TD 09
Arithmétique

1 Exercices corrigés en classe

Exercice 1. Soit n dans $\mathbb{N}^*$. Montrer que 11 divise $2^{6n-5}+3^{2n}$ et que 17 divise $3\times5^{2n-1}+2^{3n-2}$.

Correction

Déjà, $2^{6n-5} = 2^{6(n-1)+1}$. On remarque que $2^6 = 64 \equiv -2[11]$ donc $2^{6(n-1)} \equiv (-2)^{n-1}[11]$. Donc $2^{6n-5} \equiv -(-2)^n[11]$. Ensuite, $3^2 = 9 \equiv -2[11]$ donc $3^{2n} \equiv (-2)^n[11]$ donc $2^{6n-5}+3^{2n} \equiv 0[11]$, d'où le résultat.
De même, on écrit que $3 \times 5^{2n-1} + 2^{3n-2} = 3 \times 5^{2(n-1)+1} + 2^{3(n-1)+1}$. Or, $5^2 \equiv 8[17]$, et $2^3 \equiv 8[17]$, donc

$$3 \times 5^{2n-1} + 2^{3n-2} \equiv 3 \times 5 \times 8^{n-1} + 2 \times 8^{n-1} \equiv (15+2) \times 8^{n-1} \equiv 0[17],$$

d'où le résultat.

Exercice 2. Montrer que pour tout k dans $\mathbb{N}^*$, il existe a dans $\mathbb{Z}$ tel que $[\![a, a+k]\!]$ ne contienne aucun nombre premier.

Correction

Prenons $a = (k+2)! + 2$. Alors aucun entier entre a et $a+k$ ne sera premier !

Exercice 3. Soient a et b deux entiers tels que $a^2|b^2$. Montrer que $a|b$.

Correction

Soit p un nombre premier. Par hypothèse, $v_p(a^2) \leqslant v_p(b^2)$, i.e. $2v_p(a) \leqslant 2v_p(b)$, donc $v_p(a) \leqslant v_p(b)$. Donc a divise b.

Exercice 4. *Nombres de Mersenne*.

1. Soit $n > 1$. Montrer que si $a^n - 1$ est premier, alors $a = 2$ et n est premier.

Correction

Supposons $a \neq 2$. Alors $a^n - 1 = (a-1)(a^{n-1} + \cdots + a + 1)$ et $a - 1 > 1$ donc $a-1$ est un diviseur de $a^n - 1$ différent de 1 et de $a^n - 1$, donc $a^n - 1$ n'est pas premier.
Supposons n non premier. Alors on dispose de m et de p différents de 1 tels que $n = mp$. Donc

$$a^{mp} - 1 = (a^m)^p - 1 = (a^m - 1)(a^{m(p-1)} + \ldots {}^{m}_{a} + 1),$$

et $a^m - 1$ est un diviseur de $a^n - 1$ différent de $a^n - 1$ et de 1. Donc $a^n - 1$ n'est pas premier.

2. On pose, pour n dans $\mathbb{N}$, $M_n = 2^n - 1$. Montrer que

$$M_k \wedge M_l = M_{k \wedge l}.$$

(on regardera les restes dans l'algorithme d'Euclide pour M_k et M_l).

Correction

Effectuons la division euclidienne de M_k par M_ℓ. On écrit $k = 0\ell q + r$, donc

$$2^k - 1 = 2^{\ell q + r} - 1 = 2^r(2^{\ell q} - 1) + 2^r - 1 = (2^\ell - 1)2^r(2^{\ell(q-1)} + \cdots + 2^\ell + 1) + 2^r - 1.$$

Posons $Q = 2^r(2^{\ell(q-1)} + \cdots + 2^\ell + 1)$. Alors

$$2^k - 1 = (2^\ell - 1)Q + 2^r - 1,$$

et $2^r - 1 < 2^\ell - 1$. Donc le reste de la division de M_k par M_ℓ est M_r où r est le reste de la division de k par ℓ. Donc si (a_n) est la suite des entiers de l'algorithme d'Euclide pour k et ℓ, (M_{a_n}) est la suite des entiers de l'algorithme d'Euclide pour M_k et M_ℓ. D'où le résultat.

Exercice 5. Soit n un entier naturel non nul, p un nombre premier. Démontrer que

$$v_p(n!) = \sum_{\substack{k \in \mathbb{N} \\ p^k \leqslant n}} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Correction

On a déjà $v_p(n!) = \sum_{k=1}^{n} v_p(k)$. Il faut maintenant comprendre comment vont se comporter les entiers entre 1 et n. Soit $K = \max\{i \in \mathbb{N},\ p^i \leqslant n\}$. Alors pour tout $i > k$, on sait que p^i ne va diviser aucun entier entre 1 et n. Ensuite :

- Il y a $\left\lfloor \frac{n}{p^K} \right\rfloor$ entiers entre 1 et n divisibles par p^K. Ils apportent chacun une valuation de K.
- Il y a $\left\lfloor \frac{n}{p^{K-1}} \right\rfloor - \left\lfloor \frac{n}{p^K} \right\rfloor$ entiers entre 1 et n divisibles par p^{K-1} mais pas par p^K. Ils vont chacun apporter une valuation de $K - 1$.
- On continue ainsi jusqu'à $\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor$ entiers divisibles par p mais pas par p^2, qui apportent chacun une valuation de 1.

D'où, au final,

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{K} k\left(\left\lfloor \frac{n}{p^k}\right\rfloor - \left\lfloor \frac{n}{p^{k+1}}\right\rfloor\right) \\ &= \sum_{k=1}^{K} k\left\lfloor \frac{n}{p^k}\right\rfloor - (k+1)\left\lfloor \frac{n}{p^{k+1}}\right\rfloor + \sum_{k=1}^{K}\left\lfloor \frac{n}{p^{k+1}}\right\rfloor \\ &= \left\lfloor \frac{n}{p}\right\rfloor - (K+1)\left\lfloor \frac{n}{p^{K+1}}\right\rfloor + \sum_{k=1}^{K}\left\lfloor \frac{n}{p^{k+1}}\right\rfloor \\ &= \left\lfloor \frac{n}{p}\right\rfloor + \sum_{k=2}^{K}\left\lfloor \frac{n}{p^k}\right\rfloor \text{ car } \left\lfloor \frac{n}{p^{K+1}}\right\rfloor = 0 \\ &= \sum_{k=1}^{K}\left\lfloor \frac{n}{p^k}\right\rfloor, \end{aligned}$$

d'où le résultat souhaité.

