Fonctions complètement multiplicatives automatiques

Mickaël Postic

1 Introduction

Dans l'article initial, que je détaille et dont j'explicite les preuves non données ici, Jan-Christoph Schlage-Puchta montre qu'une fonction complètement multiplicative qui ne s'annule pas est presque périodique, au sens où elle peut être vue comme la limite de fonctions périodiques. Précisons quelques définitions:

Définition 1.1. *Une fonction $f : \mathbb{N} \to \mathbb{N}$ est dite complètement multiplicative si :*

$$\forall m, n \in \mathbb{N}, f(mn) = f(m) * f(n)$$

Définition 1.2. *Une fonction est dite q-automatique si elle est engendrée par un q-automate, c'est-à-dire que si $m = \sum_{i=0}^{n} a_i * q^i$, on a f(m) qui est l'image de l'état dans lequel l'automate termine après avoir lu la chaîne $a_n a_{n-1} ... a_0$. Plus généralement, une fonction f est dite automatique s'il existe un entier q tel que f est q-automatique*

Définition 1.3. *Une fonction est dite presque périodique s'il existe une suite de fonctions périodiques $(f_i)_{i\in\mathbb{N}}$ telle que la densité de l'ensemble $\{n : f(n) \neq f_i(n)\}$ tende vers 0 quand i tend vers ∞, où l'on définit la densité d'un ensemble $A \subset \mathbb{N}$ comme, si elle existe, $\lim_{n\to\infty} \frac{A \bigcap \{1,\cdots,n\}}{n}$*

Maintenant que nous avons donné ces quelques définitions, nous pouvons énoncer le théorème suivant:

Théorème 1.4. *Soit f une fonction complètement multiplicative automatique qui ne s'annule pas. Alors f est presque périodique.*

Tout le reste de cet article aura pour but de prouver ce théorème.

2 Résultats généraux

Dans la suite de la preuve, nous allons avoir besoin de deux résultats connus, l'un purement combinatoire, le théorème de coloriage de van der Waerden, l'autre plus analytique, le théorème de Wirsing-Halasz

Théorème 2.1. *Soit N un entier, S un ensemble fini, $\chi : \mathbb{N} \to S$ un coloriage. Alors il existe une séquence de progression arithmétique de longueur N+1 dont tous les termes sont coloriés de la même façon, c'est-à-dire:*

$$\exists\ a, D \in \mathbb{N} \text{ tels que } \chi(a) = \chi(a+D) = ... = \chi(a+ND)$$

Preuve. En fait, nous allons montrer quelque chose de plus fort que cela: nous allons montrer que pour tout couple $(k,l) \in \mathbb{N}^2$ il existe $W(k,l) \in \mathbb{N}$ tel que tout segment de longueur $W(k,l)$ contienne au moins une progression arithmétique monochrome de longueur l si le coloriage a au plus k couleurs. La preuve va se faire par récurrence sur l, elle est tirée de *Khinchin*.
Pour $l = 1$ et $l = 2$, le résultat est clair: $W(k,1) = 1$ et $W(k,2) = k+1$.
Supposons maintenant que le résultat est vrai pour un $l \in \mathbb{N}$ donné et montrons que pour tout $k \in \mathbb{N}$ on peut calculer $W(k, l+1)$.
Soit donc $k \in \mathbb{N}$ fixé.
La première idée de la preuve est la suivante: pour tout segment de longueur n, on peut définir la coloration de ce segment en disant que deux segments δ_1, δ_2 sont coloriés de la même façon si $\forall\ 0 \leq i \leq n,\ \chi(\delta_1(i)) = \chi(\delta_2(i))$. En particulier, il y a donc k^n colorations possibles pour un segment de longueur n.
L'idée est alors la suivante: on va construire par l'hypothèse de récurrence une progression arithmétique de longueur l de segments contenant eux même une progression arithmétique de segments de longueur l de taille plus petite et ainsi de suite k fois, la dernière progression arithmétique de

longueur l étant constituée d'éléments. A partir de là, on construira une progression arithmétique de longueur $l+1$. Construisons donc d'abord nos segments: posons

