UE USSI78 - Outils mathématiques pour l'informatique
Cours 2 - Élements d'arithmétique (suite)

Alain Faye

Cnam

2025-2026

Plan du cours

Plan

Plan

Plan

Plan

Définition

3 entiers a, b et p.
a est congru à b modulo p si (et seulement si) $a - b$ est divisible par p.
On note $a \equiv b \pmod{p}$.

- $9 \equiv 1 \pmod{2}$
- $20 \equiv 2 \pmod{3}$
- $17 \equiv 1 \pmod{4}$
- $18 \equiv 8 \pmod{10}$
- $324 \equiv 49 \pmod{55}$
- $18 \equiv 18 \pmod{55}$

Propriété

La congruence modulo p est une relation d'équivalence dans les entiers relatifs .

Notamment, on utilise souvent la transitivité.

- $40 \equiv 20 \pmod 2$ et $20 \equiv 10 \pmod 2$ et donc $40 \equiv 10 \pmod 2$
- $20 \equiv 14 \pmod 3$ et $14 \equiv 2 \pmod 3$ et donc $20 \equiv 2 \pmod 3$
- $17 \equiv 13 \pmod 4$ et $13 \equiv 1 \pmod 4$ donc $17 \equiv 1 \pmod 4$

Pour abréger on peut écrire :

- $40 \equiv 20 \equiv 10 \pmod 2$
- $20 \equiv 14 \equiv 2 \pmod 3$
- $17 \equiv 13 \equiv 1 \pmod 4$

Ćongruence modulo

Quelques propriétés

Propriété

Soit $a \equiv a' \pmod{p}$ *et* $b \equiv b' \pmod{p}$ *alors*

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

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

$$a^k \equiv (a')^k \pmod{p}$$

Soit $10 \equiv 2 \pmod{4}$ et $11 \equiv 3 \pmod{4}$.

- Pour la somme, $21 \equiv 5 \pmod{4}$. Par ailleurs , $5 \equiv 1 \pmod{4}$ donc $21 \equiv 1 \pmod{4}$.
- Pour le produit, $110 \equiv 6 \pmod{4}$. Par ailleurs, $6 \equiv 2 \pmod{4}$ et donc $110 \equiv 2 \pmod{4}$
- Pour l'élévation à la puissance, $10^7 \equiv 2^7 \pmod{4} \equiv 0 \pmod{4}$, $11^7 \equiv 3^7 \pmod{4} \equiv 3 \pmod{4}$

Ćongruence modulo

Calcul avec des chiffres comportant des exposants

- On veut calculer le reste de la division entière de 2^{11} par 15.
  $2^{11} = 2^4 2^4 2^3$ et $2^4 = 16 \equiv 1 \pmod{15}$. Donc $2^4 2^4 2^3 \equiv 1 \times 1 \times 2^3 \pmod{15}$.
  $2^3 = 8 \equiv 8 \pmod{15}$. Finalement, $2^{11} \equiv 8 \pmod{15}$. Le reste de la division de 2^{11} par 15 est 8.
- On veut calculer le reste de la division entière de 18^5 par 55 .
  $18^5 = 18^2 18^2 18$ et $18^2 = 324$.
  $324 \equiv 49 \pmod{55}$ donc $18^5 \equiv 49 \times 49 \times 18 \pmod{55}$
  $49 \times 18 = 882$ et $882 \equiv 2 \pmod{55}$ donc $49 \times 49 \times 18 \equiv 49 \times 2 \pmod{55}$
  $49 \times 2 = 98 \equiv 43 \pmod{55}$
  Finalement, $18^5 \equiv 43 \pmod{55}$

Définition

Soit e un entier premier avec p un autre entier , l'inverse de e modulo p est l'entier d tel que $ed \equiv 1 \pmod{p}$.

Lorsque e est premier avec p, on a vu qu'il existe u, v entiers tels que $ue + vp = 1$. (théorème de Bezout).
u et v peuvent se calculer en calculant le PGCD de e et p et en utilisant les résultats de l'algorithme d'Euclide.
Donc, $ue - 1 = -vp$ ce qui veut dire $ue \equiv 1 \pmod{p}$ car $-vp$ est un multiple de p. Donc u est l'inverse de e modulo p.

Remarque

L'inverse n'est pas unique car $ue + vp = 1$ *s'écrit aussi* $(u - kp)e + (v + ke)p = 1$ *pour tout entier* k. *Donc* u *l'inverse de* e *est défini à un multiple de* p *près.*

Congruence modulo

Inverse modulo

Calculons l'inverse de 30 modulo 7. On calcule le PGCD de 30 et 7.

$$30 = 4 \times 7 + 2$$

$$7 = 3 \times 2 + 1$$

Le PGCD de 30 et 7 est 1. Ils sont bien premiers entre eux. On remonte l'algorithme d'Euclide pour calculer l'inverse de 30.

$$1 = 7 - 3 \times 2$$

$$1 = 7 - 3 \times (30 - 4 \times 7) = -3 \times 30 + 13 \times 7$$

L'inverse de 30 modulo 7 est -3. Mais aussi $-3 + 7 = 4$ car

$$1 = (-3 + 7) \times 30 + (13 - 30) \times 7$$

Lemme

Soient a et b 2 entiers, p un nombre premier. Si ab est divisible par p alors a ou b est divisible par p.

