Corrigé
TD arithmétique

Exercice 1
(3694)

On va commencer par étudier les puissances de 3 modulo 13. On commence par remarquer que

$$3^1 \equiv 3\ [13], \quad 3^2 \equiv 9\ [13],\ 3^3 \equiv 1\ [13].$$

On sait donc que, puisque $126 = 3 * 42$, $3^{126} \equiv (3^3)^{42}\ [13]$, et donc $3^{126} \equiv 1\ [13]$. De même, on a

$$5^1 \equiv 5\ [13], \quad 5^2 \equiv 12\ [13], \quad 5^3 \equiv 8\ [13], \quad 5^4 \equiv 1[13].$$

Par un raisonnement similaire, et utilisant que $126 = 31 * 4 + 2$, on trouve

$$5^{126} \equiv 5^2\ [13] \text{ soit } 5^{126} \equiv 12\ [13].$$

On en déduit que

$$3^{126} + 5^{126} \equiv 0\ [13],$$

ce qui signifie bien que 13 divise $3^{126} + 5^{126}$.

Exercice 2
(3698)

Puisque $n-4$ divise $3n-17$ et que $n-4$ divise $n-4$, $n-4$ divise également $(3n-17) - 3(n-4) = -5$. Or les diviseurs dans $\mathbb{Z}$ de -5 sont $-5, -1, 1, 5$. Les valeurs possibles de $n-4$ sont donc ces valeurs, et donc on a $n \in \{-1, 3, 5, 9\}$.
Réciproquement, si $n = -1$, alors $n - 4 = -5$ divise $3n - 17 = -20$. Si $n = 3$, $n - 4 = -1$ divise $3n - 17 = -8$. Si $n = 5$, $n - 4 = 1$ divise $3n - 17 = -2$. Si $n = 9$, $n - 4 = 5$ divise $3n - 17 = 10$.
En conclusion, les valeurs de n qui conviennent sont $-1, 3, 5$ et 9.

Exercice 3
(3703)

Posons $u_n = (3-\sqrt{5})^n + (3+\sqrt{5})^n$. L'idée est de prouver que la suite (u_n) vérifie une relation de récurrence d'ordre 2. En effet, elle est de la forme $u_n = r_1^n + r_2^n$. D'après la théorie des suites récurrentes linéaires, (u_n) vérifie l'équation de récurrence linéaire dont l'équation caractéristique associée est

$$X^2 - (r_1 + r_2)X + r_1 r_2 = 0 \iff X^2 - 6X + 4 = 0.$$

Autrement dit, on a $u_{n+2} = 6u_{n+1} - 4u_n$. Bien sûr, on peut vérifier directement que la suite (u_n) satisfait cette condition de récurrence.
On prouve alors par récurrence sur n que 2^n divise u_n. C'est vrai pour $n = 0$, car $u_0 = 2$ et pour $n = 1$, car $u_1 = 6$. Supposons que $2^n | u_n$ et $2^{n+1} | u_{n+1}$. Alors, écrivant $u_n = k2^n$ et $u_{n+1} = l2^{n+1}$, on a

$$u_{n+2} = 2 \times 3 \times l2^{n+1} - 2^2 \times k2^n = 2^{n+2}(3l - k).$$

Ceci prouve le résultat demandé.

Exercice 4
(3704)

Notons d le pgcd à calculer. Puisqu'il divise les deux nombres, il divise 25 et d est donc égal à 1, 5 ou 25. S'il est égal à 5 ou 25, ceci signifie que 5 divise $3^{123} - 5$. Mais alors, puisque 5 divise -5, ceci entrainerait encore que 5 divise 3^{123}, ce qui n'est pas vrai. Donc $d = 1$.

n et $n+1$ sont deux entiers consécutifs. L'un des deux au moins est pair, et donc $2|n(n+1)(n+2)$. De même, n, $n+1$ et $n+2$ sont trois entiers consécutifs. L'un au moins est un multiple de 3, et donc $3|n(n+1)(n+2)$. Par le théorème de Gauss, puisque 2 et 3 sont premiers entre eux, $6|n(n+1)(n+2)$.

