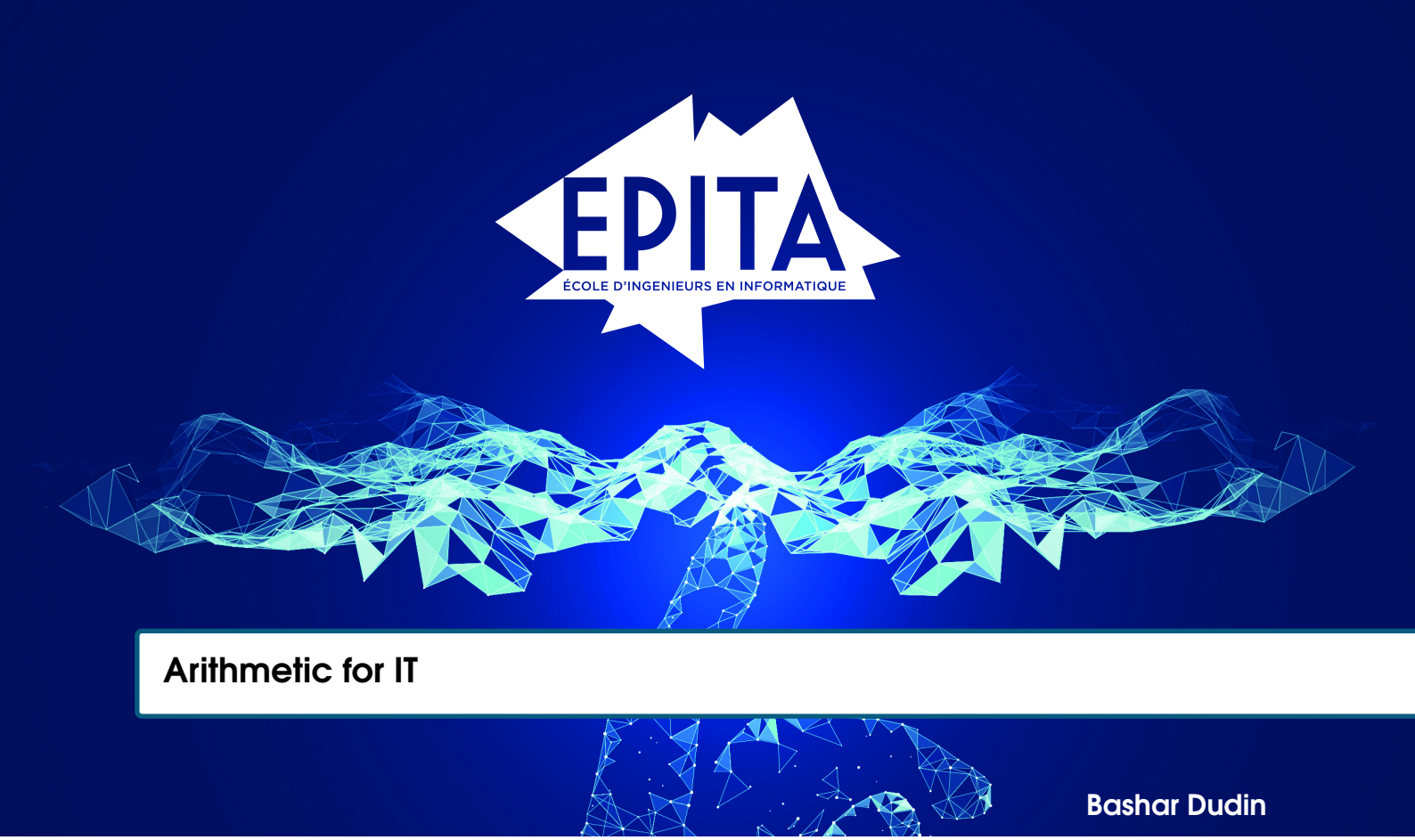

Arithmetic for IT

Bashar Dudin

Résumé

Ce document est la référence principale pour le contenu du projet ***AFIT*** (Arithmetic for IT). Ce projet vise à générer du chiffrement de données à l'aide des algorithmes RSA et ElGamal, dans un but pédagogique. Ce faisant, les étudiants devront assimiler les notions élémentaires d'arithmétique nécessaires pour générer et manipuler de tels systèmes de cryptage.

Table des matières

1 Introduction

> L'arithmétique est une branche des mathématiques consistant en l'étude des "nombres", et plus particulièrement des propriétés des opérations traditionnelles – addition, soustraction, multiplication et division [1].

En arithmétique des nombres entiers, la divisibilité est une notion au centre de nombreuses questions : est-ce que deux nombres donnés sont multiples l'un de l'autre ? Y a-t-il des nombres spécifiques qui n'ont aucun diviseur non trivial ? Peut-on décomposer un entier donné comme un produit d'entiers plus simples (voire le plus simples possible) ? Vous connaissez déjà la réponses à certaines de ces questions. Les nombres qui ne peuvent être divisés que par eux-mêmes, leur opposé ou ± 1 sont appelés ***nombres premiers***. Ainsi, tout entier peut se décomposer de manière unique (si ce n'est l'ordre) comme un produit de nombres premiers.

Ces questions, simples en apparence, sont au cœur des différents usages de l'arithmétique en informatique. Même en exceptant le fait que les ordinateurs sont des calculateurs d'entiers, les questions de divisibilité sont au centre des systèmes de chiffrement permettant un échange d'informations sécurisé entre deux parties ; en supposant qu'une troisième partie ait accès à l'information échangée, il sera encore trop difficile de la déchiffrer pour retrouver le message initial.

L'algorithme de chiffrement le plus connu, ***RSA*** [2], se base sur le fait que factoriser un nombre qui est le produit de deux nombres premiers est une question difficile et qui nécessite beaucoup de ressources, en temps comme en espace. En revanche, calculer des puissances d'entiers modulo un entier fixé prend beaucoup moins de temps.

Le but de ce projet est de vous faire parcourir l'arithmétique nécessaire pour essayer de générer des systèmes de chiffrement d'une taille raisonnable. Cependant ne vous y trompez pas ; ***nous serons encore relativement loin des implémentations d'algorithmes de chiffrement utilisées en réalité.***

2 Guide de lecture

Ce document doit servir de référence mathématique pour un projet de programmation nécessitant des notions élémentaires d'arithmétique modulaire. Il contient des exemples, preuves et discussions permettant de comprendre la raison fondamentale pour laquelle les résultats mathématiques utilisés sont énoncés tels quels et pas autrement. Tout ce que vous lirez ici s'y trouve pour une (bonne) raison, la moindre d'entre toutes étant de mettre un peu de sens dans un certain nombre d'énoncés apparemment inattendus.

Ceci dit, il n'y a pas besoin de posséder une connaissance en profondeur de tous les aspects traités dans ce document pour pouvoir rendre un travail satisfaisant sur ce projet ***AFIT***. ***N'hésitez pas à chercher de la documentation externe*** ; ce document doit servir de trame pour vos propres recherches. Si vous trouvez des références qui vous permettent de mieux comprendre le sujet et les attentes de votre projet, ***servez-vous en !***

Voici une liste des sujets abordés, classés par priorité (de la plus haute à la plus basse). C'est un bon ordre de lecture indicatif.

- La section 3 concerne des connaissances de base en arithmétique et doit être complètement maîtrisée ; une partie de cette section reformule les propriétés et résultats vus en cours.
- La section 4, jusqu'à la sous-section 4.4 incluse est d'une importance capitale si vous voulez être capable d'écrire vos premiers systèmes de chiffrement.
- La section 6 est le but principal de ce projet ***AFIT***. Même si l'on mettra plus l'accent sur l'algorithme ***RSA***, on attend de vous que vous puissiez implémenter les deux.
- Les sections 4.5 et 5 représentent des défis un peu plus exigeants, il vous est conseillé de les laisser de côté tant que vos implémentations des cryptosystèmes RSA et ElGamal n'ont pas été testées avec succès.

3 Arithmétique des entiers

Cette section présente un rappel succinct des sujets abordés en arithmétique élémentaire. Des primitives `OCaml` seront données pour les opérations basiques d'arithmétique que vous utiliserez dans vos implémentations.

Hypothèse 3.1 Nos énoncés se focaliseront sur les résultats concernant les entiers naturels. Tous peuvent être étendus au cas des entiers relatifs, mais nous n'en aurons pas besoin ici.

1. `https://en.wikipedia.org/wiki/Arithmetic` (traduit de l'anglais).
2. d'après les initiales de ses inventeurs : *Rivest*, *Shamir* et *Adleman*.

3.1 Division euclidienne

Définition 3.1 Si l'on considère un couple d'entiers naturels (n, p), on dit que p divise n, ce que l'on note par $p \mid n$, s'il existe un entier $k \in \mathbb{N}$ tel que $n = kp$.

R Un entier n est dit ***pair*** si $2 \mid n$, sinon il est dit ***impair***.

R Tout entier divise 0. En effet, pour tout $n \in \mathbb{N}$ on peut écrire $0 = 0 \times n$.

Si l'on prend deux entiers naturels au hasard, les chances que l'un soit diviseur de l'autre sont faibles. Il est cependant possible de pallier le manque de divisibilité par l'opération appelée ***division euclidienne***.

Proposition 3.2 Pour tout couple d'entiers naturels $(a,b) \in \mathbb{N} \times \mathbb{N}^*$, il existe un unique couple (q,r) d'entiers naturels vérifiant

$$a = bq + r \quad \text{avec } 0 \leq r < b.$$

R Le premier élément du couple (q,r) est appelé ***quotient*** de a par b, le second est appelé ***reste*** dans la division euclidienne de a par b. On l'abrège aussi en ***reste de*** a ***modulo*** b.

Démonstration. La proposition précédente contient en fait deux résultats, l'un concernant l'unicité, l'autre l'existence. Supposons qu'il existe deux couples (q,r) et (q',r') vérifiant la propriété ; alors

$$bq + r = bq' + r' \Rightarrow b(q - q') = r' - r.$$

Maintenant, le terme de droite appartient à l'intervalle entier $[\![-(b-1); b-1]\!]$, cependant ce doit être un multiple de b. Ce ne peut donc être que 0. Ainsi $r = r'$, d'où $q = q'$.
L'existence est basée sur l'algorithme suivant :

- Si $0 \leq a < b$ alors $(0,a)$ vérifie la propriété
- Sinon, on ajoute 1 au quotient puis on examine la division euclidienne de $a - b$ par b.

