Victor Sorokine

The proof of Fermat's last theorem for the base case

The essence of the contradiction. In hypothetical Fermat's equality, after decreasing the second digits in prime factors of the numbers *A*, *B*, *C* to zero, the new reduced numbers *A*°, *B*°, *C*° are infinitely large.

All calculations are done with numbers in base n, a prime number greater than *2*.

The notations that are used in the proofs:

A', A'', $A_{(k)}$ – the first, the second, the *k*-th digit from the end of the number *A*;

$A_{[k]}$ is the k-digit ending of the number *A* (i.e. $A_{[k]} =A \bmod n^k$);

$nn=n*n=n^2$; "=>" – it follows that... "<=" is should be from...

Consider the Fermat's equality in the base case (with known properties 1°-5°) for co-primes positive *A*, *B*, *C*, prime n, n>2:

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

From here we find that

1a°) $(C-B)P+(C-A)Q-(A+B)R=0$, where we denote with the letters *a*, *b*, *c* the greatest common divisors, respectively, of the pairs of numbers (*A*, *C-B*), (*B*, *C-A*), (*C*, *A+B*).

Then,

2°) if $(ABC)'\neq 0$, then $C-B=a^n$, $P=p^n$, $A=ap$; $C-A=b^n$, $Q=q^n$, $B=bq$; $A+B=c^n$, $R=r^n$, $C=cr$;

3°) the number $U=A+B-C=un^k$, where $k>1$, from here $(A+B)-(C-B)-(C-A)=2U$;

3a°) but if, for example, $B_{[k]}=0$ and $B_{[k+1]}\neq 0$, then $(C-A)_{[kn-1]}=0$, where $kn-1>k+1$, and in the the equality

3b°) $[(A+B)-(C-B)-(C-A)]_{[k+1]}=(2U)_{[k+1]}$ (see 3°) the number $(C-A)_{[k+1]}=0$.

4°) The digit $A^n{}_{(t+1)}$ is uniquely determined by the ending of $A_{[t]}$ (a simple consequence of the binomial theorem). That is, the endings $a^n{}_{[2]}$, $a^{n^2}{}_{[3]}$, $a^{n^3}{}_{[4]}$ etc. do not depend on the digit a''! (The decisive lemma: perhaps it should be considered as the Fermat's Middle Theorem.)

4a°) A simple consequence: if $A_{[t+1]}=d^{n\wedge t}_{[t+1]}$, where $d_{[2]}= e^{n}_{[2]}$, then $A_{[t+2]}=e^{n\wedge t}_{[t+2]}$.

At the start (that is, in the I-th cycle), with $k=2$ (see 3°) and $t=k-1=1$:

5a-I°) $A_{[2]}=a^{n}_{[2]}=a'^{n}_{[2]}$ ($=a'^{n\wedge t}_{[2]}$, ie $\underline{t=1=k-1}$), $B_{[2]}=b^{n}_{[2]}=b'^{n}_{[2]}$, $C_{[2]}=c^{n}_{[2]}=c'^{n}_{[2]}$; and
$P_{[2]}=a'^{(n-1)n}_{[2]}=1$ (with $p'=a^{n-1}_{[1]}=1$); $Q_{[2]}=b'^{(n-1)n}_{[2]}=1$ (with $q'=b^{n-1}_{[1]}=1$);
$R_{[2]}=c'^{(n-1)n}_{[2]}=1$ (with $r'=c^{n-1}_{[1]}=1$); => (see 4a°) =>

5b-I°) $A^{n}_{[3]}=a'^{nn}_{[3]}$ ($=a'^{n\wedge t}_{[3]}$, ie $t=2$), $B^{n}_{[3]}=b'^{nn}_{[3]}$; $C^{n}_{[3]}=c'^{nn}_{[3]}$; => (see 1°-2°) =>

5c-I°) $a^{nn}_{[3]}=(c^{nn}_{[3]}-b^{nn}_{[3]})_{[3]}$, from here (see the expansion formulas and 2°)

5d-I°) $a^{nn}_{[3]}=\{(c^{n}_{[3]}-b^{n}_{[3]})_{[3]}*P_{[3]}\}_{[3]}$ and $(c^{nn}_{[3]}-b^{nn}_{[3]})_{[3]}=\{(c^{n}_{[3]}-b^{n}_{[3]})*p^{n}_{[3]}\}_{[3]}$, where

5e-I°) $P_{[2]}=a^{(n-1)n}_{[2]}=1$.

