

Square and Multiply

Potencias modulares grandes, paso a paso

Daniel Felipe Triviño

Asistente graduado · Fundamentos Matemáticos para la Computación · Universidad de los Andes

El problema

$$6^{115} \bmod 19 = ?$$

$$6^{115} = \underbrace{6 \times 6 \times 6 \times \cdots \times 6}_{115 \text{ veces}}$$

El problema

$$6^{115} \bmod 19 = ?$$

$$6^{115} = \underbrace{6 \times 6 \times 6 \times \cdots \times 6}_{115 \text{ veces}}$$

307180606913594390117978657628360735703373091
543821695941623353827100004182416124412952576

un número de 90 cifras

Camino directo: 114 multiplicaciones y números enormes.

El problema

$$6^{115} \bmod 19 = ?$$

$$6^{115} = \underbrace{6 \times 6 \times 6 \times \cdots \times 6}_{115 \text{ veces}}$$

307180606913594390117978657628360735703373091
543821695941623353827100004182416124412952576

un número de 90 cifras

Square and multiply: pocas operaciones y números pequeños.

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1$$

Paso 1: el exponente en binario (suma de potencias de 2).

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \underset{3}{\textcolor{brown}{1}} \underset{2}{0} \underset{1}{\textcolor{brown}{1}} \underset{0}{\textcolor{brown}{1}})_2$$

Paso 1: el exponente en binario (suma de potencias de 2).

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \underset{3}{\color{teal}1} \underset{2}{0} \underset{1}{\color{teal}1} \underset{0}{\color{teal}1} \big)_2$$

i b_i

Exponente acumulado

$$w = 2^0$$

$w = 1$

módulo 13

Se empieza con $w = 1$ y se leen los bits de izquierda a derecha.

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \underset{3}{\color{teal}1} \underset{2}{0} \underset{1}{\color{teal}1} \underset{0}{\color{teal}1} \big)_2$$

i

b_i

Square

Multiply

Exponente acumulado

$$w = 2^0$$

$$w = 1$$

módulo 13

Square: siempre. Multiply: solo si el bit es $\color{teal}1$.

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} \boxed{1} & 0 & 1 & 1 \end{pmatrix}_2$$

3 2 1 0

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$		0
				$w = 2^0$
				$w = 1$ módulo 13

Square: siempre. Multiply: solo si el bit es 1.

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} \boxed{1} & 0 & 1 & 1 \end{pmatrix}_2$$

3 2 1 0

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1
				$w = 2^1$
				$w = 2$ módulo 13

Square: siempre. Multiply: solo si el bit es 1.

2^{11} módulo 13

$2^{11} \bmod 13$

$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1
				$w = 2^1$
				$w = 2$ módulo 13

A la derecha: la potencia que llevamos y el valor de w .

2^{11} módulo 13

$2^{11} \bmod 13$

$11 = 8 + 2 + 1 = \left(\underset{3}{1} \underset{2}{\boxed{0}} \underset{1}{1} \underset{0}{1} \right)_2$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0
2	0	$w = 2^2 = 4$		$w = 2^2$
				$w = 4$ módulo 13

A la derecha: la potencia que llevamos y el valor de w .

2^{11} módulo 13

$2^{11} \bmod 13$

$11 = 8 + 2 + 1 = \left(\underset{3}{1} \underset{2}{\boxed{0}} \underset{1}{1} \underset{0}{1} \right)_2$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0
2	0	$w = 2^2 = 4$		$w = 2^2$
				$w = 4$ módulo 13

Square duplica el exponente: agrega un 0 al final.

2^{11} módulo 13

$2^{11} \bmod 13$

$11 = 8 + 2 + 1 = \left(\underset{3}{1} \underset{2}{\boxed{0}} \underset{1}{1} \underset{0}{1} \right)_2$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0
2	0	$w = 2^2 = 4$	—	$w = 2^2$
				$w = 4$ módulo 13

Square duplica el exponente: agrega un 0 al final.

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0 0
2	0	$w = 2^2 = 4$	—	$w = 2^4$
1	1	$w = 4^2 = 16 \equiv 3$		$w = 3$ módulo 13

Square duplica el exponente: agrega un 0 al final.

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0 1
2	0	$w = 2^2 = 4$	—	$w = 2^5$
1	1	$w = 4^2 = 16 \equiv 3$	$w = 3 \times 2 = 6$	$w = 6$ módulo 13

Square duplica el exponente: agrega un 0 al final.

