La preuve du dernier théorème de Fermat pour le cas de base (quand les nombres A, B, C ont les propriétés 1°-5°),

auquel se résument tous les cas, sauf pour $n=2^k$ (voir appendice)

A la mémoire de ma mère

<u>La description sommaire de la contradiction</u>. Dans l'équation de Fermat, après la réduction des deuxièmes chiffres dans les facteurs premiers des nombres A, B, C à zéro, les nouveaux nombres A°, B°, C° deviennent infiniment grands.

Tous les nombres entiers sont traités dans un système numérique avec une base *n*, où *n* est un nobmre premier supérieur à *2*.
<u>Désignations:</u> A', A'', $A_{(k)}$ – premier, deuxième, *k*-ième chiffre à partir de la fin du nombre *A*;
$A_{[k]}$ – la terminaison de *k* chiffres du nombre *A* (où $A_{[k]}=A \bmod n^k$);
$nn=n*n=n\^2=n^2$; «=>» – de ça decoule… ; «<=» – ça decoule de.

Considérons l'égalité de Fermat dans le cas de base (avec les propriétés connues 1°-5°), pour les entiers naturels (et premiers entre eux) *A*, *B*, *C*, premier *n*, $n>2$:

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

1a°) $(C-B)P+(C-A)Q-(A+B)R=0$, où le plus grands diviseurs communs respectivement des paires de nombres (*A*, *C-B*), (*B*, *C-A*), (*C*, *A+B*) seront désignés par lettres *a*, *b*, *c*. Alors,

2°) si $(ABC)'\neq 0$, alors $C-B=a^n$, $P=p^n$, $A=ap$; $C-A=b^n$, $Q=q^n$, $B=bq$; $A+B=c^n$, $R=r^n$, $C=cr$;
3°) le nombre $U=A+B-C=un^k$, où $k>1$, d'où $(A+B)-(C-B)-(C-A)=2U$;
3a °) mais si, par exemple, $B_{[k]}=0$ et $B_{[k+1]}\neq 0$, alors $(C-A)_{[kn-1]}=0$, où $kn-1>k+1$,
alors dans l'équation
3b°) $[(A+B)-(C-B)-(C-A)]_{[k+1]}=(2U)_{[k+1]}$ (voir 3°) le nombre $(C-A)_{[k+1]}=0$.

Au début (i.e. dans le premier cycle – voir ci-dessous le début de la preuve), avec $k=2$
4a-I°) $A_{[2]}=a^n{}_{[2]}=a'^n{}_{[2]}$, $B_{[2]}=b^n{}_{[2]}=b'^n{}_{[2]}$, $C_{[2]}=c^n{}_{[2]}=c'^n{}_{[2]}$; et
$P_{[2]}=a'^{(n-1)n}{}_{[2]}=1$ (avec $p'=a^{n-1}{}_{[1]}=1$); $Q_{[2]}=b'^{(n-1)n}{}_{[2]}=1$ (avec $q'=b^{n-1}{}_{[1]}=1$);
$R_{[2]}=c'^{(n-1)n}{}_{[2]}=1$ (avec $r'=c^{n-1}{}_{[1]}=1$); => (voir 5°) =>
4b-I°) $A^n{}_{[3]}=a'^{nn}{}_{[3]}$ ($=a'^{n\^k}{}_{[3]}$, c'est-à-dire $k=2$), $B^n{}_{[3]}=b'^{nn}{}_{[3]}$; $C^n{}_{[3]}=c'^{nn}{}_{[3]}$; => (voir 1° et 2°) =>
4c-I°) $a^{nn}{}_{[3]}=(c^{nn}{}_{[3]}-b^{nn}{}_{[3]})_{[3]}$, d'où (voir les décomposition des formules et 2°)
4d-I°) $a^{nn}{}_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})P_{[3]}\}_{[3]}$ et $(c^{nn}{}_{[3]}-b^{nn}{}_{[3]})_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})p^n{}_{[3]}\}_{[3]}$, ou $P_{[2]}=a^{(n-1)n}{}_{[2]}=1$.

5°) Le chiffre $A^n{}_{(k+1)}$ est défini de manière unique par la terminaison $A_{[k]}$ (une simple conséquence de la formule du binôme de Newton). C'est-à-dire les terminaisons $a^n{}_{[2]}$, $a^{n\^2}{}_{[3]}$ etc. ne dépendent pas du chiffre a'' ! (Lemme-clé: il est possible qu'il doit être considéré comme *le Moyen Théorème de Fermat*.)

