Université de Paris

NUMÉRATION LOGIQUE

C6 : calcul modulaire

Nicole VINCENT

Université de Paris

Calculer sans retenue

- En base b, on utilise l'alphabet {0, 1, … ,b-1}
  Pour une somme de deux chiffres, on applique le principe de position

  Exemples : en base b = 10 7 + 8 = 15,

  en base b = 2 1 + 1 = 10
- En utilisant {0, 1, … ,b-1}, le 0 et le principe de position, on peut représenter les entiers
  Mais parfois, il faut tenir compte de la périodicité de ce qui est représenté
  - les heures de la journée de 1h à 24h
  - les jours de la semaine de lundi (1) à dimanche (7)
  - les angles sont mesurés de 0 à 360
  - le signal d'un phare passe de façon périodique toutes les x sec.
  - une roue mécanique à m dents fait un tour entier quand les m dents se retrouvent dans leur position initiale

2

Université de Paris

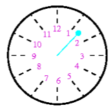
Calcul modulaire

- Pour formaliser ces problèmes, on utilise la théorie de nombres, l'arithmétique modulaire, le calcul modulaire
- Les théoriciens : Euclide (approx. de -325 à -265) et Diophante d'Alexandrie (approx. de 210 à 284) et en Chine Sun Zi (vers 300) et Qin Jiushao (approx. de 1202 à 1261)
- Applications aujourd'hui :
  Calcul de clés de contrôle, codes correcteurs, cryptographie, . . .
- Définitions : soient a et b deux entiers relatifs, on dit que
  1. a divise b s'il existe k ∈ Z tel que b = ka. On note a/b
  2. a et b sont premiers entre eux si leur plus grand commun diviseur est 1
     On note pgcd(a; b) = 1

3

Université de Paris

Calcul modulaire : exemple



Horloge avec une aiguille et 12 graduations de 1 à 12

Ici 12 est identique à 0h et 24h, tandis que 18h est identifié à 6h

De façon générale, pour **r** $\in \{1, \dots, 12\}$,

r représente les entiers de la forme $n = r + 12k$ où $k \in \mathbb{Z}$

En remplaçant 12 par 0, $r \in \{0, 1, \dots, 11\}$

On peut dire que **r** représente les entiers n tels que le reste de la division euclidienne de n par 12 est r

4

Université de Paris

Calcul modulaire – congruence $p \in \mathbb{N} \setminus \{0, 1\}$

Défintion : a et b sont **congruants** modulo p

si $a = b + pk$ pour un certain entier k

si $a - b$ est un multiple de p

$\boxed{a \equiv b \bmod p}$

- $a \equiv b \bmod p$ si et seulement si a et b ont le même reste dans la division euclidienne par p

  alors $a = k.p + r$ pour $k \in \mathbb{Z}$ et $r \equiv a \bmod p$
- Si $a \equiv b \bmod p$ et si $b \equiv c \bmod p$ alors $a \equiv c \bmod p$
- Si $a_1 \equiv b_1 \bmod p$ et $a_2 \equiv b_2 \bmod p$, alors
  $a_1 + a_2 \equiv b_1 + b_2 \bmod p$ $a_1 a_2 \equiv b_1 b_2 \bmod p$ pour tout entier $n \in \mathbb{Z}$, $na \equiv nb \bmod p$
- Tout entier $n \in \mathbb{Z}$ a un représentant dans $F_p = \{0, 1, \dots, p-1\}$
  Les calculs modulo p sur les entiers peuvent se ramener aux calculs modulo p dans F_p

5

Université de Paris

Exemples

Modulo 9 : $12 + 7 \equiv 3 + 7 \bmod 9 \equiv 10 \equiv 1 \bmod 9$

$12 . 7 \equiv 3 . 7 \equiv 21 \equiv 3 \bmod 9$ car $21 = 2 \ 9 + 3$

Modulo 6 : $2000 \equiv 20 . 100 \equiv 20 . 20 . 5 \equiv 2 . 2 . 5 \equiv 20 \equiv 2 \bmod 6$

Application : Il est 15h et ma montre sonne toutes les heures. Dans 17240 minutes, combien de temps devrais-je attendre pour que ma montre sonne ?

