L'ANNEAU $\mathbb{Z}$ ET SES QUOTIENTS

RÉSUMÉ ET QUESTIONS

1. IDÉAUX

Un anneau est un ensemble A muni de deux lois de composition internes $+$ et $\times$ telles que $(A, +)$ est un groupe commutatif d'élément neutre noté 0 et la loi $\times$ est associative et distributive à gauche et à droite par rapport à $+$. Si $\times$ admet un élément neutre 1 on dit que l'anneau est unitaire. Si $\times$ est commutative on dit que l'anneau est commutatif.

L'anneau des matrices $d \times d$ pour $d \geq 2$ est unitaire mais pas commutatif. Les ensembles $\mathbb{R}$ et $\mathbb{Z}$ sont des anneaux.

Soit A un anneau commutatif. Un *idéal* de A est un sous-ensemble non-vide I tel que $(I, +)$ est un sous-groupe de $(A, +)$ et $AI \subset I$. Par exemple $5\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Si $a \in A$ l'ensemble aA est un idéal souvent noté (a). Un tel idéal est dit principal. Tous les idéaux de $\mathbb{Z}$ sont principaux. Un anneau dont tous les idéaux sont principaux est dit principal.

L'intersection d'une famille d'idéaux est un idéal. Si S est une partie de A alors le plus petit idéal de A contenant S est l'intersection de tous les idéaux contenant S. On le note (S). Si $A = \mathbb{Z}[X]$ alors l'idéal $(2, X)$ n'est pas principal.

La somme $I + J$ de deux idéaux est par définition le plus petit idéal contenant I et J.

L'anneau $\mathbb{Z}$ est principal. Cela se montre avec la division euclidienne. Si I est un idéal non-nul alors $I = (a)$ où a est le plus petit élément positif de I. Une conséquence de l'algorithme d'Euclide étendu est le théorème de Bezout : si m et n sont deux entiers positifs il existe deux entiers u et v tels que $ua + vb = pgcd(a, b)$. On en déduit le théorème de Gauss : si a, b, c sont trois entiers positifs tels que a divise bc et a est premier à b alors a divise c. On en déduit enfin le théorème fondamental de l'arithmétique : tout entier positif s'écrit de façon unique, à permutation près, comme produit de nombres premiers.

Si $A = \mathbb{Z}$ et si m et n sont deux entiers positifs, l'idéal $(m) + (n)$ est principal, engendré par le pgcd de m et n. L'idéal $(m) \cap (n)$ est principal engendré par le ppcm de m et n.

Si A est un anneau commutatif et I un idéal, on définit une relation d'équivalence sur A par $x \equiv y$ ssi $y - x \in I$. Cette relation est compatible avec les lois $+$ et $\times$. Donc le quotient, noté A/I, est un anneau. Par exemple $\mathbb{Z}/5\mathbb{Z}$ ou $\mathbb{F}_2[x]/(x^2 + x + 1)$. Plutôt que $x \equiv y$ on écrit $x = y \bmod I$.

Deux types de quotients vont nous intéresser. Les quotients $\mathbb{Z}/N\mathbb{Z}$ et les quotients $A[x]/f(x)$. Un élément de $\mathbb{Z}/N\mathbb{Z}$ est représenté par un entier entre 0 et $N - 1$. Pour ajouter deux éléments $a \bmod N$ et $b \bmod N$ on calcule $a + b$ et on retranche N si nécessaire. Pour multiplier, on calcule ab et on fait la division euclidienne par N. Le coût est $O((\log N)^2)$ avec les algorithmes classiques.

Exercice. L'anneau $(\mathbb{Z}/N\mathbb{Z}, +, \times)$ peut être vu aussi comme un groupe additif $(\mathbb{Z}/N\mathbb{Z}, +)$.

Montrez que les sous-groupes de $(\mathbb{Z}/N\mathbb{Z}, +)$ sont aussi des idéaux de $(\mathbb{Z}/N\mathbb{Z}, +, \times)$.
Montrez que ces sous-groupes sont en bijection avec les diviseurs positifs de N.

