Introduction à la Cryptologie

Chapitre 5 : Le théorème des restes chinois

Michael Eisermann (Institut Fourier, UJF Grenoble)

Année 2008-2009
IF / IMAG, Master 1, S1-S2

document mis à jour le 7 juillet 2009

www-fourier.ujf-grenoble.fr/~eiserm/cours#crypto

Objectifs de ce chapitre

Développement mathématique :

- Étudier les éléments inversibles dans $\mathbb{Z}/m$.
- Établir le théorème chinois : $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$ si $\operatorname{pgcd}(m,n) = 1$.

Développement algorithmique :

- Calculer efficacement l'inverse dans $\mathbb{Z}/m^\times$.
- Appliquer efficacement les bijections dans le théorème chinois.

Sommaire

Éléments inversibles dans $\mathbb{Z}/m$

Définition

Un élément $x \in \mathbb{Z}/m$ est ***inversible*** s'il existe $y \in \mathbb{Z}/m$ tel que $x \cdot y = \bar{1}$.
Dans ce cas y est unique et on l'appelle ***l'inverse*** de x, noté x^{-1}.
On définit $\mathbb{Z}/m^* = \mathbb{Z}/m \smallsetminus \{\bar{0}\}$ et $\mathbb{Z}/m^\times := \{x \in \mathbb{Z}/m \mid x \text{ est inversible}\}$.

Remarque

L'élément $\bar{1}$ est inversible dans $\mathbb{Z}/m$, car $\bar{1} \cdot \bar{1} = \bar{1}$.
De même $-\bar{1}$ est inversible, car $(-\bar{1}) \cdot (-\bar{1}) = \bar{1}$.

Exemple

Dans $\mathbb{Z}/10$ l'élément $\bar{3}$ est inversible car $\bar{3} \cdot \bar{7} = \bar{1}$.
L'élément $\bar{2}$, par contre, n'est pas inversible. (Pourquoi ?)

Exercice

Expliciter les éléments inversibles dans $\mathbb{Z}/8$ et leur inverse.

Caractérisation des éléments inversibles dans $\mathbb{Z}/m$

Proposition

Nous avons $\mathbb{Z}/m^\times = \{\bar{a} \mid a \in \mathbb{Z} \text{ et } \operatorname{pgcd}(a,m) = 1\}$.

Démonstration.
« $\supset$ » Si $\operatorname{pgcd}(a,m) = 1$ alors il existe $u, v \in \mathbb{Z}$ tels que $au + mv = 1$.
Dans $\mathbb{Z}/m$ ceci veut dire que $\bar{a} \cdot \bar{u} = \bar{1}$.

« $\subset$ » Si $a \in \mathbb{Z}$ vérifie $\bar{a} \in \mathbb{Z}/m^\times$, alors il existe $u \in \mathbb{Z}$ tel que $\bar{a} \cdot \bar{u} = \bar{1}$.
Dans $\mathbb{Z}$ ceci veut dire que $au \equiv 1 \ (m)$.
Il existe donc $v \in \mathbb{Z}$ tel que $1 - au = mv$.
On conclut que $1 = au + mv$, donc $\operatorname{pgcd}(a,m) = 1$. □

Corollaire

Pour $m \geq 2$ *nous avons* $\mathbb{Z}/m^\times = \{\bar{a} \mid 0 < a < m \text{ et } \operatorname{pgcd}(a,m) = 1\}$. □

Calcul de l'inverse dans $\mathbb{Z}/m$

On peut donc encore simplifier et optimiser l'algorithme...