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0 1
2	0	$w = 2^2 = 4$	—	$w = 2^5$
1	1	$w = 4^2 = 16 \equiv 3$	$w = 3 \times 2 = 6$	$w = 6$ módulo 13

Multiply le suma 1: el último bit pasa a 1.

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0 1 0
2	0	$w = 2^2 = 4$	—	$w = 2^{10}$
1	1	$w = 4^2 = 16 \equiv 3$	$w = 3 \times 2 = 6$	
0	1	$w = 6^2 = 36 \equiv 10$		$w = 10$ módulo 13

Multiply le suma 1: el último bit pasa a 1.

2^{11} módulo 13

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0 1 1
2	0	$w = 2^2 = 4$	—	$w = 2^{11}$
1	1	$w = 4^2 = 16 \equiv 3$	$w = 3 \times 2 = 6$	$w = 7$ módulo 13
0	1	$w = 6^2 = 36 \equiv 10$	$w = 10 \times 2 = 20 \equiv 7$	

Multiply le suma 1: el último bit pasa a 1.

$$2^{11} \text{ módulo } 13$$

$$2^{11} \bmod 13$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix}_2$$

3210

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0 1 1
2	0	$w = 2^2 = 4$	—	$w = 2^{11}$
1	1	$w = 4^2 = 16 \equiv 3$	$w = 3 \times 2 = 6$	$w = 7$ módulo 13
0	1	$w = 6^2 = 36 \equiv 10$	$w = 10 \times 2 = 20 \equiv 7$	
				$2^{11} \equiv 7 \pmod{13}$

El exponente acumulado coincide con el exponente original.

2^{11} módulo 13

$2^{11} \bmod 13$

$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix}_2$
 $\begin{smallmatrix} 3 & 2 & 1 & 0 \end{smallmatrix}$

i	b_i	Square	Multiply	Exponente acumulado
3	1	$w = 1^2 = 1$	$w = 1 \times 2 = 2$	1 0 1 1
2	0	$w = 2^2 = 4$	—	$w = 2^{11}$
1	1	$w = 4^2 = 16 \equiv 3$	$w = 3 \times 2 = 6$	$w = 7$ módulo 13
0	1	$w = 6^2 = 36 \equiv 10$	$w = 10 \times 2 = 20 \equiv 7$	

$2^{11} \equiv 7 \pmod{13}$

Comprobación: $2^{11} = 2048 = 13 \times 157 + 7$.

De vuelta al problema grande

6^{115} módulo 19

$$6^{115} \bmod 19$$

$$115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{\mathbf{1}} \underset{5}{\mathbf{1}} \underset{4}{\mathbf{1}} \underset{3}{0} \underset{2}{0} \underset{1}{\mathbf{1}} \underset{0}{\mathbf{1}} \right)_2$$

Paso 1: el exponente en binario.

6^{115} módulo 19

$$6^{115} \bmod 19$$

$$115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{\mathbf{1}} \underset{5}{\mathbf{1}} \underset{4}{\mathbf{1}} \underset{3}{0} \underset{2}{0} \underset{1}{\mathbf{1}} \underset{0}{\mathbf{1}} \right)_2$$

i

b_i

Square

Multiply

Exponente acumulado

$$w = 6^0$$

$$w = 1$$

módulo 19

Square: siempre. Multiply: solo si el bit es $\mathbf{1}$.

6^{115} módulo 19

$$6^{115} \bmod 19 \qquad 115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{\boxed{1}} \underset{5}{1} \underset{4}{1} \underset{3}{0} \underset{2}{0} \underset{1}{1} \underset{0}{1} \right)_2$$

i	b_i	Square	Multiply	Exponente acumulado
6	1	$w = 1^2 = 1$		0
				$w = 6^0$
				$w = 1$ módulo 19

Square: siempre. Multiply: solo si el bit es 1.

6^{115} módulo 19

$$6^{115} \bmod 19$$

$$115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{\boxed{1}} \underset{5}{1} \underset{4}{1} \underset{3}{0} \underset{2}{0} \underset{1}{1} \underset{0}{1} \right)_2$$

i	b_i	Square	Multiply	Exponente acumulado
6	1	$w = 1^2 = 1$	$w = 1 \times 6 = 6$	1
				$w = 6^1$
				$w = 6$ módulo 19

Square: siempre. Multiply: solo si el bit es 1.