Exercice 5
(3708)

On remarque que $4(n^2+n) = (2n+1)^2 - 1$. Ainsi, si $d|(n^2+n)$ et $d|2n+1$, $d|1$. On a donc $(n^2+n) \wedge (2n+1) = 1$.

Rappelons que si $a = bq + r$, on a $a \wedge b = b \wedge r$ et que $a \wedge b = a \wedge (a-b)$ (on écrit $a = b + (a-b)$). Ainsi, on trouve ici

$$30n^2 + 21n + 13 = 2(15n^2 + 8n + 6) + 5n + 1, \quad 15n^2 + 8n + 6 = 3n(5n+1) + 5n + 6.$$

On a donc

$$\begin{aligned}(30n^2 + 21n + 13) \wedge (15n^2 + 8n + 6) &= (15n^2 + 8n + 6) \wedge (5n+1) \\ &= (5n+1) \wedge (5n+6) \\ &= (5n+1) \wedge 5 \\ &= 1.\end{aligned}$$

Exercice 6
(3710)

Admettons qu'il existe une solution rationnelle $x = p/q$, avec $p \wedge q = 1$ et $q > 0$. Alors, remplaçant x par p/q dans l'équation et multipliant tout par q^3, on obtient :

$$p^3 + p^2 q + p q^2 + q^3 = 0.$$

Puisque $q|p^2q + pq^2 + q^3$, on obtient $q|p^3$ et donc $q = 1$ puisque p et q sont premiers entre eux. En effectuant le même raisonnement avec p, on obtient $p = \pm 1$. Or 1 et -1 ne sont pas solutions de l'équation. Il y a donc contradiction.

Exercice 7
(3726)

Considérons un entier n et p l'unique entier tel que $2^p \leq n < 2^{p+1}$. Alors, tout entier $k \leq n$, différent de 2^p, s'écrit $k = 2^u v$ avec v impair et $u \leq p-1$. Ainsi,

$$\sum_{k=1}^{n} \frac{1}{k} = \frac{1}{2^p} + \sum_{k \leq n,\ k \neq 2^p} \frac{1}{k} = \frac{1}{2^p} + \frac{N}{2^{p-1} q}$$

où q est impair. On en déduit que

$$S_n = \sum_{k=1}^{n} \frac{1}{k} = \frac{q + 2N}{2^p q}$$

et le numérateur est impair alors que le dénominateur est pair.... Donc S_n n'est pas un entier.

Exercice 8
(3727)

La méthode pour ce type d'exercice est toujours la même et est très importante à savoir. On commence par rechercher le premier entier $k \geq 1$ tel que $2^k \equiv 1\ [5]$. On va ensuite raisonner modulo k. On trouve successivement :

$$2^1 \equiv 2\ [5], \quad 2^2 \equiv 4\ [5], \quad 2^3 \equiv 3\ [5], \quad 2^4 \equiv 1\ [5].$$

On va donc classer les entiers n modulo 4. En effet, si $n = 4q + r$, alors sachant que $2^{4q} \equiv 1^q\ [5]$ soit $2^{4q} \equiv 1\ [5]$, on trouve que

$$2^n \equiv 2^r\ [5].$$

Ainsi, on obtient <ul class="rien">
Si $n \equiv 0\ [4]$, alors $2^n \equiv 1\ [5]$;
Si $n \equiv 1\ [4]$, alors $2^n \equiv 2\ [5]$;
Si $n \equiv 2\ [4]$, alors $2^n \equiv 4\ [5]$;
Si $n \equiv 3\ [4]$, alors $2^n \equiv 3\ [5]$;

On commence par effectuer la division euclidienne de 1357 par 5, et on trouve que $1357 \equiv 2\ [5]$, d'où $1357^{2013} \equiv 2^{2013}\ [5]$. De plus, $2013 \equiv 3\ [5]$. On en déduit que $1357^{2013} \equiv 2^3 \equiv 3\ [5]$.

