ARITHMÉTIQUE DE BASE

Choukri Saad, Dahmouni Mohammed

Janvier, 2020

Table des matières

0.1 Division euclidienne, algorithme d'Euclide

En arithmétique des entiers, la division euclidienne ou division entière est une opération qui, à deux entiers naturels appelés dividende et diviseur, associe deux autres entiers appelés quotient et reste. Initialement définie pour deux entiers naturels non nuls, elle se généralise aux entiers relatifs. Cette division est au fondement des théorèmes de l'arithmétique élémentaire et de l'arithmétique modulaire qui traite des congruences sur les entiers.

0.1.1 Division euclidienne dans $\mathbb{N}, \mathbb{Z}$

Soient a et $b > 0$ deux entiers naturels, il existe un unique couple d'entiers naturels (q, r) tel que

$$a = bq + r$$

et $0 \leq r \leq b - 1$. L'entier q et r sont appelés respectivement le reste et le quotient de la division euclidienne de a par b.

➳ Ce théorème parait naturel, en effet en fixant deux entiers naturels $b > 0$ et a, on commence par 0 pour atteindre a, puis on ajoute un b, puis un autre b jusqu'à ce qu'on arrive un un certain à rang q tel que $bq \leq a < (b+1)q$, ce q est le premier terme qu'on cherche et on pose $r = a - bq$, on a bien $0 \leq r = a - bq < b$ (c'est à dire $0 \leq r \leq b - 1$).
On donne par la suite une démonstration du théorème rigoureuse qui se base sur une propriété propriété portant sur les entiers naturels.

DÉMONSTRATION. Soit $A = \{p \in \mathbb{N} \mid pb \leq a\}$. On a $0 \in A$, donc A est une partie de $\mathbb{N}$ non vide. De plus elle est majorée par a car $p \leq pb \leq a$. Elle admet donc un plus grand élément qu'on notera q. Alors $q \in A$ et $q + 1 \notin A$, il vient $qb \leq a < (q + 1)b$ et par suite $0 \leq a - bq \leq b - 1$, on pose $r = a - bq$, on a alors $0 \leq r \leq b - 1$. D'où l'existence de (q, r). Passons à l'unicité. Soit (q_1, r_1) un couple vérifiant $a = bq_1 + r_1$. Sans perte de généralité, on suppose que $q \geq q_1$. Si $q > q_1$, alors $q - q_1 \geq 1$ et par suite $r_1 - r = b(q - q_1) \geq b$, mais $0 \leq r \leq r_1 \leq b$, donc $q = q_1$ et il vient $r_1 = r$. D'où l'unicité.

Soient a et $b > 0$ deux entiers naturels. Montrer que

$$\text{pgcd}(a, b) = \text{pgcd}(a, a - b)$$

DÉMONSTRATION. Soient a et $b > 0$ deux entiers naturels. On pose $d_1 = \text{pgcd}(a, b)$ et $d_2 = \text{pgcd}(a, a - b)$. Montrons que d_1 divise d_2 et que d_2 divise d_1. On sait que d_1 divise a et b, donc d_1 divise a et $a - b$, par conséquent d divise le pgcd de a et $a - b$ qui vaut d_2. D'autre part, d_2 divise a et $a - b$, donc d_2 divise $a - (a - b) = b$ et par la suite, finalement d_2 divise a et b, donc d_2 divise leur pgcd qui vaut d_1. D'où le résultat.

Soient a et $b > 0$ deux entiers naturels et $a = bq + r$ la division euclidienne de a par b, alors on a

$$a \wedge b = b \wedge r$$

DÉMONSTRATION. On utilise le résultat de la proposition précédente en la appliquant plusieurs fois, plus précisément

$$\text{pgcd}(a, b) = \text{pgcd}(b, a) = \text{pgcd}(b, a - b) = \text{pgcd}(b, a - 2b) = \ldots = \text{pgcd}(b, a - qb) = \text{pgcd}(b, r)$$

➳ En applications, on utilise souvent ce résultat pour montrer que deux nombres sont premiers entre eux, ou plus généralement pour déterminer le pgcd de deux entiers naturels.

Déterminer le plus grand commun diviseurs des deux nombres 186 et 39.

SOLUTION. On écrit $186 = 4 \times 39 + 30$ puis $39 = 30 \times 1 + 9$, puis $30 = 3 \times 9 + 3$ et ensuite $9 = 3 \times 3 + 0$, donc

$$3 = 0 \wedge 3 = 3 \wedge 9 = 9 \wedge 30 = 30 \wedge 39 = 39 \wedge 186$$

Finalement, le plus grand commun diviseur des deux nombres 186 et 39 est 3.

➳ Notons que le pgcd est le dernier reste non nul dans la succession des divisions euclidiennes établie.

Montrer que pour tout entier naturel n, les deux entiers $n^{2019} + 2$ et $n^2 - n + 1$ sont premiers entre eux.

SOLUTION. Si $n = 0, 1$, c'est évident. Supposons que $n \geq 2$, on remarque $2019 = 3 \times 673$ est un multiple de 3 qui est de plus impair, on écrit alors (puisque 673 est impair)

$$n^{2019} + 2 = \left(n^3\right)^{673} + 1 + 1 = (n^3 + 1)Q(n) + 1 = T(n)(n^2 - n + 1) + 1$$

où $Q(n)$ et $T(n)$ des expressions polynomiales en fonction de n. Puisque, on a $0 \leq 1 < n^2 - n + 1$, alors 1 est le reste de la division euclidienne de $n^{2019} + 2$ par $n^2 - n + 1$, donc

$$(n^{2019} + 2) \wedge (n^2 - n + 1) = (n^2 - n + 1) \wedge 1 = 1$$

D'où le résultat.

➳ On a utilisé l'identité

$$a^n + b^n = (a + b)(a^{n-1} - ba^{n-2} + \ldots - b^{n-1})$$

vraie pour tout entier naturel n impair et tout nombres réels a et b.

Soient $b > 0$ et a deux entiers naturels tels que q_1 le quotient de la division euclidienne de a par b, q_2 le quotient de la division euclidienne de $2a$ par b et q_3 le quotient de la division euclidienne de $2a + b$ par $2b$. Montrer que

$$q_2 = q_1 + q_3$$

SOLUTION. Soient $a = bq_1 + r_1$, $2a = bq_2 + r_2$ et $2a + b = 2bq_3 + r_3$ les divisions euclidienne respectives de a par b, de $2a$ par b et $2a + b$ par $2b$. D'une part $2a + b = 2bq_3 + r_3$ et d'autre part

$$2a + b = 2(bq_1 + r_1) + b = (2q_1 + 1)b + 2r_1$$

Donc,

$$bq_2 + r_2 = b(2q_1) + 2r_1, \qquad (*)$$

Par la suite, on obtient

$$2bq_3 + r_3 = 2bq_1 + 2r_1 + b, \qquad (**)$$

Puisque $0 \leq 2r_1 < 2b$, alors ou bien $0 \leq 2r_1 < b$ ou $b \leq 2r_1 < 2b$. Plaçons nous dans le premier cas, l'unicité du quotient et du reste de la division euclidienne permet de tire de $(*)$, $q_2 = 2q_1$ et puisque $0 \leq 2r_1 + b < 2b$ et $0 \leq r_3 < 2b$, alors $(**)$ entraîne $q_1 = q_3$. D'où $q_2 = q_1 + q_3$. Le second cas entraîne $0 \leq 2r_1 - b < b$, et on réécrit $(*)$ sous la forme

$$bq_2 + r_2 = b(2q_1 + 1) + 2r_1 - b$$

Donc $q_2 = 2q_1 + 1$, et on réécrit $(**)$ sous la forme

$$2bq_3 + r_3 = 2b(q_1 + 1) + 2r_1 - b$$

Donc, par unicité du quotient on trouve $q_3 = q_1 + 1$. Donc $q_2 = q_1 + q_3$. En conclusion, dans tous les cas, on a

$$q_2 = q_1 + q_3$$

Soient $x, y > 0$ deux entiers naturels. Montrer que le plus petit entier naturel non nul k tel que y divise kx est un diviseur de y.

SOLUTION. Il s'agit de montrer que le reste de la division euclidienne de y par k est nul. Soit $y = kq + r$ la division euclidienne de y par k. On remarque que

$$rx = (y - kq)x = yx - q \times kx$$

Donc, rx est une combinaison linéaire de deux multiple yx et kx de y, rx est donc un multiple de y, mais $r \geq 0$ est inférieur strictement à k (d'après le théorème de la division euclidienne), donc r est nul puisque k est le plus petit entier naturel non nul tel que y divise kx.

Soient $a \geq 2$ un entier naturel et m et n deux entiers naturels non nuls. Montrer que

$$a^n - 1 \wedge a^m - 1 = a^m - 1 \wedge a^r - 1$$

où r est le reste de la division euclidienne de n par m.

SOLUTION. L'identité souhaitée ressemble à une identité qu'on a déjà énoncé et qu'on a montré. On procède d'une manière analogue, on montre que si $n = mq + r$ la division euclidienne de n par m,

$$a^n - 1 \wedge a^m - 1 = a^{mq+r} - 1 \wedge a^m - 1 = a^{(m-1)q+r} - 1 \wedge a^m - 1$$

Notons $\Delta_1 = a^{mq+r} - 1 \wedge a^m - 1$ et $\Delta_2 = a^{(m-1)q+r} - 1 \wedge a^m - 1$. Montrons que Δ_1 divise Δ_2 et que Δ_2 divise Δ_1. De même on montre que a et Δ_1 sont premiers entre eux. Montrons maintenant que Δ_2 divise Δ_1. On a Δ_2 divise $a^{(m-1)q+r} - 1$ et $a^m - 1$, donc il divise leur produit

$$\left(a^{(m-1)q+r} - 1\right)\left(a^m - 1\right) = a^{mq+r} - 1 - \left(a^m - 1\right) - \left(a^{m(q-1)+r} - 1\right)$$

Donc, Δ_2 divise $a^{mq+r} - 1$, par conséquent Δ_2 divise Δ_1 le pgcd de $a^m - 1$ et $a^{mq+r} - 1$. On montre de manière similaire que Δ_1 divise Δ_2. Finalement, on a montré que

$$a^{mq+r} - 1 \wedge a^m - 1 = a^{(m-1)q+r} - 1 \wedge a^m - 1$$

Donc

$$a^n - 1 \wedge a^m - 1 = a^{mq+r} - 1 \wedge a^m - 1 = a^{(m-1)q+r} - 1 \wedge a^m - 1 = a^{(m-2)q+r} - 1 \wedge a^m - 1 = \ldots = a^r - 1 \wedge a^m - 1$$

D'où le résultat.

Soient $a \geq 2$ un entier naturel et m et n deux entiers naturels non nuls. Montrer que

$$a^n - 1 \wedge a^m - 1 = a^{n \wedge m} - 1$$

DÉMONSTRATION. Soit $n = mq + r$ la division euclidienne de n par m. On sait que

$$a^n - 1 \wedge a^m - 1 = a^m - 1 \wedge a^r - 1 = a^r - 1 \wedge a^{r_1} - 1$$

où r_1 est le reste de la division euclidienne de m par r, de même

$$a^n - 1 \wedge a^m - 1 = a^m - 1 \wedge a^r - 1 = a^r - 1 \wedge a^{r_1} - 1 = a^{r_1} - 1 \wedge a^{r_2} - 1$$

où r_2 est le reste de la division euclidienne de r par r_1, et ainsi de suite jusqu'à annuler l'exposant de a, on trouve alors en notons z le dernier reste non nul de cette succession de divisions euclidiennes,

$$a^n - 1 \wedge a^m - 1 = a^m - 1 \wedge a^r - 1 = a^r - 1 \wedge a^{r_1} - 1 = a^{r_1} - 1 \wedge a^{r_2} - 1 = a^z - 1 \wedge a^0 - 1 = a^z - 1$$

Sachant que le dernier reste non nul z présente le pgcd de n et m, on a bien

$$a^n - 1 \wedge a^m - 1 = a^{n \wedge m} - 1$$

ce qui achève la preuve.

