Chapter 15 Arithmétique des entiers

15.1 Divisibilité

Solution 15.1

On peut effectuer une récurrence sur $n \in \mathbb{N}$. En effet, 7 divise $0 = 3^0 - 6^0$.

Soit $n \in \mathbb{N}$. Supposons que 7 divise $3^{6n} - 6^{2n}$, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que

$$3^{6n} - 6^{2n} = 7k.$$

Ainsi $3^{6n} = 6^{2n} + 7k$, d'où

$$3^{6n+6} - 6^{2n+2} = 3^6(6^{2n} + 7k) - 6^{2n+2} = 6^{2n}(3^6 - 6^2) + 7k \times 3^6 = 7\left(99 \times 6^{2n} + 3^6 k\right).$$

Ainsi, 7 divise $3^{6n+6} - 6^{2n+2}$.

On en déduit le résultat par récurrence.

Variante. En utilisant les opération modulo 7:

$$3^3 = 27 \equiv -1 \pmod 7 \text{ donc } 3^6 \equiv (-1)^2 \equiv 1 \pmod 7$$

de même

$$6^2 = 36 \equiv 1 \pmod 7.$$

Ainsi, pour $n \in \mathbb{N}$,

$$3^{6n} - 6^{2n} \equiv 1^n - 1^n \equiv 0 \pmod 7,$$

c'est-à-dire que 7 divise $3^{6n} - 6^{2n}$.

Solution 15.2 *Une majoration de σ (ENS MP)*

Soit $\mathcal{D}$ l'ensemble des diviseurs de n. Si $d \in \mathcal{D}$, il existe $k \in [\![1, n]\!]$ tel que $d = \frac{n}{k}$. On a donc $\mathcal{D} \subset \left\{ \frac{n}{k} \;\middle|\; k \in [\![1, n]\!] \right\}$, d'où l'on déduit l'inégalité

$$\sigma(n) \leq n \sum_{k=1}^{n} \frac{1}{k}.$$

Le résultat demandé se déduit de $\sum_{k=1}^{n} \frac{1}{k} \leq 1 + \ln n$, ce qui se démontre en remarquant que $\frac{1}{k} \leq \int_{k-1}^{k} \frac{1}{t}\,\mathrm{d}t$ pour $k \in [\![2, n]\!]$.

Solution 15.3

1. Vrai. Si a divise b et c, alors a divise $2b$ et $c \times c$ et donc divise $c^2 - 2b$.
2. Faux. On peut montrer que a divise $2b$ et $2c$, ce qui suggère un contre exemple avec $a = 2$. On a bien $a = 2$ qui divise $8 = 5 + 3$ et divise $2 = 5 - 3$ et pourtant 2 ne divise pas 5 (ni 3 d'ailleurs).
3. Faux. $4 = 2 \times 3$ et $35 = 5 \times 7$ et $4 + 35 = 39$ n'est pas multiple de $3 + 7 = 10$.
4. Vrai. On montre facilement la contraposée. Si b et c sont pairs, alors $2 \mid b$ et $2 \mid c$, donc $4 = 2 \times 2 \mid bc$.
5. Faux. $a = 2$ divise $b = 6$ et 6 ne divise pas $c = 10$ et on a bien $2 \mid 10$.

Solution 15.4

1. Puisque $n \,\Big|\, n$, alors

$$n|n+8 \iff n|n+8-n \iff n|8 \iff n \in \{\,1,2,4,8\,\}\,.$$

2. Puisque $n-1|n-1$, alors

$$\begin{aligned} n-1|n+11 &\iff n-1|(n+11)-(n-1) \iff n-1|12 \\ &\iff n-1 \in \{\,\pm1,\pm2,\pm3,\pm4,\pm6,\pm12\,\} \iff n \in \{\,0,2,3,4,5,7,13\,\} \text{ car } n \geq 0. \end{aligned}$$

3. On a $n-3|n^2(n-3)$, c'est-à-dire $n-3|n^3-3n^2$, d'où

$$n-3|n^3-3 \iff n-3|(n^3-3)-(n^3-3n^2) \iff n-3|3n^2-3.$$

De plus, $n-3|3n(n-3)$, c'est-à-dire $n-3|3n^2-9n$, d'où

$$\begin{aligned} n-3|n^3-3 &\iff n-3|3n^2-3-3n^2+9n \iff n-3|9n-3 \\ &\iff n-3|9n-3-9(n-3) \iff n-3|24 \\ &\iff n-3 \in \{\,\pm1,\pm2,\pm3,\pm4,\pm6,\pm8,\pm12,\pm24\,\} \iff n \in \{\,0,1,2,4,5,6,9,11,15,27\,\}\,. \end{aligned}$$