$$q_0 = 1; \quad n_0 = W(k,l)$$

puis par récurrence définissons

$$q_s = 2n_{s-1}q_{s-1}; \quad n_s = W(k^{q_s}, l).$$

J'affirme alors que $W(k,l+1) = q_k$ fonctionne. Considérons en effet un intervalle de longueur q_k. Puisque $q_k = 2n_{k-1}q_{k-1}$ on peut le voir comme deux intervalles de longueur $n_{k-1}q_{k-1}$ accolés. Le premier intervalle est alors vu comme n_{k-1} intervalles de longueur q_{k-1}. Par définition de n_s, on peut donc trouver une progression monochromatique de longueur l d'intervalles de longueur q_{k-1}: $\Delta_1, ..., \Delta_l$ à laquelle on rajoute le $l+1$ qui est compris dans $\{1, ..., q_k\}$. On pose d_1 la distance séparant les premiers éléments de deux intervalles consécutifs. Ensuite on réapplique le même procédé sur le premier intervalle de la progression obtenue, donnant une progression monochromatique de longueur l d'intervalles de longueur q_{k-2}, distance d_2, qui reste valable dans les intervalles suivants, et ainsi de suite.
Finalement on obtient donc des intervalles

$$\Delta_{i_1,...,i_s} |\ 1 \leq i_j \leq l,\ 0 \leq s \leq k$$

monochromatiques auxquels pour tout s, pour tout $i_1, i_2, ..., i_{s-1}$ on rajoute l'intervalle $\Delta_{i_1,...,i_{s-1},l+1_s}$ qui est la suite de la progression arithmétique d'écart d_s d'intervalles. Attention ici ce n'est pas de la même couleur que les l intervalles précédents!
On définit maintenant

$$\begin{cases} a_0 &= \Delta_{l+1,l+1,...,l+1} \\ a_1 &= \Delta_{1,l+1,...,l+1} \\ a_2 &= \Delta_{1,1,l+1,...,l+1} \\ \vdots & \\ a_k &= \Delta_{1,1,...,1} \end{cases}$$

Puisqu'on a $k+1$ éléments, il y en a au moins deux colorés de la même façon, notés a_s et a_r avec $s < r$. Posons alors

$$x_i = \Delta_{1,\cdots,1,i,\cdots,i,l+1,\cdots,l+1} \quad 1 \leq i \leq l+1$$

où les 1 sont sur les s premiers indices, les i sur les $r-s$ suivants, et les $l+1$ sur les derniers. On a donc une progression arithmétique de longueur $l+1$, et de raison $d_s + d_{s+1} + \cdots + d_{r-1}$. Par construction, elle est monochrome: les l premiers termes parce que les éléments sont au même endroit dans leur intervalle respectif de la progression, et le dernier parce que $\chi(a_s) = \chi(a_r)$ par définition de r et s.
Explicitons la coloration identique sur les l premiers:
$\chi(x_1) = \chi(\Delta_{1,\cdots,1,1,\cdots,1,l+1,\cdots,l+1}) = \chi(\Delta_{1,\cdots,1,i,1,\cdots,1,l+1,\cdots,l+1})$ car $\chi(\Delta_{1,\cdots,1,1}) = \chi(\Delta_{1,\cdots,1,i})$ en tant qu'intervalles. Puis on a de même $\chi(\Delta_{1,\cdots,1,i,1,\cdots,1,l+1,\cdots,l+1}) = \chi(\Delta_{1,\cdots,1,i,i,1,\cdots,1,l+1,\cdots,l+1})$ car $\chi(\Delta_{1,\cdots,1,i,1}) = \chi(\Delta_{1,\cdots,1,i,i})$ en tant qu'intervalles.
Et ainsi de suite, finalement, $x_1 = x_i$.
La preuve est donc complète, puisque nous avons construit une progression monochromatique de longueur $l+1$ pour un coloriage à k couleurs pour k quelconque fixé, et nous avons trouvé une borne q_k sur la longueur du plus grand segment sans tel coloriage. Par récurrence, nous pouvons donc affirmer le théorème vrai pour tout couple $(k,l) \in \mathbb{R}^2$.

