Arithmétique dans $\mathbb{Z}$

1 Divisibilité, division euclidienne

Exercice 1 Combien 15! admet-il de diviseurs ?

Exercice 2 Trouver le reste de la division par 13 du nombre 100^{1000}.

Exercice 3 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.

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.

Exercice 5 Montrer que $\forall n \in \mathbb{N}$:

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

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

Exercice 6 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.

Exercice 7

1. Pour tout couple de nombres réels (x, y) montrer, par récurrence, que pour tout $n \in \mathbb{N}^*$ on a la relation

$$(*)\ x^n - y^n = (x-y).\sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

Indication : on pourra écrire de deux manières différentes la quantité $y(x^n - y^n) + (x-y)x^n$.

2. Soit (a, b, p) des entiers éléments de $\mathbb{N}$. En utilisant la formule $(*)$, montrer que s'il existe un entier $l \in \mathbb{N}$ tel que $b = a + pl$, alors pour tout $n \in \mathbb{N}^*$, il existe un entier $m \in \mathbb{N}$ tel que $b^n = a^n + pm$.
3. Soient a, b, p des entiers éléments de $\mathbb{N}$, en utilisant la question 2, montrer que si $a - b$ est divisible par p,

$$\sum_{k=0}^{p-1} a^k b^{p-k-1}$$

est aussi divisible par p. En déduire, à l'aide de la question 2 et de la formule $(*)$, que si $a - b$ est divisible par p^n i.e. il existe un entier $l \in \mathbb{N}$ tel que $a - b = l.p^n$, alors $a^p - b^p$ est divisible par p^{n+1}.

Exercice 8

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 $x^2 = 0[8]$ ou $x^2 = 4[8]$.
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.

2 pgcd, ppcm, algorithme d'Euclide

Exercice 9 Calculer le pgcd des nombres suivants :

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

Exercice 10 Déterminer les couples d'entiers naturels de pgcd 18 et de somme 360. De même avec pgcd 18 et produit 6480.

Exercice 11 Calculer par l'algorithme d'Euclide : $18480 \wedge 9828$. En déduire une écriture de 84 comme combinaison linéaire de 18480 et 9828.

Exercice 12 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 $au + bv = p$.

Exercice 13 Résoudre dans $\mathbb{Z}$: $1665x + 1035y = 45$.

3 Nombres premiers, nombres premiers entre eux

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

1. $(2^a - 1) | (2^{ab} - 1)$;
2. $(2^a - 1) \wedge (2^b - 1) = (2^{a \wedge b} - 1)$;
3. $(2^a - 1$ premier $) \Rightarrow (a$ premier $)$.

Exercice 15 Démontrer que, si a et b sont des entiers premiers entre eux, il en est de même des entiers $a + b$ et ab.

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 :
$$\forall p \text{ premier}, \forall a \in \mathbb{N}^*, \text{ on a } a^p - a \text{ est divisible par } p.$$

Exercice 17 (Nombres de Fermat)

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.

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.

Exercice 19 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 ?

Arithmétique dans $\mathbb{Z}$

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

Indication 3 Attention le reste d'une division euclidienne est plus petit que le quotient !

Indication 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 $7^n[8]$.

Indication 8

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 14 Pour 1. et 3. utiliser l'égalité

$$x^b - 1 = (x - 1)(x^{b-1} + \cdots + x + 1).$$

Indication 15 Raisonner par l'absurde et utiliser le théorème de Gauss.

Indication 16

1. Écrire
$$C_p^i = \frac{p(p-1)(p-2)\ldots(p-(i+1))}{i!}$$
et utiliser le théorème de Gauss.
2. Raisonner avec les modulos, c'est-à-dire prouver $a^p \equiv a[p]$.

Indication 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.*

Indication 19 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.

Arithmétique dans $\mathbb{Z}$

Correction 1 Écrivons la décomposition de $15! = 1.2.3.4\ldots 15$ 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 $0 \leqslant \alpha \leqslant 11$, $0 \leqslant \beta \leqslant 6$, $0 \leqslant \gamma \leqslant 3$, $0 \leqslant \delta \leqslant 2$, $0 \leqslant \varepsilon \leqslant 1$, $0 \leqslant \eta \leqslant 1$. 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 2 Il sagit de calculer 100^{1000} modulo 13. Tout d'abord $100 \equiv 9[13]$ donc $100^{1000} \equiv 9^{1000}[13]$. Or $9^2 \equiv 81 \equiv 3[13]$, $9^3 \equiv 9^2.9 \equiv 3.9 \equiv 1[13]$, Or $9^4 \equiv 9^3.9 \equiv 9[13]$, $9^5 \equiv 9^4.9 \equiv 9.9 \equiv 3[13]$. Donc $100^{1000} \equiv 9^{1000} \equiv 9^{3.333+1} \equiv (9^3)^{333}.9 \equiv 1^{333}.9 \equiv 9[13]$.

Correction 3 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 4 Raisonnons modulo 8 :

$$7 \equiv -1(\mod 8).$$

Donc

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

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 5 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 6 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 7 Pour 2. Si p divise $b - a$ alors p divise aussi $b^n - a^n$ d'après la formule $(*)$.
Pour 3. On utilise le résultat de la question précédente avec $n = p - k - 1$ pour écrire b^{p-k-1} en fonction de a^{p-k-1} modulo p dans

$$\sum_{k=0}^{p-1} a^k b^{p-k-1}.$$

On peut alors conclure.

