Jour 2

VALUATIONS p-ADIQUES

solutions

Question 1

On divise autant de fois que possible x par p. La variable k sert à compter le nombre de divisions effectuée : c'est la valuation p-adique de x.

```
from numpy import inf as ∞
def Valuation(p, x) :
    if x == 0 :
        return ∞
    k = 0
    while x % p == 0 :
        k += 1 ; x //= p
    return k
```

Question 2

Soit x un nombre tel que $\sqrt[r]{x}$ est entier. Si $x = 0$, alors $\sqrt[r]{x} = 0$ aussi, et toutes les valuations valent $+\infty$. Écartons-donc ce cas et supposons que x (et donc $\sqrt[r]{x}$) sont au moins égaux à 1. On écrit leurs décompositions en produits de nombres premiers :

$$x = \prod_p p^{v_p(x)} \qquad \text{et} \qquad \sqrt[r]{x} = \prod_p p^{\alpha_p},$$

les produits étant pris sur tous les nombres premiers p, et les exposants α_p étant des entiers inconnus. Élevons la deuxième décomposition à la puissance r : on obtient

$$x = (\sqrt[r]{x})^r = \left(\prod_p p^{\alpha_p}\right)^r = \prod_p (p^{\alpha_p})^r = \prod_p = p^{r\times\alpha_p}.$$

On a désormais deux décompositions de x : on peut les identifier. Pour tout nombre premier p, on a $v_p(x) = r \times \alpha_p$, ce qui signifie que $v_p(x)$ est un multiple de r.

Exercice A

a) Quitte à échanger x et y, supposons que c'est x qui a la valuation la plus petite. Donc $p^{v_p(x)}$ divise x, mais aussi y, et donc il divise leur somme $x + y$. De $p^{v_p(x)} \mid x + y$ on déduit que $v_p(x + y) \geqslant v_p(x)$, ce qui démontre la relation de l'énoncé.

b) Écrivons $x = p^m \times q$ et $y = p^n \times q'$, avec q et q' deux entiers qui ne sont pas divisibles par p (de sorte que $m = v_p(x)$ et $n = v_p(y)$). Quite à les échanger, supposons que c'est x qui a la valuation la plus petite : $m < n$ (c'est-à-dire $n - m > 0$). On a alors

$$x + y = p^m \times (q + p^{n-m}q').$$

Puisque p divise p^{n-m} , et donc $p^{n-m}q'$, il ne divise pas $q + p^{n-m}q'$ (sinon il diviserait la différence $q = q + p^{n-m}q' - p^{n-m}q'$, ce qui est exclu). Donc p se factorise *exactement* m fois dans $x + y$, c'est-à-dire

$$v_p(x + y) = m = \min(v_p(x), v_p(y)).$$

c) D'après la question précédente, pour avoir une inégalité stricte, il faut choisir des cas où x et y ont la même valuation. Avant cela, observons ce qui peut se passer : prenons $x = p^n$ et $y = p^n \times (p-1)$. On a $v_p(x) = v_p(y) = n$. Mais

$$x + y = p^n + p^n \times (p-1) = p^n \times (1 + p - 1) = p^{n+1},$$

de sorte que $v_p(x+y) = n+1$. Bon, ceci étant dit, on demandait des exemples, en voici :

$$v_2(2+2) = v_2(4) = 2 \qquad \text{alors que} \qquad \min(v_2(2),\, v_2(2)) = \min(1,\, 1) = 1,$$

$$v_5(15+35) = v_5(50) = 2 \qquad \text{alors que} \qquad \min(v_5(15),\, v_5(35)) = \min(1,\, 1) = 1,$$

ou encore

$$v_3(9+234) = v_3(243) = v_3(3^5) = 5 \qquad \text{alors que} \qquad \min(v_3(9),\, v_3(234)) = \min(2,\, 2) = 2.$$

Question 3

Remarquons que la fonction « partie entière » est croissante : si $x \leqslant y$ alors $\lfloor x \rfloor \leqslant \lfloor y \rfloor$. Maintenant si p est un nombre premier (donc en particulier un nombre strictement plus grand que 1) on a $m \leqslant n$ implique $p^m \leqslant p^n$ et donc $x/p^m \geqslant x/p^n$. En appliquant la partie entière on trouve

$$m \leqslant n \qquad \text{implique} \qquad \left\lfloor \frac{x}{p^m} \right\rfloor \geqslant \left\lfloor \frac{x}{p^n} \right\rfloor,$$

ce qui signifie que la suite $(u_n)_{n \geqslant 0}$ est décroissante.

