_{1,2} & \cdots & a_{1,j} & \cdots & a_{1,\alpha} \\
1 & a_{0,1} & a_{0,2} & \cdots & a_{0,j} & \cdots & a_{0,\alpha} \\
 & & & & & & \\
1 & a_1 & a_2 & & a_j & & a_\alpha
\end{array}$$

Все числа каждого столбца возведенные в степень ***p*** сравнимы по модулю ***m***. Это свойство становится очевидным если мы в общем виде возведем любое число в степень ***p***

$$a_j = \left(g^{\frac{\varphi(m)}{p}i+j}\right)^p = g^{\varphi(m)i+jp} = g^{\varphi(m)i}\, g^{jp} = (km+1)^i\, g^{jp}$$

Теперь найдем вычет по модулю ***m*** как

$$a_j \equiv \boldsymbol{(km+1)}^i\, g^{jp} \pmod{m}$$

$$a_j \equiv g^{jp} \pmod{m}$$

Видно, что a_j не зависит от ***i*** т.е. не зависимо от того какое число столбца мы возведем в степень ***p*** т.к. $g^{\varphi(m)} = 1 \pmod{m}$. Если же мы возьмем любое другое число принадлежащее другому столбцу получим другое значение.

Для любых ***n*** от 1 до $\varphi(m)$ все g^n не сравнимы по модулю ***m***. Поэтому g^n пробегает полную систему вычетов по модулю ***m***, когда ***n*** пробегает значения от 1 до $\varphi(m)$. Этим и

обусловлен выбор числа g–первообразного корня по модулю ***m***, как основание показательной функции.

Если $\boldsymbol{a} = g^n \pmod m$, то для определения принадлежности строке и столбцу достаточно представить ***n*** как

$$n = \frac{\varphi(m)}{p} i + j$$

где: $j < \frac{\varphi(m)}{p}$.

Получившиеся ***i*** и ***j*** определят строку и столбец, к которому принадлежит это число. Как следует из построения матрицы все числа строки имеют одно значение индекса ***i***, а все числа столбца одно значение индекса ***j***.

С л е д с т в и е. Для сравнения вида $c^p \equiv b^p \pmod m$ подходят числа принадлежащие одному столбцу так как дают один наименьший положительный вычет. Каждый столбец содержит ***p*** чисел и любое их сочетание является решением сравнения. Следовательно для каждого столбца существует $\boldsymbol{p}^2$ пар чисел удовлетворяющих последнему сравнению, а поскольку столбцов $\frac{\varphi(m)}{p}$ то всего пар чисел удовлетворяющих сравнению будет $\varphi(m)\boldsymbol{p}$.

Для уравнения Ферма $c^n = b^n + a^n$, если оно имеет решение, левая и правая части должны быть сравнимы по модулю любого числа ***m***. Тогда в левой части получим вычет степени ***n***, а в правой сумму двух вычетов степени ***n.*** Это значит, что для выбранного модуля ***m*** должно иметь место разложимость степенного вычета в сумму двух степенных вычетов, но при этом не каждая сумма степенных вычетов является степенным вычетом.

Вопросы разложимости степенных вычетов в сумму двух степенных вычетов будут рассмотрены в §5.

Приведем несколько матриц для различных простых чисел и различных степеней ***n***. Для каждой матрицы будем отмечать возможность разложения степенного вычета в сумму двух степенных вычетов и наличие соседних вычетов, являющегося одним из признаков разложимости степенных вычетов. Соответствующая теорема о разложимости степенных вычетов будет доказана в **§5.**

Пусть m=41, p=5.Для ***m***=41 первообразный корень g=6.

37	17	20	38	23	15	8	7
16	14	21	2	31	22	9	13
18	26	33	34	40	35	5	30
10	19	32	28	4	24	21	3
1	6	36	11	25	27	39	29
1	27	32	3	40	14	9	38

Как видно из нижней строки степенных вычетов, соседних вычетов нет и сумма любых двух вычетов не является вычетом.

Составим матрицу вычетов для ***m***=13, ***n***=2, 3, 4,.

	12	11	9	5	10	7
	1	2	4	8	3	6
x^2	1	4	3	12	9	10
x^4	1		3		9	

Как видно из строки вычетов для квадрата существуют соседние вычеты 3,4 и 9,10. Для степени 4 соседних вычетов не существует. Вычетов степени четыре всего три и ни один из вычетов не сравним с суммой двух других по модулю ***m***.

Для степени три матрица вычетов по модулю 13 выглядит следующим образом.

	9	5	10	7
	3	6	12	11
	1	2	4	8
x^3	1	8	12	5

Здесь тоже нет соседних степенных вычетов и легко проверить, что нет разложимости степенных вычетов.

Далее приведем матрицу вычетов для простого числа ***m***=31 и степеней 2, 4, 3,5.

	30	28	22	4	12	5	15	14	11	2	6	18	23	7	21
	1	3	9	27	19	26	16	17	20	29	25	13	8	24	10

x^2	1	9	19	16	20	25	8	10	28	4	5	14	2	18	7
x^4	1		19		20		8		28		5		2		7

Как видно из матрицы, существуют соседние вычеты степени четыре 19,20 и 7.8. Все степенные вычеты разложимы в сумму двух степенных вычетов.

Матрица кубических вычетов по модулю ***m***=31.

	5	15	14	11	2	6	18	23	7	21
	25	13	8	24	10	30	28	22	4	12
	1	3	9	27	19	26	16	17	20	29
x^3	1	27	16	29	8	30	4	15	2	23

Все кубические вычеты по модулю 31 разложимы в сумму двух вычетов.

	2	6	18	23	7	21
	4	12	5	15	14	11
	8	24	10	30	28	22
	16	17	20	29	25	13
	1	3	9	27	19	26
x^5	1	26	25	30	5	6

Матрица вычетов степени пять по модулю ***m***=31.

Все вычеты степени пять по модулю 31 также разложимы.

3.1Теорпема3. ***Если*** $\frac{\varphi(m)}{p}$ ***тождественно не равен нулю по модулю p, при m и p простых, то любой вычет степени p является вычетом степени*** p^2**.**

Д о к а з а т е л ь с т в о. Для доказательства теоремы рассмотрим матрицу вычетов по модулю простого числа $m = kp+1$, где p-любое простое число.

Как мы показали в §3, вычеты полной системы вычетов в столбце матрицы связаны соотношением

$$V_2 = V_1 \cdot g^{\frac{\varphi(m)}{p} i} \pmod m \qquad (1)$$

где:*i*-разность номеров строк, в которых расположены вычеты V_2 и V_1. Допустим, что оба эти вычета являются степенными вычетами.

Умножим сравнение (1) на V_1' такой, что $V_1 \cdot V_1^{'} \equiv 1 (\mathrm{mod}\, m)$. Такой вычет существует на основании С в о й с т в а 2 степенных вычетов. Тогда получим

$$V_2 \cdot V_1^{'} \equiv g^{\frac{\varphi(m)}{p} i} \pmod m \qquad (2)$$

В левой части получим произведение двух степенных вычетов, которое также является степенным вычетом на основании С в о й с т в а 1 степенных вычетов.

По условиям теоремы $\frac{\varphi(m)}{p}$ тождественно не равно нулю по модулю p, а $i < p$ и потому не кратен p. Поскольку g является первообразным корнем правая часть может быть вычетом степени p только при $i \equiv 0 (\mathrm{mod}\, p)$ то есть $i = 0$. Это означает, что V_1 и V_2 находятся на одной строке то есть это один и тот же вычет.

Если любой столбец не может содержать два вычета степени p, а количество столбцов и количество степенных

вычетов равны $\frac{\varphi(m)}{p}$, то в каждый столбец попадет один и только один вычет степени р.

Каждый столбец, как следует из §3 содержит ***p*** чисел являющихся решениями сравнения вида

$$x^p \equiv V(\mathrm{mod}\, m) \qquad (3)$$

где:V –называется вычетом степени р.

Если одно из этих решений принадлежащих одному столбцу, как мы уже показали, является вычетом степени ***p***, то существует $x_i \equiv a^p(\mathrm{mod}\, m)$. Тогда из (3) получим

$$(a^p)^P \equiv V(\mathrm{mod}\, m)$$

$$\text{или } a^{p^2} \equiv V(\mathrm{mod}\, m) \qquad (4)$$

Таким образом, существует какое то число *a,* удовлетворяющее последнему сравнению. Следовательно V является вычетом степени p^2. Теорема доказана.

3.2 Квадратичные вычеты.

Из полной системы вычетов по модулю ***m*** половина из них то есть $\frac{\varphi(m)}{2}$, являются квадратичными вычетами [2], а другая половина квадратичными невычетами. Как мы уже говорили, любой вычет, в данном случае квадратичный вычет, можно представить как

$$\mathrm{V}= g^{\frac{\varphi(m)}{2}i+j}(\mathrm{mod}\, m) \qquad (1)$$

где: g-первообразный корень,

Для квадратичного вычета ***i*** может принимать два значения: ***i***=0 и ***i***=1.

Рассмотрим два вычета принадлежащих одному столбцу матрицы квадратичных вычетов. Они соответствуют какому то значению j и двум различным значениям ***i***

$$V_1 = g^j (\mathrm{mod}\, m) \quad (1)$$

$$V_1 = g^{\frac{\varphi(m)}{2}+j} (\mathrm{mod}\, m) \quad (2)$$

Допустим, что ***j*** четное число. Тогда V_1 является квадратичным вычетом. Тогда V_2 тоже будет квадратичным вычетом при $\frac{\varphi(m)}{2} \equiv 0(\mathrm{mod}\, 2)$.Решая совместно (2) и (3) можно получить

$$V_1 \equiv -V_2 (\mathrm{mod}\, m)$$

$$\text{или} \quad V_1 + V_2 \equiv 0(\mathrm{mod}\, m)$$

Таким образом, для случая $\frac{\varphi(m)}{2} \equiv 0(\mathrm{mod}\, 2)$ столбец матрицы содержит два квадратичных вычета, сумма которых равна ***m,*** а для нечетного ***j*** столбец содержит два квадратичных невычета.

Рассмотрим теперь случай $\frac{\varphi(m)}{2} \equiv 1(\mathrm{mod}\, 2)$.В этом случае при четном ***j*** вычет V_1 будет квадратичным вычетом, а V_2 квадратичным невычетом, а сумма их также равна ***m.***

В случае нечетного ***j*** вычет V_2 будет квадратичным вычетом, а V_1 квадратичным невычетом, а сумма их также равна ***m***.

Таким образом, все столбцы матрицы вычетов содержат по одному квадратичному вычету и по одному квадратичному невычету. К стати сказать, этот случай соответствует условиям Теоремы3 и каждый квадратичный вычет является биквадратичным вычетом. Примеры квадратичных матриц приведены выше в разделе 3.1.

3.3.Первообразные корни.

Отметим некоторые свойства первообразных корней.

а) Если g является первообразным корнем по модулю ***m***, то при $\varphi(m)$ тождественно не равном нулю по модулю ***n*** число $g_1 \equiv g^n (\mathrm{mod}\, m)$ также является первообразным корнем.

