

Correction de l'examen

Sauf indication contraire :

- k, ℓ, m, n, r et d sont des nombres naturels non nuls ;
- p et q sont des nombres premiers.

Exercice 1. Le but de cet exercice est de démontrer le Théorème de Dirichlet : pour tout $m \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ tels que $\text{pgcd}(a, m) = 1$ il existe une infinité des premiers p qui vérifient $p \equiv a \pmod{m}$.

Dans cet exercice vous êtes autorisés d'utiliser les résultats de la théorie des caractères des groupes abéliens finis, ainsi que de la théorie analytique des séries de Dirichlet sans les justifier. Mais vous êtes obligés d'énoncer précisément les résultats que vous utilisez. Les références comme « d'après un théorème du cours » etc. ne sont pas acceptés.

(a) Rappeler la définition d'un caractère de Dirichlet mod m , d'un caractère (non) principal. Quel est le nombre des caractères de Dirichlet mod m ?

(b) Montrer qu'il n'existe qu'un seul caractère non principal mod 6. Soit χ ce caractère. Déterminer $\chi(7)$, $\chi(8)$, $\chi(11)$.

(c) Existe-t-il un caractère χ de Dirichlet mod 12

- qui vérifie $\chi(5) = i$?
- qui vérifie $\chi(5) = -1$?
- qui vérifie $\chi(5) = \chi(7) = -1$?

Si un tel χ existe, est-il déterminé uniquement ?

(d) Existe-t-il un caractère χ de Dirichlet mod 9

- qui vérifie $\chi(5) = \frac{1+\sqrt{-3}}{2}$?
- qui vérifie $\chi(5) = -1$?
- qui vérifie $\chi(5) = \chi(7) = -1$?

Si un tel χ existe, est-il déterminé uniquement ?

(e) Démontrer que la fonction ζ de Riemann s'étend vers une fonction méromorphe sur le demi plan droit $\text{Re } s > 0$ et déterminer ses pôles.

(f) Rappeler la définition de la fonction L de Dirichlet associée à un caractère χ de Dirichlet mod m et la formule du produit d'Euler pour $L(s, \chi)$. Exprimer $L(s, 1)$ en termes de la fonction ζ . Décrire le comportement analytique de $L(s, \chi)$ sur le demi plan droit en fonction de χ .

Dans la suite on pose $Z_m(s) = \prod_{\chi} L(s, \chi)$, où χ parcourt les caractères de Dirichlet mod m .

(g) Soit G un groupe abélien fini et $g \in G$. Énoncer (sans démonstration) le lemme sur le produit $\prod_{\chi \in \hat{G}} (1 - \chi(g)T)$. En déduire le produit eulérien pour la fonction $Z_m(s)$. Montrer que $Z_m(s)$ se développe en série de Dirichlet avec des coefficients non négatifs.

(h) Montrer que les coefficients de la série de Dirichlet pour $Z_m(s)$ sont supérieurs ou égaux à ceux de la série

$$\sum_{\text{pgcd}(m,n)=1} \frac{1}{n^{\varphi(m)s}}$$

Quelle est l'abscisse de convergence de cette dernière série ? (Justifier votre réponse.) En déduire une minoration pour l'abscisse de convergence de la série pour $Z_m(s)$.

(i) Montrer que $L(1, \chi) \neq 0$ pour $\chi \neq 1$.

(j) En déduire que

$$\sum_p \frac{\chi(p)}{p^s} = \begin{cases} \log \frac{1}{s-1} + O(1) & \text{si } \chi = 1, \\ O(1) & \text{si } \chi \neq 1 \end{cases} \quad (\text{Re } s > 1, \quad s \rightarrow 1).$$

(k) Montrer que pour tout $a \in \mathbb{Z}$ premier avec m et pour tout $x \in \mathbb{Z}$ on a

$$\sum_{\chi} \bar{\chi}(a)\chi(x) = \begin{cases} \varphi(m) & \text{si } x \equiv a \pmod{m}, \\ 0 & \text{si } x \not\equiv a \pmod{m}, \end{cases} \quad (1)$$

où χ parcourt les caractères de Dirichlet mod m . (Vous pouvez utiliser la propriété analogue des caractères des groupes abéliens finis.)

(l) Montrer que pour tout $a \in \mathbb{Z}$ premier avec m

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} = \frac{1}{\varphi(m)} \log \frac{1}{s-1} + O(1) \quad (\text{Re } s > 1, \quad s \rightarrow 1). \quad (2)$$

En déduire l'infinité des premiers p qui vérifient $p \equiv a \pmod{m}$.

