Université Claude Bernard Lyon 1 — UE Fondamentaux des Mathématiques I
Semestre d'automne 2016-2017

Feuille 5 : Arithmétique

Exercice 1 Montrer que pour tout $n \in \mathbb{N}$:

1. $n(n+1)(n+2)(n+3)$ est divisible par 24,
2. ~~$n(n+1)(n+2)(n+3)(n+4)$ est divisible par 120~~.

Solution

Variante 1. $24 = 2 \cdot 3 \cdot 4$. De quatre nombres consécutifs, un est divisible par 2 et un autre par 4, puisque les résidus modulo 4 sont 0, 1, 2 et 3. Leur produit est donc divisible par 8. De même, de trois nombres consécutifs, un est divisible par trois. Comme 8 et 3 sont premiers entre eux, le produit est divisible par 24.

Variante 2 : le nombre $\frac{n(n+1)(n+2)(n+3)}{24} = \frac{n(n+1)(n+2)(n+3)}{4!} = \binom{n+3}{4}$: il est donc entier.

Exercice 4 Déterminer les couples d'entiers naturels de pgcd 35 et ppcm 210.

Solution

Soient a et b les deux nombres. Alors $a = 35a'$ et $b = 35b'$, $\text{pgcd}(a', b') = 1$ et $a'b' = \frac{210}{35} = 6 = 2 \cdot 3$. Alors on a comme solution pour (a', b') : $(1, 6)$, $(2, 3)$, $(3, 2)$ et $(6, 1)$. Ce qui donne les solutions $(35, 210)$, $(70, 105)$, $(105, 70)$ et $(210, 35)$.

Exercice 4 (suite) Déterminer les couples d'entiers naturels de pgcd 18 et de somme 360. De même avec pgcd 18 et produit 6480.

Solution

1. Soient a et b les deux nombres. Alors $a = 18a'$ et $b = 18b'$, $\text{pgcd}(a', b') = 1$ et $a' + b' = \frac{360}{18} = 20$. Il faut donc écrire 20 come somme de deux entiers premiers entre eux. Ils ne peuvent pas être divisibles par 2 ou 5, ce qui donne les solutions $(1, 19)$, $(3, 17)$, $(7, 13)$ et $(9, 11)$ pour (a', b') ou (b', a'), soit $(18, 342)$, $(54, 306)$, $(126, 234)$ et $(162, 198)$ pour (a, b) ou (b, a).
2. Soient a et b les deux nombres. Alors $a = 18a'$ et $b = 18b'$, $\text{pgcd}(a', b') = 1$ et $a'b' = 6480 = 18^2 \cdot 4 \cdot 5$. Alors on a comme solution pour (a', b') ou (b', a') : $(1, 20)$ et $(4, 5)$, ce qui donne les solutions $(18, 360)$, $(72, 90)$ pour (a, b) ou (b, a).

Exercice 2 Calculer le pgcd de 48 et 210, et de 81 et 237. Dans chaque cas exprimer l'identité de Bézout.

Solution

1. On a $210 = 48 \cdot 4 + 18$; $48 = 18 \cdot 2 + 12$; $18 = 12 + 6$; $12 = 6 \cdot 2$. Ainsi $\text{pgcd}(210, 48) = 6$.
   On remonte : $6 = 18 - 12 = 18 - (48 - 18 \cdot 2) = 18 \cdot 3 - 48 = (210 - 48 \cdot 4) \cdot 3 - 48 = 210 \cdot 3 - 48 \cdot 13$.
2. On a $237 = 81 \cdot 2 + 75$; $81 = 75 + 6$; $75 = 6 \cdot 12 + 3$; $6 = 3 \cdot 2$. Ainsi $\text{pgcd}(237, 81) = 3$.
   On remonte : $3 = 75 - 6 \cdot 12 = 75 - (81 - 75) \cdot 12 = 75 \cdot 13 - 81 \cdot 12 = (237 - 81 \cdot 2) \cdot 13 - 81 \cdot 12 = 237 \cdot 13 - 81 \cdot 38$.

Exercice 3 Calculer par l'algorithme d'Euclide le pgcd de 18480 et 9828. En déduire une écriture de 84 comme combinaison linéaire de 18480 et 9828.

Solution

On travaille avec des résidus de valeur absolue minimale. On a $18480 = 9828 \cdot 2 - 1176$; $9828 = 1176 \cdot 8 + 420$; $1176 = 420 \cdot 3 - 84$; $420 = 84 \cdot 5$. Donc $\text{pgcd}(18480, 9828) = 84$. On remonte :
$84 = 420 \cdot 3 - 1176 = (9828 - 1176 \cdot 8) \cdot 3 - 1176 = 9828 \cdot 3 - 1176 \cdot 25 = 9828 \cdot 3 - (9828 \cdot 2 - 18480) \cdot 25 = 18480 \cdot 25 - 9828 \cdot 47$.

