Sur un groupe associé aux entiers quadratiques

F. Arnault et G. Robin

LACO (Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation)
Département de Mathématiques
123, avenue Albert Thomas, 87060 Limoges Cedex

Résumé. Soit $\mathcal{O}$ l'anneau des entiers d'un corps quadratique et n un entier rationnel. Nous étudions un groupe multiplicatif contenu dans l'anneau $\mathcal{O}/n$, dont le rôle s'est révélé important lors d'un travail sur les tests de primalité de Lucas. Nous explicitons sa structure, ainsi que les valeurs asymptotiques de son ordre quand n tend vers ∞.

Abstract. Let $\mathcal{O}$ be the ring of integers in a quadratic field and n a rational integer. We study a multiplicative group in $\mathcal{O}/n$, which appeared in a work on Lucas primality test. We give the structure of this group, and the asymptotic values of its order, as n goes to ∞.

1. Introduction

Soit D un entier qui ne soit pas un carré parfait. Nous considérons l'anneau $\mathcal{O}$ des entiers de $\mathbb{Q}(\sqrt{D})$. Pour $\mathfrak{a}$ idéal de $\mathcal{O}$, nous notons $(\mathcal{O}/\mathfrak{a})^\times$ le groupe des inversibles de l'anneau $\mathcal{O}/\mathfrak{a}$. Pour $n \in \mathbb{Z}$, le quotient $\mathcal{O}/n$ est une algèbre et un module libre de rang 2 sur l'anneau $\mathbb{Z}/n\mathbb{Z}$. Nous notons $(\mathcal{O}/n)^\wedge$ le groupe des éléments de norme 1 dans $\mathcal{O}/n$. Par définition, c'est l'ensemble des éléments $[x]$ de $\mathcal{O}/n$ tels que le déterminant de l'application

$$\mathcal{O}/(n) \ni [y] \longmapsto [x][y] \in \mathcal{O}/n$$

soit égal à 1. Autrement dit, $(\mathcal{O}/n)^\wedge$ est l'image de l'ensemble

$$\{x \in \mathcal{O} \mid N(x) \equiv 1 \text{ modulo } n\}$$

par la surjection canonique $\mathcal{O} \to \mathcal{O}/n$.

Il est bien connu que, pour p premier et pour $r \geqslant 1$, le groupe des inversibles de $\mathbb{Z}/p^r\mathbb{Z}$ est cyclique (et d'ordre $p^{r-1}(p-1)$). L'un des objets de ce papier est de prouver le résultat suivant, utilisé lors d'un travail [1] sur les tests de primalité de Lucas.

1.1. — **Théorème.** *Soit $\mathcal{O}$ l'anneau des entiers d'un corps quadratique $\mathbb{Q}(\sqrt{D})$. Soient p un premier rationnel ne divisant pas $2D$ et $r \geqslant 1$ un entier. Le groupe $(\mathcal{O}/p^r)^\wedge$ est* **cyclique** *d'ordre $p^{r-1}\big(p-(D/p)\big)$.*

La fonction φ_D

Par analogie avec la fonction indicatrice d'Euler, le théorème 1.1 nous suggère de poser la définition suivante :

1.2. — **Définition.** Soit D un entier non nul. Pour $n \in \mathbb{N}$ tel que $\operatorname{pgcd}(n, 2D) = 1$ et dont la décomposition primaire est $p_1^{r_1} \cdots p_s^{r_s}$, on pose

$$\varphi_D(n) = \prod_{i=1}^{s} p_i^{r_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right).$$

Pour D non carré parfait, le groupe $(\mathcal{O}/n)^\wedge$ est donc d'ordre $\varphi_D(n)$. Pour D carré parfait, φ_D est la fonction d'Euler usuelle.