Solutions (a) Soit χ un caractère du groupe multiplicatif $(\mathbb{Z}/m\mathbb{Z})^\times$. On étend χ sur $\mathbb{Z}/m\mathbb{Z}$ en posant $\chi(x) = 0$ pour $x \in \mathbb{Z}/m\mathbb{Z} \setminus (\mathbb{Z}/m\mathbb{Z})^\times$. On obtient une fonction sur $\mathbb{Z}/m\mathbb{Z}$, qui définit une fonction m -périodique sur \mathbb{Z} ; cette fonction s'appelle *le caractère de Dirichlet mod m , associé à χ* . Par abus de notation, il est aussi noté χ . Le caractère de Dirichlet associé au caractère (non) principal de $(\mathbb{Z}/m\mathbb{Z})^\times$ s'appelle *caractère de Dirichlet (non) principal*.

Le groupe des caractères de Dirichlet mod m est isomorphe au groupe dual de $(\mathbb{Z}/m\mathbb{Z})^\times$ qui est isomorphe à $(\mathbb{Z}/m\mathbb{Z})^\times$. En particulier, le nombre de caractères de Dirichlet est $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$.

(b) Puisque $\varphi(6) = 2$, il n'existe qu'un seul caractère non principal mod 6. Il est d'ordre 2, donc ne prend que les valeurs ± 1 . Puisque $7 \equiv 1 \pmod{6}$, on a $\chi(7) = 1$. Puisque -1 engendre $(\mathbb{Z}/6\mathbb{Z})^\times$, on a $\chi(-1) = -1$ et donc $\chi(11) = -1$. Puisque $\text{pgcd}(8, 6) > 1$, on a $\chi(8) = 0$.

(c) Le groupe des caractères de Dirichlet mod 12 est isomorphe à

$$(\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

En particulier, tout caractère χ de Dirichlet mod 12 vérifie $\chi^2 = 1$. Ceci implique que $\chi(5) = \pm 1$, et $\chi(5) = i$ est impossible.

En revanche, il existe 2 caractères vérifiant $\chi(5) = -1$, et un seul caractère vérifiant $\chi(5) = \chi(7) = -1$, voir Tab. 1 :

χ	$\chi(1)$	$\chi(5)$	$\chi(7)$	$\chi(11)$
1	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	-1	-1	1
$\chi_1\chi_2$	1	1	-1	-1

TAB. 1 – Caractères de Dirichlet mod 12

(d) Le groupe $(\mathbb{Z}/9\mathbb{Z})^\times$ est cyclique d'ordre 6 engendré par 5. Ceci implique que pour toute racine 6-ième de unité ζ il existe un seul caractère de Dirichlet mod 9 qui vérifie $\chi(5) = \zeta$. En particulier, il existe un seul caractère de Dirichlet mod 9 qui vérifie $\chi(5) = \frac{1+\sqrt{-3}}{2}$, ainsi qu'un seul caractère de Dirichlet mod 9 qui vérifie $\chi(5) = -1$.

En revanche, si $\chi(5) = -1$ alors $\chi(7) = \chi(5^2) = \chi(5)^2 = 1$; il n'existe donc pas de caractère qui vérifie $\chi(5) = \chi(7) = -1$.

(e) Montrons que pour $\text{Re } s > 1$ on a

$$\zeta(s) = \frac{1}{s-1} + \psi(s), \tag{3}$$

où ψ est holomorphe sur le demi plan $\text{Re } s > 0$. Alors la partie droite de (3) donne le prolongement désiré de ζ .

Pour montrer (3), écrivons, pour $\text{Re } s > 1$,

$$\zeta(s) = \int_1^\infty \frac{dx}{x^s} + \sum_{n=1}^\infty \left(\frac{1}{n^s} - \int_n^{n+1} \frac{dx}{x^s} \right) = \frac{1}{s-1} + \sum_{n=1}^\infty \psi_n(s),$$

les fonctions $\psi_n(s)$ étant holomorphe sur \mathbb{C} et vérifiant

$$|\psi_n(s)| = \left| \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{x^s} \right) dx \right| \leq \sup_{n \leq x \leq n+1} \left| \frac{1}{n^s} - \frac{1}{x^s} \right| = \frac{1}{|s|} \sup_{n \leq x \leq n+1} \left| \int_n^x \frac{dt}{t^{s+1}} \right| \leq \frac{1}{|s|} \int_n^{n+1} \frac{dt}{t^{\sigma+1}} \leq \frac{1}{|s|} \frac{1}{n^{\sigma+1}},$$

où on pose $\sigma = \text{Re } s$. Ceci signifie que la série $\sum_{n=1}^\infty \psi_n(s)$ est majorée par $\frac{1}{|s|} \sum_{n=1}^\infty \frac{1}{n^{\sigma+1}}$, et donc converge absolument sur le demi plan $\text{Re } s > 0$, sa somme étant une fonction holomorphe sur ce demi plan.

