Arithmétique

Mercredi 1 Février 2017

Al Idrissi al-Qurtubi al-Hassani (1100-1165)

Géographe et botaniste marocain, connu pour son livre "Kitab Nuzhat al Mushtaq", un des meilleurs ouvrages de cartographie où il découpe le monde en 7 climats et régions et chaque climat en 10 sections, ce qui fait une grille de 70 rectangles. Pour chaque section, Al Idrissi avait rédigé une description détaillée de la géographie physique et des activités humaines. Sa connaissance du monde était remarquable à l'époque. L'image ci-contre reflète Le monde tel que Al Idrissi l'a imaginé orienté sud/nord

Blaque du jour

Un prof de Math disait à ses étudiants : Les hommes intelligents sont toujours dans le doute. Seuls les imbéciles sont constamment affirmatifs.

- Vous en êtes certain, monsieur ? demande une élève.
- Absolument certain !

Généralités.

Division dans $\mathbb{N}$.

Définition :

Soit $(a,b) \in \mathbb{N}^{*2}$, on dit que a divise b si et seulement si : $\exists k \in \mathbb{N}^*$ tel que $b = ka$

Remarque :

Si c divise a et b, alors c divise $ua + vb$, $\forall u, v \in \mathbb{Z}$.

Division euclidienne.

Théorème :

$\forall (a,b) \in \mathbb{N}^2 \quad \exists !(q,r) \in \mathbb{N}^2$ tel que $a = bq + r$ avec $0 \leqslant r < b$, q s'appelle le quotient de la division euclidienne de a par b et r son reste.

Propriétés.

Soit $(a,b) \in \mathbb{N}^2$ et $(q,r) \in \mathbb{N}^2$ tel que $a = bq + r$, avec $0 \leqslant r < b$, alors :

- a divise b si et seulement si $r = 0$.
- $a \equiv r \quad [b]$, en particulier $\overline{a} = \overline{r}$ dans $\mathbb{Z}/b\mathbb{Z}$, plus précisément $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n}\}$.

Algorithme d'Euclide.

Soit $(a,b) \in \mathbb{N}^{*2}$, on effectue les divisions euclidienne successive de a par b, en divisant à chaque fois le dernier quotient par son reste, jusqu'à trouver un reste nul. Soit r_n le dernier reste non nul, alors :

1. r_n est un diviseur commun de a et b.
2. Si d divise a et b, alors d divise r_n.
3. $\exists u, v \in \mathbb{Z}$ tel que $r_n = ua + vb$.

PGCD

Définition :

Soit $a, b \in \mathbb{N}$, l'ensemble des diviseurs communs de a et b dans $\mathbb{N}$ est une partie de $\mathbb{N}$ non vide (contenant 1) majorée par a et b, donc admet un plus grand, appelé PGCD de a et b, on le note par $a \wedge b$.

Théorème :

Soit $(a,b) \in \mathbb{N}^2$ et r_n le dernier reste non nul dans les divisions euclidiennes successives de a par b, alors $r_n = a \wedge b$.
En particulier :

1. $a \wedge b$ est un diviseur commun de a et b.
2. Si d divise a et b, alors d divise $a \wedge b$.
3. $d = a \wedge b \exists u, v \in \mathbb{Z}$ tel que $d = ua + vb$.
4. Si $\exists u, v \in \mathbb{Z}$ tel que $d = ua + vb$, alors $a \wedge b$ divise d.

Théorème :

Propriété caractéristique du PGCD.
Soit $(a,b) \in \mathbb{N}^{*2}$ et $d \in \mathbb{N}^*$ alors :

$d = a \wedge b \Leftrightarrow$ i) d divise a et b
ii) Pour tout autre diviseur commun d' de a et b on a : d' divise d aussi

Propriétés.

$\forall (a,b,c) \in \mathbb{N}^{*3}$ on a les propriétés suivantes

1. $a \wedge b = b \wedge a$, commutativité du PGCD.
2. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, associativité du PGCD.
3. $a \wedge b = a \Leftrightarrow a$ divise b.

Nombres premiers entre eux.

Définition :

Soit $(a,b) \in \mathbb{N}^2$, lorsque $a \wedge b = 1$ on dit que a et b sont premiers entre eux.

Théorème :

Théorème de Bezout.
Soit $(a,b) \in \mathbb{N}^2$, alors : $a \wedge b = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Théorème :
Théorème de Gauss.
Soit $a, b, c \in \mathbb{N}$ tel que a divise bc et $a \wedge b = 1$, alors a divise c.

Propriétés.

1. $ab \wedge ac = a(b \wedge c)$, distributivité du produit par rapport au pgcd.
2. Si d divise a et b on a : $\dfrac{a \wedge b}{d} = \dfrac{a}{d} \wedge \dfrac{b}{d}$.
3. Si $d = a \wedge b$ alors $\dfrac{a}{d} \wedge \dfrac{b}{d} = 1$, plus précisément $a = \alpha d, b = \beta d$ avec $\alpha \wedge \beta = 1$.
4. $a \wedge b = a \wedge c = 1 \Rightarrow a \wedge bc = 1$.
5. $a \wedge b \Leftrightarrow a^n \wedge b^m = 1$.

