Quelques notions de théorie des nombres

Ensembles de nombres entiers.

On désigne par $\mathbb{N}$ l'ensemble des nombres naturels : {0, 1, 2, 3, ... } et par $\mathbb{N}^*$ l'ensemble des nombres entiers positifs : {1, 2, 3, 4, ... }. La notation ensembliste $a \in \mathbb{N}^*$ signifie donc que a est un nombre entier positif. L'ensemble des nombres entiers relatifs $\{0, \pm 1, \pm 2, \pm 3, \ldots\}$ est, quant à lui, est noté $\mathbb{Z}$.

Facteurs, nombres premiers

Définition 1. Soient a et b deux nombres entiers positifs. On dit que b est un facteur ou un diviseur de a s'il existe un nombre entier c tel que $a = bc$. Dans ce cas, on dit aussi que a est un multiple de b.

Exemple. Les diviseurs de 36 sont 1, 2, 3, 4, 6, 9, 12, 18 et 36.

Remarque. Tout nombre entier positif a pour diviseur 1 et lui-même.

Définition 2. Soit p un nombre entier supérieur à 1. On dit que p est premier s'il n'a pas de diviseur autre que 1 et lui-même.

Remarque. Par convention, on ne considère pas 1 comme un nombre premier. Les nombres premiers sont donc caractérisés par le fait qu'ils ont exactement deux diviseurs.

Définition 3. Deux nombres entiers positifs a et b sont dits relativement premiers si leur seul diviseur commun est 1.

Exemple. 75 et 28 sont relativement premiers mais 15 et 36 ne le sont pas (ils ont 3 comme diviseur commun).

Remarque. D'après la définition, quel que soit le nombre entier positif a, 1 et a sont relativement premiers.

La fonction phi d'Euler

Définition 4. L'indicatrice ou fonction phi d'Euler est la fonction définie sur $\mathbb{N}^*$ de la manière suivante : si $a \in \mathbb{N}^*$, alors $\varphi(a)$ est le nombre d'entiers b avec $1 \leq b \leq a$ qui sont relativement premiers avec a.

Exemple. Tous les nombres pairs et les multiples de 3 ont un diviseur commun autre que 1 avec 36. Les nombres entre 1 et 36 qui sont relativement premiers avec 36 sont donc 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31 et 35. Donc, $\varphi(36) = 12$.

Exercice. Calculer $\varphi(a)$ pour $10 \leq a \leq 20$.

Proposition 1. Si p est premier, alors $\varphi(p) = p-1$.

Preuve : Si p est premier, aucun entier b avec $1 \le b < p$ n'a de diviseur commun avec p autre que 1. Cela veut dire qu'il y a p-1 entiers entre 1 et p qui sont relativement premiers avec p.

Exemple. Donc $\varphi(11) = 10$, $\varphi(13) = 12$, $\varphi(17) = 16$ et $\varphi(19) = 18$.

Proposition 2. Si p est premier et si n est un entier positif, alors

$$\varphi(p^n) = p^{n-1}(p-1).$$

Preuve : Si p est premier, les nombres entier b avec $1 \le b \le p^n$ qui ne sont pas relativement premiers avec p sont de la forme

$$b = kp \quad (1 \le k \le p^{n-1})$$

et leur nombre est p^{n-1}. Puisqu'il y a p^n entiers entre 1 et p^n, le nombre de ceux qui sont relativement premiers avec p^n doit être

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

Exemple. Donc $\varphi(4) = 2 \cdot 1 = 2$ et $\varphi(9) = 3 \cdot 2 = 6$.

Exercice. Calculer $\varphi(8)$, $\varphi(16)$, $\varphi(27)$ et $\varphi(81)$.

Proposition 3. Si p et q sont premiers, alors

$$\varphi(pq) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1).$$

Preuve : Si p et q sont premiers, les nombres entiers b avec $1 \le b \le pq$ qui ne sont pas relativement premiers avec pq sont de la forme

$$b = kp \quad (1 \le k < q)$$

ou

$$b = kq \quad (1 \le k < p)$$

et $b = pq$ (qu'il faut éviter de compter deux fois). Leur nombre est

$$(q-1) + (p-1) + 1 = p + q - 1.$$

Puisqu'il y a pq entiers entre 1 et pq, le nombre de ceux qui sont relativement premiers avec pq doit être

$$\varphi(pq) = pq - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1).$$

Remarque. On peut monter que ce résultat se généralise pour des nombres a et b relativement premiers : $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Exercice. Utiliser ce fait pour vérifier la valeur de $\varphi(36)$.

Congruence modulo *m*

Définition 5. Soient *a* et *b* deux nombres naturels et soit *m* un nombre entier positif. On dit que *a* et *b* sont congrus modulo *m*,

$$a \equiv b \pmod{m},$$

si *a* et *b* diffèrent par un multiple de *m*.

Exemple. 27 ≡ 12 (mod 5) car 27-12 = 15 et 15 est un multiple de 5.

On peut démontrer le théorème suivant, du à Fermat :

Théorème 1a. Si *p* est premier, pour tout entier positif *a* qui n'est pas un multiple de *p*, on a

$$a^{p-1} \equiv 1 \pmod{p}.$$

Exemple. Pour $p = 5$, on a $1^4 = 1$, $2^4 = 16 = 15 + 1$, $3^4 = 81 = 80 + 1$ et $4^4 = 256 = 255 + 1$.

Le théorème 1a porte dans la littérature le nom de « petit théorème de Fermat ». À noter qu'il peut se réécrire sous la forme :

Théorème 1b. Si *p* est premier, pour tout entier positif *a* qui n'est pas un multiple de *p*, on a

$$a^{\varphi(p)} \equiv 1 \pmod{p}.$$

Ce résultat a été généralisé par Euler :

Théorème 2. Si *a* et *m* sont relativement premiers, alors

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Erratum

Oups. Vers la fin de la vidéo, M. Deguire écrit que $5^{21} \equiv 5 \pmod{21}$. Il voulait évidemment dire que $5^{21} \equiv 5 \pmod{33}$. Vous aurez certainement corrigé par vous-mêmes.

Préparé par Bernard M. de Dormale.