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

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

Lemme 1: pour p impair ≥ 5, a et b réels
$(a+b)^p-a^p-b^p = pab\,(a+b)\,((a+b)^2-ab)^{(p-3)/2} + (ab)^3(a+b)^3J(a,b)$.
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, 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
$S_p=p(a^{(p-3)}+b^{(p-3)})+(p(p-3)/2)\,ab(a^{(p-5)}+b^{(p-5)})+\Sigma D(i,p-1)(ab)^{i-1}(a^{(p-1-2i)}+b^{(p-1-2i)})$, i=3 à (p-1)/2, avec
$a^{2i}+b^{2i}=(a^2+b^2)^i-\Sigma C_i^{\,j}\,(ab)^j\,(a^{2(i-j)}+b^{2(i-j)})$, j=1 à i/2 ou (i-1)/2, $-C_i^{\,i/2}\,(ab)^{i/2}$ pour i pair, soit
$S_p=p(a^2+b^2)^{(p-3)/2}+(p(p-3)/2)ab(a^2+b^2)^{(p-5)/2}+a^2b^2(a^2+b^2)^{(p-7)/2}....=p(a^2+b^2+ab)^{(p-3)/2}+(ab)^2\,F(a,b)$, F polynôme à coefficient entiers.

Supposons $a=\sigma(1+\varepsilon)$ et $b=\sigma(-1+\varepsilon)$, 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
$(a+b)^p-a^p-b^p=pab(a+b)(a^2+b^2+ab)^{(p-3)/2}+(ab)^3(a+b)^3G(a,b)$, G(a,b) polynôme à coefficients entiers.
En utilisant la remarque initiale **($),** p impair premier divise G et on obtient le lemme.

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 $k\,\Lambda\,p = 1$, θ = 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 ≠ ±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 $k\,\Lambda\,p=1$(premiers entre eux). Montrons que **k ≠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 $z \le -1/2$ 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
$x^p + y^p - (x+y)^p = (x+y-kp^{\alpha})^p - (x+y)^p$ ou $(kp^{\alpha})^p = (x+y-kp^{\alpha})^p - (x+y)^p + (kp^{\alpha})^p + (x+y)^p - x^p - y^p$,
en utilisant le lemme 1 deux fois
$k^p\,p^{\alpha p} = -pkp^{\alpha}(x+y)z(z^2-kp^{\alpha}(x+y))^{(p-3)/2} - p(kp^{\alpha})^3z^3(x+y)^3\,H(x+y,-kp^{\alpha}) + pxy(x+y)((x+y)^2-xy)^{(p-3)/2}$
$+ px^3y^3(x+y)^3\,H(x,y)$
en simplifiant par p,
$k^p\,p^{\alpha p-1} = -kp^{\alpha}(x+y)z(z^2-kp^{\alpha}(x+y))^{(p-3)/2} + xy(x+y)((x+y)^2-xy)^{(p-3)/2} + (x+y)^3\,(x^3y^3H(x,y) - (kp^{\alpha})^3z^3H(x+y,-kp^{\alpha}))$
pour p≥ 5, ((p-3)/2) ≥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 ≠ 0 sinon z =0).

• Supposons **$p\,\Lambda\,(x+y) =1$** et (x +y) ≠ ±1. Si k= ±1, (2) donne (x +y) divise $(p^{\alpha})^p$. Si (x +y) ≠ ±1, alors k= ±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**, (on a st ≠ ±1) on peut écrire :
$k=K\,s^c\,t^e$ (avec **$K\,\Lambda\,pst =1$**), $(x+y) = S\,s^b\,t^d$ (avec **$S\,\Lambda\,pst =1$**),par définition du pgcd : **$S\,\Lambda\,K =1$**

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

(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 $(x+y) = \pm 1$, $(x+y) = (\pm 1)^p$, $k = \pm 1K$, 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.

Conclusion

• Posons par permutation (p impair) **$p \wedge xy = 1$**, 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

$x+y = \theta Z^p$,	$z = Z(\theta Z^{p-1} - K p^\alpha)$	$K \wedge p Z = 1$, $p \wedge Z = 1$ $\theta = 1$ pour $p \wedge z = 1$, $p^{\alpha p-1}$ sinon.
$z - x = Y^p$,	$y = Y(Y^{p-1} - H p^\beta) = z - X^p$,	$H \wedge pY = 1$, $p \wedge Y = 1$
$z - y = X^p$,	$x = X(X^{p-1} - L p^\gamma) = z - Y^p$,	$L \wedge pX = 1$, $p \wedge X = 1$

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

$-z + X^p + Y^p = YH p^\beta = XL p^\gamma$,on en déduit $\beta = \gamma$ et J tel que $JXY = YH = XL$, $J \wedge XY = 1$, alors

