Devoir à rendre le 20 octobre

Exercice 1. Montrer que pour tout entier naturel n, $40^n n!$ divise $(5n)!$.

Solution. Procédons par récurrence. La propriété est vraie quand $n = 1$ car 40 divise $5! = 120$. Supposons-la vraie au rang n et montrons qu'elle le reste au rang $n+1$: par hypothèse, il y a $k \in \mathbb{Z}$ tel que $(5n)! = k \cdot 40^n n!$, si bien que :

$$(5(n+1))! = (5n)! \cdot (5n+1) \cdots (5n+5) = k \cdot 40^n n! \cdot (5n+1) \cdots (5n+5)$$

Or $(5n+1) \cdots (5n+5) = 5(n+1) \cdot (5n+1) \cdots (5n+4)$, et $(5n+1) \cdots (5n+4)$ est le produit de quatre entiers consécutifs, donc est divisible par 8. Il suit que $(5n+1) \cdots (5n+5)$ est un multiple de $40(n+1)$. Enfin, $(5(n+1))!$ est multiple de $40^n n! \cdot 40(n+1) = 40^{n+1} \cdot (n+1)!$. Ceci conclut la récurrence.

Exercice 2. Soient a, b, n, m des entiers naturels tels que $n \wedge m = 1$ et $a^n = b^m$. Montrer qu'il existe c tel que $a = c^m$ et $b = c^n$.

Solution. Écrivons la décomposition de a et de b en produits de facteurs premiers :

$$a = \prod_{p \in \mathcal{P}} p^{v_p(a)}, \qquad b = \prod_{p \in \mathcal{P}} p^{v_p(b)}$$

où $\mathcal{P}$ est l'ensemble des nombres premiers et $v_p(k)$ est la valuation p-adique de k. On sait que $v_p(a^n) = nv_p(a)$ pour chaque nombre premier p. Mais alors, $nv_p(a) = mv_p(b)$. Comme $n \wedge m = 1$, d'après le lemme de Gauß $v_p(a)$ est un multiple de m (éventuellement 0), disons $v_p(a) = mu_p$ avec $u_p \in \mathbb{N}$. On voit que ce nombre vérifie aussi $v_p(b) = nu_p$. Soit alors :

$$c = \prod_{p \in \mathcal{P}} p^{u_p}$$

Par construction, $c^m = a$ et $c^n = b$.

Exercice 3.

a) Calculer $(3^{123} - 5) \wedge 25$. Expliquer la méthode ; un résultat ne suffit pas.

b) Même question pour $(2^{445} + 7) \wedge 15$.

Solution.

a) Soit p un facteur premier, s'il en existe, de $(3^{123} - 5) \wedge 25$. Alors p divise 25, donc $p = 5$. Mais comme p divise $3^{123} - 5$, p divise 3^{123}, donc $p = 3$. C'est une contradiction. L'entier naturel non-nul $(3^{123} - 5) \wedge 25$ n'a pas de facteur premier : il vaut donc 1.

b) Soit p un facteur premier, s'il en existe, de $(2^{445} + 7) \wedge 15$. Alors p divise 15, donc p vaut 3 ou 5. Or pour tout nombre impair k, $2^k \equiv 2[3]$ (on peut voir cela comme le petit théorème de Fermat mais cela se démontrerait sans peine à la main). Donc $2^{445} + 7 \equiv 0[3]$ et 3 divise bien $2^{445} + 7$. D'autre part, pour tout nombre k congru à 1 modulo 4, $2^k \equiv 2[5]$ (ici encore, on peut l'interpréter comme le théorème de Lagrange dans le groupe $(\mathbb{Z}/5\mathbb{Z} \setminus \{0\}, \cdot)$, ou le voir par récurrence). Donc $2^{445} + 7 \equiv 4[5]$, et 5 ne divise pas $2^{445} + 7$. En conclusion, $(2^{445} + 7) \wedge 15 = 3$.

Exercice 4.

a) Résoudre (dans $\mathbb{Z}^2$) l'équation $323x - 391y = 612$. (On veillera à rédiger spécialement bien cette question, attendu que le correcteur ne lit pas les calculs.)

b) Soient a, b des entiers positifs premiers entre eux et $c > ab$. Montrer que $ax + by = c$ a des solutions dans $\mathbb{N}^2$.

Solution.

a) Commençons par déterminer le plus grand commun diviseur de 323 et 391.

Voici, pour l'étudiant perdu, le détail des calculs ; il n'est pas nécessaire de rédiger cela :

$$\begin{aligned} 391 &= 1 \cdot 323 + 68 \\ 323 &= 4 \cdot 68 + 51 \\ 68 &= 1 \cdot 51 + 17 \\ 51 &= 3 \cdot 17 + 0 \end{aligned}$$

Tous calculs faits, on trouve $323 \wedge 391 = 17$. Comme 17 divise bien 612, on aura des solutions (notons en passant que $612 = 17 \cdot 36$). Commençons par en déterminer une au moyen d'une relation de Bézout.

