Виктор Сорокин

Доказательство Великой теоремы Ферма для базового случая

Памяти МАМЫ

Суть противоречия. В гипотетическом равенстве Ферма после уменьшения до нуля вторых цифр в простых сомножителях чисел A, B, C новые УМЕНЬШЕННЫЕ числа A°, B°, C° оказываются бесконечно большими.

Все целые числа рассматриваются в системе счисления с простым основанием n>2.
Обозначения: A', A'', $A_{(k)}$ – первая, вторая, k-я цифра от конца в числе A;
$A_{[k]}$ – k-значное окончание числа A (т.е. $A_{[k]}=A \bmod n^k$);
$nn=n*n=n\wedge 2=n^2$; «=>» – из этого следует…; «<=» – это следует из… .

Рассмотрим равенство Ферма в базовом случае (с известными свойствами 1°-5°) для взаимно простых натуральных A, B, C, простого n, n>2:

1°) $A^n=C^n-B^n$ [$=(C-B)P$] //и $B^n=C^n-A^n$ [$=(C-A)Q$], $C^n=A^n+B^n$ [$=(A+B)R$]//. Откуда

1a°) $(C-B)P+(C-A)Q-(A+B)R=0$, где наибольшие общие делители соответственно в парах чисел (A, $C-B$), (B, $C-A$), (C, $A+B$) мы обозначим буквами a, b, c. Тогда,

2°) если $(ABC)'\neq 0$, то $C-B=a^n$, $P=p^n$, $A=ap$; $C-A=b^n$, $Q=q^n$, $B=bq$; $A+B=c^n$, $R=r^n$, $C=cr$;
3°) число $U=A+B-C=un^k$, где $k>1$, откуда $(A+B)-(C-B)-(C-A)=2U$;
3a°) но если, например, $B_{[k]}=0$ и $B_{[k+1]}\neq 0$, то $(C-A)_{[kn-1]}=0$, где $kn-1>k+1$, и в равенстве
3b°) $[(A+B)-(C-B)-(C-A)]_{[k+1]}=(2U)_{[k+1]}$ (см. 3°) число $(C-A)_{[k+1]}=0$.

4°) Цифра $A^n_{(t+1)}$ однозначно определяется окончанием $A_{[t]}$ (простое следствие из бинома Ньютона). То есть окончания $a^n_{[2]}$, $a^{n\wedge 2}_{[3]}$ и т.д. не зависят от цифры a''!
(Решающая лемма: возможно, ее следует считать Средней теоремой Ферма.)
4a°) Простое следствие: если $A_{[t+1]}=d^{n\wedge t}_{[t+1]}$, где $d_{[2]}=e^n_{[2]}$, то $A_{[t+2]}=e^{n\wedge t}_{[t+2]}$.

На старте (то есть в I-м цикле), при $k=2$ (см. 3°) и $t=k-1=1$:
5a-I°) $A_{[2]}=a^n_{[2]}=a''^n_{[2]}$ ($=a''^{n\wedge t}_{[2]}$, т.е. $t=1=k-1$), $B_{[2]}=b^n_{[2]}=b''^n_{[2]}$, $C_{[2]}=c^n_{[2]}=c''^n_{[2]}$; и
$P_{[2]}=a''^{(n-1)n}_{[2]}=1$ (с $p'=a^{n-1}_{[1]}=1$); $Q_{[2]}=b''^{(n-1)n}_{[2]}=1$ (с $q'=b^{n-1}_{[1]}=1$);
$R_{[2]}=c''^{(n-1)n}_{[2]}=1$ (с $r'=c^{n-1}_{[1]}=1$); => (см. 4a°) =>
5b-I°) $A^n_{[3]}=a''^{nn}_{[3]}$ ($=a''^{n\wedge t}_{[3]}$, т.е. $t=2$), $B^n_{[3]}=b''^{nn}_{[3]}$; $C^n_{[3]}=c''^{nn}_{[3]}$; => (см. 1°-2°) =>

5c-I°) $a^{nn}_{[3]}=(c^{nn}_{[3]}-b^{nn}_{[3]})_{[3]}$, откуда (см. формулы разложения и 2°)
5d-I°) $a^{nn}_{[3]}=\{(c^n_{[3]}-b^n_{[3]})_{[3]}P_{[3]}\}_{[3]}$ и $(c^{nn}_{[3]}-b^{nn}_{[3]})_{[3]}=\{(c^n_{[3]}-b^n_{[3]})p^n_{[3]}\}_{[3]}$, где
5e-I°) $P_{[2]}=a^{(n-1)n}_{[2]}=01=1$.

