Université Aix-Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

TD1 : Arithmétique
corrigé partiel

Exercice 4.

1. Par divisions euclidiennes successives, on a

$$10672 = 2.4147 + 2378 \qquad 4147 = 1.2378 + 1769 \qquad 2378 = 1.1769 + 609$$

$$1769 = 2.609 + 551 \qquad 609 = 1.551 + 58 \qquad 551 = 9.58 + 29 \qquad 58 = 2.29.$$

En en déduit que $\text{pgcd}(10672, 4147) = \text{pgcd}(4147, 2378) = \text{pgcd}(2378, 1769) = \text{pgcd}(1769, 609) = \text{pgcd}(609, 551) = \text{pgcd}(551, 58) = \text{pgcd}(58, 29) = 29$.

Pour déterminer le ppcm de 4235 et 2156, le plus simple est de diviser leur produit par leur pgcd. Or, par divisions euclidiennes successives, on a

$$4235 = 1.2156 + 2079 \qquad 2156 = 1.2079 + 77 \qquad 2079 = 27.77.$$

On en déduit que $\text{pgcd}(4235, 2079) = \text{pgcd}(2079, 77) = 77$. En remontant un peu les calculs, on obtient même $2156 = 2079 + 77 = 27.77 + 77 = 28.77$. Au final, cela donne $\text{ppcm}(4235, 2079) = \frac{4235.2156}{77} = 4235.28 = 118580$.

2. (a) Par divisions euclidiennes successives, on a

$$9 = 1.7 + 2 \qquad 7 = 3.2 + 1,$$

ce qui, en remontant les calculs, donne $1 = 7 - 3.2 = 7 - 3.(9 - 1.7) = 4.7 - 3.9$.

(b) Par le même procédé, on obtient

$$93 = 2.41 + 11 \qquad 41 = 3.11 + 8 \qquad 11 = 1.8 + 3 \qquad 8 = 2.3 + 2 \qquad 3 = 1.2 + 1$$

et donc

$$\begin{aligned} 1 &= 3 - 1.2 = 3 - (8 - 2.3) \\ &= 3.3 - 8 = 3.(11 - 1.8) - 8 \\ &= 3.11 - 4.8 = 3.11 - 4.(41 - 3.11) \\ &= 15.11 - 4.41 = 15.(93 - 2.41) - 4.41 \\ &= 15.93 - 34.41. \end{aligned}$$

(c) On a ici $15 = 3.5$, $33 = 3.11$ et $55 = 5.11$. Il est donc impossible d'obtenir 1 comme combinaison linéaire de seulement deux de ces entiers, car aucune paire ne sont premiers entre eux. Néanmoins, il est possible d'exprimer $3 = \text{pgcd}(15, 33)$ comme combinaison linéaire de 15 et 33, puis 1 comme combinaison linéaire de 3 et 55 puisque $\text{pgcd}(3, 55) = 1$. En procédant comme précédemment, on obtient alors $33 = 2.15 + 3$, donc $3 = 1.33 - 2.15$; et ensuite $55 = 18.3 + 1$, donc $1 = 1.55 - 18.3 = 1.55 - 18(33 - 2.15) = 36.15 - 18.33 + 1.55$.

Exercice 5. En notant, pour tout $n_1, n_2 \in \mathbb{Z}^*$, $D(n_1, n_2)$ l'ensemble des diviseurs communs à n_1 et n_2, montrons par double inclusions que $D(a, b) = D(a, a^2 + b) = D(a + b, 3a + 2b)$; le résultat s'en déduira en en considérant le plus petit élément.

Soit $k \in D(a, b)$, alors il existe $k_a, k_b \in \mathbb{Z}^*$ tels que $a = kk_a$ et $b = kk_b$. On a alors $a^2 + b = k^2k_a^2 + kk_b = k.(kk_a^2 + k_b)$ et donc $k \in D(a, a^2 + b)$. Similairement, on a $a + b = kk_a + kk_b = k(k_a + k_b)$ ainsi que $3a+2b = 3kk_a+2kk_b = k(3k_a+2k_b)$, et donc $k \in D(a+b, 3a+2b)$. On en déduit que $D(a, b) \subset D(a, a^2b)$ et $D(a, b) \subset D(a + b, 3a + 2b)$.

