**Элементарное доказательство Великой теоремы Ферма**

Виктор Сорокин

Идея предлагаемого вниманию читателя элементарного доказательства Великой теоремы Ферма исключительно проста: после разложения чисел a, b, c на пары слагаемых, затем группировки из них двух сумм U' и U'' и умножения равенства a^n + b^n – c^n = 0 на 11^n (т.е. на 11 в степени n, а чисел a, b, c на 11) (k+3)-я цифра в числе a^n + b^n – c^n (где k – число нулей на конце числа a + b – c) не равна 0 (числа U' и U'' умножаются по-разному!). Для постижения доказательства нужно знать лишь формулу бинома Ньютона, простейшую формулировку малой теоремы Ферма (приводится), определение простого числа, сложение двух-трех чисел и умножение двузначного числа на 11. Вот, пожалуй, и ВСЁ! Самое главное (и трудное) – не запутаться в десятке цифр, обозначенных буквами. Формальное описание истории теоремы и библиография в русском тексте опущены.

Доказательство приводится в редакции от 1 июня 2005 года (с учетом дискуссии на мехматовском сайте).

В.С.

ИНСТРУМЕНТАРИЙ: [В квадратных скобках приводится поясняющая, не обязательная информация.]

Используемые обозначения:

Все числа записаны в системе счисления с простым основанием n > 10.

[Все случаи с составным n, кроме n = 2k (который сводится к случаю n = 4), сводятся к случаю

простого n с помощью простой подстановки. Случаи n = 3, 5 и 7 здесь не рассматриваются.]

ak – k-я цифра от конца в числе a (a1 – последняя цифра).

[Пример для a = 1043: 1043 = 1x53 + 0x52 + 4x51 + 3x50; a1 = 3, a2 = 4, a3 = 0, a4 = 1.]

a(k) – окончание (число) из k цифр числа a (a(1) = a1; 1043(3) = 043). Везде в тексте a1 № 0.

[Если все три числа a, b и c оканчиваются на ноль, следует разделить равенство 1° на nn.]

(ain)1 = ai и (ain - 1)1 = 1 (см. Малую теорему Ферма для ai № 0). (0.1°)

(n + 1)n = (10 + 1)n = 11n = …101 (см. Бином Ньютона для простого n).

Простое следствие из бинома Ньютона и малой теоремы Ферма для s № 1 [a1 № 0]:

если цифра as увеличивается/уменьшается на 0 < d < n,

то цифра ans+1 увеличивается/уменьшается на d (или d + n, или d – n). (0.2°)

[В отрицательных числах цифры считаются отрицательными.]

\*\*\*

(1°) Допустим, что an + bn – cn = 0 .

Случай 1: (bc)1 ? 0.

(2°) Пусть u = a + b – c, где u(k) = 0, uk+1 ? 0, k > 0 [известно, что в 1° u > 0 и k > 0].

(3°) Умножим равенство 1° на число d1n (см. §§2 и 2a в Приложении) с целью превратить

цифру uk+1 в 5. После этой операции обозначения чисел не меняются

и равенство продолжает идти под тем же номером (1°).

Очевидно, что и в новом равенстве (1°) u = a + b – c, u(k) = 0, uk+1 = 5.

(1\*°) И пусть a\*n + b\*n – c\*n = 0, где знаком “\*” обозначены записанные в каноническом виде числа в равенстве (1°) после умножения равенства (1°) на 11n .

(4°) Введем в указанной здесь очередности следующие числа: u, u' = a(k) + b(k) – c(k),

u'' = u – u' = (a – a(k)) + (b – b(k)) – (c – c(k)), v = (ak+2 + bk+2 – ck+2)1, u\*' = a\*(k) + b\*(k) – c\*(k),

u\*'' = u\* – u\*' = (a\* – a\*(k)) + (b\* – b\*(k)) – (c\* – c\*(k)), 11u', 11u'', v\* = (a\*k+2 + b\*k+2 – c\*k+2)1,

и вычислим две последние значащие цифры в этих числах:

(3a°) uk+1 = (u'k+1 + u''k+1)1 = 5;

(5°) u'k+1 = (–1, 0 или 1) – так как – nk < a'(k) < nk, – nk < b'(k) < nk, – nk < c'(k) < nk

и числа a, b, c имеют различные знаки;

(6°) u''k+1 = (4, 5 или 6) (см. 3a° и 5°) [важно: 1 < u''k+1 < n – 1];

(7°) u'k+2 = 0 [всегда!] – так как \u'\ < 2nk ;

(8°) u''k+2 = uk+2 [всегда!];

(9°) u''k+2 = [v + (ak+1 + bk+1 – ck+1)2]1, где (ak+1 + bk+1 – ck+1)2 = (–1, 0 или 1);