Допустим, что число $g_1 \equiv g^n (\mathrm{mod}\, m)$ не является первообразным корнем. Тогда он принадлежит степени $\alpha < \varphi(m)$ по модулю ***m*** , то есть

$$(g^n)^\alpha \equiv 1(\mathrm{mod}\, m) \qquad (1)$$

Из последнего можно написать

$$(g^\alpha)^n \equiv 1(\mathrm{mod}\, m) \qquad (2)$$

Последнее сравнение имеет $d = (n, \varphi(m))$ решений. Поскольку $\varphi(m)$ тождественно не равен нулю по модулю ***n*** число решений d=1. Это единственное решение есть - $g^\alpha \equiv 1(\mathrm{mod}\, m)$. Следовательно $\alpha \equiv 0(\mathrm{mod}\ \varphi(m))$. Наше предположение $\alpha < \varphi(m)$ не верно. Число $g_1 \equiv g^n (\mathrm{mod}\, m)$ является одним из первообразных корней. Рассмотрим общую формулу представления вычетов полной системы вычетов по модулю m

$$a \equiv g^{\frac{\varphi(m)}{p} i + j} (\mathrm{mod}\, m) \qquad (3)$$

Предположим, что j делит $\varphi(m)$, и сделаем простое преобразование $g^{\frac{\varphi(m)}{p} i + j} \equiv (g^{\frac{\varphi(m)}{j \cdot p} i + 1})^j \equiv b(\mathrm{mod}\, m)$

Полученное число не является первообразным корнем потому, что он принадлежит степени $\frac{\varphi(m)}{j}$ по модулю ***m***.

Таким образом, в столбцах с номерами не делящими $\varphi(m)$ содержатся по ***p*-1** первообразных корней, а один из вычетов, как установлено при доказательстве Теоремы3, является вычетом степени p.

3.4. Случай составного модуля.

Для доказательства теоремы Ферма важно знать разложимость степенных вычетов по модулям любых чисел, в том числе и составных чисел. Чтобы можно было любой степенной вычет по модулю простого числа выразить степенной функцией основание функции должно быть первообразным корнем.

В этой связи, рассмотрим возможность поиска числа со свойствами первообразного корня простого числа.

Пусть первообразным корнем простого числа m_1 является g_1, а первообразным корнем по модулю m_2 является g_2.

Число, которое назовем первообразным корнем по модулю m_1 и модулю m_2, найдем как

$$g = m_2\, m_2'\, g_1 + m_1\, m_1'\, g_2 \pmod{m_1\, m_2} \qquad (1)$$

где: $m_2\, m_2' \equiv 1 \pmod{m_1}$,

$m_1\, m_1' \equiv 1 \pmod{m_2}$.

Поиск такого числа можно распространить и на случай большего числа простых делителей составного числа, как это сделано в [2].

Число g является первообразн**ы**м корнем по модулю m_1 и первообразным корнем по модулю m_2. Нам сейчас не важно, чтобы g был наименьшим среди всех первообразных корней.

Заметим, что первообразный корень найденный по формуле (1) не является первообразным корнем по модулю произведения модулей. Доказательство приведено в 4.5 (Теорема4).

3.5. Обратные числа по модулю составного числа.

Два числа называются взаимно обратными по модулю m, если их произведение сравнимо с 1 по модулю m. Сравнения вида

$$ax \equiv b(\mathrm{mod}\, m) \qquad (1)$$

рассмотрены в [2] Гл. 4, § 2. Сравнение (1) имеет решение всегда, если $(a, m)=d=1$ и решение единственное.

Если $d>1$ то сравнение имеет d решений в случае, когда $\boldsymbol{b}$ делится на d. В противном случае сравнение не имеет решения.

Чтобы найти число $\boldsymbol{x}$ обратное к заданному числу $\boldsymbol{a}$ по модулю $\boldsymbol{m}$, мы в сравнении (1) приравняем $\boldsymbol{b}$ к 1. Тогда

$$\boldsymbol{a \cdot x \equiv 1 (mod m)} \qquad (2)$$

Решение последнего сравнения существует только при $(a, m)=d=1$. Если $d>1$, то число $\boldsymbol{b}=1$ не делится на d и не будет решения.

Действительно, если $\boldsymbol{a}$ и $\boldsymbol{m}$ делятся на какое то число m_1, то сравнение (2) не имеет решения, так как в случае разрешимости сравнения должно иметь решение сравнения и по модулю m_1 делящее $\boldsymbol{m}$ и $\boldsymbol{a}$ и тогда приходим к неверному сравнению

$$\boldsymbol{0 \equiv 1 (mod m_1).}$$

Таким образом, чтобы существовало число $\boldsymbol{x}$ обратное по модулю $\boldsymbol{m}$ к числу $\boldsymbol{a}$, числа $\boldsymbol{a}$ и $\boldsymbol{m}$ должны быть взаимно простыми.

Если взять модуль $\boldsymbol{m!}$, то для любого $\boldsymbol{a<m}$ не существует обратного числа по модулю $\boldsymbol{m!}$.

§4. СТЕПЕННЫЕ ВЫЧЕТЫ.

4.1.Свойства степенных вычетов.

Отметим некоторые свойства степенных вычетов, которыми в дальнейшем воспользуемся.

С в о й с т в о 1. Произведение степенных вычетов есть степенной вычет.

Это утверждение следует из того, что произведение степенных функций есть степенная функция.

$$x^n \cdot y^n = (xy)^n \qquad (1)$$

Рассмотрев сравнение левой и правой частей последнего равенства по модулю ***m,*** получим

$$V_x \cdot V_y \equiv V_{xy} (\mathrm{mod}\, m) \qquad (2)$$

где: $V_x \equiv x^n (\mathrm{mod}\, m)$, $V_y \equiv y^n (\mathrm{mod}\, m)$, $V_{xy} \equiv (xy)^n (\mathrm{mod}\, m)$ - степенные вычеты.

С в о й с т в о 2. Для любого степенного вычета V по модулю простого числа ***m*** существует обратный по модулю ***m*** степенной вычет V'.

Пусть степенной вычет $V \equiv x^p (\mathrm{mod}\, m)$. Для любого ***x***, как следует из 3.3, существует обратный ему по модулю ***m*** число x' такое, что $x \cdot x' \equiv 1 (\mathrm{mod}\, m)$. Тогда $x^p \cdot x'^p = (x \cdot x')^p \equiv 1 (\mathrm{mod}\, m)$. Следовательно, существует $V' \equiv (x')^p (\mathrm{mod}\, m)$ такой, что $V \cdot V' \equiv 1 (\mathrm{mod}\, m)$.

С в о й с т в о 3. Для любого вычета степени p-простого нечетного числа, существует отрицательный вычет той же степени той же абсолютной величины, Это утверждение основано на том, что если существует решение сравнения $x^p \equiv V (\mathrm{mod}\, m)$, то верно и сравнение $(m-x)^p \equiv -V (\mathrm{mod}\, m)$. Следовательно, для любого V существует другой степенной вычет ***m*-V.**

С в о й с т в о 4. Любой степенной вычет V по модулю простого числа ***m*** можно представить как произведение любого другого степенного вычета V_1 на соответствующий третий степенной вычет V_2 такой, что

$$V_1 \cdot V_2 \equiv V (\mathrm{mod}\, m) \qquad (1)$$

Чтобы показать существование такого степенного вычета умножим последнее сравнение на V_1' -обратный по модулю ***m*** степенному вычету V_1 . Тогда из (1) получим

$$V_2 \equiv V \cdot V_1' (\mathrm{mod}\, m)$$

Правая часть, как следует из С в о й с т в а1, есть степенной вычет как произведение степенных вычетов, а следовательно существует степенной вычет V_2.

С в о й с т в о 5. Если разложим хотя бы один степенной вычет в сумму двух степенных вычетов, то любой степенной вычет разложим в сумму двух степенных вычетов.

Допустим, что один из степенных вычетов разложим в сумму двух степенных вычетов

$$u_3 \equiv u_1 + u_2 (\mathrm{mod}\, m) \qquad (1)$$

Умножим сравнение на u_3' обратный к u_3 по модулю ***m***.Тогда

$$1 \equiv u_1 \cdot u_3' + u_2 \cdot u_3' (\mathrm{mod}\, m) \qquad (2)$$

В правой части каждое произведение вычетов есть степенной вычет на основании С в о й с т в а1. Пусть $u_4 \equiv u_1 \cdot u_3' (\mathrm{mod}\, m)$ и $u_5 \equiv u_2 \cdot u_3' (\mathrm{mod}\, m)$. Из (2) получим

$$1 \equiv u_4 + u_5 (\mathrm{mod}\, m) \qquad (3)$$

Мы получили разложение степенного вычета 1 в сумму двух степенных вычетов u_4 и u_5. Теперь умножая сравнение (3) на любой степенной вычет можем получать его разложение в сумму двух степенных вычетов.

С в о й с т в о 6. Произведение степенного вычета на степенной невычет есть степенной невычет.

Допустим обратное

$$u_1 \cdot u \equiv u_2 (\mathrm{mod}\, m) \qquad (1)$$

где: u_1, u_2 - степенные вычеты,

u - степенной невычет.

Не может быть, чтобы u_2 был вычетом так как умножая сравнение на $u_1^{/}$ такой, что $u_1 \cdot u_1^{/} \equiv 1 (\mathrm{mod}\, m)$, из сравнения(1) получим невозможное сравнение

$$u \equiv u_2 \cdot u_1^{/} (\mathrm{mod}\, m) \qquad (2)$$

в правой части которого имеем произведение двух степенных вычетов, что является степенным вычетом, а левая часть по определению является невычетом. Следовательно u_2 - невычет.

4.2.Сравнения по модулю составного числа.

Сравнения вида $x^n \equiv a (\mathrm{mod}\, m)$ подробно рассмотрены в [2].Число решений такого сравнения равно $d = (n, \varphi(m))$. Решения существуют если ***a*** является степенным вычетом и ***inda*** кратен ***d***. Эти вопросы рассмотрены для $m = p^{\alpha}$ или $m = 2 \cdot p^{\alpha}$.

Мы рассмотрим сравнения по модулю произведения двух простых чисел. Пусть дано

$$x^p \equiv V (\mathrm{mod}\, m_1 \cdot m_2) \qquad (1)$$

где: ***p*** - простое нечетное число,

$\boldsymbol{m}_1$, $\boldsymbol{m}_2$ -простые числа,

Число V $< m_1 \cdot m_2$ и назовем его вычетом степени ***p*** по модулю $m_1 \cdot m_2$.

Если сравнение (1) имеет решение по модулю произведения модулей $m_1 \cdot m_2$ то имеют решения сравнения по модулю $\boldsymbol{m}_1$ и модулю $\boldsymbol{m}_2$.

$$x^p \equiv V(\mathrm{mod}\, m_1) \quad (2)$$

$$x^p \equiv V(\mathrm{mod}\, m_2) \quad (3)$$

Рассмотрим каждое из этих сравнений отдельно. Если $\varphi(m_1)$ тождественно не равен нулю по модулю p, число решений сравнения (2) равно $d = (n, \varphi(m_1))$=1. V является степенным вычетом. Класс чисел по модулю m_1 являющихся вычетами можно выразить как

$$V \equiv V_1 + k_1 \cdot m_1 \quad (4)$$

где: V_1 - наименьший положительный степенной вычет,

k_1 - целое число

Рассмотрим вопрос о существовании решения для различных значений V_1. Пусть в сравнении

$$(g^i)^p \equiv V_i(\mathrm{mod}\, m_1) \quad (5)$$

где: g- первообразный корень по модулю m_1,

V_i - наименьший положительный степенной вычет,

Целое число ***i*** изменяется от 1 до $\varphi(m_1)$. Тогда g^i пробегает полную систему вычетов по модулю m_1.Поскольку рассматриваемое сравнение имеет одно решение по модулю m_1, никакие два значения g^i и g^j не дадут один какой то степенной вычет V_i. Следовательно каждое из $\varphi(m_1)$ различных значений g^i дадут различные значения V_i, и потому число степенных вычетов также равно $\varphi(m_1)$.

Таким образом, V_i пробегает полную систему вычетов по модулю m_1 так же как g^i только в другой последовательности.

