

# Arithmétique D

On utilisera :

- la loi de réciprocité quadratique ;
- le théorème chinois ;
- l'ordre multiplicatif d'un éléments dans  $(\mathbb{Z}/p\mathbb{Z})^*$  pour  $p$  premier.

*Définition 1.* Si  $p$  est un premier et  $n$  un entier relatif non-nul, alors on appelle valuation de  $n$  à  $p$ , et on le note  $v_p n$ , le plus grand entier  $v$  tel que  $p^v$  divise  $n$ . Par convention on pose  $v_p 0 = \infty$ .

On fait la convention que  $a + \infty = \infty$  quand  $a$  est un entier relatif ou  $\infty$ . La valuation a une série de propriété comme suit.

*Théorème 1.* Soit  $p$  un premier et  $a, b$  deux entiers relatifs quelconques. Alors on a :

- (i)  $v_p(ab) = v_p a + v_p b$ ;
- (ii)  $v_p(a + b) \geq \min(v_p a, v_p b)$  avec égalité si  $v_p a \neq v_p b$ .

*Démonstration.* (i) C'est une conséquence du fait que la décomposition en facteurs premiers est unique.

(ii) On pose  $v = \min(v_p a, v_p b)$ . Comme  $p^v$  divise  $a$  et  $b$  il divise également  $a + b$ . D'où on trouve l'inégalité.

Supposons maintenant  $v_p a = k$  et  $v_p b \geq k + 1$ . On note  $v = v_p(a + b)$  et on suppose par l'absurde que  $v \geq k + 1$ . Alors  $p^{k+1}$  divise  $(a + b) - b$ . Contradiction.  $\square$

*Exercice 1.* Montrer que les équations  $x^2 = 2y^2$  et  $x^4 + 3y^4 + 27z^4 = 9t^4$  n'ont pas de solutions non-triviales.

*Démonstration.* Pour  $x^2 = 2y^2$ , on remarque que  $v_2(x^2)$  est paire alors que  $v_2(2y^2)$  est impaire. Pour la deuxième équation, les valuations  $v_3(x^4)$ ,  $v_3(3y^4)$  et  $v_3(27z^4)$  ont des rests différents modulo 4, donc elles sont toutes distinctes. Par le point (ii) de la proposition précédente,  $v_3(9t^4)$  lui est égale. Mais cela est impossible car cette dernière a rest 2 modulo 4.  $\square$

Ici le premier à utiliser était clair de l'énoncé. Dans d'autre cas il faut considérer un diviseur premier  $p$  qui divise un des côtés des équations à résoudre.

*Exercice 2.* Soient  $b$  et  $n$  deux entiers,  $n > 1$ , tels que pour tout entier  $k$  il existe un entier  $a_k$  tel que  $a_k^n \equiv b \pmod{k}$ . Montrer que  $b$  est une puissance  $n$ -ième.

*Démonstration.* On prend  $k = b^2$ . Alors

$$(a_k)^n = b + mb^2$$

pour un  $m$  entier. Pour tout diviseur premier  $p$  de  $b$  la valuation du membre droit vaut  $v_p(b)$ . D'autre part, la valuation du membre gauche est  $nv_p(a_k)$  donc  $v_p(b) \equiv 0 \pmod{n}$ . Ainsi  $b$  est une puissance  $n$ -ième.  $\square$

*Exercice 3.* a) Soient un nombre naturel  $N$  et un premier  $p$ . Alors on a

$$v_p(N!) = \sum_{k=i}^{v_p(n)} \left\lfloor \frac{N}{p^i} \right\rfloor.$$

b) On désigne par  $\binom{N}{k}$  le nombre de choix de  $k$  éléments parmi  $N$ . Alors pour tous entiers positifs  $N$  et  $k$  avec  $N \geq k$  on a

$$v_p \left( \binom{N}{k} \right) = v_p(N) - v_p(k).$$

*Exercice 4.* Soit  $P(x) = \sum_{i=0}^d a_i x^i$  un polynôme à coefficients entiers et  $p$  un nombre premier. Montrer de deux manières différentes que  $P(x)^p \equiv P(x^p) \pmod{p}$ .

