Cours d'Arithmétique

Xavier Caruso

Juillet 2002

Table des matières

Dans tout ce cours :
- $\mathbb{N}$ désignera l'ensemble des entiers naturels : $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
- $\mathbb{N}^\star$ désignera l'ensemble des entiers naturels non nuls : $\mathbb{N}^\star = \{1, 2, 3, \ldots\}$
- $\mathbb{Z}$ désignera l'ensemble des entiers relatifs : $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- $\mathbb{Z}^\star$ désignera l'ensemble des entiers relatifs non nuls : $\mathbb{Z}^\star = \{\ldots, -3, -2, -1, 1, 2, 3, \ldots\}$

1 Quand on ne regarde que le dernier chiffre...

1.1 Qu'est-ce que $\mathbb{Z}/10\mathbb{Z}$?

Commençons par introduire les notations suivantes :
- $\dot{0}$ sera un entier naturel quelconque se terminant par 0
- $\dot{1}$ sera un entier naturel quelconque se terminant par 1

  $\vdots$
- $\dot{9}$ sera un entier naturel quelconque se terminant par 9

Remarquons que la définition précédente n'a rien de rigoureux. Il aurait mieux fallu définir par exemple $\dot{0}$ comme l'ensemble des nombres se terminant par 0 plutôt que comme l'un quelconque d'entre eux, mais cela ne changera rien par la suite et c'est sans doute plus simple de voir les choses de cette façon.

L'ensemble $\mathbb{Z}/10\mathbb{Z}$ est alors par définition :

$$\mathbb{Z}/10\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}, \dot{6}, \dot{7}, \dot{8}, \dot{9}\right\}$$

Il s'agit donc d'un ensemble fini comportant 10 éléments.

1.2 Opérations dans $\mathbb{Z}/10\mathbb{Z}$

Ce que l'on sait depuis que l'on sait effectuer des opérations mais qu'il est remarquable de constater ici, c'est que pour calculer le dernier chiffre d'une somme ou d'un produit, il suffit de connaître les derniers chiffres des nombres que l'on additionne ou multiple.

Cela permet de voir que l'on peut en fait additionner et multiplier directement les éléments de $\mathbb{Z}/10\mathbb{Z}$. Par exemple supposons que l'on veuille multiplier $\dot{3}$ par $\dot{7}$. On choisit alors un nombre se terminant par 3, par exemple 13, un autre se terminant par 7 par exemple 47. On multiplie 13 et 47 entre eux, on trouve 611 et on ne garde que le dernier chiffre. Bien entendu ce dernier chiffre ne dépend pas des représentants que l'on a choisi pour faire le calcul. Ainsi il est légitime de poser :

$$\dot{3} \times \dot{7} = \dot{1}$$

Bien entendu, pour faire ce calcul, il aurait été plus rusé de choisir les représentations 3 et 7 plutôt que 13 et 47. Enfin, bon, ça tombe sous le sens.

Dressons les tables d'addition et de multiplication de $\mathbb{Z}/10\mathbb{Z}$. On trouve :

$+$	$\mathbf{\dot{0}}$	$\mathbf{\dot{1}}$	$\mathbf{\dot{2}}$	$\mathbf{\dot{3}}$	$\mathbf{\dot{4}}$	$\mathbf{\dot{5}}$	$\mathbf{\dot{6}}$	$\mathbf{\dot{7}}$	$\mathbf{\dot{8}}$	$\mathbf{\dot{9}}$
$\mathbf{\dot{0}}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$
$\mathbf{\dot{1}}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$
$\mathbf{\dot{2}}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$
$\mathbf{\dot{3}}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\mathbf{\dot{4}}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\mathbf{\dot{5}}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\mathbf{\dot{6}}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\mathbf{\dot{7}}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\mathbf{\dot{8}}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$
$\mathbf{\dot{9}}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$