Réciproquement, soit $k \in D(a, a^2+b)$, alors k divise a et $b = (a^2+b) - a^2$, donc $k \in D(a,b)$. On en déduit $D(a, a^2+b) \subset D(a,b)$ et donc $D(a,b) = D(a, a^2+b)$.

De même, soit $k \in D(a+b, 3a+2b)$, alors k divise $a = (3a+2b) - 2(a+b)$, ainsi que $b = 3(a+b) - (3a+2b)$. On en déduit $D(a+b, 3a+2b) \subset D(a,b)$ et donc $D(a,b) = D(a+b, 3a+2b)$.

Exercice 6.

1. Si n_1 divise n_2, alors il existe $k \in \mathbb{N}^*$ tel que $n_2 = kn_1$ et, par identité remarquable, on a

$$2^{n_2} - 1 = 2^{kn_1} - 1 = (2^{n_1})^k - 1^k = (2^{n_1} - 1)\left(\sum_{i=0}^{k-1} 2^{in_1}\right),$$

   dont on déduit que $2^{n_1} - 1$ divise $2^{n_2} - 1$.

2. On écrit $n_2 = qn_1 + r$ la division euclidienne de n_2 par n_1. On a alors

$$2^{n_2} - 1 = 2^{qn_1+r} - 1 = 2^{qn_1}.2^r - 1 = 2^{qn_1}.2^r - 2^r + 2^r - 1 = 2^r(2^{qn_1} - 1) + 2^r - 1.$$

   Or d'après la question précédente, $2^{qn_1} - 1$ s'écrit sous la forme $k.(2^{n_1} - 1)$ avec $k \in \mathbb{Z}$. On en déduit que $2^{n_2} - 1 = 2^r k(2^{n_1} - 1) + 2^r - 1$. Or $0 \leq 2^r - 1 < 2^{n_1} - 1$ puisque $0 \leq r < n_1$. Par unicité de la division euclidienne, on en déduit que le reste de la division euclidienne de $2^{n_2} - 1$ par $2^{n_1} - 1$ vaut bien $2^r - 1$.

3. Nous allons donner trois preuves de ce résultat.

   Une première, algorithmique : Avec l'algorithme d'Euclide appliqué à n_1 et n_2, on construit une suite finie d'entiers $a_1, a_2, \cdots, a_{\ell+1}$ tels que $a_1 = n_1$, $a_2 = n_2$, a_{k+1} est le reste de la division euclidienne de a_{k-1} par a_k, $a_\ell = \text{pgcd}(n_1, n_2)$ et $a_{\ell+1} = 0$. D'après la question précédente, en appliquant le même algorithme à $2^{n_1} - 1$ et $2^{n_2} - 1$, on obtiendra successivement les $2^{a_k} - 1$, l'algorithme se terminant par $2^{a_{\ell+1}} - 1 = 0$. On en conclut alors que $\text{pgcd}(2^{n_1} - 1, 2^{n_2} - 1) = 2^{a_\ell} - 1 = 2^{\text{pgcd}(n_1,n_2)} - 1$.

