Exercices – Arithmétique

0.1 pgcd

Exercice 1.

1. Chercher le plus petit entier positif divisible par 11 et dont le reste de la division par 13 est 1.
2. Chercher le plus petit entier positif dont le reste de la division par 8 est 5 et le reste de la division par 9 est 6.

Indications 1.

Commencer par écrire tous les multiples de 11 et effectuer ensuite la division euclidienne par 13.

Correction 1.

1. Les entiers divisibles par 11 sont les multiples de 11 : 0, 11, 22, ... Ils sont de la forme $11k$ pour un certain entier k.

k	$11k$	reste par 13
1	11	11
2	22	9
3	33	7
4	44	5
5	55	3
6	66	1

   On note sur la dernière colonne que le reste de $11k$ divisé par 13 diminue ici de deux en deux et pour $k = 6$ on obtiendra le reste 1. Ainsi le nombre cherché est $n = 66$: c'est un multiple de 11 et le reste de la division par 13 est bien 1 car $66 = 13 \times 5 + 1$.

2. Les entiers dont le reste de la division par 8 est 5 sont de la forme $8k + 5$ pour un certain entier k. Reprenons la même méthode, on calcule tous les entiers de la forme $8k+5$ et le reste de division par 9 :

k	$8k+5$	reste par 9
0	5	5
1	13	4
2	21	3
3	29	2
4	37	1
5	45	0
6	53	8
7	61	7
8	69	6

   On note sur la dernière colonne que le reste "diminue de 1" à chaque ligne et pour $k = 8$ on obtiendra le reste 6. Ainsi le nombre cherché est $n = 8 \times 8 + 5 = 69$ qui s'écrit aussi $69 = 6 \times 9 + 6$.

Exercice 2.

1. Soit $n = p^2$ le carré d'un entier. Quel peut être le reste de la division de n par 4 selon que p est pair ou impair ?
2. Montrer que si n est un entier naturel somme de deux carrés d'entiers alors le reste de la division de n par 4 n'est jamais égal à 3.

Indications 2.

Si p est pair, alors $p = 2k$ donc $p^2 = \dots$ Si p est impair, alors $p = 2k+1\dots$

Correction 2.

1. Soit $n = p^2$.
   — Si p est pair, alors $p = 2k$ (pour un certain entier k) donc $n = p^2 = (2k)^2 = 4k^2$ est un multiple de 4. Dans ce cas le reste de la division de n par 4 est 0.
   — Si p est impair, alors $p = 2k+1$ donc $n = p^2 = (2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1$, c'est l'écriture de la division euclidienne de n par 4. Donc le reste de la division de n par 4 est 1.
   — Conclusion : pour $n = p^2$ alors le reste de la division de n par 4 est soit 0, soit 1 (mais ne peut pas être 2, ni 3).
2. Soit $n = p^2+q^2$. On discute selon que p et q sont pairs ou impairs. Il y a donc 4 cas possibles.
   — Si p est pair et q est pair. Alors par la question précédente le reste de la division de p^2 par 4 est 0, de même que celui de la division de q^2 par 4. Ainsi le reste de la division de $n = p^2+q^2$ est $0+0$, il vaut donc 0.
   — Si p est pair et q est impair, alors le reste de la division de $n = p^2+q^2$ est $0+1$, il vaut donc 1.
   — Si p est impair et q est pair, alors le reste de la division de $n = p^2+q^2$ est $1+0$, il vaut donc 1.
   — Si p est impair et q est impair, alors le reste de la division de $n = p^2+q^2$ est $1+1$, il vaut donc 2.

   Dans tous les cas le reste de n divisé par 4 ne peut pas être 3.

Exercice 3.

Déterminer $\operatorname{pgcd}(254, 26)$, $\operatorname{pgcd}(654, 115)$ à l'aide de l'algorithme d'Euclide.

Indications 3.

Calculer une succession de divisions euclidiennes.

Correction 3.

