On peut aussi procéder comme dans 1) et remarquer que l'existence du p.p.c.m. de u et v équivaut à celle d'une *borne inférieure* de Au et Av dans l'ensemble ordonné des idéaux fractionnaires principaux; or celle-ci est $Au \cap Av$.

III. Deux éléments a, b *de* A sont dits *étrangers* (ou *premiers entre eux*) si 1 est un de leurs p.g.c.d. Rappelons l'important LEMME D'EUCLIDE. *Soient a, b, c des éléments d'un anneau principal* A; *si a divise bc et est étranger à b, alors a divise c.*

Démonstration succinte : par Bezout (2), on a a' et $b' \in A$ tels que $1 = a'a + b'b$; d'où $c = a'ac + b'bc$; comme a divise chaque terme du second membre, il divise c.

IV. Enfin on a l'importante « décomposition en facteurs premiers » :

THÉORÈME. *Étant donnés un anneau principal* A *et son corps des fractions* K, *il existe une partie* P *de* A *telle que tout* $x \in K$ *s'écrive de façon unique*

6. $$x = u \prod_{p \in P} p^{v_p(x)}$$

où u est un élément inversible de A, *et où les exposants* $v_p(x)$ *sont des éléments de* **Z**, *tous nuls sauf un nombre fini d'entre eux.*

Pour un exposé plus systématique de ces questions, nous renvoyons le lecteur à [1], *Algèbre*, chap. VI, § 1 et chap. VII, § 1. Une partie de la théorie (plus précisément tout ce qui ne tourne pas autour de l'identité de Bezout) s'étend à des anneaux plus généraux que les anneaux principaux, à savoir les anneaux *factoriels*; voir [7], ou [2] Algèbre commutative, chap. VII, § 3.

1.2. Un exemple : les équations $x^2 + y^2 = z^2$ et $x^4 + y^4 = z^4$

Une des parties les plus attirantes de la Théorie des Nombres est l'étude des *équations diophantiennes*. Il s'agit d'équations polynômes $P(x_1, \ldots, x_n) = 0$ à coefficients dans **Z** (resp. dans **Q**), dont on cherche les solutions (x_i) en nombres entiers (resp. en nombres rationnels). On peut remplacer **Z** (resp. **Q**) par des anneaux A (resp. des corps K) plus généraux; nous en verrons un exemple plus tard (§ 6).

Nous allons étudier ici deux cas particuliers de la fameuse *équation de Fermat:*

1. $x^n + y^n = z^n$.

Fermat a affirmé avoir démontré que, pour $n \geqslant 3$, cette équation n'a pas de solution (x, y, z) en nombres entiers tous non-nuls; sa démonstration n'a pas été retrouvée. De très nombreux mathématiciens ont, depuis, intensément travaillé sur ce problème, et montré que l'affirmation de Fermat est vraie pour un grand nombre de valeurs de l'exposant n; cependant aucune démonstration générale (i. e. valable pour tout n) n'a été trouvée.

L'opinion aujourd'hui la plus courante est que, dans sa « démonstration », Fermat avait commis une erreur, mais une erreur digne de ce mathématicien de premier ordre. Par exemple il aurait pu avoir l'idée (géniale pour son époque) d'opérer dans l'anneau des entiers du corps des racines n-ièmes de l'unité, et avoir cru que cet anneau est toujours principal. En effet, on sait démontrer l'assertion de Fermat pour tout exposant n tel que cet anneau soit principal; mais il ne l'est pas pour tout n; bien plus, pour n premier, cet anneau n'est principal que pour un nombre fini de valeurs de n [1].

Pour $n = 2$, l'équation (1) a des solutions entières, par exemple (3,4,5). On peut en donner une description complète :

THÉORÈME 1. *Si x, y, z sont des entiers $\geqslant 1$ tels que $x^2 + y^2 = z^2$, il existe un entier d et des entiers étrangers u, v tels que (à une permutation près de x et y) on ait:*

2. $x = d(u^2 - v^2) \qquad y = 2\,duv \qquad z = d(u^2 + v^2)$

Un calcul facile montre que les formules (2) donnent des solutions de $x^2 + y^2 = z^2$. Réciproquement soient x, y, z des entiers $\geqslant 1$ tels que $x^2 + y^2 = z^2$. Quitte à diviser x, y, z par leur p.g.c.d., on peut les supposer étrangers dans leur ensemble; ils sont alors étrangers deux à deux, car, si, par exemple, x et z ont un facteur premier commun p, alors p divise $y^2 = z^2 - x^2$ et donc y. En particulier deux des nombres x, y, z sont impairs, et le troisième est nécessairement pair. Les nombres x et y ne peuvent être tous deux impairs, car sinon, on aurait $x^2 \equiv 1 \pmod{4}$, $y^2 \equiv 1 \pmod{4}$ d'où $z^2 \equiv 2 \pmod{4}$ contrairement au fait que z^2 est un carré. On a donc, après échange éventuel de x et y.