$z - (X^p + Y^p) = -JXYp^\beta$, soit $z = (X^p + Y^p) - JXYp^\beta$.$X^p + Y^p = 2(z - x - y)$, $z = x + y + JXYp^\beta$, il vient

$JXYp^\beta .= -K Z p^\alpha$), on en déduit $\beta = \alpha$ et h tel que $hXYZ = JXY = -KZ$, $h \wedge XYZ = 1$. Au bilan

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

On avait au début :

$k^p p^{\alpha p-1} = -kp^\alpha (x+y) z(z^2 - kp^\alpha (x+y))^{(p-3)/2} + xy(x+y)((x+y)^2 - xy)^{(p-3)/2} + (x+y)^3 (x^3 y^3 H(x,y) - (kp^\alpha)^3 z^3 H(x+y, -kp^\alpha))$

qui devient :

$(hXYZ\, p^\alpha)^p / p = -hXYZ\, p^\alpha (x+y) z(z^2 - hXYZ\, p^\alpha (x+y))^{(p-3)/2} - (hXYZ\, p^\alpha)^3 z^3 (x+y)^3\, H(x+y, -hXYZ\, p^\alpha) +$
$xy(x+y)((x+y)^2 - xy)^{(p-3)/2} + (x+y)^3 x^3 y^3 H(x,y)$

$(hXYZ\, p^\alpha)^p / p = -hXYZ\, p^\alpha (x+y) z(z^2 - hXYZ\, p^\alpha (x+y))^{(p-3)/2} - (hXYZ\, p^\alpha)^3 z^3 (x+y)^3\, H(x+y, -hXYZ\, p^\alpha) + ((x+y)^p - z^p)/p.$

Or $(x+y) = z + hXYZ\, p^\alpha$, alors $((x+y)^p - z^p)/p = z^{p-3} hXYZ\, p^\alpha (z^2 + (p-1)/2\, z\, hXYZ\, p^\alpha + (p-1)(p-2)/6 (hXYZ\, p^\alpha)^2) + ...$

$z(z^2 - hXYZ\, p^\alpha (x+y))^{(p-3)/2} = z^{p-4} (z^2 - (p-3)/2\, z\, hXYZ\, p^\alpha + ((p-3)/2\, hXYZ\, p^\alpha)^2) + ...$

$(x+y) z(z^2 - hXYZ\, p^\alpha (x+y))^{(p-3)/2} = z^{p-3} (z^2 - (p-5)/2\, z\, hXYZ\, p^\alpha + (p-3)(p-5)/2\, (hXYZ\, p^\alpha)^2) + ...$

$(hXYZ\, p^\alpha)^p / p = z^{p-2} (hXYZ\, p^\alpha)^2 ((p-1)/2 + (p-5)/2) + ...$Soit :

$(hXYZ\, p^\alpha)^p / p = (p-3)\, z^{p-2} (hXYZ\, p^\alpha)^2 + z^{p-3} (hXYZ\, p^\alpha)^3\, U(z, hXYZ\, p^\alpha)$. U polynôme à coefficients entiers.

Supposons $p \wedge (x+y) = 1$, soit $p \wedge z = 1$, alors $\theta = 1$ et $x + y = Z^p$, l'égalité précédente devient :

$(x+y)(hXY\, p^\alpha)^p / p = z^{p-2} (hXYZ\, p^\alpha)^2 (p-3) + z^{p-3} (hXYZ\, p^\alpha)^3\, U(z, hXYZ\, p^\alpha)$

on voit que $p^{\alpha(p-3)}$ divise $z^{p-2} (hXYZ)^2 (p-3) = (Z^p - hXYZ\, p^\alpha)^{p-2} (hXYZ)^2 (p-3)$, ce qui contredit $p \wedge hXY Z = 1$.

On a donc **p divise z.** Comme on avait supposé $p \wedge x y = 1$, plus généralement, **p divise xyz.**

Il reste $\theta = p^{\alpha p-1}$ et $(x+y)(hXY)^p = (p-3)\, z^{p-2} (hXYZ\, p^\alpha)^2 + z^{p-3} (hXYZ\, p^\alpha)^3\, U(z, hXYZ\, p^\alpha)$,

soit $(hXY)^{p-2}$ divise $(Z^p - hXYZ\, p^\alpha)^{p-2} (Z\, p^\alpha)^2 (p-3)$, ce qui contredit $hXY \wedge pZ = 1$.

Cependant, on a supposé tacitement $hXY \neq \pm 1$. Si $X = Y$, $z - x = Y^p$, $z - y = X^p$, alors $x = y$,

si $X = -Y$, $2z = x + y = 2(x + y - hXYZ\, p^\alpha)$, donc $x + y = 2hXYZ\, p^\alpha = p^{\alpha p-1} Z^p$, or $p \wedge hXY = 1$, donc $hXY = \pm 1$, alors

$\pm 2 = p^{\alpha(p-1)-1} Z^{p-1}$. On a bien $hXY \neq \pm 1$. 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