Exercices d'arithmétique

Exercice 1. — *Existe-t-il des couples* $(a,b) \in \mathbb{N}^2$ *tels que :*
- $ab(a+b)$ *n'est pas divisible par* 7 *et*
- $(a+b)^7 - a^7 - b^7$ *est divisible par* 7^7 *?*

Exercice 2. — *Dans l'émission Fort-Boyard, les candidats jouent au jeu suivant : sont disposés alignées* n *craies et les deux joueurs en retirent chacun à leur tour* $1, 2$ *ou* 3*, le perdant étant celui qui retire la dernière craie. Trouver une stratégie gagnante.*

Exercice 3. — *Montrer la formule de Legendre*

$$v_p(n!) = \sum_{k\geq 1} \lfloor \frac{n}{p^k} \rfloor = a_1 + a_2 p + \cdots + a_k p^{k-1}) + (a_2 + \cdots + a_k p^{k-2}) + \cdots + (a_{k-1} + a_k p) + a_k$$

où $n = a_0 + a_1 p + \cdots + a_k p^k$ *est l'écriture de* n *en base* p*.*

Déduire que la valuation 2*-adique du coefficient binomial* $\binom{b}{a+b}$ *est égale à la somme* $\sum_{k=0}^{+\infty} a_k b_k$ *ou* $a = \sum_{k=0}^{+\infty} a_k 2^k$ *et* $b = \sum_{k=0}^{+\infty} b_k 2^k$ *sont les écritures en base* 2 *de* a *et* b*; en particulier noter que pour* $0 < k < n$, $\binom{k}{n}$ *est pair.*

Exercice 4. — ***(Un argument de descente infinie à la Fermat)*** *Soient* $a, b > 0$ *tels que* $ab + 1 | a^2 + b^2$ *; montrer que le quotient est un carré parfait.*

Exercice 5. — *Soit* $\mathcal{E}$ *un ensemble de* 2008 *entiers distincts strictement positifs dont tous les diviseurs premiers sont* ≤ 23*. Montrer que l'on peut trouver* 4 *éléments distincts de* $\mathcal{E}$ *dont le produit est la puissance quatrième d'un entier.*

Exercice 6. — *Donner en fonction de* n*, le pgcd* $(n^3 + n^2 + 1, n^2 + 2n - 1)$*.*

Exercice 7. — *Donner en fonction de* n*, le pgcd* $(n^3 + n^2 - 6n + 2, 2n^2 + 5n - 3)$*.*

Exercice 8. — *Montrer la relation*

$$F_{n+m} = F_{n+1} F_m + F_n F_{m-1}$$

et déduiser-en que $F_n \wedge F_m = F_{n \wedge m}$*.*

Exercice 9. — *Variations sur le théorème de Bezout :*

(1) En utilisant l'algorithme d'Euclide, trouver les relations de Bezout entre 650 *et* 66*.*

(2) On suppose que l'on ne dispose que de pieces de valeurs a *et* b *entières avec* $(a, b) = 1$*.*
   (i) Quelles sommes peut-on payer si on nous rend la monnaie ?
   (ii) Même question si on ne peut pas nous rendre la monnaie ? (Indication : montrer que si $m + n = ab - a - b$ *alors exactement une somme parmi* m *et* n *est payable).*

(3) Etudier le cas de 3 *pièces de valeur* 15*,* 20 *et* 48 *en montrant que* 217 *est la plus grande somme que l'on ne peut pas payer.*

(4) Généraliser la question précédente en montrant que pour $a, b, c > 0$ *premiers entre eux deux à deux,* $2abc - ab - bc - ac$ *est le plus grand entier qui ne peut pas s'écrire sous la forme* $xbc + yca + zab$ *avec* $x, y, z \geq 0$*.*

(5) *Montrer par récurrence sur n que si $a_1, \cdots, a_n$ sont n entiers strictement positifs premiers entre eux deux à deux alors*

$$a_1 \cdots a_n \Big(n - 1 - \sum_{i=1}^{n} \frac{1}{a_i} \Big)$$

est le plus grand entier qui ne peut pas s'écrire sous la forme $\sum_{i=1}^{n} x_i \prod_{j \neq i} a_j$ avec $x_i \geq 0$ pour tout $i = 1, \cdots, n$.

