Nombres entiers

Baptiste Calmès

2 mars 2021

Table des matières

1 L'anneau $\mathbb{Z}$; arithmétique élémentaire

On ne redéfinira pas ici l'ensemble des entiers $\mathbb{Z}$ ni ses deux lois, l'addition et la multiplication usuelles. Nous nous contenterons d'en rappeler les principales propriétés.

1.1 Proposition. *Muni de l'addition et de la multiplication, $\mathbb{Z}$ est un anneau commutatif.*

La valeur absolue est une fonction $\mathbb{Z} \to \mathbb{N}$, notée $|.|$, qui implique l'existence de la division euclidienne :

1.2 Définition. Étant donnés $n \in \mathbb{Z}$ et $m \in \mathbb{Z}^*$, on appelle respectivement quotient et reste de la *division euclidienne* de n par m les uniques entiers q et r tels que

$$n = mq + r \quad \text{et} \quad 0 \leq r \leq |m|.$$

Cette division euclidienne permet de montrer l'existence du *plus grand commun diviseur*.

1.3 Définition (pgcd)**.** Soient a et b deux entiers dont un non nul. Parmi leurs diviseurs, il en existe un unique plus grand (au sens que tous les autres le divisent) et positif, qu'on appelle le pgcd de a et b. Plus généralement, on peut remplacer a et b par un ensemble d'entiers quelconque (dont un non nul). On dit que des entiers (dont un non nul) sont *premiers entre eux* si leur pgcd est 1.

Ce pgcd peut être calculé en pratique par divisions euclidiennes successives, suivant l'algorithme d'Euclide.

On obtient également la propriété de Bézout :

1.4 Proposition (Bézout)**.** *Si a et b sont deux entiers dont un au moins est non nul (plus généralement d'une famille d'entiers) et de pgcd d, il existe des coefficients $u, v \in \mathbb{Z}$ tels que $ua + vb = d$. Plus précisément, l'ensemble des entiers pouvant s'écrire $ua + vb$ avec $u, v \in \mathbb{Z}$ est exactement $d\mathbb{Z}$.*

Le *plus petit commun multiple* existe également :

1.5 Définition. Soient a et b deux entiers non nuls. Parmi leurs multiples, il en existe un unique plus petit (au sens qu'il divise tous les autres) et positif, qu'on appelle le plus petit commun multiple (*ppcm*) de a et b. Plus généralement, on définit de même le ppcm d'un nombre fini d'entiers non nuls.

Le produit du ppcm et du pgcd de deux entiers est égal à $|ab|$ (attention, cela devient faux pour plus de deux entiers).

Le lemme classique suivant est très utile.

1.6 Lemme (Gauss)**.** *Soient $a, b, c \in \mathbb{Z}$ avec a et b premiers entre eux (donc a ou b non nul). Si a divise bc, alors a divise c.*

1.7 Définition. Un entier $p > 0$ est dit *premier* s'il a exactement deux diviseurs positifs, qui sont alors nécessairement 1 et p, avec $1 \neq p$. En particulier, 1 n'est pas un nombre premier.

On tire assez facilement du lemme de Gauss :

1.8 Théorème (décomposition d'un entier en facteurs premiers)**.** *Tout nombre entier (resp. rationnel) non nul n se décompose de manière unique en*

$$n = \epsilon \prod_{p \text{ premier}} p^{k_p}$$

où $\epsilon \in \{\pm 1\}$ (i.e. inversible) et les $k_p \in \mathbb{N}$ (resp. $\in \mathbb{Z}$) sont presque tous nuls (seul un nombre fini est non nul).