(f) On définit $L(s, \chi) = \sum_{n=1}^\infty \frac{\chi(n)}{n^s}$ pour $\text{Re } s > 1$. Puisque χ est totalement multiplicatif, on a

$$L(s, \chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \quad (\text{Re } s > 1). \tag{4}$$

En particulier, pour $\chi = 1$ on a $\chi(p) = 0$ si $p|m$ et $\chi(p) = 1$ sinon, ce qui signifie que

$$L(s, 1) = \zeta(s) \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{p^s}\right).$$

Ceci implique que $L(s, 1)$ se prolonge analytiquement vers une fonction méromorphe sur le demi plan $\text{Re } s > 0$, avec un seul pôle en $s = 1$ qui est simple.

Pour $\chi \neq 1$ on a $\chi(1) + \dots + \chi(m) = 0$. En écrivant $n = mb + r$ avec $0 \leq r \leq m - 1$, on trouve que

$$|\chi(1) + \dots + \chi(n)| = |\chi(mb + 1) + \dots + \chi(mb + r)| \leq r \leq m - 1.$$

Or la série de Dirichlet $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ avec les sommes $|a_1 + \dots + a_n|$ bornées converge pour $\text{Re } s > 0$. Ceci signifie que pour $\chi \neq 1$ la fonction $L(s, \chi)$ est holomorphe sur le demi plan $\text{Re } s > 0$.

(g) On a $\prod_{\chi \in \hat{G}} (1 - \chi(g)T) = (1 - t^r)^{\frac{|G|}{r}}$, où r est l'ordre de g . En utilisant ceci avec $G = (\mathbb{Z}/m\mathbb{Z})^\times$, $g = p$ et $T = \frac{1}{p^s}$, on obtient, pour $p \nmid m$

$$\prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right) = \left(1 - \frac{1}{p^{r_p s}}\right)^{\frac{\varphi(m)}{r_p}},$$

où χ parcourt les caractères de Dirichlet mod m et r_p est l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^\times$. Puisque le produit eulérien (4) converge absolument pour $\text{Re } s > 1$, on a

$$Z_m(s) = \prod_{\chi} \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} = \prod_{\chi} \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} = \prod_{p \nmid m} \left(1 - \frac{1}{p^{r_p s}}\right)^{-\frac{\varphi(m)}{r_p}} = \prod_{p \nmid m} \left(1 + \frac{1}{p^{r_p s}} + \frac{1}{p^{2r_p s}} + \dots\right)^{\frac{\varphi(m)}{r_p}}.$$

On voit que $Z_m(s)$ est un produit (infini) de séries de Dirichlet à coefficients non négatifs. Donc elle est lui même une série de Dirichlet avec des coefficients non négatifs.

(h) Soient $F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ et $G(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$ des séries de Dirichlet à coefficients non négatifs. On dira que F domine G si $a_n \geq b_n$ pour $n \in \mathbb{N}^*$. La relation de dominance est préservée par les opérations d'addition et de multiplication des séries de Dirichlet.

La série

$$\left(1 + \frac{1}{p^{r_p s}} + \frac{1}{p^{2r_p s}} + \dots\right)^{\frac{\varphi(m)}{r_p}}$$

domine la série

$$1 + \frac{1}{p^{\varphi(m)s}} + \frac{1}{p^{2\varphi(m)s}} + \dots$$

Ceci implique que $Z_m(s)$ domine la série

$$\prod_{p \nmid m} \left(1 + \frac{1}{p^{r_p s}} + \frac{1}{p^{2r_p s}} + \dots\right) = \sum_{\text{pgcd}(m,n)=1} \frac{1}{n^{\varphi(m)s}}.$$

Puisque la série $\sum_{n \in a+m\mathbb{N}} n^{-\theta}$ (où n parcourt la suite arithmétique $a, a+m, a+2m, \dots$ avec $a > 0$) converge pour $\theta > 1$ et diverge pour $\theta \leq 1$, l'abscisse de convergence de la série $\sum_{\text{pgcd}(m,n)=1} n^{-\varphi(m)s}$ est $1/\varphi(m)$. Ceci implique que $\sigma_0(Z_m) \geq 1/\varphi(m)$. En particulier, $\sigma_0(Z_m) > 0$.

