Chapitre 5

Eléments de Théorie des Groupes et Nombres

Dans ce chapitre nous allons poser le problème de Simon dans un cadre beaucoup plus général qui nous permettra de voir qu'il fait partie d'une classe plus vaste d'algorithmes qui permettent de découvrir les symétries cachées d'une structure mathématique. Nous verrons que la factorisation des entiers naturels peut être ramenée à un problème de recherche de symétrie : notamment la période d'une fonction arithmétique.

5.1 Groupes abéliens et classes d'équivalence

Soit $G = \{g_1, g_2, \ldots, g_M\}$ un groupe fini à M éléments. L'opération de groupe sera notée multiplicativement, c'est-à-dire si g et $g' \in G$ alors $gg' \in G$. Celle-ci est associative $(gg')g'' = g(g'g'')$; il existe un élément neutre $e\, g = g\, e = g$; chaque élément possède un unique inverse $gg^{-1} = g^{-1}g = e$. De plus nous nous limiterons aux groupes commutatifs (ou abéliens) $gg' = g'g$.

Soit $H \subset G$ un sous-groupe de G. C'est-à-dire que H est lui-même un groupe. En particulier si $h, h' \in H$ alors $hh' = h'h \in H$; lélément neutre $e \in H$. On peut facilement voir que ces deux propriétés suffisent pour donner á H la structure de sous-groupe. En particulier $\{e\}$ et G lui même sont toujours des sous-groupes de G (appelés triviaux). Dans ce qui suit nous supposons qu'il existe un sous groupe non-trivial.

Fixons maintenant G un groupe commutatif et H un sous groupe. Pour chaque élément $g \in G$ on peut définir la *classe d'équivalence de* g comme suit,

$$E_g = \{gh | h \in H\}\,.$$

Il s'agit de l'ensemble des éléments obtenus par l'action de H sur g. Notez

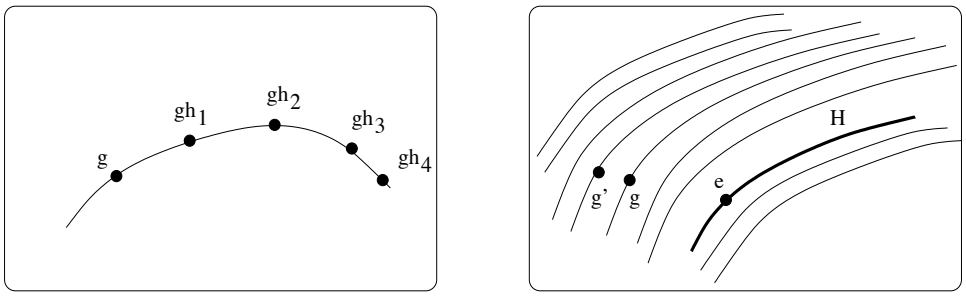

FIG. 5.1 – Gauche : orbite ou classe d'équivalence de g sous l'action du groupe H. Droite : partition ou feuilletage du groupe G en classes d'équivalences distinctes. Le sous groupe H est la classe de l'élement neutre e.

que dans le cas commutatif H peut agir à droite comme à gauche puisque $hg = gh$. Il est commode de visualiser E_g comme une *trajectoire* ou *orbite* obtenue quand H agit sur g (figure 5.1). On notera que la classe d'équivalence de lélément neutre e est H lui-même.

Prenons $g \neq g'$. On peut montrer que, de deux choses, l'une est réalisée

$$E_g = E_{g'} \qquad \text{ou bien} \qquad E_g \cap E_{g'} = \emptyset.$$

Cette propriété fondamentale constitue en fait le théorème de Lagrange (voir ci-dessous), et implique que les classes d'équivalence forment une partition ou un feuilleutage de G (voir figure 5.1. Chaque classe possède $|H|$ (la cardinalité de H) éléments et le nombre total de classes disjointes est $\frac{|G|}{|H|}$ (La cardinalité de G divisée par celle de H). L'ensemble des classes d'équivalences est noté G/H (cette notation est justifiée par le feuileutage de G par H).

Remarque : la représentation graphique des classes déquivalence grâce aux orbites est utile mais il ne faut pas forcément la prendre à la lettre. Ces orbites n'ont pas nécessairement quelque chose à voir avec des vraies trajectoires unidimensionnelles.