6°) **Lemma** /*optional*/. Every prime divisor of the factor R binomial $A^{n\wedge t}+B^{n\wedge t}=(A^{n\wedge\{t-1\}}+B^{n\wedge\{t-1\}})R$, where $t>1$, A and B are co-prime and the number $A+B$ is not a multiple of a prime $n>2$, has the form: $m=dn^{t}+1$. (See_ANNEX.)

And now **<u>the proof of FLT itself</u>**. It consists of an endless sequence of cycles in which the exponent k (in 3°), starting with the value 2, increases in 1.

<u>The first method</u>. Since in the equality $a^{nn}_{[3]}=\{(c^{n}_{[3]}-b^{n}_{[3]})_{[3]}*P_{[3]}\}_{[3]}$ (5d-I°) the endings $(c^{n}_{[3]}-b^{n}_{[3]})_{[3]}$ and $P_{[3]}$ are the endings of the co-prime factors $C-B$ and P, then these endings are also (as $a^{nn}_{[3]}$) are the endings of degree nn, at the same time (since each prime factor of the numbers P, Q, R ends in the digit 1, see 6°) each of nn factors of a number $P_{[3]}$ /$=x^{nn}$/
[and $Q_{[3]}$ /$=y^{nn}$/, and $R_{[3]}$ /$=z^{nn}$/] ends with the digit 1.

Therefore, $P_{[3]}=Q_{[3]}=R_{[3]}=1$ and $p_{[2]}=q_{[2]}=r_{[2]}=1$.

<u>The second method</u>. In each of the bases p, q, r, ending with the digit 1, we DECREASE the second digit to zero, with the result that the numbers A, B, C in the solution of the equation 1° DECREASE, but we will continue the calculations provided that:

$P_{[3]}=Q_{[3]}=R_{[3]}=1$ and $p_{[2]}=q_{[2]}=r_{[2]}=1$.

<u>The third method</u>. In the equation 5d-I°: $a^{nn}_{[3]}=\{(c^{n}_{[3]}-b^{n}_{[3]})_{[3]}*P_{[3]}\}_{[3]}$ each prime factor of the number P ends with 01 (see 6°) and enters in the number P to the power n (see 2°). Consequently, the number P ends with 001, i.e.

$P_{[3]}$ /$=Q_{[3]}=R_{[3]}$/ =1 and $p_{[2]}=q_{[2]}=r_{[2]}=1$.

And further, from the equality 3b° we have: $[(C-B)+(C-A)-(A+B)]_{[3]}=0$.

From here (see 3°) :

7-II) the number $U=A+B-C=un^3$, so NOW $k=3$,
[And if in 1°, for example, $B_{[2]}=0$, then the calculation is even simpler:

$(C-A)_{[kn-1]}=(C-A)_{[2n-1]}=0$, from here $(C-A)_{[5]}=0$, and from $U_{[3]}=0$ (see 3°) we find that $2B_{[3]}=0$, that is $k=3$.]

And now, finding from $A_{[2]}=(ap)_{[2]}$ (see 2°, where NOW $p_{[2]}=1$!) and from equations 5a-I° ($A_{[2]}=a'^{n}_{[2]}$), we find the important tool for self-expansion of endings of numbers A, B, C.

5-II°) $a_{[2]}=a'^{n}_{[2]}$ /and $b_{[2]}=b'^{n}_{[2]}$ and $c_{[2]}=c'^{n}_{[2]}$/, after that we compose the source data 5a°-5d° for the next cycle II (increasing in formulas 5a°-5b° indexes of power k /$=2$/ and t /$=1$/ in powers of integers a, b, c, and the length of the endings 1):

5a-II°) $A_{[3]}=a^{nn}_{[3]}=a'^{nn}_{[3]}$, $B_{[3]}=b^{nn}_{[3]}=b'^{nn}_{[3]}$, $C_{[3]}=c^{nn}_{[3]}=c'^{nn}_{[3]}$;
$P_{[3]}=a'^{(n-1)nn}_{[3]}=1$ (with $p_{[2]}=a'^{(n-1)n}_{[2]}=1$); $Q_{[3]}=b'^{(n-1)nn}_{[3]}=1$ (with $q_{[2]}=b'^{(n-1)n}_{[2]}=1$);
$R_{[3]}=c'^{(n-1)nn}_{[3]}=1$ (with $r_{[2]}=c'^{(n-1)n}_{[2]}=1$); =>