□

Énonçons maintenant le théorème de Wirsing-Halasz. Pour ce faire, nous avons d'abord besoin de la définition suivante:

Définition 2.2. *La* valeur moyenne *d'une fonction $f : \mathbb{N} \to \mathbb{C}$, noté $M(f)$, est la valeur, si elle existe,*

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} f(n) = M(f)$$

Théorème 2.3. *Soit f une fonction complètement multiplicative à valeurs complexes avec $\forall n \mid f(n) \mid \leq 1$. Alors il existe un réel t tel que $n \to n^{it} f(n)$ a une valeur moyenne. De plus, si $\forall t \in \mathbb{R}$, $\sum_{p\in\mathbb{N}} \frac{\mathrm{Re}(1-p^{it}f(p)}{p}$ diverge, alors la valeur moyenne de $n \to n^{it} f(n)$ est 0 pour tout réel t. Sinon, la série converge pour un t, pour ce réel la valeur moyenne existe et n'est pas nulle.*

La preuve de ce théorème classique est fort longue et assez éloignée du sujet, je ne l'ai donc pas reprise.

Pour démontrer le théorème central, on a besoin d'une proposition, et pour cette proposition, on commence par prouver ces deux lemmes:

Lemme 2.4. *Soit f une fonction complètement multiplicative ne prenant qu'un nombre fini de valeurs. Alors chaque valeur prise par f est 0 ou une racine de l'unité*

Preuve. Soit x une valeur prise par f, et soit n tel que $f(n) = x$. Mais alors comme f est complètement multiplicative, on a $f(n^i) = x^i$ et donc $\{x^i : i \in \mathbb{N}\}$ est un ensemble fini, ce qui ne se peut que si x est racine de l'unité ou 0. □

Lemme 2.5. *Soit f une fonction complètement multiplicative ne prenant qu'un nombre fini de valeurs. Alors pour tout m et a dans $\mathbb{N}$ la quantité*

$$M(m,a) := \lim_{x\to\infty} \frac{m}{x} \sum_{\substack{n\leq x \\ n\equiv a \pmod m}} f(n)$$

existe, et de plus, s'il existe m et a tels que $|M(m,a)| = 1$, alors on a $f(n) = 1\ \forall n \equiv 1 \pmod m$

Preuve. D'après le lemme précédent, nous somme dans les conditions de Wirsing-Halasz puisque $|f(n)| \leq 1$. Commençons alors par montrer le lemme dans le cas $m = 1$, c'est-à-dire montrons que f admet une valeur moyenne, ce qui revient à montrer que dans le théorème de Wirsing-Halasz on peut prendre $t = 0$. Pour cela, il suffit, d'après la deuxième partie du théorème 3, de montrer que $\forall t \neq 0$, $\sum_{p\in\mathbb{N}} \frac{\mathrm{Re}(1-p^{it}f(p)}{p}$ diverge.
Soit donc $t \neq 0$ quelconque fixé. On pose $R \subseteq \mathbb{C}$ l'image de f qui est un ensemble fini d'éléments de norme 1 ou 0. Comme il est fini, on peut trouver $\epsilon > 0$ tel que $\bigcup_{z\in R} B(z,\epsilon)$ recouvre la moitié au plus du cercle unité. Ensuite, comme

$$\left|1 - p^{it}f(p)\right| = \left|p^{-it} - f(p)\right| \left|p^{it}\right| = \left|p^{-it} - f(p)\right|,$$

on a

$$\left|1 - p^{it}f(p)\right| < \epsilon \Rightarrow p^{-it} \in \bigcup_{z\in R} B(z,\epsilon)$$

D'après le théorème des nombres premiers, on a alors

$$p_n^{-it} = \exp\left(-\left(\ln n + \ln\ln n + \ln\left(1 + o(1)\right)\right) it\right)$$

Comme $\bigcup_{z\in R} B(z,\epsilon)$ recouvre la moitié au plus du cercle unité, on a alors

$$\left|1-p^{it}f(p)\right|>\epsilon$$

sur un ensemble de densité strictement positive.

