Feuille d'exercices 2

1 Fonctions arithmétiques et fonctions génératrices

Une série de Dirichlet est une série de la forme

$$F(s) = \sum_{n=1}^{\infty} \frac{\alpha_n}{n^s}$$

La variable s peut être réelle ou complexe; ici nous ne considérerons que s réel. La somme de la série $F(s)$ est appelée la fonction génératrice de α_n. La théorie des séries de Dirichlet met en jeu des questions délicates de convergence. Nous ne traiterons pas ces questions dans cette feuille et on renvoie à la feuille 6 pour quelques uns des résultats connus sur ce sujet. Pour la suite nous utiliserons simplement les faits élémentaires suivants:

(i) Si la série $\sum \alpha_n n^{-s}$ est absolument convergente pour s_0, elle est alors absolument convergente pour tout s tel que $|s| \geq |s_0|$.

(ii) Si la série $\sum \alpha_n n^{-s}$ est absolument convergente pour $s > s_0$, alors la série peut être différenciée terme à terme pour tout $s > s_0$.

(iii) Si $\sum_n \alpha_n n^{-s} = 0$ pour $s > s_0$ alors $\alpha_n = 0$ pour tout n.

(iv) Deux séries de Dirichlet absolument convergentes peuvent être multipliée suivant la règle

$$(\sum \alpha_n n^{-s})(\sum \beta_n n^{-s}) = \sum \gamma_n n^{-s}$$

avec $\gamma_n = \sum_{\substack{n_1,n_2 \\ n_1 n_2 = n}} \alpha_{n_1}\beta_{n_2}$.

(1) Soit $f : \mathbb{N} \longrightarrow \mathbb{C}$ une fonction multiplicative, i.e. $f(nm) = f(n)f(m)$ pour $(n,m) = 1$. On suppose en outre que la série $\sum_n |f(n)|n^{-s}$ est absolument convergente. Montrez l'égalité

$$\sum_n f(n)n^{-s} = \prod_p (1 + f(p)p^{-s} + f(p^2)p^{-2s} + \cdots)$$

Sous les mêmes hypothèses de convergence, si de plus on a $f(mn) = f(m)f(n)$ pour tout n, m, montrer que

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - f(p)p^{-s}}$$

En déduire que la série $\sum_{p\in\mathcal{P}} 1/p$ est divergente.

(2) Exemples:

(a) $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ converge pour $s > 1$. Nous verrons plus tard, cf. feuille 6, que $\zeta(2n) = \frac{2^{2n-1}B_n}{(2n)!}\pi^{2n}$, et que $\zeta(s)(s-1) \to_{s\to 1} 1$.

(b) Soit $\mu : \mathbb{N} \to \mathbb{C}$ définie par $\mu(1) = 1$, $\mu(n) = 0$ si n a un facteur carré et sinon $\mu(p_1 p_2 \cdots p_k) = (-1)^k$ pour $p_1, \cdots, p_k$ distincts deux à deux. Montrer que μ est multiplicative et que $\sum_{d|n} \mu(d)$ vaut 1 si $n = 1$ et 0 si $n > 1$. En déduire que

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

(c) Montrer que

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}$$

pour $s > 2$ et où ϕ est l'indicatrice d'Euler.

(d) Montrer que

$$\zeta^2(s) = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}$$

pour $s > 1$ et où $d(n)$ est le nombre de diviseur de n en incluant 1 et n.

(e) Montrer que

$$\zeta(s)\zeta(s-k) = \sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s}$$

pour $s > 2$ et où $\sigma_k(n)$ est la somme des puissances k-ième des diviseur de n.

(3) Formule d'inversion de Möbius: pour f une fonction multiplicative soit $g(n) = \sum_{d|n} f(d)$. Prouver la formule d'inversion de Möbius

$$f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d})$$

et donner en une interprétation avec les séries génératrices.

Réciproquement si $g : \mathbb{N}^* \to \mathbb{R}$ est telle que $f(n) = \sum_{d|n} \mu(\frac{n}{d})g(d)$ pour tout n, montrer que $g(n) = \sum_{d|n} f(d)$.

(4) D'autres exemples:

(a) Soit $\Lambda(n) = \log p$ si $n = p^m$ et 0 sinon. Montrer que

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum \Lambda(n)n^{-s}$$

pour $s > 1$. En déduire que

$$\Lambda(n) = \sum_{d|n} \mu(\frac{n}{d}) \log d \qquad \log n = \sum_{d|n} \Lambda(d)$$

(b) Soit $d_k(n)$ le nombre de façons d'exprimer n comme le produit de k facteurs positifs (parmi ceux-ci un nombre quelconque peuvent être égaux à 1). Montrer que pour $s > 1$:

$$\zeta^k(s) = \sum \frac{d_k(n)}{n^s}$$

(c) Soit $l(n) = (-1)^\rho$ où ρ est le nombre de facteurs premiers de n, où les facteurs multiples sont comptés avec multiplicité. Montrer que pour $s > 1$:

$$\frac{\zeta(2s)}{\zeta(s)} = \sum_{n=1}^{\infty} l(n)n^{-s}$$

(d) Montrer que

$$\frac{\zeta(s)}{\zeta(2s)} = \sum |\mu(n)|n^{-s}$$

puis que pour $s > 1$

$$\frac{\zeta(s)}{\zeta(ks)} = \sum q_k(n)n^{-s}$$

où $q_k(n) = 0$ ou 1 suivant que n a ou n'a pas de puissance k-ième comme facteur.