□

Un anneau A commutatif est dit intègre si le produit de deux éléments non-nuls est non-nul. Soit I un idéal d'un anneau commutatif A. Le quotient A/I est intègre si et seulement si pour x et y dans A tels que $xy \in I$ on a $x \in I$ ou $y \in I$. On dit alors que I est un idéal premier. Par exemple, si $A = \mathbb{Z}$ l'idéal (N) est premier si et seulement si la valeur absolue de N est un entier naturel premier. Dans ce cas $\mathbb{Z}/N\mathbb{Z}$ est un anneau intègre. En fait c'est même un corps dans ce cas : tout élément non-nul est inversible.

2. INVERSIBLES

Soit A un anneau commutatif. Un élément a de A est dit inversible s'il existe b dans A tel que $ab = 1$. À titre d'exemple, on pourra donner la liste des inversibles de $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/pq\mathbb{Z}$ pour p et q premiers, $\mathbb{F}_2[x]/(x^2 + x + 1)$.

Les inversibles de A forment un groupe noté A^*. Si p est premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique. Si $f(x)$ est irréductible dans $\mathbb{F}_2[x]$ alors $(\mathbb{F}_2[x]/f(x))^*$ est cyclique. Donnez une générateur de $(\mathbb{Z}/7\mathbb{Z})^*$. Le groupe $(\mathbb{Z}/15\mathbb{Z})^*$ est-il cyclique ? Même question pour $(\mathbb{F}_2[x]/(x^2 + x + 1))^*$.

Soit p un entier premier. Si g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ on appelle **exponentielle discrète** de base g l'application $\exp_g : \mathbb{Z}/(p-1)\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^*$ définie par $\exp_g(k) = g^k$. C'est une bijection. L'application réciproque est notée $\log_g$ et appelé **logarithme discret** de base g. On pourra dresser la table des exponentielles et logarithmes pour un générateur de $(\mathbb{Z}/7\mathbb{Z})^*$.

On vérifie que $\log_g(ab) = \log_g(a) + \log_g(b)$ et si h est un autre générateur alors $\log_h(a) = \log_g(a)/\log_g(h)$. Et $\exp_g(k + l) = \exp_g(k)\exp_g(l)$.

Un algorithme naïf pour calculer l'exponentielle $\exp_g(k)$ calculerait successivement g, g^2, g^3, g^4, …, g^{k-1}, g^k, ce qui requiert $k - 1$ opérations dans $\mathbb{Z}/p\mathbb{Z}$. Ce n'est pas satisfaisant car on souhaite calculer g^k en temps polynomial en $\log p$ et $\log k$.

L'algorithme utilisé en pratique est connu sous le nom d'exponentiation rapide. On calcule $g_0 = g$, $g_1 = g_0^2 = g^2$, $g_2 = g_1^2 = g^4$, $g_3 = (g_2)^2 = g^8$, …, $g_x = g^{2^x}$ où 2^x est la plus grande puissance de 2 inférieure ou égale à k. On écrit alors l'exposant k en base 2 soit

$$k = \sum_{1 \leq l \leq x} \epsilon_l 2^l$$

et on vérifie que

$$g^k = \prod_{1 \leq l \leq x} g_l^{\epsilon_l}.$$

Au total le calcul de g^k n'a pas requis plus de $2\log_2 k$ opérations dans $\mathbb{Z}/p\mathbb{Z}$.

On ne connaît pas d'algorithme vraiment rapide pour calculer le logarithme discret. On dit que l'exponentielle est une fonction asymétrique.

Si N est un entier composé, alors $(\mathbb{Z}/N\mathbb{Z})^*$ n'est pas cyclique en général. Son cardinal, noté $\varphi(N)$, est le nombre d'entiers premiers à N dans l'intervalle $[1, N-1]$.

