Corrigé planche 2
Arithmétique

2.1 Divisibilité

Exercice 52 (*Division euclidienne dans* $\mathbb{Z}$)

Montrer que pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que

$$a = bq + r \quad et \quad 0 \leqslant r < |b|.$$

Solution : On commence par montrer l'existence de q et r en considérant différents cas. Si $a, b \in \mathbb{N}$, l'existence a été montrée dans le cours et on va l'exploiter pour montrer les autres cas.

Supposons d'abord $a \in \mathbb{N}$ et $b < 0$. Dans ce cas on a $-b = |b| > 0$ et le resultat du cours dit qu'il existe $a \in \mathbb{N} \subset \mathbb{Z}$ et $r \in \mathbb{N}$ tels que $0 \leqslant q < |b|$ et $a = q|b| + r = (-q)(-|b|) + r = (-q)b + r$, ce qui montre qu'on peut prendre $-q$ comme quotient et r comme reste.

Supposons maintenant $a < 0$ et $b \in \mathbb{Z}^*$. D'après les cas déjà vus on est capable de diviser $|a|$ par b : il existe $q_1 \in \mathbb{Z}$ et $r_1 \in \mathbb{N}$ tels que $|a| = q_1 b + r_1$ avec $0 \leqslant r_1 < |b|$. On a alors $a = -|a| = (-q_1)b - r_1$. Si $r_1 = 0$ il suffit de prendre $-q_1$ comme quotient et 0 comme reste. Si cela n'est pas le cas, on a $-|b| < -r_1 < 0$. En sommant $|b|$ à chaque terme de l'inégalité on obtient $0 < |b| - r_1 < |b|$. On peut alors écrire $a = (-q_1)b - |b| + (|b| - r_1) = (-q_1 - \epsilon)b + (|b| - r_1)$, où $\epsilon \in \{\pm 1\}$ est tel que $b = \epsilon|b|$. Dans ce cas il suffit alors de choisir $q = -q_1 - \epsilon \in \mathbb{Z}$ et $r = |b| - r_1$.

Puique cette analyse couvre tous les cas possibles, cela montre l'existence. La preuve de l'unicité est identique à celle vue en cours pour les naturels. Supposons que le couple $(q', r') \in \mathbb{Z} \times \mathbb{N}$ vérifie aussi $a = bq' + r'$ et $0 \leqslant r' < |b|$. On a $0 = a - a = b(q - q') + r - r'$ ce qui dit que b divise $r - r'$. Puisque $-|b| < r - r' < |b|$, $r - r' = 0$ qui est l'unique multiple de b compris entre $1 - |b|$ et $|b| - 1$. On voit alors que $b(q - q') = 0$ et, puisque $b \neq 0$ nécessairement $q = q'$. ■

Exercice⋆ 53

Déterminer les triplets $(a, b, c) \in (\mathbb{N}^*)^3$ vérifiant les trois conditions suivantes :

(i) $\text{ppcm}(a, b) = 42$ *(ii)* $\text{pgcd}(a, c) = 3$ *(iii)* $a + b + c = 29$.

Solution : On commence par expliciter l'information contenue dans les conditions données. (i) dit que a et b sont des diviseurs de 42, à savoir parmi les nombres 1, 2, 3, 6, 7, 14, 21, 42. (ii) dit que a et c sont divisibles par 3 ; en particulier a ne peut être que 3, 6, 21 ou 42. (iii) dit que les nombres sont tous $\leqslant 29$ (en particulier on ne peut pas avoir $a = 42$) ; de plus, puisque a et c sont divisibles par 3 mais 29 ne l'est pas, b n'est peut pas être divisible par 3.

On va maintenant étudier différents cas selon les possibles valeurs de a.

$a = 3$ Puisque b n'est pas divisible par 3, on a $\text{pgcd}(a, b) = 1$. La relation $ab = \text{pgcd}(a, b)\,\text{ppcm}(a, b) = 42$ permet de calculer $b = 14$. (iii) dit alors que $c = 12$. Puisque $\text{pgcd}(a, c) = 3$, on obtient un premier triplet $(3, 14, 12)$.

$a = 6$ Dans ce cas on a deux possibilités pour $\text{pgcd}(a, b)$: $\text{pgcd}(a, b) = 1$ ou $\text{pgcd}(a, b) = 2$ qui sont les diviseurs de a premiers avec 3. On peut raisonner comme au point précédent et voir que dans le premier cas on doit avoir $b = 7$ et $c = 16$ et dans le deuxième $b = 14$ et $c = 9$. Le premier triplet ne convient pas car $\text{pgcd}(a, c) = 1$, tandis que le deuxième est acceptable. On obtient donc $(6, 14, 9)$ dans ce cas.

$a = 21$ Dans ce cas on a encore une fois deux possibilités pour $\text{pgcd}(a, b)$: $\text{pgcd}(a, b) = 1$ ou $\text{pgcd}(a, b) = 7$. Dans le premier cas on doit avoir $b = 2$ et $c = 6$. Dans le deuxième $b = 14$: la somme $a+b = 35 > 29$ montre que cette possibilité ne peut pas arriver. En revanche, puisque $\text{pgcd}(21, 6) = 3$, le premier triplet est bien une solution.

En conclusion les triplets satisfaisant les trois conditions sont précisément $(3, 14, 12)$, $(6, 14, 9)$ et $(21, 2, 6)$. ■

Exercice⋆ 54

Sachant que $96842 = 256 \times 375 + 842$, *déterminer le reste de la division du nombre 96842 par chacun des nombres 256 et 375.*

Solution : Pour cela il suffit de calculer les restes des divisions de 842 par les deux nombres données. On a $842 = 3 \times 256 + 74$ et $842 = 2 \times 375 + 92$, et donc $96842 = 378 \times 256 + 74$ et $96842 = 258 \times 375 + 92$. Le premier reste vaut 74 et le deuxième 92. ■

Exercice⋆ 55

1. *Déterminer le pgcd de 4147 et 10672. Déterminer le* ppcm *de 4235 et 2156.*
2. *Donner une relation de Bezout pour :*

   a. 7 et 9, *b. 36 et 45,* *c. 41 et 93,* *d. 33 et 55.*

Solution : 1. On peut calculer le pgcd de différentes façons. On peut utiliser l'algorithme d'Euclide, mais ici on va plutôt trouver à la main les diviseurs communs aux deux nombres. On commence par chercher les diviseurs de 4147. D'après le critères de divisibilité, 2, 3 et 5 ne le divisent pas. En revanche 11 le divise et on a $4147 = 11 \times 377$. Puisque $377 < 20^2$, si 377 a des diviseurs propres, il doit en avoir parmi 7, 13, 17 et 19, car on voit que 11 ne le divise pas. On teste les différentes possibilités et on constate que $377 = 13 \times 29$. On s'intéresse maintenant à 10672 qui est pair et même divisible par 4. On voit qu'on a $10672 = 2^4 \times 667$. Il découle du lemme de Gauss que les deux nombres ont des diviseurs communs > 1 si et seulement si au moins un parmi 11, 13 et 29 divise 667. On teste les différentes possibilités et on voit que $667 = 29 \times 23$. Par conséquent $\text{pgcd}(4147, 10672) = 29$.

On raisonne de manière analogue pour trouver le ppcm de 4235 et 2156. On a $4235 = 5 \times 7 \times 11^2$ et $2156 = 2^2 \times 7^2 \times 11$. On a alors $\text{ppcm}(4235, 2156) = 2^2 \times 5 \times 7^2 \times 11^2 = 118580$.

2. Pour trouver des relations de Bézout on peut utiliser encore une fois l'algorithme d'Euclide. Parfois on peut trouver des nombres de Bézout sans faire de calculs.

   a. $4 \times 7 - 3 \times 9 = 1$,
   b. $-1 \times 36 + 1 \times 45 = 9$,
   c. $15 \times 93 - 34 \times 41 = 1$,
   d. $2 \times 33 - 1 \times 55 = 11$.

   Pour le troisième cas, on utilise l'algorithme d'Euclide qui donne

$$93 = 2 \times 41 + 1$$
$$41 = 3 \times 11 + 8$$
$$11 = 1 \times 8 + 3$$
$$8 = 2 \times 3 + 2$$
$$3 = 2 + 1$$

   et donc $1 = 3-2 = 3-(8-2\times3) = 3\times3-8 = 3(11-8)-8 = 3\times11-4\times8 = 3\times11-4(41-3\times11) = 15 \times 11 - 4 \times 41 = 15(93 - 2 \times 41) - 4 \times 41$. ■

Exercice⋆ 56

Soit $a, b \in \mathbb{Z}^*$. *Montrer que* $\text{pgcd}(a, b) = \text{pgcd}(a, a^2 + b) = \text{pgcd}(a + b, 3a + 2b)$.

Solution : Pour cela il suffit de montrer que les trois paires de nombres ont les mêmes diviseurs communs, d'après la définition de pgcd.