1. Calculons $\operatorname{pgcd}(254, 26)$.
$$\begin{array}{rcccccc} 254 & = & 26 & \times & 9 & + & 20 \\ 26 & = & 20 & \times & 1 & + & 6 \\ 20 & = & 6 & \times & 3 & + & \boxed{2} \\ 6 & = & 2 & \times & 3 & + & 0 \end{array}$$
   Ainsi $\operatorname{pgcd}(254, 26) = 2$.
2. Calculons $\operatorname{pgcd}(654, 115)$.
$$\begin{array}{rcccccc} 654 & = & 115 & \times & 5 & + & 79 \\ 115 & = & 79 & \times & 1 & + & 36 \\ 79 & = & 36 & \times & 2 & + & 7 \\ 36 & = & 7 & \times & 5 & + & \boxed{1} \\ 7 & = & 1 & \times & 7 & + & 0 \end{array}$$

Ainsi $\text{pgcd}(654, 115) = 1$.

Exercice 4.

Déterminer $\text{ppcm}(255, 204)$.

Indications 4.

Utiliser le lien entre pgcd et ppcm...

Correction 4.

On va utiliser la relation $\quad 255 \times 204 = \text{pgcd}(255, 204) \times \text{ppcm}(255, 204)$

Calculons donc $\text{pgcd}(255, 204)$.

$$\begin{array}{rcrcrcl} 255 & = & 204 & \times & 1 & + & \boxed{51} \\ 204 & = & 51 & \times & 4 & + & 0 \end{array}$$

Ainsi $\text{pgcd}(255, 204) = 51$. On en déduit donc :

$$\text{ppcm}(255, 204) = \frac{255 \times 204}{\text{pgcd}(255, 204)} = \frac{255 \times 204}{51} = \boxed{1020}$$

0.2 Théorème de Bézout

Exercice 5.

Soit $a = 84$ et $b = 75$. Calculer $d = \text{pgcd}(a, b)$ à l'aide de l'algorithme d'Euclide, puis déterminer des coefficients de Bézout $u, v \in \mathbb{Z}$ tels que $au + bv = d$.
Même exercice avec $a = 624$ et $b = 108$.

Indications 5.

Les coefficients de Bézout s'obtiennent par remontée de l'algorithme d'Euclide.

Correction 5.

1. Calculons $\text{pgcd}(84, 75)$ par l'algorithme d'Euclide :

$$\begin{array}{rcrcrcl} 84 & = & 75 & \times & 1 & + & 9 \\ 75 & = & 9 & \times & 8 & + & \boxed{3} \\ 9 & = & 3 & \times & 3 & + & 0 \end{array}$$

Ainsi $\text{pgcd}(84, 75) = 3$.
Maintenant nous reprenons ces égalités en partant de la fin (avant-dernière ligne) :

$$\boxed{3} = 75 - 9 \times 8$$

On va remplacer le 9 de cette égalité.
La première ligne fournit l'égalité :

$$9 = 84 - 75 \times 1$$

Donc

$$\boxed{3} = 75 - \big(84 - 75 \times 1\big) \times 8$$

On garde précieusement les entiers 84 et 75 et on ne cherche pas à simplifier, on factorise juste :

$$\boxed{3} = 84 \times (-8) + 75 \times 9$$

Ainsi $u = -8$ et $v = 9$ conviennent. C'est une bonne idée de faire une vérification rapide.

2. Calculons $\mathrm{pgcd}(624, 108)$.

$$\begin{array}{rclcccc} 624 & = & 108 & \times & 5 & + & 84 \\ 108 & = & 84 & \times & 1 & + & 24 \\ 84 & = & 24 & \times & 3 & + & \boxed{12} \\ 24 & = & 12 & \times & 2 & + & 0 \end{array}$$

Ainsi $\mathrm{pgcd}(624, 108) = 12$.
Remontons ces égalités, tout d'abord l'avant-dernière ligne donne le pgcd :

$$\boxed{12} = 84 - 24 \times 3$$

Mais par la ligne au-dessus on a

$$24 = 108 - 84 \times 1$$

On remplace 24 dans l'égalité ci-dessus :

$$\boxed{12} = 84 - \big(108 - 84 \times 1\big) \times 3$$

On factorise (sans trop simplifier) :

$$\boxed{12} = 108 \times (-3) + 84 \times 4$$

La première ligne donne :

$$84 = 624 - 108 \times 5$$

ce qui nous donne

$$\boxed{12} = 108 \times (-3) + \big(624 - 108 \times 5\big) \times 4$$

On factorise pour obtenir :

$$\boxed{12} = 624 \times 4 + 108 \times (-23)$$

Ainsi les coefficients de Bézout sont $u = 4$ et $v - 23$.

