Séance du 12.12. - Congruences applications

Propriété

Modulo n, les multiples de a sont les multiples de $pgcd(a, n)$.

Exemple : Modulo 28, on cherche les multiples de 21. $pgcd(21, 28) = 7$

Modulo 28, les multiples de 21 sont les multiples de 7.

Méthode

Soit une liste L de longueur 90, dont les éléments sont `L[0]`, `L[1]` ...`L[89]`.
On la parcourt en commençant par `L[0]` et en ajoutant 50 à chaque fois, modulo 90, indéfiniment.
Alors, puisque $pgcd(50, 90) = 10$, les multiples de 50 modulo 90 sont les multiples de 10 modulo 90 : cela veut dire qu'on ne parcourra pas tous les éléments de la liste, mais seulement :
`L[0]`, `L[10]`, `L[20]`, `L[30]`, `L[40]`, `L[50]`, `L[60]`, `L[70]` `L[80]`

Remarque

Si on parcourt une liste de longueur n en faisant des « sauts de p indices modulo n » alors on ne parcourra l'ensemble de la liste que si n et p sont premiers entre eux.

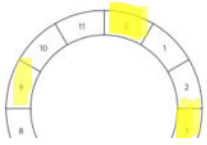
Reprenons la liste ci-dessus L[0], L[1], ..., L[89]
On parcourt en ajoutant 5 à chaque fois : Tous les éléments ne seront pas vus car 5 et 90 ne sont pas premiers entre eux.

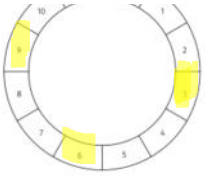
Programme Python pour tester le parcours d'une liste.
La liste comporte les numéros de 1 à N.
On modifie les éléments par -1 lorsqu'ils sont vus.

```
def creation_tableau(taille):
    L = []
    for i in range(taille):
        L.append(i)
    return(L)

def parcours_tableau(T,s,d):
    T[d] = -1 # on marque la case vue
    longueur = len(T) # len : nombre de cases du tableau
    indice = (d + s) % longueur
    while indice != d:
        T[indice] = -1
        indice = (indice + s) % longueur
    return(T)


#### DEBUT ####
N = int(input("Donner la taille de votre tableau : "))
Saut = int(input("Saut : "))
Depart = int(input("Numéro de la première case : "))
Mon_tableau = creation_tableau(N)
Mon_tab_parcouru = parcours_tableau(Mon_tableau,Saut,Depart)
print(Mon_tab_parcouru)
```

Exercice 51 : parcours d'une liste circulaire à pas constant

On considère le motif suivant : les cases sont numérotés de 0 à 11 (il y en a donc 12).





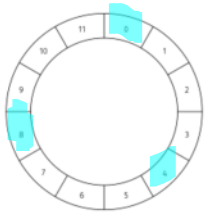
1. On choisit de parcourir les cases en partant de zéro et en se déplaçant à chaque fois de 3 cases, indéfiniment.
Colorier toutes les case parcourues.

2. Recopier leurs indices (leur numéro) :

Case parcourues : 0 ; 3 ; 6 ; 9

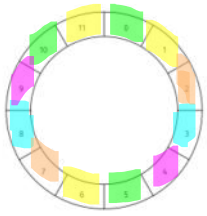
3. Refaire 1. et 2. mais en sautant 4 cases.

Case parcourues : 0 ; 4 ; 8 ; 0



4. Refaire 1. et 2. mais en sautant 5 cases.

Case parcourues : 0 à 11



5. Comment expliquer la différence entre la dernière liste et les deux premières ?

5 et 12 et premiers entre eux.

Exercice 52

On parcourt une liste circulaire de longueur 84 comme à l'exercice précédent, en partant de la case d'indice zéro et en sautant 735 cases (et oui cela fait beaucoup) à chaque fois, indéfiniment. La liste sera-t-elle parcourue entièrement ? Si ce n'est pas le cas, donner la liste des cases parcourues.
Justifier les réponses.

Regardons si 735 et 84 sont premiers entre eux.

a	b	r
735	84	63
84	63	(21)
63	21	0

pgcd (735 ; 84) = (21)

735 et 84 ne sont pas premiers entre eux.

Application : Une liste circulaire contient 254 éléments. On veut parcourir tous les éléments avec des sauts supérieurs à 100. Proposer une valeur en justifiant.

Aloys propose 107 car pgcd (254 ; 107) = 1.

Tolga propose 111 car pgcd (254 ; 111) = 1.

71. +++ **Congruences et puissances**

1. a) Compléter le résultat suivant :
$2^3 \equiv \ldots$ (modulo 7).
b) En déduire que, pour tout entier naturel n,
$2^{3n} \equiv 1$ (modulo 7).
2. a) Compléter le résultat suivant :
$2011 \equiv \ldots$ (modulo 7)
b) En déduire que $2011^{2012} \equiv 2^{2012}$ (modulo 7).
3. a) Écrire la division euclidienne de 2012 par 3.
b) En déduire que $2^{2012} \equiv (2^3)^{670} \times 2^2$.
c) Déduire de ce qui précède que
$2011^{2012} \equiv 4$ (mod 7)
et donner le reste de la division euclidienne de 2011^{2012} par 7.

1.a) $2^3 \equiv 1\ [7]$

$2^{3n} \equiv (2^3)^n \equiv 1^n \equiv 1\ [7]$

2.a) $2011 \equiv 2\ [7]$

b) $2011^{2012} \equiv 2^{2012}\ [7]$

3.a) $2012 = 670 \times 3 + 2$

$2011^{2012} \equiv 2^{2012} \equiv 2^{670\times3+2} \equiv 2^{670\times3} \times 2^2\ [7]$

$2011^{2012} \equiv (2^3)^{670} \times 4 \equiv 1^{670} \times 4 \equiv 1 \times 4 \equiv 4\ [7]$

Le reste de la division de 2011^{2012} par 7 est égal à 4.

Autre exemple : Reste de 2023^{2024} par 9.

On va travailler Modulo 9.

1ère étape. $2023 \equiv 7\ [9]$ car $2023 = 224 \times 9 + 7$

donc $2023^{2024} \equiv 7^{2024}\ [9]$

2e étape. On cherche n tel que $7^n \equiv 1\ [9]$

On a : $7^3 \equiv 343 \equiv 1\ [9]$.

car $343 = 38 \times 9 + 1$

3e étape. $2024 = 3 \times 674 + 2$

$2023^{2024} \equiv 7^{2024} \equiv 7^{3\times674+2} \equiv (7^3)^{674} \times 7^2\ [9]$

$2023^{2024} \equiv 1^{674} \times 49 \equiv 49 \equiv 4\ [9]$

Rappels $a^{n+m} = a^n \times a^m$

$a^{n\times m} = (a^n)^m$

Autre exemple : 2004^{1984} modulo 11 ?

$2004 \equiv 2\ [11]$

$2004^{1984} \equiv 2^{1984}\ [11]$

De plus $2^{10} \equiv 1\ [11]$

A terminer pour le 9 janvier