Théorème de Lagrange.

i) Soit g et $g' \in G$. Alors on a uniquement deux possibilités $E_g = E_{g'}$ ou bien $E_g \cap E_{g'} = \emptyset$.

ii) $\left|G/H\right| = \frac{|G|}{|H|}$. En particulier la cardinalité d'un sous groupe divise toujours celle du groupe.

Démonstration. Fixons g et $g' \in G$. Si $E_g \cap E_{g'} = \emptyset$ la preuve de i) est finie. Si $E_g \cap E_{g'} \neq \emptyset$ alors il existe un élément commun, appelons le $\bar{g}$. Puisque $\bar{g} \in E_g$, il existe h tel que $\bar{g} = gh$. D'autre part puisque $\bar{g} \in E_{g'}$, il existe h' tel que $\bar{g} = g'h'$. Donc $gh = g'h'$ et $g = g'(h'h^{-1})$ ce qui signifie $g \in E_{g'}$.

Mais comme on peut faire le raisonnement pour tous les éléments g de E_g on obtient $E_g \subset E_{g'}$. De même $g' = g(hh'^{-1})$ donc $g' \in E_g$ ce qui implique $E_{g'} \subset E_g$. On conclut que $E_g = E_{g'}$ ce qui achève la preuve de i).

Pour montrer ii) il suffit de remarquer que la cardinalité de claque classe d'équivalence est $|H|$. En effet $E_g = \{hg | h \in H\}$ et tous les éléments générés par l'action de H sont distincts (puisque si $gh_1 = gh_2$ alors $h_1 = h_2$, et donc, si $h_1 \neq gh_2$ alors $gh_1 \neq gh_2$). Ainsi on a :

$$|G| = |H| \times (\text{Nombre de classes d'équivalence})$$

ce qui est équivalent à

$$\left|{}^{G}\!/_{H}\right| = \frac{|G|}{|H|}.$$

Puisque le nombre de classes d'équivalences ${}^{G}\!/_{H}$ est nécessairement entier il faut que $|H|$ divise $|G|$. Cela achéve la démonstaration de ii).

Remarque : La loi de groupe induit une structure de groupe sur l'ensemble des classes d'équivalence. L'ensemble ${}^{G}\!/_{H}$ possède lui-même une structure de groupe. Nous ne nous attardons pas sur cette propriété qui ne sera pas utilisée par la suite. Néanmoins, le lecteur peut la vérifier dans chacun des exemples ci-dessous.

5.2 Exemples

Exemple 1. $G = \mathbb{F}_2^n$ l'espace vectoriel sur le corps $\mathbb{F}_2$ des vecteurs à n composantes binaires. En particulier, c'est un groupe pour l'addition $\oplus$ mod 2. Dans le problème de Simon on a $H = \{0, \vec{a}\}$ qui est un sous-groupe à deux éléments. On a : $|G| = 2^n$, $|H| = 2$ et $\left|{}^{G}\!/_{H}\right| = 2^{n-1}$. Il y a 2^{n-1} classes d'équivalence donnée par les paires $\{\vec{x}, \vec{y}\}$ tel que $\vec{x} = \vec{y} + \vec{a}$. Ici l'orbite de $\vec{y}$ est $\{\vec{y} + \vec{0} = \vec{y}, \vec{y} + \vec{a}\}$.

Exemple 2. La généralisation immédiate du cas précédent est de prendre $H =$ un sous-espace vectoriel de $\mathbb{F}_2^n$ de dimension k. C'est un sous-groupe de $\mathbb{F}_2^n$ pour l'addition $\oplus$ mod 2. Puisque la dimension du sous-espace vectoriel est k on peut trouver k vecteurs de base $\vec{h_1}, \ldots, \vec{h_k}$ et tout élément de H s'écrit comme :

$$\alpha_1 \vec{h_1} \oplus \alpha_2 \vec{h_2} \oplus \cdots \oplus \alpha_k \vec{h_k}$$

avec $\alpha_i \in \{0, 1\}$. Le sous-groupe possède donc 2^k éléments. Le nombre de classes d'équivalence est $\left|{}^{G}\!/_{H}\right| = 2^{n-k}$. Celles-ci correspondent aux "hyper-

plans" parallèles à H. Soit $\vec{x} \in \mathbb{F}_2^n$, non nul. Son orbite (ou sa classe d'équivalence) est l'ensemble des vecteurs

$$\vec{x} \oplus \alpha_1 \vec{h_1} \oplus \alpha_2 \vec{h_2} \oplus \cdots \oplus \alpha_k \vec{h_k}$$

ou $\alpha_i \in \{0,1\}$, $i = 1, \cdots, k$.

