LE GRAND THEOREME DE FERMAT :

« $\forall z, \ \forall y, \ \forall x, \ \forall n \in N^*, n>2 : z^n \neq y^n + x^n$ »

PREUVE DIRECTE :

Méthode de résolution : l'induction par récurrence.

La proposition :

(1) $(\forall y, \ \forall x, \ \forall n \in N^*, pgcd(y,x)=1, \quad n>2 : \ (1^n \neq y^n + x^n)\wedge(1^n \neq y^n - x^n))\wedge$
$(\forall y, \ \forall x, \ \forall n \in N^*, pgcd(2,y,x)=1, n>2 : \ (2^n \neq y^n + x^n)\wedge(2^n \neq y^n - x^n))\wedge$
$(\forall y, \ \forall x, \ \forall n \in N^*, pgcd(3,y,x)=1, n>2 : \ (3^n \neq y^n + x^n)\wedge(3^n \neq y^n - x^n))$,

donne les trois premiers termes d'une récurrence.

Démonstration de (1) :

Comme tout entier n>2 est un multiple de 4 ou d'un nombre premier impair, il suffit de prouver le grand théorème de Fermat pour n=4 et pour chaque nombre premier impair.

Pour n=4 :

$2^4 = y^4 - x^4 = (y^2-x^2)(y^2+x^2)$, égalité impossible, le facteur (y^2+x^2) , supérieur à 4, n'est pas une puissance de 2 ($y^2+x^2 \equiv 2 \bmod 4$).

$3^4 = y^4 - x^4 = (y^2-x^2)(y^2+x^2)$, égalité impossible, le facteur (y^2+x^2) , supérieur à 3, n'est pas une puissance de 3 ($y^2+x^2 \equiv 2 \bmod 3$).

Pour n=p , p nombre premier impair :

$2^p = y^p - x^p$

$2=y-x \bmod p \rightarrow y-x\neq 1$, $2^p = (y-x)[(y^p - x^p)/(y-x)]$,

les deux facteurs du second membre sont nécessairement premiers entre eux, l'égalité est donc impossible.

$3^p = y^p - x^p$

$3=y-x \bmod p \rightarrow y-x\neq 1$, $3^p = (y-x)[(y^p - x^p)/(y-x)]$,

pour p≠3, les deux facteurs du second membre sont nécessairement premiers entre eux, l'égalité est donc impossible.

Pour p=3 :

$3^3 = (y-x)[(y^3 - x^3)/(y-x)]= (y-x)(y^2+y*x+x^2)$, égalité impossible puisque $y^2+yx+x^2 > (y-x)^2 > y-x \geq 3 \ \rightarrow \ y-x = 3$, $(y-x)^2= 3^2$, $y^2+y*x+x^2 > 3^2$.

Etant donnée la proposition (1), supposons que pour un entier r quelconque, $r > 3$, et pour tout entier z, $1 \leq z \leq r$, nous ayons :
(2) $\forall y, \forall x, \forall n \in N^*, n>2 : (z^n \neq y^n + x^n) \wedge (z^n \neq y^n - x^n)$.

Dans cette hypothèse, nous avons aussi :
$\forall y, \forall x, \forall n \in N^*, n>2 : (r+1)^n \neq y^n + x^n$,
sinon $\exists y, \exists x, \exists n \in N^*, n>2 : (r+1)^n = y^n + x^n \rightarrow y^n = (r+1)^n - x^n$
contrairement à l' hypothèse (2),
puisque $(r+1) > y > x \rightarrow x < y \leq r \rightarrow y^n \neq (r+1)^n - x^n$.

La proposition $\forall y, \forall x, \forall n \in N^*, n>2 : z^n \neq y^n + x^n$ étant vraie pour z=1, 2, 3, …... , r (quelconque) et r+1, elle est vraie pour tout $z \in N^*$:
(3) $\forall z, \forall y, \forall x, \forall n \in N^*, n>2 : z^n \neq y^n + x^n$.

Ahmed Idrissi Bouyahyaoui