Exercice 10. — *Montrer que 7 divise $3^{105} + 4^{105}$.*

Exercice 11. — *Montrer l'équivalence $3|a$ et $3|b \iff 3|a^2 + b^2$.*

Exercice 12. — *Proposer à vos amis doués en calcul mental le jeu suivant : multiplier par 13 leur jour de naissance, multiplier par 14 leur mois de naissance, additionner ces deux résultats pour former un nombre n qu'il vous communique. Comment retrouver les données cachées ?*

Exercice 13. — *Un nouveau jeu pour des amis coopératifs : choisir un nombre k entre 1 et 8, puis communiquer le résultat $n = 10A - 9k$ où A est l'âge du candidat. Expliquer comment vous retrouvez A.*

Exercice 14. — *Donner les morphismes de groupe $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ puis ceux de $\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$. Trouver une condition nécessaire et suffisante sur m et n pour que tout morphisme $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ soit nul.*

Exercice 15. — *Montrer l'équivalence $6|a + b + c \iff 6|a^3 + b^3 + c^3$.*

Exercice 16. — *Montrer que 429 est inversible dans $\mathbb{Z}/700\mathbb{Z}$ et donner son inverse.*

Exercice 17. — *Résoudre dans $\mathbb{Z}$ les congruences suivantes :*

1) $3x \equiv 4 \mod 7$ *;*

2) $9x \equiv 12 \mod 21$ *;*

3) $103x \equiv 612 \mod 676$.

Exercice 18. — *Donner la congruence modulo 17 de $(1035125)^{5642}$.*

Exercice 19. — *Donner la congruence modulo 18 de 1823^{242} puis celle de 2222^{321} modulo 20.*

Exercice 20. — *Montrer que $n^7 \equiv n \mod 42$.*

1 Essayons de factoriser $P(x) = (x+1)^7 - x^7 - 1$ en regardant ses racines : on remarque qu'outre 0 et 1, le nombre complexe $j = e^{2i\pi/3}$ est aussi racine car $j + 1 = -j^2$ de sorte que $P(x)$ est divisible par $x(x+1)(x^2+x+1)$ le quotient étant égal à x^2+x+1 et donc

$$(a+b)^7 - a^7 - b^7 = 7ab(a+b)(a^2+ab+b^2)^2.$$

On est ainsi amené à résoudre $a^2 + ab + b^2 \equiv 0 \mod 7^3$ qui s'écrit encore

$$(a + \frac{b}{2})^2 \equiv -3(\frac{b}{2})^2 \mod 7^3$$

laquelle possède des solutions si et seulement si le symbole de Legendre $(\frac{-3}{7^3}) = 1$ ce que l'on vérifie aisément en utilisant la loi de réciprocité quadratique.

2 Analysons les dernières positions : l'unique ultime position perdante est celle où le joueur a devant lui une unique craie. Ainsi s'il reste entre 2 et 4 craies, la position est gagnante puisqu'il suffit de retirer toutes les craies sauf une.

Formulons alors la stratégie gagnante : une position est perdante (resp. gagnante) si le nombre de craies restantes est (resp. n'est pas) congrue à 1 modulo 4. La preuve de cette affirmation repose sur les points suivants :

- si le nombre de craies n'est pas congru à 1 modulo 4 alors le joueur peut, en enlevant $1, 2$ ou 3 craies, la ramener à 1 modulo 4 ;
- en revanche dans le cas contraire, où le nombre de craies est congru à 1 modulo 4, le joueur en retirant $1, 2$ ou 3 craies ramène la position à un nombre de craies non congru à 1 modulo 4.
- S'il ne reste qu'une craie alors le joueur a perdu.