Soit d un diviseur commun à a et b : il existe $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$. On voit alors que d divise $a = da'$, $a^2 + b = (aa' + b')d$, $a + b = d(a' + b')$ et $3a + 2b = (3a' + 2b')$. Cela montre que les diviseurs communs à la première paire sont des diviseurs communs aux deux autres.

Supposons maintenant que c est un diviseur commun à a et $a^2 + b$. Il est alors aussi un diviseur commun à a et à $b = (a^2 + b) - (a)a$. Cela montre que les diviseurs communs à la deuxième paire le sont aussi pour la première.

Supposons maintenant que k est un diviseur commun à $a+b$ et $3a+2b$. Il est alors aussi un diviseur commun à $a = (3a + 2b) - 2(a + b)$ et à $b = 3(a + b) - (3a + 2b)$. Cela montre que les diviseurs communs à la troisième paire le sont aussi pour la première. ■

Exercice 57

Notons $a = 1111111111$ et $b = 123456789$.

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. On a $a = 9b + 10$, à savoir $1111111111 = 9 \times 123456789 + 10$.
2. Puisque le pgcd de a et b est le même que celui de b et du reste $10 = 2 \times 5$ on voit que $\text{pgcd}(a, b) = 1$ car ni 2 ni 5 ne divisent b.
3. On exploite l'algorithme d'Euclide : $b = 12345678 \times 10 + 9$ et $10 = 9 + 1$. Cela permet de trouver les nombres de Bézout : en posant $c = 12345678$ on a $(c+1)a-(9c+10) = 12345679a-111111112b = 1$. ■

Exercice 58

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

Solution : On va montrer la contraposée : si $a + b$ et ab ont un diviseur > 1 en commun, alors a et b aussi. Si $a + b$ et ab ont un diviseur > 1 en commun, ils doivent avoir un diviseur commun qui est un nombre premier p. Le lemme de Gauss dit alors que p doit diviser a ou b. Sans perte de généralité, quitte à échanger a et b, on peut supposer que p divise a. Puisque p divise $a+b$ il doit aussi diviser $b = (a+b)-a$.

On remarque que la réciproque de cette implication est aussi vraie, car tout diviseur commun à a et b est aussi un diviseur de $a + b$ et de ab. ■

Exercice⋆ 59

Soit $n \in \mathbb{N}$.

1. *Montrer que $n(n + 1)$ est divisible par 2.*
2. *Montrer que $n(n + 1)(n + 2)$ est divisible par 6.*
3. *Montrer que $n(n + 1)(n + 2)(n + 3)$ est divisible par 24.*

Solution :

1. Parmi deux entiers consécutifs il y en a un qui est pair et l'autre qui est impair. Leur produit est donc pair. On peut aussi raisonner en considérant les deux cas $n = 2k$ pair et $n = 2k+1$ impair. Dans le premier cas on a $n(n + 1) = 2(kn + k)$ et dans le deuxième $n(n + 1) = 2(nk + n)$.
2. Parmi trois nombres consécutifs il y en a nécessairement un qui est divisible par 3. Cela dit que $n(n + 1)(n + 2)$ est divisible par 3. Cela se voit en considérant les possibles restes de la division euclidienne de n par 3. Le premier point dit de plus que $n(n + 1)(n + 2)$ est pair. Puisque 2 et 3 sont premiers entre eux, le lemme de Gauss permet de dire que 6 divise $n(n + 1)(n + 2)$.
3. Parmi quatre nombres consécutifs il y en a deux paires dont un un multiple de 4. Encore une fois, on voit cela en considérant tous les possibles restes de la division euclidienne de n par 4. Cela assure que $n(n+1)(n+2)(n+3)$ est divisible par 8. Le point précédent assure que $n(n+1)(n+2)(n+3)$ est divisible par 3. Puisque $\text{pgcd}(8, 3) = 1$ le lemme de Gauss permet de conclure encore une fois. ■

Exercice⋆ 60 (*Une exemple d'équation diophantienne*)

Soient a, b, $c \in \mathbb{Z}$, avec $a, b \neq 0$. Considérons l'équation $ax + by = c$ où x et y sont des inconnues que l'on cherche parmi les entiers. Montrer que :

i) Cette équation a des solutions entières si et seulement si $\operatorname{pgcd}(a, b)$ divise c.

ii) Si cette équation admet (x_0, y_0) pour solution, alors l'ensemble des solutions de cette équation est

$$\left\{(x, y) \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z},\ (x, y) = \left(x_0 + kb', y_0 - ka'\right)\right\}$$

où $a', b' \in \mathbb{Z}$ sont tels que $a = a' \operatorname{pgcd}(a, b)$ et $b = b' \operatorname{pgcd}(a, b)$.

Solution : i) La preuve de cette assertion suit les mêmes idées de la preuve du théorème de Bézout. Tout d'abord observons que si d est un diviseur commun à a et b, il existe $a_1, b_1 \in \mathbb{Z}$ tels que $a = da_1$ et $b = db_1$. On peut alors écrire $c = ax + by = d(a_1x + b_1y)$. Cela montre que si l'équation a une solution tout diviseur commun à a et b, en particulier $\operatorname{pgcd}(a, b)$, doit diviser c.
Il reste à montrer la réciproque. On commence par remarquer que l'équation $ax + by = c$ a une solution si et seulement si l'équation $\epsilon_a az + \epsilon_b bt = c$, où $\epsilon_a, \epsilon_b \in \{\pm 1\}$, en a une. En effet (x_0, y_0) est solution de la première équation si et seulement si $(\epsilon_a x_0, \epsilon_b y_0)$ est solution de la deuxième. Cette remarque assure qu'on peut supposer $a, b > 0$. On peut alors appliquer directement le théorème de Bézout comme montré dans le cours : il existe $u_0, v_0 \in \mathbb{Z}$ tels que $au_0 + bv_0 = \operatorname{pgcd}(a, b)$. Si $\operatorname{pgcd}(a, b)$ divise c, il existe $h \in \mathbb{Z}$ tel que $c = h \operatorname{pgcd}(a, b)$. On multiplie alors l'identité de Bézout par h et on obtient $ahu_0 + bhv_0 = h \operatorname{pgcd}(a, b) = c$, ce qui montre que l'équation admet une solution $(x_0 = hu_0, y_0 = bhv_0)$.

ii) Supposons maintenant de savoir que l'équation admet une solution (x_0, y_0) et soit (x, y) une autre solution. On doit avoir $ax + by = c = ax_0 + by_0$ et donc $a(x - x_0) = b(y_0 - y)$. En utilisant la notation de l'énoncé on a $a' \operatorname{pgcd}(a, b)(x - x_0) = b' \operatorname{pgcd}(a, b)(y_0 - y)$. Puisque $\operatorname{pgcd}(a, b) \neq 0$, on peut simplifier les deux membres par $\operatorname{pgcd}(a, b)$ et on a $a'(x - x_0) = b'(y_0 - y)$, avec $\operatorname{pgcd}(a', b') = 1$. Puisque a' et b' sont premiers entre eux, le lemme de Gauss dit que a' doit diviser $y_0 - y$. Il existe donc $k \in \mathbb{Z}$ tel que $y_0 - y = ka'$. En remplaçant on obtient $a'(x - x_0) = b'a'k$. Encore une fois on peut simplifier par $a' \neq 0$ et on obtient $x - x_0 = kb'$. Cela dit que $x = x_0 + kb'$ et $y = y_0 - ka'$. Cela montre que toute solution doit être de la forme donnée. Réciproquement, en remplaçant dans l'équation on voit que tout couple de la forme $(x_0 + kb', y_0 - ka')$ est bien une solution. ■

Exercice⋆ 61

Trouver les solutions $(x, y) \in \mathbb{Z}^2$ des équations suivantes :

1. $7x - 11y = 6$.
2. $95x + 71y = 46$.
3. $20x - 53y = 3$.
4. $1665x + 1035y = 45$.

Solution : On va appliquer le résultat de l'exercice 60.

