Arithmétique dans $\mathbb{Z}$

1 Divisibilité, division euclidienne

Exercice 1

Sachant que l'on a $96842 = 256 \times 375 + 842$, déterminer, sans faire la division, le reste de la division du nombre 96842 par chacun des nombres 256 et 375.

Indication ▼ Correction ▼ Vidéo ■ [000251]

Exercice 2

Montrer que $\forall n \in \mathbb{N}$:

$$n(n+1)(n+2)(n+3) \text{ est divisible par } 24,$$

$$n(n+1)(n+2)(n+3)(n+4) \text{ est divisible par } 120.$$

Correction ▼ Vidéo ■ [000257]

Exercice 3

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

Correction ▼ Vidéo ■ [000267]

Exercice 4

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

Indication ▼ Correction ▼ Vidéo ■ [000254]

Exercice 5

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

Indication ▼ Correction ▼ Vidéo ■ [000250]

Exercice 6

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 vérifie $x^2 = 0 \pmod 8$ ou $x^2 = 4 \pmod 8$.
3. Soient a, b, c trois entiers impairs. Déterminer le reste modulo 8 de $a^2 + b^2 + c^2$ et celui de $2(ab + bc + ca)$.
4. En déduire que ces deux nombres ne sont pas des carrés puis que $ab + bc + ca$ non plus.

Indication ▼ Correction ▼ Vidéo ■ [000285]

2 pgcd, ppcm, algorithme d'Euclide

Exercice 7

Calculer le pgcd des nombres suivants :

1. 126, 230.
2. 390, 720, 450.
3. 180, 606, 750.

Correction ▼ Vidéo ■ [000290]

Exercice 8

Déterminer les couples d'entiers naturels de pgcd 18 et de somme 360. De même avec pgcd 18 et produit 6480.

Correction ▼ Vidéo ■ [000292]

Exercice 9

Calculer par l'algorithme d'Euclide : $\text{pgcd}(18480, 9828)$. En déduire une écriture de 84 comme combinaison linéaire de 18480 et 9828.

Correction ▼ Vidéo ■ [000296]

Exercice 10

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 $au + bv = p$.

Correction ▼ Vidéo ■ [000303]

Exercice 11

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

Indication ▼ Correction ▼ Vidéo ■ [000305]

3 Nombres premiers, nombres premiers entre eux

Exercice 12

Combien $15!$ admet-il de diviseurs ?

Indication ▼ Correction ▼ Vidéo ■ [000249]

Exercice 13

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

Indication ▼ Correction ▼ Vidéo ■ [000337]

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. $\text{pgcd}(2^a - 1, 2^b - 1) = 2^{\text{pgcd}(a,b)} - 1$.

Indication ▼ Correction ▼ Vidéo ■ [000336]

Exercice 15

Soit $a \in \mathbb{N}$ tel que $a^n + 1$ soit premier, montrer que $\exists k \in \mathbb{N}, n = 2^k$. Que penser de la conjecture : $\forall n \in \mathbb{N}, 2^{2^n} + 1$ est premier ?

Indication ▼ Correction ▼ Vidéo ■ [000349]

Exercice 16

Soit p un nombre premier.

1. Montrer que $\forall i \in \mathbb{N}, 0 < i < p$ on a :
$$C_p^i \text{ est divisible par } p.$$
2. Montrer par récurence que :
$$\forall p \text{ premier}, \forall a \in \mathbb{N}^*, \text{ on a } a^p - a \text{ est divisible par } p.$$

Indication ▼ Correction ▼ Vidéo ■ [000339]

Exercice 17

1. Montrer par récurrence que $\forall n \in \mathbb{N}, \forall k \geqslant 1$ on a :
$$2^{2^{n+k}} - 1 = \left(2^{2^n} - 1\right) \times \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1).$$
2. On pose $F_n = 2^{2^n} + 1$. Montrer que pour $m \neq n$, F_n et F_m sont premiers entre eux.
3. En déduire qu'il y a une infinité de nombres premiers.

Indication ▼ Correction ▼ Vidéo ■ [000341]

Exercice 18

Soit X l'ensemble des nombres premiers de la forme $4k+3$ avec $k \in \mathbb{N}$.