$\times$	$\mathbf{\dot{0}}$	$\mathbf{\dot{1}}$	$\mathbf{\dot{2}}$	$\mathbf{\dot{3}}$	$\mathbf{\dot{4}}$	$\mathbf{\dot{5}}$	$\mathbf{\dot{6}}$	$\mathbf{\dot{7}}$	$\mathbf{\dot{8}}$	$\mathbf{\dot{9}}$
$\mathbf{\dot{0}}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\mathbf{\dot{1}}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$
$\mathbf{\dot{2}}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{8}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{8}$
$\mathbf{\dot{3}}$	$\dot{0}$	$\dot{3}$	$\dot{6}$	$\dot{9}$	$\dot{2}$	$\dot{5}$	$\dot{8}$	$\dot{1}$	$\dot{4}$	$\dot{7}$
$\mathbf{\dot{4}}$	$\dot{0}$	$\dot{4}$	$\dot{8}$	$\dot{2}$	$\dot{6}$	$\dot{0}$	$\dot{4}$	$\dot{8}$	$\dot{2}$	$\dot{6}$
$\mathbf{\dot{5}}$	$\dot{0}$	$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{0}$	$\dot{5}$
$\mathbf{\dot{6}}$	$\dot{0}$	$\dot{6}$	$\dot{2}$	$\dot{8}$	$\dot{4}$	$\dot{0}$	$\dot{6}$	$\dot{2}$	$\dot{8}$	$\dot{4}$
$\mathbf{\dot{7}}$	$\dot{0}$	$\dot{7}$	$\dot{4}$	$\dot{1}$	$\dot{8}$	$\dot{5}$	$\dot{2}$	$\dot{9}$	$\dot{6}$	$\dot{3}$
$\mathbf{\dot{8}}$	$\dot{0}$	$\dot{8}$	$\dot{6}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{8}$	$\dot{6}$	$\dot{4}$	$\dot{2}$
$\mathbf{\dot{9}}$	$\dot{0}$	$\dot{9}$	$\dot{8}$	$\dot{7}$	$\dot{6}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

On constate sur les tables précédentes que, bien évidemment, ajouter $\dot{0}$ ou multiplier par $\dot{1}$ ne change pas le résultat. En outre, multiplier par $\dot{0}$ fournit toujours un résultat égal à $\dot{0}$.

1.3 Équations dans $\mathbb{Z}/10\mathbb{Z}$

Il arrive très souvent que des problèmes d'arithmétique se réduisent à la résolution d'équation par exemple dans $\mathbb{Z}/10\mathbb{Z}$. Nous allons voir comment l'on procède pour résoudre ces équations.

1.3.1 $\dot{x} + \dot{a} = \dot{b}$

Le résultat important à remarquer ici, et que l'on peut par exemple voir sur les tables précédentes, est que pour tout élément $\dot{a} \in \mathbb{Z}/10\mathbb{Z}$, il existe un élément $\dot{a}' \in \mathbb{Z}/10\mathbb{Z}$ tel que $\dot{a} + \dot{a}' = \dot{0}$. Un tel $\dot{a}'$ est unique et s'appelle l'*opposé* de $\dot{a}$.

Ainsi résoudre l'équation de départ est quelque chose de simple, il suffit d'ajouter $\dot{a}'$ des deux côtés de l'égalité. On obtient :

$$\dot{x} = \dot{b} + \dot{a}'$$

C'est l'unique solution.

1.3.2 $\dot{a}\dot{x} = \dot{b}$

Là encore, il nous faudrait trouver un élément $\dot{a}'$ tel que le produit $\dot{a} \times \dot{a}'$ soit égal à $\dot{1}$. On multiplierait alors par $\dot{a}'$ des deux côtés et on aurait une expression pour $\dot{x}$. Un tel $\dot{a}'$ s'appelle l'*inverse* de $\dot{a}$.

Toutefois, comme on peut le constater sur les tables, il n'est pas vrai que tout élément admet un inverse. $\dot{2}$ par exemple n'en admet pas. Mais cela se conçoit très bien : prenons un entier naturel se terminant par 2, ce nombre est pair et tous ces multiples seront donc pairs. Ainsi il n'est pas possible en le multipliant par un autre nombre d'obtenir un entier se terminant par 1 qui serait alors impair.

Un élément qui admet un inverse est qualifié d'*inversible*. Il est facile de faire la liste des inversibles de $\mathbb{Z}/10\mathbb{Z}$, il s'agit de $\dot{1}$, $\dot{3}$, $\dot{7}$ et $\dot{9}$.