(10°) v = [uk+2 – (a(k+1) + b(k+1) – c(k+1))k+2]1 [где (a(k+1) + b(k+1) – c(k+1))k+2 = (–1, 0 или 1)] =

= [uk+2 – (–1, 0 или 1)]1;

(11°) u\*k+1 = uk+1 = 5 – т.к. u\*k+1 и uk+1 – последние значащие цифры в числах u\* и u;

(12°) u\*'k+1 = u'k+1 – т.к. u\*'k+1 и u'k+1 – последние значащие цифры в числах u\*' и u';

(13°) u\*''k+1 = (u\*k+1 – u\*'k+1)1 = (3 – u\*'k+1)1 = (4, 5 или 6) [важно: 1 < u\*''k+1 < n – 1];

(14°) (11u')k+2 = (u'k+2 + u'k+1)1 (затем – в результате приведения чисел к каноническому виду –

величина u'k+1 «уходит» в u\*''k+2, поскольку u\*'k+2 = 0);

(14a°) важно: числа (11u')(k+2) и u\*'(k+2) отличаются только k+2-ми цифрами, а именно:

u\*'k+2 = 0, но (11u')k+2 № 0 в общем случае;

(15°) (11u'')k+2 = (u''k+2 + u''k+1)1;

(16°) u\*k+2 = (uk+2 + uk+1)1 = (u''k+2 + uk+1)1 = (u''k+2 + 5)1;

(16а°) к сведению: u\*'k+2 = 0 (см. 7°);

(17°) u\*''k+2 = (u\*k+2 +1, u\*k+2 или u\*k+2 – 1)1 = (см. 9°) = (u''k+2 + 4, u''k+2 + 5 или u''k+2 + 6)1;

(18°) v\* = [u\*k+2 – (a\*(k+1) + b\*(k+1) – c\*(k+1))k+2]1

[где u\*k+2 = (uk+2 + uk+1)1 (см. 16°), а (a\*(k+1) + b\*(k+1) – c\*(k+1))k+2 = (–1, 0 или 1) – см. 10°] =

= [(uk+2 + uk+1)1 – (–1, 0 или 1)]1.

(19°) Введем числа U' = (ak+1)n + (bk+1)n – (ck+1)n, U'' = (an + bn – cn) – U', U = U' + U'',

U\*' = (a\*k+1)n + (b\*k+1)n – (c\*k+1)n, U\*'' = (a\*n + b\*n – c\*n) – U\*', U\* = U\*' + U\*'';

(19а°) к сведению: U'(k+1) = U\*'(k+1) = 0.

(20°) Лемма: U(k+2) = U'(k+2) = U''(k+2) = U\*(k+2) = U\*'(k+2) = U\*''(k+2) = 0 [всегда!].

Действительно, из 1° мы имеем:

U = an + bn – cn =

= (a(k+1) + nk+1ak+2 + nk+2Pa)n + (b(k+1) + nk+1bk+2 + nk+2Pb)n – (c(k+1) + nk+1ck+2 + nk+2Pc)n =

= (a(k+1)n + b(k+1)n – c(k+1)n) + nk+2(ak+2a(k+1)n - 1 + bk+2b(k+1)n - 1 – ck+2c(k+1)n - 1) + nk+3P =

= U' + U'' = 0, где

U' = a(k+1)n + b(k+1)n – c(k+1)n,

(20a°) U'' = nk+2(ak+2a(k+1)n -1 + bk+2b(k+1)n -1 – ck+2c(k+1)n -1) + nk+3P,

где (ak+2a(k+1)n -1 + bk+2b(k+1)n -1 – ck+2c(k+1)n -1)1 = (см. 0.1°)=

(20b°) = (ak+2 + bk+2 – ck+2)1 = U''k+3 = v (см. 4°).

(21°) Следствие: (U'k+3 + U''k+3)1 = (U\*'k+3 + U\*''k+3)1 = 0.

(22°) Вычислим цифру (11nU')k+3:

[так как числа (11u')(k+2) и u\*'(k+2) отличаются только k+2-ми цифрами на величину

(11u')k+2), то на эту величину будут отличаться и цифры (11nU')k+3 и U\*'k+3, это означает,

что цифра (11nU')k+3 будет на (11u')k+2 превышать цифру U\*'k+3 (см. 0.2°)]

(11nU')k+3 = U'k+3 = (U\*'k+3 + (11u')k+2)1 = (U\*'k+3 + u'k+1)1.

(23°) Откуда U\*'k+3 = U' k+3 – u'k+1.

