DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Cours et exercices

AUTEUR : Irène MARCOVICI
STAGE : Montpellier 2012

Nombres premiers

- Nombres premiers -

Définition 1 (Nombres premiers)**.** Un entier naturel $p > 1$ est dit *premier* s'il possède exactement deux diviseurs naturels, à savoir 1 et p.

Les nombres premiers inférieurs à 20 sont $2, 3, 5, 7, 11, 13, 17, 19$. Parmi les nombres suivants : $67, 77, 87, 97$, lesquels sont-ils premiers ? Le nombre 67 est premier car il n'est divisible par aucun des entiers $2, 3, 5, 7$ et comme $11^2 > 67$, si 67 avait un facteur premier plus grand que 11, il aurait aussi un facteur premier plus petit. Le nombre 77 n'est pas premier car il est divisible par 7. Le nombre 87 n'est pas premier car il est divisible par 3. Le nombre 97 est premier car il n'est pas divisible par $2, 3, 5, 7$.

Exercice 1 Soit $p > 3$ un nombre premier. Montrer que $p^2 - 1$ est un multiple de 12.

Théorème 2 (Théorème fondamental de l'arithmétique)**.** Tout entier naturel $n > 1$ se décompose de manière unique en produit de nombres premiers.

Théorème 3. L'ensemble des nombres premiers est infini.

Démonstration. Supposons par l'absurde qu'il n'y a qu'un nombre fini n de nombre premiers. Notons ces nombres premiers $p_1, \ldots, p_n$, et posons $N = p_1 p_2 \ldots p_n + 1$. L'entier N n'est divisible par aucun des p_i. Donc soit il est premier, soit il admet un diviseur premier différent de $p_1, \ldots, p_n$. Dans tous les cas, on obtient une contradiction. □

Exercice 2 Montrer que pour tout entier naturel k, il est possible de trouver un entier n tel que les nombres $n + 1, \ldots, n + k$ soient tous composés.

Exercice 3 Montrer qu'il existe une infinité de nombres premiers de la forme $4k-1$.

Si la décomposition en facteurs premiers de l'entier $n \geqslant 1$ est $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, alors les diviseurs positifs de n sont les entiers de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout $1 \leqslant i \leqslant k$. Comme conséquence, on obtient une expression du pgcd et du ppcm de deux entiers lorsqu'on connaît leur décomposition en facteurs premiers. Précisément, si

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

où les p_i sont deux à deux distincts, mais les α_i et β_i sont éventuellement nuls, on a :

$$\operatorname{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_k^{\min(\alpha_k,\beta_k)}$$
$$\operatorname{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_k^{\max(\alpha_k,\beta_k)}$$

Si l'on remarque que pour α et β des entiers (ou des réels), on a toujours $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$, on déduit directement des deux expressions précédentes la relation suivante :

$$\operatorname{pgcd}(a,b) \cdot \operatorname{ppcm}(a,b) = ab.$$

Définition 4 (Valuation p-adique)**.** Si p est un nombre premier, et n un entier non nul, la valuation p-adique de n est le plus grand entier k tel que p^k divise n. On la note $\nu_p(n)$. Si $n = 0$, on convient que $\nu_p(0) = +\infty$ pour tout nombre premier p.

Si n non nul se décompose sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, alors $\nu_{p_i}(n) = \alpha_i$ pour tout $1 \leqslant i \leqslant k$, et $\nu_p(n) = 0$ si p est distinct des p_i. Ainsi, $\nu_p(n) = 0$ sauf pour un nombre fini de p premiers. Si a et b sont deux entiers, on a, pour tout nombre premier p :

$$\nu_p(ab) = \nu_p(a) + \nu_p(b)$$

$$\nu_p(a+b) \geqslant \min(\nu_p(a), \nu_p(b))$$

et la dernière inégalité est une égalité dès que $\nu_p(a) \neq \nu_p(b)$.

Exercice 4 Soient a et b des entiers strictement positifs tels que a^n divise b^{n+1} pour tout entier $n \geqslant 1$. Montrer que a divise b.

Exercice 5 (Formule de Legendre) On note $[x]$ la partie entière du réel x. Montrer que si p est un nombre premier et n est un entier positif, on a :

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots.$$

Lorsque $p^i > n$, on a $[\frac{n}{p^i}] = 0$. Ceci assure qu'il n'y a bien qu'un nombre fini de termes non nuls dans la somme précédente.

Exercice 6 Par combien de zéros se termine le nombre 2012! ?

Exercice 7 Montrer que le nombre

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

est un entier, quels que soient les entiers naturels m et n.

Exercice 8 Montrer que si la décomposition en facteurs premiers de n est $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, alors le nombre de diviseurs positifs de n vaut :

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$$

et le produit des diviseurs positifs de n vaut :

$$p(n) = n^{\frac{d(n)}{2}}.$$

Exercice 9 Montrer que si deux entiers m et n sont tels que $p(m) = p(n)$, alors $m = n$.

- Solutions des exercices -

Solution de l'exercice 1 On factorise : $p^2 - 1 = (p+1)(p-1)$. Comme p est un nombre premier différent de 2, il est impair. Ainsi, $p-1$ et $p+1$ sont tous les deux pairs et le produit est un multiple de 4. De même $p > 3$ et donc p ne peut-être un multiple de 3. On en déduit que soit $p-1$, soit $p+1$ est un multiple de 3, et donc $p^2 - 1$ en est également un. En conclusion, $p^2 - 1$ est multiple de 3 et de 4, et donc de 12.

