Доказательство теоремы Ферма.

Камлия Р.А.

Формулировка теоремы, которую дал сам Ферма гласит: невозможно разложить куб на два куба, биквадрат - на два биквадрата и, в общем случае, любую степень, большую двух, в сумму двух таких же степеней [1].

Изучение свойств степенных вычетов, проведенное в [2], показало, что степенные вычеты по модулю простого числа могут быть не разложимы в сумму двух степенных вычетов, а в случае разложимости хотя бы одного степенного вычета разложимы все степенные вычеты по модулю выбранного числа (Свойство5 степенных вычетов [2]).

Для доказательства теоремы Ферма предварительно докажем одну теорему.

Теорема. ***Если один из вычетов степени простого нечетного числа р по модулю простого числа m разложим в сумму двух вычетов той же степени по модулю m, то любое разложение любого вычета степени р представимо как произведение этого вычета степени р и разложения единицы в сумму двух вычетов той же степени по модулю m, и соответствующее разложение единицы в сумму двух вычетов степени р существует.***

Д о к а з а т е л ь с т в о. По условию теоремы существует разложение степенного вычета в сумму двух степенных вычетов.

$$v \equiv v_1 + v_2 (\mathrm{mod}\ m) \qquad (1)$$

Если разложим хотя бы один вычет степени простого нечетного числа ***p*** в сумму двух степенных вычетов, то, как следует из 5.5 [1], все степенные вычеты разложимы, причем возможны различные варианты разложения. Признаком разложимости является наличие соседних степенных вычетов [1].

Если мы имеем пару соседних степенных вычетов ***u*** и (***u***+1), то легко найти разложение 1 в сумму двух степенных вычетов.

$$1 \equiv (m-u) + (u+1)(\mathrm{mod} m) \qquad (2)$$

Число (m-u) является степенным вычетом, поскольку степень p нечетное простое число. Умножая последнее сравнение на любой степенной вычет получаем его разложение в сумму двух степенных вычетов, так как в правой части произведение степенных вычетов дает степенной вычет (Свойство1 степенных вычетов [1]).

Таким образом, имея пару соседних степенных вычетов, можно найти разложение любого степенного вычета. Для каждой пары соседних степенных вычетов существует свой вариант разложения 1, а следовательно и любого степенного вычета.

Теперь мы должны показать, что для любого разложения любого степенного вычета существует соответствующее ему разложение 1 в сумму двух степенных вычетов, которое даст исходное разложение степенного вычета (1) при умножении его на ***v***.

Умножим исходное разложение (1) на число v' обратное к ***v*** по модулю m, то есть удовлетворяющему сравнению

$$v \cdot v' \equiv 1 (\mathrm{mod} m) \qquad (3)$$

После умножения получим

$$1 \equiv v_1 \cdot v' + v_2 \cdot v' (\bmod m) \qquad (4)$$

Такое число v' существует, поскольку число m простое, а для любого числа взаимно простого с модулем существует обратное число.

Это число v' является степенным вычетом, поскольку в противном случае произведение степенного вычета ***v*** на v' давало бы степенной невычет (Свойство6 степенных вычетов [2]), а число 1 является степенным вычетом.

В правой части последнего сравнения имеем два произведения степенных вычетов, каждое из которых является степенным вычетом (Свойство1 степенных вычетов) [2].

Следовательно, сравнение (4) является разложением 1 в сумму двух степенных вычетов.

Умножая сравнение (4) на ***v*,** получаем исходное сравнение (1) и убеждаемся в том, что нашли соответствующее ему разложение 1 в сумму двух степенных вычетов. Аналогичным путем мы можем однозначно найти разложение 1 в сумму двух степенных вычетов, соответствующее любому варианту разложения любого степенного вычета. Вариант разложения определяется парой соседних степенных вычетов.

Теорема доказана.

Д о к а з а т е л ь с т в о теоремы Ферма. Запишем уравнение Ферма для простой степени *p* в виде

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

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

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

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

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

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

Если есть решения сравнения (3), то говорят, что имеет место разложимость вычетов степени *p* в сумму двух вычетов степени *p* по модулю *m.*

Если уравнение (1) Ферма имеет решение, то сравнение (2) должно выполняться по модулю любого числа.

