THEOREME DE FERMAT « à la Fermat »

RESUME

On remarque que pour p impair ≥5, $(xy)^2(x+y)^2$ divise $((x+y)^p-x^p-y^p)/(x\,y(x+y))) - p(x^2+y^2+x\,y)^{(p-3)/2}$ (annexe 2). Il suffit de le démontrer (annexe 1) sous la forme :

Lemme 1: pour p impair ≥ 3,$(a+b)^p-a^p-b^p = -\,p(a+b)(-ab)^{(p-1)/2} + (ab)^2(a+b)^2J(a,b)$.
Pour p premier J(a,b) = p H(a,b) , J et H polynômes à coefficients entiers.

Pour p premier ≥3, on peut supposer qu'il existe 3 nombres x,y,z premiers entre eux (donc xyz ≠0) tels que
(1) $x^p + y^p = z^p$ le petit théorème de Fermat permet d'écrire :
$z = x + y - kp^\alpha$, α≥1 tel que k Λ p=1(premiers entre eux),en utilisant
(a) u premier divise v, alors $v = ku^\alpha$, α≥1 tel que k Λ u =1

On réécrit le lemme 1 de façon utile :
(2) pour p impair ≥ 5, $(x+y)(-xy)^{(p-1)/2} + k^p p^{\alpha p-1} = (x+y)^2 h(x,y)$

On suppose **p Λ (x +y) =1** . On décompose (x +y) et k selon les facteurs premiers de leur pgcd en utiliant l'astuce (a) pour avoir des nombres premiers entre eux. (2) donne :
(3) Si p Λ (x +y) =1 , k=K σ et $(x+y) = \sigma^p$, p σ Λ K =1 .

On pose par permutation **p Λ xy =1**, les hypothèses de **(3)** sont remplies pour $z - x = Y^p$ et $z - y = X^p$,
On démontre $z = X^p+Y^p+u$, avec $u= -hXY p^\alpha$ **,(1) devient $(X^p+u)^p + (Y^p+u)^p = (X^p+Y^p+u)^p$**
Alors, avec le lemme 1, on tombe sur une contradiction pour **p≥ 5,** d'où

Lemme 2 :pour p impair premier ≥ 5, x,y et z entiers,
les solutions de $x^p+y^p=z^p$ sont toutes du type xyz = 0

Pour p=3, on réécrit **(1)** $x^3 + y^3 = z^3$ sous la forme **(1')** $(x)^3 + (x-a)^3 = (x+b)^3$,
soit avec Z= x -(a+b), $Z^3 - 6\,b(a+b)\,Z - 3b(a+b)(2b+a)$. On recherche les diviseurs communs à b(a+b) et Z.
Il reste $Z= 3^\alpha \sigma\, Z'$, $Z'^3 - 2\,\sigma 3^\alpha Z' - (2b+a)=0$, et $b(a+b)= 3^{3\alpha-1}\sigma^3$,
On applique alors la méthode de Cardan pour $Z^3 + pZ +q = 0$, on obtient qu'il n'y a qu'une seule solution Z' réelle, somme de 2 racines cubiques Z' = u + v avec uv= -(p/3) entier . Si Z' est entière.u et v sont entiers.
Le théorème1(cf. annexe 3) sur la solution générale de $x^2 + ny^2 = z^2$ devient central. On obtient d'abord **$\pm 9a=9-b(a+b)$.** dont le théorème 1 permet de calculer les solutions entières en b. On obtient avec ε = ±1, a = 4ε, b= -2ε ± 7. Mais alors, $b(a+b) = (-2\varepsilon \pm 7)(2\varepsilon \pm 7) = 45 = 3^{3\alpha-1}\sigma^3$, α=1,$\sigma^3$ =5, mais 5 n'est pas un cube.

Lemme 3 : les solutions entières de $x^3 + y^3 = z^3$ sont seulement xyz=0.

Pour **p=4**.on utilise le théorème 1 en annexe 3, on obtient :
S'il existe x,y,z entiers tels que $x^4+y^4=z^4$, alors xy=0.

On peut conclure :

Pour p entier non nul, s'il existe x,y,z entiers relatifs tels que xyz ≠ 0 et $x^p+y^p=z^p$, alors p ≤ 2.
Il existe x,y,z entiers tels que $x^2+y^2=z^2$ est équivalent à
il existe a,b entiers tels que $(a^2-b^2)^2 + 4\,a^2 b^2 = (a^2+b^2)^2$.

Philippe AJASSE 09/2012

THEOREME DE FERMAT « à la Fermat »

En faisant des calculs, Fermat a du remarquer que pour p impair ≥5 :
$(xy)^2(x+y)^2$ divise **(** $(x+y)^p-x^p-y^p)/(x\,y(x+y)$ **)** - $p(x^2+y^2+x\,y)^{(p-3)/2}$, d'où l'intérêt de faire apparaître (x+y) dans z, objet du « petit théorème ». On voit cela à l'annexe 2 calculée au tableur. Cela est démontré en annexe 1 sous une forme centrale intervenant à chaque étape de la démonstration suivante, accessible à Fermat.