1.9 Remarque. L'unicité de la décomposition signifie que ϵ et les k_p sont déterminés uniquement par n.

2 Sous-groupes de $\mathbb{Z}$

Toute intersection $\bigcap_{i\in I} H_i$ d'une famille de sous-groupes H_i d'un groupe G est encore un sous-groupe (exercice : le vérifier). Pour cette raison, on a :

2.1 Lemme. *Étant donné un ensemble d'éléments S inclus dans G, il existe un plus petit (au sens qu'il est inclus dans tous les autres) sous-groupe de G qui contient S. Ce sous-groupe est égal à :*

1. *$\bigcap_{H\supset S} H$ (où H parcourt les sous-groupes de G contenant S ;*
2. *l'ensemble des produits finis d'éléments de S et de leurs inverses ;*

Ceci permet de poser :

2.2 Définition. Le sous-groupe *engendré* par un ensemble S dans G est le plus petit sous-groupe de G contenant S. On le note $\langle S\rangle$.

2.3 Définition. On dit qu'un groupe G est *monogène* s'il existe un élément $g \in G$ tel que $G = \langle g\rangle$.

Attention, cet élément g n'a aucune raison d'être unique, et il l'est très rarement, car $\langle g\rangle = \langle g^{-1}\rangle$, donc il ne l'est pas si $g \neq g^{-1}$.

⚠ Nous allons souvent travailler avec des groupes abéliens (i.e. commutatifs). Dans ce cas, la loi de groupe est le plus souvent notée $+$ et on utilise une notation additive : un terme qu'on aurait noté $n^k = n \cdot n \cdots n$ en utilisant une notation multiplicative sera noté $kn = n + n + \cdots + n$. C'est en particulier le cas dans $\mathbb{Z}$.

2.4 Théorème. *Tout sous-groupe de $\mathbb{Z}$ est monogène, et plus précisément de la forme $\langle n\rangle = n\mathbb{Z} = \{nq,\ q \in \mathbb{Z}\}$ pour un unique $n \in \mathbb{N}$. Si $n \neq 0$, un tel sous-groupe est isomorphe à $\mathbb{Z}$ et si $n = 0$, ce sous-groupe est trivial. On a $m|n$ si et seulement si $n\mathbb{Z} \subset m\mathbb{Z}$.*

2.5 Proposition. *Si $a, b \in \mathbb{N}^*$, alors le pgcd de a et b est le générateur dans $\mathbb{N}^*$ de $\langle a, b\rangle \subset \mathbb{Z}$.*

De même :

2.6 Proposition. *Si $a, b \in \mathbb{N}^*$, alors le ppcm de a et b est le générateur dans $\mathbb{N}^*$ de $\langle a\rangle \cap \langle b\rangle \subset \mathbb{Z}$.*

2.7 Proposition (quotients de $\mathbb{Z}$)**.** *Un groupe quotient de $\mathbb{Z}$ est*

— *soit isomorphe à $\mathbb{Z}$ et est infini,*

— *soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un $n \neq 0$ et est fini.*

2.8 Théorème. *Soit G un groupe, et $g \in G$. Considérons le sous-groupe $\langle g\rangle \subset G$, et l'application $\phi : \mathbb{Z} \to G$ envoyant n sur g^n. Alors, ϕ est un morphisme de groupes d'image $\langle g\rangle$, et son noyau est donc un sous-groupe de $\mathbb{Z}$. Notons n son unique générateur positif (voir théorème 2.4). Alors :*

1. *soit $n = 0$, donc $\ker(\phi) = \{0\}$. Le morphisme ϕ induit alors un isomorphisme de $\mathbb{Z}$ vers $\langle g\rangle$ qui est donc infini et $g^n = g^m$ est équivalent à $n = m$;*
2. *soit $n > 0$, donc $\ker(\phi) = n\mathbb{Z}$. Le morphisme ϕ se factorise par un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ vers $\langle g\rangle$, qui est fini, et $g^l = g^m$ est équivalent à $n|(l - m)$.*

2.9 Définition (ordre d'un élément)**.** Soit G un groupe et g un élément de G. Si l'on est dans le cas 1 du théorème 2.8, on dit que g est *d'ordre infini*. Si l'on est dans le cas 2 du théorème 2.8, on dit que g est d'ordre n.

2.10 Remarque. Par construction, l'ordre de g est donc le plus petit entier $m \in \mathbb{N}^*$ tel que $g^m = 1$, s'il existe, et g est d'ordre infini sinon. Bien entendu, si $\#G$ est fini, tout élément dedans est d'ordre fini.