Следовательно для любого $V_i < m_1$ существует решение и оно единственное.

Сравнение (3) тоже имеет единственное решение при любом V.

Вычет V по модулю m_2 можно представить как

$$V = V_2 + k_2 \cdot m_2 \qquad (6)$$

где: $V_2 < m_2$ - наименьший положительный степенной вычет по модулю m_2.

k_2 - целое число.

Равенства (4), (6) дают классы чисел по модулю m_1 и m_2 являющихся степенными вычетами по модулю m_1 и m_2. С учетом этого можно из сравнений (2), (3) написать два других сравнения

$$x^p \equiv V_1 (\mathrm{mod}\, m_1) \qquad (7)$$

$$x^p \equiv V_2 (\mathrm{mod}\, m_2) \qquad (8)$$

Таким образом, зная вычет V по модулю $m_1 \cdot m_2$, мы нашли наименьшие положительные вычеты V_1 и V_2 по модулям m_1 и m_2 соответственно. Можно провести и обратное преобразование по известной методике [2]

$$V \equiv m_2 \cdot m_2^{/} \cdot V_1 + m_1 \cdot m_1^{/} \cdot V_2 (\mathrm{mod}\, m_1 \cdot m_2) \qquad (9)$$

где: $m_2 \cdot m_2^{/} \equiv 1 (\mathrm{mod}\, m_1)$, $m_1 \cdot m_1^{/} \equiv 1 (\mathrm{mod}\, m_2)$

После такого преобразования можно из двух сравнений (7),(8) перейти к сравнениям (2),(3).

Если сравнения (7),(8) имеют по одному решению, то и сравнения (2),(3) тоже имеют по одному решению.

Пусть решениями являются соответственно для (2) и (3)

$$x = x_1 (\mathrm{mod}\, m_1) \qquad (10)$$

$$x = x_2 (\mathrm{mod}\, m_2) \qquad (11)$$

Совместное решение последних двух сравнений дает результат

$$x \equiv m_2 \cdot m_2^{/} \cdot x_1 + m_1 \cdot m_1^{/} \cdot x_2 (\mathrm{mod}\, m_1 \cdot m_2) \qquad (12)$$

Полученное решение сравнения является решением по модулю $m_1 \cdot m_2$.

Множество решений по модулю m_1 представляет собой класс чисел по модулю m_1

$$x = x_1 + k_1 \cdot m_1 \qquad (13)$$

а по модулю m_2

$$x = x_2 + k_2 \cdot m_2 \qquad (14)$$

Решение по модулю $m_1 \cdot m_2$ возможно, когда правые части (13), (14) сравнимы по модулю $m_1 \cdot m_2$

$$x_1 + k_1 \cdot m_1 \equiv x_2 + k_2 \cdot m_2 (\mathrm{mod}\, m_1 \cdot m_2) \qquad (15)$$

Решения x_1 и x_2 являются единственными по модулям m_1 и m_2 соответственно. Решение сравнения (1) тоже единственное, что очевидно из (12) и (15), а поскольку существуют решения x_1 и x_2, существует и решение для (1).

4.3 Степенные вычеты по модулю 3m.

Рассмотрим сравнение

$$g^{ip} \equiv u \,(\mathrm{modm}) \qquad (1)$$

где:***g***-первообразный корень,

u -наименьший положительный вычет,

i - целое число,

p - простое число,

m=kp+1 - простое число.

Если ***i*** пробегает все значения от 0 до $\frac{\varphi(m)}{p}$, то g^{ip}

пробегает все вычеты степени ***p*** по модулю ***m***. Если ***u*** является наименьшим степенным вычетом по модулю ***m,*** то наименьшим степенным вычетом по модулю ***3m*** будет одно из трех значений ***u, m+u,*** или ***2m+u*** . Форма степенного вычета по модулю $3m$ зависит от модуля ***m*** и от того с каким числом сравним вычет ***u*** по модулю 3.

Введем обозначения с индексами для наименьших степенных вычетов, где индекс будет показывать с каким числом 0, 1, или 2 сравним степенной вычет по модулю 3. Так, $u_0 \equiv 0(\mathrm{mod}\,3)$, $u_1 \equiv 1(\mathrm{mod}\,3)$, $u_2 \equiv 2(\mathrm{mod}\,3)$.

Методология поиска следующая. Если в сравнение (1) $u = u_1 \equiv 1(\mathrm{mod}\,m)$, то это сравнение по модулю $3\boldsymbol{m}$ для $g \equiv 0\,(\mathrm{mod}3)$ и ***m***=2(mod3) примет вид

$$g^{ip} \equiv m + u_1\,(\mathrm{mod}3\boldsymbol{m}) \qquad (2)$$

Это верно поскольку левая часть всегда сравнима с нулем по модулю 3 так как $g \equiv 0\,(\mathrm{mod}3)$, а правая часть также сравнима с нулем по модулю 3 так как $u_1 \equiv 1\,(\mathrm{mod}3)$, $m \equiv 2\,(\mathrm{mod}3)$, а следовательно $m + u_1 \equiv 0\,(\mathrm{mod}3)$. Если сравнение справедливо по модулю 3 и по модулю m, то оно справедливо и по модулю их произведения ***3m*** [2].

Если же в (1) $u = u_0 \equiv 0\,(\mathrm{mod}3)$ то сравнение (1) примет вид

$$g^{ip} \equiv u_0\,(\mathrm{mod}3\mathrm{m}) \qquad (3)$$

И наконец третий вариант. При $u = u_2 \equiv 2\ (\mathrm{mod}3)$

$$g^{ip} \equiv 2m + u_2\,(\mathrm{mod}3\mathrm{m}) \qquad (4)$$

Таким образом, зная наименьший положительный степенной вычет по модулю ***m,*** мы можем однозначно найти наименьший положительный степенной вычет по модулю ***3m***. Пользуясь этой методикой найдем степенные вычеты по модулю ***3m*** при различных ***g*** и ***m***. Все эти варианты сведем в таблицы для $\mathrm{m} \equiv 2(\mathrm{mod}3)$ и $\mathrm{m} \equiv 1(\mathrm{mod}3)$.

Таблица 3

$m \equiv 2 (\mathrm{mod} 3)$

$g \equiv 0 (\mathrm{mod} 3)$	V_0	$m+V_1$	$2m+V_2$
$g \equiv 1 (\mathrm{mod} 3)$	V_1	$m+V_2$	$2m+V_0$
$g \equiv 2 (\mathrm{mod} 3)$	V_2	$m+V_0$	$2m+V_1$

нечетная степень

Таблица 4

$m \equiv 1 (\mathrm{mod} 3)$

$g \equiv 0 \ (\mathrm{mod} 3)$	V_0	$m+V_1$	$2m+V_2$
$g \equiv 1 (\mathrm{mod} 3)$	V_1	$m+V_2$	$2m+V_0$
$g \equiv 2 (\mathrm{mod} 3)$	V_2	$m+V_0$	$2m+V_1$

нечетная степень

Четные степени для $g \equiv 2 (\mathrm{mod} 3)$ совпадают со случаем $g \equiv 1 (\mathrm{mod} 3)$ так как при $g \equiv 2 (\mathrm{mod} 3)$ $g^{2i} \equiv 1 \ (\mathrm{mod} 3)$.

С л е д с т в и е. Как следует из полученного результата разность любых двух соседних по модулю ***m*** степенных вычетов по модулю 3m сравнимы с нулем по модулю 3. Для случая $m \equiv 2 (\mathrm{mod} 3)$ разность соседних по модулю ***m*** вычетов равна m+1, и для случая $m \equiv 1 (\mathrm{mod} 3)$ разность равна 2m+1. Для одного и другого случая разность кратна трем. Это и понятно поскольку степенные функции имеют одно основание. Следует однако иметь ввиду, что степени должны быть одинаковой четности при $g \equiv 2 (\mathrm{mod} 3)$.

4.4. Количество степенных вычетов по модулю составного числа.

Рассмотрим вопрос о количестве степенных вычетов по модулю произведения двух простых чисел $m_1 \, m_2$.

Как показано в 3.4, §3, найдем число являющееся первообразным корнем по модулю m_1 и модулю m_2.

Не обязательно, чтобы этот первообразный корень был наименьшим среди всех первообразных корней. Главное, чтобы он принадлежал степени $\varphi(m_1)$ по модулю m_1 и степени $\varphi(m_2)$ по модулю m_2. Для определенности будем полагать, что $m_1 < m_2$.

Степенная функция g^j пробегает полную систему вычетов по модулю m_2 и по модулю m_1 если $\boldsymbol{j}$ изменяется от 1 до $\varphi(m_2)$ так как m_2 и m_1 простые, а $\varphi(m_2) > \varphi(m_1)$.

Поставим вопрос – существует ли такое значение $\boldsymbol{j}$, при котором

$$g^j \equiv 1 (\mathrm{mod}\, m_1 m_2) \qquad (1)$$

Более того, g^j должен пробежать все вычеты полной системы вычетов по модулю m_1 и все вычеты полной системы вычетов по модулю m_2.

Чтобы условие (1) выполнить при минимальном значении j, рассмотрим то же сравнение по модулям m_1 и m_2.

$$g^j \equiv 1 (\mathrm{mod}\, m_1) \qquad (2)$$

$$g^j \equiv 1 (\mathrm{mod}\, m_2) \qquad (3)$$

Чтобы сравнение (2) выполнить необходимо, чтобы

$$\boldsymbol{j} \equiv 0 (\mathrm{mod}\, \varphi(m_1)) \qquad (4)$$

а для сравнения (3) должно выполнятся сравнение

$$\boldsymbol{j} \equiv 0 (\mathrm{mod}\, \varphi(m_2)) \qquad (5)$$

Условия (4) и (5) выполняются тогда, когда $\boldsymbol{j}$ кратно любому делителю $\varphi(m_1)$ и кратно любому делителю $\varphi(m_2)$. Таким числом является наименьшее общее кратное (НОК) двух чисел $\varphi(m_1)$ и $\varphi(m_2)$. Таким образом, j=НОК($\varphi(m_1), \varphi(m_2)$). Обозначим α = НОК($\varphi(m_1), \varphi(m_2)$). Тогда

$$g^\alpha \equiv 1 (\mathrm{mod}\, m_1 m_2) \qquad (6)$$

Используя свойство сравнения Эйлера (**§2)** убеждаемся в справедливости последнего сравнения.

Рассмотрим теперь вопрос о количестве степенных вычетов по модулю составного числа. Для этого рассмотрим сравнение

$$x^p \equiv V\ (\mathrm{mod}\, m_1\ m_2) \qquad (7)$$

Если это сравнение имеет решения. то имеют решения и сравнения по модулю m_1 и m_2.

$$x^p \equiv V_1 (\mathrm{mod}\, m_1) \qquad (8)$$

$$x^p \equiv V_2 (\mathrm{mod}\, m_2) \qquad (9)$$

Степенной вычет V в (7) равен

$V = V_1 + k_1\ m_1 = V_2 + k_2\ m_2$. Для сравнений (8), (9) количество решений равно соответственно

$d_1 =$ (p, $\varphi(m_1)$), $d_2 =$ (p, $\varphi(m_2)$). Количество степенных вычетов по модулю m_1 и модулю m_2 равно соответственно $n_1 = \dfrac{\varphi(m_1)}{d_1}$, $n_2 = \dfrac{\varphi(m_2)}{d_2}$ и зависят они от того делятся на ***p*** $\varphi(m_1)$ и $\varphi(m_2)$ или нет. От этого зависят значения d_1 и d_2.