Les résultats suivants sur le comportement de φ sont bien connus (voir [2] et [3]) :

1991 Mathematics Subject Classification. Primary: 11R11. Secondary: 11N37, 11B25.

1.3. — Théorème. *On a les relations suivantes :*

$$\limsup \frac{\varphi(n)}{n} = 1, \qquad \liminf \frac{\varphi(n)}{n} e^{\gamma} \ln\ln n = 1.$$

où γ désigne la constante d'Euler.

Le but de ces pages est aussi de montrer des résultats analogues pour la fonction φ_D. Pour cela, nous introduisons les constantes suivantes, où pour p premier impair, $\varepsilon(p)$ désigne le symbole de Legendre (D/p) :

$$A_- = \prod_{\varepsilon(p)=-1} \Big(1 - \frac{1}{p^2}\Big), \qquad l = L(1,\varepsilon) = \prod_p \Big(1 - \frac{\varepsilon(p)}{p}\Big)^{-1}, \qquad P_0 = \prod_{p|2D} \Big(1 - \frac{1}{p}\Big).$$

1.4. — Théorème.

$$\liminf \frac{\varphi_D(n)}{n} e^{\gamma/2} \sqrt{\ln\ln n} = \frac{1}{\sqrt{l P_0 A_-}}, \qquad \limsup \frac{\varphi_D(n) e^{-\gamma/2}}{n\sqrt{\ln\ln n}} = \sqrt{\frac{P_0 A_-}{l}}.$$

2. Décomposition en produit direct

Le but de cette section est de démontrer la proposition suivante, qui sera utilisée dans la preuve du théorème 1.1.

2.1. — Proposition. *Soit $\mathcal{O}$ l'anneau des entiers d'un corps de nombres et soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$. Pour tout entier $r \geqslant 1$, on a la décomposition*

$$(\mathcal{O}/\mathfrak{p}^r)^\times = \{[1+\gamma] \in (\mathcal{O}/\mathfrak{p}^r)^\times \mid \gamma \in \mathfrak{p}\} \times \{x^{N(\mathfrak{p})^{r-1}} \mid x \in (\mathcal{O}/\mathfrak{p}^r)^\times\} \tag{1}$$

en produit direct de sous-groupes.

Lemmes préliminaires

2.2. — Lemme. *Pour $\alpha, \beta \in \mathcal{O}$, pour $r \geqslant 1$ entier et pour $k \in \mathfrak{p} \cap \mathbb{Z}$, on a l'implication*

$$\alpha \equiv \beta \text{ modulo } \mathfrak{p} \quad \Rightarrow \quad \alpha^{k^{r-1}} \equiv \beta^{k^{r-1}} \text{ modulo } \mathfrak{p}^r.$$

Démonstration — Pour $\alpha - \beta \in \mathfrak{p}$, on a

$$\begin{aligned} \alpha^k - \beta^k &= (\alpha-\beta)(\alpha^{k-1} + \alpha^{k-2}\beta + \cdots + \beta^{k-1}) \\ &\equiv (\alpha-\beta)(\alpha^{k-1} + \alpha^{k-1} + \cdots + \alpha^{k-1}) \quad \text{modulo } \mathfrak{p} \\ &= (\alpha-\beta) k \alpha^{k-1} \in \mathfrak{p}^2, \end{aligned}$$

ce qui démontre le résultat pour $r = 2$. Une récurrence facile laissée au lecteur démontrerait le résultat pour r quelconque. □

2.3. — Lemme. *Il existe une injection naturelle*

$$(\mathcal{O}/\mathfrak{p})^\times \ni [\alpha] \longmapsto [\alpha^{N(\mathfrak{p})^{r-1}}] \in (\mathcal{O}/\mathfrak{p}^r)^\times.$$

Son image est donc un groupe cyclique.

