Идея предлагаемого вниманию читателя элементарного доказательства Великой теоремы Ферма исключительно проста: после 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 не равна 0 (где k – число нулей в конце числа $a + b - c$).
Для понимания доказательства нужно знать лишь формулу бинома Ньютона, простейшую формулировку (приводится) малой теоремы Ферма, определение простого числа, сложение двух-трех чисел и умножение двузначного числа на 11. Вот и ВСЁ! Самое главное – не запутаться в десятке цифр, обозначенных буквами.
Формальное описание истории теоремы и библиография в русском тексте опущены.

В.С.

Элементарное доказательство Великой теоремы Ферма

ВИКТОР СОРОКИН

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

Используемые обозначения:
Все числа записаны в системе счисления с простым основанием $n > 5$.

[Все случаи с составным n, кроме $n = 2^k$ (который сводится к случаю $n = 4$), сводятся к случаю простого n с помощью простой подстановки.
Случай $n = 3$ или 5 доказывается с помощью другого числа u – см. 1.1.]

a_k – k-я цифра от конца в числе a (a_1 – последняя цифра).

[*Пример для* $a = 1043$: $1043 = \mathbf{1}x5^3 + \mathbf{0}x5^2 + \mathbf{4}x5^1 + \mathbf{3}x5^0$; $a_1 = \mathbf{3}$, $a_2 = \mathbf{4}$, $a_3 = \mathbf{0}$, $a_4 = \mathbf{1}$.]

$a_{(k)}$ – окончание (число) из k цифр числа a ($a_{(1)} = a_1$; $1043_{(3)} = 043$). Везде в тексте a_1 ¹ 0.

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

$(a_i^n)_1 = a_i$ и $(a_i^{n-1})_1 = 1$ (см. Малую теорему Ферма для a_i ¹ 0). (0.1°)

$(n + 1)^n = (10 + 1)^n = 11^n = \ldots 101$ (см. Бином Ньютона для простого n).

Простое следствие из бинома Ньютона и малой теоремы Ферма для s ¹ 1:
если цифра a_s увеличивается/уменьшается на $0 < d < n$, то цифра a^n_{s+1} увеличивается/уменьшается на d (или $d + n$, или $d - n$).

***

Допустим, что $a^n + b^n - c^n = 0$ (1°)

и $a^{*n} + b^{*n} - c^{*n} = 0$, (1*°)

где знаком “*” обозначены числа в равенстве 1°
после умножения равенства (1°) на $d_1{}^n 11^n$ (см. 1.2° и 2.2°).

Случай 1: $(bc)_1$ ¹ 0.

Пусть $u = a + b - c = n^k v$, где $u_{k+1} = v_1$ ¹ 0, $k > 0$ [в 1° $u > 0$ и $k > 0$]. (1-1°)

Умножим равенство 1° на число $d_1{}^n$ (см. §§2 и 2a в Приложении)
с целью превратить цифру v_1 (см. 01°) в 3. (1.2°)

Пусть:

$u = u' + u''$, где $u' = a_{(k)} + b_{(k)} - c_{(k)}$, $u'' = u - u' = (a - a_{(k)}) + (b - b_{(k)}) - (c - c_{(k)})$, (1.3°)

откуда $u''_{(k)} = 0$, $u''_{k+1} = (a_{k+1} + b_{k+1} - c_{k+1})_1 = (u_{(k+1)} - u')_1$;

$u_{k+1} = v_1 = v'_1 + v''_1 = 3$, где $v'_1 = u'_{k+1}$ и $v''_1 = u''_{k+1}$; (1.4°)

здесь $/a_{(k)}/ < n^{k+1}$, $/b_{(k)}/ < n^{k+1}$, $/c_{(k)}/ < n^{k+1}$, следовательно $/a_{(k)} + b_{(k)} - c_{(k)}/ = /u'/ < 3n^{k+1} < n^{k+2}$,

следовательно $u'_{(k)} = 0$, $u'_{k+2} = 0$ [всегда!], $u''_{k+2} = u_{k+2}$ [всегда!], $u''_{k+1} = v''_1$ ¹ 0; (1.5°)

$U = a^n + b^n - c^n = U' + U''$ [= 0], где (1.6°)

$U' = a_{(k+1)}{}^n + b_{(k+1)}{}^n - c_{(k+1)}{}^n$, $U'' = U - U' = (a^n - a_{(k+1)}{}^n) + (b^n - b_{(k+1)}{}^n) - (c^n - c_{(k+1)})$. (1.7°)

Покажем, что $U_{(k+2)} = U'_{(k+2)} = U''_{(k+2)} = U^*_{(k+2)} = U^{*\prime}_{(k+2)} = U^{*\prime\prime}_{(k+2)} = 0$ [всегда!]. (1.8°)