On peut le voir en considérant la décomposition en facteurs premiers de ab, a et b.
Exemple : $a = 18$, $b = 50$, $ab = 900$, $p = 5$. $p = 5$ divise $ab = 900$ et $b = 50$. En décomposant en facteurs premiers, $a = 2 \times 3^2$, $b = 2 \times 5^2$. Donc $ab = 2^2 \times 3^2 \times 5^2$. Le facteur 5 qui apparait dans le produit ab vient de b.

Théorème

Soit p nombre premier et a entier non multiple de p

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

- $9^1 \equiv 1 \pmod 2$
- $8^2 \equiv 1 \pmod 3$
- $2^4 \equiv 1 \pmod 5$
- $2^6 \equiv 1 \pmod 7$

Si p pas premier, cela n'est plus vrai : $2^5 \equiv 2 \pmod 6$

Petit théorème de Fermat

Démonstration

Considérons le nombre $N = a \times 2a \times \ldots \times (p-1)a$.
En appliquant la division euclidienne par p sur chaque terme ia $(i = 1, \ldots, p-1)$ on obtient $ia = q_i \times p + r_i$ où $0 \leq r_i \leq p-1$ est le reste de la division. En reportant dans N on obtient :

$$N = (q_1 p + r_1) \times (q_2 p + r_2) \times \ldots \times (q_{p-1} p + r_{p-1}) = r_1 r_2 \ldots r_{p-1} + N'$$

où N' est un multiple de p. Donc $N \equiv r_1 r_2 \ldots r_{p-1} \pmod{p}$.
r_i $(i = 1, \ldots, p-1)$ n'est pas nul car ia n'est pas divisible par p. En effet, si ia était divisible par p alors p diviserait i ou p (Lemme d'Euclide) . Or a n'est pas un multiple de p et $i \leq p-1$. Donc $1 \leq r_i \leq p-1$.
Maintenant supposons que deux r_i, r_j, avec $i \neq j$, soient égaux. Supposons sans perte de généralité $i > j$. Alors,

$$ia - ja = q_i p + r_i - (q_j p + r_j) = (q_i - q_j)p$$

. Donc $(i-j)a$ est divisible par p. Par le Lemme d'Euclide, p divise $i - j$ ou a. Or $i - j \leq p-1$ et a n'est pas un multiple de p. Contradiction donc $r_i \neq r_j$.

Petit théorème de Fermat

Démonstration (suite)

Ainsi tous les r_i sont distincts, ils commencent à 1 et il y en a exactement $p-1$. Par conséquent, $r_1 r_2 \ldots r_{p-1} = 1 \times 2 \times \ldots \times (p-1) = (p-1)!$. Par ailleurs, $N = (p-1)! \times a^{p-1}$.
On arrive donc à $(p-1)! \times a^{p-1} \equiv (p-1)! \pmod{p}$. Soit de façon équivalente, $(p-1)!(a^{p-1}-1)$ est un multiple de p. Par le lemme d'Euclide, p divise $(p-1)!$ ou $(a^{p-1}-1)$. En appliquant $p-2$ fois le lemme d'Euclide sur le produit $1 \times 2 \times \ldots \times (p-1)$ dont tous les termes sont plus petits que p, on en déduit que $(p-1)!$ n'est pas un multiple de p. Donc forcément, $(a^{p-1}-1)$ est un multiple de p ce qui s'écrit $a^{p-1} \equiv 1 \pmod{p}$.

Algorithme RSA

RSA (Rivest, Shamir, Adleman)

L'algorithme RSA est conçu pour échanger des messages, de façon sûre, entre 2 personnes A et B. De façon sûre signifie qu'une tierce personne ne peut lire les messages échangés.

- A choisit 2 (grands) entiers $p \neq q$ premiers, calcule $n = pq$
- A choisit un entier e premier avec $(p-1)(q-1)$
- A calcule d l'inverse de e modulo $(p-1)(q-1)$
- (n, e) est la clé publique. d reste secret. p et q peuvent être détruits
- B découpe son message en nombres entiers m tels que $0 \leq m \leq n-1$
- B code son message, un entier m, par c tel que $m^e \equiv c \pmod{n}$
- A décode le message de B en calculant $c^d \pmod{n}$ qui vaut m

Remarque

Les congruences modulo n sont calculés par les restes de la division euclidienne de m^e et de c^d par n i.e. $0 \leq c \leq n-1$ et $0 \leq m \leq n-1$.