Ainsi pour résoudre l'équation $\dot{3}\dot{x} = \dot{2}$ par exemple, il suffit de multiplier par $\dot{7}$ des deux côtés. Cela n'est plus valable pour l'équation $\dot{2}\dot{x} = \dot{3}$ qui, elle, n'a pas de solution. En revanche, l'équation $\dot{4}\dot{x} = \dot{2}$ admet deux solutions qui sont $\dot{3}$ et $\dot{8}$.

2 10 n'est-il pas un peu arbitraire ?

2.1 Division euclidienne

Théorème 1. *Soient a et b deux entiers relatifs, on suppose $b \neq 0$. Alors il existe un* unique *couple d'entiers (q, r) tels que*

i) $a = bq + r$

ii) $0 \leqslant r < |b|$

Trouver le couple (q, r) du théorème est ce que l'on appelle *effectuer la division euclidienne de a par b*. q s'appelle le *quotient* de cette division euclidienne et r le *reste*.

Pour effectuer une division euclidienne, on fait par exemple comme l'on a appris dans les petites classes. Il faut faire attention cependant lorsque des nombres négatifs interviennent. Par exemple, la division euclidienne de -17 par -4 s'écrit :

$$-17 = (-4) \times (-5) + 3$$

et non pas :

$$-17 = (-4) \times (-4) - 1$$

En effet il faut bien se rappeler que l'on impose que le reste soit positif (et strictement plus petit que $|b|$).

2.2 Décomposition en base n

On fixe dans ce chapitre et dans le suivant un entier $n \geqslant 2$.

Théorème 2. *Soit a un entier naturel. Il existe une* unique *suite $(a_i)_{i \geqslant 0}$ d'entiers telle que :*
i) (a_i) est nulle à partir d'un certain rang
ii) pour tout i, $0 \leqslant a_i < n$
iii) $a = a_0 + a_1 n + a_2 n^2 + \ldots + a_i n^i + \ldots$

On remarque dans un tout premier temps que la dernière somme écrite est en réalité finie puisque la suite (a_i) est nulle à partir d'un certain moment. La suite (a_i) est appelée la *décomposition en base n* de l'entier a.

Pour démontrer ce théorème, il s'agit simplement de faire des divisions euclidiennes. Plus précisément la dernière condition nous dit que a_0 *doit* être le reste de la division euclidienne de a par n, le quotient de cette division sera $a_1 + a_2 n + \ldots + a_i n^{i-1} + \ldots$.

Pour déterminer la décomposition de a en base n, on commence donc par effectuer la division euclidienne de a par n. Le reste fournit alors l'élément a_0. Quant au quotient, sa décomposition en base n va fournir les autres termes de la suite. On décompose donc ce quotient en base n et pour cela on effectue la division euclidienne de celui-ci par n. Le reste de cette division va en fait fournir a_1 et on continue ensuite avec le nouveau quotient obtenu.

Pour prouver finalement le théorème, il s'agit de voir que cela s'arrête en un nombre fini de divisions euclidiennes, c'est-à-dire qu'au bout d'un moment on tombe sur un quotient nul. Mais si le quotient n'est pas nul, il va décroître strictement puisque l'on divise par un nombre plus grand ou égal à 2. On conclut alors en disant que toute suite strictement décroissante d'entiers naturels s'arrête forcément.

Présentons les calculs sur un exemple. Supposons que l'on veuille déterminer la décomposition en base 7 de 125487. On effectue alors successivement les divisions euclidiennes :

$$\begin{aligned}
125487 &= 7 \times 17926 + 5 \\
17926 &= 7 \times 2560 + 6 \\
2560 &= 7 \times 365 + 5 \\
365 &= 7 \times 52 + 1 \\
52 &= 7 \times 7 + 3 \\
7 &= 7 \times 1 + 0 \\
1 &= 7 \times 0 + 1
\end{aligned}$$

On voit ainsi que :

$$125487 = 5 + 6 \cdot 7 + 5 \cdot 7^2 + 1 \cdot 7^3 + 3 \cdot 7^4 + 0 \cdot 7^5 + 1 \cdot 7^6$$

On écrit parfois cela sous la forme $125487 = \underline{1031565}_7$.

