Congruences, arithmétique modulaire

1. Activité d'introduction

On prend un médicament toutes les 5 heures. On commence à midi.

- Donner la liste des prochains horaires auxquels il faut prendre le médicament.
- Finira-t-on par prendre le médicament à toutes les heures du jour et de la nuit ?
- Mêmes questions si on prend le médicament toutes les 3 heures.

2. La théorie

2.1. Définition

Soit n un entier supérieur ou égal à 2 et a et b deux entiers relatifs.

On dit que a et b sont congrus modulo n si a et b ont le même reste dans la division euclidienne par n. On note : $a \equiv b [n]$ ou parfois $a \equiv b \pmod{n}$

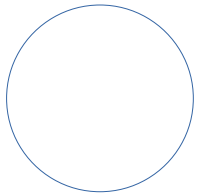
La définition est équivalente à l'une de ces phrases :

- $a-b$ est un multiple de n
- Il existe un entier relatif k tel que $a-b=kn$.

2.2. Exemples

Les deux premiers exemples sont fondamentaux.

21≡21[5] (un nombre est toujours congru à lui-même)
21≡1[5] (un nombre est toujours congru à son reste)
21≡6[5] mais aussi à 11, 16… de 5 en 5 (tjrs le même reste, seul q change)



2.3. Remarques

- La notation [n] ou (mod n) ne correspond pas à une opération :
  il ne faut pas confondre « modulo » et « modulo » !
  La confusion vient du fait que le reste de la division euclidienne de x par y est donnée dans certains langages de programmation par l'écriture x % y et se lit « x modulo y ».
- S'il n'y a pas ambiguïté sur le n, on peut omettre le « [n] ».

n≡0[2] <=> n est … ; n≡1[2] <=> n est … ; a≡0[p] <=> a est…

2.4. Deux exercices classiques

1) Montrer que 12≡166[7].

2) Donner le plus petit entier positif congru à 183 modulo 6.

2.5. Propriétés

Les propriétés sont données modulo n.

2.5.1. Symétrie : Si $a \equiv b$, alors $b \equiv a$.
2.5.2. Transitivité : Si $a \equiv b$ et $b \equiv c$, alors $a \equiv c$.
2.5.3. Règles de réduction, ou de compatibilité

Si a, a', b *et* b' sont des entiers tels que $a \equiv a'$ et $b \equiv b'$, alors on a :

$a+b \equiv a'+b'$ $a-b \equiv a'-b'$ $a \times b \equiv a' \times b'$ $a^k \equiv a'^k$ pour k entier

2.5.4. Finalement

La congruence peut être considérée comme une sorte d'égalité, mais plus faible que celle que l'on connaît. On peut dire qu'on cache dans ≡ les multiples de n.