Chap 3. Intermède Mathématique : Théorie des Groupes et des 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 symétries (notamment la période d'une fonction).

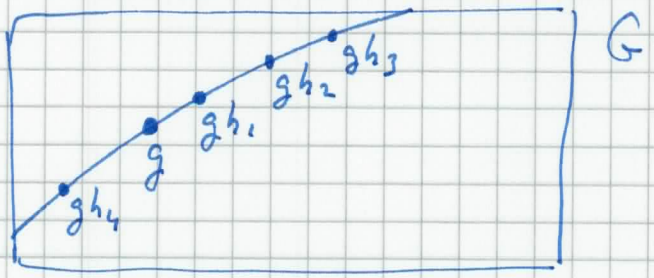
3.1. Groupes Abéliens et classes d'équivalences.

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

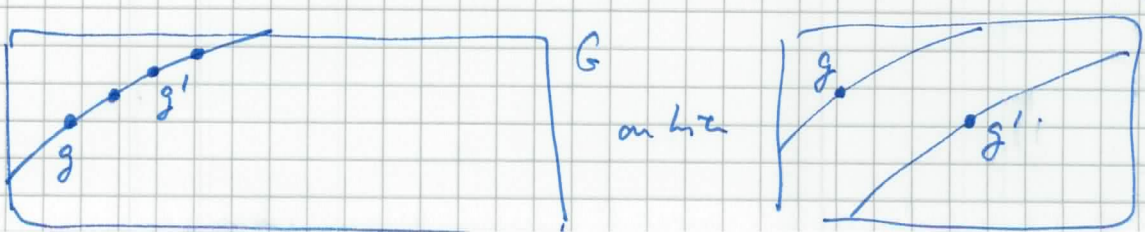
Soit $H \subset G$ un sous-groupe de G. C'est à dire que H est lui-même un groupe et si $h, h' \in H$ alors $hh' = h'h \in H$. Pour chaque élément $g \in G$ on peut définir "sa classe d'équivalence" comme suit :

$$E_g = \{ gh \mid h \in H \}$$

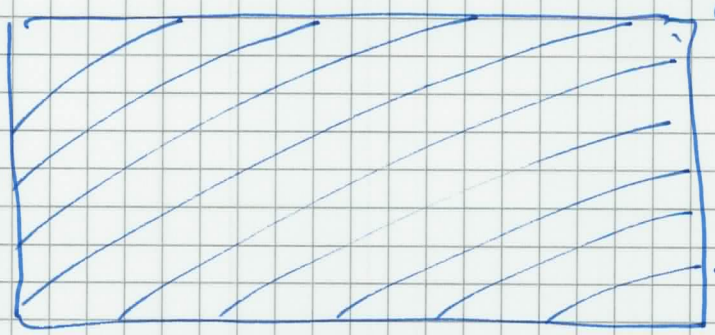
Il s'agit de l'ensemble des éléments obtenus par l'action de H sur g. Notez que dans le cas commutatif H peut agir à droite comme à gauche puisque $gh = hg$. Il est commode de visualiser E_g comme une "trajectoire" ou "orbite" obtenue quand H agit sur g (figure 1).



Prenons $g \neq g'$. On peut montrer que de deux choses l'une : $E_g = E_{g'}$ ou bien $E_g \cap E_{g'} = \emptyset$ (figure 2).



Cette propriété fondamentale constitue en fait le théorème de Lagrange (voir ci-dessous) et implique que les classes d'équivalences forment une partition de G (figure 3). 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.



Remarque : les représentations graphiques des classes grâce aux orbites est utile mais il ne faut pas leur donner ici une signification géométrique. En particulier ces orbites n'ont pas nécessairement quelque chose à voir avec des vrais trajectoires unidimensionnelles.

Théorème de Lagrange.

a) Soit g et $g' \in G$. Alors on a uniquement deux possibilités

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

b) $|G/H| = \dfrac{|G|}{|H|}$ et en particulier la cardinalité d'un

sous groupe divise toujours celle du groupe.

Démonstration.

Fixons g et $g' \in G$. Si $E_g \cap E_{g'} = \emptyset$ (de a)) la preuve est finie.