Ici encore, indiquons comment nous procéderions (non demandé sur la copie) :

$$\begin{aligned} 17 &= 68 - 51 \\ &= 68 - (323 - 4 \cdot 68) \\ &= 5 \cdot 68 - 323 \\ &= 5 \cdot (391 - 323) - 323 \\ &= 5 \cdot 391 - 6 \cdot 323 \end{aligned}$$

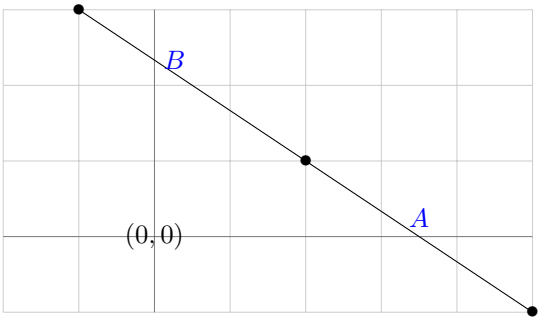
On voit que $323 \cdot (-6) - 391 \cdot (-5) = 17 = \frac{612}{36}$. Donc une première solution est $(-216, -180)$. Voyons enfin que $\frac{323}{17} = 19$ et $\frac{391}{17} = 23$. On sait alors que les solutions forment l'ensemble :

$$\{(-216 + 23k, -180 + 19k) : k \in \mathbb{Z}\}$$

b) C'était la question difficile du jour, celle qui demandait un peu de réflexion.
Comme $a \wedge b = 1$ on sait qu'il y a des solutions. Si l'on note (x_0, y_0) une solution quelconque, on sait que l'ensemble des solutions est :

$$\{(x_0 + kb, y_0 - ka) : k \in \mathbb{Z}\}$$

Nous cherchons à montrer qu'il existe $k \in \mathbb{Z}$ tel que $(x_0 + kb, y_0 - ka)$ soit dans $\mathbb{N}^2$. L'absence totale d'inspiration face aux inégalités en jeu suggère de raisonner géométriquement.
Les solutions sont les point à coordonnées entières sur la droite d'équation $ax + by = c$:



Nous voulons montrer qu'il y a sur la droite un point entier du quart nord-est. Commençons par remarquer que le dessin est conforme à nos attentes : tout d'abord, un vecteur directeur de la droite est $\begin{pmatrix} b \\ -a \end{pmatrix}$, qui pointe bien vers le sud-est. En outre la droite est passe bien par le quart nord-est : sinon, c serait négatif.
Vu la structure de l'ensemble des solutions, la distance (dans le plan) entre deux solutions est :

$$\left\| \begin{pmatrix} b \\ -a \end{pmatrix} \right\| = \sqrt{a^2 + b^2}$$

En outre la droite coupe les axes aux points $A(\frac{c}{a}, 0)$ et $B(0, \frac{c}{b})$, qui sont à distance :

$$AB = \sqrt{\left(\frac{c}{a}\right)^2 + \left(\frac{c}{b}\right)^2} = \sqrt{\frac{(a^2 + b^2)c^2}{a^2 b^2}}$$

Mais grâce à l'hyopthèse $c > ab$, on trouve :

$$AB = \sqrt{\frac{(a^2+b^2)c^2}{a^2b^2}} \geq \sqrt{a^2+b^2} = \left\| \begin{pmatrix} b \\ -a \end{pmatrix} \right\|$$

Il y a donc une solution entre A et B. Ce qu'on voulait démontrer.

Exercice 5. Soit $n \geq 2$ un entier ; on écrit sa décomposition $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

a) Cas particulier : $n = 504$. Effectuer sa décomposition en facteurs premiers, et lister ses diviseurs. Dans la suite on revient au cas général.

b) Montrer que le nombre de diviseurs de n est :

$$d(n) = \prod_{i=1}^{r} (\alpha_i + 1)$$

c) Montrer que n est un carré si et seulement si $d(n)$ est impair.

d) Montrer que si n est un carré alors le produit des diviseurs de n est :

$$\prod_{d|n} d = \sqrt{n}^{d(n)}$$

Solution.

a) Tous calculs faits, on trouve : $504 = 2^3 \cdot 3^2 \cdot 7$. On peut alors lister les diviseurs en ordre croissant : $\{1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 18, 21, 24, 28, 36, 42, 56, 63, 72, 84, 126, 168, 252, 504\}$. Il y en a 24.

b) Rappelons que m divise n ssi pour tout premier p, $v_p(m) \leq v_p(n)$. Par l'existence et l'unicité de la décomposition, il y a autant de diviseurs de n que de choix de suites $(u_p)_{p\in\mathcal{P}}$ telles que pour tout premier p, $0 \leq u_p \leq v_p(n)$. Pour chaque entier p il y a $v_p(n)+1$ possibilités. Au total le nombre de diviseurs de n est :

$$\prod_{p\in\mathcal{P}} v_p(n) + 1$$

Ce produit est fini car $v_p(n) \neq 0$ un nombre fini de fois ; avec nos notations, le nombre de diviseurs est $(\alpha_1 + 1) \cdot (\alpha_r + 1)$.

c) On voit que n est un carré ssi pour chaque nombre premier p, $v_p(n)$ est pair. Or d'après la formule que nous venons d'établir, $d(n)$ est impair ssi pour chaque nombre premier p, $v_p(n)+1$ est impair. On a bien l'équivalence.

d) C'est une adaptation de l'argument donnant $1 + \cdots + n$.
Listons les diviseurs de n par paires $(d, \frac{n}{d})$: il y a $d(n)$ paires dans cet ensemble E. On remarque que le produit de d et de $\frac{n}{d}$ est toujours n. Prenant le produit de toutes les paires :

$$\left(\prod_{d|n} d\right)^2 = \left(\prod_{(d,\frac{n}{d})\in E} d\right)^2 = \prod_{(d,\frac{n}{d})\in E} d \cdot \prod_{(d,\frac{n}{d})\in E} \frac{n}{d} = \prod_{(d,\frac{n}{d})\in E} n = n^{d(n)}$$

si bien que :

$$\prod_{d|n} d = \sqrt{n}^{d(n)}$$

On remarque qu'il n'était pas nécessaire de supposer que n est carré : le résultat est général.