Voici un algorithme qui est 30% plus rapide :

Algorithme 5.2 calcul de l'inverse dans $\mathbb{Z}/m$ (légèrement optimisé)

Entrée: deux entiers x, m tels que $0 \leq x < m$
Sortie: l'entier y vérifiant $0 < y < m$ tel que $xy \equiv 1 \ (m)$
ou 0 pour signaler que $\bar{x} \in \mathbb{Z}/m$ n'est pas inversible

$\begin{pmatrix} a & u \\ b & s \end{pmatrix} \leftarrow \begin{pmatrix} x & 1 \\ m & 0 \end{pmatrix}$ // invariant $\begin{cases} a \equiv xu \ (m) \\ b \equiv xs \ (m) \end{cases}$
tant que $b \neq 0$ **faire**
  effectuer la division euclidienne $a = qb + r$, $0 \leq r < |b|$
  $\begin{pmatrix} a & u \\ b & s \end{pmatrix} \leftarrow \begin{pmatrix} b & s \\ r = a - qb & u - qs \end{pmatrix}$
fin tant que
si $a < 0$ **alors** $a \leftarrow -a, \ \ u \leftarrow -u$
si $a = 1$ **alors retourner** $u \operatorname{rem} m$ **sinon retourner** 0

Calcul de l'inverse dans $\mathbb{Z}/m$

La démonstration nous indique un algorithme pour calculer l'inverse :

Algorithme 5.1 calcul de l'inverse dans $\mathbb{Z}/m$ (non optimisé)

Entrée: deux entiers x, m tels que $0 < x < m$
Sortie: l'entier y vérifiant $0 < y < m$ tel que $xy \equiv 1 \ (m)$
ou 0 pour signaler que $\bar{x} \in \mathbb{Z}/m$ n'est pas inversible

// Calculer $a = \operatorname{pgcd}(x,m)$ et des coefficients de Bézout $u, v \in \mathbb{Z}$ tel que $xu + mv = a$.
$\begin{pmatrix} a & u & v \\ b & s & t \end{pmatrix} \leftarrow \begin{pmatrix} x & 1 & 0 \\ m & 0 & 1 \end{pmatrix}$ // invariant $\begin{cases} a = xu + mv \\ b = xs + mt \end{cases}$
tant que $b \neq 0$ **faire**
  effectuer la division euclidienne $a = qb + r$, $0 \leq r < |b|$
  $\begin{pmatrix} a & u & v \\ b & s & t \end{pmatrix} \leftarrow \begin{pmatrix} b & s & t \\ r = a - qb & u - qs & v - qt \end{pmatrix}$
fin tant que
si $a < 0$ **alors** $a \leftarrow -a, \ \ u \leftarrow -u, \ \ v \leftarrow -v$
si $a = 1$ **alors retourner** $u \operatorname{rem} m$ **sinon retourner** 0

Avantage : La correction a déjà été montrée.

Inconvénient : Un tiers des calculs est inutile.

Les cas particuliers $\mathbb{Z}/p$ et $\mathbb{Z}/p^n$

Corollaire

Si p *est premier, alors tout* $x \in \mathbb{Z}/p^*$ *est inversible.*

Démonstration. Nous avons $x = \bar{a}$ pour un entier $a \in \mathbb{Z}$.
Puisque p est premier on a soit $\operatorname{pgcd}(a,p) = 1$ soit $\operatorname{pgcd}(a,p) = p$.
D'où $\operatorname{pgcd}(a,p) = 1 \iff p \nmid a \iff a \not\equiv 0 \ (p) \iff \bar{a} \neq 0$. □

Remarque

Nous savons déjà que $\mathbb{Z}/m$ est un anneau.
Si p est premier, alors $\mathbb{Z}/p$ est un corps.

Corollaire

Soit p *premier et* $n \geq 1$. *Dans* $\mathbb{Z}/p^n$ *il existe exactement* p^{n-1} *éléments non inversibles, à savoir* $\overline{0}, \overline{p}, \overline{2p}, \ldots, \overline{p^n - p}$. *Ainsi* $|\mathbb{Z}/p^{n\times}| = (p-1)p^{n-1}$.

