# Corrigé de l'exercice 12, Série 18

## 1 Introduction

Combien de coefficients sont impairs dans le développement de l'expression $(x+1)^{1000}$? Pour aborder cette question, nous allons d'abords introduire un nouveau type d'anneaux (dans certains cas de corps) de nombres: les modulos. Avec cet outil, la question se simplifiera énormément. Nous allons finalement aborder les généralisations.

## 2 L'arithmétique modulaire

Nous allons introduire ici le concept du modulo. Nous savons que:

$$\forall a, b \in \mathbb{N}, \exists! q, r \in \mathbb{N} \; tq \; a = q * b + r, r < b$$

$\exists!$ signifie qu'il existe une unique solution. Il faut noter qu'il est possible que $q = 0$. Ceci est la base de la division euclidienne avec reste. on dit deux nombres entiers $x, y$ sont congruents modulo $b$ s'ils ont le même reste après division euclidienne par b. Comme la solution pour $r$ de l'équation ci-dessus est unique, cette définition a du sens. On notera ceci:

$$x \equiv y \; (mod \; b)$$

Voici deux exemples:

- $16 \equiv 1 \; (mod \; 5)$
- $15 \equiv 3 \; (mod \; 4)$

Combien de possibilités y-a-t'il pour le reste après division par b? il y en a exactement b:

$$\{0, 1, 2, ..., b-2, b-1\}$$

Subdivisons les nombres entiers en classes d'équivalence de nombres qui ont le même reste après division par b.

Voici un exemple pour illustrer:
Nous travaillons avec b=4

- $r = 0 : \{0, 4, 8, 12, 16, ...\}$
- $r = 1 : \{1, 5, 9, 13, 17, ...\}$
- $r = 2 : \{2, 6, 10, 14, 18, ...\}$
- $r = 3 : \{3, 7, 11, 15, 19, ...\}$

Nous allons maintenant introduire les modulos! Au lieu de travailler avec tout les nombres entiers, nous manipuleront les classes d'équivalence. Nous représenterons chacune par un nombre qu'elle contient, qui peut être quelconque (mais nous verrons que certains choix sont judicieux). On notera une classe contenant $a$ $[a]$, ou $[a]_b$ pour mettre l'emphase sur b. Ceci semble compliqué, mais est en fait très simple: Il faut se l'imaginer comme une horloge.

Figure 1

Quand nous additionnons deux classes, nous choisissions un nombre de chacune et les additionnons comme dans $\mathbb{N}$. Ensuite, nous regardons dans quelle classe est le résultat. Un exemple:

$$[9]_{12} + [7]_{12} \equiv [16]_{12} \equiv [4]_{12}$$

Tout comme 16:00 heures est en fait 4:00 heures! Vous voyez donc que vous utilisiez déjà les modulos dans la vie de tout les jours. La multiplication fonctionne de la même manière:

$$[5]_6 + [3]_6 \equiv [15]_6 \equiv [3]_6$$

Revenons a présent au problème initial.

# 3 Le problème

Que signifie t'il pour un nombre d'être impair? Une manière de l'exprimer et que

$$a\ impair \Leftrightarrow a \equiv 1(mod\ 2)$$

L'idée est donc de développer $(x+1)^{1000}$ modulo 2 et de compter le nombre de termes, car les coefficients pairs vaudront 0. Pour cela, il nous faut un résultat supplémentaire:

**Théorème 1.**

$$(1+x)^{2^n} \equiv (1+x^{2^n})\ (mod\ 2)$$

*preuve.* Nous allons le démontrer par récurrence. Cela signifie que nous le montrerons pour $n = 1$, puis nous montrerons que si la formule est vraie pour un nombre $n$, elle doit être vraie pour $n+1$. Pour n=1, la vérification est simple:

$$(1+x)^{2^1} = (1+x)^2 = 1+2x+x^2 \equiv 1+0*x+x^2\ (mod\ 2) \equiv 1+x^2\ (mod\ 2)$$

car $2 \equiv 0\ (mod\ 2)$. Montrons donc que la formule est vraie pour n+1 en nous basons sur le fait qu'elle est vraie pour n.