Lemme 1: (cf. annexe 1) pour p impair ≥ 3
$(a+b)^p-a^p-b^p = -\,p(a+b)(-ab)^{(p-1)/2} + (ab)^2(a+b)^2J(a,b)$.
Pour p premier $J(a,b) = p\,H(a,b)$, J et H polynômes à coefficients entiers.

Pour p premier ≥3, on peut supposer qu'il existe 3 nombres x,y,z premiers entre eux (donc xyz ≠0) tels que

(1) $\mathbf{x^p + y^p = z^p}$

la racine p-ième de 2 n'étant pas entière, on peut aussi supposer **zx, xy, yz ≠ ±1.**
le petit théorème de Fermat (les coefficients ≠1 de $(x+y)^p$ sont divisibles par p) donne
$z = x + y - kp^\alpha$, α≥1 tel que k Λ p=1(premiers entre eux), (on suppose k ≠0 , cf. lemme 0 en annexe1) et **(1)** s'écrit
$(x+y)^p - x^p - y^p=(x+y)^p-(x+y-kp^\alpha)^p=(x+y)^p+(-x-y+kp^\alpha)^p$
en utilisant le lemme 1 de part et d'autre
$-p(x+y)(-xy)^{(p-1)/2} + p\,x^2\,y^2(x+y)^2\,r(x,y) = k^p\,p^{\alpha p} + p\,kp^\alpha\,(-(x+y)(kp^\alpha-x-y))^{(p-1)/2} - p(kp^\alpha)^2\,(kp^\alpha-x-y)^2\,(x+y)^2r(x+y,-z)$
en simplifiant par p,
$;-(x+y)(-xy)^{(p-1)/2} + x^2\,y^2\,(x+y)^2\,r(x,y) = k^p\,p^{\alpha p-1} + kp^\alpha\,(z(x+y))^{(p-1)/2} - (kzp^\alpha)^2(x+y)^2r(x+y,-z)$,
pour p ≥ 5, $((p-1)/2) \geq 2$, $(x+y)^2$ divise $(z(x+y))^{(p-1)/2}$.

A/ p impair premier ≥ 5

(2) pour p≥ 5, $\mathbf{(x+y)\,(-xy)^{(p-1)/2} + k^p\,p^{\alpha p-1} = (x+y)^2\,h(x,y)}$
donc (x +y) divise $(kp^\alpha)^p$,(x + y ≠ 0 sinon z =0).

• Supposons **p Λ (x +y) =1** et (x +y) ≠ ±1. Si k= ±1, (2) donne p divise (x +y), on a k et (x +y)≠ ±1. On **décompose en facteurs premiers** :pgcd(x +y,k)= $s^u\,t^v$ (pour la clarté on limite à deux facteurs), puis k et x +y : **s et t étant premiers**, (on a st ≠ ±1) on peut écrire :
$k=K\,s^c\,t^e$ (avec **K Λ pst =1**), $(x+y) = S\,s^b\,t^d$ (avec **S Λ pst =1**),par définition du pgcd : **S Λ K =1**
(2) devient :$S\,s^b\,t^d\,(-xy)^{(p-1)/2} + K^p\,s^{pc}\,t^{pe}\,p^{\alpha p-1} = (S\,s^b\,t^d)^2\,h(x,y)$
pc≥ b , sinon s divise K^p, de même pe≥ d . On a aussi S divise $K^p\,p^{\alpha p-1}$,comme S Λ Kp =1, S = ±1.
en divisant par x +y: $(-xy)^{(p-1)/2} + K^p\,s^{pc-b}\,t^{pe-d}\,p^{\alpha p-1} = (s^b\,t^d)\,h(x,y)$
x Λ y =1et xy ≠ ±1, donc (x +y) Λ xy =1 et st Λ xy =1, or st ≠ ±1, donc pc=b et pe=d, c'est-à-dire :

(3) Si p Λ (x +y) =1 , k=K σ et (x +y) = $\mathbf{\sigma^p}$ **, p σ Λ K =1** . Cela reste vrai pour (x +y) = ±1.

• Posons par permutation (p impair) **p Λ xy =1**, en effet x,y et z étant premiers entre eux, p ne peut diviser au plus qu'un des trois, les hypothèses de **(3)** sont remplies et

