

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

En faisant des calculs, Fermat a du remarquer que pour p impair ≥ 5 :

$(x+y)^3$ divise $((x+y)^p - x^p - y^p) - px y(x+y)(x^2 + y^2 + xy)^{(p-3)/2}$, 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

$$(a+b)^p - a^p - b^p = pab(a+b) \left((a+b)^2 - ab \right)^{(p-3)/2} + (ab)^3 (a+b)^3 J(a,b).$$

Pour p premier $J(a,b) = p H(a,b)$, J et H polynômes à coefficients entiers.

On a $(a+b)^p - a^p - b^p = \sum C_p^i (ab)^i (a^{(p-2i)} + b^{(p-2i)})$, $i=1$ à $(p-1)/2$, quand p est premier, p divise les C_p^i ($i \neq 1$ et p) donc le second membre. (\$)

On a aussi $(a+b)^p - a^p - b^p = (a+b) \left((a+b)^{p-1} - \frac{(a^p + b^p)}{(a+b)} \right)$
 $(a+b)^p - a^p - b^p = (a+b) \left(C_{p-1}^{(p-1)/2} (-1)^{(p-1)/2} (ab)^{(p-1)/2} + (a+b) \sum (C_{p-1}^i (-1)^i (ab)^i (a^{(p-1-2i)} + b^{(p-1-2i)}), i=1 \text{ à } (p-3)/2 \right)$, soit
 Notons $D_{p-1}^i = (C_{p-1}^i (-1)^i)$, on remarque que $C_{p-1}^2 - 1 = p(p-3)/2$, en posant $(a+b)^p - a^p - b^p = S_p ab(a+b)$, on a
 $S_p = p(a^{(p-3)} + b^{(p-3)}) + (p(p-3)/2) ab(a^{(p-5)} + b^{(p-5)}) + \sum D(i,p-1)(ab)^{i-1} (a^{(p-1-2i)} + b^{(p-1-2i)})$, $i=3$ à $(p-1)/2$, avec
 $a^{2i} + b^{2i} = (a^2 + b^2)^i - \sum C_i^j (ab)^j (a^{2(i-j)} + b^{2(i-j)})$, $j=1$ à $i/2$ ou $(i-1)/2$, $-C_i^{i/2} (ab)^{i/2}$ pour i pair, soit
 $S_p = p(a^2 + b^2)^{(p-3)/2} + (p(p-3)/2) ab(a^2 + b^2)^{(p-5)/2} + a^2 b^2 (a^2 + b^2)^{(p-7)/2} \dots = p(a^2 + b^2 + ab)^{(p-3)/2} + (ab)^2 F(a,b)$, F polynôme à coefficient entiers.

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

donc $(a+b)^2$ divise $F(a,b)$, soit

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

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 $p \sigma \wedge K = 1$, K et σ entiers relatifs non nuls.

Pour $k \wedge p = 1$, $\theta = 1$, sinon $p \theta = p^{ap}$.

Pour p premier ≥ 3 , on peut supposer qu'il existe 3 nombres x, y, z premiers entre eux (donc $xyz \neq 0$) 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 $\neq 1$ de $(x+y)^p$ sont divisibles par p) donne

$z = x + y - kp^a$, $a \geq 1$ tel que $k \wedge p = 1$ (premiers entre eux). Montrons que $k \neq 0$.

Comme $y \neq 0$, 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 $n \geq 1$:

$g_{2n}(z)$ 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

$$x^p + y^p - (x+y)^p = (x+y-kp^a)^p - (x+y)^p \text{ ou } (kp^a)^p = (x+y-kp^a)^p - (x+y)^p + (kp^a)^p + (x+y)^p - x^p - y^p,$$

en utilisant le lemme 1 deux fois

$$k^p p^{ap} = -pkp^a (x+y)z(z^2 - kp^a(x+y))^{(p-3)/2} - p(kp^a)^3 z^3 (x+y)^3 H(x+y, -kp^a) + pxy(x+y)((x+y)^2 - xy)^{(p-3)/2} + px^3 y^3 (x+y)^3 H(x,y)$$

en simplifiant par p ,

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

pour $p \geq 5$, $((p-3)/2) \geq 1$, $(x+y)^2$ divise $k^p p^{ap-1} + kp^a (x+y)z^{p-2} + (x+y)(-xy)^{(p-1)/2}$

ou $k^p p^{ap-1} - (x+y)(kp^a)^{p-1} + (x+y)(-xy)^{(p-1)/2}$.

$$(2) \text{ pour } p \geq 5, k^p p^{ap-1} - (x+y)(kp^a)^{p-1} + (x+y)(-xy)^{(p-1)/2} = (x+y)^2 h(x,y,k),$$

h polynôme à coefficients entiers.

donc $(x+y)$ divise $(kp^a)^p$, ($x+y \neq 0$ sinon $z=0$).

