Feuille 7 : Arithmétique (correction)

Exercice 7.1

Première solution : De quatre nombres consécutifs, deux sont nécessairement pairs et l'un de ces deux nombres pairs est divisible par 4. Leur produit est donc divisible par 8. De même, l'un de trois nombres consécutifs est divisible par 3. Le produit de quatre nombres consécutifs est donc divisible par 8 et par 3 ; comme 8 et 3 sont premiers entre eux, il est divisible par $8 \times 3 = 24$.

Deuxième solution : Soit $n \in \mathbb{N}$. On regarde avec un peu d'attention le nombre (à priori fractionnaire) :

$$\frac{n(n+1)(n+2)(n+3)}{24} = \frac{n(n+1)(n+2)(n+3)}{4!} = \binom{n+3}{4}$$

et on s'aperçoit qu'il est donc entier.

Exercice 7.2

1. On pratique des divisions euclidiennes successives : $210 = 48 \times 4 + 18$; $48 = 18 \times 2 + 12$; $18 = 12 + 6$; $12 = 6 \times 2$. On en conclut que $\text{pgcd}(210, 48) = 6$.

   Pour Bézout, on remonte dans ces identités :

   $$6 = 18 - 12 = 18 - (48 - 18 \times 2) = 18 \times 3 - 48 = (210 - 48 \times 4) \times 3 - 48 = 210 \times 3 - 48 \times 13.$$

2. Même jeu : on calcule $237 = 81 \times 2 + 75$; $81 = 75 + 6$; $75 = 6 \times 12 + 3$; $6 = 3 \times 2$ donc $\text{pgcd}(237, 81) = 3$ puis :

   $$3 = 75 - 6 \times 12 = 75 - (81 - 75) \times 12 = 75 \times 13 - 81 \times 12 = (237 - 81 \times 2) \times 13 - 81 \times 12 = 237 \times 13 - 81 \times 38.$$

Exercice 7.3 On applique l'algorithme d'Euclide :

$$18480 = 9828 \times 1 + 8652\,; \quad 9828 = 8652 \times 1 + 1176\,; \quad 8652 = 1176 \times 7 + 420$$

$$1176 = 420 \times 2 + 336\,; \quad 420 = 336 \times 1 + 84\,; \quad 336 = 4 \times 84$$

Donc $18480 \wedge 9828 = 84$. En remontant les étapes de l'algorithme, on obtient :

$$84 = 420 - 336 = 420 - (1176 - 2 \times 420) = 3 \times 420 - 1176 = 3 \times (8652 - 7 \times 1176) - 1176 = 3 \times 8652 - 22 \times 1176$$

$$= 3 \times 8652 - 22 \times (9828 - 8652) = 25 \times 8652 - 22 \times 9828 = 25 \times (18480 - 9828) - 22 \times 9828 = 25 \times 18480 - 47 \times 9828$$

Donc 84 s'écrit comme combinaison linéaire de 18480 et 9828 comme suit :

$$84 = 25 \times 18480 - 47 \times 9828$$

Exercice 7.4

1) Par énumération, ce sont $(1, 6)$, $(2, 3)$, $(3, 2)$ et $(6, 1)$.

2) Pour (a, b) solution, le produit ab vaut $\text{ppcm}(a, b) \times \text{pgcd}(a, b) = 35 \times 210$ tandis que le couple $(x, y) = (a/35, b/35)$ est également un couple d'entiers, le pgcd de x et y est 1 et le produit xy vaut $ab/(35)^2 = 210/35 = 6$. Réciproquement, on vérifie de même que si (x, y) est un couple d'entiers premiers entre eux dont le produit est 5, le couple $(35x, 35y)$ est solution. Les solutions sont finalement obtenues en multipliant par 35 celles trouvées au 1) : ce sont les couples $(35, 210)$, $(70, 105)$, $(105, 70)$ et $(210, 35)$.