$z - x = Y^p$, $y = Y(Y^{p-1} - H\,p^\beta) = z - X^p$, $H\,\Lambda\,pY = 1$
$z - y = X^p$, $x = X(X^{p-1} - L\,p^\alpha) = z - Y^p$, $L\,\Lambda\,pX = 1$

les égalités de la seconde colonne donnent **X et Y premiers entre eux et p Λ XY =1**, et
$-z + X^p + Y^p = YH\,p^\beta = XL\,p^\alpha$,on en déduit β = α et h tel que hXY =YH = XL, h Λ XY =1, alors
$z - (X^p + Y^p) = -hXYp^\alpha$, soit $z = (X^p + Y^p) - hXYp^\alpha$.
Posons $\mathbf{u= -hXY\,p^\alpha}$ **, on a hpΛXY =1, hΛp=1, (1) devient** $\mathbf{(X^p+u)^p + (Y^p+u)^p = (X^p+Y^p+u)^p}$
En développant :
$(X^p+Y^p)^p - X^{pp} - Y^{pp} - u^p + pu\,((X^p+Y^p)^{p-1} - X^{p(p-1)} - Y^{p(p-1)}) + pM\,u^2 \ldots\ldots = 0$
on voit que $X^p\,Y^p$ divise les coefficients des pu^δ (δ = 1 à p-2, le terme en pu^{p-1} =0) donc
$(XY)^{p+1}$ divise $(X^p+Y^p)^p - X^{pp} - Y^{pp} - u^p$
Or $(X^p+Y^p)^p - X^{pp} - Y^{pp} = -p(X^p+Y^p)(-X^pY^p)^{(p-1)/2} + p\,X^{2p}\,Y^{2p}\,(X^p+Y^p)^2\,r(X^p,Y^p)$
pour p ≥ 5 , $((p-1)/2) \geq 2$, $(XY)^{p+1}$ divise $(X^p+Y^p)^p - X^{pp} - Y^{pp}$, **donc** $\mathbf{(XY)^{p+1}}$ **divise** $\mathbf{-u^p = (hXY\,p^\alpha)^p}$,
soit XY divise $(h\,p^\alpha)^p$, mais XY Λ h p^α =1 donc XY = ±1. Si X=Y = ±1, x = y, reste X= -Y = ±1, alors 2z = x +y,
soit x +y = 2 (x + y- kp^α) = 2 kp^α . On substitue dans **(2)** $(x+y)\,(-xy)^{(p-1)/2} + k^p\,p^{\alpha p-1} = (x+y)^2\,h(x,y)$,
$2(-xy)^{(p-1)/2} + k^{p-1}\,p^{\alpha(p-1)} = 4\,k\,p^\alpha\,h(x,y)$, soit p divise xy, qui contredit p Λ xy =1.

Lemme 2 :pour p impair premier ≥ 5, x,y et z entiers,
les solutions de $x^p+y^p=z^p$ sont toutes du type xyz = 0

Philippe AJASSE 09/2012

THEOREME DE FERMAT « à la Fermat »