Имея сравнения (8),(9) и пользуясь формулой (9) из раздела 4.2 можно определить степенной вычет V по модулю $m_1 \cdot m_2$

$$V = m_2 m_2' \cdot V_1 + m_1 m_1' \cdot V_2 (\mathrm{mod}\, m_1 m_2) \qquad (10)$$

Сочетания любого степенного вычета V_1 по модулю m_1 с любым степенным вычетом V_2 по модулю m_2 дает степенной вычет по модулю $m_1 \cdot m_2$.

Любое число кратное m_1 или m_2 в степени ***p*** дает степенной вычет по модулю $m_1 \cdot m_2$. Рассмотрим сравнение

$$(km_1)^p \equiv V\ (\mathrm{mod}\, m_1 \cdot m_2) \qquad (11)$$

Левая часть сравнима с нулем по модулю m_1, а следовательно и правая часть также сравнима с нулем по модулю m_1. По модулю m_1 сравнение всегда выполняется.

Если V является степенным вычетом, то существует решение и по модулю m_2. Для сравнения $(km_1)^p \equiv V \pmod{m_2}$ количество решений, как известно [2], равно d_2=(p, $\varphi(m_2)$), а количество степенных вычетов - $\frac{\varphi(m_2)}{d_2}$.

Совершенно аналогично находим количество степенных вычетов для ряда чисел кратных m_2 и меньших чем $m_1 \cdot m_2$.

Исходя из вышеизложенного находим общее количество степенных вычетов по модулю $m_1 \cdot m_2$

$$n=\frac{\varphi(m_1)}{d_1} \cdot \frac{\varphi(m_2)}{d_2} + \frac{\varphi(m_1)}{d_1} + \frac{\varphi(m_2)}{d_2} \qquad (12)$$

4.5.Теорема 4

Теорема4. ***Первообразного корня по модулю нечетного составного числа не существует.***

Д о к а з а т е л ь с т в о. Пусть нам даны два нечетных простых числа m_1 и m_2. Число являющееся первообразным корнем по модулю m_1 и по модулю m_2 мы можем найти по формуле (9) раздела 4.2

$$g = m_2 m_2' \cdot g_1 + m_1 m_1' \cdot g_2 \pmod{m_1 m_2} \qquad (1)$$

где: g_1 - первообразный корень по модулю m_1,

g_2 -первообразный корень по модулю m_2,

$m_2 m_2' \equiv 1 \pmod{m_1}$

$m_1 m_1' \equiv 1 \pmod{m_2}$

Любое сочетание различных первообразных корней по модулю m_1 и модулю m_2 дает нам число являющееся одновременно первообразным корнем по модулю m_1 и первообразным корнем по модулю m_2.

Введем обозначения $\varphi(m_1)=\mathrm{n}\,k_1$, $\varphi(m_2)=\mathrm{n}\,k_2$

где: n- наибольший общий делитель $\varphi(m_1)$ и $\varphi(m_2)$

-НОД($\varphi(m_1), \varphi(m_2)$).

Числа k_1 и k_2 взаимно простые так как все общие делители вошли в ***n***. Тогда будем иметь $\mathrm{n}\,k_1\,k_2$=НОК($\varphi(m_1), \varphi(m_2)$). Произведение $\varphi(m_1)$ и $\varphi(m_2)$ можно представит как

$$\varphi(m_1)\,\varphi(m_2)=\text{НОД}(\varphi(m_1),\varphi(m_2))\cdot\text{НОК}(\varphi(m_1),\varphi(m_2))=\beta\cdot\alpha \quad (2)$$

Рассмотрим теперь последовательность g^j при изменениях ***j*** от 1 до $\alpha =$ НОК($\varphi(m_1), \varphi(m_2)$). При этом g^j пробегает вычетов степени p в количестве $\frac{\alpha}{p}$. Изменения ***j*** берем от 1 до α потому, что $g^{\alpha}\equiv 1(\mathrm{mod}\, m_1 m_2)$ и при дальнейших изменениях ***j*** получаем повторение степенных вычетов. Это утверждение верно потому, что два числа g^{j_1} и g^{j_2} сравнимы по модулю $m_1\cdot m_2$ если $g^{j_1-j_2}\equiv 1(\mathrm{mod}\, m_1\cdot m_2)$, а последнее имеет место если $j_1\equiv j_2(\mathrm{mod}\,\alpha)$.

Количество степенных вычетов, как следует из 4.5, равно

$\mathrm{n}=\frac{\varphi(m_1)}{d_1}\cdot\frac{\varphi(m_2)}{d_2}+\frac{\varphi(m_1)}{d_1}+\frac{\varphi(m_2)}{d_2}$. Число $\frac{\alpha}{d_2}$ - это число вычетов степени p, которое пробегает g^j, причем не зависимо от выбранного g, так как для любого g имеет место сравнение $g^{\alpha}\equiv 1(\mathrm{mod}\,\alpha)$.

Если используем в качестве основания степенной функции другое число, которое также является первообразным корнем по модулю m_1 и m_2, то g^j также пробегает $\frac{\alpha}{p}$ степенных вычета. но это количество всегда меньше чем общее количество степенных вычетов потому, что для любого простого числа m_1 значение $\frac{\varphi(m_1)}{d_1} \geq 2$. Последнее утверждение верно потому, что для любого $m_1 \geq 3$, НОД $\varphi(m_1)$ и $\varphi(m_2)$ всегда содержит число 2.

Таким образом, какое бы число мы не взяли в качестве основания степенной функции, g^j пробегает не все степенные вычеты. Следовательно, нет первообразного корня по модулю $m_1 \cdot m_2$. Теорема доказана.

§5. РАЗЛОЖИМОСТЬ СТЕПЕННЫХ ВЫЧЕТОВ.

5.1. Разложимость степенных вычетов по модулю простого числа.

Степенной вычет по модулю m считается разложимым в сумму двух вычетов той же степени, если справедливо сравнение

$$U_1 \equiv U_2 + U_3 \ (mod\ m) \qquad (1)$$

Где: U_1, U_2, U_3 – степенные вычеты.

Если рассматривать разложение степенного вычета в сумму двух вычетов применительно к уравнению Ферма $c^p = b^p + a^p$, то $U_1 \equiv c^p (mod\ m)$, $U_2 \equiv в^p (mod\ m)$, $U_3 \equiv a^p (mod\ m)$.

Разложимость степенных вычетов в сумму двух вычетов той же степени тесно связано с доказательством теоремы Ферма.

Есть основание полагать, что Пьер Ферма анализируя разложимость степенных вычетов по модулям различных чисел пришел к своему выводу и дал именно такую формулировку теоремы: невозможно разложить куб на два куба, биквадрат на два биквадрата и в общем случае, любую степень большую двух в сумму двух таких же степеней [4].

Если уравнение Ферма

$$c^p=b^p+a^p \qquad (2)$$

имеет целочисленные решения, то левая и правая части равноостаточны при делении на любое число, в том числе и на какое то из чисел ***a, b, c*** или их делители. Другими словами, левая и правая части (2) сравнимы по модулю любого числа.

Существуют простые числа, по модулю которых для какого-то простого числа *m* вычеты степени ***p*** не разложимы в сумму двух вычетов той же степени. Примером может служить простое число 13, по модулю которого вычетами степени 3 являются числа 1, 5, 8, 12 и ни одно из них нельзя представить как сумму двух других.

В этом случае, чтобы уравнение Ферма для $p=3$ имело решение, какое то из чисел ***a, b,c*** должно быть кратным 13. Тогда возможно найти решения уравнения

$$c^n \equiv b^n+a^n \ (mod 13) \qquad (3)$$

Если по модулю ***m*** нет разложимости, то это **m** должно делить какое то из чисел ***a, b, c.***

Для степени 2 такими числами являются 3 и 5 и потому любая тройка Пифагоровых чисел содержит числа делящиеся на 3 и 5.

При попытках доказать теорему Ферма рассматривают сравнения по модулю ***p*** так как известно соотношение $a^p \equiv a \ (mod \ p)$ и потому как правило, доказательство разделяют на два случая теоремы Ферма.

Мы рассмотрим в общем виде сравнения (1) по модулю простого числа ***m*** формы ***kp+1***. Если сравнение (1) получено из уравнения Ферма (2) и какое то из чисел ***a, b***, с делится на

m, то это будет частным случаем общего, когда одно из чисел U_1, U_2, U_3 равно нулю, т.е. это будет разложением с одним нулевым решением по модулю ***m***.

Чтобы изучить некоторые свойства и соотношения разложимых степенных вычетов проведем некоторые преобразования сравнения (1), в котором $U_1>0, U_2>0, U_3>0$.

На основании Свойства 2 (§4, 4.1) степенных вычетов существует степенной вычет U_1', такой, что $U_1 \cdot U_1' \equiv 1 \pmod m$.

Произведение степенных вычетов, как следует из С в о й с т в а1 степенных вычетов, есть степенной вычет.

На основании С в о й с т в а3 степенных вычетов существуют отрицательные степенные вычеты, поскольку ***p*** нечетное число.

Введем обозначения

$$V_1 \equiv U_3 \cdot U_1' (\mathrm{mod}\, m) \qquad (4)$$

$$V_3' \equiv U_2 \cdot U_1' (\mathrm{mod}\, m) \qquad (5)$$

После умножения сравнения (1) на U_1' и переноса всех членов в левую часть с учетом принятых обозначений получим

$$V_3' + V_1 + 1 \equiv 0 (\mathrm{mod}\, m) \qquad (6)$$

Умножим последнее сравнение на V_1' такой, что $V_1 \cdot V_1' \equiv 1 (\mathrm{mod}\, m)$ и получим

$$V_1' + V_3' \cdot V_1' + 1 \equiv 0 (\mathrm{mod}\, m) \qquad (7)$$

Умножим сравнение (6) на V_3 такой, что $V_3 \cdot V_3' \equiv 1 (\mathrm{mod}\, m)$. Тогда

$$V_1 \cdot V_3 + V_3 + 1 \equiv 0 (\mathrm{mod}\, m) \qquad (8)$$

Сравнения (7), (8) содержат взаимно обратные по модулю ***m*** степенные вычеты $V_3' \cdot V_1'$ и $V_1 \cdot V_3$ являющиеся произведением степенных вычетов.

Обозначим $V_2 \equiv V_3' \cdot V_1' (\mathrm{mod}\, m)$.

Тогда обратный к V_2 степенной вычет
$V_2' \equiv V_1 \cdot V_3 (\mathrm{mod}\, m)$. Это верно так как
$(V_1 \cdot V_3) \cdot (V_1' \cdot V_3') \equiv (V_1 \cdot V_1') \cdot (V_3 \cdot V_3') \equiv 1 \cdot 1 \equiv 1 (\mathrm{mod}\, m)$.

С учетом принятых обозначений из сравнений (6), (7), (8) получим три сравнения

$$V_3' + V_1 + 1 \equiv 0 (\mathrm{mod}\, m) \quad (9)$$

$$V_1' + V_2 + 1 \equiv 0 (\mathrm{mod}\, m) \quad (10)$$

$$V_2' + V_3 + 1 \equiv 0 (\mathrm{mod}\, m) \quad (11)$$

в которых вычеты со штрихами являются обратными по модулю ***m*** к соответствующим степенным вычетам без штрихов. Соотношения вычетов следующие

$$\begin{aligned} V_1' &= V_2 \cdot V_3 (\mathrm{mod}\, m) \\ V_2' &= V_1 \cdot V_3 (\mathrm{mod}\, m) \\ V_3' &= V_1 \cdot V_2 (\mathrm{mod}\, m) \end{aligned} \quad (12)$$

Из сравнений (9), (10), (11) видно, что любой из шести степенных вычетов имеет соседний степенной вычет, как например $V_1 + 1 = -V_3' (\mathrm{mod}\, m)$ или $V_3' + 1 = -V_1' (\mathrm{mod}\, m)$. Поскольку ***p*** нечетное число $-V_3'$ и $-V_1$, тоже являются степенными вычетами.