Действительно, из 1° мы имеем:

$$U = a^n + b^n - c^n =$$
$$= (a_{(k+1)} + n^{k+1}a_{k+2} + n^{k+2}P_a)^n + (b_{(k+1)} + n^{k+1}b_{k+2} + n^{k+2}P_b)^n - (c_{(k+1)} + n^{k+1}c_{k+2} + n^{k+2}P_c)^n =$$
$$= (a_{(k+1)}{}^n + b_{(k+1)}{}^n - c_{(k+1)}{}^n) + n^{k+2}(a_{k+2}a_{(k+1)}{}^{n-1} + b_{k+2b(k+1)}{}^{n-1} - c_{k+2c(k+1)}{}^{n-1}) + n^{k+3}P =$$
$$= U' + U'' = 0, \text{ где}$$
$$U' = a_{(k+1)}{}^n + b_{(k+1)}{}^n - c_{(k+1)}{}^n,$$
$$U'' = n^{k+2}(a_{k+2}a_{(k+1)}{}^{n-1} + b_{k+2b(k+1)}{}^{n-1} - c_{k+2c(k+1)}{}^{n-1}) + n^{k+3}P; \quad (1.9°)$$

где $(a_{k+2}a_{(k+1)}{}^{n-1} + b_{k+2}b_{(k+1)}{}^{n-1} - c_{k+2}c_{(k+1)}{}^{n-1})_1 =$ (см. 0.1°)=

$= (a_{k+2} + b_{k+2} - c_{k+2})_1 = u_{k+2}$ (так как $u'_{k+2} = 0$!) $= U_{k+3}$. (1.10°)

Из 1.9° мы имеем: $U_{(k+2)} = U'_{(k+2)} = U''_{(k+2)} = U^*_{(k+2)} = U^{*\prime}_{(k+2)} = U^{*\prime\prime}_{(k+2)} = 0$;

$\boldsymbol{(U'_{k+3} + U''_{k+3})_1 = (U^{*\prime}_{k+3} + U^{*\prime\prime}_{k+3})_1 = 0}$. (1.10a°)

Легко вычислить следующие цифры:

1.11 $u^{*\prime}_{k+2} = u'_{k+2} = 0$ (ñм. 1.5°);

1.12 $(11u')_{k+2} = (u'_{k+2} + u'_{k+1})_1 = (u'_{k+2} + v'_1)_1$ (затем v'_1 «уходит» в $u^{*\prime\prime}_{k+2}$, поскольку $u^{*\prime}_{k+2} = 0$);

1.13 $(11u'')_{k+2} = (u''_{k+2} + v''_1)_1$;

1.14 $u^{*\prime\prime}_{k+2} = (u''_{k+2} + v''_1 + v'_1)_1$ (пришедший из $u^{*\prime}_{k+2}$ – см. 1.12) $= (u''_{k+2} + v_1)_1$;

1.15 $u^*_{\boldsymbol{k+2}} = (11u)_{k+2} = (u_{k+2} + v_1)_1 = [u_{k+2} + (v'_1 + v''_1)_1]_1$;

1.16 $(11^nU')_{k+3} = U'_{k+3} =$ (cf. 1.12) $= [U^{*\prime}_{k+3} + (11u')_{k+2}]_1 = (U^{*\prime}_{k+3} + u'_{k+1})_1 = (U^{*\prime}_{k+3} + v'_1)_1$,

откуда $U^{*\prime}_{k+3} = U'_{k+3} - v'_1$;

1.17 $U^{*\prime\prime}_{k+3} = u^{*\prime\prime}_{k+2} =$ (cf. 1.14.) $= (u''_{k+2} + v_1)_1 = (U''_{k+3} + \boldsymbol{v_1})_1$;

1.18 $(11^nU)_{k+3} = U^*_{k+3} = 0 = (U^{*\prime}_{k+3} + U^{*\prime}_{k+3})_1 = (U'_{k+3} - v'_1 + U''_{k+3} + v_1)_1 = (v_1 - v'_1)_1 = v''_1$.

Откуда $\boldsymbol{v''_1 = 0}$, что противоречит 1.5° и 10a°.

Случай 2 [доказывается аналогично]**:** b (или c) $= n^ta'$, где $b_1 = 0$ и $b_{t+1} = a'_1$ ¹ 0.

Но здесь: $u = a - c = n^{tn-1}v > 0$, где v_1 ¹ 0 (см. §1 в Приложении). (2.1°)

Умножим равенство 1° на число $d_1{}^n$ с целью превратить цифру v_1 (см. 01°) в 3 (2.2°)

(см. §§2 и 2a в Приложении).