3) En notant $(x, y) = (a/18, b/18)$ et en raisonnant comme au 2 on voit qu'on a à trouver les couples d'entiers (x, y) premiers entre eux dont le produit est $xy = 6480/(18)^2 = 20$ c'est-à-dire $(1, 20)$, $(4, 5)$, $(5, 4)$ et $(20, 1)$ puis les multiplier par 18 pour avoir la liste des solutions, qui sont donc $(18, 360)$, $(72, 90)$, $(90, 72)$ et $(360, 18)$.

4) En divisant par 18 comme au 3, on a cette fois à identifier les couples (x, y) d'entiers premier entre eux dont la somme est $360/1 = 20$. Ce sont $(1, 19)$, $(3, 17)$, $(7, 13)$, $(9, 11)$, $(11, 9)$, $(13, 7)$, $(17, 3)$ et $(19, 1)$. Les solutions s'obtiennent en multipliant par 18 tous ces couples, et ce sont $(18, 342)$, $(54, 306)$, $(126, 234)$, $(162, 198)$, $(198, 162)$, $(234, 126)$, $(306, 54)$ et $(342, 18)$.

Exercice 7.5 Soit a et b deux entiers premiers entre eux et soit p un nombre premier qui divise $a + b$ et ab. Il divise alors $a(a + b) - ab = a^2$ donc figure dans la décomposition en facteurs premiers de a^2 donc figure dans celle de a donc divise a. De même p divise b. Comme on a supposé a et b premiers entre eux, l'entier p ne peut pas exister: 1 est le seul diviseur commun de $a + b$ et ab qui sont donc premiers entre eux.

Exercice 7.6

Soit a et b deux nombres premiers entre eux et (u_n) la suite initialisée par $u_0 = a$, $u_1 = b$ et telle que pour tout $n \in \mathbb{N}, u_{n+2} = u_{n+1} + u_n$. Montrons par récurrence que $\forall n \in \mathbb{N}, u_{n+1} \wedge u_n = 1$.

Initialisation (n=0) : d'après les hypothèses de l'énoncé, $u_0 \wedge u_1 = a \wedge b = 1$.

Hypothèse de récurrence : Soit $n \in \mathbb{N}$, tel que $u_{n+1} \wedge u_n = 1$. Soit $d \in \mathbb{N}^*$ un diviseur commun à u_{n+1} et u_{n+2}. On a : $u_n = u_{n+2} - u_{n+1} \equiv 0\,[d]$. Donc d divise également u_n. Par suite, d divise $u_{n+1} \wedge u_n = 1$ (HR), soit$d = 1$.

On a donc : $\forall n \in \mathbb{N}, u_n \wedge u_{n+1} = 1$.

Exercice 7.7 1) $2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)(2^{ab-a} + 2^{ab-2a} + \cdots + 2^a + 1)$.

2) Soit p un entier naturel ; supposons $2^p - 1$ premier, et soit d un diviseur positif de p. Alors $2^d - 1$ est un diviseur positif de $2^p - 1$ au vu de la question 1. Vu la primalité de $2^p - 1$ c'est donc que $2^d - 1 = 1$ (et, dans ce cas, $d = 1$) ou que $2^d - 1 = 2^p - 1$ (et, dans ce cas, $d = p$). L'entier p est donc premier ou égal à 1 ; le deuxième terme de l'alternative ne se produit pas puisque $2^p - 1$ étant premier, il n'est lui-même pas égal à 1.

Exercice 7.8 Un entier $m \in \mathbb{N}$ peut être congru modulo 4 à 0, ± 1 ou 2. Son carré m^2 peut donc être congru à 0, 1 ou 4, lui-même congru à 0. Dans les deux cas extrêmes, m^2 est divisible par 4 donc fournit un reste nul. Dans le cas central, m^2 fournit le reste 1.

Si maintenant un entier n est somme de carrés, notons a et b des entiers pour lesquels $n = a^2 + b^2$. Alors $n = a^2 + b^2 \equiv 0 + 0$, $0 + 1$, $1 + 0$ ou $1 + 1$ modulo 4. Il n'est donc jamais congru à 3.