2 Exercices à faire en TD

Plan de travail

1. Des exercices de base sur les congruences : le 6, 7 et 8. Le 10 est plus difficile !
2. Des exercices sur les notions de pgcd et ppcm : le 11, le 12, le 13 sont assez basiques, le 14 est conseillé (classique), le 15 est simple quand on a la solution mais peut parfois poser problème !
3. Des exercices sur les nombres premiers, utilisant la notion de valuation (16 et 17), d'autres sur le petit théorème de Fermat (18) et d'autres plus généraux (20 et 21)
4. Le théorème de Wilson est un exercice intéressant (19)
5. Des exercices un peu plus accessoires sur les résolutions d'équations arithmétiques : équations avec pgcd et ppcm (23), des équations diophantiennes (22 et 24), un résultat qui utilise ou les valuations, ou des résultats d'analyse (25).
6. Enfin, le dernier exercice (26) est un oral d'ENS, très difficile mais intéressant !

Minimum vital faire le 6, questions 1 et 2, le 7, question 1, le 11, questions 1 et 2, le 14, le 16, le 22.

2.1 Divisibilité –congruences

Exercice 6. *Jouons avec les congruences*. ◐○○

1. Déterminer le reste modulo 11 de $2^{123} + 2^{121}$.

Correction

On écrit $2^{123}+2^{121}=2^{121}\times 5$. Or, d'après le petit théorème de Fermat,

$$\begin{aligned}(2^{11})^{11} &\equiv 2^{11}[11]\\ &\equiv 2[11].\end{aligned}$$

Donc $2^{121}\times 5\equiv 10[11]$.

2. Montrer que $\forall n\in\mathbb{N},\ 7|3^{2n+1}+2^{n+2}$.

Correction

On remarque que $3^2\equiv 2[7]$. Donc $3^{2n}\equiv 2^n[7]$. Donc $3^{2n+1}+2^{n+2}\equiv 2^n\times 3+2^2\times 4[7]$, i.e. $3^{2n+1}+2^{n+1}\equiv 7\times 2^n[7]$ donc 7 divise $3^{2n+1}+2^{n+1}$.

3. Montrer que $\forall n\in\mathbb{N},\ n^2|(n+1)^n-1$.

Correction

Soit n dans n. Alors

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

Or, $n^2|n^2$ et pour $k\geqslant 2$, $n^2|n^k$, donc $n^2|(n+1)^n-1$.

Exercice 7. ●◐○ Soit n un entier naturel non nul. Montrer que...

1. ...$n^3(n^6-1)$ est divisible par 8.

Correction

On factorise l'expression :

$$\begin{aligned} n^3(n^6-1) &= n^3(n^3-1)(n^3+1) \\ &= n^3(n-1)(1+n+n^2)(n+1)(n^2-n+1). \end{aligned}$$

- Si n est pair, alors on dispose de k tel que $n = 2k$ donc $n^3 = 8k^3$ donc 8 divise $n^3(n^6-1)$.
- Si n est impair
  - si $n \equiv 1[4]$, alors on dispose de k tel que $n = 4k+1$, donc $(n-1)(n+1) = 4k(4k+2) = 8k(2k+1)$, donc 8 divise $n^3(n^6-1)$.
  - si $n \equiv 3[4]$, alors on dispose de k tel que $n = 4k+3$, donc $(n-1)(n+1) = (4k+2)4k = 8k(2k+1)$, donc 8 divise $n^3(n^6-1)$.

2. ...$n^3 - n$ est divisible par 3.

Correction

On écrit $n^3 - n = n(n^2-1) = (n-1)n(n+1)$. Or dans trois entiers consécutifs, l'un au moins est multiple de 3, donc 3 divise $n^3 - n$.

3. ...$3^{n+3} - 4^{4n+2}$ est divisible par 11.

Correction

On remarque que $4^2 \equiv 5[11]$, donc $4^4 \equiv 3[11]$, donc $4^{4n+2} \equiv 3^n \times 5[11]$. Donc $3^{n+3} - 4^{4n+2} \equiv 3^n(3^3-5)[11]$. Or $3^3 = 27 \equiv 5[11]$. Le résultat est donc démontré.

4. ...lorsque n est impair, $n(n^2-1)$ est divisible par 24.

Correction

On remarque que $n(n^2-1) = n(n-1)(n+1)$, divisible par 3 par la première question. Si n est impair, on écrit $n = 2k+1$. Alors $n-1 = 2k$ et $n+1 = 2k+2$, donc $(n-1)(n+1) = 4k(k+1)$. Or le produit de deux entiers consécutifs est pair, donc 8 divise $4k(k+1)$. Donc $n(n^2-1)$ est divisible par 3 et 8, qui sont premiers entre eux, donc il est divisible par leur produit, c'est-à-dire par 24.

Exercice 8. ●◐○ Un nombre palindrome est un nombre qui se lit indifféremment de gauche à droite ou de droite à gauche. Par exemple, 2002, 12321 sont des nombres palindromes. Prouver qu'un nombre palindrome ayant un nombre pair de chiffres est divisible par 11.

Exercice 9. ●●○ Soit x un entier naturel non nul, $x = \overline{a_N a_{N-1} \dots a_1 a_0}$ son écriture en base 10 (a_0 est le chiffre des unités, a_1 des dizaines, etc.)

1. Démontrer que 7 divise x si, et seulement si 7 divise $5a_0 + \overline{a_N a_{N-1} \dots a_2 a_1}$.

Correction

Remarquons que

$$\begin{aligned} x &= \overline{a_N a_{N-1} \dots a_1 a_0} \\ &= \overline{a_N a_{N-1} \dots a_1 0} + a_0 \\ &= 10 \times \overline{a_N a_{N-1} \dots a_1} + a_0 \\ &= 10 \times \overline{a_N a_{N-1} \dots a_1} + a_0 + 49a_0 - 49a_0 \\ &= 10 \times (\overline{a_N a_{N-1} \dots a_1} + 5a_0) - 49a_0, \end{aligned}$$

donc, comme $49 \equiv 0[7]$,

$$x \equiv 10 \times (\overline{a_N a_{N-1} \dots a_1} + 5a_0)\,[7]$$

Donc 7 divise x si et seulement si 7 divise $10 \times (\overline{a_N a_{N-1} \dots a_1} + 5a_0)$.
Donc 7 divise x si et seulement si 7 divise $\overline{a_N a_{N-1} \dots a_1} + 5a_0$ (par le théorème de Gauss, car 7 est premier avec 10).