6^{115} módulo 19

$6^{115} \bmod 19$

$$115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{\textcolor{brown}{1}} \underset{5}{\boxed{\textcolor{brown}{1}}} \underset{4}{\textcolor{brown}{1}} \underset{3}{0} \underset{2}{0} \underset{1}{\textcolor{brown}{1}} \underset{0}{\textcolor{brown}{1}} \right)_2$$

i	b_i	Square	Multiply	Exponente acumulado
6	$\textcolor{brown}{1}$	$w = 1^2 = \textcolor{teal}{1}$	$w = 1 \times \textcolor{red}{6} = \textcolor{teal}{6}$	$\textcolor{brown}{1} 0$
5	$\textcolor{brown}{1}$	$w = 6^2 = 36 \equiv \textcolor{teal}{17}$		$w = 6^2$
				$w = \textcolor{teal}{17}$ módulo 19

Square: siempre. Multiply: solo si el bit es $\textcolor{brown}{1}$.

6^{115} módulo 19

$6^{115} \bmod 19$

$$115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{\textcolor{brown}{1}} \underset{5}{\boxed{\textcolor{brown}{1}}} \underset{4}{\textcolor{brown}{1}} \underset{3}{0} \underset{2}{0} \underset{1}{\textcolor{brown}{1}} \underset{0}{\textcolor{brown}{1}} \right)_2$$

i	b_i	Square	Multiply	Exponente acumulado
6	$\textcolor{brown}{1}$	$w = 1^2 = \textcolor{teal}{1}$	$w = 1 \times \textcolor{red}{6} = \textcolor{teal}{6}$	$\textcolor{brown}{1} \textcolor{brown}{1}$
5	$\textcolor{brown}{1}$	$w = 6^2 = 36 \equiv \textcolor{teal}{17}$	$w = 17 \times \textcolor{red}{6} = 102 \equiv \textcolor{teal}{7}$	$w = 6^3$
				$w = \textcolor{teal}{7}$ módulo 19

Square: siempre. Multiply: solo si el bit es $\textcolor{brown}{1}$.

6^{115} módulo 19

$6^{115} \bmod 19$

$$115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{\textcolor{brown}{1}} \underset{5}{\textcolor{brown}{1}} \boxed{\underset{4}{\textcolor{brown}{1}}} \underset{3}{0} \underset{2}{0} \underset{1}{\textcolor{brown}{1}} \underset{0}{\textcolor{brown}{1}} \right)_2$$

i	b_i	Square	Multiply	Exponente acumulado
6	$\textcolor{brown}{1}$	$w = 1^2 = 1$	$w = 1 \times \textcolor{red}{6} = \textcolor{teal}{6}$	$\textcolor{brown}{1} \textcolor{brown}{1} \textcolor{brown}{1}$
5	$\textcolor{brown}{1}$	$w = 6^2 = 36 \equiv \textcolor{teal}{17}$	$w = 17 \times \textcolor{red}{6} = 102 \equiv \textcolor{teal}{7}$	$w = 6^7$
4	$\textcolor{brown}{1}$	$w = 7^2 = 49 \equiv \textcolor{teal}{11}$	$w = 11 \times \textcolor{red}{6} = 66 \equiv \textcolor{teal}{9}$	$w = 9$ módulo 19

Square: siempre. Multiply: solo si el bit es $\textcolor{brown}{1}$.

6^{115} módulo 19

$6^{115} \bmod 19$

$$115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{\textcolor{brown}{1}} \underset{5}{\textcolor{brown}{1}} \underset{4}{\textcolor{brown}{1}} \underset{3}{\boxed{\textcolor{brown}{0}}} \underset{2}{0} \underset{1}{\textcolor{brown}{1}} \underset{0}{\textcolor{brown}{1}} \right)_2$$

i	b_i	Square	Multiply	Exponente acumulado
6	$\textcolor{brown}{1}$	$w = 1^2 = 1$	$w = 1 \times \textcolor{red}{6} = \textcolor{teal}{6}$	$\textcolor{brown}{1} \textcolor{brown}{1} \textcolor{brown}{1} 0$
5	$\textcolor{brown}{1}$	$w = 6^2 = 36 \equiv \textcolor{teal}{17}$	$w = 17 \times \textcolor{red}{6} = 102 \equiv \textcolor{teal}{7}$	$w = 6^{14}$
4	$\textcolor{brown}{1}$	$w = 7^2 = 49 \equiv \textcolor{teal}{11}$	$w = 11 \times \textcolor{red}{6} = 66 \equiv \textcolor{teal}{9}$	
3	0	$w = 9^2 = 81 \equiv \textcolor{teal}{5}$		$w = \textcolor{teal}{5}$ módulo 19

Square: siempre. Multiply: solo si el bit es $\textcolor{brown}{1}$.