On fait les calculs modulo 60

$17240 = 1724.10 = 862.2.10 = 2.(600 + 262).10 = 2.(240+22).10$

$\equiv 2 . 22 . 10 \bmod 60 \equiv 440 \equiv (360 + 80) \bmod 60$

$\equiv (60 + 20) \bmod 60 \equiv 20 \bmod 60$

Il faudra attendre 60 - 20 = 40 minutes

6

Université de Paris

Application 2

Jean est né un mardi. Jacques est né 4 ans et 212 jours plus tard. Quel jour est né Jacques?

$3 \,.\, 365 + 366 + 212 \equiv ?$ mod 7

On a $350 = 7 \,.\, 50$ donc $365 = 350 + 15 \equiv 15$ mod 7

$366 \equiv 16$ mod 7

$210 = 3 \,.\, 70$ donc $212 \equiv 2$ mod 7

$3 \,.\, 365 + 366 + 212 \equiv 3 \,.\, 15 + 16 + 2 \equiv 3 \,.\, 1 + 2 + 2 \equiv 0$

donc Jacques est né un mardi

Calcul modulaire

Exemple : calculer $x \equiv 23^6$ mod 7 et $y \equiv 233^6$ mod 7,

$23^6 = 148035889 = 7 \,.\, 21147984 + 1$ $233^6 = 160005726539569$

mais modulo 7 on a : $23^6 \equiv 2^6 = 2^3 \cdot 2^3 \equiv 1 \,.\, 1$

$233 = 210 + 23$ donc $233^6 \equiv 1$ mod 7

On représente les opérations dans F_p grâce à des tableaux :

Pour $p = 2$, $F_2 = \{0; 1\}$

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

Pour $p = 3$, $F_3 = \{0; 1; 2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Pour $p = 4$, $F_4 = \{0; 1; 2; 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

X	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Inverse et opposé

- **opposé** d'un nombre x dans F_p est le nombre y tel que $x + y \equiv 0$
  On note aussi $y \equiv -x$ mod p Exemple : $-5 = 3$ mod 8
- **inverse** d'un nombre x modulo p un nombre y tel que $x \,.\, y \equiv 1$ mod p
  Exemple : $3^{-1} = 2$ mod 5 $2 \,.\, 3 = 6 \equiv 1$ mod 5
  - Un nombre n'a pas toujours d'inverse
    Exemple : 2 n'a pas d'inverse modulo 4, car 2x est toujours pair
  - Si p est un nombre premier,
    tous les éléments de F_p ont un inverse, sauf 0

Petit théorème de Fermat

Théorème : Soit p un nombre premier, dans F_p, tout nombre x vérifie $x^{p-1} = 1$, c'est-à-dire

$$x^{p-1} \equiv 1 \text{ modulo } p$$

Dans F_3 : $2^2 = 4 \equiv 1$

Dans F_5 : $2^4 = 16 \equiv 1$

Dans F_7 : $2^6 = 64 = 63 + 1 \equiv 1$

Dans F_7 : $6^6 \equiv (-1)^6 \equiv 1$

Dans F_7 : $4^6 = 2^6 \,.\, 2^6 \equiv 1 \,.\, 1 \equiv 1$

La preuve du petit théorème de Fermat (1640) repose sur des principes d'arithmétique, et prend environ une demi-page

A ne pas confondre avec le "grand théorème de Fermat", dont la preuve fait une centaine de pages, démontré en 2001 par Andrew Wiles ce qui lui a valu la médaille Fields

Petit théorème de Fermat

- Dans F_{17} :

$2^{16} = 65\,536 = 51\,000 + 14536 = (3 \;\; 17\,000) + 14536$

$\equiv 17\,000 - 2464 \equiv -2464 \equiv -3400 + 1000 - 64 \equiv 936$

$\equiv 680 + 256 \equiv 170 + 86 \equiv 85 + 1 \equiv 1$

17
34
51
68
85
102
119
136

- Dans F_{17} :