Démonstration — Comme $N(\mathfrak{p}) \in \mathfrak{p}$, le lemme 2.2 montre que le morphisme ci-dessus est bien défini. De plus, si l'on a une congruence

$$\alpha^{N(\mathfrak{p})^{r-1}} \equiv \beta^{N(\mathfrak{p})^{r-1}} \quad \text{modulo } \mathfrak{p}^r,$$

alors on a la même congruence modulo $\mathfrak{p}$. Donc, puisque $\alpha^{N(\mathfrak{p})} \equiv \alpha$ et $\beta^{N(\mathfrak{p})} \equiv \beta$ modulo $\mathfrak{p}$, on a alors

$$\alpha \equiv \alpha^{N(\mathfrak{p})^{r-1}} \equiv \beta^{N(\mathfrak{p})^{r-1}} \equiv \beta \quad \text{modulo } \mathfrak{p},$$

ce qui montre que le morphisme est injectif. Son image est donc isomorphe à $(\mathcal{O}/\mathfrak{p})^\times$ qui est cyclique puisque $\mathcal{O}/\mathfrak{p}$ est un corps fini. □

Démonstration de la proposition 2.1

Pour $\alpha \in \mathcal{O}$ on a la congruence $\alpha^{N(\mathfrak{p})} \equiv \alpha$ modulo $\mathfrak{p}$ et donc, par récurrence, $\alpha^{N(\mathfrak{p})^{r-1}} \equiv \alpha$ modulo $\mathfrak{p}$. On a donc, si $\alpha \notin \mathfrak{p}$,

$$\alpha^{N(\mathfrak{p})^{r-1}-1} \equiv 1 \quad \text{modulo } \mathfrak{p}.$$

Ainsi, l'égalité

$$\alpha = (\alpha^{N(\mathfrak{p})^{r-1}-1})^{-1}\, \alpha^{N(\mathfrak{p})^{r-1}} \tag{2}$$

montre que $(\mathcal{O}/\mathfrak{p}^r)^\times$ est bien le produit des deux sous-groupes. Montrons que ce produit est direct. Supposons que l'on ait une congruence

$$1+\gamma \equiv \alpha^{N(\mathfrak{p})^{r-1}} \quad \text{modulo } \mathfrak{p}^r \qquad \text{avec } \gamma \in \mathfrak{p},\ \alpha \in \mathcal{O}.$$

De $\alpha^{N(\mathfrak{p})} \equiv \alpha$ modulo $\mathfrak{p}$ on tire, par récurrence,

$$\alpha \equiv \alpha^{N(\mathfrak{p})^{r-1}} \equiv 1+\gamma \equiv 1 \text{ modulo } \mathfrak{p}.$$

Puis, d'après le lemme 2.2, on obtient

$$\alpha^{N(\mathfrak{p})^{r-1}} \equiv 1 \quad \text{modulo } \mathfrak{p}^r$$

ce qui montre bien que l'intersection des deux sous-groupes est réduite à l'unité. □

3. Sous-groupe des éléments de norme 1

Lemme préliminaire

3.1. — **Lemme.** *Avec les notations du théorème 1.1 et en supposant que $r \geqslant 2$, le morphisme canonique*

$$(\mathcal{O}/p^r)^\wedge \longrightarrow (\mathcal{O}/p^{r-1})^\wedge$$

est surjectif et son noyau est de cardinal p.

Démonstration — Soit α élément de $(\mathcal{O}/p^{r-1})^\wedge$ et soient $u, v \in \mathbb{Z}/p^r\mathbb{Z}$ tels que $u+v\sqrt{D}$ modulo $p^{r-1} = \alpha$. Nous devons montrer qu'il existe exactement p couples d'entiers (k,l) tels que $0 \leqslant k,l < p$ et

$$N\big((u+kp^{r-1}) + (v+lp^{r-1})\sqrt{D}\big) \equiv 1 \text{ modulo } p^r.$$

Cela s'écrit

$$u^2 - Dv^2 + 2p^{r-1}(uk - vld) + p^{2(r-1)}(k^2 + Dl^2) \equiv 1 \text{ modulo } p^r,$$

ou encore, puisque $r \geqslant 2$,

$$u^2 - Dv^2 + 2p^{r-1}(uk - vld) \equiv 1 \text{ modulo } p^r.$$

Finalement, cela revient à compter les couples (k,l) solutions de

$$uk \equiv \frac{1-(u^2-Dv^2)}{2p^{r-1}} + vlD \text{ modulo } p.$$

Or, cette équation admet exactement p solutions (une pour chaque valeur fixée de l), ce qui termine la démonstration. □