Exercice 16 et 15 Trouver toutes les solutions des systèmes suivants dans $\mathbb{Z}^2$:

$$(a)\ 58x + 21y = 1 \qquad (b)\ 14x + 35y = 21 \qquad (c)\ 637x + 595y = 29$$

Solution

1. On a $58 = 21 \cdot 3 - 5$; $21 = 5 \cdot 4 + 1$. Donc $\text{pgcd}(58, 21) = 1$ et il y a une solution. On remonte : $1 = 21 - 5 \cdot 4 = 21 - (21 \cdot 3 - 58) \cdot 4 = 58 \cdot 4 - 21 \cdot 11$. Les solutions sont $(x, y) \in \{(4 + 21n, -11 - 58n) : n \in \mathbb{Z}\}$.
2. On a $35 = 7 \cdot 5$ et $14 = 7 \cdot 2$. Ainsi $\text{pgcd}(35, 14) = 7$; comme $7 \mid 21$ il y a une solution. En divisant par 7, le système est équivalent à $2x + 5y = 3$. Une solutions évidente est $(4, -1)$. Les solutions sont donc $(x, y) \in \{(4 + 5n, -1 - 2n) : n \in \mathbb{Z}\}$.
3. On a $637 = 595 + 42$; $595 = 42 \cdot 14 + 7$; $42 = 7 \cdot 6$. Donc $\text{pgcd}(637, 595) = 7$; comme $7 \nmid 29$ il n'y a pas de solution.

Exercice 7 Notons $a = 1\,111\,111\,111$ et $b = 123\,456\,789$.

1. Calculer le quotient et le reste de la division euclidienne de a par b.
2. Calculer $p = \text{pgcd}(a, b)$.
3. Déterminer deux entiers relatifs u et v tels que $au + bv = p$.

Solution

1. $10b - b = 1\,111\,101$. Donc $1\,111\,111\,111 = 123\,456\,789 \cdot 9 + 10$.
2. $p = \text{pgcd}(1\,111\,111\,111, 123\,456\,789) = \text{pgcd}(123\,456\,789, 10) = 1$, puisque $123\,456\,789$ est divisible ni par 2 ni par 5.
3. On a $1 = 10 \cdot 12\,345\,679 - 123\,456\,789 = (1\,111\,111\,111 - 123\,456\,789 \cdot 9) \cdot 12\,345\,679 - 123\,456\,789$
$= 1\,111\,111\,111 \cdot 12\,345\,679 - 123\,456\,789 \cdot 111\,111\,112$. On a donc $u = 12\,345\,679$ et $v = 111\,111\,112$.

Exercice 16 Résoudre dans $\mathbb{Z}$: $1665x + 1035y = 45$.

Solution

On divise par 45 : Le système est équivalent à $37x + 23y = 1$. On a $37 = 23 \cdot 2 - 9$; $23 = 9 \cdot 2 + 5$; $9 = 5 \cdot 2 - 1$. Donc $\text{pgcd}(37, 23) = 1$ et il y a une solution. On remonte :
$1 = 5 \cdot 2 - 9 = (23 - 9 \cdot 2) \cdot 2 - 9 = 23 \cdot 2 - 9 \cdot 5 = 23 \cdot 2 - (37 - 23 \cdot 2) \cdot 5 = 37 \cdot 5 - 23 \cdot 8$. Les solutions sont donc $(x, y) \in \{(5 + 23n, -8 - 37n) : n \in \mathbb{Z}\}$.

Exercice 10 Combien 15! admet-il de diviseurs dans $\mathbb{N}$?

Solution

On décompose 15! en facteurs premiers. On constate aisément que ses facteurs seront exactement $2, 3, 5, 7, 11, 13$. De 1 à 15, il y a 7 nombres pairs. Donc 2 apparaît au moins 7 fois. Il y a aussi 3 multiples de $2^2 = 4$. Donc 2 apparaît 3 fois de plus (au moins 10 fois). Il y a aussi 1 multiple de $2^3 = 8$. Donc 2 apparaît 1 fois de plus (au moins 11 fois). Il n'y a pas de multiples de plus grandes puissances de 2. Donc 2 apparaît exactement 11 fois. On fait de même avec 3 : il y a 5 multiples de 3, 1 seul multiple de $3^2 = 9$, et pas de puissance plus grande, donc 3 apparaît exactement 6 fois. Avec ce raisonnement, 5 apparaît exactement 3 fois, 7 apparaît exactement 2 fois, 11 et 13 apparaîssent exactement 1 fois chacun.
Donc $15! = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$. Ainsi, il y a $12 \cdot 7 \cdot 4 \cdot 3 \cdot 2 \cdot 2$ possibilités pour les diviseurs positifs. On en déduit que 15! a 4032 diviseurs positifs.