(i) Si $L(1, \chi) = 0$ pour un certain $\chi \neq 1$, le produit $Z_m(s) = \prod_{\chi} L(s, \chi)$ serait régulier sur le demi plan droit $\text{Re } s > 0$: le pôle simple de $L(s, 1)$ serait éliminé par le zéro de $L(s, \chi)$. Mais Z_m est la somme d'une série de Dirichlet à coefficients non négatifs, et ne peut donc pas être régulière en son abscisse de convergence σ_0 . Puisque $\sigma_0 > 0$, nous arrivons à une contradiction.

(j) D'après les question (f) et (i), on a

$$\log L(s, \chi) = \begin{cases} \log \frac{1}{s-1} + O(1) & \text{si } \chi = 1, \\ O(1) & \text{si } \chi \neq 1 \end{cases} \quad (s \rightarrow 1). \quad (5)$$

D'autre part, le produit eulérien implique que pour $\text{Re } s = \sigma > 1$

$$\log L(s, \chi) = - \sum_p \log \left(1 - \frac{\chi(p)}{p^s} \right) = \sum_p \frac{\chi(p)}{p^s} + O \left(\sum_p \frac{1}{p^{2\sigma}} \right) = \sum_p \frac{\chi(p)}{p^s} + O \left(\sum_n \frac{1}{n^2} \right) = \sum_p \frac{\chi(p)}{p^s} + O(1) \quad (6)$$

(rappelons que $-\log(1-z) = z + O(|z|^2)$ quand $z \rightarrow 0$). La combinaison de (5) et (6) implique le résultat.

(k) Si G est un groupe abélien fini et $a \in G$ alors

$$\sum_{\chi \in \hat{G}} \bar{\chi}(a) \chi(x) = \sum_{\chi \in \hat{G}} \chi(a^{-1}x) = \begin{cases} |G| & \text{si } x = a, \\ 0 & \text{si } x \neq a. \end{cases}$$

En l'utilisant avec $G = (\mathbb{Z}/m\mathbb{Z})^\times$ on obtient (1) dans le cas $\text{pgcd}(x, m) = 1$. Et si $\text{pgcd}(x, m) > 1$ alors $\chi(x) = 0$ pour tous χ et (1) est évident.

(l) D'après la question précédente on a

$$\sum_{\chi} \bar{\chi}(a) \sum_p \frac{\chi(p)}{p^s} = \sum_p \frac{1}{p^s} \sum_{\chi} \bar{\chi}(a) \chi(p) = \varphi(m) \sum_{p \equiv a \pmod{m}} \frac{1}{p^s} \quad (\text{Re } s > 1). \quad (7)$$

D'autre part, la question (j) implique que la partie gauche de (7) est $\log \frac{1}{s-1} + O(1)$. D'où (2).

Si l'ensemble des premiers vérifiant $p \equiv a \pmod{m}$ était fini, la somme $\sum_{p \equiv a \pmod{m}} p^{-s}$ serait bornée sur le demi plan $\text{Re } s > 0$, ce qui contredit (2).

Exercice 2. On note par $\omega(n)$ le nombre de diviseurs premiers distincts de n . Le but de cet exercice est de démontrer que pour « presque tout » naturel n on a $\omega(n)/\log \log n \approx 1$ (Hardy-Ramanujan).

(a) Rappeler (sans démonstration) l'asymptotique pour $\sum_{p \leq x} \frac{1}{p}$.

En déduire que

$$\sum_{\substack{(p,q), p \neq q \\ pq \leq x}} \frac{1}{pq} = (\log \log x)^2 + O(\log \log x), \quad (8)$$

où (p, q) parcourt les couples des premiers qui vérifient $p \neq q$ et $pq \leq x$.

