PROPRIETES ELEMENTAIRES LIEES A LA NOTION DE NOMBRE PREMIER

Introduction

Les nombres premiers sont étudiés depuis l'Antiquité. Euclide a démontré dans ses "Eléments" *(proposition 20 du livre IX)* que « *les nombres premiers sont en plus grande quantité que toute quantité proposée de nombres premiers* ». Autrement dit, il existe une infinité de nombres premiers…

-Théorème de Dirichlet : Toute suite arithmétique (an + b), avec a et b premiers entre eux, contient une infinité de nombres premiers.

-Théorème des nombres premiers (Hadamard, De La Vallée Poussin) : Si $\pi(x)$ désigne le nombre de nombres premiers inférieurs ou égaux à x, on a $\pi(x) \approx \frac{x}{\ln(x)}$

La première preuve de ce théorème date de 1896 par Jacques Hadamard (France) et Charles de la Vallée Poussin (Belgique)

Les nombres premiers ont de nombreuses utilisations pratiques, dont la cryptographie asymétrique. Les nombres utilisés n'ont d'intérêt que s'ils comportent beaucoup de chiffres, rendant ainsi impossible dans l'état officiel actuel de la technique un craquage en temps réel...

*Dans **Z**, on suppose connues la relation de divisibilité, les notions de pgcd et ppcm, les théorèmes de Gauss et de Bézout, ainsi que la théorie des congruences. On rappelle que les propriétés de divisibilité sont vraies "à association près" et donc qu'il suffit en général de travailler dans **N**.*

1. Notion de nombre premier

• Définition : Entier naturel $p \geq 2$ dont les seuls diviseurs sont 1 et p.

• Théorème fondamental de l'arithmétique : Tout entier naturel non nul est de façon unique (à l'ordre près des facteurs) produit d'un nombre fini de nombres premiers. (En d'autres termes, Z est un anneau factoriel)
Application : calcul du PPCM, du PGCD, simplification de fractions et de racines, etc.
• Théorème d'Euclide : L'ensemble des nombres premiers est infini.

Exercice 1 : Il existe une infinité de nombres premiers de la forme 4n + 3.

2. Algorithmes et exemples

• Crible d'Eratosthène

Test de primalité : $n \geq 2$ est premier si et seulement si aucun entier a, avec $2 \leq a \leq \sqrt{n}$, ne divise n.

• Nombres de Fermat : **Si a^m+1 est premier (avec $a \geq 2$ et $m \geq 1$), alors a est pair et m est une puissance de 2.**

En particulier, on appelle **nombres de Fermat les entiers $F_n = 2^{2^n} + 1$, avec $n \geq 0$.**

Exemples : $F_0 = 3$; $F_1 = 5$; $F_2 = 17$; $F_3 = 257$; $F_4 = 65\,537$

$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297$ n'est pas premier, il est divisible par 641 *(conjecture infirmée par Leonhardt Euler en 1732).*

Les nombres de Fermat interviennent dans le problème de la construction à la règle et au compas des polygones réguliers. *(Théorème de Gauss: un polygone régulier à n côtés est C-constructible ssi n est de la forme $2^r p_1 p_2 ... p_k$ où les p_i sont des nombres premier de Fermat distincts.)*

• Nombres de Mersenne : **Si $a^m - 1$ est premier (avec $a \geq 2$ et $m \geq 2$), alors a = 2 et m est premier.** On appelle **nombres de Mersenne les entiers $Mn = 2^n - 1$, avec $n \geq 2$.**

3. Nombres premiers et congruences

• Nombres premiers et anneaux **Z**/n**Z** :

- n est premier ⇔ **Z**/n**Z** est intègre ⇔ **Z**/n**Z** est un corps.

- Si p premier : $(\overline{a} + \overline{b})^p = (\overline{a})^p + (\overline{b})^p$ dans Z/pZ

• Petit théorème de Fermat :

Si p est premier et si a n'est pas divisible par p, alors $a^{p-1} \equiv 1[p]$

• Théorème de Wilson :

Soit $p \geq 2$; p est premier si et seulement si $(p-1)! \equiv -1\ (p)$

Ex2 : Soit p premier tel que p=4k+1. Trouver n tel que p divise $n^2 + 1$. (Montrer d'abord que $(4k)! + 1 \equiv 0 \bmod(p)$)

Remarque :
*Le dernier nombre premier a été trouvé par les docteurs Curtis Cooper et Steven Boone de l'université centrale de l'Etat du Missouri (CMSU) dans le cadre du projet **Gimps** (grâce au grid computing, en français la «grille de calcul»,une technologie au nom barbare et pourtant assez simple, fondée sur l'utilisation, non pas d'un seul ordinateur, ni de quelques-uns, mais sur celle d'ordinateurs de volontaires, n'importe où dans le monde, du moment qu'ils sont reliés à Internet, pour participer à ces opérations de recherche).*
Il est composé de 9 152 052 chiffres très exactement : il s'agit de $2^{30402457} - 1$

"M(43)" est devenu, le 15 décembre 2005, le plus grand nombre premier de Mersenne jamais calculé, soit un nombre divisible uniquement par «1» et par lui-même, dont l'exposant 30402457 est également premier.

Références :

184 exercices d'arithmétique *Joachim Llorca* (Ts spécialité) ; exercices d'arithmétique *de J.Fitz-Patrick*
Encyclopédie sur Internet : Wikimemia