Exercice 6.1

Éléments de correction. — on trouve les couples (quotient,reste) suivants : $(990,11)$, $(59696,9)$ $(5094,5)$

Exercice 6.2

Indication. — On se rappellera bien la condition que le reste d'une division euclidienne est positif et strictement majoré par la valeur absolue du diviseur

Éléments de correction. — Puisque $12079233 = 75968 \times 159 + 321$ et que $0 \leqslant 321 < 75968$, le reste de la division par 75968 est 321.

En outre

$$12079233 = 75968 \times 159 + 321 = 75968 \times 159 + 2 \times 159 + 3 = (75968 + 2) \times 159 + 3$$

donc le reste de la division par 159 est 3

Exercice 6.3

Indication. — Calculer les puissances de 3 modulo 7. À quoi est égal 38 modulo 7 ?

Éléments de correction. — $3^0 = 1 \pmod 7$, $3^1 = 3 \pmod 7$, $3^2 = 9 \pmod 7$ soit $3^2 = 2 \pmod 7$,

$3^3 = 2 \times 3 \pmod 7$ soit $3^3 = 6 \pmod 7$

$3^4 = 6 \times 3 \pmod 7$ soit $3^4 = 4 \pmod 7$

$3^5 = 4 \times 3 \pmod 7$ soit $3^5 = 5 \pmod 7$

$3^6 = 5 \times 3 \pmod 7$ soit $3^6 = 1 \pmod 7$

Ces calculs montrent notamment que tous les restes de l'ensemble $\{1,2,3,4,5,6\}$ peuvent intervenir. En termes plus formels, soit f l'application qui à $n \in \mathbf{N}$ associe le reste de la division euclidienne de 3^n par 7. Alors ces calculs montrent que tout élément de l'ensemble $\{1,2,3,4,5,6\}$ possède un antécédent par f. La question qui reste a priori en suspens est de savoir si 0 est ou non "atteint" par f. On va montrer que ce n'est pas le cas (en d'autres termes, que f induit une application surjective de $\mathbf{N}$ sur $\{1,2,3,4,5,6\}$).

Une façon de procéder est, prenant un entier naturel n quelconque, d'écrire la division euclidienne de n par 6, soit $n = 6 \cdot q + r$ avec $q \in \mathbf{N}$ et $r \in \{0,1,2,3,4,5\}$.

Alors $3^n = (3^6)^q \cdot 3^r$ d'où $3^n = (3^6)^q \cdot 3^r \pmod 7$ d'où $3^n = 1^q \cdot 3^r \pmod 7$ d'où $3^n = 3^r \pmod 7$. Or on connaît les valeurs de $3^r \pmod 7$ pour $r \in \{0,1,2,3,4,5\}$ et aucune n'est égale à 0 modulo 7. Donc 3^n n'est pas égal à 0 modulo 7.

Une autre possibilité est de montrer par récurrence que pour tout entier naturel n, 7 ne divise pas 3^n, en utilisant le lemme d'Euclide et le fait que 7 est premier.

Comme $38 = 3 \pmod 7$, toutes les congruences ci-dessus sont encore valables en remplaçant les puissances de 3 par des puissances de 38, et on aboutit à la même conclusion

Exercice 6.4

Indication. — Commencer par regarder pour de petites valeurs de n pour se faire une idée On pourra utiliser le petit théorème de Fermat.

Éléments de correction. — Pour le 1. (les autres sont similaires), on devine que 7 divise 4^n+2^n+1 si et seulement si 3 ne divise pas n. Montrons le. Comme 7 est premier, on a $4^6 = 1 \pmod 7$ et $2^6 = 1 \pmod 7$. Soit n un entier naturel quelconque et $n = 6\cdot q + r$ la division euclidienne de n par 6. On a $4^n+2^n+1 = (4^6)^n\cdot 4^r + (2^6)^n\cdot 2^r + 1$ d'où

$$4^n+2^n+1 = 1^n\cdot 4^r + 1^n\cdot 2^r + 1 \pmod 7$$

soit

$$4^n+2^n+1 = 4^r+2^r+1 \pmod 7$$

Il suffit donc d'examiner si 4^r+2^r+1 est divisible par 7 pour $r\in\{0,1,2,3,4,5\}$ et on trouve que c'est le cas si et seulement si $r\in\{1,2,4,5\}$.