Exemple 3 Soit $G = (\mathbb{Z}, +)$ les entiers (positifs et négatifs) munis de l'addition ordinaire et soit $H = r\mathbb{Z}$ les multiples de r (r un entier quelconque). Deux entiers x et y sont équivalents si $x = y + qr$ c'est-à-dire si $x - y = 0 \mod r$. Donc les classes d'équivalence sont les entiers $\mod r$ c'est-à-dire

$$\mathbb{Z}/_{r\mathbb{Z}} = \{0, 1, 2, 3, \ldots, r-1\}$$

L'orbite d'un élément x est

$$\{x + qr, q \in \mathbb{Z}\}$$

Ici G et H sont infinis donc la formule $\frac{|G|}{|H|}$ a un sens formel, mais, il y a r classes d'équivalence. Par exemple, si $r = 2$ il y en a 2 : ce sont les entiers pairs (0 inclus) et impairs. On peut prendre $\{0, 1\}$ pour leur représentants. Si $r = 3$ il y a 3 classes d'équivalence représentées par $\{0, 1, 2\}$.

Exemple 4. Dans l'exemple précédent les groupes G et H étaient infinis. Ce sera l'exemple relevant dans la suite, mais nous voudrons travailler avec des groupes finis (car le nombre de bits manipulé est toujours fini). Nous remplacerons donc $\mathbb{Z}$ par $G = \mathbb{Z}/_{M\mathbb{Z}} = \{0, 1, 2, \ldots, M-1\}$ muni de l'addition modulo M. L'idée est que pour M très grand ce groupe ce comporte essentiellement comme $\mathbb{Z}$; tant qu'on s'interesse aux entiers $\ll M$, et il a l'avantage d'être fini. Soit maintenant r un diviseur de M. Alors les multiples de r contenus dans $\{0, 1, 2, \ldots, M-1\}$ forment un sous-groupe appelé H et à nouveau $G/_H = \mathbb{Z}/_{r\mathbb{Z}}$ les entiers modulo r.

Remarque importante : si r n'est pas un diviseur de M les multiples de r inférieurs à M ne forment pas un sous-groupe de $\mathbb{Z}/_{M\mathbb{Z}}$. En effet $(qr + q'r) = s \mod M$ n'est pas un multiple de r. Pour le voir on note que si c'était le cas on aurait

$$qr + q'r = s + kM$$

avec s multiple de r. Alors on aurait $qr + q'r - s = kM$ un multiple de r. On peut toujours prendre q et q' (pas trop grands) tels que $k = 1$. et alors il faudrait que M soit un multiple de r (contradiction). En conclusion, pour que H soit un sous-groupe, il faut que r divise M . On arrive à la même conclusion grâce au théorème de Lagrange. En effet, si $G/_H = \frac{|G|}{|G/_H|} = \frac{M}{r}$ et

pour que $|H|$ soit entier il faut que r divise M. Notons finalement que pour chaque diviseur de M on obtient un sous-groupe.

Exemple 5 L'exemple précédent est équivalent au suivant. Soit $G = \{$rotations d'angle $\frac{2\pi}{M}$autour du cercle$\}$. Ce groupe est isomorphe aux entiers modulo M (c'est-à-dire $\mathbb{Z}/M\mathbb{Z}$). Soit r qui divise M et soit $H_r = \{$rotations d'angle $r \cdot \frac{2\pi}{M}\}$ est un sous-groupe. Par exemple si $M = 6$ et $r = 2$ on a explicitement,

$$G/H_{r=2} = \left\{(0,\pi), (\frac{2\pi}{6}, \frac{8\pi}{6}), (\frac{4\pi}{6}, \frac{10\pi}{6})\right\}$$

$$G/H_{r=3} = \left\{((0, \frac{4\pi}{6}, \frac{8\pi}{6}), (\frac{2\pi}{6}, \frac{6\pi}{6}, \frac{10\pi}{6})\right\}$$

Dans le premier cas il y a trois classes d'équivalence constituée de deux élements. Dans le deuxième, il y a deux classes contenant trois éléments.