Or on a:

$$\left|1-p^{it}f(p)\right|>\epsilon \Rightarrow \mathrm{Re}(1-p^{it}f(p))>\frac{\epsilon^2}{2}$$

En effet on a $|f(p)|=1$ ou 0. Si $|f(p)|=0$ alors la réponse est immédiate car $\epsilon<1$. Sinon on écrit $p^{it}f(p)=x+iy$, on a $x^2+y^2=1$ soit $y^2=1-x^2$. Donc $|1-x-iy|>\epsilon \Leftrightarrow 1+x^2-2x+1-x^2>\epsilon^2 \Leftrightarrow 2-2x>\epsilon^2 \Leftrightarrow 1-x>\frac{\epsilon^2}{2} \Leftrightarrow \mathrm{Re}(1-p^{it}f(p))>\frac{\epsilon^2}{2}$.

Mais alors on a aussi $\sum_{p\in\mathbb{N}} \frac{\mathrm{Re}(1-p^{it}f(p)}{p}$ qui diverge puisque la somme des inverses des nombres premiers est divergente:

$$p_n\sim n\ln n \Rightarrow \frac{1}{p_n}\sim\frac{1}{n\ln n}$$

et le résultat tombe par les séries de Bertrand.

En appliquant le théorème 3, on trouve alors que f admet une valeur moyenne.

Pour avoir l'existence de $M(m,a)$ on va se servir des caractères de Dirichlet, comme ils sont périodiques et complètement multiplicatifs on peut appliquer le résultat précédent à $n:\to\chi(n)f(n)$ pour tout caractère $\chi(n)$. Un résultat classique sur les caractères de Dirichlet est le suivant: Les caractères de Dirichlet modulo m forment une base orthonormale du $\mathbb{C}$-espace vectoriel $\mathbb{C}^U$ des fonctions de U dans $\mathbb{C}$, où U est l'ensemble des unités de $(\mathbb{Z}/n\mathbb{Z})^\times$, pour le produit hermitien $<,>$ défini par :

$$\forall f,g\in\mathbb{C}^U, <f,g>=\frac{1}{\varphi(n)}\sum_{x\in U}\overline{f(x)}g(x)$$

Ici φ est l'indicatrice d'Euler, et les caractères de Dirichlet sont vus comme des morphismes de groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$ dans $\mathbb{C}^*$. Il est facile de repasser aux fonctions nous intéressant en étendant à tout $\mathbb{N}$ périodiquement.

En combinant linéairement les caractères, on peut donc trouver une fonction qui vaut 1 en $\overline{a}$ et 0 ailleurs si $\overline{a} \in U$. En considérant les fonctions étendues par périodicité et multipliées par $f(n)$, on récupère une fonction qui vaut $f(n)$ si $n \equiv a \pmod{m}$ et 0 sinon.

On obtient donc le résultat recherché, l'existence de $M(m,a)$ dès que $\overline{a} \in U$ ou autrement dit dès que $a \wedge m = 1$. Si $m \wedge a = d$, on a $a = da'$ et $m = dm'$ et alors $n \equiv a \pmod{m}$ équivaut à : $(n = dn')$ et $n' \equiv a' \pmod{m'}$. Comme par totale multiplicativité, $f(n) = f(d)f(n')$, on obtient $M(m,a) = f(d)M(m',a')$ et l'existence vaut pour tout couple (m,a).

Si maintenant $|M(m,a)| = 1$, on a $f(n) = M(m,a)$ dès que $n \equiv a \pmod{m}$ sauf peut-être sur un ensemble de densité nulle car $|f(n)| \leq 1$. Mais alors, si $f(n) \neq M(m,a)$, on a $f(n(mr+1)) = f(n)f(mr+1)$ pour tout r. Or, $\forall r \in \mathbb{N}$, $n(mr+1) \equiv a \pmod{m}$ et cela permet de construire un ensemble de densité non nulle tel que $f(n) \neq M(m,a)$. En effet, soit $f(m+1) = 0$ et c'est réglé en considérant l'ensemble $\{n(m+1)^p : p \in \mathbb{N}\}$, soit c'est une racine de l'unité, donc il existe $p \in \mathbb{N}$ tel que $f((m+1)^p) = 1$ et on considère l'ensemble $\{n(m+1)^{pq} : q \in \mathbb{N}\}$.
Montrons maintenant que $f(n) \equiv 1 \pmod{m}$. Cela apparaît déjà dans ce que l'on vient de faire en filigrane: si $f(mr+1) \neq 1$ soit c'est 0 et dans ce cas l'ensemble $\{a(mr+1)^p : p \in \mathbb{N}\}$ fournit un ensemble où $f = 0$ de densité non nulle, soit c'est une racine de l'unité et comme précédemment $\{a(m+1)^{pq+1} : q \in \mathbb{N}\}$ fournit un ensemble de densité non nulle où $f \neq M(m,a)$. □