2.11 Définition. Un groupe est *cyclique* s'il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un $n > 0$.

En particulier, tout groupe cyclique est à la fois fini et commutatif et le théorème 2.8 nous dit :

2.12 Corollaire. *Tout groupe monogène est soit cyclique soit isomorphe à $\mathbb{Z}$, ou encore tout groupe monogène est isomorphe à un quotient de $\mathbb{Z}$.*

2.13 Proposition. *Si un groupe G est de cardinal fini, l'ordre d'un élément $g \in G$ est fini et divise $\#G$.*

2.14 Proposition. *Si d divise n, on considère l'application $m_d : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qui envoie $\overline{x}$ sur $\overline{d}\,\overline{x}$. Alors*

- *L'image de m_d est le sous-groupe $d(\mathbb{Z}/n\mathbb{Z})$, de cardinal $\frac{n}{d}$, donc isomorphe à $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$.*
- *Le noyau de m_d est le sous-groupe $\frac{n}{d}\mathbb{Z}/n\mathbb{Z}$, il est de cardinal d, donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$.*

2.15 Proposition. *Si d ne divise pas n, alors $\mathbb{Z}/n\mathbb{Z}$ n'a aucun sous-groupe de cardinal d. Si d divise n, alors le noyau de la multiplication par d est l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d.*

2.16 Corollaire. *Tout sous-groupe d'un groupe cyclique est cyclique.*

2.17 Corollaire. *Soient $m, n \in \mathbb{N}^*$. Le groupe $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique si et seulement si $\mathrm{pgcd}(m, n) = 1$.*

2.18 Proposition. *Tout groupe de cardinal au plus 5 est abélien.*

2.19 Remarque. Remarquons que le petit calcul de la preuve précédente montre au passage que tout groupe dont tous les éléments sont d'ordre 2 (sauf le neutre) est abélien.

3 Congruences

Nous allons maintenant étudier les propriétés d'anneau de $\mathbb{Z}/n\mathbb{Z}$ et en tirer des conséquences arithmétiques.

Rappelons rapidement les faits généraux suivants pour un anneau (unitaire) A.

3.1 Définition (inversible)**.** Un élément $a \in A$ est *inversible* s'il existe s'il existe $b \in A$ tel que $ab = ba = 1$. On note $A^\times$ l'ensembles des éléments inversibles de A.

3.2 Définition (diviseur de zéro)**.** Étant donné un anneau A commutatif, un élément $a \in A$ est appelé *diviseur de zéro* s'il existe un élément $b \in A$, $b \neq 0$, tel que $ab = 0$.

En particulier, 0 est toujours un diviseur de 0, sauf si A est l'anneau nul.

3.3 Remarque. Un élément d'un anneau ne peut être à la fois inversible et diviseur de zéro, puisque $ab = 0$ implique $b = 0$ si a est inversible.

3.4 Lemme. *Dans un anneau commutatif de cardinal fini, un élément est soit inversible, soit diviseur de zéro.*

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

3.5 Lemme. *Si H est un sous-groupe de $\mathbb{Z}$, alors c'est automatiquement un idéal de $\mathbb{Z}$. En particulier, toute combinaison linéaire (finie) $\sum_i k_i m_i$ où $k_i \in \mathbb{Z}$ et $m_i \in H$ est dans H.*

3.6 Définition. Soit $n \in \mathbb{N}$. La structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$ que nous considérons toujours par la suite est celle induite par le fait que c'est un quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

3.7 Remarque. En pratique, cela veut dire que

- $\overline{a} + \overline{b} = \overline{a + b}$;
- $\overline{0}$ est l'élément neutre de l'addition ;

— $\overline{a}\overline{b} = \overline{ab}$;

— $\overline{1}$ est l'élément neutre de la multiplication.

De plus, puisque $\mathbb{Z}$ est commutatif, il en est de même de $\mathbb{Z}/n\mathbb{Z}$. Par contre, contrairement à $\mathbb{Z}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de cardinal *fini* (et égal à n), ce qui simplifie beaucoup les choses.