Exercice 6.

Nous allons montrer que « Deux entiers consécutifs sont toujours premiers entre eux. »

1. *Première méthode.* On considère deux entiers consécutifs notés n et $n+1$. Montrer que si d divise n et $n+1$ alors nécessairement $d = 1$.
2. *Seconde méthode.* Soit $a = n$ et $b = n+1$. Trouver $u, v \in \mathbb{Z}$ (très simples) tels que $au + bv = 1$. Conclure.

Indications 6.

Pour la première méthode considérer une différence. Pour la seconde méthode, utiliser la variante du théorème de Bézout.

Correction 6.

1. Si d divise n et $n+1$ alors d divise aussi la différence $(n+1)-n$ (qui vaut 1), donc d divise 1. Ainsi $d=1$ (ou $d=-1$) et $\mathrm{pgcd}(n,n+1)=1$.
2. Avec $u=-1$ et $v=+1$ on a $nu+(n+1)v=1$. Par la variante du théorème de Bézout « a et b sont premiers entre eux $\iff$ il existe $(u,v)\in\mathbb{Z}^2$ tels que $au+bv=1$ », cela implique que n et $n+1$ sont premiers entre eux.

Exercice 7.

Soit $\alpha\in\mathbb{Z}$ un entier fixé que l'on cherchera à déterminer par la suite. Pour $k\in\mathbb{Z}$, on pose : $N_1(k)=7k+11$ et $N_2(k)=2k+\alpha$.

1. Déterminer deux entiers u,v tels que le nombre $uN_1(k)+vN_2(k)$ ne dépende pas de l'entier k.
2. En déduire une valeur de α pour obtenir $\mathrm{pgcd}(N_1(k),N_2(k))=1$ pour tout entier k.
3. Application : en déduire $\mathrm{pgcd}(95,27)$ d'une part, et $\mathrm{ppcm}(361,103)$ d'autre part.

Indications 7.

On cherche "des bons coefficients" pour obtenir une relation de Bézout traduisant le fait que $N_1(k)$ et $N_2(k)$ sont premiers entre eux ! Ensuite, on peut utiliser le lien entre pgcd et ppcm...

Correction 7.

1. En prenant $u=2$ et $v=-7$, on obtient l'égalité :

$$uN_1(k)+vN_2(k)=2(7k+11)+(-7)(2k+\alpha)=22-7\alpha$$

   Cette quantité ne dépend donc plus de l'entier k. (On aurait aussi pu prendre $u=-2$ et $v=7$).
2. Si l'on fixe α tel que $uN_1(k)+vN_2(k)=1$, le théorème de Bézout nous garantira l'obtention de $\mathrm{pgcd}(N_1(k),N_2(k))=1$ pour tout entier k. On va donc fixer :

$$22-7\alpha=1 \iff \alpha=3$$

3. On remarque que pour $k=12$, on obtient :

$$N_1(12)=7\times 12+11=95 \qquad ; \qquad N_2(12)=2\times 12+3=27$$

   D'après ce qui précède, on sait donc que $\mathrm{pgcd}(N_1(12),N_2(12))=\mathrm{pgcd}(95,27)=1$.
   On a ensuite pour $k=50$:

$$N_1(50)=7\times 50+11=361 \qquad ; \qquad N_2(50)=2\times 50+3=103$$

   D'après nos résultats précédents, on sait que $\mathrm{pgcd}(N_1(50),N_2(50))=\mathrm{pgcd}(361,103)=1$. Par conséquent, on a :

$$\mathrm{ppcm}(361,103)=\frac{361\times 103}{1}=37\,183$$

0.3 Nombres premiers

Exercice 8.