Exercice 6.5

Indication. — Commencer par réduire 247 modulo 7, puis calcul de puissances modulaire en s'aidant ou non du petit théorème de Fermat

Éléments de correction. — On a $247 = 35\times 7+2$ donc $247 = 2 \pmod 7$ d'où $247^{349} = 2^{349} \pmod 7$ D'après Fermat, $2^6 = 1 \pmod 7$; la division euclidienne de 349 par 6 s'écrit $349 = 6\times 58+1$. Donc $2^{349} = 2^1 \pmod 7$ donc le reste cherché est 2 (car 0≤ 2<7$)

Exercice 6.6

Indication. — Comme toujours, on pourra commencer si nécessaire par se faire une idée sur de petites valeurs de n. On pourra aussi se rappeler que $7 = -1 \pmod 8$

Éléments de correction. — Comme $7 = -1 \pmod 8$, pour tout entier naturel n on a $7^n + 1 = (-1)^n + 1 \pmod 8$ or $(-1)^n+1$ vaut 0 si n est impair et 2 si n est pair.

Exercice 6.7.1

Indication. — Attention, ici Fermat ne s'applique pas

Éléments de correction. — Par récurrence, en notant que si $6^n = 6 \pmod{10}$ alors $6^{n+1} = 6\times 6 \pmod{10}$ or $36 = 6 \pmod{10}$

Exercice 6.7.2

Indication. — chiffre des unités = reste modulo 10
on pensera à réduire 123456 modulo $10

Éléments de correction. — On a $123456 = 6 \pmod{10}$ donc a $123456^{789} = 6^{789} \pmod{10}$ et on conclut grâce à la première question (réponse : 6)

Exercice 6.7.3

Indication. — On pourra par exemple décomposer $56 = 50 + 6$ et appliquer la formule du binôme

Éléments de correction. — D'après la formule du binôme et le fait que 10 divise 50 (donc pour tout $n \geqslant 2$, $50^n = 0 \pmod{100}$), on a

$$56^6 = 6 \cdot 50 \cdot 6^5 + 6^6 \pmod{100}$$

or $6 \cdot 50 = 0 \pmod{100}$ donc $56^6 = 6^6 \pmod{100}$ Or $6^3 = 216$ donc $6^6 = 16^2 \pmod{100}$ et $16^2 = 256$.

Exercice 6.7.4

Indication. — chiffre des dizaines = chiffres des dizaines du reste modulo 100

Éléments de correction. — On a $123456 = 56 \pmod{100}$ donc on a $123456^{789} = 56^{789} \pmod{100}$ Or $789 = 131 \cdot 6 + 3$ donc $56^{789} = 56^{131+3} \pmod{100}$ d'après la question précédent. $134 = 22 \cdot 6 + 2$ donc $56^{134} = 56^{22+2} \pmod{100}$. Et $24 = 6 \times 4$ donc $56^2 4 = 56^4 \pmod{100}$. En utilisant le binome de Newton, $56^4 = 6^4 \pmod{100}$ or $6^3 = 16 \pmod{100}$ et on trouve au final $6 \cdot 16 = 96$ comme reste modulo 100 (réponse : 9)

Exercice 6.8

Indication. — Trois derniers chiffres = reste modulo 1000
Si 10 divise a, alors pour tout $n \geqslant 3$, on a $a^n = 0 \pmod{1000}$