Variante. On peut aussi remarquer que $n^3-3=(n-3)(n^2+3n+9)+24$ (division euclidienne de polynômes) et on retrouve

$$n-3|n^3-3 \iff n-3|24.$$

Solution 15.5
Solution 15.6

15.2 Division euclidienne

15.3 Les nombres premiers

Solution 15.7
Soit $n \in \mathbb{N}$. Soit $k \in [\![2,n]\!]$,

$$k \,\Big|\, n!+k \text{ et } 2 \leq k < n!+k.$$

L'entier $n!+k$ n'est donc pas premier.
Solution 15.8 *Infinité des nombres premiers congrus à* 3 *modulo* 4*, (X MP)*

15.4 Plus grand commun diviseur, algorithme d'Euclide

Solution 15.9
Solution 15.10
Solution 15.11
Solution 15.12
L'idée est de trier les entiers $k \in [1,n]$ selon la valeur de $t = k \wedge n$.

Soit E l'ensemble des couples d'entiers (d,h) tels que $d > 0$ soit un diviseur de n et $h \in [\![1,d]\!]$ soit premier avec d.

On a donc

$$\operatorname{card}(E) = \sum_{d|n} \varphi(d). \tag{1}$$

Soit $f : E \to [\![1, n]\!]$ l'application associant à tout couple $(d, h) \in E$ le produit th, où t est le seul entier tel que $n = td$. Il suffit de montrer que f est bijective.

Soit $k \in [\![1, n]\!]$. Un couple $(d, h) \in E$ avec $n = td$ comme ci-dessus, est un antécédent de k par f si et seulement si $k = th$. Si c'est le cas, $n \wedge k = td \wedge th = t$, d'où l'unicité de t, donc de d et h.

Inversement, posons $t = k \wedge n$. On peut écrire $k = th$, $n = td$, où $h, d \in \mathbb{N}^\star$ et $h \wedge d = 1$. Mais $th = k \leq n = td$, donc $h \in [\![1, d]\!]$; alors $(d, h) \in E$ est un antécédent de k par f. Ainsi k a un unique antécédent par f, donc f est bijective.

Solution 15.13

1. Vrai. 19 est un nombre premier : c'est le lemme d'Euclide.
2. Faux. $91 = 7 \times 13$ n'est pas premier. Avec $a = 7$ et $b = 13$, on a bien $91 | ab$ mais 91 ne divise ne a, ni b.
3. Vrai. 5 est premier et $5 | b \times b$, donc (lemme d'Euclide) $5 | b$, d'où $25 | b^2$.
4. Faux. Avec $b = 6$, on a bien $12 | b^2$ mais 4 ne divise pas $b^2 = 36$.
5. On écrit la décompostion en facteur premiers de b:
$$b = 2^u 3^v p_1^{\alpha_1} \dots p_r^{\alpha_r}$$
où $2, 3, p_1, \dots, p_r$ sont des nombre premiers distincts, $u \in \mathbb{N}$, $v \in \mathbb{N}$ (donc éventuellement nuls), $\alpha_i \in \mathbb{N}^\star$. On a donc
$$b^2 = 2^{2u} 3^{2v} p_1^{2\alpha_1} \dots p_r^{2\alpha_r}$$
Si $12 | b^2$ alors $2 | b^2$ et $3 | b^2$, donc $2u \geq 1$ et $2v \geq 1$, et puisque $v \in \mathbb{N}$, $2v \geq 2$, donc $12 = 2^1 \times 3^2 | b^2$.

Solution 15.14

Solution 15.15 *Multiples formésde* 1

Solution 15.16

On a successivement

$$\begin{aligned} 424 &= 6 \times 68 + 16 & &\text{donc } 424 \mod 68 = 16 \\ 68 &= 4 \times 16 + 4 & &\text{donc } 68 \mod 16 = 4 \\ 16 &= 4 \times 4 + 0 & &\text{donc } 16 \mod 4 = 0. \end{aligned}$$

Ainsi $\mathrm{pgcd}(424, 68) = 4$.

Solution 15.17

$\mathrm{pgcd}(18480, 9828) = 84$.