6^{115} módulo 19

$6^{115} \bmod 19$

$$115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{\textcolor{brown}{1}} \underset{5}{\textcolor{brown}{1}} \underset{4}{\textcolor{brown}{1}} \underset{3}{0} \underset{2}{\boxed{0}} \underset{1}{\textcolor{brown}{1}} \underset{0}{\textcolor{brown}{1}} \right)_2$$

i	b_i	Square	Multiply	Exponente acumulado
6	$\textcolor{brown}{1}$	$w = 1^2 = 1$	$w = 1 \times \textcolor{red}{6} = \textcolor{teal}{6}$	$\textcolor{brown}{1} \textcolor{brown}{1} \textcolor{brown}{1} 0 0$
5	$\textcolor{brown}{1}$	$w = 6^2 = 36 \equiv \textcolor{teal}{17}$	$w = 17 \times \textcolor{red}{6} = 102 \equiv \textcolor{teal}{7}$	$w = 6^{28}$
4	$\textcolor{brown}{1}$	$w = 7^2 = 49 \equiv \textcolor{teal}{11}$	$w = 11 \times \textcolor{red}{6} = 66 \equiv \textcolor{teal}{9}$	
3	0	$w = 9^2 = 81 \equiv \textcolor{teal}{5}$	—	$w = \textcolor{teal}{6}$
2	0	$w = 5^2 = 25 \equiv \textcolor{teal}{6}$		módulo 19

Square: siempre. Multiply: solo si el bit es $\textcolor{brown}{1}$.

$$6^{115} \text{ módulo } 19$$

$$6^{115} \text{ mod } 19 \qquad 115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{1} \underset{5}{1} \underset{4}{1} \underset{3}{0} \underset{2}{0} \boxed{\underset{1}{1}} \underset{0}{1} \right)_2$$

i	b_i	Square	Multiply	Exponente acumulado
6	1	$w = 1^2 = 1$	$w = 1 \times 6 = 6$	1 1 1 0 0 1
5	1	$w = 6^2 = 36 \equiv 17$	$w = 17 \times 6 = 102 \equiv 7$	$w = 6^{57}$
4	1	$w = 7^2 = 49 \equiv 11$	$w = 11 \times 6 = 66 \equiv 9$	
3	0	$w = 9^2 = 81 \equiv 5$	—	$w = 7$
2	0	$w = 5^2 = 25 \equiv 6$	—	módulo 19
1	1	$w = 6^2 = 36 \equiv 17$	$w = 17 \times 6 = 102 \equiv 7$	

Square: siempre. Multiply: solo si el bit es 1.

$$6^{115} \text{ módulo } 19$$

$$6^{115} \bmod 19$$

$$115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{1} \underset{5}{1} \underset{4}{1} \underset{3}{0} \underset{2}{0} \underset{1}{1} \boxed{\underset{0}{1}} \right)_2$$

i	b_i	Square	Multiply	Exponente acumulado
6	1	$w = 1^2 = 1$	$w = 1 \times 6 = 6$	1 1 1 0 0 1 1
5	1	$w = 6^2 = 36 \equiv 17$	$w = 17 \times 6 = 102 \equiv 7$	$w = 6^{115}$
4	1	$w = 7^2 = 49 \equiv 11$	$w = 11 \times 6 = 66 \equiv 9$	
3	0	$w = 9^2 = 81 \equiv 5$	—	$w = 9$
2	0	$w = 5^2 = 25 \equiv 6$	—	módulo 19
1	1	$w = 6^2 = 36 \equiv 17$	$w = 17 \times 6 = 102 \equiv 7$	
0	1	$w = 7^2 = 49 \equiv 11$	$w = 11 \times 6 = 66 \equiv 9$	

Square: siempre. Multiply: solo si el bit es 1.