Cet algorithme se termine en un nombre fini d'étapes à cause d'une propriété structurelle de $\mathbb{N}$: toute partie non vide de $\mathbb{N}$ admet un élément minimal. Il faut donc montrer que l'ensemble $\{q \in \mathbb{N} \mid a - bq < b\}$ n'est pas vide. L'intuition semble indiquer que c'est bien le cas, puisque le membre de gauche de la condition peut être rendu aussi négatif que l'on veut. C'est en effet vrai, mais cela vient d'un fait important que nous n'avons pas montré. Sachant qu'il est non vide, il admet un élément minimal q^*. Pour q^* l'expression $a - bq^*$ ne peut donc qu'être positive. En effet, comme q^* est le plus petit élément vérifiant $a - bq^* < b$ alors $a - b(q^* - 1) \geq b$. Remarquez que la dernière inégalité est obtenue en ajoutant b au membre de gauche. Ainsi, les deux inégalités ne peuvent pas être vraies simultanément si $a - bq^*$ n'est pas positif, car sinon, en ajoutant b au membre de gauche on ne pourrait pas obtenir un résultat plus grand que b. □

En `OCaml` il n'y a pas de primitive qui calcule une division euclidienne d'un seul coup, mais deux opérateurs infixes qui calculent respectivement le quotient et le reste : `/` et `mod`.

R En utilisant la caractérisation donnée par la division euclidienne, "$b \mid a$" équivaut à " le reste dans la division euclidienne de a par b est 0". Ainsi, pour tester si un nombre a est un multiple de b en `OCaml` on écrit :

```
let est_divisible a b = (a mod b = 0) ;;
```

3.2 Primalité

Définition 3.2 Un nombre naturel strictement supérieur à 1 est dit ***premier*** s'il n'admet comme diviseurs (positifs) que 1 et lui-même.

Vérifier si un nombre donné n est premier est un problème difficile ; il n'y a pas d'autre option que de parcourir la liste des entiers naturels inférieurs et de tester la divisibilité. En réalité il suffit de s'arrêter à $\lfloor \sqrt{n} \rfloor$; en effet, si $k \mid n$ alors n/k divise

lui aussi n. Si l'on écrit les couples $(k, n/k)$ de diviseurs de n on voit qu'à partir de $\sqrt{n}$ on obtient les couples symétriques, c'est-à-dire dont les entrées sont dans l'ordre inverse. Par exemple, pour les diviseurs de 36 on obtient

$$\begin{array}{cc} (1,36) & (36,1) \\ (2,18) & (18,2) \\ (4,9) & (9,4) \\ (6,6) & \end{array}$$

L'importance des nombres premiers apparaît grâce au résultat fondamental suivant :

Théorème 3.3 Tout nombre naturel non nul[a] n peut être décomposé en un produit de nombres premiers. Cette décomposition est unique si l'on ne tient pas compte de l'ordre des termes.

a. cela inclut donc 1 que l'on peut écrire comme un produit vide. Pour rappel, un produit vide représente l'élément neutre de la multiplication, c'est-à-dire 1.

R Un nombre premier qui apparaît dans la décomposition de n est appelé facteur de n. On parle ainsi souvent de "décomposition en facteurs premiers".

Ce théorème énonce *grosso modo* qu'il suffit de connaître les nombres premiers pour comprendre l'architecture des entiers naturels. Le fait est que générer des nombres premiers d'une part, reconnaître si un nombre est premier d'autre part, sont des problèmes relativement compliqués. On peut se consoler en considérant un problème plus simple à résoudre, celui de savoir si deux entiers naturels choisis ont des facteurs premiers en commun.

Définition 3.3 Deux entiers naturels non nuls sont dits ***premiers entre eux*** s'ils n'ont aucun facteur premier en commun.

Pour résoudre le problème que nous venons d'introduire, nous allons définir un nouveau concept : le PGCD de deux entiers.

Définition 3.4 Le PGCD (Plus Grand Commun Diviseur) de deux entiers non nuls a et b est le plus grand entier d vérifiant $d \mid a$ et $d \mid b$.

Avant d'aller plus loin, il reste un point à clarifier : pourquoi un tel entier existerait-il bien ?

— 1 vérifie toujours les deux propriétés, ce qui signifie que l'ensemble des entiers naturels vérifiant ces deux propriétés est non vide.

— Tout entier vérifiant ces propriétés est par ailleurs inférieur à $\min\{|a|, |b|\}$, ce qui implique que l'ensemble est majoré. Ce qui nous ramène à la propriété fondamentale de $\mathbb{N}$ selon laquelle toute partie non vide et majorée de $\mathbb{N}$ admet un élément maximum.

N Le PGCD de deux entiers naturels non nuls a et b est noté $a \wedge b$.

Proposition 3.4 Deux entiers naturels non nuls a et b sont premiers entre eux si et seulement si $a \wedge b = 1$.

3.3 Algorithme d'Euclide

Cet algorithme est crucial pour tout ce qui concerne les applications de l'arithmétique en informatique. C'est grâce à lui notamment que l'on peut générer des clés publiques et privées pour l'algorithme RSA, ou encore que l'on peut paralléliser les calculs d'entiers.

L'idée de cet algorithme se base sur la remarque suivante : si a et b sont deux entiers naturels non nuls, leur division euclidienne donne un couple (q, r) d'entiers naturels tels que

$$a = bq + r \qquad 0 \leq r < b. \tag{1}$$

Si d divise a et b alors il divise aussi $a - bq$; si $a = kd$ et $b = \ell d$,

$$a - bq = kd - q\ell d = (k - q\ell)d.$$

Ainsi, d divise r. Cela est vrai pour n'importe quel diviseur commun de a et b, et plus particulièrement pour leur PGCD. Supposoons alors que l'on répète ce procédé : en notant $r_0 = a$, $r_1 = b$, $q_1 = q$ et $r_2 = r$, l'équation (1) devient

$$r_0 = q_1 r_1 + r_2 \qquad 0 \leq r_2 < r_1 \tag{2}$$

où chaque diviseur de r_0 et r_1 est également un diviseur de r_2. En itérant

$$\begin{array}{rcl} q_{n+1} & = & r_n / r_{n+1} \\ r_{n+2} & = & r_n \mod r_{n+1} \end{array}$$

on obtient une suite de relations via divisions euclidiennes successives

$$\begin{array}{ccccccc} r_0 & = & q_1 r_1 & + & r_2 & & 0 \leq r_2 < r_1 \\ r_1 & = & q_2 r_2 & + & r_3 & & 0 \leq r_3 < r_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ r_{n-1} & = & q_n r_n & + & r_{n+1} & & 0 \leq r_{n+1} < r_n \end{array}$$

À chaque niveau de ce système d'équations, tout diviseur commun de r_{n+1} et r_n est un diviseur de r_{n+2}. De plus, à chaque niveau le reste r_n est un entier strictement inférieur au reste précédent – à moins que celui-ci ne soit déjà 0. Tous les restes obtenus sont des entiers positifs, il y a donc nécessairement une étape à laquelle on atteint 0. Notons ℓ l'indice du dernier reste non nul dans la suite précédente. On a alors

$$\begin{array}{ccccccc} r_0 & = & q_1 r_1 & + & r_2 & & 0 \leq r_2 < r_1 \\ r_1 & = & q_2 r_2 & + & r_3 & & 0 \leq r_3 < r_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ r_{n-1} & = & q_n r_n & + & r_{n+1} & & 0 \leq r_{n+1} < r_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ r_{\ell-2} & = & q_{\ell-1} r_{\ell-1} & + & r_\ell & & 0 \leq r_\ell < r_{\ell-1} \\ r_{\ell-1} & = & q_\ell r_\ell & & & & \end{array} \tag{3}$$

Regardons ces équations de bas en haut. Le dernier reste non nul r_ℓ divise $r_{\ell-1}$. D'après la ligne précédente, il doit aussi diviser $r_{\ell-2}$. En remontant ainsi toutes les équations, on se rend compte que r_ℓ divise r_0 et r_1, c'est-à-dire a et b. En conséquence [3], $r_\ell \mid a \wedge b$. Si l'on descend le système d'équations maintenant, on voit vite par récurrence que tout diviseur d commun à r_0 et r_1 divise aussi r_ℓ, c'est donc le cas pour $a \wedge b$. On obtient donc $a \wedge b \mid r_\ell$ et *vice versa* ; ainsi $r_\ell = a \wedge b$.

Proposition 3.5 Le dernier reste non nul obtenu par l'algorithme précédent est le PGCD des deux termes de départ.

R Il est légitime de se demander combien de divisions euclidiennes successives on doit effectuer au maximum pour obtenir le PGCD de deux entiers naturels. Un majorant évident est b, la suite (r_n) des restes étant strictement décroissante de premier terme b. Il existe en fait une bien meilleure [4] approximation supérieure, qui est $2\log_2(b)+2$. Il n'est pas nécessaire de comprendre comment obtenir ce résultat, il donne cependant une bonne idée de la vitesse de l'algorithme d'Euclide.

R Déterminer si deux entiers non nuls sont premiers entre eux revient à exécuter l'algorithme d'Euclide et à trouver 1 comme dernier reste non nul.

3. En réalité, on n'a pas encore expliqué que tout diviseur commun divise le PGCD. Ceci dit, même sans utiliser cette propriété, on obtient $r_\ell \leq a \wedge b$, ce qui suffit pour cette preuve : au lieu de conclure à l'égalité par divisibilité réciproque, on utilise des inégalités réciproques.

4. on peut même (théorème de Lamé) obtenir $\log_\varphi(b)$ soit $\dfrac{\ln(b)}{\ln(\varphi)}$, où φ désigne le nombre d'or ; cela correspond à un peu moins de 5 fois le nombre de chiffres de b en base 10. L'approximation donnée n'est pas si mauvaise puisque cela revient à un peu moins de $\dfrac{3}{2}\, log_2(b)$. Cette complexité ne tient pas compte des étapes de conclusion, d'où le $+2$ dans la formule donnée.

3.4 Théorème de Bézout

Cette sectionest dédiée au théorème de Bézout, qui énonce l'existence d'une combinaison diophantienne [5] de deux entiers donnés égale à leur PGCD ; c'est-à-dire que le PGCD de deux nombres peut s'écrire comme somme (différence) de multiples entiers de ces deux nombres.

Théorème 3.6 Pour tout couple (a,b) d'entiers naturels non nuls, il existe [a] un couple d'entiers relatifs (u,v) vérifiant

$$ua+vb=a\wedge b.$$

a. un tel couple n'est jamais unique

Ⓡ De tels entiers u et v sont appelés coefficients de Bézout associés à a et b.

