Les congruences

Principe des congruences

Les congruences sont très utiles car elles permettent de ramener des calculs avec de très grands nombres à des calculs avec des nombres raisonnables .
Elles permettent aussi d'utiliser facilement les raisonnements par disjonction des cas .

Comment ça marche ?

Pour déterminer des congruences modulo n , on élimine du nombre les multiples de n .

Exemple 1

On sait que $15 = 14 + 1 = 7 \times 2 + 1$; 15 est donc égal à un multiple de 7 plus 1 ; on a donc : $15 \equiv 1[7]$
On a donc un nombre limité de possibilités quand on travaille avec les congruences .
Si on travaille modulo 5 , les seuls nombres possibles sont 0 , 1 , 2 , 3 et 4 .

Exemple 2

Cherchons la valeur de 17 modulo 5 : 17 = 15 + 2 donc $17 \equiv 2[5]$
Il peut aussi être utile de penser aux valeurs négatives : $4 \equiv 4[5] \equiv -1[5]$

Comment les utiliser ?

On peut additionner , soustraire , multiplier des congruences .

Attention : on ne peut pas les diviser ni prendre de racines !

Exemple :
Soit la table modulo 5

n≡	0	1	2	3	4
$n^2 \equiv$	0	1	-1	-1	1

Car $2^2 = 4 \equiv -1[5]$ et $3^2 = 9 \equiv 4 \equiv -1[5]$

Traduction avec des congruences

On utilise beaucoup les congruences pour montrer des divisibilités , pour déterminer des restes de divisions euclidiennes , pour simplifier des écritures …

Dire qu'un nombre a est divisible par n , c'est équivalent à : $a \equiv 0[n]$

Dire que deux nombres a et b ont même reste dans la division euclidienne par n , c'est équivalent à $a \equiv b[n]$

Montrer des divisibilités

Quand on demande si une expression est divisible par un nombre , on peut facilement utiliser une table de congruence

Exemple 1

Pour quelles valeurs de x , $3x^2 - 5x + 7$ est-il divisible par 4 ?
Divisible par 4 = congruence modulo 4
On dresse une table de congruence , soit en détaillant (ça évite les erreurs de calculs) , soit directement :

x ≡	0	1	2	3
$3x^2 \equiv$	0	3	0	3
5x ≡	0	1	2	3
$3x^2 - 5x + 7 \equiv$	3	1	1	3

Conclusion : dans la dernière ligne le reste n'est jamais égal à 0 donc pour tout x , $3x^2 - 5x + 7$ n'est jamais divisible par 4

Exemple 2

Montrer que $n^7 + 2n^3$ est divisible par 3

Divisible par 3 = congruences modulo 3

n	0	1	2
n^7	0	1	2
$2n^3$	0	2	1
$n^7 + 2n^3$	0	$3 \equiv 0$	$3 \equiv 0$

Dans la dernière ligne , le reste est toujours nul donc $n^7 + 2n^3$ est divisible par 3 pour tout n .

- *Déterminer des restes dans des divisions euclidiennes*

Pour déterminer des restes , on peut utiliser les congruences mais attention

- Un reste est toujours positif

Exemple 1

Déterminer le reste de 754 dans la divisions euclidienne par 8 .

On doit donc chercher à quel nombre 754 est congru modulo 8

Or $754 = 94 \times 8 + 2$ donc $754 \equiv 2[8]$ donc le reste de 754 par 8 est 2 .

Exemple 2

Déterminer le reste dans la division euclidienne de 3^7 par 7

On commence par calculer avec les congruences les puissances de 3 :

$$3 \equiv 3[7] \; ; \; 3^2 = 9 \equiv 2[7] \; ; \; 3^3 = 27 \equiv -1[7]$$

Pourquoi prendre – 1 plutôt que 6 ?

Parce que des puissances de – 1 sont plus faciles à calculer de tête que des puissances de 6 .