Éléments de correction. — \$ 49^2=50^2-2· 50+1 \$ or $50^2 = 2500 = 500 \pmod{1000}$ donc $49^2 = 401 \pmod{1000}$

$$401^5 = \sum_{k=0}^{5} \binom{5}{k} 400^k \cdot 1^{5-k}$$

donc

$$401^5 = \sum_{k=0}^{2} \binom{5}{k} 400^k \pmod{1000}$$

or $\binom{5}{k} \cdot 400 = 0 \pmod{1000}$ pour $k = 1, 2$ donc

$$401^5 = 1 \pmod{1000}$$

Comme $7^20 = (((7^2))^2)^5 = (49^2)^5$ on en déduit $7^20 = 401^5 \pmod{1000}$ soit $7^20 = 1 \pmod{1000}$

Comme $1001 = 20 \cdot 50 + 1$ on en déduit $7^{1001} = 7^1 \pmod{1000}$

Exercice 6.9

Indication. — Algorithme d'Euclide pour le calcul du pgcd ; pour le ppcm on pourra utiliser la proposition 6.4.4.1 du cours

Éléments de correction. — Algorithme d'Euclide appliqué à 231868 et 8190:

$$\begin{aligned} 231868 &= 28\cdot 8190 + 2548 \\ 8190 &= 3\cdot 2548 + 546 \\ 2548 &= 4\cdot 546 + 364 \\ 546 &= 1\cdot 364 + 182 \\ 364 &= 2\cdot 182 + 0 \end{aligned}$$

Le dernier reste non nul est 182, donc $231868 \wedge 8190 = 182$

Donc $231868 \vee 8190 = \frac{231868\cdot 8190}{231868\wedge 8190} = 10434060$

De la même façon, on trouve $23145 \wedge 17 = 1$ et $23145 \vee 17 = 23145\cdot 17 = 393465$ ainsi que $12345 \wedge 678 = 3$ et $12345 \vee 678 = \frac{12345\cdot 678}{12345\wedge 678} = 2789970$

Exercice 6.10

Indication. — Algorithme d'Euclide étendu (exemple p. 77 et remarque p. 78 du cours)

Éléments de correction. — \'Ecrivons

$$\begin{aligned} 35\cdot 1 + 23\cdot 0 &= 35 && (L_1) \\ 35\cdot 0 + 23\cdot 1 &= 23 && (L_2) \end{aligned}$$

La première division euclidienne de l'algorithme d'Euclide pour 35 et 23 s'écrit $35 = 1\cdot 23 + 12$. L'opération $(L_3) = (L_1) - 1\cdot(L_2)$ donne alors

$$\begin{aligned} 35\cdot 1 + 23\cdot 0 &= 35 && (L_1) \\ 35\cdot 0 + 23\cdot 1 &= 23 && (L_2) \\ 35\cdot 1 - 23\cdot 0 &= 12 && (L_3) \end{aligned}$$

La deuxième division euclidienne de l'algorithme d'Euclide pour 35 et 23 s'écrit $23 = 1\cdot 12 + 11$. L'opération $(L_4) = (L_2) - 1\cdot(L_3)$ donne alors

$$\begin{aligned} 35\cdot 1 + 23\cdot 0 &= 35 && (L_1) \\ 35\cdot 0 + 23\cdot 1 &= 23 && (L_2) \\ 35\cdot 1 + 23\cdot(-1) &= 12 && (L_3) \\ 35\cdot(-1) + 23\cdot 2 &= 11 && (L_4) \end{aligned}$$

La troisième division euclidienne de l'algorithme d'Euclide pour 35 et 23 s'écrit $12 = 1\cdot 11 + 1$. L'opération $(L_5) = (L_3) - 1\cdot(L_4)$ donne alors

$$\begin{aligned} 35\cdot 1 + 23\cdot 0 &= 35 && (L_1) \\ 35\cdot 0 + 23\cdot 1 &= 23 && (L_2) \\ 35\cdot 1 + 23\cdot(-1) &= 12 && (L_3) \\ 35\cdot(-1) + 23\cdot 2 &= 11 && (L_4) \\ 35\cdot 2 + 23\cdot(-3) &= 1 && (L_5) \end{aligned}$$

Donc le pgcd est 1 (comme l'énoncé le laissait supposer) et (L_5) donne une relation de Bezout.