Определенное удобство может дать, если степенные вычеты выразить через функции с каким то одним основанием. Для сравнения по модулю простого числа удобно в качестве основания использовать первообразный корень, так как g^j пробегает полную систему вычетов по модулю ***m*** если ***j*** пробегает значения от 1 до $\varphi(m)$. Следовательно любой вычет можно изобразить в виде степенной функции Выразим степенные вычеты в виде степенных функций и продолжим анализ.

$$
\begin{aligned}
V_1 &\equiv g^{j_1 p} (\mathrm{mod}\, m) \\
V_1^{'} &\equiv g^{j_1^{'} p} (\mathrm{mod}\, m) \\
V_2 &\equiv g^{j_2 p} (\mathrm{mod}\, m) \\
V_2^{'} &\equiv g^{j_2^{'} p} (\mathrm{mod}\, m) \\
V_3 &\equiv g^{j_3 p} (\mathrm{mod}\, m) \\
V_3^{'} &\equiv g^{j_3^{'} p} (\mathrm{mod}\, m)
\end{aligned}
\qquad (13)
$$

где g – первообразный корень по модулю m.

Сумма степеней степенных функций, соответствующих взаимообратным вычетам, сравнимы с нулем по модулю $\varphi(m)$.

Следовательно, можно написать

$$
\begin{aligned}
j_1^{'} p + j_1 p &\equiv 0 (\mathrm{mod}\, \varphi(m)) \\
j_2^{'} p + j_2 p &\equiv 0 (\mathrm{mod}\, \varphi(m)) \\
j_3^{'} p + j_3 p &\equiv 0 (\mathrm{mod}\, \varphi(m))
\end{aligned}
\qquad (14)
$$

Поскольку соотношения (13) и (14) рассматриваем по модулю $\boldsymbol{m}$, а $g^{\varphi(m)\cdot k} \equiv 1 (\mathrm{mod}\, m)$ мы можем без ущерба отбросить степени, кратные $\varphi(m)$, т.е. довести степени до величин, меньших $\varphi(m)$. Поэтому в дальнейшем будем полагать, что $j_1 p < \varphi(m)$, $j_2 p < \varphi(m)$, $j_3 p < \varphi(m)$, $j_1^{'} p < \varphi(m)$, $j_2^{'} p < \varphi(m)$, $j_3^{'} p < \varphi(m)$. Тогда из (14) можно перейти к равенствам

$$
\begin{aligned}
j_1^{'} p + j_1 p &= \varphi(m) \\
j_2^{'} p + j_2 p &= \varphi(m) \\
j_3^{'} p + j_3 p &= \varphi(m)
\end{aligned}
\qquad (15)
$$

Из последнего можно написать

$$
\begin{aligned}
j_1^{'} p &= \varphi(m) - j_1 p \\
j_2^{'} p &= \varphi(m) - j_3 p \\
j_3^{'} p &= \varphi(m) - j_3 p
\end{aligned}
\qquad (16)
$$

Подставим соответствующие степенные функции в (12)

$$g^{\varphi(m)-j_3p} \equiv g^{j_1p} \cdot g^{j_2p} (\mathrm{mod}\, m)$$
$$g^{\varphi(m)-j_2p} \equiv g^{j_1p} \cdot g^{j_3p} (\mathrm{mod}\, m)$$
$$g^{\varphi(m)-j_1p} \equiv g^{j_2p} \cdot g^{j_3p} (\mathrm{mod}\, m)$$

Сравнивая степени любого из последних сравнений, получим

$$j_1p + j_2p + j_3p \equiv 0(\mathrm{mod}\, \varphi(m)) \qquad (17)$$

Теперь сложим левые и правые части равенства (16). Тогда

$$j_1^{'}p + j_2^{'}p + j_3^{'}p = 3\varphi(m) - j_1p - j_2p - j_3p \qquad (18)$$

Каждое слагаемое в (17) меньше $\varphi(m)$ и потому сумма меньше чем $3\varphi(m)$, а следовательно эта сумма равна $\varphi(m)$ либо $2\varphi(m)$. Если сумма в (17) равна $2\varphi(m)$, то другая сумма степеней со штрихами равна $\varphi(m)$. Если обратить внимание на сравнения (9), (10), (11), то эти сравнения содержат степенные вычеты V_1, V_2, V_3 и три обратных к ним степенных вычета V_1', V_2', V_3'.

Мы для определенности будем полагать, что

$$j_1p + j_2p + j_3p = \varphi(m) \qquad (19)$$
$$j_1^{'}p + j_2^{'}p + j_3^{'}p = 2\varphi(m)$$

Из последних двух равенств получим соотношение

$$2(j_1p + j_2p + j_3p) = j_1^{'}p + j_2^{'}p + j_3^{'}p \qquad (20)$$

Для определенности будем полагать, что $j_1p < j_2p < j_3p$, так как равных степеней нет в силу несравнимости вычетов V_1, V_2, V_3 по модулю m. Тогда из (22) следует $j_3^{'} < j_2^{'} < j_1^{'}$.

Попытка найти класс простых чисел, по модулю которых степенные вычеты не разложимы в сумму двух степенных вычетов, не увенчалась успехом.

5.2 Признаки разложимости степенных вычетов.

Признак1. ***Наличие соседних степенных вычетов.***

Из условия разложимости степенных вычетов

$$u_1 \equiv u_2 + u_3 (\mathrm{mod}\, m) \qquad (1)$$

где:m-простое число.

Обратный степенной вычет существует на основании С в о й с т в а2.

После умножения сравнения на u_3' обратный по модулю ***m*** к степенному вычету u_3 получим

$$u_1 \cdot u_3' \equiv u_2 \cdot u_3' + 1 (\mathrm{mod}\, m) \qquad (2)$$

Произведение степенных вычетов есть степенной вычет (Свойчтво1). Поэтому из последнего можно написать

$$u_4 \equiv u_5 + 1 (\mathrm{mod}\, m) \qquad (3)$$

где: $u_4 \equiv u_1 \cdot u_3' (\mathrm{mod}\, m)$, $u_5 \equiv u_2 \cdot u_3' (\mathrm{mod}\, m)$.

Из последнего видно, что степенные вычеты u_4 и u_5 являются соседними. Мы получили, что при разложимости хотя бы одного степенного вычета u_1 обязательно существуют какие то два соседних степенных вычета. Это можно считать как один из признаков разложимости степенных вычетов.

Как мы увидели выше, наличие соседних степенных вычетов является обязательным условием разложимости степенных вычетов, а их отсутствие – невозможность разложения любого степенного вычета.

В этом случае уравнение Ферма может иметь место только в том случае если какое то из чисел ***a, b, c*** кратно ***m***. Тогда сравнение $c^n \equiv b^n + a^n (\mathrm{mod}\, m)$ возможно.

Как будет показано ниже, квадратичные вычеты по модулю 3 и модулю 5 не разложимы и потому любая тройка Пифагоровых чисел содержит число кратное трем и число кратное пяти.

Признак 2. Если существуют два таких степенных вычета, что их произведение сравнимо с их же суммой по модулю ***m,*** то степенные вычеты по модулю m разложимы по модулю ***m***.

Допустим, что $V_1 \cdot V_2 \equiv V_1 + V_2 (\mathrm{mod}\, m)$. Перенося влево V_1 и вынося его за скобки получим $V_1 (V_2 - 1) \equiv V_2 (\mathrm{modm})$.

Если V_1 и V_2 являются степенными вычетами, то (V_2-1) тоже является степенным вычетом так как в противном случае в последнем сравнении V_2 был бы степенным невычетом, как следует из Свойства 6. Следовательно V_2 имеет соседний степенной вычет (V_2-1). Аналогичное можно сделать и для вычета V_1 и тогда $V_2 (V_1 - 1) \equiv V_1 (\mathrm{modm})$. Из последнего делаем вывод: у вычета V_1 тоже есть соседний степенной вычет.

Если возьмем из уравнений (9),(10) предыдущего раздела 5.1 два степенных вычета имеющих соседние степенные вычеты $(V_1 + 1)$ и $(V_1' + 1)$, то их произведение сравнимо с их суммой по модулю ***m***

$(V_1 + 1) \cdot (V_1' + 1) \equiv 1 + V_1 + V_1' + 1$ (modm).

Два признака разложимости тесно взаимосвязаны и одно из них следует из другого и обратно.

Признак3.Если $\varphi(m)$ не кратно ***p***, то сравнение вида $x^p \equiv V (\mathrm{mod}\, m)$ имеет единственное решение [2],Гл.6,§5, если V является степенным вычетом.

Любое число в степени ***p*** дает какой то степенной вычет, а поскольку вышеуказанное сравнение имеет единственное решение, любой вычет полной системы вычетов является степенью какого то числа из этой полной системы вычетов, то есть является степенным вычетом.

В связи с изложенным, вычеты степени ***p*** по модулю ***m*** при $\varphi(m)$ не кратном ***p***, разложимы в сумму двух степенных вычетов.

5.3. Частные случаи разложимости степенных вычетов.

Как следует из П р и з н а к а1 разложимости степенных вычетов, чтобы квадратичные вычеты были разложимы в сумму двух квадратичных вычетов необходимо и достаточно, чтобы из всех квадратичных вычетов были хотя бы два соседних квадратичных вычета.

Рассмотрим разложимость квадратичных вычетов по модулю некоторых простых чисел.

5.3.1 Модуль 3. По модулю 3 квадратичным вычетом является единственное число – единица. Разложимость квадратичного вычета в сумму двух квадратичных вычетов не имеет места.

5.3.2 Модуль 5. По модулю 5 квадратичных вычетов два. Это числа 1,4 и они не соседние. Здесь тоже разложимость квадратичных вычетов по модулю 5 не имеет места.

В связи с тем, что квадратичные вычеты по модулю 3 и по модулю 5 не разложимы в сумму двух квадратичных вычетов, любая тройка Пифагоровых чисел содержит число кратное трем и содержит число кратное пяти. Это и видно если проанализировать формулы для получения Пифагоровых троек чисел: $m^2+n^2, m^2-n^2, 2mn,$ где ***m*** и ***n*** взаимно простые числа. Примеры Пифагоровых троек: 5,4,3 и 13,12,5.

5.3.3Модуль 2p+1. Если число 2p+1 простое, то вычетов степени ***p*** всего два – вычет 1 и m-1. Любой из этих вычетов не разложим в сумму двух степенных вычетов при $p \geq 3$ по модулю 2p+1.

5.3.4Модуль 4p+1. Если число 4p+1 является простым числом, то количество вычетов степени ***p*** равно

$\frac{\varphi(m)}{p} = \frac{4p}{p} = 4$. Два степенных вычета мы знаем не зависимо от значения простого нечетного р – это единица и минус единица или ***m***-1. Сумма двух оставшихся степенных вычета тоже равна ***m***. Обозначим их как V и ***m***-V.

Теперь рассмотрим вопрос разложимости степенных вычетов в сумму двух степенных вычетов.

Как следует из Пр и з н а к а1 разложимости степенных вычетов, чтобы разложимость имела место должны быть хотя бы два соседних степенных вычета.

Пусть для определенности V<***m***-V. Чтобы вычет V был соседним к единице, он должен быть равен двум. В этом случае и число $2 \cdot 2 = 4$ тоже должен быть степенным вычетом как произведение степенных вычетов. Число 4p=m-1 является степенным вычетом, а следовательно и ***p*** является степенным вычетом, так как 4 и ***m***-1 являются степенными вычетами. Число ***2p*** тоже является степенным вычетом как произведение двух степенных вычетов.