3. Théorèmes de Fermat, Lagrange, Euler

Le petit théorème de Fermat affirme que si p est un nombre premier et x un entier premier à p alors $x^{p-1} \equiv 1 \bmod p$. Plus général, le théorème d'Euler affirme que pour $N \geq 2$ entier, et x premier à N, on a $x^{\varphi(N)} = 1 \bmod N$. Par exemple, on pourra vérifier les calculs suivants.

```
gp > N=101
%1 = 101
gp > Mod(2,N)^(N-1)
%2 = Mod(1, 101)
gp > N=17*19
%3 = 323
gp > Mod(3,N)^(N-1)
%4 = Mod(264, 323)
gp > N=3*11*17
%5 = 561
> for(k=1,N-1,if(gcd(N,k)==1,print(Mod(k,N)^(N-1))))
Mod(1, 561)
Mod(1, 561)
...
Mod(1, 561)
```

On voit que 561 vérifie le petit théorème de Fermat bien qu'il soit composé. Autrement dit, le petit théorème de Fermat donne une conditions nécessaire de primalité, pas une condition suffisante.

On peut donc déduire du théorème de Fermat un critère de composition. S'il existe x premier à N tel que $x^{N-1} \not\equiv 1 \bmod N$, alors N est composé. Par exemple

```
gp > N=2^(2^8)+1
%1 = 115792089237316195423570985008687907853269984665640564039
5758400791312963993 7
gp > Mod(3,N)^(N-1)
%2 = Mod(113080593127052224644745291961064595403241347689552251
078258028018246279223993, 115792089237316195423570985008687907853
5326998466564056403945758400791312963993 7)
```

montre que $2^{2^8} + 1$ n'est pas premier. Sans pour autant donner un facteur non-trivial. On observe qu'il n'est pas difficile de vérifier la congruence de Fermat. On utilise l'exponentiation rapide.

Les théorèmes de Fermat et Euler sont des conséquences du théorème de Lagrange. Ce théorème affirme que pour G un groupe de cardinal e et g un élément de G, on a $g^e = 1$ dans G.

Exercice. Soit G est un groupe et $H \subset G$ un sous-groupe. On définit une relation $\mathcal{R}$ sur G par $x\mathcal{R}y$ si et seulement si $x^{-1}y \in H$.

Montrer que c'est une relation d'équivalence.

Montrer que toutes les classes d'équivalence ont le même cardinal, soit $\#H$.

En déduire une preuve du théorème de Lagrange.

□

4. Le critère de Miller-Rabin

Le critère de Fermat n'est pas assez fort pour départager les nombres premiers et les nombres composés. On peut cependant renforcer ce critère. Soit en effet N un nombre premier impair. On pose

$$N - 1 = 2^k m$$

avec $k \geq 1$ et m impair. Soit x dans $(\mathbb{Z}/N\mathbb{Z})^*$. Le théorème de Fermat implique

$$x^{N-1} - 1 = 0.$$

Donc

$$x^{m2^k} - 1 = (x^{m2^{k-1}} - 1)(x^{m2^{k-1}} + 1) = 0.$$

Comme $\mathbb{Z}/N\mathbb{Z}$ est un corps on a

$$x^{m2^{k-1}} - 1 = 0 \text{ ou } x^{m2^{k-1}} + 1 = 0.$$

Dans le premier cas, si $k \geq 2$ on peut poursuivre la factorisation

$$x^{m2^{k-1}} - 1 = (x^{m2^{k-2}} - 1)(x^{m2^{k-2}} + 1) = 0,$$

donc

$$x^{m2^{k-2}} - 1 = 0 \text{ ou } x^{m2^{k-2}} + 1 = 0,$$

et ainsi de suite.

En fin de compte on a montré que pour N premier impair et x premier à N on a

$$x^m = 1 \text{ ou } x^{m2^i} = -1 \text{ pour un } 0 \leq i \leq k-1.$$

Dans ce cas on dit que la propriété $\mathrm{MR}(n, x)$ est satisfaite. S'il existe x premier à N tel que $\mathrm{MR}(n, x)$ soit fausse alors n est composé. C'est le critère de composition de Miller-Rabin.