Algorithme RSA

Exemple

- A choisit 2 nombres premiers $p = 3$ et $q = 5$
- $n = pq = 15$ et $(p-1)(q-1) = 8$
- A choisit $e = 11$ premier avec 8
- A calcule d l'inverse de $e = 11$ modulo $(p-1)(q-1) = 8$:
  - Algorithme d'Euclide pour calculer PGCD(11,8)

$$11 = 1 \times 8 + 3$$

$$8 = 2 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

  - On remonte

$$1 = 3 - 1 \times 2$$

$$1 = 3 - (8 - 2 \times 3) = -8 + 3 \times 3$$

$$1 = -8 + 3(11 - 1 \times 8) = {\color{red}3} \times 11 - 4 \times 8$$

- l'inverse de $e = 11$ modulo 8 est $d = 3$.

Algorithme RSA
Exemple (suite)

- la clé publique est $(n, e) = (15, 11)$. d reste privé.
- B code le message $m = 2$ pour l'envoyer à A.
  - il calcule $c \equiv m^e \pmod{n} = 2^{11} \pmod{15} = 8$
  - il envoie $c = 8$ à A
- A reçoit $c = 8$. Il doit le décoder.
  - il calcule $c^d \pmod{n} = 8^3 \mod 15 = 2$
  - A peut lire le message décodé $m = 2$

Algorithme RSA
Exemple (suite)

- la clé publique est $(n, e) = (15, 11)$. d reste privé.
- B code le message $m = 13$ pour l'envoyer à A.
  - Que va-t-il envoyer ?
- A reçoit le message codé c. Il doit le décoder.
  - Que doit-t-il faire ?

Algorithme RSA

Exemple (suite)

- la clé publique est $(n, e) = (15, 11)$. d reste privé.
- B code le message $m = 13$ pour l'envoyer à A.
  - il calcule $c \equiv m^e \pmod{n} = 13^{11} \pmod{15} = 7$
  - il envoie $c = 7$ à A
- A reçoit $c = 7$. Il doit le décoder.
  - il calcule $c^d \pmod{n} = 7^3 \mod 15 = 13$
  - A peut lire le message décodé $m = 13$

Algorithme RSA
Pourquoi est-il sûr ?

La sureté repose sur le fait qu'il est difficile de trouver la décomposition de n en facteurs premiers p et q si n est grand.
Si une tierce personne ne connait pas p et q, même connaissant e qui est publique, elle ne peut pas calculer d l'inverse de e modulo $(p-1)(q-1)$.
En pratique, n peut comporter des centaines de chiffres.

Algorithme RSA
Validité

Théorème

- *Soit* $n = pq$ *avec* p *et* q *premiers et* $p \neq q$,
- *Soit* e *premier avec* $(p-1)(q-1)$,
- *Soit* d *l'inverse de* e *modulo* $(p-1)(q-1)$ *i.e. tel que* $ed \equiv 1 \mod (p-1)(q-1)$
- *Soit un entier* m

alors $m^{ed} \equiv m \pmod{n}$

La démonstration repose sur le petit théorème de Fermat.

Algorithme RSA

Validité démonstration

$ed \equiv 1 \mod (p-1)(q-1)$. Donc $ed = k(p-1)(q-1)+1$ pour un entier k.
Si m n'est pas un multiple de p, alors par le petit théorème de Fermat, $m^{p-1} \equiv 1 \pmod p$ car p premier. Donc, en élevant à la puissance $k(q-1)$, on obtient $m^{k(q-1)(p-1)} \equiv 1^{k(q-1)} \pmod p \equiv 1 \pmod p$. En multipliant par m, on obtient $m^{1+k(q-1)(p-1)} \equiv m \pmod p$. Maintenant, si m est un multiple de p alors $m = k'p$, et alors $m^{1+k(q-1)(p-1)} \equiv 0 \pmod p$ et de même $m \equiv 0 \pmod p$. Donc,

$$m^{1+k(q-1)(p-1)} \equiv m \pmod p$$

est valide pour tout entier m. De même, on peut étabilr que

$$m^{1+k(q-1)(p-1)} \equiv m \pmod q$$

Algorithme RSA

Validité démonstration (suite)

Par conséquent, $m^{1+k(q-1)(p-1)} - m$ est divisible à la fois par p et q donc il est divisible aussi par le produit pq car p et q sont des nombres premiers distincts (ceci découle du lemme d'Euclide).
Donc,

$$m^{1+k(q-1)(p-1)} - m \equiv 0 \pmod{pq}$$

Ce qui s'écrit aussi,

$$m^{1+k(q-1)(p-1)} \equiv m \pmod{pq}$$

Plan

Plan