   Une seconde, récursive : Montrons le résultat par récurrence sur $m := \max(n_1, n_2)$. Le résultat est vrai lorsque $n_1 = n_2 = 1$. En effet, dans ce cas, $\text{pgcd}(2^1 - 1, 2^1 - 1) = \text{pgcd}(1,1) = 1 = 2^1 - 1 = 2^{\text{pgcd}(1,1)} - 1$. Supposons maintenant le résultat jusqu'à m et considérons $n_1, n_2 \in \mathbb{N}^*$ tels que $\max(n_1, n_2) = m + 1$. Quitte à échanger les rôles de n_1 et n_2, on peut supposer que $n_1 = m + 1$ et $n_2 \leq m + 1$. Si $n_2 = m + 1$ alors, comme ci-dessus, le résultat est vrai car $\text{pgcd}(2^{n_1} - 1, 2^{n_2} - 1) = \text{pgcd}(2^{m+1} - 1, 2^{m+1} - 1) = 2^{m+1} - 1 = 2^{\text{pgcd}(m+1,m+1)} - 1 = 2^{\text{pgcd}(n_1,n_2)} - 1$. Autrement, on a $n_2 \leq m$. Posons alors $n_1 = qn_2 + r$ la division euclidienne de n_1 par n_2. D'après la question 2., le reste de la division euclidienne de $2^{n_1} - 1$ par $2^{n_2} - 1$ vaut $2^r - 1$ et on a $\text{pgcd}(2^{n_1} - 1, 2^{n_2} - 1) = \text{pgcd}(2^{n_2} - 1, 2^r - 1)$. Or $0 \leq r < n_2 \leq m$, donc par HR, $\text{pgcd}(2^{n_2} - 1, 2^r - 1) = 2^{\text{pgcd}(n_2,r)} - 1 = 2^{\text{pgcd}(n_1,n_2)} - 1$. Le résultat est donc vrai au rang $m + 1$ et, par le principe de raisonnemment par récurrence, il est vrai pour tout $m \in \mathbb{N}^*$, donc pour tous $n_1, n_2 \in \mathbb{N}^*$.

   Une troisième, par double divisiblité : Puisque $\text{pgcd}n_1, n_2$ divise n_1 et n_2, on déduit de la question 1. que $2^{\text{pgcd}(n_1,n_2)} - 1$ divise $2^{n_1} - 1$ et $2^{n_2} - 1$, et donc divise $\text{pgcd}(2^{n_1} - 1, 2^{n_2} - 1)$.

   Réciproquement, d'après le théorème de Bachet–Bézout, il existe $a, b \in \mathbb{Z}$ tels que $an_1 + bn_2 = \text{pgcd}(n_1, n_2)$. On a alors

$$2^{\text{pgcd}(n_1,n_2)} - 1 = 2^{an_1+bn_2} - 1 = 2^{an_1}.2^{bn_2} - 1 = 2^{an_1}(2^{bn_2} - 1) + 2^{an_1} - 1.$$

   Or, d'après la question 1., il existe $k_1, k_2 \in \mathbb{Z}$ tels que $2^{an_1} - 1 = k_1(2^{n_1} - 1)$ et $2^{bn_2} - 1 = k_2(2^{n_2} - 1)$, on a donc

$$2^{\text{pgcd}(n_1,n_2)} - 1 = 2^{an_1}k_2(2^{n_2} - 1) + k_1(2^{n_1} - 1) = A(2^{n_2} - 1) + B(2^{n_1} - 1)$$

   avec $A, B \in \mathbb{Z}$. On en déduit que, puisqu'il divise simultanément $2^{n_1} - 1$ et $2^{n_2} - 1$, $\text{pgcd}(2^{n_1} - 1, 2^{n_2} - 1)$ divise également $2^{\text{pgcd}(n_1,n_2)} - 1$. La relation de divisibilité étant une relation d'ordre sur les entiers positifs, on en déduit que $\text{pgcd}(2^{n_1} - 1, 2^{n_2} - 1) = 2^{\text{pgcd}(n_1,n_2)} - 1$.

Exercice 7.

1. L'entier N_0 est égal au produit des 20 premiers entiers (19 en enlevant 1). Or d'après le lemme d'Euclide, tout diviseur premier doit diviser l'un de ces facteurs, et doit donc être inférieur à 20. Réciproquement, tout nombre premier inférieur à 20 apparait dans le produit et divise donc N_0. On en déduit que N_0 possède huit diviseurs premiers, à savoir :

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19.$$

2. Pour connaitre le nombre total de diviseurs de N_0, le plus simple est d'écrire sa décomposition en facteurs premiers. Pour cela, il suffit de déterminer la factorisation de chacun des entiers entre 2 et 20. cela donne :

$$2=2 \quad 3=3 \quad 4=2^2 \quad 5=5 \quad 6=2.3 \quad 7=7 \quad 8=2^3 \quad 9=3^2 \quad 10=2.5 \quad 11=11$$

$$12=2^2.3 \quad 13=13 \quad 14=2.7 \quad 15=3.5 \quad 16=2^4 \quad 17=17 \quad 18=2.3^2 \quad 19=19 \quad 20=2^2.5.$$