D'autre part, puisque $p > 1$, on a $p^n \longrightarrow +\infty$ lorsque $n \to \infty$. Il est donc plus strictement grand que x à partir d'un rang, disons, n_0 ; et donc pour $n \geqslant n_0$ on a $x/p^n < 1$ c'est-à-dire $u_n = 0$ (la partie entière d'un nombre dans $[0\,;\,1[$ étant 0 évidemment).

Question 4

Une première chose importante : si d est un entier strictement positif, le nombre de multiples de d entre 1 et x est $\lfloor x/d \rfloor$. Voyons pourquoi : les multiples sont $1d$, $2d$, $3d$, etc. jusqu'à md disons ; c'est-à-dire qu'on a $md \leqslant x < (m+1)d$. Mézalor en divisant par d on obtient

$$m \leqslant \frac{x}{d} < m + 1$$

ce qui veut bien dire que m est la partie entière de x/d.

Maintenant la question. Dans le produit

$$x! = 1 \times 2 \times 3 \times 4 \times 5 \times \ldots \times x,$$

les multiples de p apportent 1 facteur p, sauf ceux qui sont multiples de p^2 (qui en apportent 2), sauf ceux qui sont multiples de p^3 (qui en apportent 3), etc.. Notons N_1 le nombre de multiples de p (entre 1 et x, nous le redirons pas) qui ne sont pas multiples de p^2, N_2 le nombre de multiples de p^2 qui ne sont pas multiples de p^3, etc., et plus généralement N_n le nombre de multiples de p^n qui ne sont pas multiples de p^{n+1}. On a

$$v_p(x!) = 1 \times \mathrm{N}_1 + 2 \times \mathrm{N}_2 + 3 \times \mathrm{N}_3 + 4 \times \mathrm{N}_4 + \ldots$$

et cette somme, même si on ne sait pas jusqu'où l'écrire, se termine, puisque nous l'avons dit dans la question précédente : N_n est toujours égal à 0 à partir d'un certain rang. Réorganisons les termes (il y a bien le même nombre de chaque N_n, en tout, que dans l'écriture précédente !) :

$$v_p(x!) = (\mathrm{N}_1 + \mathrm{N}_2 + \mathrm{N}_3 + \mathrm{N}_4 + \ldots) + (\mathrm{N}_2 + \mathrm{N}_3 + \mathrm{N}_4 + \ldots) + (\mathrm{N}_3 + \mathrm{N}_4 + \ldots) + (\mathrm{N}_4 + \ldots) + \ldots.$$

Enfin, on constate que $\mathrm{N}_1 + \mathrm{N}_2 + \mathrm{N}_3 + \mathrm{N}_4 + \dots$ est égal au nombre de multiples de p entre 1 et x (puisqu'on avait exclu ceux qui sont multiples de p^2, de p^3, etc., mais qu'ici on les remet). Plus généralement, $\mathrm{N}_n + \mathrm{N}_{n+1} + \mathrm{N}_{n+2} + \dots$ est le nombre de multiples de p^n entre 1 et x ; et comme nous l'avons dit ce nombre est égal à $\lfloor x/p^n \rfloor$. De sorte qu'au final

$$v_p(x!) = \left\lfloor \frac{x}{p^1} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \left\lfloor \frac{x}{p^3} \right\rfloor + \left\lfloor \frac{x}{p^4} \right\rfloor + \left\lfloor \frac{x}{p^5} \right\rfloor + \dots$$

qui est bien la formule annoncée. Insistons : cette somme s'arrête, puisque tous les termes sont nuls à partir d'un certain rang.