3 Pour tout $k > 0$, l'ensemble $[1, n]$ contient $\lfloor n/p^k \rfloor$ multiples de p^k de sorte qu'il y a exactement $\lfloor n/p^k \rfloor - \lfloor n/p^{k+1} \rfloor$ éléments i tels que $v_p(i) = k$ ce qui donne le résultat.

En ce qui concerne la valuation 2-adique de $\binom{b}{a+b}$ elle découle directement de la formule de Legendre en remarquant que

$$\lfloor \frac{a+b}{2^k} \rfloor - \lfloor \frac{a}{2^k} \rfloor - \lfloor \frac{b}{2^k} \rfloor$$

est non nulle si et seulement si $a_k = b_k = 1$.

4 On raisonne par l'absurde ; on prend (a, b) tel que $\max\{a, b\}$ soit minimal avec $\frac{a^2+b^2}{ab+1} = k$ qui n'est pas un carré parfait. Remarquons déjà que si $a = b$ alors $a = b = k = 1$ ne convient pas. Supposons donc $0 < a < b$ et écrivons l'égalité précédente sous la forme

$$b^2 - (ka)b + a^2 - k = 0$$

de sorte que b est une racine du polynôme $X^2 - (ka)X + a^2 - k$, lequel possède une deuxième racine b' telle que $b + b' = ka$ et donc $b' \in \mathbb{Z}$. Par ailleurs on a :

- $bb' = a^2 - k$ et donc $b' = (a^2 - k)/b < a$;
- $b' > 0$: en effet si $b' < 0$ alors $k = (a^2 + (b')^2)/(ab' + 1) < 0$ ce qui n'est pas et si $b' = 0$ alors $k = a^2$ ce qui n'est pas non plus.

En résumé le couple (a, b') avec $0 < b' < a$ est plus petit que (a, b) vérifie les mêmes hypothèses ce qui contredit la minimalité de (a, b).

5 A tout élément n de $\mathcal{E}$, on associe bijectivement un vecteur $(n_1, \cdots, n_9) \in \mathbb{Z}^9$ tel que $n = 2^{n_1}3^{n_2}\cdots 23^{n_9}$; il s'agit alors de démontrer que l'on peut trouver 4 vecteurs de $\mathbb{Z}^9$ dont la somme appartient à $4\mathbb{Z}^9$. Remarquons déjà que d'après le principe des tiroirs, étant donnés $2^9 + 1$ vecteurs de $\mathbb{Z}^9$, il en existe 2 dont la somme est dans $2\mathbb{Z}^9$. L'idée est alors la suivante : construire des a_k, b_k deux à deux distincts pour $1 \leq k \leq 2^9 + 1$ tels que $s_k = a_k + b_k \in 2\mathbb{Z}^9$ de

sorte que l'on pourra trouver $i \neq j$ avec $(s_i/2)$ et $(s_j/2)$ de somme appartenant à $\mathbb{Z}^9$. Pour cela il suffit d'avoir au départ $(2^9+1)+2.2^9 = 1537 < 2008$ éléments distincts : on commence par prendre $a_1 + b_1 \in 2\mathbb{Z}^9$, puis ainsi de suite. S'il existe $i \neq j$ tels que $s_i = s_j$ c'est gagné, sinon on réapplique ce qui précède à l'ensemble de $2^9 + 1$ éléments distincts constitués des $s_i/2$.

6 Le but est de faire des combinaisons pour faire descendre le degré ; concrètement appelons $\delta(n)$ ce pgcd. On a $n^3 + n^2 + 1 = (n^2 + 2n - 1)(n - 1) - (n + 1)$ de sorte que $\delta(n) = (n^2+2n-1, n+1)$. De même $n^2+2n-1 = (n+1)^2-2$ et donc $\delta(n) = (n+1, 2)$ soit $\delta(n) = 2$ si $n \equiv 1 \mod 2$ et $\delta(n) = 1$ si $n \equiv 0 \mod 2$.