0.1.2 Théorème de Bezout

L'identité de Bezout affirme que deux nombres entiers x et y sont premiers entre eux si et seulement si le 1 est une combinaison linéaire de x et y. On donne par la suite un exemple illustratif.

Montrer que les deux nombres 26 et 57 sont premiers entre eux et déterminer deux entiers relatifs u et v vérifiant

$$26u + 57v = 1$$

SOLUTION. On utilise l'algorithme d'Euclide pour montrer que 57 et 26 sont premiers entre eux. On écrit $57 = 2\times 26+5$ puis $26 = 5 \times 5 + 1$, donc en remontant on obtient

$$1 = 26 - 5 \times 5 = 26 - 5 \times (57 - 2 \times 26) = 26 + 10 \times 26 - 5 \times 57 = 11 \times 26 - 5 \times 57$$

Donc le couple $(u, v) = (11, -5)$ convient.

De manière générale, on énonce (sans démonstration) le théorème dit de Bezout.

Soient x et y deux entiers relatifs. Alors x et y sont premiers entre eux si et seulement s'il existe un couple d'entiers relatifs (u, v) tel que

$$ux + vy = 1$$

➳ La preuve de l'implication réciproque dans le théorème de Bezout est évidente. Pour l'implication directe, on utilise une remonté de l'algorithme d'Euclide comme dans l'exemple précédent.

Il résulte du théorème de Bezout la proposition suivante,

Soient x et y deux entiers relatifs et d leur plus grand commun diviseur, alors d est une combinaison linéaire de x et y, autrement dit, il existe un couple d'entiers relatifs (u, v) tel que

$$ux + vy = d$$

DÉMONSTRATION. Puisque d est le plus grand diviseur commun de x et y, alors il existe a et b deux entiers relatifs tels que $x = ad$ et $y = bd$ et de plus $a \wedge b = 1$. Les deux entiers a et b étant premiers eux, le théorème de Bezout assure l'existence d'un couple d'entiers (u', v') vérifiant $au' + bv' = 1$, en multipliant les deux côtés de cette égalité par d, on obtient l'existence d'un couple d'entiers $(u, v) = (du', dv')$ tel que $ux + vy = d$. D'où le résultat.

➳ Attention ! Dans cette proposition, on n'a pas d'équivalence comme dans le théorème de Bezout.

Pour tout entier naturel non nul n, on pose

$$a_n = 2 \times 10^n + 1 \qquad \text{et} \qquad b_n = 2 \times 10^n - 1$$

Déterminer un couple d'entier relatifs (u, v) vérifiant

$$u \times a_n + v \times b_n = 1$$

SOLUTION. On utilise le remonté de l'algorithme d'Euclide pour déterminer le couple d'entiers relatifs (u, v), on a

$$a_n = 2 \times 10^n + 1 = 2 \times (10^n - 1) + 2 = 1 \times b_n + 2$$

Et on a aussi

$$b_n = 2 \times 10^n - 1 = 2 \times (10^n - 1) + 1$$

Donc en remontant

$$1 = b_n - 2 \times (10^n - 1) = b_n - (a_n - b_n)(10^n - 1) = 10^n b_n - (10^n - 1)a_n$$

Donc, le couple $(u, v) = \big(-(10^n - 1), 10^n\big)$ convient.

Soient a, b et c trois entiers relatifs tels que a divise bc, si a et b sont premiers entre eux, alors a divise c.

DÉMONSTRATION. Les deux entiers a et b sont premiers entre eux, donc d'après le théorème de Bezout, il existe deux entiers u et v tels que $au + bv = 1$, en multipliant par c les deux côtés de l'égalité, on trouve $acu + bcv = c$, sachant que acu et bcv sont des multiples de a, alors c est un multiple de a. D'où le résultat.

Soient x et y deux entiers tels que $2x + 1$ divise $8y$. Montrer que $2x + 1$ divise y.

SOLUTION. On sait que $2x + 1$ est un nombre impair qui divise $8y$, donc $2x + 1$ divise y puisque $2x + 1 \wedge 8 = 1$.

Soient a et b deux entiers relatifs et p un nombre premier divisant ab, alors p divise a ou b.

DÉMONSTRATION. Supposons que p ne divise pas a, alors p et a sont premiers entre eux, mais p divise ab, donc d'après le théorème de Gauss, p divise b. On montre de même qui si p ne divise pas b, alors p divise a. D'où le résultat.

➳ Ce résultat peut être généralisée pour un produit fini ; si un nombre premier p divise un produit d'entiers relatifs, alors p divise nécessairement un parmi eux.

Soient a, b et c trois entiers relatifs tels que a divise c, b divise c et $a \wedge b = 1$, alors ab divise c.

DÉMONSTRATION. Puisque a divise c, alors $c = ak$ pour un entier k, mais on sait que b divise $c = ak$, donc et que b et a sont premiers entre eux, donc par le théorème de Gauss, b divise k, mais $c = ak$, donc ab divise c.

Montrer que $n^3 - n$ est divisible par 6 pour tout entier relatif n.

SOLUTION. Soit n un entier relatif, celui-ci possède la même parité que n^3, donc $n^3 - n$ est pair, autrement dit 2 divise $n^3 - n$. D'autre pat, on remarque que

$$n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1) = (n - 1)n(n + 1)$$

Donc, $n^3 - n$ est le produit de trois entiers consécutifs, sachant que parmi trois entiers consécutifs, on trouve toujours un qui est multiple de 3, alors 3 divise $n^3 - n$. Finalement, on a montré que 2 divise $n^3 - n$ et 3 divise $n^3 - n$ et puisque l'on a 2 et 3 premiers entre eux, alors $6 = 2 \times 3$ divise $n^3 - n$.

Soient x et y deux entiers naturels ≥ 2 premiers entre eux. Il existe un unique couple d'entiers naturels (u_0, v_0) tel que

$$u_0 x - v_0 y = 1$$

DÉMONSTRATION. Les deux entiers naturels x et $y \geq 2$ étant premiers entre eux, le théorème de Bezout assure l'existence de $u_1, v_1 \in \mathbb{Z}$ tels que $u_1 x - v_1 y = 1$. Soit $u_1 = qy + r$ la division euclidienne de u_1 par y, on obtient $1 = (qy + r)x - v_1 y = rx - (v_1 - qx)y = u_0 x - v_0 y$ avec $u_0 = r$ et $v_9 = v_1 - qx$. De l'égalité $(v_1 - qx)y = rx - 1 \geq -1$, or $(v_1 - qx)y$ ne peut pas être égal à -1 puisque y est ≥ 2 par hypothèse. Donc $v_0 = (v_1 - qx)y \geq 0$. Le couple d'entiers

naturels (u_0, v_0) convient donc.
Montrons par la suite que le couple (u_0, v_0) est unique. Soit alors (u'_0, v'_0) un couple vérifiant la même propriété que (u_0, v_0) vérifie. On a alors $(u'_0 - u_0)x = (v'_0 - v_0)y$, ceci montre que a divise $b|u'_0 - u_0|$, mais a et b sont premiers entre eux, donc d'après le théorème de Gauss, on peut déduire que a divise $|u'_0 - u'_0|$, sachant que $0 \leq |u'_0 - u'_0| \leq a-1$, donc $|u'_0 - u_0| = 0$, par conséquent $u'_0 = u_0$, et de même on trouve $v'_0 = v_0$, les couples (u_0, v_0) et (u'_0, v'_0) sont alors identiques. D'où l'unicité.

Soit a un entier relatif, montrer que pour tout entier naturels n et m, on a

$$a^n - 1 \wedge a^m - 1 = a^{n \wedge m} - 1$$

SOLUTION. Si l'un des deux entiers n et m divise l'autre. Par exemple, n divise m. Montrons que

$$a^n - 1 \wedge a^m - 1 = a^n - 1$$

On écrit $m = kn$, on a alors

$$a^m - 1 = a^{kn} - 1 = (a^n - 1)(1 + a^n + a^{2n} + \ldots + a^{(k-1)n})$$

Donc $a^n - 1$ divise $a^m - 1$ et par la suite, on a le résultat. Supposons maintenant que aucun des deux entiers naturels n et m ne divise l'autre, de sorte que le pgcd de n et m est différent de n et de m. Écrivons alors $n = d\alpha$ et $m = d\beta$ où $d = \text{pgcd}(n, m)$, de $d \neq n, m$ on peut tirer que $\alpha \geq 2$ et $\beta \geq 2$, et de plus on sait que α et β sont premiers entre eux. Donc α et β remplissent les conditions de la proposition précédente. Il résulte qu'il existe un couple d'entiers naturels (u', v') tel que $u'\alpha = v'\beta + 1$. En multipliant par d, les deux côtés de cette égalité, on déduit l'existence d'un couple (u, v) d'entiers naturels vérifiant $nu = mv + d$, il s'agit de montrer que

$$a^n - 1 \wedge a^m - 1 = a^d - 1$$

On montre que chacun des membres des deux côtés de cette égalité divise l'autre. On sait déjà que le côté de droite divise le côté de gauche puisque l'on peut écrire par exemple

$$a^n - 1 = a^{\alpha d} - 1 = (a^d - 1)(1 + a^d + a^{2d} + \ldots + a^{(\alpha-1)d}), \qquad (*)$$

Par la suite, $a^d - 1$ divise $a^n - 1$, de même on montre que $a^d - 1$ divise $a^m - 1$. Donc, $a^d - 1$ divise le pgcd de $a^n - 1$ et $a^m - 1$. Montrons maintenant que Δ divise $a^d - 1$ où Δ est le pgcd de $a^n - 1$ et $a^m - 1$. On sait que Δ divise $a^n - 1$, donc Δ divise $a^{nu} - 1$ par le même argument utilisé dans $(*)$. Donc Δ divise $a^{mv+d} - 1$, mais on sait que Δ divise $a^{mv} - 1$ (par le même argument que dans $(*)$), donc Δ divise la différence

$$a^{mv+d} - 1 - (a^{mv} - 1) = a^{mv+d} - a^{mv} = a^{mv}(a^d - 1)$$

mais Δ et a sont premiers entre eux puisque l'on a Δ divise $a^m - 1$ (si $z = \Delta \wedge a$, alors z va diviser $a^n - 1$ et a^n, donc z divisera 1, d'où $z = 1$), Finalement Δ divise $a^d - 1$. Ceci permet de conclure.

Soient a et b deux entiers relatifs et n et m deux entiers naturels. Montrer que a et b sont premiers entre eux si et seulement si a^n et b^m sont premiers entre eux.

DÉMONSTRATION. Supposons que a et b sont premiers entre eux et montrons que a^n et b^m sont premiers entre eux. Supposons que a^n et b^m ne sont pas premiers entre eux de sorte qu'il existe un nombre premier p qui les divises tous les deux. Donc p divise a^n et p divise a^m et par la suite p divise a et b et ceci est impossible avec a et b premiers entre eux d'où la condition nécessaire. Réciproquement si a^n et b^m sont premiers entre eux, il existe alors deux coefficients de Bezout u et v vérifiant

$$u \times a^n + v \times b^m = 1$$

En posant $U = ua^{n-1}$ et $V = vb^{m-1}$, on déduit l'existence de deux entiers U et V vérifiant $aU + bV = 1$, donc par le théorème de Bezout, les deux entiers a et b sont premiers entre eux.

