TD 4 correction

- **Exercice 1** (crible d'Erathostène jusqu'à 200)

  Commençons par remarquer qu'en calculant les carrés successifs des entiers, on constate qu'on a $14^2 = (10+4)^2 = 100 + 2 \times 4 \times 10 + 16 = 196 < 200$ et $15^2 = (10+5)^2 = 100 + 2 \times 5 \times 10 + 25 = 225 > 200$ donc on a l'encadrement $14 < \sqrt{200} < 15$

  L'algorithme se déroule alors ainsi.

  On écrit la liste de tous les entiers entre 2 et 200.

  - On barre tous les multiples de 2 inférieurs à 200, ce sont

    4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192, 194, 196, 198, 200

  - On considère le plus petit entier non barré strictement supérieur à 2, c'est 3 ; on barre tous les multiples de $3^2 = 9$ supérieurs à 3^2 et inférieurs à 200, ce sont (ici et dans la suite les entiers déjà barrés aux étapes précédentes sont néanmoins à nouveau listés)

    9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96, 99, 102, 105, 108, 111, 114, 117, 120, 123, 126, 129, 132, 135, 138, 141, 144, 147, 150, 153, 156, 159, 162, 165, 168, 171, 174, 177, 180, 183, 186, 189, 192, 195, 198

  - On considère le plus petit entier non barré strictement supérieur à 3, c'est 5 ; on barre tous les multiples de 5 supérieurs à $5^2 = 25$ et inférieurs à 200, ce sont

    25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100, 105, 110, 115, 120, 125, 130, 135, 140, 145, 150, 155, 160, 165, 170, 175, 180, 185, 190, 195, 200

  - On considère le plus petit entier non barré strictement supérieur à 5, c'est 7 ; on barre tous les multiples de 7 supérieurs à $7^2 = 49$ et inférieurs à 200, ce sont

    49, 56, 63, 70, 77, 84, 91, 98, 105, 112, 119, 126, 133, 140, 147, 154, 161, 168, 175, 182, 189, 196

  - On considère le plus petit entier non barré strictement supérieur à 7, c'est 11 ; on barre tous les multiples de 11 supérieurs à $11^2 = 121$ et inférieurs à 200, ce sont

    121, 132, 143, 154, 165, 176, 187, 198

  - On considère le plus petit entier non barré strictement supérieur à 11, c'est 13 ; on barre tous les multiples de 13 supérieurs à $13^2 = 121$ et inférieurs à 200, ce sont

    169, 182, 195

  - On considère le plus petit entier non barré strictement supérieur à 13, c'est 17. Comme $15 > \sqrt{200}$ on a $17 > \sqrt{200}$. En particulier tous les multiples de 17 inférieurs à 200 à partir de 2×17 ont déjà été barrés lors des étapes précédentes. Le même raisonnement vaut pour tous les entiers non barrés supérieurs à 17. Ainsi l'algorithme est terminé et les entiers non barrés sont les nombres premiers inférieurs à 200. Ce sont

    2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199

- **Exercice 3**

  Énoncé du lemme d'Euclide : soit p un nombre premier et a et b des entiers; on suppose que p divise le produit ab ; alors p divise a ou p divise b.

  Démonstration : d'après les principes de logique élémentaire, il est équivalent de montrer l'énoncé suivant : *on suppose que p divise le produit ab et ne divise pas a; alors p divise b.*

  Comme p ne divise pas a et est un nombre premier, p et a sont premiers entre eux. Comme en outre p divise le produit ab, d'après le lemme de Gauss, p divise b. Ce qui conclut la démonstration.

  Montrons à présent l'énoncé demandé par récurrence. On fixe un nombre premier p. L'hypothèse de récurrence H_n, pour n entier au moins égal à 2, s'énonce ainsi : "soit $a_1, \ldots, a_n$ n entiers tels que p divise le produit $\prod_{i=1}^{n} a_i$. Alors il existe un indice i tel que $1 \leq i \leq n$ et p divise a_i".

L'assertion H_2 n'est autre qu'une reformulation du lemme d'Euclide, ce qui initialise la récurrence.

Supposons H_n vérifiée pour un entier $n \geq 2$ et montrons que H_{n+1} est encore vraie. Soit $a_1, \ldots, a_{n+1}$ n entiers tels que p divise le produit $\prod_{i=1}^{n+1} a_i$. Il s'agit de démontrer qu'il existe un indice i tel que $1 \leq i \leq n+1$ et p divise a_i. On constate que le produit $\prod_{i=1}^{n+1} a_i$ s'écrit comme le produit des deux entiers $\prod_{i=1}^{n} a_i$ et a_{n+1}. D'après H_2, en d'autres termes d'après le lemme d'Euclide, p divise $\prod_{i=1}^{n} a_i$ ou p divise a_{n+1}. Si p divise a_{n+1}, on a terminé : on prend $i = n+1$. Si p divise $\prod_{i=1}^{n} a_i$, on applique H_n et on en conclut qu'il existe un indice i tel que $1 \leq i \leq n$ et p divise a_i. Finalement, H_{n+1} est bien vérifiée.