2.3 Présentation de $\mathbb{Z}/n\mathbb{Z}$

Il s'agit exactement de la même chose que celle qui a été présentée dans la première partie sauf que l'on remplace 10 par un entier $n \geqslant 2$ quelconque.

Plus précisément si a est un chiffre de la base n, c'est-à-dire un entier compris entre 0 et $n-1$, on note $\dot{a}$ un entier naturel naturel quelconque se terminant par a en base n. D'après ce que l'on a dit précédemment, il s'agit donc d'un entier dont le reste de la division euclidienne par n est précisément a[1]. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est alors :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0}, \dot{1}, \ldots, \overline{n-1}\right\}$$

Là encore sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$, on peut définir une addition et une multiplication : pour calculer le dernier chiffre d'une somme ou d'un produit, on n'a encore besoin que des derniers chiffres des nombres que l'on souhaite additionner ou multiplier.

2.4 Congruences

On dit que deux entiers naturels a et b sont congrus modulo n s'ils se terminent par le chiffre lorsqu'ils sont écrits en base n. On peut généraliser aux entiers relatifs en disant que deux entiers relatifs a et b sont congrus modulo n s'ils ont même reste dans la division euclidienne par n. En fait, on préfère classiquement prendre la définition suivante peut-être moins visuelle mais qui a l'avantage non négligeable de ne pas utiliser de notions compliquées et qui est ainsi plus facilement maniable :

Definition 3. Soient a et b deux entiers relatifs. On dit que a et b sont *congrus* modulo n (et on note $a \equiv b \pmod{n}$) si n divise la différence $a - b$.

Les propriétés qui disent que le dernier chiffre d'une somme ou d'un produit se calcule simplement en utilisant les derniers chiffres des termes ou des facteurs se retraduisent directement en termes de congruence. Plus précisément, on a la propriété suivante :

Théorème 4. *Si a, a', b et b' sont des entiers relatifs tels que $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors :*

$$a + b \equiv a' + b' \pmod{n}$$
$$ab \equiv a'b' \pmod{n}$$

Nous allons démontrer ce théorème. Par hypothèse n divise $a - a'$ et $b - b'$, il divise donc la somme $(a - a') + (b - b') = (a + b) - (a' + b')$, ce qui signifie exactement que :

$$a + b \equiv a' + b' \pmod{n}$$

Pour la multiplication, on écrit $a' = a + kn$ et $b' = b + ln$. Ainsi :

$$a'b' = ab + n\left(kb + al + knl\right)$$

et donc finalement :

$$ab \equiv a'b' \pmod{n}$$

[1] Cela permet d'ailleurs de donner un sens précis et agréable à ce qu'est le dernier chiffre d'un entier négatif.

3 Équations dans $\mathbb{Z}/n\mathbb{Z}$

3.1 $\dot{x} + \dot{a} = \dot{b}$

Comme dans le cas $n = 10$, il est facile de constater que tout nombre admet un opposé. Pour cela, il suffit de prouver que si a est un entier, relatif, il existe toujours a' tel que $a + a' \equiv 0 \pmod{n}$. Bien entendu, il suffit de prendre $a' = -a$.

Cela signifie que l'on peut passer les éléments de l'autre côté de l'égalité en changeant le signe bien sûr, comme on le fait classiquement pour résoudre ces équations.

3.2 $\dot{a}\dot{x} = \dot{b}$

Ici, déjà dans le cas $n = 10$, on a vu que ce n'était pas toujours possible de *diviser*. Nous allons dans ce chapitre donner un critère qui explique lorsque l'on a le droit de diviser et qui explique ce que l'on a quand même le droit de faire si ce n'est pas le cas. Pour cela, nous aurons besoin de faire quelques rappels sur le plus grand diviseur commun (PGCD).

3.2.1 Notion de PGCD

Definition 5. Soient a et b deux entiers non tous les deux nuls. Le PGCD de a et b (noté $\text{PGCD}\,(a, b)$) le plus grand des diviseurs commun à a et à b.