Par un procédé similaire, on trouve la relation

$$27 \cdot (-12) + 25 \cdot 13 = 1.$$

Exercice 6.11

Indication. — Pour 6.11.1, algorithme d'Euclide étendu (exemple p. 77 et remarque p. 78 du cours)

Pour 6.11.2, le d trouvé au 6.11.1 ne divise pas 15

Éléments de correction. — Pour 6.11.1, on trouve $d = 13$ et la relation

$$2873 \times 23 + 1001 \times (-66) = 13$$

Raisonnons par l'absurde et supposons qu'il existe $(u, v) \in \mathbf{Z}^2$ tels que $au + bv = 15$. Comme 13 diviser a et b, 13 divise $au + bv$. Donc 13 divise 15.

Exercice 6.12

Indication. — Se rappeler que si a est un entier pair, il existe un entier b tel que $a = 2b$ et si a est un entier impair, il existe un entier b tel que $a = 2b + 1$. Prendre alors le carré...

Le début de 6.12.3(a) découle des deux premières questions et de la compatibilité des congruences à l'addition. Pour la fin de 6.12.3(a), regarder les carrés modulo 8.

Dans 6.12.3(b), on précise qu'on demande de montrer que $ab + bc + ac$ n'est pas un carré modulo 4. Commencer par travailler modulo 8 en utilisant 6.12.2.

Éléments de correction. — 4 divise $(2b)^2 = 4b^2$....

$(2b+1)^2 = 4(b^2+b)+1$ or $b^2 + b = b(b+1)$ est pair quel que soit la parité de b (si b est impair, $b+1$ est pair)

Si a, b, c sont impairs, on a $a^2 = 1 \pmod 8$, $b^2 = 1 \pmod 8$ et $c^2 = 1 \pmod 8$ soit en ajoutant $a^2 + b^2 + c^2 = 3 \pmod 8$ et comme $0 \leqslant 3 < 8$ le reste est 3 Si d est un entier et r est le reste de la division euclidienne de d par 8, on a $d^2 = r^2 \pmod 8$. En calculant $r^2 \pmod 8$ pour $r \in \{0,1,2,3,4,5,6,7\}$, on trouve les valeurs 0, 1, 4 et uniquement ces valeurs (au passage on le savait déjà pour toutes les valeurs impaires de r) Donc aucun carré d'entier n'est congru à 3 modulo 8.

$(a+b+c)^2 = a^2 + b^2 + c^2 + 2(ab+bc+ac)$; en réduisant modulo 8 et en utilisante 6.12.2, on trouve $1 = 3 + 2(ab+bc+ac) \pmod 8$ soit $2(ab+bc+ac) \pmod 8 = 6 \pmod 8$. Donc 8 divise $2(ab+bc+ac) - 6$.

Exercice 6.13

Indication 1. — On peut essayer d'utiliser le corollaire 6.4.2 du cours. On peut aussi essayer d'utiliser le fait que deux entiers a et b sont premiers entre eux si et seulement si pour tout nombre premier p, p ne divise pas a ou p ne divise pas b (énoncé favorables aux raisonnements par l'absurde)

Indication 2. — En utilisant le corollaire 6.4.2 : pour 6.13.1 écrire une identité de Bezout pour a et b et essayer d'en déduire une identité de Bezout pour a et $a+b$. Pour 6.13.2 écrire une identité de Bezout pour a et b, une identité de Bezout pour a et c, et les multiplier terme à terme. Pour 6.13.3 écrire une identité de Bezout pour a et b, et l'élever à une puissance bien choisie pour obtenir (grâce à la formule du binôme) une identité de Bezout pour a^k et b^l

Éléments de correction. — Pour 6.13.1, supposons qu'il existe un nombre premier p qui divise a et $a+b$. Comme p divise a et $a+b$, p divise $(a+b)-a$, donc p divise b. Donc p divise a et b, ce qui contredit le fait que a et b sont premiers entre eux (ici on pouvait remplacer p nombre premier par d entier tel que $d>2$)

Alternativement, pour 6.13.1, comme a et b sont premiers entre eux, il existe $(u,v)\in\mathbf{Z}^2$ tels que $au+bv=1$. Donc $au-av+(b+a)v=1$. Donc $a(u-v)+(b+a)v=1$. On en déduit que a et $b+a$ sont premiers entre eux.

