Concepts de base en arithmétique : solutions des exercices.

Thomas Budzinski

1 Préliminaires

Pas d'exercices.

2 Divisibilité

Solution 2.1.

Il existe u et v tels que $b = au$ et $d = cv$ donc $bd = (ac)(uv)$ donc $ac \mid bd$.

Solution 2.2.

Si $n \mid n+7$, comme $n \mid n$, alors $n \mid (n+7) - n = 7$ donc n vaut 1 ou 7. Dans ces deux cas, on voit que n divise bien $n+7$.

Solution 2.3.

Si $n^2+1|n$, alors $n = 0$ ou $n^2+1 \leq n$. Mais si $n > 0$, alors $n^2+1 > n^2 \geq n$, ce qui est absurde, donc seul $n = 0$ est solution.

Solution 2.4.

Si n est pair, alors $2|n$ et $n|n(n+1)$ donc $n(n+1)$ est pair. Si n est impair, alors $2|n+1$ et $n+1|n(n+1)$ donc $n(n+1)$ est pair.

Solution 2.5.

n, $n+1$ et $n+2$ sont trois entiers consécutifs donc un des trois est divisible par 3, donc $n(n+1)(n+2)$ est divisible par 3 : on peut écrire $n(n+1)(n+2) = 3u$. De plus, $n(n+1)$ est pair par l'exercice précédent donc $n(n+1)(n+2)$ aussi, donc $3u$ est pair. Or, le produit de deux nombres impairs est impairs donc u doit être pair, donc $6 = 3 \times 2 \mid 3u$, d'où le résultat.

Solution 2.6.

On a $c = -an^2 - bn$. Or, $n \mid -an^2$ et $n \mid -bn$ donc $n \mid c$.

Solution 2.7.

On raisonne comme dans l'exercice précédent : $3 = -n^5 + 2n^4 + 7n^2 + 7n$ et n divise le membre de droite donc $n|3$ donc n vaut -3, -1, 1 ou 3. En testant ces quatre valeurs, on trouve que les seules solutions sont -1 et 3.

Solution 2.8.

On a $a \mid n(n+2) = n^2 + 2n$ donc $a \mid n^2 + n + 5 - (n^2 + 2n) = -n + 5$. On en déduit que $a \mid (n+2) + (-n+5) = 7$, puis que $a = 1$ ou $a = 7$.

Solution 2.9.

$$\begin{aligned}
\boxed{364} &= \boxed{154} \times 2 + \boxed{56} \\
\boxed{154} &= \boxed{56} \times 2 + \boxed{42} \\
\boxed{56} &= \boxed{42} \times 1 + \boxed{14} \\
\boxed{42} &= \boxed{14} \times 3 + \boxed{0}
\end{aligned}$$

Solution 2.10.

Pour tout entier d, d divise 10^{100} et $10^{121} + 10^{813} + 10$ si et seulement si d divise leur $PGCD$. On calcule donc ce PGCD avec l'alogrithme d'Euclide :

$$\begin{aligned}
\boxed{10^{121} + 10^{813} + 10} &= \boxed{10^{100}} \times (10^{21} + 10^{713}) + \boxed{10} \\
\boxed{10^{100}} &= \boxed{10} \times 10^{99} + \boxed{0}
\end{aligned}$$

Le PGCD vaut 10 donc les diviseurs communs sont les diviseurs de 10, soit -10, -5, -2, -1, 1, 2, 5 et 10. Il y en a 8.

Solution 2.11.

D'après la proposition précédente pour $q = 1$, $b = 10^9$ et $r = 5$ on a :

$$PGCD(10^9 + 5, 10^9) = PGCD(10^9, 5) = 5$$

car $5 \mid 10^9$.

Solution 2.12.

131 est premier (la vérification peut être un peu laborieuse...).
$221 = 13 \times 17$ n'est pas premier.

Solution 2.13.

