Comment calculer les puissances d’un nombre ?

Christophe.Troestler@umh.ac.be
http://www.umh.ac.be/math/an/

1. Première idée

$$x^0 = 1$$
$$x^1 = x$$
$$x^2 = x \cdot x$$
$$x^3 = x^2 \cdot x = x \cdot x \cdot x$$
$$x^4 = x^3 \cdot x = x \cdot x \cdot x \cdot x$$
$$\vdots$$
$$x^n = x^{n-1} \cdot x = \underbrace{x \cdot x \cdot x \cdots x}_{n \text{ fois}}$$

Donc, pour calculer, disons, x^5, on va « accumuler » des produits de x en nombre suffisant :

$$x \cdot x \cdot x \cdot x \cdot x$$

1. Première idée

$$x^0 = 1$$
$$x^1 = x$$
$$x^2 = x \cdot x$$
$$x^3 = x^2 \cdot x = x \cdot x \cdot x$$
$$x^4 = x^3 \cdot x = x \cdot x \cdot x \cdot x$$
$$\vdots$$
$$x^n = x^{n-1} \cdot x = \underbrace{x \cdot x \cdot x \cdots x}_{n \text{ fois}}$$

Donc, pour calculer, disons, x^5, on va « accumuler » des produits de x en nombre suffisant :

$$\underbrace{x}_{R} \cdot x \cdot x \cdot x \cdot x$$

1. Première idée

$$x^0 = 1$$
$$x^1 = x$$
$$x^2 = x \cdot x$$
$$x^3 = x^2 \cdot x = x \cdot x \cdot x$$
$$x^4 = x^3 \cdot x = x \cdot x \cdot x \cdot x$$
$$\vdots$$
$$x^n = x^{n-1} \cdot x = \underbrace{x \cdot x \cdot x \cdots x}_{n \text{ fois}}$$

Donc, pour calculer, disons, x^5, on va « accumuler » des produits de x en nombre suffisant :

$$\underbrace{x \cdot x}_{R} \cdot x \cdot x \cdot x$$

1. Première idée

$$
\begin{aligned}
x^0 &= 1\\
x^1 &= x\\
x^2 &= x \cdot x\\
x^3 &= x^2 \cdot x = x \cdot x \cdot x\\
x^4 &= x^3 \cdot x = x \cdot x \cdot x \cdot x\\
&\vdots\\
x^n &= x^{n-1} \cdot x = \underbrace{x \cdot x \cdot x \cdots x}_{n \text{ fois}}
\end{aligned}
$$

Donc, pour calculer, disons, x^5, on va « accumuler » des produits de x en nombre suffisant :

$$\underbrace{x \cdot x \cdot x}_{R} \cdot x \cdot x$$

1. Première idée

$$
\begin{aligned}
x^0 &= 1\\
x^1 &= x\\
x^2 &= x\cdot x\\
x^3 &= x^2\cdot x = x\cdot x\cdot x\\
x^4 &= x^3\cdot x = x\cdot x\cdot x\cdot x\\
&\vdots\\
x^n &= x^{n-1}\cdot x = \underbrace{x\cdot x\cdot x\cdots x}_{n \text{ fois}}
\end{aligned}
$$

Donc, pour calculer, disons, x^5, on va « accumuler » des produits de x en nombre suffisant :

$$\underbrace{x\cdot x\cdot x\cdot x}_{R}\cdot x$$

1. Première idée

$$
\begin{aligned}
x^0 &= 1 \\
x^1 &= x \\
x^2 &= x \cdot x \\
x^3 &= x^2 \cdot x = x \cdot x \cdot x \\
x^4 &= x^3 \cdot x = x \cdot x \cdot x \cdot x \\
&\vdots \\
x^n &= x^{n-1} \cdot x = \underbrace{x \cdot x \cdot x \cdots x}_{n \text{ fois}}
\end{aligned}
$$

Donc, pour calculer, disons, x^5, on va « accumuler » des produits de x en nombre suffisant :

$$\underbrace{x \cdot x \cdot x \cdot x \cdot x}_{R}$$

1. Première idée

$$
\begin{aligned}
x^0 &= 1\\
x^1 &= x\\
x^2 &= x \cdot x\\
x^3 &= x^2 \cdot x = x \cdot x \cdot x\\
x^4 &= x^3 \cdot x = x \cdot x \cdot x \cdot x\\
&\vdots\\
x^n &= x^{n-1} \cdot x = \underbrace{x \cdot x \cdot x \cdots x}_{n \text{ fois}}
\end{aligned}
$$

Donc, pour calculer, disons, x^5, on va « accumuler » des produits de x en nombre suffisant :

$$\underbrace{x \cdot x \cdot x \cdot x \cdot x}_{R}$$

Écrivez un programme qui utilise cette idée pour calculer

$$(x, n) \mapsto x^n.$$

Prouvez que votre programme est correct.

