Solutions des exercices d'arithmétiques

Exercice 1: Diviseurs et raisonnement (exo 43-44-45 page 459)

Il est toujours utile de préciser qu'un raisonnement par récurrence s'effectue sur un indice prenant des valeurs dans $\mathbb{N}$

1. Raisonnons donc par récurrence sur l'entier naturel n.
   Initialisation: $n = 0$: Nous savons que tout entier naturel est un diviseur de 0, d'où $6|0$. Aussi, l'hypothèse de récurrence est bien vérifiée au rang $n = 0$.
   Hérédité: Supposons l'hypothèse de récurrence vraie au rang $n \geq 1$ et démontrons-là au rang $n+1$: $(n+1)^3 + 5(n+1) = n^3 + 3n^2 + 3n + 1 + 5n + 6 = n^3 + 3n^2 + 8n + 6 = (n^3 + 5n) + 3n^2 + 3n + 6$. D'après l'hypothèse de récurrence, nous savons que $6|n^3 + 5$, d'où $(n+1)^3 + 5(n+1) \equiv 3n^2 + 3n + 6 \mod 6$, d'où $(n+1)^3 + 5(n+1) \equiv 3n(n+1) \mod 6$. Or, $n(n+1)$ est le produit de deux entiers consécutifs, donc est pair. Aussi, il existe $k \in \mathbb{N}$ tel que $n(n+) = 2k$ d'où $(n+1)^3 + 5(n+1) \equiv 0 \mod 6$.

   On peut aussi ici raisonner par épuisement des cas, en considérant tous les restes possibles de la division euclidienne de n par 6

   Nous en déduisons alors que la propriété est vraie au rang $n+1$.

   Il s'ensuit, d'après le théorème de la récurrence, que pour tout entier naturel n, $6|n^3+5n$.

2. Remarquons déjà que 5 et -1 ont même reste dans la division euclidienne par 6. Aussi, nous en déduisons que $5 \equiv -1 \mod 6$. Partons de la factorisation $n^3 + 5n = n(n^2+5)$. Comme $5 \equiv -1 \mod 6$, nous en déduisons que $n^2 + 5 \equiv n^2 - 1 \mod 6$. Comme $n^2 - 1 = (n-1)(n+1)$, nous en déduisons finalement $n^3 + 5n \equiv n(n-1)(n+1) \mod 6$.

   On utilise ici le théorème de compatibilité des opérations algébriques avec la relation de congruence

   Raisonnons alors par épuisement des cas selon le reste de la division euclidienne de n par 6. Nous avons

   Tout comme précédement, il était possible d'utiliser aussi des critères de divisibilité: par exemple, $n(n+1)(n-1)$ est le produit de trois entiers naturels consécutifs, donc est divisible par 3 et aussi par 2; comme $2 \wedge 3 = 1$, il est alors dibisible par 6.

n	0	1	2	3	4	5
$n-1$	5	0	1	2	3	4
$n+1$	1	2	3	4	5	0
$n(n-1)(n+1)$	0	0	0	0	0	0

3. Nous avons $3^{2n+1} + 2^{n+2} = 3 \times 9^n + 4 \times 2^n$. Considérons cette égalité modulo 7: puisque $9 \equiv 2 \mod 7$, nous avons pour tout entier naturel n $9^n \equiv 2^n \mod 7$. Par suite, nous avons $3 \times 9^n + 4 \times 2^n \equiv 3 \times 2^n + 4 \times 2^n \equiv \underbrace{(3+4)}_{=7} \times 2^n \equiv 0 \mod 7$.

Exercice 2: Nombre de diviseurs d'un entier (exo 57 page 460)

Il s'agit de la propriété de transitivité vérifiée par la relation de divisibilité: si $a|b$ et $b|c$ alors $a|c$.

1. Si $p|d$, alors $p|n$ et donc p est un nombre premier apparaissant dans la décomposition en produit de facteurs premiers de n. Aussi, $p \in \{p_1 n p_2, \ldots, p_m\}$.

2. Soit β_i la puissance de p_i dans la décomposition de d en facteurs premiers (ie. $p_i^{\beta_i} | d$ et $p_i^{\beta_i+1} \not| d$). Alors, puisque $d|n$, nous en déduisons que $p_i^{\beta_i}|n$. Il s'ensuit donc que $\beta_i \leq \alpha_i$.