B/ p=3

On réécrit **(1) $x^3 + y^3 = z^3$** sous la forme **(1') $(x)^3 + (x-a)^3 = (x+b)^3$**,
soit $x^3 -3(a+b)x^2 +3(a^2 -b^2)x -a^3 -b^3 =0$, ab=0 contredit $x\Lambda yz= 1$ donc $ab\neq 0$. Si w divise a et b, w divise x^3 , mais $x \Lambda (x-a) = 1$, **donc $a \Lambda b = 1$.**
Posons Z= x -(a+b), $x^3 -3(a+b)x^2 +3(a^2 -b^2)x -a^3 -b^3 =Z^3 - 6b(a+b)x +3ab(a+b) = Z^3 - 6 b(a+b) Z - 3b(a+b)(2b+a)$.
$a+b=0$ contredit $y\Lambda z= 1$ donc $a+b\neq 0$. Si 2b+a = 0, on a $Z^3 + 12 b^2 Z = 0$ donc Z = 0, x = a+b = -b soit z= 0.
Posons N = b(a+b), on a $Z^3 - 6NZ -3N(2b+a)=0$, si N= ±1, a(2b+a)=0, donc $N \neq \pm 1$, (2b+a)=b+a+b, $N\Lambda(2b+a)=1$.
On voit que 3 divise Z, donc Z= ±1 . On décompose en facteurs premiers :
pgcd(N, Z)= $3^w s^u t^v$ (pour la clarté on limite à deux facteurs), puis N et Z :
$Z = k\, 3^\alpha s^c t^e$ (avec $k \Lambda 3st =1$), $N = n\, 3^\beta s^b t^d$ (avec $n \Lambda 3st =1$), par définition du pgcd, $n \Lambda k =1$,
$k^3 3^{3\alpha} s^{3c} t^{3e} = 6 (k\, 3^\alpha s^c t^e)(n\, 3^\beta s^b t^d) + 3(2b+a)(n\, 3^\beta s^b t^d)$. 3c≥ b, sinon s divise k^3, de même 3e≥ d
$(N\Lambda(2b+a)=1)$. On a aussi n divise $k^3 3^{3\alpha} s^{3c} t^{3e}$ comme $n\Lambda 3kst =1$, **n=1**. En divisant par 3N:
$k^3 3^{3\alpha-\beta-1} s^{3c-b} t^{3e-d} =2(k\, 3^{3\alpha} s^c t^e) +(2b+a). (2b+a)\Lambda N =1$, donc $(2b+a)\Lambda st =1$, et donc 3c=b et 3e=d, c'est-à-dire :
$k^3 3^{3\alpha-\beta-1} = 2(k\, 3^{3\alpha} s^c t^e) +(2b+a). (2b+a) \Lambda N =1$, donc si 3 divise N, β = 3α-1, sinon (2b+a) = h k $3^{3\alpha-\beta-1}$, soit :
$Z=3^\alpha k\sigma$ et $b(a+b)= N = 3^{3\alpha-1}\sigma^3$, $(2b+a) =h'k$, ou $b(a+b)= N = \sigma^3$, $(2b+a) =3^{3\alpha-1} hk$, avec $3 \Lambda \sigma =1$.
Posons **$Z= 3^\alpha \sigma Z'$, $3 \Lambda \sigma Z' =1$,** $Z'^3 - 2\, \sigma 3^\alpha Z' – (2b+a)=0$, ou $3^{3\alpha}Z'^3 -6\, \sigma 3^\alpha Z' -3(2b+a)=3^{3\alpha}Z'^3 -6\, \sigma 3^\alpha Z' -3^{3\alpha} hk=0$,
mais $3^{2\alpha-1}$ diviserait $2\, \sigma Z'$. **Il reste $Z'^3 - 2\, \sigma 3^\alpha Z' – (2b+a)=0$, et $b(a+b)= 3^{3\alpha-1}\sigma^3$,**
On applique la méthode de Cardan pour $Z^3 + pZ +q = 0$ à **(1'') $Z'^3 - 2\, \sigma 3^\alpha Z' – (2b+a)=0$, avec $pq\neq 0$.**
Calculons $D = q^2 + 4(p/3)^3$. $D = (2b+a)^2 - 32(3^{3(\alpha-1)}\sigma^3)= (1/9)(9(2b+a)^2 -32b(a+b)) = (1/9)(4b^2 +4ab +9a^2)$, le discriminant de la forme quadratique est strictement négatif, ab≠0,donc $D= \delta^2 >0$.
Il n'y a alors qu'**une seule racine réelle** ; Z_1 = racine cubique $((-q + \delta)/2)$ + racine cubique $((-q - \delta)/2) = u + v$.
$(q^2 - \delta^2)/4 = -(p/3)^3 =(3^{\alpha-1}\, \sigma)^3 = u^3v^3$. On voudrait u+v entier. D'après la remarque en fin d'annexe 3 :
si u+v entier, alors u et v sont entiers. $\delta^2 = (1/9)(4b(a+b) + 9a^2)= (1/9) (4\, 3^{3\alpha-1}\sigma^3 + 9a^2) =(4\, 3^{3(\alpha-1)}\sigma^3 + a^2)$.
u et v entiers implique u^3 et v^3 entiers, donc δ entier, donc il existe c tel que $4\, 3^{3(\alpha-1)}\sigma^3 + a^2 = c^2$. On reconnaît (cf. théorème1, annexe 3) la solution générale de $a^2 + ny^2 = c^2$, $n= 3^{(\alpha-1)}\sigma$, A=B=γ=1. Si on répartissait les diviseurs de 3σ sur les deux membres de a, on aurait un diviseur commun à a et b(a+b), contraire à $a \Lambda b =1$. **Il reste $\pm a = 1- 3^{3(\alpha-1)}\sigma^3$, $\pm c = 1 +3^{3(\alpha-1)}\sigma^3$, et $\pm 9a=9-b(a+b)$.**(idem si on pose $3^{3(\alpha-1)}\sigma^3 =(3^{\alpha'}\sigma')^6$, n=1)
$b^2 + ab – 9(1+\varepsilon a) = 0$, ε = ±1, dont le discriminant est $d = a^2 + 36 (1+\varepsilon a) = (a+18\, \varepsilon)^2 - 4.72 = (a+18\, \varepsilon)^2 - 4.2(2.3)^2$,
b entier implique d=d'² , soit $(a+18\, \varepsilon)^2 = d'^2 + 4.2(2.3)^2$. On reconnaît encore la solution générale de $x^2 + ny^2 = z^2$, n=2, (A,B) ou (B,A)=(1,3) et γ=1 ou (A,B) ou (B,A)=(2,3) et γ=0. Seule cette dernière convient et $(a+18\, \varepsilon)^2 = (4 + 18)^2$. On a $\varepsilon a = 4$, $d'^2 = (4 - 18)^2$, b= -2ε ± 7.
Mais alors, $b(a+b) = (-2\varepsilon \pm 7)(2\varepsilon \pm 7) = 45$, or $b(a+b) = 3^{3\alpha-1}\sigma^3$, $\alpha=1, \sigma^3 =5$, mais 5 n'est pas un cube.

Lemme 3 : les solutions entières de $x^3 + y^3 = z^3$ sont seulement xyz=0.

