Théorème caché de Platon

Introduction

Dans le livre 5 des Lois de Platon, celui-ci remarque que $5040 = 7\,!$ est divisible par tous les entiers de $[\![1, 10]\!]$. Cet intervalle est l'ensemble des entiers plus petits que 11, le successeur de 7 dans la suite des nombres premiers. Ceci a conduit Andreas Zachariou à énoncer, sans démonstration, le théorème suivant [1] :

Théorème 1 (Théorème caché de Platon). *Soit P premier, supérieur ou égal à 5, et Q le successeur de P dans la suite des nombres premiers. Alors tous les entiers de l'intervalle $[\![1, Q-1]\!]$ divisent $P\,!$.*

La première démonstration, élémentaire en admettant le postulat de Bertrand, démontré par Tchebychev en 1850, semble remonter à 2003.

Théorème 2 (Postulat de Bertrand). *Si est un entier plus grand que 1 il existe au moins un nombre premier dans l'intervalle ouvert $]n, 2n[$.*

En 2007, Georgios Velisaris, étudiant en première année de médecine à l'université de Thessalonique a énoncé lemme suivant, et en a déduit une démonstration particulièrement simple du théorème caché de Platon.

Lemme 1. *Si $N \geq 6$ est un entier naturel, tout entier n non premier et inférieur ou égal à $2N$ divise $N\,!$.*

Démonstration: Puisque tous les entiers jusqu'à N divisent $N!$, on peut supposer $N + 1 \leq n \leq 2N$, non premier ; il s'écrit $n = ab$, avec $2 \leq a \leq b$. Puisque $a \geq 2$ et $ab = n$, a et b sont tous les deux inférieurs à $n/2$ donc à N puisque $n \leq 2N$. Puisque n n'est pas premier, le nombre k des diviseurs de n est supérieur ou égal à 3. Notons $1 = d_1 < d_2 < \cdots < d_k = n$ la suite croissante de ses diviseurs. Alors :

— Si $k > 3$, on a :

$$n = d_2 \times d_{k-1} \quad \text{avec} \quad k - 1 \geq 3.$$

1. Vardulakis et Georgios, Clive Pugh and Peter Shiu :Plato's hidden theorem on the distribution of primes. Proceedings of the European Control Conference 2007 Kos, Greece, July 2-5, 2007.

Les deux entiers d_2 et d_{k-1} sont deux facteurs distincts du produit $N\,!$. Leur produit n divise donc $N\,!$.

— Si $k = 3$, n n'a que 3 diviseurs, c'est donc le carré d'un nombre premier $n = p^2$.

1. Si $p = 2$, $n = 4$ divise $N!$ qui est un multiple de $6! = 720$.
2. Si $p = 3$, $n = 9$ divise $N!$ qui est un multiple de $6! = 720$.
3. Si $p \geq 5$, $n = p^2 \geq 5p$. Et la majoration $n \leq 2N$ donne $5p \leq 2N$ puis $N > 2p$. Il en résulte que $N!$ est un multiple de $p \times 2p$ donc un multiple de $p^2 = n$.

Démonstration du théorème caché de Platon

Si $P = 5$ son successeur Q est 7 et tous les entiers jusqu'à $Q - 1 = 6$ divisent $5! = 120$; le théorème est donc vrai dans ce cas, et on peut donc supposer $P \geq 7$.

Par le postulat de Bertrand, le successeur Q de P satisfait $Q < 2P$. L'intervalle $[P + 1, Q - 1]$ est donc contenu dans l'intervalle $[P + 1, 2P]$, et, puisque $P \geq 6$, par le lemme précédent, tous les entiers non premiers de $[P + 1, Q - 1]$ divisent $P!$, ce qui termine la démonstration car, par définition de Q, cet intervalle ne contient pas de nombre premier.