$9^{16} \equiv (-8)^{16} \equiv (-1)^{16} \, (2^{16})^3 \equiv 1$

$9 + 8 = 17$ $8 = 2^3$ $2^{16} \equiv 1$

Calcul modulaire : clé de sécurité

Pour éviter des erreurs lors de la saisie d'un numéro, comme un chiffre erroné ou la permutation de chiffres, on adjoint souvent une clé de sécurité

Exemple : numéro de sécurité sociale composé de 13 chiffres

$$s = s_{12}s_{11} \dots\ s_0$$

On lui associe **une** clé de sécurité c(s) à deux chiffres calculée par

$$c(s) = 97 - (s \bmod 97) \in \{1, \dots, 97\}$$

Le calcul modulo le nombre premier 97 aide à détecter des erreurs de saisie dans s

Autre exemple : les codes barres EAN 13 …

Codes asymétriques basés sur la décomposition de grand nombres : principe simplifié

- On choisit un nombre premier p très grand, et **secret**, beaucoup plus grand que le nombre de mots qu'on veut coder Exemple : p = 927662347
- On choisit un nombre **e** premier avec p -1 dans {1, … , p -1} qui est public . C'est la **clé publique** Exemple : e = 101
- Théorème : Il existe un nombre d tel que : d e = k (p - 1) + 1

(d e ≡ 1 mod (p – 1). (e est l'inverse de d dans F_{p-1}) **d** est la **clé privée**

On peut la trouver en essayant toutes les possibilités.

Exemple : d = 587825645 car

101 . 587825645 = 64 . 927662346 + 1

13

Codes asymétriques basés sur la décomposition de grand nombres : principe simplifié : codage et décodage

- Coder un message, le message est un nombre m dans {1, … , p - 1}
- On transmet le message codé **c(m) = mᵉ mod p**

  Bien que e soit public, quelqu'un qui intercepterait le message ne pourrait pas en déduire m car il faut connaître p
- Exemple :

$m = 100\,000$, $c(m) = 100\,000^{101} \equiv 54446622 \bmod F_p$ (rapide pour l'ordinateur)

- Pour décoder le message, il faut calculer $\mathbf{c(m)^d}$

théorème de Fermat $x^{p-1} \equiv 1$ modulo p

$$c(m)^d \equiv (m^e)^d = m^{ed} = m^{1+k(p-1)} = m.(m^{p-1})^k \equiv m \bmod p$$

Exemple : $54446622^{587825645} \equiv 100\,000 \bmod p$

14

Problème du code précédent

- Pour coder un message, il faut connaître e et p. Il est donc facile d'en déduire d, et ainsi décoder tous les messages
- Ca ne convient pas pour permettre de coder un message au seul détenteur de la clé privée

15

Calcul modulaire : Algorithme RSA

Proposé par Rivest, Shamir et Adleman en 1977, Algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique (protocole SSL)

C'est un algorithme à **clé publique** CPub pour chiffrer

et à **clé privée** CPriv pour déchiffrer un message

Alice engendre les clés CPub et CPriv
Alice envoie CPub à Bob
Bob utilise CPub pour coder son message M en C(M)
Bob envoie C(M) à Alice par un canal non sécurisé
Seule Alice peut décoder C(M) grâce à CPriv et retrouve M

16 N'importe quel nombre M peut être envoyé
(pas seulement un grand nombre premier)

Calcul modulaire : Algorithme RSA

Calcul des clés :

1. Choisir deux nombres premiers distincts (et grands) p et q
2. Calculer $n = pq$ et $\varphi = (p - 1)(q - 1)$
3. Choisir e, avec $1 < e < \varphi$ et $pgcd(e, \varphi) = 1$
4. Déterminer d vérifiant $e\,d \equiv 1 \bmod \varphi$ ($\Leftrightarrow \exists\, k \in \mathbb{Z} /\ ed = \varphi . k + 1$)