Et on sait que $(-1)^2 = 1$ donc on met tout au carré :

On a donc : $(3^3)^2 \equiv (-1)^2 \equiv 1[7]$ ce qui donne donc $3^6 \equiv 1[7]$

Conclusion : $3^7 = 3^6 \times 3 \equiv 1 \times 3 \equiv 3[7]$

Le reste cherché est donc 3

Exemple 3

Déterminer le reste de 3^{27} dans la division euclidienne par 7

On a vu que $3^3 = 27 \equiv -1[7]$ *donc* $3^{27} = (3^3)^9 \equiv (-1)^9 \equiv -1[7]$ mais le reste doit être positif donc le reste est égal à 6 car $6 \equiv -1[7]$

- *Résoudre des équations*

On peut utiliser les congruences de deux façons : soit pour simplifier une équation ; soit parce que c'est une équation avec des congruences qu'on demande de résoudre

Exemple 1

Résoudre $3x \equiv 5[7]$

Le plus simple (et qui marche tout le temps) : faire une table de congruence modulo 7

x	0	1	2	3	4	5	6
3x	0	3	6	2	5	1	4

On trouve par lecture du tableau que x = 4 + 7 k .

Exemple 2

Résoudre 2x + 5y = 7

On peut travailler modulo 2 (puis modulo 5) pour faire disparaître une inconnue :

Modulo 2 : $y \equiv 1[2]$ donc y = 1 + 2p

Modulo 5 : $2x \equiv 2[5]$

x	0	1	2	3	4
2x	0	2	4	1	3

Donc par lecture du tableau x = 1 + 5k

On résume les deux : 2 (1 + 5k) + 5 (1 + 2p) = 7 donc 10k + 10p = 0 donc k = - p

Les solutions possibles sont donc les couples (x ;y) = (1 + 5k ; 1 – 2k) .

Avec ce procédé on a montré qu'il n'y a pas d'autres formes possibles pour des solutions mais on n'a pas prouvé que ces formes sont obligatoirement solutions ; il faut donc vérifier , c'est-à-dire faire la réciproque :

On remplace donc dans l'équation de départ : 2(1+5k) + 5(1-2k) = 7 OK

Les solutions sont donc : (1 + 5k ; 1 – 2k)

Des exemples plus élaborés

Exemple 1

Montrer que $16 \times 7^{2n} - 28 \times 3^{2n+3}$ est divisible par 5

On va commencer par exprimer tous les nombres présents modulo 5 ; attention , certains nombres jouent un peu à cache - cache !

$16 \equiv 1[5]$; $7^2 = 49 \equiv -1[5]$; $28 \equiv 3[5] \equiv -2[5]$;$3^2 = 9 \equiv -1[5]$; $3^3 = 27 \equiv 2[5]$

Et maintenant , on remplace :

$$16 \times 7^{2n} - 28 \times 3^{2n+3} = 16 \times (7^2)^n - 28 \times (3^2)^n \times 3^3 \equiv 1 \times (-1)^n + 2 \times (-1)^n \times 2$$
$$\equiv 5(-1)^n \equiv 0[5]$$

Exemple 2

Déterminer en fonction de n le reste de la division euclidienne de 2^n par 3 .

Puisqu'on cherche à diviser par 3 , on va travailler modulo 3 . On va commencer par calculer les premières puissances de 2 et déterminer leurs congruences modulo 3 .

$2 \equiv 2[3]; 2^2 = 4 \equiv 1[3]$

C'est suffisant car puisqu'on a trouvé un résultat égal à 1 , les simplifications deviennent faciles . Les nombres entiers se répartissent en deux catégories qui font intervenir un lien avec le « 2 » du carré : les nombres pairs et les nombres impairs , donc toutes les puissances possibles vont s'écrire soit sous la forme 2k , soit 2k + 1 . On a alors :

$2^{2k} = (2^2)^k \equiv 1^k \equiv 1[3]$ et $2^{2k+1} = 2(2^2)^k \equiv 2(1)^k \equiv 2[3]$

Conclusion : le reste de la division euclidienne de 2^{2k} par 3 est 1 et le reste de la division euclidienne de 2^{2k+1} par 3 est 2 .

Exemple 3

Démontrer que $n \equiv 2[3] \Leftrightarrow n^3 \equiv -1[9]$

On va travailler dans le plus grand ensemble donc modulo 9 . On écrit tous les n possibles puis on calcule leurs cubes et on regarde :

$n \equiv$	0	1	2	3	4	- 4	- 3	- 2	- 1
$n^3 \equiv$	0	1	-1	0	1	- 1	0	1	-1

On a donc $n^3 \equiv -1[9] \Leftrightarrow n \equiv 2\ ;\ -4\ ;\ -1\ [9] \Leftrightarrow n \equiv 2\ ;\ -1\ [3] \equiv 2[3]$

- En résumé , de l'entrainement et de la méthode et les congruences sont à la portée de tous !