5.3 Problème du sous-groupe caché

Nous sommes maintenant prêts pour formuler une généralisation du problème de Simon. Soit G un groupe commutatif et $H \subset G$ un sous-groupe. On dispose d'un oracle qui sait calculer une fonction :

$$\begin{aligned} f :& G \to X \\ & g \mapsto f(g) \end{aligned}$$

telle que f soit constante sur chaque classe d'équivalence et prend $\left|G/H\right|$ valeurs. Le lien avec les notations du chapitre 4 est $|X| = \left|G/H\right|$ et $f(g_1) = f(g_2)$ *si et seulement si* $g_1 g_2^{-1} \in H$ (avec la notation additive cela signifie $g_1 + (-g_2)$). Le problème est de découvrir le sous-groupe caché H en posant le moins de questions possible à l'oracle.

Pour $G = (\mathbb{F}_2^n, \oplus)$ et H un sous-espace vectoriel de dimension k nous avons présenté un algorithme quantique de complexité polynomiale qui permet de trouver H (chap 4). Il existe une généralisation au cas des groupes commutatifs. Celle-ci passe par la notion de transformée de Fourier générale sur les groupes finis, que nous n'abordons pas explicitement dans ce cours. Le cas des groupes non-commutatifs est en général un problème ouvert important.

Le cas particulier qui nous interessera est $G = \mathbb{Z}/M\mathbb{Z}$ (M *très* grand). Ce cas est important car il mène de façon naturelle à l'algorithme de Shor pour la factorisation des entiers.

5.4 La période d'une fonction

Considérons le problème suivant. Soit $f : \mathbb{Z} \to \mathbb{Z}$ une fonction périodique de période r, sur les entiers $x \mapsto f(x)$. On a

$$f(x+r) = f(x) \quad \forall x \in \mathbb{Z}$$

où r est le plus petit entier satisfaisant l'équation. Nous supposons que r est inconnu mais qu'un oracle nous retourne les valeurs de $f(x)$ quand on lui soumet l'entier x. Le problème est de déterminer la période r en posant le moins de questions possibles à l'oracle. Si r est *très grand* ce problème est difficile à priori car il faudra soumettre à l'oracle environ r questions. C'est-à-dire que la complexité du calcul est en gros $r = \mathrm{O}\left(2^{\log_2 r}\right)$ où $\log_2 r$ représente est le nombre de bits nécessaires pour représenter r. C'est á dire que la complexité est exponentielle dans la taille de r. Nous verrons qu'un algorithme quantique apparenté à celui de Simon requiert une complexité polynomiale.

Quel est le lien avec le problème du sous-groupe caché ? Ici $G = \mathbb{Z}$ et $H = r\mathbb{Z}$. Alors f satisfait.

$$f(x) = f(y) \text{ si et seulement si } x - y \in r\mathbb{Z}.$$

En d'autres termes f est constant sur les classes d'équivalence G/H (voir figure 5.4). Comme nous devons travailler avec des groupes finis nous devons tronquer $G = \mathbb{Z}$ à un grand entier M. Pour préserver la structure de groupe il faut en principe prendre pour M un grand multiple de r, et $G = \mathbb{Z}/M\mathbb{Z}$ et $H = \{\text{multiples de } r \text{ inférieurs à } M\}$. Puisque r est en fait inconnu, il nous est difficile de bien choisir M pour qu'il soit un grand multiple de r. Comme nous le verrons, en pratique nous choisirons M grand mais pas nécessairement multiple de r. Cela va détruire la structure de groupe (voir figure 5.4). Néanmoins si $M \gg r$ celle-ci est *approximativement préservée*. En effet il existe $k \in \{0, 1, \ldots, r-1\}$ tel que $M + k$ avec soit multiple de r. La correction k est plus petite que r et est donc négligeable par rapport à M. Quelques ennuis techniques vont compliquer légèrement les calculs mais essentiellement l'algorithme quantique de la détermination de la période de f sera similaire à celui de Simon.