Décomposition en produit direct

3.2. — Proposition. *Avec les notations du théorème 1.1, si p est inerte dans $\mathcal{O}$, on a la décomposition*

$$(\mathcal{O}/p^r)^\wedge = \{[1+\gamma] \in (\mathcal{O}/p^r)^\wedge \mid \gamma \in p\} \times \{x^{p^{2(r-1)}} \mid x \in (\mathcal{O}/p^r)^\wedge\} \tag{3}$$

en produit direct de sous-groupes.

Démonstration — Reprenons l'égalité (2) : elle s'écrit ici

$$\alpha = (\alpha^{p^{2(r-1)}-1})^{-1}\, \alpha^{p^{2(r-1)}}. \tag{4}$$

La norme étant multiplicative, si α est de norme 1 modulo p^r, il en est de même du facteur $\alpha^{p^{2(r-1)}}$ de l'égalité ci-dessus, et donc aussi de l'autre facteur. Ainsi, l'égalité (4) montre que $(\mathcal{O}/p^r)^\wedge$ est bien le produit (3) des deux sous-groupes. De plus, puisque l'on a les relations

$$\{x^{p^{2(r-1)}} \mid x \in (\mathcal{O}/p^r)^\wedge\} = \{x^{p^{2(r-1)}} \mid x \in (\mathcal{O}/p^r)^\times\} \cap (\mathcal{O}/p^r)^\wedge \tag{5}$$

et

$$\{[1+\gamma] \in (\mathcal{O}/p^r)^\wedge \mid \gamma \in p\} = \{[1+\gamma] \in (\mathcal{O}/p^r)^\times \mid \gamma \in p\} \cap (\mathcal{O}/p^r)^\wedge,$$

le fait que le produit (3) soit direct résulte du fait que le produit (1) le soit. □

Démonstration du théorème 1.1

• Supposons d'abord que p soit inerte dans $\mathcal{O}$. Le lemme 2.3 montre que le deuxième facteur de la décomposition (1) (pour $\mathfrak{p} = (p)$) est cyclique d'ordre p^2-1. Or, le deuxième facteur de la décomposition (3) est un sous-groupe de celui de (1) d'après (5). Il est donc, lui aussi, cyclique.

De plus, d'après 2.2, l'injection du lemme 2.3 induit une bijection

$$(\mathcal{O}/p)^\wedge \to \{x^{p^{2(r-1)}} \mid x \in (\mathcal{O}/p^r)^\wedge\}.$$

Puisque le conjugué d'un élément x de $\mathcal{O}/p$ est x^p, les éléments de norme 1 dans $\mathcal{O}/p$ y sont les racines $(p+1)$-ièmes de l'unité, qui sont en nombre $p+1$. Donc, le facteur de droite de la décomposition (3) est d'ordre $p+1$.

Considérons maintenant le premier facteur de la décomposition (3). Le lemme 3.1 montre par récurrence qu'il est d'ordre p^{r-1}.

