Université Paul Sabatier
Licence L3 ESR 2016–2017
Arithmétique

TD 1 : Nombres premiers et fonctions arithmétiques.

Exercice 1. Montrer que dans $\mathbb{Z}[X]$, il n'existe pas d'éléments U et V tels que $\mathrm{PGCD}(X, 2) = XU + 2V$.

Exercice 2. (facultatif) Montrer que dans $\mathbb{Z}[\mathrm{i}\sqrt{5}]$, 6 et $2(1 + \mathrm{i}\sqrt{5})$ n'ont pas de pgcd. Indication : $6 = (1 + \mathrm{i}\sqrt{5})(1 - \mathrm{i}\sqrt{5})$. Montrer de même que $1 + \mathrm{i}\sqrt{5}$ et 2 ont pour pgcd 1 mais n'ont pas de ppcm.

Exercice 3. On se place dans un anneau commutatif unitaire intègre et l'on ne spécifie les pgcd et ppcm qu'"à produit près par un élément inversible de l'anneau". Démontrer que :

1) si $c \neq 0$ et si ac et bc ont un pgcd alors a et b en ont aussi un et $\mathrm{PGCD}(ac, bc) = c\ \mathrm{PGCD}(a, b)$;
2) si a et b ont un ppcm alors ac et bc en ont aussi un et $\mathrm{PPCM}(ac, bc) = c\ \mathrm{PPCM}(a, b)$;
3) si $\mathrm{PPCM}(a, b)$ existe alors $\mathrm{PGCD}(a, b)$ aussi et leur produit est égal à ab.
4) si *tous* les PGCD existent alors tous les PPCM aussi.

Exercice 4. (facultatif) Montrer que $\ln m/\ln n$ est irrationnel pour tous entiers $m, n > 1$ qui n'ont pas le même ensemble de facteurs premiers. En déduire que pour tout complexe $a \neq 0$, on a $p^a = 1$ pour au plus un nombre premier p.

Exercice 5. Soit p premier et a non divisible par p. En évaluant mod p, de deux façons différentes, le produit $a \cdot 2a \cdot 3a \cdot (p - 1)a$, redémontrer le petit théorème de Fermat.

Exercice 6. Montrer deux fois (par le calcul et par la caractérisation en termes de générateurs) que $\sum_{d|n} \varphi(d) = n$.

Exercice 7. Démontrer que l'ensemble des fonctions arithmétiques, muni de l'addition et de la convolution de Dirichlet, forme un anneau commutatif (d'unité δ_1).

Exercice 8. (facultatif)

1) Transcrire la formule d'inversion de Möbius dans le cas où les fonctions f et g, au lieu d'être à valeurs dans $(\mathbb{C}, +)$, sont à valeurs dans un groupe abélien noté multiplicativement $(G, \times)$.
2) On définit le n-ième polynôme cyclotomique Φ_n comme le polynôme unitaire dont les racines sont simples et sont les racines primitives n-ièmes de 1 dans $\mathbb{C}$ (les éléments du groupe $(\mathbb{C}^*, \times)$ dont l'ordre est exactement n). Vérifier que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
3) Déduire des deux questions précédentes un moyen de calculer Φ_n. Indication : prendre pour G le groupe des fractions rationnelles non nulles à coefficients rationnels.
4) En considérant les degrés des polynômes en jeu dans les deux questions précédentes, retrouver deux formules connues.

Exercice 9. Démontrer que la suite $(p_{n+1} - p_n)$ des écarts d'un nombre premier au suivant n'est pas majorée. Indication : poser $q = p_1 \dots p_n$ et montrer que tous les entiers de $q + 2$ à $q + p_n$ sont composés.

Exercice 10. (facultatif) Fixons n et posons $t = \log_2(p_n)$. En examinant les décompositions possibles en facteurs premiers pour tous les entiers de 1 à p_n, démontrer que $p_n \leq (t + 1)^n$. En déduire que si $n \geq 5$ alors $t < n^2$ (indication : on pourra admettre que si $x \geq 5$, $\log_2(x^2 + 1) < x$). En déduire, pour tout $n \in \mathbb{N}^*$, la majoration (grossière) $p_n \leq 2^{n^2}$.

Exercice 11.

