L'exponentielle modulaire rapide

Problème

On veut calculer $5^{13} \mod 187$. La calculatrice refuse.

Remarque

En fait, ça dépend des calculatrices !
Mais le problème est le même pour calculer $40^{384} \mod 187$
Et là, toutes les calculatrices refusent...

La cause du problème

- La raison de ce refus est que le résultat intermédiaire 5^{13} est trop grand pour être calculé exactement avec une calculatrice.
- On obtient seulement une valeur approchée en notation scientifique.
- Cependant, on sait à l'avance que le résultat final sera forcément inférieur à 187, puisqu'on calcule modulo 187.
- La méthode expliquée ci-dessous permet de ne pas passer par des résultats intermédiaires qui dépassent les capacités des calculatrices.
- En effet, tous les nombres qu'on sera amené à manipuler seront inférieurs à $187^2 = 34969$.

Rappels sur les exposants

Avant d'en venir à la solution du problème, on rappelle quelques propriétés utiles sur les exposants :

Propriétés

Quels que soient les entiers naturels a, b, c, on a :

1. $a^{(2^0)} = a$
2. $a^{(2^{b+1})} = (a^{(2^b)})^2$
3. *Attention :* $a^{(b^c)} \neq \left(a^b\right)^c$. *Par exemple* $5^{\left(2^3\right)} = 5^8$ *mais* $\left(5^2\right)^3 = 5^{2\times 3} = 5^6$.
4. $a^{(2^b+2^c)} = a^{(2^b)} \times a^{(2^c)}$

Application

Exemple

Quand on prend comme exposant les puissances de 2 successives, on obtient une suite d'élévations au carré :

$5^{(2^0)} = 5$
$5^{(2^1)} = 5^{(2^{0+1})} = (5^{(2^0)})^2 = 5^2 = 25$
$5^{(2^2)} = 5^{(2^{1+1})} = (5^{(2^1)})^2 = 25^2 = 625$
$5^{(2^3)} = 5^{(2^{2+1})} = (5^{(2^2)})^2 = 625^2 = 390625$
etc.

Exponentiation modulaire rapide

Solution 1/2

- On écrit l'exposant 13 en binaire, c.-à-d.

$$13_{dec} = 1101_{bin}$$

Autrement dit, on a $13 = 2^3 + 2^2 + 2^0$, donc :

$$5^{13} = 5^{(2^3+2^2+2^0)} = 5^{(2^3)} \times 5^{(2^2)} \times 5^{(2^0)}$$

- En passant au modulo, on a toujours :

$$5^{13} \equiv 5^{(2^3)} \times 5^{(2^2)} \times 5^{(2^0)} \mod 187$$

Il nous suffit donc de connaître $5^{(2^0)} \mod 187$, $5^{(2^2)} \mod 187$ et $5^{(2^3)} \mod 187$.

Exemple

- On veut calculer $174^{37} \mod 187$.
- On écrit l'exposant 37 en binaire, c.-à-d.

$$37_{dec} = 100101_{bin}$$

Autrement dit, on a $37 = 2^5 + 2^2 + 2^0$, donc :

$$174^{37} = 174^{(2^5)} \times 174^{(2^2)} \times 174^{(2^0)}$$

Exponentiation modulaire rapide

Solution 2/2

- On calcule les restes modulo 187 des carrés successifs de 5 jusqu'à la plus grande valeur dont on a besoin :

2^0	$5^{(2^0)}$	mod 187	$\rightsquigarrow$	$5 \equiv 5 \mod 187$
2^1	$5^{(2^1)}$	mod 187		$5^2 \equiv 25 \mod 187$
2^2	$5^{(2^2)}$	mod 187		$25^2 \equiv 625 \equiv 64 \mod 187$
2^3	$5^{(2^3)}$	mod 187		$64^2 \equiv 4096 \equiv 169 \mod 187$

- On prend les restes correspondant aux puissances qui nous intéressent (2^3, 2^2 et 2^0) :

$5^{13} \equiv 5^{(2^3)} \times 5^{(2^2)} \times 5^{(2^0)} \equiv 169 \times 64 \times 5 \equiv 54080 \equiv 37 \mod 187$

- On calcule les restes modulo 187 des carrés successifs de 174 jusqu'à la plus grande valeur dont on a besoin :

2^0	$\rightsquigarrow$	$174 \equiv 174 \mod 187$
2^1		$174^2 \equiv 30276 \equiv 169 \mod 187$
2^2		$169^2 \equiv 28561 \equiv 137 \mod 187$
2^3		$137^2 \equiv 18769 \equiv 69 \mod 187$
2^4		$69^2 \equiv 4761 \equiv 86 \mod 187$
2^5		$86^2 \equiv 7396 \equiv 103 \mod 187$

- On prend les restes correspondant aux puissances qui nous intéressent (2^5, 2^2 et 2^0) :

$174^{37} \equiv 174^{(2^5)} \times 174^{(2^2)} \times 174^{(2^0)} \equiv 103 \times 137 \times 174 \equiv 2455314 \equiv 4 \mod 187$

Application!

En utilisant la méthode d'exponentiation modulaire rapide, calculer $16^{23} \mod 19$.

Calculer le nombre de multiplications et d'élévations au carré que vous avez utilisées.

Exponentielle Modulaire rapide

Exercice 1.

1. Démontrer que l'on peut calculer x^{43} en employant trois produits et des élévations au carré.
2. Calculer $1247^{43} \mod 27$.

Exercice 2. Calculer le nombre de multiplications et d'élévations au carré que vous devez faire en utilisant la méthode d'exponentiation rapide pour élever un nombre à la puissance 10262.

Exercice 3. En utilisant la méthode d'exponentiation modulaire rapide, calculer :

1. $51^{21} \mod 8$;
2. $231^{545} \mod 173$;
3. $51447^{6478} \mod 3241$.

x

Exercice 4. Quels sont les nombres inversibles dans $\mathbb{Z}/30\,\mathbb{Z}$?

Exercice 5. On admet que les décomposition en facteurs premiers de 1139062500 et 4665600 sont $2^2 \times 3^6 \times 5^8$ et $2^8 \times 3^6 \times 5^2$ respectivement. Calculer le pgcd de ces deux nombres.

Exercice 6. On rappelle que les 12 premiers nombres premiers sont les suivants :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.$$

Quelle est la forme de la décomposition en facteurs premiers d'un entier $1 \leq a \leq 25$ premier avec 35 ?

Exercice 7. En utilisant la méthode d'exponentiation modulaire rapide, calculer :

1. $84^{18} \mod 9$;
2. $156^{312} \mod 38$;

Exercice 8. Calculer le nombre de multiplications et d'élévations au carré que vous devez faire en utilisant la méthode d'exponentiation rapide pour élever un nombre à la puissance 7645.