1. Les nombres 7 et 11 sont premiers entre eux et on a l'identité de Bézout $7 \times (-3) - 11 \times (-2) = 1$. En multipliant par 6 on obtient $7 \times (-18) - 11 \times (-12) = 6$. Cela donne une solution particulière $(x_0 = -18, y_0 = -12)$ de l'équation $7x - 11y = 6$. L'ensemble des solutions est alors $\{(x, y) \in \mathbb{Z}^2 \mid \exists k \in \mathbb{N},\ x = -18 + 11k,\ y = -12 + 7k\}$.
2. L'algorithme d'Euclide permet de trouver une identité de Bézout : $95 \times 3 + 71 \times (-4) = 1$. Comme au point précédent, cela permet de trouver une solution particulière $(x_0 = 138, y_0 = -184)$ de l'équation $95x + 71y = 46$. L'ensemble des solutions est alors $\{(x, y) \in \mathbb{Z}^2 \mid \exists k \in \mathbb{N},\ x = 136 + 71k,\ y = -184 - 95k\}$.
3. Comme dans le cas précédent on calcule une identité de Bézout : $20 \times 8 - 53 \times 3 = 1$. On voit alors qu'une solution particulière de l'équation $20x - 53y = 3$ est $(x_0 = 24, y_0 = 9)$. Cela permet de donner l'ensembe des solutions : $\{(x, y) \in \mathbb{Z}^2 \mid \exists k \in \mathbb{N},\ x = 24 + 53k,\ y = 9 + 20k\}$.
4. On commence par remarquer que 45 divise tous les coefficients de l'équation $1665x + 1035y = 45$: $45 \times 37x + 45 \times 23y = 45$. L'équation donnée est donc équivalene à $37x + 23y = 1$. On calcule une identité de Bézout : $37 \times 5 + 23 \times (-8) = 1$ ce qui donne directement une solution particulière $(x_0 = 5, y_0 = -8)$. L'ensemble des solutions est : $\{(x, y) \in \mathbb{Z}^2 \mid \exists k \in \mathbb{N},\ x = 5 + 23k,\ y = -8 - 37k\}$. ■

2.2 Nombres premiers

Exercice⋆ 62

On définit la suite $(F_n)_{n\in\mathbb{N}}$ de Fibonacci par $F_0 = F_1 = 1$ et $F_{n+1} = F_n + F_{n-1}$.

1. *Déterminer les dix premiers termes de la suite.*
2. *Montrer que F_n est pair si et seulement si 3 divise $n+1$.*
3. *Montrer que deux termes consécutifs sont toujours premiers entre eux.*

Solution : 1. On a $F_0 = 1$, $F_1 = 1$, $F_2 = 2$, $F_3 = 3$, $F_4 = 5$, $F_5 = 8$, $F_6 = 13$, $F_7 = 21$, $F_8 = 34$ et $F_9 = 55$.

2. L'assertion est équivalente à "F_n est pair si 3 divise $n+1$ et impair sinon". On va la montrer par récurrence sur n. Puisque la relation $F_{n+1} = F_n + F_{n-1}$ n'est valable que pour $n \geqslant 1$, dans l'initialisaton on doit montrer $n = 0$ et $n = 1$. Dans les deux cas on a $n+1$ non divisible par 3 et $F_0 = F_1 = 1$ impair. Supposons alors la propriété vraie pour tout naturel juqu'à $n \geqslant 1$ et montrons-la pour $n+1$. On a trois cas à considérer selon le reste de la division euclidienne de $n+2$ par 3 :

$n+2 = 3k$ Si 3 divise $n+2$, il ne divise pas $n+1$ ou n. Par hypothèse de récurrence, F_n et F_{n-1} sont impairs. Leur somme, F_{n+1}, est donc paire et l'assertion est vraie dans ce cas.

$n+2 = 3k+1$ Dans ce cas 3 divise $n+1$ et donc, par hypothèse de récurrence, F_n est pair tandis que F_{n-1} est impair. On a donc F_{n+1} impair et $(n+1)+1$ non divisible par 3 : l'assertion est vraie dans ce cas.

$n+2 = 3k+2$ Dans ce cas 3 divise n et donc, par hypothèse de récurrence, F_{n-1} est pair tandis que F_n est impair. On a donc F_{n+1} impair et $(n+1)+1$ non divisible par 3 : l'assertion est vraie dans ce cas aussi.

Ceci achève la preuve de la récurrence.

3. On va prouver l'assertion par l'absurde. Supposons qu'il existe deux termes consécutifs, F_m et F_{m+1}, qui ne sont pas premiers entre eux. Considèrons le sous-ensemble $A \subset \mathbb{N}$ des naturels tels que F_n et F_{n+1} ne sont pas premiers entre eux. Puisque $m \in A$, A est non vide. L'axiome du bon ordre assure que A admet un minimum k. Puisque $F_0 = F_1 = 1$, F_0 et $F_1 = 1$ sont premiers entre eux, $0 \notin A$ et $k \geqslant 1$. De ce fait $k-1 \in \mathbb{N}$ et on peut écrire $F_{k-1} = F_{k+1} - F_k$. Cette égalité dit que tout diviseur commun à F_k et F_{k+1} est aussi un diviseur de F_{k-1}. Cela assure que puisque F_k et F_{k+1} ne sont pas premiers entre eux, F_{k-1} et F_k non plus, ce qui contredit le fait que k est le minimum de A. A doit être donc vide, ce qui montre l'assertion. ■

Exercice⋆ 63

Pour des entiers x, $y \in \mathbb{N}^*$ on note $P(x,y)$ la proposition

"x divise y".

Soit $Q(y)$ la proposition

$$\forall x \in \mathbb{N}^*(P(x,y) \Longrightarrow (x = y \text{ ou } x = 1)).$$

1. *Déterminer si $Q(y)$ est vraie pour $y = 1, 2, 3, 4$ et 5.*
2. *Déterminer l'ensemble $\{y \in \mathbb{N}^* \mid Q(y) \text{ est vraie }\}$*

Solution : L'assertion dit que si x divise y alors $x = 1$ ou $x = y$. En d'autres termes, les seuls diviseurs d'y sont 1 et lui-même. On en déduit :

1. $Q(y)$ est vraie pour $y = 1, 2, 3$ et 5, mais fausse pour $y = 4$ qui admet $x = 2 \neq 1, 4$ comme diviseur.
2. L'ensemble $\{y \in \mathbb{N}^* \mid Q(y) \text{ est vraie }\}$ est égal à l'ensemble des nombres premiers union le singleton $\{1\}$. ■

Exercice⋆ 64

Soit p un nombre premier. Montrer que $\sqrt{p}$ est irrationnel. (Suggestion : utiliser le lemme d'Euclide).

Solution : On peut raisonner par l'absurde comme on l'a fait pour $p = 2$ dans le cours. Supposons par l'absurde que $\sqrt{p} \in \mathbb{Q}$: il existe alors $a, b \in \mathbb{N}^*$ tels que $\sqrt{p} = \frac{a}{b}$. Quitte à simplifier la fraction on peut de plus supposer $\text{pgcd}(a, b) = 1$. L'égalité $\sqrt{p} = \frac{a}{b}$ est équivalente à $b\sqrt{p} = a$. En prenant les carrés des deux membres on a $b^2 p = a^2$. On voit alors que p divise le produit a^2. Le lemme d'Euclide assure que p divise a : il existe $c \in \mathbb{N}$ tel que $a = pc$. En remplaçant cette expression pour a dans l'égalité on obtient $b^2 p = p^2 c^2$. On peut simplifier les deux membres par p et on a $b^2 = pc^2$ ce qui dit que p divise b^2. Encore une fois le lemme d'Euclide assure que p divise b. Puisque $\text{pgcd}(a, b) = 1$ on a la contradiction cherchée. ■

Exercice 65

On énumère les nombres premiers en ordre croissant : $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, etc. Plus rigoureusement, on pose $p_1 = 2$, puis on définit récursivement

$$p_{n+1} = \min\{k \text{ premier} \mid k > p_n\}.$$

1. *Montrer par récurrence qu'à partir d'un certain rang (qu'on déterminera), on a $p_n > 2n$.*
2. *Montrer par récurrence qu'à partir d'un certain rang $p_n > 3n$. (Indication : montrer que pour tout $n \geqslant 3$, $p_{n+2} - p_n \geqslant 6$).*

Solution : 1. On observe d'abord que, pour $n \leqslant 4$, $p_n \leqslant 2n$ mais, pour $n = 5$, $p_n = 11 > 2 \times 5 = 10$. On va donc montrer la propriété par récurrence sur $n \geqslant 5$. On vient d'observer que l'assertion est vraie pour $n = 5$. Supposons alors qu'elle est vraie jusqu'à $n \geqslant 5$ et montrons qu'elle l'est aussi pour $n+1$. Considérons p_n. Puisque $n > 1$, $p_n > 2$ est impair. De ce fait, $p_n + 1 > 2$ est pair et ne peut pas être premier. Cela dit alors que $p_{n+1} \geqslant p_n + 2 > 2n + 2$ d'après l'hypothèse de récurrence. Puisque $2n + 2 = 2(n + 1)$, l'assertion est vraie pour $n + 1$ ce qui achève la preuve par récurrence.

2. On commence par montrer que $p_{n+2} - p_n \geqslant 6$ si $n \geqslant 3$. Comme dans le cas précédent, on remarque que l'assertion est vraie pour $n = 3$ puisque $p_5 - p_3 = 11 - 5 = 6$ mais qu'elle ne l'est pas pour $n = 1$ et 2. Considérons p_n, p_{n+1} et p_{n+2}. Puisque $n > 2$ ces nombres sont impairs et non divisibles par 3. Si, par l'absurde $p_{n+2} - p_n < 6$ on doit avoir $p_{n+1} = p_n + 2$ et $p_{n+2} = p_n + 4$. Parmi cinq nombres consecutifs, au moins un est divisible par 3. Puisque, p_n, p_{n+1} et p_{n+2} ne le sont pas, ou bien $p_n + 1$ ou bien $p_n + 3$ doit l'être. Cependant, dans le premier cas $p_{n+2} = (p_n + 1) + 3$ doit aussi être divisible par 3 et dans le deuxième p_n doit l'être. Ceci est absurde et donc $p_{n+2} - p_n \geqslant 6$ ce qui montre l'assertion.