C/ p=2 et p= 4

(1) $x^2 + y^2 = z^2$ est un cas particulier du théorème 1 en annexe 3,

p=4
$(2r +1)^4 = (z^2 + y^2)$, $(2R +1)^4 = (z^2 - y^2)$, $(2r +1)\Lambda(2R +1)=1$, (2r +1) et $(2R +1) \neq \pm 1$ car $z^2 \pm y^2 \neq 1$.
Posons 2R+1= $(a^2 -b^2)$, avec $(a+b) \Lambda(a-b)=1$, soit $a \Lambda b=1$(cf. théorème 1 en annexe 3).
$2\, y^2 = (2r +1)^4 - (a^2 - b^2)^4$, $2\, y = (a + b)^4 - (a - b)^4$,= $8\, ab(a^2 + b^2)$, $(2r +1)^4 = (a^2 - b^2)^4 + 32\, a^2 b^2 (a^2 + b^2)^2$,
$(2r +1)^4 = ((a^2 + b^2)^2 - 4a^2 b^2)^4 + 32\, a^2 b^2 (a^2 + b^2)^2 = (a^2 + b^2)^4 + 24\, a^2 b^2 (a^2 + b^2)^2 + 16\, a^4 b^4$,
$(2r +1)^4 + 128\, a^4 b^4 = ((a^2 + b^2)^2 +12a^2 b^2)^2$, on reconnaît $X^2 +4nY^2 = Z^2$ avec n = 2, Y= ±4 $a^2 b^2$ = ±(n^γ AB),d'après le théorème 1 en annexe 3, $Z = (A^2 + n^{2\gamma+1} B^2) =(a^2 + b^2)^2 +12a^2 b^2$, si a (resp. b) divise A^2 et B^2 , a divise b (resp.b divise a), le coefficient de $a^4 = 1$, $A^2 = a^4$ ***(ou b^4)***, de Y=±4 $a^2 b^2$= ±(n^γ AB), $B^2 =16b^4$,γ = 0, ou $B^2 =b^4$,γ = 2. Alors $n^{2\gamma+1}B^2 =32\, b^4 =b^2(b^2+14a^2)$, donc $31b^4 =14a^2 b^2$, donc b=0, ***(ou a=0)***, pas de solution pour $z^2 \pm y^2 \neq 1$.
S'il existe x,y,z entiers tels que $x^4 +y^4 =z^4$, alors xy=0.
On peut conclure :

Pour p entier non nul, s'il existe x,y,z entiers relatifs tels que $xyz \neq 0$ et $x^p +y^p =z^p$, alors $p \leq 2$.
Il existe x,y,z entiers tels que $x^2 +y^2 =z^2$ est équivalent à
il existe a,b entiers tels que $(a^2 -b^2)^2 + 4\, a^2 b^2 = (a^2 +b^2)^2$.

Tout ce qui précède était accessible à Fermat.

Philippe AJASSE 09/2012

THEOREME DE FERMAT « à la Fermat »

ANNEXE 1

Lemme 1: pour p impair ≥ 3, $(a+b)^p-a^p-b^p = - p(a+b)(-ab)^{(p-1)/2} + (ab)^2(a+b)^2J(a,b)$. Pour p premier J(a,b) = p H(a,b) , J et H polynômes à coefficients entiers.

On a $(a+b)^p-a^p-b^p=\Sigma C(p,i)\ (ab)^i(a^{(p-2i)}+b^{(p-2i)})$, i=1 à (p-1)/2, comme p est premier, p divise les C(p,i) (i≠1 et p) donc le second membre.**($)**

On a aussi $(a+b)^p-a^p-b^p=(a+b)\ (\ (a+b)^{p-1}-((a^p+b^p)/(a+b)))$ =
$(a+b)\ (C((p-1)/2,p-1)-(-1)^{(p-1)/2})\ (ab)^{(p-1)/2}+(a+b)\ \Sigma\ (C(i,p-1)-(-1)^i)\ (ab)^i\ (\ a^{(p-1-2i)}+b^{(p-1-2i)})$,i=1 à (p-3)/2, soit
$(a+b)^p-a^p-b^p=ab(a+b)\Sigma D(i,p-1)(ab)^{i-1}(a^{(p-1-2i)}+b^{(p-1-2i)})$, i=1 à (p-1)/2,
en posant $((a+b)^p-a^p-b^p)/(ab(a+b)) = S_p$,
$S_p=p(a^{(p-3)}+b^{(p-3)})+(((p-1)(p-2)/2)-1)ab(a^{(p-5)}+b^{(p-5)})+\Sigma D(i,p-1)(ab)^{i-1}(a^{(p-1-2i)}+b^{(p-1-2i)})$, i=3 à (p-1)/2, avec
$a^{(p-1-2i)}+b^{(p-1-2i)}=(a^2+b^2)^{(p-1-2i)/2}-\Sigma C((p-1-2i)/2,j)\ (ab)^{2j}(a^{(p-1-2i-2j)}+b^{(p-1-2i-2j)})$, j=1 à (p-1-2i)/4, et un terme en $(ab)^{2j}$ pour (p-1-2i)/2 pair, soit
$S_p=p(a^2+b^2)^{(p-3)/2}+(p(p-3)/2)ab(a^2+b^2)^{(p-5)/2}+\ \Sigma E(i,p-1)\ (ab)^{i-1}(a^2+b^2)^{(p-1-2i)/2}$, i=3 à (p-1)/2