   Techniquement, $p_1^{\beta_1} \ldots p_m^{\beta_m}$ n'est pas (nécessairement) la décomposition de d en produit de facteurs premiers, car certains β_i peuvent être nuls. On rappel que la condition de non-nullité des puissances de nombres premiers impliquent l'unicité de la décomposition (à l'ordre des facteurs près)

3. Nous savons donc par **1.** que tout facteur premier de d est dans l'ensemble $\{p_1, p_2, \ldots, p_m\}$ des facteurs premiers de n. Aussi, il existe $(\beta_1, \beta_2, \ldots, \beta_m) \in \mathbb{N}^n$ tel que $d = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \ldots p_m^{\beta_m}$. D'après la question **2.**, nous avons $\forall i \in \{1, \ldots, m\}$, $\beta_i \leq \alpha_i$.

4. Il y a donc autant de diviseurs d de n qu'il y a de couples $(\beta_1, \ldots, \beta_m) \in \mathbb{N}^m$ avec $\forall i \in \{1, \ldots, m\}$, $\beta_i \leq \alpha_i$. Il y en a donc $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_m + 1)$.

   Plus formellement, il y a une bijection entre l'ensemble des diviseurs de n et l'ensemble $\{\beta_i; 1 \leq i \leq m; 0 \leq \beta_i \leq \alpha_i\}$

Exercice 3 (exo 59 page 461)

Sans perte de généralité, nous pouvons supposer que $a \geq b$. Par l'identité remarquable, nous avons $a^2 - b^2 = (a+b)(a-b)$. Or, $(a+b)(a-b)$ étant premier, il s'ensuit que l'un des deux termes est égal à ± 1. Dans le premier cas, nous obtenons nécessairement que $a + b = 1$, soit que $a = 1$ et $b = 0$, ce qui est absurde car alors $a^2 - b^2 = 1$ qui n'est pas un nombre premier. Il s'ensuit donc que $a - b = 1$, soit $a = b + 1$ et donc a est le succésseur de b.

Un nombre premier admet exactement deux diviseurs strictement positifs: 1 et lui-même.

Exercice 4: Reste de la division euclidienne (exo 89 page 464)

1. $5^3 = 125$ d'où $5^3 \equiv 6 \mod 17$. Il s'ensuit donc que $5^{3n} - 6^n \equiv 0 \mod 17$.

2. Nous savons que $39 = 35 + 4 = 7 \times 5 + 4$; aussi, $39 \equiv 4 \mod 7$. Or, $4^3 = 64 = 63 + 1$ d'où $4^3 \equiv 1 \mod 7$. Il s'ensuit donc que $39^{60} \equiv 1 \mod 7$ et donc le reste de la division euclidienne de 39^{60} par 7 est 1.

3. Effectuons la division euclidienne de 2012 par 11: nous obtenons $2012 = 11 \times 182 + 10$. Aussi, $2012 \equiv 10 \mod 11$. Par suite, $2012 \equiv -1 \mod 11$ et donc $2012^{2012} \equiv (-1)^{2012} \mod 11$ d'où $2012 \equiv 1 \mod 11$. Aussi, le reste de la division euclidienne de 2012^{2012} par 11 est-il 1.

Dans ce type d'exercice, il faut utiliser de façon astucieuse le théorème de compatibilité des opérations algbriques avec la relation de congruence; cela évite de longs et fastidieux calculs. Il est intéressant de donner aux élèves de TS une idée de la taille des nombres que l'on manipule ainsi. En augmentant la puissance, on parvient très facilement à dépasser les capacités d'affichage des calculatrices /ordinateurs

Exercice 4: Rep-unit (exo 90+96 page 464)

1. (a) Le reste de la division de 1 111 111 par 5 est 1 puisque 1 111 110 est un multiple de 5. De même, comme 1 111 113 est un multiple de 9, nous en déduisons que le reste de la division de 1 111 111 est 7. Enfin, remarquons que les sommes des chiffres de rang pair et de rang impaire de 1 111 110 sont égales. Aussi, 1 111 110 est-il un multiple de 11, et donc le reste de la division euclidienne de 1 111 111 par 11 est 1.