Exercice 7.9

On a : $3^{2n} - 2^n = 9^n - 2^n \equiv 2^n - 2^n \equiv 0\,[7]$. D'où le résultat.

Exercice 7.10 Soit $n \in \mathbb{N}$. Modulo 8, $7^n + 1 \equiv (-1)^n + 1$, qui vaut 0 si n est impair et 1 si n est pair.

Exercice 7.11 On a $100^{1000} \equiv 9^{1000} \quad [13]$.

Par le "petit théorème de Fermat", $9^{12} \equiv 1 \quad [13]$ donc $9^{1000} = 9^{996+4} = (9^{12})^8 3 \times 9^4 \equiv 9^4 = 81^2 \equiv 3^2 = 9 \quad [13]$. Le reste cherché est donc 9.

Variante : $9^2 = 81 \equiv 3 \quad [13]$ puis $9^3 \equiv 9^2 \times 9 \equiv 3 \times 9 = 27 \equiv 1 \quad [13]$ et enfin $9^{1000} = 9^{999} \times 9 = (9^3)^{333} \times 9 \equiv 9 \quad [13]$.

Exercice 7.12 Soit $n \in \mathbb{N}$, $n \geq 2$.

1. Supposons n impair. Le résultat est vrai pour 1. Sinon, soit $m \geq 1$ tel que $n = 2m + 1$. On a :

$$n^2 - 1 = (2m + 2)2m = 4m(m + 1)$$

Comme $m(m + 1)$ est pair, on a $n^2 \equiv 1\,[8]$.

2. Supposons n pair. Soit $m \geq 1$ tel que $n = 2m$, soit : $n^2 = 4m^2$. Si m est pair, alors m^2 l'est également et $n^2 \equiv 0\,[8]$. Sinon, d'après la première question, $m^2 \equiv 1\,[8]$, et par conséquent, $n^2 \equiv 4\,[8]$.

3.

(i) Soient a, b et c trois entiers impairs ; $(a + b + c)$ est donc également impair. D'après 1., on obtient : $a^2 + b^2 + c^2 \equiv 3\,[8]$ et $(a + b + c)^2 \equiv 1\,[8]$. Donc $2(ab + ac + bc) = (a + b + c)^2 - a^2 - b^2 - c^2 \equiv -2\,[8]$.
(ii) Supposons qu'il existe $m \in \mathbb{N}$ tel que $m^2 = ab + bc + ca$. Si $m \geq 2$, alors, d'après les deux premières questions, $2m^2$ est égale à 0 ou 2 modulo 8. Donc $m < 2$. Or $ab + bc + ca \geq 3$. Contradiction. Donc il n'existe pas de $m \in \mathbb{N}$ tel que $m^2 = ab + bc + ca$.

Exercice 7.13

1. $2^m = 2^3 2^{m-3} \equiv 0 \times 2^{m-3} = 0(\mod 8)$.
   – Si n est pair, notons $n = 2k$. Alors $2^n - 3^m \equiv 0 - 9^k \equiv -1^k = -1 \not\equiv 1(\mod 8)$
   – Si n est impair, notons $n = 2k+1$. Alors $2^n - 3^m \equiv 0 - 3 \times 9^k \equiv -3 \not\equiv 1(\mod 8)$.
   Dans les deux cas $2^n - 3 \neq 1$.
2. Pour $m = 0$ et tout $n \in \mathbb{N}$ on a que $2^n - 3^m = 1 - 3^n \leq 0$, donc $2^n - 3^m \neq 1$
   Pour $m = 1$ et tout $n \in \mathbb{N}$ on a que $2^n - 3^m = 1$ ssi $2 - 3^n = 1$ ssi $3^n = 1$ ssi $n = 0$.
   Pour $m = 2$ et tout $n \in \mathbb{N}$ on a qu $2^n - 3^m = 1$ ssi $4 - 3^n = 1$ ssi $3 * n = 3$ ssi $n = 1$.
   Les solutions sont $(1, 0)$ et $(2, 1)$.