1) Démontrer qu'il n'existe aucun polynôme P non constant à coefficients entiers dont toutes les valeurs à partir d'un certain rang soient des nombres premiers. Indication : par l'absurde, montrer qu'il existerait un $m = P(n_0) > 1$ et que tous les $P(n_0 + rm)$ seraient alors divisibles par m.
2) Démontrer que plus généralement, si $f(n) = P(n, 2^n, 3^n, 4^n, \dots, k^n)$ où P est un polynôme en k variables à coefficients entiers, et si $\lim_{n\to\infty} f(n) = \infty$, alors $f(n)$ est un nombre composé pour une infinité de valeurs de n. Indication : par l'absurde, montrer qu'il existerait un nombre premier $p = f(n_0) > k$ puis, en utilisant le petit théorème de Fermat, que tous les $f(n_0 + rp(p - 1))$ seraient alors divisibles par p.

Exercice 12. Démontrer que les formulations (1), (2) et (3) du théorème des nombres premiers sont équivalentes.

$$(1) : p_n \sim n \ln n, \quad (2) : \pi(x) \ln \pi(x) \sim x, \quad (3) : \pi(x) \sim x / \ln x.$$

Exercice 13.

1) En isolant la partie sans facteur carré dans chaque entier n, démontrer que

$$\ln\left(\sum_{n \leq x} \frac{1}{n}\right) \leq \ln 2 + \sum_{p_i \leq x} \frac{1}{p_i}.$$

2) En étudiant la série de terme général $\int_n^{n+1} (\frac{1}{n} - \frac{1}{t}) \mathrm{d}t$, démontrer que la suite $\sum_{k=1}^n \frac{1}{k} - \ln(n)$ converge (sa limite γ est appelée la constante d'Euler-Mascheroni)

Exercice 14. (facultatif)

1) Calculer $\int_0^1 \frac{\arcsin x}{\sqrt{1-x^2}} \mathrm{d}x$.
2) En appliquant la formule du binôme généralisée $(1+t)^r = \sum_{k=0}^\infty \binom{r}{k} t^k$ (pour tous réels – ou même complexes – r et t tels que $|t| < 1$), où $\binom{r}{k} := \frac{r(r-1)(r-2)\cdots(r-k+1)}{k!}$, calculer les coefficients a_k tels que $\frac{1}{\sqrt{1-t^2}} = \sum_{k=0}^\infty a_k t^{2k}$.
3) En déduire un développement en série de $\arcsin x$, pour $|x| < 1$.
4) Démontrer par récurrence (à l'aide d'une intégration par parties) que $a_k \int_0^1 \frac{x^{2k+1}}{\sqrt{1-x^2}} \mathrm{d}x = \frac{1}{2k+1}$.
5) Déduire de tout ce qui précède que $\sum_{k=0}^\infty \frac{1}{(2k+1)^2} = \frac{\pi^2}{8}$.
6) En déduire que $\zeta(2) = \frac{\pi^2}{6}$.

Exercice 15. Démontrer que $\sum_{n=1}^\infty \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$. Trouver de même une expression (qui met en jeu ζ) de $\mathrm{DG}(\mathrm{Id})$, $\mathrm{DG}(\varphi)$ et $\mathrm{DG}(\sigma_a)$.

Exercice 16.

1) Combien (en fonction de $n \in \mathbb{N}^*$) y a-t-il de couples d'entiers (p, q) tels que $1 \leq p \leq q \leq n$?
2) Montrer que parmi eux, le nombre de couples pour lesquels p et q sont premiers entre eux est égal à $\Phi(n) := \sum_{q=1}^n \varphi(q)$.
3) Montrer que $\Phi(n) = \sum_{d=1}^n \mu(d) \frac{[n/d]([n/d]+1)}{2}$.
4) En déduire que $\Phi(n) = \frac{n^2}{2} \sum_{d=1}^n \frac{\mu(d)}{d^2} + O(n \ln n)$.
5) En déduire que $\Phi(n) = \frac{n^2}{2} \sum_{d=1}^\infty \frac{\mu(d)}{d^2} + O(n \ln n)$
6) On rappelle que $\sum_{d=1}^\infty \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$. En déduire la "probabilité" (au sens : limite de la proportion, quand $n \to \infty$) pour que deux entiers ≥ 1 soient premiers entre eux.