   (b) Les restes des divisions euclidiennes de $(1\ 111\ 111)^8$ par 5 et 11 sont 1. Nous avons $1\ 111\ 111 \equiv 7 \mod 9$, soit encore $1\ 111\ 111 \equiv -2 \mod 9$ d'où $(1\ 111\ 111)^8 \equiv (-2)^8 \mod 9$. Or $2^8 = 256$. Comme 252 est un multiple de 9, il s'ensuit que $256 \equiv 4 \mod 9$ d'où $(1\ 111\ 111)^8 \equiv 4 \mod 9$.

Il faut ici utiliser les critères classiques (ou avancés) de divisibilité

2. (a) On peut donc conjecturer que N_k est divisible par 3 lorsque k est un multiple de 3. Il semble que N_k soit un multiple de 9 lorsque k l'est.

   Démontrons la première conjecture: nous avons $N_k = \sum_{i=0}^{k-1} 10^i$. Or, $\forall i \in \mathbb{N}$, $10^i \equiv 1 \mod 3$ d'où $N_k \equiv k \mod 3$.

   De même, pour la seconde conjecture, nous avons $N_k = \sum_{i=0}^{k} 10^i$ d'où comme $10 \equiv 1 \mod 9$ nous en déduisons que $N_k \equiv k \mod 9$.

   (b) i. Supposons donc que l'écriture décimale de n^2 se termine par 1. Aussi, $n^2 \equiv 1 \mod 10$, soit $n^2 - 1 \equiv 0 \mod 10$. Or, $n^2 - 1 = (n-1)(n+1)$ d'où nous avons $10|(n-1)(n+1)$. Aussi, $2|(n-1)(n+1)$ et $5|(n-1)(n+1)$. Comme 2 et 5 sont des nombres premiers, nous en déduisons que 2 et 5 divisent l'un des facteurs: étudions les différents cas.
   Si $2|n-1$ et $5|n-1$, alors $10|n-1$ d'où n se termine par un 1.
   Si $2|n+1$ et $5|n+1$ alors $10|n+1$ et donc n se termine par un 9.
   Si $2|n-1$, alors n se termine par $\{1,3,5,7,9\}$, et $5|n+1$ alors n se termine par $\{4,9\}$: aussi dans ce cas, n se termine par 9.
   Si $2|n+1$, alors n se termine par $\{1,3,5,7,9\}$, et $5|n-1$ alors n se termine par $\{1;6\}$: aussi dans ce cas, le chiffre des unités de n est 1.
   Nous en déduisons-donc que lorsque n^2 se termine par 1, n se termine par 1 ou 9.

   ii. Aussi, il existe $p \in \mathbb{N}$ tel que $n = 10p \pm 1$. Il s'ensuit que $n^2 = (10p \pm 1)^2 = 100p^2 \pm 20p + 1$. En passant à la classe de congruence modulo 20, nous en déduisons que $n^2 \equiv 1 \mod 20$.

   iii. Soit $k \geq 2$. Alors $N_k = \sum_{i=0}^{k-1} 10^i$. Aussi, il existe $p \in \mathbb{N}$ tel que $N_k = 100p + 11$. Comme 100 est un multiple de 20, il s'ensuit que $N_k \equiv 11 \mod 20$.

   iv. Raisonnons par l'absurde en supposant qu'il existe $k \geq 2$ tel que N_k soit un carré parfait. Il existe donc $n \in \mathbb{N}$ tel que $N_k = n^2$. Or, n^2 se termine par le chiffre 1, donc d'après la question **4.b**, $N_k \equiv 1 \mod 20$, ce qui contredit le résultat de la question **4.c**. Aussi, pour tout $k \geq 2$, N_k n'est pas un carré parfait. On vérifie alors que $N_1 = 1$ est un carré parfait, et donc 1 est l'unique rep-unit qui soit un carré parfait.

Si p est premier et $p|ab$, alors $p|a$ ou $p|b$. C'est une conséquence du Lemme de Gauss, puisque si p premier et n non multiple de p, alors $p \wedge n = 1$

On utilise ici les critères classiques de divisibilité: si $2|m$ alors le chiffre des unités de m est dans l'ensemble $\{0,2,4,6,8\}$, et si $5|m$, alors le chiffre des unités de m est 0 ou 5.