5.5 La factorisation des entiers

Le théorème fondamental de l'arithmétique nous assure que tout entier N peut être décomposé de façon unique en un produit de nombres premiers.

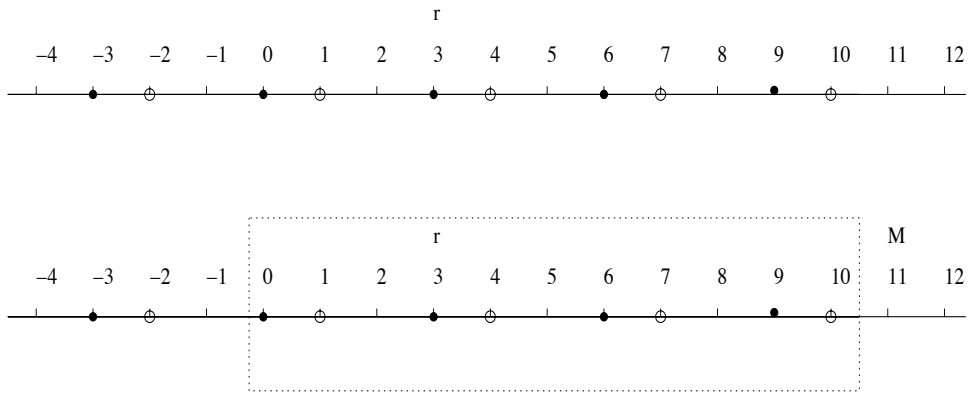

FIG. 5.2 – Haut : le groupe $(\mathbb{Z}, +)$ et le sous goupe $H = 3\mathbb{Z}$. Il y a 3 classes d'équivalences : les nombres $\equiv 0 \mod 3$; $\equiv 1 \mod 3$; $\equiv 2 \mod 3$. Bas : le groupe fini $\mathbb{Z}/_{11\mathbb{Z}}$. Les multiples de 3 inférieurs à 11 ne forment pas un sous-groupe. Par exemple 3 et 9 sont multiples de 3, mais $3+9 = 12 \equiv 1 \mod 11$ n'est pas multiple de 3.

Étant donné les facteurs de N, il est facile de vérifier que le produit de ces facteurs redonne N. Plus précisément supposons que $N = p \cdot q$ avec p et q deux nombres premiers à $\mathrm{O}(b)$ bits. Si p et q sont connus, la vérification $N = p \cdot q$ peut se faire facilement avec $\mathrm{O}(b^2)$ opérations. Par contre étant donné un entier général N avec $\mathrm{O}(b)$ bits on ne connaît pas d'algorithme polynomial permettant de calculer p et q (on ne sait même pas s'il en existe un ou non). On connaît plusieurs algorithmes plus rapides que $\mathrm{O}\left((1+\epsilon)^b\right)$ pour tout $\epsilon > 0$. Le meilleur algorithme connu possède un temps de calcul $\mathrm{O}\left(\exp(\frac{64}{9}b)^{\frac{1}{3}}(\log b)^{\frac{2}{3}}\right)$. Concrètement un des records[1] de factorisation atteint le 12 décembre 2009 pour un nombre à 232 décimales (b=768 bits) a utilisé des centaines de processeurs sur deux années de calcul.

Comme nous le verrons plus tard, l'algorithme de Shor permet une factorisation en temps polynomial avec un circuit quantique de taille polynomiale. L'algorithme de Shor résoud en fait un autre problème de théorie des nombres appelé *la recherche de l'ordre*. Il est connu depuis 1976 (environ) que la factorisation peut se réduire à la recherche de l'ordre. C'est l'objet de ce paragraphe.

Soit $N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ avec $p_i \neq 2$ et $k \geq 2$. En d'autres termes N ne contient pas de puissance de 2 et N n'est pas la puissance d'un nombre premier unique ($N \neq p^e$). Notez que les puissances de 2 sont aisément extraites car il est facile de voir si un entier et pair et de diviser par 2. De plus si

[1] Voir `http://en.wikipedia.org/wiki/RSA_numbers#RSA-768`

$N = p^e$ il existe une méthode efficace pour trouver p et e.