5b-II°) $A^{n}_{[4]}=a'^{nnn}_{[4]}$ ($=a'^{n\wedge t}_{[4]}$, ie $t=3$), $B^{n}_{[4]}=b'^{nnn}_{[4]}$; $C^{n}_{[4]}=c'^{nnn}_{[4]}$; => (see 1°-2°) =>

5c-II°) $a^{nnn}_{[4]}=(c^{nnn}_{[4]}-b^{nnn}_{[4]})_{[4]}$, => (see the expansion formulas and 2°) =>

5d-II°) $a^{nnn}_{[4]}=\{(c^{nn}_{[4]}-b^{nn}_{[4]})_{[4]}*P_{[4]}\}_{[4]}$ and $(c^{nnn}_{[4]}-b^{nnn}_{[4]})_{[4]}=\{(c^{nn}_{[4]}-b^{nn}_{[4]})*p^{n}_{[4]}\}_{[4]}$.

And then we repeat the arguments of the I-th cycle, repeating the increase values of k and t and the length of the endings (lower indices) by 1. And so on to infinity. That is the end of the numbers A, B, C take the following form:

8°) $A_{[t+1]}=a'^{n\wedge t}_{[t+1]}$, $B_{[t+1]}=b'^{n\wedge t}_{[t+1]}$, $C_{[t+1]}=c'^{n\wedge t}_{[t+1]}$, where t tends to infinity.

And if (in the second method) we restore the values of the second digits in the factors a, b, c, p, q, r, then the infinite values of the numbers A, B, C only increase. That indicates the impossibility of the equality of 1° and of the truth of the FLT.

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

Mezos. May 5-11, 2017

+++++++++++++++++

ANNEX

Theorem. All the Fermat's equality $X^m=Z^m-Y^m$ (from FLT), with the exception of the case $m=2^k$, are reduced to basic equality $A^n=C^n-B^n$ (see 1°) with the properties 1°-5° (see above):

Proof

0a°) If $m=nd$, it is substitution: $X^d=A$, $Y^d=B$, $Z^d=C$. => (see 1°).

0b°) If $X=Ad$, $Y=Bd$, $Z=Cd$, где d – the greatest common divisor of numbers A, B, C, it is substitution $X/d=A$, $Y/d=B$, $Z/d=C$. => $A^n=C^n-B^n$ (see 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° after substitution of the expressions in parentheses in the first equality],where the greatest common divisor respectively in pairs of numbers (A, $C-B$), (B, $C-A$), (C, $A+B$) we denote by letters a, b, c. =>

2°) If $(ABC)'\neq0$, then $C-B=a^n$, $P=p^n$, $A=ap$; //similarly $C-A=b^n$, $Q=q^n$, $B=bq$; $A+B=c^n$, $R=r^n$, $C=cr\cdot$

2a°) This follows from the fact that the numbers in the pairs ($C-B$, P), ($C-A$, Q), ($A+B$, R) are co-prime . Indeed, for example, after grouping the members of the polynomial P in terms of a pair, equally spaced from the ends, and allocating in each pair complete the square, we obtain the sum of $(n-1)/2$ pairs with cofactor $(C-B)^2$ and another item:

2a-1°) $P=D(C-B)^2+nC^{(n-1)/2}B^{(n-1)/2}$, where $C- B$ and P are co-prime , because the numbers $C-B$, C, B and n are co-prime .

3°) The number$U=A+B-C=un^k$, where $k>1$, from here $(A+B)-(C-B)-(C-A)=2U$.
Equality $A'+B'-C'=0$ follows from Little theorem, as, if A' $/B'$, $C'/\neq0$, then

3-1°) $A^{(n-1)}{}'=B^{(n-1)}{}'=C^{(n-1)}{}'=1$. =>

3-2°) $P'=Q'=R'=1$ (where $P=p^n$, $Q=q^n$, $R=r^n$). =>

3-3°) $p'=q'=r'=1$. => (see 4°) =>

3-4°) $P_{[2]}=Q_{[2]}=R_{[2]}=01=1$. =>

3-5°) $U=A+B-C=un^2$ => $k=2$.