*Exercice 5* (Théorème de Pépin). Pour  $n > 0$ , le  $n$ -ième nombre de Fermat  $F_n$  est premier si et seulement si

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \quad (1)$$

*Exercice 6* (shortlist 2010). Montrer que l'équation suivante n'a qu'un nombre fini de solutions avec  $(m, n)$  entiers non-négatifs :

$$m^2 + 2 \cdot 3^n = m(2^{n+1} - 1).$$

*Exercice 7* (shortlist 2010). Pour tout couple d'entiers relatifs  $(a, b)$  on pose  $f(k) = ak^3 + bk$ . On dit qu'un couple  $(a, b)$  est  $n$ -bon si pour tout couple  $(m, k)$  d'entiers relatifs on a

$$\text{si } n \mid f(k) - f(m) \text{ alors } n \mid (k - m).$$

Si un couple est  $n$ -bon pour une infinité de valeurs de  $n$ , alors on dit qu'il est très bon. Trouver un couple  $(a, b)$  qui est 51-bon mais pas très bon. Montrer que si un couple est 2013-bon alors il est très bon.

*Exercice 8* (shortlist 2009). On dit qu'un nombre entier  $N$  est équilibré si  $N = 1$  ou si  $N$  s'écrit comme produit d'un nombre pair de facteurs premiers, pas nécessairement distincts. Etant donné deux entiers positifs  $a$  et  $b$  on considère le polynôme  $P(x) = (x+a)(x+b)$ .

a) Montrez qu'il existe des entiers distincts  $a$  et  $b$  tels que  $P(1), \dots, P(50)$  sont équilibrés.

b) Si  $P(n)$  est équilibré pour tout  $n$ , alors  $a = b$ .

*Exercice 9.* Si  $a$  et  $b$  sont deux nombres impairs alors

$$\left( \frac{a}{b} \right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}} \left( \frac{b}{a} \right). \quad (2)$$

*Exercice 10.* Soit  $a$  un nombre entier impair qui n'est pas un carré parfait. Montrer qu'il existe une infinité de nombres premiers  $p$  tels que  $a$  est un non-résidu quadratique modulo  $p$ .

### Solutions

*Solution de l'exercice 5. Implication*  $\Leftarrow$ . On suppose que  $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ . Remarquez qu'il suffit de montrer que l'ordre multiplicatif de 3,  $\text{ord}(3)$ , vaut  $F_n - 1$ . En effet, cela permet de conclure car, comme  $\text{ord}(3)$  divise  $\varphi(F_n)$  on déduit  $\varphi(F_n) = F_n - 1$ , donc  $F_n$  est premier.

Comme  $3^{(F_n-1)/2} \not\equiv 1 \pmod{F_n}$ ,  $\text{ord}(3)$  ne divise pas  $(F_n - 1)/2 = 2^{2^n - 1}$ . D'autre part, en élevant l'équation (1) au carré on a  $3^{F_n-1} \equiv 1 \pmod{F_n}$ . Alors  $\text{ord}(3)$  divise  $F_n - 1 = 2^{2^n}$ , donc  $\text{ord}(3) = F_n - 1$ .

**Implication**  $\Rightarrow$ . Supposons que  $F_n$  est premier. Rappelons l'identité

$$(X^{(F_n-1)/2} - 1)(X^{(F_n+1)/2} + 1) = X^{F_n-1} - 1 \equiv \prod_{a=0}^{F_n-1} (X - a) \pmod{F_n}.$$

Ainsi, exactement la moitié des valeurs de  $a$ , résidue non-nul modulo  $F_n$ , vérifient  $a^{(F_n-1)/2} \equiv 1 \pmod{F_n}$ . Comme, tous les restes quadratiques ont cette propriété, on déduit que  $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$  si et seulement si 3 est un non-résidue quadratique.

Par la loi de réciprocité quadratique, on a

$$\left(\frac{3}{F_n}\right) = (-1)^{\frac{F_n-1}{2} \cdot \frac{3-1}{2}} \left(\frac{F_n}{3}\right).$$

Comme  $F_n \equiv 4^{2^{n-1}} + 1 \equiv 2 \pmod{3}$ , et comme 2 est un non-résidue modulo 3, on a  $\left(\frac{F_n}{3}\right) = -1$ . Donc 3 est un non-résidue modulo  $F_n$  et alors  $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ .  $\square$

*Solution de l'exercice 6.* L'idée de base de l'exo est que, si  $a$  et  $b$  sont deux nombres réels positifs et  $a < b$  alors, pour deux nombre réels fixés  $c$  et  $d$ , l'ensemble d'entiers positifs  $n$  tels que  $a^n > c \cdot b^n - d$  est fini.

