УДК 511.522.2

С. М. Вахтеров
МГТУ им. Н.Э.Баумана
г. Москва, Россия

ДОКАЗАТЕЛЬСТВО ВЕЛИКОЙ ТЕОРЕМЫ ФЕРМА ПРИ УСЛОВИИ: НОД($\varphi(x)$, $\varphi(y)$, $\varphi(z)$, e) = e

В работе доказывается теорема, касающаяся Великой теоремы Ферма, для указанного в заголовке условия.

Полученный результат не завершает доказательство ВТФ, начатое в работе "Криптосистема RSA против ВТФ"[5], но приводит к результатам, которые помогают существенно ограничить область допустимых значений переменных уравнения простыми математическими операциями.

Данное доказательство ВТФ [1] для уравнения Ферма, слегка измененного вида:

$$x^e + y^e + z^e = 0,$$

где e - простое число больше двух, подразумевает две части (по свойствам функции Эйлера):

1) $(\varphi(x), \varphi(y), \varphi(z), e) = 1$,
2) $(\varphi(x), \varphi(y), \varphi(z), e) = e$.

Здесь и далее именно так (скобками) будет обозначаться наибольший общий делитель - Greatest Common Divisor.

Оба указанных случая не надо путать с известными Случаями 1 и 2 ВТФ, о которых можно почитать в [1]. Случай 1 рассматривает доказательство ВТФ, при условии, что ни одно из значений переменных уравнения, не кратно степени e, Случай 2, подразумевает доказательство противного случая, когда только одно из значений переменных кратно e:

В данном доказательстве активно используется функция Эйлера $\varphi(n)$, где n — натуральное число, равна количеству натуральных чисел, не больших n и взаимно простых с ним, [4]. Например, $\varphi(9)$ имеет шесть таких чисел: 1, 2, 4, 5, 7 и 8 взаимно простых 9.

$a^{\varphi(q)} \equiv 1 \ mod\ (q)$, для всех a взаимно простых с q.

Функция Эйлера играет ключевую роль в криптосистеме RSA.

Для случая $(\varphi(x), \varphi(y), \varphi(z), e) = 1$ доказательство выполнено на математических свойств функции Эйлера, использованных также в криптосистеме RSA в работе [2]. С упрощенным вариантом полученного результата (для уравнения $x^3 + y^3 + z^3 = 0$) можно ознакомиться здесь: “Доказательство ВТФ для n=3 (для любителей)” [6].

Данное доказательство развивает идеи метода Лежандра, использованные при доказательстве теоремы Софи Жермен [1] и первоначальной версии подобного доказательства [5].

Теорема. *Уравнение* $x^e+y^e+z^e = 0$ *не имеет решений, если:*

1) $(\varphi(x), \varphi(y), \varphi(z), e) = e$, *т.е. все целые числа* x, y, z, *имеют значения функции Эйлера, кратные* e. e *– простое число больше 2*.
2) *Выполняется хоть одно из следующих условий:*

$e^{\varphi(x)/e} \not\equiv 1 \ mod\ (x)$ и $(x,e)=1$;

$e^{\varphi(y)/e} \not\equiv 1 \ mod\ (y)$ и $(y,e)=1$;

$e^{\varphi(z)/e} \not\equiv 1 \ mod\ (z)$ и $(z,e)=1$.

Доказательство

Предположим, что условия теоремы выполнены.

Все переменные в основном уравнении ВТФ равноправны:

$x^e+y^e+z^e = 0$ (1).

Согласно арифметическим ограничениям ВТФ [1] переменные уравнения (1) взаимно просты:

$(x,y) = (x,z) = (y,z) = 1$ (2).

Для получения дальнейших результатов, определимся, что y кратно e. В доказательстве используются соотношения Барлоу для случая 2 ВТФ [1].