Remarquons qu'il n'y a pas de problèmes avec cette définition : l'ensemble des entiers divisant à la fois a et b est fini, il en existe bien donc un plus grand. Remarquons également la chose suivante. Si $d = \text{PGCD}\,(a, b)$, on a toujours l'équivalence suivante :

$$x \text{ divise } d \quad \Leftrightarrow \quad x \text{ divise } a \text{ et } x \text{ divise } b$$

Une autre façon de présenter le PGCD de a et de b, si $b \neq 0$ disons, est de dire qu'il s'agit du plus grand entier par lequel on peut simplifier la fraction $\frac{a}{b}$. En particulier, dire que cette fraction est irréductible c'est exactement dire que $\text{PGCD}\,(a, b) = 1$. On dit dans ce cas que les entiers a et b sont *premiers entre eux*.

Une chose intéressante est que le calcul du PGCD peut se faire simplement et de façon systématique. Pour cela, on applique ce que l'on appelle couramment l'*algorithme d'Euclide*. On commence par écrire a et b l'un à côté de l'autre en mettant le plus grand des deux à gauche[2]. On effectue ensuite la division euclidienne du dernier nombre écrit avec celui qui le précède et on inscrit le reste de cette division à droite du dernier nombre. On continue ainsi jusqu'à obtenir un reste nul. Le PGCD cherché est alors le dernier nombre non nul écrit.

Voyons peut-être un exemple. Supposons que l'on veuille calculer $\text{PGCD}\,(1848, 804)$. On écrit donc :

$$1848 \quad 804 \quad 240 \quad 84 \quad 72 \quad 12 \quad 0$$

En effet, le reste de la division euclidienne de 1848 par 804 est 240, celui de la division euclidienne de 804 par 240 est 84 et ainsi de suite. On déduit de cela que le PGCD cherché est 12.

Une démonstration du fait que cet algorithme retrouve effectivement le PGCD et même un petit complément sont fournis dans l'exercice 2.

[2] Si $a = b$, le PGCD cherché est cette valeur commune.

3.2.2 Cas où a est premier avec n

Théorème 6. *$\dot{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a et n sont premiers entre eux.*

Nous n'allons pas prouver complètement ce théorème, donnons toutefois quelques idées. Notons $d = \text{PGCD}\,(a, n)$ et supposons dans un premier temps que $d \neq 1$. Dans ce cas tout multiple de a sera encore un multiple de d mais être un multiple de d, comme d divise n, se traduit en base n simplement en disant que le dernier chiffre reste parmi les chiffres multiples de d. On voit bien alors que 1 ne pourra jamais être dernier chiffre, et donc que $\dot{a}$ n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$.

La réciproque est un peu plus compliquée, il s'agit en fait d'une application directe du théorème de Bézout. Celui-ci est énoncé et démontré dans l'exercice 2. Cet exercice fournit même un moyen de calculer effectivement l'inverse.

Ce résultat a pour conséquence directe la chose suivante :

Théorème 7 (Lemme de Gauss). *Soient a, b et c trois entiers. On suppose que a divise le produit bc et que a et b sont premiers entre eux. Alors a divise c.*

En effet plaçons nous dans $\mathbb{Z}/a\mathbb{Z}$ (on peut bien entendu supposer $a \geqslant 2$). L'hypothèse nous dit que $\dot{b}\dot{c} = \dot{0}$ et que $\dot{b}$ est inversible. En multipliant par son inverse, on obtient directement $\dot{c} = \dot{0}$ et donc la conclusion voulue.

Une remarque importante à faire est que si p est un nombre premier, les entiers $1, \ldots, p-1$ sont tous premiers avec p. Ainsi tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. Autrement dit, dans $\mathbb{Z}/p\mathbb{Z}$ quand p est premier, les choses se passent un peu comme dans $\mathbb{R}$: pour diviser, il s'agit juste de faire attention à ce que le nombre par lequel on divise soit non nul.

Attention, cela n'est plus vrai si p n'est pas premier : on a vu par exemple de $\dot{2}$ n'est pas inversible dans $\mathbb{Z}/10\mathbb{Z}$.