0.2 L'équation $ax + by = c$

Dans cette section nous allons voir une résolution de l'équation

$$(E), \quad ax + by = c$$

en $(x, y) \in \mathbb{Z}^2$ avec a, b et c des entiers donnés. Nous allons pas faire une étude générale de l'équation, mais plutôt nous allons nous baser sur des exemples en pratique pour savoir résoudre ce genre d'équations.

Trouver tous les couples d'entiers relatifs (x, y) vérifiant

$$(E) \qquad 2x + 3y = 1$$

SOLUTION. On remarque facilement que le couple $(-1, 1)$ est une solution particulière. Et on écrit en considérant le couple (x, y) comme solution particulière de l'équation (E), $2x + 3y = -2 + 3$, alors

$$2(x + 1) = 3(1 - y), \qquad (*)$$

, donc 2 divise $3(1 - y)$ et puisque 2 et 3 sont premiers entre eux, alors par le théorème de Gauss, on déduit que 2 divise $y - 1$ et alors, il existe $k \in \mathbb{Z}$ tel que $y - 1 = 2k$, autrement dit il existe $k \in \mathbb{Z}$ tel que $y = 2k + 1$. En substituant dans $(*)$, on trouve $x + 1 = -3(k$, autrement dit, on a $(x, y) = (-3k - 1, 2k + 1)$ pour un certain entier relatif k. Réciproquement, on a

$$2(-3k - 1) + 3(2k + 1) = -6k - 2 + 6k + 3 = 1$$

vraie pour tout entier relatif k. Donc l'ensemble des solutions de l'équation (E) est

$$\{(-3k - 1, 2k + 1)/ \quad k \in \mathbb{Z}\}$$

➳ Remarquer que la solution particulière constitue l'étape fondamentale de résolution de ce type d'équations. Cependant, déterminer une solution particulière n'est pas toujours évident. Souvent, pour des valeurs numériques des coefficients de l'équation, on utilise la remonté d'Euclide qui consiste à faire l'algorithme d'Euclide puis remonter !

Résoudre dans $\mathbb{Z}^2$ l'équation suivante d'inconnu (x, y),

$$(F), \qquad 5x = 3 + 10^{100}y$$

SOLUTION. Suppose que l'équation (F) admet une solution (x, y), on sait que $5x$ et $10^{100}y$ sont divisibles par 5, donc $3 = 5x - 10^{100}y = 3$ est un multiple de 5, ceci est bien évidemment impossible.

➳ L'équation $ax + by = c$ à paramètres entiers admet une solution dans $\mathbb{Z}^2$ si et seulement le pgcd de a et b divise c.

On considère l'équation (G) en (x, y) définie par

$$(G), \qquad 61x - 33y = 1$$

1. Sans utiliser l'algorithme d'Euclide, montrer que l'équation (G) admet une solution.
2. Résoudre dans $\mathbb{Z}^2$ l'équation (G).

SOLUTION.

1. On remarque que 61 est un nombre premier puisque tous les nombres premiers $2, 3, 5, 7$ inférieurs ou égal à $\sqrt{61}$ ne les divises pas. De plus 61 ne divise pas 33, donc 61 et 33 sont premiers entre eux. Donc, le théorème de Bezout garantit l'existence d'une solution de l'équation (G).

2. On commence par chercher une solution particulière de l'équation (G), on utilise l'algorithme d'Euclide, on écrit $61 = 33 + 27$, puis $33 = 27 + 4$, ensuite $27 = 6 \times 4 + 3$ et enfin $4 = 3 + 1$. En remontant, on trouve

$$1 = 4 - 3 = 4 - (27 - 6 \times 4) = 7 \times 4 - 27 = 7 \times (33 - 27) - 27 = 7 \times 33 - 8 \times 27 = 7 \times 33 - 8(61 - 33) = 15 \times 33 - 8 \times 61$$

Donc

$$-8 \times 61 - (-15) \times 31 = 1$$

Finalement, on a trouvé une solution particulière $(-8, -15)$. Ensuite on écrit le 1 de l'équation sous forme de combinaison linéaire des coefficients de l'équation 61 et -33, autrement dit si le couple (x, y) est solution de l'équation (G), alors $61x - 33y = -8 \times 61 - (-15) \times 31$. Ensuite, on factorise pour obtenir

$$61(x + 8) = 33(y + 15), \qquad (*)$$

Par la suite, on obtient que 61 divise $33(y + 15)$, donc par le théorème de Gauss, 61 divise $y + 15$, il s'en suit que $y = 61k - 15$. En substituant y dans $(*)$, on obtient $x + 8 = 33k$, c'est à dire $x = 33k - 8$. Donc, si (x, y) est une solution de l'équation (G), alors il existe $k \in \mathbb{Z}$ tel que $(x, y) = (33k - 8, 61k - 15)$. Réciproquement, on vérifie facilement que tous les couples $(33k - 8, 61k - 15)$ pour $k \in \mathbb{Z}$ sont solutions de l'équation (G). Donc, l'ensemble des solutions de l'équation (G) est

$$S = \{(33k - 8, 61k - 15) / \quad k \in \mathbb{Z}\}$$

0.3 Nombres premiers

0.3.1 Généralités

Un nombre premier est un entier naturel qui admet exactement deux diviseurs distincts entiers et positifs. Ces deux diviseurs sont 1 et le nombre considéré, puisque tout nombre a pour diviseurs 1 et lui-même (comme le montre l'égalité $n = 1 \times n$), les nombres premiers étant ceux qui n'en possèdent aucun autre. On a déjà prouvé dans ce cours que l'ensemble des nombres premiers est infini.

Soient a et n deux entiers ≥ 2. Montrer que si $a^n - 1$ est un nombre premier, alors $a = 2$ et n est un nombre premier.

SOLUTION. Montrons d'abord que $a = 2$, si jamais on avait $a \geq 3$, alors $a - 1 \geq 2$ et alors l'entier $M_n = a^n - 1 = (a - 1)(a^{n-1} + \ldots + 1)$ ne sera pas premier et on déduit que $a = 2$. Montrons maintenant que n est premier. Supposons par absurde qu'il existe $2 \leq x, y \leq n - 1$ tels que $n = xy$. Donc

$$M_n = 2^n - 1 = 2^{xy} - 1 = (2^x - 1)(2^{x(y-1)} + \ldots + 1)$$

qui n'est pas premier, ce qui contredit l'hypothèse de départ. Donc n est un nombre premier.

Montrer que tout nombre premier ≥ 5 s'écrit sous la forme $6k - 1$ ou la forme $6k + 1$ où k un entier naturel.

SOLUTION. Soit p un nombre premier, Soit $p = 6k + r$ la division euclidienne de p par 6, on a alors $r \in \{0, 1, 2, 3, 4, 5\}$. Bien évidemment, r doit être différent de $0, 2, 3, 4$, sinon p sera respectivement divisible par $6, 2, 3$ et 2 ce qui contredira le caractère primaire de $p \geq 5$. Donc $r \in \{1, 5\}$, donc $p = 6k + 1$ ou $p = 6k + 5 = 6(k + 1) - 1 = 6k' + 1$ où $k = k + 1$. Donc, p s'écrit sous la forme $6k + 1$ ou $6k - 1$ avec k un entier naturel.

Un entier naturel a est composé (non premier) si et seulement s'il admet un diviseur premier inférieur ou égal à $\sqrt{a}$.

DÉMONSTRATION. Si l'entier admet un diviseur premier inférieur ou égal à $\sqrt{a}$, alors il n'est pas premier. Supposons maintenant que a est un entier composé de sorte qu'il existe deux entiers b et c compris entre 2 et $a - 1$ tels que

$$2 \leq c \leq b \leq a - 1$$

et soit p un diviseur premier de c (il existe puisque $c \geq 2$), le nombre premier p est un diviseur premier de a et de plus $p^2 \leq c^2 \leq bc = a$, d'où $p \leq \sqrt{a}$, donc p convient.

Soit p un entier naturel. Si tous les nombres premiers inférieurs ou égal à $\sqrt{p}$ ne divise pas p, alors p est un nombre premier.

DÉMONSTRATION. Si p n'était pas premier, alors p va admettre un diviseur premier qui lui est inférieur à sa racine d'après la proposition précédente, et ceci est contraire à l'hypothèse sur l'entier naturel p.

➳ Ce critère est pratique pour décider la primalité d'un entier naturel.

Montrer qu'il existe une infinité de nombres premiers de la forme $6k-1$ ou il existe une infinité de nombres premiers de la forme $6k+1$.

SOLUTION. Puisqu'un nombre premier ≥ 5 s'écrit sous la forme $6k-1$ ou $6k+1$, et que l'ensemble des nombres premiers ≥ 5 est infini (puisque l'ensemble des nombres premiers est infini), alors il existe un nombre infini de nombre premiers de la forme $6k-1$ ou il existe un nombre infini de nombres premiers de la forme $6k+1$.

Montrer qu'il existe une infinité de nombre premiers de la forme $4k-1$ pour $k \geq 1$ un entier naturel.

SOLUTION. Notons qu'un nombre premier $k \geq 3$ s'écrit ou bien sous la forme $4k-1$ ou bien sous la forme $4k+1$ pour $k \geq 1$ un entier naturel. Par l'absurde, supposons que les nombres premiers de la forme $4k-1$ (il en existe, par exemple 3) sont en nombre fini $s \geq 1$, notons les $p_1, p_2, \ldots, p_s$. On pose

$$N = 4p_1p_2 \ldots p_s - 1$$

L'entier $N \geq 2$ admet un diviseur premier p de la forme $4k-1$ (en remarquant un produit fini d'entiers de la forme $4k+1$ est lui même de la forme $4k+1$, mais N est de la forme $4k-1$). Malheureusement, p apparaît dans le produit $p_1p_2 \ldots p_s$, donc p divise $4p_1p_2 \ldots p_s$, mais p divise $N = 4p_1p_2 \ldots p_s - 1$, donc p divise 1, ce qui est bien évidemment impossible.

Montrer qu'il existe une infinité de nombre premiers de la forme $6k-1$ pour $k \geq 1$ un entier naturel.

SOLUTION. On utilise le fait qu'un nombre premier sous la forme $6k-1$ ou bien sous la forme $6k+1$. Supposons que les nombres premiers de la forme $6k-1$ (il en existe, par exemple 5). Soit, alors P le plus grand nombre premier de la forme $6k-1$. On pose

$$N = 6P! - 1$$

L'entier $N \geq 2$ admet un diviseur premier p de la forme $6k-1$ (en remarquant un produit fini d'entiers de la forme $6k+1$ est lui même de la forme $6k+1$, mais N est de la forme $6k-1$). Mais p apparaît dans la factorielle $P!$ puisque $p \leq P$, donc p divise $P!$ et par la suite p divise $6P!$, mais p divise $N = 6P! - 1$, d'où l'absurdité.

Montrer que l'entier

$$4^{3^{2019}} + 1$$

n'est pas un nombre premier.

SOLUTION. Il suffit de remarquer que 3^{2019} est un nombre impair, donc

$$4^{3^{2019}} + 1 = (4+1) \times K = 5K$$

Donc notre entier est divisible par 5 est il est supérieur strictement à 5. Alors, l'entier en question n'est pas premier.