$$\begin{aligned}(1+x)^{2^{n+1}} &= (1+x)^{2^n*2} = ((1+x)^{2^n})^2 \overset{\text{hyp.}}{\equiv} (1+x^{2^n})^2\ (mod\ 2) \equiv 1+x^{2^n}+x^{2^n}+x^{2^{n+1}} \\ &\equiv 1+2*x^{2^n}+x^{2^{n+1}}\ (mod\ 2) \equiv 1+x^{2^{n+1}}\ (mod\ 2)\end{aligned}$$

□

Ecrivons donc 1000 sous forme binaire (en base 2), c'est a dire sous forme de somme de puissance de deux, ou chaque puissance est utilisée une seule fois. On a par exemple que
$11 = 1*2^3+0*2^2+1*2^1+1*2^0$. On écrira ceci $11 = 1011_2$. Les chiffres sont les coefficients des puissances. Il s'avère que cette écriture est unique, essayez de vous en convaincre par vous même. Nous utilisons la base 10 tout les jours, et les ordinateurs fonctionnent en base 2. On trouve que

$$1000 = 1*2^9+1*2^8+1*2^7+1*2^6+1*2^5+0*2^4+1*2^3+0*2^2+0*2^1+0*2^0$$

$$\Rightarrow 1000 = 1111101000_2$$

$$\Rightarrow (x+1)^{1000} = (x+1)^{2^9}*(x+1)^{2^8}*(x+1)^{2^7}*(x+1)^{2^6}*(x+1)^{2^5}*(x+1)^{2^3}$$
Par le Théorème 1, on a:

$$(x+1)^{2^9}*(x+1)^{2^8}*(x+1)^{2^7}*(x+1)^{2^6}*(x+1)^{2^5}*(x+1)^{2^3} \equiv$$
$$(x^{2^9}+1)*(x^{2^8}+1)*(x^{2^7}+1)*(x^{2^6}+1)*(x^{2^5}+1)*(x^{2^3}+1)\ (mod\ 2)$$

Combien de termes y-aura-t'il dans ce développement? On peut choisir un terme par parenthèse, et on constate qu'il y a donc $2 * 2 * 2 * 2 * 2 * 2 = 2^6 = 64$ termes. On peut facilement généraliser à $(1 + x)^n$: On calcule le développement de $n$ en base 2, puis on compte le nombre de 1. Appelons ce nombre j. Alors il y a $2^j$ termes impairs. Généralisons encore! Que signifie-t'il pour un nombre $a$ de ne pas être divisible par $k$? cela signifie que $a \not\equiv 0 \ (mod\ k)$. On peut donc adapter le théorème 1 de la manière suivante:

**Théorème 2** (Généralisation)**.**

$$Soit\ p\ un\ nombre\ premier.\ Alors (1 + x)^{p^n} \equiv (1 + x^{p^n})\ (mod\ p)$$

(*Sans preuve*)
On écrirait donc d'abords un nombre $n$ en base $p$. Voici un exemple avec $p = 5$:
$36_{10} = 121_5$. Donc

$$\begin{aligned}(1 + x)^{36} &= (1 + x)^{25} * (1 + x)^{2*5} * (1 + x) \\ &\equiv (1 + x^{25}) * (1 + x^5)^2 * (1 + x)\ (mod\ 5) \\ &\equiv (1 + x^{25}) * (1 + 2x^5 + x^{10}) * (1 + x)\ (mod\ 5)\end{aligned}$$

Il y a donc $2*3*2 = 12$ nombres non-divisibles par 5 dans le développement de $(x+1)^{36}$. Nous voyons donc que si $p > 2$, il y a des difficultés avec les "2" dans le développement en base $p$. Ce serait surmontable, mais nous n'allons pas l'aborder ici.