Correction 8

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 $n^2 \equiv 1[8]$.

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 $n^2 \equiv 0[8]$. Si p est impair alors p^2 est impair et donc $n^2 = 4p^2$ est divisible par 4 mais pas par 8, donc $n^2 \equiv 4[8]$.
3. Comme a est impair alors d'après la première question $a^2 \equiv 1[8]$, et de même $c^2 \equiv 1[8]$, $c^2 \equiv 1[8]$. Donc $a^2 + b^2 + c^2 \equiv 1 + 1 + 1 \equiv 3[8]$. 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 $2(ab + bc + ca) \equiv 6[8]$.
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 $a^2 + b^2 + c^2 \equiv 3[8]$. Si n est impair alors $n^2 \equiv 1[8]$ et si n est pair alors $n^2 \equiv 0[8]$ ou $n^2 \equiv 4[8]$. 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 $ab + bc + ca$ il faut rafiner un peut l'argument. Si $ab + bc + ca = n^2$ alors selon la parité de n nous avons $2(ab + bc + ca) \equiv 2n^2 \equiv 2[8]$ ou à $0[8]$. Nous remarquons enfin que ab, bc, ca sont trois nombres impairs, et donc leur somme est impaire. Par conséquent n est impair (sinon n^2 serait pair), donc $ab + bc + ca =\equiv n^2 \equiv 1[8]$. Ce qui aboutit à une contradiction. Nous avons montrer que $ab + bc + ca$ n'est pas un carré.

Correction 9 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 10 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 :

$$(1, 20), (3, 17), (6, 14), (7, 13), (8, 12), (9, 11).$$

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

$$(18, 360), (54, 306), (108, 252), (126, 234), (144, 216), (162, 198).$$

Correction 11 1. $\mathrm{pgcd}(18480, 9828) = 84$;

2. $25 \times 18480 + (-47) \times 9828 = 84$.

Correction 12 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 : $1 = -b + 12345679(a - 9b) = 1234579a - 111111112b$.

Correction 13 En divisant par 45 nous obtenons l'équation équivalente : $37x + 83y = 1$. Comme le pgcd de 37 et 83 est 1, donc d'après le théorème de Bézout cette équation a des solutions. Par exemple une solution particulière est $(x_0, y_0) = (9, -4)$. Les solutions sont exactement les couples $(x, y) = (x_0 - 83k, y_0 + 37k)$, pour $k \in \mathbb{Z}$.

Correction 14 Pour 3. Montrons plutôt la contraposée. Soit $p = ab$ un entier avec $a, b \in \mathbb{N}^*$. Montrons que $2^p - 1$ n'est pas premier.
Nous savons que

$$x^b - 1 = (x - 1)(x^{b-1} + \cdots + x + 1),$$

pour $x = 2^a$ nous obtenons :

$$2^p - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)\left(2^{a(b-1)} + \cdots + 2^a + 1\right).$$

De plus $2^a - 1$ n'est ni 1 ni 2^{ab} donc nous avons décomposer $2^p - 1$ en produit d'entier différents de 1. Donc $2^p - 1$ n'est pas premier.
Par contraposition nous obtenons que si $2^p - 1$ est premier alors p est premier.

Correction 15 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 δ un nombre premier divisant ab et $a + b$. L'entier δ ne peut diviser a et b car a et b sont premiers entre eux. Par exemple supposons que δ ne divise pas b cela implique que δ et b sont premiers entre eux.
D'après le théorème de Gauss, comme δ divise ab et δ premier avec b alors δ divise a.
Maintenant δ divise a et divise $a + b$ alors δ divise $a + b - a = b$. δ est un facteur premier de a et de b ce qui est absurde.

Correction 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 $a^p \equiv a[p]$. Fixons p. Soit l'assertion
$$(\mathcal{H}_a) \quad a^p \equiv a[p].$$
Pour $a = 1$ cette assertion est vraie ! Étant donné $a \leqslant 1$ supposons que $\mathcal{H}_a$ 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 :
$$(a+1)^p \equiv C_p^0 a^0 + C_p^p a^p \equiv 1 + a^p[p].$$
Par l'hypothèse de récurrence nous savons que $a^p \equiv a[p]$, donc
$$(a+1)^p \equiv a + 1[p].$$
Nous venons de prouver que $\mathcal{H}_{a+1}$ est vraie. Par le principe de récurrence alors quelque soit $a \in \mathbb{N}^*$ nous avons :
$$a^p \equiv a[p].$$

Correction 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 $1 \leqslant k,k' \leqslant N+1$) 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 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 $a \equiv 1[4]$. Mais comme $a = 4p_1p_2\ldots p_n - 1$, $a \equiv -1 \equiv 3[4]$. 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 $p = p_i$: $a \equiv 0[p]$ car p divise a. D'autre part $a = 4p_1\ldots p_n - 1$ donc $a \equiv -1[p]$. (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.

Correction 19 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 $x = a^q$:

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

Ces deux derniers facteurs sont > 1. Et donc $a^n + 1$ 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 :

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