Algorithme de factorisation basé sur la recherche de l'ordre.

a. Choisir aléatoirement uniformément $a \in \{2, \cdots, N-1\}$ et calculer

$$d = \mathrm{PGCD}\,(a, N)$$

grâce à l'algorithme d'Euclide (de complexité $O((\log_2 N)^3)$).

b. Si $d > 1$ nous avons un facteur non-trivial de N car $d|N$, (d divise N). On garde ce facteur et on retourne à a.

c. Si $d = 1$ (c'est-à-dire que a et N sont premiers entre eux) on calcule *le plus petit* entier r tel que

$$a^r = 1 \mod N.$$

Cet entier s'appelle *l'ordre de* $a \mod N$ aussi noté $r = \mathrm{Ord}_N(a)$. *Pour cette étape on ne connaît pas d'algorithme classique polynomial. C'est l'étape qui sera traitée par l'algorithme de Shor.*

d. Supposons que r soit impair. Output `Fail` et retourner à a.

e. Si r est pair alors on sait que

$$a^r - 1 = \left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right)$$

Notez que N divise $a^r - 1$. Donc il y a a priori 3 possibilités :

e1. N divise $a^{\frac{r}{2}} - 1$. Ceci est en fait impossible car alors on aurait $a^{\frac{r}{2}} = 1 \mod N$ et $\frac{r}{2}$ serait l'ordre.

e2. N divise $a^{\frac{r}{2}} + 1$. C'est-à-dire $a^{\frac{r}{2}} = -1 \mod N$. Output `Fail` et retourner à a.

e3. N partage des facteurs non-triviaux avec $a^{\frac{r}{2}} - 1$ et $a^{\frac{r}{2}} + 1$. Par exemple si $N = pq$ il faut que $p|(a^{\frac{r}{2}} - 1)$ et $q(|a^{\frac{r}{2}} + 1)$ ou vice versa. En d'autres termes

$$d_\pm = \mathrm{PGCD}\left(a^{\frac{r}{2}} \pm 1, N\right)$$

sont non-triviaux $d_+ > 1$ et $d_- > 1$ et nous avons 2 facteurs non-triviaux de N. Ceux-ci sont calculés grâce à l'algorithme d'Euclide (Complexité $\mathrm{O}\left((\log_2 N)^3\right)$).

f. Vérifier si le produit des facteurs trouvés dans les étapes précédentes vaut N. Si ce n'est pas encore le cas retourner à a.

Nous voyons qu'en présence d'un oracle qui permettrait résoudre l'étape c. la complexité d'une expérience (un round) provient uniquement de l'algorithme d'Euclide qui est $\mathrm{O}\,(b^3)$. Néanmoins cette expérience est probabiliste

(étape a) et nous devons nous assurer que la probabilité de succès est non-négligeable. En fait on peut prouver Prob (succès) $\leq \frac{3}{4}$. Cela implique qu'avec $T = \frac{|\ln \epsilon|}{|\ln 2|}$ expériences (rounds) on peut amplifier cette probabilité de succès à Prob (succès en T rounds) $\geq 1 - \epsilon$.

Lors d'un round les seuls output `Fail` interviennent en d. et e2. Cela correspond à l'évènement

$$(r \text{ est impair}) \text{ ou } (a^{\frac{r}{2}} = -1 \mod N)$$

Ainsi

$$\text{Prob (échec)} = \text{Prob}\left((r \text{ est impair}) \text{ ou } (a^{\frac{r}{2}} = -1 \mod N)\right)$$

.

Théorème. Soit a pris uniformément aléatoirement dans $2, \cdots, N-1$. Soit r les plus petit entier satisfaisant à $a^r = 1 \mod N$. Alors Prob (échec) $\leq \frac{1}{4}$.

Nous ne donnons pas de preuve ici. Ce théorème assure que la probabilité de succès de l'algorithme de factorisation basé sur la recherche de l'ordre est d'au moins $\frac{3}{4}$ lors d'un seul round. En faisant des ronds successifs il est possible d'amplifier cette probabilité à $1 - \epsilon$ ($\epsilon \ll 1$). Comme d'habitude le nombre de rounds requis est de l'ordre de O ($|\ln \epsilon|$).