Au final, on obtient $N_0 = 2^{18}.3^8.5^4.7^2.11.13.17.19$. Maintenant, pour obtenir un diviseur de N_0, il faut et suffit de choisir, pour chacun des facteurs premiers, une multiplicité inférieure à celle de N_0. Cela fait 19 possibilités pour la puissance de 2 (la multiplicité peut être 0), 9 pour 3, 5 pour 5, 3 pour 7 et 2 pour 11, 13, 17 et 19. Par unicité de la factorisation en facteurs premiers, chacun de ces diviseurs seront alors bien distincts. Au final, N_0 a donc $19.9.5.3.2.2.2.2 = 2^4.3^3.5.19 = 41040$ diviseurs distincts.

Exercice 8. L'entier 3 étant premier, la plus grande puissance de 3 divisant 100! correspond à la multiplicité de 3 dans la décmposition de 100! en facteurs premiers. Il suffit donc de déterminer quels sont les entiers entre 2 et 100 que 3 divise et avec quelle multiplicité. Or 1 entier sur 3 est divisible par 3, 1 sur 9 est divisible par $9 = 3^2$, 1 sur 27 est divisible par $27 = 3^2$ et 1 sur 81 est divisible par $81 = 3^4$. En-dessous de 100, aucun n'est divisible par une puissance plus grande de 3. Or, par division euclidienne, on a

$$100 = 33.3 + 1 \qquad 100 = 11.9 + 1 \qquad 100 = 3.27 + 19 \qquad 100 = 1.81 + 19.$$

Il y a donc 33 termes qui contiennent un facteur 3, 11 qui en contiennent au moins un de plus, 3 qui en ont au moins un troisième et 1 seul qui en contient même un dernier. Au final, 3 apparait $33+11+3+1 = 48$ fois, et on a donc $100! = 3^{48}.k_0$ avec $k_0 \in \mathbb{N}^*$ non divisible par 3.

Exercice 11.

1. On a $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ et donc p divise

$$p.(p-1)! = p! = k!(p-k)!\binom{p}{k} = 2.3.\cdots.k.2.3.\cdots.(p-k).\binom{p}{k}.$$

Or, p étant premier, il divise l'un de ces facteurs d'après le lemme d'Euclide. Mais, hormis $\binom{p}{k}$, tous ces facteurs sont strictement plus petits que p et ne peuvent donc pas être divisible par p. On en déduit que p divise $\binom{p}{k}$.

2. Le résultat est clairement vrai pour $n = 1$. Supposons-le vrai pour n, on a alors

$$\begin{aligned}(n+1)^p - (n+1) &= \left(\sum_{k=0}^{p}\binom{p}{k}n^k\right) - n - 1 \\ &= \left(1 + n^p + \sum_{k=1}^{p-1}\binom{p}{k}n^k\right) - n - 1 \\ &= n^p - n + \sum_{k=1}^{p-1}\binom{p}{k}n^k.\end{aligned}$$

Or, par HR, $n^p - n$ est divisible par p, et d'après la question précédente, chaque terme de la somme est également divisible par p. On en déduit que $(n+1)^p - (n+1)$ est lui-même divisible par p. D'après le principe de raisonnement par récurrence, le résultat est donc vrai pour tout $n \in \mathbb{N}^*$.

3. Supposons d'abord que n est non divisible par p. Puisque p est premier, n et p sont alors premiers entre eux. Or, d'après la question précédente, p divise $n^p - n = n(n^{p-1} - 1)$. On en déduit par le lemme de Gauss que p divise $n^{p-1} - 1$.

   Supposons maintenant que p divise n, alors il divise n^p et ne peut donc pas diviser $n^p - 1$.

Exercice 16.