$S_p=p(a^2+b^2+ab)^{(p-3)/2}+(ab)^2\Sigma E(i,p-1)\ (ab)^{i-3}(a^2+b^2)^{(p-1-2i)/2}$, i=3 à (p-1)/2

Supposons $a=\sigma(1+\varepsilon)$ et $b=\sigma(-1+\varepsilon)$,$S_p-p(a^2+b^2+ab)^{(p-3)/2}=(p(p-5)(p-7)/6)\varepsilon^2\sigma^{(p-3)/2}+A\ \varepsilon^4$,
donc $(a+b)^2$ divise $S_p-p(a^2+b^2+ab)^{(p-3)/2}$,soit

$(a+b)^p-a^p-b^p=pab(a+b)(a^2+b^2+ab)^{(p-3)/2}+\ (ab)^3(a+b)^3G(a,b)$, G(a,b) polynôme à coefficients entiers.

en utilisant **($),** p divise G, et comme $a^2+b^2+ab= (a+b)^2-ab$, on obtient
$(a+b)^p-a^p-b^p=-p(a+b)(-ab)^{(p-1)/2}+\ p(ab)^2(a+b)^2H(a,b)$
pour p=3, $(a+b)^3-a^3b^3=-3(a+b)(-ab)^{(3-1)/2} = 3ab(a+b)$, H(a,b)=0

Lemme 0 :pour p entier impair ≥ 3, et x,y deux entiers relatifs (≥ ou ≤ 0) , $x^p+y^p=(x+y)^p$ implique xy(x+y) =0 .

Si y ≠0 **,** posons z = x/y et $f(z) = (z + 1)^p - z^p - 1 = g_p(z) – 1$.On remarque pour la dérivée de $g_p(z)$:
$g_p'(z) = p\ g_{p-1}(z)$. On démontre alors par récurrence pour n≥ 1 :
$g_{2n}(z)$ est croissante, $g_{2n+1}(z)$ décroît pour z ≤ -1/2 puis croît.
On en déduit l'existence de au plus deux solutions pour $g_p(z) = 1$.
En remarquant que $g_p(0) = 1$ et que $g_p(-1) = 1$, on obtient xy(x+y) =0.

THEOREME DE FERMAT « à la Fermat »

ANNEXE 2

Calcul de $((a+b)^p-a^p-b^p)/(ab(a+b)) = S_p$

Posons $\nu^3 = ab(a+b)$ et $\mu^2 = a^2+b^2+ab$

$S_3 = 3$
$S_5 = 5\ \mu^2$
$S_7 = 7\ \mu^4$
$S_9 = 9\ \mu^6 + 3\ \nu^6$
$S_{11} = 11\ \mu^8 + 11\ \nu^6 \mu^2$
$S_{13} = 13\ \mu^{10} + 26\ \nu^6 \mu^4$
$S_{15} = 15\ \mu^{12} + 50\ \nu^6 \mu^6 + 3\ \nu^{12}$
$S_{17} = 17\ \mu^{14} + 85\ \nu^6 \mu^8 + 17\ \nu^{12} \mu^2$
$S_{19} = 19\ \mu^{16} + 133\ \nu^6 \mu^{10} + 57\ \nu^{12} \mu^4$
$S_{21} = 21\ \mu^{18} + 196\ \nu^6 \mu^{12} + 147\ \nu^{12} \mu^6 + 3\ \nu^{18}$
$S_{23} = 23\ \mu^{20} + 276\ \nu^6 \mu^{14} + 322\ \nu^{12} \mu^8 + 23\ \nu^{18} \mu^2$
$S_{25} = 25\ \mu^{22} + 375\ \nu^6 \mu^{16} + 630\ \nu^{12} \mu^{10} + 100\ \nu^{18} \mu^4$
$S_{27} = 27\ \mu^{24} + 495\ \nu^6 \mu^{18} + 1134\ \nu^{12} \mu^{12} + 324\ \nu^{18} \mu^6 + 3\ \nu^{24}$
$S_{29} = 29\ \mu^{26} + 638\ \nu^6 \mu^{20} + 1914\ \nu^{12} \mu^{14} + 870\ \nu^{18} \mu^8 + 29\ \nu^{24} \mu^2$
$S_{31} = 31\ \mu^{28} + 806\ \nu^6 \mu^{22} + 3069\ \nu^{12} \mu^{16} + 2046\ \nu^{18} \mu^{10} + 155\ \nu^{24} \mu^4$
$S_{33} = 33\ \mu^{30} + 1001\ \nu^6 \mu^{24} + 4719\ \nu^{12} \mu^{18} + 4356\ \nu^{18} \mu^{12} + 605\ \nu^{24} \mu^6 + 3\ \nu^{30}$
$S_{35} = 35\ \mu^{32} + 1225\ \nu^6 \mu^{26} + 7007\ \nu^{12} \mu^{20} + 8580\ \nu^{18} \mu^{14} + 1925\ \nu^{24} \mu^8 + 35\ \nu^{30} \mu^2$
$S_{37} = 37\ \mu^{34} + 1480\ \nu^6 \mu^{28} + 10101\ \nu^{12} \mu^{22} + 15873\ \nu^{18} \mu^{16} + 5291\ \nu^{24} \mu^{10} + 222\ \nu^{30} \mu^4$
$S_{39} = 39\ \mu^{36} + 1768\ \nu^6 \mu^{30} + 14196\ \nu^{12} \mu^{24} + 27885\ \nu^{18} \mu^{18} + 13013\ \nu^{24} \mu^{12} + 1014\ \nu^{30} \mu^6 + 3\ \nu^{36}$