2. Démontrer que 7 divise x si, et seulement si 7 divise $\overline{a_N a_{N-1} \dots a_2 a_1} - 2a_0$.

Correction

Remarquons que

$$\begin{aligned} x &= \overline{a_N a_{N-1} \dots a_1 a_0} \\ &= \overline{a_N a_{N-1} \dots a_1 0} + a_0 \\ &= 10 \times \overline{a_N a_{N-1} \dots a_1} + a_0 \\ &= 10 \times \overline{a_N a_{N-1} \dots a_1} + a_0 - 21a_0 + 21a_0 \\ &= 10 \times (\overline{a_N a_{N-1} \dots a_1} + 5a_0) + 21a_0, \end{aligned}$$

donc, comme $21 \equiv 0[7]$,

$$x \equiv 10 \times (\overline{a_N a_{N-1} \dots a_1} - 2a_0)\,[7]$$

Donc 7 divise x si et seulement si 7 divise $10 \times (\overline{a_N a_{N-1} \dots a_1} - 2a_0)$.
Donc 7 divise x si et seulement si 7 divise $\overline{a_N a_{N-1} \dots a_1} - 2a_0$ (par le théorème de Gauss, car 7 est premier avec 10).

3. On propose une recette pour déterminer si un grand nombre est divisible par 7. Soit par exemple le nombre 7905669884. On l'écrit en séparant les nombres en paquets de 3 :

7 905 669 884

puis on fait la somme alternée $7 - 905 + 669 - 884 = -1113$.
On prend la valeur absolue du résultat, 1113 et, s'il est divisible par 7, alors le nombre de départ l'est !
(ici, on utilise la méthode du 2 : $111 - 2 \times 3 = 105$, $10 - 2 \times 5 = 0$ donc 7 divise 105 donc 1113 donc 7905669884).
Expliquer cette méthode.

Correction

On écrit, si $x = \sum_{k=0}^{3n-1} a_k 10^k$ (quitte à mettre des zéros, on fait en sorte d'avoir un multiple de 3 de chiffres),

$$\begin{aligned} x &= a_0 + 10a_1 + 100a_2 + 1000(a_3 + 10a_4 + 100a_5) + \dots \\ &= \sum_{p=0}^{n-1} 10^{3p} \times \overline{a_{3p+2}a_{3p+1}a_{3p}}. \end{aligned}$$

Mais $10 \equiv 3[7]$ donc $100 \equiv 30 \equiv 2[7]$ donc $1000 \equiv 20 \equiv -1[7]$. DOnc

$$x \equiv \sum_{p=0}^{n-1} (-1)^p \times \overline{a_{3p+2}a_{3p+1}a_{3p}}[7],$$

d'où la méthode utilisée !

Exercice 10. ●●● On pose, pour tout n dans $\mathbb{N}$, $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Montrer que pour tout $n \geqslant 2$, H_n n'est pas entier.

Correction

On montre $\mathcal{P}_n$: Soit p tel que $2^p \leqslant n < 2^{p+1}$, alors $H_n = \frac{a}{2^p b}$ avec a et b impairs.
On démontre le résultat par récurrence, pour $n \geqslant 2$. Pour $n = 2$ c'est immédiat.
Si le résultat est vrai en n, avec $2^p \leqslant n < 2^{p+1}$, alors on regarde $n+1$. Ou bien $n+1 = 2^{p+1}$ et alors

$$H_{n+1} = H_n + \frac{1}{2^{p+1}} = \frac{a}{2^p b} + \frac{1}{2^{p+1}} = \frac{2a+b}{2^{p+1}b},$$

d'où le résultat. Sinon $n+1 < 2^{p+1}$ donc on peut écrire $n+1 = 2^q c$ avec $q < p+1$ et c impair. Donc

$$H_{n+1} = H_n + \frac{1}{2^q c} = \frac{a}{2^p b} + \frac{1}{2^q c} = \frac{ac + b2^{p-q}}{2^p bc},$$

d'où le résultat.

2.2 PGCD, PPCM

Exercice 11. ◐○○ Soit $n \in \mathbb{N}^*$.

1. Trouver le pgcd de $n! + 1$ et $(n+1)! + 1$.

Correction

Nommons $a = n! + 1$ et $b = (n+1)! + 1$. Remarquons que $(n+1)a - b = n$, donc $a \wedge b$ divise n. Il divise donc $n!$. Il divise donc $a - n! = 1$. Donc $a \wedge b = 1$.

2. Montrer que $2n + 1$ et $14n + 3$ sont premiers entre eux.

Correction

Posons $a = 2n+1$ et $b = 14n+3$. On remarque que $a \wedge b$ divise $7a - b = 4$. Donc $a \wedge b = 1, 2$ ou 4. Or a est impair et $a \wedge b$ divise a. Donc $a \wedge b = 1$.

3. Montrer que $n^4 + 3n^2 + 1$ et $n^3 + 2n$ sont premiers entre eux.

Correction

Posons $a = n^4 + 3n^2 + 1$ et $b = n^3 + 2n$. Donc $a \wedge b$ divise $c = a - nb = n^2 + 1$. Donc $a \wedge b$ divise $d = b - nc = n$. Donc $a \wedge b$ divise $a - (n^3 + 3n)d = 1$. Donc $a \wedge b = 1$.

Exercice 12. ●●○ Soit $(P, m) \in (\mathbb{N}^*)^2$. Trouver une condition nécessaire et suffisante pour qu'il existe deux entiers dont le produit soit P et le ppcm m. Comment déterminer alors les entiers solutions ? À titre d'exemple, traiter le cas $P = 24$, $m = 12$.