   Pour la deuxième partie, on note d'abord que $p_{12} = 37 > 3 \times 12 = 36$ et $p_{13} = 41 > 3 \times 13 = 39$. On raisonne alors par récurrence sur $n \geqslant 12$. On sait la propriété vraie pour $n = 12$ et 13. On la suppose alors vraie pour $n \geqslant 13$ et on la montre pour $n + 1$. On a $p_{n+1} \geqslant p_{n-1} + 6$ puisque $n - 1 \geqslant 3$. Par ailleurs, puisque $n - 1 \geqslant 12$, par hypothèse de récurrence $p_{n-1} > 3(n - 1)$ et donc $p_{n+1} \geqslant p_{n-1} + 6 > 3n - 3 + 6 = 3(n + 1)$. ■

Exercice† 66

Soient $a_0, \ldots, a_d \in \mathbb{Z}$. Supposons que $a_d > 0$, et notons

$$\forall n \in \mathbb{N},\ f(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_d n^d.$$

L'objectif de l'exercice est de montrer que $f(n)$ n'est pas premier pour une infinité d'entiers n. On admet[1] *que comme $a_d > 0$, $f(n) \xrightarrow[n\to+\infty]{} +\infty$, il existe un entier $N \in \mathbb{N}$ tel que*

$$\forall n \geqslant N,\ f(n) > 1.$$

Soit $a \geqslant N$, et notons $b = f(a)$.

1. *Montrer que $(a + \ell b)^k$ est congru à a^k modulo b pour tous entiers k, $\ell \in \mathbb{N}$.*
2. *Montrer que $f(a + \ell b)$ est divisible par b pour tout entier $\ell \in \mathbb{N}$.*
3. *Conclure. (Indication : On rappelle qu'un polynôme de degré d à au plus d racines, cf cours de Mathématiques générales.)*

1. La justification rigoureuse de ce fait sera donnée dans le cours sur les suites.

Solution : On commence par observer que b est un entier > 1 d'après la propriété admise. Cela a donc un sens de considérer des congruences modulo b.

1. On utilise le point iii) de la proposition 2.3.3 qui dit que si deux nombres sont congruents modulo b alors toute leur puissance l'est aussi. Dans ce cas $a + \ell b$ est congru à a modulo b et donc pour tout $k \in \mathbb{N}$ on doit avoir $(a + \ell b)^k$ congru à a^k modulo b.
2. Le point précédent et la proposition 2.3.3 assurent que $f(a)$ est congru à $f(a+\ell b)$ pour tout $\ell \in \mathbb{N}$. Puisque un nombre est divisible par b si et seulement s'il est congru à 0 modulo b, la conclusion suit.
3. Pour tout $\ell \in \mathbb{N}$ on a $a + \ell b \geqslant a \geqslant N$. La propriété admise dit alors que $f(a + \ell b)$ est un entier > 1. Puisque b divise $f(a + \ell b)$ pour tout $\ell \in \mathbb{N}$, ou bien b est premier et, pour tout $\ell \in \mathbb{N}$ sauf un nombre fini, $f(a + \ell b) = b$, ou bien $f(a + \ell b)$ n'est pas premier pour une infinité de $\ell \in \mathbb{N}$ (dans ce deuxième cas, pour tout ℓ si b n'est pas premier). Puisque un polynôme de degré d a au plus d racines, on voit que l'équation $f(n) = b$ a au plus d solutions. Cela permet de conclure que, même si b est premier, $f(a+\ell b)$ n'est pas premier pour une infinité de $\ell \in \mathbb{N}$. Le même argument permet même de dire qu'il y a une infinité de valeurs différentes dans l'ensemble $\{f(a + \ell b) : \ell \in \mathbb{N}\}$. ■

Exercice 67

L'objectif de cet exercice est de montrer que l'on peut majorer p_n en analysant la preuve du théorème d'Euclide.

1. *Soit $n \in \mathbb{N}^*$. Montrer que*
$$p_{n+1} \leqslant p_1 p_2 \cdots p_n + 1.$$
2. *En déduire que*
$$\forall n \in \mathbb{N}^*,\ p_{n+1} \leqslant p_n^n + 1.$$
3. *Montrer par récurrence sur n que*
$$\forall n \in \mathbb{N}^*,\ p_n < 2^{2^n}.$$
4. *Pour $x \in \mathbb{R}_+$, on pose $\pi(x) = |\{p \text{ premier } \mid p \leqslant x\}|$.*
Soit $x \in \mathbb{R}$ tel que $x > e^{e^3}$, et $n \geqslant 4$ entier tel que $e^{e^{n-1}} < x \leqslant e^{e^n}$. Déduire de la question précédente et de l'inégalité $e^{n-1} > 2^n$ (à démontrer[2]) que
$$\pi(x) \geqslant \pi(2^{2^n}) \geqslant n.$$
En déduire que $\pi(x) \geqslant \ln(\ln(x))$. Cette inégalité vous semble-t-elle optimale ?

Solution :

1. On considère la décomposition en facteurs premiers de $a = p_1 p_2 \cdots p_n + 1$. Puisque pour tout $i \leqslant n$, a est congru à 1 modulo p_i, les diviseurs premiers de a sont $\geqslant p_{n+1}$ et $\leqslant a$. On a donc $p_{n+1} \leqslant p_1 p_2 \cdots p_n + 1$.
2. Pour tout $i \leqslant n$ on a $p_i \leqslant p_n$ et donc $p_{n+1} \leqslant p_1 p_2 \cdots p_n + 1 \leqslant p_n^n + 1$. Puisque n est arbitraire, la conclusion suit.
3. Pour $n = 1$ on a $p_1 = 2$ et $2^{2^1} = 4$. Puisque $2 < 4$ l'assertion est vraie dans ce cas. Supposons l'assertion vraie pour tout naturel jusqu'à $n \geqslant 1$ et montrons qu'elle est vraie pour $n + 1$. On a $p_{n+1} \leqslant \prod_{i=1}^n p_i + 1$ d'après le premier point et, puisque $p_i < 2^{2^i}$ si $i \leqslant n$ par hypothèse de récurrence, on a $p_{n+1} < \prod_{i=1}^n 2^{2^i} + 1 = 2^{\sum_{i=1}^n 2^i} + 1 = 2^{2^{n+1}-2} + 1$ d'après la formule pour la somme d'une suite géométrique. Puisque 1 est plus petit ou égal que tout naturel non nul et en particulier de $3 \times 2^{2^{n+1}-2}$, on peut majorer le dernier terme par $4 \times 2^{2^{n+1}-2} = 2^{2^{n+1}}$. Ceci montre que l'assertion est vraie.
4. On commence par démontrer l'inégalité $e^{n-1} > 2^n$. On remarque que $2^n = e^{n \ln 2}$. Le logarithme étant strictement croissant, l'inégalité donnée est équivalente à $n - 1 > n \ln 2$ qui à son tour est équivalente à $n(1-\ln 2) > 1$. On remarque maintenant que $\ln 2 < 1$ du fait que $2 < e$. L'équivalence est vraie dès que $n > \frac{1}{1-\ln 2}$. Puisque $\frac{1}{1-\ln 2} \approx 3,26 < 4$ l'inégalité est bien vérifiée si $n \geqslant 4$.

   Puisque l'exponentielle est strictement croissante on a $e^{e^{n-1}} > e^{2^n}$. Par ailleurs, puisque $e > 2$ on a aussi $e^{2^n} > 2^{2^n}$, du fait que la fonction x^{2^n} est strictement croissante sur $\mathbb{R}_+$. Par ailleurs, il

2. On pourra utiliser l'approximation $\ln 2 \approx 0,693$.

est clair que la fonction π est croissante. On a donc $\pi(x) \geqslant \pi(e^{e^{n-1}}) \geqslant \pi(2^{2^n}) \geqslant \pi(p_n) = n$ où la dernière égalité découle de la définition même de π et p_n.

Pour terminer, en exploitant encore la croissance du logarithme et l'inégalité $x \leqslant e^{e^n}$, on a $\ln(\ln(x)) \leqslant n \leqslant \pi(x)$.

En tenant compte des majorations faites au point 3, cette inégalité semble loins d'être optimale. ■

Exercice 68

Soit $N \in \mathbb{N} \setminus \{0, 1\}$. Montrer qu'aucun des N entiers successifs suivants

$$(N+1)! + 2, (N+1)! + 3, \ldots, (N+1)! + N + 1$$

n'est premier.