6°) **Le Lemme** /*facultatif*/. Chaque diviseur premier de cofacteur R du binôme $A^{n^\wedge k}+B^{n^\wedge k}=(A^{n^\wedge\{k-1\}}+B^{n^\wedge\{k-1\}})R$, où $k>1$, les nombres A et B sont premiers entre eux et le nombre $A+B$ n'est pas un multiple premier de $n>2$, a la forme: $m=dn^k+1$.

Et maintenant **<u>la preuve proprement dite du DTF</u>**. Elle se compose d'une suite infinie de cycles dans lesquels l'exposant k (dans 3°), à partir de la valeur *2*, est augmenté de *1*.

<u>La première méthode.</u> Car dans l'égalité $a^{nn}{}_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})_{[3]}P_{[3]}\}_{[3]}$ (4d-I°) les terminaisons $(c^n{}_{[3]}-b^n{}_{[3]})_{[3]}$ et $P_{[3]}$ sont les terminaisons de facteurs $C-B$ et P premiers entre eux, alors ces terminaisons aussi (comme $a^{nn}{}_{[3]}$) sont terminaisons d'une puissance de *nn*, en cela (car chaque premier cofacteur de nombres P, Q, R se termine par le chiffre *1* - voir 6°) chacun d'nn cofacteurs du nombre $P_{[3]}$ /$=x^{nn}{}_{[3]}$/ [et $Q_{[3]}$ /$=y^{nn}{}_{[3]}$/ et $R_{[3]}$ /$=z^{nn}{}_{[3]}$/] aussi se termine par le chiffre *1*. Par conséquent, $P_{[3]}=Q_{[3]}=R_{[3]}=1$ et $p_{[2]}=q_{[2]}=r_{[2]}=1$.

<u>La deuxième méthode.</u> Dans chacune des bases p, q, r, se terminant par le chiffre *1*, nous RÉDUISONS les deuxièmes chiffres à zéro, à la suite de quoi les nombres A, B, C dans une solution de l'équation 1° DIMINUERONT, mais nous continuerons les calculs à condition que: $P_{[3]}=Q_{[3]}=R_{[3]}=1$ et $p_{[2]}=q_{[2]}=r_{[2]}=1$.

<u>La troisième méthode.</u> Dans l'égalité 4d-I°: $a^{nn}{}_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})_{[3]}P_{[3]}\}_{[3]}$ chaque premier cofacteur du nombre P se termine par *01* (voir 6°) et est inclus dans le nombre P de degré n (voir 2°). Par conséquent, le nombre P se termine par *001*, c'est-à-dire $P[3]$ /$=Q[3]=R[3]$/ $=1$ et $p[2]=q[2]=r[2]=1$.

A la suite de l'égalité 3b° nous avons:
6°) $[(C-B)+(C-A)-(A+B)]_{[3]}=0$. D'où (voir 3°):
7°-II) le nombre $U=A+B-C=un^3$, c'est-à-dire **maintenant** $k=3$.
[<u>Et si</u> dans 1°, par exemple, $B_{[2]}=0$, alors les calculs sont encore plus faciles:
$(C-A)_{[kn-1]}=(C-A)_{[2n-1]}=0$, d'où $(C-A)_{[5]}=0$, et de $U_{[3]}=0$ (voir 3°) on trouve que $2B_{[3]}=0$ et $U_{[3]}=0$, c'est-à-dire $k=3$.]

Et maintenant, trouvant de $A_{[2]}=(ap)_{[2]}$ (v. 2°, où $p_{[2]}=1$) et des équations 4a-I° ($A_{[2]}=a'^n{}_{[2]}$), que
4-II°) $a_{[2]}=a'^n{}_{[2]}$ /*u* $b_{[2]}=b'^n{}_{[2]}$ *u* $c_{[2]}=c'^n{}_{[2]}$/,
on prépare les données initiales 4a°-4d° pour le prochain cycle II (en augmentant dans les formules 4a°-4b° l'indice k /$=2$/ dans les puissances des nombres a, b, c et la longueur des terminaisons de *1*):