Solution 15.18 *Une équation avec un PGCD et un PPCM*

Solution 15.19

$$\mathrm{pgcd}(A, B) = \mathrm{pgcd}(A - B, B) = \mathrm{pgcd}(2n + 2, 9n^2 + 8n - 1).$$

En remarquant que $9n^2 + 8n - 1 = (n + 1)(9n - 1)$, on a donc

$$\mathrm{pgcd}(A, B) = \mathrm{pgcd}(2(n + 1), (n + 1)(9n - 1)) = (n + 1)\,\mathrm{pgcd}\,(2, 9n - 1) = (n + 1)\,\mathrm{pgcd}\,(2, n - 1)$$

puisque $9n - 1 = 2(4n) + n - 1$. Finalement

$$\mathrm{pgcd}(A, B) = \begin{cases} 2(n + 1) & : n \text{ impair} \\ (n + 1) & : n \text{ pair} \end{cases}$$

Solution 15.20

1. On a succéssivement

$$\begin{aligned}
u_0 &= 0\\
u_1 &= 1\\
u_2 &= 3u_1 - 2u_0 = 3\\
u_3 &= 3u_2 - 2u_1 = 9 - 2 = 7\\
u_4 &= 3u_3 - 2u_2 = 21 - 6 = 15\\
u_5 &= 3u_4 - 2u_3 = 45 - 14 = 31\\
u_6 &= 3u_5 - 2u_4 = 93 - 30 = 63.
\end{aligned}$$

2. Pour $n \in \mathbb{N}$, on pose $R(n)$ l'assertion $u_{n+1} = 2u_n + 1$.

On a $u_1 = 1$ et $2u_0 + 1 = 1$, d'où $R(0)$.

Soit $n \in \mathbb{N}$ tel que $R(n)$. On a alors

$$\begin{aligned}
u_{n+2} &= 3u_{n+1} - 2u_n \\
&= 3u_{n+1} - (u_{n+1} - 1) && \text{d'après } R(n)\\
&= 2u_{n+1} + 1 && \text{d'où } R(n+1).
\end{aligned}$$

Conclusion

Par récurrence, on obtient pour tout $n \in \mathbb{N}$, $u_{n+1} = 2u_n + 1$.

De plus la relation $u_{n+1} - 2u_n = 1$ et le théorème de Bézout montre que u_{n+1} et u_n sont premiers entre eux.

3. Pour $n \in \mathbb{N}$, on a $u_{n+1} + 1 = 2(u_n + 1)$, ainsi, la suite $\left(u_n + 1\right)$ est géométrique de raison 2 et pour $n \in \mathbb{N}$,

$$u_n + 1 = 2^n \left(u_0 + 1\right) = 2^n,$$

d'où $u_n = 2^n - 1$. Comme vu à la question précédente $2^{n+1} - 1$ et $2^n - 1$ sont premiers entre eux.

4. Pour $n, p \in \mathbb{N}$,

$$u_n \left(u_p + 1\right) + u_p = (2^n - 1) \times 2^p + (2^p - 1) = 2^{n+p} - 2^p + 2^p - 1 = 2^{n+p} - 1 = u_{n+p}.$$

On en déduit alors

$$\operatorname{pgcd}\left(u_n, u_{n+p}\right) = \operatorname{pgcd}\left(u_n, u_{n+p} - (u_p + 1)u_n\right) = \operatorname{pgcd}\left(u_n, u_p\right).$$

5. Notons q et r la quotient le reste de la division euclidienne de a par b : $a = bq + r$. En écrivant $a = bq + r = b + (b(q-1) + r)$, on a d'après la question précédente

$$\begin{aligned}
\operatorname{pgcd}\left(u_a, u_b\right) = \operatorname{pgcd}\left(u_b, u_a\right) &= \operatorname{pgcd}\left(u_b, u_{bq+r}\right)\\
&= \operatorname{pgcd}\left(u_b, u_{b+(b(q-1)+r)}\right) = \operatorname{pgcd}\left(u_b, u_{b(q-1)+r}\right)
\end{aligned}$$

En itérant le procédé (ou avec une récurrence), on obtient

$$\begin{aligned}
\operatorname{pgcd}\left(u_b, u_{bq+r}\right) = \operatorname{pgcd}\left(u_b, u_{b(q-1)+r}\right) &= \operatorname{pgcd}\left(u_b, u_{b(q-2)+r}\right) = \dots\\
&= \operatorname{pgcd}\left(u_b, u_{q+r}\right) = \operatorname{pgcd}\left(u_b, u_r\right).
\end{aligned}$$

Notons $a_0 = a$, $a_1 = b$ et définissons par récurrence l'entier a_{j+2} par

$$a_{j+2} = a_j \mod a_{j+1}$$

tant que $a_{j+1} \neq 0$. On note $k \in \mathbb{N}$ le premier indice j tel que $a_{j+2} = 0$. Alors, l'algorithme d'Euclide donne $\mathrm{pgcd}(a, b) = a_{k+1}$.