Voici par exemple une table des inverses de $\mathbb{Z}/7\mathbb{Z}$:

a	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\mathbf{a}^{-1}$	$\times$	$\dot{1}$	$\dot{4}$	$\dot{5}$	$\dot{2}$	$\dot{3}$	$\dot{6}$

3.2.3 Cas général

On rappelle que l'on a à résoudre l'équation :

$$ax = b \pmod{n}$$

Notons $d = \text{PGCD}\,(a, n)$ et supposons $d \neq 1$. On remarque dans un premier temps que si b n'est pas un multiple de d, l'équation n'a pas de solutions.

Si maintenant b lui aussi est un multiple de d, l'équation se réécrit sous la forme :

$$\left(\frac{a}{d}\right) x = \frac{b}{d} \pmod{\frac{n}{d}}$$

Mais ce coup-ci les quantités $\frac{a}{d}$ et $\frac{n}{d}$ sont premières entre elles, et donc on peut inverser $\frac{a}{d}$ modulo $\frac{n}{d}$ comme on l'a vu dans le cas précédent. Il est important de noter ici que les solutions

sont définies modulo $\frac{n}{d}$, en particulier si l'on veut vraiment résoudre l'équation dans $\mathbb{Z}/n\mathbb{Z}$, on aura d solutions.

Mais prenons plutôt un exemple sans doute plus parlant. Disons que l'on veuille résoudre dans $\mathbb{Z}/10\mathbb{Z}$, l'équation $\dot{4}\dot{x} = \dot{2}$. 4 et 10 ne sont pas premiers entre eux, leur PGCD est 2. Comme 2 est un multiple de 2, on sait déjà qu'il va y avoir des solutions et même deux solutions.

Pour les trouver, on divise on divise notre équation par 2, et il faut donc résoudre dans $\mathbb{Z}/5\mathbb{Z}$, la nouvelle équation $\dot{2}\dot{x} = \dot{1}$. $\dot{2}$ admet bien un inverse dans $\mathbb{Z}/5\mathbb{Z}$, c'est $\dot{3}$. On multiplie donc notre équation par $\dot{3}$ et on obtient :

$$\dot{x} = \dot{3}$$

dans $\mathbb{Z}/5\mathbb{Z}$. Les solutions dans $\mathbb{Z}/10\mathbb{Z}$ sont donc $\dot{3}$ et $\dot{8}$.

3.3 $\dot{a}^x = \dot{b}$

3.3.1 Puissances successives de $\dot{a}$

Posons par exemple $u_k = \dot{a}^k$ pour tout entier naturel k. On obtient une suite à valeurs dans l'ensemble fini $\mathbb{Z}/n\mathbb{Z}$. Ainsi il va exister deux entiers i et j tels que $u_i = u_j$ et disons $i < j$. Mais u_{k+1} se calcule seulement à partir de u_k, simplement en multipliant par $\dot{a}$ et donc on en déduit que $u_{i+1} = u_{j+1}$, puis $u_{i+2} = u_{j+2}$ et ainsi de suite.

Cela prouve en fait que la suite (u_k) va être périodique de période $j - i$ au moins à partir du rang i.

Toutefois, il n'est pas vrai en général que cette suite est périodique à partir du rang 0. Plus exactement, il est facile de calculer $u_0 = \dot{1}$. Si la suite était périodique à partir du rang 0, il existe un entier $k > 0$ tel que $u_k = 1$. Mais alors $\dot{a} \cdot \dot{a}^{k-1} = \dot{1}$ et donc $\dot{a}$ serait inversible. Ainsi si $\dot{a}$ n'est pas inversible, notre suite n'est pas périodique dès le commencement.

Déterminer le rang à partir duquel la suite devient périodique et la plus courte période est un problème en général difficile. Nous allons, dans le paragraphe suivant, essayer de donner quelque élément de réponse lorsque $\dot{a}$ est inversible.

3.3.2 Cas où a est premier avec n

Lorsque a est premier avec n (ou encore lorsque $\dot{a}$ est inversible), la suite définie précédemment est en fait périodique à partir du rang 0.

Il n'est en fait pas difficile de voir cela. On sait déjà qu'il existe des entiers $i < j$ tels que :

$$\dot{a}^i = \dot{a}^j$$

Notons maintenant $\dot{a}'$ un inverse de $\dot{a}$, c'est-à-dire un élément de $\mathbb{Z}/n\mathbb{Z}$ tel que $\dot{a}\dot{a}' = \dot{1}$. En multipliant l'égalité précédente par $(\dot{a}')^i$, il vient :

$$\dot{a}^{j-i} = \dot{1}$$

ce qui prouve bien ce que l'on veut.