Si $E_g \cap E_{g'} \neq \emptyset$ alors il existe un élément commun, appelons

le $\bar{g}$. Puisque $\bar{g} \in E_g$, $\exists\, h$ t.q $\bar{g} = gh$. D'autre part

puisque $\bar{g} \in E_{g'}$, $\exists\, h'$ t.q $\bar{g} = g'h'$. 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 conclue que

$E_g = E_{g'}$ ce qui achève la preuve de a).

Pour montrer b) il suffit de remarquer que la cardinalité de

chaque classe d'équivalence est $|H|$. En effet

$$E_g = \{ gh ;\ h \in H \}$$

et tous les éléments générés par l'action de H sont distincts.

(En effet si $gh_1 = gh_2$ alors $h_1 = h_2$)

Ainsi on a :

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

ce qui est équivalent à

$$|G/H| = \frac{|G|}{|H|}.$$

Puisque le nombre de classes d'équivalences $|G/H|$ est nécessairement entier il faut que $|H|$ divise $|G|$.

■

Exemples.

(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 avait $H = \{0, \vec{a}\}$ qui est un sous groupe à 2 éléments. On a : $|G| = 2^n$, $|H| = 2$ et $|G/H| = 2^{n-1}$. Il y a 2^{n-1} classes d'équivalences données par des paires $\{\vec{x}, \vec{y}\}$ t.q $\vec{x} = \vec{y} + \vec{a}$.

Ici l'orbite de $\vec{y}$ est $\{\vec{y} + \vec{0} = \vec{y}, \vec{y} + \vec{a}\}$.

(2) La généralisation immédiate du cas précédent est de prendre H = un sous-espace vectoriel de $\vec{\mathbb{F}}_2^n$ de dimension K. C'est un sous-groupe de $\vec{\mathbb{F}}_2^n$ pour l'addition $\oplus$ mod 2.

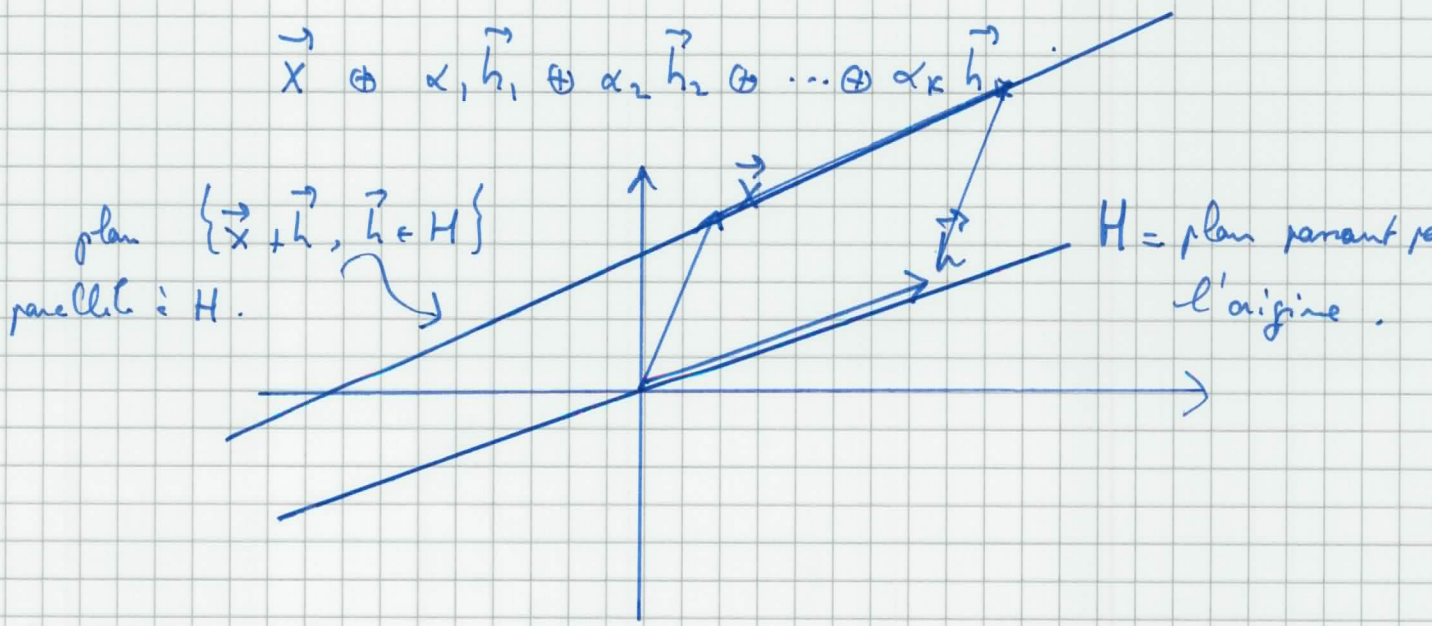
Puisque la dimension du sous-espace vectoriel est K on peut trouver K vecteurs de base $\vec{h}_1, \dots, \vec{h}_K$ et tout élément de H s'écrit comme :