6°) **Лемма** /*факультативно*/. Каждый простой делитель сомножителя *R* бинома $A^{n\wedge t}+B^{n\wedge t}=(A^{n\wedge\{t-1\}}+B^{n\wedge\{t-1\}})R$, где $t>1$, числа *A* и *B* взаимно простые и число *A+B* не кратно простому $n>2$, имеет вид: $m=dn^t+1$. (См.Приложение.)

А теперь само ***Доказательство ВТФ***. Оно состоит из бесконечной последовательности циклов, в которых показатель степени k (в 3°), начиная со значения 2, возрастает на 1.

Первый способ. Так как в равенстве $a^{nn}_{[3]}=\{(c^n_{[3]}-b^n_{[3]})_{[3]}P_{[3]}\}_{[3]}$ (5d-I°) окончания $(c^n_{[3]}-b^n_{[3]})_{[3]}$ и $P_{[3]}$ есть окончания взаимно простых сомножителей *C-B* и *P*, то эти окончания также (как и левая часть – $a^{nn}_{[3]}$) являются окончаниями степени *nn*, при этом (поскольку каждый простой сомножитель чисел *P, Q, R* оканчивается на цифру *1* – см. 6°) каждый из nn сомножителей *x* числа $P_{[3]}/=x^{nn}_{[3]}/$ [и $Q_{[3]}/=y^{nn}_{[3]}/$ и $R_{[3]}/=z^{nn}_{[3]}/$] также оканчивается на цифру 1. Следовательно, $P_{[3]}=Q_{[3]}=R_{[3]}=1$ и $p_{[2]}=q_{[2]}=r_{[2]}=1$.

Второй способ. В каждом из оснований *p, q, r*, оканчивающихся на цифру *1*, мы УМЕНЬШАЕМ вторые цифры до нуля, в результате чего числа *A, B, C* в решении уравнения 1° УМЕНЬШАТСЯ, но мы, тем не менее, продолжим расчеты при условии: $P_{[3]}=Q_{[3]}=R_{[3]}=1$ и $p_{[2]}=q_{[2]}=r_{[2]}=1$.

Третий способ. В равенстве 5d-I°: $a^{nn}_{[3]}=\{(c^n_{[3]}-b^n_{[3]})_{[3]}P_{[3]}\}_{[3]}$ каждый простой сомножитель числа *P* оканчивается на *01* (см. 6°) и входит в число *P* в степени *n* (см. 2°). Следовательно, число *P* оканчивается на *001*, т.е. $P_{[3]}/=Q_{[3]}=R_{[3]}/=1$, откуда и $p_{[2]}=q_{[2]}=r_{[2]}=1$.

А далее из равенства 3b° мы имеем: $[(C-B)+(C-A)-(A+B)]_{[3]}=0$. Откуда (см. 3°):
7-II°) число $U=A+B-C=un^3$ $[=un^k]$, то есть ТЕПЕРЬ $k=3$.
[А если в 1°, например, $B_{[2]}=0$, тогда расчеты еще проще: $(C-A)_{[kn-1]}=(C-A)_{[2n-1]}=0$, откуда $(C-A)_{[5]}=0$, и из $U_{[3]}=0$ (см. 3°) находим, что $2B_{[3]}=0$, то есть $k=3$.]

И теперь из $A_{[2]}=(ap)_{[2]}$ (см. 2°, где ТЕПЕРЬ $p_{[2]}=1$!) и из равенств 5a-I° ($A_{[2]}=a'^n_{[2]}$), мы находим важный инструмент для самовозрастания окончаний чисел A, B, C:
5-II°) $a_{[2]}=a'^n_{[2]}$ /и $b_{[2]}=b'^n_{[2]}$ и $c_{[2]}=c'^n_{[2]}$/, после чего составляем исходные данные 5a°-5d° для следующего цикла II (увеличивая в формулах 5a°-5b° показатели *k* /=2/ и t /=1/ в степенях чисел *a, b, c* и длины окончаний на *1*):