Proposition 2.6. *Soit $q \in \mathbb{N}, n \geq 2$, et f une fonction complètement multiplicative q-automatique, qui ne s'annule pas.*
Alors il existe $k \in \mathbb{N}$ tel que si n_1, n_2, l sont des entiers vérifiant $\mathrm{pgcd}(n_1, q^{l+1})|q^l$, et $n_1 \equiv n_2 \pmod{q^{k+l}}$ alors $f(n_1) = f(n_2)$

Preuve. Puisque notre fonction f est q-automatique, on peut définir un coloriage de la façon suivante: $\chi(n)$ est l'état dans lequel se trouve l'automate après avoir lu n. Puisque l'automate est fini, il n'a qu'un nombre fini d'état et on a bien définit un coloriage sur $\mathbb{N}$. Par le théorème de van der Waerden, on peut alors trouver une progression arithmétique monochromatique aussi longue que souhaitée. Soit $a, a+D, \cdots, a+ND$ une telle progression.

Constatons alors la chose suivante: si $k \in \mathbb{N}, b \in \{0, 1, \cdots, q^k - 1\}$ on a $f(aq^k + b) = f((a + D)q^k + b) = \cdots = f((a + ND)q^k + b)$ puisque l'automate lit d'abord $a + rD$, se retrouve dans l'état $\chi(a)$, puis lit b ce qui l'amène donc toujours au même endroit, l'automate n'ayant pas la mémoire du trajet effectué, être arrivé en $\chi(a)$ après avoir lu a ou $a + ND$ est indiscernable. En choisissant k assez grand, on a $q^k > D$ et en choisissant bien b on a $aq^k + b \equiv 0 \pmod{D}$. Alors $f(aq^k + b) = f((a + rD)q^k + b) = f(D)f(\frac{aq^k+b}{D} + rq^k) = f(D)f(\frac{aq^k+b}{D})$ et en divisant par $f(D)$ qui est non nul puisque f ne s'annule pas on se retrouve avec une progression arithmétique de raison q^k sur laquelle f est constante.

Il est maintenant temps de fixer N: nous prenons $n = 2q^{|S|!}$. Ainsi le premier terme de notre progression peut s'écrire $aq^k+b = uq^{k+|s|!}+vq^k+w$ avec $v < q^{|S|!}$ et $w < q^k$. Quitte à ne pas commencer au premier terme de notre progression mais au $q^{|S|!} - v$-ième, on peut considérer que $v = 0$, il nous reste encore au moins $q^{|S|!}$.

Soit alors s l'état dans lequel se trouve l'automate après avoir lu u. Dans la progression arithmétique, on peut lire n'importe quel v dans l'écriture ci-dessus. On s'intéresse donc aux chemins de longueur $|S|!$ au départ de s. Un tel chemin (dans l'automate vu comme un graphe orienté) est constitué d'un chemin sans répétitions de sommet de longueur l_0 en somme avec des cycles disjoints de longueur $l_1, ..., l_m$ répétés $x_1, ..., x_m$ fois chacun respectivement. On a donc: $|S|! = l_0 + l_1x_1 + ... + x_ml_m$, soit $|S|! - l_0 = l_1x_1 + ... + x_ml_m$. On a $\text{pgcd}(l_1, l_2, \cdots, l_m) \mid |S|!$ puisque les cycles de longueur l_i sont disjoints, donc $l_1 + \cdots + l_m \leq |S|$. De plus $|S|! \geq l_1l_m$. On peut donc appliquer le lemme suivant:

Lemme 2.7. *Soient $l_1 \leq \cdots \leq l_m \in \mathbb{N}$ des entiers positifs, et $G \subseteq \mathbb{N}$ le semi-groupe additif engendré par ces entiers. Si $n \geq l_1l_m$, alors $n \in G$ si et seulement si* $\text{pgcd}(l_1, \cdots, l_m)$ *divise n.*

