

# Ch 3 : Arithmétique modulaire

$$349 = 349 * 1$$

Les nombres premiers sont des nombres qui ne peuvent être divisé entièrement que par eux même et par 1. Par exemple 349 ne peut être divisé entièrement que par 349 et 1. Soit la seule factorisation possible de  $p$  est  $p = 1 * p$ . Exemples: 2, 3, 5, 7, 11, 13, 17, ...

$$1875 = 3 * 5 * 5 * 5 * 5$$

N'importe quel nombre peut être factorisé en nombres premiers. Et il y a une infinité de nombres premiers.

## Tester si un nombre est premier en utilisant un algorithme basique

```
def is_prime(n):  
    for i in range(2,n):  
        if (n%i) == 0:  
            return False  
    return True
```

Pour tester si un nombre est premier, on peut tester la division de tous les nombres jusqu'à  $\sqrt{n}$ . Ce qui est peu efficace car on va aussi tester des nombres non premiers.

## Tester si un nombre est premier en utilisant le crible d'Eratosthène

Pour calculer tous les nombres premiers  $\leq n$ .

1. Lister les entiers de 2 à  $n$
2. Pour chaque nombre plus petit que  $\sqrt{n}$  barrer tous les multiples du nombre (mais pas le nombre en lui même).

3. Tous les nombres qui restent sont des nombres premiers

# Décomposer un nombre en produits de facteurs premiers

1. On divise le nombre successivement par des nombres premiers de plus en plus grand jusqu'à arriver à \$1\$. Dans cet exemple, on va factoriser le nombre \$4410\$.

$$4410 / 2 / 3 / 3 / 5 / 7 / 7 = 1$$

2. Donc On arrive avec les valeurs suivantes

$$4410 = 2 * 3 * 3 * 5 * 7 * 7$$

3. Qui peut donc être simplifié de la manière suivante

$$4410 = 2 * 3^2 * 5 * 7^2$$

---

Revision #1

Created 27 April 2023 06:28:54 by SnowCode

Updated 24 May 2023 13:07:21 by SnowCode