Démonstration. Les diviseurs de p^n sont p^k où $0 \leq k \leq n$.
Donc $\operatorname{pgcd}(a,p) = p^k$ pour un $0 \leq k \leq n$, d'où $\operatorname{pgcd}(a,p^n) = 1 \iff p \nmid a$.
Les éléments non inversibles $\bar{a} \in \mathbb{Z}/p^n$ proviennent des multiples $a \in p\mathbb{Z}$. □

Le théorème chinois : motivation

Commençons par un exemple concret. Le système

$$\begin{cases} x \equiv 7 & \mod 8 \\ x \equiv 48 & \mod 125 \end{cases}$$

admet une unique solution $x \in \mathbb{Z}$ où $0 \leq x < 1000$.
Pourquoi ? Comment la trouver efficacement ?

Soient m et n deux entiers premiers entre eux, autrement dit $\operatorname{pgcd}(m, n) = 1$.
Le théorème des restes chinois affirme que pour tout $x_1, x_2 \in \mathbb{Z}$ le système

$$\begin{cases} x \equiv x_1 & \mod m \\ x \equiv x_2 & \mod n \end{cases}$$

admet une solution $x \in \mathbb{Z}$, et que $x + \mathbb{Z}mn$ est l'ensemble des solutions.

Le développement suivant établit des preuves et des algorithmes efficaces.

L'anneau produit $\mathbb{Z}/m \times \mathbb{Z}/n$

Définition & proposition

Sur le produit cartésien $\mathbb{Z}/m \times \mathbb{Z}/n$ on définit une addition

$$+ \colon (\mathbb{Z}/m \times \mathbb{Z}/n) \times (\mathbb{Z}/m \times \mathbb{Z}/n) \to (\mathbb{Z}/m \times \mathbb{Z}/n)$$
$$\text{par} \qquad (x, y) + (x', y') := (x + x', y + y'),$$

et une multiplication

$$\cdot \colon (\mathbb{Z}/m \times \mathbb{Z}/n) \times (\mathbb{Z}/m \times \mathbb{Z}/n) \to (\mathbb{Z}/m \times \mathbb{Z}/n)$$
$$\text{par} \qquad (x, y) \cdot (x', y') := (x \cdot x', y \cdot y').$$

Ainsi $(\mathbb{Z}/m \times \mathbb{Z}/n, +, \cdot)$ devient un anneau.

Exercice

Que faut-il vérifier pour prouver l'affirmation ? Effectuer ces vérifications.

Éléments inversibles dans $\mathbb{Z}/m \times \mathbb{Z}/n$

Dans $\mathbb{Z}/m \times \mathbb{Z}/n$ On pose $0 := (\bar{0}, \bar{0})$ et $1 := (\bar{1}, \bar{1})$.

Définition

$z \in \mathbb{Z}/m \times \mathbb{Z}/n$ est inversible s'il existe $z' \in \mathbb{Z}/m \times \mathbb{Z}/n$ tel que $zz' = 1$.
On pose $(\mathbb{Z}/m \times \mathbb{Z}/n)^\times := \{z \in \mathbb{Z}/m \times \mathbb{Z}/n \mid z \text{ est inversible}\}$.

Proposition

Nous avons

$$(\mathbb{Z}/m \times \mathbb{Z}/n)^\times = \mathbb{Z}/m^\times \times \mathbb{Z}/n^\times,$$

et en particulier

$$|(\mathbb{Z}/m \times \mathbb{Z}/n)^\times| = |\mathbb{Z}/m^\times| \cdot |\mathbb{Z}/n^\times|.$$

Démonstration. Pour $z = (x, y)$ et $z' = (x', y')$ nous avons
$zz' = 1 \iff (x, y) \cdot (x', y') = (\bar{1}, \bar{1}) \iff xx' = \bar{1}$ et $yy' = \bar{1}$. □

L'application naturelle $\Phi \colon \mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$