1) Si $p \geq 3$ est premier, alors il est impair, donc $p-1$ et $p+1$ sont deux nombres pairs consécutifs, et un des deux est divisible par 4. Si c'est $p-1$, on peut écrire $p-1 = 4k$ donc $p = 4k+1$. Si c'est $p+1$ on peut écrire $p = 4k-1$.
2) Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers de la forme $4k-1$ notés $p_1 < p_2 < \cdots < p_r$ avec $p_1 = 3$, $p_2 = 7$ etc. Soit $n = 4(p_1 \dots p_r) - 1$: on a $n \geq 4p_1 - 1 \geq 11 > 2$ donc n est un produit de nombres premiers. Or, un produit de nombres de la forme $4k+1$ est de la forme $4k+1$ (la vérification est facile), donc n admet un facteur premier de la forme $4k-1$, qui doit être égal à un des p_i. Mais alors p_i divise $4p_1 \dots p_r$ donc p_i divise 1, d'où la contradiction.

Solution 2.14.

1) On a $PGCD(n, n+2) = PGCD(n, 2)$ donc n et $n+2$ sont premiers entre eux si et seulement si n et 2 sont premiers entre eux ssi n est impair.
2) On a $n^2 - 1 = (n+1)(n-1)$ et $(n^2 - 2n + 1) = (n-1)^2$ donc $n-1$ est un diviseur commun. Pour que les deux nombres soient premiers entre eux, il faut donc que $n-1$ soit égal à -1 ou 1, donc que $n = 0$ ou $n = 2$. Dans ces deux cas, $n^2 - 2n + 1 = 1$ donc les deux nombres sont bien premiers entre eux.

Solution 2.15.

On reprend les restes successifs de l'exercice 9 :

$$\begin{aligned}
\boxed{56} &= \boxed{364} - \boxed{154} \times 2 \\
\boxed{42} &= \boxed{154} - \boxed{56} \times 2 = \boxed{154} \times 5 - \boxed{364} \times 2 \\
\boxed{14} &= \boxed{56} - \boxed{42} = \boxed{364} \times 3 - \boxed{154} \times 7
\end{aligned}$$

Solution 2.16.

$2x+1$ est impair donc est premier avec 8 (car les seuls diviseurs de 8 sont 1, 2, 4 et 8) donc d'après le lemme de Gauss, si $2x+1 \mid 8y$ alors $2x+1 \mid y$.

Solution 2.17.

7 et 9 sont premiers entre eux et l'algorithme d'Euclide nous donne la solution particulière $(u_0, v_0) = (-3, -4)$. D'après ce qui précède, un couple (u, v) est donc solution ssi il existe $k \in \mathbb{Z}$ tel que $u = 7k-3$ et $v = 9k-4$.

Solution 2.18.

On a $PGCD(16, 26) = 2$. Si n est impair, l'équation n'a donc pas de solution. Si n est pair, on pose $n = 2n'$ et on est ramené à l'équation $8x + 13y = n'$ avec 8 et 13 premiers entre eux.
De plus, l'algorithme d'Euclide nous donne pour $n' = 1$ la solution $(x_0, y_0) = (-8, 5)$ donc pour tout n' on a une solution particulière $(-8n', 5n')$. Un couple (x, y) est donc solution ssi il existe $k \in \mathbb{Z}$ tel que $x = 13k - 8n'$ et $y = -8k + 5n'$.

Solution 2.19.

$18^{100} = (2 \times 3^2)^{100} = 2^{100} \times 3^{200}$ donc $v_3(18^{100}) = 200$.

Solution 2.20.

$2^{100} + 2^{200} = 2^{100} \times (1 + 2^{100})$ où le deuxième facteur est impair, donc n'admet pas 2 comme facteur premier. On a donc $v_2(2^{100} + 2^{200}) = 100$.

Solution 2.21.