Solution : On remarque que tout naturel non nul $n \leqslant N+1$ divise $(N+1)!$ et de ce fait est un diviseur propre de $(N+1)! + n$. Puisque $n \geqslant 2$, cela montre que les nombres ne peuvent pas être premiers. ■

Exercice 69

1. *Soit $p > 2$ un nombre premier. Montrer que $p \equiv 1$ ou 3 modulo 4.*
2. *Soient $k_1, \ldots, k_s \in \mathbb{N}$ tels que*
$$\forall i,\ k_i \equiv 1\ [4].$$
Montrer que $k_1 \cdots k_s \equiv 1\ [4]$.
3. *Soit $n \in \mathbb{N}^*$. Notons*
$$q = p_1^2 p_2 p_3 \cdots p_n - 1.$$
Soit p un diviseur premier de q. Montrer que $p > p_n$.
4. *Montrer que $q \equiv 3\ [4]$. En déduire que q admet un diviseur premier $p \equiv 3\ [4]$.*
5. *En déduire qu'il existe une infinité de nombres premiers de la forme $4k + 3$.*

Solution : 1. Puisque $p > 2$, p doit être impair, ce qui implique que le reste de sa division par 4 doit aussi être impair. Les seuls possibles restes sont alors 1 et 3 ce qui permet de conclure.

2. Ceci découle du point ii) de la proposition 2.3.3 par récurrence immediate sur $s \in \mathbb{N}^*$.
3. Pour tout $i \leqslant n$ on a $q \equiv -1$ modulo p_i : aucun nombre premier $\leqslant p_n$ ne divise $q > 1$ et donc les diviseurs premiers de q doivent être $> p_n$.
4. On a $q = p_1^2 p_2 p_3 \cdots p_n - 1 = 4(p_2 p_3 \cdots p_n - 1) + 3$ ce qui montre que $q \equiv 3\ [4]$. Pour la deuxième partie de la question on raisonne pas l'absurde : si les diviseurs premiers de q étaient tous $\equiv 1\ [4]$, q devrait aussi être $\equiv 1\ [4]$ d'après le deuxième point, ce qui contredit ce qu'on vient de montrer.
5. Supposons par l'absurde que cela ne soit pas le cas et soit p_n le plus grand premier de la forme $4k + 3$. Les points précédents assurent alors qu'il existe un permier $p > p_n$ de la forme $\equiv 3\ [4]$ ce qui donne la contradiction cherchée. On peut même donner une preuve de cette affirmation en construisant une suite $(r_k)_{k \in \mathbb{N}^*}$ strictement croissante de nombres premiers r_k de la forme $4k + 3$. Pour cela on pose $r_1 = 3$ puis, en supposant r_k déjà connu, on va définir r_{k+1}. Soit $p_n = r_k$: la première partie de l'exercice assure alors qu'il existe un $p > p_n = r_k$ de la forme cherchée et on pose $r_{k+1} = p$. ■

Exercice† 70 (*Une situation où irréductible et premier ne sont pas équivalents.*)

On considère l'ensemble $A = \{a + ib\sqrt{5} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$.

1. *Montrer que si $z, z \in A$ alors $z + z'$ et $zz' \in A$.*
2. *Déterminer les éléments inversibles de A. (Suggestion : utiliser les propriétés du module).*
3. *Montrer que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont des éléments irréductibles de A.*
4. *Déduire que $6 \in A$ a deux factorisations distinctes dans A.*
5. *Conclure.*

Solution : 1. La propriété vient du fait que sommes et produits d'entiers sont des entiers. Soient $z = a+ib\sqrt{5}$ et $z' = a'+ib'\sqrt{5}$. On a $z+z' = (a+a')+i(b+b')\sqrt{5}$ et $zz' = (aa'-5bb')+i(ab'+ba')\sqrt{5}$. Ceci montre que A a des opérations ayant les mêmes propriétés que celles de $\mathbb{N}$ ou $\mathbb{Z}$: associativité, commutativité et distributivité viennent du fait que les opérations des nombres complexes les satisfont. A, de plus, contient $\mathbb{Z}$.

2. On remarque que $|a+ib\sqrt{5}|^2 = a^2+5b^2 \in \mathbb{N}$ et on rappelle que $|zz'| = |z||z'|$. Un élément $z \in A$ est inversible s'il existe $z' \in A$ tel que $zz' = 1$. On doit alors avoir $|z|^2|z'|^2 = 1$. Puisque le produit de deux naturels vaut 1 si et seulement si les deux naturels sont égaux à 1, on voit que $|z|^2 = |z'|^2 = 1$. Soit $z = a + ib\sqrt{5}$: si $b \neq 0$, $|z|^2 \geqslant 5$. Dans notre cas, on doit alors avoir $b = 0$, à savoir $z \in \mathbb{Z}$, et nécessairement $z = z' = \pm 1$. On remarque de plus que z est inversible si et seulement si $|z|^2 = 1$.

3. Supposons d'avoir $2 = zz'$. En raisonnant comme au point précédent on a que $|z|^2$ ne peut être que 1, 2 ou 4. Dans le premier et dernier cas, le point précédent permet de conclure que 2 est irréductible, car à chaque fois qu'on l'écrit comme produit de deux nombre l'un des deux nombres est inversible. Si $|z|^2 = 2 < 5$ on voit que dans ce cas aussi $b = 0$ et $2 = |z|^2 = a^2$. Cela est cependant impossible car $a \in \mathbb{Z}$ et 2 n'est pas le carré d'un entier. Le même raisonnement montre que 3 est irréducible. Supposons alors d'avoir $1 \pm i\sqrt{5} = zz'$. Puisque $|1 \pm i\sqrt{5}|^2 = 6$ encore une fois on doit avoir $|z|^2 = 1$, 2, 3 ou 6 et la conclusion suit en argumentant comme dans les cas précédents.

4. On a $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Le point précédent permet de conclure.

5. Le point précédent montre que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ divisent un produit sans diviser aucun des facteurs. Ces nombres ne sont donc pas premiers (le lemme d'Euclide est faux dans A). ■

2.3 Congruences

Exercice⋆ 71

1. Soit n un entier. Montrer que si n est pair alors $n^2 \equiv 0$ [4].

2. Soit n un entier. Montrer que si n est impair alors $n^2 \equiv 1$ [4].

3. En déduire que si n est un entier naturel somme de deux carrés alors le reste de la division de n par 4 n'est jamais égal à 3.

Solution : 1. Soit n pair. Il existe un entier k tel que $n = 2k$. En prenant le carré on voit que $n^2 = 4k^2$, à savoir $n^2 \equiv 0$ [4].

2. Soit n impair. Il existe un entier k tel que $n = 2k + 1$. En prenant le carré on voit que $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, à savoir $n^2 \equiv 1$ [4].

3. Puisque les deux carrés ne peuvent être congrus qu'à 0 ou 1 modulo 4 leur somme peut seulement être congrue à $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, ou $1 + 1 = 2$ modulo 4. Le reste de la division euclidienne de la somme de deux carrés par 4 n'est donc jamais égal à 3. ■

Exercice⋆ 72

Montrer par récurrence sur $n \in \mathbb{N}$ que 7 divise $2^{4^n} + 5$.

Solution : Pour $n = 0$ on a $2^{4^n} + 5 = 2^{4^0} + 5 = 2 + 5 = 7$ qui est bien divisible par 7. Supposons la propriété vraie pour un $n \geqslant 0$ et montrons qu'elle l'est aussi pour $n + 1$. Par hypothèse de recurrence $2^{4^n} + 5$ est divisible par 7. Ce fait est équivalent à dire que $2^{4^n} + 5$ est congru à 0 modulo 7 ce qui est le cas si et seulement si 2^{4^n} est congru à 2 modulo 7. Considérons alors $2^{4^{n+1}} = 2^{4^n \times 4} = (2^{4^n})^4$. On voit alors que ce nombre est congru à $(2)^4 = 16$ modulo 7. Puisque $16 + 5 = 21 = 3 \times 7$ on voit que $2^{4^{n+1}} + 5$ est divisible par 7 ce qui achève la preuve. ■

Exercice⋆ 73

Montrer que la somme des cubes de trois entiers consecutifs est congrue à 0 modulo 9.

Solution : Soit $n \in \mathbb{Z}$. Considérons la somme $s = (n-1)^2 + n^3 + (n+1)^3 = (n^3 - 3n^2 + 3n - 1) + n^3 + (n^3 + 3n^2 + 3n + 1) = 3n^3 + 6n = 3n(n^2 + 2)$. Si 3 divise n on a $n = 3k$ et donc $s = 9(kn^2 + 2k)$. Sinon

n est de la forme $3k \pm 1$. On a donc $n^2 + 2 = (9k^2 \pm 6k + 1) + 2 = 3(3k^2 \pm 2k + 1)$ et par la suite $s = 9(3nk^2 \pm 2nk + n)$. ■

Exercice⋆ 74

Démontrer que le nombre $7^n + 1$ est divisible par 8 si n est impair ; dans le cas où n est pair, donner le reste de sa division par 8.