$\mathbb{Z}/4 \to \mathbb{Z}/2 \times \mathbb{Z}/2$
$\bar{0} \mapsto (\bar{0}, \bar{0})$
$\bar{1} \mapsto (\bar{1}, \bar{1})$
$\bar{2} \mapsto (\bar{0}, \bar{0})$
$\bar{3} \mapsto (\bar{1}, \bar{1})$

$\mathbb{Z}/6 \to \mathbb{Z}/2 \times \mathbb{Z}/3$
$\bar{0} \mapsto (\bar{0}, \bar{0})$
$\bar{1} \mapsto (\bar{1}, \bar{1})$
$\bar{2} \mapsto (\bar{0}, \bar{2})$
$\bar{3} \mapsto (\bar{1}, \bar{0})$
$\bar{4} \mapsto (\bar{0}, \bar{1})$
$\bar{5} \mapsto (\bar{1}, \bar{2})$

$\mathbb{Z}/8 \to \mathbb{Z}/2 \times \mathbb{Z}/4$
$\bar{0} \mapsto (\bar{0}, \bar{0})$
$\bar{1} \mapsto (\bar{1}, \bar{1})$
$\bar{2} \mapsto (\bar{0}, \bar{2})$
$\bar{3} \mapsto (\bar{1}, \bar{3})$
$\bar{4} \mapsto (\bar{0}, \bar{0})$
$\bar{5} \mapsto (\bar{1}, \bar{1})$
$\bar{6} \mapsto (\bar{0}, \bar{2})$
$\bar{7} \mapsto (\bar{1}, \bar{3})$

$\mathbb{Z}/10 \to \mathbb{Z}/2 \times \mathbb{Z}/5$
$\bar{0} \mapsto (\bar{0}, \bar{0})$
$\bar{1} \mapsto (\bar{1}, \bar{1})$
$\bar{2} \mapsto (\bar{0}, \bar{2})$
$\bar{3} \mapsto (\bar{1}, \bar{3})$
$\bar{4} \mapsto (\bar{0}, \bar{4})$
$\bar{5} \mapsto (\bar{1}, \bar{0})$
$\bar{6} \mapsto (\bar{0}, \bar{1})$
$\bar{7} \mapsto (\bar{1}, \bar{2})$
$\bar{8} \mapsto (\bar{0}, \bar{3})$
$\bar{9} \mapsto (\bar{1}, \bar{4})$

L'application naturelle : existence et unicité

Proposition

Soient m, n deux entiers.

Il existe une et une seule application $\Phi\colon \mathbb{Z}/_{mn} \to \mathbb{Z}/_m \times \mathbb{Z}/_n$ vérifiant

$$\begin{aligned} \Phi(x+y) &= \Phi(x) + \Phi(y), & \Phi(\bar{0}) &= (\bar{0}, \bar{0}), \\ \Phi(x \cdot y) &= \Phi(x) \cdot \Phi(y), & \Phi(\bar{1}) &= (\bar{1}, \bar{1}). \end{aligned}$$

On l'appelle l'application naturelle de $\mathbb{Z}/_{mn}$ vers $\mathbb{Z}/_m \times \mathbb{Z}/_n$.

Plus explicitement elle est donnée pour tout $a \in \mathbb{Z}$ par

$$\Phi\big(\pi_{mn}(a)\big) = \big(\pi_m(a), \pi_n(a)\big).$$

Exercice

Vérifier que $\Phi\big(\pi_{mn}(a)\big) = \big(\pi_m(a), \pi_n(a)\big)$ est bien définie.

Vérifier que cette application a toutes les propriétés requises.

Montrer que c'est la seule application satisfaisant aux exigences.

L'application naturelle : vérifications

Démonstration. $\Phi\big(\pi_{mn}(a)\big) = \big(\pi_m(a), \pi_n(a)\big)$ est bien définie :

Si $\pi_{mn}(a) = \pi_{mn}(a')$, alors $a \equiv a' \pmod{mn}$, autrement dit $mn \mid a - a'$.