7 On procède comme dans l'exercice précédent au détail près que l'on ne divise plus par un polynôme unitaire ; appelons $\delta(n)$ le pgcd cherché et $\delta_1(n) = (2n^3+2n^2-12n+4, 2n^2+5n-3)$; de manière générale on a $\delta_1(n) = \delta(n)$ si la multiplicité de 2 [(1)] dans $n^3 + n^2 - 6n + 2$ est supérieure ou égale à celle dans $2n^2 + 5n - 3$, sinon $\delta_1(n) = 2\delta(n)$: en particulier si $n \equiv 0 \mod 2$ alors $2n^2 + 5n - 3$ est impair et donc $\delta(n) = \delta_1(n)$. De l'égalité $2n^3 + 2n^2 - 12n + 4 = n(2n^2 + 5n - 1) - (3n^2 + 9n - 4)$ on en déduit $\delta_1(n) = (2n^2 + 5n - 3, 3n^2 + 9n - 4) = (2n^2 + 5n - 3, n^2 + 4n - 1) = (n^2 + 4n - 1, 3n + 1)$ par simples soustractions. On introduit à nouveau $\delta_2(n) = (3n^2 + 12n - 3, 3n + 1)$ et comme $3n + 1$ n'est pas divisible par 3, on a $\delta_1(n) = \delta_2(n)$ et de l'égalité $3n^2 + 12n - 3 = (3n + 1)(n + 3) + 2n - 6$, on en déduit $\delta_2(n) = (2n - 6, 3n + 1)$. On introduit $\delta_3(n) = (n - 3, 3n + 1)$ avec $\delta_3(n) = \delta_2(n)$ si la multiplicité de 2 dans $n-3$ est supérieure ou égale à celle dans $3n+1$ et sinon $\delta_2(n) = 2\delta_3(n)$. On a $\delta_3(n) = (n - 3, 10)$ de sorte que

$$\delta_3(n) = \begin{cases} 10 \text{ si } n \equiv 3 \mod 10 \\ 5 \text{ si } n \equiv 3 \mod 5 \text{ et } n \equiv 0 \mod 2 \\ 2 \text{ si } n \equiv 1 \mod 2 \text{ et } n \not\equiv 3 \mod 5 \\ 1 \text{ si } n \equiv 0 \mod 2 \text{ et } n \not\equiv 3 \mod 5 \end{cases}$$

On traite alors les cas un par un :

(a) Si $\delta_3(n) = 1$ ou 5 soit $n \equiv 0 \mod 2$, soit $3n + 1 \equiv 1 \mod 2$ et donc $\delta_3(n) = \delta_2(n) = \delta_1(n)$; on a de même $2n^2 + 5n - 3 \equiv 1 \mod 2$ soit $\delta(n) = \delta_1(n)$;

(b) si $\delta_3(n) = 2$ ou 10 soit $n \equiv 1 \mod 2$ et $n \not\equiv 3 \mod 5$, alors si $n \equiv 3 \mod 4$ on a $3n + 1 \equiv 2 \mod 4$ et $\delta_2(n) = \delta_3(n) = \delta_1(n)$; en outre $2n^2 + 5n - 3 \equiv 2 \mod 4$ et $n^3 + n^2 - 6n + 2 \equiv 0 \mod 4$ et donc $\delta(n) = \delta_1(n)$. Si on a $n \equiv 1 \mod 4$ alors de même $3n+1 \equiv 0 \mod 4$ et $n-3 \equiv 2 \mod 4$ soit $\delta_1(n) = \delta_2(n) = 2\delta_3(n)$; $2n^2+5n-3 \equiv 0 \mod 4$ et $n^3 + n^2 - 6n + 2 \equiv 2 \mod 4$ de sorte que $\delta_1(n) = 2\delta(n)$;

Ainsi on a toujours $\delta(n) = \delta_3(n)$.