On regarde l'équation de l'exercice comme une equation de deuxième degré en  $m$  pour laquelle  $n$  est un paramètre. Son déterminant doit être le carré d'un entier  $d$  :  $(2^{n+1} - 1)^2 - 8 \cdot 3^n = d^2$ . On obtient

$$(2^{n+1} - 1 - d)(2^{n+1} - 1 + d) = 8 \cdot 3^n. \quad (3)$$

Les deux parenthèses ci-dessus ont la même parité, donc  $d$  est impair, notons le  $d = 2d' + 1$ . On a deux cas : soit  $2^n - d' = 2 \cdot 3^p$  et  $2^n - d' - 1 = 3^q$  avec  $p+q = n$ , soit  $2^n - d' = 3^q$  et  $2^n - d' - 1 = 2 \cdot 3^p$  avec  $p+q = n$ . Dans les deux cas on a :

$$2^{n+1} - 1 = 3^q + 2 \cdot 3^p, \quad (4)$$

avec  $p+q = n$ . En particulier on a  $2^n > \frac{1}{2}3^{\max(p,q)}$ . Comme  $2 < 3^{2/3}$ , pour tout  $n$  sauf un ensemble fini on a

$$\max(p, q) < \frac{2}{3}n. \quad (5)$$

En particulier, pour  $n > 6$ , on a  $\min(p, q) \geq 2$ , donc le membre droit dans l'Equation (4) est divisible par 9. Comme le membre gauche doit aussi être divisible par 9, on a  $\text{ord}_9(2) \mid (n+1)$ . Ainsi,  $n = 6n' + 5$  pour un entier  $n'$ . En utilisant l'identité  $x^3 - 1 = (x-1)(x^2 + x + 1)$ , l'Equation (4) devient

$$(4^{2n'} + 4^{n'} + 1)(4^{n'} - 1) = 2 \cdot 3^p + 3^q. \quad (6)$$

On écrit  $(4^{2n'} + 4^{n'} + 1)$  comme  $(4^{n'} - 1)^2 + 3 \cdot 4^{n'}$ . Puisque  $4^{n'} \equiv 1 \pmod{3}$ , on déduit que 9 ne divise pas  $(4^{2n'} + 4^{n'} + 1)$ . Donc  $3^{\min(p,q)-1}$  divise  $4^{n'} - 1$ . On a donc

$$3^{n/3-1} \leq 3^{\min(p,q)-1} \leq 4^{n'} - 1 = 2^{(n-5)/3} - 1. \quad (7)$$

De nouveau le fait énoncé en début de preuve pour  $a = 2$  et  $b = 3$  montre qu'il n'y a qu'un nombre fini de valeurs de  $n$  qui vérifie cette inégalité.  $\square$

*Solution de l'exercice 7.* Montrons que le couple  $(1, -51^2)$  est 51-bon mais pas très bon. Si  $(k, m)$  est un couple tel que  $k^3 - 51^2 k \equiv m^3 - 51^2 m \pmod{51}$ . Alors  $(km^{-1})^3 \equiv 1 \pmod{17}$  et  $(km^{-1})^3 \equiv 1 \pmod{3}$ . Puisque 3 est relativement premier avec  $\#(\mathbb{Z}/17\mathbb{Z})^*$  et respectivement  $\#(\mathbb{Z}/3\mathbb{Z})^*$ , on doit avoir  $k \equiv m \pmod{51}$ . Soit maintenant  $n$  tel que  $(1, -51^2)$  est très bon. En prenant  $k = 51$  et  $m = 0$  on voit que  $n$  divise  $0 = f(51) - f(0)$ . Alors  $n$  divise 51, donc on a un nombre fini de valeurs possibles.

Pour la dixième partie de l'exercice on procède en trois étapes :

1. Soit  $p$  et  $q$  deux nombre premiers entre eux. Si un couple est  $pq$ -bon alors il est  $p$ -bon.
2. Si un couple est 61-bon alors  $a$  est divisible par 61 et  $b$  ne l'est pas.
3. Si  $a$  est divisible par 61 et  $b$  ne l'est pas, alors  $(a, b)$  est  $61^i$ -bon pour tout  $i \in \mathbb{N}$ .

**1.** Soit  $(a, b)$  un couple  $pq$ -bon. Soit  $(k, m)$  un couple tel que  $f(k) - f(m) \equiv 0 \pmod{p}$ . D'après le théorème chinois, il existe  $K$  et  $M$  tels que  $K \equiv k \pmod{p}$  et  $K \equiv M \equiv 0 \pmod{q}$ . Alors  $pq$  divise  $f(k) - f(m)$  donc  $pq$  divise  $(K - M)$ . En particulier  $p$  divise  $K - M$ , donc  $p$  divise  $(k - m)$ .