1) Comptons combien de facteurs sont divisibles par 7 : il y en a $\lfloor \frac{100}{7} \rfloor = 14$. De plus, parmi ces 14 facteurs, 49 et 98 sont divisibles par $49 = 7^2$, et aucun des facteurs n'est divisibles par $7^3 = 243$. On a donc $v_7(n) = 14 + 2 = 16$.
2) Pour commencer, le nombre de zéros dans l'écriture décimale de n est le plus grand k tel que $10^k \mid n$. Or, $10^k \mid n$ ssi $2^k \mid n$ et $5^k \mid n$ (d'après le lemme de Gauss) donc on recherche le plus grand k tel que 2^k et 5^k divisent n. Il s'agit par définition de $\min\big(v_2(n), v_5(n)\big)$.
   Calculons maintenant $v_5(n)$: il y a 20 facteurs divisibles par 5 dont 4 divisibles par $5^2 = 25$ donc $v_5(n) = 20 + 4 = 24$.
   De plus, il y a 50 facteurs pairs donc $v_2(n) \geq 50 > 24$ donc la plus petite des deux valuations vaut 24 : il y a 24 zéros à la fin de l'écriture décimale de n.

Solution 2.22.

Le premier nombre a une valuation 5-adique non nulle mais pas le second (car son écriture décimale termine par un 7).

Solution 2.23.

Si $b = 0$ alors on a bien $a \mid b$. Sinon, $a \neq 0$ car si a était nul on aurait $0 \mid b^2$ donc $b^2 = 0$ et $b = 0$. On peut donc supposer $a, b \neq 0$.
L'hypothèse $a^2 \mid b^2$ revient alors à dire que pour tout p premier, $2v_p(a) \leq 2v_p(b)$ donc $v_p(a) \leq v_p(b)$ pour tout p d'où $a \mid b$.

Solution 2.24.

On a $v_p(a^2) \geq 1$ mais $v_p(a^2) = 2v_p(a)$ est pair donc $v_p(a^2) \geq 2$ et $p^2 \mid a^2$.

Solution 2.25.

Pour tout p premier, $v_p(ab) = v_p(a) + v_p(b)$. De plus, $v_p(PGCD(a,b)) = \min\big(v_p(a), v_p(b)\big)$ et $v_p(PPCM(a,b)) = \max\big(v_p(a), v_p(b)\big)$ donc $v_p(PGCD(a,b)PPCM(a,b)) = v_p(a) + v_p(b) = v_p(ab)$ pour tout p premier. ab et $PGCD(a,b)PPCM(a,b)$ ont donc la même décomposition en facteurs premiers donc sont égaux.

Solution 2.26.

On peut écrire $x = 8x'$ et $y = 8y'$. $x + y = 128$ donne alors $x' + y' = \frac{128}{8} = 16$ et l'exercice précédent donne $8x' \times 8y' = 8 \times 440$ donc $x'y' = \frac{440}{8} = 55$ donc x' et y' valent 1, 5, 11 ou 55. Comme $x' + y' = 16$, ils doivent valoir 5 et 11 donc les solutions sont $(x, y) = (40, 88)$ et $(88, 40)$.

Solution 2.27.

Si $p = 2^{k+1} - 1$ est premier, alors la décomposition du nombre n qui nous intéresse est $2^k p$: il s'agit des 2^i avec i entre 0 et k et des $2^i p$ avec i entre 0 et k. La somme des premiers vaut $2^{k+1} - 1 = p$ et la somme des seconds $(2^{k+1} - 1)p = p^2$. La somme des diviseurs de n vaut donc $p + p^2 = p(p+1) = 2^{k+1}(2^{k+1} - 1) = 2n$.
Pour la réciproque, on notera $s(n)$ la somme des diviseurs d'un entier n. Soit n un nombre parfait pair : on peut écrire $n = 2^k m$ avec m impair et $k = v_2(n)$. Se donner un diviseur de n revient alors à se donner un diviseur de 2^k (c'est-à-dire un 2^i avec i entre 0 et k) et un diviseur de m et à faire leur produit. En sommant sur tous les choix possibles, on en déduit $s(n) = s(2^k)s(m) = (2^{k+1} - 1)s(m)$, soit $2^{k+1}m = (2^{k+1} - 1)s(m)$. Or, $2^{k+1} - 1$ est premier avec 2^{k+1} donc d'après le lemme de Gauss il divise m. Notons $M = \frac{m}{2^{k+1}-1}$: si $M > 1$, alors les nombres de la forme 2^i, $2^i M$ et $2^i m$ sont tous distaincts et sont des diviseurs de n donc $s(n)$ vaut au moins leur somme, soit :

$$s(n) \geq (2^{k+1}-1)(m+M+1) = (2^{k+1}-1)(m+\frac{m}{2^{k+1}-1})+1 = 2^{k+1}m-m+m+2^{k+1}-1$$

donc $s(n) > 2n$ et n n'est pas parfait. On doit donc avoir $M = 1$ donc $m = 2^{k+1} - 1$. La somme des diviseurs de la forme 2^i ou $2^i m$ vaut alors exactement $2n$ et pour qu'il n'y ait pas d'autre diviseur il faut que m soit premier.

