Cours Arithmétique et Groupes 2012-2013 – Emmanuel Breuillard

Devoir à la maison facultatif :

Le but de ce problème est de démontrer avec des moyens très rudimentaires les premiers résultats marquants sur la répartition des nombres premiers obtenus au XIX ème siècle. Nous allons démontrer:

A) Le postulat de Bertrand (Tchebychev 1850) : pour tout entier naturel $n \geq 1$ il existe un nombre premier compris entre n et $2n$ strictement.

B) Le théorème de Tchebychev (1848) : il existe des constantes $C_1, C_2 > 0$ telles que pour tout entier $n \geq 1$,

$$C_2 \frac{n}{\log n} \leq |\{1 \leq p \leq n, p \text{ premier}\}| \leq C_1 \frac{n}{\log n}$$

Dans tout ce qui suit p désigne toujours un nombre premier.

Part 1. La borne supérieure

Nous démontrons d'abord (assez rapidement) la borne supérieure dans le théorème de Tchebychev.

0) Vérifier que pour tout $n \in \mathbb{N}$, $k \mapsto C_n^k$ est croissante de $k = 0$ à $k = [n/2]$ puis décroissante ensuite ($[n/2]$ est la partie entière de $n/2$).

1) Montrer (en utilisant le lemme de Gauss) que pour tout $m \in \mathbb{N}$

$$\prod_{m+2 \leq p \leq 2m+1} p \leq C_{2m+1}^m \leq 4^m,$$

où p désigne toujours un nombre premier (i.e. le produit est effectué sur les nombres premiers seulement).

2) Montrer par récurrence sur n en utilisant la question précédente que pour tout entier $n \geq 1$ on a

$$\prod_{1 \leq p \leq n} p \leq 4^n,$$

où le membre de gauche est le produit des nombres premiers p compris entre 1 et n.

Date: Octobre 2012.

3) Déduire du 2) précédent qu'il existe une constante $C > 0$ telle que $|\{n/2 \leq p \leq n, p \text{ premier}\}| \leq C\frac{n}{\log n}$ pour tout entier $n \geq 1$, puis qu'il existe une constante $C_1 > 0$ telle que

$$|\{1 \leq p \leq n, p \text{ premier}\}| \leq C_1 \frac{n}{\log n}$$

pour tout entier $n \geq 1$.

Part 2. Décomposition en facteurs premiers de C_{2n}^n

Soit $v_p(C_{2n}^n)$ l'exposant de p dans la décomposition en facteurs premiers de C_{2n}^n. Nous allons montrer que

a) si $p > \sqrt{2n}$ alors p apparaît au plus une fois dans la décomposition de C_{2n}^n,

b) si $\frac{2n}{3} < p \leq n$ alors p ne divise pas C_{2n}^n.

c) pour tout p on a $v_p(C_{2n}^n) \leq \frac{\log 2n}{\log p}$.

0) Rappeler la formule de Legendre qui donne l'exposant de p dans la décomposition en facteurs premiers de $n!$.

1) En déduire a) et b).

2) Montrer que pour tout réel x la quantité $[2x] - 2[x]$ est égale à 0 ou à 1 ($[x]$ désigne la partie entière de x, i.e. le plus grand entier plus petit ou égal à x). Puis en déduire c).

Part 3. La borne inférieure

0) Vérifier que $\frac{4^n}{2n} \leq C_{2n}^n \leq 4^n$ pour tout $n \geq 1$ (cf. question I.0.)

1) Déduire du c) de la section précédente la borne inférieure dans le théorème de Tchebychev, i.e. qu'il existe une constante $C_2 > 0$ telle que

$$|\{1 \leq p \leq n, p \text{ premier}\}| \geq C_2 \frac{n}{\log n}$$

pour tout entier $n \geq 2$.

Part 4. Postulat de Bertrand

Le but de cet exercice est de démontrer le *Postulat de Bertrand*, conjecturé par Joseph Bertrand en 1845 et démontré peu après par le grand mathématicien russe Pafnouti Tchebychev. Il énonce que pour tout entier naturel $n \geq 1$ il existe un nombre premier compris entre n et $2n$ strictement.

On raisonne par l'absurde et on suppose qu'il existe un entier n tel que tous les entiers entre n et $2n$ soient composés.

1) En utilisant a), b) et c) de la partie II. et III.0., montrer que

$$\frac{4^n}{2n} \leq C_{2n}^n \leq (2n)^{\pi(\sqrt{2n})} 4^{\frac{2n}{3}},$$

où $\pi(x)$ désigne le nombre de nombres premiers $\leq x$.

2) En déduire que n doit être borné. Quelle borne vous donne ce raisonnement ?

3) Vérifier les cas restants (i.e. pour n plus petit que cette borne).

Remarques historiques.
A) Gauss avait conjecturé en 1792 que l'on a même l'équivalent suivant:

$$|\{1 \leq p \leq n, p \text{ premier}\}| \sim \frac{n}{\log n},$$

mais la démonstration de ce fait a résisté à de nombreux mathématiciens éminents tout au long du XIX ème siècle avant que Jacques Hadamard et Charles-Jean de la Vallée Poussin ne le démontrent en 1896 (presque en même temps et indépendamment) en utilisant des outils beaucoup plus sophistiqués d'analyse complexe et de théorie des fonctions. Ce théorème porte le nom de "théorème des nombres premiers". Le théorème de Tchebychev peut être vu comme une forme faible du théorème des nombres premiers. Il suffit amplement dans bien des applications.

B) On sait désormais que pour tout n assez grand il existe un nombre premier entre n et $n + n^{0.6}$. On conjecture (conjecture de Cramer) que si n est assez grand il existe un premier entre n et $n + C(\log n)^2$. Cependant même en supposant vraie l'hypothèse de Riemann (le problème ouvert le plus fameux des mathématiques) on sait seulement en déduire que pour tout ε il y a toujours un nombre premier entre n et $n + n^{\frac{1}{2}+\varepsilon}$ pour n assez grand. Dans l'autre direction la borne supérieure dans le Tchebychev montre qu'il y a des intervalles d'entiers sans premiers entre n et $n + c\log n$. On sait battre $\log n$, mais on n'a pas reussi a aller jusqu'a $(\log n)^2$.