Correction

Analyse. Supposons qu'il existe a et b deux entiers tels que $ab = P$ et $a \vee b = m$. Alors P est un multiple commun à a et à b, donc m divise P.
De plus, $ab = a \wedge b \times a \vee b$. Donc $\dfrac{P}{m} = a \wedge b$. Or $a \wedge b$ divise $a \vee b$. Donc $\dfrac{P}{m}$ divise m, donc P divise m^2.
Finalement, $m|P|m^2$.
Synthèse. Supposons que $m|P$ et $P|m^2$. Posons alors $a = m$ et $b = \dfrac{P}{m}$. Alors $ab = P$. Reste à montrer que $m = a \vee b$. Par hypothèse, $\dfrac{P}{m}$ divise m, donc b divise $m = a$. Donc $a \vee b = a = m$. D'où le résultat !

Exercice 13. ●◐○ Soit $n \in \mathbb{N}^*$. Montrer que $\text{ppcm}(1, 2, \dots, 2n) = \text{ppcm}(n+1, \dots, 2n)$.

Correction

Soit k dans $\{1, \dots, n\}$. On va montrer qu'un des multiples de k est dans $\{n+1, \dots, 2n\}$. Cela permettra de dire qu'un multiple commun à $\{n+1, \dots, 2n\}$ est aussi multiple commun à $\{1, \dots, 2n\}$. L'idée est de regarder $2k$, $4k$, $8k$, etc. et de se dire qu'il y en a bien un qui sera dans $\{n+1, \dots, 2n\}$.
Considérons l'ensemble $A = \{2^s k,\ s \in \mathbb{N}\}$. Alors $A \cap [\![1, n]\!]$ est non vide (il contient k) et majoré. Il contient donc un plus grand élément, de la forme $2^a k$, avec $a \in \mathbb{N}$. Alors $2^a k \leqslant n$, donc $2^{a+1} k \leqslant 2n$ et $2^{a+1} k \geqslant n+1$. En effet, si ce n'était pas le cas, on aurait $2^{a+1} k \leqslant n$, donc $2^{a+1} k$ serait dans A, contradiction.
Donc tout multiple commun à $\{n+1, \dots, 2n\}$ est multiple de tous les entiers de 1 à n. Donc les multiples communs de $(1, 2, \dots, 2n)$ et $(n+1, \dots, 2n)$ sont les mêmes. Donc $\text{ppcm}(1, 2, \dots, 2n) = \text{ppcm}(n+1, \dots, 2n)$.

Exercice 14. ●●○

1. Montrer que pour tout n dans $\mathbb{N}$, il existe un unique couple $(a_n, b_n) \in \mathbb{Z}^2$ tel que

$$(1+\sqrt{2})^n = a_n + \sqrt{2} b_n.$$

Correction

Unicité : soit n dans $\mathbb{N}$, $(a_n, b_n, a'_n, b'_n) \in \mathbb{Z}^4$ tels que $a_n + \sqrt{2}b_n = a'_n + \sqrt{2}b'_n$. Alors $a_n - a'_n = \sqrt{2}(b'_n - b_n)$, donc, si $b_n \neq b'_n$, $\sqrt{2} = \dfrac{a_n - a'_n}{b'_n - b_n}$, donc $\sqrt{2}$ est rationnel, absurde ! Donc $b_n = b'_n$, donc $a_n = a'_n$.

Existence, méthode 1. Soit n dans $\mathbb{N}$. Alors on écrit

$$\begin{aligned}(1+\sqrt{2})^n &= \sum_{k=0}^{n} \binom{n}{k} \sqrt{2}^k \\ &= \sum_{\substack{0\leqslant k\leqslant n \\ k \text{ pair}}} \binom{n}{k} \sqrt{2}^k + \sum_{\substack{0\leqslant k\leqslant n \\ k \text{ impair}}} \binom{n}{k} \sqrt{2}^k \\ &= \sum_{p=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{2p} \sqrt{2}^{2p} + \sum_{p=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n}{2p+1} \sqrt{2}^{2p+1} \\ &= \sum_{p=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{2p} 2^p + \sqrt{2} \sum_{p=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n}{2p+1} 2^p,\end{aligned}$$

d'où le résultat en posant $a_n = \displaystyle\sum_{p=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{2p} 2^p$ et $b_n = \displaystyle\sum_{p=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n}{2p+1} 2^p$.

Existence, méthode 2. On démontre la proposition $\mathbb{P}_n : \exists (a_n, b_n) \in \mathbb{N}^2,\ (1+\sqrt{2})^n = a_n + \sqrt{2}b_n$.
Initialisation : pour $n = 0$, on pose $a_0 = 1$ et $b_0 = 0$, d'où le résultat.
Hérédité : si la proposition est vraie au rang n, alors on dispose de a_n et b_n tels que

$$(1+\sqrt{2})^n = a_n + \sqrt{2}b_n.$$

Alors

$$(1+\sqrt{2})^{n+1} = (a_n + \sqrt{2}b_n)(1+\sqrt{2}) = a_n + \sqrt{2}a_n + \sqrt{2}b_n + 2b_n,$$

d'où le résultat en posant $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = a_n + b_n$.

2. Montrer que pour tout n dans $\mathbb{N}$, $\text{pgcd}(a_n, b_n) = 1$.

Correction

Montrons le résultat par récurrence sur n. Comme pour tout n, $\begin{cases} a_{n+1} = a_n + 2b_n \\ b_{n+1} = a_n + b_n. \end{cases}$ On montre alors que si $d_n = a_n \wedge b_n$. Déjà a_{n+1} et b_{n+1} sont combinaisons linéaires de a_n et b_n donc d_n divise a_{n+1} et b_{n+1} donc d_n divise d_{n+1}. De plus, $a_{n+1} - b_{n+1} = b_n$ et $2b_{n+1} - a_{n+1} = a_n$ donc d_{n+1} divise d_n. Donc $d_{n+1} = d_n = d_1 = 1$ par récurrence immédiate.

Exercice 15. ●●○ Soit a et b deux entiers naturels non nuls.