Trouver tous les nombres premiers plus petits que 100.

Indications 8.

Il s'agit d'écarter les entiers qui ne sont pas des nombres premiers car divisibles par 2 ou par 3...

Correction 8.

Les nombres premiers jusqu'à 100 sont :

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97$$

On les obtient simplement par une méthode appelée le *crible d'Ératosthène* :

— en excluant d'abord tous les entiers pairs (sauf 2 bien sûr),

— puis tous les entiers divisibles par 3 (sauf 3),

— on n'a pas besoin d'exclure les multiples de 4 car ils sont déjà exclus en tant que multiples de 2,

— ensuite on exclut les multiples de 5 (sauf 5),

— les multiples de 6 sont déjà exclus (ce sont des multiples de 2 et de 3),

— il reste à exclure les multiples de 7,

— les multiples de 8, 9, 10 sont déjà exclus,

— et c'est terminé car un entier non premier plus petit que 100 doit avoir un facteur inférieur à $\sqrt{100} = 10$.

Exercice 9.

Calculer la décomposition en facteurs premiers de a puis de b, en déduire $\mathrm{pgcd}(a,b)$ et $\mathrm{ppcm}(a,b)$.

1. $a = 1500$, $b = 1470$.
2. $a = 18\,135$, $b = 92\,950$.

Indications 9.

Le pgcd et les ppcm s'obtiennent facilement une fois les entiers décomposés en facteurs premiers. Pour le pgcd prendre, pour chaque facteur premier, l'exposant minimum entre celui de a et celui de b, pour le ppcm prendre le maximum.

Correction 9.

1. $a = 1500 = 2^2 \times 3 \times 5^3$.
   Pour obtenir cette décomposition, on remarque que 1500 est divisible par 2 donc $1500 = 2 \times 750$, puis 750 est encore divisible par 2, donc $1500 = 2^2 \times 375$, cette fois 375 n'est pas divisible par 2 mais par contre il est divisible par 3, ainsi $1500 = 2^2 \times 3 \times 125$ et enfin $125 = 5^3$.
   On obtient de même : $b = 2 \times 3 \times 5 \times 7^2$.
   Pour le pgcd et le ppcm on écrit les entiers avec tous les facteurs présents dans a ou b, quitte à mettre des exposants qui valent 0 :
   $$a = 1500 = 2^2 \times 3^1 \times 5^3 \times 7^0$$
   $$b = 1470 = 2^1 \times 3^1 \times 5^1 \times 7^2$$
   Pour le pgcd on prend, pour chaque facteur premier, l'exposant *minimum* entre celui de a et celui de b :
   $$\mathrm{pgcd}(a,b) = 2^1 \times 3^1 \times 5^1 \times 7^0 = 30$$
   Pour le ppcm on prend, pour chaque facteur premier, l'exposant *maximum* entre celui de a et celui de b :
   $$\mathrm{ppcm}(a,b) = 2^2 \times 3^1 \times 5^3 \times 7^2 = 73\,500$$

2.
$$a = 18\,135 = 3^2 \times 5 \times 13 \times 31 \qquad b = 92\,950 = 2 \times 5^2 \times 11 \times 13^2$$

$$\text{pgcd}(a, b) = 2^0 \times 3^0 \times 5^1 \times 11^0 \times 13^1 \times 31^0 = 5 \times 13 = 65$$

$$\text{ppcm}(a, b) = 2^1 \times 3^2 \times 5^2 \times 11^1 \times 13^2 \times 31^1 = 25\,933\,050$$

Exercice 10.

Soit p un nombre premier. Montrer que pour tout entier k tel que $1 \leqslant k \leqslant p-1$, alors p divise $\binom{p}{k}$.
On rappelle l'expression du coefficient binomial :

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Indications 10.

Trouver un entier A tel que $\binom{p}{k} = p! \times A$ et utiliser le lemme de Gauss.

Correction 10.

