THEOREME DE FERMAT « à la Fermat » pour p ≥ 5

RESUME

Lemme 1: pour p impair ≥ 5, a et b réels
$(a+b)^p-a^p-b^p = pab\,(a+b)\,((a+b)^2-ab)^{(p-3)/2} + (ab)^3(a+b)^3G(a,b)$. Pour p premier $G(a,b)=pH(a,b)$, G et H polynômes à coefficients entiers.

Lemme 2: pour p premier ≥ 5, x, y et z entiers relatifs premiers entre eux, et solutions de $x^p + y^p = z^p$,
$z = \theta\sigma^p - K\sigma$, avec $(x+y) = \theta\sigma^p$ et $p\sigma \Lambda K = 1$, K et σ entiers relatifs non nuls.
Pour $k \Lambda p = 1$, $\theta = 1$, sinon $p\theta = p^{\alpha p}$.

Lemme 3: pour p premier ≥ 5, x, y et z entiers relatifs premiers entre eux, et solutions de $x^p + y^p = z^p$, alors p divise xyz. Si $p \Lambda xy = 1$, il existe h, X, Y, entiers relatifs premiers entre eux, tels que $p \Lambda hXY = 1$, $XY \neq \pm 1$, et que :
$z = \theta - hXY\,p^{\alpha}$, $y = Y^p + hXY\,p^{\alpha}$, $x = X^p + hXY\,p^{\alpha}$, $x+y = \theta$, $z-x = Y^p$, $z-y = X^p$, avec $p\theta = p^{\alpha p}$.

En trois étapes :
1 / $z = \theta Z^p - hXYZ\,p^{\alpha}$, $y = Y^p + hXYZ\,p^{\alpha}$, $x = X^p + hXYZ\,p^{\alpha}$, $x+y = \theta Z^p$, $z-x = Y^p$, $z-y = X^p$.
2/ **$Z^2 = 1$**.
3/ **p divise z**
Puis conclusion_____

En faisant des calculs, Fermat a du remarquer que pour p impair ≥5 :
$(x+y)^3$ divise **(** $(x+y)^p-x^p-y^p$ **)** - $pxy(x+y)(x^2+y^2+xy)^{(p-3)/2}$, d'où l'intérêt de faire apparaître (x+y) dans z, objet du « petit théorème ». Cela est démontré ci-dessous.

Lemme 1: pour p impair ≥ 5, a et b réels
$(a+b)^p-a^p-b^p = pab\,(a+b)\,((a+b)^2-ab)^{(p-3)/2} + (ab)^3(a+b)^3G(a,b)$. Pour p premier $G(a,b)=pH(a,b)$, G 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, quand p est premier, p divise les $C_p^{\,i}$ (i≠1 et p) donc le second membre.**($)**

On a aussi $(a+b)^p-a^p-b^p=(a+b)\,(\,(a+b)^{p-1}-((a^p+b^p)/(a+b)))$
$(a+b)^p-a^p-b^p = (a+b)(C_{p-1}^{(p-1)/2}-(-1)^{(p-1)/2})\,(ab)^{(p-1)/2}+(a+b)\,\Sigma\,(C_{p-1}^{\,i}-(-1)^i)\,(ab)^i\,(\,a^{(p-1-2i)}+b^{(p-1-2i)})$, i=1 à (p-3)/2, soit
Notons $D_{p-1}^{\,i} = (C_{p-1}^{\,i}-(-1)^i)$, on remarque que $\mathbf{C_{p-1}^{\,2}-1 = p(p-3)/2}$, en posant $(a+b)^p-a^p-b^p = S_p\,ab(a+b)$, on a
$S_p=p(a^{(p-3)}+b^{(p-3)})+(p(p-3)/2)\,ab(a^{(p-5)}+b^{(p-5)})+ab\Sigma D(i,p-1)(ab)^{i-1}(a^{(p-1-2i)}+b^{(p-1-2i)})$, i=3 à (p-1)/2, avec
pour i impair : $a^{2i}+b^{2i}=(a^2+b^2)^i-ab\Sigma C_i^{\,j}\,(ab)^{\,j-1}\,(a^{2(i-j)}+b^{2(i-j)})$, j=1 à (i-1)/2,
pour i pair : $a^{2i}+b^{2i}=(a^2+b^2)^{\mathbf{i}}-(ab\mathbf{\Sigma C_i^{\,j}}\,(ab)^{\,j-1}\,(a^{2(i-j)}+b^{2(i-j)})\,)-C_i^{\,i/2}\,(ab)^{i/2}$,, j=1 à (i/2) -1),
soit $S_p(a,b)$ est un polynôme de (a^2+b^2) et ab, à coefficients entiers et on peut écrire :
$S_p=p(a^2+b^2)^{(p-3)/2}+(p(p-3)/2)ab(a^2+b^2)^{(p-5)/2}+(ab)^2\,F(a,b)$, F polynôme à coefficients entiers.