Soit p un nombre premier ≥ 5. Montrer que 24 divise $p^2 - 1$.

SOLUTION. On voit facilement que $p^2 - 1$ est divisible par 8 puisque $p = 4k \pm 1$, en levant au carré, on trouve que $p^2 - 1$ est multiple de 8. D'autre part, on a $p = 3k \pm 1$, dans les deux cas $p^2 - 1$ est divisible par 3. Finalement, on a montré que $p^2 - 1$ est divisible par 8 et 3. Par conséquent, $p^2 - 1$ est multiple de $24 = 3 \times 8$.

0.4 Décomposition en facteurs premiers

Le théorème fondamentale de l'arithmétique, appelé également, le théorème de factorisation en facteurs premiers. Ce théorème est d'une importance capitale en théorie des nombres, en effet il permet de résoudre plusieurs situations compliqués.

Tout entier naturel $N \geq 2$ s'écrit d'une manière unique sous la forme

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \qquad (*)$$

où $p_1 < p_2 < \dots < p_k$ des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_k \geq 1$ des entiers naturels.
L'écriture $(*)$ s'appelle la décomposition en facteurs premiers (ou décomposition primaire) de l'entier naturel N.

DÉMONSTRATION. Montrons d'abord l'existence de la décomposition primaire. On procède par récurrence forte. Pour $N = 2$, c'est évident. Supposons que tout entier naturel $n \geq 2$ inférieur ou égal à N admet une décomposition primaire et montrons que $N + 1$, possède une décomposition primaire. Puisque $N + 1$ est $geq2$, alors il admet un diviseur premier qu'on noter p, si $N + 1 = p$, c'est bon. Sinon $(N = 1)/p \geq 2$ et de plus on a $(N + 1)/p \leq N$, donc par hypothèse de récurrence, l'entier $(N + 1)/p$ admet une décomposition primaire, d'où N admet une décomposition primaire.
Montrons maintenant l'unicité de lé décomposition primaire. Soient $N \geq 2$ un entier naturel et k le nombre de ses diviseurs premiers et

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \dots q_k^{\beta_k}$$

deux décompositions primaires de N. On observe que p_1 apparaît dans le produit $q_1^{\beta_1} q_2^{\beta_2} \dots q_k^{\beta_k}$, puisque p_1 est un nombre premier, alors p_1 divise $q_l^{\beta^l}$ pour un certain $l \in \{1, 2, \dots, k\}$, puisque p_1 est un nombre premier, alors p_1 divise q_l. Alors $p_1 = q_l$ puisque p_1 et q_l sont des nombres premiers. De plus α_1 doit être égal à β_l, sinon on aura par exemple (en supposant $\alpha_1 > \beta_l$) la chose suivante ; $p_1^{\alpha_1 - \beta_l}$ va diviser le produit $q_1^{\beta_1} \dots q_{l-1}^{\beta_{l-1}} q_{l+1}^{\beta_{l+1}} \dots q_k^{\beta_k}$ et dans ce dernier produit, $q_l = p_1$ ne figure pas, ceci bien évidemment est impossible. De même, on montre que l'on ne peut pas avoir $\alpha_1 < \beta_l$. De proche en proche, on montre que pour tout indice $i \in \{1, 2, \dots, k\}$, il existe un unique indice $l \in \{1, 2, \dots, k\}$ tel que $(p_i, \alpha_i) = (q_l, \beta_l)$, mais on sait que $p_1 < p_2 < \dots < p_k$ et $q_1 < q_2 < \dots < q_k$. Donc $(p_i, \alpha_i) = (q_i, \beta_i)$ pour tout $i \in \{1, 2, \dots, k\}$. D'où l'unicité de la décomposition primaire.

Soient a et b deux entiers naturels premiers entre eux tels que leur produit ab est un carré parfait. Montrer que a et b sont des carrés parfaits.

SOLUTION. Soit $a = p_1^{\alpha_1} \dots p_l^{\alpha_l}$ et $b = q_1^{\beta}{}_1 \dots p_s^{\alpha_s}$ les décompositions primaires respectives de a et b. On sait que les $p_1, \dots, p_l, q_1, \dots, q_s$ sont deux à deux distincts. Il s'agit donc de montrer que les α_i et les β_j sont des entiers pairs. Ceci est bien évidemment facile à voir par unicité de décomposition primaire de $c = ab$ qui est un carré parfait (car pour tout i et tout j, p_i et q_j apparaît dans la décomposition primaire de c, avec les p_i et q_j ont des exposants α_i et β_j pairs). D'où le résultat.

➳ De même, on montre que si le produit de deux entiers naturels premiers entre eux est une puissance n-ème. Alors, chacun de ces deux entiers est une puissance n-ème.

Existe t-il un entier relatif x vérifiant

$$x + x^3 = 2^{1998} \quad ?$$

SOLUTION. On remarque que $x = 0, 1$ n'est pas une solution bien évidemment, et que les entiers négatifs ne sont pas solutions également. Donc, si x est une solution entière, elle est nécessairement ≥ 2. On remarque que

$$1 \times (x^2 + 1) - x \times x = 1$$

Donc, par le théorème de Bezout, x et $x^2 + 1$ sont premiers entre eux. Or,

$$x(x^2 + 1) = x + x^3 = \left(2^{999}\right)^2$$

un carré parfait, donc d'après ce qui précède x et $x^2 + 1$ sont des carrés parfaits. De plus, il sont différents de 1, et alors il sont tous les deux divisibles par 2, ceci bien évidemment n'est pas possible puisque x et $x^2 + 1$ sont premiers entre eux comme déjà mentionné.

Soit N un entier naturel qui une puissance 2019-ème et une puissance 2021-ème. Montrer qu'il existe un entier naturel n tel que

$$N = n^{4080399}$$

SOLUTION. On commence par remarquer que $4080399 = 2019 \times 2021$. Soient a et b deux entiers naturels tels que $N = a^{2019}$ et $N = b^{2021}$. L'unicité de la décomposition primaire permet de voir que 2019 divise l'exposant α de chaque nombre premier p qui figure dans la décomposition primaire de $N = b^{2021}$, mais $\alpha = 2021\gamma$ où γ l'exposant de p dans la décomposition primaire de b. Donc 2019 divise $\alpha = 2021\gamma$, donc par le théorème de Gauss, il vient que 2019 divise γ. Finalement $b = n^{2019}$ pour un certain entier naturel n, donc

$$N = b^{2021} = n^{2021 \times 2019} = n^{4080399}$$

Donc, n convient.

Décomposer l'entier naturel $N = 27000001$ en facteurs premiers.

SOLUTION. On remarque que

$$N = 27000001 = 300^3 + 1 = (300 + 1)(300^2 - 300 + 1) = 301 \times [(300 + 1)^2 - 900]$$

$$= 301 \times (301^2 - 30^2) = 301 \times 331 \times 271 = 7 \times 43 \times 271 \times 331$$

On vérifie que les facteurs $7, 43, 271$ et 331 sont des nombres premiers par un critère cité précédemment.

Existe t-il un entier relatif x vérifiant l'équation

$$x^2 + x^6 = 8^{1997} \quad ?$$

SOLUTION. Si x est une solution, alors $-x$ est également une solution puisque l'expression $x^2 + x^6$ est paire. Supposons donc que x est une solution qui est positive. Il est facile de voir que x est différent de 0 et de 1 puisque 0 x ne peut pas être impair, puisque x divise $8^{1997} = (2^3)^{1997}$ qui est une puissance de 2, par conséquent x est une puissance de 2, donc x est en particulier pair. De même, on obtient que $x^4 + 1$ est pair (puisque $x^2(1 + x^4) = x^2 + x^6$). Finalement, on a montrer que 2 divise x et $x^4 + 1$, donc 2 divise x^4 et $x^4 + 1$, donc 2 divise leur différence qui vaut 1. Ceci bien sur n'est pas possible, donc l'équation n'admet pas de solution entière.

0.5 Arithmétique modulaire

Avant de commencer cette section, le lecteur doit s'assurer qu'il a bien assimiler la totalité des propriétés et des techniques établies précédemment.

Les congruences sont largement utilisées dans la résolutions de problèmes en théorie des nombres ; plus spécifiquement au monde olympique. Nous allons introduire la notion de congruence modulo un entier, et on illustrera les techniques et les propriétés à travers les exemples et les exercices.

Soient a et b deux entiers relatifs et n un entier non nul. On dit que a est congru à b modulo n et on écrit $a \equiv b \pmod{n}$ si n divise la différence $a - b$. On dit que a et b sont congrus modulo n.

Montrer que

$$4^{2n+1} \equiv 4 \pmod{60}$$

pour tout entier naturel non nul n.

SOLUTION. Il s'agit de montrer que la différence $4^{2n+1} - 4$ est un multiple de 15, on écrit pour un entier naturel non nul n,

$$4^{2n+1} - 4 = 4(4^{2n} - 1) = 4 \times (16^n - 1) = 4 \times (16 - 1)(1 + 16 + 16^2 + \ldots + 16^{n-1}) = 60K$$

où K un entier naturel. Donc 60 divise $4^{2n+1} - 4$, par conséquent $4^{2n+1} \equiv 4 \pmod{60}$.

Soit n un entier naturel qui n'est pas multiple de 3. Montrer que

$$n^2 \equiv 1 \pmod{3}$$

SOLUTION. Soit n un entier naturel qui n'est pas divisible par 3. Il s'agit de montrer que 3 divise $n^2 - 1$. Puisque n n'est pas divisible par 3, alors les restes de la division euclidienne de n par 3 sont 1 ou 2, autrement dit s'écrit sous la forme $n = 3k + 1$ ou sous la forme $n = 3k - 1$. Dans le premier cas, on a

$$n^2 - 1 = (n - 1)(n + 1) = 3k(3k + 1)$$

Et dans le second cas, on a

$$n^2 - 1 = (n - 1)(n + 1) = (3k + 1)(3k + 3) = 3(k + 1)(3k + 1)$$

Dans les deux cas, $n^2 - 1$ est divisible par 3, par conséquent n^2 est congru à 1 modulo 3.

➳ Pour tout entier relatif a et tout entier non nul n, si $a \equiv n \pmod{n}$, alors $a \equiv 0 \pmod{n}$.

La relation de congruence est compatible avec la somme des entiers. Autrement dit, si a, b, c et d sont des entiers relatifs et n un entier non nul et $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors

$$a + c \equiv b + d \pmod{n}$$

DÉMONSTRATION. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors n divise $a - b$ et n divise $c - d$, donc n divise leur somme,

$$(a - b) + (c - d) = (a + c) - (b + d)$$

Donc $a + c \equiv b + d \pmod{n}$.

➳ Le résultat se généralise facilement pour un nombre fini de termes.

Montrer que

$$5 \quad \text{divise} \quad 16^{100} + 16^{200} + 16^{300} + 16^{400} + 16^{500}$$

SOLUTION. Pour $e \in \{1, 2, 3, 4, 5\}$, on a $16^{100e} - 1$ divisible par 5 puisque

$$16^{100e} - 1 = (16 - 1)(1 + 16 + 16^2 + \ldots + 16^{100e-1})$$

Donc, pour tout $e \in \{1, 2, 3, 4, 5\}$, $16^{100e} \equiv 1 \pmod 5$ Alors,

$$16^{100} + 16^{200} + 16^{300} + 16^{400} + 16^{500} \equiv \underbrace{1 + 1 + \ldots + 1}_{5 \text{ fois}} \equiv 5 \equiv 0 \pmod 5$$

La relation de congruence est compatible avec le produit des entiers. Autrement dit, si a, b, c et d sont des entiers relatifs et n un entier non nul et $a \equiv b \pmod n$ et $c \equiv d \pmod n$, alors

$$ac \equiv bd \pmod n$$

DÉMONSTRATION. Il suffit d'écrire la chose suivante,

$$ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b)$$

Puisque n divise $c - d$ et $a - b$, alors n divise $ac - bd$. Donc, $ac \equiv bd \pmod n$.