5a-II°) $A_{[3]}=a^{nn}_{[3]}=a'^{nn}_{[3]}$, $B_{[3]}=b^{nn}_{[3]}=b'^{nn}_{[3]}$, $C_{[3]}=c^{nn}_{[3]}=c'^{nn}_{[3]}$;
$P_{[3]}=a'^{(n-1)nn}_{[3]}=1$ (с $p_{[2]}=a'^{(n-1)n}_{[2]}=1$); $Q_{[3]}=b'^{(n-1)nn}_{[3]}=1$ (с $q_{[2]}=b'^{(n-1)n}_{[2]}=1$);
$R_{[3]}=c'^{(n-1)nn}_{[3]}=1$ (с $r_{[2]}=c'^{(n-1)n}_{[2]}=1$); =>
5b-II°) $A^n_{[4]}=a'^{nnn}_{[4]}$ $(=a'^{n\wedge t}_{[4]}$, т.е. $t=3$), $B^n_{[4]}=b'^{nnn}_{[4]}$; $C^n_{[4]}=c'^{nnn}_{[4]}$; => (см. 1°-2°) =>
5c-II°) $a^{nnn}_{[4]}=(c^{nnn}_{[4]}-b^{nnn}_{[4]})_{[4]}$, => (см. формулы разложения и 2°) =>
5d-II°) $a^{nnn}_{[4]}=\{(c^{nn}_{[4]}-b^{nn}_{[4]})_{[4]}P_{[4]}\}_{[4]}$ и $(c^{nnn}_{[4]}-b^{nnn}_{[4]})_{[4]}=\{(c^{nn}_{[4]}-b^{nn}_{[4]})p^n_{[4]}\}_{[4]}$.

А далее мы повторяем рассуждения I-го цикла, повторяя увеличение значений *k* и t и длин окончаний на *1*. И так до бесконечности. То есть окончания чисел *A, B, C* принимают вид:

8°) $A_{[t+1]}=a^{n\wedge t}{}_{[t+1]}$, $B_{[t+1]}=b^{n\wedge t}{}_{[t+1]}$, $C_{[t+1]}=c^{n\wedge t}{}_{[t+1]}$, где *t* стремится к бесконечности.
И если во втором способе мы восстановим значения вторых цифр в сомножителях *p, q, r*, то бесконечные значения чисел *A, B, C* лишь увеличатся, что свидетельствует о невозможности равенства 1° и истинности ВТФ.
==========
Мезос. 5-11 мая 2017
++++++++++++++++

ПРИЛОЖЕНИЕ

Теорема. Все равенства Ферма $X^m=Z^m-Y^m$ (из ВТФ), за исключением случая $m=2^k$, сводятся к базовому равенству $A^n=C^n-B^n$ (см. 1°) со свойствами 1°-5° (см. выше).

Доказательство

0a°) Если $m=nd$, то делается подстановка: $X^d=A$, $Y^d=B$, $Z^d=C$. => $A^n=C^n-B^n$ (см. 1°).

0b°) Если $X=Ad$, $Y=Bd$, $Z=Cd$, где *d* – наибольший общий делитель чисел *A, B, C*, то делается подстановка $X/d=A$, $Y/d=B$, $Z/d=C$. => $A^n=C^n-B^n$ (см. 1°). =>

1°) $A^n=C^n-B^n$ [$=(C-B)P$] => //$B^n=C^n-A^n$ [$=(C-A)Q$], $C^n=A^n+B^n$ [$=(A+B)R$]//.

1a°) $(C-B)P+(C-A)Q-(A+B)R=0$ [<= 1° после подстановки выражений в скобках в первое равенство], где наибольшие общие делители соответственно в парах чисел (*A, C-B*), (*B, C-A*), (*C, A+B*) мы обозначим буквами *a, b, c*. =>

2°) Если A'/B', $C'/\neq 0$, то $C-B=a^n$, $P=p^n$, $A=ap$ //аналогично и $C-A=b^n$, $Q=q^n$, $B=bq$; $A+B=c^n$, $R=r^n$, $C=cr$//.
Это следует из того, что числа в парах (*C-B, P*), (*C-A, Q*), (*A+B, R*) являются взаимно простыми. Действительно после группировки членов, например, многочлена *P* в пары слагаемых, равноотстоящих от его концов, и выделяя в каждой паре полный квадрат, мы получаем сумму $(n-1)/2$ пар с сомножителем $(C-B)^2$ и еще одного элемента:
2a°) $P=D(C-B)^2+nC^{(n-1)/2}B^{(n-1)/2}$, где *C-B* и *P* взаимно простые, т.к. числа *C-B, C, B* и *n* являются взаимно простыми.

3°) Число $U=A+B-C=un^k$, где $k>1$, откуда $(A+B)-(C-B)-(C-A)=2U$.
Равенство $A'+B'-C'=0$ следует из малой теоремы, ибо если A'/B', $C'/\neq 0$, то
3-1°) $A^{(n-1)\prime}=B^{(n-1)\prime}=C^{(n-1)\prime}=1$. =>
3-2°) $P'=Q'=R'=1$ (где $P=p^n$, $Q=q^n$, $R=r^n$). =>

3-3°) $p'=q'=r'=1$. => (см. 5°) =>
3-4°) $P_{[2]}=Q_{[2]}=R_{[2]}=01=1$. =>
3-5°) $U=A+B-C=un^2$ [$=un^k$ => т.е. число нулей на конце числа U, $k=2$].