Exercice 7.14 On peut prend $x = -2$ comme solution à l'équation $5x \equiv 1\,[11]$. Ensuite, pour $x \in \mathbb{Z}$, $5x \equiv 0\,[11] \Leftrightarrow 11 \mid 5x \Leftrightarrow 11 \mid x$ (lemme de Gauss). Les solutions sont donc les éléments de la forme $11k$, $k \in \mathbb{Z}$. Soit $x \in \mathbb{Z}$ on a $5x \equiv 1\,[11] \Leftrightarrow 5x \equiv 5(-2)\,[11] \Leftrightarrow 5(x+2) \equiv 0\,[11] \Leftrightarrow \exists k \in \mathbb{Z}, x+2 = 11k \Leftrightarrow \exists k \in \mathbb{Z}, x = -2+11k$.

Exercice 7.15

(i) Appliquons l'algorithme d'Euclide à 58 et 21. On a :

$$58 = 2 \times 21 + 16, \quad 21 = 16 + 5, \quad 16 = 3 \times 5 + 1.$$

En remontant les étapes de l'algorithme, on a :

$$1 = 16 - 3 \times 5 = 16 - 3 \times (21 - 16) = 4 \times 16 - 3 \times 21 = 4(58 - 2 \times 21) - 3 \times 21 = 4 \times 58 - 11 \times 21$$

Donc $(4, -11)$ est solution de $58x + 21y = 1$ dans $\mathbb{Z}^2$.

(ii) Soit $(x, y) \in \mathbb{Z}^2$ une solution de $58x + 21y = 0$. Comme $58 \wedge 21 = 1$, d'après le lemme de Gauss, $21|x$ et $58|y$. Soit $k_x \in \mathbb{Z}$ et $k_y \in \mathbb{Z}$ tels que $x = 21k_x$ et $y = 58k_y$. On a :

$$0 = 58x + 21y = 58 \times 21(k_x + k_y)$$

Donc $k_x = -k_y$.

Réciproquement, soit $k \in \mathbb{Z}$. On a :

$$k \times 21 \times 58 - k \times 58 \times 21 = 0.$$

Donc l'ensemble des solutions dans $\mathbb{Z}^2$ de $58x + 21y = 0$ est $\{(k \times 21, -k \times 58), k \in \mathbb{Z}\}$.

(iii) Soit $(x, y) \in \mathbb{Z}^2$. On a, d'après (i) : $58x + 21y = 1 \iff 58x + 21y = 4 \times 58 - 11 \times 21 \iff 58(x-4) + 21(y+11) = 0$. D'après (ii) on a donc : $58x + 21y = 1 \iff \exists k \in \mathbb{Z}, x - 4 = 21k, y + 11 = 58k \iff \exists k \in \mathbb{Z}, x = 4 + 21k, y = 58k - 11$. Donc l'ensemble des solutions de $58x + 21y = 1$ dans $\mathbb{Z}^2$ est $\{(4 + 21k, 58k - 11), k \in \mathbb{Z}\}$.

Exercice 7.16

1. On divise par 45. Le systeme est alors equivaut a $37x+23y = 1$. On a $37 = 23 \cdot 2 - 9$ puis $23 = 2 \cdot 9 + 5$ puis $9 = 2 \cdot 5 - 1$. Donc $PGCD(37, 23) = 1$. On remonte: $1 = 5 \cdot 2 - 9 = (23 - 9 \cdot 2) \cdot 2 - 9 = 23 \cdot 2 - 9 \cdot 5 = 23 \cdot 2 - (23 \cdot 2 - 37) \cdot 5 = 37 \cdot 5 - 23 \cdot 8$. Les solution du systeme sont donc: $(x, y) \in \{5+23n, -8-37n | n \in \mathbb{Z}\}$.
2. $PGCD(35, 14) = 7$ et donc le systeme est alors equivaut a $2x+5y = 3$, une solution evident est $(4, -1)$, et les solution sont donc $(x, y) \in \{5 + 5n, -1 - 2n | n \in \mathbb{Z}\}$.
3. $637 = 7^2 \cdot 13$ et $595 = 5 \cdot 7 \cdot 17$ donc $PGCD(637, 595) = 7$ et 7 ne divise pas 29, donc le systeme n'a pas de solution.

