Arithmétique – Partie 3 : Nombres premiers

Exercice 1.

Trouver tous les nombres premiers plus petits que 100.

Indications 1.

Il s'agit d'écarter les entiers qui ne sont pas des nombres premiers car divisibles par 2 ou par 3...

Correction 1.

Les nombres premiers jusqu'à 100 sont :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

On les obtient simplement par une méthode appelée le *crible d'Ératosthène* :

— en excluant d'abord tous les entiers pairs (sauf 2 bien sûr),

— puis tous les entiers divisibles par 3 (sauf 3),

— on n'a pas besoin d'exclure les multiples de 4 car ils sont déjà exclus en tant que multiples de 2,

— ensuite on exclut les multiples de 5 (sauf 5),

— les multiples de 6 sont déjà exclus (ce sont des multiples de 2 et de 3),

— il reste à exclure les multiples de 7,

— les multiples de 8, 9, 10 sont déjà exclus,

— et c'est terminé car un entier non premier plus petit que 100 doit avoir un facteur inférieur à $\sqrt{100} = 10$.

Exercice 2.

Calculer la décomposition en facteurs premiers de a puis de b, en déduire $\operatorname{pgcd}(a, b)$ et $\operatorname{ppcm}(a, b)$.

1. $a = 1500$, $b = 1470$.
2. $a = 18\,135$, $b = 92\,950$.

Indications 2.

Le pgcd et les ppcm s'obtiennent facilement une fois les entiers décomposés en facteurs premiers. Pour le pgcd prendre, pour chaque facteur premier, l'exposant minimum entre celui de a et celui de b, pour le ppcm prendre le maximum.

Correction 2.

1. $a = 1500 = 2^2 \times 3 \times 5^3$.

   Pour obtenir cette décomposition, on remarque que 1500 est divisible par 2 donc $1500 = 2 \times 750$, puis 750 est encore divisible par 2, donc $1500 = 2^2 \times 375$, cette fois 375 n'est pas divisible par 2 mais par contre il est divisible par 3, ainsi $1500 = 2^2 \times 3 \times 125$ et enfin $125 = 5^3$.

On obtient de même : $\quad b = 2 \times 3 \times 5 \times 7^2$.

Pour le pgcd et le ppcm on écrit les entiers avec tous les facteurs présents dans a ou b, quitte à mettre des exposants qui valent 0 :

$$a = 1500 = 2^2 \times 3^1 \times 5^3 \times 7^0$$

$$b = 1470 = 2^1 \times 3^1 \times 5^1 \times 7^2$$

Pour le pgcd on prend, pour chaque facteur premier, l'exposant *minimum* entre celui de a et celui de b :

$$\operatorname{pgcd}(a,b) = 2^1 \times 3^1 \times 5^1 \times 7^0 = 30$$

Pour le ppcm on prend, pour chaque facteur premier, l'exposant *maximum* entre celui de a et celui de b :

$$\operatorname{ppcm}(a,b) = 2^2 \times 3^1 \times 5^3 \times 7^2 = 73\,500$$

2.

$$a = 18\,135 = 3^2 \times 5 \times 13 \times 31 \qquad b = 92\,950 = 2 \times 5^2 \times 11 \times 13^2$$

$$\operatorname{pgcd}(a,b) = 2^0 \times 3^0 \times 5^1 \times 11^0 \times 13^1 \times 31^0 = 5 \times 13 = 65$$

$$\operatorname{ppcm}(a,b) = 2^1 \times 3^2 \times 5^2 \times 11^1 \times 13^2 \times 31^1 = 25\,933\,050$$

Exercice 3.

Soit p un nombre premier. Montrer que pour tout entier k tel que $1 \leqslant k \leqslant p-1$, alors p divise $\binom{p}{k}$.
On rappelle l'expression du coefficient binomial :

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

Indications 3.

Trouver un entier A tel que $\binom{p}{k} = p! \times A$ et utiliser le lemme de Gauss.

Correction 3.

Faisons d'abord la remarque suivante : si a et b sont deux entiers, si p est un nombre premier avec $p > a$ et $p > b$ alors bien sûr p ne peut pas diviser a, ni b (car p est plus grand que a et b) mais en plus p ne peut pas diviser $a \times b$. En effet par le lemme d'Euclide, si p divisait ab alors p diviserait a ou p diviserait b.

On sait que $\binom{p}{k} = \frac{p!}{k!(p-k)!} \iff p! = \binom{p}{k} \times k!(p-k)!$. Puisque p divise $p!$, p divise donc $\binom{p}{k} \times k!(p-k)!$.
Mais pour $1 \leqslant k \leqslant p-1$, tous les facteurs de $k!$ sont strictement inférieurs à p : cela signifie que p ne divise pas $k!$, et donc que $\operatorname{pgcd}(p, k!) = 1$. D'après le lemme de Gauss, on a donc : p divise $\binom{p}{k} \times (p-k)!$.
Mais il en va de même avec $(p-k)!$: pour $1 \leqslant k \leqslant p-1$, les facteurs de $(p-k)!$ sont tous strictement inférieurs à p. Donc p ne divise pas $(p-k)!$, et $\operatorname{pgcd}(p,(p-k)!) = 1$. Une nouvelle application du lemme de Gauss offre donc :

$$\boxed{\text{Pour } 1 \leqslant k \leqslant p-1, \qquad p \text{ divise } \binom{p}{k}.}$$