$$6^{115} \text{ módulo } 19$$

$6^{115} \text{ mod } 19$
 $115 = 64 + 32 + 16 + 2 + 1 = \left(\underset{6}{1} \underset{5}{1} \underset{4}{1} \underset{3}{0} \underset{2}{0} \underset{1}{1} \underset{0}{1} \right)_2$

i	b_i	Square	Multiply	Exponente acumulado
6	1	$w = 1^2 = 1$	$w = 1 \times 6 = 6$	1 1 1 0 0 1 1
5	1	$w = 6^2 = 36 \equiv 17$	$w = 17 \times 6 = 102 \equiv 7$	$w = 6^{115}$
4	1	$w = 7^2 = 49 \equiv 11$	$w = 11 \times 6 = 66 \equiv 9$	
3	0	$w = 9^2 = 81 \equiv 5$	—	$w = 9$
2	0	$w = 5^2 = 25 \equiv 6$	—	módulo 19
1	1	$w = 6^2 = 36 \equiv 17$	$w = 17 \times 6 = 102 \equiv 7$	
0	1	$w = 7^2 = 49 \equiv 11$	$w = 11 \times 6 = 66 \equiv 9$	$6^{115} \equiv 9 \pmod{19}$

El exponente acumulado coincide con el exponente original.

6^{115} módulo 19

$6^{115} \bmod 19$

$115 = 64 + 32 + 16 + 2 + 1 = \begin{pmatrix} \textcolor{brown}{1} & \textcolor{brown}{1} & \textcolor{brown}{1} & 0 & 0 & \textcolor{brown}{1} & \textcolor{brown}{1} \end{pmatrix}_2$

6

5

4

3

2

1

0

i	b_i	Square	Multiply	Exponente acumulado
6	$\textcolor{brown}{1}$	$w = 1^2 = 1$	$w = 1 \times \textcolor{red}{6} = \textcolor{teal}{6}$	$\textcolor{brown}{1} \textcolor{brown}{1} \textcolor{brown}{1} 0 0 \textcolor{brown}{1} \textcolor{brown}{1}$
5	$\textcolor{brown}{1}$	$w = 6^2 = 36 \equiv \textcolor{teal}{17}$	$w = 17 \times \textcolor{red}{6} = 102 \equiv \textcolor{teal}{7}$	$w = 6^{115}$
4	$\textcolor{brown}{1}$	$w = 7^2 = 49 \equiv \textcolor{teal}{11}$	$w = 11 \times \textcolor{red}{6} = 66 \equiv \textcolor{teal}{9}$	
3	0	$w = 9^2 = 81 \equiv 5$	—	$w = 9$
2	0	$w = 5^2 = 25 \equiv 6$	—	módulo 19
1	$\textcolor{brown}{1}$	$w = 6^2 = 36 \equiv \textcolor{teal}{17}$	$w = 17 \times \textcolor{red}{6} = 102 \equiv \textcolor{teal}{7}$	
0	$\textcolor{brown}{1}$	$w = 7^2 = 49 \equiv \textcolor{teal}{11}$	$w = 11 \times \textcolor{red}{6} = 66 \equiv \textcolor{teal}{9}$	$6^{115} \equiv \textcolor{teal}{9} \pmod{19}$

7 cuadrados y 5 multiplicaciones, en lugar de 114.

Para calcular a^e módulo m

Para calcular a^e módulo m

1. Escribir el exponente e en binario.

Para calcular a^e módulo m

1. Escribir el exponente e en binario.
2. Empezar con $w = 1$.

Para calcular a^e módulo m

1. Escribir el exponente e en binario.
2. Empezar con $w = 1$.
3. Por cada bit, de izquierda a derecha: Square, $w = w^2$ módulo m .

Para calcular a^e módulo m

1. Escribir el exponente e en binario.
2. Empezar con $w = 1$.
3. Por cada bit, de izquierda a derecha: Square, $w = w^2$ módulo m .
4. Si el bit es 1: Multiply, $w = w \times a$ módulo m .

Para calcular a^e módulo m

1. Escribir el exponente e en binario.
2. Empezar con $w = 1$.
3. Por cada bit, de izquierda a derecha: Square, $w = w^2$ módulo m .
4. Si el bit es 1: Multiply, $w = w \times a$ módulo m .
5. Al terminar los bits, w es la respuesta.