Il suffit de remarquer que $20|100$. Aussi, on utilise l'écriture décimale de N_k et la congruence modulo 20 pour exprimer son reste dans la division euclidienne par 20

Assez classiquement, pour répondre à la question, on doit utiliser les questions précédentes qui détaillent le raisonnement aboutissant au résultat souhaité

Exercice 5: Critère de divisibilité par 11 (exo 104 page 167)

Partie A

1. Soit $x = 10a + b$ et $y = 10b + a$. Aussi, $x + y = 11(a + b)$ d'où $x + y$ est divisible par 11.

2. Supposons que l'écriture décimale de x soit $\overline{abcd}$. Aussi, $x = d + 10c + 100b + 1000a = d + 10c + 10^2b + 10^3a$. Or, $10 \equiv -1 \mod 11$ d'où $10^2 \equiv 1 \mod 11$ et $10^3 \equiv -1 \mod 11$. En passant alors à la classe de congruence modulo 11 l'égalité précédente, nous obtenons que $x \equiv d - c + b - a \mod 11$. Aussi, x est un multiple de 11 si et seulement si $d - c + b - a$ l'est.

3. En posant $d = a$ et $c = b$ dans la précédente condition, nous obtenons que les entiers de la forme $\overline{abba}$ avec $a \neq 0$ sont divisible par 11.

Il faut ici passer de l'écriture décimale $\overline{ab}$ d'un nombre à son expression arithmétique $10a + b$

Il est souvent intéressant de remarquer que $n - 1 \equiv -1 \mod n$

La condition $a \neq 0$ est là pour s'assurer que $\overline{abba}$ est bien une écriture décimale: en effet, $\overline{022}$ n'est pas l'écriture décimale de 22

Partie B

1. Nous avons donc $a = \sum_{k=0}^{n} a_k 10^k$ d'où $a \equiv \sum_{k=0}^{n} (-1)^k a_k \mod 11$. Aussi, a est divisible par 11 si et seulement si la somme de ses chiffres de rang pair diminuée de la somme de ses chiffres de rang impair est divisible par 11.

2. La somme des chiffres de rang pair est 42 alors que la somme de ses chiffres de rang impair est 31. La différence est donc égale à 11, d'où l'entier considéré est bien un multiple de 11.

3. On cherche donc les chiffres ayant pour écriture décimale $\overline{abcd}$ avec $a \neq 0$ tels que $a + b + c + d = 11$ et qui sont multiples de 11. D'après la question précédente, nous devons donc avoir $11 | (a + c - (b + d))$. Comme $a, b, c, d \geq 0$, de l'inégalité $a + c - b - d \leq a + b + c + d$, nous déduisons que $a + b - c - d = 0$, et donc $a + b = c + d$. Aussi, $a + b + c + d = 2(a + b)$, et la condition $a + b + c + d = 11$ ne peut être réalisée (puisque 11 est impair alors que $a + b + c + d$ est pair). Aussi, il n'existe pas d'entier naturel multiple de 11 compris entre 1000 et 9999 dont la somme des chiffres soit 11.

Rappelons qu'un diviseur de n est dit propre s'il est différent de n lui-même

Puisque $220 = 2^2 \times 5 \times 11$, nous savons que 220 possède 12 diviseurs, donc seulement 10 propres

Exercice 6: Nombres amiables (exo 111 page 469)

1. Les diviseurs de 220 sont $\{1, 2, 4, 5, 10; 11, 20, 22, 44, 55, 110, 220\}$. Aussi, la somme de ses diviseurs propres est-elle égale à $1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$. De même, les diviseurs de 284 sont $\{1, 2, 4, 71, 142, 284\}$. Aussi, la somme de ses diviseurs propres est $1 + 2 + 4 + 71 + 142 = 220$. On en déduit donc que 220 et 284 sont amiables.

2. (a) Posons $n = 2$. Alors $a = 6 \times 2 - 1 = 5$, $b = 3 \times 4 - 1 = 11$, $c = 9 \times 2^3 - 1 = 71$. Aussi, $A = 2^2 \times 5 \times 11 = 220$ et $B = 2^2 \times 71 = 284$. Aussi, 220 et 284 sont-ils bien de la forme A et B.