Le programme a comme données $x \in \mathbb{R}$ et $n \in \mathbb{N}$:

$$\text{puiss}_1(x, n) : \begin{cases} R \leftarrow 1 \\ \langle R = 1 = x^0 \rangle \\ \text{Pour } i = 1, \ldots, n \text{ faire} \\ \qquad R \leftarrow R \cdot x \\ \qquad \langle R = x^i \rangle \\ \langle R = x^n \rangle \end{cases}$$

Remarquez que ce programme marche si $n = 0$.

2. Deuxième idée

Plutôt que de multiplier x trois fois pour avoir x^4, on peut aller plus vite en remarquant que $x^4 = (x^2)^2$ ce qui donne deux multiplications (une pour $x^2 = x \cdot x$, une pour $(x^2)^2 = x^2 \cdot x^2$). Essayons d'exploiter cette idée de manière générale :

$$
\begin{array}{ll}
 & x^9 = x^8 \cdot x \\
x^2 = x \cdot x & x^{10} = x^8 \cdot x^2 \\
x^3 = x^2 \cdot x & x^{11} = x^8 \cdot x^2 \cdot x \\
x^4 = (x^2)^2 & x^{12} = x^8 \cdot x^4 \\
x^5 = x^4 \cdot x & x^{13} = x^8 \cdot x^4 \cdot x \\
x^6 = x^4 \cdot x^2 & x^{14} = x^8 \cdot x^4 \cdot x^2 \\
x^7 = x^4 \cdot x^2 \cdot x & x^{15} = x^8 \cdot x^4 \cdot x^2 \cdot x \\
x^8 = (x^4)^2 & x^{16} = (x^8)^2
\end{array}
$$

Quelle est la relation : exposant $\leftrightarrow$ décomposition ?

n	$((x^2)^2)^2$	$(x^2)^2$	x^2	x^1	2^3	2^2	2	1
3			1	1			2	$+\,1$
4		1				2^2		
5		1		1		2^2		
6		1	1			2^2	$+\,2$	
7		1	1	1		2^2	$+\,2$	$+\,1$
8	1				2^3			
9	1			1	2^3			$+\,1$

n	$((x^2)^2)^2$	$(x^2)^2$	x^2	x^1	2^3	2^2	2	1
3			1	1			$2 +$	1
4		1	0	0		$2^2 +$	$0 +$	0
5		1	0	1		$2^2 +$	$0 +$	0
6		1	1	0		$2^2 +$	$2 +$	0
7		1	1	1		$2^2 +$	$2 +$	1
8	1	0	0	0	$2^3 +$	$0 +$	$0 +$	0
9	1	0	0	1	$2^3 +$	$0 +$	$0 +$	1

Cette table résulte du fait général :

$$x^n = x^{a_3 2^3 + a_2 2^2 + a_1 2 + a_0} = \left((x^4)^2\right)^{a_3} \cdot \left((x^2)^2\right)^{a_2} \cdot (x^2)^{a_1} \cdot x^{a_0}$$

Voyez-vous pourquoi ? Comment trouver les a_i à partir de n ?

2.1. Écriture binaire des nombres

Réponse à la question précédente :

$$n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$$

où $a_i \in \{0, 1\}$ pour tout $i = 0, 1, \ldots, p$. Le terme x^{2^i} apparaît dans x^n si et seulement si $a_i = 1$. Une telle décomposition existe-t-elle toujours ? Est-elle unique ?
Regardons a_0. Essayez pour $n = 4$, $n = 5$, $n = 6$ et $n = 7$...

2.1. Écriture binaire des nombres

Réponse à la question précédente :

$$n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$$

où $a_i \in \{0, 1\}$ pour tout $i = 0, 1, \ldots, p$. Le terme x^{2^i} apparaît dans x^n si et seulement si $a_i = 1$. Une telle décomposition existe-t-elle toujours ? Est-elle unique ?
Regardons a_0. Puisque

$$n = (a_p 2^{p-1} + \cdots + a_2 2 + a_1) 2 + a_0,$$

on a : $a_0 = 0$ si n est pair et $a_0 = 1$ si n est impair. Autrement dit :

$$\mathbf{a_0 = n \bmod 2}.$$

Qu'en est-il pour a_1 ?