Solution de l'exercice 2 Il suffit de prendre $n = (k+1)! + 1$.

Solution de l'exercice 3 On raisonne par l'absurde en supposant qu'il n'existe qu'un nombre fini de nombres premiers de cette forme, notés $p_1, p_2, \dots p_k$. On

considère alors $N = 4p_1p_2\dots p_k - 1$. Les diviseurs premiers de N sont distincts de 2 et des $p_i, 1 \leqslant i \leqslant k$. Or s'ils étaient tous de la forme $4n+1$, N s'écrirait aussi sous cette forme, donc il en existe au moins un qui est de la forme $4k-1$. Contradiction.

Solution de l'exercice 4 Soit p un nombre premier. L'hypothèse nous dit que $nv_p(a) \geqslant (n+1)v_p(b)$, soit encore :

$$v_p(a) \geqslant \Big(1 + \frac{1}{n}\Big)v_p(b)$$

et par passage à la limite $v_p(a) \geqslant v_p(b)$ pour tout nombre premier p. On en déduit que a divise b.

Solution de l'exercice 5 Pour un entier positif ou nul i, appelons n_i le nombre d'entiers compris entre 1 et n dont la valuation p-adique est exactement i. On a alors : $v_p(n!) = n_1 + 2n_2 + 3n_3 + \dots$. D'autre part, les entiers dont la valuation excède i sont exactement les multiples de p^i et sont au nombre de $\left[\frac{n}{p^i}\right]$, d'où :

$$\left[\frac{n}{p^i}\right] = n_i + n_{i+1} + \dots + n_{i+2} + \dots$$

Les deux formules précédentes mises ensemble démontrent la proposition.

Solution de l'exercice 6 L'entier 10 n'est pas premier : on ne peut donc pas appliquer directement la formule de Legendre. En décomposant 10 en facteurs premiers, on se rend compte que le plus grand exposant n tel que 10^n divise 2012! est le plus petit des deux nombres $v_2(2012!)$ et $v_5(2012!)$. La formule de Legendre prouve directement que c'est $v_5(2012!)$. Il vaut :

$$\left[\frac{2012}{5}\right] + \left[\frac{2012}{25}\right] + \left[\frac{2012}{125}\right] + \left[\frac{2012}{625}\right] + \left[\frac{2012}{3125}\right] + \dots = 402 + 80 + 16 + 3 + 0 + \dots = 501.$$

Le nombre 2012! se termine donc par 501 zéros.

Solution de l'exercice 7 Compte tenu de la formule de Legendre, il suffit de montrer que pour tout nombre premier p et pour tout entier k,

$$\left[\frac{2m}{p^k}\right] + \left[\frac{2n}{p^k}\right] \geqslant \left[\frac{m}{p^k}\right] + \left[\frac{n}{p^k}\right] + \left[\frac{m+n}{p^k}\right].$$

Or l'inégalité $[2a] + [2b] \geqslant [a] + [b] + [a+b]$ est vraie pour tous réels a et b.

Solution de l'exercice 8 On ne démontre que l'expression de $p(n)$ qui est la plus difficile. Un diviseur positif de n s'écrit $n = p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k}$ où $0 \leqslant \beta_i \leqslant \alpha_i$.

Le produit de tous ces nombres est de la forme $p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$. Il suffit donc de calculer les exposants γ_i. Fixons un entier $\nu \in \{0, 1, \dots, \alpha_1\}$. Il y a exactement $(\alpha_2+1)\dots(\alpha_k+1)$ diviseurs de n pour lesquels $\beta_1 = b$. Lorsque l'on multiplie tous ces diviseurs, on aura donc :

$$\gamma_1 = (\alpha_2+1)\dots(\alpha_k+1)\sum_{\nu=0}^{\alpha_1}\nu = \frac{1}{2}\alpha_1(\alpha_1+1)\dots(\alpha_k+1) = \alpha_1 \cdot \frac{d(n)}{2}.$$

On a bien entendu une formule analogue pour γ_i. En remettant tout bout à bout, on obtient la formule annoncée.

Solution de l'exercice 9 Écrivons : $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ et $n = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ où les p_i sont des nombres premiers deux à deux distincts et les exposants α_i et β_i sont des entiers positifs ou nuls. On a vu que le produit des diviseurs de m s'écrit : $p(m) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$ pour :

$$\gamma_i = \frac{1}{2}\alpha_i(\alpha_1+1)\dots(\alpha_k+1).$$

L'hypothèse de l'énoncé assure que pour tout i :

$$\frac{1}{2}\alpha_i(\alpha_1+1)\dots(\alpha_k+1) = \frac{1}{2}\beta_i(\beta_1+1)\dots(\beta_k+1)$$

et donc il existe un rationnel q, indépendant de i, tel que $\alpha_i = q\beta_i$. Quitte à intervertir m et n, on peut supposer $q \geqslant 1$. L'hypothèse se réécrit alors :

$$q(q\beta_1+1)\dots(q\beta_k+1) = (\beta_1+1)\dots(\beta_k+1)$$

et on voit directement que si $q > 1$, le membre de gauche est strictement supérieur à celui de droite. On a donc $q = 1$ et $m = n$.