Supposons $a=\sigma(1+\varepsilon)$ et $b=\sigma(-1+\varepsilon)$, de sorte que $a+b=2\sigma\varepsilon$, $a-b=2\sigma$, alors :
$S_p-p(a^2+b^2+ab)^{(p-3)/2} = (p(p-5)(p-7)/6)\varepsilon^2\sigma^{(p-3)/2}+A\,\varepsilon^4$, donc $(a+b)^2$ divise F(a,b), soit $F(a,b)=(a+b)^2\,G(a,b)$
$a+b=2\sigma\varepsilon$, $a-b=2\sigma$, est une transformation réversible pour des réels, (sauf a+b=0), donc G(a,b) est à coefficients réels. Deux polynômes sont égaux si leurs coefficients sont égaux, de l'égalité
$(a+b)^p-a^p-b^p=pab(a+b)(a^2+b^2+ab)^{(p-3)/2}+(ab)^3(a+b)^3G(a,b)$, vraie pour des réels donc pour tout entier, on déduit que G(a,b) est un polynôme à coefficients entiers.
En utilisant la remarque initiale **($),** p impair premier divise G et on obtient le lemme.

Philippe AJASSE 11/2012

THEOREME DE FERMAT « à la Fermat » pour p ≥ 5

Lemme 2: pour p premier ≥ 5, x, y et z entiers relatifs premiers entre eux, et solutions de $x^p + y^p = z^p$,
$z = \theta\sigma^p - K\sigma$, avec $(x+y) = \theta\sigma^p$ et $p\sigma \wedge K = 1$, K et σ entiers relatifs non nuls.
Pour $k \wedge p = 1$, $\theta = 1$, sinon $p\theta = p^{\alpha p}$.

Pour p premier ≥3, on peut supposer qu'il existe 3 nombres x,y,z premiers entre eux (donc xyz ≠0) tels que
(1) $x^p + y^p = z^p$
la racine p-ième de 2 n'étant pas entière, on peut aussi supposer **$zx, xy, yz \neq \pm 1$.**
le petit théorème de Fermat (les coefficients ≠1 de $(x+y)^p$ sont divisibles par p) donne
$z = x + y - kp^\alpha$, $\alpha \geq 1$ tel que $k \wedge p = 1$(premiers entre eux). Montrons que **$k \neq 0$** .
Comme 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 $z \leq -1/2$ 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 $xy(x+y) = 0$.
(1) s'écrit
$$x^p + y^p - (x+y)^p = (x+y-kp^\alpha)^p - (x+y)^p \text{ ou } (kp^\alpha)^p = (x+y-kp^\alpha)^p - (x+y)^p + (kp^\alpha)^p + (x+y)^p - x^p - y^p \text{ (A-B, A, -B)},$$
en utilisant le lemme 1 deux fois
$$k^p p^{\alpha p} = -pkp^\alpha (x+y)z(z^2 + kp^\alpha(x+y))^{(p-3)/2} - p(kp^\alpha)^3 z^3 (x+y)^3 H(x+y,-kp^\alpha) + pxy(x+y)((x+y)^2 - xy)^{(p-3)/2} + px^3y^3(x+y)^3 H(x,y)$$
en simplifiant par p,
$$k^p p^{\alpha p-1} = -kp^\alpha (x+y)z(z^2 + kp^\alpha(x+y))^{(p-3)/2} + xy(x+y)((x+y)^2 - xy)^{(p-3)/2} + (x+y)^3 (x^3y^3 H(x,y) - (kp^\alpha)^3 z^3 H(x+y,-kp^\alpha))$$
pour p≥ 5, $((p-3)/2) \geq 1$, $(x+y)^2$ divise $k^p p^{\alpha p-1} + kp^\alpha (x+y) z^{p-2} + (x+y)(-xy)^{(p-1)/2}$
ou $k^p p^{\alpha p-1} - (x+y)(kp^\alpha)^{p-1} + (x+y)(-xy)^{(p-1)/2}$.
(2) pour p≥ 5, $k^p p^{\alpha p-1} - (x+y)(kp^\alpha)^{p-1} + (x+y)(-xy)^{(p-1)/2} = (x+y)^2 h(x,y,k)$,
h polynôme à coefficients entiers.
donc $(x+y)$ divise $(kp^\alpha)^p$,($x + y \neq 0$ sinon z =0).

