INVERSE MODULAIRE D'UN ENTIER RELATIF

Notions réinvesties : PGCD, congruences, théorèmes de Bézout et de Gauss

Pour résoudre une équation du type $ax=b$, *on multiplie par* $\frac{1}{a}$ *chaque membre car* $\frac{1}{a}\times a=1$.
On dit d'ailleurs que $\frac{1}{a}$ *est l'inverse de a, on le note aussi* a^{-1}.

En arithmétique modulaire, il peut être très intéressant de vouloir faire la même chose et de trouver « l'inverse de a » (noté a^{-1}*). Ainsi on aura :* $ax \equiv b\ [n] \Leftrightarrow x \equiv a^{-1}\ b\ [n]$.

Mais peut-on toujours inverser ainsi un entier relatif ?

A. Une caractérisation cruciale en arithmétique modulaire

Soient a, b et x trois entiers relatifs tels que $ax \equiv b\ [n]$, avec $n \in \mathbb{N}^*$.

A.1 Une condition nécessaire...

Supposons que x est premier avec n.

1. Démontrer qu'il existe un entier relatif u tel que $ux \equiv 1\ [n]$.

2. Soit x' tel que $x' \equiv u\ [n]$.
Démontrer que $x\ x' \equiv 1\ [n]$.

3. Énoncer la propriété démontrée :

……

A.2 ... et suffisante ?

Supposons que x est inversible modulo n.

A-t-on : x premier avec n ? Justifier rigoureusement, puis énoncer la propriété démontrée :

……

A.3 Conclusion : un théorème bien pratique

Conclure en écrivant le théorème démontré :

CARACTÉRISATION DE L'INVERSIBILITÉ MODULAIRE
Soient a un entier relatif et $n \in \mathbb{N}^*$.

A.4 Et si *n* est premier ?

Si n est un nombre premier, combien de nombres admettent un inverse modulo n ?

B. Comment calculer un inverse modulaire quand il existe ?

B.1 Un premier exemple

Nous allons calculer l'inverse de 13 modulo 27.

1. Pourquoi cet inverse existe-t-il ?

2. a) Déterminer un entier relatif x tel que : $13x \equiv 1$ [27].

b) En déduire qu'il existe un unique entier m tel que $0 \leqslant m \leqslant 26$ et $13m \equiv 1$ [27].
Déterminer cet entier.

B.2 Généralisation

Écrire une méthode puis éventuellement un algorithme pour calculer l'inverse de a modulo n.

C. Résolution de l'équation $a\,x \equiv b\ [n]$

1. Supposons a et n premiers entre eux.

a) Pourquoi l'équation admet-elle au moins une solution ?

b) Cette solution est-elle unique modulo n ?

2. a) Supposons que le PGCD de a et n (noté d) divise b.

Démontrer que résoudre l'équation $a\,x \equiv b\ [n]$ revient à résoudre l'équation $\frac{a}{d}x \equiv \frac{b}{d}\ [\frac{n}{d}]$.

Cette dernière équation admet-elle une solution ?

b) Supposons que l'équation admette une solution x.

Démontrer qu'alors le PGCD de a et n (noté d) divise b.

Conclure en énonçant le théorème démontré :

RÉSOLUTION MODULAIRE DE L'ÉQUATION $a\,x = b$

Soient a un entier relatif et $n \in \mathbb{N}^*$.