3.8 Proposition. *Pour tout $n \in \mathbb{N}^*$, un élément $\overline{m}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si m est premier avec n, et diviseur de zéro sinon.*

3.9 Remarque. Cette preuve montre en fait que pour trouver en pratique l'inverse d'un m (premier avec n) dans $\mathbb{Z}/n\mathbb{Z}$, il suffit de calculer des coefficients de Bézout, ce que l'on sait faire. Si au contraire m n'est pas premier avec n, il est facile de trouver $k \neq 0$ tel que $mk = 0$, comme nous le verrons un peu plus loin.

3.10 Corollaire. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

3.11 Définition (anneau intègre)**.** Un anneau est *intègre* si son seul diviseur de zéro est 0.

3.12 Exemple. L'anneau nul n'est pas intègre. Tout corps est intègre. L'anneau $\mathbb{Z}$ est intègre. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

3.2 Équations affines

On s'intéresse maintenant à la résolution d'équations ou de systèmes d'équations de la forme

$$ax \equiv b \mod n \tag{3.1}$$

où a, b et n sont des entiers fixés, et x est l'inconnue dans $\mathbb{Z}$.

Notons tout d'abord que cette équation fait bien sens dans $\mathbb{Z}/n\mathbb{Z}$: si x est solution, alors tout x' tel que $x' \equiv x \mod n$ est encore solution, et que l'ensemble des solutions ne change pas lorsqu'on change a ou b dans sa classe d'équivalence. En trouver les solutions se ramène donc à résoudre

$$\overline{a}\,\overline{x} = \overline{b} \text{ dans } \mathbb{Z}/n\mathbb{Z}. \tag{3.2}$$

Comme d'habitude, commençons par l'équations homogène

$$\overline{a}\,\overline{x} = \overline{0} \tag{3.3}$$

dont l'ensemble des solutions forme de manière évidente un idéal de $\mathbb{Z}/n\mathbb{Z}$.

Regardons deux cas extrêmes :

1. le cas où a est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Alors, en multipliant par son inverse, on trouve que l'équation est équivalente à $\overline{x} = \overline{0}$.
2. le cas où a est nul dans $\mathbb{Z}/n\mathbb{Z}$. Alors, tout élément de $\mathbb{Z}/n\mathbb{Z}$ est solution.

Lorsque n est premier, et donc que $\mathbb{Z}/n\mathbb{Z}$ est un corps (cf. corollaire 3.10), ce sont donc les seuls cas qui se présentent.

Mais lorsque n n'est pas premier, il y a des cas où a n'est ni inversible ni nul (par exemple $a = 2$ si $n = 4$).

3.13 Proposition. *Si $n \in \mathbb{N}^*$, l'ensemble des solutions de $\overline{a}\,\overline{x} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ est*

$$\{\overline{k\tfrac{n}{d}},\ k = 0, \dots, d-1\} = \operatorname{im}\left(\mathbb{Z}/d\mathbb{Z} \xrightarrow{\cdot\frac{n}{d}} \mathbb{Z}/n\mathbb{Z} \right)$$

où $d = \operatorname{pgcd}(a, n)$.

Examinons maintenant ce qui se passe en présence d'un second membre $\overline{b} \neq \overline{0}$ dans (3.2).

Si $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, d'inverse $\overline{u}$, alors

$$\overline{a}\,\overline{x} = \overline{b} \iff \overline{x} = \overline{u}\,\overline{b}$$

et l'équation a donc une unique solution dans $\mathbb{Z}/n\mathbb{Z}$.

Si $\overline{a} \notin (\mathbb{Z}/n\mathbb{Z})^\times$, i.e. $d = \mathrm{pgcd}(a, n) \neq 1$, on raisonne comme ceci :

$$\overline{ax} = \overline{b} \iff \exists k \in \mathbb{Z} \text{ tel que } ax = b + kn. \tag{3.4}$$

Donc si $d \nmid b$, il n'y a pas de solution puisqu'il divise tous les autres termes.