3.3.3 Fonction indicatrice d'Euler

Calculer la période n'est vraiment pas quelque chose de facile. Par contre, il n'est pas très difficile de déteminer un nombre k tel que $\dot{a}^k = \dot{1}$, le problème étant que ce n'est pas forcément le plus petit.

Nous allons pour cela définir une fonction φ qui s'appelle la *fonction indicatrice* d'Euler. Si $n \geqslant 2$ est un entier, $\varphi(n)$ désigne le nombre d'entiers naturels inférieurs à n et premiers avec n. Il s'agit donc d'après ce que l'on a vu précédemment du cardinal de l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 8. *Soit $\dot{a}$ un inversible de $\mathbb{Z}/n\mathbb{Z}$, alors :*

$$\dot{a}^{\varphi(n)} = \dot{1}$$

On peut reformuler le théorème précédent simplement en termes de congruences :

Théorème 9. *Soit a et n deux entiers premiers entre eux. Alors :*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

On insiste bien sur le fait que l'hypothèse de relative primalité est primordiale, cela est totalement faux sinon.

Nous n'allons pas prouver ce théorème : cela n'est pas bien difficile lorsque l'on connait un peu de théorie des groupes, il n'est pas d'ailleurs bien difficile non plus de refaire le peu de théorie des groupes qui nous manque pour arriver à cette conclusion mais cela n'entre pas dans le cadre de ce cours.

Un cas particulier intéressant du théorème précédent est quand même celui où $n = p$ est un nombre premier. Dans ce cas, on a vu que tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ étaient en fait inversibles. Le théorème nous dit donc que si $\dot{a} \in \mathbb{Z}/p\mathbb{Z}$ est tel que $\dot{a} \neq \dot{0}$, alors $\dot{a}^{\varphi(p)} = \dot{1}$. Mais $\varphi(p)$ est par définition le nombre d'inversibles de $\mathbb{Z}/p\mathbb{Z}$. Comme seul $\dot{0}$ n'est pas inversible, on a $\varphi(p) = p - 1$. Ainsi $\dot{a}^{p-1} = \dot{1}$. Mais cela n'est vrai que si $\dot{a} \neq \dot{0}$. Pour ne pas avoir à distinguer ce cas particulier, il est usuel de multiplier l'égalité précédente par $\dot{a}$ qui donc deviendra vraie même si $\dot{a}$ est nul. On vient donc de prouver le théorème suivant :

Théorème 10 (Petit théorème de Fermat). *Soit p un nombre premier. Pour tout $\dot{a} \in \mathbb{Z}/p\mathbb{Z}$, on a l'égalité :*

$$\dot{a}^p = \dot{a}$$

On peut bien entendu énoncer le même théorème avec des congruences. Il devient :

Théorème 11 (Petit théorème de Fermat). *Soit p un nombre premier. Pour tout entier a, on a la congruence :*

$$a^p \equiv a \pmod{p}$$

Ce dernier résultat peut en fait se démontrer de façon relativement simple. Sans prétendre faire une preuve complète, nous donnons ici quelques éléments pour y aboutir. Le premier point est de vérifier que si p est premier et si k est un entier compris au sens large entre 1 et $p - 1$, alors le nombre :

$$C_p^k = \frac{p\,(p-1)\dots(p-k+1)}{k\,(k-1)\dots 1}$$

est un multiple de p.

On utilise ensuite la formule du binôme de Newton qui dit :

$$(x+y)^p = \sum_{k=0}^{p} C_p^k x^k y^{n-k}$$

On déduit de ces deux remarques que pour tous entiers x et y, on a la congruence :

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

Par récurrence ensuite, on prouve que si $x_1, \ldots, x_n$ sont des entiers, on a de façon analogue la congruence :

$$(x_1 + \ldots + x_n)^p = x_1^p + \ldots + x_n^p \pmod{p}$$

On applique ensuite ce résultat avec $n = a$ et $x_1 = \ldots = x_a = 1$.

