Arithmétique des entiers

Solutions

Exercice 1 – On a les identités $2015 = 5 \cdot 13 \cdot 31$ et $2016 = 2^5 \cdot 3^2 \cdot 7$.

Exercice 2 – $\mathcal{D}_{12} = \{1, 2, 3, 4, 6, 12\}$ et $\mathcal{D}_{2^8} = \{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8\}$.

Exercice 3 –

1. Pour tout entier $n \geq 2$ et tout $k \in \{2, \ldots, , n\}$ on a les inégalités $N+k \geq n+2 > k$. L'entier N étant divisible par k, il en est de même pour $N + k$, qui possède alors un diviseur autre que 1 et lui-même et n'est donc pas premier.

2. D'après le point précédent, les dix entiers entiers consécutifs $11! + 2, \ldots, 11! + 11$ ne sont pas premiers. En fait, une recherche explicite montre que les plus petits entiers consécutifs non premiers sont $114, \ldots, 123$ (on vérifie de plus qu'il en est de même pour $124, 125$ et 126, ce qui donne 13 entiers consécutifs composés).

Exercice 4 – En notant n l'effectif de l'école, l'entier $n - 2$ est divisible par $3, 5$ et 7. Les entiers $3, 5$ et 7 étant premiers entre eux deux à deux, on en déduit que leur produit divise $n - 2$, soit $n - 2 = 105m$, avec m entier, ou encore $n = 105m + 2$. Les inégalités $100 \leq n \leq 200$ impliquent alors que $m = 1$, d'où $n = 107$.

Exercice 5 – Pour tout entier $b > 0$, l'entier b^3 divise a si et seulement si, pour tout nombre premier p, on a l'inégalité $v_p(b^3) \leq v_p(a)$. L'identité $v_p(b^3) = 3v_p(b)$ amène alors aux relations $v_2(b) \leq \frac{4}{3}, v_3(b) \leq 2, v_7(b) \leq \frac{1}{3}$ et $v_p(b) = 0$ pour tout $p > 7$. Tenant compte du fait que $v_p(b)$ est un entier, on en déduit que la plus grande valeur de b est $18 = 2 \cdot 3^2$.

Exercice 6 – Le petit théorème de Fermat affirme que p divise $2^p - 2$. On en déduit que p divise $2^p + 1$ si et seulement s'il divise $2^p + 1 - (2^p - 2) = 3$, d'où l'identité $p = 3$.

Exercice 7 – On a les factorisations $165 = 3 \cdot 5 \cdot 13$ et $143 = 11 \cdot 13$. Le ppcm de ces deux entiers est donc égal à $2145 = 3 \cdot 5 \cdot 11 \cdot 13$.

Exercice 8 –

1. On commence par déterminer une solution particulière (x_0, y_0). Dans le cas présent, sans utiliser l'algorithme d'Euclide, on remarque que les valeurs $x_0 = 2$ et $y_0 = -1$ conviennent. Les entiers 4 et 9 étant premiers entre eux, la solution générale est donnée par $x = 2 + 36n$ et $y = -1 - 36n$, avec n entier.

2. On procède en suivant la méthode présentée en cours : on commence par déterminer une identité de Bézout pour les entiers 18 et 7. Pour ce faire, on utilise l'algorithme d'Euclide, qui amène à l'identité $2\cdot 18 - 5\cdot 7 = 1$. On en déduit la solution particulière $x_0 = 4 = 2\cdot 2$ et $y_0 = -10 = -5\cdot 2$. Les entiers 7 et 18 étant premiers entre eux, leur ppcm est égal à $7\cdot 18 = 126$ et la solution générale est donnée par $x = 4 + 126n$ et $y = -10 - 126n$, avec n entier.

Exercice 9 – Supposons que l'entier $d = ax + by > 0$ divise a et b. Si c est un diviseur commun à a et b, soit $a = cu$ et $b = cv$, on obtient les identités $d = cux + cvy = c(ux + vy)$ et donc c divise d, d'où le résultat.

Exercice 10 –

1. L'entier cd divise ac et bc. Si x et y sont deux entiers tels que $d = ax + by$, on obtient l'identité $cd = acx + bcy$ et l'exercice précédent permet de conclure.

2. Par contraposée si p est un nombre premier divisant $\mathrm{pgcd}(a, bc) > 1$, il divise b ou c. L'entier a étant un multiple de p, on en déduit que p divise $\mathrm{pgcd}(a, b)$ ou $\mathrm{pgcd}(a, c)$, qui ne peuvent donc pas être tous deux égaux à 1.

3. Comme pour le point précédent, si p est un diviseur premier de $\mathrm{pgcd}(a^n, b^m) > 1$, il divise a^n (respectivement b^m) et donc a (respectivement b). Il s'en suit que $\mathrm{pgcd}(a, b)$ est un multiple de p et ne peut être égal à 1.

4. Posons $u = \frac{a}{d}$ et $v = \frac{b}{d}$. Le point 1 amène aux identités
$$d = \mathrm{pgcd}(a, b) = \mathrm{pgcd}(du, dv) = d\mathrm{pgcd}(u, v').$$
Les entiers u' et v' sont donc premiers entre eux et, en appliquant le point 3, il en est de même pour u'^n et v'^n. Finalement, en utilisant une fois de plus le point 1, on obtient les relations
$$\mathrm{pgcd}(a^n, b^n) = \mathrm{pgcd}(d^n u^n, d^n v^n) = d^n \mathrm{pgcd}(u^n, v^n) = d^n.$$

Exercice 11 – Pour tout nombre premier p divisant m, on a l'identité
$$v_p(m) = \max\{v_p(a), v_p(b)\}.$$
En posant
$$e_p = \begin{cases} v_p(a) \text{ si } v_p(a) \geq v_p(b), \\ \\ 0 \text{ sinon} \end{cases} \quad \text{et} \quad f_p = \begin{cases} v_p(b) \text{ si } v_p(a) < v_p(b), \\ \\ 0 \text{ sinon,} \end{cases}$$
les entiers $a' = \prod_{p|m} p^{e_p}$ et $b' = \prod_{p|m} p^{e_f}$ sont des diviseurs respectifs de a et b, premiers entre eux et vérifiant l'identité $m = a'b'$.

Exercice 12 – Si m et n sont deux entiers, on a l'identité
$$\max\{n, m\} + \min\{n, m\} = n + m.$$
La propriété découle alors des identités
$$\mathrm{pgcd}(a, b) = \prod_{p|ab} p^{\min\{v_p(a), v_p(b)\}} \quad \text{et} \quad \mathrm{ppcm}(a, b) = \prod_{p|ab} p^{\max\{v_p(a), v_p(b)\}},$$
les produits ci-dessus étant étendus à tous les diviseurs premiers p de ab.