Выберем два простых модуля $m_1 > c^p$ и $m_2 > c^p$, $m_1 < m_2$.

Будем считать, что вычеты степени ***p*** по модулям m_1 и m_2 разложимы в сумму двух степенных вычетов. Если бы это было не так, то сравнение (3) не имело бы нетривиального решения, а следовательно остается только тривиальное решение, когда какое то из чисел *a,b,c* сравнимо с нулем по модулю m_1 или m_2. Последнее означает, что наше предположение о существовании решения в (1) неверно, так как мы выбрали $m_1 > c^p$, $m_2 > c^p$. Для доказательства теоремы Ферма следует рассматривать уравнение Ферма в виде разложения степеней чисел, именно так как сформулирована теорема [2].

Как следует из доказанной выше теоремы, любое разложение степенных вычетов можно представить как произведение этого степенного вычета и разложения 1 в сумму двух степенных вычетов. Следовательно, существует такое разложение 1

$$1 \equiv u_{1,1} + u_{2,1} (\bmod m_1) \tag{4}$$

которое после умножения на V_c даст сравнение

$$V_c \equiv u_{1,1} \cdot V_c + u_{2,1} \cdot V_c (\bmod m_1) \tag{5}$$

то есть даст сравнение (3).

где: $V_b \equiv u_{1,1} \cdot V_c (\bmod m_1)$, $V_a \equiv u_{2,1} \cdot V_c (\bmod m_1)$

Так как сравнение (3) должно выполняться и по модулю простого числа m_2, то существует разложение 1 и по модулю m_2

$$1 \equiv u_{1,2} + u_{2,2} (\bmod m_2) \tag{6}$$

которое также должно дать сравнение (3) после умножения на V_c

$$V_c \equiv u_{1,2} \cdot V_c + u_{2,2} \cdot V_c (\bmod m_2) \tag{7}$$

где: $V_b \equiv u_{1,2} \cdot V_c (\bmod m_2)$, $V_a \equiv u_{2,2} \cdot V_c (\bmod m_2)$

Если сравнение (3) выполняется по модулю m_1 и модулю m_2, то оно должно выполняться и по модулю произведения модулей $m_1 \cdot m_2$.

Теперь найдем разложение V_c по модулю $m_1 \cdot m_2$. Для этого найдем разложение вычета 1 в сумму двух степенных вычетов по модулю $m_1 \cdot m_2$ совместным решением сравнений (4),(6) [2]. Разложения (4) и 6) различны, так как $m_1 \neq m_2$.

Найдем слагаемые правой части следующим образом

$$u_1 \equiv m_2 \cdot m_1' \cdot u_{1,1} + m_1 \cdot m_2' \cdot u_{1,2} (\bmod m_1 \cdot m_2) \tag{8}$$

$$u_1 \equiv m_2 \cdot m_1' \cdot u_{2,1} + m_1 \cdot m_2' \cdot u_{2,2} (\bmod m_1 \cdot m_2) \tag{9}$$

где: $m_2 \cdot m_1' \equiv 1 (\bmod m_1)$, $m_1 \cdot m_2' \equiv 1 (\bmod m_2)$

Теперь можем написать разложение 1 в сумму двух степенных вычетов по модулю $m_1 \cdot m_2$.

$$1 \equiv u_1 + u_2 (\bmod m_1 \cdot m_2) \tag{10}$$

и соответственно разложение V_c по модулю $m_1 \cdot m_2$

$$V_c \equiv u_1 \cdot V_c + u_2 \cdot V_c (\bmod m_1 \cdot m_2) \tag{11}$$

В правильности последнего сравнения по модулю $m_1 \cdot m_2$ можно убедиться, проверив его по модулю m_1 и модулю m_2. Теперь перейдем к решениям для (10),(11). Вычеты u_1 и u_2 в (10) это степенные вычеты по модулю $m_1 \cdot m_2$. Они имеют какие то решения

$$1 \equiv k_1^{\,p} + k_2^{\,p} (nod m_1 \cdot m_2) \tag{12}$$

Степенной вычет $V_c \equiv c^p (\bmod m_1 \cdot m_2)$. Число c^p является наименьшим положительным степенным вычетом по модулю $m_1 \cdot m_2$ так как мы задали выше $m_1 > c^p$, $m_2 > c^p$. Подставим значения степенных вычетов в (11).