Pour montrer qu'il est lui-aussi cyclique, montrons d'abord par récurrence sur r qu'il existe $\gamma \in p\mathcal{O} \setminus p^2\mathcal{O}$ tel que $[1+\gamma]$ appartient à $(\mathcal{O}/p^r)^\wedge$. Pour $r = 1$ ou 2, il suffit de prendre $\gamma = p^2 + p\sqrt{D}$ puisque

$$\begin{aligned} N(1+\gamma) &= (1+p^2)^2 + p^2 D \\ &\equiv 1 \text{ modulo } p^r. \end{aligned}$$

Pour $r \geqslant 3$, l'hypothèse de récurrence affirme qu'il existe $\gamma \in p\mathcal{O} \setminus p^2\mathcal{O}$ avec $N(1+\gamma) \equiv 1$ modulo p^{r-1}. Mais le lemme 3.1 montre l'existence d'un élément $1+\gamma'$ tel que

$$\begin{cases} 1+\gamma' \equiv 1+\gamma \text{ modulo } p^{r-1} \\ [1+\gamma'] \in (\mathcal{O}/p^r)^\wedge. \end{cases}$$

Comme $\gamma \equiv \gamma'$ modulo p^2, on a bien $\gamma' \in p\mathcal{O} \setminus p^2\mathcal{O}$ ce qui termine la récurrence. On vérifie alors aisément que

$$(1+\gamma)^{p^{k-1}} \equiv 1 + p^{k-1}\gamma \quad \text{modulo } p^k \qquad \text{pour } k \geqslant 1.$$

Donc, $1+\gamma$ est d'ordre p^{r-1} dans le facteur de gauche de (3) et en est un générateur, ce qui prouve que ce facteur est cyclique.

Enfin, on a montré que $(\mathcal{O}/p^r)^\wedge$ est le produit d'un groupe cyclique d'ordre $p+1$ par un autre d'ordre p^{r-1}. Il est donc cyclique d'ordre $p^{r-1}(p+1)$.

• Supposons maintenant que $p = \mathfrak{p}\overline{\mathfrak{p}}$ soit scindé dans $\mathcal{O}$. Montrons grâce à la décomposition (1) que le groupe $(\mathcal{O}/\mathfrak{p}^r)^\times$ est cyclique. Nous savons grâce au lemme 2.3 que le facteur de droite est cyclique d'ordre $p-1$. Quant au facteur de gauche, il est d'ordre

$$N(\mathfrak{p}^r)/N(\mathfrak{p}) = N(\mathfrak{p})^{r-1} = p^{r-1}.$$

Il est facile de voir que, si γ est un élément de $\mathfrak{p}\setminus\mathfrak{p}^2$, alors on a

$$(1+\gamma)^{p^{k-1}} \equiv 1 \text{ modulo } \mathfrak{p}^k$$

mais

$$(1+\gamma)^{p^{k-1}} \not\equiv 1 \text{ modulo } \mathfrak{p}^{k-1} \qquad \text{pour } k \geqslant 1.$$

Donc $1+\gamma$ est d'ordre p^{r-1} et est un générateur du facteur de gauche qui est donc, lui-aussi, cyclique.

On a montré que $(\mathcal{O}/\mathfrak{p}^r)^\times$ est le produit d'un groupe cyclique d'ordre $p-1$ par un autre d'ordre p^{r-1}. Il est donc cyclique d'ordre $p^{r-1}(p-1)$. Enfin, on a un morphisme injectif

$$(\mathcal{O}/\mathfrak{p}^r)^\times \ni x \quad \longmapsto \quad (x, 1/x) \in (\mathcal{O}/\mathfrak{p}^r)^\times \times (\mathcal{O}/\overline{\mathfrak{p}}^r)^\times \simeq (\mathcal{O}/p^r)^\times$$

dont l'image est $(\mathcal{O}/p^r)^\wedge$. □

4. Valeurs asymptotiques

Nous rassemblons ici les outils que nous utiliserons pour la démonstration du théorème 1.4.

Lemmes techniques

4.1. — Lemme. *Les deux expressions*

$$\left(1 \pm \frac{1}{\ln n}\right)^{\ln(n)/\ln\ln(n)}$$

convergent vers 1 lorsque n tend vers $+\infty$.

