Le problème des bonbons

ou l'incompatibilité entre une société élitiste
et une société égalitaire

Daniel PERRIN

1. L'histoire.

L'institutrice[1] du cours moyen de Saint-Tricotin-sur-Pelote (Marne et Garonne) avait l'habitude de récompenser ses élèves en leur donnant des bonbons. Comme ses convictions l'incitaient à des positions élitistes, elle procédait de la manière suivante : elle donnait un bonbon au dernier de la classe, deux à l'avant dernier, quatre à l'antépénultième et ainsi de suite jusqu'au premier en doublant le nombre de bonbons à chaque fois[2].
Un jour qu'elle partait en stage elle confia à sa remplaçante les bonbons, qu'elle avait préparés en nombre exactement suffisant, avec mission de les répartir selon la règle ci-dessus.
Mais, la remplaçante, qui optait pour l'égalitarisme décida de donner le même nombre de bonbons à chaque élève. Pourquoi n'y parvint-elle qu'en mangeant elle-même quelques bonbons[3] ?

2. La solution.

Si n est le nombre d'élèves, le nombre de bonbons à distribuer est

$$1 + 2 + 4 + \cdots + 2^i + \cdots + 2^{n-1} = 2^n - 1.$$

Il suffit donc de montrer le lemme suivant :

Lemme.
Il n'existe pas d'entier $n \geq 2$ tel que n divise $2^n - 1$.

Démonstration. Supposons qu'un tel entier existe. Il serait nécessairement impair. Soit p son plus petit facteur premier ($p \geq 3$) et posons $n = pm$. On rappelle qu'on a $2^p \equiv 2 \pmod p$ et $2^{p-1} \equiv 1 \pmod p$ (développer $(1+1)^p$ par la formule du binôme en se souvenant que p divise $\binom{p}{i}$ pour $1 \leq i \leq p-1$).
Or, on a, par hypothèse, $2^n \equiv 1 \pmod n$, et cette congruence vaut, *a fortiori*, modulo p. On a donc $1 \equiv 2^n = (2^p)^m \equiv 2^m \pmod p$.
Mais, $p-1$ et m sont premiers entre eux car les facteurs premiers de m sont $\geq p$ et, par Bézout, il existe donc $a, b \in \mathbf{Z}$ tels que l'on ait $am + b(p-1) = 1$. Les entiers a et b sont de signes contraires, supposons par exemple $a > 0$ et $b < 0$, $b = -c$. On a alors $am = 1 + c(p-1)$ d'où $2^{am} = (2^m)^a = 2 \times 2^{c(p-1)} = 2 \times (2^{p-1})^c$. Le premier membre est congru à 1 modulo p et le second à 2, ce qui est absurde.

[1] Cette histoire est ancienne. On dirait maintenant professeur(e) des écoles.
[2] Espérons pour ses finances qu'elle n'avait pas 30 élèves !
[3] On rappelle que le rectorat ferme les classes en dessous d'un certain seuil et qu'en tous cas une classe a au moins deux élèves.