Finalement, H_2 est vraie et la propriété H_n est héréditaire. Donc pour tout entier n au moins égal à 2, H_n est vrai. Ceci montre l'énoncé visé.

- **Exercice 4**

Rappelons l'algorithme de base pour décomposer un entier N en facteurs premiers. On teste si N est divisible par 2 ; si oui, on remplace N par $N/2$ et on teste à nouveau si $N est divisible par 2 ; on poursuit cette procédure jusqu'à le test échoue ; le nombre de tests positifs de divisibilité par 2 donne la puissance de 2 dans la décomposition en facteurs premiers de l'entier N initial.

On teste ensuite si le N obtenu est divisible par 3 ; si oui, on remplace N par $N/3$ et on teste à nouveau si $N est divisible par 3 ; on poursuit cette procédure jusqu'à le test échoue ; le nombre de tests positifs de divisibilité par 3 donne la puissance de 3 dans la décomposition en facteurs premiers de l'entier N initial.

On recommence en remplaçant 3 par 5, puis 7, etc... On continue ainsi tant qu'on n'a pas obtenu $N = 1$, en testant à chaque nouvelle étape la divisibilité par le nombre premier suivant dans la liste des nombres premiers. Au pire il faudra faire ces tests jusqu'au plus grand nombre premier inférieur à la racine carré de l'entier N initial.

De manière générale, les tests de divisibilité ci-dessus s'effectuent a priori en calculant la division euclidienne correspondante. Noter que pour un nombre premier p donné, même s'il existe des tests efficaces de divisibilité par p, ces tests, lorsqu'ils sont positifs, ne donnent pas en général le quotient, or on en a besoin pour poursuivre l'algorithme.

Illustrons ce qui précède sur les énoncés a) et b), à savoir 2310 et 1124.

2310 est divisible par 2 et $2310/2 = 1155$

1155 n'est pas divisible par 2, on teste la divisibilité par 3.

2310 est divisible par 3, $1155/3 = 385$

385 n'est pas divisible par 3, on teste la divisibilité par 5.

385 est divisible par 5 et $385/5 = 77$

77 n'est pas divisible par 5, on teste la divisibilité par 7.

77 est divisible par 7 et $77/7 = 11$

11 n'est pas divisible par 7, on teste la divisibilité par 11.

11 est divisible par 11 et $11/11 = 1$.

Ainsi la factorisation de 2310 s'écrit $\boxed{2310 = 2.3.5.7.11}$

1224 est divisible par 2 et $1224/2 = 612$.

612 est divisible par 2 et $612/2 = 306$.

306 est divisible par 2 et $306/2 = 153$.

153 n'est pas divisible par 2, on teste la divisibilité par 3.

153 est divisible par 3 et $153/3 = 51$.

51 est divisible par 3 et $51/3 = 17$.

Si on poursuit l'algorithme rigoureusement, on constate que 17 n'est pas divisible par 3, et on teste sans succès la divisibilité de 17 par 5, 7, 11 et 13, jusqu'à voir que $17/17 = 1$. Bien sûr tout le monde ici aura reconnu directement que 17 était un nombre premier.

Ainsi la factorisation de 1224 s'écrit $\boxed{1224 = 2^3 \times 3^2 \times 17}$.

Dans certains cas, la décomposition peut se faire à vue, et par ailleurs les règles de calcul sur les produits de puissance permettent d'obtenir la décomposition d'un produit d'entiers si on connait la décomposition de chacun des facteurs.

Ainsi pour le c) on voit que $770000000 = 77 \times 10^7$. Par ailleurs la décomposition de 77 est $77 = 7 \times 11$ et comme $10 = 2 \times 5$, la décomposition de 10^7 est $2^7 \times 5^7$. Au final la décomposition de 770000000 est $\boxed{770000000 = 2^7 \times 5^7 \times 7 \times 11}$.

De même, pour le d), on a $14 = 2 \times 7$ donc $14^{2020} = 2^{2020} \times 7^{2020}$. On en déduit que $7^{24} \times 14^{2020} = 7^{24+2020} \times 2^{2020} = 2^{2020} \times 7^{2044}$. Au final la décomposition de $7^{24} \times 14^{2020}$ est $\boxed{7^{24} \times 14^{2020} = 2^{2020} \times 7^{2044}}$.

Enfin, pour le e), on peut tirer profit des résultats de a) et b), en écrivant

$$2310 \times 1224 = (2 \times 3 \times 5 \times 7 \times 11) \times (2^3 \times 3^2 \times 17) = 2^{1+3} \times 3^{1+2} \times 5^{1+0} \times 7^{1+0} \times 11^{1+0} \times 17^{0+1}$$

soit finalement $\boxed{2310 \times 1224 = 2^4 \times 3^3 \times 5 \times 7 \times 11 \times 17}$

- **Exercice 5** L'information sur l'aire du terrain donnée par l'énoncé se traduit par la relation $ab = 3024$ et on doit calculer les valeurs possibles du périmère du terrain, soit $2(a + b)$. L'énoncé impose en outre $\mathrm{pgcd}(a, b) = 6$. On peut donc écrire $a = 6\alpha$ et $b = 6\beta$, où α et β sont des entiers premiers entre eux. La relation $ab = 3024$ est alors équivalente à $\alpha\beta = 3024/6^2 = 84$. Le périmètre cherché s'exprime alors comme $2 \times 6(\alpha + \beta) = 12(\alpha + \beta)$.