2.1. Écriture binaire des nombres

Réponse à la question précédente :

$$n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$$

où $a_i \in \{0, 1\}$ pour tout $i = 0, 1, \ldots, p$. Le terme x^{2^i} apparaît dans x^n si et seulement si $a_i = 1$. Une telle décomposition existe-t-elle toujours ? Est-elle unique ?
Regardons a_0. Puisque

$$n = (a_p 2^{p-1} + \cdots + a_2 2 + a_1) 2 + a_0,$$

on a : $a_0 = 0$ si n est pair et $a_0 = 1$ si n est impair. Autrement dit :

$$\mathbf{a_0 = n \bmod 2}.$$

Comme $a_p 2^{p-1} + \cdots + a_2 2 + a_1 = n \operatorname{div} 2$, on a

$$\mathbf{a_1 = (n \operatorname{div} 2) \bmod 2}.$$

EXEMPLE : $11 = n = \cdots + a_3 2^3 + a_2 2^2 + a_1 2 + a_0$ pour quels a_i ?.

$$a_0 = n \bmod 2 = 11 \bmod 2 = 1 \qquad \Rightarrow a_0 = 1$$
$$n_0 := \cdots + a_3 2^2 + a_2 2^2 + a_1 = n \operatorname{div} 2 = 11 \operatorname{div} 2 = 5$$

EXEMPLE : $11 = n = \cdots + a_3 2^3 + a_2 2^2 + a_1 2 + a_0$ pour quels a_i ?.

$$a_0 = n \bmod 2 = 11 \bmod 2 = 1 \qquad \Rightarrow a_0 = 1$$
$$n_0 := \cdots + a_3 2^2 + a_2 2^2 + a_1 = n \operatorname{div} 2 = 11 \operatorname{div} 2 = 5$$

$$a_1 = n_0 \bmod 2 = 5 \bmod 2 = 1 \qquad \Rightarrow a_1 = 1$$
$$n_1 := \cdots + a_3 2 + a_2 2 = n_0 \operatorname{div} 2 = 5 \operatorname{div} 2 = 2$$

EXEMPLE : $11 = n = \cdots + a_3 2^3 + a_2 2^2 + a_1 2 + a_0$ pour quels a_i ?.

$$a_0 = n \bmod 2 = 11 \bmod 2 = 1 \qquad \Rightarrow a_0 = 1$$
$$n_0 := \cdots + a_3 2^2 + a_2 2^2 + a_1 = n \operatorname{div} 2 = 11 \operatorname{div} 2 = 5$$

$$a_1 = n_0 \bmod 2 = 5 \bmod 2 = 1 \qquad \Rightarrow a_1 = 1$$
$$n_1 := \cdots + a_3 2 + a_2 2 = n_0 \operatorname{div} 2 = 5 \operatorname{div} 2 = 2$$

$$a_2 = n_1 \bmod 2 = 2 \bmod 2 = 0 \qquad \Rightarrow a_2 = 0$$
$$n_2 := \cdots + a_3 2 + a_2 = n_1 \operatorname{div} 2 = 2 \operatorname{div} 2 = 1$$

EXEMPLE : $11 = n = \cdots + a_3 2^3 + a_2 2^2 + a_1 2 + a_0$ pour quels a_i ?.

$$a_0 = n \bmod 2 = 11 \bmod 2 = 1 \qquad \Rightarrow a_0 = 1$$
$$n_0 := \cdots + a_3 2^2 + a_2 2^2 + a_1 = n \operatorname{div} 2 = 11 \operatorname{div} 2 = 5$$

$$a_1 = n_0 \bmod 2 = 5 \bmod 2 = 1 \qquad \Rightarrow a_1 = 1$$
$$n_1 := \cdots + a_3 2 + a_2 2 = n_0 \operatorname{div} 2 = 5 \operatorname{div} 2 = 2$$

$$a_2 = n_1 \bmod 2 = 2 \bmod 2 = 0 \qquad \Rightarrow a_2 = 0$$
$$n_2 := \cdots + a_3 2 + a_2 = n_1 \operatorname{div} 2 = 2 \operatorname{div} 2 = 1$$

$$a_3 = n_2 \bmod 2 = 1 \bmod 2 = 1 \qquad \Rightarrow a_3 = 1$$
$$n_3 := \cdots + a_3 = n_2 \operatorname{div} 2 = 2 \operatorname{div} 2 = 0$$

En conclusion $11 = \mathbf{1} \cdot 2^3 + \mathbf{0} \cdot 2^4 + \mathbf{1} \cdot 2^1 + \mathbf{1} \cdot 2^0$. On appelle **1011** l'écriture binaire de 11.