• Supposons **$p \wedge (x+y) = 1$** et $(x+y) \neq \pm 1$. Si k= ±1, (2) donne $(x+y)$ divise $p^{\alpha p-1}$. Si $(x+y) \neq \pm 1$, alors $k \neq \pm 1$ et $(x+y)$ divise k^p . 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**, (de $k \neq \pm 1$ on a $st \neq \pm 1$) on peut écrire :
$k = K s^c t^e$ (avec **$K \wedge pst = 1$**), $(x+y) = S s^b t^d$ (avec **$S \wedge pst = 1$**),par définition du pgcd : **$S \wedge K = 1$**
(2) devient : $S s^b t^d (-xy)^{(p-1)/2} + K^p s^{pc} t^{pe} p^{\alpha p-1} - S s^b t^d (K s^c t^e p^\alpha)^{p-1} = (S s^b t^d)^2 h(x,y,k)$
$S s^b t^d (-xy)^{(p-1)/2} + K^p s^{pc} t^{pe} p^{\alpha p-1} - S K^{p-1} s^{b+c(p-1)} t^{d+e(p-1)} p^{\alpha(p-1)} = (S s^b t^d)^2 h(x,y,k)$
$pc \geq b$, sinon s divise K^p, de même $pe \geq d$. On a aussi S divise $K^p p^{\alpha p-1}$,comme $S \wedge Kp = 1$, $S = \pm 1$.
en divisant par x +y: $(-xy)^{(p-1)/2} + K^p s^{pc-b} t^{pe-d} p^{\alpha p-1} - K^{p-1} s^{(p-1)c} t^{(p-1)e} p^{\alpha(p-1)} = s^b t^d h(x,y,k)$
$x \wedge y = 1$et $xy \neq \pm 1$, donc $(x+y) \wedge xy = 1$ et $st \wedge xy = 1$, or $st \neq \pm 1$, donc pc=b et pe=d, c'est-à-dire :
$k = K s^c t^e$, $(x+y) = (s^c t^e)^p$, pour $(x+y) = \pm 1$, $(x+y) = (\pm 1)^p$, k= ±1K, cela reste vrai.
(3) Si $p \wedge (x+y) = 1$, $k = K\sigma$ et $(x+y) = \sigma^p$, $p\sigma \wedge K = 1$, $p \wedge \sigma = 1$.
• Supposons p divise (x +y). Alors $(x+y) = Sp^\delta$, $\delta \geq 1$, tel que $S \wedge p = 1$.(2) devient
$Sp^\delta (-xy)^{(p-1)/2} + k^p p^{\alpha p-1} - S p^\delta (kp^\alpha)^{p-1} = (S p^\delta)^2 h(x,y,k)$, comme $S \wedge \delta = 1$, $\delta = \alpha p - 1$, on a
$S(-xy)^{(p-1)/2} + k^p - S k^{p-1} p^{\alpha(p-1)} = S^2 p^{\alpha p-1} h(x,y,k)$, on est ramené au problème précédent.
On a $k = K s^c t^e$, $S = (s^c t^e)^p$, au total $k = K\sigma$ et $(x+y) = p^{\alpha p-1}\sigma^p$, $p\sigma \wedge K = 1$
(4) Si p divise (x +y), $k = K\sigma$ et $(x+y) = p^{\alpha p-1}\sigma^p$, $p\sigma \wedge K = 1$, $p \wedge \sigma = 1$
le lemme 2 est ainsi démontré.

Lemme 3: pour p premier ≥ 5, x, y et z entiers relatifs premiers entre eux, et solutions de $x^p + y^p = z^p$, alors p divise xyz. Si $p \wedge xy = 1$, il existe h, X, Y, entiers relatifs premiers entre eux, tels que $p \wedge hXY = 1$, $XY \neq \pm 1$, et que :
$z = \theta - hXY p^\alpha$, $y = Y^p + hXY p^\alpha$, $x = X^p + hXY p^\alpha$, $x + y = \theta$, $z - x = Y^p$, $z - y = X^p$,
avec $p\theta = p^{\alpha p}$.