Exercice 9
(3734)

Puisque $n \wedge m = 1$, le théorème de Bezout nous donne l'existence de $u, v \in \mathbb{Z}$ tel que $un + vm = 1$. L'équation $nx \equiv a\ [m]$ implique $unx \equiv ua\ [m]$. Or, $un \equiv 1[m]$ et donc l'équation devient $x \equiv ua[m]$. Réciproquement, si $x \equiv ua\ [m]$, alors $nx \equiv nua \equiv a[m]$. Ainsi, l'ensemble des solutions de l'équation est $\{ua + mk;\ k \in \mathbb{Z}\}$.

On a l' équivalence suivante :

$$\begin{cases} x & \equiv & a\ [n] \\ x & \equiv & b\ [m] \end{cases} \iff \begin{cases} \exists k \in \mathbb{Z},\ x = a + nk \\ nk \equiv b - a\ [m]. \end{cases}$$

On applique alors le résultat de la question précédente pour obtenir les valeurs possibles de k. Soit $(u, v) \in \mathbb{Z}^2$ tels que $un + vm = 1$.

$$\begin{cases} x & \equiv & a\ [n] \\ x & \equiv & b\ [m] \end{cases} \iff \begin{cases} \exists k \in \mathbb{Z},\ x = a + nk \\ k \equiv u(b - a)\ [m] \end{cases}$$

$$\iff \begin{cases} \exists k \in \mathbb{Z},\ x = a + nk \\ \exists l \in \mathbb{Z},\ k = u(b - a) + ml. \end{cases}$$

On remplace alors k par sa valeur dans la première équation, et on trouve que x est solution si et seulement si il existe $l \in \mathbb{Z}$ tel que $x = a + nu(b - a) + nml$. On obtient bien des solutions qui sont uniques modulo nm.

On commence par mettre en équation le problème. Soit x les temps, en secondes depuis minuit, où les deux phares sont allumés au même moment. Les données du problème nous disent que x est solution du système :

$$\begin{cases} x & \equiv & 2\ [15] \\ x & \equiv & 8\ [28]. \end{cases}$$

On cherche le plus petit entier naturel x solution de ce système. Comme $15 \wedge 28 = 1$, on peut appliquer les résultats de la question précédente. Il suffit de chercher (u, v) tels que $15u + 28v = 1$. On applique

l'algorithme d'Euclide :

$$\begin{aligned} 28 &= 15 \times 1 + 13 \\ 15 &= 13 \times 1 + 2 \\ 13 &= 6 \times 2 + 1 \end{aligned}$$

soit, en remontant les calculs

$$\begin{aligned} 1 &= -6 \times 2 + 1 \times 13 \\ &= -6 \times (15 - 13) + 13 = 7 \times 13 - 6 \times 15 \\ &= 7 \times (28 - 15) - 6 \times 15 \\ &= 7 \times 28 - 13 \times 15. \end{aligned}$$

x est donc le plus petit entier naturel de

$$\{2 + 15 \times (-13) \times (8 - 2) + 28 \times 15 \times k;\ k \in \mathbb{Z}\} = \{-1168 + 420k;\ k \in \mathbb{Z}\}.$$

Le plus petit entier naturel de cet ensemble est obtenu pour $k = 3$, et on trouve $x = 92$: les deux phares seront allumés au même moment pour la première fois 1 minute et 32 secondes après minuit.