$$c^p \equiv k_1^{\,p} \cdot c^p + k_2^{\,p} \cdot c^p (\bmod m_1 \cdot m_2) \tag{13}$$

Очевидно, что $k_1^{\,p} \cdot c^p > m_1 \cdot m_2$, $k_2^{\,p} \cdot c^p > m_1 \cdot m_2$. Если бы это было не так, то сравнение (13) можно было сократить на c^p и ясно, что уравнение Ферма получить нельзя.

Можно ли из (13) получить уравнение (1). Если такое было бы возможно, то должно выполняться сравнение (2) по модулю $m_3 > m_2$. Однако разложение 1 по модулю m_3 отличается от (4),(6),(10). Поэтому мы должны найти разложение 1 по модулю m_3 и далее это сравнение решить совместно с (10) и найти разложение 1 в сумму двух степенных вычетов по модулю $m_1 \cdot m_2 \cdot m_3$. В полученном решении по модулю $m_1 \cdot m_2 \cdot m_3$ слагаемые в правой части будут больше чем $m_1 \cdot m_2 \cdot m_3$.

Таким образом, процесс поиска решений сравнения (3) по модулю $m_1 \cdot m_2 \cdot m_3$ свелся к поиску разложения 1 по модулю m_3, если вообще имеет место разложимость степенных вычетов по модулю m_3, и его совместному решению с (10) и умножению на c^p. Для каждого следующего простого модуля вышеописанный процесс следует повторить. Количество простых чисел-бесконечное множество. Поэтому найти решение уравнения Ферма в конечных числах невозможно.

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

$$(c^{2^{i_1}})^4 = (b^{2^{i_1}})^4 + (a^{2^{i_1}})^4 \qquad (14)$$

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

$$(c^{n_1})^p = (b^{n_1})^p + (a^{n_1})^p \qquad (15)$$

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 степени больше двух.

Теорема Ферма доказана полностью.

Литература

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

2. Камлия Р.А. Теорема Ферма и разложимость степенных вычетов, Абхазский научный центр Российской академии космонавтики им. К.Э. Циолковского, Сухум,2008г.

Доказательство теоремы Ферма.

Камлия Р.А.

Формулировка теоремы, которую дал сам Ферма гласит: невозможно разложить куб на два куба, биквадрат - на два биквадрата и, в общем случае, любую степень, большую двух, в сумму двух таких же степеней [1].

Изучение свойств степенных вычетов, проведенное в [2], показало, что степенные вычеты по модулю простого числа могут быть не разложимы в сумму двух степенных вычетов, а в случае разложимости хотя бы одного степенного вычета разложимы все степенные вычеты по модулю выбранного числа (Свойство5 степенных вычетов [2]).

Для доказательства теоремы Ферма предварительно докажем одну теорему.

Теорема. ***Если один из вычетов степени простого нечетного числа p по модулю простого числа m разложим в сумму двух вычетов той же степени по модулю m, то любое разложение любого вычета степени p представимо как произведение этого вычета степени p и разложения единицы в сумму двух вычетов той же степени по модулю m, и соответствующее разложение единицы в сумму двух вычетов степени p существует.***

Д о к а з а т е л ь с т в о. По условию теоремы существует разложение степенного вычета в сумму двух степенных вычетов.

$$v \equiv v_1 + v_2 (\mathrm{mod}\, m) \tag{1}$$

Если разложим хотя бы один вычет степени простого нечетного числа ***p*** в сумму двух степенных вычетов, то, как следует из 5.5 [1], все степенные вычеты разложимы, причем возможны различные варианты разложения. Признаком разложимости является наличие соседних степенных вычетов [1].