4a-II°) $A_{[3]}=a^{nn}{}_{[3]}=a'^{nn}{}_{[3]}$, $B_{[3]}=b^{nn}{}_{[3]}=b'^{nn}{}_{[3]}$, $C_{[3]}=c^{nn}{}_{[3]}=c'^{nn}{}_{[3]}$;
$P_{[3]}=a'^{(n-1)nn}{}_{[3]}=1$ (avec $p_{[2]}=a'^{(n-1)n}{}_{[2]}=1$); $Q_{[3]}=b'^{(n-1)nn}{}_{[3]}=1$ (avec $q_{[2]}=b'^{(n-1)n}{}_{[2]}=1$);
$R_{[3]}=c'^{(n-1)nn}{}_{[3]}=1$ (avec $r_{[2]}=c'^{(n-1)n}{}_{[2]}=1$); =>
4b-II°) $A^n{}_{[4]}=a'^{nnn}{}_{[4]}$ $(=a'^{n^\wedge k}{}_{[4]}$, т.е. k=3), $B^n{}_{[4]}=b'^{nnn}{}_{[4]}$; $C^n{}_{[4]}=c'^{nnn}{}_{[4]}$; => (см. 1°-2°) =>
4c-II°) $a^{nnn}{}_{[4]}=(c^{nnn}{}_{[4]}-b^{nnn}{}_{[4]})_{[4]}$, =>
4d-II°) $a^{nnn}{}_{[4]}=\{(c^{nn}{}_{[4]}-b^{nn}{}_{[4]})_{[4]}P_{[4]}\}_{[4]}$ et $(c^{nnn}{}_{[4]}-b^{nnn}{}_{[4]})_{[4]}=\{(c^{nn}{}_{[4]}-b^{nn}{}_{[4]})p^n{}_{[4]}\}_{[4]}$.

Et puis on répète les arguments du I^er cycle en répétant l'augmentation de la valeur de k et des indices inférieurs de 1. Et ainsi jusqu'à l'infini. En conséquence, les terminaisons des nombres A, B, C prennent la forme suivante :

8°) $A_{[k+1]}=a^{m^\wedge k}{}_{[k+1]}$, $B_{[k+1]}=b^{m^\wedge k}{}_{[k+1]}$, $C_{[k+1]}=c^{m^\wedge k}{}_{[k+1]}$, où k tend vers l'infini.
Et, dans la deuxième méthode, si nous reconstituons les valeurs des deuxièmes chiffres dans les facteurs a, b, c, p, q, r, alors les valeurs infinies des nombres A, B, C ne pourront qu'augmenter, ce qui témoigne de l'impossibilité de l'égalité 1° et de la vérité du DTF.

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

Victor Sorokine. Mézos. Le 5-11 Mai 2017

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

APPENDICE

Le cas de base de l'égalité de Fermat (de DTF)

(Il a au moins trois preuves élémentaires de DTF sur la base Lemme 5 °)

Tous les nombres entiers sont traités dans un système numérique avec une base n, où n est un nobmre premier supérieur à 2.
Désignations: A', A'', $A_{(k)}$ – premier, deuxième, k-ième chiffre à partir de la fin du nombre A;
$A_{[k]}$ – la terminaison de k chiffres du nombre A (où $A_{[k]}=A$ mod n^k);
$nn=n*n=n$^$2=n^2$; "=>" – cela devrait être ...; "<=" – il résulte de ...

Théorème. Tous les égalités de Fermat $X^m=Z^m-Y^m$ (à partir de DTF), sauf pour le cas $m=2^k$, sont réduits à une équation de base $A^n=C^n-B^n$ (*)ayant des propriétés 1°-6°:
Farm Xm = Zm-ym (),m = 2k, An = Cn-Bn (*)1 ° -6 °:

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

1a°) $(C-B)P+(C-A)Q-(A+B)R=0$, où le plus grands diviseurs communs respectivement des paires de nombres (A, $C-B$), (B, $C-A$), (C, $A+B$) seront désignés par lettres a, b, c. Alors,

2°) si $(ABC)'\neq 0$, 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°) le nombre $U=A+B-C=un^k$, où $k>1$, d'où $(A+B)-(C-B)-(C-A)=2U$;
3a °) mais si, par exemple, $B_{[k]}=0$ et $B_{[k+1]}\neq 0$, alors $(C-A)_{[kn-1]}=0$, où $kn-1>k+1$,
alors dans l'équation
3b°) $[(A+B)-(C-B)-(C-A)]_{[k+1]}=(2U)_{[k+1]}$ (voir 3°) le nombre $(C-A)_{[k+1]}=0$.