Démonstration. La preuve est constructive et basée sur l'algorithme d'Euclide. Elle consiste essentiellement en une réécriture des équations 3. En isolant à droite les restes des divisions successives on obtient

$$\begin{array}{ccccc} a & - & q_1 b & = & r_2 \\ b & - & q_2 r_2 & = & r_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{\ell-2} & - & q_{\ell-1} r_{\ell-1} & = & a\wedge b \end{array} \tag{4}$$

Si l'on parcourt ce système en remontant, on voit qu'il est à chaque fois possible d'exprimer les restes en fonctions des deux restes précédents ; en utilisant cette propriété de manière transitive on peut donc exprimer tous les restes en fonction de a and b. Cela peut également être montré en descendant par une récurrence finie. Voici une manière un peu plus visuelle de le constater [6]. Regardez les trois équations qui suivent, dont la dernière est la première équation de notre algorithme 4 :

$$\begin{array}{ccccc} 1\times a & - & 0\times b & = & r_0 \\ 0\times a & - & 1\times b & = & r_1 \\ 1\times a & - & q_1\times b & = & r_2 \end{array} \tag{5}$$

Remarquez que l'on obtient la dernière équation en ôtant q_1 fois la seconde à la première. En fait, ce schéma se propage jusqu'à ce que le PGCD apparaisse dans le membre de droite de l'équation ; par exemple, pour la division euclidienne de r_1 par r_2 (la seconde équation de 4), en soustrayant à la seconde équation q_2 fois la troisième dans 5 on obtient

$$\begin{array}{ccccc} 1\times a & + & 0\times b & = & r_0 \\ 0\times a & + & (-1)\times b & = & r_1 \\ 1\times a & + & (-q_1)\times b & = & r_2 \\ (-q_2)\times a & + & (-1+q_1q_2)\times b & = & r_3 \end{array} \tag{6}$$

En continuant étape par étape, en effectuant les divisions euclidiennes des restes successifs (les membres de droite) on fait finalement apparaître une relation entre a, b, et $a\wedge b$ qui s'écrit donc comme une combinaison entière des deux. Si l'on désigne par (u_n) et (v_n) les suites de coefficients respectivement associés à a et b, on obtient des définitions récursives de ces deux suites données par la relation :

$$\begin{cases} u_{n+1} = u_{n-1}-q_n u_n \\ v_{n+1} = v_{n-1}-q_n v_n \end{cases} \tag{7}$$

Cette relation sera le point de départ d'une implémentation convenable [7] de l'algorithme de Bézout que vous devrez essayer de réaliser. □

Corollaire 3.7 Deux entiers naturels a et b sont premiers entre eux si et seulement s'il existe un couple de relatifs (u,v) vérifiant

$$ua+vb=1. \tag{8}$$

5. ou combinaison entière
6. qui, de plus, permet de l'implémenter !
7. la méthode naïve qui consiste à faire toutes les divisions puis remonter serait une perte de temps, mais surtout d'espace phénoménale !

Démonstration. Si a et b sont premiers entre eux, alors $a \wedge b = 1$. D'après le théorème 3.6 il existe un couple (u,v) vérifiant la relation attendue. Maintenant s'il existe une relation telle que la relation 8, alors tout diviseur commun de a et b est aussi un diviseur de 1. Puisque $a \wedge b$ est un diviseur positif de 1, il ne peut être que 1 ; ainsi a et b sont premiers entre eux. □

Nous avons déjà brièvement évoqué la complexité de l'algorithme d'Euclide. Celle de l'algorithme étendu qui donne les coefficients de Bézout est similaire en temps [8]. Ainsi, nous avons bien un algorithme efficace pour déterminer si deux entiers naturels sont premiers entre eux. Mais ce n'est qu'une des nombreuses applications de cet algorithme ; nous y reviendrons plus tard.

4 Arithmétique modulaire

Les entiers ne sont pas les seuls objets mathématiques sur lesquels on peut utiliser les résultats d'arithmétique ; bien qu'au départ prévue pour les nombres, cette théorie s'adapte à beaucoup d'autres objets partageant certaines propriétés structurelles avec les entiers. En particulier, la structure principale dans laquelle on utilise l'arithmétique est celle que l'on appelle un ***anneau***. L'ensemble $\mathbb{Z}$ des entiers relatifs peut être muni d'une telle structure, mais c'est le cas de nombreux autres ensembles. Nous allons en étudier quelques exemples simples sur lesquels nous nous contenterons d'effectuer des calculs de base.

4.1 Jour de la semaine

Avant de nous plonger au cœur de l'arithmétique modulaire, prenons le temps d'examiner un exemple basique d'application de cette théorie : le calcul du jour de la semaine selon la date.

Question 4-1 Supposons que nous soyons un lundi aujourd'hui ; comment calculer quel jour de la semaine nous serons dans 37 jours ?

Une manière simple de répondre à cette question est de numéroter les jours de la semaine de 0 à 6 en commençant par le jour d'aujourd'hui : lundi. Tous les 7 jours on retombe sur un lundi –certains d'entre vous le savent peut-être déjà :-p . La division euclidienne de 37 par 7 donne

$$37 = 5 \times 7 + 2.$$

On repasse donc 5 fois par lundi avant de continuer jusqu'à mercredi, qui est le jour portant le numéro 2. Ainsi, le seul nombre pertinent dans cette question est `37 mod 7`. Cela est vrai dans le cas général : si l'on compte n jours à partir du lundi initial, on arrive au jour portant le numéro `n mod 7` (c'est un entier entre 0 et 6).

Essayons de formaliser tout ça pour expliquer de manière plus rigoureuse comment calculer ainsi les jours de la semaine. On va partir du premier jour de notre ère d'après le calendrier grégorien : le 1er janvier de l'an 0001 était un samedi [9]. On note $\mathscr{W}$ l'ensemble des indices représentant les jours de la semaine :

$$\mathscr{W} = \{0,1,2,3,4,5,6\},$$

en initialisant en faisant correspondre le 0 au samedi. On va de plus supposer que le nombre de jours avant et après le 1er janvier 0001 est infini [10].

On appellera ***date*** le nombre de jours avant ou après le « zéro », c'est-à-dire l'origine fixée au 1er janvier 0001, afin d'éviter l'ambiguïté entre le jour de la semaine que l'on cherche à calculer et la date.

Le problème principal peut alors être reformulé en :

> Quel est le jour de la semaine correspondant à une date $d \in \mathbb{Z}$ donnée ?

Nous avons déjà donné la réponse à cete question plus haut : ***il suffit de trouver le reste de la division euclidienne de*** d ***modulo*** 7**.**

8. regardez l'espace mémoire supplémentaire nécessaire en analysant votre implémentation
9. well-known fact :-)
10. Ce qui, en ce qui concerne les jours avant, est difficile à concevoir, et en ce qui concerne les jours après, est plutôt mal parti …

Attention : la primitive `OCaml mod` ne donne pas le résultat attendu si l'argument préfixe (i.e. celui de gauche) est négatif. La fonction `OCaml mod` renvoie l'opposé du reste de la division de la valeur absolue de l'argument préfixe si celui-ci est négatif, ce qui ne coïncide pas avec la définition de la division standard (euclidienne) des entiers : en effet celle-ci garde la même définition [11] pour les entiers relatifs que pour les naturels, le reste est donc toujours un nombre positif.

Les calculs utilisés pour déterminer le jour de la semaine correspondant à une date impliquent un certain nombre de compatibilités heureuses, en ce qui concerne l'addition et la multiplication.

Par exemple, on pourrait se demander si le $37^{\text{ème}}$ jour après un vendredi (6) est le même que le $(37 \bmod 7)^{\text{ème}}$ jour après un vendredi. Le jour que nous recherchons est le $43^{\text{ème}}$ jour après samedi, on peut alors écrire

$$43 = 6 \times 7 + 1$$

ce qui nous dit que l'on cherche un dimanche. Nous avons fait l'opération suivante :

```
(37 + 6) mod 7.
```

Si l'on essaie le calcul (qui correspond à la suggestion précédente) :

```
((37 mod 7) + (6 mod 7)) mod 7
```

on retrouve le même résultat. C'est un fait général. Si l'on se donne deux dates d_1 et d_2, on peut écrire ainsi leurs divisions euclidiennes par 7 :

$$d_1 = 7 \times q_1 + r_1 \tag{9}$$
$$d_2 = 7 \times q_2 + r_2 \tag{10}$$

En additionnant ces deux équations on obtient :

$$(d_1 + d_2) = 7 \times (q_1 + q_2) + (r_1 + r_2).$$

Mais ici, $(r_1 + r_2)$ n'est pas forcément plus petit que 7. Si l'on refait la division

$$(r_1 + r_2) = 7 \times s + t$$

on obtient

$$(d_1 + d_2) = 7 \times (q_1 + q_2 + s) + t$$

où t est positif et strictement inférieur à 7. D'après les deux dernières relations, on peut déduire que

$$(r_1 + r_2) \mod 7 = (d_1 + d_2) \mod 7$$

ce qui est exactement ce que nous avons conclu dans notre exemple.

Il se passe la même chose si l'on utilise des multiplications. Supposons que l'on veuille déterminer quel jour nous serons après 3 périodes de 32 jours. Cela fait 96 jours, le jour en question est donc donné par `96 mod 7 = 5` : c'est un jeudi. On obtient exactement le même résultat si l'on fait

```
((3 mod 7) * (32 mod 7)) mod 7
```

Cette propriété également est toujours vraie ; en réutilisant les équations 9 on peut écrire :

$$d_1 d_2 = 7 \times (7 q_1 q_2 + q_2 r_1 + q_1 r_2) + r_1 r_2$$

mais encore une fois $r_1 r_2$ n'est pas forcément positif et strictement inférieur à 7. En utilisant une division supplémentaire

$$r_1 r_2 = 7 \times s + t$$

on parvient à la division euclidienne

$$d_1 d_2 = 7 \times (7 q_1 q_2 + q_2 r_1 + q_1 r_2 + s) + t$$

dont on peut déduire que

$$d_1 d_2 \mod 7 = r_1 r_2 \mod 7.$$

En résumé :

11. le reste de la division de a par b est compris entre 0 et $|b| - 1$

— Le jour de la semaine associé à une date d est le reste dans la division euclidienne de d par 7.
— Le jour de la semaine atteint après deux périodes d_1 et d_2 est le reste modulo 7 de la somme d_1+d_2, ou de manière équivalente la somme modulo 7 des restes de d_1 et d_2 modulo 7.
— Le point précédent est également vrai pour l'opération de multiplication. Le reste de la multiplication de deux nombres d_1 et d_2 modulo 7 est le même nombre que celui obtenu en multipliant les deux restes de d_1 et d_2 modulo 7, puis en prenant le reste modulo 7 du résultat.

Les opérations dont nous venons de parler sont une manifestation simple de propriétés plus générales, et de constructions d'importance capitale en arithmétique. Elles jouent un rôle très important en ce qui concerne la programmation entière.