Pour 6.13.2, supposons qu'il existe un nombre premier p qui divise a et bc. Comme p divise bc et est premier, p divise b ou p divise c (Euclide)$. Dans le premier cas, p divise a et b, ce qui contredit le fait que a et b sont premiers entre eux. Itou dans le second cas.

Alternativement, pour 6.13.2, comme a et b sont premiers entre eux, il existe $(u_1,v_1)\in\mathbf{Z}^2$ tels que $au_1+bv_1=1$. Comme a et c sont premiers entre eux, il existe $(u_1,v_1)\in\mathbf{Z}^2$ tels que $au_2+cv_2=1$. Donc $1=(au_1+bv_1)(au_2+cv_2)$. Développer le membre de droite et reconnaître une identité de Bezout pour a et bc.

Pour 6.13.3, supposons qu'il existe un nombre premier p qui divise a^k et b^l. Par la généralisation du lemme d'Euclide à un nombre fini de facteurs, comme p divise a^k, p divise a. De même p divise b. Ceci le fait que a et b sont premiers entre eux. *NB* on a implicitement supposé k et l strictement positifs ; si par exemple $k=0$, $a^k=1$ et donc a^k et b^l sont automatiquement premiers entre eux.

Alternativement, pour 6.13.3, comme a et b sont premiers entre eux, il existe $(u,v)\in\mathbf{Z}^2$ tels que $au+bv=1$. Donc $1=1^{k+l}=(au+bv)^{k+l}$. Développer $(au+bv)^{k+l}$ à l'aide de la formule du binôme, et essayer de reconnaître une identité de Bezout pour a^k et b^l (regarder éventuellement pour de petites valeurs explicites de k et l pour comprendre ce qu'il se passe)

Pour 6.13.2, on pourrait envisager de généraliser en la démonstration de la formule de distributivité suivante $(a\wedge b)\cdot(a\wedge c)=a\wedge(bc)$ (où a b et c sont quelconques) ; en effet il existe $(u_1,v_1)\in\mathbf{Z}^2$ tels que $au_1+bv_1=a\wedge b$ et $(u_2,v_2)\in\mathbf{Z}^2$ tels que $au_2+cv_2=a\wedge c$. Donc $(a\wedge b)\cdot(a\wedge c)=(au_1+bv_1)(au_2+cv_2)$. En développant le membre de droite, on trouve des entiers u' et v' tels que $au'+bcv'=(a\wedge b)\cdot(a\wedge c)$. On aimerait en déduire que $a\wedge(bc)=(a\wedge b)\cdot(a\wedge c)$, *sauf que* le théorème de Bezout ne se généralise pas ainsi. De manière générale, il n'est pas vrai que si on a des entiers a, u, b, v et d tel que $au+bv=d$, alors $a\wedge b=|d|$. Tout ce qu'on peut déduire de cette situation en général est que $a\wedge b$ divise d. *Il est bon de retenir ce qui précède, car l'erreur est assez fréquemment commise.* On pourra méditer sur l'exemple $a=3$, $b=2$, $u=d$ et $v=-d$. En particulier une telle démonstration de la relation $(a\wedge b)\cdot(a\wedge c)=a\wedge(bc)$ n'est pas valide. Et en fait la relation $(a\wedge b)\cdot(a\wedge c)=a\wedge(bc)$ est fausse en général (attention, le fait que la démonstration ci-dessus n'était pas correcte ne montrait pas nécessairement que la relation n'était pas vraie). Pour un contre-exemple minimal, prendre $a=b=c=2$. Pour des contre-exemples plus

systématiques, il est utile de connaître la formule (non explicitée en cours, mais qu'on peut éventuellement deviner) permettant de calculer le pgcd de a et de b en fonctions des décomposition en facteurs premiers de a et de b.