Faisons d'abord la remarque suivante : si a et b sont deux entiers, si p est un nombre premier avec $p > a$ et $p > b$ alors bien sûr p ne peut pas diviser a, ni b (car p est plus grand que a et b) mais en plus p ne peut pas diviser $a \times b$. En effet par le lemme d'Euclide, si p divisait ab alors p diviserait a ou p diviserait b.

On sait que $\binom{p}{k} = \frac{p!}{k!(p-k)!} \iff p! = \binom{p}{k} \times k!(p-k)!$. Puisque p divise $p!$, p divise donc $\binom{p}{k} \times k!(p-k)!$.
Mais pour $1 \leqslant k \leqslant p-1$, tous les facteurs de $k!$ sont strictement inférieurs à p : cela signifie que p ne divise pas $k!$, et donc que $\text{pgcd}(p, k!) = 1$. D'après le lemme de Gauss, on a donc : p divise $\binom{p}{k} \times (p-k)!$.
Mais il en va de même avec $(p-k)!$: pour $1 \leqslant k \leqslant p-1$, les facteurs de $(p-k)!$ sont tous strictement inférieurs à p. Donc p ne divise pas $(p-k)!$, et $\text{pgcd}(p, (p-k)!) = 1$. Une nouvelle application du lemme de Gauss offre donc :

$$\boxed{\text{Pour } 1 \leqslant k \leqslant p-1, \qquad p \text{ divise } \binom{p}{k}.}$$

0.4 Congruences

Exercice 11.

Simplifier les expressions suivantes (sans calculatrice). Par exemple "simplifier 72 [7]" signifie "trouver n entre 0 et 6 tel que $72 \equiv n\ [7]$" ; la réponse est $n = 2$.

— $45\ [7]$, $39\ [7]$, $45 + 39\ [7]$, $45 \times 39\ [7]$, $45^2\ [7]$, $39^3\ [7]$.

— $1052\ [22]$, $2384\ [22]$, $2384 - 1052\ [22]$, $1052^2 \times 2384\ [22]$.

Indications 11.

Pour les calculs modulo 7 on se ramène à un entier compris entre 0 et 6. Modulo 22 on se ramène à un entier compris entre 0 et 21.

Correction 11.

1. — $45 = 42 + 3 = 7 \times 6 + 3$, ainsi $45 \equiv 3\,[7]$.
   — $39 = 35 + 4 = 7 \times 5 + 4$, ainsi $39 \equiv 4\,[7]$.
   — Pour réduire $45 + 39$, on ne fait pas d'abord la somme, on utilise en premier nos réductions précédentes :
   $$45 + 39 \equiv 3 + 4 \equiv 7 \equiv 0\,[7].$$
   Ainsi, sans effort, on sait que $45 + 39$ est divisible par 7.
   — $45 \times 39 \equiv 3 \times 4 \equiv 12 \equiv 5\,[7]$.
   — $45^2 \equiv 3^2 \equiv 9 \equiv 2\,[7]$.
   — $39^3 \equiv 4^3 \equiv 64 \equiv 1\,[7]$.
2. — $1052 = 22 \times 47 + 18$ donc $1052 \equiv 18\,[22]$.
   — $2384 = 22 \times 108 + 8$ donc $2384 \equiv 8\,[22]$.
   — $2384 - 1052 \equiv 8 - 18 \equiv -10 \equiv 12\,[22]$.
   — $1052^2 \times 2384 \equiv 18^2 \times 8\,[22]$. Or $18^2 = 324 \equiv 16\,[22]$ donc $1052^2 \times 2384 \equiv 16 \times 8 \equiv 128 \equiv 18\,[22]$.

Exercice 12.

1. Calculer 2^{500} modulo 13 (utiliser le petit théorème de Fermat).
2. Calculer 1000^{123} modulo 17.
3. Calculer 3^{1234} modulo 15 (attention on ne peut pas appliquer le petit théorème de Fermat, étudier d'abord 3^k modulo 15 pour les petites valeurs de k).

Indications 12.