Si $d|b$, on simplifie l'équation d'entiers (3.4) par d ; elle est donc équivalente à

$$\exists k \in \mathbb{Z} \text{ tel que } a'x = b' + kn' \tag{3.5}$$

où $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ et $n' = \frac{n}{d}$. Mais cette fois, nous connaissons les solutions, puisque $\mathrm{pgcd}(a', n') = 1$.

On a donc montré :

3.14 Proposition. *Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Posons $d = \mathrm{pgcd}(a, n)$. L'ensemble des solutions dans $\mathbb{Z}/n\mathbb{Z}$ de $\overline{ax} = \overline{b}$ est :*

- *vide si d ne divise pas b ;*
- *$\{\overline{u'b'} + k\overline{n'},\ k = 0, \ldots, d-1\}$ où*
  - *$n' = \frac{n}{d}$,*
  - *$\overline{u'}$ est un inverse de $\overline{a'} = \overline{\frac{a}{d}}$ dans $\mathbb{Z}/n'\mathbb{Z}$,*
  - *$b' = \frac{b}{d}$.*

Passons maintenant aux systèmes d'équations de la forme

$$\begin{cases} a_1 x \equiv b_1 \mod n_1 \\ a_2 x \equiv b_2 \mod n_2 \\ \quad \cdots \\ a_l x \equiv b_l \mod n_l \end{cases} \tag{3.6}$$

où les $a_i, b_i \in \mathbb{Z}$ et $n_i \in \mathbb{N}^*$ pour tout i.

Comme nous aurons à manipuler les classes du même entier modulo plusieurs entiers différents, posons :

3.15 Notation. Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. On note $\overline{a}^{\mathrm{mod}\, n}$ la classe de a modulo n. C'est donc un élément de $\mathbb{Z}/n\mathbb{Z}$.

Posons $d_i = \mathrm{pgcd}(a_i, n_i)$.

Par le raisonnement précédent, on a immédiatement qu'un tel système n'a aucune solution si d_i ne divise pas b_i pour un i.

Sinon, en divisant chaque a_i, b_i et n_i par d_i, on se ramène au cas où $d_i = 1$ pour tout i. Nous supposerons donc cela vérifié à partir de maintenant. On peut alors trouver un inverse u_i pour chaque a_i modulo n_i, et le système est encore équivalent à un système de la forme

$$\begin{cases} x \equiv c_1 \mod n_1 \\ x \equiv c_2 \mod n_2 \\ \quad \cdots \\ x \equiv c_l \mod n_l \end{cases} \tag{3.7}$$

où $c_i = u_i b_i$.

La résolution d'un tel système est basée sur le fameux "théorème chinois" que nous allons maintenant introduire.

On prend m et n dans $\mathbb{N}^*$, et on considère le morphisme d'anneaux

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & (\overline{k}^{\bmod m}, \overline{k}^{\bmod n}). \end{array}$$

Il envoie $\operatorname{ppcm}(m,n)$ sur $(0,0)$ et se factorise donc par $\mathbb{Z}/\operatorname{ppcm}(m,n)\mathbb{Z}$. On en déduit un morphisme d'anneaux

$$\begin{array}{ccc} \mathbb{Z}/\operatorname{ppcm}(m,n)\mathbb{Z} & \to & \mathbb{Z}/m \times \mathbb{Z}/n\mathbb{Z} \\ \overline{k}^{\bmod \operatorname{ppcm}(m,n)} & \mapsto & (\overline{k}^{\bmod m}, \overline{k}^{\bmod n}) \end{array} \tag{3.8}$$

dont nous allons étudier les propriétés.

3.16 Théorème (chinois)**.** *Le morphisme d'anneaux* (3.8) *est injectif. Il est surjectif (donc bijectif) si et seulement si m et n sont premiers entre eux, auquel cas on a $\operatorname{ppcm}(m,n) = mn$ et donc un isomorphisme*

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Si m et n sont premiers entre eux, il est facile de trouver un antécédent d'un élément quelconque : il existe u et v tels que $um + vn = 1$. Donc

$$\begin{aligned} um &\equiv 1 \mod n \\ vn &\equiv 0 \mod n \\ um &\equiv 0 \mod m \\ vn &\equiv 1 \mod m. \end{aligned}$$

Autrement dit, $\overline{um}$ est un antécédent de $(\overline{0}, \overline{1})$ et $\overline{vn}$ est un antécédent de $(\overline{1}, \overline{0})$. Il suffit alors de faire une combinaison linéaire $\overline{b\,um + a\,vn}$ pour obtenir un antécédent d'un élément quelconque $(\overline{a}, \overline{b}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Caractérisons maintenant l'image du morphisme (3.8), dans le cas où m et n sont quelconques.