Là encore, il faut traduire ceci en termes de congruences. On a :

$$\begin{cases} x \equiv 3\ [17] \\ x \equiv 4\ [11] \\ x \equiv 5\ [6] \end{cases}$$

Ce problème se traite exactement de la même façon. On peut aussi résoudre d'abord les deux premières équations ensembles, puis introduire dans la troisième. Ici, tout est facilité si on remarque que 37 est tel que $37 \equiv 3\ [17]$ et $37 \equiv 4\ [11]$. Puisque $17 \wedge 11 = 1$, on sait d'après la deuxième question que

$$\begin{cases} x \equiv 3\ [17] \\ x \equiv 4\ [11] \end{cases} \iff x \equiv 37[187].$$

On doit donc résoudre le système

$$\begin{cases} x \equiv 37\ [187] \\ x \equiv 5\ [6]. \end{cases}$$

Or, $1 = 1 \times 187 - 6 \times 37$. L'ensemble des solutions de ce système est donc :

$$\{37 + 187 \times 1 \times (5 - 37) + 1122k;\ k \in \mathbb{Z}\} = \{-5947 + 1122k;\ k \in \mathbb{Z}\}.$$

Le plus petit entier positif est obtenu pour $k = 6$ et donne 785. Le cuisinier est sûr d'obtenir au moins 785 pièces d'or.

Exercice 10

(675)

Posons $d = \text{pgcd}\,(a, a + b)$. On a $d\langle 8739\rangle a$ et $d\langle 8739\rangle\,(a + b)$ alors $d\langle 8739\rangle b = (a + b) - a$ donc $d\langle 8739\rangle \text{pgcd}\,(a, b) = 1$ puis $d = 1$. De même $\text{pgcd}\,(b, a + b) = 1$. Ainsi

$$a \wedge (a + b) = b \wedge (a + b) = 1$$

et par suite $ab \wedge (a+b) = 1$.

Exercice 11
(676)
(a)

$$\text{pgcd}\,(a, a+b) = \text{pgcd}\,(a, b)$$

et

$$\text{pgcd}\,(b, a+b) = \text{pgcd}\,(a, b) = 1.$$

Ainsi $(a+b) \wedge a = 1$ et $(a+b) \wedge b = 1$ donc $(a+b) \wedge ab = 1$. (b) Posons $\delta = \text{pgcd}\,(a, b)$. On peut écrire $a = \delta a^{'}$ et $b = \delta b^{'}$ avec $a^{'} \wedge b^{'} = 1$.

$$\text{pgcd}\,(a+b, \text{ppcm}\,(a, b)) = \delta \text{pgcd}\,(a^{'} + b^{'}, \text{ppcm}\,(a^{'}, b^{'})) = \delta$$

Exercice 12
(677)
(a) $n^2 + n = n(n+1)$. $1 \times (2n+1) - 2 \times n = 1$ donc $(2n+1) \wedge n = 1$.

$$2 \times (n+1) - 1 \times (2n+1) = 1$$

donc $(2n+1) \wedge (n+1) = 1$
Par produit

$$(2n+1) \wedge (n^2 + n) = 1.$$

(b) $3n^2 + 2n = n(3n+2)$. $1 \times (n+1) - 1 \times n = 1$ donc $n \wedge (n+1) = 1$.

$$3 \times (n+1) - 1 \times (3n+2) = 1$$

donc $(3n+2) \wedge (n+1) = 1$. Par produit

$$(3n^2 + 2n) \wedge (n+1) = 1.$$

Exercice 13
(678)

$$2 \times (n+1) - 1 \times (2n+1) = 1$$

donc $(n+1) \wedge (2n+1) = 1$. On a

$$\binom{2n+1}{n+1} = \frac{2n+1}{n+1} \binom{2n}{n}$$

donc

$$(n+1) \binom{2n+1}{n+1} = (2n+1) \binom{2n}{n}$$

Puisque

$$\binom{2n+1}{n+1} \in \mathbb{Z},$$

on a

$$(n+1)\,\langle 8739\rangle\,(2n+1)\binom{2n}{n}$$

or $(n+1) \wedge (2n+1) = 1$ donc

$$(n+1)\,\langle 8739\rangle \binom{2n}{n}$$

Exercice 14
(679)