(b) Démontrer que

$$\sum_{n \leq x} \omega(n) = \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor. \quad (9)$$

En déduire que

$$\sum_{n \leq x} \omega(n) = x \log \log x + O(x)$$

(c) Démontrer que

$$\omega(n)^2 = \sum_{\substack{(p,q), p \neq q \\ pq | n}} 1 + \omega(n). \quad (10)$$

En déduire que

$$\sum_{n \leq x} \omega(n)^2 = \sum_{\substack{(p,q), p \neq q \\ pq \leq x}} \left\lfloor \frac{x}{pq} \right\rfloor + \sum_{n \leq x} \omega(n),$$

et que

$$\sum_{n \leq x} \omega(n)^2 = x(\log \log x)^2 + O(x \log \log x).$$

(d) Utiliser les questions précédentes pour montrer que

$$\sum_{3 \leq n \leq x} (\omega(n) - \log \log n)^2 = O(x \log \log x). \quad (11)$$

(e) Soit $\varepsilon > 0$. On dit qu'un naturel $n \geq 3$ est ε -irrégulier si

$$|\omega(n) - \log \log n| > (\log \log n)^{1/2+\varepsilon}.$$

Montrer que le nombre de naturels $n \leq x$ qui sont ε -irréguliers est $O(x(\log \log x)^{-2\varepsilon})$. En particulier, c'est $o(x)$.

Solutions (a) On a $\sum_{p \leq x} \frac{1}{p} = \log \log x + O(1)$. Posons

$$S = \sum_{\substack{(p,q), p \neq q \\ pq \leq x}} \frac{1}{pq}.$$

On a la majoration évidente

$$S \leq \sum_{p,q \leq x} \frac{1}{pq} = \left(\sum_{p \leq x} \frac{1}{p} \right)^2 = (\log \log x + O(1))^2 = (\log \log x)^2 + O(\log \log x).$$

Puis, si $p, q \leq \sqrt{x}$ alors $pq \leq x$, ce qui implique la minoration

$$S \geq \sum_{\substack{p,q \leq \sqrt{x} \\ p \neq q}} \frac{1}{pq} = \left(\sum_{p \leq \sqrt{x}} \frac{1}{p} \right)^2 - \sum_{p \leq \sqrt{x}} \frac{1}{p^2}.$$

Puisque $\sum_{p \leq \sqrt{x}} \frac{1}{p} = \log \log \sqrt{x} + O(1) = \log \log x + O(1)$ et $\sum_{p \leq \sqrt{x}} \frac{1}{p^2} = O(1)$, on obtient la minoration $S \geq (\log \log x)^2 + O(\log \log x)$.

(b) On a

$$\sum_{n \leq x} \omega(n) = \sum_{n \leq x} \sum_{p|n} 1 = \sum_{p \leq x} \sum_{m \leq \frac{x}{p}} 1 = \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor.$$

La dernière somme est

$$\sum_{p \leq x} \frac{x}{p} + O(x) = x(\log \log x + O(1)) + O(x) = x \log \log x + O(x).$$

(c) On a

$$\omega(n)^2 = \left(\sum_{p|n} 1 \right)^2 = \sum_{\substack{p|n \\ q|n}} 1 = \sum_{\substack{p|n, q|n \\ p \neq q}} 1 + \sum_{p|n} 1 = \sum_{\substack{(p,q), p \neq q \\ pq|n}} 1 + \omega(n).$$

Puisque

$$\sum_{n \leq x} \sum_{\substack{(p,q), p \neq q \\ pq|n}} 1 = \sum_{\substack{(p,q), p \neq q \\ pq \leq x}} \sum_{m \leq \frac{x}{pq}} 1 = \sum_{\substack{(p,q), p \neq q \\ pq \leq x}} \left\lfloor \frac{x}{pq} \right\rfloor,$$

on a (10). D'après (8) et (9), la partie droite de (10) est

$$\sum_{\substack{(p,q), p \neq q \\ pq \leq x}} \frac{x}{pq} + x \log \log x + O(x) = x(\log \log x)^2 + O(x \log \log x).$$

(d) On a

$$\sum_{3 \leq n \leq x} (\omega(n) - \log \log n)^2 = \sum_{3 \leq n \leq x} \omega(n)^2 - 2 \sum_{3 \leq n \leq x} \omega(n) \log \log n + \sum_{3 \leq n \leq x} (\log \log n)^2 = \Sigma_1 - 2\Sigma_2 + \Sigma_3$$

La somme Σ_1 est $x(\log \log x)^2 + O(x \log \log x)$ d'après la question précédente. La somme Σ_2 est majorée par

$$\log \log x \sum_{3 \leq n \leq x} \omega(n) = x(\log \log x)^2 + O(x \log \log x),$$

et minorée (pour $x \geq 9$) par

$$\log \log \sqrt{x} \sum_{\sqrt{x} \leq n \leq x} \omega(n) = (\log \log x - \log 2) \left(\sum_{n \leq x} \omega(n) + O(\sqrt{x} \log \log x) \right) = x(\log \log x)^2 + O(x \log \log x),$$

donc $\Sigma_2 = x(\log \log x)^2 + O(x \log \log x)$.