3.17 Théorème. *Choisissons des coefficients de Bézout u et v tels que $um + vn = \operatorname{pgcd}(m,n)$. Alors :*

1. *L'image du morphisme* (3.8) *est l'ensemble des éléments $(\overline{a}^{\bmod m}, \overline{b}^{\bmod n})$ tels que $\overline{a}^{\bmod \operatorname{pgcd}(m,n)} = \overline{b}^{\bmod \operatorname{pgcd}(m,n)}$.*
2. *Si un couple $(\overline{a}, \overline{b})$ est dans l'image, on a donc $b = a + k \operatorname{pgcd}(m,n)$ avec $k \in \mathbb{Z}$, et $\overline{a + kum}^{\bmod \operatorname{ppcm}(m,n)}$ en est un antécédent.*

Il devient maintenant facile de résoudre les systèmes de la forme (3.7). Commençons par deux équations :

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned} \tag{3.9}$$

Nous cherchons donc un $x \in \mathbb{Z}$ qui s'envoie sur $(\overline{a}^{\bmod m}, \overline{b}^{\bmod n})$ par les deux projections. Mais comme nous l'avons vu, cette application $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ se factorise par $\mathbb{Z} \to \mathbb{Z}/\operatorname{ppcm}(m,n)\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Cela revient donc à chercher $\overline{x}^{\bmod \operatorname{ppcm}(m,n)}$ qui s'envoie sur $(\overline{a}^{\bmod m}, \overline{b}^{\bmod n})$ ce que nous savons faire par le théorème 3.17.

Nous obtenons donc en résumé :

3.18 Proposition. *Soient $m, n \in \mathbb{N}^*$. Notons $\operatorname{pgcd}(m,n) = d$ et soient u et v des coefficients de Bézout tels que $um + vn = d$. Soient $a, b \in \mathbb{Z}$. L'ensemble de solutions du système* (3.9) *est*

— *vide si $\overline{a}^{\bmod d} \neq \overline{b}^{\bmod d}$;*

— $\{x \in \mathbb{Z}$ *t.q.* $x = a + kum \mod \mathrm{ppcm}(m,n)\}$ *si* $b - a = kd$*;*

Nous avons donc transformé le système à deux équations (3.9) en une seule équation (s'il y a des solutions). De proche en proche, nous pouvons déterminer si le système (3.7) a des solutions, et s'il en a, le ramener à une seule équation déterminant x modulo un seul entier.

Il est possible de raisonner directement un peu plus globalement. On considère le morphisme d'anneaux

$$\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_l\mathbb{Z}$$

qui se factorise à nouveau par un morphisme injectif

$$\mathbb{Z}/\mathrm{ppcm}(n_1, \ldots, n_l)\mathbb{Z} \hookrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_l\mathbb{Z}. \tag{3.10}$$

3.19 Théorème. *L'image du morphisme* (3.10) *est constituée de l'ensemble des éléments* $(\overline{c_1}^{\bmod n_1}, \ldots, \overline{c_l}^{\bmod n_l})$ *tels que pour tout* $i \neq j$*, on a* $\overline{c_i}^{\bmod \mathrm{pgcd}(n_i,n_j)} = \overline{c_j}^{\bmod \mathrm{pgcd}(n_i,n_j)}$.