4.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Nous n'allons pas définir formellement ce qu'est un anneau. Il suffit ici de savoir que c'est un ensemble muni de deux opérations binaires, l'***addition*** et la ***multiplication*** qui ont les mêmes propriétés [12] que l'addition et la multiplication d'entiers. L'anneau sur lequel nous allons travailler est basé sur un ensemble ***fini***. Ceci est d'une importance capitale du point de vue machine : tout ce qui se passe dans un tel anneau devrait être implémentable en machine – si ce n'est en ce qui concerne les problèmes de mémoire (dépassements par exemple).

Définition 4.1 Soit $n>1$ un entier positif. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble

$$\mathbb{Z}/n\mathbb{Z}=\{0,\dots,n-1\}=[\![0;n-1]\!]$$

muni des deux opérateurs binaires $\oplus$ et $\otimes$ définis comme suit : étant donnés deux éléments x et y appartenant à $\mathbb{Z}/n\mathbb{Z}$:

$$x\oplus y=(x+y) \mod n \qquad \text{(addition)}$$

$$x\otimes y=(x\times y) \mod n. \qquad \text{(multiplication)}$$

Exemple 4.1 L'exemple le plus simple est $n=2$. Dans ce cas $\mathbb{Z}/2\mathbb{Z}=\{0,1\}$. L'addition et la multiplication sont simplement données par les règles de calcul suivantes :

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

Exemple 4.2 Le cas $n=3$ représente l'ensemble $\{0,1,2\}$ muni des lois d'addition et de multiplication suivantes :

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

En pratique, on est souvent intéressé par la projection d'un entier quelconque modulo un entier positif donné. On peut représenter cette approche du problème par la fonction :

$$\pi_n : \begin{cases} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & x \mod n \end{cases}$$

Exemple 4.3 L'image d'un élément $x\in\mathbb{Z}$ par π_2 nous dit si x est pair ou impair. Si $\pi_2(x)=0$ alors x est pair, il est impair sinon. Si l'image de x par π_3 est 0, alors x est divisible par 3. Si $\pi_3(x)=1$ alors x est de la forme $3k+1$ pour un certain $k\in\mathbb{Z}$.

12. Associativité de l'addition et de la multiplication, distributivité de la multiplication sur l'addition, commutativité de l'addition. La multiplication n'est pas forcément commutative (dans le cas étudié elle le sera). De plus, ces deux lois admettent un élément neutre (0 pour l'addition et 1 pour la multiplication) et chaque élément admet un opposé par l'addition.

N Il est fréquent de noter $\bar{x}_n$ la quantité $\pi_n(x)$ ou $x \mod n$. Selon le contexte (s'il n'y a pas d'ambiguïté), on peut même se passer de l'indice.

De nombreuses questions en arithmétique moderne se résument à :

> Soit x un entier dont les restes $\bar{x}_n$ modulo un grand nombre d'entiers positifs n vérifient une propriété $\mathscr{P}$. Est-ce que x satisfait aussi $\mathscr{P}$?

Exemple 4.4 Soit $\mathscr{P}$ la propriété «être plus petit que 100». Prenons un entier x, si l'on regarde les quantités $\bar{x}_n$ pour $n \leq 100$ on ne peut absolument rien en déduire quant à la question de savoir si $x \leq 100$. En effet, n'importe quel nombre aura un reste inférieur à 100 si l'on fait la division modulo un nombre inférieur à 100. De même, le fait que $\bar{x}_{101}$ soit plus petit que 100 ne signifie pas que x l'est aussi. Par exemple $\overline{102}_{101} = 1$. En réfléchissant à la question, on se rend compte que si $x \leq 100$ alors tous les restes modulo $n \geq 101$ seront égaux à x. La réciproque [a] est également vraie : si ***tous*** les restes $\bar{x}_n$ pour $n \geq 101$ sont égaux à x alors $x \leq 100$.

a. intéressante pour sa contraposée : s'il existe un nombre $n \geq 101$ tel que $\bar{x}_n \neq x$ alors $x > 100$.

R L'exemple précédent est un exemple un peu simpliste, pour des questions de recherche plus précises, n'hésitez pas à demander !

Les compatibilités mises en lumière dans la section 4.1, à propos du comportement de l'addition et de la multiplication par rapport aux opérations de modulo, sont des propriétés générales que l'on exprime par : soient deux entiers x et y dans $\mathbb{Z}$ alors

$$\overline{(x+y)}_n = \bar{x}_n \oplus \bar{y}_n \qquad \text{(addition)}$$

$$\overline{(xy)}_n = \bar{x}_n \otimes \bar{y}_n. \qquad \text{(multiplication)}$$

N Dans ce domaine, les abus de notation sont fréquents. La plupart du temps, la barre $\bar{\cdot}$ et l'indice sont sous-entendus. C'est également les cas des notations $\oplus$ et $\otimes$ qui ne sont pas standard ; on les remplace simplement par $+$ and $-$. Dans la suite, nous ne les utiliserons plus. Cela mis à part, soit on gardera à la fois le $\bar{\cdot}$ et l'indice, soit on laissera tomber les deux ; on utilisera aussi la notation suivante : pour x et y dans $\mathbb{Z}$ alors l'égalité

$$\bar{x}_n = \bar{y}_n$$

s'écrit aussi

$$x \equiv y \ [n]$$

ou encore

$$x \equiv_n y.$$

L'égalité est remplacée par le symbole $\equiv$ et $[n]$ indique que nous regardons les restes de x et y modulo n, ce qui correspond à $\bar{x}_n$ et $\bar{y}_n$ dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, les compatibilités précédentes peuvent être réécrites de la manière suivante :

$$x + y \equiv \bar{x}_n + \bar{y}_n \ [n] \qquad \text{(addition)}$$

$$xy \equiv \bar{x}_n \bar{y}_n \ [n] \qquad \text{(multiplication)}$$

4.3 Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Si l'on se penche sur la multiplication des nombres rationnels ou réels, on sait que pour tout nombre non nul $x \in \mathbb{R}^*$ il existe un nombre y tel que $xy = 1$. Par exemple, si $x = 2$ alors $y = 0.5$. En général, ce n'est pas le cas dans $\mathbb{Z}/n\mathbb{Z}$. Voici par exemple la table de multiplication de $\mathbb{Z}/4\mathbb{Z}$:

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

.

On peut voir que tout élément x différent de 0 et 2 admet un homologue y tel que $xy \equiv 1 \ [n]$. Le fait est que 2 n'est pas nul mais n'admet pas de tel homologue, un comportement différent de ce à quoi vous êtes habitués.

Définition 4.2 Un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible s'il existe $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $xy \equiv 1\ [n]$.

L'élément y est alors ***unique*** et appelé inverse de x dans $\mathbb{Z}/n\mathbb{Z}$.

N L'inverse d'un élément inversible $x \in \mathbb{Z}/n\mathbb{Z}$ est notée x^{-1}. L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^\times$. On note aussi $\varphi(n)$ le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$; cela correspond au cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$. Dans la littérature, $\varphi(n)$ est appelé indicatrice d'Euler de n.

Soit x un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ dont l'inverse est y. Par définition cela signifie $xy \equiv 1\ [n]$; de manière plus explicite, il existe $k \in \mathbb{Z}$ tel que

$$xy + kn = 1. \tag{11}$$

Si l'on se reporte au théorème de Bézout, cela implique que n et x sont premiers entre eux. Réciproquement, si x et n sont premiers entre eux, il existe une relation du type 11, modulo n cela montre que x admet en y une inverse.

Proposition 4.1 L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des éléments de $\{0,\dots,n-1\}$ qui sont premiers avec n. Cet ensemble est appelé groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 4.2 Si p est un nombre premier, tous les éléments de $\{1,\dots,p-1\}$ sont inversibles, i.e.

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1,\dots,p-1\}.$$

Démonstration. Tout entier qui n'est pas un multiple de p est premier avec p. C'est en particulier le cas de tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$. □

Écrire une fonction qui teste si un entier est inversible modulo n consiste à utiliser proprement l'algorithme d'Euclide ; nous sommes déjà capables de faire ceci. La recherche peut être facilitée drastiquement dans un certain cas, si l'on connaît un peu mieux les propriétés intrinsèques des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 4.3 Si x et y sont deux éléments inversibles modulo n alors xy est aussi inversible modulo n.

Démonstration. Notons x^{-1} et y^{-1} les inverses respectives de x et y. Le produit $y^{-1}x^{-1}$ est alors l'inverse de xy. □

Ainsi, si l'on a trouvé un élément inversible, toutes les puissances de cet élément sont encore des éléments inversibles.

Exemple 4.5 Par exemple, dans le cas de $\mathbb{Z}/5\mathbb{Z}$ le groupe multiplicatif est $\{1,2,3,4\}$. Les puissances de 1 ne permettent de trouver que 1. Mais les puissances de 2 modulo 5 engendrent l'ensemble $\{1,2,3,4\}$.

On n'aura pas toujours la chance de pouvoir trouver un entier dont les puissances engendrent le groupe multiplicatif, i.e. qui permet de trouver tous les éléments dudit groupe.

Exemple 4.6 Dans le cas de $\mathbb{Z}/8\mathbb{Z}$, le groupe multiplicatif est $\{1,3,5,7\}$. On peut vérifier que le carré de chacun des éléments de $(\mathbb{Z}/8\mathbb{Z})^\times$ vaut 1. Si l'on cherche donc parmi les puissances d'un élément inversible x, ici on ne trouve aucun autre élément inversible, mis à part 1 dans le cas où $x \neq 1$.

Le sous-ensemble du groupe multiplicatif composé des différents éléments que l'on peut engendrer en cherchant parmi les puissances d'un élément inversible donné a un grand intérêt en arithmétique modulaire (modulo n). De tels sous-ensembles peuvent par exemple être une bonne mesure de la solidité d'une clé privée RSA. Pour le cryptosystème ElGamal, des données publiques valides consistent partiellement en un élément qui engendre le groupe multiplicatif d'un anneau $\mathbb{Z}/n\mathbb{Z}$ spécifique. La section qui suit se consacre à regarder plus en détail les puissances d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$.

4.4 Petit théorème de Fermat

Définition 4.3 Soit x un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ (i.e. un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$). On appelle ordre de x ***le*** plus petit $k \in \mathbb{N}^*$ tel que $x^k \equiv 1\ [n]$. L'ordre de x modulo n est noté $\mathrm{ord}_n(x)$.

Exemple 4.7 Dans le cas $n = 8$, les éléments inversibles de $\mathbb{Z}/8\mathbb{Z}$ sont 1, 3, 5, 7. Le premier est d'ordre 1, les autres d'ordre 2.