Par exemple pour $N = 29$ on a $k = 2$ et $m = 7$. On choisit $x = 2$, et on vérifie que $2^{14} = -1 \bmod 29$. Donc $\mathrm{MR}(29, 2)$ est vrai. Cela ne prouve pas que 29 est premier. En effet, même si n est composé il peut exister des x tels que $\mathrm{MR}(n, x)$ soit vrai. Par exemple $x = 1$. Cependant, Monier a montré que si $n \geq 15$ est composé alors au plus un quart des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ satisfont $\mathrm{MR}(n, x)$. On les appelle des faux témoins. Donc si l'on choisit x au hasard, un nombre composé a au plus une chance sur quatre de passer le test de Miller-Rabin. Après quelques tests positifs on est donc convaincu que n est premier, mais ce n'est pas une preuve.

On peut tester la condition $\mathrm{MR}(N, x)$ au prix de $(\log N)^3$ opérations élémentaires, et même $(\log N)^{2+o(1)}$ avec l'arithmétique rapide.

5. Densités de nombres premiers

Rappelons que la taille d'un entier positif N peut être définie comme le nombre de chiffres dans sa représentation décimale soit $\lceil \log_{10}(a+1) \rceil$. On peut ajouter et multiplier des entiers en temps polynomial en leur taille. Même chose pour la division euclidienne et l'algorithme d'Euclide étendu.

On rappelle aussi qu'un nombre premier est un entier plus grand que 1 qui n'a pas d'autre diviseur que 1 et lui même.

On a vu aussi que l'algorithme d'Euclide prouve le théorème de Bezout et le théorème de Gauss, ainsi que le théorème fondamental de l'arithmétique.

On sait depuis l'antiquité qu'il existe une infinité de nombres premiers. Le crible d'Eratosthènes permet de trouver tous les nombres premiers dans un intervalle $[1, A]$ en temps $A^{1+o(1)}$. Il permet aussi de factoriser un entier N en temps $N^{1+o(1)}$.

Comme les nombres premiers sont très utiles, on peut se demander s'il y en a beaucoup dans l'intervalle $[1, A]$? On note $\pi(A)$ le nombre de premiers dans cet intervalle. Hadamard et de la Vallée-Poussin ont montré que

$$\pi(A) = \frac{A}{\log A}(1 + o(1)).$$

L'expérimentation confirme ce théorème.

A	10	100	1000	10000	100000
$\pi(A)$	4	25	168	1229	9592
$A/\pi(A)$	2.5	4	5.95	8.14	10.4
$\log A$	2.3	4.6	6.9	9.2	11.5

Ainsi un nombre choisi au hasard dans $[1, A]$ ou dans $[A, 2A]$ est premier avec probabilité $1/\log(A)$ à peu près. Si on cherche un nombre premier dans $[A, 2A]$ en tirant au hasard des nombres et en les testant avec le critère de Miller-Rabin, on trouvera un pseudo-premier en temps $(\log A)^4$ ou même $(\log A)^{3+o(1)}$ avec l'arithmétique rapide. On peut accélérer cette recherche à l'aide d'un crible.

6. Densités de nombres friables

On considère l'anneau $\mathbb{Z}$ des entiers naturels. On note $\mathbb{Z}^*$ le semi-groupe des entiers non nuls. Le semigroupe $\mathbb{Z}^*$ est muni d'une fonction $t : \mathbb{Z}^* \to \mathbb{R}$ appelée taille et définie par

$$t(n) = \log(|n|).$$

On note que la taille est multiplicative, c'est-à-dire que la taille d'un produit est la somme des tailles des facteurs.