Preuve. L'un des sens est clair: si $n = r_1l_1+\cdots+r_ml_m$, alors $\text{pgcd}(l_1, \cdots, l_m) \mid n$ puisqu'il divise tous les termes de la somme.
Montrons alors l'autre sens: posons R_k l'ensemble des classes de $\mathbb{Z}/l_1\mathbb{Z}$ pouvant s'écrire $x_2l_2 + \cdots + x_ml_m$ avec $x_2 + \cdots + x_m \leq k$. La suite des R_k est clairement croissante, et comme il n'y a qu'un nombre fini de classes modulo l_1, elle est stable à partir d'un certain rang. En fait, la croissance est même strict jusqu'à la stabilité: $R_k = R_{k+1} \Rightarrow R_{k+1} =$

R_{k+2}. En effet, si $x_2 + \cdots + x_m = k+2$, en supposant sans perte de généralité $x_2 \leq 1$, on a $(x_2-1)l_2 + x_3l_3 + \cdots + x_ml_m \in R_k$ donc on a $x_2l_2 + x_3l_3 + \cdots + x_ml_m \in R_{k+1} = R_k$ et donc $R_k = R_{k+1} = R_{k+2}$.
Maintenant, puisqu'il y a l_1 éléments dans $\mathbb{Z}/l_1\mathbb{Z}$, on a $R_{l_1} = R_{l_1+1}$. Du coup, si $\overline{x} \in R_{l_1}$ on a $\overline{x+l_i} \in R_{l_1}$ et on en déduit par induction finie que R_{l_1} est un stable pour l'addition, donc c'est un sous-groupe de $\mathbb{Z}/l_1\mathbb{Z}$. Comme il contient tous les l_i et que tous ces éléments sont multiples de $\text{pgcd}(l_2, \cdots, l_m)$ c'est le sous-groupe de $\mathbb{Z}/l_1\mathbb{Z}$ engendré par $\text{pgcd}(l_2, \cdots, l_m)$.
Cela nous permet alors de compléter la preuve:
Soit $n \geq l_1l_m$: $\text{pgcd}(l_1, \cdots, l_m) \mid n$. On a alors $n = pl_1 + r, r < l_1$, et $\text{pgcd}(l_1, \cdots, l_m) \mid r$. En appliquant le résultat précédent, $r \in R_{l_1}$ donc $n = (p+p')l_1 + x_2l_2 + \cdots + x_ml_m$, $x_2 + ... + x_m \leq l_1$. Pour conclure il reste seulement à prouver $p + p' \geq 0$. Or, $x_2l_2 + ... + x_ml_m \leq (x_2 + ... + x_m)l_m \leq l_1l_m$ et on conclut par $n \geq l_1l_m$. □

On récupère donc $\exists(z_1, \cdots, z_m) \in \mathbb{N}^m$ tels que $|S|! = z_1l_1 + \cdots + z_ml_m$. Cela permet d'écrire $y|S|! - l_0 = (x_1 + (y-1)z_1)l_1 + \cdots + (x_m + (y-1)z_m)l_m$ et donc il existe un chemin de s à s' de longueur $y|S|!$ pour tout $y \in \mathbb{N}^*$. A l'inverse, si s' peut être atteint en $y|S|!$ pas, on peut définir de la même façon le chemin direct et les cycles, et le même raisonnement montre que s' peut déjà être atteint en $|S|!$ pas.

Appelons donc X l'ensemble des états atteignables à partir de s en $|S|!$ pas. Puisque $\forall v < q^{|S|!}, f(uq^{k+|S|!} + vq^k + w) = f(a')$ où $a' := uq^{k+|S|!} + w$ est le premier terme de notre progression arithmétique (tronquée), on a que pour tout état s' de X, si depuis cet état on lit w on se retrouve sur un état x produisant $f(a')$. Puisque X est aussi l'ensemble des états atteignables en $y|S|!$ pas pour tout $y \in \mathbb{N}^*$, on a même $\forall v < q^{y|S|!}, f(uq^{k+y|S|!} + vq^k + w) = f(a')$. En sommant cette relation, on obtient:

$$\sum_{\substack{uq^{k+y|S|!} \leq n < (u+1)q^{k+y|S|!} \\ n \equiv w \pmod{q^k}}} f(n) = q^{y|S|!} f(a')$$