Exemple 4.8 Le groupe multiplicatif de $\mathbb{Z}/9\mathbb{Z}$ est composé des éléments 1, 2, 4, 5, 7 et 8, d'ordres respectifs 1, 6, 3, 6, 3 et 2.

L'article défini mis en valeur dans la définition 4.3 suggère qu'il existe toujours un tel plus petit entier strictement positif et donc que l'ordre de x est bien défini. Cela exprime de manière implicite le fait que l'ensemble $\{k \in \mathbb{N}^* \mid x^k \equiv 1\ [n]\}$ n'est pas vide. Bien que nous ayons vérifié ce fait sur deux exemples, nous n'avons pas jusqu'à présent démontré que cela était forcément le cas.

Théorème 4.4 Soit x un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. Alors $x^{\varphi(n)} \equiv 1\ [n]$.

Démonstration. Afin de simplifier les notations, notons G_n le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$. La preuve que nous donnons ici se base sur une compréhension structurelle de l'action des éléments de G_n sur leur environnement. Soit m_x la fonction de G_n vers G_n qui à y associe xy. Par exemple, avec $n = 9$ et $x = 2$ la fonction m_2 a pour domaine (et ensemble d'arrivée) $G_9 = \{1,2,4,5,7,8\}$. Elle envoie la liste d'éléments $[1;2;4;5;7;8]$ vers la liste $[2;4;8;1;5;7]$, c'est-à-dire :

$$\begin{array}{ccc} 1 & \to & 2 \\ 2 & \to & 4 \\ 4 & \to & 8 \\ 5 & \to & 1 \\ 7 & \to & 5 \\ 8 & \to & 7 \end{array}$$

On peut vérifier que m_2 définit ainsi une bijection de G_9 vers lui-même ; c'est ce que nous appellons une permutation. L'ensemble image de m_2 est ici égal à G_9. Cette observation se généralise : m_x est toujours une permutation de G_n.

Pour montrer que m_x est injective, supposons qu'il existe deux éléments y_1 et y_2 de G_n tels que $m_x(y_1) = m_x(y_2)$. Cela signifie :

$$xy_1 \equiv xy_2\ [n].$$

Par définition x est inversible, en multipliant la relation précédente par x^{-1} on obtient alors $y_1 \equiv y_2\ [n]$.

Pour constater que m_x est surjective, on peut voir que pour tout élément y de G_n, l'élément $t = x^{-1}y$ de G_n vérifie $m_x(t) = y$.

Le fait que m_x soit bijective implique l'égalité des ensembles

$$\{xy \mid y \in G_n\} = \{y \mid y \in G_n\}.$$

En conséquence, le produit de tous les éléments de l'ensemble de gauche et celui de tous les éléments de l'ensemble de droite sont égaux (les ensembles contiennent les mêmes éléments). Ainsi [13]

$$x^{\varphi(n)} \Big(\prod_{y \in G_n} y \Big) \equiv \Big(\prod_{y \in G_n} y \Big)\ [n].$$

Comme le produit d'éléments inversibles est encore inversible, en multipliant la relation précédente par l'inverse du terme de droite on obtient

$$x^{\varphi(n)} \equiv 1\ [n],$$

ce qui est le résultat attendu. □

Corollaire 4.5(Petit théorème de Fermat Soit p un nombre premier, et soit x un élément non nul de $\mathbb{Z}/p\mathbb{Z}$; alors

$$x^{p-1} \equiv 1\ [p].$$

Démonstration. L'ensemble des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ est encore l'ensemble de ses éléments non nuls, dans ce cas-là $\varphi(p) = p - 1$. □

13. Cette preuve, simple, utilise la commutativité de la multiplication. Le résultat reste vrai même si l'on enlève cette hypothèse.

Ⓡ Le petit théorème de Fermat s'énonce également ainsi : pour tout x de $\mathbb{Z}/p\mathbb{Z}$, $x^p \equiv x\ [p]$. Cet énoncé est équivalent au précédent si x est inversible : en multipliant cette équation par x^{-1} on retrouve 4.5. Si x n'est pas inversible, il est nul, et la relation donne alors $0 \equiv 0\ [p]$ ce qui est encore vrai.

Dans les deux exemples 4.7 et 4.8, on a $\varphi(8) = 4$ et $\varphi(9) = 6$. Les ordres des éléments inversibles de $\mathbb{Z}/8\mathbb{Z}$ sont tous des diviseurs de $\varphi(8)$. C'est également le cas pour les inversibles de $\mathbb{Z}/9\mathbb{Z}$; en fait c'est un résultat général.

Proposition 4.6 Soit x un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. Un élément $m \in \mathbb{N}^*$ vérifie $x^m \equiv 1\ [n]$ si et seulement si c'est un multiple de $\mathrm{ord}_n(x)$.

Démonstration. Notons k l'ordre de x modulo n. La division euclidienne de m par k donne la relation $m = kq + r$ où $0 \leq r < k$. Ainsi, on obtient

$$x^m \equiv x^{kq}x^r\ [n] \tag{12}$$
$$1 \equiv x^r\ [n]. \tag{13}$$

Si r était strictement positif, alors r vérifierait $x^r \equiv 1\ [n]$ tout en étant strictement plus petit que k, ce qui contredirait la définition de k (qui est le plus petit entier strictement positif tel que $x^k \equiv 1\ [n]$). Nécessairement $r = 0$, et m est donc un multiple de l'ordre de x. □

Corollaire 4.7 L'ordre d'un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ divise $\varphi(n)$.

Démonstration. Cela découle du fait que $x^{\varphi(n)} \equiv 1\ [n]$, d'après 4.4. □

4.5 Théorème des restes chinois

Il est fréquent en mathématiques d'essayer de comprendre un objet en le décrivant comme étant composé de plusieurs sous-objets plus faciles à comprendre. C'est également une philosophie très répandue en informatique : c'est plus ou moins le principe des stratégies de "diviser pour régner" ; sans parler du fait qu'un logiciel est principalement pensé comme une série de composants reliés, chacun voué à une tâche particulière. Dans le cas de l'arithmétique modulaire, il est possible de décomposer de nombreux ensembles $\mathbb{Z}/n\mathbb{Z}$ en produits cartésiens d'ensembles $\mathbb{Z}/m\mathbb{Z}$ plus petits : c'est ce que nous allons évoquer dans cette section.

Soient m et n deux entiers premiers entre eux, plus grands que 1. On considère la fonction

$$\psi : \begin{cases} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ x & \longmapsto & (\bar{x}_n, \bar{x}_m) \end{cases}$$

qui à $x \in \{0, \ldots, nm-1\}$ associe le couple formé de ses restes modulo n et modulo m respectivement, ce qui donne un couple de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Exemple 4.9 Considérons par exemple le cas $(n,m) = (2,3)$. La fonction ψ a pour domaine de départ $\mathbb{Z}/6\mathbb{Z}$ et d'arrivée $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Voici la liste des images des 6 éléments de $\mathbb{Z}/6\mathbb{Z}$ par ψ :

$$\begin{array}{ccc} 0 & \to & (0,0) \\ 1 & \to & (1,1) \\ 2 & \to & (0,2) \\ 3 & \to & (1,0) \\ 4 & \to & (0,1) \\ 5 & \to & (1,2) \end{array}$$

On remarque tout de suite que cette fonction est bijective ; ainsi $\mathbb{Z}/6\mathbb{Z}$ contient autant d'information que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Le résultat est encore plus puissant : les opérations arithmétiques sur $\mathbb{Z}/6\mathbb{Z}$ se reflètent sur $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ via la fonction ψ. Définissons les opérations d'addition et de multiplication sur $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ comme suit : pour tout (x_1,x_2) et (y_1,y_2) dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, on a

$$(x_1,x_2) + (y_1,y_2) = (x_1 + y_1, x_2 + y_2) \qquad \text{(addition)}$$
$$(x_1,x_2) \times (y_1,y_2) = (x_1y_1, x_2y_2). \qquad \text{(multiplication)}$$

Ce sont en fait l'addition et la multiplication coordonnée par coordonnée. Voici les tables d'addition et de multiplication

pour $\mathbb{Z}/6\mathbb{Z}$ muni des opérations usuelles, et pour $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ avec les opérations que l'on vient de définir.

$\mathbb{Z}/6\mathbb{Z}$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$

$+$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(1,1)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$	$(0,0)$
$(0,2)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$	$(0,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,1)$	$(1,2)$	$(0,0)$	$(1,1)$	$(0,2)$
$(0,1)$	$(0,1)$	$(1,2)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$
$(1,2)$	$(1,2)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$

$\times$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,1)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(0,2)$	$(0,0)$	$(0,2)$	$(0,1)$	$(0,0)$	$(0,2)$	$(0,1)$
$(1,0)$	$(0,0)$	$(1,0)$	$(0,0)$	$(1,0)$	$(0,0)$	$(1,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,2)$	$(0,0)$	$(1,2)$	$(0,1)$	$(1,0)$	$(0,2)$	$(1,1)$

Les éléments $x\in\mathbb{Z}/6\mathbb{Z}$ et leurs images $\psi(x)\in\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ occupent la même position dans leurs tableaux respectifs. En examinant ceux-ci de plus près, on peut vérifier les deux faits suivants : pour tout x, $y\in\mathbb{Z}/6\mathbb{Z}$ on a

$$\psi(x+y)=\psi(x)+\psi(y)\qquad\psi(x\times y)=\psi(x)\times\psi(y).$$

Pour résumer, ψ est une bijection qui transforme les opérations arithmétiques de son domaine de définition en les opérations analogues de son ensemble d'arrivée. On peut donc faire au choix les opérations voulues sur le tableau de droite, puis les utiliser pour obtenir des résultats sur celui de gauche, ou bien l'inverse.

L'exemple précédent n'est qu'un cas particulier d'un résultat général. Ce résultat est explicité par le théorème des restes chinois, dont voici l'énoncé.

Théorème 4.8 Soient n et m deux entiers strictement supérieurs à 1 et premiers entre eux. La fonction

$$\psi:\begin{cases}\mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}\\ x & \longmapsto & (\bar{x}_n,\bar{x}_m)\end{cases}$$

est bijective ; de plus pour tout $(x,y)\in(\mathbb{Z}/nm\mathbb{Z})^2$ on a les compatibilités

$$\psi(x+y)=\psi(x)+\psi(y)\qquad\text{(addition)}$$
$$\psi(x\times y)=\psi(x)\times\psi(y).\qquad\text{(multiplication)}$$

R Il faut prendre garde au fait que les opérations arithmétiques dans les compatibilités ci-dessus ne sont pas définies de la même façon des deux côtés de l'égalité. À gauche on a l'opération telle qu'on l'entend dans $\mathbb{Z}/nm\mathbb{Z}$, à droite l'opération coordonnée par coordonnée dans $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$.