Posons $d = \operatorname{pgcd}(a, bc)$ et $\delta = \operatorname{pgcd}(a, c)$. On $\delta\langle 8739\rangle a$ et $\delta\langle 8739\rangle c$ donc $\delta\langle 8739\rangle bc$ puis $\delta\langle 8739\rangle d$. Inversement $d\langle 8739\rangle a$ et $d\langle 8739\rangle bc$. Or $d \wedge b = 1$ car $d\langle 8739\rangle a$ et $a \wedge b = 1$. Donc $d\langle 8739\rangle c$ puis $d\langle 8739\rangle \delta$. Par double divisibilité $d = \delta$.

Exercice 15
(680)

(a) Théorème de Bézout. (b) Soit $(u, v) \in \mathbb{Z}^2$ un couple solution. On a $au + bv = 1 = au_0 + bv_0$ donc

$$a\,(u - u_0) = b\,(v_0 - v)$$

On a $a\langle 8739\rangle b\,(v_0 - v)$ or $a \wedge b = 1$ donc $a\langle 8739\rangle v_0 - v$. Ainsi $\exists k \in \mathbb{Z}$ tel que $v = v_0 - ka$ et alors

$$a\,(u - u_0) = b\,(v_0 - v)$$

donne $a\,(u - u_0) = abk$ puis $u = u_0 + kb$ (sachant $a \neq 0$). (c) Inversement les couples de la forme ci-dessus sont solutions.

Exercice 16
(681)

(a) Unicité : Si (a_n, b_n) et (α_n, β_n) sont solutions alors $a_n + b_n\sqrt{2} = \alpha_n + \beta_n\sqrt{2}$ donc

$$(b_n - \beta_n)\sqrt{2} = (\alpha_n - a_n)$$

Si $b_n \neq \beta_n$ alors

$$\sqrt{2} = \frac{\alpha_n - a}{b_n - \beta_n} \in \mathbb{Q}$$

ce qui est absurde. On en déduit $b_n = \beta_n$ puis $a_n = \alpha_n$

Existence : Par la formule du binôme

$$(1 + \sqrt{2})^n = \sum_{k=0}^{n} \binom{n}{k} \sqrt{2}^k$$

En séparant les termes d'indices pairs de ceux d'indices impairs, on a

$$(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$$

avec

$$a_n = \sum_{p=0}^{E(n/2)} \binom{n}{2p} 2^p \text{ et } b_n = \sum_{p=0}^{E((n-1)/2)} \binom{n}{2p+1} 2^p$$

(b) On a

$$a_n^2 - 2b_n^2 = (a_n + b_n\sqrt{2})\left(a_n - b_n\sqrt{2}\right)$$

Or en reprenant les calculs qui précèdent

$$(1-\sqrt{2})^n = a_n - b_n\sqrt{2}$$

donc

$$a_n^2 - 2b_n^2 = (1+\sqrt{2})^n (1-\sqrt{2})^n = (-1)^n$$

(c) La relation qui précède permet d'écrire $a_n u + b_n v = 1$ avec $u, v \in \mathbb{Z}$ On en déduit que a_n et b_n sont premiers entre eux.

Exercice 17
(684)

Si le couple (x_0, y_0) est entier la conclusion est entendue. Sinon, on peut écrire

$$x_0 = p_0/d_0 \text{ et } y_0 = q_0/d_0 \text{ avec } p_0, q_0 \in \mathbb{Z} \text{ et } d_0 \in \mathbb{N} \setminus \{0, 1\}$$

Considérons alors un couple entier $(x_0^{'}, y_0^{'})$ obtenu par arrondi de (x_0, y_0). On a

$$D^2 = (x_0 - x_0^{'})^2 + (y_0 - y_0^{'})^2 \leq 1/4 + 1/4$$

La droite joignant nos deux couples peut être paramétrée par

$$\begin{cases} x &= x_0^{'} + \lambda(x_0 - x_0^{'}) \\ y &= y_0^{'} + \lambda(y_0 - y_0^{'}) \end{cases} \text{ avec } \lambda \in \mathbb{R}$$