Alors **CPub = (n, e)** et **CPriv = d**

- Chiffrement du message : Si M est un entier à chiffrer, $0 \leq M < n$, alors $\mathbf{C(M) \equiv M^e \bmod n}$
- Déchiffrement du message : Si C(M) est un entier chiffré, alors $\mathbf{C(M)^d \equiv M \bmod n}$

  Grâce ente autres au Petit théorème de Fermat
- La force de RSA est qu'il n'existe actuellement pas d'algorithme rapide pour factoriser un entier n grand en ses facteurs

17

Calcul modulaire : Algorithme RSA

$n = pq$ et $\varphi = (p - 1)(q - 1)$

$Pgcd(e, \varphi) = 1$ $\quad e . d \equiv 1 \bmod \varphi$ $\quad$: $\quad$ CPub = (n, e) et CPriv = d

$C(M) \equiv M^e \bmod n$ $\quad$ et $C(M)^d \equiv M \bmod n$

$x^{p-1} \equiv 1$ modulo p

$$C(M)^d = M^{ed} = M^{1+k(p-1)(q-1)} = M.(M^{p-1})^{k(q-1)} \equiv M \bmod p$$

$$C(M)^d = M^{ed} = M^{1+k(p-1)(q-1)} = M.(M^{q-1})^{k(p-1)} \equiv M \bmod q$$

$C(M)^d$-M est multiple de p et de q donc de n=pq

$$C(M)^d \equiv M \bmod n$$

18

Exemple

Cpub : (n,e) = (1073,71)
Cpriv : d = 1079

- On prend p = 29 et q = 37 qui sont secrets

  On a donc n = pq = 1073, ce nombre est public

  On a φ = (p - 1)(q - 1) = (29 - 1)(37 - 1) = 1008, qui reste secret.

  On choisit un nombre e premier avec φ = 1008. Par exemple, e = 71. Il est public

  On calcule d tel que d . e = 1 mod φ d = 1079 reste privé

  71 . 1079 ≡ 1 mod 1073 (⟺ 71 . 1079 = 1 + k . 1073)

- Comment envoyer un message codé ? Par exemple 'HELLO'

  code ASCII : M = 7269767679 (en réalité : 072069076076079)

  Le système est basé sur n, transmission des nombres < n

  On découpe donc en plusieurs mots (le récepteur recollera les mots)

  726 ; 976 ; 767 ; 900

19

Université de Paris

Exemple suite

Cpub : (n,e) = (1073,71)
Cpriv : d = 1079

- Codage

C(726) -> 726^{71} ≡ 436 mod 1073

C(976) -> 976^{71} ≡ 822 mod 1073

C(767) -> 767^{71} ≡ 825 mod 1073

C(900) -> 900^{71} ≡ 552 mod 1073

C(M) = 436; 822; 825; 552

- décodage

d est le nombre tel que d . e = 1 mod φ

φ = (p - 1)(q - 1) mais difficile de retrouver p et q

20

Université de Paris

Exemple décodage : $C(M)^d \equiv M$ mod n

Cpub : (n,e) = (1073,71)
Cpriv : d = 1079

- C(M1) = 436 d connu

d = 1079 car 71 . 1079 ≡ 1 mod 1073 (⟺ 71 . 1079 = 1 + k . 1073)

d.e ≡ 1 mod φ

- 436^{1079} ≡ 726 mod pq Donc M1 ≡ 726
- 822^{1079} ≡ $976^{1+k.1008}$ ≡ 976 mod 1073
- 825^{1079} ≡ 767 mod 1073
- 552^{1079} ≡ 900 mod 1073

21

Université de Paris

Calcul modulaire : Factorisation RSA-768

Le nombre RSA-768 a 232 décimales en base 10 et 768 bits en base 2. Il a été factorisé en 2009, après 31 mois de calculs avec plusieurs centaines de machines, en deux nombres premiers de 116 décimales.

RSA-768

=

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469
3899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377
94080665351419597459856902143413

=

3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308
773781446799489

X

3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027
009279873630891 7

22

Université de Paris