Согласно результатов Барлоу и других исследователей следует существование таких целых чисел: $x_1, x_2, y_1, y_2, z_1, z_2$, что:

множители x^e:

$y + z = x_1^e$ (3) ,

$y^{e-1} - y^{e-2}z + y^{e-3}z^2 - \ldots + z^{e-1} = x_2^e$ (4),

т.о. $x = -x_1 x_2$ (5),

множители y^e, $(y, e) = e$ (Случай 2 ВТФ):

$x + z = y_1^e e^{ne-1}$ (6),

$x^{e-1} - x^{e-2}z + x^{e-3}z^2 - \ldots + z^{e-1} = y_2^e e$ (7),

т.о. $y = -y_1 e^{ne} y_2$ (8), при n=0 – имеем Случай 1 ВТФ.

множители z^e:

$x + y = z_1^e$ (9),

$x^{e-1} - x^{e-2}y + x^{e-3}y^2 - \ldots + y^{e-1} = z_2^e$ (10),

т.о. $z = -z_1 z_2$ (11).

Для доказательства используем делители числа z. Если выполняются определенные условия в теореме, с таким же успехом, доказательство проводится с помощью делителей числа x.

Подслучай $(\varphi(z_1), e) = e$.

Так как по условию $(\varphi(z), e) = e$, а $z = z_1 z_2$, сначала рассмотрим случай $(\varphi(z_1), e) = e$ (12), затем возможность случая $(\varphi(z_1), e) = 1$ (13). Если в обоих случаях основное уравнение Ферма не имеет решений, то справедливость теоремы подтверждается.

(9) $\Rightarrow x \equiv -y \ mod\ (z_1)$ (14), (4) $\Rightarrow$

$x^e / \ (y + z) = (y^{e-1} - y^{e-2}z + y^{e-3}z^2 - \ldots + z^{e-1}) = x_2^e$ (15),

поэтому:

$x^{e-1} \equiv y^{e-1} \equiv x_2^e \ mod\ (z_1)$ (16). Тогда:

$$z_2^e = (x^e + y^e)/(x + y) =$$

$$= x^{e-1} + x^{e-2}(-y) + x^{e-3}(-y)^2 + \ldots + (-y)^{e-1} \equiv$$

$$\equiv ex^{e-1} \equiv ex_2^e \ mod\ (z_1)\ (17).$$

Пусть значение функции Эйлера числа z_1 равно $2ke$. В таком случае, возводим в степень $\varphi(z_1)/e = 2k$ левую и правую часть сравнения, чтобы получить значение показателя степени равным значению функции Эйлера числа z_1.

Возводим в степень $2k$ левую и правую часть сравнения:

$$(z_2)^{2ke} \equiv e^{2k}\ x_2{}^{2ke}\ mod\ (z_1)\ (18),$$

$$z_2{}^{2ke} \equiv z_2{}^{\varphi(z_1)} \equiv 1 \equiv e^{2k} \equiv e^{\varphi(z_1)/e}\ mod(z_1)\ (19).$$

Несложно проверить, что это условие эквивалентно условию:

$$1 \equiv 2k^{2k} \equiv 2k^{\varphi(z_1)/e}\ mod(z_1)\ (20).$$

И это невозможно, т.к. это условие заложено в условие нашей теоремы. Данное условие было “подсмотрено” в доказательстве теоремы Лежандра.

Тем самым, доказан случай - $(\varphi(z_1), e) = e$ теоремы.

Примеры:

Пусть z_1=31. Тогда $\varphi(z_1)$ = 2*3*5.

Для e=3, $(\varphi(z_1), 3) = 3$: $e^{2k}=3^{2*5} \equiv 25\ (mod\ 31)$, т.е. ВТФ справедлива, т.к. соответствует условию теоремы.

Для e=5, $(\varphi(z_1), 5) = 5$: $e^{2k}=5^{2*3} \equiv 1\ (mod\ 31)$, т.е. не соответствует требованию теоремы, устанавливающему справедливость ВТФ для данного случая. (Дополнение к примеру: $7^5 \equiv 5\ (mod\ 31)$, $19^5 \equiv 5\ (mod\ 31)$, что является альтернативным свойством, использованным Лежандром, при доказательстве теоремы ВТФ для Случая 1).