8 Une façon agréable de faire des calculs est d'écrire matriciellement

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

Le résultat découle alors directement de la multiplication de cette égalité pour n et m. On en déduit alors que $F_{n+m} \wedge F_m = F_n F_{m-1} \wedge F_m = F_n \wedge F_m$ car par une récurrence immédiate $F_m \wedge F_{m-1} = 1$. En appliquant l'algorithme d'Euclide (soustractif, i.e. on ne fait pas de division euclidienne mais on soustrait simplement), on obtient le résultat.

1. i.e. le plus grand entier r tel que 2^r divise le nombre en question

9 1) On remarque tout d'abord que $650 = 2.325$ et $66 = 2.33$. On va appliquer l'algorithme d'Euclide à 325 et 33 puis on multipliera par deux, ce qui nous permet de gagner quelques lignes de calculs (on n'est pas un ordinateur...)

$$325 = 33.9 + 28 \quad 33 = 28 + 5 \quad 28 = 5.5 + 3$$
$$5 = 3 + 2 \qquad 3 = 2 + 1$$

On remonte alors les calculs :

$$\begin{aligned} 1 &= 3 - 2 \\ 1 &= 3 - (5 - 3) = 2.3 - 5 \\ 1 &= 2.(28 - 5.5) - 5 = 2.28 - 11.5 \\ 1 &= 2.28 - 11.(33 - 28) = 13.28 - 11.33 \\ 1 &= 13.(325 - 9.33) - 11.33 = 13.325 - 128.33 \end{aligned}$$

Finalement la relation de Bezout est $2 = 13.650 - 128.66$, c'est la plus "simple" ; on rappelle que les autres sont données par

$$2 = (13 + k.66)650 - (128 - k.650)66$$

pour $k \in \mathbb{Z}$. (2-i) D'après la relation de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $1 = ua + vb$, i.e. si on nous rend la monnaie (u ou v est forcément négatif), pouvant payer la somme 1, on peut payer n'importe quelle somme entière.

(2-ii) On écrit $m = ax + by$ et $n = au + bv$ de la façon la plus simple possible, i.e. $0 \leq x, u \leq b - 1$, de sorte que l'écriture est unique ; en effet on rappelle que $m = a(x - bt) + b(y + at)$, de sorte qu'il existe un unique t tel que $0 \leq x - bt < b$. L'égalité $m + n = ab - a - b$ donne alors $ab = a(x + u + 1) + b(v + y + 1)$: a et b étant premier entre eux, "le" théorème de Gauss nous dit que b divise $x + u + 1$. Or on a $1 \leq x + u + 1 \leq 2b - 1$, le seul multiple de b dans cet intervalle est b lui-même, soit $x + u + 1 = b$ et donc $v + y + 1 = 0$. Les nombres y et v étant des entiers, exactement un parmi eux deux est positif ou nul, l'autre étant strictement négatif. En language clair exactement une somme parmi m et n est payable sans rendu de monnaie. En remarquant que 0 est payable, alors $ab - a - b$ n'est pas payable. De même une somme négative n'est pas payable de sorte que si $m > ab - a - b$, la somme m est payable. 3) On écrit $48x + 20y + 15z = 3(16x + 5z) + 20y$. D'après ce qui précède tout nombre de la forme $60 + t$ avec $t \geq 0$ peut s'écrire sous la forme $16x + 5Z$. De même tout nombre de la forme $38 + s$ avec $s \geq 0$, peut s'écrire sous la forme $3t + 20y$. Finalement toute somme supérieure ou égale à 218 est payable. Étudions le cas de 217 : $217 = 20y + 3u$, $217 \equiv -3 \mod 20$, on en déduit que $-3(u + 1)$ doit être divisible par 20, soit $u = 20k - 1$ et $220 = 20(y + 3k)$ soit $11 = y + 3k$ ce qui donne $u = 19, 39, 59$ et on vérifie aisément qu'aucune de ses possibilités ne s'écrit sous la forme $16x + 5z$ avec x, y positifs.