(24°) Вычислим цифру U\*'' k+3 :

U\*'' k+3 = v\* = (uk+2 + uk+1)1 – (–1, 0 или 1) – см. (18°);

(25°) Наконец, вычислим цифру (U\*'k+3 + U\*''k+3)1:

(U\*'k+3 + U\*''k+3)1 = (U\*'k+3 + U\*''k+3 – U'k+3 – U''k+3)1 = (U\*'k+3 – U'k+3 + U\*''k+3 – U''k+3)1 =

(см. 23° и 24°) = (– u'k+1 + v\* – v) = (см. 18° и 10°) =

= (– u'k+1 + [uk+2 + uk+1 – (–1, 0 или 1)] – [uk+2 – (–1, 0 или 1)])1 =

= (– u'k+1 + uk+1 + (–2, –1, 0, 1, или 2))1 = (см. 3a°) =

( u''k+1 + (–2, –1, 0, 1, или 2))1 = (см. 6°) = (2, 3, 4, 5, 6, 7 или 8) № 0,

что противоречит 21° и, следовательно, выражение 1° есть неравенство.

Случай 2 [доказывается аналогично, но намного проще]: b (или c) = ntb', где b1 = 0 и bt+1 = b'1 № 0.

(26°) Введем число u = c – a > 0, где u(nt – 1) = 0, а unt ? 0 (см. §1 в Приложении).

(27°) После умножения равенства 1° на число d1n (с целью превратить цифру unt в 5)

(см. §§2 и 2a в Приложении) обозначения чисел сохраняются.

(28°) Пусть: u' = a(nt – 1) – c(nt – 1), u'' = (a – a(nt – 1)) – (c – c(nt – 1)) (где, очевидно, u''nt = (ant – cnt)1);

U' = a(nt)n + bn – c(nt)n (где U'(nt + 1) = 0 – см. 1° и 26°), U'' = (an – a(nt)n) – (cn – c(nt)n),

U\*' = a\*(nt)n + b\*n – c\*(nt)n (где U\*'(nt + 1) = 0), U\*'' = (a\*n – a\*(nt)n) – (c\*n – c\*(nt)n),

v = ant+1 – cnt+1.

Вычисления, полностью аналогичные вычислениям в случае 1, показывают, что nt+2-я цифра в равенстве Ферма не равна нулю. Число b во всех расчетах (кроме самой последней операции и в п. 27°) можно проигнорировать, т.к. цифры bnnt+1 и bnnt+2 при умножении равенства 1° на 11n не меняются (т.к. 11n(3) = 101).

Таким образом, для простых n > 7 теорема доказана.

==================

ПРИЛОЖЕНИЕ

§1. Если числа a, b, c не имеют общих сомножителей и b1 = (c – a)1 = 0,

тогда из числа R = (cn – an)/(c – a) =

= cn –1 + cn –2a + cn –3a2 + … c2an - 3 + can - 2 + an - 1 =

= (cn –1 + an –1) + ca(cn –3 + an –3) + … + c(n –1)/2a(n –1)/2 =

= (cn –1 – 2c(n –1)/2a(n –1)/2 + an –1 + 2c(n –1)/2a(n –1)/2) + ca(cn –3 – 2c(n –3)/2a(n –3)/2 + an –3 + 2c(n –3)/2a(n –3)/2) +

+ … + c(n –1)/2a(n –1)/2 = (c – a)2P + nc(n –1)/2a(n –1)/2 следует, что:

c – a делится на n2, следовательно R делится на n и не делится на n2;

так как R > n, то число R имеет простой сомножитель r не равный n;

c – a не делится на r;

если b = ntb', где b'1 № 0, то число c – a делится на ntn – 1 и не делится ntn.

§2. Лемма. Все n цифр (a1di)1, где di = 0, 1, … n – 1, различны.

Действительно, допустив, что (a1d1\*)1 = (a1d1\*\*)1, мы находим: ((d1\* – d1\*\*)a1)1 = 0.

Откуда d1\* = d1\*\*. Следовательно, множества цифр a1 (здесь вместе с a1 = 0) и d1 совпадают.

[Пример для a1 = 2: 0: 2x0 = 0; 1: 2x3 = 11; 2: 2x1 = 2; 3: 2x4 = 13; 4: 2x2 = 4.

При составном n Лемма несправедлива: в базе 10 и (2х2)1 = 4, и (2х7)1 = 4.]

§2a. Следствие. Для любой цифры a1 № 0 cуществует такая цифра di, что (a1di)1 = 1.

[Пример для a1 = 1, 2, 3, 4: 1x1 = 1; 2x3 = 11; 3x2 = 11; 4x4 = 31.]

ВИКТОР СОРОКИН

e-mail: victor.sorokine@wanadoo.fr

4 ноября 2004, Франция

P.S. Доказательство для случаев n = 3, 5 , 7 аналогично, но в (3°) цифра uk+1 превращается не в 5, а в 1, и в (1\*°) равенство (1°) умножается не на 11n, а на некоторое hn, где h – некоторое однозначное число.