Démonstration. Les compatibilités de l'addition et de la multiplication sont indépendantes du caractère bijectif de ψ. Si l'on prend deux éléments x et y de $\mathbb{Z}/nm\mathbb{Z}$, alors par définition

$$\psi(x+y)=\left(\overline{(x+y)}_n,\overline{(x+y)}_m\right)\tag{14}$$

en utilisant la compatibilité du modulo avec l'addition

$$\psi(x+y)=(\bar{x}_n+\bar{y}_n,\bar{x}_m+\bar{y}_m)\tag{15}$$

par définition de l'addition dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$$\psi(x+y) = (\bar{x}_n, \bar{y}_m) + (\bar{x}_n, \bar{y}_m) \tag{16}$$

enfin, par définition de ψ

$$\psi(x+y) = \psi(x) + \psi(y) \tag{17}$$

En appliquant le même raisonnement à la multiplication, on arrive à

$$\psi(x \times y) = \psi(x) \times \psi(y).$$

Regardons maintenant les aspects injectif et surjectif. La raison principale pour laquelle ψ est à la fois surjective et injective vient du fait que n et m sont premiers entre eux. Ce résultat peut en fait être étendu à des contextes beaucoup plus larges.

Injectivité de ψ :

Supposons qu'il existe deux éléments x et y de $\mathbb{Z}/nm\mathbb{Z}$ ayant la même image par ψ, i.e. $\psi(x) = \psi(y)$. Ceci équivaut à

$$\begin{array}{rcl} \bar{x}_n & \equiv & \bar{y}_n \ [n] \\ \bar{x}_m & \equiv & \bar{y}_m \ [m] \end{array}$$

Ainsi

$$\begin{array}{rcl} \overline{(x-y)}_n & \equiv & 0 \ [n] \\ \overline{(x-y)}_m & \equiv & 0 \ [m] \end{array}$$

donc n et m divisent tous les deux $x-y$. Le PPCM de n et m divise alors $x-y$. Puisque $n \wedge m = 1$, ce PPCM est nm [14]. On obtient ainsi $x \equiv y \ [nm]$ qui est le résultat attendu.

Surjectivité de ψ :

Le côté surjectif de ψ peut être déduit d'un argument de cardinal : la fonction ψ est injective et les ensembles de départ et d'arrivée ont le même cardinal fini, elle est donc bijective. Mais comme toujours en informatique, il est plus intéressant d'exhiber une preuve constructive qui donne un moyen d'écrire la fonction réciproque de ψ : c'est la fonction ϕ qui à $y = (y_1, y_2) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ associe l'élément $x \in \mathbb{Z}/nm\mathbb{Z}$ tel que $\psi(x) = y$. Par hypothèse, on peut trouver des entiers u et v tels que

$$\begin{array}{rcll} vm & \equiv & 1 & [n] \\ un & \equiv & 1 & [m] \end{array}$$

L'entier $x = y_1 vm + y_2 un$ vérifie alors

$$\begin{array}{rcccl} y_1 vm + y_2 un & \equiv & y_1 vm & \equiv & y_1 \ [n] \\ y_1 vm + y_2 un & \equiv & y_2 un & \equiv & y_2 \ [m] \end{array}$$

ce qui signifie exactement $\psi(x) = y$. Ainsi, ϕ est définie par

$$\phi(y_1, y_2) = y_1 vm + y_2 un \ [nm]$$

où v et u sont les entiers, définis auparavant, qui viennent de la relation de Bézout, $y_1 \in \{0, \ldots, n-1\}$ et $y_2 \in \{0, \ldots, m-1\}$. Pour être plus précis, il faudrait vérifier qu'un choix différent de coefficients de Bézout (u', v') donnerait toujours la même fonction ϕ. Mais tout autre couple de coefficients de Bézout est de la forme $(u', v') = (u + km, v - kn)$ avec $k \in \mathbb{Z}$; l'expression devient alors

$$\begin{aligned} y_1 v'm + y_2 u'n &= y_1(v - kn)m + y_2(u + km)n && (18) \\ &= y_1 v + y_2 m + (-y_1 k + y_2 k)mn && (19) \\ &\equiv y_1 v + y_2 m \ [nm]. && (20) \end{aligned}$$

Un choix différent de coefficients de Bézout définit donc bien la même fonction réciproque ϕ. □

14. On le déduit du lemme de Gauss. La décomposition en facteurs premiers des PGCD et PPCM établit aussi ce résultat. Pour rappel : avec a et b positifs, $\text{PGCD}(a,b) \times \text{PPCM}(a,b) = a \times b$.

Exemple 4.10 Regardons un exemple simple pour établir une stratégie de calcul de l'antécédent d'un élément par ψ. Prenons $(n,m) = (4,7)$ et considérons le couple $(2,5) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Si l'on suit les étapes du raisonnement précédent, il nous faut d'abord trouver un couple de coefficients de Bézout associés aux nombres 4 et 7 premiers entre eux. Un calcul rapide permet d'obtenir

$$(-5) \times 4 + 3 \times 7 = 1.^a$$

L'élément

$$5 \times (-5) \times 4 + 2 \times 3 \times 7 \equiv 26\ [28]$$

a un reste modulo 4 égal à 2 et un reste modulo 7 égal à 5, i.e. $\psi(26) = (2,5)$.

a. Ce sont les coefficients donnés par l'algorithme d'Euclide, qui ne sont pas forcément les plus «simples» (ici 2 et -1 marchaient aussi).

Corollaire 4.9 Étant donné un entier $k > 1$, soit $m_1, \ldots, m_k$ une liste d'entiers strictement supérieurs à 1 qui sont deux à deux premiers entre eux. On note m le produit de tous les m_i. Alors la fonction

$$\psi : \begin{cases} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ x & \longmapsto & (\bar{x}_{m_1}, \ldots, \bar{x}_{m_k}) \end{cases}$$

est une bijection compatible avec l'addition et la multiplication coordonnée par coordonnée dans l'ensemble d'arrivée.

Démonstration. Nous n'allons qu'indiquer les étapes principales de la démonstration dans ce qui suit, formaliser le tout serait une perte de temps.

La compatibilité avec l'addition et la multiplication deux à deux est tautologique, issue du fait que l'opération modulo est elle-même compatible avec les deux. La preuve de la bijectivité est algorithmique ; elle se base sur une utilisation du théorème des restes chinois par récurrence pour construire une fonction réciproque.

Si l'on voulait vérifier l'injectivité de la fonction, on se trouverait exactement dans la même situation que lors de la preuve de 4.8. Deux éléments ayant la même image ont une différence divisible par m_1, …, m_k. Puisque ces entiers sont deux à deux premiers entre eux, ladite différence divise leur produit m. Ainsi les deux nombres sont égaux modulo m. Cela suffit même à montrer la bijectivité, encore une fois car les ensembles de départ et d'arrivée ont le même cardinal.

Voici comment construire l'image réciproque d'un élément $(y_1, \ldots, y_k)$: supposons qu'on a déjà l'antécédent $y_{1\cdots j}$ de $(y_1, \ldots, y_j)$ pour $1 \leq j < k$ in $\mathbb{Z}/(m_1 \cdots m_j)\mathbb{Z}$. Alors, l'antécédent de $(y_1, \ldots, y_j, y_{j+1})$ dans $\mathbb{Z}/(m_1 \cdots m_{j+1})\mathbb{Z}$ est

$$y_{1\cdots j} u m_{j+1} + y_{j+1} v (m_1 \cdots m_j)$$

où u et v sont des coefficients de Bézout associés au couple $(m_{j+1}, m_1 \cdots m_j)$. □

5 Intérêt du théorème des restes chinois

Un bon nombre de questions centrales en arithmétique reviennent à identifier des nombres premiers et des nombres inversibles. Le but est d'être capable de factoriser un élément non inversible donné selon ses composantes premières. La factorisation est un processus coûteux ; c'est la raison pour laquelle la méthode de chiffrement RSA est relativement sûre quand elle fait intervenir des nombres premiers assez grands. Une autre difficulté est liée au fait que calculer des puissances d'entiers suffisamment grands a un impact extrêmement coûteux sur les calculs. De nombreuses méthodes de cryptage standard se basent justement sur l'utilisation de puissances de grands nombres.

Le théorème des restes chinois peut aider à séparer en plusieurs sous-problèmes plus petits chacune des difficultés précédentes. C'est quelque chose que l'on peut déjà réaliser en ce qui concerne les puissances d'un entier.
Supposons que l'on travaille avec des entiers plus petits qu'un entier M fixé. Soit la décomposition

$$M = M_1 M_2 \cdots M_h$$

où les M_j sont deux à deux premiers entre eux. D'après le théorème des restes chinois, on a alors

$$\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/M_1\mathbb{Z} \times \cdots \times \mathbb{Z}/M_h\mathbb{Z}$$

où la notation $\simeq$ signifie qu'il existe entre les deux ensembles une bijection compatible avec les opérations arithmétiques ; c'est ce que l'on appelle un ***isomorphisme***. Si l'on prend des entiers positifs x et k tels que x^k est inférieur à M, alors on peut calculer x^k en regardant la $k^{\text{ème}}$ puissance de chaque composante de

$$\left(\bar{x}_{M_1}, \bar{x}_{M_2}, \ldots, \bar{x}_{M_h}\right)$$

puis en reconstruisant son image réciproque à l'aide du théorème chinois. Chaque calcul est plus rapide en utilisant le terme de droite, puisque les facteurs impliqués sont plus petits en premier lieu, mais aussi puisque, comme ce sont des constantes du système, on peut calculer en amont leurs indicatrices d'Euler et ainsi utiliser des simplifications (à base de divisions euclidiennes) pour pouvoir calculer les puissances.

Remarquez que si M est un nombre premier, ou une puissance d'un nombre premier, il n'est pas possible d'appliquer une telle stratégie ; dans ce cas-là le théorème des restes chinois ne donne aucune décomposition et n'est donc d'aucune aide.

L'approche précédente est l'approche canonique en ce qui concerne l'utilisation du théorème des restes chinois : si l'on veut faire une vérification, un test ou un calcul spécifique dans $\mathbb{Z}/M\mathbb{Z}$, on regarde l'image de notre donnée dans $\mathbb{Z}/M_1\mathbb{Z} \times \cdots \mathbb{Z}/M_h\mathbb{Z}$, on fait dans cet ensemble les calculs composante par composante, équivalents mais plus rapides, puis on retransforme les résultats pour les écrire dans $\mathbb{Z}/M\mathbb{Z}$.