Exercice 7.17 On remarque que $n = -6$ est solution de (S). Soit $n \in \mathbb{Z}$, $(S_0) \Leftrightarrow n$ est un multiple commun de 19 et 12 $\Leftrightarrow n$ multiple de ppcm$(19, 12) = 228$.

Soit $n \in \mathbb{Z}$, $(S) \Leftrightarrow \begin{cases} n \equiv -6 \pmod{19} \\ n \equiv -6 \pmod{12} \end{cases} \Leftrightarrow \begin{cases} n + 6 \equiv 0 \pmod{19} \\ n + 6 \equiv 0 \pmod{12} \end{cases} \Leftrightarrow \exists k \in \mathbb{Z}, n = 228k - 6.$

Exercice 7.18

(i) On a :

$$5 \times 7 - 2 \times 17 = 1$$

En regardant la précédente égalité modulo 17 puis modulo 7, on en déduit que 35 est une solution de S_1 et -34 est solution de S_2.

(ii) Soit $n \in \mathbb{N}$. Comme 7 et 17 sont premiers entre eux, n est divisible par 7 et 17 si et seulement si n est divisible par $7 \wedge 17 = 119$. On en déduit que l'ensemble des solutions de S_0 est $\{119l, l \in \mathbb{Z}\}$.

(iii) D'après (i), n solution de S si et seulement si $n - a35 + b34$ est solution de S_0. Donc, d'après (ii), l'ensemble des solutions de S est $\{119l + 35a - 34b, l \in \mathbb{Z}\}$.

Exercice 7.19

1. $3 \in X$
2. Si $a_1, \ldots, a_n \in \mathbb{Z}$et sont tous congrus a 1 modulo 4 leur produit est congru a $1^n = 1$ modulo 4 donc de la forme $4k + 1$.
3. On remarque d'abord que $a = 4p_1p_2 \cdots p_n - 1 \equiv 0 - 1 \equiv -1 \equiv 3(\mod 4)$. Il est donc impair donc tout ses facteurs premiers lle sont aussi. Vu le **2.** ils ne peuvent pas etre tous de la forme $4k + 1$ car si tel etait le cas, a serait lui-meme congru a 1 modulo 4. L'un au moins de ces facteurs premiers est de la forme $4k + 3$.
4. Pour tout $i \in \{1, \ldots, n\}$ on a que $a \equiv -1(\mod p_i)$ donc p_i ne divise pas a . Donc aucun element de X ne divise a. Pourtant on a vu au **3.** qu'un element de X au moins divise a. Cela est totalement absurde. On etait dans l'erreur en supposant que X est fini. Il ne l'est pas.

Exercice 7.20 On écrit $n = 2^k m$ avec m impair et $b = a^{2^k}$. Par l'absurde, on suppose $m > 1$. Comme m est impair, $a^n + 1 = (b + 1)(b^{m-1} - b^{m-2} - \ldots - b + 1)$. C'est absurde car $a^n + 1$ est premier. Donc $m = 1$, et ainsi $n = 2^k$. Ceci ne nous dit pas à priori, que la conjecture est vraie. On teste : $2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$, $2^{2^4} + 1 = 65537$ sont premiers. Mais $2^{2^5} + 1 = 4294967297$ n'est pas premier.