1. Par calcul direct, on a

$$F_0 = 1 \qquad F_1 = 1 \qquad F_2 = 2 \qquad F_3 = 3 \qquad F_4 = 5$$

$$F_5 = 8 \qquad F_6 = 13 \qquad F_7 = 21 \qquad F_8 = 34 \qquad F_9 = 55.$$

2. Montrons cela par récurrence généralisée sur n. Le résultat est vrai pour $n = 0$ et $n = 1$. Supposons le résultat vrai jusqu'au rang n et considérons le reste r de la division euclidienne de $n + 2$ par 3.
   Si $r = 0$ **:** alors $(n + 1) + 1 = n + 2$ est divisible par 3, mais ni $n + 1$ ni $(n - 1) + 1 = n$ ne le sont. Par HR, les entiers F_n et F_{n-1} sont donc impairs, et $F_{n+1} = F_n + F_{n-1}$ pair.
   Si $r = 1$ **:** alors $(n + 1) + 1 = n + 2$ et $(n - 1) + 1 = n$ ne sont pas divisibles par 3, mais $n + 1$ l'est. Par HR, F_n est pair et F_{n-1} impair. On en déduit que $F_{n+1} = F_n + F_{n-1}$ est impair.
   Si $r = 2$ **:** alors $(n + 1) + 1 = n + 2$ et $n + 1$ ne sont pas divisibles par 3, mais $(n - 1) + 1 = n$ l'est. Par HR, F_n est impair et F_{n-1} pair. On en déduit que $F_{n+1} = F_n + F_{n-1}$ est impair.

   Le propriété est donc encore vraie au rang $n + 1$.

   D'après le principe de raisonnement par récurrence, la propriété est donc vraie pour tout $n \in \mathbb{N}$.
3. Commençons par remarquer que, pour tous entiers $a, b \in \mathbb{N}^*$, $\text{pgcd}(a, a + b) = \text{pgcd}(b, a)$. En effet, tout diviseur commun à a et b divisera également $a + b$ et, réciproquement, tout diviseur commun $a + b$ et a divisera également $b = (a + b) - a$.

   On peut alors montrer que $\text{pgcd}(F_n, F_{n+1}) = 1$ par récurrence sur $n \in \mathbb{N}$. On a en effet $\text{pgcd}(F_1, F_1) = \text{pgcd}(1, 1) = 1$ et, pour tout $n \in \mathbb{N}$, $\text{pgcd}(F_{n+1}, F_{n+2}) = \text{pgcd}(F_{n+1}, F_{n+1} + F_n) = \text{pgcd}(F_n, F_{n+1})$. Cela permet d'initialiser la récurrence et assure le passage du rang n au rang $n + 1$. D'après le principe de raisonnement par récurrence, la propriété est donc vraie pour tout $n \in \mathbb{N}$.

Exercice 17. Ceci est un lemme important en arithmétique, corollaire du lemme de Gauss.

Puisque q divise n, il existe $k \in \mathbb{Z}$ tel que $n = kq$. Mais alors p divise kq tout en étant premier avec q ; d'après le lemme de Gauss p divise donc k et il existe $k' \in \mathbb{Z}$ tel que $k = k'p$. On a donc $n = kq = k'pq$, et pq divise n.

Exercice 18.

1. Commençons par déterminer une solution à l'aide de l'agorithme d'Euclide. Par divisions euclidiennes successives, on a

$$2045 = 31.64 + 61 \qquad 64 = 1.61 + 3 \qquad 61 = 20.3 + 1,$$

   puis, en remontant les calculs

$$1 = 61 - 20.3 = 61 - 20(64 - 61) = 21.61 - 20.64 = 21(2045 - 31.64) - 20.64 = 21.2045 - 671.64.$$

   On en déduit que $(21, 671)$ est solution.

   Considéront maintenant une autre solution (x, y). On a alors $2045x - 64y = 1 = 2045.21 - 64.671$ et donc $2045(x - 21) = 64(y - 671)$. Puisque, d'après les calculs précédents, $\text{pgcd}(64, 2045) = 1$, on en déduit par le lemme de Gauss que 64 divise $x - 21$. Il existe donc $k \in \mathbb{Z}$ tels que $x - 21 = 64k$, ce qui donne $64(y - 671) = 2045.64k$ et donc $y = 2045k + 671$. On en conlut que $(x, y) = (64k + 21, 2045k + 671)$

   Réciproquement, on vérifie par un calcul direct que pour tout $k \in \mathbb{Z}$, $(64k+21, 2045k+671)$ est bien solution de l'équation. On en déduit que l'ensemble des solutions est $\{(64k + 21, 2045k + 671) \mid k \in \mathbb{Z}\}$.