Exercice 6.14

Indication. — La réponse est non, et un argument de divisibilité permet de le montrer. Rappelons que la somme des entiers de 1 à 30 est $\frac{30(30+1)}{2}$

Éléments de correction. — Si N est la valeur commune de la somme de chacune des six colonnes, on doit avoir $6 \cdot N = \frac{30(30+1)}{2}$ or $\frac{30(30+1)}{2} = 15 \cdot 31$ n'est pas pair

Exercice 6.15

Indication. — On peut essayer d'utiliser le corollaire 6.4.2 du cours. On peut aussi (ce qui revient un peu au même) essayer d'appliquer l'algorithme d'Euclide. Pour 6.15.1 on pourra par exemple commencer par essayer d'appliquer Euclide à $3(8n+7)$ et $6n+5$.

Éléments de correction. — Pour 6.15.1, on a $3(8n+7) = 4(6n+5)+1$ (on a multiplié $8n+7$ par 3 pour pouvoir faire la division euclidienne par $6n+5$ indépendamment de la valeur de n) soit $3(8n+7) - 4(6n+5) = 1$

Pour 6.15.2, on peut par exemple écrire directement

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

(on a essayé de se "débarasser" des termes en n^2)

Pour 6.15.3, on a

$$6^{n+1} + 5^{n+1} = 6 \cdot (6^n + 5^n) - 6 \cdot 5^n + 5 \cdot 5^n = 6 \cdot (6^n + 5^n) - 5^n$$

donc (*cf.* proposition 6.3.2 du cours, pour laquelle on remarquera au passage que la condition sur r est inutile) $(6^{n+1} + 5^{n+1}) \wedge (6^n + 5^n) = (6^n + 5^n) \wedge 5^n$ Or

$$6^n + 5^n = 1 \cdot 5^n + 6^n$$

donc $(6^n + 5^n) \wedge 5^n = 5^n \wedge 6^n$. Or $5 \wedge 6 = 1$ et on peut conclure par l'exercice 6.13.3

Exercice 6.16

Indication. — Pour 6.16.1, trouver une solution particulière (a_0, b_0) avec Euclide étendu (ou directement). Si (a,b) est une solution quelconque, en déduire une relation entre $a - a_0$ et $b - b_0$ qu'on pourra étudier à l'aide du lemme de Gauss.

Même chose pour 6.16.2 (pour la solution particulière, on pourra partir de celle obtenue en 6.16.1)

Pour 6.16.3, penser à la situation de 6.11.2

Éléments de correction. — Pour 6.16.1, soit avec Euclide étendu, soit directement, on trouve que $(a_0, b_0) = (2, -1)$. Si $(a, b) \in \mathbf{Z}$ vérifie $6a+11b = 1$, on a donc $6a+11b = 6a_0+11b_0$ d'où $6(a-a_0) = 11(b_0-b)$. En particulier 6 divise $11(b_0-b)$ et comme $6 \wedge 11 = 1$ on en déduit (Gauss) que 6 divise b_0-b. Soit $k \in \mathbf{Z}$ tel que $b_0-b = 6k$. En remplaçant dans l'égalité $6(a-a_0) = 11(b_0-b)$, on trouve $6(a-a_0) = 11 \cdot 6k$ d'où $a-a_0 = 11k$. Finalement on a montré : si $(a, b) \in \mathbf{Z}^2$ vérifie $6a+11b = 1$, alors il existe $k \in \mathbf{Z}$ tel que $a = a_0+11k$ et $b = b_0-6k$.

