Arithmétique – TD 4

Nombres premiers

Exercice 1. Donner la liste de tous les nombres premiers inférieurs à 100.

Correction 1. Voir l'autre feuille de correction.

Exercice 2. Prouver que pour vérifier qu'un entier p est premier, il suffit de vérifier qu'il n'a pas de diviseurs compris entre 2 et $\sqrt{p}$.

Correction 2. (Il faut supposer $p \geqslant 2$ dans l'énoncé.)
On demande de montrer « si p n'a pas de diviseur compris entre 2 et $\sqrt{p}$, alors il est premier », ce qui revient, logiquement, à montrer : « si p n'est pas premier, alors il possède un diviseur compris entre 2 et $\sqrt{p}$ ». Montrons cette dernière assertion.
Si $p \geqslant 2$ n'est pas premier, on peut l'écrire $p = ab$ où $a \in \mathbb{N}^*$, $a \neq 1$ et $b \neq 1$ (donc $a \geqslant 2$, $b \geqslant 2$). Si a et b sont strictement supérieurs à $\sqrt{p}$, alors le produit ab est strictement supérieur $\sqrt{p}^2 = p$, ce qui est impossible. Donc l'un des deux, a ou b, est bien inférieur à $\sqrt{p}$, CQFD.

Exercice 3. Rappeler l'énoncé et la démonstration du Lemme d'Euclide.
En déduire par récurrence que si un nombre premier p divise un produit d'entiers, alors il divise au moins l'un d'entre eux.

Correction 3. Voir l'autre feuille de correction.

Exercice 4. Donner la décomposition en facteurs premiers de

a) 2310

b) 1224

c) 770000000

d) $7^{24} \times 14^{2020}$

e) 2310×1224

Correction 4. Voir l'autre feuille de correction.

Exercice 5. Un terrain rectangulaire dont les dimensions en mètres a et b sont des nombres entiers, a pour aire 3024 m^2. Calculer son périmètre sachant que le pgcd de a et b est 6. Combien y a-t-il de solutions possibles ?

Correction 5. Voir l'autre feuille de correction.

Exercice 6. Soient a et b deux entiers naturels. On écrit leur décomposition en facteurs premiers :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, \qquad b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}. \tag{1}$$

Donner une condition nécessaire et suffisante sur ces décompositions pour avoir $a|b$.
En appliquant cette idée, vérifier si 1224 divise 770000000 ou non.

Correction 6. Voir l'autre feuille de correction.

Exercice 7. Soient a et b deux entiers naturels. On suppose que a^2 divise b^2. En utilisant la décomposition en facteurs premiers, montrer que a divise b.

Correction 7. On utilise la méthode de l'Exercice 6. Comme dans la correction de l'Exercice 6, on note $p_1, \dots, p_n$ l'ensemble des facteurs premiers de a **et** b, et quitte à autoriser certains exposants α_j ou β_j nuls, on peut écrire

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \quad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}.$$

Du coup en prenant les carrés,

$$a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_n^{2\alpha_n} \quad \text{et } b^2 = \quad p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_n^{2\beta_n}.$$

Donc, par l'Exercice 6, on sait que $a^2 | b^2$ si et seulement si $\forall i$, $2\alpha_i \leqslant 2\beta_i$, ou encore $2(\alpha_i - \beta_i) \leqslant 0$. En divisant par 2, on obtient la condition équivalente $\alpha_i - \beta_i \leqslant 0$, soit $\alpha_i \leqslant \beta_i$. Par l'Exercice 6, cette condition est équivalente à $a|b$.

Exercice 8. Soient a et b deux entiers naturels. On écrit leur décomposition en facteurs premiers comme en (1). Donner une condition nécessaire et suffisante sur ces décompositions pour que a et b soient premiers entre eux.

Correction 8. Attention, dans (1) on utilise la convention du cours : en particulier les exposants sont strictement positifs.

