A detailed explanation of each statement

/machine translation/

Fermat's Last Theorem (main case: n is prime):

For integers A, B, C and prime n>2 the equal $A^n+B^n=C^n$ does not exist.

From this it follows that equation $a^{dn}+b^{dn}=c^{dn}$, or $(a^d)^n+(b^d)^n=(c^d)^n$, also does not exist.

The essence of the contradiction: If A, B, C are integers and $A^n+B^n=C^n$, then A+B-C=0 and $A^n+B^n<C^n$.

If A+B=C then $A^n+B^n<(A+B)^n$.

Notations are done in a number system with a prime base n:

Prime base we have because in this case, there are important properties of the integers evidence: Fermat's Little Theorem, and others.

$A_{(t)}$ – t-th digit from the end in the number A; for convenience: $A_{(1)}=A'$, $A_{(2)}=A''$, $A_{(3)}=A'''$;

Use a dash to indicate the numbers greatly simplifies the writing of formulas, especially that only the last three digits are primarily used in the proof.

$A_{[t]}$ – t-digits ending of the number A; $A_{/t/}$, where A=pq…r, – the product of $p_{[t]}*q_{[t]}*...*r_{[t]}$.

The factors p, q, ... r can be as simple and composite numbers.

For example, in the decimal system for p=321, q=1433:

$p_{(1)}=p'=1$, $p_{(2)}=p''=2$, $p_{(2)}=p'''=3$, и т.д.; $q_{(1)}=q'=3$, $q_{(2)}=q''=3$, $q_{(3)}= q'''=4$, etc.

$p_{[2]}=21$; $q_{[2]}=33$; $(pq)_{\{2\}}=p_{[2]}*q_{[2]}=21*33$, wherein $(pq)_{[2]}=93$.

From binomial theorem (for prime n) its follow two simple lemmas:

0a°) if $A_{[t+1]}=xn^t+1$, where t>0 and A is the base of a degree A^n, then the digit $(A^n)_{(t+2)}=x$;

Proof. We write the last three terms of the expansion of the binomial:

$(xn^t+1)^n=...+0{,}5*n*(n-1)*(xn^t)^2+n*xn^t+1=...+0{,}5(n-1)x^2*n^{2t+1}+xn^{t+1}+1$, where the second (from the end) member has t+1 zeros, and all subsequent (from the end) the members have at least t+2 zeros. Consequently, the digit with number t+2 is equal to x, i.e. $(A^n)_{(t+2)}=x$.

0b°) if $a_{[t+1]}=xn^t+1$, where digit $a_{(t+1)}=x>0$ and t>0, then the digit $[(a_{[t+1]})^{n-1}]_{(t+1)}$ = «-x» = n-x.

In this case $(xn^t+1)^{n-1}=...+(n-1)*xn^t+1=...+(-x)n^t+1=Sn^{t+1}+(-x)n^t+1$, where the second (from the end) member has t zeros, and the sum S has not less than t+1 zeros. At the same time the absolute value $Sn^{t+1}>|(-x)n^t+1|$. Therefore, to get a positive value of $(-x)n^t+1$ [and $(-x)n^t$], the number S must be reduced by n^{t+1} and by this number increase the amount of the last two terms $(-x)n^t+1$ with the results obtained $(n-x)n^t+1$, where the digit n-x is simple and positive number.

So, let us assume that for a prime number n>2, relatively prime A, B, C, and A'[or B']≠0

1°) $A^n=(C-B)P$ [$=aP=C^n-B^n$, where $P=p^n$ and /for convenience/ a=C-B] where, as known,

C^n-B^n=(C-B)P, where P=C^{n-1}+BC^{n-2}+...+$B^{n-2}C$+C^{n-1}, – formula of elementary algebra course. If the digit A'=0, instead of A we consider the number B.

1a°) P'=p'=1 (a consequence of Fermat's little theorem),
Indeed, since A'≠0, then, according to Fermat's little theorem, A^{n-1}'=1. If B'=0, then B^{n-1}'=0. As a result from (A'A^{n-1}')=(C'C^{n-1}'-B'B^{n-1}') follows A'=(C'-B')', from here P'=1. Equality p'=1 follows from the equality P=p^n. The equality P=p^n follows from the fact that:
1) the numbers (C-B) and P are relatively prime (if A'≠0 and the numbers A, B, C are mutually prime), and their product is the n-th degree. Therefore, the numbers (C-B) and P are the n-th powers. The numbers (C-B) and P are relatively prime, because the number P can be represented as: P=D$(C-B)^2$+n$(CB)^{n-1}$.

1b°) [U=] A+B-C=un^k, where k [>0] – the number of zeroes after the digit u' (i.e. $\mathbf{U}_{[k+1]}$≠0).
Equality U'=0 follows from the equation A'=C'-B'. Since U>0, then it has a significant digits, the first of which from the end has the number k+1.