   (b) Effectuons déjà la décomposition en facteurs premiers de 1184 et 1210. Nous obtenons $1184 = 2^5 \times 37$ et $1210 = 2 \times 5 \times 11^2$. Aussi, les diviseurs de 1184 sont $\{1, 2, 4, 8, 16, 32, 37, 74, 148, 296, 592, 1184\}$. Les diviseurs de 1210 sont $\{1, 2, 5, 10, 11, 22, 55, 121, 242, 605, 1210\}$. La somme des diviseurs propres de 1184 est égale à 1210 alors que la somme des diviseurs propres de 1210 est égale à 1184, d'où ces deux entiers sont amiables.
   Pourtant, ils ne sont pas de la forme A et B après calculs.

   (c) Pour $n = 4$, nous avons $a = 3 \times 2^3 - 1 = 23$ et $b = 3 \times 2^4 - 1 = 47$. Enfin, $c = 9 \times 2^7 - 1 = 1151$. On vérifie que ces entiers naturels sont premiers, et on obtient que $A = 2^4 \times 23 \times 47 = 17\,296$ et $B = 2^4 \times 1151 = 18\,416$.

   (d) Même question avec $n = 7$.

3. (a) Nous savons donc que la décomposition de B en produit de facteurs premiers est $B = 2^n \times c$ d'où l'ensemble des diviseurs de B est $\{1, 2, 2^2, \ldots, 2^n, c, 2c, 2^2c, \ldots, 2^nc\}$.

   (b) Puisque $A = 2^n \times a \times b$, nous en déduisons que l'ensemble de ses diviseurs est $\{1, 2, 2^2, \ldots, 2^n, a, 2a, 2^2a, \ldots, 2^na; b, 2b, 2^2b, \ldots, 2^nb, ab, 2ab, 2^2ab, \ldots, 2^nab\}$.

On reconnaît dans la somme $\sum_{k=0}^{n} 2^k$ la somme des $n+1$ premiers termes d'une suite géométrique de premier terme 1 et de raison 2

(c) La somme des diviseurs de B est égale à:

$$S_B = \sum_{k=0}^{n} 2^k + c\sum_{k=0}^{n} 2^k = (1+c)\sum_{k=0}^{n} 2^k = \frac{1-2^{n+1}}{1-2}(1+c) = (2^{n+1}-1)(1+c)$$

(d) Nous avons de même

$$\begin{aligned} S_A &= \textstyle\sum_{k=0}^{n} 2^k + a\sum_{k=0}^{n} 2^k + b\sum_{k=0}^{n} 2^k + ab\sum_{k=0}^{n} 2^k \\ &= (1+a+b+ab)\textstyle\sum_{k=0}^{n} 2^k = (1+a+b+ab)(2^{n+1}-1) \end{aligned}$$

(e) Nous avons alors $S_B = (1+9\times 2^{2n-1}-1)(2^{n+1}-1)$ et $S_A = (1+3\times(2^{n-1}-1)+(3\times 2^n - 1 =)+)\times(2^{n+1}-1)$. Or, $S_A =$

Exercice 8: Nombres parfaits pairs (exo 112 page 469)

On dit qu'un entier naturel est parfait s'il est égal à la somme de ses diviseurs positifs autre que lui-même. Par exemple 6 est parfait puisque l'ensemble de ses diviseurs est $\{1,2,3,6\}$ et donc la somme de ses diviseurs autres que lui-même est égale à $1+2+3=6$.

1. Le but de cette question est de montrer que si 2^p-1 est premier, alors $N = 2^{p-1}(2^p-1)$ est parfait. Notons q l'entier premier $q = 2^p-1$.
   (a) Ecrire la liste des diviseurs de N (on remarquera que l'écriture connue de N est sa décomposition en facteurs premiers).
   (b) Montrer que N est parfait.
2. Soit N un nombre parfait pair. En notant n l'exposant de 2 dans la décomposition de N en facteurs premiers, on peut écrire $N = 2^n q$ où q est impair. On note $s(N)$ la somme des diviseurs de N (N étant parfait, nous avons $s(N) = 2N$), et $s(q)$ la somme des diviseurs de q.
   (a) En remarquant que chaque diviseur d de q engendre $n+1$ diviseur de N: $d, 2d, \ldots, 2^n d$, montrer que
   $$s(N) = (1+2+2^2+\ldots+2^n)\times s(q), \quad \text{puis que} \quad 2N = (2^{n+1}-1)\times s(q).$$
   (b) En notant σ la somme des diviseurs de q autre que q, déduire de la question précédente que $q = \sigma(2^{n+1}-1)$.
   (c) En déduire que $\sigma = 1$, puis que q est premier égal à $2^{n+1}-1$.
3. Conclure.