3a°) Но если, например, $B_{[k]}=0$ и $B_{[k+1]}\neq 0$, то $(C-A)_{[kn-1]}=0$, где $kn-1>k+1$, и в равенстве
3b°) $[(A+B)-(C-B)-(C-A)]_{[k+1]}=(2U)_{[k+1]}$ (см. 3°) число $(C-A)_{[k+1]}=0$.
Действительно, из равенства 2a° для Q видно, что если $C-A$ делится на n, то Q на n^2 не делится, т.к. один и только один сомножитель n находится в числе Q. =>
Если B делится на n^s, то $C-A$ делится на n^{sn-1} и не делится на n^{sn}.

4°) Цифра $A^n{}_{(s+1)}$ однозначно определяется окончанием $A_{[s]}$ и, следовательно, окончания $a^n{}_{[2]}$, $a^{n\wedge 2}{}_{[3]}$ и т.д. не зависят от цифры a''!
Это вытекает из записи числа A в виде $A=dn+A'$ и разложения бинома $A^n=(dn+A')^n$.

При наименьшем значении $k=2$ (см. 3°):
5a°) $A_{[2]}=a^n{}_{[2]}=a''{}_{[2]}$, $B_{[2]}=b^n{}_{[2]}=b''{}_{[2]}$, $C_{[2]}=c^n{}_{[2]}=c''{}_{[2]}$; и $P_{[2]}=a'^{(n-1)n}{}_{[2]}=1$ (с $p'=a^{n-1}{}_{[1]}=1$);
$Q_{[2]}=b'^{(n-1)n}{}_{[2]}=1$ (с $q'=b^{n-1}{}_{[1]}=1$); $R_{[2]}=c'^{(n-1)n}{}_{[2]}=1$ (с $r'=c^{n-1}{}_{[1]}=1$).
Это следует из равенств $(A+B-C)_{[2]}=0$ (3°) и 2b°: $(A-a^n)_{[2]}=(B-b^n)_{[2]}=(c^n-C)_{[2]}=0$.

5b°) $A^n{}_{[3]}=a''^{nn}{}_{[3]}$ ($=a''^{n\wedge k}{}_{[3]}$, т.е. $k=2$), $B^n{}_{[3]}=b''^{nn}{}_{[3]}$; $C^n{}_{[3]}=c''^{nn}{}_{[3]}$; <= 4°. => (см. 1°-2°)
5c°) $a^{nn}{}_{[3]}=(c^{nn}{}_{[3]}-b^{nn}{}_{[3]})_{[3]}$, => (см. формулы разложения и 2°) =>
5d°) $a^{nn}{}_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})_{[3]}P_{[3]}\}_{[3]}$ и $(c^{nn}{}_{[3]}-b^{nn}{}_{[3]})_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})p^n{}_{[3]}\}_{[3]}$, где $P_{[2]}=a^{(n-1)n}{}_{[2]}=1$;

***
6°) **Лемма** /*факультативно*/. Каждый простой делитель сомножителя R бинома $A^{n\wedge k}+B^{n\wedge k}=(A^{n\wedge\{k-1\}}+B^{n\wedge\{k-1\}})R$, где $k>1$, числа A и B взаимно простые и число $A+B$ не кратно простому $n>2$, имеет вид: $m=dn^k+1$.

Доказательство

Допустим, что среди простых делителей сомножителя R есть делитель вида: $m=dn^{k-1}+1$, где d не кратно n. Тогда числа

6-1°) $A^{n\wedge k}+B^{n\wedge k}$ и, согласно малой теореме Ферма для простой степени m,
6-2°) $A^{dn\wedge(k-1)}-B^{dn\wedge(k-1)}$ (где d четно) делятся на m.

Теорема о НОД двух степенных биномов $A^{dn}+B^{dn}$ и $A^{dq}+B^{dq}$, где натуральные A и B взаимно простые, n [>2] и q [>2] взаимно простые и $d>0$, утверждает, что наибольший общий делитель этих биномов равен A^d+B^d .
В нашем случае НОД, кратный m, есть число $A^{n\wedge(k-1)}-B^{n\wedge(k-1)}$, которое является взаимно простым с числом R. Следовательно, никакой сомножитель m вида $m=dn\wedge\{k-1\}+1$ не принадлежит числу R. Из чего следует истинность Леммы.
Тем самым теорема о базовом равенстве Ферма доказана.