3a°) But if, for example, $B_{[k]}=0$ and $B_{[k+1]}\neq0$, then $(C-A)_{[kn-1]}=0$, where $kn-1>k+1$, and in the equation

3b°) $[(A+B)-(C-B)-(C-A)]_{[k+1]}=(2U)_{[k+1]}$ (see 3°) the number $(C-A)_{[k+1]}=0$.
Indeed, from the equality 2a° for Q it shows that if C-A is divisible by n, then Q in n^2 is not divisible, since one and only one factor n is the number of Q. =>
If B is divided by n^k, then C-A is divisible into n^{kn-1} and is not divisible into n^{kn-1}.

4°) The digit $A^n_{(s+1)}$ is uniquely determined by the ending of $A_{[s]}$. That is, the endings $a^n_{[2]}$, $a^{n\wedge 2}_{[3]}$,… $a^{n\wedge t}_{[t+1]}$ etc. do not depend on the digit a''!
The fact follows from the representation of a number A in the form $A=dn+A'$ and from the expansion of the binomial

4a°) $A^n=(dn+A')^n$.

Under least $k=2$ (see 3°):

5a°) $A_{[2]}=a^n_{[2]}=a'^n_{[2]}$, $B_{[2]}=b^n_{[2]}=b'^n_{[2]}$, $C_{[2]}=c^n_{[2]}=c'^n_{[2]}$; and
$P_{[2]}=a'^{(n-1)n}_{[2]}=1$ (with $p'=a^{n-1}_{[1]}=1$); $Q_{[2]}=b'^{(n-1)n}_{[2]}=1$ (with $q'=b^{n-1}_{[1]}=1$);
$R_{[2]}=c'^{(n-1)n}_{[2]}=1$ (with $r'=c^{n-1}_{[1]}=1$).

This follows from the equalities $(A+B-C)_{[2]}=0$ (3°) and 2b°: $(A+a^n)_{[2]}=(B+b^n)_{[2]}=(c^n+C)_{[2]}=0$.

5b°) $A^n_{[3]}=a'^{nn}_{[3]}$ ($=a'^{n\wedge t}_{[3]}$, ie $t=2$), $B^n_{[3]}=b'^{nn}_{[3]}$; $C^n_{[3]}=c'^{nn}_{[3]}$; <= 4°. => (see 1°-2°)

5c°) $a^{nn}_{[3]}=(c^{nn}_{[3]}-b^{nn}_{[3]})_{[3]}$, => (see formulas decomposition and 2°) =>

5d°) $a^{nn}_{[3]}=\{(c^n_{[3]}-b^n_{[3]})_{[3]}P_{[3]}\}_{[3]}$ and $(c^{nn}_{[3]}-b^{nn}_{[3]})_{[3]}=\{(c^n_{[3]}-b^n_{[3]})p^n_{[3]}\}_{[3]}$, where $P_{[2]}=a^{(n-1)n}_{[2]}=1$.

6°) **Lemma** /*optional*/. Every prime divisor of the factor R binomial $A^{n\wedge t}+B^{n\wedge t}=(A^{n\wedge\{t-1\}}+B^{n\wedge\{t-1\}})R$, where $t>1$, A and B are co-prime and the number $A+B$ is not a multiple of a prime $n>2$, has the form: $m=dn^t+1$.

<u>Proof</u>

Suppose that among the prime divisors of the number R there is a divisor of the form: $m=dn^{k-1}+1$, where d is not a multiple of n. Then the number

6-1°) $A^{n\wedge t}+B^{n\wedge t}$ and, according to the Little Fermat's theorem for prime degree m,

6-2°) $A^{dn\wedge(t-1)}-B^{dn\wedge(t-1)}$ (where d is an even) are divided into m.

Theorem about GCD of two power binomials $A^{dn}+B^{dn}$ and $A^{dq}+B^{dq}$, where the natural A and B are co-prime , n [>2] and q [>2] are co-prime and $d>0$, says that the greatest common divisor of these binomials is equal to A^d+B^d .

In our case, the GCD multiple m, is the number $A^{n^\wedge(t-1)}$-$B^{n^\wedge(t-1)}$, which is co-prime with the number R. Hence, any factor m of the form $m=dn^{n^\wedge(t-1)}+1$ does not belong to the number R. From which follows the truth of the lemma.

This proves the theorem on the basic Fermat's equality.