Solution 2.28.

$1000000 = 10^6 = 2^6 \times 5^6$ admet $(6+1)(6+1) = 49$ diviseurs.

Solution 2.29.

Soit n tel que $\tau(n) = 7$: on écrit $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en nombres premiers : on a $(\alpha_1 + 1) \dots (\alpha_r + 1) = 7$ mais 7 est premier donc $r = 1$ et $\alpha_1 = 6$ donc n est de la forme p^6 avec p premier. Si $n \leq 1000$, les seules possibilités sont $2^6 = 64$ et $3^6 = 729$.

Solution 2.30.

On peut regrouper les diviseurs de n par paires telles que le produit de chaque pair soit égal à n. Par exemple, pour 12 on regroupe 1 avec 12, 2 avec 6 et 3 avec 4. Si (a, b) est une de ces paires avec $a \leq b$, alors $n = ab \geq a^2$ donc $a \leq \sqrt{n}$: toute paire contient un élément $\leq \sqrt{n}$ donc il y a au plus $\sqrt{n}$ paires, soit $2\sqrt{n}$ diviseurs.

Remarque 2.1.

Cet argument des paires montre aussi que si on veut vérifier qu'un nombre n est premier, il suffit de vérifier qu'il n'a pas de diviseurs $\leq \sqrt{n}$ à part 1.

Solution 2.31.

$480 = 2^5 \times 3 \times 5$ donc 480 a $(5+1)(2+1)(2+1) = 54$ diviseurs dont 1, 2, 3, 4, et 5. Le nombre d'arbres par rangée doit être un de ces diviseurs mais pas 1, 2, 3, 4 ou 5. Le jardinier a donc $54 - 5 = 49$ possibilités.

Solution 2.32.

Écrivons $N = p_1^{\alpha_1} \dots p_r^{\alpha_r}$: on a $(\alpha_1 + 1) \dots (\alpha_r + 1) = 15 = 3 \times 5$ avec 3 et 5 premiers donc $r \leq 2$. Mais 2 et 3 divisent N donc $r = 2$, $p_1 = 2$ et $p_2 = 3$. De plus, on a $\alpha_1 + 1 = 5$ et $\alpha_2 + 1 = 3$ ou l'inverse. Mais dans le premier cas, $8 = 2^3 \mid N$ donc seul le deuxième marche, d'où $N = 2^2 \times 3^4 = 324$.

Solution 2.33.

n a un nombre impair de diviseurs ssi tous les $\alpha_i + 1$ sont impairs ssi tous les α_i sont pairs. C'est le cas si n est un carré. Réciproquement, si tous les α_i sont pairs, on peut écrire $\alpha_i = 2\beta_i$ et alors $n = \left(p_1^{\beta_1} \dots p_r^{\beta_r}\right)^2$.

Solution 2.34.

Si m et n sont premiers entre eux, on écrit $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $n = q_1^{\beta_1} \dots q_s^{\beta_s}$: les p_i et les q_j sont tous distincts, de sorte que :

$$\tau(mn) = (\alpha_1 + 1) \dots (\alpha_r + 1)(\beta_1 + 1) \dots (\beta_s + 1) = \tau(m)\tau(n)$$