On constate aussi que le nombre $V(t_0)$ d'éléments de taille inférieure à une taille t_0 donnée est exponentiel en t_0. En effet

$$V(t_0) = 2\lfloor \exp(t_0) \rfloor.$$

On qualifie d'y-*friable* ou y-*lisse* un entier produit d'entiers inférieurs ou égaux à y. Par exemple, $330 = 2 \times 3 \times 5 \times 11$ est 13-friable et même 11-friable. Les entiers friables jouent un rôle très important en algorithmique des nombres.

On étudie la proportion d'entiers friables. Soient $x \geq 2$ et $y \geq 2$ deux entiers. Montrons comment estimer la proportion d'éléments y-friables parmi les entiers inférieurs ou égaux à x. L'argumentation que nous donnons est à la fois simple et générale mais elle est grossière.

Soit

$$n = \lfloor t(x)/t(y) \rfloor = \lfloor \log(x)/\log(y) \rfloor$$

le plus grand entier inférieur ou égal au quotient des tailles $t(x)/t(y)$. Prenons n entiers premiers positifs y_1, y_2,..., y_n, inférieurs ou égaux à y. Alors le produit $y_1 y_2 ... y_n$ est inférieur ou égal à x et il est y-friable.

On cherche alors à compter les éléments y-friables ainsi obtenus. On se souvient que la proportion de nombre premiers parmi les entiers positifs inférieurs ou égaux à y est

$$\frac{1}{\log(y)}(1 + \epsilon(y)) = \frac{1}{t(y)}(1 + \epsilon(y))$$

où ϵ est une fonction de la classe $o(1)$. C'est le théorème des nombres premiers prouvé par Hadamard et de la Vallée Poussin. En fait on sait que cette proportion est

$$\geq \frac{1}{\log(y)}$$

dès que $y \geq 52$. Voir [Ten, Chapitre I.1].

Ainsi le nombre de n-uplets $(y_1, ..., y_n)$ est

$$\geq \frac{y^n}{(\log y)^n} \geq \frac{x}{y} \times \frac{1}{(\log(y))^n} \geq x^{1-\frac{1}{n}} \times \frac{1}{(\log(y))^n},$$

dès que $y \geq 52$.

Comme la multiplication est commutative, toutes les permutations d'un n-uplet $(y_1, \ldots, y_n)$ ont le même produit. En fait, deux n-uplets dont les coordonnées sont des entiers premiers ont le même produit si et seulement s'ils sont permutés l'un de l'autre. C'est le théorème fondamental de l'arithmétique. On a donc au plus $n!$ différents n-uplets qui donnent le même produit. Aussi, on a fabriqué au moins

$$\frac{x}{n! x^{\frac{1}{n}} (\log(y))^n}$$

éléments y-friables dans l'intervalle $[1, x]$.

Cette estimation très grossière fait intervenir le facteur intéressant $n!$ au dénominateur. Ce dénominateur est majoré par $n^{O(n)}$ dès que $\log x \geq (\log y)^2$ et $y \gg 1$. Une étude plus poussée [Gra] montre que la densité de nombres friables est proche de n^{-n}. Plus précisèment,

Théorème 6.1 (Canfield, Erdös, Pomerance)**.** *Soit $\Psi(x, y)$ la proportion d'entiers y-friables parmi les entiers de l'intervale $[1, x]$. On note $u = \frac{\ln x}{\ln y}$. Soit $\varepsilon \in]0, 1[$ fixé. Il existe une fonction μ de la classe $o(1)$ telle que*

$$\Psi(x, y) = x u^{-u(1+\mu(u))}$$

si $(\ln x)^{\varepsilon} < u < (\ln x)^{1-\varepsilon}$.

Cette proportion n'est ni trop grande ni trop petite. Il y a beaucoup plus d'entiers friables que de carrés par exemple. Mais moins que de nombres premiers.

REFERENCES

[Gra] Andrew Granville. *Smooth numbers: computational number theory and beyond*. Algorithmic Number Theory, MSRI Publications, Volume 44, 2008.

[Ten] Gérald Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres*. Société mathématique de France, 1995.