Université Paul Sabatier
Licence L3 ESR 2017–2018
Arithmétique

TD 1 : Nombres premiers et fonctions arithmétiques.

Exercice 1. (facultatif) On se place dans un anneau commutatif unitaire intègre quelconque, et l'on ne spécifie donc les pgcd et ppcm qu'à association près, c.-à-d. à produit près par un élément inversible de l'anneau. Démontrer que si $c \neq 0$:

1) si PPCM(a, b) existe alors PGCD(a, b) aussi (pour info : la réciproque est fausse : cf. Anneau à PGCD) et leur produit est associé à ab ;
2) si *tous* les PGCD existent alors tous les PPCM aussi.
3) si PGCD(ac, bc) existe alors PGCD(a, b) existe et est associé à PGCD$(ac, bc)/c$;
4) PPCM(ac, bc) existe si et seulement si PPCM(a, b) existe, et dans ce cas : PPCM(ac, bc) est associé à c PPCM(a, b).

Exercice 2. Soient $m, n \in \mathbb{N}^*$ premiers entre eux. Démontrer que l'application $(x, y) \mapsto xy$, de l'ensemble des couples $(x, y) \in \mathbb{N}^*$ tels que $x \mid m$ et $y \mid n$ dans l'ensemble des diviseurs positifs de mn, est bijective, en explicitant la bijection réciproque.

Exercice 3. Soit p premier et a non divisible par p. Montrer que dans $\mathbb{Z}/p\mathbb{Z}$,

$$\{\overline{ka} \mid 1 \leq k \leq p-1\} = \{\overline{k} \mid 1 \leq k \leq p-1\}.$$

En déduire que $(p-1)!\, a^{p-1} \equiv (p-1)! \mod p$. En déduire le petit théorème de Fermat.

Exercice 4. (facultatif)

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 $f(n) = P(n, 2^n, 3^n, 4^n, \ldots, k^n)$ 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 5. 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 6. Soit $n \in \mathbb{N}^*$.

1) Soit $d \in \mathbb{N}^*$ un diviseur de n. On note $q = n/d$ et $G = \{\overline{0}, \overline{q}, 2\overline{q}, \ldots, (d-1)\overline{q}\} \subset \mathbb{Z}/n\mathbb{Z}$. Pour tout $\overline{r} \in \mathbb{Z}/n\mathbb{Z}$, montrer que $d\overline{r} = \overline{0} \Leftrightarrow \overline{r} \in G$, et en déduire que les éléments d'ordre d du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les générateurs du sous-groupe G.
2) En déduire que $\sum_{d|n} \varphi(d) = n$.
3) Retrouver ce résultat par calcul direct, en considérant d'abord le cas où n est une puissance d'un nombre premier, puis en utilisant que $\mathbf{1} * \varphi$ et id sont multiplicatives (pourquoi ?).

Exercice 7. Soit $(p_n)_{n\geq 1}$ la suite des nombres premiers. On va en donner deux majorations faciles, donc bien plus grossières que celle du théorème des nombres premiers.

1) En examinant l'argument d'Euclide (qui montre que la suite $(p_n)_{n\geq 1}$ des nombres premiers est infinie), montrer (par récurrence) que $p_n \leq 2^{2^{n-1}}$.
2) (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 $t < n^2$ (on pourra admettre que $\forall x \geq 5 \quad \log_2(x^2+1) < x$). En déduire, pour tout $n \in \mathbb{N}^*$: $p_n \leq 2^{n^2}$.

Exercice 8. (facultatif) On veut démontrer que la suite $(p_{n+1} - p_n)$ n'est pas majorée.

1) Soit $m \in \mathbb{N}^*$. Montrer que tous les entiers de $p_1 \ldots p_m + 2$ à $p_1 \ldots p_m + p_m$ sont composés.
2) En déduire qu'il existe $n \in \mathbb{N}^*$ tel que $p_{n+1} - p_n \geq p_m$.
3) Conclure.

Exercice 9. Démontrer que les formulations (1), (2) et (3) du théorème des nombres premiers sont équivalentes.

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

(La motivation est (1) $\Leftrightarrow$ (3) ; (2) est un intermédiaire technique.) Indication pour (2) $\Leftrightarrow$ (3) : montrer que chacun des énoncés (2) et (3) implique $\ln(\pi(x)) \sim \ln x$.

Exercice 10. Démontrer que :

$$\zeta(s)\,\mathrm{DG}(\mu)(s) = 1$$

pour tout $s \in \mathbb{C}$ de partie réelle > 1, et que (pour tout $a \in \mathbb{C}$) :

$$\mathrm{DG}(\sigma_a)(s) = \zeta(s-a)\zeta(s)$$

pour tout $s \in \mathbb{C}$ de partie réelle $> 1 + \max(\mathrm{Re}(a), 0)$.

Exercice 11. (facultatif : extrait du partiel de novembre 2016)

Pour tout entier $k \geq 1$, on définit la fonction totient de Jordan $J_k : \mathbb{N}^* \to \mathbb{N}^*$ par :

$J_k(n)$ est le nombre de k-uplets $(a_1, \ldots, a_k) \in \{1, \ldots, n\}^k$ tels que $\mathrm{pgcd}(a_1, \ldots, a_k, n) = 1$.

1) (0,5 pt) Reconnaître J_1.
2) (2 pts) En partitionnant $\{1, \ldots, n\}^k$ selon les valeurs que prend, sur cet ensemble, l'application $(x_1, \ldots, x_k) \mapsto \mathrm{pgcd}(x_1, \ldots, x_k, n)$, démontrer que (pour tout $n \in \mathbb{N}^*$)
$$n^k = \sum_{d|n} J_k(n/d).$$
3) (3 pts) En déduire que
$$J_k(n) = \sum_{d|n} (n/d)^k \mu(d)$$
(où μ désigne la fonction de Möbius) et que J_k est multiplicative.
4) (2 pts) En déduire que
$$J_k(n) = n^k \prod_{p \text{ premier}|n} \left(1 - \frac{1}{p^k}\right).$$
5) (0,5 pt) J_k est-elle complètement multiplicative ?
6) (2 pts) On rappelle que $\sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$ et $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$. Calculer
$$\sum_{n=1}^{\infty} \frac{J_k(n)}{n^s}$$
(sans préciser le domaine de convergence).