5.1 Calcul d'inversibles

Revenons à l'exemple précédent : $\mathbb{Z}/6\mathbb{Z}$. Selon le théorème des restes chinois, nous avons un isomorphisme entre $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ donné par la fonction dont l'image est composée des réductions modulo 2 et 3 du nombre de départ.

$\mathbb{Z}/6\mathbb{Z}$
0
1
2
3
4
5

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

	0	1
0	(0,0)	(0,1)
1	(1,0)	(1,1)
2	(2,0)	(2,1)

Les éléments inversibles dans $\mathbb{Z}/6\mathbb{Z}$ sont les éléments grisés. Leurs images dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ sont les cellules grisées correspondant à $(1,1)$ et $(1,2)$. Dans $\mathbb{Z}/6\mathbb{Z}$, 1 est sa propre inverse, ce qui est également le cas pour 5. Si l'on multiplie $(1,1)$ et $(1,2)$ par eux-mêmes, on obtient $(1,1)$ pour le premier et $(1,4) = (1,1)$ pour le second. Ainsi, pour tout élément x parmi les deux précédents, il existe un élément y tel que $xy = (1,1)$. En un sens, on affirme que les deux éléments $(1,1)$ et $(1,2)$ sont inversibles dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Dans ce contexte, l'élément $(1,1)$ remplace l'élément 1 de $\mathbb{Z}/6\mathbb{Z}$. On l'appelle élément neutre de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ car la multiplication de tout élément de $z \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ par $(1,1)$ donne encore z. Une manière de reformuler cette remarque serait de dire que les éléments inversibles de $\mathbb{Z}/6\mathbb{Z}$ correspondent (via notre bijection) aux éléments inversibles de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

L'élément du produit $\mathbb{Z}/M_1\mathbb{Z} \times \cdots \times \mathbb{Z}/M_h\mathbb{Z}$ dont toutes les coordonnées sont égales à 1 est appelé élément neutre de cet ensemble produit. Le résultat de la multiplication de n'importe quel élément z par $(1,\ldots,1)$ vaut encore z. Un élément $x \in \mathbb{Z}/M_1\mathbb{Z} \times \cdots \times \mathbb{Z}/M_h\mathbb{Z}$ est dit inversible s'il existe un élément y tel que $xy = (1,\ldots,1)$. Ces définitions généralisent celles que nous avons vues précédemment dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition 5.1 Un élément $x \in \mathbb{Z}/M\mathbb{Z}$ est inversible si et seulement si son image $\psi(x)$ par l'isomorphisme donné par le théorème des restes chinois est inversible.

Démonstration. Soit x un élément inversible de $\mathbb{Z}/M\mathbb{Z}$. Par définition, il existe $y \in \mathbb{Z}/M\mathbb{Z}$ tel que $xy \equiv 1\ [M]$. En prenant l'image par ψ des deux membres de l'équation, on obtient

$$\psi(xy) = \psi(x)\psi(y) = (1,\ldots,1)$$

ce qui signifie exactement que tout élément inversible x de $\mathbb{Z}/M\mathbb{Z}$ est envoyé sur un élément inversible de $\mathbb{Z}/M_1\mathbb{Z} \times \cdots \times \mathbb{Z}/M_h\mathbb{Z}$.
Réciproquement, soit x un élément de $\mathbb{Z}/M\mathbb{Z}$ dont l'image $\psi(x)$ est inversible dans $\mathbb{Z}/M_1\mathbb{Z} \times \cdots \times \mathbb{Z}/M_h\mathbb{Z}$. Par définition, on peut trouver un élément $\bar{y} \in \mathbb{Z}/M_1 \times \cdots \times \mathbb{Z}/M_h\mathbb{Z}$ tel que $\psi(x)\bar{y} = (1,\ldots,1)$. Puisque ψ est un isomorphisme, il existe $y \in \mathbb{Z}/M\mathbb{Z}$ tel que $\psi(y) = \bar{y}$. Ainsi, on peut écrire

$$\psi(1) = (1,\ldots,1) = \psi(x)\psi(y) = \psi(xy).$$

En appliquant ψ^{-1} aux deux extrémités de l'égalité précédente, on obtient $xy \equiv 1\ [M]$. □

Corollaire 5.2 La fonction induite par ψ sur $(\mathbb{Z}/M\mathbb{Z})^\times$ définit une bijection

$$\psi^\times : (\mathbb{Z}/M\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/M_1 \times \cdots \times \mathbb{Z}/M_h\mathbb{Z})^\times$$

compatible avec la multiplication. L'image par cette fonction est le h-uplet composé des réductions modulo M_i de l'argument, comme c'est le cas pour ψ.

Afin de calculer l'inverse d'un élément x de $\mathbb{Z}/M\mathbb{Z}$, on peut :
- calculer l'image $(\bar{x}_1, \ldots, \bar{x}_h)$ de x par la fonction ψ dans $\mathbb{Z}/M_1 \times \cdots \times \mathbb{Z}/M_h\mathbb{Z}$;
- Trouver l'inverse $\bar{y}_i$ de chaque élément $\bar{x}_i$ dans $\mathbb{Z}/M_i\mathbb{Z}$ s'il y en a une ;
- si l'on ne peut pas réaliser l'étape précédente, x n'est pas inversible, sinon on calcule l'image réciproque y par ψ de $(\bar{y}_1, \ldots, \bar{y}_h)$;
- Le y obtenu est l'inverse de x.

5.2 Factorisation d'entiers

Avec un peu de travail, on peut adapter la stratégie "diviser pour régner" précédente à la résolution d'un autre problème épineux : la factorisation d'entiers inférieurs à M. Commençons par examiner le cas $M = 15$. Le théorème des restes chinois établit un isomorphisme ψ traduisant le résultat

$$\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Si l'on se place dans le membre de gauche, on obtient la décomposition $14 = 2 \times 7$. En prenant l'image par ψ des deux membres de cette égalité, on obtient l'équation $(2,4) = (2,2) \times (1,2)$, que l'on peut encore écrire

$$\psi(14) = (2,4) = (2 \times 1, 2 \times 2) = (2,2) \times (1,2) = \psi(2) \times \psi(7).$$

Cela suggère que factoriser 14 revient à factoriser chaque composante de son image par ψ, puis reconstruire l'image réciproque de chaque facteur par la fonction ψ. Pour que ceci ait du sens, il faudrait en premier lieu que chaque facteur ait un antécédent par ψ qui soit plus petit que l'entier que l'on essaie de factoriser : par exemple, si on prend 12, son image dans $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ est $(0,2)$, qui peut se décomposer comme étant le produit de $(0,4)$ et $(0,3)$. L'image réciproque de $(0,4)$ est 9 et celle de $(0,3)$ est 3. Le produit 9×3 ne donne 12 que modulo 15, et n'est pas une factorisation de 12. Remarquez que la décomposition en produit de $(0,2)$ n'est pas unique et qu'un autre choix aurait pu amener à un résultat différent. Un exemple encore plus fragrant est celui de l'entier 5. Son image par ψ est $(2,0)$ que l'on peut écrire comme le produit de $(2,0)$ et $(1,0)$. Leurs images réciproques respectives étant 5 et 10, le produit obtenu vaut bien encore 5 modulo 15, mais n'est bien évidemment pas une factorisation non triviale de l'entier 5 qui est ***premier*** dans $\mathbb{Z}$.

Plutôt que de donner une compréhension exhaustive du phénomène, examinons-le à travers la recherche de facteurs par force brute. Considérons que l'on cherche un facteur d'un entier m inférieur à M. Une méthode naïve mais valide consiste à parcourir tous les entiers de 2 à $\sqrt{m}$ en testant la divisibilité de m. Une manière de le faire est de parcourir les entiers k en partant de 2, en incrémentant jusqu'à ce qu'on trouve un diviseur de m ou que $k^2 > m$. Dans l'ensemble d'arrivée de l'isomorphisme ψ, c'est-à-dire $\mathbb{Z}/M_1\mathbb{Z} \times \cdots \mathbb{Z}/M_h\mathbb{Z}$, cela est donné par :

1. Soit $k = 2$ et $\kappa = (\bar{k}_{M_1}, \ldots, \bar{k}_{M_h})$.
2. Si κ a une coordonnée dont le carré est plus grand que la coordonnée correspondante dans $\psi(m)$, on incrémente k de 1 et on recommence.
3. On teste si κ divise $\psi(m)$ composante par composante ;
   - si ce n'est pas le cas, on incrémente k de 1 et on recommence ;
   - si cela fonctionne, l'image réciproque k de κ est un facteur de m.

R Au cas où m est inversible et peut être factorisé par k, alors le quotient de m par k est mk^{-1}. Si ce n'est pas le cas, le quotient n'est pas unique ; c'est par exemple le cas pour l'exemple précédent $12 \equiv 3 \times 9 \equiv 3 \times 4$ [15].

6 Cryptage : un *ersatz*

Le cryptage est l'action de transformer un message en une suite de caractères inintelligible excepté pour le récipiendaire. Cela implique une procédure de chiffrement et une procédure de déchiffrement. D'une perspective abstraite, si l'on note $\mathscr{M}$ l'ensemble de messages et $\mathscr{C}$ l'ensemble des messages cryptés, une méthode de cryptage nécessite deux fonctions $\mathfrak{c} : \mathscr{M} \to \mathscr{C}$ et $\mathfrak{d} : \mathscr{C} \to \mathscr{M}$ telles que $\mathfrak{d} \circ \mathfrak{c} = \mathrm{id}_{\mathscr{M}}$. L'expéditeur doit connaître $\mathfrak{c}$ et le récipiendaire $\mathfrak{d}$. On attend d'un bon cryptage qu'il vérifie un certain nombre de propriétés :

— Les calculs d'images par $\mathfrak{c}$ et $\mathfrak{d}$ doivent être faciles et rapides ;
— Les méthodes $\mathfrak{c}$ et $\mathfrak{d}$ doivent être difficiles à déterminer si l'on ne possède qu'un sous-ensemble (ou mieux, tous) des messages cryptés $\mathscr{C}$.

R Comme tout dans un ordinateur n'est que suites de nombres, les ensembles de messages $\mathscr{M}$ et de messages cryptés $\mathscr{C}$ seront généralement considérés comme ayant le type entier. Transformer un message lisible pour un humain en un entier consiste principalement à encoder les caractères.