Если мы имеем пару соседних степенных вычетов ***u*** и (***u***+1), то легко найти разложение 1 в сумму двух степенных вычетов.

$$1 \equiv (m-u) + (u+1) (\mathrm{mod} m) \tag{2}$$

Число (m-u) является степенным вычетом, поскольку степень p нечетное простое число. Умножая последнее сравнение на любой степенной вычет получаем его разложение в сумму двух степенных вычетов, так как в правой части произведение степенных вычетов дает степенной вычет (Свойство1 степенных вычетов [1]).

Таким образом, имея пару соседних степенных вычетов, можно найти разложение любого степенного вычета. Для каждой пары соседних степенных вычетов существует свой вариант разложения 1, а следовательно и любого степенного вычета.

Теперь мы должны показать, что для любого разложения любого степенного вычета существует соответствующее ему разложение 1 в сумму двух степенных вычетов, которое даст исходное разложение степенного вычета (1) при умножении его на ***v***.

Умножим исходное разложение (1) на число v' обратное к ***v*** по модулю m, то есть удовлетворяющему сравнению

$$v \cdot v' \equiv 1(\mathrm{mod}\, m) \tag{3}$$

После умножения получим

$$1 \equiv v_1 \cdot v' + v_2 \cdot v'(\mathrm{mod}\, m) \tag{4}$$

Такое число v' существует, поскольку число m простое, а для любого числа взаимно простого с модулем существует обратное число.

Это число v' является степенным вычетом, поскольку в противном случае произведение степенного вычета ***v*** на v' давало бы степенной невычет (Свойство6 степенных вычетов [2]), а число 1 является степенным вычетом.

В правой части последнего сравнения имеем два произведения степенных вычетов, каждое из которых является степенным вычетом (Свойство1 степенных вычетов) [2].

Следовательно, сравнение (4) является разложением 1 в сумму двух степенных вычетов.

Умножая сравнение (4) на ***v*,** получаем исходное сравнение (1) и убеждаемся в том, что нашли соответствующее ему разложение 1 в сумму двух степенных вычетов. Аналогичным путем мы можем однозначно найти разложение 1 в сумму двух степенных вычетов, соответствующее любому варианту разложения любого степенного вычета. Вариант разложения определяется парой соседних степенных вычетов.

Теорема доказана.

Д о к а з а т е л ь с т в о теоремы Ферма. Запишем уравнение Ферма для простой степени *p* в виде

$$c^p = b^p + a^p \tag{1}$$

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

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

$$c^p \equiv b^p + a^p(\mathrm{mod}\, m) \tag{2}$$

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

$$V_c \equiv V_b + V_a(\mathrm{mod}\, m) \tag{3}$$

Если есть решения сравнения (3), то говорят, что имеет место разложимость вычетов степени *p* в сумму двух вычетов степени *p* по модулю *m*.

Если уравнение (1) Ферма имеет решение, то сравнение (2) должно выполняться по модулю любого числа.

Выберем два простых модуля $m_1 > c^p$ и $m_2 > c^p$, $m_1 < m_2$.

Будем считать, что вычеты степени ***p*** по модулям m_1 и m_2 разложимы в сумму двух степенных вычетов. Если бы это было не так, то сравнение (3) не имело бы нетривиального решения, а следовательно остается только тривиальное решение, когда какое то из чисел *a*,*b*,*c* сравнимо с нулем по модулю m_1 или m_2 .

Последнее означает, что наше предположение о существовании решения в (1) неверно, так как мы выбрали $m_1 > c^p$, $m_2 > c^p$. Для доказательства теоремы Ферма следует рассматривать уравнение Ферма в виде разложения степеней чисел, именно так как сформулирована теорема [2].

Как следует из доказанной выше теоремы, любое разложение степенных вычетов можно представить как произведение этого степенного вычета и разложения 1 в сумму двух степенных вычетов. Следовательно, существует такое разложение 1

$$1 \equiv u_{1,1} + u_{2,1} (\mathrm{mod}\ m_1) \tag{4}$$

которое после умножения на V_c даст сравнение

$$V_c \equiv u_{1,1} \cdot V_c + u_{2,1} \cdot V_c (\mathrm{mod}\ m_1) \tag{5}$$

то есть даст сравнение (3).