2. Dans le but d'éventuellement simplifier l'équation, commençons par déterminer le pgcd de 171 et 207. Par divisions euclidiennes successives, on a

$$207 = 171 + 36 \qquad 171 = 4.36 + 27 \qquad 36 = 27 + 9 \qquad 27 = 3.9.$$

On en déduit que $\text{pgcd}(171, 207) = 9$, or $324 = 9.36$ est bien divisible par 3. L'équation peut donc se réécrire

$$19x + 23y = 36.$$

On peut alors simplifier chaque étape de l'algorithme d'Euclide ci-dessus en divisant tout par 9 :

$$23 = 19 + 4 \qquad 19 = 4.4 + 3 \qquad 4 = 3 + 1,$$

ce qui, en remontant les calculs, donne

$$1 = 4 - 3 = 4 - (19 - 4.4) = 5.4 - 19 = 5.(23 - 19) - 19 = 5.23 - 6.19.$$

En multipliant tout par 36, on obtient que $(-6.36, 5.36) = (-216, 180)$ est solution.

Considérons maintenant (x, y) une autre solution. On a alors $19x + 23y = 36 = -19.216 + 23.180$ et donc $19(x + 216) = 23(180 - y)$. Puisque 19 et 23 sont premiers entre eux, on en déduit que 23 divise $x + 216$ et qu'il existe donc $k \in \mathbb{Z}$ tel que $x + 216 = 23k$. On a alors $23(180 - y) = 19.23k$ et donc $y = 180 - 19k$. Au final, $(x, y) = (23k - 216, 180 - 19k)$.

Réciproquement, on vérifie par un calcul direct que pour tout $k \in \mathbb{Z}$, $(23k - 216, 180 - 19k)$ est bien solution de l'équation. On en déduit que l'ensemble des solutions est $\Big\{(23k-216, 180-19k) \;\Big|\; k \in \mathbb{Z}\Big\}$.

Exercice 21.
L'idée de cette exercice est d'utiliser le fait que a est divisible par n ssi $\overline{a} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ (ou, de manière équivalente $a \equiv 0\ [n]$, nous rédigerons d'ailleurs les solutions alternativement dans les deux modes) pour tout simplifier en faisant les calculs modulo n.

1. Dans $\mathbb{Z}/3\mathbb{Z}$, on a

$$\overline{2^{2n+1} + 1} = \overline{2.4^n + 1} = \overline{2}.\overline{4}^n + \overline{1} = \overline{-1}.\overline{1}^n + 1 = -\overline{1} + \overline{1} = \overline{0}.$$

On en déduit donc que $2^{2n+1} + 1$ est divisible par 3.

2. On a

$$5n^3 + n \equiv -n^3 + n \equiv n(1 - n^2) \equiv n(1 - n)(1 + n) \equiv -(n - 1)n(1 + n)\ [6].$$

Or nous avons vu qu'un produit de trois entiers consécutifs est toujours divisible par 6 (pour mémoire, l'un au moins est divisible par 2, pareil par 3 ; or 2 et 3 sont premiers entre eux, donc le produit est divisible par $2.3 = 6$). On en déduit que $5n^3 + n \equiv 0\ [6]$ et donc $5n^3 + n$ est divisible par 6.

3. Dans $\mathbb{Z}/7\mathbb{Z}$, on a

$$\overline{3^{2n+1} + 2^{n+2}} = \overline{3.9^n + 4.2^n} = \overline{3}.\overline{9}^n + \overline{4}.\overline{2}^n = \overline{3}.\overline{2}^n + \overline{4}.\overline{2}^n = (\overline{3} + \overline{4}).\overline{2}^n = \overline{7}.\overline{2}^n = \overline{0}.$$

On en déduit donc que $3^{2n+1} + 2^{n+2}$ est divisible par 7.