Solution : Pour la première partie on peut utiliser l'identité $a^n - b^n = (a-b)\sum_{i=0}^{n-1} a^i b^{n-1-i}$. Dans notre cas on a $a = 7$, $b = -1$, où l'on utilise que n est impair et donc $-(-1)^n = +1$. On peut donc écrire $7^n + 1 = (7 - (-1))\sum_{i=0}^{n-1}(-1)^{n-1-i}7^i$. Puisque $7 - (-1) = 8$ la conclusion suit.

Supposons maintenant n pair. On a $7^0 = 1$, $7^2 = 49 = 48 + 1$ qui est congru à 1 modulo 8. On déduit alors que le reste de la division de $7^n + 1$ par 8 vaut toujours 2 quand $n = 2k$ est pair. En effet on peut écrire $7^n = (7^2)^k$ et la conclusion vient du calcul précédent. ■

Exercice 75

Soit $n \in \mathbb{N}$. Montrer que :

(a) 3 *divise* $2^{2n+1} + 1$,

(b) 6 *divise* $5n^3 + n$,

(c) 7 *divise* $3^{2n+1} + 2^{n+2}$,

(d) 17 *divise* $3 \times 5^{2n+1} + 2^{3n+1}$.

Solution : (a) Puisque $2 \equiv -1$ [3] on a $2^{2n+1} + 1 \equiv (-1)^{2n+1} + 1 \equiv -1 + 1 \equiv 0$ [3] ce qui montre que 3 divise $2^{2n+1} + 1$.

(b) Puisque $5 \equiv -1$ [6] on a $5n^3 + n \equiv -n^3 + n \equiv -n(n-1)(n+1)$ [6]. On a déjà vu que le produit de trois entiers consécutifs est divisible par 6 car un doit être divisible par 3 et au moins un est pair. Cela montre que 6 divise $5n^3 + n$.

(c) Puisque $3 \equiv -4$ [7] on a $3^{2n+1} + 2^{n+2} \equiv (-4)^{2n+1} + 2^{n+2} \equiv (-1)^{2n+1}2^{4n+2} + 2^{n+2} \equiv -(2^3)^n \times 2^{n+1} + 2^{n+2}$. Or $2^3 = 8 \equiv 1$ [7] et on a donc $3^{2n+1} + 2^{n+2} \equiv 0$ [7] ce qui montre que 7 divise $3^{2n+1} + 2^{n+2}$.

(d) On a $3 \times 5^{2n+1} + 2^{3n+1} = 15 \times 25^n + 2 \times 8^n$. On remarque alors que $15 \equiv -2$ [17] et $25 \equiv 8$ [17] et donc $15 \times 25^n + 2^n \equiv 0$ [17] ce qui montre que 17 divise $3^{2n+1} + 2^{3n+1}$. ■

Exercice 76

On se propose de déterminer le chiffre des unités de 7^{7^7}.

1. *Montrer que $7^4 \equiv 1$ modulo 10.*
2. *Soit r le reste de la division euclidienne de 7^7 par 4. Montrer que $7^{7^7} \equiv 7^r$ modulo 10.*
3. *Calculer la valeur de 7^7 modulo 4.*
4. *En déduire le chiffre des unités de 7^{7^7}.*

Solution :

1. On a $7^4 = (7^2)^2 = 49^2 \equiv (-1)^2$ [10] et donc $7^4 \equiv 1$ modulo 10.
2. D'après la définition de division euclidienne, il existe $k \in \mathbb{N}$ tel que $7^7 = 4k + r$. On a alors $7^{7^7} = 7^{4k+r} = (7^4)^k \times 7^r$. Puisque $7^4 \equiv 1$ [10], on voit que $7^{7^7} \equiv 7^r$ modulo 10.
3. Puisque $7 \equiv -1$ [4] on a $7^7 \equiv -1 \equiv 3$ modulo 4. Cela dit que $r = 3$.
4. Le chiffre des unités d'un naturel étant précisement le reste de sa division euclidienne par 10, pour la trouver il suffit de déterminer le chiffre des unités de $7^3 = 343$ qui est 3. ■

Exercice 77

Trouver le reste de la division euclidienne de 100^{1000} par 13.

Solution : On remarque que $10 \equiv -3$ [13]. De ce fait $100 = 10^2 \equiv 9$ [13] et par la suite $10^3 \equiv -27 \equiv -1$ [13]. On voit alors que $10^6 = 100^3 \equiv 1$ [13]. On peut alors écrire $100^{1000} = 100^{3\times 333+1} = (100^3)^{333} \times 100^1$ ce qui permet de dire que le reste de la division euclidienne de 100^{1000} par 13 est le même que celui de 100 par 13, à savoir 9. ■

Exercice 78

1. *Montrer que le reste de la division euclidienne par 8 du carré de tout nombre impair est 1.*
2. *Montrer de même que tout nombre pair x vérifie $x^2 \equiv 0$ [8] ou $x^2 \equiv 4$ [8].*
3. *Soient a, b, c trois entiers impairs. Déterminer le reste de la division de $a^2+b^2+c^2$ et de $2(ab+bc+ca)$ par 8.*
4. *En déduire que ces deux nombres ne sont pas des carrés puis que $ab+bc+ca$ non plus.*

Solution : 1. Soit $x = 2k+1$ un nombre impair. On calcule $(2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$. Puisque un parmi k et $k+1$ est pair, on voit que $4k(k+1)$ est divisible par 8 ce qui montre que le reste de la division euclidienne par 8 du carré de tout nombre impair est 1.

2. Soit x pair. Dans ce cas $x = 4k$ si n est divisible par 4 et $x = 4k+2$ s'il n'est pas divisible par 4. Dans le premier cas on a $x^2 = 16k^2$ et donc $x^2 \equiv 0$ modulo 8 tandis que dans le deuxième on a $x^2 = 8(2x^2+2x)+4$ et donc $x^2 \equiv 4$ modulo 8.
3. D'après le premier point on a $a^2+b^2+c^2 \equiv 1+1+1$ modulo 8 et donc le reste de la division euclidienne de $a^2+b^2+c^2$ par 8 vaut 3.
   On considère maintenant $a+b+c$. Ce nombre est impair, donc $(a+b+c)^2 \equiv 1$ [8]. Or $(a+b+c)^2 = a^2+b^2+c^2+2(ab+bc+ca)$, ce qui dit que $2(ab+bc+ca) \equiv (a+b+c)^2-(a^2+b^2+c^2)$ [8]. Puisque $-3 \equiv 5$ [8], on déduit que le reste de la division euclidienne de $2(ab+bc+ca)$ par 8 vaut 6.
4. Le nombre $a^2+b^2+c^2$ étant impair, il ne peut qu'être le carré d'un nombre impair, mais puisque le carré d'un nombre impair est congru à 1 modulo 8, on voit que $a^2+b^2+c^2$ ne peut pas être un carré.
   Le nombre $2(ab+bc+ca)$ étant pair, il ne peut qu'être le carré d'un nombre pair, mais puisque le carré d'un nombre pair est congru soit à 0 soit à 4 modulo 8, on voit que $2(ab+bc+ca)$ ne peut pas être un carré.
   Pour terminer, on remarque qu'afin d'avoir $2(ab+bc+ca) \equiv 6$ [8], le reste de la division euclidienne de $ab+bc+ca$ par 8 ne peut être que 3 ou 7. Dans les deux cas, on voit que $ab+bc+ca$ ne peut pas être un carré. ■

Exercice⋆ 79

Soient a, n et m des entiers strictement positifs, avec $a > 1$.

1. *Soir r le reste de la division euclidienne de n par m. Montrer que*
$$a^n \equiv a^r \ [a^m-1].$$
2. *Montrer que $a^r-1 < a^m-1$. En déduire que a^r-1 est le reste de la division euclidienne de a^n-1 par a^m-1.*
3. *Notons $r_0 = n$, $r_1 = m$, r_2, …, $r_k = pgcd(n,m)$ les restes obtenus en appliquant l'algorithme d'Euclide à $r_0 = n$ et $r_1 = m$. Déduire que $a^{r_i}-1$ est le reste de la division euclidienne de $a^{r_{i-1}}-1$ par $a^{r_{i-2}}-1$.*
4. *En déduire que*
$$pgcd\,(a^n-1, na^m-1) = a^{pgcd(n,m)}-1.$$

Solution : 1. On a $n = mq+r$ avec $q \in \mathbb{N}$ et on peut écrire $a^n = a^{qm+r}-a^r+a^r = a^r((a^m)^q-1)-a^r$. Il suffit maintenant de remarquer que $(a^m)^q-1 = (a^m-1)\sum_{i=0}^{q-1} a^i$ pour conclure que $a^n \equiv a^r$ $[a^m-1]$.