4) Soit $n > 2abc - bc - ac - ab$. D'après le théorème de Bezout, il existe $0 \leq x < a$ avec $n \equiv x \mod xbc \mod a$; soit $y' \in \mathbb{Z}$ tel que $n = xbc + y'a$ de sorte que

$$y'a = n - xbc > 2abc - bc - ac - ab - (a - 1)bc = (bc - b - c)a$$

et donc $y' > bc - b - c$. D'après (b), il existe $y, z \geq 0$ tel que $y' = zb + yc$ et donc $n = xbc + yac + zab$.

Supposons par l'absurde que $2abc - bc - ac - ab = xbc + yac + zab$ avec $x, y, z \geq 0$; on aurait alors $a|(x + 1)bc$ et donc $a|x + 1$ d'après le lemme de Gauss, soit $x \geq a - 1$. De même

on aurait $y \geq b-1$ et $z \geq c-1$ si bien que

$$xbc + yac + zbc \geq 3abc - bc - ac - ab > 2abc - bc - ac - ab$$

ce qui n'est pas.

5) D'après ce qui précède la propriété est vraie pour $n = 2, 3$; on la suppose vraie jusqu'au rang $n-1$ et prouvons la au rang n. Soit $k > M = a_1 \cdots a_n\Big(n - 1 - \sum_{i=1}^{n} \frac{1}{a_i}\Big)$; comme a_n est premier avec $a_1 \cdots a_{n-1}$, d'après le théorème de Bezout, il existe $0 \leq x_n < a_n$ tel que $k \equiv x_n a_1 \cdots a_{n-1} \mod a_n$; notons $q_n = (k - x_n a_1 \cdots a_{n-1})/a_n$ de sorte que

$$N > \frac{a_1 \cdots a_n\Big(n - 1 - \sum_{i=1}^{n} \frac{1}{a_i}\Big) - (a_n - 1)a_1 \cdots a_{n-1}}{a_n} = a_1 \cdots a_{n-1}\Big(n - 2 - \sum_{i=1}^{n-1} \frac{1}{a_i}\Big).$$

D'après l'hypothèse de récurrence $N = \sum_{i=1}^{n-1} \prod_{j \neq i} a_j$ avec $x_i \geq 0$ pour tout $i = 1, \cdots, n-1$ et donc $k = \sum_{i=1}^{n} x_i \prod_{j \neq i} a_j$.

Supposons désormais que $M = \sum_{i=1}^{n} x_i \prod_{j \neq i} a_j$ avec $x_i \geq 0$ pour tout $i = 1, \cdots, n$. Alors comme dans (d), le lemme de Gauss donne que $a_i | (x_i + 1)$ et donc $x_i \geq a_i - 1$ et finalement que

$$M \geq \sum_{i=1}^{n} (a_i - 1) \prod_{j \neq i} a_j > a_1 \cdots a_n\Big(n - 1 \sum_{i=1}^{n} \frac{1}{a_i}\Big) = M$$

d'où la contradiction.

10 Comme $4 \equiv -3 \mod 7$ et que 105 est impair, on a $4^{105} \equiv -3^{105}$ d'où le résultat.

11 Le sens $\Rightarrow$ est évident ; en ce qui concerne l'autre sens, il suffit de faire un petit tableau des sommes $a^2 + b^2$ avec $a, b \in \mathbb{Z}/3\mathbb{Z}$ pour s'apercevoir que $a^2 + b^2 \equiv 0 \mod 3 \Rightarrow a, b \equiv 0 \mod 3$.

12 L'entier n est congru au mois M de naissance modulo 13 ce qui le détermine parfaitement ; il suffit alors de calculer le jour directement à partir de $n - 14M$.