Ainsi $m \mid a - a'$ et $n \mid a - a'$, donc $a \equiv a' \pmod{m}$ et $a \equiv a' \pmod{n}$.

On conclut que $\pi_m(a) = \pi_m(a')$ et $\pi_n(a) = \pi_n(a')$.

Ensuite on vérifie que

$$\begin{aligned} \Phi(x+y) &= \Phi\big(\pi_{mn}(a) + \pi_{mn}(b)\big) = \Phi\big(\pi_{mn}(a+b)\big) = \big(\pi_m(a+b), \pi_m(a+b)\big) \\ &= \big(\pi_m(a) + \pi_m(b), \pi_n(a) + \pi_n(b)\big) = \big(\pi_m(a), \pi_n(a)\big) + \big(\pi_m(b), \pi_n(b)\big) \\ &= \Phi\big(\pi_{mn}(a)\big) + \Phi\big(\pi_{mn}(b)\big) = \Phi(x) + \Phi(y) \end{aligned}$$

Il en est de même pour les trois autres propriétés. Ceci montre l'existence.

Pour l'unicité supposons que deux applications $\Phi, \Phi'\colon \mathbb{Z}/_{mn} \to \mathbb{Z}/_m \times \mathbb{Z}/_n$ satisfont toutes les deux aux propriétés exigées.

Alors $\Phi(\bar{0}) = (\bar{0}, \bar{0}) = \Phi'(\bar{0})$ et $\Phi(\bar{1}) = (\bar{1}, \bar{1}) = \Phi'(\bar{1})$.

Par récurrence on montre que $\Phi(\bar{n}) = (\bar{n}, \bar{n}) = \Phi'(\bar{n})$ pour tout $n \in \mathbb{N}$ puis pour tout $n \in \mathbb{Z}$. Ceci prouve que $\Phi = \Phi'$. □

Le théorème des restes chinois

Théorème (des restes chinois)

Soient $m, n \in \mathbb{Z}$ deux entiers. L'application naturelle

$$\Phi\colon \mathbb{Z}/_{mn} \to \mathbb{Z}/_m \times \mathbb{Z}/_n, \qquad \Phi\big(\pi_{mn}(a)\big) = \big(\pi_m(a), \pi_n(a)\big)$$

est une bijection si et seulement si $\operatorname{pgcd}(m, n) = 1$.

Si $mu + nv = 1$, alors l'application inverse de Φ est donnée par

$$\Psi\colon \mathbb{Z}/_m \times \mathbb{Z}/_n \to\colon \mathbb{Z}/_{mn}, \qquad \Psi\big(\pi_m(a), \pi_n(b)\big) = \pi_{mn}(anv + bmu).$$

Remarque / exercice

Comme Φ, son inverse Ψ jouit des propriétés suivantes :

$$\begin{aligned} \Psi(x+y) &= \Psi(x) + \Psi(y), & \Psi(\bar{0}, \bar{0}) &= \bar{0}, \\ \Psi(x \cdot y) &= \Psi(x) \cdot \Psi(y), & \Psi(\bar{1}, \bar{1}) &= \bar{1}. \end{aligned}$$

Slogan

Calculer dans $\mathbb{Z}/_{mn}$ revient à calculer dans $\mathbb{Z}/_m \times \mathbb{Z}/_n$, si $\operatorname{pgcd}(m, n) = 1$!
Toute propriété vraie pour $\mathbb{Z}/_{mn}$ est vraie pour $\mathbb{Z}/_m \times \mathbb{Z}/_n$, et inversement.
On peut identifier $\mathbb{Z}/_{mn}$ et $\mathbb{Z}/_m \times \mathbb{Z}/_n$ à l'aide des bijections Φ et Ψ.

Le théorème chinois : démonstration

Démonstration. Si $d = \operatorname{pgcd}(m, n) > 1$ alors $x = \pi_{mn}(mn/d) \neq 0$ mais $\Phi(x) = (\bar{0}, \bar{0}) = \Phi(0)$. Donc Φ n'est pas injectif (ni surjectif).