2. Pour montrer que $a^r-1 < a^m-1$ il suffit de montrer que $a^r < a^m$. Puisque $a > 1$ et $r < m$, on a $a^{m-r} > 1$. La conclusion suit en multipliant par a^r les deux membres de l'inégalité.
   Pour la deuxième partie, il suffit de soustraire 1 des deux membres de l'égalité $a^n = a^r((a^m)^q-1)-a^r$ et observer que $0 \leqslant a^r-1 < a^m-1$ satisfait la condition requise pour être un reste.
3. Le point précédent assure que l'algorithme d'Euclide appliqué à a^n-1 et a^m-1 donne précisement comme restes la suite $a^{r_i}-1$.
4. Puisque $r_{k_1} = qr_k+0$, on doit avoir $a^{r_{k-1}}-1 = (a^{r_k}-1)Q(a)+(a^0-1)$ ce qui montre que $a^{r_k}-1$ doit être le pgcd de a^n-1 et a^m-1. ■

Exercice⋆ 80

Soient $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$ et $n \geqslant 2$ un entier naturel. On considère l'équation $ax \equiv b\ [n]$ d'inconnue $x \in \mathbb{Z}$.

1. *Montrer que cette équation a au moins une solution si et seulement si $\mathrm{pgcd}(a, n)$ divise b.*
2. *Montrer que si $x_0 \in \mathbb{Z}$ est une solution de cette équation, alors l'ensemble des solutions de cette équation est*
$$\left\{x \in \mathbb{Z} \mid \exists \ell \in \mathbb{Z},\ x = x_0 + n'\ell\right\}$$
où $n' \in \mathbb{Z}$ est tel que $n = n' \mathrm{pgcd}(a, n)$.

Solution : On commence par remarquer que l'équation donnée est équivalente à l'équation $ax = b + ny$, où $y \in \mathbb{Z}$. Cette dernière équation peut se réécrire comme

$$ax + (-n)y = b.$$

Il s'agit donc d'une équation diophantienne linéaire du même type de celle étudiée dans l'exercice 60. Les assertions sont donc une conséquence immédiate de l'exercice 60 appliqué à $a = a$, $b = -n$ et $c = b$. ■

Exercice⋆ 81 (*Petit théorème de Fermat*)

Soit p premier.

1. *Montrer que $\forall i \in \mathbb{N}$, $0 < i < p$, p divise $\binom{p}{i}$. (Indication : utiliser le lemme d'Euclide)*
2. *Montrer par récurrence que pour tout entier n on a $n^p \equiv n\ [p]$. (Suggestion : traiter d'abord le cas $n \in \mathbb{N}$ en raisonnant par récurrence.)*

Solution : 1. On va montrer que pour tout $0 < i < p$, $\binom{p}{i}$ est divisible par p. Soit $m = \binom{p}{i}$. On a $p(p-1)! = mi!(p-i)!$. On observe alors que, puisque $i, p-i < p$, chaque facteur qui apparaît dans $i!$ ou $(p-i)!$ est premier avec p. Le lemme d'Euclide dit alors que p divise m. On peut aussi observer que $p(p-1)! = mi!(p-i)! = im(i-1)!((p-1)-(i-1))!$ avec $i - 1 \geqslant 0$ et donc $p\binom{p-1}{i-1} = im$. Puisque $i < p$, p et i sont premiers entre eux et le lemme de Gauss dit alors que p divise m.

2. Soit $n \in \mathbb{N}$. Comme suggéré on va d'abord montrer l'assertion par récurrence sur $n \geqslant 0$. Si $n = 0$ on a $n^p = 0$ et l'assertion est évidente.

   On va alors montrer l'hérédité. Supposons donc la propriété vraie pour n et montrons-la pour $n + 1$. On a $(n+1)^p = \sum_{i=0}^{p} \binom{p}{i} n^k$ d'après la formule du binôme de Newton. En tenant compte du fait que dans la somme tous les termes sauf le premier et le dernier sont divisibles par p on a $(n+1)^p \equiv n^p + 1$. L'hypothèse de récurrence permet de conclure car $n^p \equiv n$.

   Soit maintenant $n < 0$. On peut écrire $n = -|n|$. Considérons $n^p = (-|n|)^p$. Si p est impair on a $n^p = -|n|^p$ la conclusion suit en multipliant par -1 la congruence obenue dans la première partie. Si p est pair, on doit avoir $p = 2$ et $n^p = |n|^p$, mais dans ce cas on sait que $n \equiv -n$ modulo 2 et l'assertion est vraie dans ce cas aussi. ■

2.4 Développement décimal

Exercice⋆ 82

1. *Écrire $n = 10011$ en base 3.*
2. *Soit n l'entier dont l'écriture en base 2 est 110011. L'écrire en base 6.*

Solution : 1. On commence par calculer les puissances de 3 : $3^0 = 1$, $3^1 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 = 81$, $3^5 = 243$, $3^6 = 729$, $3^7 = 2187$, $3^8 = 6561$, $3^9 = 19683$. La pluissance la plus grande inférieure à n est 3^8. La division de n par 3^8 donne $n = 3^8 + 3450$. La plus grande puissance de 3 plus petite que 3450 est 3^7 et la division donne $3450 = 3^7 + 1263$. La plus grande puissance de 3 plus petite que 1263 est 3^6 et la division donne $1263 = 3^6 + 534$. La plus grande puissance de 3 plus petite que 534 est 3^5 et la division donne $534 = 2 \times 3^5 + 48$. La plus grande puissance de 3 plus petite que 48 est 3^3 et la division donne $48 = 3^3 + 21$. Pour terminer on a $21 = 2 \times 3^2 + 3$. L'écriture de n en base 3 est donc égale à 111201210.

2. L'entier n est égal à $1+2+16+32 = 51 = 48+3 = 8\times 6+3 = 6^2+2\times 6+3$ ce qui dit que son écriture en base 6 est 123. ■

Exercice⋆ 83 (*Critères de divisibilité par 2, 4 et 5*)

1. *Montrer qu'un entier est divisible par 2 si et seulement le dernier chiffre de son développement en base 10 est divisible par 2.*
2. *Montrer qu'un entier est divisible par 4 si et seulement si le nombre formé des deux derniers chiffres de son développement en base 10 est divisible par 4.*
3. *Montrer qu'un entier est divisible par 5 si et seulement le dernier chiffre de son développement en base 10 est un 0 ou un 5.*

Solution : Soit $n \in \mathbb{N}$ et soit $a_d \dots a_0$ son écriture décimale : pour tout $0 \leqslant i \leqslant d$ on a $a_i \in \mathbb{N}$, $0 \leqslant a_i \leqslant 9$, $a_d \neq 0$ si $d \geqslant 1$, et $n = \sum_{i=0}^{d} a_i 10^i$. On va utiliser cette notation dans le reste de l'exercice.

1. Si $n = a_0$ n'a qu'un chiffre dans son écriture décimale cela est clair. Sinon $d \geqslant 1$ et on peut écrire $n = a_0 + 10\sum_{i=1}^{d} a_i 10^{i-1}$. Puisque 2 divise 10, on voit que 2 divise n si et seulement s'il divise a_0.
2. Si $d \leqslant 1$ cela est clair car on demande précisement que le nombre soit divisible par 4. Si $d \geqslant 2$ on peut écrire $n = a_0 + 10a_1 + 100\sum_{i=2}^{d} a_i 10^{i-2}$. Puisque 4 divise $4\times 25 = 100$ la conclusion suit comme au point précédent.
3. Puisque 5 divise 10 le même argument vu dans le premier point montre l'assertion dans ce cas. ■

Exercice⋆ 84 (*Critères de divisibilité par 3 et 9*)

1. *Montrer qu'un entier est divisible par 3 si et seulement la somme des ses chiffres en base 10 est divisible par 3 (indication : calculer les restes des divisions euclidiennes des puissances de 10 par 3).*
2. *Soit n un entier. Montrer que n est divisible par 9 si et seulement la somme des ses chiffres en base 10 est divisible par 9.*

Solution : On utilise la même notation de l'exercice précédent : $a_d \dots a_0$ est l'écriture décimale du nombre n, de tel façon qu'on a $n = \sum_{i=0}^{d} a_i 10^i$, avec $a_i \in \mathbb{N}$, $0 \leqslant a_i \leqslant 9$, pour tout $0 \leqslant i \leqslant d$, et $a_d \neq 0$ si $d \geqslant 1$.

1. On observe que $10 \equiv 1$ [3] et donc pour tout $i \in \mathbb{N}$ on a $10^i \equiv 1$ [3]. On a alors $\sum_{i=0}^{d} a_i 10^i \equiv \sum_{i=0}^{d} a_i$ [3]. Puisque un nombre est divisible par 3 si et seulement s'il est congru à 0 modulo 3, cela montre l'équivalence.
2. L'argument vu au point précédent s'applique verbatim du fait que $10 \equiv 1$ [9] aussi. ■

Exercice⋆ 85 (*Critère de divisibilité par 11*)

Soit d un entier positif écrit en base 10 sous la forme

$$d = [a_n a_{n-1} \cdots a_0]_{10}$$

avec $a_n \neq 0$ et $a_i \in \{0, \dots, 9\}$. Montrer que d est divisible par 11 si et seulement si $\sum_{i=0}^{n}(-1)^i a_i$ l'est. (On rappelle que pour $a, b \in \mathbb{Z}$, a divise b si et seulement s'il divise $-b$).