EXEMPLE : $11 = n = \cdots + a_3 2^3 + a_2 2^2 + a_1 2 + a_0$ pour quels a_i ?.

$$a_0 = n \bmod 2 = 11 \bmod 2 = 1 \qquad \Rightarrow a_0 = 1$$
$$n_0 := \cdots + a_3 2^2 + a_2 2^2 + a_1 = n \operatorname{div} 2 = 11 \operatorname{div} 2 = 5$$

$$a_1 = n_0 \bmod 2 = 5 \bmod 2 = 1 \qquad \Rightarrow a_1 = 1$$
$$n_1 := \cdots + a_3 2 + a_2 2 = n_0 \operatorname{div} 2 = 5 \operatorname{div} 2 = 2$$

$$a_2 = n_1 \bmod 2 = 2 \bmod 2 = 0 \qquad \Rightarrow a_2 = 0$$
$$n_2 := \cdots + a_3 2 + a_2 = n_1 \operatorname{div} 2 = 2 \operatorname{div} 2 = 1$$

$$a_3 = n_2 \bmod 2 = 1 \bmod 2 = 1 \qquad \Rightarrow a_3 = 1$$
$$n_3 := \cdots + a_3 = n_2 \operatorname{div} 2 = 2 \operatorname{div} 2 = 0$$

En conclusion $11 = \mathbf{1} \cdot 2^3 + \mathbf{0} \cdot 2^4 + \mathbf{1} \cdot 2^1 + \mathbf{1} \cdot 2^0$. On appelle **1011** l'écriture binaire de 11.
Pouvez-vous généraliser ce procédé en écrivant un algorithme de calcul des a_i ?

Soit $n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$.

Mathématique	Algorithmique
	$N \leftarrow n$

$$N = \overset{1}{\boxed{n}}$$

$$a_0 =$$

$$a_1 =$$

$$a_2 =$$

$$\vdots$$

Soit $n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$.

Mathématique	Algorithmique
	$N \leftarrow n$
$a_0 = n \bmod 2$	$a_0 \leftarrow N \bmod 2$

$$
\begin{array}{lcc}
 & 1 & 2 \\
N = & \boxed{n} & \\
a_0 = & & \boxed{n \bmod 2} \\
a_1 = & & \\
a_2 = & & \\
\vdots & &
\end{array}
$$

Soit $n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$.

Mathématique	Algorithmique
	$N \leftarrow n$
$a_0 = n \bmod 2$	$a_0 \leftarrow N \bmod 2$
$n_0 = n \operatorname{div} 2$	$N \leftarrow N \operatorname{div} 2$

	1	2	3
$N =$	$\boxed{n}$		$\boxed{n_0}$
$a_0 =$		$\boxed{n \bmod 2}$	
$a_1 =$			
$a_2 =$			
$\vdots$			

Soit $n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$.

Mathématique	Algorithmique
	$N \leftarrow n$
$a_0 = n \bmod 2$	$a_0 \leftarrow N \bmod 2$
$n_0 = n \operatorname{div} 2$	$N \leftarrow N \operatorname{div} 2$
$a_1 = n_0 \bmod 2$	$a_1 \leftarrow N \bmod 2$

	1	2	3	4
$N =$	$\boxed{n}$		$\boxed{n_0}$	
$a_0 =$		$\boxed{n \bmod 2}$		
$a_1 =$				$\boxed{n_0 \bmod 2}$
$a_2 =$				
$\vdots$				

Soit $n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$.

Mathématique	Algorithmique
	$N \leftarrow n$
$a_0 = n \bmod 2$	$a_0 \leftarrow N \bmod 2$
$n_0 = n \operatorname{div} 2$	$N \leftarrow N \operatorname{div} 2$
$a_1 = n_0 \bmod 2$	$a_1 \leftarrow N \bmod 2$
$n_1 = n_0 \operatorname{div} 2$	$N \leftarrow N \operatorname{div} 2$

	1	2	3	4	5
$N =$	$\boxed{n}$		$\boxed{n_0}$		$\boxed{n_1}$
$a_0 =$		$\boxed{n \bmod 2}$			
$a_1 =$				$\boxed{n_0 \bmod 2}$	
$a_2 =$					
$\vdots$					

Soit $n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$.

Mathématique	Algorithmique
	$N \leftarrow n$
$a_0 = n \bmod 2$	$a_0 \leftarrow N \bmod 2$
$n_0 = n \operatorname{div} 2$	$N \leftarrow N \operatorname{div} 2$
$a_1 = n_0 \bmod 2$	$a_1 \leftarrow N \bmod 2$
$n_1 = n_0 \operatorname{div} 2$	$N \leftarrow N \operatorname{div} 2$
$a_2 = n_1 \bmod 2$	$a_2 \leftarrow N \bmod 2$

	1	2	3	4	5	6
$N =$	$\boxed{n}$		$\boxed{n_0}$		$\boxed{n_1}$	
$a_0 =$		$\boxed{n \bmod 2}$				
$a_1 =$				$\boxed{n_0 \bmod 2}$		
$a_2 =$						$\boxed{n_1 \bmod 2}$
$\vdots$						

Soit $n = a_p 2^p + a_{p-1} 2^{p-1} + \cdots + a_2 2^2 + a_2 2 + a_0$.