1. Montrer que X est non vide.
2. Montrer que le produit de nombres de la forme $4k+1$ est encore de cette forme.
3. On suppose que X est fini et on l'écrit alors $X = \{p_1, \dots, p_n\}$.
   Soit $a = 4p_1p_2 \dots p_n - 1$. Montrer par l'absurde que a admet un diviseur premier de la forme $4k+3$.
4. Montrer que ceci est impossible et donc que X est infini.

Correction ▼ Vidéo ■ [000348]

Indication pour l'exercice 1 ▲

Attention le reste d'une division euclidienne est plus petit que le quotient !

Indication pour l'exercice 4 ▲

Utiliser les modulos (ici modulo 8), un entier est divisible par 8 si et seulement si il est équivalent à 0 modulo 8. Ici vous pouvez commencer par calculer $7^n \pmod 8$.

Indication pour l'exercice 5 ▲

Il faut travailler modulo 13, tout d'abord réduire 100 modulo 13. Se souvenir que si $a \equiv b \pmod{13}$ alors $a^k \equiv b^k \pmod{13}$. Enfin calculer ce que cela donne pour les exposants $k = 1,2,3,\dots$ en essayant de trouver une règle générale.

Indication pour l'exercice 6 ▲

1. Écrire $n = 2p+1$.
2. Écrire $n = 2p$ et discuter selon que p est pair ou impair.
3. Utiliser la première question.
4. Par l'absurde supposer que cela s'écrive comme un carré, par exemple $a^2+b^2+c^2 = n^2$ puis discuter selon que n est pair ou impair.

Indication pour l'exercice 11 ▲

Commencer par simplifier l'équation ! Ensuite trouver une solution particulière (x_0, y_0) à l'aide de l'algorithme d'Euclide par exemple. Ensuite trouver un expression pour une solution générale.

Indication pour l'exercice 12 ▲

Il ne faut surtout pas chercher à calculer $15! = 1 \times 2 \times 3 \times 4 \times \cdots \times 15$, mais profiter du fait qu'il est déjà "presque" factorisé.

Indication pour l'exercice 13 ▲

Raisonner par l'absurde et utiliser le lemme de Gauss.

Indication pour l'exercice 14 ▲

Pour 1. utiliser l'égalité
$$x^b - 1 = (x-1)(x^{b-1} + \cdots + x + 1).$$
Pour 2. raisonner par contraposition et utiliser la question 1.
La question 3. est difficile ! Supposer $a \geq b$. Commencer par montrer que $\mathrm{pgcd}(2^a-1, 2^b-1) = \mathrm{pgcd}(2^a-2^b, 2^b-1) = \mathrm{pgcd}(2^{a-b}-1, 2^b-1)$. Cela vour permettra de comparer l'agorithme d'Euclide pour le calcul de $\mathrm{pgcd}(a,b)$ avec l'algorithme d'Euclide pour le calcul de $\mathrm{pgcd}(2^a-1, 2^b-1)$.

Indication pour l'exercice 15 ▲

Raisonner par contraposition (ou par l'absurde) : supposer que n n'est pas de la forme 2^k, alors n admet un facteur irréductible $p > 2$. Utiliser aussi $x^p + 1 = (x+1)(1 - x + x^2 - x^3 + \ldots + x^{p-1})$ avec x bien choisi.

Indication pour l'exercice 16 ▲

1. Écrire
$$C_p^i = \frac{p(p-1)(p-2)\dots(p-(i+1))}{i!}$$
et utiliser le lemme de Gauss ou le lemme d'Euclide.
2. Raisonner avec les modulos, c'est-à-dire prouver $a^p \equiv a \pmod p$.

Indication pour l'exercice 17 ▲

1. Il faut être très soigneux : n est fixé une fois pour toute, la récurrence se fait sur $k \in \mathbb{N}$.
2. Utiliser la question précédente avec $m = n+k$.

3. Par l'absurde, supposer qu'il y a seulement N nombres premiers, considérer $N+1$ nombres du type F_i. Appliquer le "principe du tiroir" : *si vous avez $N+1$ chaussettes rangées dans N tiroirs alors il existe (au moins) un tiroir contenant (plus de) deux chaussettes.*

Correction de l'exercice 1 ▲

La seule chose à voir est que pour une division euclidienne le reste doit être plus petit que le quotient. Donc les divisions euclidiennes s'écrivent : $96842 = 256\times 378 + 74$ et $96842 = 258\times 375 + 92$.