1. Le petit théorème de Fermat nous dit que $2^{12} \equiv 1\,[13]$, il faut ensuite écrire $500 = 12\times ? + ?$.
2. Commencer par simplifier le calcul en réduisant $1000\,[17]$.

Correction 12.

1. — 13 est un nombre premier (et ne divise pas 2), alors le petit théorème de Fermat nous dit que $2^{12} \equiv 1\,[13]$. Ainsi les puissances sont périodiques de période 12 : $2^0 \equiv 1\,[13]$, $2^{12} \equiv 1\,[13]$, $2^{24} \equiv 1\,[13]$, $2^{36} \equiv 1\,[13]$,...
   — Il s'agit maintenant d'approcher 500 au plus près par un multiple de 12, on effectue donc la division euclidienne de 500 par 12 :
   $$500 = 12 \times 41 + 8$$
   Ainsi $500 = 492 + 8$ où 492 est un multiple de 12.
   — On peut maintenant réduire 2^{500} modulo 13 :
   $$2^{500} = 2^{492+8} = 2^{492} \times 2^8 \equiv 1 \times 2^8\,[13]$$
   — Il reste à calculer 2^8 modulo 13. $2^8 = 256 \equiv 9\,[13]$. Ainsi
   $$2^{500} \equiv 1 \times 9 \equiv 9\,[13].$$
2. — On commence par réduire 1000 modulo 17, comme $1000 = 17 \times 58 + 14$ alors $1000 \equiv 14\,[17]$. On sait que si $a \equiv b\,[n]$ alors $a^k \equiv b^k\,[n]$ donc $1000^k \equiv 14^k\,[17]$. On va donc calculer $14^{123}\,[17]$.

— Le petit théorème de Fermat nous dit que $14^{16} \equiv 1\ [17]$ car 17 est un nombre premier. On obtient donc aussi $14^{32} \equiv 1\,[17]$, $14^{48} \equiv 1\,[17]$,...

— On cherche le multiple de 16 le plus proche en dessous de 123, comme $123 = 16 \times 7 + 11$ alors $123 = 112 + 11$ où 112 est un multiple de 16. Ainsi :

$$14^{123} = 14^{112+11} = 14^{112} \times 14^{11} \equiv 1 \times 14^{11}\ [17].$$

— Il reste à calculer 14^{11} modulo 17. Pour éviter de faire des calculs avec des entiers trop gros, on calcule les puissances successives de 14 et on réduit modulo 17 à chaque étape :

$$\begin{gathered}
14^1 \equiv 14\,[17] \\
14^2 = 196 \equiv 9\,[17] \\
14^3 = 14 \times 14^2 \equiv 14 \times 9 \equiv 126 \equiv 7\,[17] \\
14^4 = 14 \times 14^3 \equiv 14 \times 7 \equiv 98 \equiv 13\,[17] \\
14^5 = 14 \times 14^4 \equiv 14 \times 13 \equiv 182 \equiv 12\,[17] \\
\cdots \\
14^{11} = 14 \times 14^{10} \equiv 10\,[17]
\end{gathered}$$

— Conclusion : $1000^{123} \equiv 14^{123} \equiv 14^{11} \equiv 10\,[17]$.

3. On ne peut pas appliquer le petit théorème de Fermat car 15 n'est pas pas un nombre premier. On commence donc par étudier $3^k \equiv 1\ [15]$ pour les petites valeurs de k :

k	3^k	$3^k\,[15]$
1	3	3
2	9	9
3	27	12
4	81	6
5	243	3
6	729	9
7	2187	12
8	6561	6
9	19683	3

On voit apparaître une période de longueur 4 (même si on n'obtient pas 1 comme résultat) : par exemple si l'exposant est congru à 1 modulo 4 (i.e. $k = 1, 5, 9, \ldots$) :

$$3^1 \equiv 3\,[15] \qquad 3^5 \equiv 3\,[15] \qquad 3^9 \equiv 3\,[15] \qquad \ldots$$

Si l'exposant est congru à 2 modulo 4 (i.e. $k = 2, 6, 10, \ldots$) :

$$3^2 \equiv 9\,[15] \qquad 3^6 \equiv 9\,[15] \qquad 3^{10} \equiv 9\,[15] \qquad \ldots$$

Dans notre cas l'exposant est $k = 1234$. On écrit alors $1234 = 4 \times 308 + 2$. Ainsi $k \equiv 2\,[4]$, donc

$$3^{1234} \equiv 9\,[15].$$

Exercice 13.