Cette droite coupe le cercle en (x_0, y_0) pour $\lambda = 1$ et recoupe encore celui-ci en (x_1, y_1) obtenu pour

$$\lambda = \frac{(x_0^{'})^2 + (y_0^{'})^2 - N^2}{D^2}$$

Puisque

$$D^2 = N^2 - 2(x_0 x_0^{'} + y_0 y_0^{'}) + (x_0^{'})^2 + (y_0^{'})^2 = \frac{d_1}{d_0}$$

avec $d_1 \in \mathbb{N}^*$ et $d_1 < d_0$ car $D^2 < 1$. Le nombre λ est donc de la forme $d_0 k/d_1$ avec k entier et les coordonnées (x_1, y_1) sont alors de la forme

$$x_1 = p_1/d_1 \text{ et } y_1 = q_1/d_1 \text{ avec } p_1, q_1 \in \mathbb{Z} \text{ et } d_1 \in \mathbb{N}^*, d_1 < d_0$$

Si $d_1 = 1$, le processus s'arrête, sinon il suffit de répéter l'opération jusqu'à obtention d'un couple entier.

Exercice 18
(686)

($\langle 10232 \rangle$) ok ($\langle 10233 \rangle$) Si $\sqrt{n} \in \mathbb{Q}$ alors on peut écrire $\sqrt{n} = \dfrac{p}{q}$ avec $p \wedge q = 1$. On a alors $q^2 n = p^2$ donc $n \langle 8739 \rangle p^2$

De plus $q^2 n = p^2$ et $p^2 \wedge q^2 = 1$ donne $p^2 \langle 8739 \rangle n$. Par double divisibilité $n = p^2$. ni 2, ni 3 ne sont des carrés d'un entier, donc $\sqrt{2} \notin \mathbb{Q}$ et $\sqrt{3} \notin \mathbb{Q}$.

Exercice 19
(693)
Supposons $a^2 \langle 8739 \rangle b^2$. Posons $d = \operatorname{pgcd}(a, b)$. On a

$$d^2 = \operatorname{pgcd}(a, b)^2 = \operatorname{pgcd}(a^2, b^2) = a^2$$

donc $d = |a|$ puis $a \langle 8739 \rangle b$.

Exercice 20
(696)
Le nombre de côté du polygone construit est le plus petit entier $k \in \mathbb{N}^*$ tel que $n \langle 8739 \rangle kp$. Posons $\delta = \operatorname{pgcd}(n, p)$. On peut écrire $n = \delta n'$ et $p = \delta p'$ avec $n' \wedge p' = 1$. $n \langle 8739 \rangle kp \Leftrightarrow n' \langle 8739 \rangle kp'$ i.e. $n' \langle 8739 \rangle k$. Ainsi $k = n' = n/\delta$.

Exercice 21
(697)
On peut écrire
$n = 2^k (2p + 1)$ On a alors

$$a^n + 1 = b^{2p+1} - (-1)^{2p+1} = (b - (-1)) \sum_{k=0}^{2p} b^k (-1)^{2p-k} = (b + 1) c$$

avec $b = a^{2^k}$. On en déduit que $b + 1 \langle 8739 \rangle a^n + 1$, or $a^n + 1$ est supposé premier et $b + 1 > 1$ donc $b + 1 = a^n + 1$ puis $n = 2^k$.