➳ Le résultat se généralise facilement pour un nombre fini de termes, une conséquence est la suivante.

Soient a et b deux entiers relatifs qui sont congrus modulo $n \in \mathbb{Z}^*$, alors pour tout entier naturel m, a^m et b^m sont congrus modulo n.

Soient a, b, c, a', b', c' six entiers relatifs et $n \in \mathbb{Z}^*$ un entier qui divise les différences $a - a', b - b'$ et $c - c'$. Montrer que n divise la différence $abc - a'b'c'$.

SOLUTION. Il suffit de traduire les données, on écrit

$$a \equiv a' \pmod n, \qquad b \equiv b' \pmod n, \qquad c \equiv c' \pmod n$$

Puisque, la congruence est compatible avec le produit, on a bien $abc \equiv a'b'c' \pmod n$. Donc, n divise $abc - a'b'c'$.

Soit P un polynôme à coefficients entiers, a et b deux entiers et n un entier non nul tel que $a \equiv b \pmod n$, alors

$$P(a) \equiv P(b) \pmod n$$

DÉMONSTRATION. On écrit

$$P = c_l X^l + c_{l-1} X^{l-1} + \ldots + c_1 X + c_0$$

Pour tout $k \in \{0, 1, \ldots, l\}$, on a $a^k \equiv b^k \pmod{n}$, et alors $c_k a^k \equiv c_k b^k \pmod{n}$. En sommant, sur les $k \in \{0, 1, \ldots, l\}$, on trouve

$$P(a) = c_l a^l + c_{l-1} a^{l-1} + \ldots + c_1 a + c_0 \equiv c_l b^l + c_{l-1} b^{l-1} + \ldots + c_1 b + c_0 = P(b) \pmod{n}$$

Déterminer tous les entiers n vérifiant

$$n^2 + 3n + 6 \equiv 0 \pmod{5}$$

SOLUTION. Soit P le polynôme $X^2 + 3X + 6$, On sait que pour tout n, on a $n \equiv 0, 1, 2, 3, 4 \pmod{5}$, donc $n \equiv 0, 1, 2, -2, -1$, par la suite

$$P(n) \equiv P(0), P(1), P(2), P(-2), P(-1) = 6, 10, 16, 4, 4 \equiv 1, 0, 1, 4, 4 \pmod{5}$$

Donc $P(n) \equiv 0 \pmod{5}$ si et seulement si $n \equiv 1 \pmod{5}$. Finalement, l'ensemble des solutions du problème est

$$S = \{5k + 1, \quad k \in \mathbb{Z}\}$$

1. Déterminer suivant les valeurs de l'entier naturel n le reste de la division euclidienne de 2^n par 5.
2. En déduire que $x \equiv 2 \pmod{5}$, alors $1 + x + x^2 + \ldots + x^{2047}$ est divisible par 5.

SOLUTION.

1. On remarque que $2^2 = 4 \equiv -1 \pmod{5}$, donc $2^4 \equiv 1 \pmod{5}$, par la suite $2^{4k} \equiv 1 \pmod{5}$, $2^{4k+1} \equiv 2 \pmod{5}$, $2^{4k+2} \equiv 4 \pmod{5}$ et $2^{4k+3} \equiv 8 \equiv 3 \pmod{5}$. Donc, on obtient comme précédemment, le reste de 2^n modulo 5 suivant les restes de n modulo 4.
2. On remarque que la somme de quatre puissances consécutifs de 2 est congrue à $1 + 2 + 4 + 3 = 10$ modulo 5. Donc, la somme de quatre puissances consécutifs de 2 est divisible par 5 et on écrit pour $x \equiv 2 \pmod{5}$,

$$1 + x + x^2 + \ldots + x^{2047} \equiv \underbrace{(1 + 2 + 2^3 + 2^4)}_{\equiv 0 \pmod{5}} + \ldots + \underbrace{(2^{2044} + 2^{2045} + 2^{2046} + 2^{2047})}_{\equiv 0 \pmod{5}} \equiv 0 \pmod{5}$$

   Puisque on a 2048 termes et 2048 est un multiple de 4.

➳ Souvent, pour déterminer la valeur numérique du reste d'une puissance divisée par un entier, on cherche à faire apparaître un 1 ou -1 puisque les puissance de ces deux entiers sont faciles à déterminer. La première question de l'exercice précédent est un bon exemple.

Soient a et b deux entiers relatifs et n un entier non nul tel que $ab \pmod{n}$, alors pour tout entier non nul c, on a

$$ac \equiv bc \pmod{cn}$$

DÉMONSTRATION. Il suffit de remarquer que si n divise $a - b$, alors cn divise $c(a - b) = ca - cb$.

Soient a et b deux entiers relatifs et n et m deux entiers non nuls premiers entre eux tels que $a \equiv b \pmod{n}$, et $a \equiv b \pmod{m}$

$$a \equiv b \pmod{nm}$$

DÉMONSTRATION. Il suffit de voir que n divise $a-b$ et m divise $a-b$, donc nm divise $a-b$ puisque n et m sont premiers entre eux.

➳ Plus généralement, si $a \equiv b \pmod{n}$, et $a \equiv b \pmod{m}$, alors $a \equiv b \pmod{n \vee m}$.

Montrer que pour tout entier x, l'entier

$$X = x(x+1)(x+2)(x+3)(x+4)(x+5)$$

est divisible par 720.

SOLUTION. L'entier X est produit de 6 entiers consécutifs, il est donc divisible par 6. D'autre part, $x(x+1)(x+2)(x+3)(x+4)$ est produit de 5 entiers consécutifs et finalement X est divisible par 8, puisque $x(x+1)$, $(x+2)(x+3)$ et $(x+4)(x+5)$ sont divisibles par 2, donc leur produit X. Donc X est divisible par le ppcm de $5, 6$ et 8 et celui-ci vaut 720.

(OLYMPIADE ANGLAISE 2000)
Montrer que pour tout entier naturel n, l'entier

$$A_n = 121^n - 25^n + 1900^n - (-4)^n$$

est divisible par 2000.

SOLUTION. Puisque $2000 = 16 \times 125$ et que $16 \wedge 125 = 1$, alors il suffit de montrer que l'entier A_n est divisible par 2000. Modulo 16, on a $121 \equiv 25 \pmod{16}$, donc $121^n \equiv 25^n \pmod{16}$, et on a aussi $1900 \equiv -4 \pmod{16}$, donc $100^n \equiv (-4)^n \pmod{16}$, d'où $A_n \equiv 0 \pmod{16}$. D'autre part, on a $121^n \equiv (-4)^n \pmod{125}$ et aussi $1900^n \equiv 25^n \pmod{125}$. Finalement $A_n \equiv 0 \pmod{125}$. En conclusion, $A_n \equiv 0 \pmod{16}$ et $A_n \equiv 0 \pmod{125}$, donc $A_n \equiv 0 \pmod{2000}$ puisque 16 et 25 sont premiers entre eux.

(OLYMPIADE IRLANDAISE 1996)
Soit p un nombre premier, a et n deux entiers naturels ≥ 1 tels que

$$2^p + 3^p = a^n$$

SOLUTION. Il est clair que si $p = 2$, le résultat est évident. Supposons maintenant que le nombre premier p est ≥ 3. On remarque que $5 = 2 + 3$ divise $2^p + 3^p$ puisque p est un nombre impair. donc 5 divise a^n, si n était ≥ 2, alors 25 va diviser $5(2^{p-1} - 2^{p-2}3 + \ldots - 3^{p-1})$, puisque $3 \equiv -2 \pmod{5}$, alors

$$2^{p-1} - 2^{p-2}3 + \ldots - 3^{p-1} \equiv \underbrace{2^{p-1} + 2^{p-1} + \ldots + 2^{p-1}}_{p \text{ fois}} \equiv p2^{p-1} \pmod{5}$$

Donc p divise $p2^{p-1}$ et alors 5 divise p par le théorème de Gauss puisque 5 et 2 sont premiers entre eux. D'où, $p = 5$ et alors en substituant p dans l'équation de base, on retrouve une contradiction.

Montrer que 7 divise

$$13^{682} - 1$$

SOLUTION. On remarque que

$$13^{682} = (14-1)^{682} = (2 \times 7 - 1)^{682} \equiv (-1)^{682} \equiv 1 \pmod{7}$$

D'où le résultat.

➳ De manière générale, on a pour tout entiers a, b et tout entier non nul n,

$$(an+b)^m \equiv b^m \pmod{n}$$

où $m \geq 1$ un entier naturel.

Montrer que les entiers

$$a_n = 1 + 6 + 6^2 + \ldots + 6^{n-1} - n$$

sont divisibles par 5 pour tout entier naturel non nul n.

SOLUTION. On remarque que $6^k \equiv 1 \pmod{5}$ pour tout entier naturel k, donc

$$1 + 6 + + \ldots + 6^{n-1} \equiv \underbrace{1 + 1 + \ldots + 1}_{n \quad \text{fois}} \pmod{5}$$

D'où le résultat.

Deux entiers naturels sont dit des nombres jumeaux sont deux nombres premiers qui ne différent que de 2.

Soient $\overline{a_1 a_2 \ldots a_n}_{(10)}$ et $\overline{b_1 b_2 \ldots b_n}_{(10)}$ la représentation en base décimale de deux nombres jumeaux ≥ 5. Montrer que l'entier N de représentation en base décimale $\overline{a_1 b_1 a_2 b_2 \ldots a_n b_n}_{(10)}$ ne peut pas être un nombre premier.

SOLUTION. Pour un entier naturel x quelconque dont la représentation en base décimale $\overline{x_1 \ldots x_n}_{(10)}$, on a $x \equiv x_1 + \ldots + x_n \pmod{10}$. En effet, on écrit

$$x = \overline{x_1 \ldots x_n}_{(10)} = 10^n x_1 + 10^{n-1} x_2 + \ldots + x_n \equiv x_1 + \ldots + x_n \pmod{3}$$

Les deux entiers a et b étant des nombres jumeaux, ils sont en particuliers des nombres premiers et on aura donc par exemple (en supposant que $a < b$) $a \equiv 2 \pmod{3}$ et $b \equiv 1$ (on ne pas avoir $a \equiv 0 \pmod{3}$ ou $b \equiv 0 \pmod{3}$ car $b > a \geq 5$ des nombres premiers). Par conséquent

$$\overline{a_1 b_1 a_2 b_2 \ldots a_n b_n}_{(10)} \equiv a_1 + b_1 + \ldots + a_n + b_n \equiv (a_1 + \ldots + a_n) + (b_1 + \ldots + b_n) \equiv a + b \equiv 2 + 1 \equiv 0 \pmod{3}$$

Donc, l'entier $\overline{a_1 b_1 a_2 b_2 \ldots a_n b_n}_{(10)}$ est divisible par 3 et puisqu'il est > 3, il est alors non premier.