где: $V_b \equiv u_{1,1} \cdot V_c (\mathrm{mod}\ m_1)$, $V_a \equiv u_{2,1} \cdot V_c (\mathrm{mod}\ m_1)$

Так как сравнение (3) должно выполняться и по модулю простого числа m_2, то существует разложение 1 и по модулю m_2

$$1 \equiv u_{1,2} + u_{2,2} (\mathrm{mod}\ m_2) \tag{6}$$

которое также должно дать сравнение (3) после умножения на V_c

$$V_c \equiv u_{1,2} \cdot V_c + u_{2,2} \cdot V_c (\mathrm{mod}\ m_2) \tag{7}$$

где: $V_b \equiv u_{1,2} \cdot V_c (\mathrm{mod}\ m_2)$, $V_a \equiv u_{2,2} \cdot V_c (\mathrm{mod}\ m_2)$

Если сравнение (3) выполняется по модулю m_1 и модулю m_2, то оно должно выполняться и по модулю произведения модулей $m_1 \cdot m_2$.

Теперь найдем разложение V_c по модулю $m_1 \cdot m_2$. Для этого найдем разложение вычета 1 в сумму двух степенных вычетов по модулю $m_1 \cdot m_2$ совместным решением сравнений (4),(6) [2]. Разложения (4) и 6) различны, так как $m_1 \neq m_2$.

Найдем слагаемые правой части следующим образом

$$u_1 \equiv m_2 \cdot m_1' \cdot u_{1,1} + m_1 \cdot m_2' \cdot u_{1,2} (\mathrm{mod}\ m_1 \cdot m_2) \tag{8}$$

$$u_1 \equiv m_2 \cdot m_1' \cdot u_{2,1} + m_1 \cdot m_2' \cdot u_{2,2} (\mathrm{mod}\ m_1 \cdot m_2) \tag{9}$$

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

Теперь можем написать разложение 1 в сумму двух степенных вычетов по модулю $m_1 \cdot m_2$.

$$1 \equiv u_1 + u_2 (\mathrm{mod}\ m_1 \cdot m_2) \tag{10}$$

и соответственно разложение V_c по модулю $m_1 \cdot m_2$

$$V_c \equiv u_1 \cdot V_c + u_2 \cdot V_c (\mathrm{mod}\ m_1 \cdot m_2) \tag{11}$$

В правильности последнего сравнения по модулю $m_1 \cdot m_2$ можно убедиться, проверив его по модулю m_1 и модулю m_2. Теперь перейдем к решениям для (10),(11). Вычеты u_1 и u_2 в (10) это степенные вычеты по модулю $m_1 \cdot m_2$. Они имеют какие то решения

$$1 \equiv k_1{}^p + k_2{}^p (nod m_1 \cdot m_2) \tag{12}$$

Степенной вычет $V_c \equiv c^p (\mathrm{mod}\ m_1 \cdot m_2)$. Число c^p является наименьшим положительным степенным вычетом по модулю $m_1 \cdot m_2$ так как мы задали выше $m_1 > c^p$, $m_2 > c^p$. Подставим значения степенных вычетов в (11).

$$c^p \equiv k_1{}^p \cdot c^p + k_2{}^p \cdot c^p (\mathrm{mod} m_1 \cdot m_2) \tag{13}$$

Очевидно, что $k_1{}^p \cdot c^p > m_1 \cdot m_2$, $k_2{}^p \cdot c^p > m_1 \cdot m_2$. Если бы это было не так, то сравнение (13) можно было сократить на c^p и ясно, что уравнение Ферма получить нельзя.