Si $k=2$ (см. 3°), alors :
4a°) $A_{[2]}=a^n{}_{[2]}=a'^n{}_{[2]}$, $B_{[2]}=b^n{}_{[2]}=b'^n{}_{[2]}$, $C_{[2]}=c^n{}_{[2]}=c'^n{}_{[2]}$; и
$P_{[2]}=a'^{(n-1)n}{}_{[2]}=1$ (avec $p'=a^{n-1}{}_{[1]}=1$); $Q_{[2]}=b'^{(n-1)n}{}_{[2]}=1$ (avec $q'=b^{n-1}{}_{[1]}=1$);
$R_{[2]}=c'^{(n-1)n}{}_{[2]}=1$ (avec $r'=c^{n-1}{}_{[1]}=1$); => (voir 5°) =>
4b°) $A^n{}_{[3]}=a'^{nn}{}_{[3]}$ ($=a'^{n^k}{}_{[3]}$, c'est-à-dire $k=2$), $B^n{}_{[3]}=b'^{nn}{}_{[3]}$; $C^n{}_{[3]}=c'^{nn}{}_{[3]}$; => (voir 1°-2°) =>
4c°) $a^{nn}{}_{[3]}=(c^{nn}{}_{[3]}-b^{nn}{}_{[3]})_{[3]}$, d'où (voir les décomposition des formules et de 2°)
4d°) $a^{nn}{}_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})_{[3]}P_{[3]}\}_{[3]}$ et $(c^{nn}{}_{[3]}-b^{nn}{}_{[3]})_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})p^n{}_{[3]}\}_{[3]}$, ou $P_{[2]}=a^{(n-1)n}{}_{[2]}=1$.

5°) Le chiffre $A^n{}_{(k+1)}$ est défini de manière unique par la terminaison $A_{[k]}$ (une simple conséquence de la formule du binôme de Newton). C'est-à-dire les terminaisons $a^n{}_{[2]}$, $a^{n^2}{}_{[3]}$ etc. ne dépendent pas du chiffre a'' ! (Lemme-clé: il est possible qu'il doit être considéré comme *le Moyen Théorème de Fermat*.)

6°) **Le Lemme**. Chaque diviseur premier de cofacteur R du binôme

$A^{n^k}+B^{n^k}=(A^{n^{k-1}}+B^{n^{k-1}})R$, où $k>1$, les nombres A et B sont premiers entre eux et le nombre $A+B$ n'est pas un multiple premier de $n>2$, a la forme: $m=dn^k+1$.

<u>Preuve</u>

0-1°) Si $m=nd$, la substitution est : $X^d=A$, $Y^d=B$, $Z^d=C$. => (Voir. *).

0-2°) Si $X=Ad$, $Y=Bd$, $Z=Cd$, où d – le plus grand diviseur commun des nombres A, B, C, la substitution : $X/d=A$, $Y/d=B$, $Z/d=C$. => (Voir *).

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

1a°) $(C-B)P+(C-A)Q-(A+B)R=0$ [<= 1° après substitution parties droites de 1° dans (*)], où les plus grands communs diviseurs respectivement par paires de nombres (A, $C-B$), (B, $C-A$), (C, $A+B$) désigné par les lettres a, b, c. =>

2°) Si $(ABC)'\neq 0$, alors $C-B=a^n$, $P=p^n$, $A=ap$; $C-A=b^n$, $Q=q^n$, $B=bq$; $A+B=c^n$, $R=r^n$, $C=cr$.
2a°) Cela découle du fait que les nombres en paires ($C-B$, P), ($C-A$, Q), ($A+B$, R) sont premiers entre eux.
En effet, par exemple, après que les membres du groupe de P d'une paire de termes à égale distance de ses extrémités et se démarquer de chaque paire de carré parfait, on obtient la somme de $(n-1)/2$ paires d'un facteur $(C-B)^2$ et un autre élément:

2a-1°) $P=D(C-B)^2+nC^{(n-1)/2}B^{(n-1)/2}$, où $C-B$ et P sont premiers entre eux, parce que les nombres $C-B$, C et B sont premiers entre eux. =>
2b°) $C-B=a^n$, $C-A=b^n$, $A+B=c^n$,
2c°) $P=p^n$, $Q=q^n$, $R=r^n$.

3°) le nombre $U=A+B-C=un^k$, où $k>1$, d'où $(A+B)-(C-B)-(C-A)=2U$;
L'équation $(A'+B'-C')'=0$ découle du petit théorème, parce que
3-1°) $A^{(n-1)}{}'=B^{(n-1)}{}'=C^{(n-1)}{}'=1$. =>
3-2°) $P'=Q'=R'=1$ (où $P=p^n$, $Q=q^n$, $R=r^n$). =>
3-3°) $p'=q'=r'=1$. =>
3-4°) $P_{[2]}=Q_{[2]}=R_{[2]}=01=1$. =>
3-5°) $U=A+B-C=un^2$ => $k=2$.