Si $mu + nv = 1$ vérifions d'abord que Ψ est bien définie :

$$\begin{aligned} & \pi_m(a) = \pi_m(a') \quad \text{et} \quad \pi_n(b) = \pi_n(b') \\ \Rightarrow \quad & a \equiv a' \mod m \quad \text{et} \quad b \equiv b' \mod n \\ \Rightarrow \quad & anv \equiv a'nv \mod mn \quad \text{et} \quad bmu \equiv b'mu \mod mn \\ \Rightarrow \quad & anv + bmu \equiv a'nv + b'mu \mod mn \\ \Rightarrow \quad & \pi_{mn}(anv + bmu) = \pi_{mn}(a'nv + b'mu). \end{aligned}$$

Montrons ensuite que $\Phi \circ \Psi = \mathrm{id}$:

$$\begin{aligned} \Phi\Psi\big(\pi_m(a), \pi_n(b)\big) &= \Phi\big(\pi_{mn}(anv + bmu)\big) \\ &= \big(\pi_m(anv + bmu), \pi_n(anv + bmu)\big) \\ &= \big(\pi_m(a), \pi_n(b)\big). \end{aligned}$$

Montrons finalement que $\Psi \circ \Phi = \mathrm{id}$:

$$\begin{aligned} \Psi\Phi\big(\pi_{mn}(a)\big) &= \Psi\big(\pi_m(a), \pi_n(a)\big) \\ &= \pi_{mn}(anv + amu) \\ &= \pi_{mn}(a). \end{aligned}$$

Ceci prouve que Φ et Ψ sont des bijections mutuellement inverses. □

Exemples

Exercice

Résoudre le système $\begin{cases} x \equiv 7 & \mod 8 \\ x \equiv 48 & \mod 125 \end{cases}$ à l'aide de $8 \cdot 47 - 125 \cdot 3 = 1$.

Solution. On applique la formule explicite du théorème chinois :
$\Psi(\overline{8}, \overline{48}) = \pi_{1000}(-7 \cdot 125 \cdot 3 + 48 \cdot 8 \cdot 47) = \pi_{1000}(15423) = \overline{423}$.
Une fois trouvée, c'est facile à vérifier : $\pi_8(423) = \overline{7}$ et $\pi_{125}(423) = \overline{48}$.
L'ensemble des solutions $x \in \mathbb{Z}$ est $423 + \mathbb{Z}1000 = \{423 + k1000 \mid k \in \mathbb{Z}\}$. ☺

Exercice

Pour son examen oral un étudiant X doit réunir deux examinateurs :
Le professeur A ne peut que tous les 12 jours à partir de lundi, 1er janvier.
Le professeur B ne peut que les mercredis. Quelles dates sont possibles ?

Bien sûr, vous pouvez trouver la solution sans aucune théorie, en tâtonnant.
Il sera néanmoins instructif de comparer votre solution avec les formules ci-dessus en précisant les étapes du calcul.

Solution. On trouve d'abord $12 \cdot 3 + 7 \cdot (-5) = 1$,
puis on calcule $\Psi(\overline{1}, \overline{3}) = \pi_{84}(1 \cdot (-35) + 3 \cdot 36) = \overline{73}$.
Sont possibles le 14 mars, le 6 juin, le 29 août, et le 21 novembre. ☺

Généralisation à plusieurs facteurs

Théorème (des restes chinois)

Soit $m_1, \dots, m_k \geq 1$ une famille d'entiers et soit $m = m_1 \cdots m_k$ leur produit.
L'application naturelle

$$\begin{aligned} \Phi \colon \mathbb{Z}/_m &\to \mathbb{Z}/_{m_1} \times \cdots \times \mathbb{Z}/_{m_k} \\ \pi_m(x) &\mapsto \big(\pi_{m_1}(x), \dots, \pi_{m_k}(x)\big) \end{aligned}$$

est une bijection si et seulement si $\operatorname{pgcd}(m_i, m_j) = 1$ pour tout $i \neq j$.