13 On a $n \equiv A \mod 9$; il reste alors à déterminer A exactement ce qui est aisé puisque $k < 9$ de sorte que l'ordre de grandeur de n fixe A.

14 On rappelle qu'un morphisme d'un groupe cyclique de cardinal n dans un groupe G est complètement déterminé par l'image g d'un générateur quelconque telle $g^n = 1_G$, soit g d'ordre divisant n. Dans le premier cas comme 3 et 4 sont premiers entre eux, les seuls éléments d'ordre divisant 3 dans $\mathbb{Z}/4\mathbb{Z}$ sont le seul d'ordre 1 à savoir 0 de sorte que tout morphisme $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ est nul.

Dans $\mathbb{Z}/15\mathbb{Z}$ les éléments d'ordre divisant 12 sont donc d'ordre divisant $12 \wedge 15 = 3$ et sont donc $0, 5, 10$, ce qui donne 3 morphismes distincts.

D'après les raisonnements ci-dessus, on en déduit donc qu'une CNS pour qu'il n'y ait pas de morphisme non nul $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ est donc $n \wedge m = 1$.

15 Il suffit de remarquer que $a^3 - a$ est divisible par 2 et 3 et donc 6 divise $(a^3 - a) + (b^3 - b) + (c^3 - c)$ et donc $a^3 + b^3 + c^3 \equiv a + b + b \mod 6$.

16 On rappelle que 700 n'étant pas premier, 429 est inversible dans $\mathbb{Z}/700\mathbb{Z}$ si et seulement si il est premier avec 700 et son inverse est donné par la relation de Bezout, i.e. si $1 = 700a + 429b$ alors l'inverse cherché est b. Il suffit alors d'appliquer l'algorithme d'Euclide :

$$700 = 429 + 271 \quad 429 = 271 + 158 \quad 271 = 158 + 113 \quad 158 = 113 + 45$$
$$113 = 2.45 + 23 \qquad 45 = 23 + 22 \qquad 23 = 22 + 1$$

On remonte alors les calculs et on obtient la relation de Bezout : $1 = 19.700 - 31.429$ de sorte que l'inverse de 429 dans $\mathbb{Z}/700\mathbb{Z}$ est -31.

17 1) Comme 3 est premier avec 7, il est inversible dans $\mathbb{Z}/7\mathbb{Z}$; on calcule rapidement que $3.5 \equiv 1 \mod 7$, i.e. $5 = 1/3$ dans $\mathbb{Z}/7\mathbb{Z}$ de sorte que l'équation s'écrit $x \equiv 20 \mod 7$ soit $x \equiv -1 \mod 7$.

2) D'après le théorème chinois, il suffit de vérifier l'équation modulo 3 et 7. Modulo 3 l'équation s'écrit $0.x \equiv 0 \mod 3$ et est donc toujours vérifiée. Modulo 7, on obtient $2x \equiv -2 \mod 7$; l'inverse de 2 dans $\mathbb{Z}/7\mathbb{Z}$ est -3, soit donc $x \equiv -1 \mod 7$. Le résultat final est donc $x \equiv -1 \mod 7$;

3) On calcule rapidement $676 = 2^2.13^2$; par le théorème chinois, on est donc ramené à résoudre $-x \equiv 0 \mod 4$ et $103x \equiv 105 \mod 169$. L'algorithme d'euclide fournit $64.103 - 39.169 = 1$ soit donc $x \equiv 64.105 \mod 69$ soit $x \equiv -40 \mod 169$ et donc $x \equiv -40 \mod 676$.