5.6 Fractions continues

Dans ce paragraphe nous donnons, sans démonstration, quelques résultats de théorie des nombres, utiles pour le développement ultérieur de l'algorithme de Shor.

Tout nombre réel peut être développé en *fraction continue*. Commençons par décrire ce processus pour les *fractions rationnelles*, sur un exemple. Soit $x = \frac{263}{189}$. Les étapes succesives de l'algorithme d'Euclide du calcul du PGCD $(263, 189)$ sont :

$$\begin{aligned} 263 &= 1 \cdot 189 + 74 \\ 189 &= 2 \cdot 74 + 41 \\ 74 &= 1 \cdot 41 + 33 \\ 41 &= 1 \cdot 33 + 8 \\ 33 &= 4 \cdot 8 + 1 \end{aligned}$$

On voit que PGCD $(263, 189) = 1$. Étant donné qu'à chaque fois on divise par un nombre ≥ 2 le nombre d'étapes (de lignes ci-dessus) est de l'ordre de

$\log_2(263)$, c'est-à-dire $\log_2(N)$ en général. De plus, chaque division requiert $\mathrm{O}\left((\log_2 N)^2\right)$ opérations. Donc le nombre total d'opérations pour l'algorithme d'Euclide est $\mathrm{O}\left((\log_2 N)^3\right)$. Maintenant, pour obtenir le *développement en fraction continue*, on procède de la sorte :

$$\frac{263}{189} = 1 + \frac{74}{189} = 1 + \frac{1}{\frac{189}{74}} = 1 + \frac{1}{2 + \frac{41}{74}}$$

$$= 1 + \frac{1}{2 + \frac{1}{\frac{74}{41}}} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{33}{41}}}$$

$$= 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{41}{33}}}}$$

$$= 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{8}{33}}}}$$

$$= 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{33}{8}}}}}$$

$$= 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{4 + \frac{1}{8}}}}}$$

On dit que le développement en fraction continue est

$$\frac{263}{189} = [1; 2; 1; 1; 4; 8]$$

La forme générale du développement est :

$$x = [a_0; a_1; \cdots; a_n]$$

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Si $x > 1$ on a $a_0 \geq 1$ et si $x < 1$ on a $a_0 = 0$. De plus, ce développement n'est pas unique car on peut toujours écrire le dernier terme $\frac{1}{a_n}$ comme $\frac{1}{(a_n - 1) + \frac{1}{1}}$. Ainsi

$$x = [a_0; a_1; \cdots a_{n-1}; a_n] = [a_0; a_1; \cdots; a_{n-1}; a_n - 1; 1]$$

Mais à cette ambigüité près le développement est unique. De plus on peut le rendre unique en déclarant que l'on choisit toujours le développement le plus court possible. Le nombre d'opérations requises est le même que pour l'algorithme d'Euclide, $\mathrm{O}\left((\log_2 N)^3\right)$ ou $N = \max(\text{numérateur, dénominateur})$. La longueur du développement est $\mathrm{O}\left((\log_2 N)\right)$.

Un tel développement peut être étendu aux nombres *irrationnels* comme suit. Soit x irrationnel. On peut toujours écrire $x = a_0 + \beta$ avec $a_0 \in \mathbb{N}$ et $0 < \beta < 1$. On écrit

$$x = a_0 + \frac{1}{1/\beta}$$

Maintenant $1/\beta = a_1 + \gamma$ avec $a_1 \in \mathbb{N}$ et $0 < \gamma < 1$. On itère :

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{1/\gamma}}$$

Cela donne en général un développement

$$x = [a_0; a_1; a_2; \cdots]$$

infini. Si x est rationnel le développement s'arrête et est donc fini comme avant.

Définition : notion de convergent. Soit $x = [a_0; a_1; a_2; \cdots; a_n; \cdots]$ un développement en fraction continue de x. On appelle *convergents* les séries tronquées $[a_0; a_1; a_2; \cdots; a_n]$. Ces convergents sont des nombres rationnels

$$[a_0; a_1; a_2; \cdots; a_n] = \frac{p_n}{q_n}$$

et on a $\lim \frac{p_n}{q_n} = x$. Si x est irrationnel il faut prendre $n \to +\infty$ pour atteindre la limite ; alors que si x est rationnel celle-ci est atteinte pour n fini ($\approx \log_2 N$).