Dans ce cas $m_i' = m/m_i = \prod_{j \neq i} m_j$ est inversible modulo m_i.
Il existe donc $u_i \in \mathbb{Z}$ où $0 < u_i < m_i$ tel que $u_i m_i' \equiv 1$ modulo m_i.
L'application inverse de Φ est alors donnée par

$$\begin{aligned} \Psi \colon \mathbb{Z}/_{m_1} \times \cdots \times \mathbb{Z}/_{m_k} &\to \mathbb{Z}/_m \\ \big(\pi_{m_1}(y_1), \dots, \pi_{m_1}(y_k)\big) &\mapsto \pi_m\big(y_1 u_1 m_1' + \cdots + y_k u_k m_k'\big). \end{aligned}$$

Exercice

Montrer que Φ et Ψ sont bien définies et vérifient $\Phi \circ \Psi = \mathrm{id}$ et $\Psi \circ \Phi = \mathrm{id}$.

Exemples classiques

Exercice (de Sun Zi, 3e siècle)

Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste 2 soldats, rangés par 5 colonnes, il reste 3 soldats et, rangés par 7 colonnes, il reste 2 soldats ?

Exercice (une histoire de pirates)

Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces.

Mais les pirates se querellent, et six d'entre eux sont tués.
Un nouveau partage donnerait au cuisinier 4 pièces.

Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier.

Quelle est la fortune minimale que peut espérer le cuisinier
s'il décide d'empoisonner le reste des pirates ?

Un exemple plus grand

Exemple

Résoudre le système $\begin{cases} x \equiv 18000 & \mod 19687 \\ x \equiv 13 & \mod 17 \end{cases}$

Pour $m = 19687$ et $n = 17$ on trouve $mu + nv = 1$ pour $u = 1$ et $v = -1158$.
On a $mn = 334679$ et $nv = -19686$ et $mu = 19687$, et ainsi

$$\Psi\big(\pi_m(a), \pi_n(b)\big) = \pi_{mn}(-19686a + 19687b).$$

Pour $a = 18000$ et $b = 13$ on trouve la solution $x = -354092069$.
On réduit ensuite ce nombre modulo mn, ce qui donne $x = 332992$.
Vous pouvez finalement vérifier que $x \equiv a \mod m$ et $x \equiv b \mod n$.

Observation

Malgré la petitesse du nombre cherché $x \in \mathbb{Z}$ où $0 \leq x < mn$,
le calcul provoque l'apparition d'une quantité mille fois plus grande.
La formule du théorème n'est donc pas optimale pour le calcul.

⚠ L'application Ψ est unique, mais la formule utilisée ne l'est pas !
Il convient donc d'en développer une autre qui soit plus efficace.

Optimisation du calcul : l'idée

Observation (représentation en base mixte)

Tout entier x vérifiant $0 \leq x < m_1 m_2 \cdots m_k$ s'écrit de manière unique comme

$$x = c_1 + m_1 c_2 + m_1 m_2 c_3 + \cdots + m_1 m_2 \cdots m_{k-1} c_k$$

où chaque « chiffre » $c_i \in \mathbb{Z}$ vérifie $0 \leq c_i < m_i$.

1. Comment trouver x tel que $x \equiv y_1 \pmod{m_1}$?
   Évidemment il suffit de poser $c_1 \leftarrow y_1 \operatorname{rem} m_1$.

2. Comment satisfaire en plus à $x \equiv y_2 \pmod{m_2}$?
   Il suffit de résoudre $c_1 + m_1 c_2 \equiv y_2 \pmod{m_2}$.
   Ceci équivaut à $m_1 c_2 \equiv y_2 - c_1 \pmod{m_2}$.
   Posons donc $c_2 \leftarrow [u_2(y_2 - c_1)] \operatorname{rem} m_2$,
   où $u_2 \in \mathbb{Z}$, $0 \leq u_2 < m_2$, représente l'inverse de m_1 modulo m_2.