On peut aussi résoudre la congruence $103x \equiv 105 \mod 13^2$ de proche en proche, de la façon suivante. On la résoud tout d'abord modulo 13 soit $2x \equiv 4 \mod 13$ soit $x \equiv 2 \mod 13$. On écrit alors $x = 2 + 13k$ et on est donc ramené à résoudre $206 + 13.103k \equiv 105 \mod 13^2$ soit $13.103k \equiv -13.8 \mod 13^2$ soit en simplifiant par 13, $103k \equiv -8 \mod 13$, soit $2k \equiv -8 \mod 4$ et donc $k \equiv -4 \mod 13$ et donc finalement $x \equiv 2 - 4.13 \mod 13^2$.

18 On a $1035125 \equiv 12 \mod 17$. On pourrait maintenant calculer l'ordre de 12 dans $\mathbb{Z}/17\mathbb{Z}$. D'après le petit théorème de Fermat on a $12^16 \equiv 1 \mod 17$. Or $5642 \equiv 10 \mod 16$; la réponse est alors 12^10 modulo 17. Or $12 \equiv -5 \mod 17$ et $12^2 \equiv 8 \mod 17$ soit $12^4 \equiv -4$ soit $12^8 \equiv -1$ de sorte que l'ordre de 12 est 16. Finalement $12^10 = 12^8 12^2 = -12^2 = -8 = 9 \mod 17$.

19 On a $1823 \equiv 5 \mod 18$; or $5 \in (\mathbb{Z}/18\mathbb{Z})^\times$ on peut donc utiliser le petit théorème de Fermat avec $\varphi(18) = \varphi(2)\varphi(9) = 1.6 = 4$ soit $5^6 \equiv 1 \mod 18$. Or on a $242 \equiv 2 \mod 6$ soit $1823^{242} \equiv 5^2 = 7 \mod 18$. De même $2222 \equiv 2 \mod 20$ avec $2 \notin (\mathbb{Z}/20\mathbb{Z})^\times$; on ne peut donc pas utiliser le petit théorème de Fermat (2^8 est pair et ne peut donc pas être congru à 1 modulo 20). On étudie alors la suite $u_n = 2^n$ modulo 20 pour $n \in \mathbb{Z}$: $u_0 = 1$, $u_1 = 2$, $u_2 = 4$, $u_3 = 8$, $u_4 = -4$, $u_5 = -8$, $u_6 = 4$. On remarque qu'à partir de $n \geq 2$ la suite est périodique de période 4 : $u_{n+4} = u_n$. Or $321 \equiv 1 \mod 4$ de sorte que $u_{321} = u_5 = -8$ et donc $2222^{321} \equiv -8 \mod 20$.

La bonne façon de comprendre le phénomène est d'utiliser le lemme chinois. On a $2222 \equiv 2 \mod 4$ de sorte que $2222^n \equiv 0 \mod 4$ dès que $n \geq 2$. On a aussi $2222 \equiv 2 \mod 5$ et $321 \equiv 1 \mod 4$ et donc d'après le petit théorème de Fermat $2222^{321} \equiv 2 \mod 5$ et donc $2222^{321} \equiv 12 \mod 20$.

Remarque : On comprend ainsi que de manière générale la suite $u_n = a^n \mod m$ pour a non premier avec m est périodique à partir d'un certain rang (le temps que pour les premiers p divisant $a \wedge m$, $a^k \equiv 0 \mod m$ soit $k\alpha_a(p) \geq \alpha_m(p)$ où $\alpha_a(p)$ (resp. $\alpha_m(p)$) est la multiplicité de p dans a (resp. dans m)). Une autre façon de le remarquer et de dire qu'elle ne prend qu'un nombre fini de valeurs de sorte qu'il existe n_0 et $n_0 + r$ tels que $u_{n_0} = u_{n_0+r}$ ce qui implique que $u_{n_0+r+k} = u_{n_0+k}$ et donc la périodicité de u_n à partir d'un certain rang.

20 On a $42 = 2.3.7$, il suffit alors de vérifier la congruence modulo 2, 3 et 7. Pour 2 et 3, on a clairement $n^7 \equiv n$ et pour 7 le résultat découle du petit théorème de Fermat.