Les deux premières questions reprennent un exercice précédent et montrent l'efficacité des congruences pour les calculs.

1. Soit $n = p^2$ le carré d'un entier. Déterminer les valeurs possibles de n modulo 4.
2. Montrer que si n est un entier naturel somme de deux carrés d'entiers alors n modulo 4 n'est jamais égal à 3.
3. Soit $n = p^2$ le carré d'un entier. Déterminer les valeurs possibles de n modulo 8.

4. Montrer que si n est un entier naturel somme de trois carrés d'entiers alors n modulo 8 n'est jamais égal à 7.

Indications 13.

Modulo 4, p est congru à 0, 1, 2 ou 3, donc p^2...

Correction 13.

1. Soit $n = p^2$. Modulo 4, p est congru à 0, 1, 2 ou 3. Calculons alors la valeur de p^2 modulo 4 dans chacun de ces cas.

$p\,[4]$	$p^2\,[4]$
0	0
1	1
2	$2^2 \equiv 4 \equiv 0$
3	$3^2 \equiv 9 \equiv 1$

   Conclusion : pour $n = p^2$ alors $n\,[4]$ est congru soit à 0, soit à 1 (mais ne peut pas être 2, ni 3).
2. Soit $n = p^2 + q^2$. D'après la question précédente p^2 et q^2 sont congrus à 0 ou 1 modulo 4. Il y a donc 4 cas possibles, mais dans tous les cas la somme ne peut pas faire 3 ($0+0=0$, $0+1=1$, $1+0=1$, $1+1=2$).
3. Soit $n = p^2$. Modulo 8, p est congru à l'un des entiers $0, 1, \ldots, 7$. Calculons la valeur de p^2 modulo 8 dans chacun de ces cas.

$p\,[8]$	$p^2\,[8]$
0	0
1	1
2	4
3	$3^2 \equiv 9 \equiv 1$
4	$4^2 \equiv 16 \equiv 0$
5	$5^2 \equiv 25 \equiv 1$
6	$6^2 \equiv 36 \equiv 0$
7	$7^2 \equiv 49 \equiv 1$

   Conclusion : pour $n = p^2$ alors $n\,[8]$ est congru soit à 0, soit à 1, soit à 4 (mais ne peut pas être 2, 3, 5, 6, ni 7).
4. Soit $n = p^2 + q^2 + r^2$. Chaque carré vaut 0 ou 1 ou 4 modulo 8. La somme de trois tels termes ne peut pas faire 7 (toutes les autres valeurs de 0 à 6 sont possibles). Donc n n'est pas congru à 7 modulo 8.

Exercice 14.

1. Montrer que $p = 101$ est un nombre premier.
2. Soit a un entier avec $1 \leqslant a < p$. Montrer que $\text{pgcd}(a, p) = 1$.
3. Écrire le théorème de Bézout pour le pgcd précédent ; en déduire qu'il existe $u \in \mathbb{Z}$ tel que $au \equiv 1\,[p]$. *Un tel u s'appelle un* ***inverse*** *de a modulo p.*
4. Trouver un inverse de $a = 15$ modulo $p = 101$.
5. Trouver une solution de l'équation d'inconnue x (un entier) : $15x \equiv 7\,[101]$.
6. Reprendre tout l'exercice avec $p = 103$.

Indications 14.

Ici le théorème de Bézout s'écrit $au + pv = 1$. Le u est l'inverse cherché.

Correction 14.