Exercice 7.21

1. Soit $n \in \mathbb{N}$. Montrons par récurrence que pour tout $k \in \mathbb{N}^*$, on a :

$$2^{2^{n+k}} - 1 = (2^{2^n} - 1) \cdot \prod_{i=0}^{k} (2^{2^{n+i}} + 1)$$

Initialisation : pour $k = 1$, on a $2^{2^{n+1}} - 1 = \left(2^{2^n}\right)^2 - 1 = (2^{2^n} - 1)(2^{2^n} + 1)$.
Hypothèse de récurrence : Supposons qu'il existe $k \in \mathbb{N}^*$ tel que :

$$2^{2^{n+k}} - 1 = (2^{2^n} - 1) \cdot \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1)$$

Hérédité : Alors : $2^{2^{n+k+1}} - 1 = \left(2^{2^{n+k}}\right)^2 - 1 = (2^{2^{n+k}} - 1)(2^{2^{n+k}} + 1) = (2^{2^n} - 1) \cdot \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1)(2^{2^{n+k}} + 1)$, d'après l'hypothèse de récurrence. Ce qui conclut.

2. Soient $(m, n) \in \mathbb{N}^2$ tel que $n \neq m$. Supposons sans perdre en généralité que $n < m$ et soit $k \in \mathbb{N}^*$ tel que $m = n + k$. Soit $d = F_n \wedge F_m$. Alors :

$$F_m = (2^{2^n} - 1) \cdot \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1) + 2 = F_n(2^{2^n} - 1) \cdot \prod_{i=1}^{k-1} (2^{2^{n+i}} + 1) + 2 \equiv 2[d]$$

Or $F_m \equiv 0[d]$ par hypothèse. Donc $d|2$. Comme les F_n sont impairs, $d = 1$.

3. Supposons par l'absurde qu'il existe $N \in \mathbb{N}^*$ nombre premiers. D'après le principe des tiroirs, il existe p premier et $1 \leq k < l \leq N + 1$ tels que p divise F_k et F_l. Ce qui est absurde d'après la question précédente.

Exercice 7.22

1. $2^8 + 2^7 + 2^5 + 2^3 + 1 = 424$

2. $3^8 + 3^7 + 3^5 + 3^3 + 1 = 9019$

3. $8^3 + 3 \cdot 8^2 + 6 \cdot 8 + 7 = 759$

4. $5^3 + 4 \cdot 5^2 + 2 = 227$

Exercice 7.23

1. $255 = 2^8 - 1 = 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2 + 1 = (11111111)_2$.

2. On estime aisément que $16^2 < 1907 < 16^3$. On calcule $16^2 = 2^8 = 256$. On effectue la division euclidienne de 1907 par 256 : $1907 = 7 \cdot 256 + 115$. Puis on effectue la division euclidienne de 115 par 16 : $115 = 7 \cdot 16 + 3$. Donc $1907 = (773)_{16}$.

3. On estime aisément que $7^3 < 2016 < 7^4$. On calcule $7^3 = 343$. On effectue la division euclidienne de 2016 par 343 : $2016 = 5 \cdot 343 + 301$. Puis on effectue la division euclidienne de 301 par $7^2 = 49$: $301 = 6 \cdot 49 + 7$. Et $7 = (10)_7$. Donc $2016 = (5610)_7$.

4. $2000 = (10)_{2000}$.

Exercice 7.101 Il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$. On a donc $n^2 - 1 = 4k(k + 1)$ et puisque k ou $k + 1$ est un entier pair on a bien $8 \mid 4k(k + 1)$.

Exercice 7.102

Soit $n \in \mathbb{N}^*$. On a : $9n + 4 \wedge 2n + 1 = 2n + 1 \wedge n + 1 = n + 1 \wedge n = 1$. De même : si $n = 1$, alors $3n - 2 = 1$. Si $n \geq 2$, $5n - 3 \wedge 3n - 2 = 3n - 2 \wedge 2n - 1 = 2n - 1 \wedge n - 1 = n - 1 \wedge 1 = 1$.