Пусть: $u = u' + u''$, где $u' = a_{(nt-1)} - c_{(nt-1)}$, $u'' = (a - a_{(nt-1)}) - (c - c_{(nt-1)})$, где $u''_{nt} = (a_{nt} - c_{nt})_1$; (2.3°)

$U' = a_{(nt)}{}^n + b^n - c_{(nt)}{}^n$, $U'_{(nt+1)} = 0$, $U'' = (a^n - a_{(nt)}{}^n) - (c^n - c_{(nt)}{}^n)$, $W_{nt+2} = a_{nt+1} - c_{nt+1}$. (2.6°)

Легко вычислить следующие цифры:

2.11 $u^{*\prime}_{nt+1} = u'_{nt+1} = 0$;

2.12 $(11u')_{nt+1} = (u'_{nt+1} + u'_{nt})_1 = (u'_{nt+1} + v'_1)_1$ (затем v'_1 «уходит» в $u^{*\prime\prime}_{nt+1}$, поскольку $u^{*\prime}_{nt+1} = 0$);

2.13 $(11u'')_{nt+1} = (u''_{nt+1} + v''_1)_1$;

2.14 $u^{*\prime\prime}_{nt+1} = (u''_{nt+1} + v''_1 + v'_1)_1$ (пришедший из $u^{*\prime}_{nt+1}$ – см. 1.12) $= (u''_{nt+1} + v_1)_1$;

2.15 $u^*_{\boldsymbol{nt+1}} = (11u)_{nt+1} = (u_{nt+1} + v_1)_1 = [u_{nt+1} + (v'_1 + v''_1)_1]_1$;

2.16 $(11^nU')_{nt+2} = U'_{nt+2} =$ (cf. 1.12) $= [U^{*\prime}_{nt+2} + (11u')_{nt+1}]_1 = (U^{*\prime}_{nt+2} + u'_{nt})_1 = (U^{*\prime}_{nt+2} + v'_1)_1$,

откуда $U^{*\prime}_{nt+2} = (U'_{nt+2} - v'_1)_1$;

2.17 $U^{*\prime\prime}_{nt+2} = u^{*\prime\prime}_{nt+1} =$ (ñì. 1.14.) $= (u''_{nt+1} + v_1)_1 = (U''_{nt+2} + \boldsymbol{v_1})_1$;

2.18 $(11^nU)_{nt+2} = U^*_{nt+2} = 0 = (U^{*\prime}_{nt+2} + U^{*\prime}_{nt+2})_1 = (U'_{nt+2} - v'_1 + U''_{nt+2} + v_1)_1 = (v_1 - v'_1)_1 = v''_1$.

Откуда $\boldsymbol{v''_1 = 0}$, что **противоречит** 1.5° и 10a°.

Теорема доказана.

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

ПРИЛОЖЕНИЕ

§1. Если числа a, b, c не имеют общих сомножителей и $b_1 = (c - a)_1 = 0,$

тогда из числа $R = (c^n - a^n)/(c - a) =$

$= c^{n-1} + c^{n-2}a + c^{n-3}a^2 + \dots c^2a^{n-3} + ca^{n-2} + a^{n-1} =$

$= (c^{n-1} + a^{n-1}) + ca(c^{n-3} + a^{n-3}) + \dots + c^{(n-1)/2}a^{(n-1)/2} =$

$= (c^{n-1} - 2c^{(n-1)/2}a^{(n-1)/2} + a^{n-1} + 2c^{(n-1)/2}a^{(n-1)/2}) + ca(c^{n-3} - 2c^{(n-3)/2}a^{(n-3)/2} + a^{n-3} + 2c^{(n-3)/2}a^{(n-3)/2}) +$

$+ \dots + c^{(n-1)/2}a^{(n-1)/2} = (c - a)^2P + nc^{(n-1)/2}a^{(n-1)/2}$ следует, что:

$c - a$ делится на n^2, therefore R делится на n и не делится на n^2;

$R > n$, следовательно, число R имеет простой сомножитель r не равный n;

$c - a$ не делится на r;

СЛЕДОВАТЕЛЬНО, в 2.1° u ¹ 0.

§2. ***Лемма.*** Все n цифр $(ab_1d_i)_1$, где $d_i = 0, 1, \dots n - 1$, различны.

Действительно, допустив, что $(ab_1d_1*)_1 = (a_1d_1**)_1$, мы находим: $((d_1* - d_1**)a_1)_1 = 0.$

Откуда $d_1* = d_1**$. Следовательно, множества цифр a_1 (здесь месте с $a_1 = 0$) и d_1 совпадают.

[*Пример для* $a_1 = 2$: 0: 2x0 = **0**; 1: 2x3 = 1**1**; 2: 2x1 = **2**; 3: 2x4 = 1**3**; 4: 2x2 = **4**.

При составном n ***Лемма*** несправедлива: в базе *10* и $(2x2)_1$ = **4**, и $(2x7)_1$ = **4**.]

§2a. ***Следствие.*** Существует такое d_i, что $(bd_i)_1 = 1$.

[*Пример для* $a_1 = 1, 2, 3, 4$: 1x1 = **1**; 2x3 = 1**1**; 3x2 = 1**1**; 4x4 = 3**1**.

При составном n ***Следствие 1а*** не работает.]

ВИКТОР СОРОКИН
e-mail: victor.sorokine@wanadoo.fr

Ноябрь 2004, Франция