Можно ли из (13) получить уравнение (1). Если такое было бы возможно, то должно выполняться сравнение (2) по модулю $m_3 > m_2$. Однако разложение 1 по модулю m_3 отличается от (4),(6),(10). Поэтому мы должны найти разложение 1 по модулю m_3 и далее это сравнение решить совместно с (10) и найти разложение 1 в сумму двух степенных вычетов по модулю $m_1 \cdot m_2 \cdot m_3$. В полученном решении по модулю $m_1 \cdot m_2 \cdot m_3$ слагаемые в правой части будут больше чем $m_1 \cdot m_2 \cdot m_3$.

Таким образом, процесс поиска решений сравнения (3) по модулю $m_1 \cdot m_2 \cdot m_3$ свелся к поиску разложения 1 по модулю m_3, если вообще имеет место разложимость степенных вычетов по модулю m_3, и его совместному решению с (10) и умножению на c^p. Для каждого следующего простого модуля вышеописанный процесс следует повторить. Количество простых чисел-бесконечное множество. Поэтому найти решение уравнения Ферма в конечных числах невозможно.

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

$$(c^{2^{i_1}})^4 = (b^{2^{i_1}})^4 + (a^{2^{i_1}})^4 \qquad (14)$$

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

$$(c^{n_1})^p = (b^{n_1})^p + (a^{n_1})^p \qquad (15)$$

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 степени больше двух.

Теорема Ферма доказана полностью.

Литература

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

2. Камлия Р.А. Теорема Ферма и разложимость степенных вычетов, Абхазский научный центр Российской академии космонавтики им. К.Э. Циолковского, Сухум,2008г.

Доказательство теоремы Ферма.

Камлия Р.А.

Формулировка теоремы, которую дал сам Ферма гласит: невозможно разложить куб на два куба, биквадрат - на два биквадрата и, в общем случае, любую степень, большую двух, в сумму двух таких же степеней [1].

Изучение свойств степенных вычетов, проведенное в [2], показало, что степенные вычеты по модулю простого числа могут быть не разложимы в сумму двух степенных вычетов, а в случае разложимости хотя бы одного степенного вычета разложимы все степенные вычеты по модулю выбранного числа (Свойство5 степенных вычетов [2]).

Для доказательства теоремы Ферма предварительно докажем одну теорему.

Теорема. ***Если один из вычетов степени простого нечетного числа р по модулю простого числа m разложим в сумму двух вычетов той же степени по модулю m, то любое разложение любого вычета степени р представимо как произведение этого вычета степени р и разложения единицы в сумму двух вычетов той же степени по модулю m, и соответствующее разложение единицы в сумму двух вычетов степени р существует.***

Д о к а з а т е л ь с т в о. По условию теоремы существует разложение степенного вычета в сумму двух степенных вычетов.

$$v \equiv v_1 + v_2 (\mathrm{mod}\, m) \qquad (1)$$

Если разложим хотя бы один вычет степени простого нечетного числа ***p*** в сумму двух степенных вычетов, то, как следует из 5.5 [1], все степенные вычеты разложимы, причем возможны различные варианты разложения. Признаком разложимости является наличие соседних степенных вычетов [1].

Если мы имеем пару соседних степенных вычетов ***u*** и (***u***+1), то легко найти разложение 1 в сумму двух степенных вычетов.

$$1 \equiv (m - u) + (u + 1)(\mathrm{mod} m) \qquad (2)$$

Число (m-u) является степенным вычетом, поскольку степень р нечетное простое число. Умножая последнее сравнение на любой степенной вычет получаем его разложение в сумму двух степенных вычетов, так как в правой части произведение степенных вычетов дает степенной вычет (Свойство1 степенных вычетов [1]).

Таким образом, имея пару соседних степенных вычетов, можно найти разложение любого степенного вычета. Для каждой пары соседних степенных вычетов существует свой вариант разложения 1, а следовательно и любого степенного вычета.

Теперь мы должны показать, что для любого разложения любого степенного вычета существует соответствующее ему разложение 1 в сумму двух степенных вычетов, которое даст исходное разложение степенного вычета (1) при умножении его на ***v***.

