Vídeo : `https://youtu.be/zxsQ5SfSafY`

1. Resumen

El algoritmo de exponenciación modular trata de resolver el problema de calcular $a^e \pmod{m}$ cuando e es un exponente muy grande. El procedimiento se basa en reducir el problema a exponentes más pequeños agrupando cuadrados. Dicho de otra forma, tenemos dos casos para e, que sea par o impar:

1. Si e es impar, es decir, $e = 2f+1$ entonces pondremos $a^e = a^{1+2f} = a \cdot (a^2)^f$. Calculando $a^2 \pmod{m}$ reducimos el tamaño del exponente a la mitad.
2. Si e es par, es decir $e = 2f$ entonces pondremos $a^e = a^{2f} = (a^2)^f$. De nuevo, calculando $a^2 \pmod{m}$ reduciremos el tamaño del exponente a la mitad.

En unos pocos pasos, el exponente llegará a 1 y podremos multiplicar los factores que hayamos sacado por los exponentes impares para completar la operación.
Lo mejor para entender el proceso es seguirlo mendiante los ejemplos.

2. Erratas

(No detectadas)

3. Ejercicios

Aquí tienes 50 exponenciales modulares. En aquellas en las que es posible reducir el exponente mediante la Fórmula de Euler se ha hecho, pero eso sólo es posible cuando a es una unidad módulo m. En los casos en los que no es una unidad, se procederá directamente a realizar el cálculo. Eso también se podría hacer en el otro caso, obteniendo el mismo resultado, pero con algunas operaciones más.

Ejercicio 1. *Calcula* $10^{60} \pmod{42}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $10^{60} \pmod{42}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$
\begin{aligned}
10^{60} &\equiv 10^{60} \equiv \left(10^2\right)^{30} \equiv 16^{30} && (\text{Porque } 10^2 \equiv 16 \pmod{42})\\
&\equiv 16^{30} \equiv \left(16^2\right)^{15} \equiv 4^{15} && (\text{Porque } 16^2 \equiv 4 \pmod{42})\\
&\equiv 4{\cdot}4^{14} \equiv 4{\cdot} \left(4^2\right)^{7} \equiv 4{\cdot}16^{7} && (\text{Porque } 4^2 \equiv 16 \pmod{42})\\
&\equiv 4 \cdot 16{\cdot}16^{6} \equiv 4 \cdot 16{\cdot} \left(16^2\right)^{3} \equiv 4 \cdot 16{\cdot}4^{3} && (\text{Porque } 16^2 \equiv 4 \pmod{42})\\
&\equiv 4 \cdot 16 \cdot 4{\cdot}4^{2} \equiv 4 \cdot 16 \cdot 4{\cdot} \left(4^2\right)^{1} \equiv 4 \cdot 16 \cdot 4{\cdot}16^{1} && (\text{Porque } 4^2 \equiv 16 \pmod{42})\\
&\equiv 22 \cdot 4 \cdot 16 && (\text{Porque } 4 \cdot 16 \equiv 22 \pmod{42})\\
&\equiv 4 \cdot 16 && (\text{Porque } 22 \cdot 4 \equiv 4 \pmod{42})\\
&\equiv 22 && (\text{Porque } 4 \cdot 16 \equiv 22 \pmod{42})
\end{aligned}
$$

◊

Ejercicio 2. *Calcula* $23^{84} \pmod{35}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $35 = 5 \cdot 7$, entonces aplicamos la fórmula y tenemos que $\varphi(35) = \varphi(5 \cdot 7) = \varphi(5^1) \cdot \varphi(7^1) = (5^1 - 5^0) \cdot (7^1 - 7^0) = 24$. Esto nos deja $23^{84} = 23^{12+24 \cdot 3} = 23^{12} \cdot \left(23^{24}\right)^3 \equiv 23^{12} \pmod{35}$ porque $23^{24} \equiv 1 \pmod{35}$ por la Fórmula de Euler.