Степенных вычетов уже более четырех, а этого не может быть. Следовательно, число 2 не может быть степенным вычетом по модулю m=4p+1.

Если единица не имеет соседнего степенного вычета, то и (m-1) не имеет соседнего степенного вычета.

Чтобы разложимость степенных вычетов имело место остается единственное – предположить, что V и m-V соседние степенные вычеты. Тогда m-V=V+1 или m-1=2V Из последнего имеем

$$V = \frac{m-1}{2} = 2p$$

$$m\text{-}V = m - \frac{m-1}{2} = \frac{m+1}{2} = 2p+1$$

Полученное значение V=2p, как мы уже говорили выше, не является степенным вычетом, а следовательно нет соседних степенных вычетов по модулю ***m=4p+1*** и поэтому

делаем вывод: степенные вычеты по модулю m=4p+1 не разложимы в сумму двух степенных вычетов.

5.4. Разложимость квадратичных вычетов.

Для всех простых чисел m>5 квадратичные вычеты по модулю ***m*** разложимы в сумму двух квадратичных вычетов. Докажем теорему.

Теорема5 . ***Квадратичные вычеты по модулю любого простого числа m>5 разложимы в сумму двух квадратичных вычетов.***

Д о к а з а т е л ь с т в о. Как известно [2], число квадратичных вычетов по модулю простого числа равно $\frac{\varphi(m)}{2}$ и столько же квадратичных невычетов.

Для доказательства теоремы следует рассмотреть два случая:

1. $\frac{\varphi(m)}{2} \equiv 1(\mathrm{mod}2)$

2. $\frac{\varphi(m)}{2} \equiv 0(\mathrm{mod}2)$

Для первого случая ***m***-1 не является квадратичным вычетом. Из условия разложимости хотя бы одного квадратичного вычета имеем $u \equiv u_1 + u_2(\mathrm{mod}\, m)$. С в о й с т в а 1,2 и П р и з н а к 1 разложимости степенных вычетов применимы и для квадратичных вычетов. Покажем теперь наличие соседних квадратичных вычетов для каждого из двух вышеуказанных случаев.

С л у ч а й 1. Пусть $\frac{\varphi(m)}{2} \equiv 1(\mathrm{mod}2)$. Рассмотрим ряд чисел полной системы вычетов от 1 до m-1.

Как сказано в §3, любой вычет полной системы вычетов может быть представлен как $\boldsymbol{a} \equiv g^{\frac{\varphi(m)}{P}i+j} (\mathrm{mod}m)$

где:g- первообразный корень.

Тогда число дополняющее *a* до m равно

$$\mathrm{m}\text{-}a \equiv g^{\frac{\varphi(m)}{P}i+j+\frac{\varphi(m)}{2}} (\mathrm{mod}m)$$

В правой части последних двух сравнений степени $\boldsymbol{g}$ имеют различную четность так как их разность сравнима с единицей по модулю два.

$$\frac{\varphi(m)}{2}i + j + \frac{\varphi(m)}{2} - (\frac{\varphi(m)}{2}i + j) \equiv 1(\mathrm{mod}\,2)$$

Следовательно, одно из чисел $\boldsymbol{a}$ или $\boldsymbol{m}$-$\boldsymbol{a}$ является квадратичным вычетом, а другое - квадратичным невычетом.

Рассмотрим теперь ряд чисел полной системы вычетов по модулю $\boldsymbol{m}$. Числа 1 и 4 являются квадратичными вычетами. Если число 2 или 3 является квадратичным вычетом, то мы имеем соседние 1 и 2 или соседние 3 и 4 квадратичные вычеты. Если 2 и 3 являются квадратичными невычетами, то их дополнения до $\boldsymbol{m}$ то есть $\boldsymbol{m}$-2 и $\boldsymbol{m}$-3 являются соседними квадратичными вычетами.

Таким образом, для С л у ч а я1 соседние квадратичные вычеты имеются всегда, а следовательно квадратичные вычеты разложимы в сумму двух степенных вычетов.

С л у ч а й 2. Пусть $\frac{\varphi(m)}{2} \equiv 0(\mathrm{mod}\,2)$. В данном случае оба числа

$$a \equiv g^{\frac{\varphi(m)}{2}i+j} (\mathrm{mod}\, m) \quad \text{и} \quad m-a \equiv g^{\frac{\varphi(m)}{2}i+j+\frac{\varphi(m)}{2}} (\mathrm{mod}\, m)$$

принадлежат одному столбцу матрицы вычетов. Как и в предыдущем случае, рассмотрим ряд чисел полной системы вычетов по модулю ***m*** от 1 до $\frac{m-1}{2}$ и другой ряд чисел, которые дополняют числа первого ряда до ***m***.

Изобразим вычеты по модулю ***m*** в виде степенной функции с основанием равным первообразному корню g. Если какой то вычет первого ряда *a* изображается как

$$a \equiv g^{\frac{\varphi(m)}{2}i+j} (\mathrm{mod}\, m) \qquad (1)$$

то его дополнение до ***m*** изображается как

$$m-a \equiv g^{\frac{\varphi(m)}{2}i+j+\frac{\varphi(m)}{2}} (\mathrm{mod}\, m) \qquad (2)$$

Степени в правых частях последних двух сравнений отличаются, как и должно быть, на $\frac{\varphi(m)}{2}$. Если разность степеней равна $\frac{\varphi(m)}{2}$, а $\frac{\varphi(m)}{2} \equiv 0(\mathrm{mod}\, m)$ в рассматриваемом случае, степени имеют одинаковую четность. Это значит, что не зависимо от того какое число ***a*** из ряда мы выбираем, числа ***a*** и (***m-a***) являются квадратичными вычетами или оба являются квадратичными невычетами.

Числа первого ряда 1 и 4 являются квадратичными вычетами. Допустим худшее, что числа 2,3,5. являются квадратичными невычетами, чтобы не было ни одной пары квадратичных вычетов до 5.

Далее. Как уже говорилось, количество квадратичных вычетов и невычетов в полной системе вычетов по модулю простого ***m*** равны по $\frac{\varphi(m)}{2}$. Так как ***a*** и (***m-a***) могут быть оба квадратичными вычетами или оба квадратичными невычетами. Первый и второй ряды содержат одинаковое число квадратичных вычетов и квадратичных невычетов. Следовательно количество квадратичных вычетов и невычетов поделены пополам. В этом случае, чтобы общее количество квадратичных вычетов было равно общему количеству квадратичных невычетов, в каждом ряду количество квадратичных вычетов должно быть равно количеству квадратичных невычетов.

Из чисел меньших 5 имеем два квадратичных вычета и два квадратичных невычета. Возможно ли для всех чисел выше 5 только чередование квадратичных вычетов и квадратичных невычетов, чтобы отсутствовали соседние квадратичные вычеты.

Если такое чередование квадратичных вычетов с квадратичными невычетами возможно, а число 5 является квадратичным невычетом, как мы предположили, то все четные числа вплоть до $\frac{m-1}{2}=\frac{\varphi(m)}{2}$, являющееся четным числом в нашем случае, будут квадратичными вычетами. Тогда, как следует из §3, 3.2, его дополнение до ***m*** равно $m-\frac{m-1}{2}=\frac{m+1}{2}$ тоже является квадратичным вычетом. А он всегда является соседним к $\frac{m+1}{2}$, так как их разность равна

$$\frac{m+1}{2}-\frac{m-1}{2}=1$$

Таким образом, при самом худшем распределении квадратичных вычетов всегда имеется хотя бы одна пара соседних квадратичных вычетов. Следовательно квадратичные вычеты по модулю любого простого числа m>5 разложимы в сумму двух квадратичных вычетов. Теорема доказана.

5.5 Разложение степенных вычетов по модулю составного числа.

Везде, где идет речь о разложимости степенных вычетов, если это не оговорено, имеется ввиду разложение вычета степени простого нечетного числа ***p*** в сумму двух вычетов той же степени. При рассмотрении разложимости степенных вычетов по модулю простого числа (§1, 1.4) мы показали, что при разложимости хотя бы одного степенного вычета, разложимы все степенные вычеты, в том числе степенного вычета 1.

Вычет 1 является степенным вычетом по модулю любого числа и удобен тем, что имея разложение вычета 1 можно умножением сравнения на интересующий нас степенной вычет получить его разложение поскольку в правой части при умножении степенного вычета на степенные вычеты (слагаемые) получим опять степенные вычеты (С в о й с т в о 1, §4, 4.1).

Если вариантов разложения вычета 1 несколько, то умножая каждый вариант разложения 1 на этот степенной вычет, получим все варианты его разложения. Существуют простые числа, по модулю которых степенные вычеты не разложимы. Примерами таких чисел являются простые числа имеющие форму **2p+1** и ***4p+1*** для степени ***p***, простые числа 13, 7 для степени ***p=3,*** простое число 41 для степени ***p=5*** и т.д.

Если вычеты степени ***p*** по модулю ***m*** не разложимы, то уравнение Ферма может иметь решение только в том случае, если одно из чисел уравнения кратно ***m***. В этом случае мы находим решения для сравнения типа $x^p \equiv a^p (\mathrm{mod}\, m)$, как в §1, 1.4, и получаем разложение степенных вычетов с одним нулевым

решением по модулю ***m***. Как мы показали в 5.3, квадратичные вычеты по модулю 3 и модулю 5 не разложимы в сумму двух квадратичных вычетов и потому любая тройка Пифагоровых чисел содержит число кратное 3 и число кратное 5. Возможно одно число кратным 15. Докажем теорему по разложимости степенных вычетов в сумму двух вычетов той же степени по модулю составного числа.

Теорема 6. ***Степенные вычеты по модулю любого составного числа разложимы в сумму двух вычетов той же степени.***

Доказательство. Рассмотрим разложения степенного вычета 1 в сумму двух степенных вычетов по модулю составного числа $m_1 \cdot m_2 \cdots m_n = M$

$$\begin{aligned} 1 &\equiv V_1 + V_2 \ (mod m_1) \\ 1 &\equiv V_3 + V_4 \ (\mathrm{mod} m_2) \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ 1 &\equiv V_{2n-1} + V_{2n} (\mathrm{mod}\, m_n) \end{aligned} \qquad (1)$$

Если степенной вычет 1 разложим по модулю какого то числа m_i, то в правой части сравнения оба степенных вычета больше 1.

Если разложимость степенного вычета не имеет места, то один из степенных вычетов правой части по модулю ***m*** равен нулю – нулевое решение, а другой равен 1. Для определенности будем полагать, что в сравнениях (1), для которых разложимость степенных вычетов не имеет места, в правой части степенной вычет с четным индексом равен нулю, а другой равен единице, чтобы сравнение имело место.

Нам необходимо найти разложение степенного вычета 1 в сумму двух степенных вычетов по модулю произведения модулей $m_1 \cdot m_2 \cdots m_n = M$.

$$1 \equiv U_1 + U_2 (\mathrm{mod}\, M) \qquad (2)$$

Нам также необходимо показать, что существует хотя бы одно такое разложение степенного вычета 1 в сумму двух степенных вычетов при $U_1 > 1$ и $U_2 > 1$.