Умножим исходное разложение (1) на число v' обратное к ***v*** по модулю m, то есть удовлетворяющему сравнению

$$v \cdot v' \equiv 1 (\mathrm{mod} m) \qquad (3)$$

После умножения получим

$$1 \equiv v_1 \cdot v' + v_2 \cdot v' (\mathrm{mod}\ m) \qquad (4)$$

Такое число v' существует, поскольку число m простое, а для любого числа взаимно простого с модулем существует обратное число.

Это число v' является степенным вычетом, поскольку в противном случае произведение степенного вычета ***v*** на v' давало бы степенной невычет (Свойство6 степенных вычетов [2]), а число 1 является степенным вычетом.

В правой части последнего сравнения имеем два произведения степенных вычетов, каждое из которых является степенным вычетом (Свойство1 степенных вычетов) [2].

Следовательно, сравнение (4) является разложением 1 в сумму двух степенных вычетов.

Умножая сравнение (4) на ***v,*** получаем исходное сравнение (1) и убеждаемся в том, что нашли соответствующее ему разложение 1 в сумму двух степенных вычетов. Аналогичным путем мы можем однозначно найти разложение 1 в сумму двух степенных вычетов, соответствующее любому варианту разложения любого степенного вычета. Вариант разложения определяется парой соседних степенных вычетов.

Теорема доказана.

Д о к а з а т е л ь с т в о теоремы Ферма. Запишем уравнение Ферма для простой степени *p* в виде

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

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

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

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

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

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

Если есть решения сравнения (3), то говорят, что имеет место разложимость вычетов степени *p* в сумму двух вычетов степени *p* по модулю *m.*

Если уравнение (1) Ферма имеет решение, то сравнение (2) должно выполняться по модулю любого числа.

Выберем два простых модуля $m_1 > c^p$ и $m_2 > c^p$, $m_1 < m_2$.

Будем считать, что вычеты степени ***p*** по модулям m_1 и m_2 разложимы в сумму двух степенных вычетов. Если бы это было не так, то сравнение (3) не имело бы нетривиального решения, а следовательно остается только тривиальное решение, когда какое то из чисел *a,b,c* сравнимо с нулем по модулю m_1 или m_2 .

Последнее означает, что наше предположение о существовании решения в (1) неверно, так как мы выбрали $m_1 > c^p$, $m_2 > c^p$. Для доказательства теоремы Ферма следует рассматривать уравнение Ферма в виде разложения степеней чисел, именно так как сформулирована теорема [2].

Как следует из доказанной выше теоремы, любое разложение степенных вычетов можно представить как произведение этого степенного вычета и разложения 1 в сумму двух степенных вычетов. Следовательно, существует такое разложение 1

$$1 \equiv u_{1,1} + u_{2,1} (\mathrm{mod}\ m_1) \tag{4}$$

которое после умножения на V_c даст сравнение

$$V_c \equiv u_{1,1} \cdot V_c + u_{2,1} \cdot V_c (\mathrm{mod}\ m_1) \tag{5}$$

то есть даст сравнение (3).

где: $V_b \equiv u_{1,1} \cdot V_c (\mathrm{mod}\ m_1)$, $V_a \equiv u_{2,1} \cdot V_c (\mathrm{mod}\ m_1)$

Так как сравнение (3) должно выполняться и по модулю простого числа m_2, то существует разложение 1 и по модулю m_2

$$1 \equiv u_{1,2} + u_{2,2} (\mathrm{mod}\ m_2) \tag{6}$$

которое также должно дать сравнение (3) после умножения на V_c

$$V_c \equiv u_{1,2} \cdot V_c + u_{2,2} \cdot V_c (\mathrm{mod}\ m_2) \tag{7}$$

где: $V_b \equiv u_{1,2} \cdot V_c (\mathrm{mod}\ m_2)$, $V_a \equiv u_{2,2} \cdot V_c (\mathrm{mod}\ m_2)$

Если сравнение (3) выполняется по модулю m_1 и модулю m_2, то оно должно выполняться и по модулю произведения модулей $m_1 \cdot m_2$.

Теперь найдем разложение V_c по модулю $m_1 \cdot m_2$. Для этого найдем разложение вычета 1 в сумму двух степенных вычетов по модулю $m_1 \cdot m_2$ совместным решением сравнений (4),(6) [2]. Разложения (4) и 6) различны, так как $m_1 \neq m_2$.