  Cherchons donc tous les couples (α, β) d'entiers premiers entre eux vérifiant $\alpha\beta = 84$. Ceci peut se faire "à la main" en examinant toutes les décompositions possibles de 84 en produit de deux entiers positifs. Expliquons une méthode plus systématique. On calcule la décomposition en facteurs premiers de 84, on trouve $84 = 2^2 \times 3 \times 7$. Comme α et β sont des diviseurs de 84, leurs facteurs premiers sont nécessairement dans l'ensemble $\{2, 3, 7\}$. Et comme α et β sont premiers entre eux, α et β n'ont pas de facteur premier commun. Si on fixe l'ensemble des facteurs premiers de α (c'est une partie de $\{2, 3, 7\}$), α et β sont uniquement déterminés, et on obtient ainsi un et un seul couple solution correspondant. Par exemple, si l'ensemble des facteurs premiers de α est $\{2\}$, celui de β est nécessairement $\{3, 7\}$, et comme $\alpha\beta = 2^2 \times 3 \times 7$, on a nécessairement $\alpha = 2^2$ et $\beta = 3 \times 7$. Il y a donc autant de couples (α, β) solutions que de parties de l'ensemble $\{2, 3, 7\}$. Comme cet ensemble a 3 éléments, il possède exactement 8 parties. Ce sont

  $$\varnothing, \{2\}, \{3\}, \{7\}, \{2, 3\}, \{2, 7\}, \{3, 7\}, \{2, 3, 7\}$$

  Les couples (α, β) correspondant sont dans l'ordre

  $$(1, 84), (4, 21), (3, 28), (7, 12), (12, 7), (28, 3), (21, 4), (84, 1)$$

  Il y a 4 valeurs de périmètres possible (exprimées en mètres):

  $$12(84 + 1) = 1020, \quad 12(4 + 21) = 300, \quad 12(3 + 28) = 372, \quad 12(7 + 12) = 228.$$

- **Exercice 6**

  On peut toujours supposer en fait que les décompositions de a et b s'écrivent

  $$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$$

  où $p_1, \dots, p_n$ sont des nombres premiers deux à deux distincts. Il suffit pour cela de tolérer des exposants nuls (et non nécessairement strictement positifs) parmi les α_i et β_i. Montrons alors le critère suivant :/a divise b si et seulement si pour tout entier i compris entre 1 et n on a $\alpha_i \leq \beta_i$.

  Supposons que pour tout entier i compris entre 1 et n on a $\alpha_i \leq \beta_i$ et montrons que a divise b. Pour i compris entre 1 et n, posons $\gamma_i := \beta_i - \alpha_i$. Par hypothèse, γ_i est un entier positif. On peut donc considérer l'entier

$$c := p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n}.$$

On a alors

$$ac := \prod_{i=1}^{n} p_i^{\alpha_i} \prod_{i=1}^{n} p_i^{\gamma_i} = \prod_{i=1}^{n} p_i^{\alpha_i+\gamma_i} = \prod_{i=1}^{n} p_i^{\beta_i} = b.$$

Ainsi a divise b.

Supposons que a divise b et montrons que pour tout entier i compris entre 1 et n on a $\alpha_i \leq \beta_i$ Soit c l'entier positif tel que $b = ac$. Comme c divise b, tout facteur premier de c est un facteur premier de b. Ainsi les facteurs premiers de c sont dans l'ensemble $\{p_1, \dots, p_n\}$. La décomposition de c s'écrit donc

$$c := p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n}$$

où les γ_i sont des entiers positifs (pas nécessairement strictement positifs). Un calcul similaire à celui effectué précédemment montre alors qu'on a

$$b = \prod_{i=1}^{n} p_i^{\alpha_i+\gamma_i}.$$

Par unicité de la décomposition en facteurs premiers, pour tout entier i compris entre 1 et n on a $\beta_i = \alpha_i + \gamma_i$. Comme γ_i est positif, on a bien $\beta_i \geq \alpha_i$

Pour l'application demandée, écrivons, d'après l'exercice 4,

$$1224 = 2^3 \times 3^2 \times 5^0 \times 7^0 \times 11^0 \times 17^1 \quad \text{et} \quad 770000000 = 2^7 \times 3^0 \times 5^7 \times 7^1 \times 11^1 \times 17^0.$$

L'exposant de 3 dans la décomposition de 1224 est 2 pour 1224 et 0 pour 77770000000. Comme $2 > 0$, 1224 ne divise pas 77770000000.

Notons que le critère démontré ci-dessus peut se reformuler ainsi avec les notations initiales de l'énoncé (où les α_i et β_i sont supposés strictement positifs): a divise b si et seulement si pour tout entier i compris entre 1 et n, il existe un entier j compris entre 1 et m tel que $q_j = p_i$ et $\alpha_i \leq \beta_j$.