$$\alpha_1 \vec{h}_1 \oplus \alpha_2 \vec{h}_2 \oplus \dots \oplus \alpha_K \vec{h}_K$$

avec $\alpha_i = 0, 1$. Le sous-groupe possède donc 2^K éléments. Le nombre de classes d'équivalences est $|G/H| = 2^{n-K}$. Celles-ci correspondent aux "hyperplans" parallèles à H.

Soit $\vec{x} \in \vec{\mathbb{F}}_2^n$, mon mal, son orbite (ou sa classe d'équivalence) est l'ensemble des vecteurs (voir figure).

$$\vec{x} \oplus \alpha_1 \vec{h}_1 \oplus \alpha_2 \vec{h}_2 \oplus \dots \oplus \alpha_K \vec{h}_K .$$



(3). Soit $G = (\mathbb{Z}, +)$ les entiers munis de l'addition ordinaire et soit $H = n\mathbb{Z}$ les multiples de n (n un entier quelconque). Deux entiers x et y sont équivalents si $x = y + qn$ c.a.d si $x - y = 0 \mod n$. Donc les classes d'équivalences sont les entiers mod n c.a.d $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, 3 \dots n-1\}$. L'orbite d'un élément x est

$$\{x + qn \ , \ q \in \mathbb{Z}\}.$$

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

Remarque : l'ensemble des classes d'équivalence $\mathbb{Z}/n\mathbb{Z} = \{0, 1 \dots n-1\}$ possède lui-même une structure de groupe, "l'addition modulo n". Ceci est un fait général : la loi de groupe induit une structure de groupe sur l'ensemble des classes d'équivalence G/H.

(4) Dans l'exemple précédent les groupes G et H étaient infinis. Plus tard nous voudrons travailler avec des groupes finis (car le nombre de bits manipulés est toujours fini). Nous remplacerons donc $\mathbb{Z}$ par $G = \frac{\mathbb{Z}}{M\mathbb{Z}} = \{0, 1 \dots M-1\}$ muni de l'addition mod M. L'idée est que pour M très grand ce groupe se comporte essentiellement comme $\mathbb{Z}$ tant qu'on s'intéresse 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 $\{0, 1, \dots, M-1\}$ forment un sous groupe appelé H et à nouveau $G/H = \frac{\mathbb{Z}}{r\mathbb{Z}}$ les entiers mod r. Notez que si r n'est pas un diviseur de M les multiples de r inférieurs à M ne forment pas un sous groupe de G. En effet $(qr + q'r) \bmod M$ n'est pas un multiple de r. Pour le voir on note que si c'était le cas on aurait