Exercice 5 Démontrer que, si a et b sont des entiers premiers entre eux, il en est de même des entiers $a + b$ et ab.

Solution

D'abord, on remarque que si a et b sont premiers entre eux, aussi a^2 et b^2 le sont.
Soit d un diviseur commun de ab et de $a + b$. Alors d divise $a(a + b) - ab = a^2$. De même d divise b^2. D'après la remarque précédente, les entiers a^2 et b^2 sont premiers entre eux. Ainsi $d = \pm 1$, ce qui conclut.

Exercice 14 Soient a, b des entiers supérieurs ou égaux à 1. Montrer :

1. $(2^a - 1) | (2^{ab} - 1)$;
2. $2^p - 1$ premier $\Rightarrow$ p premier ;
3. ~~$\text{pgcd}(2^a - 1, 2^b - 1) = 2^{\text{pgcd}(a,b)} - 1$.~~

Solution

1. $(2^{ab} - 1) = (2^a - 1)(2^{ab-a} + 2^{ab-2a} + \ldots + 2^a + 1)$.

Exercice 6 : on va montrer par récurrence l'énoncé

(H_n) « u_n et u_{n+1} sont premiers entre eux »

* Pour $n=0$ $u_0 = a$ et $u_1 = b$ sont premiers entre eux par hypothèse

* Soit $n \geq 0$, supposons (H_n)

Soit alors $d \geq 1$ un diviseur commun à u_{n+1} et $u_{n+2} = u_{n+1} + u_n$

Comme d divise u_{n+1} et u_{n+2}, il divise $u_{n+2} - u_{n+1} = u_n$. C'est donc un diviseur (positif) commun de u_n et u_{n+1}, qui sont premiers entre eux via (H_n).

Donc $d = 1$

Ceci prouve (H_{n+1})

Par le principe de récurrence, (H_n) est vraie pour tout $n \geq 0$.

Exercice 8 Un entier $n \in \mathbb{N}$ peut être congru modulo 4 à $0, \pm 1$ ou 2

Son carré n^2 peut donc être congru à $0, 1$ ou $4 \equiv 0$.

Dans les deux cas extrêmes, n^2 est divisible par 4 donc fournit le reste 0

Dans le cas central, n^2 fournit le reste 1

Les restes possibles sont 0 et 1

Si maintenant un $n \in \mathbb{N}$ est somme de carrés, notons $a, b \in \mathbb{N}$ 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 9 Soit $n \in \mathbb{N}$

Modulo 7, $3^{2n} - 2^n = 9^n - 2^n \equiv 2^n - 2^n = 0$. Donc 7 divise $3^{2n} - 2^n$.

Exercice 10 Soit $n \in \mathbb{N}$

Modulo 8, $7^n + 1 \equiv (-1)^n + 1 = \begin{cases} 0 & \text{si } n \text{ est impair} \\ 2 & \text{si } n \text{ est pair} \end{cases}$

Exercice 11 Modulo 13, $100^{1000} \equiv 9^{1000}$

Par le "petit théorème de Fermat", $9^{12} \equiv 1$ [13] donc $9^{1000} = 9^{996+4}$

$= (9^{12})^{83} \times 9^4 \equiv 9^4 = 81^2 \equiv 3^2 = 9$ [13]. Le reste cherché est 9.

[Variante : $9^2 - 81 \equiv 3$ [13] puis $9^3 = 9^2 \times 9 \equiv 3 \times 9 = 27 \equiv 1$ [13]

et enfin $9^{1000} = 9^{999} \times 9 = (9^3)^{333} \times 9 \equiv 9$ [13]]

Exercice 12 1) Si n est impair, $n \equiv \pm 1$ ou $n \equiv \pm 3$ [8]
donc $n^2 \equiv 1$ ou $n^2 \equiv 9 \equiv 1$ [8]

2) Si n est pair, $n \equiv 0$ ou $n \equiv \pm 2$ ou $n \equiv 4$ [8]
donc $n^2 \equiv 0$ ou $n^2 \equiv 4$ ou $n^2 \equiv 16 \equiv 0$ [8]