0.6 Petit théorème de Fermat

En mathématiques, le petit théorème de Fermat est un résultat de l'arithmétique modulaire, qui peut aussi se démontrer avec les outils de l'arithmétique élémentaire.

Il s'énonce comme suit : « si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} - 1$ est un multiple de p », autrement dit (sous les mêmes conditions sur a et p), a^{p-1} est congru à 1 modulo p,

$$a^{p-1} \equiv 1 \pmod{p}$$

Un énoncé équivalent est : « si p est un nombre premier et si a est un entier quelconque, alors a $a^p - a$ est un multiple de p »,

$$a^p \equiv a \pmod{p}$$

Il doit son nom à Pierre de Fermat, qui l'énonce pour la première fois en 1640.

Dans ce cours, on énonce (sans démonstration) le petit théorème de Fermat. Pour une démonstration, on renvoie le lecteur vers le chapitre d'algèbre, dans la section concernant la loi de composition interne et la structure de Groupe.

Soit a un entier relatif et p, un nombre premier. Alors

$$a^p \equiv a \pmod{p}$$

➳ On a déjà vu des cas particuliers de ce théorème. En effet, pour tout entier relatif n, on a $n^2 \equiv n \pmod 2$ et $n^3 \equiv n \pmod 3$.

Montrer que pour tout entier a, on a

$$26 \quad \text{divise} \quad a^{13} - a$$

SOLUTION. Soit a un entier relatif. Le petit théorème de Fermat nous assure (puisque 13 est un nombre premier) que

$$a^{13} \equiv a \pmod{13}$$

De plus, on a

$$a^{13} \equiv a \pmod 2$$

puisque les entiers a et a^{13} possèdent la même parité. On sait que $26 = 2 \times 13$ et que 2 et 13 sont premiers entre eux. Alors

$$a^{13} \equiv a \pmod{26}$$

D'où le résultat.

Montrer que que

$$1998^{1321^{2019}} \equiv 678 \pmod{1321}$$

SOLUTION. Puisque tous les nombres premiers inférieurs ou égals à $\sqrt{1321}$ ne divise pas ce dernier, alors 1321 est un nombre premier, il vient que

$$1998^{1321} \equiv 1998 \equiv 678 \pmod{1321}$$

Donc,

$$1998^{1321^{2019}} \equiv 1998^{1321^{2018}} \equiv \ldots \equiv 1998^{1321^2} \equiv 1998^{1321} \equiv 678 \pmod{1321}$$

D'où, le résultat souhaité.

Soient a, b et c trois entiers relatifs. Montrer l'équivalence suivante

$$6 \mid a^{81} + b^{81} + c^{81} \iff 6 \mid a + b + c$$

SOLUTION. On commence par remarquer que les entiers x et x^{81} ont même parité, donc 2 divise leur différence. Par conséquent $x^{81} \equiv x \pmod 2$ pour $x \in \{a, b, c\}$. On montre également que $x^{81} \equiv x \pmod 3$ pour $x \in \{a, b, c\}$. En effet, pour un entier x d'après le théorème de Fermat, on a $x^3 \equiv x \pmod 3$, par conséquent $x^{81} \equiv x^{27} \equiv x^9 \equiv x^3 \equiv x \pmod 3$, d'ou le résultat. Donc $x^{81} \equiv x \pmod 6$ (puisque 2 et 3 sont premiers entre eux) et par conséquent

$$a^{81} + b^{81} + c^{81} \equiv a + b + c \pmod 6$$

Ce qui permet de conclure.

Soit p un nombre premier. Montrer qu'il existe une infinité d'entiers naturels k tels que

$$p \quad \text{divise} \quad 1^k + 2^k + 3^k + \ldots + (p+1)^k$$

SOLUTION. Pour tout $x \in \{1, 2, \ldots, p-1, p+1\}$, on sait d'après le petit théorème de Fermat que $x^{p-1} \equiv 1 \pmod{p}$, donc on on prend les entiers naturels k comme étant les multiples de $p-1$ (qui sont bien évidemment en nombre infini), on trouve $x^k \equiv 1 \pmod{p}$ pour tout $x \in \{1, 2, \ldots, p-1, p+1\}$, les $x \in \{1, 2, \ldots, p-1, p+1\}$ étant en nombre p, alors leur somme est congru à $\underbrace{1+1+\ldots+1}_{p} = p$ modulo p. La quantité $1^k + 2^k + 3^k + \ldots + (p+1)^k$ est alors divisible par p (puisque p divise p^k. Les entiers naturels k étant en nombre infini, on a alors répondu à la question.

Déterminer tous les polynômes P à coefficients entiers tels que $P(n)$ divise $2^n - 1$ pour tout entier naturel non nul n.

SOLUTION. Rappelons une propriété utile qu'on utilisera par la suite ; Soit Q un polynôme à coefficients entiers et a et b deux entiers, alors $a-b$ divise $Q(a)-Q(b)$. En effet, pour $Q(x) = c_d x^d + \ldots + c_0$, regardons les monômes x^k, remarquons que $a-b$ divise $a^k - b^k$, donc par combinaison linéaire $a-b$ divise $Q(a)-Q(b)$.
Fixons maintenant un nombre premier q diviseur de $P(n_0)$ pour un entier naturel non nul n_0 (en supposant qu'il existe un tel n_0 tel que $|P(n_0)| \geq 2$), $q = n_0 + q - n_0$ divise $Q(n+q) - Q(n_0)$, mais q divise $P(n_0)$, alors q divise $P(n_0+q)$ qui divise à son tour $2^{n_0+q} - 1$, donc par transitivité q divise $2^{n_0+q} - 1$. Or

$$0 \equiv 2^{n_0+q} - 1 \equiv 2^q \times 2^{n_0} - 1 \equiv 2 \times 2^{n_0} - 1 \equiv 2^{n_0+1} - 1 \pmod{q}$$

mais $2^{n_0} \equiv 1 \pmod{q}$ (puisque q divise $2^{n_0} - 1$), donc q divise 1, ce qui est impossible. Donc pour tout entier naturel non nui n, $P(n) \in \{-1, 1\}$, mais le polynôme P va prendre pour une infinité d'entiers naturels, la, soit la valeur -1 ou 1, il va par conséquent être constamment égal à cette valeur. Réciproquement, on vérifie que les polynômes qui sont constamment égaux à -1 et 1 sont solutions du problème.

Montrer que

$$7 \quad \text{divise} \quad 2222^{5555} + 5555^{2222}$$

SOLUTION. On sait que $2222 \equiv 3 \pmod{7}$ et $5555 \equiv 4 \pmod{7}$, et la division euclidienne par 6 fournit $2222 = 370 \times 6 + 2$ et $5555 = 925 \times 6 + 5$. Le petit théorème de Fermat permet d'écrire alors,

$$2222^{5555} \equiv 3^{5555} \equiv 3^{925 \times 6 + 5} \equiv (3^6)^{925} \times 3^5 \equiv 243 \equiv 5 \pmod{7}$$

Et de même, on trouve $5555^{2222} \equiv 2 \pmod{7}$, d'où

$$7 \quad \text{divise} \quad 2222^{5555} + 5555^{2222}$$

1. Soient a et b deux entiers et n un entier naturel non nul tels que

$$a \equiv b \pmod{n}$$

Montrer que

$$a^n \equiv b^n \pmod{n^2}$$

2. Déterminer les chiffres des unités et des dizaines du nombre $N = 67^{40}$.

SOLUTION.

1. Soient a et b deux entiers et n un entier naturel non nul tels que

$$a \equiv b \pmod{n}$$

Il s'agit de montrer que n divise $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$, puisque n divise $a-b$, il reste à prouver que n divise aussi $a^{n-1} + a^{n-2}b + \ldots + b^{n-1}$, or on sait que $a^k \equiv b^k \pmod{n}$ pour tout entier naturel k, donc

$$a^{n-1} + a^{n-2}b + \ldots + b^{n-1} \equiv a^{n-1} + a^{n-2}a + \ldots + a^{n-1} \equiv \underbrace{a^{n-1} + a^{n-1} + \ldots + a^{n-1}}_{n \text{ fois}} \equiv na^{n-1} \equiv 0 \pmod{n}$$

D'où le résultat.

2. Il s'agit de déterminer le reste de $N = 67^{40}$ modulo 100. Or, on a

$$67^4 \equiv 7^4 \equiv 49^2 \equiv (-1)^2 \equiv 1 \pmod{10}$$

Donc, en levant à la puissance 10, on retrouve en utilisant la question précédente

$$N = 67^{40} \equiv 1 \pmod{100}$$

Donc, les chiffres des unités de l'entier $N = 67^{40}$ est 1 et le chiffre des dizaines est 0.

0.7 Carrés parfaits

Un entier naturel c est dit carré parfait s'il s'écrit sous la forme d'un carré d'un autre entier naturel. Dans cette section, on va voir de différentes techniques et idées portant sur ce type d'entiers spéciales.

Déterminer tous les entiers naturels n tels que

$$\sqrt{1 + 5^n + 6^n + 11^n} \in \mathbb{N}$$

SOLUTION. L'entier $n = 0$ est clairement une solution. Montrons que c'est la seule solution. Soit $n \geq 1$ un entier naturel, on regarde les chiffres de l'unité des entiers naturels $1, 5^n, 6^n$ et 11^n. Le chiffre des unités de 5^n est 5, celui de 6^n est 6 et finalement le chiffre des unité de l'entier 11^n est 1. Donc, le chiffres des unités de $1 + 5^n + 6^n + 11^n$ est 3. Mais le chiffre des unités d'un carré parfaits ne peut jamais être égal à 3. Ceci permet de conclure.

Montrer que si on a ajoute 1 au produit de quatre entiers naturels consécutifs, on obtient un carré parfait.

SOLUTION. Soit n un entier naturel, on remarque que

$$N = n(n+1)(n+2)(n+3) + 1 = (n+1)(n+2)n(n+3) + 1 = (n^2 + 3n + 2)(n^2 + 3n) + 1$$

$$= (n^2 + 3n)^2 + 2(n^2 + 3n) + 1 = (n^2 + 3n + 1)^2$$

Ceci est est suffisant pour conclure.

Les restes possibles de la division euclidienne d'un carré parfait par 3 sont 0 et 1.

DÉMONSTRATION. En effet pour un entier x, on a $x \equiv 0, 1, 2 \pmod{3}$, donc $x^2 \equiv 0, 1, 4 \equiv 0, 1, 1 \pmod{3}$. Finalement, les restes possibles d'un carré parfait modulo 3 sont 0 et 1.

Existe t-il un entier x tel que

$$x^4 = 10^{100} + 7 \quad ?$$

SOLUTION. Le côté de gauche de l'équation est un carré parfait, mais le côté de droite est congru à 2 modulo 3. Ceci est bien sur suffisant pour affirmer que l'équation de base n'admet pas de solution entière.

Soient x et y deux entiers relatifs tels que 3 divise $x^2 + y^2$. Montrer que 3 divise x et 3 divise y.

SOLUTION. On utilise un tableau de congruence,

	0	1
0	0	1
1	1	2

On voit que le seul cas portant sur le couple (x, y) tel que $x^2 + y^2 \equiv 0 \pmod 3$ est le cas où $x \equiv 0 \pmod 3$ et $y^2 \equiv 0 \pmod 3$, donc 3 divise x^2 et y^2. Par conséquent, 3 divise x et y puisque 3 est un nombre premier.

➳ Le résultat de l'exemple précédent peut être généralisé comme ce qui suit.

Soit $p \equiv 3 \pmod 4$ un nombre premier divisant la somme de deux carrés x^2 et y^2. Alors p divise x et y.