On en tire immédiatement la reformulation :

3.20 Théorème. *Soient* $n_1, \ldots, n_l \in \mathbb{N}^*$ *et soient* $c_1, \ldots, c_l \in \mathbb{Z}$*. L'ensemble des solutions du système*

$$\begin{cases} x \equiv c_1 \mod n_1 \\ x \equiv c_2 \mod n_2 \\ \quad \cdots \\ x \equiv c_l \mod n_l \end{cases}$$

est non vide si et seulement si $\mathrm{pgcd}(n_i, n_j)$ *divise* $c_i - c_j$ *pour tous* $i \neq j$ *et dans ce cas,* x *est déterminé uniquement modulo* $\mathrm{ppcm}(n_1, \ldots, n_l)$.

Si l'ensemble des solutions est non vide, outre la méthode vue plus haut qui permet de déterminer une solution en réduisant les deux premières équations en une seule, puis en itérant, il en existe une autre, qui consiste à remplacer le système par un système équivalent où les modulos sont premiers entre eux.

3.21 Lemme. *Soit* $n_1, \ldots, n_l \in \mathbb{N}^*$*. Alors il existe* $m_1, \ldots, m_l \in \mathbb{N}^*$ *tels que*

— m_i *divise* n_i *pour* $i = 1, \ldots, l$*;*

— $\mathrm{ppcm}(n_1, \ldots, n_l) = \mathrm{ppcm}(m_1, \ldots, m_l)$*;*

— $\mathrm{pgcd}(m_i, m_j) = 1$ *si* $i \neq j$.

3.22 Proposition. *Si les* m_i *satisfont aux conditions du lemme et si pour tous* $i \neq j$*, on a bien que* $\mathrm{pgcd}(n_i, n_j)$ *divise* $c_i - c_j$*, alors le système* (3.7) *est équivalent au système*

$$\begin{cases} x \equiv c_1 \mod m_1 \\ x \equiv c_2 \mod m_2 \\ \quad \cdots \\ x \equiv c_l \mod m_l \end{cases} \tag{3.11}$$

Mais résoudre un tel système avec des modulos premiers entre eux deux à deux est facile :

3.23 Théorème. *Si les* m_i *sont premiers entre eux deux à deux, le système* (3.11) *admet la solution* $x = \sum_i c_i v_i m'_i$ *où* $m'i = \prod_{j \neq i} m_j$ *et* u_i *est un coefficient de Bézout tel que* $u_i m_i + v_i m'_i = 1$ *et cette solution est uniquement déterminée modulo* $\mathrm{ppcm}(m_1, \ldots, m_l) = \prod_i m_i$.

3.3 Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

Dans cette partie, on s'intéresse aux résultats arithmétiques que l'on peut obtenir en examinant la structure multiplicative de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Commençons par rappeler un fait simple : la multiplication définit une loi de groupe sur $A^\times$, l'ensemble des éléments inversibles d'un anneau unitaire A.

3.24 Lemme. *Si $a \in A$ commutatif, on a $aA = A$ si et seulement si a est inversible.*

En particulier, un élément $\overline{x}$ engendre additivement $\mathbb{Z}/n\mathbb{Z}$, i.e. le sous-groupe engendré $\langle \bar{x} \rangle = \mathbb{Z}/n\mathbb{Z}$, si et seulement si $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

3.25 Définition. On définit la *fonction indicatrice d'Euler* $\phi : \mathbb{N}^* \to \mathbb{N}$ qui à n associe le nombre de nombres entiers compris entre 1 et n et premiers à n. Autrement dit

$$\phi(n) = \#\{m,\ 1 \leq m \leq n,\ \mathrm{pgcd}(m,n) = 1\}.$$

Voici un tableau des premières valeurs de ϕ.

n	1	2	3	4	5	6	7	8	9	10	11
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10

3.26 Proposition. *On a $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{\overline{x}$ tel que $\langle \overline{x} \rangle = \mathbb{Z}/n\mathbb{Z}\}$.*

3.27 Proposition. *La fonction d'Euler est dite multiplicative, c'est-à-dire que si m et n sont premiers entre eux, alors $\phi(mn) = \phi(m)\phi(n)$.*

Il suffit donc de la connaître pour les puissances de nombres premiers.