Exercice 9: Astronomie et équation diophantienne (exo 74 page 499)

Le 27 décembre 2011, un astronome a observé le corps céleste A dont la fréquence d'apparition est 105 jours. Le 2 janvier 2012, ce même astronome a vu le corps céleste B qui apparaît tous les 81 jours. L'astronome veut connaître la date de la prochaine apparition simultanée des deux corps.

On note x le nombre de jours séparant la date cherchée du 27 décembre 2011.

1. Montrer qu'il existe des entiers u et v tels que $\begin{cases} x = 105u \\ x-6 = 81v \end{cases}$
2. Vérifier que u et v sont tels que $35u - 27v = 2$.
3. (a) A l'aide de l'algorithme d'Euclide, déterminer un couple d'entiers solution de l'équation $35x - 27y = 1$.
   (b) En déduire une solution particulière $(u_0; v_0)$ de l'équation $35u - 27v = 2$.
4. En remarquant que $35u - 27v = 2$ équivaut à $35(u-u_0) = 27(v-v_0)$, déterminer toutes les solutions de l'équation $35u - 27v = 2$.

5. Conclure.

Exercice 10 Suite et arithmétique (exo 76 page 499)

1. (a) Calculer $(1+\sqrt{6})^2$, $(1+\sqrt{6})^4$, $(1+\sqrt{6})^6$.
   (b) Appliquer l'algorithme d'Euclide aux entiers 847 et 342. Que peut-on déduire de ces deux entiers ?

2. Soit n un entier naturel non nul. On note a_n et b_n les entiers naturels tels que $(1+\sqrt{6})^n = a_n + b_n\sqrt{6}$.
   (a) Quelles sont les valeurs de a_1 et b_1 ? De a_2 et b_2?
   (b) Calculer a_{n+1} et b_{n+1} en fonction de a_n et b_n.

3. (a) Démontrer que 5 ne divise pas $a_n + b_n$ alors 5 ne divise pas non plus $a_{n+1} + b_{n+1}$.
   (b) En déduire que pour tout entier naturel n non nul, 5 ne divise pas $a_n + b_n$.

4. (a) Démontrer que si a_n et b_n sont premiers entre eux, alors a_{n+1} et b_{n+1} sont également premiers entre eux.
   (b) En déduire que pour tout entier naturel n non nul, a_n et b_n sont premiers entre eux.

Exercice 11 Nombres de Carmiochael (exo 78 et 78 page 500)

Partie A

D'après le petit théorème de Fermat, si p est un entier premier, alors pour tout entier a premier avec p, nous avons $a^{p-1} \equiv 1 \mod p$.
La réciproque de ce théorème est fausse: nous allons en effet démontrer ici l'existence de nombres entiers naturels p non premiers vérifiant l'hypothèse, pour tout entier a premier avec p, $a^{p-1} \equiv 1 \mod p$. Ces nombres sont appelés nombres de Carmichael (mathématicien américain, 1879-1967). Supposons qu'il existe un entier n tel que $n = p_1 \times p_2 \times \ldots \times p_k$ où $p_1, p_2, \ldots, p_k$ sont des nombres premiers deux à deux distincts et qui sont tels que, pour tout entier i, $1 \leq i \leq k$, $(p_i - 1)$ divise $(n-1)$.

1. Vérifier que l'entier n n'est pas premier.

2. On considère à présent un entier a premier avec n.
   (a) Démontrer que, pour tout entier $i \in \{1, \ldots, k\}$, l'entier a n'est pas divisible par p_i.
   (b) En déduire que pour tout i, $1 \leq i \leq k$, l'entier $a^{p_i - 1} \equiv 1 \mod p_i$.
   (c) En utilisant l'hupothèse *pour tout entier* $i \in \{1, \ldots, k\}$, $(p_i - 1)$ *divise* $(n-1)$, démontrer que pour tout $i \in \{1, \ldots, k\}$, $a^{n-1} \equiv 1 \mod p_i$.

3. (a) Démontrer que $a^{n-1} \equiv 1 \mod n$.
   (b) En déduire que n est un nombre de Carmichael.