Примеры чисел, которые "*мешают*" полному доказательству ВТФ, предложенным способом:

$3^{\varphi(61)/3} \equiv 1 \bmod (61)$; $5^{\varphi(31)/5} \equiv 1 \bmod (31)$.

Для простых чисел вида $2ke+1$ выполняется $e^{\varphi(2ke+1)/e} \equiv 1 \; mod \; (2ke+1)$, когда:

e =3; k =10, 11, 12, 15, 17;
e =7; k =3;
e =11; k =6;
e =13; k =4, 6;
e =19; k =4.

Подслучай при $(\varphi(z_1), e) = 1$

Так как $(\varphi(z_1), e) = 1$, а по предусловию $(\varphi(z), e) = e$, то следует, что $(\varphi(z_2), e) = e$, т.е. $\varphi(z_2) = 2ke$ (21).

Сгруппируем переменные следующим образом:

$(y+z) + (x+z) - (x+y) = 2z$ (22).

Для этого уравнения, согласно соотношений Барлоу для Случая 1 и Случая 2 ВТФ [1], выводятся следующие уравнения:

Случай 1 ВТФ: $(y, e) = 1$ и $(\varphi(z_2), e) = e$ (23):

$x_1^e + y_1^e - z_1^e = 2z = -2z_1 z_2$ (24),

$2z \equiv x_1^e + y_1^e - z_1^e \equiv 0 \; mod \; (z_2)$ (25),

$x_1^e + y_1^e \equiv z_1^e \; mod \; (z_2)$ (26),

$(x_1^e + y_1^e)^{2k} \equiv z_1^{\varphi(z_2)} \equiv 1 \; mod \; (z_2)$ (27), что невозможно по условию 2 теоремы.

Рассмотрим тривиальный пример с использованием простых чисел Софи Жермен. Пусть e – число Софи Жермен. Согласно определению чисел Софи Жермен: $2e+1$ – тоже простое число. Рассмотрим, $\varphi(z_2) = 2e$. На самом

деле, мы можем выбрать любой вариант представления числа, но вариант с числом Софи Жермен, является наиболее наглядным, с точки зрения, истории доказательства теоремы. Тогда:

$(x_1^e + y_1^e)^2 \equiv z_1^{2e} \ mod\ (z_2{=}2e{+}1)$,

$(x_1^e + y_1^e)^2 \equiv 1 \ mod\ (z_2{=}2e{+}1)$ (28),

$x_1^{2e} + y_1^{2e} + 2x_1^e y_1^e \equiv 1 \ mod\ (2e{+}1)$ (29),

$1 + 1 + 2x_1^e y_1^e \equiv 1 \ mod\ (2e{+}1)$ (30),

$2x_1^e y_1^e \equiv -1 \ mod\ (2e{+}1)$ (31), возведем в квадрат левую и правую часть, чтобы получить в показателе значение функции Эйлера числа $2e{+}1$:

$2^2 x_1^{\varphi(z_2)} y_1^{\varphi(z_2)} \equiv 1 \ mod\ (2e{+}1)$ (32),

$2^2 \equiv 1 \ mod\ (2e{+}1)$ (33), что невозможно.

{*Гипотеза.* Для этого случая возможно и другое доказательство - через соотношения Барлоу “второго порядка”, которые можно вывести из сравнения

$x_1^e + y_1^e + (-z_1^e) \equiv 0 \ mod\ (z_2)$ (34).

По методу Барлоу можно получить соотношения и множители для данного сравнения: $x_{1x}, x_{2x}, y_{1y}, y_{2y}, z_{1z}, z_{2z}$:

$x_1 = -x_{1x}x_{2x}$, $z_1 = -z_{1z}z_{2z}$ и $y_1 = -y_{1y}e^{ne}y_{2y}$ (35).