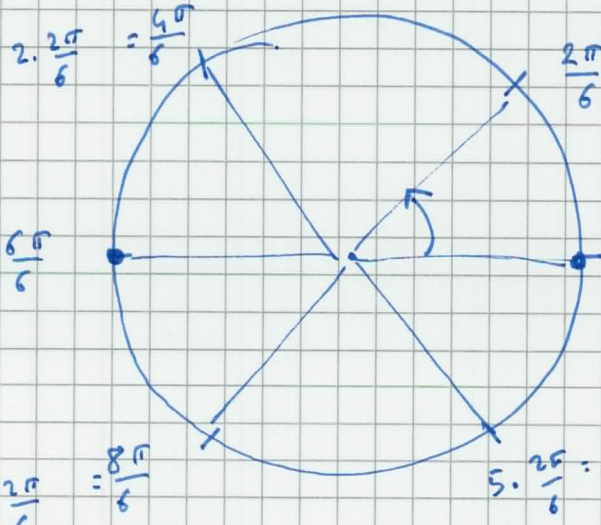
$$qr + q'r = s + kM$$

avec s multiple de r. Alors on aurait $qr + q'r - s = kM$ un multiple de r. On peut prendre q et q' (pas trop grands) t.q $k = 1$.

et alors il faudrait que M soit un multiple de n.

En conclusion il faut que n divise M pour que H soit un sous groupe. On arrive à la même conclusion grâce au théorème de Lagrange. En effet si $G/H = \frac{\mathbb{Z}}{n\mathbb{Z}}$ il y a n classes d'équivalence. Mais alors $|H| = \frac{|G|}{|G/H|} = \frac{M}{n}$ et pour que $|H|$ soit entier il faut que n divise M. Notons finalement que pour chaque diviseur de M on obtient un sous-groupe.

(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 mod M (c.a.d $\frac{\mathbb{Z}}{M\mathbb{Z}}$). Si n divise M $H = \{$ rotations d'angle $n \cdot \frac{2\pi}{M}\}$ forme un sous groupe. La figure ci-dessous illustre les cas $M = 6$ et $n = 2$; $n = 3$.



$H_{n=3} = \{0, \pi\}$

$H_{n=2} = \{0, \frac{4\pi}{6}, \frac{8\pi}{6}\}$.

$G/H_{n=3} = \{\{0,\pi\}; \{\frac{2\pi}{6}, \frac{8\pi}{6}\}; \{\frac{4\pi}{6}, \frac{10\pi}{6}\}\}$; $G/H_{n=2} = \{\{0, \frac{4\pi}{6}, \frac{8\pi}{6}\}; \{\frac{2\pi}{6}, \frac{6\pi}{6}, \frac{10\pi}{6}\}\}$.

3.2. 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 a disposition un oracle qui sait calculer une fonction :

$$f : G \to X.$$

$$g \mapsto f(g)$$

telle que f soit constante sur chaque classe d'équivalence et prend au moins $|G/H|$ valeurs. De plus le lien avec les notations du chap 2 est $|X| = |G/H|$ et $f(g_1) = f(g_2)$ si et seulement si $g_1 g_2^{-1} \in H$.

Pour $G = (\mathbb{F}_2^n, \oplus)$ et $H = \{0, \vec{a}\}$ un sous-espace vectoriel de dimension K nous avons présenté un algorithme quantique de complexité polynomiale qui permet de trouver H.

Le problème est de découvrir le sous groupe "caché" H en posant le moins de questions possibles à l'oracle.

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'étudions pas dans ce cours.

Le cas des groupes non-commutatifs est en général un problème ouvert important.

Nous allons étudier le cas particulier très important $G = \frac{\mathbb{Z}}{M\mathbb{Z}}$ (M "très grand"). Le cas est important car il mène de façon naturelle à l'algorithme de Shor pour la factorisation des entiers de $\mathbb{Z}$.

3.3. La période d'une fonction.

Considérons le problème suivant. Soit $f : \mathbb{Z} \to \mathbb{Z}$ une fonction périodique sur les entiers $x \longmapsto f(x)$ telle que

$$f(x+r) = f(x) \qquad \forall\, x \in \mathbb{Z}. \qquad (*)$$

où r est le plus petit entier satisfaisant (*). L'entier r est la période de f. Nous supposons que r est inconnu mais qu'un Oracle nous retourne les valeurs de $f(x)$ quand on