6.1 Chiffrements symétriques

Le chiffrement symétrique le plus simple est celui connu sous le nom de «code [15] de César». Il consiste à prendre l'alphabet et décaler toutes les lettres d'une constante donnée, comme sur la figure 1.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e

FIGURE 1 – Décalage alphabétique de 6 lettres pour le code de César

La fonction de chiffrement $\mathfrak{c}$, dans ce cas, est lue de haut en bas : elle envoie a sur f, b sur g etc. Pour chiffrer *hello* on procède alors ainsi :

$$\mathfrak{c}(\text{hello}) = \text{mjqqt}$$

en appliquant la fonction caractère par caractère. Pour déchiffrer un message et retrouver le message original, il suffit de lire le tableau de bas en haut. La fonction $\mathfrak{d}$ renvoie f sur a, g sur b etc. La connaissance de $\mathfrak{d}$ ou $\mathfrak{c}$ dépend donc de deux manières de lire le même tableau. Ainsi, l'expéditeur et le récipiendaire ont une connaissance équivalente du cryptosystème utilisé : il suffit d'avoir $\mathfrak{d}$ pour deviner $\mathfrak{c}$ et *vice versa*. C'est pourquoi un tel cryptosystème est dit symétrique.

Si l'on excepte ce qui concerne l'encodage des caractères, le principe du code de César peut être résumé de la manière suivante : en se donnant un entier $n > 1$ modulo lequel nous allons travailler, déterminer un code de César revient à choisir un entier $k \in \mathbb{Z}$ correspondant au décalage. La fonction $\mathfrak{c} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est la translation $\mathfrak{c}(x) = x + k$. Sa réciproque est donc la translation réciproque $\mathfrak{d}(x) = x - k$.

R Le système de chiffrement précédent est entièrement déterminé par la donnée de k. Quand un système de cryptage dépend ainsi d'une donnée numérique, cette donné est appelée clé.

Question 6-2 Comment peut-on généraliser le système précédent ?

Question 6-3 Pouvez-vous imaginer un moyen de déchiffrer (on dit ***casser***) un code de César, pourvu que vous disposiez d'assez de données codées ?

6.2 Chiffrements asymétriques

Un système de cryptage asymétrique, au contraire du cas précédent, est un cryptosystème dans lequel l'expéditeur aura autant de difficultés qu'une quelconque tierce partie à connaître la méthode de déchiffrement. Cela implique la publication par le récipiendaire de données publiques permettant à quiconque de lui envoyer un message chiffré, qu'il sera le seul à pouvoir déchiffrer. Ainsi $\mathfrak{c}$ est publique et accessible à tous, tandis que le récipiendaire est le seul à détenir la méthode de déchiffrement $\mathfrak{d}$. L'intérêt mais aussi la difficulté est de bâtir un tel système de manière à ce que $\mathfrak{d}$ soit dure à déterminer quand on ne dispose que de $\mathfrak{c}$.

6.2.1 Chiffrement RSA

Le ***cryptosystème RSA*** est basé sur le fait qu'il est long de décomposer un nombre en produit de facteurs premiers. Ce constat a été utilisé de la manière suivante : il est beaucoup trop coûteux en temps d'essayer de déterminer un facteur premier d'un nombre qui est le produit de deux nombres premiers gigantesques.

Le chiffrement RSA nécessite à la fois des clés publiques et privées. La première, accessible à tous, est nécessaire pour construire la fonction $\mathfrak{c}$; la seconde n'est connue que du récipiendaire qui publie la clé publique associée.

15. ou chiffre de César

Pour construire ces deux clés, il faut deux nombres ***premiers*** gigantesques (distincts), p et q, dont le produit pq est noté n ; et un élément e inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$, dont l'inverse est notée d.

Clé publique La donnée (n,e).

Clé privée La donnée d.

Avant de nous pencher sur les méthodes de chiffrement et déchiffrement, prenons le temps d'expliquer comment on génère de telles clés. Nous avons vu dans la section 5 que le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}$ est de cardinal

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

Afin de trouver un élément inversible $e \in \mathbb{Z}/\varphi(n)\mathbb{Z}$, il faut donc chercher un élément e qui soit premier avec $(p-1)(q-1)$.

Étant données les clés publiques et privées pour un chiffrement RSA :

Chiffrement Pour tout message $x \in \mathbb{Z}/n\mathbb{Z}$, le message chiffré correspondant est $x^e\ [n]$. La fonction $\mathfrak{c}$ est tout simplement la fonction d'expression $\mathfrak{c}(x) \equiv x^e\ [n]$.

Déchiffrement Pour déchiffrer un message $y \in \mathbb{Z}/n\mathbb{Z}$, il faut calculer $y^d\ [n]$. La fonction de déchiffrement est donnée par $\mathfrak{d}(y) \equiv y^d\ [n]$.

Remarquez que les deux fonctions, de chiffrement et de déchiffrement, consistent à calculer des puissances d'un entier modulo n. L'exponentiation modulaire est rapide et facile à calculer, ce qui est un pré-requis pour que le cryptosystème soit utilisable.

Proposition 6.1 Les données précédentes définissent bien un système de cryptage, i.e. $\mathfrak{d} \circ \mathfrak{c} = \mathrm{id}$.

Démonstration. Supposons tout d'abord que l'on a un élément inversible $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. On veut montrer que pour un tel x

$$\mathfrak{d}\big(\mathfrak{c}(x)\big) \equiv \mathfrak{d}\big(x^e\big) \equiv x^{ed} \equiv x\ [n].$$

Par définition $ed \equiv 1\ [\varphi(n)]$. Cela signifie qu'il existe $k \in \mathbb{Z}$ tel que

$$ed + k\varphi(n) = 1.$$

D'après le théorème 4.4

$$x^{ed} \equiv x^{1-k\varphi(n)} \equiv x \times \left(x^{\varphi(n)}\right)^{-k} \equiv x\ [n].$$

Remarquez que si k est positif, on regarde une puissance négative de 1, ce qui doit être compris comme étant une puissance de l'inverse de 1 (qui de toute manière vaut encore 1).

Supposons maintenant que x n'est pas inversible. D'après le théorème des restes chinois :

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times.$$

Comme les éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ sont tous leurs éléments non nuls, cela signifie que les éléments non inversibles modulo n correspondent aux couples de la forme $(0,x_2)$ avec $x_2 \in \mathbb{Z}/q\mathbb{Z}$ ou $(x_1,0)$ avec $x_1 \in \mathbb{Z}/p\mathbb{Z}$. Si les deux entrées sont 0 le résultat attendu est évident. Supposons donc que x_1 et x_2 sont différents de 0. En réutilisant la notation du cas précédent, on a

$$(0,x_2)^{ed} \equiv (0,x_2^{1-k\varphi(p)\varphi(q)}) \equiv \left(0, x_2 \times \left(x_2^{\varphi(q)}\right)^{-k\varphi(p)}\right) \equiv (0,x_2)\ [n]$$

qui est le résultat attendu. Le cas symétrique avec x_1 est analogue. □

6.2.2 Cryptosystème ElGamal

Le cryptosystème ElGamal repose sur la difficulté de résoudre des équations du type $a^k \equiv b\ [n]$ pour a, b et n fixés, k étant l'inconnue dans l'équation. Ce problème est appelé problème de logarithme discret [16]. Il est un peu plus complexe à écrire que le chiffrement RSA.

Le cryptosystème ElGamal est défini au cœur d'un environnement consistant en une clé publique (p,g) :

— p est un nombre premier modulo lequel le problème logarithmique est difficile à résoudre.

— g est un élément modulo p ayant un ordre [17] suffisamment grand.

16. Vous êtes encouragés à demander à vos enseignants en mathématiques pour quelle raison ce problème est lié aux logarithmes.
17. Il est recommandé que cet ordre soit un nombre premier.

De telles données peuvent être générées par le récipiendaire, ou une tierce partie fiable. Avec de telles données publiques à disposition, le récipiendaire choisit une clé privée $a \in \mathbb{Z}$ et calcule et rend disponible sa clé publique $A = g^a \ [p]$. Donc, ayant dans l'environnement la donnée (p,g) publique :

Clé privée (Presque) n'importe quel entier a choisi (assez grand).

Clé publique L'entier $A = g^a$ modulo p.

Étant donné un nombre premier p pour lequel le problème logarithmique est suffisamment difficile, trouver g consiste d'abord à tester si des nombres choisis ont un ordre assez grand. L'ordre d'un élément g est un diviseur de $p-1$. Par exemple, si l'on choisit un nombre premier de la forme $p = 2q+1$ où q est encore premier, alors l'ordre de g sera parmi 1, 2, q et $2q$. Ainsi, si g^2 est différent de 1 modulo p, g sera d'ordre q ou $2q$ ce qui peut être suffisant.

Avec les données publiques et une clé publique ElGamal :

Chiffrement Pour un message $x \in \mathbb{Z}/p\mathbb{Z}$, l'expéditeur génère un entier aléatoire k éphémère [18]. Le message chiffré est le couple (c_1,c_2) où $c_1 = g^k$ et $c_2 = xA^k$. La fonction $\mathfrak{c}$ est donc définie par l'expression $\mathfrak{c}(x) = (g^k, xA^k)$ où k est un entier éphémère.

Déchiffrement Pour déchiffrer un message $(y_1,y_2) \in \mathbb{Z}/p\mathbb{Z}$, le récipiendaire calcule $(y_1^a)^{-1} y_2$. La fonction $\mathfrak{d}$ est donnée par $\mathfrak{d}(y_1,y_2) = (y_1^a)^{-1} y_2$.

Proposition 6.2 Les données précédentes définissent bien un système de cryptage, i.e. $\mathfrak{d} \circ \mathfrak{c} = \mathrm{id}$.

Démonstration. En utilisant les notations précédentes, le but est de prouver

$$(c_1^a)^{-1} c_2 = \left(g^{ak}\right)^{-1} xA^k = x$$

La première égalité n'est rien de moins que la définition. Pour la seconde, par construction :

$$g^a \equiv A \ [p]$$

ainsi

$$\left(g^{ak}\right)^{-1} A^k x \equiv x \ [p]$$

ce qui est le résultat attendu. □

Conclusion

Enfin, voici une citation qui résume tout ce qu'il faut retenir de l'arithmétique :

> Cet après-midi, en allant à l'école, j'ai rencontré Alceste qui m'a dit : "Si on n'allait pas à l'école ?" Moi, je lui ai dit que ce n'était pas bien de ne pas aller à l'école, que la maîtresse ne serait pas contente, que mon papa m'avait dit qu'il fallait travailler si on voulait arriver dans la vie et devenir aviateur, que ça ferait de la peine à maman et que ce n'était pas beau de mentir. Alceste m'a répondu que cet après-midi on avait arithmétique, alors j'ai dit "bon" et nous ne sommes pas allés à l'école.
>
> ***Le petit Nicolas***, Sempé-Goscinny

18. On ne s'en servira qu'une seule fois !