La somme Σ_3 est majorée par $x(\log \log x)^2$ et minorée (pour $x \geq 9$) par

$$(\log \log \sqrt{x})^2 \sum_{\sqrt{x} \leq n \leq x} 1 \geq (\log \log x - \log 2)^2 (x - \sqrt{x} - 1) = x(\log \log x)^2 + O(x \log \log x),$$

ce qui montre que $\Sigma_3 = x(\log \log x)^2 + O(x \log \log x)$.

On a démontré l'asymptotique $x(\log \log x)^2 + O(x \log \log x)$ pour chacune de trois sommes Σ_1 , Σ_2 et Σ_3 . Ceci implique que $\Sigma_1 - 2\Sigma_2 + \Sigma_3 = O(x \log \log x)$.

(e) Notons par $T(x)$ le nombre de $n \leq x$ qui sont ε -irréguliers. La partie gauche de (11) est minorée (pour $x \geq 9$) par

$$\sum_{\substack{\sqrt{x} \leq n \leq x \\ n \text{ est } \varepsilon\text{-irrégulier}}} (\log \log n)^{1+2\varepsilon} \geq (\log \log \sqrt{x})^{1+2\varepsilon} \sum_{\substack{\sqrt{x} \leq n \leq x \\ n \text{ est } \varepsilon\text{-irrégulier}}} 1 \geq (\log \log \sqrt{x})^{1+2\varepsilon} (T(x) - \sqrt{x}).$$

Puisque

$$(\log \log \sqrt{x})^{1+2\varepsilon} = (\log \log x)^{1+2\varepsilon} \left(1 - \frac{\log 2}{\log \log x}\right)^{1+2\varepsilon} \geq \frac{1}{2} (\log \log x)^{1+2\varepsilon}$$

pour x suffisamment grand, on a

$$T(x) = O\left(\frac{x \log \log x}{(\log \log x)^{1+2\varepsilon}}\right) + \sqrt{x} = O\left(\frac{x}{(\log \log x)^{2\varepsilon}}\right).$$

Exercice 3. Soit $\Phi(\mathbf{x}) \in \mathbb{F}_p[\mathbf{x}]$ un polynôme de n variables $\mathbf{x} = (x_1, \dots, x_n)$ sur \mathbb{F}_p . Soit $N(\Phi)$ le nombre de solutions de l'équation $\Phi(\mathbf{x}) = 0$ en $\mathbf{x} \in \mathbb{F}_p^n$. Le théorème célèbre de Weil-Lang affirme que pour Φ absolument irréductible¹ on a $|N(\Phi) - p^{n-1}| \leq Cp^{n-1-1/2}$, où la constante C ne dépend que du degré de Φ et du nombre des variables n . Le but de cet exercice est de démontrer ce théorème (en forme raffinée) pour les *polynômes diagonaux*

$$\Phi(\mathbf{x}) = a_1 x_1^{r_1} + \dots + a_n x_n^{r_n} \quad (12)$$

(où $a_1, \dots, a_n \in \mathbb{F}_p^\times$) en $n \geq 3$ variables.

(a) Rappeler les définitions d'un caractère additif et d'un caractère multiplicatif du corps fini \mathbb{F}_p . Soit ψ un caractère additif non principal et χ un caractère multiplicatif. Rappeler la définition de la somme de Gauss $g(\psi, \chi)$. Déterminer $g(\psi, \chi)$ dans le cas quand χ est principal. Énoncer (sans démonstration) le théorème sur le module de la somme de Gauss quand χ n'est pas principal.

(b) Considérons l'espace vectoriel des fonctions $f : \mathbb{F}_p^\times \rightarrow \mathbb{C}$ muni du produit scalaire défini par

$$(f, g) = \frac{1}{p-1} \sum_{x \in \mathbb{F}_p^\times} f(x) \overline{g(x)}. \quad (13)$$

Montrer que les caractères multiplicatifs forment une base orthonormée de cet espace. (Vous pouvez utiliser la propriété correspondante des caractères d'un groupe abélien fini.) Pour un caractère additif non principal ψ , exprimer les coordonnées de $\psi|_{\mathbb{F}_p^\times}$ dans cette base en termes des sommes de Gauss. En déduire que

$$\psi(x) = \frac{1}{p-1} \sum_{\chi} g(\psi, \bar{\chi}) \chi(x) \quad (x \in \mathbb{F}_p^\times). \quad (14)$$