3.28 Lemme. *Si p est premier et $\nu \geq 1$, on a $\phi(p^\nu) = p^{\nu-1}(p-1)$.*

Toutefois, pour les grandes valeurs de n, le décomposer en facteurs premiers est algorithmiquement coûteux.

3.29 Proposition. *Pour tout $n \in \mathbb{N}^*$, on a*

$$n = \sum_{d|n} \phi(d)$$

3.30 Théorème (Euler)**.** *Soit $n \in \mathbb{N}^*$ et soit a premier avec n. Alors*

$$a^{\phi(n)} \equiv 1 \mod n.$$

3.31 Théorème (petit théorème de Fermat)**.** *Si p est un nombre premier et si $a \in \mathbb{Z}$ n'est pas un multiple de p, alors*

$$a^{p-1} \equiv 1 \mod p$$

3.32 Corollaire. *Si p est premier et a est un entier quelconque, alors*

$$a^p \equiv a \mod p$$

3.4 Convolution et inversion de Möbius

Montrons encore une formule utile sur l'indicatrice d'Euler. Cela nécessite de faire un petit détour et d'introduire la convolution de Dirichlet.

Soit A un anneau commutatif unitaire (souvent $\mathbb{Z}$ ou $\mathbb{C}$).

3.33 Définition. Une *fonction arithmétique* à valeur dans A est une fonction $\phi : \mathbb{N}^* \to A$. Elle est dite multiplicative si $\phi(1) = 1$ et $\phi(mn) = \phi(m)\phi(n)$ dès que $\mathrm{pgcd}(m,n) = 1$. On note $\mathrm{Arith}(A)$ l'ensemble des fonctions arithmétiques à valeurs dans A et $\mathrm{Mult}(A)$ son sous-ensemble des fonctions multiplicatives.

3.34 Exemple. La fonction constante $\mathbb{1} : n \mapsto 1$ est arithmétique à valeurs dans $\mathbb{Z}$ et multiplicative.
L'indicatrice d'Euler est également arithmétique à valeurs dans $\mathbb{Z}$ et multiplicative.

3.35 Définition (convolution de Dirichlet)**.** On définit une loi interne $*$ sur $\mathrm{Arith}(A)$ appelée *convolution de Dirichlet* en posant :

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}).$$

3.36 Proposition. *Muni de l'addition et de la convolution de Dirichlet,* $\mathrm{Arith}(A)$ *est un anneau commutatif unitaire, dont l'unité est la fonction* $\epsilon : n \mapsto \delta_{1,n}$*. L'anneau* $\mathrm{Arith}(A)$ *est intègre si et seulement si* A *l'est. Ses éléments inversibles sont les fonctions* f *telles que* $f(1) \in A^\times$*.*

3.37 Théorème. *Le sous-ensemble* $\mathrm{Mult}(A) \subset \mathrm{Arith}(A)$ *est un sous-groupe de* $\mathrm{Arith}(A)^\times$*.*

3.38 Définition. La fonction de Möbius est la fonction arithmétique $\mu : \mathbb{N}^* \to A$ telle que :

$$\mu(n) = \begin{cases} 0 & \text{si un carré >1 divise } n \\ (-1)^l & \text{si } n \text{ est un produit de } l \text{ nombres premiers distincts} \end{cases}$$

3.39 Lemme. *La fonction de Möbius est multiplicative et son inverse pour la convolution est la fonction constante* $\mathbb{1}$*.*

3.40 Proposition (inversion de Möbius)**.** *Soient* f *et* g *deux fonctions arithmétiques. Les deux conditions suivantes sont équivalentes :*

$$\forall n \in \mathbb{N}^*, \qquad f(n) = \sum_{d|n} g(d)\frac{n}{d}$$

et

$$\forall n \in \mathbb{N}^*, \qquad g(n) = \sum_{d|n} f(d)\mu(\frac{n}{d})$$

3.41 Proposition. *Pour tout* $n \in \mathbb{N}^*$*, on a*

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

où μ *est la fonction de Möbius, qui vaut* 1 *sur les entiers divisibles par un carré non trivial et* $(-1)^i$ *si* n *est un produit de* i *nombres premiers distincts.*