Nous avons déjà montré que

$$\mathrm{pgcd}\left(u_{a_j}, u_{a_{j+1}}\right) = \mathrm{pgcd}\left(u_{a_{j+1}}, u_{a_{j+2}}\right).$$

et en itérant le procédé, on obtient finalement

$$\begin{aligned}\mathrm{pgcd}\left(u_{a_0}, u_{a_1}\right) &= \mathrm{pgcd}\left(u_{a_1}, u_{a_2}\right) = \dots \\ &= \mathrm{pgcd}\left(u_{a_{k-1}}, u_{a_k}\right) = \mathrm{pgcd}\left(u_{a_k}, u_{a_{k+1}}\right) = \mathrm{pgcd}\left(u_{a_{k+1}}, 0\right) = u_{a_{k+1}}\end{aligned}$$

c'est-à-dire

$$\mathrm{pgcd}(u_a, u_b) = u_{\mathrm{pgcd}(a,b)}.$$

6. Puisque $\mathrm{pgcd}(1982, 312) = 2$, on a $\mathrm{pgcd}(u_{1982}, u_{312}) = u_2 = 3$.

Solution 15.21

1. On a

$$26 = 1 \times 15 + 11 \qquad 15 = 1 \times 11 + 4 \qquad 11 = 2 \times 4 + 3 \qquad 4 = 1 \times 3 + 1 \qquad 3 = 3 \times 1 + 0.$$

Donc $\mathrm{pgcd}(26, 15) = 1$.

2. On remonte les calculs précédents:

$$\begin{aligned} 1 &= 4 - 1 \times 3 & &= 3 \times 4 - 1 \times 11 \because 3 & &= 11 - 2 \times 4 \\ &= 3 \times 15 - 4 \times 11 & &\because 4 = 15 - 1 \times 11 \\ &= 7 \times 15 - 4 \times 26 & &\because 11 = 26 - 1 \times 15 \end{aligned}$$

D'où la solution particulière $(x_0, y_0) = (-4, 7)$.

On a donc

$$26x + 15y = 1 \iff 26x + 15y = 26 \times (-4) + 15 \times 7 \iff 26(x + 4) = -15(y - 7)$$

Or $15 = 3 \times 5$ est premier avec 26, donc 3 et 5 n'apparaissent pas dans la décomposition en facteurs premiers de 26. On en déduit que 15 divise $x + 4$ dons l'équation précédente. Plus précisement, en posant $x + 4 = 15m$ ($m \in \mathbb{Z}$), nous avons $y - 7 = -26m$.

Nous pouvons alors vérifier que l'ensemble des solutions de (E) est l'ensemble des couples

$$(15m - 4, -26m + 7) \quad \text{lorsque } m \text{ décrit } \mathbb{Z}.$$

3. Une solution particulière de $26x + 15y = 4$ est $(x_0, y_0) = (-16, 28)$. Un raisonnement analogue au précédent donne tous les couples de solutions $(15m - 16, -26m + 28)$, où $m \in \mathbb{Z}$.

Solution 15.22

Solution 15.23 *Développement de* $(1 + \sqrt{2})^n$

Solution 15.24 *Suite de Farey*

Montrer qu'il existe un unique couple $(u, v) \in \mathbb{Z}^2$ tel que $ub - av = 1$ et $n - b < v \leq n$. Posant $t = \frac{u}{v}$, montrer ensuite que t appartient à $\mathcal{F}_n$ et $t \geq y$. Montrer enfin que $t = y$, en raisonnant par l'absurde ; on évaluera les différences $y - x$, $t - y$, $t - x$.