**2.** Supposons par l'absurde que  $(a, b)$  est 61-bon mais  $a \not\equiv 0 \pmod{61}$ . D'abord on élimine le cas  $b \equiv 0 \pmod{61}$ . En effet, comme 3 divise  $61 - 1$ , l'équation  $w^3 \equiv 1 \pmod{61}$  a deux solution différentes de 1. En prenant  $(k, m) = (w, 1)$  on voit que 61 divise  $ak^3 - am^3$  mais pas  $(k - m)$ .

Supposons par l'absurde que  $a$  n'est pas un multiple de 61. Comme 7 est un non-résidue quadratique modulo 61 exactement une des équations suivantes a solution modulo 61 :

$$\begin{aligned} u^2 &\equiv ba^{-1} \pmod{61} \\ 7v^2 &\equiv ba^{-1} \pmod{61}. \end{aligned}$$

Dans le premier cas on pose  $(k, m) = (u, 0)$ . On a  $f(k) - f(m) \equiv (k - m)a(u^2 - ba^{-1}) \equiv 0 \pmod{61}$  et  $k - m = u$ . Comme  $b \not\equiv 0 \pmod{61}$ ,  $u \not\equiv 0 \pmod{61}$ , ce qui contredit le fait que  $(a, b)$  est 61-bon. Dans le deuxième cas on pose  $(k, m) = (2v, v)$ . Alors  $f(k) - f(m) \equiv (k - m)a(7v^2 - ba^{-1}) \equiv 0 \pmod{61}$ . Comme  $(a, b)$  est 61-bon, on doit avoir  $k - m = v \equiv 0 \pmod{61}$ , mais cela contredit le fait que  $a \not\equiv 0 \pmod{61}$ .

**3.** Soit  $i \in \mathbb{N}$ ,  $i \geq 1$  et soit  $(a, b)$  un couple qui est 61-bon. Soit  $(k, m)$  tel que  $61^i$  divise  $f(k) - f(m)$ . Alors  $61^i$  divise  $(k - m)(ak^2 + akm + am^2 - b)$ . Comme  $a$  est divisible par 61 et  $b$  ne l'est pas, la deuxième parenthèse est relativement première avec 61. Donc  $(k - m)$  est divisible par  $61^i$ . On conclut que  $(a, b)$  est  $61^i$ -bon.  $\square$

*Solution de l'exercice 8. a)* On définit  $f : \mathbb{N}^* \rightarrow \{0, 1\}$  en mettant  $f(n) = 1$  si  $n$  a un nombre impair de diviseurs premiers non-distincts et 0 sinon. Ensuite on définit  $F : \mathbb{N}^* \rightarrow \{0, 1\}^{50}$  par  $F(a) = (f(a + 1), f(a + 2), \dots, f(a + 50))$ . Comme  $F$  ne peut prendre qu'un nombre fini de valeurs, elle prend forcément deux fois la même valeur, disons  $F(a) = F(b)$ . Alors on voit que  $P(x) = (x + a)(x + b)$  convient.

**b)** On procède par l'absurde. L'idée est de chercher des valeurs de  $x$  où l'expression de  $P(x)$  se simplifie. Comme  $(x + a) - (x + b) = a - b$  on essaie de diviser les deux parenthèses par  $(a - b)$ . On prend  $k \in \mathbb{N}$ ,  $k > a/|a - b|$  et on pose  $x = k(a - b) - a$ . Alors  $P(x) = (a - b)^2 k(k + 1)$ . Comme  $f(P(x)) = 1$ , on a  $f(k) = f(k + 1)$ . Comme  $k$  est arbitraire,  $f$  est constante à partir d'un certain  $k$ . Cela est impossible car  $f(p) = 1$  pour tout premier  $p$  et  $f(c) = 0$  pour tout carré  $c$ .  $\square$

*Solution de l'exercice 9.* Soient  $a = \prod_{i \in I} a_i$  et  $b = \prod_{j \in J} b_j$  les décompositions en facteurs premiers

de  $a$  et  $b$ . Alors on a

$$\begin{aligned} \left(\frac{a}{b}\right) &= \prod_{i \in I, j \in J} \left(\frac{a_i}{b_j}\right) \\ \left(\frac{b}{a}\right) &= \prod_{i \in I, j \in J} \left(\frac{b_j}{a_i}\right). \end{aligned}$$

D'après la Loi de réciprocité quadratique, pour tous  $i$  et  $j$  on a  $\left(\frac{a_i}{b_j}\right) = (-1)^{(a_i-1)(b_j-1)/4} \left(\frac{b_j}{a_i}\right)$ . Il reste donc à montrer que  $((\prod_{i \in I} a_i) - 1) ((\prod_{j \in J} b_j) - 1) / 4 \equiv \sum_{i \in I, j \in J} (a_i - 1)(b_j - 1) / 4 \pmod{2}$ .