1. On suppose $\text{pgcd}(a,b)=1$. Déterminer le pgcd de ab et $a+b$.

Correction

On pose d ce pgcd. Il divise ab et $a+b$ donc il divise $ab-a(a+b)=-a^2$, et de même il divise $ab-b(a+b)=-b^2$ donc d divise a^2 et b^2 donc leur pgcd. Or, $a^2\wedge b^2=1$ (car si $p\in\mathbb{P}$, $v_p(a^2\wedge b^2)=\min(v_p(a^2),v_p(b^2))=\min(2v_p(a),2v_p(b))2\min(v_p(a),v_p(b))=0$. Donc ce pgcd est égal à 1.
Autre méthode. Si d est un diviseur commun à a et à $a+b$ alors il divise $a+b-a=b$ donc il est commun à a et à b donc est égal à 1, donc $a\wedge(a+b)=1$. De même, $b\wedge(a+b)=1$. Donc $ab\wedge(a+b)=1$ (car tout diviseur premier de ab divise a ou b).

2. Dans le cas général, quel est le pgcd de $a+b$ et $\text{ppcm}(a,b)$?

Correction

Si $\delta=a\wedge b$, $\dfrac{a}{\delta}\wedge\dfrac{b}{\delta}=1$ donc

$$\left(\frac{a}{\delta}+\frac{b}{\delta}\right)\wedge\frac{a}{\delta}\frac{b}{\delta}=1,$$

donc, en multipliant par δ, $(a+b)\wedge\dfrac{ab}{\delta}=\delta$, donc $(a+b)\wedge(a\vee b)=\delta$.

2.3 Nombres premiers

Exercice 16. ◐○○ Soient a et b deux entiers naturels tels qu'il existe n dans $\mathbb{N}^*$ tel que a^n divise b^n. Montrer que a divise b.

Correction

Soit p un nombre premier. Alors par hypothèse $v_p(a^n)\leqslant v_p(b^n)$ donc $nv_p(a)\leqslant nv_p(b)$ donc, comme $n\in\mathbb{N}^*$, $v_p(a)\leqslant v_p(b)$, donc a divise b.

Exercice 17. ●○○ Soit n un entier positif. Montrer que $\sqrt{n}\in\mathbb{N}\Leftrightarrow\sqrt{n}\in\mathbb{Q}\Leftrightarrow n$ est un carré parfait (i.e. $\exists k\in\mathbb{N}$, $n=k^2$).

Correction

On procède par implications circulaires :

- (n est un carré parfait $\Rightarrow\sqrt{n}\in\mathbb{Q}$:) Évident car $\mathbb{N}\subset\mathbb{Q}$.
- ($\sqrt{n}\in\mathbb{Q}\Rightarrow n$ est un carré parfait :) On suppose $\sqrt{n}\in\mathbb{Q}$, alors on dispose de p et q dans $(\mathbb{N}^*)^2$ tels que $\sqrt{n}=\dfrac{p}{q}$. Alors $nq^2=p^2$, donc q^2 divise p^2 donc (exercice 3) q divise p, donc on dispose de $k\in\mathbb{N}$ tel que $p=kq$, donc $\sqrt{n}=k$, donc $n=k^2$ donc n est un carré parfait.
- (n est un carré parfait $\Rightarrow\sqrt{n}\in\mathbb{N}$:)si on dispose de k tel que $n=k^2$, alors $\sqrt{n}=k\in\mathbb{N}$.

Exercice 18. *Applications du petit théorème de Fermat.* ●●○

1. Quel est le reste de la division euclidienne de $2^{70^{71}}$ par 13 ?

Correction

On sait que $2^{12} \equiv 1[13]$ par le petit théorème de Fermat. Il faut donc trouver le reste de la division euclidienne de 70^{71} par 12. Or, $72 \equiv 0[12]$ donc $70 \equiv -2[12]$. Mais on remarque que $(-2)^2 \equiv 4[12]$ et que pour tout k dans $\mathbb{N}$, $k \geqslant 2$, $(-2)^k \equiv 4[12]$. Ainsi, $70^{71} \equiv 4[12]$ donc $2^{70^{71}} \equiv 4[12]$.

2. Montrer que pour tout $n \in \mathbb{Z}$, on a $n^7 \equiv n$ [42].

Correction

Soit n dans $\mathbb{Z}$. Déjà, $n^7 \equiv n[7]$ par le petit théorème de Fermat. Donc 7 divise $n^7 - n = n(n^6-1) = n(n^3-1)(n^3+1) = n(n-1)(n^2+n+1)(n+1)(n^2-n+1)$, nombre divisible par 2 et par 3 (produit de 3 entiers consécutifs) donc par 6 donc par 42 (théorème de Gauss).

3. Trouver les nombres premiers p tels que p divise $2^p + 1$.

Correction

On sait que si $p \in \mathbb{P}$, $2^p \equiv 2[p]$. On veut aussi $2^p \equiv -1[p]$ donc on veut p tel que $2 \equiv -1[p]$ i.e. p divise 3. Donc 3 est la seule solution.

Exercice 19. *Théorème de Wilson.* ●●○ Soit p un nombre premier différent de 2.

1. Montrer que $(p-1)^2 \equiv 1[p]$.

Correction

$(p-1)^2 = p^2 - 2p + 1$. Or, $p^2 \equiv 0[p]$ et $-2p \equiv 0[p]$, donc $(p-1)^2 \equiv 1[p]$.

2. Montrer que $x^2 \equiv 1[p]$ si, et seulement si $x \equiv 1[p]$ ou $x \equiv -1[p]$.

Correction

$\boxed{\Leftarrow}$ Déjà si $x \equiv 1[p]$ ou $x \equiv -1[p]$, $x^2 \equiv 1[p]$ par les règles de calcul sur les congruences.

$\boxed{\Rightarrow}$ Ensuite, si $x^2 \equiv 1[p]$, alors p divise $x^2 - 1 = (x-1)(x+1)$, donc, comme p est premier, p divise $x-1$ ou p divise $x+1$, donc $x \equiv 1[p]$ ou $x \equiv -1[p]$.

3. Soit n dans $\{1, 2, \ldots, p-1\}$ Montrer qu'il existe un unique entier m dans $\{1, 2, \ldots, p-1\}$ tel que $mn \equiv 1[p]$. Quand a-t-on $m = n$?