Réciproquement, soit $k \in \mathbf{Z}$. Alors

$$6(a_0+11k)+11(b_0-6k) = 6a_0+11b_0+6 \cdot 11k+11 \cdot (-6k) = 6a_0+11b_0 = 1$$

Finalement

$$\{(a, b) \in \mathbf{Z}^2, \quad 6a+11b = 1\} = \{(a_0+11k, b_0-6k), \quad k \in \mathbf{Z}\}$$

Pour 6.16.2, on peut remarquer que $(6a_0, 6b_0)$ est solution particulière et procéder comme pour 6.16.1

Pour 6.16.3, le membre de gauche est nécessairement pair ; or 5 n'est pas pair. Donc l'ensemble des solutions est vide.

Exercice 6.17

Indication. — On peut écrire $a = 18 \cdot a'$ et $b = 18 \cdot b'$ avec $a' \wedge b' = 1$ Penser aussi à utiliser la proposition 6.4.4.1 du cours

Éléments de correction. — Comme $18 = a \wedge b$, 18 divise en particulier a et b. On peut écrire $a = 18 \cdot a'$ et $b = 18 \cdot b'$ avec $a', b' \in \mathbf{N}$. On sait (corollaire 6.4.5.1) que $(18 \cdot a') \wedge (18 \cdot b') = 18 \cdot a' \wedge b'$ donc $a' \wedge b' = 1$.

D'après 6.4.4.1, on a $a \cdot b = 18 \cdot 360$, d'où $18 \cdot a' \cdot b' = 360$ soit $a' \cdot b' = 360/18 = 20$. On est donc ramené à chercher les couples (a', b') d'entiers naturels tels que $a' \wedge b' = 1$ et $a' \cdot b' = 20$. Ici il est facile de lister toutes les possibilités pour la deuxième condition. On ne retient ensuite que les couples vérifiant la première condition. On trouve (à permutation des composantes près) près $(1, 20)$ et $(4, 5)$, soit pour (a, b) les solutions $(18, 360)$ et $(72, 90)$

Exercice 6.18

Indication. — Pour 6.18.2, on peut bien sûr utiliser Euclide. On peut aussi deviner une formule qui donne le pgcd de deux entiers en fonction de leur décomposition en facteurs premiers.

Pour 6.18.3, on peut le faire à la main ou (plus rapide) raisonner sur la décomposition en facteurs premiers. Il découle des résultats du cours que deux entiers a et b sont premiers entre eux si et seulement si pour tout nombre premier p on a $v_p(a) = 0$ ou $v_p(b) = 0$.

Pour 6.18.4, penser à utiliser la proposition 6.4.4.2 du cours

Éléments de correction. — $51 = 3 \cdot 17$, $72 = 2^3 \cdot 3^2$, $216 = 3 \cdot 72 = 2^3 \cdot 3^3$

$51 \wedge 216 = 3$

Cherchons α et β entiers naturels premiers entre eux tels que $\alpha \cdot \beta = 72 = 2^3 \cdot 3^2$ En particulier, les seuls nombres premiers qui peuvent diviser α et β sont donc 2 et 3. Et comme α et β sont premiers entre eux, 2 ne peut pas diviser simultanément α et β, idem pour 3. Finalement on est dans l'une des situations suivantes :

- 2 et 3 divisent α mais pas β
- 2 divise α mais pas β ; 3 divise β mais pas α
- 3 divise α mais pas β ; 2 divise β mais pas α
- 2 et 3 divisent β mais pas α

Ainsi vu la contrainte $\alpha \cdot \beta = 2^3 \cdot 3^2$ et à permutation des composantes près les couples (α, β) solutions sont $(2^3 \cdot 3^2, 1)$ et $(2^3, 3^2)$

Par un raisonnement analogue, à permutation des composantes près les couples (α, β) d'entiers naturels premiers entre eux tels que $\alpha \cdot \beta = 216 = 2^3 \cdot 3^3$ sont $(2^3 \cdot 3^3, 1)$ et $(2^3, 3^3)$.

Soit d le pgcd de a et b solution de (6.1). Comme d divise a et b, d divise $a+b$, donc d divise 51. Comme d divise a et que $a \vee b$ est un multiple de a, d divise $a \vee b = 216$. Donc d est un diviseur commun de 51 et 216. Par la proposition 6.4.4.2, d divise $51 \wedge 216$.