Solution : On peut utiliser le même raisonnement (et notation) de l'exercice précédent : puisque $10 \equiv -1$ [11], on a $\sum_{i=0}^{d} a_i 10^i \equiv \sum_{i=0}^{d}(-1)^i a_i$ [11]. La conclusion suit. ■

Exercice 86 (*Critère de divisibilité par 7*)

Soit d un entier positif écrit en base 10 sous la forme

$$d = [a_n a_{n-1} \cdots a_0]_{10}$$

avec $a_n \neq 0$. Notons alors

$$k = [a_n a_{n-1} \cdots a_1]_{10} - 2a_0.$$

1. *Montrer que*
$$d = 10k + 21a_0$$
2. *Montrer que*
$$k = -2d + 21[a_n a_{n-1} \cdots a_1]_{10}.$$
3. *En déduire que d est divisible par 7 si et seulement si*
$$[a_n a_{n-1} \cdots a_1]_{10} - 2a_0$$
est divisible par 7.
4. *Le nombre 3456789 est-il divisible par 7 ?*

Solution : 1. Par définition d'écriture dans une base on a $d = \sum_{i=0}^{n} a_i 10^i$ et $k = \sum_{i=1}^{n} a_{i+1} 10^i - 2a_0$. On voit alors que $d = 10 \sum_{i=0}^{n-1} a_{i+1} 10^i + a_0 = 10(k + 2a_0) + a_0 = 10k + 21a_0$.

2. Par simplicité on note $r = \sum_{i=0}^{n-1} a_{i+1} 10^i$, de façon que $d = 10r + a_0$ et $k = r - 2a_0$. On a alors $k = r - 2(d - 10r) = -2d + 21r$.
3. Puisque 21 est divisible par 7 et 2 est premier avc 7, l'égalité établie au point précédent assure que d est divisible par 7 si et seulement si $k = [a_n a_{n-1} \cdots a_1]_{10} - 2a_0$ l'est.
4. Pour $d = 3456789$ on a $k = 345678 - 18 = 345660$. Ce dernier nombre est divisible par 7 si et seulement si $34566 - 2 \times 0$ l'est, si et seulement si $3456 - 12 = 3444$ l'est, si et seulement si $344 - 8 = 336$ l'est, si et seulement si $33 - 12 = 21$ l'est. On voit donc que 3456789 est bien divisible par 7. ■

Exercice 87 (*Critères de divisibilité par 13 et 19*)

Soit n un entier, dont la division euclidienne par 10 est $n = 10q + r$.

1. *Montrer que n est divisible par 13 si et seulement si $q + 4r$ est divisible par 13 (indication : considérer $4n$).*
2. *Montrer que n est divisible par 19 si et seulement si $q + 2r$ est divisible par 19 (indication : considérer $2n$).*
3. *Les nombres 107341 et 156883 sont-ils divisibles par 13 ? par 19 ?*

Solution : 1. L'indication dit de considérer $4n$: en effet, puisque 4 est premier avec 13, 13 divise n si et seulement s'il divise $4n$ d'après le lemme de Gauss. On a alors $4n = 40q + 4r$. Puisque $40 \equiv 1$ [13], on a $4n \equiv q + 4r$ [13] ce qui assure que 13 divise n si et seulement s'il divise $q + 4r$.

2. On raisonne comme au point précédent, cette fois-ci en exploitant le fait que 2 est premier avec 19 et $20 \equiv 1$ [19]. On a donc $2n = 20q + 2r \equiv q + 2r$ [19].
3. On exploite les points précédents pour trouver des suites de nombres de plus en plus petits qui sont tous divisibles par 13 (respectivement 19) si et seulement si le nombre de départ l'est.
   — *Divisibilité par* 13 *de* 107341 : On a $10734 + 4 = 10738$, $1073 + 32 = 1105$, $110 + 20 = 130 = 13 \times 10$, ce qui dit que 107341 est divisible par 13
   — *Divisibilité par* 13 *de* 156883 : On a $15688 + 12 = 15700$. On remarque que puisque 100 est premier avec 13 il suffit de considérer 157 et on a alors $15 + 28 = 43$ qui n'est pas divisible par 13 et donc 156883 non plus.
   — *Divisibilité par* 19 *de* 107341 : On a $10734 + 2 = 10736$, $1073 + 12 = 1085$, $108 + 10 = 118$ et $11 + 16 = 27$ qui n'est pas divisible par 19 et donc 107341 non plus.
   — *Divisibilité par* 19 *de* 156883 : On a $15688 + 6 = 15694$, $1569 + 8 = 1577$, $157 + 14 = 171$ et $17 + 2 = 19$, ce qui dit que 156883 est divisible par 19. ■

Exercice 88 (*Critère de divisibilité en base 8*)

Soit $n \in \mathbb{N}$. Montrer que n est divisible par 7 si et seulement si la somme de ses chiffres dans son développement en base 8 est divisible par 7.

Peut-on généraliser ce résultat ?

Solution : Soit $n = \sum_{i=0}^{d} a_i 8^i$ l'écriture de n en base 8. Ici donc, pour tout $0 \leqslant i \leqslant d$, on a $a_i \in \{0, \dots, 7\} \subset \mathbb{N}$ avec $a_d \neq 0$ si $d \geqslant 1$. Puisque $8 \equiv 1$ [7] on a donc $n \equiv \sum_{i=0}^{d} a_i$ [7]. Encore une fois, puisque un nombre est divisible par 7 si et seulement s'il est congru à 0 modulo 7, la conclusion suit.

Il est facile de voir que ce résultat se généralise et donne un critère de divisibilité par $b-1$ pour tout nombre écrit en base b. Par ailleurs, on a déjà vu le cas de la divisibilité par $b - 1 = 9$ en base $b = 10$. ■

Exercice† 89 (*Caractérisation de la rationnalité en termes de développement décimal*)

Soit $x \in \mathbb{R}$. Montrer que x est rationnel si, et seulement si, il admet un développement décimal qui se répète à partir d'un certain rang (on dit aussi ultimement périodique*).*

Plus généralement montrer que x est rationnel si, et seulement si, il admet un développement ultimement périodique dans une base b quelconque.

Solution : Les arguments étant les mêmes pour l'écriture décimale ou en base b quelconque, on va montrer l'équivalence directement dans le cas général.

On commence par montrer qu'un nombre ayant un développement ultimement périodique dans une base b doit être rationnel. Soit x un tel nombre. Son écriture en base b doit être alors de la forme $[a_d \dots a_0, a_{-1} \dots a_{-s}\overline{a_{-s-1} \dots a_{-s-t}}]_b$, avec $t \in \mathbb{N}^*$. On peut alors décomposer x comme somme de trois nombres : $n = \sum_{i=0}^{d} a_i b^i \in \mathbb{N}$, $q = \sum_{i=1}^{s} \frac{a_{-i}}{b^i} \in \mathbb{Q}$ et $y = \sum_{i \geqslant 1} a_{-(s+i)} b^{-s-i}$. Puisque n et q sont des rationnels, pour montrer l'implication il suffit de montrer que y l'est aussi. On remarque alors que $b^t y = \sum_{i=1}^{t} a_{-s-i} b^{t-s-i} + y$. Puisque le premier terme de la somme est une somme finie de fractions de nombres entiers, on voit que $u = \sum_{i=1}^{t} a_{-s-i} b^{t-s-i} \in \mathbb{Q}$. On a donc $y = \frac{u}{b^t - 1} \in \mathbb{Q}$ ce qui montre l'implication.

Considérons maintenant l'implication réciproque. Soit $q = \frac{n}{m} \in \mathbb{Q}_+^*$ un rationnel. Puisque on s'intéresse à son dévelppement en base b après la virgule, quitte à enlever la partie entière de q, on peut supposer $q < 1$ et donc $n < m$. Soit $\sum_{i \geqslant 1} a_{-i} b^{-i}$ son développement en base b. On multiplie alors l'égalité $q = \sum_{i \geqslant 1} a_{-i} b^{-i}$ par mb et on a $bn = a_{-1} m + r$, où $r = m \sum_{i \geqslant 2} a_{-i} b^{1-i} < m$ est le reste de la division euclidienne de nb par m. Par la suite, pour obtenir a_{-2}, on fera la division euclidienne de br par m. Puisque la division euclidienne d'un nombre par m n'a que m possibles restes, après un nombre fini de divisions on doit trouver un reste déjà obtenu et, de ce fait, refaire les mêmes divisions déjà vues dans le même ordre. Cela montre que l'écriture de q en base b doit être ultimement périodique ce qui achève la preuve. ■