Exercice 7.103

Pour un nombre entier positif n, on pose $\tau(n) =$ nombre des diviseurs positifs de n. Alors si m, n sont des entiers positifs premiers entre eux on a $\tau(mn) = \tau(n)\tau(m)$, car un diviseur positif de mn est le produit (unique) d'un diviseur de n par un diviseur de m. Aussi , pour un nombre premier p et un nombre poisitif a on a $\tau(p^a) = a + 1$. Ceci dit, les reposes aux questions sont les suivants:

1. $\tau(36) = \tau(2^2)\tau(3^2) = 3 \cdot 3 = 9$

2. Si $n = p_1^{a_1} \cdots p_k^{a_k}$ alors $\tau(n^2) = \Pi_{i=1}^k (a_i + 1)^2$ est un nombre impair.

3. Si $n = 15!$ alors $n = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$ et donc $\tau(15!) = 12 \cdot 7 \cdot 4 \cdot 3 \cdot 2 \cdot 2 = 2848$.

Exercice 7.104

1. Soit i tel que le i-ème chiffre de a et b diffère. Si $-a \equiv -b\,[97]$ alors il existe un entier x tel que $-a \equiv x - a_i 10^i \equiv x - b_i 10^i \equiv -b\,[97]$ où a_i (resp. b_i) est le i-ème chiffre dans l'écriture de a (resp. b) en base 10. On en déduit alors $a_i 10^i \equiv b_i 10^i\,[97]$ et puisque 10^i et 97 sont premiers entre eux $a_i \equiv b_i\,[97]$ et donc $a_i = b_i$ ce qui est absurde.

2. On suppose comme avant $-a \equiv -b\,[97]$. Il existe un entier x et $i \in \{0, \ldots, 11\}$ tels que $-a \equiv x - a_i 10^i - a_{i+1} 10^{i+1} \equiv x - a_{i+1} 10^i - a_i 10^{i+1} \equiv -b\,[97]$. on en déduit $(a_i - a_{i+1})10^i \equiv (a_i - a_{i+1})10^{i+1}$ et a nouveau puisque $(a_i - a_{i+1})10$ est premier avec 97 on a $1 \equiv 10\,[97]$ ce qui est absurde.

Exercice 7.105

1. (i) Soient $x, y \in A$. Par définition de $(a_i - a_{i+1})10A$, on a $2 \leq x + y \leq p - 1$, les égalités étant obtenues que si $x = y = 1$ et $x = y = \dfrac{p-1}{2}$. Donc, si $x \neq y$, on a : $2 < x + y < p - 1$. Comme $0 < x + y < p$, p ne divise pas $x + y$. (ii) Sans perdre en généralités, on peut supposer que $x > y$. Alors , on a $p > \dfrac{p-1}{2} > x - y > 0$. Donc p ne divise pas $x - y$. (iii) On a $x^2 - y^2 = (x - y)(x + y)$. Comme p ne divise ni $x - y$ ni $x + y$, p ne divise pas $x^2 - y^2$. (iv) Erreur dans la question : D'après ce qui précède, **les carrés** des éléments de A ont des restes distincts par al division euclidienne par p.

2. Soit $k \in \mathbb{N}$. On a $(p-k)^2 = p^2 - 2pk + k^2 \equiv 0 + 0 + k^2[p]$. En appliquant cela à $k \in A$, on en déduit que les carrés des éléments de $\{\frac{p+1}{2}, ..., p-1\}$ ont les mêmes restes que les carrés des éléments de A par la division euclidienne par p.

3. Le reste de la division euclidienne d'un carré par p peut donc prendre $\frac{p+1}{2}$ valeurs (un par élément de A ainsi que 0). Pour $p = 7$, ces quatre valeurs sont $0, 1, 2, 4$.

Exercice 7.106 Si on pose$z := x - 3y$ on a que $x^2 - 6xy + 2y^2 \equiv (x-3y)^2 = z^2(\mod 7)$, or pour un entier z on a que $z^2 \equiv 0, 1, 2, 4(\mod 7)$. Mais $7003 \equiv 3(\mod 7)$. Donc il n'existe pas des x, y entiers avec $x^2 - 6xy + 2y^2 = 7003$.