Correction

On sait que n est premier avec p donc par le théorème de Bézout, on dispose de u et v tels que $un + vp = 1$. Effectuons la division euclidienne de u par p : $u = pq + r$, avec

$1 \leqslant r < p$. Donc $un + vp = (pq + r)n + vp = rn + (qn + v)p$. Donc $rn - 1$ est divisible par p, i.e. $rn \equiv 1[p]$. D'où l'existence de cet entier.
Pour l'unicité, si $rn \equiv 1[p]$ et $mn \equiv 1[p]$, alors $rn \equiv nm[p]$, donc, comme n est premier avec p, $r = m$. D'où l'unicité.
Pour avoir $m = n$, il faut avoir $m^2 \equiv 1[p]$, i.e. $m \equiv 1[p]$ ou $m \equiv -1[p]$, i.e., comme $m \in \{1, \dots p-1\}$, $m = 1$ ou $m = p - 1$. Réciproquement, si $m = 1$ ou $m = p - 1$, $m^2 \equiv 1[p]$.

4. Démontrer que $(p-1)! \equiv p - 1[p]$.

Correction

Écrivons $(p-1)! = (p-1) \times (2 \times \cdots \times (p-2))$. On sait que pour tout élément m de $\{2, \dots, p-2\}$ il existe un unique *m différent de m* tel que $mn \equiv 1[p]$. En regroupant par paires ces éléments, on en déduit que $2 \times \cdots \times (p-2) \equiv 1[p]$, et donc $(p-1)! \equiv p-1[p]$.

5. Déduire de ce qui précède une preuve du théorème de Wilson : pour tout entier naturel q, q est premier si, et seulement si $(q-1)! \equiv q - 1[q]$.

Correction

On vient de montrer que si q est premier alors $(q-1)! \equiv q - 1[q]$.
Réciproquement, si q vérifie $(q-1)! \equiv q - 1[q]$, alors q divise $(q-1)! - (q-1) = (q-1)((q-2)! - 1)$, donc, come $q \wedge (q-1) = 1$, q divise $(q-2)! - 1$. Donc on dispose de k dans $\mathbb{Z}$ tel que

$$(q-2)! - kq = 1,$$

donc tous les entiers de 1 à $q-2$ satisfont une relation de Bézout avec q. Donc q est premier avec touts les entiers de 2 à $q-2$, donc, en particulier, n'est divisible par aucun de ces entiers. Il n'est pas non plus divisible par $q-1$, donc q n'est divisible par aucun des entiers entre 2 et $q-1$, donc q est premier.

Exercice 20. *Nombres premiers jumeaux*. ●◐○ Deux nombres premiers p et q sont dits jumeaux si leur différence est égale à 2.

1. Donner des exemples de nombres premiers jumeaux.

Correction

3 et 5 sont deux nombres premiers jumeaux.

2. Soient p et q deux nombres premiers. Montrer p et q sont jumeaux si, et seulement si $pq + 1$ est un carré.

Correction

Supposons que p et q sont deux nombres jumeaux. Alors $q = p + 2$, donc $pq + 1 = p^2 + 2p + 2 = (p+1)^2$.
Supposons que $pq + 1$ est un carré, c'est-à-dire qu'on dispose de k tel que $pq + 1 = k^2$.

Alors $pq = k^2 - 1 = (k-1)(k+1)$. Donc p divise $k-1$ ou $k+1$, et q divise $k-1$ ou $k+1$. Ils ne peuvent diviser le même de ces entiers, sinon on aurait pq qui le diviserait, i.e. pq serait strictement inférieur à $(k-1)(k+1)$. Mettons-nous dans la situation où p divise $k-1$ et q divise $k+1$. Alors $p = k-1$ et $q = k+1$ car sinon $pq < (k-1)(k+1)$. Donc $q - p = 2$, i.e. p et q sont jumeaux.

3. Montrer que si p et q sont deux nombres premiers jumeaux supérieurs ou égaux à 5, alors $p+q$ est divisible par 12.

Correction

Comme $p+q$ est la somme de deux entiers impairs consécutifs, leur somme est divisible par 4 (on les écrit $4k+1$ et $4k+3$). De plus, comme l'un est congru à 1 modulo 3 et l'autre congru à 2 modulo 3 donc leur somme est divisible par 3, donc (Gauss) elle est divisible par 12.

Exercice 21. ●●◐ On veut montrer qu'il existe une infinité de nombres premiers de la forme $4k+3$, avec $k \in \mathbb{Z}$. On note leur ensemble $\mathbb{P}_{3,4}$ et suppose, par l'absurde, que $\mathbb{P}_{3,4} = \{p_1, \dots, p_N\}$ avec $N \in \mathbb{N}$. On pose $q = 4(p_1 \dots p_N) - 1$.

1. Montrer que q possède un facteur premier congru à 3 modulo 4.

Correction

Déjà, q est impair donc 2 ne divise pas q. Or, si tous les facteurs premiers de q étaient congrus à 1 modulo 4, q serait congru à 1 modulo 4 (car le produit de deux éléments confrus à 1 modulo 4 est congru à 1 modulo 4). Or, $q \equiv -1[4]$, absurde.

2. Montrer que ce facteur premier ne peut pas être égal à $p_1, \dots, p_N$, et conclure.

Correction

Soit p un facteur premier de $4(p_1 \dots p_N) - 1$. Alors, si p était égal à l'un des $p_1, \dots, p_N$, on aurait p qui divise $4p_1 \times \dots \times p_N$, donc p diviserait -1, absurde.
On conclut que $\mathbb{P}_{3,4}$ est infini.

2.4 Résolution d'équations

Exercice 22. ●◐○

1. Trouver toutes les solutions en nombres entiers de $29x - 11y = 1$.

Correction

Appliquons l'algorithme d'Euclide à 29 et à 11.

$$29 = 2 \times 11 + 7$$
$$11 = 1 \times 7 + 4$$
$$7 = 1 \times 4 + 3$$
$$4 = 1 \times 3 + 1$$
$$3 = 3 \times 1 + 0$$

Donc 29 et 11 sont premiers entre eux. On remonte alors l'algorithme d'Euclide.