Exercice 22
(699)
(a)

$$4n^3 + 6n^2 + 4n + 1 = (n + 1)^4 - n^4 = ((n + 1)^2 - n^2)((n + 1)^2 + n^2) = (2n + 1)(2n^2 + 2n + 1).$$

Cet entier est composé pour $n \in \mathbb{N}^*$ car $2n + 1 \geq 2$ et $2n^2 + 2n + 1 \geq 2$. (b)

$$n^4 - n^2 + 16 = (n^2 + 4)^2 - 9n^2 = (n^2 - 3n + 4)(n^2 + 3n + 4).$$

De plus les équations

$$n^2 - 3n + 4 = 0, 1 \text{ ou } -1 \text{ et } n^2 + 3\text{n} + 4 = 0, 1 \text{ ou } -1$$

n'ont pas de solutions car toutes de discriminant négatif. Par conséquent $n^4 - n^2 + 16$ est composée.

Exercice 23
(702)

Considérons les $x_k = 1001! + k$ avec $2 \leq k \leq 1001$. Ce sont 1 000 entiers consécutifs. Pour tout $2 \leq k \leq 1001$, on a $k\langle 8739\rangle\,(1001)\,!$ donc $k\langle 8739\rangle x_k$ avec $2 \leq k < x_k$ donc $x_k \notin \mathcal{P}$.

Exercice 24
(705)

(a) Quitte à échanger, supposons $n < m$. On remarque que

$$(F_n - 1)^{2^{m-n}} = F_m - 1$$

En développant cette relation par la formule du binôme, on parvient à une relation de la forme $F_m + vF_n = 2$ avec $v \in \mathbb{Z}$ car les coefficients binomiaux sont des entiers. On en déduit que $\operatorname{pgcd}(F_n, F_m) = 1$ ou 2 . Puisque F_n et F_m ne sont pas tous deux pairs, ils sont premiers entre eux. (b) Les F_n sont en nombre infini et possèdent des facteurs premiers distincts, il existe donc une infinité de nombres premiers.

Exercice 25
(711)

Par hypothèse, on peut écrire $n = p_1 p_2 \ldots p_r$ avec $p_1, \ldots, p_r$ nombres premiers deux à deux distincts. Soit $a \in \mathbb{Z}$. Considérons $i \in \{1,\ldots, r\}$. Si p_i ne divise pas a, le petit théorème de Fermat assure

$$a^{p_i - 1} \equiv 1\ [p_i].$$

Puisque $p_i - 1$ divise $n - 1$, on a encore

$$a^{n-1} \equiv 1\ [p_i]$$

et donc

$$a^n \equiv a\ [p_i]$$

Si p_i divise a alors p_i divise aussi a^n et donc

$$a^n \equiv 0 \equiv a\ [p_i].$$

Enfin, chaque p_i divisant $a^n - a$ et les p_i étant deux à deux premiers entre eux, $n = p_1 \ldots p_r$ divise $a^n - a$ et finalement

$$a^n \equiv a\ [n].$$

La réciproque de ce résultat est vraie. Ce résultat montre que le petit théorème de Fermat ne caractérise pas les nombres premiers. Les nombres non premiers satisfaisant le petit théorème de Fermat, sont les nombres de Carmichael. Le plus petit d'entre eux est 561, le suivant 1105.

Exercice 26
(715)

(a) $x = 1$ n'est pas solution. Pour $x \neq 1$:

$$x - 1\langle 8739\rangle x + 3 \Leftrightarrow \frac{x+3}{x-1} = 1 + \frac{4}{x-1} \in \mathbb{Z} \Leftrightarrow x - 1 \in \mathcal{D}(4) = \{1, 2, 4, -1, -2, -4\}$$

Ainsi $\mathcal{S} = \{2, 3, 5, 0, -1, -3\}$. (b) $x = -2$ n'est pas solution. Pour $x \neq -2$:

$$x + 2\langle 8739\rangle x^2 + 2 \Leftrightarrow \frac{x^2+2}{x+2} = x - 2 + \frac{6}{x+2} \in \mathbb{Z} \Leftrightarrow x + 2 \in \mathcal{D}(6) = \{1, 2, 3, 6, -1, -2, -3, -6\}.$$

Ainsi

$$\mathcal{S} = \{-1, 0, 1, 4, -3, -4, -5, -8\}.$$