On remarque que pour deux nombres impairs  $x$  et  $y$ ,  $(x-1)(y-1)/4$  est pair si et seulement si au moins un des nombres  $x$  et  $y$  est congruent à 1 modulo 4. Ainsi le membre droit est égal à la parité de  $\#\{i \in I \mid a_i \equiv 3 \pmod{4}\} \cdot \#\{j \in J \mid b_j \equiv 3 \pmod{4}\}$ . Ce nombre est impair si et seulement si  $a \equiv 3 \pmod{4}$  et  $b \equiv 3 \pmod{4}$ . Or, dans ce cas le membre gauche est aussi impair.  $\square$

*Solution de l'exercice 10.* On montre le résultat par récurrence; on suppose qu'on a déjà trouvé  $k$  nombre premiers  $p_1, \dots, p_k$  qui conviennent. On considère  $\ell$  un facteur premier de  $a$  qui a une valuation impaire dans  $a$  et on pose  $a' = \frac{a}{\ell^{v_\ell(a)}}$ . Soit  $s$  un non-résidue quadratique modulo  $\ell$ . D'après le théorème chinois il existe un entier  $b$  tel que :

$$\begin{aligned} b &\equiv 1 \pmod{4} \\ b &\equiv 1 \pmod{(p_1 p_2 \dots p_k) a'} \\ b &\equiv s \pmod{\ell}. \end{aligned}$$

Puisque  $b$  est congruent à 1 modulo 4 on a  $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ . Or on a

$$\left(\frac{b}{a}\right) = \left(\frac{b}{a'}\right) \cdot \left(\frac{b}{\ell^{v_\ell(a)}}\right) = \left(\frac{s}{\ell^{v_\ell(a)}}\right) = -1.$$

Ainsi  $a$  est un non-résidue modulo  $b$  et, en particulier, modulo un de ses facteurs premiers. Comme  $b$  est relativement premier avec le produit  $(p_1 \dots p_k)$ , ce nouveau nombre premier est distinct de  $p_1, \dots, p_k$ .  $\square$

*Solution de l'exercice 3.* a) On écrit les nombres de 1 à  $N$  dans une liste. Pour tout  $i$  de 1 à  $v_p(N)$  on met un point à tous les multiples de  $p^i$ . Le nombre total de points est le membre droit de l'équation on doit montrer. D'autre part, tout nombre  $k \in [1, N]$  à reçu exactement  $v_p(k)$  points. Ainsi le nombre total de points est aussi égal au membre gauche de l'équation.

b) On applique le résultat précédent pour évaluer  $v_p(N!)$  et  $v_p(k!(N-k)!)$ . Pour tout  $i \in [1, v_p(k)]$  on a  $\lfloor \frac{N}{p^i} \rfloor = \lfloor \frac{k}{p^i} \rfloor + \lfloor \frac{N-k}{p^i} \rfloor$ . Pour  $i \in [v_p(k) + 1, v_p(N)]$  la différence  $\lfloor \frac{N}{p^i} \rfloor = \lfloor \frac{k}{p^i} \rfloor + \lfloor \frac{N-k}{p^i} \rfloor$  vaut 1.  $\square$

*Solution de l'exercice 4.* Soit d'abord  $A(x)$  et  $B(x)$  deux polynômes à coefficients entiers. Alors  $(A(x) + B(x))^p = a^p + b^p + \sum_{k=1}^p \binom{p}{k} a^k b^{p-k}$ . Comme tous les coefficients binomiaux qui apparaissent dans la somme de droite sont divisibles par  $p$  on obtient  $(A(x) + B(x))^p \equiv A(x)^p + B(x)^p \pmod{p}$ .

Par récurrence on obtient que la somme de n'importe quel nombre de polynômes élevée à la puissance  $p$ -ième est égale à la somme des puissances  $p$ -ième. Quand on applique ce résultat aux monômes  $a_0, a_1 x, \dots, a_d x^d$  de  $P(x)$  on trouve

$$P(x)^p \equiv a_0^p + a_1^p x^p + \dots + a_d^p (x^p)^d \pmod{p}.$$

D'après le petit théorème de Fermat on a  $a_i^p \equiv a_i \pmod p$  pour tout  $i \in [0, d]$ , ce qui permet de conclure.

*Remarque* : L'application  $P(x) \mapsto P(x)^p$  s'appelle morphisme de Frobenius et joue un rôle important dans l'étude des ensembles  $\mathbb{Z}/p\mathbb{Z}$ .  $\square$