3) i) $a+b+c$ est lui aussi impair donc $(a+b+c)^2 \equiv 1$ [8]
tandis que $a^2+b^2+c^2 \equiv 1+1+1 = 3$ [8]. On en déduit que
$2(ab+ac+bc) = (a+b+c)^2 - (a^2+b^2+c^2) \equiv 1-3 \equiv 6$ [8]

ii) Soit $n \in \mathbb{N}$. Par les questions 1 et 2, $2n^2 \equiv 2$ ou 0 [8]
Il n'est donc pas congru à $2(ab+bc+ca)$ et, a fortiori, $n^2 \neq ab+bc+ca$

Exercice 13

1) $2^n = 2^3 2^{n-3} \equiv 0 \times 2^{n-3} = 0$ [8]
* Si n est pair, notons $n = 2k$. Alors $2^n - 3^n \equiv 0 - 9^k \equiv -1^k = -1 \neq 1$ [8]
* Si n est impair, notons $n = 2k+1$. Alors $2^n - 3^n \equiv 0 - 3 \times 9^k \equiv -3 \neq 1$ [8]
Dans les deux cas $2^n - 3^n \neq 1$

2) Pour $m = 0$ et tout $n \in \mathbb{N}$ $2^m - 3^n = 1 - 3^n \leq 0$ donc $2^m - 3^n \neq 1$
Pour $m = 1$ et tout $n \in \mathbb{N}$ $2^m - 3^n = 1 \iff 2 - 3^n = 1 \iff 3^n = 1 \iff n = 0$
Pour $m = 2$ et tout $n \in \mathbb{N}$ $2^m - 3^n = 1 \iff 4 - 3^n = 1 \iff 3^n = 3 \iff n = 1$
Les solutions sont $(1,0)$ et $(2,1)$.

Exercice 14 $x = -2$ saute aux yeux. Pour $x \in \mathbb{Z}$, $5x \equiv 0$ [11] $\iff 11 \mid 5x \iff 11 \mid x$ (lemme de Gauss).
Les solutions sont donc les $11k$, $k \in \mathbb{Z}$. Soit $x \in \mathbb{Z}$: $5x \equiv 1$ [11] $\iff 5x \equiv 5 \times (-2)$ [11]
$\iff 5(x+2) \equiv 0$ [11] $\iff \exists k \in \mathbb{Z}$, $x+2 = 11k \iff \exists k \in \mathbb{Z}$, $x = -2 + 11k$

Exercice 15: par recherche d'une identité de Bézout (via algorithme d'Euclide) on trouve par exemple la solution $(4, -11)$. Soit $(x,y) \in \mathbb{Z}^2$: $58x + 21y = 0 \iff 58x = -21y$ (*)
Par le lemme de Gauss, si (x,y) vérifie (*) 21 divise x: notons $x = 21k$ on obtient
$58 \times 21 \times k = -21 \times y$ donc $y = -58k$. Réciproquement il est clair que pour tout $k \in \mathbb{Z}$
$(21k, -58k)$ est solution de (*).
Soit $(x,y) \in \mathbb{Z}^2$: $58x + 21y = 1 \iff 58x + 21y = 58 \times 4 - 21 \times 11 \iff 58(x-4) + 21(y+11) = 0$
$\iff \exists k \in \mathbb{Z}$ $\begin{cases} x - 4 = 21k \\ y + 11 = -58k \end{cases} \iff \exists k \in \mathbb{Z}$, $(x,y) = (21k+4, -58k-11)$.

Exercice 17 en tâtonnant on remarque que $n = -6$ est solution de (S)
Soit $n \in \mathbb{Z}$, $(S_n) \iff n$ multiple commun de 19 et 12 $\iff n$ multiple de $\text{ppcm}(19,12) = 228$
Soit $n \in \mathbb{Z}$, $(S) \iff \begin{cases} n \equiv -6 & [19] \\ n \equiv -6 & [12] \end{cases} \iff \begin{cases} n+6 \equiv 0 & [19] \\ n+6 \equiv 0 & [12] \end{cases} \iff \exists k \in \mathbb{Z}$, $n+6 = 228k$
$\iff \exists k \in \mathbb{Z}$, $n = 228k - 6$

Exercice 18 : 1) On peut trouver $5\times 7 - 2\times 17 = 35 - 34 = 1$

2) Au vu du 1 on remarque que 35 est solution de $(\mathcal{S}_1)$ et -34 de $(\mathcal{S}_2)$ puis que $35a - 34b$ est solution de $(\mathcal{S})$

On fait comme à l'exercice précédent : les solutions de $(\mathcal{S}_0)$ sont les $119k$, $k\in\mathbb{Z}$ puis celles de $(\mathcal{S})$ sont les $119k + 35a - 34b$, $k\in\mathbb{Z}$

Exercice 19 : 1) $3\in X$

2) Si $a_1, \dots, a_n \in \mathbb{Z}$ et sont tous congrus à 1 modulo 4, leur produit est congru à $1^n = 1$ modulo 4, donc de la forme $4k+1$

3) On remarque d'abord que $a = 4p_1p_2\cdots p_n - 1 \equiv 0 - 1 = -1 \equiv 3\ [4]$

Il est donc impair, donc tous ses facteurs premiers le sont aussi.