Mathématique	Algorithmique
	$N \leftarrow n$
$a_0 = n \bmod 2$	$a_0 \leftarrow N \bmod 2$
$n_0 = n \operatorname{div} 2$	$N \leftarrow N \operatorname{div} 2$
$a_1 = n_0 \bmod 2$	$a_1 \leftarrow N \bmod 2$
$n_1 = n_0 \operatorname{div} 2$	$N \leftarrow N \operatorname{div} 2$
$a_2 = n_1 \bmod 2$	$a_2 \leftarrow N \bmod 2$
$n_2 = n_1 \operatorname{div} 2$	$N \leftarrow N \operatorname{div} 2$
$\vdots$	$\vdots$

	1	2	3	4	5	6	7	
$N =$	$\boxed{n}$		$\boxed{n_0}$		$\boxed{n_1}$		$\boxed{n_2}$	$\cdots$
$a_0 =$		$\boxed{n \bmod 2}$						
$a_1 =$				$\boxed{n_0 \bmod 2}$				
$a_2 =$						$\boxed{n_1 \bmod 2}$		
$\vdots$								

☞ Réécrivez le tableau précédent à l’aide d’une boucle. Quel est le test qui décide de l’arrêt de la boucle ?

☞ Réécrivez le tableau précédent à l'aide d'une boucle. Quel est le test qui décide de l'arrêt de la boucle ?

Un programme de calcul des digits binaires a_i d'un entier $n \in \mathbb{N}$ est :

$$\text{digits}(n) : \begin{cases} N \leftarrow n;\ i \leftarrow 0 \\ \text{Tant que } N > 0 \text{ faire} \\ \qquad \begin{cases} a_i \leftarrow N \bmod 2 \\ N \leftarrow N \operatorname{div} 2 \\ i \leftarrow i + 1 \end{cases} \\ \langle \text{si } i = 0, \text{ c'est que } n = 0 \,; \text{ sinon, } n = \sum_{0 \leqslant j < i} a_j 2^j \rangle \end{cases}$$

☞ Réécrivez le tableau précédent à l'aide d'une boucle. Quel est le test qui décide de l'arrêt de la boucle ?

Un programme de calcul des digits binaires a_i d'un entier $n \in \mathbb{N}$ est :

$$\text{digits}(n) : \begin{cases} N \leftarrow n;\ i \leftarrow 0 \\ \text{Tant que } N > 0 \text{ faire} \\ \qquad \begin{cases} a_i \leftarrow N \bmod 2 \\ N \leftarrow N \operatorname{div} 2 \\ i \leftarrow i+1 \end{cases} \\ \left\langle \text{si } i = 0\text{, c'est que } n = 0\,;\ \text{sinon, } n = \sum_{0 \leqslant j < i} a_j 2^j \right\rangle \end{cases}$$

REMARQUE : L'algorithme ci-dessus montre que les a_i existent toujours. La manière dont on a déduit l'algorithme montre que les a_i sont uniques. On appelle $a_p a_{p-1} \ldots a_2 a_1 a_0$ l'*écriture binaire* de n.

2.2. Revenons au calcul de x^n...

Repartons de :

$$x^n = x^{a_3 2^3 + a_2 2^2 + a_1 2 + a_0} = \left((x^4)^2\right)^{a_3} \cdot \left((x^2)^2\right)^{a_2} \cdot (x^2)^{a_1} \cdot x^{a_0}$$

Il y a deux ingrédients :
– les puissances de x : x, x^2, $x^4 = (x^2)^2$, $x^8 = (x^4)^2$,... ;
– le terme x^{2^i} est présent dans le produit de x^n ssi $a_i = 1$.
Comment construire x^n à partir des remarques ci-dessus en « accumulant » le nécessaire dans une variable R initialisée à 1 ?

2.2. Revenons au calcul de x^n...

Repartons de :

$$x^n = x^{a_3 2^3 + a_2 2^2 + a_1 2 + a_0} = \left((x^4)^2\right)^{a_3} \cdot \left((x^2)^2\right)^{a_2} \cdot (x^2)^{a_1} \cdot x^{a_0}$$

Il y a deux ingrédients :
– les puissances de x : x, x^2, $x^4 = (x^2)^2$, $x^8 = (x^4)^2$,... ;
– le terme x^{2^i} est présent dans le produit de x^n ssi $a_i = 1$.
On peut voir le calcul de x^n comme suit :

$R \leftarrow 1$	
Si $a_0 = 1$ alors $R \leftarrow R \cdot x$	$R = x^{a_0}$
Si $a_1 = 1$ alors $R \leftarrow R \cdot x^2$	$R = (x^2)^{a_1} x^{a_0} = x^{a_1 2 + a_0}$
Si $a_2 = 1$ alors $R \leftarrow R \cdot x^4$	$R = (x^4)^{a_2} (x^2)^{a_1} x^{a_0} = x^{a_2 2^2 + a_1 2 + a_0}$
$\vdots$	$\vdots$

Comment calculer x^2, x^4,... ?