On applique alors le lemme 2.5 permettant d'affirmer que $\forall (m, a) \in \mathbb{N}^2, M(m, a)$ existe, en prenant $m = q^k$ et $a = w$ on a pour ϵ fixé, pour y

assez grand,

$$\mid M(q^k, w) - \frac{q^k}{(u+1)q^{k+y|S|!}} \sum_{\substack{n<(u+1)q^{k+y|S|!} \\ n\equiv w \pmod{q^k}}} f(n) \mid \leq \epsilon$$

et

$$\mid M(q^k, w) - \frac{q^k}{uq^{k+y|S|!}} \sum_{\substack{n<uq^{k+y|S|!} \\ n\equiv w \pmod{q^k}}} f(n) \mid \leq \epsilon.$$

Or,

$$|A - \frac{1}{x}\sum^{x} f(k)| \leq \epsilon$$

et

$$|A - \frac{1}{x+y}\sum^{x+y} f(k)| \leq \epsilon$$

donne

$$|A - \frac{1}{x}\sum^{x} f(k) + (\frac{1}{x} - \frac{1}{x+y})\sum^{x} f(k) - \frac{1}{x+y}\sum_{x}^{x+y} f(k)| \leq \epsilon$$

donc

$$-2\epsilon \leq \frac{1}{x+y}(\frac{y}{x}\sum^{x} f(k) - \sum_{x}^{x+y} f(k)) \leq 2\epsilon$$

et donc

$$-(2 + \frac{y}{x+y})\epsilon \leq \frac{1}{x+y}(yA - \sum_{x}^{x+y} f(k)) \leq (2 + \frac{y}{x+y})\epsilon.$$

Finalement, en appliquant ce résultat à nos deux inégalités, et en faisant tendre ϵ vers 0, puisque le rapport $\frac{y}{x+y}$ ne tend pas vers 0, on récupère $M(q^k, w) = f(a')$. On a donc par le premier lemme 2.4 $|M(m, a)| = 1$ et le lemme 2.5 permet alors de conclure

$$f(n) = 1 \quad \forall n \equiv 1 \pmod{q^k}$$

Soient maintenant n_1, n_2, l tels que définis dans la proposition. Montrons que $f(n_1) = f(n_2)$.
On a $n_1 = n'_1 q^l$ et $n_1 = n_2 + aq^{k+l}$, donc $n_2 = q^l(n'_1 - aq^k) = n'_2 q^l$. On a alors $f(n_1) = f(n'_1)f(q^l)$ et $f(n_2) = f(n'_2)f(q^k)$, donc $f(n_1) = f(n_2) \Leftrightarrow f(n'_1) = f(n'_2)$ puisque f ne s'annule pas.
Comme $\text{pgcd}(n'_1, q^k) = 1, \exists {n'_1}^{-1} : n'_1 {n'_1}^{-1} = bq^k + 1$. Mais alors, via le résultat concluant le paragraphe précédent, $f(n'_1 {n'_1}^{-1}) = 1$ donc on a $f(n' - 1) = f({n'_1}^{-1})^{-1}$.
De même, $n'_2 {n'_1}^{-1} = {n'_1}^{-1}(n'_1 - aq^k) = 1 + cq^k$ et donc

$$f(n'_2) = f({n'_1}^{-1})^{-1} = f(n'_1).$$

On a donc

$$f(n_1) = f(n_2)$$

et la preuve est complète. □

Maintenant à l'aide de cette proposition il est facile de démontrer le théorème recherché: il nous suffit de construire la suite $(f_i)_{i\in\mathbb{N}}$. On la définit de la manière suivante: soit k donné par la proposition. On pose alors $f_i(n) := f(n \mod q^{k+i})$. Par définition de k, on a $f_i(n) = f(n)$ dès que $\text{pgcd}(n_1, q^{i+1})|q^i$, donc $\{n : f(n) \neq f_i(n)\} \subseteq \{n : \text{pgcd}(n, q^{i+1}) \nmid q^i\}$
Il est alors aisé de voir que la densité de $\{n : f(n) \neq f_i(n)\}$ tend vers 0 puisque la densité de l'ensemble $\{n : q^i|n\}$ tend vers 0 quand $i \to \infty$.
Cela complète notre preuve du théorème.