Correction de l'exercice 2 ▲

Il suffit de constater que pour 4 nombres consécutifs il y a nécessairement : un diviseur de 2, un diviseur de 3, un diviseur de 4 (tous distincts). Donc le produit de 4 nombres consécutifs est divisible par $2\times 3\times 4 = 24$.

Correction de l'exercice 3 ▲

Ecrire $n = p^2+q^2$ et étudier le reste de la division euclidienne de n par 4 en distinguant les différents cas de parité de p et q.

Correction de l'exercice 4 ▲

Raisonnons modulo 8 :

$$7 \equiv -1 \pmod 8.$$

Donc

$$7^n + 1 \equiv (-1)^n + 1 \pmod 8.$$

Le reste de la division euclidienne de 7^n+1 par 8 est donc $(-1)^n+1$ donc Si n est impair alors 7^n+1 est divisible par 8. Et si n est pair 7^n+1 n'est pas divisible par 8.

Correction de l'exercice 5 ▲

Il sagit de calculer 100^{1000} modulo 13. Tout d'abord $100 \equiv 9 \pmod{13}$ donc $100^{1000} \equiv 9^{1000} \pmod{13}$. Or $9^2 \equiv 81 \equiv 3 \pmod{13}$, $9^3 \equiv 9^2.9 \equiv 3.9 \equiv 1 \pmod{13}$, Or $9^4 \equiv 9^3.9 \equiv 9 \pmod{13}$, $9^5 \equiv 9^4.9 \equiv 9.9 \equiv 3 \pmod{13}$. Donc $100^{1000} \equiv 9^{1000} \equiv 9^{3.333+1} \equiv (9^3)^{333}.9 \equiv 1^{333}.9 \equiv 9 \pmod{13}$.

Correction de l'exercice 6 ▲

1. Soit n un nombre impair, alors il s'écrit $n = 2p+1$ avec $p \in \mathbb{N}$. Maintenant $n^2 = (2p+1)^2 = 4p^2+4p+1 = 4p(p+1)+1$. Donc $n^2 \equiv 1 \pmod 8$.
2. Si n est pair alors il existe $p \in \mathbb{N}$ tel que $n = 2p$. Et $n^2 = 4p^2$. Si p est pair alors p^2 est pair et donc $n^2 = 4p^2$ est divisible par 8, donc $n^2 \equiv 0 \pmod 8$. Si p est impair alors p^2 est impair et donc $n^2 = 4p^2$ est divisible par 4 mais pas par 8, donc $n^2 \equiv 4 \pmod 8$.
3. Comme a est impair alors d'après la première question $a^2 \equiv 1 \pmod 8$, et de même $c^2 \equiv 1 \pmod 8$, $c^2 \equiv 1 \pmod 8$. Donc $a^2+b^2+c^2 \equiv 1+1+1 \equiv 3 \pmod 8$. Pour l'autre reste, écrivons $a = 2p+1$ et $b = 2q+1$, $c = 2r+1$, alors $2ab = 2(2p+1)(2q+1) = 8pq+4(p+q)+2$. Alors $2(ab+bc+ca) = 8pq+8qr+8pr+8(p+q+r)+6$, donc $2(ab+bc+ca) \equiv 6 \pmod 8$.
4. Montrons par l'absurde que le nombre $a^2+b^2+c^2$ n'est pas le carré d'un nombre entier. Supposons qu'il existe $n \in \mathbb{N}$ tel que $a^2+b^2+c^2 = n^2$. Nous savons que $a^2+b^2+c^2 \equiv 3 \pmod 8$. Si n est impair alors $n^2 \equiv 1 \pmod 8$ et si n est pair alors $n^2 \equiv 0 \pmod 8$ ou $n^2 \equiv 4 \pmod 8$. Dans tous les cas n^2 n'est pas congru à 3 modulo 8. Donc il y a une contradiction. La conclusion est que l'hypothèse de départ est fausse donc $a^2+b^2+c^2$ n'est pas un carré. Le même type de raisonnement est valide pour $2(ab+bc+ca)$.