Supposons a et b premiers entre eux. Puisque a et b n'ont pas de diviseurs communs positifs autre que 1, ils ne peuvent pas avoir de diviseurs premiers communs. Autrement dit :

$$\text{Les ensembles} \{p_1, \dots, p_n\} \text{ et } \{q_1, \dots, q_m\} \text{ sont } \textbf{disjoints.} \tag{2}$$

Montrons que cette condition nécessaire est également suffisante. Par contraposée, supposons que a et b ne soient pas premiers entre eux ; il existe donc un diviseur commun $d \geqslant 2$. Soit $p \geqslant 0$ un diviseur premier de d (ça existe toujours, cf. le cours ! — il suffit de prendre $d \geqslant 2$ le plus petit possible). Alors p appartient à la fois aux diviseurs premiers de a et à ceux de b, ce qui contredit (2).
On a donc bien montré que cette condition (2) est nécessaire et suffisante pour que a et b soient premiers entre eux.

Exercice 9. Soient $a = 2^5 \times 7^4 \times 17^{2019}$ et $b = 3^6 \times 7 \times 17 \times 23$. Quel est le pgcd de (a, b) ? Donner la décomposition en facteurs premiers du ppcm de (a, b).

Correction 9. Tout d'abord remarquons que les décompositions données dans l'énoncé sont bien les décompositions en facteurs premiers de a et b.
Notons $d = \text{pgcd}(a, b)$. De façon similaire à l'exercice 8, on voit que tout diviseur premier de d doit être un diviseur commun à a et b, donc appartient à la fois à l'ensemble $\{2, 7, 17\}$ et à l'ensemble $\{3, 7, 17, 23\}$. L'ensemble des diviseurs premiers de d est donc l'**intersection** de ces ensembles, soit l'ensemble $\{7, 17\}$. D'après l'Exercice 6, les exposants autorisés dans la décomposition de d en facteurs premiers sont les entiers naturels inférieurs ou égaux à la fois aux exposants correspondants dans la décomposition de a et dans celle de b. Puisqu'on cherche le **plus grand possible**, c'est exactement, pour chaque nombre premier 7 ou 17, le **plus petit exposant** (eh oui !) correspondant. Pour 7, l'exposant dans la décomposition de a est 4, et pour b, c'est 1 ; on doit donc choisir 7^1. De même, on doit choisir 17^1. Donc le pgcd est $d = 7 \times 17$.

Le **ppcm** n'a pas été introduit en cours, il devait être introduit dans la séance de TD. Il s'agit du *plus petit commun multiple*. De façon générale, pour obtenir le ppcm de deux entiers a et b, on regarde l'intersection de l'ensemble des multiples positifs de a avec l'ensemble des multiples positifs de b, et on prend **le plus petit élément non nul** de cette intersection. Par exemple, le ppcm

de 10 et 12 est 60, car les multiples positifs non nuls de 10 sont $\{10, 20, 30, 40, 50, 60, 70, \ldots\}$ tandis que les multiples positifs non nuls de 12 sont $\{12, 24, 36, 48, 60, 72, \ldots\}$.
La décomposition en facteurs premiers donne une façon pratique de calculer le ppcm. En effet, si $q = \text{ppcm}(a, b)$, alors $a|q$ et $b|q$, donc les facteurs premiers de a et b doivent **tous** être présents dans la décomposition de q, et leurs exposants dans la décomposition de q doivent être supérieurs ou égaux à ceux correspondant dans a **et** b. Pour obtenir le ppcm, il suffit donc de considérer l'**union** des facteurs premiers de a et b, et de choisir comme exposants le **maximum des exposants** respectifs de a et b.
Ainsi, pour cet exercice, on doit choisir les nombres premiers $\{2, 3, 7, 17, 23\}$ et

$$q = \text{ppcm}(a, b) = 2^{\max\{5,0\}} \times 3^{\max\{0,6\}} \times 7^{\max\{4,1\}} \times 17^{\max\{2019,1\}} \times 23^{\max\{0,1\}} = 2^5 \times 3^6 \times 7^4 \times 17^{2019} \times 23.$$

Remarque : Si on effectue le produit pgcd $\times$ ppcm, c'est-à-dire dq, on retrouve pour chaque facteur premier la somme des exposants correspondants pour a **et** pour b, donc

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = a \times b.$$

Exercice 10. Quel est le nombre de diviseurs premiers de $n = 72000000$? Quel est le nombre de diviseurs positifs de n ?