DÉMONSTRATION. Il suffit de montrer que p divise x ou y (car si par exemple p divise x, il va diviser $y^2 = x^2 + y^2 - x^2$, par conséquent p va diviser y^2, et par la suite p divisera y. Supposons par l'absurde que x et y ne sont pas divisibles par p. Il vient que x et p sont premiers entre eux, donc le théorème de Bezout nous assure l'existence de deux coefficients entiers u et v tels que $ux = vp + 1$. Un passage modulo p, fournit $ux \equiv 1 \pmod p$, donc $(ux)^2 \equiv 1 \pmod p$ mais on sait que $x^2 \equiv -y^2 \pmod p$, donc

$$(uy)^2 \equiv -1 \pmod p, \qquad (*)$$

D'autre par p ne peut pas diviser uy (sinon p divisera 1), donc uy et p sont premiers entre eux, puisque p est un nombre premier, alors le théorème de Fermat nous assure que $(uy)^{p-1} \equiv 1 \pmod p$. En comparant avec $(*)$ on trouver (puisque $\frac{p-1}{2}$ est un entier),

$$(-1)^{\frac{p-1}{2}} \equiv (uy)^{p-1} \equiv 1 \pmod p$$

Donc, $\frac{p-1}{2}$ est pair, par conséquent il existe un entier k tel que $p - 1 = 4k$, c'est à dire $p \equiv 1 \pmod 4$. Ceci contredit clairement la donnée de $p \equiv 3 \pmod 4$.

Trouver tous les couples d'entiers relatifs (x, y) vérifiant l'équation

$$(E), \qquad x^2 + y^2 = 7^{2020}$$

SOLUTION. Soit (x, y) une solution éventuelle du problème. On sait que 7 divise $x^2 + y^2$, donc 7 divise x et y puisque 7 est un nombre premier congru à 3 modulo 4. En posant $(x, y) = (7x', 7y')$, on trouve que le couple (x', y') est solution de l'équation

$$(E'), \qquad x'^2 + y'^2 = 7^{2018}$$

Supposons que $x \neq 0$ et $y \neq 0$. Soit α l'exposant de 7 dans la décomposition en facteurs premiers de x et β l'exposant de 7 dans la décomposition en facteurs premiers de y et $\gamma = \min(\alpha, \beta)$. Donc $x = 7^\gamma x_0$ et $y = 7^\gamma y_0$, en substituant dans l'équation (E), on trouve

$$7^{2\gamma} x_0^2 + 7^{2\gamma} y_0^2 = 7^{2018}, \qquad (*)$$

Bien sur γ est inférieur où égal à 2020, sinon un argument de majoration permet de trouver une absurdité. Donc $(*)$ entraîne

$$x_0^2 + y_0^2 = 7^{2020-2\gamma}$$

Si jamais, on a avait $2\gamma \neq 2020$, alors 7 divisera $x_0^2 + y_0^2$, par conséquent 7 va diviser x_0 et y_0, et ceci n'est pas possible puisque si par exemple $\gamma = \alpha$, on aura $7^{\alpha+1}$ divise x, et ceci contredira la définition de α (7^α la plus grande puissance avec laquelle 7^α divise x). Donc $2\gamma = 2020$, c'est à dire $\gamma = 1010$, mais $\gamma = \min(\alpha, \beta)$ et $2\alpha, 2\beta \leq 2020$, donc $\alpha = \beta = 1010$, il vient que $x_0^2 + y_0^2 = 1$, donc l'un des deux entiers x_0 et y_0 est nul. Par conséquent, l'un des deux entiers x et y est nul et ceci est contraire à l'hypothèse de départ ($x \neq 0$ et $y \neq 0$). Donc, $x = 0$ ou $y = 0$, d'où l'ensemble des solutions de l'équation (E) (après avoir étudier la réciproque) est

$$S = \{(0, -7^{1010}), (-7^{1010}, 0), (0, 7^{1010}), (7^{1010}, 0)\}$$

Les restes possibles de la division euclidienne d'un carré parfait par 4 sont 0 et 1.

DÉMONSTRATION. En effet pour un entier x, on a $x \equiv 0, 1, 2, 3 \pmod 4$, donc $x^2 \equiv 0, 1, 4, 9 \equiv 0, 1, 0, 1 \pmod 3$. Finalement, les restes possibles d'un carré parfait modulo 3 sont 0 et 1.

Existe t-il des entiers a et b tels que

$$a^2 + b^2 = 2019 \quad ?$$

SOLUTION. Un carré parfait est congru à 0 ou 1 modulo 4. Donc, la somme de deux carrés est congru à $0, 1, 2$ modulo 4 mais on voit que 2019 est congru à 3 modulo 4. Par conséquent, il n'existe pas d'entiers a et b tels que $a^2 + b^2 = 2019$.

Les restes possibles de la division euclidienne d'un carré parfait par 8 sont 0 et 1 et 4.

DÉMONSTRATION. En effet pour un entier x, on a $x \equiv 0, 1, 2, 3, 5, 6, 7 \pmod 8$, donc

$$x^2 \equiv 0, 1, 4, 9, 16, 25, 36, 49 \equiv 0, 1, 4, 1, 0, 1, 4, 1 \pmod 3$$

Finalement, les restes possibles d'un carré parfait modulo 8 sont 0 et 1 et 4.

Existe t-il des entiers a, b et c tels que

$$9a^2 + 33b^2 + 17c^2 = 2023$$

SOLUTION. Soit (a, b, c) une solution éventuelle du problème. On raisonne modulo 8, en remarquant que

$$9a^2 + 33b^2 + 17c^2 \equiv a^2 + b^2 + c^2 \pmod 8$$

D'autre part, 2023 est congru à 7 modulo 8. Or la somme de 3 carrés parfaits ne peut pas être congrue à 7 modulo 8 (puisque un carré est congru à $0, 1$ ou 4 modulo 8). Donc un tel triplet (a, b, c) n'existe pas.

Montrer que de deux entiers qui s'écrivent sous forme de somme de deux carrés est encore somme de deux carrés.

SOLUTION. Il suffit de remarquer que

$$(a^2 + b^2)(x^2 + y^2) = (ax)^2 + (by)^2 + (ay)^2 + (bx)^2 = (ax + by)^2 + (ay - bx)^2$$

D'où le résultat.

0.8 Introduction aux équations diophantiennes

Une équation diophantienne est une équation à coefficients entiers dont on cherche des solutions entières. Il n'existe pas de méthode générale pour résoudre une équation diophantienne. Cependant, il existe plusieurs techniques et approches pour attaquer de telles équationd. Dans ce cours on va découvrir plusieurs techniques à savoir les méthodes élémentaires de résolution, l'utilisation des congruences, l'utilisation des inégalités et autres méthodes et techniques ...

0.9 Factorisations

Dans plusieurs équations diophantiennes, la clé de résolution se base sur des identités, nous allons dans cette section donner les identités remarsuables les plus célèbres et les plus utiles ...

Soient a et b des nombres réels et n un entier naturel non nul,

$$a^{2^n} - b^{2^n} = (a-b) \times (a+b) \times (a^2+b^2) \times (a^4+b^4) \times ... \times (a^{2^{n-1}} + b^{2^{n-1}}) = (a-b) \times \prod_{p=1}^{n-1} (a^{2^p} + b^{2^p})$$

DÉMONSTRATION. On procède par récurrence pour montrer cette identité. Pour $n = 1$, c'est trivial. Supposons l'identité vraie pour le rang $n \geq 1$ et montrons qu'elle est vraie pour le rang $n+1$. Soient a et b des nombres réels, on a

$$a^{2^{n+1}} - b^{2^{n+1}} = \left(a^{2^n}\right)^2 - \left(b^{2^n}\right)^2 = (a^{2^n} - b^{2^n}) \times (a^{2^n} + b^{2^n}) = (a-b) \times \prod_{p=1}^{n-1} (a^{2^p} + b^{2^p}) \times (a^{2^n} + b^{2^n}) = (a-b) \times \prod_{p=1}^{n} (a^{2^p} + b^{2^p})$$

d'où le résultat est vrai pour le rang $n+1$. Donc l'identité est vrai pour tous réels a et b et pour tout entier naturel non nul n.

➳ La notation $\prod_{k=1}^{n} a_k$ désigne le produit des nombres réels $a_1, a_2, \ldots, a_n$ où $n \geq 1$ un entier naturel. On étudiera les propriétés concernant ce symbole dans la suite de ce cours.

1. Soit n un entier naturel, le n-ème nombre de Fermat est défini par $F_n = 2^{2^n} + 1$. Montrer que tous les nombres de Fermat sont premiers entre eux deux à deux.
2. Soit n un entier naturel. Montrer que si l'entier $2^n + 1$ est premier, alors n est une puissance de 2.

SOLUTION.

1. Soient $n < m$ deux entiers naturels. Il s'agit de montrer que F_n et F_m sont premiers entre eux, on note classiquement Δ leur plus grand diviseurde F_n et F_m commun et montre qu'il vaut 1. L'entier Δ divise $F_m - 2$. En effet,

$$F_m - 2 = 2^{2^m} - 1 = \prod_{k=1}^{m-1} (2^{2^k} + 1) = F_n \times \prod_{k=1, k\neq n}^{m-1} (2^{2^k} + 1)$$

   Donc Δ divise 2, i.e. $\Delta \in \{1, 2\}$. Or, Δ ne peut pas être égal à 2 puisque 2 ne peut pas divise un nombre de Fermat. Donc $\Delta = 1$, ce qui est équivaut à dire que F_n et F_m sont premiers entre eux.

2. On écrit $n = 2^p(2q+1)$ où p et q deux entiers naturels. Il s'agit de montrer que $q = 0$, supposons que $q \geq 1$. On remarque que

$$2^n + 1 = 2^{2^p(2q+1)} + 1 = (2^{2^p} + 1)K$$

   En utilisant une identité remarquable classique. Donc, $2^n + 1$ n'est pas premier, ce qui contredit l'hypothèse. Donc, n est une puissance de 2.

(IDENTITÉ DE SOPHIE GERMAIN).
Soient a et b des nombres réels, alors

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$$

DÉMONSTRATION. Soient a et b des nombres réels, alors

$$a^4 + 4b^4 + 4a^2b^2 - 4a^2b^2 = (a^2 + 2b^2)^2 - (2ab)^2 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$$

D'où l'identité.

(OLYMPIADE MAROCAINE 2018).
Déterminer tous les couples d'entiers naturels (x, y) tels que,

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$$

SOLUTION. Soit (x, y) une solution éventuelle de l'équation ci-dessus. L'équation ci-dessus est équivalente à

$$5x + 5y - xy = 0$$

Ce qui est équivaut à

$$5x - xy + 5y = (5 - y)x + 5y - 25 = -25$$

qui est équivalente à

$$(x - 5)(y - 5) = 25$$

Ceci est équivalent à

$$\begin{cases} x - 5 = 1 \\ y - 5 = 25 \end{cases} \quad \begin{cases} x - 5 = 25 \\ y - 5 = 1 \end{cases} \quad \begin{cases} x - 5 = 5 \\ y - 5 = 5 \end{cases}$$

c-à-d

$$\begin{cases} x = 6 \\ y = 30 \end{cases} \quad \begin{cases} x = 30 \\ y = 6 \end{cases} \quad \begin{cases} x = 10 \\ y = 10 \end{cases}$$

Donc l'ensemble des solution de l'équation est

$$S = \{(5, 5), (6, 30), (30, 6)\}$$

Trouver tous les entiers naturels x et n tels que

$$2^n + 1 = x^2$$

SOLUTION. On passe le 1 de l'autre côté de l'égalité et on factorise,

$$(x - 1)(x + 1) = 2^n$$

Donc $x - 1$ et $x + 1$ sont des puissances de 2, or les seules puissances de 2 qui différent de 2 sont 2 et 4, il vient que $x = 3$ et par suite $2^n + 1 = 9$, donc $n = 3$. Réciproquement le couple $(3, 3)$ est une solution. Donc l'unique solution du problème est $(3, 3)$.