4. Nous allons donner deux preuves de ce résultat.

Solution 1 : Par calcul direct, on a

$$4^0 \equiv 1\ [9] \qquad 4^1 \equiv 4\ [9] \qquad 4^2 \equiv 16 \equiv -2\ [9] \qquad 4^3 \equiv -8 \equiv 1\ [9].$$

La suite des puissances de 4 devient donc cyclique, et on montre par une récurrence immédiate que

$$\begin{cases} 1 \text{ si } n \equiv 0\ [3] \\ 4 \text{ si } n \equiv 1\ [3] \\ -2 \text{ si } n \equiv 2\ [3] \end{cases}$$

Dès lors, on notant $n = 3k + r$ la division euclidienne de n par 3, on obtient que

si $r=0$ **:** alors $4^n+15n-1\equiv 1+15.3k-1\equiv 45k\equiv 0$ [9] ;
si $r=1$ **:** alors $4^n+15n-1\equiv 4+15.3k+15-1\equiv 45k+18\equiv 0$ [9] ;
si $r=2$ **:** alors $4^n+15n-1\equiv -2+15.3k+30-1\equiv 45k+27\equiv 0$ [9].
Dans tous les cas, $4^n+15n-1\equiv 0$ [9] et donc $4^n+15n-1$ est divisible par 9.

Solution 2 : Par identité remarquable, on a

$$4^n+15n-1=4^n-1^n+15n=(4-1).\sum_{k=0}^{n-1}4^k+3.5n=3\left(5n+\sum_{k=0}^{n-1}4^k\right)$$

qui est déjà divisible par 3. Il suffit donc de montrer que $5n+\sum_{k=0}^{n-1}4^k$ est encore divisible par 3. Or

$$5n+\sum_{k=0}^{n-1}4^k\equiv -n+\sum_{k=0}^{n-1}1^k\equiv -n+n\equiv 0\ [3].$$

On en déduit donc que $4^n+15n-1$ est deux fois divisible par 3, donc divisible par 9.

5. Pour cette question, il faut faire attention à ne pas factoriser 2^{-7} et 3^{-2} qui ne sont pas des entiers. De fait, le résultat de divisibilité n'a de sens que pour $n\geq 1$. Mais dans ce cas, on a dans $\mathbb{Z}/11\mathbb{Z}$

$$\overline{2^{10n-7}+3^{5n-2}-2}=\overline{2^{10(n-1)+3}+3^{5(n-1)+3}-2}=\overline{2^{10(n-1)+3}+3^{5(n-1)+3}-2}=\overline{8}.\left(\overline{2}^{10}\right)^{n-1}+\overline{27}.\left(\overline{3}^5\right)^{n-1}-\overline{2}.$$

Or d'après le petit théorème de Fermat, 11 étant premier et 2 non divisible par 11, $2^{10}-1$ est divisible par 11, donc $\overline{2^{10}}=\overline{1}$, et $\overline{3}^5=\overline{3}\left(\overline{3}^2\right)^2=\overline{3}.\overline{-2}^2=\overline{12}=\overline{1}$. Au final, on a donc

$$\overline{2^{10n-7}+3^{5n-2}-2}=\overline{8}.\overline{1}^{n-1}+\overline{27}.\overline{1}^{n-1}-\overline{2}=\overline{8}+\overline{5}-\overline{2}=\overline{11}=\overline{0}.$$

On en déduit donc que $2^{10n-7}+3^{5n-2}-2$ est divisible par 11.

6. On a

$$3.5^{2n+1}+2^{3n+1}\equiv 3.5.(25)^n+2.8^n\equiv 15.8^n+2.8^n\equiv 17.8^n\equiv 0\ [17].$$

On en déduit que $3.5^{2n+1}+2^{3n+1}$ est divisible par 17.

Exercice 22.
On a $n^2-3n+6\equiv n^2+2n+1\equiv (n+1)^2$ [5]. Donc n^2-3n+6 est divisible par 5 ssi $(n+1)^2$ l'est. Or 5 étant premier, d'après le lemme d'Euclide, $(n+1)^2$ est divisible par 5 ssi $n+1$ l'est. On en déduit n^2-3n+6 est divisible par 5 ssi n est de la forme $5k-1\big(=5(k-1)+4\big)$ avec $k\in\mathbb{Z}$, c'est-à-dire ssi le reste de la division euclidienne de n par 5 vaut 4.