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (7 - 4) \\ &= 2 \times 4 - 7 \\ &= 2 \times (11 - 7) - 7 \\ &= 2 \times 11 - 3 \times 7 \\ &= 2 \times 11 - 3 \times (29 - 2 \times 11) \\ &= 8 \times 11 - 3 \times 29. \end{aligned}$$

Donc $(x, y) = (-3, -8)$ est une solution de l'équation. L'ensemble des solutions est donc

$$\{(-3 + 11k, -8 + 29k), k \in \mathbb{Z}\}.$$

2. Résoudre dans $\mathbb{Z}^3$ l'équation $5x - 3y + 8z = 1$.

Correction

Résolvons l'équation

$$5x - 3y = 1 - 8z,$$

de paramètre z. On sait que pour $x = 2$ et $y = 3$, $5x - 3y = 1$, donc $(x, y) = (2 - 16z, 3 - 24z)$ est une solution de l'équation. Donc l'ensemble des solutions de l'équation à paramètre est

$$\{(2 - 16z + 3k, 3 - 24z + 5k), k \in \mathbb{Z}\}.$$

Aucune contrainte n'est à poser sur z donc l'ensemble des solutions de l'équation à trois inconnues est l'ensemble

$$\{(2 - 16z + 3k, 3 - 24z + 5k, z), k \in \mathbb{Z}, z \in \mathbb{Z}\}.$$

Remarque : l'exercice aurait été beaucoup plus diffiicle si les trois nombres étaient juste premeirs entre eux dans leur ensemble, mais pas premiers entre eux deux à deux (par exemple, $6, 15, 10$).

Exercice 23. ●○○ Résoudre dans $\mathbb{Z}^2$ le système

$$\begin{cases} x + y = 56, \\ x \vee y = 105. \end{cases}$$

Correction

On remarque que $105 = 5 \times 21 = 5 \times 3 \times 7$. Or $x \wedge y$ divise à la fois 56 et 105, donc il divise $56 \wedge 105$, donc il divise 7. Donc $x \wedge y = 1$ ou 7. Si $x \wedge y = 1$, alors $xy = 105$ Donc $(x, y) \in \{(1, 105), (3, 35), (5, 21), (7, 15)\}$ (et les symétriques). Or aucune des sommes des couples décrits ici ne fait 56.
Si $x \wedge y = 7$, alors on pose $x' = x/7$ et $y' = y/7$. Alors $x'y' = 15$ et $x' + y' = 8$. Donc $x' = 3$ et $y' = 5$ ou l'inverse. Donc les deux solutions de l'équation sont $(x, y) = (21, 35)$ et $(x, y) = (35, 21)$.

Exercice 24. ●●○ Soit p un nombre premier. Résoudre l'équation suivante d'équations $(x, y) \in \mathbb{N}^2$

$$x^2 + px = y^2.$$

Correction

Analyse. Soit (x, y) un couple solution.

- si $p|x$, alors $x = px'$ avec $x' \in \mathbb{N}$, donc $p|x^2 + px$ donc $p|y^2$, donc $p|y$, donc $y = py'$, $y' \in \mathbb{N}$. Donc $p^2x'^2 + p^2x' = p^2y'^2$, donc $x'^2 + x' = y'^2$, donc $x'(x' + 1) = y'^2$.
  Si $x' = 0$, $y' = 0$ et $(0, 0)$ est bien solution. Sinon, $x'(x'+1)$ n'est pas un carré (si $p|x'$ En effet, x' et $x' + 1$ sont premiers entre eux, donc pour tout nombre premier p, $v_p(x') = 0$ ou $v_p(x' + 1) = 0$. Donc nécessairement $v_p(x')$ et $v_p(x' + 1)$ sont paires (car $v_p(y'^2)$ est paire), donc x' et $x' + 1$ sont des carrés, impossible (si c'était le cas, on aurait $x' = k^2$ et $x' + 1 = \ell^2$ avec $\ell \geqslant k$, donc $1 = x' + 1 - x' = \ell^2 - k^2 = (\ell - k)(\ell + k)$ impossible.
  Donc, si $p|x$, alors la solution est $(0, 0)$.
- sinon, soit $q \in \mathbb{P}$, $q \neq p$. Soit $\alpha = v_q(x)$ et $\beta = v_q(y)$. Alors $x = q^\alpha r$ et $y = q^\beta s$ avec r et s non divisibles par q. Alors l'équation devient

  $$q^{2\alpha} r^2 + pq^\alpha r = q^{2\beta} s^2.$$

  c'est-à-dire, comme q^α divise le membre de gauche, et que $q \nmid s$,

  $$q^\alpha r^2 + pr = q^{2\beta - \alpha} s^2.$$

  Or, si $\alpha > 0$, alors $2\beta - \alpha = 0$. Sinon cela signifierait que q divise pr, ce qui est impossible car $q \neq p$ et $q \nmid r$.
  Donc si $q|x$, $\alpha = 2\beta$. En particulier, cela signifie que x est un carré : $x = a^2$ avec $a \in \mathbb{N}$, et $y = a.b$ avec $b \in \mathbb{N}$. L'équation devient alors

  $$a^4 + pa^2 = a^2 b^2,$$

soit, en divisant par a^2, $a^2 + p = b^2$, ou encore

$$p = b^2 - a^2 = (b-a)(b+a)$$

Donc, ou bien $b - a = p$ et $b + a = 1$, ou bien $b - a = 1$ et $b + a = p$. Le premier cas est exclu car $a > 0$, donc

$$a = \frac{p-1}{2} \text{ et } b = \frac{p+1}{2},$$

donc

$$x = \frac{(p-1)^2}{4} \text{ et } y = ab = \frac{p^2-1}{4}.$$

La solution non nulle de l'équation est alors $\left(\frac{(p-1)^2}{4}, \frac{p^2-1}{4}\right)$.

Exercice 25. *Résolution de l'équation $x^y = y^x$.* ●●○ On veut résoudre l'équation $x^y = y^x$ d'inconnues $(x, y) \in \mathbb{N}^*$, non triviales, i.e. telles que $x \neq y$. On suppose $x < y$. On va proposer deux méthodes de résolution.

1. En étudiant les valuations p-adiques, montrer que $x|y$. Conclure.

Correction

Soit p un nombre premier. Alors $v_p(x^y) = yv_p(x)$ et $v_p(y^x) = xv_p(y)$. On a donc $yv_p(x) = xv_p(y)$. Or, $x \leqslant y$, donc $v_p(x) \leqslant v_p(y)$. Donc $x|y$, donc on peut écrire $y = kx$, donc $x^y = x^{kx}$ donc $y^x = (x^k)^x$ donc $y = x^k$. Donc $x^k = kx$. Donc $k = x^{k-1}$. Or, si $x > 2$, pour tout $k \geqslant 2$, $k < x^{k-1}$. Donc $x = 2$ et $k = 2$. Donc $x = 2$ et $y = 4$.