PPCM

Définition :
Soit $a, b \in \mathbb{N}$, l'ensemble des multiples communs de a et b dans $\mathbb{N}$ est une partie de $\mathbb{N}$ non vide (contenant ab) donc admet un plus petit élément, appelé ppcm de a et b et noté $a \vee b$.

Théorème :
Propriété caractéristique du PPCM.
Soit $(a, b) \in \mathbb{N}^{*2}$ et $m \in \mathbb{N}^*$ alors :
$d = m = a \vee b \Leftrightarrow$ i) m multiple a et b
ii) Pour tout autre multiple commun m' de a et b on a : m' multiple de m aussi

Propriété.

1. $a \vee b = b \vee a$, commutativité du PPCM.
2. $(a \vee b) \vee c = a \vee (b \vee c)$, associativité.
3. $\forall (a, b) \in \mathbb{N}^{*2}$ on a : $(a \wedge b)(a \vee b) = ab$
   En particulier : $a \vee b = ab \Leftrightarrow a \wedge b = 1$

Nombres premiers.

Définition :
On appelle nombre premier, tout nombre différent de 1, dont les seuls diviseurs dans $\mathbb{N}^*$ sont 1 et lui même. Dans le cas contraire il est dit composée.

Théorème :
Tout entier naturel supérieur à 2 admet au moins un diviseur premier.

Théorème :
L'ensemble des nombres premiers est infini.

Théorème :

Tout entier naturel n supérieur à 2 s'écrit de façon unique sous la forme :
$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, avec $p_1, p_2, \dots, p_r$ des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_r$ des entiers naturels non nuls.
Cette écriture s'appelle décomposition primaire de n.

Théorème :

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$, avec $p_1, p_2, \dots, p_r$ des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_r$ des entiers naturels éventuellement nuls, alors :
$n \wedge m = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)}$
$n \vee m = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_r^{\max(\alpha_r,\beta_r)}$

Le plus grand nombre premier.

Un nouveau nombre premier dit « de Mersenne » vient d'être découvert par un chercheur de la University of Central Missouri, aux Etats-Unis. Le nombre 274 207 281– 1 contient plus de 22 millions de chiffres. C'est 5 millions de plus que l'ancien record du nombre premier de Mersenne le plus long, découvert en janvier 2013.

Les nombres premiers sont divisibles uniquement par eux-même et par 1, comme par exemple 2,3, 5, 7, 11 et 13. La recherche du plus grand nombre premier est une quête ancienne chez les mathématiciens ; un challenge qui a le mérite de ne jamais s'épuiser, car il en existe une infinité.

Le nouveau nombre record est de ceux désignés en arithmétique comme des « nombres premiers de Mersenne », du nom de Marin Mersenne, un mathématicien français du XVIe siècle. Ces nombres peuvent s'écrire sous la forme 2n-1, n étant un nombre premier. Comme le souligne le Guardian, l'intérêt d'écrire un nombre sous cette forme est que l'on peut aisément vérifier s'il est premier ou non.

Une plateforme mondiale de recherche des nombres premiers

Le nouveau record a été découvert grâce à une plateforme, le Great Internet Mersenne Prime Search (GIMPS), qui propose à des volontaires de télécharger un logiciel de recherche de nombres premiers. Depuis sa création il y a tout juste vingt ans, ce projet a permis de dévoiler les 15 plus grands nombres premiers de Mersenne.

Le nombre aux 22 millions de chiffres a été repéré par un ordinateur en septembre, sans être remarqué dans un premier temps par le professeur Curtis Cooper, qui s'en est rendu compte lors d'un contrôle de maintenance. Le site du GIMPS précise que seule la date de la découverte par l'homme compte. Après 31 jours de vérifications par des logiciels indépendants, le nouveau record a été annoncé officiellement le 7 janvier.

Curtis Cooper a installé le logiciel du GIMPS sur les ordinateurs de son université il y a déjà plusieurs année, et comptabilise aujourd'hui son quatrième record. Interviewé par la chaîne Youtube Standupmaths, il a déclaré être « aussi heureux d'avoir découvert [son] quatrième nombre record [qu'il l'était lorsqu'il] a découvert le premier».

Trouver des nombres premiers peut rapporter gros : M. Cooper gagne une récompense de 3 000 dollars offerte par le GIMPS. Le prochain objectif sera le premier nombre premier à 100 millions de chiffres. Un prix de 150 000 dollars est promis par la Electronic Frontier Foundation à l'heureux chercheur qui le trouvera en premier. Quiconque voudrait tenter sa chance peut rejoindre l'équipe déjà conséquente des 150 000 ordinateurs connectés en permanence à la plateforme du GIMPS via le logiciel de recherche Prime95, disponible en téléchargement gratuit.