Algorithme	Contenu des variables
$R \leftarrow 1$	

1

$X =$

$R = \boxed{1}$

Algorithme	Contenu des variables
$R \leftarrow 1$	
$X \leftarrow x$	$X = x$

	1	2
$X =$		$\boxed{x}$
$R =$	$\boxed{1}$	

Algorithme	Contenu des variables
$R \leftarrow 1$	
$X \leftarrow x$	$X = x$
Si $a_0 = 1$ alors $R \leftarrow R \cdot X$	$R = x^{a_0}$

	1	2	3
$X =$		$\boxed{x}$	
$R =$	$\boxed{1}$		$\boxed{x^{a_0}}$

Algorithme	Contenu des variables
$R \leftarrow 1$	
$X \leftarrow x$	$X = x$
Si $a_0 = 1$ alors $R \leftarrow R \cdot X$	$R = x^{a_0}$
$X \leftarrow X \cdot X$	$X = x^2$

	1	2	3	4
$X =$		$\boxed{x}$		$\boxed{x^2}$
$R =$	$\boxed{1}$		$\boxed{x^{a_0}}$	

Algorithme	Contenu des variables
$R \leftarrow 1$	
$X \leftarrow x$	$X = x$
Si $a_0 = 1$ alors $R \leftarrow R \cdot X$	$R = x^{a_0}$
$X \leftarrow X \cdot X$	$X = x^2$
Si $a_1 = 1$ alors $R \leftarrow R \cdot X$	$R = (x^2)^{a_1} x^{a_0} = x^{a_1 2 + a_0}$

	1	2	3	4	5
$X =$		$\boxed{x}$		$\boxed{x^2}$	
$R =$	$\boxed{1}$		$\boxed{x^{a_0}}$		$\boxed{x^{a_1 2 + a_0}}$

Algorithme	Contenu des variables
$R \leftarrow 1$	
$X \leftarrow x$	$X = x$
Si $a_0 = 1$ alors $R \leftarrow R \cdot X$	$R = x^{a_0}$
$X \leftarrow X \cdot X$	$X = x^2$
Si $a_1 = 1$ alors $R \leftarrow R \cdot X$	$R = (x^2)^{a_1} x^{a_0} = x^{a_1 2 + a_0}$
$X \leftarrow X \cdot X$	$X = x^4$

	1	2	3	4	5	6
$X =$		$\boxed{x}$		$\boxed{x^2}$		$\boxed{x^4}$
$R =$	$\boxed{1}$		$\boxed{x^{a_0}}$		$\boxed{x^{a_1 2 + a_0}}$	

Algorithme	Contenu des variables
$R \leftarrow 1$	
$X \leftarrow x$	$X = x$
Si $a_0 = 1$ alors $R \leftarrow R \cdot X$	$R = x^{a_0}$
$X \leftarrow X \cdot X$	$X = x^2$
Si $a_1 = 1$ alors $R \leftarrow R \cdot X$	$R = (x^2)^{a_1} x^{a_0} = x^{a_1 2 + a_0}$
$X \leftarrow X \cdot X$	$X = x^4$
Si $a_2 = 1$ alors $R \leftarrow R \cdot X$	$R = (x^4)^{a_2}(x^2)^{a_1} x^{a_0} = x^{a_2 2^2 + a_1 2 + a_0}$
$\vdots$	$\vdots$

	1	2	3	4	5	6	7	
$X =$		$\boxed{x}$		$\boxed{x^2}$		$\boxed{x^4}$		$\dots$
$R =$	$\boxed{1}$		$\boxed{x^{a_0}}$		$\boxed{x^{a_1 2 + a_0}}$		$\boxed{x^{a_2 2^2 + a_1 2 + a_0}}$	

☞ Écrivez cet algorithme à l'aide d'une boucle.

En conclusion, en supposant qu'on ai calculé l'expansion binaire $a_p \dots a_1 a_0$ de n, on trouve le programme :

$$\text{puiss}_3(x,n) : \begin{cases} R \leftarrow 1;\ X \leftarrow x \\ \text{Pour tout } i = 0, \dots, p \text{ faire} \\ \quad \begin{cases} \text{Si } a_i = 1 \text{ alors } R \leftarrow R \cdot X \\ X \leftarrow X \cdot X \end{cases} \\ \langle \text{On pense que } R = x^n \rangle \end{cases}$$

Comment éviter de calculer *préalablement* l'expansion binaire $a_p \dots a_1 a_0$ de n ?