Exercice 23.
D'après le petit théorème de Fermat, 7 étant premier et 10 premier avec 7, on a $10^6\equiv 1$ [7]. On en déduit que, modulo 7, la classe de 10^N ne dépend que du reste de la division euclidienne de N par 6. Or, pour tout $k\in\mathbb{N}^*$, 10^k-4 est clairement pair donc divisible par 2, et on a $10^k-4\equiv 1^k-1\equiv 0$ [3], montrant qu'il est egalement divisible par 3. Mais 2 et 3 étant premiers entre eux, 10^k-4 est donc divisible par 6 ; le reste de la division euclidienne de 10^k par 6 vaut donc 4. On en déduit que

$$10^{10^k}\equiv 10^4\equiv 3^4\equiv\left(3^2\right)^2\equiv 9^2\equiv 2^2\equiv 4\ [7]$$

et, de fait,

$$\sum_{k=1}^{2n}10^{10^k}\equiv\sum_{k=1}^{2n}4\equiv 8n\equiv n\ [7].$$

Exercice 31.

1. En terme de congruence, le petit théorème de Fermat dit que, pour tout nombre premier p et tout $n\in\mathbb{Z}$ non multiple de p, on a $p^{n-1}\equiv 1\ [p]$.
2. (a) Puisque 31 est premier et que 239 n'est pas un multiple de 31, on a, d'après le petit théorème de Fermat, $239^{30}\equiv 1$ [31]. On en conclut que $30^{239}+239^{30}\equiv(-1)^{239}+1\equiv -1+1\equiv 0$ [31]. L'entier $30^{239}+239^{30}$ est donc divisible par 31 et n'est donc pas premier.

(b) Puisque 2, 3 et p sont des nombres premiers distincts, ils sont deux à deux premiers entre eux, et il suffit donc de montrer séparemment que chacun divise $ab^p - ba^p$, c'est-à-dire que $ab^p - ba^p$ est congru à 0 modulo 2, 3 et p.

Pour 2, il suffit de remarquer que, pour tout $n \in \mathbb{Z}$, $n^p \equiv n$ [2]. En effet, $0^p \equiv 0$ [2] et $1^p \equiv 1$ [2]. Dès lors, on a $ab^p - ab^p \equiv ab - ab \equiv 0$ [2].

De même, puisque p est impair (car premier distinct de 2), on a aussi, pour tout $n \in \mathbb{Z}$, $n^p \equiv n$ [3]. En effet, $(-1)^p \equiv -1$ [3], $0^p \equiv 0$ [3] et $1^p \equiv 1$ [3]. Dès lors, on a $ab^p - ab^p \equiv ab - ab \equiv 0$ [3].

Enfin, pour p, si a ou b est un multiple de p, alors $ab^p - ba^p = ab(b^{p-1} - a^{p-1})$ est divisible par p et on a $ab^p - ba^p \equiv 0$ [p]. Sinon, d'après le petit théorème de Fermat, on $ab(b^{p-1} - a^{p-1}) \equiv ab(1-1) \equiv 0$ [p].

(c) On a $56786730 = 2.3.5.7.11.13.31.61$ avec 2, 3, 5, 7, 11, 13, 31 et 61 premiers, donc deux à deux premiers entre eux. Il suffit donc de montrer que $ab(a^{60} - b^{60})$ est divisible par chacune de ces valeurs. Fixons-en une et notons-là p. On a donc p premier, et on peut remarquer que 60 est un multiple de $p-1$. On a donc, ou bien a ou b multiple de p et dans ce cas p divise $ab(a^{60} - b^{60})$, ou bien a et b premiers avec p, et alors d'après le petit théorème de Fermat, on a

$$ab(a^{60} - b^{60}) \equiv ab\big((a^{p-1})^{\frac{60}{p-1}} - (b^{p-1})^{\frac{60}{p-1}}\big) \equiv ab\big(1^{\frac{60}{p-1}} - 1^{\frac{60}{p-1}}\big) \equiv ab(1-1) \equiv 0 \ [p].$$

Dans tous les cas, p divise bien $ab(a^{60} - b^{60})$.