2 Nombres de solutions d'équations polynomiales dans $\mathbb{F}_q$

On considère dans la suite un corps fini $\mathbb{F}_q$ de caractéristique p avec $q = p^r$.

(1) Calculer pour tout $k \geq 0$, $S_k = \sum_{x \in \mathbb{F}_q} x^k$.

(2) **Théorème de Chevalley-Warning**:

(i) Soit $P \in \mathbb{F}_q[X_1, \cdots, X_n]$ un polynôme en n variables de degré total strictement inférieur à n. En considérant le polynôme $Q = 1 - P^{q-1}$ montrer que

$$\text{card}\{x \in \mathbb{F}_q^n \ / \ P(x) = 0\} \equiv 0 \mod p$$

(ii) Soient $P_1, \cdots, P_s \in \mathbb{F}_q[X_1, \ldots, X_n]$ de degré respectifs $d_1, \cdots, d_s$ tels que $d_1 + \cdots + d_s < n$. Montrer que

$$\text{card}\{x \in \mathbb{F}_q^n \ / \ P_1(x) = \cdots = P_s(x) = 0\} \equiv 0 \mod p$$

En particulier si les P_i sont homogènes, ils possèdent une racine commune non triviale.

(3) **Formes quadratiques non dégénérées: DEVOIR A RENDRE** On suppose ici $p \neq 2$ et on considère une forme quadratique Q sur $\mathbb{F}_q$ en n variables non dégénérée.

(i) Montrer que quitte à effectuer un changement de base on peut se ramener à $Q'(y) = a_1 y_1^2 + \cdots + a_n y_n^2$ avec $\left(\frac{D_Q}{p}\right) = \left(\frac{D_{Q'}}{p}\right)$ où D_Q est le discriminant de Q.

(ii) On introduit les sommes de Gauss

$$\tau(a) = \sum_{x=0}^{p-1} \exp(\frac{2i\pi a x^2}{p})$$

Montrer que $\tau(a) = (\frac{a}{p})\tau(1)$ puis que $\tau(a)$ est la somme de Gauss introduite dans le cours, i.e. $\sum_{x \in \mathbb{F}_p} (\frac{x}{p}) \exp(\frac{2i\pi a x}{p})$.

(iii) Soit N_p le nombre de solutions dans $\mathbb{F}_p^n$ de $Q(x) = 0$. En écrivant

$$pN_p = \sum_{a=0}^{p-1} \sum_{x \in \mathbb{F}_p} \exp(\frac{2i\pi Q(x)}{p})$$

montrer que $N_p = p^{n-1} + \epsilon(p-1)p^{\frac{n}{2}-1}$ avec

$$\epsilon = \begin{cases} 0 \text{ si } n \equiv 1 \mod 2 \\ \left(\frac{(-1)^{n/2} D_Q}{p}\right) \text{ si } n \equiv 0 \mod 2 \end{cases}$$

(iv) Soit désormais pour $m \geq 2$

$$N_{p^m} = \text{card}\{x \mod p^m \ / \ Q(x) \equiv 0 \mod p^m \text{ et } x \not\equiv 0 \mod p\}$$

Montrer que $N_{p^m} = p^{(m-1)(n-1)} N_p$.

(v) Comment calculer le nombre de solutions modulo N de l'équation $Q(x) \equiv 0 \mod N$?

3 Notions élémentaires de complexité

On utilise la notation $O(f(n))$ pour une fonction $\leq Cf(n)$ pour une constante C; par ailleurs les constantes apparaissant n'ayant d'un point de vue théorique, aucune importance, seront négligées.

Soit n un entier que en base b: $n = a_0 + a_1 b + \cdots + a_r b^r$ avec $0 \leq a_i < b$ et $a_r \neq 0$. On considérera une opération sur les r chiffres de n comme une unique opération, ou encore comme une opération nécessitant $O(1)$ temps machine. On appelle complexité du nombre n le nombre de chiffres nécessaires pour le décrire, i.e. r tel que $b^r \leq n < b^{r+1}$ soit

$$r \leq \frac{\log n}{\log b} \leq r + 1$$

donc proportionnelle à $\log n$. Il est clair que la manipulation de nombres **quelconques** de taille n nécessite au moins $\log n$ opérations élémentaires; on considère tant du point de vue pratique que théorique, qu'un "bon" algorithme est un algorithme polynomial c'est à dire utilisant $O(\log n)^k)$ opérations élémentaires. Inversement un algorithme "exponentiel", i.e. nécessitant un nombre d'opérations élémentaires supérieur à $\exp(k \log n) = n^k$ est impraticable pour n grand.
Exemples: on dispose de "bons" algorithme pour l'addition, la multiplication, la division euclidienne, l'exponentiation de deux nombres entiers (resp. de $\mathbb{Z}/N\mathbb{Z}$, resp du corps fini $\mathbb{F}_q$).