1. $p = 101$ n'est pas divisible par $k = 2, 3, 5, 7$ qui sont les diviseurs premiers possibles $\leqslant \sqrt{101}$, donc c'est un nombre premier.
2. Si d est un diviseur commun à a et à p alors $d = 1$ ou $d = p$ car p est un nombre premier. Mais comme d doit être plus petit que a (et $a < p$) alors $d < p$. Conclusion : $d = 1$, ce qui prouve que a et p sont premiers entre eux.
3. Le théorème de Bézout avec a, $b = p$ et $d = \mathrm{pgcd}(a, p) = 1$ donne l'existence de deux entiers u, v tels que :
$$au + pv = 1.$$
Autrement dit $au - 1 = -pv$. Ce qui implique que $au \equiv 1\,[p]$.
4. Pour $a = 15$ et $p = 101$ les coefficients de Bézout u, v sont obtenus par remontée de l'algorithme d'Euclide. Après calculs on trouve :
$$a \times 27 + 101 \times (-4) = 1.$$
Donc avec $u = 27$ on a $au \equiv 1\,[101]$ c'est-à-dire $15 \times 27 \equiv 1\,[101]$. 27 est donc un inverse de 15 modulo 101.
5. Toujours avec $a = 15$, l'équation à résoudre est $ax \equiv 7\,[101]$. On a envie de diviser par a pour trouver x. Pour l'écrire de façon correcte, on va plutôt multiplier à gauche et droite par l'inverse de a (c'est-à-dire par $u = 27$), pour obtenir une équation équivalente :
$$(au)x \equiv 7u\,[101]$$
Mais $au \equiv 1\,[101]$ (par construction de u), donc on obtient
$$x \equiv 7u\,[101]$$
Ici $u = 27$ donc $x = 7 \times 27 = 189 \equiv 88\,[101]$. On vérifie facilement qu'avec $x = 88$ on a bien $15 \times 88 \equiv 7\,[101]$. C'est aussi ce que l'on retrouve si l'on part de la relation de Bézout (trouvée à la question 4) et qu'on la multiplie par 7.
6. Avec $a = 15$ et $p = 103$ on trouve $au + pv = 1$ pour $u = -48$, $v = 7$. Un inverse de 15 modulo 103 est donc $u = -48$. Si on préfère un entier positif on peut prendre $u' = 55$ (qui est congru à -48 modulo 103). Une solution de l'équation $15x \equiv 7\,[103]$ est donc $x = 76$, car $7u = 7 \times (-48) = -336 \equiv 76\,[103]$.

Exercice 15.

Les **nombres de Fermat** F_n sont les entiers définis pour $n \in \mathbb{N}$ par
$$F_n = 2^{2^n} + 1$$

1. Montrer que pour tout entier naturel n, on a $F_{n+1} = (F_n - 1)^2 + 1$.
2. Démontrer que pour $n \geqslant 2$, l'écriture décimale des nombres de Fermat (F_n) se termine par le chiffre 7.

Indications 15.

On rappelle que 2^{2^n} signifie $2^{(2^n)}$. Utiliser un raisonnement par récurrence et les congruences modulo 10.

Correction 15.

1. On calcule :
$$(F_n-1)^2+1=(2^{2^n})^2+1=2^{2^n\times 2}+1=2^{2^{n+1}}+1=F_{n+1}$$
2. L'écriture décimale d'un entier N se termine par le chiffre 7 si et seulement si on a $N\equiv 7\,[10]$.
Démontrons donc par récurrence la proposition : "$F_n\equiv 7\,[10]$", pour $n\geqslant 2$.
Initialisation. Pour $n=2$, on a :
$$F_2=2^{2^2}+1=16+1=17\equiv 7\,[10]$$
Hérédité. Supposons que pour un entier $n\geqslant 2$, on ait en effet $F_n\equiv 7\,[10]$. On a alors :
$$F_{n+1}=(F_n-1)^2+1\equiv(7-1)^2+1=36+1=37\equiv 7\,[10]$$
Ainsi la proposition est bien héréditaire.
Conclusion. On a bien démontré par récurrence que tous les nombres de Fermat F_n, pour $n\geqslant 2$, sont congrus à 7 modulo 10 : leur écriture décimale se termine donc par le chiffre 7.