Для нахождения степенных вычетов U_1 и U_2 воспользуемся известной методикой [2], Гл.IV, §3. Определим числа M_i и M_i' из условия $M_i \cdot M_i' \equiv 1 (\mathrm{mod} m_i)$, где $M_i = \frac{M}{m_i}$.

$$U_1 \equiv M_1 \cdot M_1' \cdot V_1 + M_2 \cdot M_2' \cdot V_3 + \cdots + M_n \cdot M_n' \cdot V_{2n-1} (\mathrm{modM}) \quad (3)$$

$$U_2 \equiv M_1 \cdot M_1' \cdot V_2 + M_2 \cdot M_2' \cdot V_4 + \cdots + M_n \cdot M_n' \cdot V_{2n} (\mathrm{modM}) \quad (4)$$

Если полученные значения U_1 и U_2 подставим в сравнение (2) получим разложение вычета 1 в сумму двух степенных вычетов по модулю М. Легко проверить, что сравнение (2) выполняется по модулю каждого делителя М, а следовательно сравнение выполняется по модулю их произведения . Обратим внимание, что в (3) включены все степенные вычеты с нечетными индексами , а в (4) с четными индексами. Если например поменять местами любую пару вычетов любого сравнения в (1), то мы получим другой вариант разложения 1 в (2), который мы получим из (3),(4). В (3),(4) можно например поменять местами V_1 и V_2 относящиеся к первому сравнению в (1). Легко определить число различных вариантов разложения если количество сравнений в (1) равно ***n***. Это число равно 2^n.

Отметим ещё одно обстоятельство. Если по модулю какого то m_i существует несколько вариантов разложения вычета 1, то в систему (1) включаем только один из этих вариантов. Другие варианты дадут ещё больше вариантов разложения вычета 1 по модулю М.

Чтобы показать существование хотя бы одного разложения 1 по модулю произведения модулей, предположим худшее, что по модулю любого простого m_i степенные вычеты не разложимы. Тогда в разложениях (1) в каждом сравнении один из вычетов равен нулю, а другой должен быть равен 1, чтобы

сравнение имело место. Для определенности полагаем, что все степенные вычеты с четными индексами равны нулю. В этом случае в (4) $U_2 \equiv 0(\mathrm{mod}\, m)$ и мы не получим разложения (2) с ненулевым решением.

Чтобы в (2) U_1 и U_2 были больше 1 нам достаточно в сравнениях (3),(4) поменять местами вычеты любой пары V_1, V_2 или V_3, V_4 и т.д. Тогда U_2 не будет равен нулю так как V_1 или V_3 не равны нулю.

Если $m \geq 2$, то в любом сравнении (1) в правой части есть степенной вычет равный 1 даже для модуля, по которому нет разложимости. Поэтому в (3),(4) для каждого сравнения при $m \geq 2$ есть хотя бы один степенной вычет и потому мы можем всегда найти разложение (2) с ненулевым решением.

Если n=1, то может быть по модулю m_1 степенные вычеты не разложимы и один из слагаемых правой части (2) будет равен нулю, а следовательно мы не можем получить разложения степенных вычетов умножая это сравнение на степенные вычеты.

Таким образом, чтобы разложение степенных вычетов по модулю числа имело место необходимо, чтобы модуль был составным числом, то есть имел по крайней мере 2 делителя. В этом случае степенные вычеты всегда разложимы в сумму двух степенных вычетов. Теорема доказана.

Для случая n=2 сравнения (1) будут иметь вид

$$1 \equiv 1 + 0(\mathrm{mod}\, m_1)$$
$$1 \equiv 0 + 1(\mathrm{mod}\, m)$$

Совместное решение дает результат

$$1 \equiv m_2 \cdot m_2' + m_1 \cdot m_1'(\mathrm{mod}\, m_1 \cdot m_2)$$

где: $m_2 \cdot m_2' \equiv 1(\mathrm{mod}\, m_1)$, $m_1 \cdot m_1' \equiv 1(\mathrm{mod}\, m_2)$.

Таким образом, мы нашли разложение степенного вычета 1 в сумму двух степенных вычетов по модулю произведения m_1 и m_2, когда по модулю каждого числа степенные вычеты не разложимы. Следовательно, все степенные вычеты по модулю

$m_1 \cdot m_2$ разложимы, так как умножая полученное разложение на любой степенной вычет по модулю $m_1 \cdot m_2$ и в левой и в правой части сравнения получаем степенные вычеты, как произведение степенных вычетов.

Приведем пример. Кубические вычеты по модулю 7 и модулю 13 не разложимы в сумму двух кубических вычетов. Тогда разложения 1 будут иметь вид

$1 \equiv 1+0 \ (mod7)$

$1 \equiv 1+0 \ (mod13)$

После совместного решения получим $1 \equiv 78+14 \ (mod91)$

Теорема7. ***Разложение любого вычета степени простого нечетного числа p по модулю числа m в сумму двух вычетов той же степени есть произведение этого степенного вычета на разложение степенного вычета 1 в сумму двух степенных вычетов и соответствующее разложение 1 в сумму двух вычетов той же степени существует.***

Д о к а з а т е л ь с т в о. На первом этапе найдем все возможные варианты разложения всех вычетов полной системы вычетов по модулю m в сумму двух других вычетов полной системы вычетов по модулю m.

Представим вычет v полной системы вычетов по модулю m в виде следующей суммы

$$v=(m-u)+(u+v) \ (modm) \qquad (1)$$

где:m-любое составное число,

u,v-вычеты полной системы вычетов по модулю m.

В справедливости последнего сравнения легко убедится раскрыв скобки в правой части сравнения.

Найдем теперь количество всевозможных разложений.

Всего вычетов по модулю m имеем $(m-1)$ и каждый из них может быть разложим в сумму двух вычетов различными вариантами. Вариант разложения определяется значением u в (1). Из всех (m-1) вычетов u может принимать ($m-2$) значения

исключая значение $u \equiv -v(\mathrm{mod}\, m)$ так как в этом случае $u + v \equiv 0(\mathrm{mod}\, m)$ и в сравнении (1) один из слагаемых будет равен нулю, а этот вариант с нулевым решением нас не интересует. Следовательно общее количество всевозможных разложений равно

$$N=(m-1)(m-2) \qquad (2)$$

Теперь в сравнении (1) приравняем единице вычет ***v*** и получим один из вариантов разложения 1 в сумму двух вычетов при заданном u

$$1 \equiv (m-u)+(u+1)(\mathrm{mod}\, m) \qquad (3)$$

Изменяя ***u*** от 1 до ***m-2,*** получим ***m-2*** варианта разложения. Значение ***u*** изменяем до ***m-2*** потому, что при ***u=m-1*** второе слагаемое

$u+1=m-1+1=m \equiv 0(\mathrm{mod}\, m)$, а нулевое решение нас не интересует.

Далее. Умножая ***m-1*** различных вычетов на ***m-2*** варианта разложения 1 получим то же самое количество возможных разложений вычетов ***N=(m-1)(m-2).***

Таким образом, оба способа разложения дают исчерпывающее количество всевозможных разложений.

Действительно, максимальное количество пар вычетов ***из m-1*** равно ***(m-1)(m-2)*** так как каждый из ***m-1*** вычетов берем в сочетании с ***m-2*** вычетами исключая вариант, при котором сумма двух вычетов сравнима с нулем по модулю ***m.***

Мы показали, что все возможные разложения вычетов можно получить умножая все варианты разложения 1 на интересующий нас вычет. Следовательно, для любого разложения любого вычета существует соответствующее разложение вычета 1, которое можно умножить на интересующий нас вычет и получить его разложение.

Теперь из всех разложений вычетов полной системы вычетов выбираем те разложения, у которых слева от знака тождественного равенства и оба вычета справа от знака ра-

венства являются вычетами степени ***p*** по модулю ***m***, а такие разложения всегда существуют на основании Теоремы 6.

Разложения вычета 1 в сумму двух вычетов, которые дают разложения степенных вычетов в сумму двух степенных вычетов, также является разложением степенного вычета 1 в сумму двух степенных вычетов. В противном случае, при умножении разложения 1 на степенной вычет в правой части сравнения были бы степенные невычеты (Свойство 2 степенных вычетов). Существование разложения 1 доказано.

Мы исчерпали все варианты разложения степенных вычетов и каждый из них получен путем умножения этого степенного вычета на разложение вычета 1, существование которого так же доказано. Теорема доказана полностью.

§6. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ФЕРМА.

Запишем уравнение Ферма для простого числа ***p*** в виде

$$c^p = b^p + a^p \qquad (1)$$

и будем предполагать, что оно имеет целочисленное ненулевое решение при взаимно простых числах ***a,b,c.***

Если уравнение имеет решение, то левая и правая части сравнимы по модулю любого числа ***m.***

$$c^p \equiv b^p + a^p (\mathrm{modm}) \qquad (2)$$

При доказательстве Теоремы6 и Теоремы7 мы не касались вопроса о решениях и рассматривали только вопросы разложения степенных вычетов по модулю какого то числа.

Если ввести обозначения - $V_c \equiv c^p (\mathrm{modm})$, $V_b \equiv b^p (\mathrm{modm})$, $V_a \equiv a^p (\mathrm{modm})$ сравнение (2) примет вид

$$V_c \equiv V_b + V_a (\mathrm{modm}) \qquad (3)$$

Если числа ***a,b,c*** взаимно простые и ни одно из них не делится на ***m***, и есть решения сравнений (2),(3) говорят, что имеет место разложимость вычетов степени ***p*** в сумму двух вычетов степени ***p*** по модулю ***m.***

Если какое то число в (2), например ***a***, делится на какое то простое число m_1, то получаем сравнение $c^з \equiv b^p (\mathrm{mod}\, m_1)$, для которого, как мы показали в 1.4, существуют решения. Второе слагаемое в сравнении равно нулю по модулю m_1.

Существуют простые числа, по модулю которых для каких то простых степеней ***p*** степенные вычеты не разложимы в сумму двух степенных вычетов. Примерами могут служить вычеты степени 3 по модулю 13, вычеты степени 5 по модулю 41.

Поскольку сравнение (2) должно выполнятся по модулю любого числа, и есть числа, по модулю которых вычеты степени ***p*** не разложимы в сумму двух вычетов степени ***p***, одно из чисел ***a,b,c*** должно быть кратно этому числу, но не равно нулю. Тем самим обеспечивается выполнимость сравнения (2) по модулю этого числа.

Рассуждения применимы и для степени 2. По модулю 3 и модулю 5 квадратичные вычеты не разложимы в сумму двух квадратичных вычетов (§5, 5.3). Поэтому любая тройка пифагоровых чисел содержит число делящееся на 3 и содержит число делящееся на 5.

Для анализа разрешимости уравнения Ферма рассмотрим сравнение (2) по модулю различных чисел.

Выберем любое конечное число $m \geq c$, при котором, как мы предполагаем, уравнение Ферма имеет решение, и $m < c^p$

Сравнение (2) должно выполнятся не только по модулю ***m*** но и по модулю любого числа $m_i \leq m$, а следовательно сравнение (2) выполняется по модулю произведения этих модулей. Выберем модуль $M = m!$.

Как следует из Теоремы6, разложимость степенных вычетов по модулю составного числа в сумму двух степенных вычетов имеет место.

$$V_c \equiv V_b + V_a (\mathrm{mod}\, M) \qquad (4)$$

Как следует из Теоремы7, разложение степенного вычета можно представить как произведение вычета V_c на разложение вычета 1 в сумму двух степенных вычетов. Такое разложение вычета 1 существует и следует это из той же Теоремы7. Таких разложений может быть несколько, а следовательно существуют различные варианты разложения вычета V_c.

Допустим, что один из вариантов разложения 1, подходящий для уравнения Ферма, имеет вид

$$1 \equiv u_1 + u_2 \ (\boldsymbol{mod M}) \qquad (5)$$

где**:** u_1, u_2 - вычеты степени ***p*** по модулю М.