15.5 Décomposition en facteurs premiers

Solution 15.25
On écrit la décompostion en facteurs premiers de 15!:

$$\begin{aligned}15! &= 2\times 3\times 4\times 5\times 6\times 7\times 8\times 9\times 10\times 11\times 12\times 13\times 14\times 15\\ &= 2\times 3\times 2^2\times 5\times 2\times 3\times 7\times 2^3\times 3^2\times 2\times 5\times 11\times 2^2\times 3\times 13\times 2\times 7\times 3\times 5\\ &= 2^{11}3^6 5^3 7^2 11^1 13^1.\end{aligned}$$

Les diviseurs positifs de 15! sont donc les entiers de la forme

$$2^a 3^b 5^c 7^d 11^e 13^f \quad \text{avec} \quad \begin{cases} 0\le a\le 11\\ 0\le b\le 6\\ 0\le c\le 3\\ 0\le d\le 2\\ 0\le e\le 1\\ 0\le f\le 1\end{cases}$$

Il y en a donc $12\cdot 7\cdot 4\cdot 3\cdot 2\cdot 2 = 4032$.

Solution 15.26
Pour $(x,y)\in\mathbb{Z}^2$,

$$xy+6x-3y=40 \iff (x-3)(y+6)+18=40 \iff (x-3)(y+6)=22.$$

Or l'ensemble des diviseurs (dans $\mathbb{Z}$) de 22 sont $\{\pm1,\pm2,\pm11,\pm22\}$. On distingue ainsi huit cas:

$$\begin{gathered}
x-3=1 \text{ et } y+6=22 \iff x=4 \text{ et } y=16\\
x-3=2 \text{ et } y+6=11 \iff x=5 \text{ et } y=5\\
x-3=11 \text{ et } y+6=2 \iff x=14 \text{ et } y=-4\\
x-3=22 \text{ et } y+6=1 \iff x=25 \text{ et } y=-5\\
x-3=-1 \text{ et } y+6=-22 \iff x=2 \text{ et } y=-28\\
x-3=-2 \text{ et } y+6=-11 \iff x=1 \text{ et } y=-17\\
x-3=-11 \text{ et } y+6=-2 \iff x=-8 \text{ et } y=-8\\
x-3=-22 \text{ et } y+6=-1 \iff x=-19 \text{ et } y=-7
\end{gathered}$$

L'ensemble des solutions de l'équation $xy+6x-3y=40$ est

$$\{(4,16),(5,5),(14,-4),(25,-5),(2,-28),(1,-17),(-8,-8),(-19,-7)\}.$$

On note $d(n)$ le nombre de diviseurs positifs de n et $\sigma(n)$ la somme de ceux-ci. Montrer

$$d(n)=\prod_{k=1}^{r}\left(\alpha_k+1\right) \quad \text{et} \quad \sigma(n)=\prod_{k=1}^{r}\frac{p_k^{\alpha_k+1}-1}{p_k-1}.$$

Solution 15.27
Solution 15.28
N impair.
Solution 15.29 *Un théorème de Kurshchak*

L'ensemble $\left\{ v_2(a) \mid a \in [\![n, m]\!] \right\}$ est une partie finie non vide de $\mathbb{N}$, d'où l'existence du maximum, noté v dans la suite. On démontre par l'absurde que ce maximum n'est réalisé qu'une seule fois. Si ce n'est pas le cas, on choisit $x < y$ dans $[\![n, m]\!]$ tel que $v_2(n) = v_2(y) = v$. Il existe x', y' impairs tels que $x = 2^v x'$ et $y = 2^v y'$. Entre deux entier impairs x' et y', se trouve un entier pair $z = 2z'$ avec $z' \in \mathbb{N}$. Alors $x = 2^v x' < 2^v z < 2^v y' = y$ donc $2^v z$ appartient à $[\![n, m]\!]$ et est de valuation 2-adique supérieure ou égale à $v + 1$, ce qui est absurde.

Soit D le ppcm de $n, n + 1, \dots, m$. Puisque dans l'intervalle $[\![n, m]\!]$, il y a au moins un entier pair, D est pair. On note k_0 l'entier de $[\![n, m]\!]$ de valuation 2-adique maximale. Alors $v_2(D) = v_2(k_0)$. De plus, pour tout $k \in [\![n, m]\!]$, D est un multiple de k. Par unicité de k_0, $\frac{D}{k}$ est un entier pair, sauf pour $k = k_0$.