   Pour $ab+bc+ca$ l'argument est similaire : d'une part $2(ab+bc+ca) \equiv 6 \pmod 8$ et d'autre part si, par l'absurde, on suppose $ab+bc+ca = n^2$ alors selon la parité de n nous avons $2(ab+bc+ca) \equiv 2n^2 \equiv 2 \pmod 8$ ou à $0 \pmod 8$. Dans les deux cas cela aboutit à une contradiction. Nous avons montrer que $ab+bc+ca$ n'est pas un carré.

Correction de l'exercice 7 ▲

Il s'agit ici d'utiliser la décomposition des nombres en facteurs premiers.

1. $126 = 2.3^2.7$ et $230 = 2.5.23$ donc le pgcd de 126 et 230 est 2.
2. $390 = 2.3.5.13$, $720 = 2^4.3^2.5$, $450 = 2.3^2.5^2$ et donc le pgcd de ces trois nombres est $2.3.5 = 30$.
3. $\mathrm{pgcd}(180,606,750) = 6$.

Correction de l'exercice 8 ▲

Soient a,b deux entiers de pgcd 18 et de somme 360. Soit a',b' tel que $a = 18a'$ et $b = 18b'$. Alors a' et b' sont premiers entre eux, et leur somme est $360/18 = 20$.

Nous pouvons facilement énumérer tous les couples d'entiers naturels (a',b') $(a' \leqslant b')$ qui vérifient cette condition, ce sont les couples :

$$(1,20),(3,17),(7,13),(9,11).$$

Pour obtenir les couples (a,b) recherchés ($a \leqslant b$), il suffit de multiplier les couples précédents par 18 :

$$(18,342),(54,306),(126,234),(162,198).$$

Correction de l'exercice 9 ▲

1. $\mathrm{pgcd}(18480,9828) = 84$;
2. $25 \times 18480 + (-47) \times 9828 = 84$.

Correction de l'exercice 10 ▲

1. $a = 9b + 10$.
2. Calculons le pgcd par l'algorithme d'Euclide. $a = 9b + 10$, $b = 12345678 \times 10 + 9$, $10 = 1 \times 9 + 1$. Donc le pgcd vaut 1 ;
3. Nous reprenons les équations précédentes en partant de la fin : $1 = 10 - 9$, puis nous remplaçons 9 grâce à la deuxième équation de l'algorithme d'Euclide : $1 = 10 - (b - 12345678 \times 10) = -b + 1234679 \times 10$. Maintenant nous remplaçons 10 grâce à la première équation : $1 = -b + 12345679(a - 9b) = 12345679a - 111111112b$.

Correction de l'exercice 11 ▲

En divisant par 45 (qui est le pgcd de $1665, 1035, 45$) nous obtenons l'équation équivalente :

$$37x + 23y = 1 \qquad (E)$$

Comme le pgcd de 37 et 23 est 1, alors d'après le théorème de Bézout cette équation (E) a des solutions.
L'algorithme d'Euclide pour le calcul du pgcd de 37 et 23 fourni les coefficients de Bézout : $37 \times 5 + 23 \times (-8) = 1$. Une solution particulière de (E) est donc $(x_0, y_0) = (5, -8)$.
Nous allons maintenant trouver l'expression générale pour les solutions de l'équation (E). Soient (x,y) une solution de l'équation $37x + 23y = 1$. Comme (x_0, y_0) est aussi solution, nous avons $37x_0 + 23y_0 = 1$. Faisons la différence de ces deux égalités pour obtenir $37(x - x_0) + 23(y - y_0) = 0$. Autrement dit

$$37(x - x_0) = -23(y - y_0) \quad (*)$$

On en déduit que $37|23(y - y_0)$, or $\mathrm{pgcd}(23,37) = 1$ donc par le lemme de Gauss, $37|(y - y_0)$. (C'est ici qu'il est important d'avoir divisé par 45 dès le début !) Cela nous permet d'écrire $y - y_0 = 37k$ pour un $k \in \mathbb{Z}$.
Repartant de l'égalité $(*)$: nous obtenons $37(x - x_0) = -23 \times 37 \times k$. Ce qui donne $x - x_0 = -23k$. Donc si (x,y) est solution de (E) alors elle est de la forme : $(x,y) = (x_0 - 23k, y_0 + 37k)$, avec $k \in \mathbb{Z}$.
Réciproquement pour chaque $k \in \mathbb{Z}$, si (x,y) est de cette forme alors c'est une solution de (E) (vérifiez-le !).
Conclusion : les solutions sont