On peut ainsi continuer à calculer un par un les coefficients $c_1, c_2, \ldots, c_n$.

Optimisation du calcul : l'algorithme

Théorème

Soit $m_1, \ldots, m_k \geq 1$ une famille d'entiers, premiers entre eux deux à deux.

Pour tout i soit $u_i \in \mathbb{Z}$, $0 \leq u_i < m_i$ l'inverse de $m_1 \ldots m_{i-1}$ modulo m_i.

Étant donné $y_1, \ldots, y_k \in \mathbb{Z}$ l'algorithme suivant calcule l'unique entier $x \in \mathbb{Z}$ vérifiant $0 \leq x < m_1 \cdots m_k$ et $x \equiv y_1 \pmod{m_1}$, …, $x \equiv y_k \pmod{m_k}$:

$$\begin{aligned}
&c_1 \leftarrow y_1 \operatorname{rem} m_1, && x_1 \leftarrow c_1,\\
&c_2 \leftarrow [u_2(y_2 - x_1)] \operatorname{rem} m_2, && x_2 \leftarrow x_1 + m_1 c_2,\\
&c_3 \leftarrow [u_3(y_3 - x_2)] \operatorname{rem} m_3, && x_3 \leftarrow x_2 + m_1 m_2 c_3,\\
&\quad\vdots\\
&c_k \leftarrow [u_k(y_k - x_{k-1})] \operatorname{rem} m_k, && x_k \leftarrow x_{k-1} + m_1 \cdots m_{k-1} c_k.
\end{aligned}$$

De plus, cet algorithme est le plus économe possible dans le sens que tous les calculs intermédiaires se placent dans l'intervalle $\{0, m_1 \cdots m_k - 1\}$.

Exercice

Prouver ce théorème : vérifier que $0 \leq c_i < m_i$ et $0 \leq x_i < m_1 \cdots m_i$,
puis montrer les congruences souhaitées $x_i \equiv y_j \pmod{m_j}$ pour $j \leq i$.

L'indicatrice d'Euler

Définition (indicatrice d'Euler)

On définit $\varphi \colon \mathbb{N} \to \mathbb{N}$ par

$$\varphi(n) := |\mathbb{Z}/n^\times| = \operatorname{card}\{a \in \mathbb{Z} \mid 0 < a < n \wedge \operatorname{pgcd}(a, n) = 1\}.$$

Théorème

Si $n = p_1^{e_1} \cdots p_\ell^{e_\ell}$ où $1 < p_1 < \cdots < p_\ell$ sont premiers et $e_1, \ldots, e_\ell \geq 1$, alors

$$\varphi(n) = (p_1 - 1) p_1^{e_1 - 1} \cdots (p_\ell - 1) p_\ell^{e_\ell - 1}.$$

Autrement dit, pour tout $n \in \mathbb{N}$ on a

$$\varphi(n) = n \prod_{p \text{ premier}, p \mid n} \Big(1 - \frac{1}{p}\Big).$$

Démonstration. On a $\operatorname{pgcd}(p_i^{e_i}, p_j^{e_j}) = 1$ pour tout $i \neq j$.
Le théorème chinois nous fournit donc une bijection naturelle

$$\begin{aligned}
\Phi \colon \mathbb{Z}/n &\xrightarrow{\sim} \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_\ell^{e_\ell},\\
\mathbb{Z}/n^\times &\xrightarrow{\sim} (\mathbb{Z}/p_1^{e_1})^\times \times \cdots \times (\mathbb{Z}/p_\ell^{e_\ell})^\times.
\end{aligned}$$

Pour p premier nous avons déjà montré que $\varphi(p^e) = (p-1)p^{e-1}$. □