Si $\tau(mn) = \tau(m)\tau(n)$, écrivons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $m = p_1^{\beta_1} \dots p_r^{\beta_r}$ (il se peut qu'un p_i divise m mais pas n, auquel cas on prend $\beta_i = 0$). On a alors :

$$(\alpha_1 + \beta_1 + 1) \dots (\alpha_r + \beta_r + 1) = (\alpha_1 + 1) \dots (\alpha_r + 1)(\beta_1 + 1) \dots (\beta_r + 1) \dots$$

ce qui se réécrit :

$$\frac{\alpha_1 + \beta_1 + 1}{(\alpha_1 + 1)(\beta_1 + 1)} \cdots \frac{\alpha_r + \beta_r + 1}{(\alpha_r + 1)(\beta_r + 1)} = 1$$

Mais pour tout i, on a $\frac{\alpha_i + \beta_i + 1}{(\alpha_i + 1)(\beta_i + 1)} = 1 - \frac{\alpha_i \beta_i}{(\alpha_i + 1)(\beta_i + 1)} \leq 1$. Pour que le produit soit égal à 1, il faut donc que chaque terme soit égal à 1 et donc que pour tout i on ait $\alpha_i \beta_i = 0$. Autrement dit, il n'existe aucun i tel que p_i divise à la fois m et n, donc m et n sont premiers entre eux.

3 Congruences

Solution 3.1.

$p = 2$ convient. Si $p \geq 3$, on raisonne modulo 2 : si $p \equiv 0 \pmod{n}$ alors p est pair et si $p \equiv 1 \pmod{n}$ alors $p+1$ est pair. Mais $p > 2$ et $p+1 > 2$ donc ils ne peuvent pas tous deux être premiers. 2 est donc la seule solution.

Solution 3.2.

$p = 2$ ne convient pas et $p = 3$ convient. Si $p \geq 4$ on raisonne modulo 3 : si $p \equiv 0 \pmod{3}$ alors $3 \mid p$. Si $p \equiv 1 \pmod{3}$ alors $3 \mid p+2$. Si $p \equiv 2 \pmod{3}$ alors $3 \mid p+4$. Un des trois nombres est donc divisible par 3 et ne peut valoir 3 donc les trois nombres ne sont pas tous premiers, donc 3 est la seule solution.

Solution 3.3.

48767621 est divisible ssi $4+8+7+6+7+6+2+1 = 41$ l'est, donc il n'est pas divisible par 9.

Solution 3.4.

98473092 est divisible par 11 ssi $-9+8-4+7-3+0-9+2 = -8$ l'est, donc il n'est pas divisible par 11.

Solution 3.5.

$3+6+4+5 = 18$ est divisible par 9 donc 9 divise 3645. 5 le divise aussi et 9 et 5 sont premiers entre eux donc $9 \times 5 = 45$ divise 3645.

Solution 3.6.

2 ne divise pas 127413 donc le PGCD est impair.
$1+9+3+1+1+6 = 21$ est divisible par 3 donc 193116 aussi. $1+2+7+4+1+3 = 18$ est divisible par 3 donc 127413 aussi, donc leur PGCD est divisible par 3.
$1+9+3+1+1+6 = 21$ n'est pas divisible par 9 donc 193116 non plus et le PGCD non plus.
$-1+9-3+1-1+6 = 11$ est divisible par 11 donc 193116 aussi. $-1+2-7+4-1+3 = 0$ est divisible par 11 donc 127413 aussi, et le PGCD aussi.
Le PGCD est divisible par 3 et 11 qui sont premiers entre eux, donc il est divisible par 33 d'après le lemme de Gauss.
Le PGCD n'est pas divisible par 9 donc il n'est pas divisible par 99.

Solution 3.7.

Le nombre est divisible par 33 ssi il est divisible par 3 et 11. Il est divisible par 11 ssi $-2+7-x+8-5+y=13-x+y$ l'est ssi $x-y \equiv 2 \pmod{11}$ ssi $x-y$ vaut 2 ou -9 (car x et y sont des chiffres). Cela laisse comme possibilités $(2,0)$, $(3,1)$, $(4,2)$, $(5,3)$, $(6,4)$, $(7,5)$, $(8,6)$, $(9,7)$ et $(0,9)$.
Il est divisible par 3 ssi $2+7+x+8+5+y=22+x+y$ l'est ssi $x+y \equiv 2 \pmod 3$. Les solutions sont donc $(2,0)$, $(5,3)$ et $(8,6)$.