Correction 10. Écrivons la décomposition en facteurs premiers de n. Puisque $72 = 8 \times 9 = 2^3 \times 3^2$, et que $10 = 2 \times 5$, on obtient

$$72000000 = 2^3 \times 3^2 \times (2 \times 5)^6 = 2^{3+6} \times 3^2 \times 5^6 = 2^9 \times 3^2 \times 5^6.$$

Donc n a seulement trois diviseurs premiers : $\{2, 3, 5\}$.
Cherchons maintenant tous les diviseurs. Ils s'obtiennent à partir des diviseurs premiers $\{2, 3, 5\}$ en mettant tous les exposants possibles, c'est-à-dire compris entre 0 et l'exposant correspondant dans n. Pour le nombre premier 2, on peut choisir tout exposant entre 0 et 9, il a donc 10 choix. De même on trouve 3 choix pour le nombre premier 3, et 7 choix pour le nombre premier 5. Par unicité de la décomposition en facteurs premiers, tous les choix donnent lieu à des diviseurs différents. Le nombre de diviseurs (positifs) de n est donc $10 \times 3 \times 7 = 210$.

Exercice 11. Quel est le nombre de zéros à la fin du nombre $100! = 1 \times 2 \times 3 \times \cdots \times 100$?

Correction 11. Comment trouver le nombre de zéros à la fin d'un nombre n (dans son écriture décimale, bien sûr) ? C'est le nombre maximal de fois qu'on peut « diviser par 10 » ce nombre. Écrivons en pensée la décomposition en facteurs premier de n. Ce nombre est divisible par 10 si la décomposition contient au moins 2×5. Tant qu'il reste un facteur 2 **et** un facteur 5, on peut diviser à nouveau par 10. Donc si la décomposition de n contient $2^\alpha \times 5^\beta$, on peut diviser $\min\{\alpha, \beta\}$ fois par 10. Moralité :

Le nombre de zéros à la fin de l'écriture décimale de n est $\min\{\alpha, \beta\}$, où α est l'exposant de 2 dans la décomposition en facteurs premiers de n, et β est l'exposant de 5.

Il reste à trouver ces exposants pour 100!. Parmi les nombres $1, 2, 3, \ldots, 100$, chaque nombre pair contribue **au moins** à un exposant 1 pour le nombre premier 2 ; donc l'exposant de 2 dans 100! est supérieur ou égal à $100/2 = 50$. Mais il y a beaucoup moins de facteurs de 5 : ils n'apparaissent que dans les nombres divsibles par 5, soit $\{5, 10, 15, \ldots, 100\}$ (il y en a $100/5 = 20$). Quels sont leurs exposants de 5 ? Puisque $5^2 = 25$ et $5^3 = 125$, les exposants ne peuvent être que 1 ou 2 ! L'exposant 2 apparaît seulement pour les multiples de 25, soit $\{25, 50, 75, 100\}$: 4 fois. Dans les $20 - 4 = 16$ multiples de 5 restants, l'exposant est 1. Donc l'exposant de 5 dans la décomposition de 100! est $2 \times 4 + 16 = 24$.

Il y a donc 24 zéros à la fin de 100!

Remarque : Essayer de programmer la fonction « factorielle » en python. Vous trouverez :

$$\begin{aligned}100! = 93326215443944152681699238856266700490715968264381621468592963895\cdots\\ \cdots 17599993229915608941463976156518286253697920827223758251185\cdots\\ \cdots 52109168640000000000000000000000000\end{aligned}$$

Il y a bien 24 zéros la fin !

Exercice 12. On rappelle la formule du coefficient binomial :

$$\binom{N}{k} = \frac{N!}{k!(N-k)!}$$

Soit p un nombre premier. Montrer que pour tout entier k tel que $0 < k < p$, p divise $\binom{p}{k}$.

Correction 12. Posons $n = \binom{p}{k}$. On a donc $p! = n \times k!(p-k)!$. Puisque p divise $p!$, forcément p divise le membre de droite. D'après le Lemme d'Euclide (Exercice 3), si un nombre premier divise un produit d'entiers, il doit diviser au moins l'un d'entre eux. Or p ne divise aucun des « facteurs » de $k! = 1 \times 2 \times \cdots \times k$ car $k < p$. De même p ne divise aucun des « facteurs » de $(p-k)! = 1 \times 2 \times \cdots \times (p-k)$ car $k > 1$. Donc p ne divise aucun des facteurs de $k!(p-k)!$. Le seul « facteur » encore possible dans le produit $n \times k!(p-k)!$, c'est n ; donc $p|n$.