(OLYMPIADE INDIENNE 1993)
Déterminer les solutions entières positives de l'équation

$$(xy-7)^2 = x^2 + y^2$$

SOLUTION. L'équation est équivalente à l'équation

$$(xy-6)^2 + 13 = (x+y)^2$$

c'est à dire

$$[xy-6-(x+y)] \times [xy-6+(x+y)] = -13$$

Ce qui donne les systèmes d'équations

$$\begin{cases} xy-6-(x+y) = -1 \\ xy-6+(x+y) = 13 \end{cases} \qquad \begin{cases} xy-6-(x+y) = -13 \\ xy-6+(x+y) = 1 \end{cases}$$

Ce qui est équivalent à

$$\begin{cases} x+y = 7 \\ xy = 12 \end{cases} \qquad \begin{cases} x+y = 7 \\ xy = 0 \end{cases}$$

Donc l'ensemble des solutions de l'équation proposée est

$$S = \{(3,4),(4,3),(0,7),(7,0)\}$$

0.10 Discriminant d'un trinôme à coefficients entiers

Commençons par donner une proposition concernant les trinômes unitaires à coefficients dans $\mathbb{Z}$.

Soient $a, b \in \mathbb{Z}$, alors l'équation

$$x^2 + ax + b = 0$$

admet une solution dans $\mathbb{Z}$ si et seulement son discriminant est un carré parfait.

DÉMONSTRATION. Soient a et b deux entiers relatifs. Supposons que l'équation $x^2 + ax + b$ admet une solution dans $\mathbb{Z}$, soit x_0 cette solution et soit x_1 la seconde solution. On sait que $x_0 + x_1 = -a$, donc $x_1 \in \mathbb{Z}$ et on a $x_0 x_1 = b$. Le discriminant de l'équation $x^2 + ax + b = 0$ est

$$\Delta = a^2 - 4b = (x_0 + x_1)^2 - 4x_0x_1 = (x_0 - x_1)^2$$

qui est évidemment un carré parfait. D'où la condition nécessaire. Réciproquement, supposons que le discriminant Δ de l'équation x^2+ax+b est un carré parfait,c'est à dire $\Delta = a^2-4b = k^2$ et par suite les solutions de l'équation $x^2+ax+b=0$ sont

$$x_0 = \frac{-a+k}{2}, \quad x_1 = \frac{-a-k}{2}$$

Sachant que $a^2 - 4b = \alpha^2$, ce qui signifie que $4b = a^2 - \alpha^2 = (a-\alpha)(a+\alpha)$ donc l'un des deux entiers $a-\alpha$ et $a+\alpha$ est pair, il s'en suit que a et α ont la même parité, et par suite les deux entiers $a-\alpha$ et $a+\alpha$ sont pairs. Par suite les deux solutions x_0 et x_1 sont des entiers, d'où la condition suffisante.

Déterminer tous les entiers naturels n tels que $n+1$ divise $n^2 - 2n + 3$.

SOLUTION. On peut résoudre ce petit problème en utilisant uniquement des arguments de divisibilité. Mais on va utiliser la technique décrite précédemment. Soit n un entier naturel éventuel vérifiant la condition ci-dessus. Alors il existe k entier naturel tel que $n^2 - 2n + 3 = k(n+1)$, ce qui est équivalent à $n^2 - (k+2)n + 3 - k = 0$, cette équation admet une solution en vertu de notre hypothèse, donc son discriminant est un carré parfait, c-à-d

$$(2+k)^2 - 4(3-k) = \alpha^2$$

Ce qui est équivalent à

$$(k+4)^2-\alpha^2=(k+4-\alpha)(k+4+\alpha)=24$$

Les solutions de cette équation sont $(k,\alpha)=(1,1)$ et $(k,\alpha)=(3,5)$. Il s'en suit que $n\in\{0,1,2,5\}$, réciproquement il s'agit bien de solutions du problème.

(OLYMPIADE AMÉRICAINE 2002)
Déterminer les solutions entières non nuls de l'équation

$$(x^2+y)(x+y^2)=(x-y)^3$$

SOLUTION. L'équation diophantienne ci-dessus est équivalente à

$$2y^2+(x^2-3x)y+3x^2+x=0$$

Cette équation admet une solution si et seulement si sont discriminant $x(x+1)^2(x-8)$ est un carré parfait, il s'en suit que $x(x-8)$ est un carré parfait, i.e. $x(x-8)=z^2$ donc $(x-4)^2-z^2=16$. Ceci fournit $x\in\{-1,8,9\}$ et alors $(x,y)\in\{(-1,-1),(8,-10),(9,-10),(9,-21)\}$. La réciproque donne

$$S=\{(-1,-1),(8,-10),(9,-10),(9,-21)\}$$

(OLYMPIADE MAROCAINE 2016)
Trouver tous les nombres premiers p et q vérifiant

$$p^3+p=q^2+q$$

SOLUTION. Soit (p,q) une solution éventuelle de l'équation. Il est clair que les deux nombres premiers p et q sont différents et que $p<q$ et en particulier p et q sont premiers entre eux. D'autre part p divise $q(q+1)$, et par le lemme de Gauss p divise $q+1$. On pose $q+1=kp$, i.e. $q=kp-1$ et en substituant dans l'équation de base on trouve

$$p^3+p=q^2+q=(kp-1)^2+(kp-1)=k^2p^2-2kp+kp=k^2p^2-kp$$

Ce qui est équivalent à

$$p^2-k^2p+kp+1=p^2-(k^2-k)p+1=0$$

Donc le discriminant de cette équation est un carré parfait, i.e.

$$(k^2-k)^2-4=\alpha^2$$

où α est un entier naturel. Ceci fournit les systèmes d'équations

$$\begin{cases}k^2-k+\alpha=4\\k^2-k-\alpha=1\end{cases}\quad\begin{cases}k^2-k+\alpha=1\\k^2-k-\alpha=4\end{cases}\quad\begin{cases}k^2-k+\alpha=2\\k^2-k-\alpha=2\end{cases}$$

Ce qui implique que

$$2k^2-2k-5=0,\quad 2k^2-2k-4=0$$

La première équation n'admet pas de solution entière puisque sont discriminant n'est pas un carré parfait. La seconde équation à pour solutions entières -1 et 2, donc $k=2$ et par suite

$$q+1=2p$$

En substituant dans l'équation de base on trouve

$$p^3+p=(2p-1)^2+2p-1=4p^2-2p$$

i.e.

$$p^2-4p+3=0$$

Donc $p=3$, et par suite $q=5$. Réciproquement le couple $(3,5)$ s'agit bien d'une solution du problème. Alors

$$S=\{(3,5)\}$$

0.11 Équations diophantiennes et inégalités

L'utilisation des majorations, des minorations peuvent s'avérer utile dans certaines situations, dans cette dernière partie de cette section, on va voir de nombreux exemples dont la résolution se fait en utilisant des inégalités.

(OLYMPIADE MAROCAINE 2018)
Trouver tous les entiers naturels x et y tels que

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{5}$$

SOLUTION. Soient (x,y) solution éventuelle de l'équation ci-dessus. Les entiers naturels x et y jouent des rôles symétrique, on peut alors supposer que $x \leq y$, il vient

$$\frac{1}{5} \leq \frac{1}{x}+\frac{1}{y} \leq \frac{2}{x}$$

Par conséquent $x \leq 10$. Sachant que $1/5 \geq 1/x$ d'après l'équation de base, alors $x \geq 5$. En substituant x par les valeurs $5,6,7,8,9,10$, on trouve $S=\{(5,30),(10,10),(30,5)\}$.

0.12 Exercices

EXERCICE 1. Soient x et y deux entiers relatifs. Montrer que 17 divise $2x + 3y$ si et seulement si 17 divise $9x + 5y$.

EXERCICE 2. Montrer que l'entier

$$n^3 + (n+1)^3 + (n+2)^3$$

est divisible par 9 pour tout entier relatif n.

EXERCICE 3. Déterminer tous les couples d'entiers naturels (m, n) tels que

$$m^2 - n! = 780$$

EXERCICE 4. Existe-t-il un polynôme à coefficients entiers P tel que $P(1) = 2$ et $P(3) = 5$?

EXERCICE 5. Montrer que pour tout $n > 11$, l'entier $n^2 - 19n + 89$ n'est pas un carré parfait.

EXERCICE 6. Montrer que si n est un cube parfait, l'entier $n^2 + 3n + 3$ ne peut pas être un cube parfait.

EXERCICE 7. L'entier

$$4^{2019} + 2019^4$$

est-il un nombre premier ?

EXERCICE 8. Déterminer tous les couples d'entiers naturels (n, m) vérifiant

$$2^{2m} - 3^{2n} = 175$$

EXERCICE 9. Déterminer tous les couples (p, q) de nombres premiers tel que $p^2 + pq + q^2$ est un carré parfait.

EXERCICE 10. On considère l'équation

$$(E), \quad x^2 - 2px + p^2 - 5p - 1 = 0$$

où p est un nombre premier. Trouver les valeurs possibles du nombres premier p sachant que l'équation (E) admet deux racines entières.

EXERCICE 11. Décomposer l'entier

$$1001001001$$

en facteurs premiers.

EXERCICE 12. Soient p et q deux nombres premiers, et on pose

$$r = \frac{p^2 + q^2}{p + q}$$

Montrer que si r est un entier, alors il est un carré parfait.

EXERCICE 13. Déterminer les chiffres des unités et des dizaines des entiers,

$$N_1 = 7^{2019}, \qquad N_2 = 2^{999}$$

EXERCICE 14. Déterminer les entiers naturels n tels que

$$n! + 5$$

un cube parfait.

EXERCICE 15. Montrer qu'il existe une infinité de nombres premiers de la forme $4k + 1$.

EXERCICE 16. Montrer que

$$2^{11 \times 31} \equiv 2 \pmod{11 \times 31}$$

EXERCICE 17. Déterminer les carrés parfaits dans la suite suivante,

$$1!,\ 1! + 2!,\ 1! + 2! + 3!,\ \ldots,\ 1! + 2! + \ldots + n!, \ldots$$

EXERCICE 18. Quelle est la valeur minimale positive de $12^m - 5^n$ pour m et n des entiers strictement positifs ?

EXERCICE 19. Soient $m, n \geq 1$ des entiers. Montrer que $3^m + 3^n + 1$ n'est pas un carré parfait.

EXERCICE 20. Trouver tous les entiers $x, y \geq 1$ tels que $3^x - 2^y = 7$.

EXERCICE 21. Trouver tous les entiers $n \geq 1$ tels que $2^n + 12^n + 2014^n$ soit un carré parfait.

EXERCICE 22. Montrer que tout entier relatif peut s'écrire comme la somme de cinq cubes d'entiers relatifs d'une infinité de manières différentes.

EXERCICE 23(SAINT PETERSBOURG 1997).
Soient x, y et z des entiers strictement positifs tels que $2x^x + y^y = 3z^z$. Montrer que $x = y = z$.