Solution 3.8.

Seuls 1, 3, 5 et 7 sont impairs donc premiers avec 8, donc ce sont les inversibles modulo 8. De plus, on a $1 \times 1 \equiv 1 \pmod 8$, $3 \times 3 \equiv 9 \equiv 1 \pmod 8$, $5 \times 5 \equiv 25 \equiv 1 \pmod 8$ et $7 \times 7 \equiv 49 \equiv 1 \pmod 8$ donc ces nombres sont tous égaux à leur inverse modulo 8.

Solution 3.9.

On a besoin d'une relation de Bézout entre 37 et 53. On applique donc l'algorithme d'Euclide :

$$\begin{aligned}
\boxed{53} &= \boxed{37} \times 1 + \boxed{16} \\
\boxed{37} &= \boxed{16} \times 2 + \boxed{5} \\
\boxed{16} &= \boxed{5} \times 3 + \boxed{1}
\end{aligned}$$

Ainsi :

$$\begin{aligned}
\boxed{16} &= \boxed{53} \times 1 - \boxed{37} \times 1 \\
\boxed{5} = \boxed{37} - \boxed{16} \times 2 &= \boxed{37} \times 3 - \boxed{53} \times 2 \\
\boxed{1} = \boxed{16} - \boxed{5} \times 3 &= \boxed{53} \times 7 - \boxed{37} \times 10
\end{aligned}$$

On a donc $37 \times 10 \equiv 1 \pmod{53}$ donc l'inverse de 37 modulo 53 est 10.

Solution 3.10.

a) $6^{11} + n + 2 \equiv (-1)^{11} + 2 + n \equiv n + 1 \pmod 7$ donc ce sont les n congrus à -1 modulo 7.
b) On a $705432^{50} \equiv (705432^{10})^5 \equiv 1^5 \equiv 1 \pmod{11}$, en utilisant à l'avant-dernière étape le petit théorème de Fermat, donc le reste vaut 1.
c) $5^{6n} + 5^n + 2 \equiv 1 + 5^n + 2 \equiv 5^n + 3 \pmod 7$. Or, si $n = 6k + 1$ on trouve $5^n + 3 \equiv 5^{6k} \times 5 + 3 \equiv 1 \pmod 7$. De même, si $n = 6k + 2$ on obtient $0 \pmod 7$. Si $n = 6k + 3$ on obtient $2 \pmod 7$. Si $n = 6k + 4$ on obtient $5 \pmod 7$. Si $n = 6k+5$ on obtient $6 \pmod 7$ et si $n = 6k$ on obtient $4 \pmod 7$. Les solutions sont donc les n congrus à 2 modulo 6.
d) Pour tout n entier $81n^5 - 45n^3 + 4n \equiv n^5 - n \equiv 0 \pmod 5$ en utilisant le petit théorème de Fermat à la fin, donc tous les entiers n marchent.

Solution 3.11.

On étudie les puissances de 7 modulo 10 : $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$ et $7^4 \equiv 1 \pmod{10}$. Il faut donc s'intéresser à l'exposant modulo 4 : $3^9 \equiv (-1)^9 \equiv -1 \pmod 4$ donc on peut poser $3^9 = 4k + 3$, de sorte que :

$$7^{3^9} \equiv (7^4)^k \times 7^3 \equiv 1^k \times 3 \equiv 3 \pmod{10}$$

donc le dernier chiffre est 3.

Solution 3.12.

$27^{12} = (3^3)^{12} = 3^{36}$ qui est divisible par 3 et 9 mais pas par 5, 7 et 11.

Solution 3.13.

Corrigé dans le cours.

Solution 3.14.

On a :
$0^2 \equiv 0 \pmod 5$
$1^2 \equiv 1 \pmod 5$
$2^2 \equiv 4 \pmod 5$
$3^2 \equiv 4 \pmod 5$
$4^2 \equiv 1 \pmod 5$
donc les carrés modulo 5 sont 0, 1 et 4. De même, on trouve que les carrés modulo 8 sont 0, 1 et 4.

Solution 3.15.