$$\left\{(5 - 23k, -8 + 37k) \mid k \in \mathbb{Z}\right\}.$$

Correction de l'exercice 12 ▲

Écrivons la décomposition de $15! = 1.2.3.4\ldots15$ en facteurs premiers. $15! = 2^{11}.3^6.5^3.7^2.11.13$. Un diviseur de $15!$ s'écrit $d = 2^\alpha.3^\beta.5^\gamma.7^\delta.11^\varepsilon.13^\eta$ avec $0 \le \alpha \le 11$, $0 \le \beta \le 6$, $0 \le \gamma \le 3$, $0 \le \delta \le 2$, $0 \le \varepsilon \le 1$, $0 \le \eta \le 1$. De plus tout nombre d de cette forme est un diviseur de $15!$. Le nombre de diviseurs est donc $(11+1)(6+1)(3+1)(2+1)(1+1)(1+1) = 4032$.

Correction de l'exercice 13 ▲

Soit a et b des entiers premiers entre eux. Raisonnons par l'absurde et supposons que ab et $a+b$ ne sont pas premiers entre eux. Il existe alors un nombre premier divisant ab et $a+b$. Par le lemme d'Euclide comme $p|ab$ alors $p|a$ ou $p|b$. Par exemple supposons que $p|a$. Comme $p|a+b$ alors p divise aussi $(a+b)-a$, donc $p|b$. δ ne divise pas b cela implique que δ et b sont premiers entre eux.
D'après le lemme de Gauss, comme δ divise ab et δ premier avec b alors δ divise a. Donc p est un facteur premier de a et de b ce qui est absurde.

Correction de l'exercice 14 ▲

1. Nous savons que
$$x^b - 1 = (x-1)(x^{b-1} + \cdots + x + 1),$$
pour $x = 2^a$ nous obtenons :
$$2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)\left(2^{a(b-1)} + \cdots + 2^a + 1\right).$$
Donc $(2^a - 1)|(2^{ab} - 1)$.

2. Montrons la contraposée. Supposons que p ne soit pas premier. Donc $p = ab$ avec $1 < p, q < a$. Par la question précédente $2^a - 1$ divise $2^p - 1$ (et $1 < 2^a - 1 < 2^p - 1$). Donc $2^p - 1$ n'est pas un nombre premier.
3. Nous supposons $a \geq b$. Nous allons montrer que faire l'algorithme d'Euclide pour le couple $(2^a - 1, 2^b - 1)$ revient à faire l'algorithme d'Euclide pour (a, b). Tout d'abord rappellons la formule qui est à la base de l'algorithme d'Euclide : $\text{pgcd}(a, b) = \text{pgcd}(a - b, b)$. Appliqué à $2^a - 1$ et $2^b - 1$ cela donne directement $\text{pgcd}(2^a - 1, 2^b - 1) = \text{pgcd}(2^a - 2^b, 2^b - 1)$. Mais $2^a - 2^b = 2^b(2^{a-b} - 1)$ d'où $\text{pgcd}(2^a - 1, 2^b - 1) = \text{pgcd}(2^b(2^{a-b} - 1), 2^b - 1) = \text{pgcd}(2^{a-b} - 1, 2^b - 1)$. La dernière égalité vient du fait 2^b et $2^b - 1$ sont premiers entre eux (deux entiers consécutifs sont toujours premiers entre eux).