En conclusion, en supposant qu'on ai calculé l'expansion binaire $a_p \dots a_1 a_0$ de n, on trouve le programme :

$$\text{puiss}_3(x, n) : \begin{cases} R \leftarrow 1;\ X \leftarrow x \\ \text{Pour tout } i = 0, \dots, p \text{ faire} \\ \quad \begin{cases} \text{Si } a_i = 1 \text{ alors } R \leftarrow R \cdot X \\ X \leftarrow X \cdot X \end{cases} \\ \langle \text{On pense que } R = x^n \rangle \end{cases}$$

Comment éviter de calculer *préalablement* l'expansion binaire $a_p \dots a_1 a_0$ de n ? Notons qu'à une étape donnée, on n'a besoin que d'*un* a_i... Comparons le programme de calcul de de x^n et celui de calcul des a_i.

Calcul de x^n	Calcul des a_i
$R \leftarrow 1;\ X \leftarrow x$ Pour tout $i = 0, \ldots, p$ faire $\begin{cases} \text{Si } a_i = 1 \text{ alors } R \leftarrow R \cdot X \\ X \leftarrow X \cdot X \end{cases}$	$N \leftarrow n;\ i \leftarrow 0$ Tant que $N > 0$ faire $\begin{cases} a_i \leftarrow N \bmod 2 \\ N \leftarrow N \operatorname{div} 2 \\ i \leftarrow i + 1 \end{cases}$

De ceci, quelles remarques peut-on faire, en particulier au sujet
– des a_i, et en particulier de l'indice i ?
– du critère de terminaison de la boucle ?

Calcul de x^n	Calcul des a_i
$R \leftarrow 1;\ X \leftarrow x$ Pour tout $i = 0, \ldots, p$ faire $\left\{ \begin{array}{l} \text{Si } a_i = 1 \text{ alors } R \leftarrow R \cdot X \\ X \leftarrow X \cdot X \end{array} \right.$	$N \leftarrow n;\ i \leftarrow 0$ Tant que $N > 0$ faire $\left\{ \begin{array}{l} a_i \leftarrow N \bmod 2 \\ N \leftarrow N \operatorname{div} 2 \\ i \leftarrow i + 1 \end{array} \right.$

De ceci, on peut conclure que :

– Le a_i du programme de droite est celui nécessaire dans le programme de gauche. Il faut donc « synchroniser » les deux boucles ;

– On n'a besoin que d'un a_i à la fois (donc on peut utiliser une variable non indicée, disons A) et on n'a pas besoin de l'indice i ;

– Si les boucles sont synchronisées, i variera de 0 à p tant que $N > 0$, p étant atteint lorsque $N = 0$. Comme on n'a pas besoin de i, le critère qui nous intéresse est « $N > 0$ ».

☞ Écrivez un algorithme qui « fond » ces deux programmes en un seul. Simplifiez le autant que possible.

Le programme correspondant est :

$$\text{puiss}_4(x,n) : \begin{cases} R \leftarrow 1;\ X \leftarrow x;\ N \leftarrow n \\ \text{Tant que } N > 0 \text{ faire} \\ \quad \begin{cases} \text{Si } N \text{ impair, } R \leftarrow R \cdot X \\ N \leftarrow N \operatorname{div} 2 \\ X \leftarrow X \cdot X \end{cases} \\ \langle \text{A-t-on bien } R = x^n\,? \rangle \end{cases}$$

Les questions suivantes sont cruciales :

– Cet algorithme se termine-t-il pour n'importe quelles données $x \in \mathbb{R}$ et $n \in \mathbb{N}$?
– Ce programme est-il correct ?
– puiss_4 est-il vraiment plus rapide que le procédé « naïf » ? Si oui, dans quelle mesure — peut-on le quantifier ?

2.3. Terminaison

$$\mathrm{puiss}_4(x, n) : \begin{cases} R \leftarrow 1;\ X \leftarrow x;\ N \leftarrow n \\ \text{Tant que } \mathbf{N} > \mathbf{0} \text{ faire} \\ \quad \begin{cases} \text{Si } N \text{ impair, } R \leftarrow R \cdot X \\ \mathbf{N} \leftarrow \mathbf{N}\,\mathrm{div}\,\mathbf{2} \\ X \leftarrow X \cdot X \end{cases} \\ \langle \text{Le résultat est dans } R \rangle \end{cases}$$

À chaque tour de boucle, la valeur de N est divisée par 2. Les valeurs de N forment donc une suite strictement décroissante de naturels. Forcément, il arrivera un moment où $N = 0$ et la boucle s'arrêtera.