Exercice 7.107 Supposons $p \equiv 3\,[4]$ et $n^2 \equiv -1\,[p]$ pour certain $n \in \mathbb{N}$. On peut supposer que p et n premiers entre eux sinon p divise n^2 et donc p ne peut pas diviser n^2+1. Par le "petit théorème de Fermat" on a donc $n^{p-1} \equiv 1\,[p]$. D'autre part puisque $n^2 \equiv -1\,[p]$ on déduit $n^{2\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1\,[p]$ et donc $n^{p-1} \equiv -1\,[p]$ ce qui est impossible car $1 \not\equiv -1\,[p]$.

Exercice 7.108

D'après le petit théorème de Fermat, on a : $2^{70} + 3^{70} \equiv 2^{10} + 3^{10}\,[13]$. D'autre part, les puissances consécutives de 2 modulo 13 sont : $2, 4, 8, 3, 6, -1, -2, -4, -8, -3$ et celles de 3 modulo 13 sont : $3, 9, 1$. Donc $2^{10} + 3^{10} \equiv -3 + 3 \equiv 0[13]$. Donc $13|2^{70} + 3^{70}$.

Exercice 7.109

$n := 7^{9^9} = 7^{729}$ or $7^4 = 2401$ donc $7^4 \equiv 1(\mod 100)$ mais $729 = 4 \cdot 182 + 1$ donc $7^{729} = (7^4)^{182} \cdot 7 \equiv 1 \cdot 7(\mod 100)$ donc les deux derniers chiffres de n sont 07.

Exercice 7.110 On a $1996 = 4 \cdot 499$ donc $\text{pgcd}(11, 1996) = 1$. Par le petit theorème de Fermat, $1996^{10} \equiv 1\,[11]$ et donc $1996^{1990} \equiv 1^{199} \equiv 1\,[11]$. D'autre part $1996 \equiv 5\,[11]$, $5^2 \equiv 3\,[11]$ et donc $5^6 \equiv 27 \equiv 5\,[11]$. On a finalement $1996^{1996} \equiv 5\,[11]$.

Exercice 7.111 1) Soit $x \in \mathbb{Z}$. On a : $10x \equiv 25\,[15] \iff 10x \equiv 10\,[15] \iff 10(x-1) \equiv 0\,[15] \iff 2(x-1) \equiv 0[3] \iff x \equiv 1[3]$ car $2 \wedge 3 = 1$.

2) Soit $x \in \mathbb{Z}$. On a : $10x \equiv 35\,[21] \iff 10x \equiv -60\,[21] \iff 10(x+6) \equiv 0\,[21] \iff x \equiv -6[21]$ car $10 \wedge 21 = 1$.

Exercice 7.112

D'apres le petit theoreme de Fermat : $2^{16} \equiv 1(\mod 17)$ et $2^{22} \equiv 1(\mod 23)$. donc $(2^{22n}-1)(2^{16n}-1) \equiv 0(\mod 23 \cdot 17 = 391)$

Exercice 7.113 Pour $k \in \mathbb{N}$ on note $P(k)$ la propriété $2^{2^{6k+2}} \equiv -3\,[19]$. On démontre cette propriété par récurrence.

Initialisation : $2^{2^2} = 16 \equiv -3\,[19]$ donc $P(0)$ est vraie.

Hérédité : $k \in \mathbb{N}$. On suppose $P(k)$ vraie. On calcule $2^{2^{6(k+1)+2}} = (2^{2^{6k+2}})^{2^6}$ donc $2^{2^{6(k+1)+2}} \equiv (-3)^{2^6}\,[19]$. Or $(-3)^{2^6} \equiv (-3)^{18 \cdot 3}(-3)^{10} \equiv -3\,[19]$. Donc $P(k+1)$ est vraie.

On en déduit que $P(k)$ est vraie pour tout $k \in \mathbb{N}$.