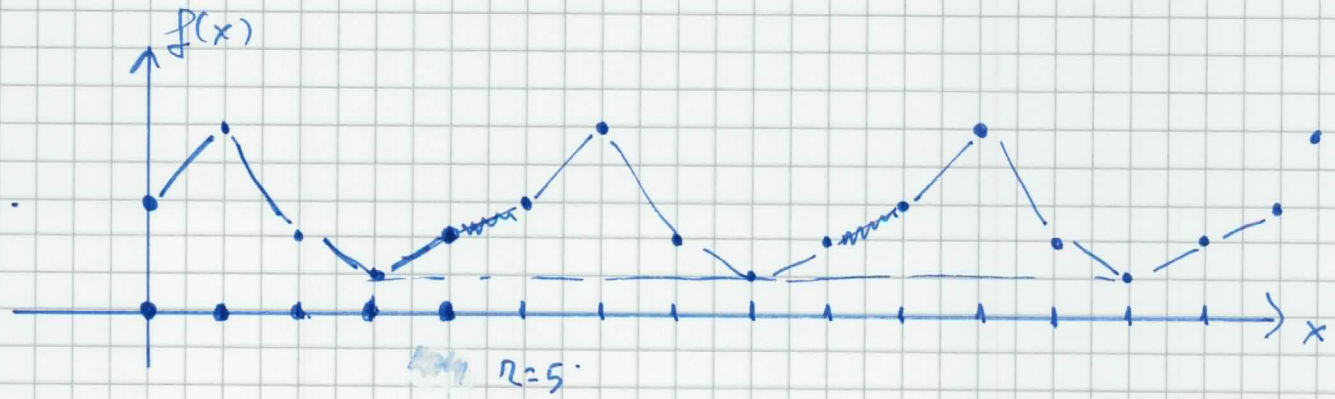
lui soumet l'entier x. Le problème est de déterminer la période r. Si r est "très grand" ce problème est difficile à priori car il faudra soumettre à l'Oracle environ r questions. C'est à dire que la complexité du calcul est en gros $O(\exp(\log_2 r))$ où $(\log_2 r)$ est le nombre de bits nécessaires pour représenter 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 est telle que

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

En d'autre termes f est constante sur les classes d'équivalence G/H (voir figure).



Comme nous devons travailler avec des groupes finis nous devons transformer $G = \mathbb{Z}$ à un grand entier M. Pour préserver la structure du groupe il faut en principe prendre un grand multiple de r et nous aurons $G = \frac{\mathbb{Z}}{M\mathbb{Z}}$ et $H = \{$ multiples de r inférieurs à $M\}$. Dans l'exemple de la figure $r = 5$ et par exemple $M = 5 \times 10^{40} = (\infty!)$

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 nous choisirons M grand, pas nécessairement multiple de r. Cela va détruire la structure du groupe mais si $M \gg r$ celle-ci est "approximativement préservée" car $M \pm K$ avec $1 \leq K \leq r-1$ sera un multiple de r et la "correction" K est négligeable par rapport à M. Ces ennuis techniques vont compliqué légèrement les calculs mais essentiellement l'algorithme quantique de la détermination de la période de f sera similaire à celui de Simon.

3.4. La factorisation des entiers.

Le théorème fondamental de l'arithmétique nous assure que tout entier N peut être décomposer de façon unique en un produit de nombres premiers. Etant donné des facteurs de N, il est facile de vérifier que le produit de ces facteurs redonne N. Plus précisément supposons que $N = p.q$ avec p et q deux nombres premiers à $O(b)$ bits. La vérification $N = p.q$ peut se faire facilement avec $O(b^2)$ opérations. Par contre étant donné un entier N (générique) $O(b)$ bits on ne connait pas d'algorithme polynomial permettant de calculer p & q.

On connait plusieurs algorithmes plus rapides que $O((1+\epsilon)^b)$ pour tout ϵ. Le meilleur algorithme connu possède un temps de calcul $O\left(\exp\left(\left(\frac{64}{9}b\right)^{1/3}(\log b)^{2/3}\right)\right)$.

Concrètement le record de factorisation (le 12 déc 2009) atteint pour un nombre à 232 décimales (768 bits) (voir en.wikipedia.org/wiki/RSA_numbers#RSA-768) et utilisa des centaines de processeurs sur 2 années de calculs.