   Nous avons montrer : $\text{pgcd}(2^a - 1, 2^b - 1) = \text{pgcd}(2^{a-b} - 1, 2^b - 1)$. Cette formule est à mettre en parallèle de $\text{pgcd}(a, b) = \text{pgcd}(a - b, b)$. En itérant cette formule nous obtenons que si $a = bq + r$ alors : $\text{pgcd}(2^a - 1, 2^b - 1) = \text{pgcd}(2^{a-bq} - 1, 2^b - 1) = \text{pgcd}(2^r - 1, 2^b - 1)$ à comparer avec $\text{pgcd}(a, b) = \text{pgcd}(a - bq, b) = \text{pgcd}(r, b)$. Nous avons notre première étape de l'algorithme d'Euclide. En itérant l'algorithme d'Euclide pour (a, b), nous nous arêtons au dernier reste non nul : $\text{pgcd}(a, b) = \text{pgcd}(b, r) = \cdots = \text{pgcd}(r_n, 0) = r_n$. Ce qui va donner pour nous $\text{pgcd}(2^a - 1, 2^b - 1) = \text{pgcd}(2^b - 1, 2^r - 1) = \cdots = \text{pgcd}(2^{r_n} - 1, 2^0 - 1) = 2^{r_n} - 1$.

   Bilan : $\text{pgcd}(2^a - 1, 2^b - 1) = 2^{\text{pgcd}(a,b)} - 1$.

Correction de l'exercice 15 ▲

1. Supposons que $a^n + 1$ est premier. Nous allons montrer la contraposée. Supposons que n n'est pas de la forme 2^k, c'est-à-dire que $n = p \times q$ avec p un nombre premier > 2 et $q \in \mathbb{N}$. Nous utilisons la formule

$$x^p + 1 = (x + 1)(1 - x + x^2 - x^3 + \ldots + x^{p-1})$$

   avec $x = a^q$:

$$a^n + 1 = a^{pq} + 1 = (a^q)^p + 1 = (a^q + 1)(1 - a^q + (a^q)^2 + \cdots + (a^q)^{p-1}).$$

   Donc $a^q + 1$ divise $a^n + 1$ et comme $1 < a^q + 1 < a^n + 1$ alors $a^n + 1$ n'est pas premier. Par contraposition si $a^n + 1$ est premier alor $n = 2^k$.
2. Cette conjecture est fausse, mais pas facile à vérifier sans une bonne calculette ! En effet pour $n = 5$ nous obtenons :

$$2^{2^5} + 1 = 4294967297 = 641 \times 6700417.$$

Correction de l'exercice 16 ▲

1. Étant donné $0 < i < p$, nous avons

$$C_p^i = \frac{p!}{i!(p-i)!} = \frac{p(p-1)(p-2)\ldots(p-(i+1))}{i!}$$

   Comme C_p^i est un entier alors $i!$ divise $p(p-1)\ldots(p-(i+1))$. Mais $i!$ et p sont premiers entre eux (en utilisant l'hypothèse $0 < i < p$). Donc d'après le théorème de Gauss : $i!$ divise $(p-1)\ldots(p-(i+1))$, autrement dit il existe $k \in \mathbb{Z}$ tel que $ki! = (p-1)\ldots(p-(i+1))$. Maintenant nous avons $C_p^i = pk$ donc p divise C_p^i.
2. Il s'agit de montrer le petit théorème de Fermat : pour p premier et $a \in \mathbb{N}^*$, alors $a^p \equiv a \pmod p$. Fixons p. Soit l'assertion

$$(\mathscr{H}_a) \quad a^p \equiv a \pmod p.$$

   Pour $a = 1$ cette assertion est vraie ! Étant donné $a \geq 1$ supposons que $\mathscr{H}_a$ soit vraie. Alors

$$(a+1)^p = \sum_{i=0}^{p} C_p^i a^i.$$

   Mais d'après la question précédente pour $0 < i < p$, p divise C_p^i. En termes de modulo nous obtenons :

$$(a+1)^p \equiv C_p^0 a^0 + C_p^p a^p \equiv 1 + a^p \pmod p.$$

   Par l'hypothèse de récurrence nous savons que $a^p \equiv a \pmod p$, donc

$$(a+1)^p \equiv a + 1 \pmod p.$$

   Nous venons de prouver que $\mathscr{H}_{a+1}$ est vraie. Par le principe de récurrence alors quelque soit $a \in \mathbb{N}^*$ nous avons :

$$a^p \equiv a \pmod p.$$

Correction de l'exercice 17 ▲

1. Fixons n et montrons la récurrence sur $k \in \mathbb{N}$. La formule est vraie pour $k = 0$. Supposons la formule vraie au rang k. Alors

$$\begin{aligned}(2^{2^n} - 1) \times \prod_{i=0}^{k}(2^{2^{n+i}} + 1) &= (2^{2^n} - 1) \times \prod_{i=0}^{k-1}(2^{2^{n+i}} + 1) \times (2^{2^{n+k}} + 1) \\ &= (2^{2^{n+k}} - 1) \times (2^{2^{n+k}} + 1) = (2^{2^{n+k}})^2 - 1 = 2^{2^{n+k+1}} - 1.\end{aligned}$$

Nous avons utiliser l'hypothèse de récurrence dans ces égalités. Nous avons ainsi montrer la formule au rang $k+1$. Et donc par le principe de récurrence elle est vraie.

