

Laboratoire 30

• Buts

- Intégrer une fonction de génération de nombres aléatoires premiers à la classe `Uint`

• Travail à réaliser

- Programmer une fonction `division_reste` qui retourne le quotient et le reste de la division de deux `Uint`
- Commencer par programmer une fonction permettant de diviser un `Uint` par 2, pour mettre facilement en œuvre l'algorithme ci-après.
- Intégrer les opérateurs de division et de reste de la division entière dans la classe `Uint`.
- Tester le bon fonctionnement de la classe en générant des nombres aléatoires comportant un nombre de chiffres spécifié par l'utilisateur et en vérifiant s'ils sont probablement premiers, au moyen de l'algorithme programmé au labo 16.

• Délai

- Fin 2021

Input: $dividende \in \mathbb{N}$, $diviseur \in \mathbb{N}_0$

Output: $quotient, reste < diviseur \mid dividende = quotient \cdot diviseur + reste$

```

1 begin
2   puissance2  $\leftarrow$  1
3   b  $\leftarrow$  diviseur
4   while b  $\leq$  dividende do
5     | puissance2  $\leftarrow$  2  $\cdot$  puissance2
6     | b  $\leftarrow$  2  $\cdot$  b
7   end
8   quotient  $\leftarrow$  0
9   reste  $\leftarrow$  dividende
10  while reste  $\geq$  diviseur do
11    | b  $\leftarrow$  b/2
12    | puissance2  $\leftarrow$  puissance2/2
13    if reste  $\geq$  b then
14      | quotient  $\leftarrow$  quotient + puissance2
15      | reste  $\leftarrow$  reste - b
16  end
17 end
18 return quotient, reste

```