(c) Montrer que pour $a \in \mathbb{F}_p^\times$ et $r \in \mathbb{N}^*$ on a

$$\sum_{x \in \mathbb{F}_p} \psi(ax^r) = \frac{1}{p-1} \sum_{\chi \neq 1} g(\psi, \bar{\chi}) \chi(a) \sum_{x \in \mathbb{F}_p^\times} \chi^r(x).$$

(d) Montrer que le nombre des caractères multiplicatifs vérifiant $\chi^r = 1$ est $d = \text{pgcd}(r, p-1)$. En déduire que

$$\left| \sum_{x \in \mathbb{F}_p} \psi(ax^r) \right| \leq (d-1)\sqrt{p}. \quad (15)$$

(e) Montrer que pour tout $\Phi \in \mathbb{F}_p[\mathbf{x}]$ on a

$$N(\Phi) = \frac{1}{p} \sum_{\psi} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \psi(\Phi(\mathbf{x})).$$

¹c'est-à-dire, irréductible sur la clôture algébrique $\bar{\mathbb{F}}_p$

En déduire que

$$N(\Phi) = p^{n-1} + \frac{1}{p} \sum_{\psi \neq 1} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \psi(\Phi(\mathbf{x})). \quad (16)$$

(f) Montrer que pour Φ diagonal, comme dans (12), on a

$$\sum_{\mathbf{x} \in \mathbb{F}_p^n} \psi(\Phi(\mathbf{x})) = \prod_{i=1}^n \sum_{x \in \mathbb{F}_p} \psi(a_i x^{r_i}). \quad (17)$$

(g) En déduire que pour Φ diagonal on a $|N(\Phi) - p^{n-1}| \leq Cp^{n/2}$, où $C = (d_1 - 1) \cdots (d_n - 1)$ avec $d_i = \text{pgcd}(r_i, p - 1)$.

Solutions (a) Un caractère additif ψ du corps fini $\mathbb{F} = \mathbb{F}_p$ est un caractère du groupe additif de \mathbb{F} . Un caractère multiplicatif de \mathbb{F} est un caractère χ du groupe multiplicatif \mathbb{F}^\times , étendu à \mathbb{F} en posant $\chi(0) = 0$. Le caractère additif principal est défini par $\psi(x) = 1$ pour tout $x \in \mathbb{F}$. Le caractère multiplicatif principal est défini par $\chi(x) = 1$ pour tout $x \in \mathbb{F}^\times$ (et $\chi(0) = 0$).

Si χ est un caractère d'un groupe abélien fini G alors $\sum_{x \in G} \chi(x)$ est $|G|$ si χ est principal et 0 sinon. En particulier, $\sum_{x \in \mathbb{F}} \psi(x) = 0$ pour un caractère additif non principal, et $\sum_{x \in \mathbb{F}^\times} \chi(x) = \sum_{x \in \mathbb{F}} \chi(x) = 0$ pour un caractère multiplicatif non principal.

La somme de Gauss est définie par $g = g(\psi, \chi) = \sum_{x \in \mathbb{F}} \psi(x)\chi(x)$. Si χ est principal alors

$$g(\psi, \chi) = \sum_{x \in \mathbb{F}^\times} \psi(x) = \sum_{x \in \mathbb{F}} \psi(x) - \psi(0) = -1.$$

Si χ n'est pas principal alors $|g| = \sqrt{p}$.

(b) Les caractères d'un groupe abélien fini G forment une base orthonormée de l'espace \mathbb{C}^G par rapport au produit scalaire $(f \cdot g) = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$. En particulier, les caractères multiplicatifs forment une base orthonormée de $\mathbb{C}^{\mathbb{F}^\times}$ par rapport au produit scalaire (13). Pour $f \in \mathbb{C}^{\mathbb{F}^\times}$ on a $f = \sum_{\chi} (f \cdot \chi)\chi$. En particulier, pour $f = \psi|_{\mathbb{F}^\times}$ on a $(f \cdot \chi) = \frac{1}{p-1}g(\psi, \bar{\chi})$, ce qui implique (14).