2. Écrivons $m = n + k$, alors l'égalité précédente devient :

$$F_m + 2 = (2^{2^n} - 1) \times \prod_{i=n}^{m-1} F_i.$$

Soit encore :

$$F_n \times (2^{2^n} - 1) \times \prod_{i=n+1}^{m-1} F_i \quad - \quad F_m = 2.$$

Si d est un diviseur de F_n et F_m alors d divise 2 (ou alors on peut utiliser le théorème de Bézout). En conséquent $d = 1$ ou $d = 2$. Mais F_n est impair donc $d = 1$. Nous avons montrer que tous diviseurs de F_n et F_m est 1, cela signifie que F_n et F_m sont premiers entre eux.

3. Supposons qu'il y a un nombre fini de nombres premiers. Nous les notons alors $\{p_1, \ldots, p_N\}$. Prenons alors $N+1$ nombres de la famille F_i, par exemple $\{F_1, \ldots, F_{N+1}\}$. Chaque F_i, $i = 1, \ldots, N+1$ est divisible par (au moins) un facteur premier p_j, $j = 1, \ldots, N$. Nous avons $N+1$ nombres F_i et seulement N facteurs premiers p_j. Donc par le principe des tiroirs il existe deux nombres distincts F_k et $F_{k'}$ (avec $1 \leq k, k' \leq N+1$) qui ont un facteur premier en commun. En conséquent F_k et $F_{k'}$ ne sont pas premiers entre eux. Ce qui contredit la question précédente. Il existe donc une infinité de nombres premiers.

Correction de l'exercice 18 ▲

1. X est non vide car, par exemple pour $k = 2$, $4k+3 = 11$ est premier.
2. $(4k+1)(4\ell+1) = 16k\ell + 4(k+\ell) + 1 = 4(4k\ell + k + \ell) + 1$. Si l'on note l'entier $k' = 4k\ell + k + \ell$ alors $(4k+1)(4\ell+1) = 4k' + 1$, ce qui est bien de la forme voulue.
3. Remarquons que 2 est le seul nombre premier pair, les autres sont de la forme $4k+1$ ou $4k+3$. Ici a n'est pas divisible par 2, supposons –par l'absurde– que a n'a pas de diviseur de la forme $4k+3$, alors tous les diviseurs de a sont de la forme $4k+1$. C'est-à-dire que a s'écrit comme produit de nombre de la forme $4k+1$, et par la question précédente a peut s'écrire $a = 4k' + 1$. Donc $a \equiv 1 \pmod 4$. Mais comme $a = 4p_1p_2 \ldots p_n - 1$, $a \equiv -1 \equiv 3 \pmod 4$. Nous obtenons une contradiction. Donc a admet une diviseur premier p de la forme $p = 4\ell + 3$.
4. Dans l'ensemble $X = \{p_1, \ldots, p_n\}$ il y a tous les nombres premiers de la formes $4k+3$. Le nombre p est premier et s'écrit $p = 4\ell + 3$ donc p est un élément de X, donc il existe $i \in \{1, \ldots, n\}$ tel que $p = p_i$. Raisonnons modulo $p = p_i$: $a \equiv 0 \pmod p$ car p divise a. D'autre part $a = 4p_1 \ldots p_n - 1$ donc $a \equiv -1 \pmod p$. (car p_i divise $p_1 \ldots p_n$). Nous obtenons une contradiction, donc X est infini : il existe une infinité de nombre premier de la forme $4k+3$. Petite remarque, tous les nombres de la forme $4k+3$ ne sont pas des nombres premiers, par exemple pour $k = 3$, $4k+3 = 15$ n'est pas premier.