Non. On raisonne modulo 8 : si a, b et c sont solutions, alors $a^2+b^2+c^2 \equiv 7 \pmod 8$ donc au moins un des carrés est impair (a par exemple) donc congru à 1 modulo 8, ce qui laisse $b^2+c^2 \equiv 6 \pmod 8$. Comme b^2 est congru à 0, 1 ou 4, c^2 doit donc être congru à 6, 5 ou 2, ce qui est impossible.

Solution 3.16.

Oui : $10^2 \equiv 100 \equiv -3 \pmod{103}$.

Solution 3.17.

Notons x le nombre considéré : $1000x = 3157,157157\cdots = 3154 + x$ donc $x = \frac{3154}{999}$, qui est irréductible (algorithme d'Euclide par exemple).

Solution 3.18.

Si $\sqrt[n]{a} = \frac{x}{y}$, alors $x^n = ay^n$ donc pour tout p, $nv_p(x) = v_p(a) + nv_p(y)$ donc $v_p(a) = n(v_p(x) - v_p(y))$ est divisible par n pour tout p, donc a est la puissance n-ième d'un nombre entier, ce qu'on avait supposé faux.

Solution 3.19.

Si $\sqrt{2}+\sqrt{3} = \frac{x}{y}$ avec x et y premiers entre eux, alors $x^2 \equiv y^2(2+3+2\sqrt{6})$ soit $x^2-5y^2 = 2y^2\sqrt{6}$ donc $(x^2-5y^2)^2 = 24y^4$ soit $x^4-10x^2y^2+y^4 = 0$. Si p est un diviseur premier de x, alors il divise les deux premiers termes donc il divise y^4 donc p divise y, ce qui est absurde car on a supposé x et y premiers entre eux. x n'a donc pas de diviseur premier donc $x=1$ ou $x=-1$ et de même pour y. On a donc $\sqrt{2}+\sqrt{3}$ égal à 1 ou à -1, ce qui est absurde.

4 Utilisation de factorisations

Solution 4.1.

On a $a^n-1 = (a-1)(a^{n-1}+a^{n-2}+\cdots+1$. Le second facteur est toujours strictement plus grand que 1 donc si a^n-1 est premier, le premier facteur vaut 1, soit $a=2$. Si de plus n n'est pas premier, écrivons $n = dd'$ avec $d \neq 1, n$: on a $2^n-1 = (2^d-1)(2^{d(d'-1)}+2^{d(d'-2)}+\cdots+1$. Le premier facteur est plus grand que 1 car $d>1$ et le second l'est car $d'>1$ donc il n'y a pas que le dernier terme, donc si n n'est pas premier, a^n-1 ne peut pas l'être.

Solution 4.2.

Si n n'est pas une puissance de 2, il admet un diviseur impair d. En posant $n = dd'$ on obtient $2^n + 1 = (2^{d'} + 1)(2^{d'(d-1)} - 2^{d'(d-2)} + ... - 2^{d'} + 1)$, où les deux facteurs sont strictement supérieurs à 1, donc $2^n + 1$ ne peut pas être premier.

Solution 4.3.

L'équation se réécrit $(x - y)(x^2 + xy + y^2) = 24$ donc si (x, y) est solution alors $x^2 + xy + y^2 \mid 24$. De plus, $x \geq y$. Si $y \geq 3$ alors $x^2 + xy + y^2 \geq y^2 + y^2 + y^2 \geq 27$ ce qui est impossible. y vaut donc 0, 1 ou 2. Si $y = 0$ on obtient $x^3 = 0$ qui n'a pas de solution. Si $y = 1$ on obtient $x^3 = 25$ qui n'a pas de solution. Si $y = 2$ on obtient $x^3 = 32$ qui n'a pas de solution. L'équation n'a donc pas de solution.

Solution 4.4.

Solution 4.5.