Comme nous le verrons plus tard l'algorithme de Shor permet une factorisation en temps polynomial avec un circuit quantique de taille polynomial. L'algorithme de Shor résout en fait un autre problème de théorie des nombres appelé "la

recherche de l'ordre". Il est connu depuis 1576 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'autre terme 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 est pair et de diviser par 2. De plus si $N = p^e$ il existe des méthodes efficaces pour trouver p & e.

Soit $\left(\frac{\mathbb{Z}}{N\mathbb{Z}}, +\right)$ le groupe additif des entiers $\{0, 1, \ldots, N-1\}$ mod N.

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

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

$$d = PGCD(a, N)$$

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

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

c) Si $d = 1$ (c.e.d que a et N sont "premiers entre eux") on calcule le plus petit entier r t.q

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

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

d) Supposons que r soit impair. Output FAIL et retourner à a).

e) Sinon r est pair et alors on sait que

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

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 $a^{\frac{r}{2}} + 1$. Cas par C. è d $a^{\frac{r}{2}} = -1 \mod N$, 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 $p \mid a^{\frac{r}{2}} - 1$ et

$q \mid a^{\frac{r}{2}} + 1$ ou vice versa. En d'autre termes

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

sont non triviaux $d_+ > 1$ et $d_- > 1$. et nous avons 2 facteurs non triviaux de N. Ceux-ci sont calculé grâce à l'algorithme d'Euclide. (complexité $O(b^3)$).

f) [illegible]. 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 de résoudre l'étape c) la complexité provient uniquement de l'algorithme d'Euclide qui est de $O(b^3)$. Néanmoins cet algorithme est probabiliste et nous devons nous assurer que la probabilité de succès pour un round est non-négligeable. En fait on peut montrer $\text{Prob}(\text{succès}) \geq \frac{3}{4}$. Cela implique qu'avec $T = \frac{|\ln \epsilon|}{|\ln 2|}$ rounds on peut amplifier cette probabilité de succès à $\text{Prob}(\underbrace{\text{succès}}_{T \text{ rounds}}) \geq 1 - \epsilon$.

Lors d'un round les seuls outputs FAIL interviennent en d) et e2). Cela correspond à l'événement

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

Ainsi

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

Théorème. Soit a pris uniformément aléatoirement dans $\{2, \ldots, N-1\}$. Soit r le plus petit entier satisfaisant à $a^r = 1 \mod N$. Alors

$$P_r(\text{échec}) \leq \frac{1}{4}.$$

Nous ne donnons pas la preuve ici (voir Appendice). 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 rounds 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 $O(|\ln \epsilon|)$.

3.5 Fractions Continues.

Dans ce paragraphe nous donnons, sans démonstration, quelques faits 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 $x = \frac{263}{189}$.

Par l'algorithme d'Euclide :

$$263 = 1 \cdot 189 + 74$$
$$189 = 2 \cdot 74 + 41$$
$$74 = 1 \cdot 41 + 33$$
$$41 = 1 \cdot 33 + 8$$
$$33 = 4 \cdot 8 + 1.$$

(Ici on voit que $PGCD(263; 189) = 1$.). Etant donné qu'à chaque fois on divise par un nombre au moins ≥ 2 le nombre d'étapes (de lignes ci-dessus) est de l'ordre de $\log_2(263)$, c.a.d $\log_2(N)$ en général. De plus chaque division requiert $O((\log_2 N)^2)$ opérations. Donc le nombre total d'ops pour l'algorithme d'Euclide est $O((\log_2 N)^3)$.

Maintenant, pour obtenir le "développement en fraction continue" on procède ainsi :

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

$$= 1 + \cfrac{1}{2 + \cfrac{1}{74/41}} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{33}{41}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{41/33}}} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\frac{8}{33}}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1/(33/8)}}} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{8}}}}}$$

On dit que le développement est

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

La forme générale du développement est :

$$x = [a_0 , a_1 , \ldots , a_m]$$

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

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 $\frac{1}{a_m}$ comme $\cfrac{1}{a_m - 1 + \frac{1}{1}}$.

Ainsi

$$x = [a_0 ; a_1 ; \ldots ; a_m] = [a_0 ; a_1 ; \ldots ; a_m - 1 , 1]$$

Mais à cette ambiguité près le développement est unique. Le nombre d'opérations requises est $O(\log_2 N)$ où N = numérateur & dénominateur.