Supposons maintenant que $N = \sum_{k=n}^{m} \frac{1}{k}$ est un entier. Alors

$$DN = \sum k = n^m \frac{D}{k} = \sum_{\substack{k=n \\ k \neq k_0}}^{m} \frac{D}{k} + \frac{D}{k_0}$$

est un entier impair. Ce qui est absurde car D est pair.

15.6 La relation de congruence

Solution 15.30

On a successivement,

$$3 \equiv 3 \pmod{11} \quad 3^2 \equiv 9 \pmod{11} \quad 3^3 \equiv 5 \pmod{11} \quad 3^4 \equiv 4 \pmod{11} \quad 3^5 \equiv 1 \pmod{11}.$$

De plus, $2015 = 403 \times 5$, d'où

$$3^{2015} = \left(3^5\right)^{403} \equiv 1^{403} \equiv 1 \pmod{11}.$$

Solution 15.31

On a $2000 = 285 \times 7 + 5$, d'où

$$\begin{aligned}
2000 &\equiv 5 \pmod{7} \\
2000^2 &\equiv 5^2 \equiv 25 \equiv 4 \pmod{7} \\
2000^3 &\equiv 5 \times 4 \equiv 20 \equiv 6 \pmod{7} \\
2000^4 &\equiv 5 \times 6 \equiv 30 \equiv 2 \pmod{7} \\
2000^5 &\equiv 5 \times 2 \equiv 10 \equiv 3 \pmod{7} \\
2000^6 &\equiv 5 \times 3 \equiv 15 \equiv 1 \pmod{7}
\end{aligned}$$

De plus, $2000 = 333 \times 6 + 2$, d'où

$$2000^{2000} = 2000^{333 \times 6 + 2} = \left(2000^6\right)^{333} \times 2000^2 \equiv 1^{333} 4 \pmod{7} \equiv 4 \pmod{7}.$$

De manière analogue, on trouve $2^2 \equiv 1 \pmod{3}$, d'où

$$2^{500} = \left(2^2\right)^{250} \equiv 1^{250} \equiv 1 \pmod{3}.$$

Solution 15.32 *Reste de la division euclidiene du carré d'un entier par* 8

Solution 15.33

Résumons sous forme de tableau

$x \mod 17$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$x^2 \mod 17$	0	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1
$x^2-2x+2 \mod 17$	2	1	2	5	10	0	9	3	16	14	14	16	3	9	0	10	5

Ainsi x^2-2x+2 est divisible par 17 si, et seulement si

$$x \equiv 5 \pmod{17} \text{ ou } x \equiv 14 \pmod{17}.$$

Solution 15.34
$(0,0,0)$
Solution 15.35
Solution 15.36
Solution 15.37
Solution 15.38 *Le petit théorème de Fermat*

1. Pour $k \in [\![1, p-1]\!]$, on a

$$\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1} \quad \text{d'où} \quad k\binom{p}{k} = p\binom{p-1}{k-1}.$$

Or $1 \leq k \leq p$, donc p ne divise pas k et puisque p est un nombre premier, le lemme d'Euclide assure que p divise $\binom{p}{k}$.

2. Pour $a, b \in \mathbb{N}$,

$$(a+b)^p = \sum_{k=0}^{p}\binom{p}{k}a^{p-k}b^k = a^p + \sum_{k=1}^{p-1}\binom{p}{k}a^{p-k}b^k + b^p.$$

Or pour $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$, donc p divise $\sum_{k=1}^{p-1}\binom{p}{k}a^{p-k}b^k$. Ainsi

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

3. On effectue une récurrence sur $a \in \mathbb{N}$. On a $0^p = 0 \equiv 0 \pmod{p}$.
Soit $a \in \mathbb{N}$ tel que $a^p \equiv a \pmod{p}$. D'après la question précédente (avec $b = 1$), on a

$$(a+1)^p \equiv a^p + 1^p \pmod{p};$$

et puisque $a^p \equiv a \pmod{p}$, on a finalement

$$(a+1)^p \equiv a + 1 \pmod{p}.$$

Conclusion

Par récurrence, on a pour tout $a \in \mathbb{N}$, $a^p \equiv a \pmod{p}$.

4. On a montrer que si p est premier, alors $p \mid a^p - a = a(a^{p-1}-1)$. Si deplus p ne divise pas a, alors il divise $a^{p-1}-1$, c'est-à-dire

$$a^{p-1} \equiv 1 \pmod{p}.$$

Solution 15.39 *Étude de l'irréductibilité d'une fraction*