Théorème : propriétés des convergents. Soit p_n/q_n les convergents de x. Alors

a) $\mathrm{PGCD}\,(p_n, q_n) = 1$ (p_n et q_n sont premiers entre eux).

b) $\left|x - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2}$ (les convergents forment de bonnes approximations de x).

c) Si x est rationnel toutes les approximations de la forme p/q avec p et q premiers entre eux et tels que $\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$ sont données par l'ensemble des convergents de x. On peut donc calculer ces approximations de facon systématique.

d) Si x est irrationnel on a une infinité de convergents. Ceux-ci donnent les meilleures approximations rationnelles au sens suivant :

$$\left|x - \frac{p_n}{q_n}\right| < \left|\frac{p}{q} - x\right|$$

pour toute fraction $\frac{p}{q} \neq \frac{p_n}{q_n}, 0 < q \leq q_n$ (si $n \geq 2$ et p, q premiers entre eux).

Pour nous, c'est la propriété c) qui sera utile dans l'analyse de l'algorithme de Shor. Donnons un exemple illustrant d). Le développement en fraction continue de π commence par

$$\pi = [3; 7; 15; 1; 292; 1; 1; \ldots]$$

Le convergent

$$\frac{p_4}{q_4} = [3; 7; 15; 1; 292] = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292}}}} = \frac{355}{113}$$

est déjà une bonne approximation. D'apres le théorème on a $\left|\pi - \frac{355}{113}\right| \leq \frac{1}{(113)^2} \approx 10^{-4}$. En fait on peut vérifier $\left|\pi - \frac{355}{113}\right| \approx 0.26 \cdot 10^{-6}$.

Exercice : Donnez la liste de tous les convergents de $x = \frac{263}{189}$ et vérifiez les affirmations a, b, c du théorème..

5.7 Fonction d'Euler

Pour un entier $r > 2$ on dit que $a \in \{1, 2, 3, \ldots, r-1\}$ est premier avec r (a is coprime with r) si $\mathrm{PGCD}\,(a, r) = 1$. Le nombre de tels entiers a est donné par $\varphi(r)$, la *fonction d'Euler*. Si N est premier, $N = p$ on a bien sur : $a = 1, 2, 3, \ldots, p-1$ et $\varphi(p) = p - 1$. En général on montre que si

$$N = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

est la décomposition (unique) en facteurs premiers de N,

$$\begin{aligned} \varphi(N) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \ldots \varphi(p_k^{e_k}) \\ &= p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \ldots p_k^{e_k-1}(p_k - 1) \end{aligned}$$

Exemple. Si $N = 9$ les a premiers avec N sont $a = 1, 2, 4, 5, 7, 8$ et donc $\varphi(9) = 6$. On vérifie $\varphi(9) = 3^{2-1}(3-1) = 6$

L' inégalité suivante (valable pour r assez grand) sera utile pour nous :

$$\varphi(r) \geq \frac{r}{4 \ln \ln r}$$

Le dénominateur $\ln \ln r$ croît très lentement : en première approximation on peut y penser comme étant un nombre $O(1)$. Par exemple pour $r = 10^{1000}$ (ce qui représente un nombre à 1000 dècimales) on a $\ln \ln r = \ln(1000 \ln 10) = 3 \ln 10 + \ln \ln 10 \leq 8$. En d'autre termes, étant donné r, une fraction appréciable des $r - 1$ nombres inférieurs sont premiers avec r (dans l'exemple cette fraction est supérieure à $1/32$). Cette propriété peut être ré-exprimée comme suit. Fixons r et tirons $k \in \{1, 2, \ldots, r\}$ au hasard, uniformément, (c.a.d avec probabilité $\frac{1}{r}$. Alors :

$$\mathrm{Prob}\,(\mathrm{PGCD}\,(k, r) = 1) = \frac{\varphi(r)}{r} \geq \frac{1}{4(\ln \ln r)}$$

Le membre de droite de l'inégalité décroît trés lentement : on pourra y penser comme étant $O(1)$.