1c°) g – any integer solution [which exists!] of the equation $(Ag)_{[k+2]}$=1.
This follows from the lemma for the number system with the prime base n: in the multiplication table $Ag_{(i)}$ (i=1, 2... n-1), where A'≠0 and $g_{(i)}$ – digits in a number system with the prime base n, all the latest digits $[Ag_{(i)}]'$ (i=0, 1, 2, … n-1) are different (the lemma is easily proved by contradiction). Consequently, for any digit A' not equal to zero, there is a one-digit number $G_{[1]}$=g, that (A'g)'=1.
Further, if the number x>0, then we take the number A with ending $A_{[2]}$=xn+1.
It is easy to find such number $G_{[2]}$=yn+1, that $[(xn+1)(yn+1)]_{[2]}$=1, from here (x+y)n+1=1, from here y=n-x. Etc. Thus, by multiplying of the number A by corresponding numbers $G_{[i]}$, or as a result by the number g=$G_{[1]}$*$G_{[2]}$*... $G_{[t]}$, we can get the number Ag with the end $(Ag)_{[t]}$=1, where t is arbitrarily large.
An example of the last digits in multiplication table for n=7 and g=2:
0 x 2 = ...0, 1 x 2 = ...2, 2 x 2 = ...4, 3 x 2 = ...6, 4 x 2 = ...1, 5 x 2 = ...3, 6 x 2 = ...5, with a set of the latest digits 0, 2, 4, 6, 1, 3, 5, where no figure is not repeated!

An elementary proof of the Fermat's Last Theorem

Let's multiply the equation 1° by the number g^n from 1c° received the new equality **1°**:
1°) A^n=(**C-B**)**P**, where **P**=Pg^{n-1}, **A**=Ag, **A**^{n}=$A^n g^n$ and $\mathbf{A}_{[k+2]}$=$\mathbf{A}^n{}_{[k+2]}$=1; k and n are const.
Let us show that the ending $(\mathbf{C-B})_{[k+2]}$, or $\mathbf{a}_{[k+2]}$, is also equal to 1.
To do this, the number **P** will be represented in the following form: **P**=$\mathbf{q}^{n-1}$+**Q**n^{k+2}
[this is the **KEY** to the demonstration], where q and Q are integers.
Now, leaving in the numbers A, C-B [or a] and P only (k+2)-digit ending, we obtain the equation: $\mathbf{A}^n{}_{[k+2]}$=$(\mathbf{a}_{[k+2]}*\mathbf{q}^{n-1}{}_{[k+2]})_{[k+2]}$. And then, based on the digits **a**'', **a**''' etc. up to (k+2)-th digit of **a**, we will consistently calculate the second, third, etc. digit of numbers **q**'', ($\mathbf{q}^{n-1}$)'', **a**''', then **a**''', **q**''', ($\mathbf{q}^{n-1}$) ''', **a**'''', etc. (All of them are equl to zero. Hence **P**=**1**+**Q**n^{k+2}=1^{n-1}+**Q**n^{k+2}.)

2°) **a**'= **q**'=1, which is deduced from 1°b.

Because (**aP**)'=1, where **P**'=1.

3°) From the identity $\mathbf{A}^n_{(2)}=[(\mathbf{a}''n+1)(\mathbf{q}''n+1)^{n-1}]_{(2)}$=(cf. 0b°)=$[(\mathbf{a}''n+1)(-\mathbf{q}''n+1)]_{(2)}$ [=0] we find**:** **a**''=**q**'' and the degree of endings $\mathbf{A}^n_{\{2\}}=(\mathbf{a}''n+1)_{[2]}{}^n$, from here (cf. 0a°) we find the digit $\mathbf{A}^n_{(3)}$:
This main logic double-thread operation: from the ending $\mathbf{A}^n_{(2)}$ [=1] we find a parity digits **a**'' and **q**'', hence, and the equality of endings $\mathbf{a}_{[2]}$ and $\mathbf{q}_{[2]}$. But the latter form (make) product of the endings in the form of degree $\mathbf{A}^n_{\{2\}}=(\mathbf{a}''n+1)_{[2]}{}^n$.
And it is important that this work is the degree $\mathbf{A}^n$, in which the meaning of the digit $\mathbf{A}^n_{(3)}$ is uniquely determined by the degree of ending $\mathbf{A}^n_{/t/}$!

4°) $\mathbf{A}^n_{(3)}$ (=0 – cf. **1°**) = **a**'' and therefore **a**''=**q**''=0 (otherwise $\mathbf{A}^n_{(3)} \neq 0$).
That is, from $(\mathbf{A}^n)'''=\mathbf{A}''$, where $\mathbf{A}''=\mathbf{a}''$ and $(\mathbf{A}^n)'''=0$, we find3: **a**''=**q**''=0.

And then, we makes calculations 3°-4° with all subsequent digits [until the (k+1)-th] of the numbers **A**, **P** and **a**, with the result equality $\mathbf{A}_{[k+1]}=\mathbf{P}_{[k+1]}=\mathbf{a}_{[k+1]}=(\mathbf{C}-\mathbf{B})_{[k+1]}=1$ and

5°) $[\mathbf{A}-(\mathbf{C}-\mathbf{B})]_{[k+1]}=[\mathbf{A}+\mathbf{B}-\mathbf{C}]_{[k+1]}=\mathbf{U}_{[k+1]}=0$, which contradicts to 1b°. Thus FLT proved.

Victor SOROKINE
(May 3, 2015. Mezos, France. victor.sorokine@gmail.com)