Pour p impair, p=6n-1 (ε=-1, ε'=1), ou p=6n+3 (ε=3, ε'=0), ou p=6n+1 (ε=1, ε'=2),
posons $S_p = (a^2+b^2+ab)^{\varepsilon'}\ \sigma_{n,\varepsilon}((a^2+b^2+ab)^3, a^2b^2(a+b)^2)$, on observe
$\sigma_{n,\varepsilon}(u,v) = \Sigma\ c_i(n,\varepsilon)\ v^i\ u^{n-i}$, i = 0 à n, $c_0(n,\varepsilon)=6n+\varepsilon=p$, $c_n(n,3)=3$, et plus généralement (i≠0),
$c_i(n,\varepsilon) = ((6n+\varepsilon)/((2i+1)!)\ \Pi(3n-i+((\varepsilon-3)/2), 3(n-i)+((\varepsilon-1)/2),)$, (a)
où Π(h,k) désigne le produit des entiers de h à k inclus.
Plus simplement, pour p=2m+1, $c_i(n,\varepsilon) = c_i(m) = (2m+1)\Pi(m-i-1, m-3i)/((2i+1)!)$, formule déduite de $c_i(m+1)+c_i(m-1)-2c_i(m)=c_{i-1}(m-2)$.

Remarque : la première factorisation de S_p tentée est avec μ^2 et ab. On observe
$S_p = p\ \mu^{p-3} + A\ (ab)^2\ \mu^{p-7} + A\ (ab)^3\ \mu^{p-9} + \ldots$, en posant b = aj(1+ ε), on retrouve $c_n(n,3)=3$ ou la divisibilité par μ^2. Mais $A\ (ab)^2\ \mu^{p-7} + A\ (ab)^3\ \mu^{p-9} = A\ (ab)^2\ \mu^{p-9}\ (\mu^2 + ab) = A\ \nu^6\ \mu^{p-9}$. Vient alors la factorisation en μ^6 et ν^6. Le tableur utilisé pour obtenir la liste ci-dessus suit les étapes :
• $(a+b)^p-a^p-b^p = (a+b)((a+b)^{p-1}-((a^p+b^p)/(a+b))) = ab(a+b)\Sigma D(i,p-1)(ab)^{i-1}(a^{(p-1-2i)}+b^{(p-1-2i)})$, i=1 à (p-1)/2,
• transformation de $(a^{(p-1-2i)}+b^{(p-1-2i)})$ en $(a^2+b^2)^{(p-1-2i)/2}$,
• factorisation de S_p en μ^2 et ab
• factorisation de S_p en μ^6 et ν^6.
Pour p=39 on voit des chiffres après la virgule, limite de la simple précision.

Philippe AJASSE 09/2012

THEOREME DE FERMAT « à la Fermat »

ANNEXE 3

Théorème 1
Il existe x,y,z entiers tels que $x^2 + ny^2 = z^2$, est équivalent à :
pour ±n premier (ou =1) :il existe A,B, γ entiers tels que
$(A^2 - n^{2\gamma+1} B^2)^2 + 4n (n^\gamma AB)^2 = (A^2 + n^{2\gamma+1} B^2)^2$.
pour $n = n_1 n_2$, $n_1 \neq n_2$:il existe A,B,α,α',β,β',γ entiers tels que $\alpha + \alpha' = \beta + \beta' = 2\gamma + 1$, et
$(n_1^\alpha n_2^\beta A^2 - n_1^{\alpha'} n_2^{\beta'} B^2)^2 + 4n (n^\gamma AB)^2 = (n_1^\alpha n_2^\beta A^2 + n_1^{\alpha'} n_2^{\beta'} B^2)^2$.