Если последнее сравнение умножим на V_c получим

$$V_c \equiv u_1 \cdot V_c + u_2 \cdot V_c \ (\boldsymbol{mod}\text{М}) \qquad (6)$$

Произведения степенных вычетов $u_1 \cdot V_c$ и $u_2 \cdot V_c$ являются степенными вычетами (С в о й с т в о 1).

Если среди всех вариантов разложения вычета 1 существует разложение подходящее для уравнения Ферма и мы выбрали именно его, то должны получить $u_1 \cdot V_c \equiv V_b$ (***mod***М), $u_2 \cdot V_c \equiv V_a$ (***mod***М), то есть получить сравнение (3).

Теперь перейдем к вопросу о решениях сравнений и уравнения Ферма. Допустим, что $u_1 \equiv x^p (\mathrm{mod}\, M)$, $u_2 \equiv y^p (\mathrm{mod}\, M)$. Подставляя эти значения в (5) будем иметь

$$1 \equiv x^3 + y^3 (\mathrm{mod}\, M) \qquad (7)$$

Чтобы получить уравнение Ферма нам необходимо каждый из степенных вычетов (6) выразить в виде степеней каких то чисел. Поскольку V_c, u_1, u_2 являются степенными вычетами то такие числа существуют.

В общем случае уравнение вида

$$x^p \equiv V (\mathrm{mod}\, m) \qquad (8)$$

может иметь не единственное решение. В этой связи, переход от сравнения (6), в котором фигурируют степенные вычеты по модулю M=m!, к степеням чисел должен быть выполнен корректно. Чтобы сделать вывод о неразрешимости уравнения Ферма, мы должны исчерпать всевозможные сочетания чисел ***a,b,c*** при ***a<m,b<m,c<m.***

Чтобы сравнение (6) выполнялось можно использовать любые решения, которые могут иметь место, а для получения уравнения Ферма, если это вообще возможно, важно выбрать подходящие решения для сравнения $c^p \equiv V_c (\mathrm{mod}\, M)$.

Выбранные решения ***x*** и ***y*** в (7) могут быть больше ***m,*** но меньше чем ***m!.***

Число ***c*** удовлетворяющее уравнению (1) меньше ***m***. Имея это ввиду рассмотрим вопрос о решениях сравнения

$$c^p \equiv V_c (\mathrm{mod}\, M) \qquad (9)$$

Число ***c*** является одним из решений, которое мы предполагаем решением уравнения Ферма, и хотим разложить в сумму двух других степеней.

Дело в том, что в разложениях степенного вычета V_c в (6) этот вычет встречается и в правой части.

У нас нет основания считать, что в правой части тоже можно применять то же решение для ***c,*** что и в левой части. Степенной вычет может быть один, а решения могу быть различные и при других решениях можно получить значения ***a*** и ***b*** по модулю M, то есть получить не только справедливое сравнение но и равенство.

Допустим, что сравнение (9)имеет еще и другие решения кроме известного ***c<m*** по определению

$$c_i^{\,p} \equiv V_c (\mathrm{mod}\, M) \qquad (10)$$

Правые части (9) и (10) одинаковы, а следовательно левые части сравнимы по модулю M

$$c_i^{\,p} \equiv c^p (\mathrm{mod}\, M) \qquad (11)$$

Число ***c*** делит M=m!. Следовательно сравнение выполнимо по модулю ***c*** и тогда

$$c_i^{\,p} \equiv 0(\mathrm{mod}\, c) \qquad (12)$$

Из последнего очевидно $c_i \equiv 0(\mathrm{mod}\, c)$, а решения для ***c*** имеют форму $c_i \equiv k_i \cdot c$.

Число ***c*** удовлетворяет уравнению Ферма, а любое $c_i^{\,p}$ дает тот же степенной вычет V_c, если вообще существуют такие решения для каких то ***p*** и ***m***.

Вопрос о количестве решений – это предмет других исследований. Для доказательства теоремы Ферма этот вопрос не важен. Важно, что все решения, если даже их больше одного, кратны ***c***, а коэффициент кратности $k_i \equiv 1$ при единственном решении и больше 1, когда количество решений больше одного.

Теперь, когда мы нашли в общем виде решения, заменим в (6) все степенные вычеты степенями ***p*** найденных решений в общем виде.

$$c^p \equiv x^p \cdot (k_i \cdot c)^p + y^p (k_j \cdot c)^p (\mathrm{mod}\, M) \qquad (13)$$

где: k_i, k_j - целые числа.

Последнее сравнение выполняется всегда не зависимо от того какое решение для c_i сравнения (10) мы подставляем.

В левой части мы оставляем c^p потому, что по нашему изначальному предположению оно разложимо в сумму двух других степеней b^p и a^p.

Таким образом, сравнение (13) должно дать уравнение Ферма если оно вообще имеет решение и мы правильно выбрали k_i, k_j и выбран правильный вариант разложения 1 и решения ***x*** и ***y***.

После перемножения получим

$$c^p \equiv (x \cdot k_i \cdot c)^p + (y \cdot k_j \cdot c)^p (\mathrm{mod} M) \quad (14)$$

Из последнего можем написать

$$b \equiv x \cdot k_i \cdot c (\mathrm{mod} M) \quad (15)$$

$$a \equiv y \cdot k_j \cdot c (\mathrm{mod} M) \quad (16)$$

Не зависимо от того сравнение (10) имеет единственное решение, для которого $k_i = 1$, $k_j = 1$, или не единственное решение, для которого $k_i \geq 1$, $k_j \geq 1$, последние сравнения выполнимы по модулю любого делителя М, в частности по модулю с. Тогда

$$b \equiv 0 (\mathrm{mod} c) \quad (17)$$

$$a \equiv 0 (\mathrm{mod} c) \quad (18)$$

Мы получили, что независимо от ***x,y.*** k_i, k_j числа ***b*** и ***a*** кратны ***c***. Пусть $b = k_1 \cdot c$, $a = k_2 \cdot c$.

Подставим теперь полученные решения в уравнение (1) Ферма.

$$c^p = (k_1 \cdot c)^p + (k_2 \cdot c)^p \quad (19)$$

После сокращения на c^p получим невыполнимое при $k_1 > 1$, и $k_2 > 1$ равенство

$$1 = {k_1}^p + {k_2}^p \quad (20)$$

Уравнение Ферма не имеет решения. Теорема Ферма для нечетных простых степеней верна.

Представляется целесообразным рассмотреть и другой подход.

Если уравнение Ферма имеет решение при взаимно простых ***a,b,c*** то левая и правая его части сравнимы по модулю любого числа, в том числе и по модулю m!, где m больше или равно с, при котором уравнение имеет решение. Тогда имеет место разложение степенного вычета в сумму двух степенных вычетов по модулю любого числа

Как следует из Теоремы7 разложение степенного вычета c^p можно представить как произведение c^p на разложение степенного вычета 1 в сумму двух степенных вычетов по модулю m!.

Попытаемся найти соответствующее разложение степенного вычета 1 в сумму двух степенных вычетов из уравнения Ферма. Такое разложение существует (Теорема7).

Поскольку c>b, c>***a*** нельзя разделить каждый член уравнения Ферма на c^p даже по модулю m! так как представляя b^p в виде

$$b^p \equiv (b + k \cdot m!)^p (\mathrm{mod}\, m!) \qquad (21)$$

$$\text{или } b^p \equiv b^p + k \cdot m! \ (\mathrm{mod} m!) \qquad (22)$$

становится очевидным, что при любом ***k*** число ***c*** делит ***km***! так как c≤m и делит ***m***!, а b^p не делится на ***c*** и тем более на c^p.

Чтобы получить разложение 1, соответствующее уравнению (1) Ферма, как в (5) попытаемся найти число, на которое следует умножить сравнение $c^p = b^p + a^p (\mathrm{mod}\, m!)$.

Это число должно быть p-той степени какого то числа, чтобы после умножения в правой части тоже получились ***p***-тые степени каких то чисел.

$$c^p \cdot c'^p = (b \cdot c')^p + (a \cdot c')^p \ (\mathrm{modm!})$$

Если уравнение Ферма имеет решение, то имеет место разложение степенных вычетов, а следовательно, как следует из Теоремы7, существует разложение 1 в сумму двух степенных вычетов. Однако такого числа c', которое давало бы решение сравнения $c^p \cdot c'^p \equiv 1 (\mathrm{mod}\, m!)$ не существует при ***c*** ≤ ***m***. В этом можно убедится если последнее сравнение рассмотреть по модулю c, которое делит m!.

Получим не верное сравнение

$$0 \equiv 1 (\mathrm{mod}\, c) \qquad (23)$$

Теорема Ферма для простых нечетных степеней верна.

Таким образом, не удается найти разложение степенного вычета 1 в сумму двух степенных вычетов по модулю m! при $c \le m$ и разрешимости уравнения Ферма, а такое разложение степенного вычета 1 в сумму двух степенных вычетов, как следует из Теоремы 7, должно существовать. Следовательно, уравнение Ферма не имеет решения. Теорема Ферма для простых нечетных степеней верна.

Далее. Если в уравнении Ферма степень является составным числом, то доказательство следует разбить на два случая:

1. Степень имеет форму 2^i
2. Степень кратна какому то простому нечетному числу

Рассмотрим каждый случай отдельно.

Случай1. Если степень имеет форму 2^i, то представим ее как $n = 4 \cdot 2^{i_1}$. Если $i_1 = 0$, то в этом случае n=4 и теорему для этой степени доказал сам Ферма. Поэтому мы будем полагать $i_1 > 0$.

Напишем уравнение Ферма в виде

$$(c^{2^{i_1}})^4 = (b^{2^{i_1}})^4 + (a^{2^{i_1}})^4 \qquad (24)$$

Если последнее уравнение рассмотрим как уравнение Ферма для степени 4, то оно не имеет решения, как доказал сам Ферма, уже не говоря о том, что этими решениями должны быть какие то степени чисел. Поэтому уравнение Ферма не имеет решения для любых степеней $n = 2^i$ при ***i***>1.

Случай2. Пусть степень кратна какому то простому нечетному числу p, то есть $n = n_1 \cdot p$. Тогда уравнение Ферма можно написать в виде

$$(c^{n_1})^p = (b^{n_1})^p + (a^{n_1})^p \qquad (25)$$

Если последнее уравнение рассмотрим как уравнение Ферма для простой нечетной степени p, то оно не имеет решения, как мы уже доказали выше для любых нечетных простых p, уже не

говоря о том, что этими решениями должны быть какие то степени чисел ***a,b,c***. Поэтому уравнение Ферма не имеет решений для любых $n = n_1 \cdot p$ при $n_1 > 0$.

Два рассмотренных случая исчерпывают все числа n>2 и потому можно утверждать: уравнение Ферма не имеет решений для любых степеней больше двух.

Теорема Ферма доказана полностью.

Литература

1.Постников М.М. Введение в теорию алгебраических чисел. М, Наука ,1992г.

2.Виноградов И .М.Основы теории чисел. Государственное издательство технико-теоретической литературы, Москва, 1953г.

3.Г.Дэвенпорт, Мультипликативная теория чисел, Москва, “Наука”, 1971г.

4.П.Рибенбоим, Последняя Теорема Ферма, Москва, “Мир”, 2003г.

С о д е р ж а н и е

Камлия Расим Аркадьевич

Теорема Ферма и разложимость степенных вычетов.

В авторской редакции

Компьютерная верстка и техническое редактирование

Садзба И.Н.

Сдано в набор 30.06.2008 г. Формат 60x84 1/16. Тираж 600 экз. Объем услов. печ. л. 4,0 Книга напечатана в типографии газетно-типографического комплекса газеты «Республика Абхазия» г. Сухум, ул. Званба, 9.