Exercice B

a) Pour tout entier n on a

$$\left\lfloor \frac{x}{2^n} \right\rfloor \geqslant \left\lfloor \frac{x}{5^n} \right\rfloor$$

puisque $2 \leqslant 5$. Les sommes préservent les inégalités, donc

$$\sum_{n \geqslant 0} \left\lfloor \frac{x}{2^n} \right\rfloor \geqslant \sum_{n \geqslant 0} \left\lfloor \frac{x}{5^n} \right\rfloor \qquad \text{c'est-à-dire} \qquad v_2(x!) \geqslant v_5(x!).$$

b) Le nombre de zéros à la fin de $x!$ est égal au nombre de fois qu'on peut factoriser 10 dans $x!$. Écrivons la décomposition en produit de nombres premiers de $x!$:

$$x! = \prod_p p^{v_p(x!)} = 2^{v_2(x!)} \times 5^{v_5(x!)} \times \prod_{p \neq 2,\,5} p^{v_p(x!)} = (2 \times 5)^{v_5(x!)} \times 2^{v_2(x!) - v_5(x!)} \times \prod_{p \neq 2,\,5} p^{v_p(x!)},$$

et on peut écrire la dernière égalité car (nous l'avons dit, et même écrit) il y a plus de facteurs 2 que de facteurs 5 dans $x!$: c'est la question **a**. Puisque 5 ne se factorise pas dans

$$2^{v_2(x!) - v_5(x!)} \times \prod_{p \neq 2,\,5} p^{v_p(x!)},$$

le nombre 10 ne s'y factorise pas non plus, et donc $10 = 2 \times 5$ se met exactement $v_5(x!)$ fois en facteur dans $x!$.

c) Écrivons le programme qui calcule cette somme de la **Question 4**, pour un x et un p donnés. On utilise une variable P qui parcourt les puissances de p : elle vaut successivement p, p^2, p^3, etc..

```
def ValuationFactorielle(x, p) :
    v = 0 ; P = p
    while P <= x :
        v += x // P ; P *= p
    return v
```

d) Il ne reste plus qu'à utiliser ce programme !

```
>>> ValuationFactorielle(10 ** 6, 5)
249998
```

Il y a donc 249 998 zéros à la fin de $10^6!$.

Question 5

Puisque k divise k', il existe un entier d tel que $k' = d \times k$. Et puisque k' divise k, il existe un entier d' tel que $k = d' \times k'$. C'est-à-dire finalement $k' = d \times k = d \times d' \times k'$. Donc $d \times d' = 1$. Et donc $d = \pm 1$ (tout comme $d' = \pm 1$) ce qui veut dire que $k' = \pm k$.

Exercice C

a) Commençons par rappeler comment voir, à partir de la décomposition en facteurs premiers, si un nombre en divise un autre :

$$\prod_p p^{\alpha_p} \qquad \text{divise} \qquad \prod_p p^{\beta_p}$$

si et seulement si pour tout nombre premier p on a $\alpha_p \leqslant \beta_p$. Maintenant venons-en à la question : puisque $\min(v_p(x),\, v_p(y)) \leqslant v_p(x)$ pour tout nombre premier p, on en déduit que

$$\delta = \prod_p p^{\min(v_p(x),\, v_p(y))} \qquad \text{divise} \qquad \prod_p p^{v_p(x)} = x.$$

De la même manière, il divise aussi y. Et donc leur PGCD. Montrons inversement que $\mathrm{PGCD}(x\,;\,y)$ divise δ. Comme $\mathrm{PGCD}(x\,;\,y)$ est un diviseur de x, on en déduit que $v_p(\mathrm{PGCD}(x\,;\,y)) \leqslant v_p(x)$ pour tout nombre premier p. De même, comme $\mathrm{PGCD}(x\,;\,y)$ est un diviseur de y, on en déduit que $v_p(\mathrm{PGCD}(x\,;\,y)) \leqslant v_p(y)$ pour tout nombre premier p. Et finalement, pour tout nombre premier p, $v_p(\mathrm{PGCD}(x\,;\,y))$ est inférieur à la fois à $v_p(x)$ et $v_p(y)$, donc au plus petit d'entre eux (c'est-à-dire leur minimum). Ceci étant vrai pour tout p, on en déduit que

$$\mathrm{PGCD}(x\,;\,y) = \prod_p p^{v_p(\mathrm{PGCD}(x\,;\,y))} \qquad \text{divise} \qquad \prod_p p^{\min(v_p(x),\, v_p(y))} = \delta.$$

b) Puisque $\mathrm{PGCD}(x\,;\,y)$ et δ se divisent l'un l'autre, ils sont (d'après la question **a**) égaux ou opposés. Et puisqu'ils sont par définition tous les deux positifs, ils sont égaux.