Démonstration — Posons $t = 1/\ln n$, la limite cherchée est

$$\lim_{t\to 0^+} (1\pm t)^{-1/(t\ln t)} = \lim_{t\to 0^+} \exp\left(-\frac{\ln(1\pm t)}{t}\frac{1}{\ln t}\right) = 1.$$

4.2. — Lemme. *Soit $n \in \mathbb{N}$ et soit ρ le nombre de facteurs premiers de n supérieurs à $\ln n$. On a la majoration*

$$\rho \leqslant \ln(n)/\ln\ln(n).$$

Démonstration — On a clairement

$$(\ln n)^\rho \leqslant \prod_{\substack{p\mid n \\ p\geqslant \ln n}} p \leqslant n.$$

En prenant les logarithmes des deux membres extrêmes, on obtient le résultat. □

Progressions arithmétiques

Pour k et l entiers premiers entre eux avec $k > 0$, on pose

$$\pi_{k,l}(x) = \sum_{\substack{p \leqslant x \\ p \equiv l \ (k)}} 1, \qquad \theta_{k,l}(x) = \sum_{\substack{p \leqslant x \\ p \equiv l \ (k)}} \ln p.$$

Le *théorème des nombres premiers* se généralise ainsi (voir par exemple [4]) :

4.3. — Théorème. *On a les relations*

$$\pi_{k,l}(x) \sim \frac{1}{\varphi(k)} \frac{x}{\ln x}, \qquad \theta_{k,l}(x) \sim \frac{x}{\varphi(k)}.$$

Pour D non carré parfait et en notant $\varepsilon(p) = (D/p)$ (pour p premier impair), nous poserons

$$\pi^+(x) = \sum_{\substack{p \leqslant x \\ \varepsilon(p)=1}} 1, \qquad \theta^+(x) = \sum_{\substack{p \leqslant x \\ \varepsilon(p)=1}} \ln p.$$

Nous utiliserons le théorème précédent sous la forme suivante :

4.4. — Théorème. *On a les relations*

$$\pi^+(x) \sim \frac{1}{2} \frac{x}{\ln x}, \qquad \theta^+(x) \sim x/2.$$

Produits partiels

Cette section est une généralisation évidente de [5]. Introduisons quelques notations : désignons par $\varepsilon(n)$ le symbole de Jacobi (D/n) (et, pour n pair, $\varepsilon(n) = 0$) et posons

$$A_+ = \prod_{\varepsilon(p)=1} \left(1 - \frac{1}{p^2}\right), \qquad A_- = \prod_{\varepsilon(p)=-1} \left(1 - \frac{1}{p^2}\right), \qquad A_0 = \prod_{p|2D} \left(1 - \frac{1}{p^2}\right),$$

de telle sorte que $\frac{A_0 A_+ A_- = 1/}{\zeta(2) = 6/\pi^2}$. On pose aussi

$$l = L(1, \varepsilon) = \prod_p \left(1 - \frac{\varepsilon(p)}{p}\right)^{-1}$$

où $L(s, \varepsilon) = \sum_{n=1}^{\infty} \varepsilon(n)/n^s$ est la L-fonction de Dirichlet associée au caractère ε. Il est connu en particulier que si $D = -1, 3$ ou 5 alors l vaut respectivement $\pi/4, \ln(7 + 4\sqrt{3})/(2\sqrt{3})$ et $-\ln(9 - 4\sqrt{5})/(2\sqrt{5})$.

Nous allons exprimer les valeurs asymptotiques des fonctions

$$P_+(x) = \prod_{\substack{p \leqslant x \\ \varepsilon(p)=1}} \left(1 - \frac{1}{p}\right), \qquad P_-(x) = \prod_{\substack{p \leqslant x \\ \varepsilon(p)=-1}} \left(1 - \frac{1}{p}\right),$$

$$Q_+(x) = \prod_{\substack{p \leqslant x \\ \varepsilon(p)=1}} \left(1 + \frac{1}{p}\right), \qquad Q_-(x) = \prod_{\substack{p \leqslant x \\ \varepsilon(p)=-1}} \left(1 + \frac{1}{p}\right),$$