А далее методом, изложенным здесь для подслучая - НОД($\varphi(z_1)$, e) = e, выполнить подобное доказательство по модулю z_{1z}.}

<u>Случай 2 ВТФ</u>: НОД(y, e) = e и НОД($\varphi(z_2)$, e) = e (36):

$x_1^e + y_1^e e^{ne-1} - z_1^e = 2z = -2z_1 z_2$ (37),

$x_1^e \equiv -y_1^e e^{ne-1} \ mod\ (z_1)$ (38),

Возведём левую и правую часть сравнения в степень $\varphi(z_1)/e$:

$x_1^{\varphi(z_1)} \equiv y_1{}^{\varphi(z_1)} e^{\varphi(z_1)(ne-1)/e} \; mod\,(z_1)$ (39),

$1 \equiv e^{(ne-1)/e} \; mod\,(z_1)$ (40).

Однако, ne -1 не делится на e, поэтому $1 \not\equiv e^{(ne-1)/e} \; mod\,(z_1)$,

$x_1^e + y_1^e e^{en-1} - z_1^e \not\equiv 0 \; mod\,(z_1)$ (41).

Рассмотрим ещё один вариант доказательства этого случая, через модуль z_2.

$x_1^e + y_1^e e^{ne-1} - z_1^e = 2z = -\,2z_1 z_2$ (42),

$2z \equiv x_1^e + y_1^e e^{ne-1} - z_1^e \equiv 0 \; mod\,(z_2)$ (43).

Если данное сравнение справедливо, то должно быть справедливым и сравнение:

$2z \equiv x_1^e + y_1^e - z_1^e \equiv 0 \; mod\,(z_2)$ (44), справедливость для которого рассмотрена ранее. Т.е. сравнение

$x_1^e + y_1^e e^{ne-1} - z_1^e \equiv 0 \; mod\,(z_2)$ (45) справедливо тогда и только тогда, когда справедливо сравнение:

$x_1^e + y_1^e - z_1^e \equiv 0 \; mod\,(z_2)$ (46). Однако, как нами доказано, оно не имеет решения, при выполнении условий теоремы.

Т.о., при заданных условиях, теорема справедлива.

Усилить теорему можно, доказав, что ВТФ справедлива и для случая, без выполнения условия 2 теоремы.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. P. Ribenboim, Fermat's last theorem for amateurs, Springer-Verlag, New York, NY, 1999.
2. The RSA Cryptosystem against Last Fermat’s Theorem [fermat.2000.ru - http://fermat.2000.ru/fermats/2000ru_vsm_rsa1a_01_04_2010.htm]. // http:// fermat.2000.ru (Data 07.06.2010).
3. RSA [Vikipedia - http://en.wikipedia.org]. – Режим доступа: http://en.wikipedia.org/wiki/RSA (дата обращения 07.01.2010).

4. Euler's_theorem [Vikipedia - http://en.wikipedia.org]. – Режим доступа: http://en.wikipedia.org/wiki/Euler's_theorem (дата обращения 07.06.2010).
5. Криптосистема RSA против ВТФ [fermat.2000.ru - // http:// fermat.2000.ru http://www.fermat.2000.ru/fermats/2000ru_vsm_rsa1a_01_04_2010.htm (дата обращения - Data 07.06.2010).
6. "Доказательство ВТФ для n=3 (для любителей)" [fermat.2000.ru - http://www.fermat.2000.ru/fermats/proof_fermat_n3_last_theorem_rus_vakhterov.htm (дата обращения - Data 07.06.2010).

S.M. Vakhterov, student, Moscow State Technical University n.a. N.E. Bauman
M.I. Vakhterov, editor

Contact: 2000@2000.ru

http:// fermat.2000.ru/fermats/ case2vtf_version_actual.htm

Last Modified: August, 19, 2010