n=1
Supposons z = 2k, d'après le petit théorème x + y= 2s, **(1) $x^2 + y^2 = z^2$** s'écrit sous la forme $4 (k^2 - s^2) = -2 xy$, donc 2 divise xy, on a supposé x,y,z premiers entre eux, donc z est impair, donc au moins x ou y est impair.
Supposons $x = 2k +1$, $x^2 + y^2 = z^2$ s'écrit $(2k +1)^2 = (z + y)(z - y)$. si h divise (z + y) et (z – y), h divise 2y, 2z et $(2k +1)^2$, donc $(z + y) \Lambda (z - y) = 1$. On a $x = (2m +1)(2n +1)$ avec éventuellement m ou n=0, mais
$(2m +1)\Lambda(2n +1)=1$, alors $(2m +1)^2 = (z + y)$, $(2n +1)^2 = (z - y)$.
$2z = (2m +1)^2 + (2n +1)^2$, $2y = (2m +1)^2 - (2n +1)^2$. Faisons le changement de variables
$b = m-n$, $a = m+n+1$, alors $2m+1= a+b$, $2n+1= a-b$, $x = (a^2 -b^2)$, $z = (a^2 +b^2)$, $y = 2ab$. Supprimer x,y,z premiers entre eux revient à ne pas mettre de condition sur a et b.
n premier
$x^2 + ny^2 = z^2$ s'écrit $ny^2 =(z + x)(z – x)$. si h divise (z + x) et (z – x), h divise 2x , 2z et ny^2,
donc $(x \Lambda z = 1)$ h = ±1 ou 2. On décompose ny^2 en facteurs premiers :
$ny^2 =2^{\alpha+\beta+\delta} n^\gamma u^\eta v^\theta =(z + x)(z – x)= 2^\alpha(z '+ x')2^\beta(z' – x')$, α et β tels que $2 \Lambda(z'^2 – x'^2)= 1$,ou $(z' + x')\Lambda(z' – x')=1$.
On a $(z'^2 – x'^2) =2^\delta n^\gamma u^\eta v^\theta =$, mais $2 \Lambda(z'^2 – x'^2)= 1$, donc δ =0, alors,
(a) $(z '+ x')= v^\theta$,$(z' – x')= n^\gamma u^\eta$, d'où $2x'= v^\theta - n^\gamma u^\eta$, $2z'= v^\theta + n^\gamma u^\eta$, ou encore
$2x= 2^\alpha v^\theta - 2^\beta n^\gamma u^\eta$, $2z= 2^\alpha v^\theta + 2^\beta n^\gamma u^\eta$, $x \Lambda z = 1$, donc α =1 ou β=1,
β=1 : $x= 2^{\alpha-1} v^\theta - n^\gamma u^\eta$, $z= 2^{\alpha-1} v^\theta + n^\gamma u^\eta$, $ny^2 = 4\, 2^{\alpha-1} n^\gamma u^\eta v^\theta$, $2^{\alpha-1}$ devient un facteur premier ordinaire.
$y^2 = 4\, n^{\gamma-1} u^\eta v^\theta$, soit $\gamma =2\gamma' +1$, $\eta =2\eta'$, $\theta=2\theta'$, d'où le résultat.
$n = n_1 n_2$;
On voit qu'il faut $n^{2\gamma'+1}$ dans ny^2, que l'on obtient par le produit $(n_1^\alpha n_2^\beta)(n_1^{\alpha'} n_2^{\beta'})$ avec $\alpha + \alpha' = \beta + \beta' = 2\gamma' +1$.

Remarque :
Soit (1) $Z^3 + pZ + q = 0$ avec p/3, q entiers et $q^2 + 4(p/3)^3 = \delta^2 > 0$. Il n'y a alors qu'une seule racine réelle ;
Z_1 = racine cubique $((-q + \delta)/2)$ + racine cubique $((-q - \delta)/2) = u + v$.
u+v entier est équivalent à u et v sont entiers.

On a $(q^2 - \delta^2)/4 = -(p/3)^3 = u^3v^3$, $uv= -p/3$. Posons $u=x+\varepsilon$, $v=x-\varepsilon$, ε peut-être non entier, $uv = x^2 -\varepsilon^2$,donc $x^2 + p/3 = \varepsilon^2$ (a), qu'on utilise pour calculer
(2) $-q = (x+\varepsilon)^3 + (x-\varepsilon)^3 = 2x^3 + 6\varepsilon^2 x = 8x^3 + 2px$: 2x est solution de (1)
$\delta =(x+\varepsilon)^3 - (x-\varepsilon)^3 = 2\varepsilon (\varepsilon^2 + 3x^2) = 2\varepsilon (4x^2 + p/3)$, qu'on élève au carré, en utilisant (a) et (2) :
$\delta^2 /4 = (x^2 + p/3) (4x^2 + p/3)^2 = (x^2 + p/3)(-(4p/3)x^2 -2q\, x +(p^2 /9))=(-(4p/3)x^4-2q\, x^3 -(p^2 /3)x^2-(2pq/3)x+ (p/3)^3)$, soit
$\delta^2 /4 = - (pq/6)x + (p/3)^3 + (q^2 /4)$, soit $pqx = 0$. Donc $uv \neq x^2 -\varepsilon^2$.
Posons $u = U+\varepsilon$, $v = V-\varepsilon$, U et V entiers, ε peut-être non entier, $uv =.UV -\varepsilon(\varepsilon+U-V)$,
donc $\varepsilon(\varepsilon+U-V)$ est entier. Comme **U** ≠ V, ε est entier.