à l'aide des constantes introduites ci-dessus et de

$$P_0 = \prod_{p|2D} \left(1 - \frac{1}{p}\right).$$

4.5. — Théorème. *On a les valeurs asymptotiques suivantes :*

$$P_+(x) \sim \sqrt{\frac{e^{-\gamma}}{lA_-P_0\ln x}}, \qquad P_-(x) \sim \sqrt{\frac{e^{-\gamma}lA_-}{P_0\ln x}},$$
$$Q_+(x) \sim A_+\sqrt{e^{\gamma}lA_-P_0\ln x}, \qquad Q_-(x) \sim \sqrt{\frac{e^{\gamma}A_-P_0\ln x}{l}}.$$

Démonstration — Notons tout d'abord les relations

$$P_-(x)Q_-(x) = \prod_{\substack{p\leqslant x\\ \varepsilon(p)=-1}}\left(1-\frac{1}{p}\right)\prod_{\substack{p\leqslant x\\ \varepsilon(p)=-1}}\left(1+\frac{1}{p}\right) = \prod_{\substack{p\leqslant x\\ \varepsilon(p)=-1}}\left(1-\frac{1}{p^2}\right) \sim A_-,$$

$$P_+(x)Q_-(x) = \prod_{\substack{p\leqslant x\\ \varepsilon(p)=1}}\left(1-\frac{1}{p}\right)\prod_{\substack{p\leqslant x\\ \varepsilon(p)=-1}}\left(1+\frac{1}{p}\right) = \prod_{p\leqslant x}\left(1-\frac{\varepsilon(p)}{p}\right) \sim 1/l. \tag{6}$$

On en déduit

$$\frac{P_-(x)}{P_+(x)} = \frac{P_-(x)Q_-(x)}{P_+(x)Q_-(x)} \sim lA_-.$$

Les valeurs asymptotiques de $P_+(x)$ et $P_-(x)$ s'obtiennent alors facilement en remarquant que, par la formule de Mertens (voir par exemple [2]), on a

$$P_0P_+(x)P_-(x) \sim \frac{e^{-\gamma}}{\ln x}.$$

Ensuite, l'équation (6) permet de calculer la valeur asymptotique de $Q_-(x)$. Pour déterminer celle de $Q_+(x)$, remarquons que

$$P_+(x)P_-(x)Q_+(x)Q_-(x) \sim A_+A_-,$$

et donc, par (6),

$$P_-(x)Q_+(x) \sim lA_+A_-.$$

ce qui permet de conclure. □

5. Démonstration du théorème 1.4

Limite inférieure

Nous commençons par minorer $\varphi_D(n)e^{\gamma/2}\sqrt{\ln\ln n}/n$ par une suite ayant $1/\sqrt{lA_-P_0}$ pour limite, puis nous extrairons une sous-suite convergeant vers $1/\sqrt{lA_-P_0}$.

• On a

$$\frac{\varphi_D(n)}{n} = \prod_{\substack{p\mid n\\ p>\ln n}}\left(1-\frac{\varepsilon(p)}{p}\right)\prod_{\substack{p\mid n\\ p\leqslant\ln n}}\left(1-\frac{\varepsilon(p)}{p}\right)$$
$$\geqslant \left(1-\frac{1}{\ln n}\right)^{\rho}\prod_{\substack{p\leqslant\ln n\\ \varepsilon(p)=1}}\left(1-\frac{1}{p}\right)$$

où ρ est le nombre de facteurs premiers de n supérieurs à $\ln n$. Mais puisque, d'après 4.2 nous avons $\rho\leqslant\ln(n)/\ln\ln(n)$, nous obtenons :

$$\frac{\varphi_D(n)}{n}e^{\gamma/2}\sqrt{\ln\ln n} \geqslant e^{\gamma/2}\sqrt{\ln\ln n}\prod_{\substack{p\leqslant\ln n\\ \varepsilon(p)=1}}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{\ln n}\right)^{\ln(n)/\ln\ln(n)}.$$

D'après 4.1, le dernier facteur de cette majoration tend vers 1 et, d'après 4.5, le facteur restant tend vers $1/\sqrt{lA_-P_0}$. Le tout converge donc vers $1/\sqrt{lA_-P_0}$, ce qui termine la démonstration du premier point.