THEOREME DE FERMAT « à la Fermat » pour p ≥ 5

• 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 du lemme 2 sont remplies et

$x + y = \theta Z^p$, $z = Z(\theta Z^{p-1} - K p^{\alpha})$ $K \Lambda p Z = 1$, $p \Lambda Z = 1$ $\theta=1$ pour $p \Lambda z = 1$, $p^{\alpha p-1}$ sinon.

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

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

les égalités de la seconde colonne donnent **X, Y et Z premiers entre eux et p Λ XY Z =1**, et :

$z - x - y = -K Z p^{\alpha} = HY p^{\beta} = L X p^{\gamma}$, de $KHLXYZ \Lambda p = 1$, on déduit $\alpha = \beta = \gamma$. X, Y et Z étant premiers entre eux, il existe h entier tel que $hXYZ = HY = L X = -KZ$, $h \Lambda pXYZ = 1$. Au bilan

$z = \theta Z^p - hXYZ p^{\alpha}$, $y = Y^p + hXYZ p^{\alpha}$, $x = X^p + hXYZ p^{\alpha}$, $x + y = \theta Z^p$, $z - x = Y^p$, $z - y = X^p$.

• Supposons X=Y, alors x=y. Si X=-Y, de $x = X^p + hXYZ p^{\alpha} = z - Y^p$, $z = hXYZ p^{\alpha}$, donc $2hXY p^{\alpha} = \theta Z^{p-1}$, selon θ, soit p divise Z, soit p divise hXY, contrairement aux hypothèses. Donc $XY \neq \pm 1$.

• Posons **u= hXY ,** on a $z = \theta Z^p - uZp^{\alpha} = X^p + Y^p + uZp^{\alpha}$, **$x^p + y^p = z^p$** s'écrit :

$(X^p + uZp^{\alpha})^p + (Y^p + uZp^{\alpha})^p = (X^p + Y^p + uZp^{\alpha})^p$, en développant :

$(uZp^{\alpha})^p = (X^p + Y^p)^p - (X^{pp} + Y^{pp}) + puZp^{\alpha}((X^p + Y^p)^{p-1} - X^{p(p-1)} - Y^{p(p-1)}) +$

$p(p-1)/2\ (uZp^{\alpha})^2((X^p + Y^p)^{(p-2)} - X^{p(p-2)} - Y^{p(p-2)}) + \ldots$

$(uZp^{\alpha})^3$ divise : $(X^p + Y^p)^p - (X^{pp} + Y^{pp}) + puZp^{\alpha}((X^p + Y^p)^{p-1} - X^{p(p-1)} - Y^{p(p-1)}) +$

$p(p-1)/2\ (uZp^{\alpha})^2((X^p + Y^p)^{(p-2)} - X^{p(p-2)} - Y^{p(p-2)})$

or $(X^p + Y^p)^p = (\theta Z^p - 2uZp^{\alpha})^p = Z^p(\theta Z^{p-1} - 2up^{\alpha})^p$, et :

$(X^p + Y^p)^p - (X^{pp} + Y^{pp}) = p X^p Y^p (X^p + Y^p) \big(((X^p + Y^p)^2 - X^p Y^p)^{(p-3)/2} + X^{2p} Y^{2p} (X^p + Y^p)^2 H(X^p, Y^p)\big)$.

$(X^p + Y^p)^{(p-2)} - X^{p(p-2)} - Y^{p(p-2)} = (p-2) X^p Y^p (X^p + Y^p) \big(((X^p + Y^p)^2 - X^p Y^p)^{(p-5)/2} + X^{2p} Y^{2p} (X^p + Y^p)^2 J(X^p, Y^p)\big)$.

Z^3 divise : $puZp^{\alpha}((X^p + Y^p)^{p-1} - X^{p(p-1)} - Y^{p(p-1)})$, et Z^2 divise : $up^{\alpha+1}((X^p + Y^p)^{p-1} - X^{p(p-1)} - Y^{p(p-1)})$.