2.4. Invariant de boucle

$$\text{puiss}_4(x,n) : \begin{cases} R \leftarrow 1;\ X \leftarrow x;\ N \leftarrow n \\ \left\langle \mathbf{x^n = X^N R} \right\rangle \\ \text{Tant que } N > 0 \text{ faire} \\ \quad \begin{cases} \text{Si } N \text{ impair, } R \leftarrow R \cdot X \\ N \leftarrow N \operatorname{div} 2 \\ X \leftarrow X \cdot X \\ \left\langle \mathbf{x^n = X^N R} \right\rangle \end{cases} \\ \left\langle \begin{array}{l} N = 0 \text{ (fin de boucle),} \\ \text{donc } R = x^n \end{array} \right\rangle \end{cases}$$

2.5. Complexité

En comparant puiss_4 avec puiss_3, on voit que, si $n = (a_p \ldots a_1 a_0)_2$, on a

$$\text{puiss}_4(x, n) : \begin{cases} R \leftarrow 1;\ X \leftarrow x;\ N \leftarrow n;\ \mathbf{i} \leftarrow \mathbf{0} \\ \text{Tant que } N > 0 \Leftrightarrow \mathbf{i} = \mathbf{0}, \ldots, \mathbf{p} \text{ faire} \\ \qquad \begin{cases} \text{Si } N \text{ impair} \Leftrightarrow \mathbf{a_i} = \mathbf{1},\ R \leftarrow R \cdot X \\ N \leftarrow N \operatorname{div} 2 \\ X \leftarrow X \cdot X \\ \mathbf{i} \leftarrow \mathbf{i} + \mathbf{1} \end{cases} \\ \langle \text{Le résultat est dans } R \rangle \end{cases}$$

Que peut-on en déduire sur le nombre d'opérations effectuées par puiss_4 ?

2.5. Complexité

En comparant puiss$_4$ avec puiss$_3$, on voit que, si $n = (a_p \dots a_1 a_0)_2$, on a

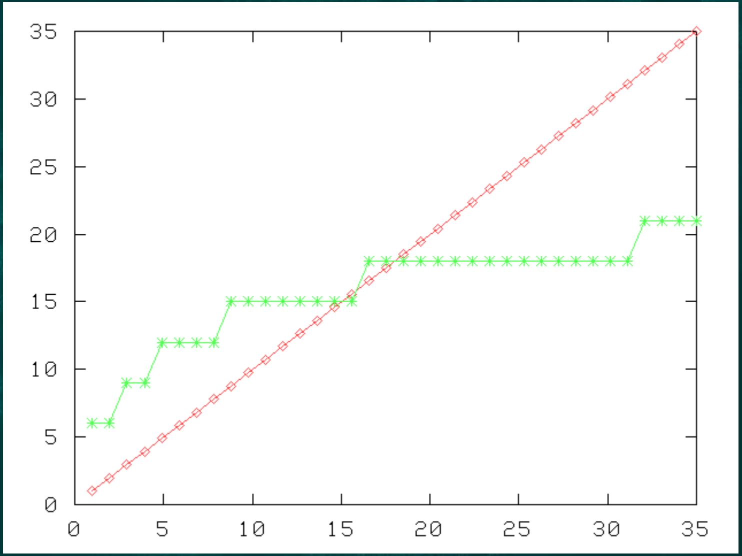
$$\text{puiss}_4(x,n) : \begin{cases} R \leftarrow 1;\ X \leftarrow x;\ N \leftarrow n;\ \mathbf{i} \leftarrow \mathbf{0} \\ \text{Tant que } N > 0 \Leftrightarrow \mathbf{i} = \mathbf{0}, \dots, \mathbf{p} \text{ faire} \\ \qquad \begin{cases} \text{Si } N \text{ impair } \Leftrightarrow \mathbf{a_i} = \mathbf{1},\ R \leftarrow R \cdot X \\ N \leftarrow N \operatorname{div} 2 \\ X \leftarrow X \cdot X \\ \mathbf{i} \leftarrow \mathbf{i} + \mathbf{1} \end{cases} \\ \langle \text{Le résultat est dans } R \rangle \end{cases}$$

– On fait $p+1$ tours de boucle et, à chaque tour, toujours 2 opérations, plus une troisième si $a_i = 1$. Le nombre total d'opérations est donc

$$3 + (p+1)2 + \sum_{i=0}^{p} a_i = 5 + 2p + \sum_{i=0}^{p} a_i \leqslant 6 + 3p$$

– $2^p \leqslant n < 2^{p+1} \Rightarrow p \leqslant \log_2 n < p+1 \Rightarrow p = \lfloor \log_2 n \rfloor$

En rouge, $n \mapsto n$
En vert, $n \mapsto 6 + 3\lfloor \log_2 n \rfloor$.



n	puiss$_1$ n	puiss$_4$ $6 + 3\lfloor \log_2 n \rfloor$
2	2	9
3	3	9
4	4	12
10	10	15
15	15	15
16	16	18
17	17	18
18	18	18
19	19	18
20	20	18
100	100	24
1000	1000	33
2^k	2^k	k