4 La méthode de cryptographie RSA

(1) Soit p et q deux nombres premiers distincts impairs et $n = pq$. Soit $0 \leq c < n$ un entier premier avec $\phi(n)$. Étant donné un message en clair $0 \leq x < n$, $x \in \mathbb{N}$, on calcule $y = x^c$ qui représente le message codé.

   (i) Expliquez comment décrypter le message. Que se passe-t-il si x n'est pas premier avec n?

   (ii) On suppose maintenant que p et q sont fortement pseudo-premier pour r bases choisies au hasard. Que peut-on dire du système cryptographique précédent.

(2) Montrer que si on prend p, q tels que $|p - q|$ est petit par rapport à p et q, il est alors aisé de factoriser pq.

(3) On suppose que tous les facteurs premiers de $p - 1$ sont plus petits que C avec C très petit par rapport à p. Montrer en étudiant $(a^s - 1, pq)$ pour $s \in S = \{p_1^{k_1} \cdots p_r^{k_r} \leq N\}$ où les p_i sont les premiers inférieurs à C, que l'on peut factoriser rapidement N.

   Remarque: Il faut bien entendu éviter que l'exposant secret $d = c^{-1}$ soit trop petit. On peut en fait montrer qu'il faut éviter $d \leq N^{1/4}$!

5 Algorithmes de factorisation

Soit N un entier grand que l'on essaie de factoriser.

(1) *Algorithme ρ de Pollard* On choisit a_0 entre 1 et N et on considère la suite $a_{i+1} = f(a_i)$ avec $f(a) = a^2 + 1 \mod N$. On suppose que la suite des a_i modulo p est suffisamment aléatoire, ce qui est assez bien vérifié par l'expérience et la pratique.

   (i) Montrer que la probabilité pour que r nombres pris au hasard modulo p soient tous distincts est

$$P_r = (1 - \frac{1}{p})(1 - \frac{2}{p}) \cdots (1 - \frac{r-1}{p}) \leq \exp(-\frac{r(r-1)}{2p})$$

   (ii) Prenons r de l'ordre de $\sqrt{p}$ et disons $r > 2\sqrt{p}$. En déduire que $P_r < 1/2$. On a ainsi une bonne chance qu'il existe $1 < i < j < r$ tels que $a_i \equiv a_j \mod p$ ce qui implique $a_{i+m} \equiv a_{j+m} \mod p$ pour tout $m \geq 0$. Ainsi pour $m = j - 2i$ et $k = j - i$ on aura $a_k \equiv a_{2k} \mod p$.
   Donner alors un algorithme qui avec une bonne probabilité donne une factorisation de N en temps $O(\sqrt[4]{N})$.

(2) On choisit a proche de $\sqrt{N}$ au hasard et on réduit a^2 modulo N en prenant le représentation dans $[-N/2, N/2]$ et on regarde si on peut le factoriser avec des petits facteurs premiers. Une fois que l'on a obtenu quelques a_i, b_j on essaie de construire une égalité du type

$$a^2 = \prod_i a_i^2 \equiv \prod_j b_j = b^2 \mod N$$

Expliquer pourquoi on a alors une chance sur deux en étudiant $(a - b \wedge N)$ et $(a + b \wedge N)$ d'obtenir une factorisation non triviale de N.

6 Test de primalité

(1) cf. le critère de Lucas et de Pépin dans la feuille 1.

(2) cf. le critère de Rabin-Miller dans la feuille 1.

(3) En juillet 2002, Agrawal-Kayal-Saxena ont donné un test de primalité en temps polynomial.

(i) Soient a et N deux entiers tels que $a \wedge N = 1$. Montrer que les conditions suivantes sont équivalentes:
- l'entier N est premier;
- on a $(X - a)^N \equiv X^N - a \mod N$ dans l'anneau $\mathbb{Z}[X]$.

(ii) Le problème avec le critère précédent est qu'il requiert le calcul de N coefficients. Montrer que si N est premier et si $h \in \mathbb{Z}[X]$ est un polynôme de degré r alors

$$(X - a)^N \equiv X^N - a \mod (N, h(X))$$

et remarquer que si $r = O((\log N)^k)$ alors le test est polynomial.
Remarque: Le problème est alors de choisir les paires $(a, h(X))$ afin de détecter la non primalité. La solution AKS est $h(X) = X^r - 1$ avec r très bien choisi, en particulier $r = O((\log N)^k)$ et de montrer qu'il suffit alors de tester les $a \in [1, L]$ avec $L = O(\sqrt{r}N)$ pour s'assurer que N est premier ou une puissance d'un nombre premier ce qui n'est pas gênant.