Comme $51 \wedge 216 = 3$, on en déduit que si a et b est solution de (6.1) alors $a \wedge b = 1$ ou $a \wedge b = 3$.

Supposons $a \wedge b = 1$. Alors $216 = a \vee b = a \cdot b$. D'après 6.18.4, à permutation près on a $(a, b) = (216, 1)$ ou $(a, b) = (8, 27)$. Dans tous les cas $a + b$ n'est pas égal à 51.

Supposons $a \wedge b = 3$ et écrivons $a = 3a'$ et $b = 3b'$. Alors $a' \wedge b' = 1$, et $a' + b' = \frac{51}{3} = 17$. Par ailleurs $a \vee b = \frac{a \cdot b}{a \wedge b} = 3a'b'$ donc $a'b' = \frac{216}{3} = 72$. D'après 6.18.4, à permutation près on a $(a', b') = (72, 1)$ ou $(a', b') = (8, 9)$. soit $(a, b) = (216, 3)$ ou $(a, b) = (24, 27)$. En regardant la somme, on en déduit que l'unique solution de (6.1), à permutation près, est $(24, 27)$

Exercice 6.19

Indication. — On peut éventuellement se rappeler ou redémontrer des critères de divisibilité par 3 et 11.

Éléments de correction. — Les décompositions en facteurs premiers sont $111 = 3 \cdot 37$, $1111 = 11 \cdot 101$, $11111 = 41 \cdot 271$, $111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$

Hormis pour 11111, les critères de divisibilité par 3 ou 11 permettaient de conclure aussitôt à la non primalité (sans factoriser)

Exercice 6.20

Éléments de correction. — $48648 = 2^8 \cdot 3 \cdot 61$, $2379 = 3 \cdot 13 \cdot 61$, $1001 = 7 \cdot 11 \cdot 13$, $2873 = 13^2 \cdot 17$

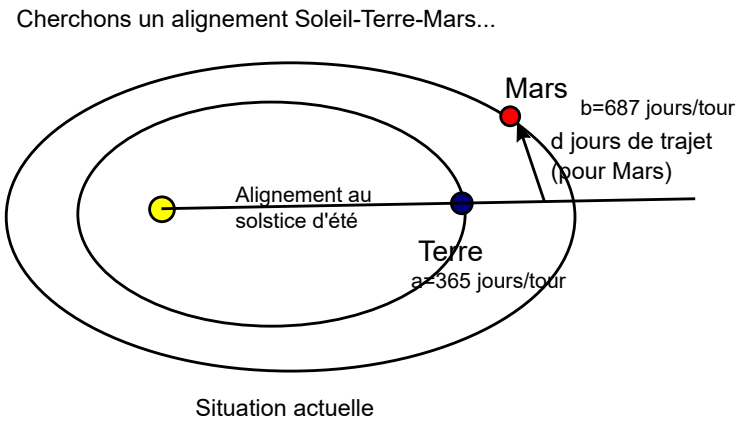
Exercice 6.21

Indication. — Pour 6.21.1 montrer que p divise a^2 et utiliser Euclide

Pour 6.21.2, *cf.* l'indication 1 de 6.13

Éléments de correction. — Comme p divise $a+b$, p divise $a(a+b) = a^2 + ab$ Comme p divise ab et $a^2 + ab$, p divise $a^2 + ab - ab = a^2$. D'après le lemme d'Euclide, p divise a. En échangeant a et b (qui jouent des rôles symétriques dans l'énoncé) on en déduit que p divise b

Exercice d'astronomie



Aujourd'hui, c'est le solstice d'été pour la Terre. J'ai observé qu'il y a 46 jours, Mars était également à son solstice d'été. Je sais que la Terre met 365 jours pour tourner autour du soleil, alors que Mars en met 687. J'ai l'impression d'avoir assez d'éléments pour prédire la prochaine fois que Mars et la Terre connaîtront leurs solstices d'été simultanément, mais quelle équation devrais-je savoir résoudre?

AG1