L'équation se réécrit $(y + x)(xy - p) = 5p$ donc $x + y$ peut valoir 1, 5, p et $5p$. Quitte à échanger x et y, on suppose $x \leq y$.
Si $x + y = 1$ alors par exemple $x = 0$ et $y = 1$ ce qui donne $1 - p = 5p$, absurde.
Si $x + y = 5$, alors $xy - p = p$ donc $xy = 2p$. (x, y) peut valoir $(0, 5)$, $(1, 4)$ ou $(2, 3)$. Les deux dernières donnent des solutions pour $p = 2$ et $p = 3$.
Si $x + y = p$ alors $xy - p = 5$ soit $xy - x - y = 5$ donc $(x - 1)(y - 1) = 6$. Les valeurs possibles de (x, y) sont $(2, 7)$ et $(3, 4)$. La première donne $p = 9$ qui n'est pas premier. La seconde donne une solution pour $p = 7$.
Si $x + y = 5p$ alors $xy - p = 1$ soit $5xy + 1 = x + y$. Si $x, y \geq 2$ alors $xy > x, y$ donc $5xy + 1 > x + y$ donc on a $x = 1$ ou $x = 0$. Si $x = 1$ alors $5y + 1 = y + 1$ et $y = 0$, absurde. Si $x = 0$, on obtient $y = 1$ et $5p = 1$, absurde.
Les p qui marchent sont donc 2, 3 et 7.

Solution 4.6.

Pour $n = 0$ il n'y a pas de solution. Pour $n = 1$, $m = 0$ marche. Pour $n = 2$, $m = 1$ marche. Si $n \geq 3$, on raisonne modulo 8 : on a $8 \mid 2^n$ donc $3^m \equiv 2^n - 1 \equiv 7 \pmod 8$. Mais si $m = 2k$ alors $3^m \equiv 9^k \equiv 1^k \equiv 1 \pmod 8$, et si $m = 2k + 1$ alors $3^m \equiv 9^k \times 3 \equiv 3 \pmod 8$. Il n'y a donc pas de solution pour $n \geq 3$.
Passons la seconde équation : si $n = 0$ il n'y a pas de solution. Si $n = 1$ alors $m = 1$ est solution. Pour $n \geq 2$, on a $3^m \equiv 2^n + 1 \equiv 1 \pmod 4$ donc m doit être pair. On pose donc $m = 2m'$. L'équation se réécrit $3^{2m'} - 1 = 2^n$, soit $(3^{m'} + 1)(3^{m'} - 1) = 2^n$. Les nombres $3^{m'} + 1$ et $3^{m'} - 1$ sont donc deux puissances de 2 distantes de 2, donc valent 2 et 4, ce qui donne $m' = 1$ donc $m = 2$ et $n = 3$.

Solution 4.7.

L'équation se réécrit $2^a 3^b = c^2 - 9 = (c+3)(c-3)$. Si $b = 0$, alors $c-3$ et $c+3$ sont deux puissances de 2 espacées de 6 donc valent 2 et 8, ce qui donne la solution $(4, 0, 5)$. Si $a = 0$, alors $c-3$ et $c+3$ sont deux puissances de 3 espacées de 6 donc valent 3 et 9, ce qui donne la solution $(0, 3, 6)$.
On suppose donc $a, b \geq 1$: $(c+3)(c-3)$ est divisible par 6 et $c+3 \equiv c-3 \pmod 6$ donc tous deux sont divisibles par 6. On écrit $c-3 = 6k$ et $c+3 = 6(k+1)$. L'équation se réécrit $2^a 3^b = 36k(k+1)$ donc $a, b \geq 2$ et $2^{a-2} 3^{b-2} = k(k+1)$. Si $k = 1$, on trouve $2^{a-2} 3^{b-2} = 2$ donc $a = 3$ et $b = 2$ et on trouve la solution $(3, 2, 9)$.
Si $k > 1$, alors k et $k+1$ sont premiers entre eux donc un seul est divisible par 2 et l'autre par 3, donc $a-2$ et $b-2$ vérifient une des deux équations de l'exercice précédent. En utilisant l'exercice précédent, on trouve comme seules solutions $(4, 3, 21)$, $(3, 2, 9)$ (déjà vue plus haut) et $(5, 4, 51)$.
On a donc finalement 5 triplets solutions : $(4, 0, 5)$, $(0, 3, 6)$, $(3, 2, 9)$, $(4, 3, 21)$ et $(5, 4, 51)$.