• Posons

$$n_k^+ = \prod_{\substack{p\leqslant k\\ \varepsilon(p)=1}} p$$

de telle sorte que $\ln n_k^+ = \theta^+(k)$. On a

$$\frac{\varphi_D(n_k^+)}{n_k^+} = \prod_{p|n_k^+}\left(1-\frac{1}{p}\right) = \prod_{\substack{p\leqslant k\\ \varepsilon(p)=1}}\left(1-\frac{1}{p}\right).$$

Donc, d'après 4.5,

$$\begin{aligned}\frac{\varphi_D(n_k^+)}{n_k^+}e^{\gamma/2}\sqrt{\ln\ln n_k^+} &= \frac{\varphi_D(n_k^+)}{n_k^+}e^{\gamma/2}\sqrt{\ln k}\sqrt{\frac{\ln\theta^+(k)}{\ln k}}\\ &= \prod_{\substack{p\leqslant k\\ \varepsilon(p)=1}}\left(1-\frac{1}{p}\right)e^{\gamma/2}\sqrt{\ln k}\sqrt{\frac{\ln\theta^+(k)}{\ln k}}\\ &\sim \frac{1}{\sqrt{lA_-P_0}}\end{aligned}$$

puisque, au voisinage de $+\infty$,

$$\ln\theta^+(x) \sim \ln\frac{x}{2} \sim \ln x.$$

Ainsi s'achève la démonstration du deuxième point. □

Limite supérieure

• Par les mêmes méthodes, nous obtenons

$$\frac{\varphi_D(n)e^{-\gamma/2}}{n\sqrt{\ln\ln n}} \leqslant \frac{e^{-\gamma/2}}{\sqrt{\ln\ln n}} \prod_{\substack{p\leqslant \ln n\\ \varepsilon(p)=-1}}\left(1+\frac{1}{p}\right)\left(1+\frac{1}{\ln n}\right)^{\ln(n)/\ln\ln(n)}.$$

D'après 4.1 et 4.5, le membre de droite converge vers $\sqrt{\frac{A_-P_0}{l}}$.

• En posant

$$n_k^- = \prod_{\substack{p\leqslant k\\ \varepsilon(p)=-1}} p,$$

le second point de la démonstration est semblable à celui du théorème précédent ; il suffit de considérer cette fois-ci la sous-suite

$$\frac{\varphi_D(n_k^-)e^{-\gamma/2}}{n_k^-\sqrt{\ln\ln n_k^-}}$$

et de montrer qu'elle est équivalente à $Q_-(k)e^{-\gamma/2}/\sqrt{\ln k}$ et donc qu'elle converge vers $\sqrt{\frac{A_-P_0}{l}}$. □

6. Bibliographie

[1] F. Arnault : *The Rabin-Monier theorem for Lucas pseudoprimes.* To appear in Mathematics of Computation.

[2] G.H. Hardy, E.M. Wright : *An Introduction to the Theory of Numbers (5th edition).* Clarendon Press, 1960–1979.

[3] P. Ribenboim : *The Book of Prime Number Records.* Springer-Verlag, 1988.

[4] A. Selberg : *An elementary proof of the prime-number theorem for arithmetical progressions.* Canadian Journal of Mathematics, vol. 2, pp. 66–78, 1950.

[5] S. Uchiyama : *On some products involving primes.* Proceedings of the American Mathematical Society, vol. 28, pp. 629–630, 1971.

LACO (Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation)
Département de Mathématiques
123, avenue Albert Thomas, 87060 Limoges Cedex
E-Mail : arnault@unilim.fr, robin@cict.fr