2. Retrouver le même résultat en étudiant la fonction $x \mapsto \frac{\ln(x)}{x}$ sur $\mathbb{R}_+^*$.

Correction

On étudie $f : x \mapsto \frac{\ln(x)}{x}$, de dérivée $x \mapsto \frac{1-\ln(x)}{x^2}$, donc croissante jusqu'en e et décroissante ensuite. L'équation $x^y = y^x$ s'écrit $f(x) = f(y)$, avec $x < y$. Étant donné le sens de variation de f, les solutions $x < y$ de cette équation sont de part et d'autre de e. Donc $x = 1$ ou $x = 2$. Le cas $x = 1$ donne $1 = y$, impossible. Le cas $x = 2$ donne $2^y = y^2$, donc $y = 4$.

Exercice 26. *Oral ENS.* ●●●

1. Montrer que pour tout (a, b) dans $(\mathbb{N}^*)^2$, $a\binom{a+b}{b}$ divise $\mathrm{ppcm}((b+i)_{1\leqslant i\leqslant a})$.

Correction

Déjà, $a\binom{a+b}{b} = \frac{((b+a)!}{(a-1)!b!} = \frac{(b+1)\dots(b+a)}{(a-1)!}$. On sait que pour tout p dans $\mathbb{P}$, $v_p(((b+i)_{1\leqslant i\leqslant a})) = \max(v_p(b+i))_{1\leqslant i\leqslant a}$. Déjà, si $p \geqslant a$ est un diviseur premier d'un

certain $b+i$, il n'est diviseur que d'un des $b+i$, car sinon il diviserait $b+i$ et $b+j$ avec $1 \leqslant i < j \leqslant a$ donc $j-i$ qui est dans $[\![1, a-1]\!]$, absurde. Donc le ppcm des $(b+i)$ sera divisible par le produit de tous les diviseurs premiers de l'un des $(b+i)$, supérieurs ou égaux à a.
Ensuite, si p est un diviseur premier de l'un des b_i inférieur ou égal à $a-1$, soit i_0 tel que $v_p(b+i_0) = \max((b+i), 1 \leqslant i \leqslant a) = \alpha$, alors il suffit de compter le nombre de $b+i$ qui sont aussi divisibles par p. Il y en a $\left\lfloor \frac{a-1}{p^{\alpha-1}} \right\rfloor - 1$ qui sont divisibles par $p^{\alpha-1}$ (on enlève $b+i_0$, $\left\lfloor \frac{a-1}{p^{\alpha-2}} \right\rfloor - \left\lfloor \frac{a-1}{p^{\alpha-1}} \right\rfloor - 1$ qui sont divisibles par $p^{\alpha-2}$ mais pas par $p^{\alpha-1}$, etc. En d'autres termes (cf. exercice sur la valuation de p dans $n!$), $v_p\left(\prod_{\substack{1\leqslant i\leqslant a \\ i\neq i_0}} (b+i)\right)$ est inférieur à $v_p((a-1)!)$. D'où

$$v_p\left(\frac{(b+1)\dots(b+a)}{(a-1)!}\right) \leqslant \max(v_p(b+i), 1 \leqslant i \leqslant a).$$

D'où le résultat.

2. Montrer que pour tout $n \in \mathbb{N}$, $(n+1)\mathrm{ppcm}\left(\binom{n}{i},\ 0 \leqslant i \leqslant n\right) = \mathrm{ppcm}(1, 2, \dots, n+1)$.

Correction

Déjà ,si $i \in [\![0, n]\!]$, $(n+1)\binom{n}{i} = (i+1)\binom{n+1}{i+1}$, donc $i+1$ divise $(n+1)\binom{n}{i}$, donc $i+1$ divise $(n+1)\mathrm{ppcm}\left(\binom{n}{i},\ 0 \leqslant i \leqslant n\right)$. Donc $(n+1)\mathrm{ppcm}\left(\binom{n}{i},\ 0 \leqslant i \leqslant n\right)$ est un multiple commun à $1, 2, \dots, n+1$, donc est divisible par $\mathrm{ppcm}(1, 2, \dots, n+1)$.
Réciproquement, on sait que si $i \in [\![0, n]\!]$, $(n+1)\binom{n-i+i}{i}$ divise $\mathrm{ppcm}(i+1, i+2, \dots, i+n-i) = \mathrm{ppcm}(i+1, i+2, \dots, n)$, qui divise $\mathrm{ppcm}(1, 2, i+1, i+2, \dots, n)$. Donc $\mathrm{ppcm}(1, 2, i+1, i+2, \dots, n)$ est un multiple commun à tous les $(n+1)\binom{n-i+i}{i}$ donc est divisible par leur ppcm. D'où l'autre divisibilité et le résultat.

3. Démontrer que pour tout $n \geqslant 1$, $\mathrm{ppcm}(1, 2, \dots, n) \geqslant 2^{n-1}$.

Correction

C'est évident : le ppcm de n nombres est supérieur au max de ces nombres, donc à leur moyenne ! Donc

$$\mathrm{ppcm}(1, 2, \dots, n) = n\mathrm{ppcm}\left(\binom{n-1}{i},\ 0 \leqslant i \leqslant n-1\right) \geqslant \sum_{k=0}^{n-1} \binom{n-1}{k} = 2^{n-1}.$$

4. En déduire une minoration du nombre de nombres premiers inférieurs ou égaux à n.

Correction

Si on appelle π_n ce nombre, on sait que $\mathrm{ppcm}(1,2,\dots,n) \leqslant \prod_{\substack{p \text{ premier} \\ p \leqslant n}} p \leqslant \prod_{\substack{p \text{ premier} \\ p \leqslant n}} n = n^{\pi_n}$,

d'où $n^{\pi_n} \geqslant 2^{n-1}$ d'où $\pi_n \geqslant \dfrac{(n-1)\ln(2)}{\ln(n)}$.