Pour a et b réels, n entier :

$a^{n+2} + b^{n+2} = (a+b)^2(a^n + b^n) - 2ab(a^n + b^n) - a^2 b^2 (a^{n-2} + b^{n-2})$, d'où par récurrence :

$(a+b)^{2n} - (a^{2n} + b^{2n}) = ab(a+b)^2 C(a,b) - 2(-1)^n a^n b^n$, C(a,b) polynôme à coefficients entiers, on a donc :

Z^2 divise : $2(-1)^{(p-1)/2} up^{\alpha+1} (X^p Y^p)^{(p-1)/2} = 2h(-1)^{(p-1)/2} XYp^{\alpha+1} (X^p Y^p)^{(p-1)/2}$, or $Z \Lambda hpXY = 1$, 2 non carré, **donc $Z^2 = 1$**. Si (x,y,z) est solution de (1), (-x,-y,-z) est aussi solution. **On peut choisir Z =1.**

• Supposons $p \Lambda xyz = 1$. On vient d'obtenir en raisonnant sur Z : x + y =1,, de même, en raisonnant sur X, on aurait $X^2 = 1$, ou $z = y \pm 1 = 1 - x \pm 1$, il reste $z = 2 - x$, soit X =1, et sur Y, $Y^2 = 1$, $z = x \pm 1$, ou $2x = 2 \pm 1$, ce qui est incompatible, de toute façon $XY \neq \pm 1$. Donc **p divise z**, ce qui finit de démontrer le lemme 3.

Conclusion

• Il reste $p\theta = p^{\alpha p}$, ou p divise $z.(X^p + up^{\alpha})^p + (Y^p + up^{\alpha})^p = (X^p + Y^p + up^{\alpha})^p$, en développant :

$(up^{\alpha})^p = (X^p + Y^p)^p - (X^{pp} + Y^{pp}) + pup^{\alpha}((X^p + Y^p)^{p-1} - X^{p(p-1)} - Y^{p(p-1)}) +$

$p(p-1)/2\ (up^{\alpha})^2((X^p + Y^p)^{(p-2)} - X^{p(p-2)} - Y^{p(p-2)}) + \ldots + p(p-1)/2\ (up^{\alpha})^{(p-2)}((X^p + Y^p)^2 - X^{2p} - Y^{2p})$

$(X^p + Y^p)^p - (X^{pp} + Y^{pp}) = p X^p Y^p (X^p + Y^p) \big(((X^p + Y^p)^2 - X^p Y^p)^{(p-3)/2} + X^{2p} Y^{2p} (X^p + Y^p)^2 H(X^p, Y^p)\big)$.

$(X^p + Y^p)^{(p-2)} - X^{p(p-2)} - Y^{p(p-2)} = (p-2) X^p Y^p (X^p + Y^p) \big(((X^p + Y^p)^2 - X^p Y^p)^{(p-5)/2} + X^{2p} Y^{2p} (X^p + Y^p)^2 J(X^p, Y^p)\big)$.

$(X^p + Y^p)^p = (p^{\alpha p-1} - 2up^{\alpha})^p = p^{\alpha p}(p^{\alpha p(p-1)-1} - 2u)^p$, donc :

$X^p Y^p p^{\alpha(p-2i)}$ divise les termes impairs d'exposant p-2i. Or, $(a+b)^{2n} - (a^{2n} + b^{2n}) = ab(a+b)^2 C(a,b) - 2(-1)^n a^n b^n$,

$((X^p + Y^p)^{p-1-2i} - X^{p(p-1-2i)} - Y^{p(p-1-2i)}) = X^p Y^p (X^p + Y^p)^2 C(X^p, Y^p) - 2(-1)^{(p-1-2i)/2} (X^p Y^p)^{(p-1-2i)/2}$, on a :

$(hp^{\alpha})^p = Ap^{\alpha p} + pup^{\alpha}(Bp^{2\alpha} - 2(-1)^{(p-1-2i)/2} (X^p Y^p)^{(p-3-2i)/2}) + C(up^{\alpha})^2 p^{\alpha(p-2)} + \ldots + p(p-1)(up^{\alpha})^{(p-2)}$,

donc : $p^{3\alpha}$ divise : $2up^{\alpha+1}(X^p Y^p)^{(p-3)/2}$, $p^{2\alpha-1}$ divise : $2h(XY)^{(p-1)(p-2)/2}$, **ce qui contredit p Λ hXY =1.**

On a donc p Λ z =1. On peut conclure :

Pour p premier ≥ 5, x, y et z entiers relatifs, les solutions de $x^p + y^p = z^p$, sont toutes du type xyz = 0.

Philippe AJASSE 11/2012

THEOREME DE FERMAT « à la Fermat » pour $p \geq 5$

Philippe AJASSE 11/2012