4. Montrer que 561 est un nombre de Carmichael.

Partie B

On admet le théorème suivant, dû au mathématicien allemand Korselt:

> Un entier naturel n supérieur à 1 et non premier est un nombre de Carmichael si et seulement si pour tout entier premier p divisant n, on a p^2 ne divise pas n et $(p-1)$ divise $(n-1)$.

1. (a) Ecrire la décomposition en produit de facteurs premiers des nombres 561, 1 105 et 1 729.

(b) A l'aide du théorème précédent, vérifier que se sont des nombres de Carmichael.

Ces trois entiers sont les trois plus petits nombres de Carmichael.

2. Soit n un nombre de Carmichael et p l'un de ses facteurs premiers.

   (a) Montrer que $p \equiv 1 \mod p-1$, puis que $n \equiv 1 \mod p-1$.

   (b) En écrivant n sous la forme $\left(\frac{n}{p}\right) \times p$, vérifier que $\frac{n}{p}$ est un entier et démontrer que $\frac{n}{p} \equiv 1 \mod p-1$.

   (c) En déduire que si p est un facteur premier d'un nombre de Carmichael, alors le produit des autres facteurs premiers est congru à 1 modulo $(p-1)$.

3. A l'aide de la question précédente, démontrer qu'un nombre de Carmichael ne peut pas être le produit de deux nombres premiers.

4. Démontrer que tout nombre de Carmichael est impair.

Exercice 13: Indicateur d'Euler (exo 81 page 501)

On considère un entier n supérieur ou égal à 2 et l'ensemble $S_n = \{1, 2, 3, \ldots, n\}$. On considère également la décomposition en produit de facteurs premiers de l'entier n sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$ où l'on a $p_1 < p_2 < \ldots < p_m$.

Le but de cet exercice est d'établir un résultat, dont la généralisation sera admise, qui permet de déterminer le nombre d'entiers de S_n qui sont premiers avec n. On appelle $\varphi(n)$ ce nombre.

1. Dans cette question, on pose $n = 12$. On a donc $S_{12} = \{1, 2, 3, \ldots, 11, 12\}$. On prend au hasad, de manière équiprobable, un des entiers de cet ensemble, on appelle X la variable aléatoire égale à la valeur choisie. On a donc par exemple $P(X = 5) = \frac{1}{12}$.

   (a) Ecrire la décomposition en produit de facteurs premiers de 12.

   (b) On nomme A l'évènement *l'entier prélevé est un multiple de* 2 et B l'évènement *l'entier prélevé est un multiple de* 3. Calculer $P(A)$ et $P(B)$.

   (c) Quelle est la valeur de $\varphi(12)$? On note E l'évènement *l'entier prélevé est premuier avec* 12. Calculer $P(E)$.

2. On considère un entier naturel et l'on suppose que sa décomposition en facteurs premiers est $n = p^\alpha \times q^\beta$, où α et β sont des entiers naturels non nuls.

   Comme dans la question **1.** on prend un entier au hasard et de manière équiprobable dans l'ensemble $S_n = \{1, 2, \ldots, n\}$. On appelle X la variable aléatoire égale au nombre prélevé. On nomme C l'évènement *l'entier prélevé est un multiple de* p, D l'évènement *l'entier prélevé est un multiple de* q, et F l'évènement *l'entier prélevé est premier avec* n.

   (a) Combien y a-t-il de multiples de p appartenant à S_n ? En déduire que $P(C) = \frac{1}{p}$.

   (b) Calculer $P(D)$.

   (c) Démontrer l'équivalence suivante: p et q étant des nombres distincts, $p|a$ et $q|a$ si et seulement si $pq|a$.

   (d) Quel est l'évènement $C \cap D$? Combien a-t-il d'éléments ? Calculer $P(C \cap D)$.

   (e) En déduire que C et D sont des évènements indépendants.

   (f) Justifier que $F = \overline{C} \cap \overline{D}$.

   (g) Déduire des questions précédents que $\varphi(n) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)$.

Ce résultat se généralise à tout nombre entier supérieur ou égal à 2 ayant une décomposition en facteurs premiers de la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$. On admettra le résultat

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_m}\right).$$

La fonction ainsi définie est appelée *indicatrice d'Euler*.