3.3.4 Formule pour $\varphi(n)$

Théorème 12. *Si la décomposition en facteurs premiers de l'entier n est :*

$$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$$

alors $\varphi(n)$ peut se calculer à l'aide de la formule suivante :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

La preuve de ce théorème fait l'objet de l'exercice 3.

3.4 $\dot{a}\dot{x}^2 + \dot{b}\dot{x} + \dot{c} = 0$

3.4.1 Dans $\mathbb{Z}/p\mathbb{Z}$, p premier impair

On utilise pour résoudre la méthode classique, celle du discriminant. Plus précisément, on écrit successivement les étapes suivantes :

$$\begin{aligned}
\dot{a}\dot{x}^2 + \dot{b}\dot{x} + \dot{c} &= 0 \\
\dot{a}\left(\dot{x}^2 + \frac{\dot{b}}{\dot{a}}\dot{x} + \frac{\dot{c}}{\dot{a}}\right) &= 0 \\
\dot{a}\left(\dot{x} + \frac{\dot{b}}{\dot{2}\dot{a}}\right)^2 - \frac{\dot{b}^2}{\dot{4}\dot{a}} + \frac{\dot{c}}{\dot{a}} &= 0 \\
\left(\dot{x} + \frac{\dot{b}}{\dot{2}\dot{a}}\right)^2 &= \frac{\dot{\Delta}}{\dot{4}\dot{a}^2}
\end{aligned}$$

où $\dot{\Delta} = \dot{b}^2 - \dot{4}\dot{a}\dot{c}$.

Bien entendu, les divisions par $\dot{2}$, $\dot{4}$ et $\dot{a}$ correspondent respectivement aux multiplications par les inverses de ces nombres. C'est pour cela qu'il est important de supposer que p est impair

dans un premier temps. On ne voit pas encore bien où intervient de façon cruciale le fait que p soit premier, il aurait pour l'instant seulement fallu qu'il soit premier avec a. Mais cela vient.

Il s'agit maintenant de déterminer une racine carrée de $\dot{\Delta}$, c'est-à-dire un élément $\dot{\delta} \in \mathbb{Z}/p\mathbb{Z}$ tel que $\dot{\delta}^2 = \dot{\Delta}$. Il existe un critère pour savoir dans un premier temps si un tel élément existe et le calculer effectivement par la suite. Cela est présenté dans l'exercice 4. Supposons qu'on ait trouvé un tel élément et continuons la question.

L'équation devient :

$$\begin{aligned} \left(\dot{x} + \frac{\dot{b}}{\dot{2}\dot{a}}\right)^2 &= \left(\frac{\dot{\delta}}{\dot{2}\dot{a}}\right)^2 \\ \left(\dot{x} + \frac{\dot{b}+\dot{\delta}}{\dot{2}\dot{a}}\right)\left(\dot{x} + \frac{\dot{b}-\dot{\delta}}{\dot{2}\dot{a}}\right) &= 0 \end{aligned}$$

On est donc arrivé à un produit nul, la question est de savoir si l'on peut en déduire que l'un des facteurs est nul. La réponse est *oui* mais cela bien parce que l'on a supposé p premier (penser par exemple que dans $\mathbb{Z}/10\mathbb{Z}$, $\dot{2} \cdot \dot{5} = \dot{0}$). En effet, supposons que le premier facteur soit non nul, alors il est inversible et on trouve que le deuxième facteur est nul après avoir multiplié par l'inverse en question.

3.4.2 Dans $\mathbb{Z}/n\mathbb{Z}$, c'est plus compliqué

C'est en effet plus compliqué, et je ne connais pas de méthode générale pour résoudre l'équation. Déjà calculer une racine carrée est du même ordre de complexité que déterminer la décomposition en facteurs premiers de n. Mais même une fois cela fait, cela ne résout pas du tout le problème.

Une approche peut-être pas trop mauvaise est la suivante. Supposons que l'on connaisse la décomposition en facteurs premiers de n, disons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Il est alors bon de commencer par chercher les solutions dans les $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ et de recoller les morceaux grâce à ce que l'on appelle le lemme chinois et qui est présenté dans l'exercice 3.