Найдем слагаемые правой части следующим образом

$$u_1 \equiv m_2 \cdot m_1' \cdot u_{1,1} + m_1 \cdot m_2' \cdot u_{1,2} (\mathrm{mod}\ m_1 \cdot m_2) \tag{8}$$

$$u_1 \equiv m_2 \cdot m_1' \cdot u_{2,1} + m_1 \cdot m_2' \cdot u_{2,2} (\mathrm{mod}\ m_1 \cdot m_2) \tag{9}$$

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

Теперь можем написать разложение 1 в сумму двух степенных вычетов по модулю $m_1 \cdot m_2$.

$$1 \equiv u_1 + u_2 (\mathrm{mod}\ m_1 \cdot m_2) \tag{10}$$

и соответственно разложение V_c по модулю $m_1 \cdot m_2$

$$V_c \equiv u_1 \cdot V_c + u_2 \cdot V_c (\mathrm{mod}\ m_1 \cdot m_2) \tag{11}$$

В правильности последнего сравнения по модулю $m_1 \cdot m_2$ можно убедиться, проверив его по модулю m_1 и модулю m_2. Теперь перейдем к решениям для (10),(11). Вычеты u_1 и u_2 в (10) это степенные вычеты по модулю $m_1 \cdot m_2$. Они имеют какие то решения

$$1 \equiv {k_1}^p + {k_2}^p (nod m_1 \cdot m_2) \tag{12}$$

Степенной вычет $V_c \equiv c^p (\mathrm{mod}\ m_1 \cdot m_2)$. Число c^p является наименьшим положительным степенным вычетом по модулю $m_1 \cdot m_2$ так как мы задали выше $m_1 > c^p$, $m_2 > c^p$. Подставим значения степенных вычетов в (11).

$$c^p \equiv {k_1}^p \cdot c^p + {k_2}^p \cdot c^p (\mathrm{mod} m_1 \cdot m_2) \tag{13}$$

Очевидно, что ${k_1}^p \cdot c^p > m_1 \cdot m_2$, ${k_2}^p \cdot c^p > m_1 \cdot m_2$. Если бы это было не так, то сравнение (13) можно было сократить на c^p и ясно, что уравнение Ферма получить нельзя.

Можно ли из (13) получить уравнение (1). Если такое было бы возможно, то должно выполняться сравнение (2) по модулю $m_3 > m_2$. Однако разложение 1 по модулю m_3 отличается от (4),(6),(10). Поэтому мы должны найти разложение 1 по модулю m_3 и далее это сравнение решить совместно с (10) и найти разложение 1 в сумму двух степенных вычетов по модулю $m_1 \cdot m_2 \cdot m_3$. В полученном решении по модулю $m_1 \cdot m_2 \cdot m_3$ слагаемые в правой части будут больше чем $m_1 \cdot m_2 \cdot m_3$.

Таким образом, процесс поиска решений сравнения (3) по модулю $m_1 \cdot m_2 \cdot m_3$ свелся к поиску разложения 1 по модулю m_3, если вообще имеет место разложимость степенных вычетов по модулю m_3, и его совместному решению с (10) и умножению на c^p. Для каждого следующего простого модуля вышеописанный процесс следует повторить. Количество простых чисел-бесконечное множество. Поэтому найти решение уравнения Ферма в конечных числах невозможно.

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

$$(c^{2^{i_1}})^4 = (b^{2^{i_1}})^4 + (a^{2^{i_1}})^4 \qquad (14)$$

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 р, то есть $n = n_1 \cdot p$. Тогда уравнение Ферма можно написать в виде

$$(c^{n_1})^p = (b^{n_1})^p + (a^{n_1})^p \qquad (15)$$

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

Теорема Ферма доказана полностью.

Литература

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

2. Камлия Р.А. Теорема Ферма и разложимость степенных вычетов, Абхазский научный центр Российской академии космонавтики им. К.Э. Циолковского, Сухум,2008г.