(c) D'après la question précédente,

$$\sum_{x \in \mathbb{F}_p} \psi(ax^r) = \psi(0) + \sum_{x \in \mathbb{F}_p^\times} \psi(ax^r) = 1 + \frac{1}{p-1} \sum_{x \in \mathbb{F}_p^\times} \sum_{\chi} g(\psi, \bar{\chi})\chi(ax^r). \quad (18)$$

Pour le caractère principal $\chi = 1$ on a $g(\psi, \bar{\chi}) = -1$ (voir question (a)), ce qui implique que pour $\chi = 1$

$$\frac{1}{p-1} \sum_{x \in \mathbb{F}_p^\times} g(\psi, \bar{\chi})\chi(ax^r) = \frac{1}{p-1} \sum_{x \in \mathbb{F}_p^\times} (-1) = -1.$$

Donc la partie droite de (18) est

$$1 + (-1) + \frac{1}{p-1} \sum_{x \in \mathbb{F}_p^\times} \sum_{\chi \neq 1} g(\psi, \bar{\chi})\chi(ax^r) = \frac{1}{p-1} \sum_{\chi \neq 1} g(\psi, \bar{\chi})\chi(a) \sum_{x \in \mathbb{F}_p^\times} \chi^r(x).$$

(d) Si $d \mid m$, alors dans un groupe cyclique d'ordre m il existe d éléments x vérifiant $x^d = 1$ (c'est la partie simple du "critère de la cyclicité"). Plus généralement, pour tout r le même groupe contient $d = \text{pgcd}(r, m)$ éléments vérifiant $x^r = 1$, parce que les conditions $x^r = 1$ et $x^d = 1$ sont équivalentes. En fait, il est évident que $x^d = 1 \Rightarrow x^r = 1$; réciproquement, puisque $d = ar + bm$ avec $a, b \in \mathbb{Z}$, on a $x^d = x^{ar} x^{mb} = x^{ar} = 1$ si $x^r = 1$.

Le groupe des caractères multiplicatifs est isomorphe au groupe \mathbb{F}^\times , qui est cyclique d'ordre $p - 1$. Donc il existe $d = \text{pgcd}(r, p - 1)$ caractères vérifiant $\chi^r = 1$, et $d - 1$ caractères non principaux avec cette propriété. D'après la question (a) on a $\sum_{x \in \mathbb{F}_p^\times} \chi^r(x) = 0$ si $\chi^r \neq 1$, et $\sum_{x \in \mathbb{F}_p^\times} \chi^r(x) = p - 1$ si $\chi^r = 1$. Donc

$$\sum_{x \in \mathbb{F}_p} \psi(ax^r) = \frac{1}{p-1} \sum_{\substack{\chi \neq 1 \\ \chi^r = 1}} g(\psi, \bar{\chi})\chi(a)(p-1) = \sum_{\substack{\chi \neq 1 \\ \chi^r = 1}} g(\psi, \bar{\chi})\chi(a).$$

Puisque $|g(\psi, \bar{\chi})| = \sqrt{p}$, la valeur absolue de la partie droite est majorée par $(d - 1)\sqrt{p}$.

(e) Si G est un groupe abélien fini écrit additivement alors $\sum_{\chi \in \widehat{G}} \chi(a) = 0$ si $a \neq 0$ et la somme est égale à $|G|$ si $a = 0$. En utilisant cette propriété avec G comme le groupe additif de \mathbb{F} , on trouve que l'expression $\frac{1}{p} \sum_{\psi} \psi(\Phi(\mathbf{x}))$ est égale à 1 si \mathbf{x} est une solution de l'équation $\Phi(\mathbf{x}) = 0$ et à 0 sinon. On obtient donc

$$N(\Phi) = \frac{1}{p} \sum_{\mathbf{x} \in \mathbb{F}^n} \sum_{\psi} \psi(\Phi(\mathbf{x})) = \frac{1}{p} \sum_{\psi} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \psi(\Phi(\mathbf{x}))$$

Puisque

$$\frac{1}{p} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \psi(\Phi(\mathbf{x})) = \frac{1}{p} \sum_{\mathbf{x} \in \mathbb{F}_p^n} 1 = p^n$$

pour $\psi = 1$, on a (16).

(f) On a

$$\sum_{\mathbf{x} \in \mathbb{F}_p^n} \psi(\Phi(\mathbf{x})) = \sum_{\mathbf{x} \in \mathbb{F}_p^n} \prod_{i=1}^n \psi(a_i x_i^{r_i}) = \prod_{i=1}^n \sum_{x_i \in \mathbb{F}} \psi(a_i x_i^{r_i}),$$

ce qui est (17).

(g) C'est une conséquence immédiate de (15), (16) et (17).