c) Démontrons que μ est à la fois un multiple de x et de y. C'est le même argument qu'à la question `a` : pour tout nombre premier p, on a $v_p(x) \leqslant \max(v_p(x),\, v_p(y))$, de sorte que

$$x = \prod_p p^{v_p(x)} \qquad \text{divise} \qquad \prod_p p^{\max(v_p(x),\, v_p(y))} = \mu.$$

(Autrement dit μ est un multiple de x.) De même y divise μ (ou μ est un multiple de y). Ainsi μ est un multiple à la fois de x et de y, donc aussi un multiple de leur PPCM. Inversement montrons que $\mathrm{PPCM}(x\,;\,y)$ est un multiple de μ. D'abord $\mathrm{PPCM}(x\,;\,y)$ est un multiple de x, donc pour tout nombre premier p on a $v_p(x) \leqslant v_p(\mathrm{PPCM}(x\,;\,y))$. De même c'est un multiple de y donc pour tout nombre premier p on a aussi $v_p(y) \leqslant v_p(\mathrm{PPCM}(x\,;\,y))$. Et puisque $v_p(\mathrm{PPCM}(x\,;\,y))$ est supérieur ou égal au deux, il est en particulier supérieur ou égal au plus grand des deux, c'est-à-dire

$$\max(v_p(x),\, v_p(y)) \leqslant v_p(\mathrm{PPCM}(x\,;\,y))$$

(pour tout nombre premier p). Et donc

$$\mu = p^{\max(v_p(x),\, v_p(y))} \qquad \text{divise} \qquad \prod_p p^{v_p(\mathrm{PPCM}(x\,;\,y))} = \mathrm{PPCM}(x\,;\,y).$$

d) Toujours le même argument : puisque μ et $\mathrm{PPCM}(x\,;\,y)$ se divisent l'un l'autre, ils sont égaux ou opposés ; et puisqu'ils sont par définition tous les deux positifs, ils sont donc égaux.

e) Deux arguments à donner dans cette question. D'abord, comme on ne connaît pas les signes de x et de y, on a

$$x = \pm \prod_p p^{v_p(x)} \qquad \text{et} \qquad y = \pm \prod_p p^{v_p(y)},$$

donc

$$|x \times y| = \prod_p p^{v_p(x)} \times \prod_p p^{v_p(y)} = \prod_p p^{v_p(x)+v_p(y)}.$$

Ensuite, il faut remarquer que pour tous réels a et b, on a $\min(a,\, b) + \max(a,\, b) = a + b$. Donc

$$\delta \times \mu = \prod_p p^{\min(v_p(x),\, v_p(y))} \times \prod_p p^{\max(v_p(x),\, v_p(y))} = \prod_p p^{\min(v_p(x),\, v_p(y))+\max(v_p(x),\, v_p(y))} = \prod_p p^{v_p(x)+v_p(y)}.$$

Et donc finalement $\delta \times \mu = |x \times y|$.

f) Si $x = 0$ ou $y = 0$, alors $\text{PPCM}(x\,;\,y) = 0$ donc on a à la fois $|x \times y| = 0$ et $\text{PGCD}(x\,;\,y) \times \text{PPCM}(x\,;\,y) = 0$. Ainsi la formule reste vraie dans ce cas.

Question 6

Et voici donc l'algorithme efficace (puisque basé sur celui des restes successifs d'Euclide) pour calculer le PPCM. On n'oublie pas de traiter à part le cas particulier, pour éviter une division par zéro.

```
def PPCM(x, y) :
    if x == 0 or y == 0 :
        return 0
    else :
        return abs(x * y) // PGCD(x, y)
```