3. x impair, y pair, z impair.

Écrivons l'équation

4. $y^2 = z^2 - x^2 = (z - x)(z + x)$.

Comme le p.g.c.d. de $2x$ et de $2z$ est 2, et que $2x = (z + x) - (z - x)$ et $2z = (z + x) + (z - x)$, le p.g.c.d. de $z - x$ et $z + x$ ne peut être que 2. Posons $y = 2y'$, $z + x = 2x'$, $z - x = 2z'$, où y', x', z' sont des entiers, car $y, z + x$ et $z - x$ sont pairs par (3). On a alors $y'^2 = x'z'$. Comme x' et z' sont étrangers, la décomposition en facteurs premiers de y'^2 montre que x' et z' sont des *carrés* u^2 et v^2 : en effet tout facteur premier de y'^2 va, avec son exposant pair, soit tout entier dans x', soit tout entier dans z'. On a donc $z + x = 2u^2$, $z - x = 2v^2$, $y^2 = 2u^2 . 2v^2$, d'où $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$. Ici u et v sont étrangers, sinon x, y, z auraient un facteur premier commun. On en déduit (2) en remultipliant par d le p.g.c.d. CQFD.

1. Voir C. L. Siegel — « Gesammelte Werke », t. III, p. 436-442.

THÉORÈME 2. *L'équation* $x^4 + y^4 = z^2$ *n'a pas de solution en nombres entiers* $x, y, z \geqslant 1$.

Raisonnons par l'absurde. On a alors une solution (x, y, z) où z est *minimal*. Pour celle-ci, x, y et z sont étrangers deux à deux : en effet, si par exemple, x et y avaient un facteur premier commun p, alors p^4 diviserait z^2, donc p^2 diviserait z, et $\left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2}\right)$ serait une solution contredisant la minimalité de z; les deux autres cas sont analogues et plus faciles. Comme notre équation s'écrit $(x^2)^2 + (y^2)^2 = z^2$, on peut lui appliquer le th. 1 : après permutation éventuelle de x et y, on voit qu'on a des entiers $u, v \geqslant 1$ et étrangers tels que

5. $x^2 = u^2 - v^2, \qquad y^2 = 2uv, \qquad z = u^2 + v^2.$

Comme $4 | y^2$, la relation $y^2 = 2uv$, montre que l'un des deux nombres u et v est pair; l'autre est nécessairement impair; la répartition « u pair, v impair » donne $u^2 \equiv 0 \pmod 4$, $v^2 \equiv 1 \pmod 4$, d'où $x^2 = u^2 - v^2 \equiv -1 \pmod 4$ ce qui est absurde; donc u est impair et $v = 2v'$. La relation $y^2 = 4uv'$ et le fait que u et v' sont étrangers montrent que u et v' sont des carrés a^2 et b^2. Appliquons encore le th. 1, cette fois à l'équation $x^2 + v^2 = u^2$ (cf. (5)); comme x et u sont impairs, v pair, et x, v, u étrangers deux à deux, on a des entiers étrangers $c, d \geqslant 1$ tels que :

6. $x = c^2 + d^2, \qquad v = 2cd, \qquad u = c^2 + d^2.$

Or, de $v = 2v' = 2b^2$, on déduit $cd = b^2$, de sorte que c et d sont encore des carrés x'^2 et y'^2, car ils sont étrangers. Comme $u = a^2$, la dernière équation (6) s'écrit

7. $a^2 = x'^4 + y'^4$

et a la *même forme* que l'équation donnée. Mais, on a, par (5), $z = u^2 + v^2 = a^4 + 4b^4 > a^4$, d'où $z > a$, ce qui contredit le caractère minimal de z. Notre assertion est donc démontrée

Une légère variante de notre démonstration montre que, étant donnée une solution (x, y, z) en entiers $\geqslant 1$ de $x^4 + y^4 = z^2$, on construit une suite (x_n, y_n, z_n) de telles solutions, où la suite (z_n) est strictement décroissante, ce qui est absurde. Ceci est la méthode de *descente infinie*, due à Fermat.

COROLLAIRE. *L'équation* $x^4 + y^4 = z^4$ *n'a pas de solution en nombres entiers* $x, y, z \geqslant 1$.

En effet cette équation s'écrit $x^4 + y^4 = (z^2)^2$, et on applique le th. 2.

1.3. Quelques lemmes sur les idéaux; l'indicateur d'Euler

Soit $n \geqslant 1$ un entier naturel. On appelle *indicateur d'Euler* de n, et on note $\varphi(n)$ le nombre des entiers q premiers à n et tels que $0 \leqslant q \leqslant n$ (il