En fait un tel dév peut être étendu aux nombres irrationnels, comme suit. Soit x irrationnel. On peut toujours écrire

$$x = a_0 + \xi \quad \text{avec} \quad a_0 \in \mathbb{N} \text{ et } 0 < \xi < 1.$$

On pose $x = a_0 + \cfrac{1}{1/\xi}$. Maintenant $\frac{1}{\xi} = a_1 + \gamma$ avec $a_1 \in \mathbb{N}$ et $0 < \gamma < 1$. On itère :

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

et ... Cela donne en général un <u>développement</u>

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

<u>infini mais unique</u>.

Comme nous aurons besoin uniquement du cas x rationnel par la suite nous n'étudierons pas ici les propriétés très intéressantes de ces développements infinis.

Notion de "convergent". Soit $x = [a_0, a_1, a_2, \dots, a_n, \dots]$ un développement en fraction continue de x. On appelle "convergents" les séries tronquées $[a_0, a_1, a_2 \dots a_n]$. Ces convergents sont des nombres rationels

$$[a_0, a_1, a_2 \dots a_n] = \frac{p_n}{q_n}$$

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

Propriétés importantes des convergents.

a) PGCD $(p_n, q_n) = 1$.

b) $\left| \frac{p_n}{q_n} - x \right| \leq \frac{1}{q_n^2}$

c) Si x est irrationel on a une infinité de convergents. Ceux-ci donnent les meilleures approximation rationelles au sens suivant :

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

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

d) Si x est rationnel il existe un nombre fini d'approximations t.q $\left| \frac{p}{q} - x \right| < \frac{1}{q^2}$ et on peut toutes les trouver grâce aux convergents.

Pour nous c'est cette dernière propriété d) qui sera utile.

Exemple : le développement en fraction continue de π commence par

$$\pi = [3, 7, 15, 1, 292, 1, 1, \dots]$$

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 :

$$\left| \pi - \frac{355}{113} \right| \leq \frac{1}{(113)^2} \approx 10^{-4}.$$

En fait on a $\left| \pi - \frac{355}{113} \right| \approx 0,26 \times 10^{-6}$.

Exercice : Donnez la liste (finie) des convergents de $x = \frac{263}{189}$.

3.6. Fonction d'Euler.

Pour un entier $n \geq 2$ on dit que $a \in \{1, 2, 3, \ldots, n-1\}$ est premier avec n (a is coprime with n) si $PGCD(a, n) = 1$.

Le nombre de tels a est donné par $\varphi(n)$, la fonction d'Euler.

Exemple : si $N = 9$ les a premiers avec N sont

$a = 1, 2, 4, 5, 7, 8$ et donc $\varphi(9) = 6$.

si N est premier, $N = p$ on a :

$a = 1, 2, 3, \ldots, p-1$ et $\varphi(p) = p-1$.

En général on montre que si

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

est la décomposition en facteurs premiers de N,

$$\varphi(N) = \varphi(p_1^{e_1}) \varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k})$$

$$= p_1^{e_1-1}(p_1-1) \cdot p_2^{e_2-1}(p_2-1) \cdots p_k^{e_k-1}(p_k-1).$$

Pour $N = 9 = 3^2$ on a par exemple $\varphi(9) = 3^{2-1} \cdot (3-1) = 6$.

Une propriété utile pour nous avec la suivante :

$$\varphi(n) \geq \frac{n}{4(\log\log n)}.$$

En d'autre terme, étant donné n, "la plupart" des $n-1$ nombres inférieurs sont premier avec n. Cette propriété peut être exprimée comme suit. Fixons n et choisons $K \in \{1, 2, \ldots n-1\}$ uniformément aléatoirement (avec probabilité $\frac{1}{n}$). Alors :

$$\text{Prob}\left(\text{PGCD}(K, n) = 1\right) \geq \frac{1}{4(\log\log n)}$$

$$\left(\text{car } \frac{\varphi(n)}{n} = \frac{1}{4\log\log n}\right).$$