Or le 2) ils ne peuvent tous être de la forme $4k+1$ car si tel était le cas, a serait lui-même congru à 1 modulo 4.

L'un au moins de ces facteurs premiers est de la forme $4k+3$.

4) Pour tout $i\in\{1,\dots,n\}$, $a \equiv -1\ [p_i]$ donc p_i ne divise pas a.

Donc aucun élément de X ne divise a

Pourtant on a vu au 3) qu'un élément de X au moins divise a.

Cela est totalement absurde. On était donc dans l'erreur en supposant X fini : il ne l'est pas.

Exercice 20* Soit $a \in \mathbb{N}$ tel que $a^n + 1$ soit premier. Montrer que n est de la forme $n = 2^k$ pour un entier $k \in \mathbb{N}$. Que penser de la conjecture : $2^{2^n} + 1$ est premier pour tout entier $n \in \mathbb{N}$?

Solution

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, $a^n + 1 = (b+1)(b^{m-1} - b^{m-2} + \cdots - b + 1)$. Absurde car $a^n + 1$ est premier. Donc $m = 1$, et ainsi $n = 2^k$. Ceci ne nous dit pas, *a 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 21

Solution

1. Il faut faire la récurrence sur k.
   Initialisation : $(2^{2^n}-1)(2^{2^n}+1) = (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1$.
   Hérédité : Supposons la propriété vraie en un k fixé. Alors
   $\left(2^{2^n}-1\right) \cdot \prod_{i=0}^{k} \left(2^{2^{n+i}}+1\right) = (2^{2^{n+k}}+1)(2^{2^n}-1) \cdot \prod_{i=0}^{k-1} \left(2^{2^{n+i}}+1\right) = (2^{2^{n+k}}+1)(2^{2^{n+k}}-1)$.
   Et $(2^{2^{n+k}}+1)(2^{2^{n+k}}-1) = (2^{2^{n+k}})^2 - 1 = 2^{2^{n+k+1}} - 1$. D'où le résultat.
2. Par l'absurde, on suppose qu'il existe $n < m$ tels que F_n et F_m ne sont pas premiers entre eux. On pose $k = m - n \in \mathbb{N}^\times$ pour avoir $m = n + k$. Il existe p premier tel que $p|F_n$ et $p|F_{n+k}$. Comme $p|2^{2^n}+1$, par 1., on a $p|2^{2^{n+k}} - 1$. Or $p|2^{2^{n+k}} + 1$, donc $p|2$, donc $p = 2$. Absurde car F_n est impair.
3. $F_n \geq 2$, donc il existe p_n premier tel que $p_n|F_n$. D'après 2., pour $m \neq n$, $p_m \neq p_n$. Ainsi, il existe une infinité de nombres premiers (les p_n).

Exercice 22 Donner la valeur en base dix des nombres suivants :

1. $(110101001)_2$;
2. $(110101001)_3$;
3. $(1367)_8$;
4. $(1402)_5$.

Solution

1. $2^8 + 2^7 + 2^5 + 2^3 + 1 = 425$
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 23 Écrire les nombres suivants (donnés en base dix) dans la base cible indiquée.

1. 255 en base deux ;
2. 1907 en base seize ;
3. 2016 en base sept ;
4. 2000 en base deux mille.

Solution

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 : $1907 = \mathbf{7} \cdot 256 + 115$. Puis on effectue la division euclidienne de 115 par 16 : $115 = \mathbf{7} \cdot 16 + \mathbf{3}$. Donc $1907 = (\mathbf{773})_{16}$.
3. On estime aisément que $7^3 < 2016 < 7^4$. On calcule $7^3 = 343$. On effectue la division euclidienne de 2016 par 343 : $2016 = \mathbf{5} \cdot 343 + 301$. Puis on effectue la division euclidienne de 301 par $7^2 = 49$: $301 = \mathbf{6} \cdot 49 + 7$. Et $7 = (\mathbf{10})_7$. Donc $2016 = (\mathbf{5610})_7$.
4. $2000 = (10)_{2000}$