3a°) mais si, par exemple, $B_{[k]}=0$, et $B_{[k+1]}\neq 0$, то $(C-A)_{[kn-1]}=0$, où $kn-1>k+1$, alors dans l'équation
3b°) $[(A+B)-(C-B)-(C-A)]_{[k+1]}=(2U)_{[k+1]}$ (см. 3°) le nombre $(C-A)_{[k+1]}=0$.
En effet, à partir de l'équation 2a-1° puor Q nous voyons que si $C-A$ est divisé en n, alors Q est pas divisible en n^2, parce que Q a un seul facteur n. =>
Si B est divisé en n^k, alors C-A est divisé en n^{kn-1}.

Si $k=2$ (см. 3°), alors :

4a°) $A_{[2]}=a^n{}_{[2]}=a'''{}_{[2]}$, $B_{[2]}=b^n{}_{[2]}=b'''{}_{[2]}$, $C_{[2]}=c^n{}_{[2]}=c'''{}_{[2]}$; и $P_{[2]}=a'^{(n-1)n}{}_{[2]}=1$ (c $p'=a^{n-1}{}_{[1]}=1$);
$Q_{[2]}=b'^{(n-1)n}{}_{[2]}=1$ (c $q'=b^{n-1}{}_{[1]}=1$); $R_{[2]}=c'^{(n-1)n}{}_{[2]}=1$ (c $r'=c^{n-1}{}_{[1]}=1$).
Cela découle de l'équation $(A+B-C)_{[2]}=0$ (3°) et 2b°: $(A+a^n)_{[2]}=(B+b^n)_{[2]}=(c^n+C)_{[2]}=0$.

4b°) $A^n{}_{[3]}=a'''^{n}{}_{[3]}$ $(=a'''^{n\wedge k}{}_{[3]}$, c'est-à-dire $k=2)$, $B^n{}_{[3]}=b'''^{n}{}_{[3]}$; $C^n{}_{[3]}=c'''^{n}{}_{[3]}$; <= 5°. => (v. 1°-2°)
4c°) $a^{nn}{}_{[3]}=(c^{nn}{}_{[3]}-b^{nn}{}_{[3]})_{[3]}$, => (voir les décomposition des formules et 2°) =>
4d°) $a^{nn}{}_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})_{[3]}P_{[3]}\}_{[3]}$ et $(c^{nn}{}_{[3]}-b^{nn}{}_{[3]})_{[3]}=\{(c^n{}_{[3]}-b^n{}_{[3]})p^n{}_{[3]}\}_{[3]}$, où $P_{[2]}=a^{(n-1)n}{}_{[2]}=1$;

5°) Le chiffre $A^n{}_{(k+1)}$ est défini de manière unique par la terminaison $A_{[k]}$ (une simple conséquence de la formule du binôme de Newton). C'est-à-dire les terminaisons $a^n{}_{[2]}$, $a^{n\wedge 2}{}_{[3]}$ etc. ne dépendent pas du chiffre a'' !
Il résulte de la représentation de A sous la forme $A=dn+A'$ et de l'expansion binomiale
5a°) $A^n=(dn+A')^n$.

6°) **Le Lemme**. Chaque diviseur premier de cofacteur R du binôme $A^{n\wedge k}+B^{n\wedge k}=(A^{n\wedge\{k-1\}}+B^{n\wedge\{k-1\}})R$, où $k>1$, les nombres A et B sont premiers entre eux et le nombre $A+B$ n'est pas un multiple premier de $n>2$, a la forme : $m=dn^k+1$.

Preuve

Supposons que parmi les diviseurs premiers du facteur R il y a un diviseur de la forme: $m=dn^{k-1}+1$, où d est pas un multiple de n. Ensuite, les nombres

6-1°) $A^{n\wedge k}+B^{n\wedge k}$ et, d'après le petit théorème de Fermat pour premier degré m,
6-2°) $A^{dn\wedge(k-1)}-B^{dn\wedge(k-1)}$ (où d est pair) sont divisées en m.

Théorème sur le PGCD de deux binômes d'alimentation $A^{dn}+B^{dn}$ et $A^{dq}+B^{dq}$, où les nombres naturel A et B sont premiers entre eux, n [>2] et q [>2] sont premiers entre eux et d> 0, indique que le plus grand diviseur commun de ces binômes égale à A^d+B^d .
Dans notre cas, GCD, divisible en m, est le nombre $A^{n\wedge(k-1)}-B^{n\wedge(k-1)}$, qui est premier au nombre R. Par conséquent, aucun facteur m de la forme $m=dn\wedge\{k-1\}+1$ n'est pas facteur du R. Il résulte de cette vérité lemmes.
Cela prouve le lemme et le théorème !

Victor Sorokin
/ Mézos, France /