• Supposons $p \wedge (x+y) = 1$ et $(x+y) \neq \pm 1$. Si $k = \pm 1$, (2) donne $(x+y)$ divise $(p^a)^p$. Si $(x+y) \neq \pm 1$, alors $k = \pm 1$ et $(x+y)$ divise k^p . On décompose en facteurs premiers : $\text{pgcd}(x+y, k) = s^u t^v$ (pour la clarté on limite à deux facteurs), puis k et $x+y : s$ et t étant premiers, (on a $st \neq \pm 1$) on peut écrire :

$$k = K s^c t^e \text{ (avec } K \wedge \text{pst} = 1), (x+y) = S s^b t^d \text{ (avec } S \wedge \text{pst} = 1), \text{ par définition du pgcd : } S \wedge K = 1$$

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

(2) devient : $S s^b t^d (-xy)^{(p-1)/2} + K^p s^{pc} t^{pe} p^{ap-1} - S s^b t^d (K s^c t^e p^a)^{p-1} = (S s^b t^d)^2 h(x,y,k)$

$S s^b t^d (-xy)^{(p-1)/2} + K^p s^{pc} t^{pe} p^{ap-1} - S K^{p-1} s^{b+c(p-1)} t^{d+e(p-1)} p^{a(p-1)} = (S s^b t^d)^2 h(x,y,k)$

$pc \geq b$, sinon s divise K^p , de même $pe \geq d$. On a aussi S divise $K^p p^{ap-1}$, comme $S \wedge Kp = 1$, $S = \pm 1$.

en divisant par $x+y$: $(-xy)^{(p-1)/2} + K^p s^{pc-b} t^{pe-d} p^{ap-1} - K^{p-1} s^{(p-1)c} t^{(p-1)e} p^{a(p-1)} = s^b t^d h(x,y,k)$

$x \wedge y = 1$ 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

$Sp^\delta (-xy)^{(p-1)/2} + k^p p^{ap-1} - S p^\delta (kp^a)^{p-1} = (S p^\delta)^2 h(x,y,k)$, comme $S \wedge \delta = 1$, $\delta = ap-1$, on a

$S(-xy)^{(p-1)/2} + k^p - S k^{p-1} p^{a(p-1)} = S^2 p^{ap-1} h(x,y,k)$, 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 $(x+y) = p^{ap-1} \sigma^p$, $p \sigma \wedge K = 1$

(4) Si p divise $(x+y)$, $k = K \sigma$ et $(x+y) = p^{ap-1} \sigma^p$, $p \sigma \wedge K = 1$, $p \wedge \sigma = 1$

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

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

$z-x = Y^p$, $y = Y(Y^{p-1} - H p^b) = z - X^p$, $H \wedge p Y = 1$, $p \wedge Y = 1$

$z-y = X^p$, $x = X(X^{p-1} - L p^c) = z - Y^p$, $L \wedge p X = 1$, $p \wedge X = 1$

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

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

$z - (X^p + Y^p) = -JXY p^b$, soit $z = (X^p + Y^p) - JXY p^b$. $X^p + Y^p = 2(z - x - y)$, $z = x + y + JXY p^b$, il vient

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

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

On avait au début :

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

qui devient :

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

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

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

$z(z^2 - hXYZ p^a(x+y))^{(p-3)/2} = z^{p-4}(z^2 - (p-3)/2 z hXYZ p^a + ((p-3)/2 hXYZ p^a)^2) + \dots$

$(x+y)z(z^2 - hXYZ p^a(x+y))^{(p-3)/2} = z^{p-3}(z^2 - (p-5)/2 z hXYZ p^a + (p-3)(p-5)/2 (hXYZ p^a)^2) + \dots$

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

$(hXYZ p^a)^p / p = (p-3) z^{p-2} (hXYZ p^a)^2 + z^{p-3} (hXYZ p^a)^3 U(z, hXYZ p^a)$. 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 :

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

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

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

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

$p^{a(p-1)} Z^p (hXY)^p = (p-3) z^{p-2} (hXYZ p^a)^2 + z^{p-3} (hXYZ p^a)^3 U(z, hXYZ p^a)$,

$z = p^a Z (p^{a(p-1)-1} Z^p - hXY)$, donc $p^{a(p-1)} Z^p (hXY)^p = (p-3) (p^a Z)^p (hXY)^2 (p^{a(p-1)-1} Z^p - hXY)^{p-2} +$

$+ z^{p-3} (hXYZ p^a)^3 U(z, hXYZ p^a) = (p^a Z)^p ((p-3)(hXY)^2 (p^{a(p-1)-1} Z^p - hXY)^{p-2} + (hXY)^3 V(Z, hXY, p^a))$.

soit $p^{a(p-1)} Z^p (hXY)^p = (p^a Z)^p (hXY)^2 ((p-3) (p^{a(p-1)-1} Z^p - hXY)^{p-2} + (hXY) V(Z, hXY, p^a))$.

donc **p divise (hXY)^{p-2}**, ce qui contredit $p \wedge hXY = 1$. 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 $xyz = 0$.