Para calcular $23^{12} \pmod{35}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
23^{12} &\equiv 23^{12} \equiv \left(23^2\right)^6 \equiv 4^6 && (\text{Porque } 23^2 \equiv 4 \pmod{35})\\
&\equiv 4^6 \equiv \left(4^2\right)^3 \equiv 16^3 && (\text{Porque } 4^2 \equiv 16 \pmod{35})\\
&\equiv 16 \cdot 16^2 \equiv 16 \cdot \left(16^2\right)^1 \equiv 16 \cdot 11^1 && (\text{Porque } 16^2 \equiv 11 \pmod{35})\\
&\equiv 1 && (\text{Porque } 16 \cdot 11 \equiv 1 \pmod{35})
\end{aligned}$$

◊

Ejercicio 3. *Calcula* $25^{86} \pmod{35}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $25^{86} \pmod{35}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
25^{86} &\equiv 25^{86} \equiv \left(25^2\right)^{43} \equiv 30^{43} && (\text{Porque } 25^2 \equiv 30 \pmod{35})\\
&\equiv 30 \cdot 30^{42} \equiv 30 \cdot \left(30^2\right)^{21} \equiv 30 \cdot 25^{21} && (\text{Porque } 30^2 \equiv 25 \pmod{35})\\
&\equiv 30 \cdot 25 \cdot 25^{20} \equiv 30 \cdot 25 \cdot \left(25^2\right)^{10} \equiv 30 \cdot 25 \cdot 30^{10} && (\text{Porque } 25^2 \equiv 30 \pmod{35})\\
&\equiv 30 \cdot 25 \cdot 30^{10} \equiv 30 \cdot 25 \cdot \left(30^2\right)^5 \equiv 30 \cdot 25 \cdot 25^5 && (\text{Porque } 30^2 \equiv 25 \pmod{35})\\
&\equiv 30 \cdot 25 \cdot 25 \cdot 25^4 \equiv 30 \cdot 25 \cdot 25 \cdot \left(25^2\right)^2 \equiv 30 \cdot 25 \cdot 25 \cdot 30^2 && (\text{Porque } 25^2 \equiv 30 \pmod{35})\\
&\equiv 30 \cdot 25 \cdot 25 \cdot 30^2 \equiv 30 \cdot 25 \cdot 25 \cdot \left(30^2\right)^1 \equiv 30 \cdot 25 \cdot 25 \cdot 25^1 && (\text{Porque } 30^2 \equiv 25 \pmod{35})\\
&\equiv 15 \cdot 25 \cdot 25 && (\text{Porque } 30 \cdot 25 \equiv 15 \pmod{35})\\
&\equiv 25 \cdot 25 && (\text{Porque } 15 \cdot 25 \equiv 25 \pmod{35})\\
&\equiv 30 && (\text{Porque } 25 \cdot 25 \equiv 30 \pmod{35})
\end{aligned}$$

◊

Ejercicio 4. *Calcula* $34^{33} \pmod{38}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $34^{33} \pmod{38}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo

paso a paso:

$$\begin{aligned}
34^{33} &\equiv 34{\cdot}34^{32} \equiv 34{\cdot}\left(34^2\right)^{16} \equiv 34{\cdot}16^{16} && (\text{Porque } 34^2 \equiv 16 \pmod{38})\\
&\equiv 34{\cdot}16^{16} \equiv 34{\cdot}\left(16^2\right)^{8} \equiv 34{\cdot}28^{8} && (\text{Porque } 16^2 \equiv 28 \pmod{38})\\
&\equiv 34{\cdot}28^{8} \equiv 34{\cdot}\left(28^2\right)^{4} \equiv 34{\cdot}24^{4} && (\text{Porque } 28^2 \equiv 24 \pmod{38})\\
&\equiv 34{\cdot}24^{4} \equiv 34{\cdot}\left(24^2\right)^{2} \equiv 34{\cdot}6^{2} && (\text{Porque } 24^2 \equiv 6 \pmod{38})\\
&\equiv 34{\cdot}6^{2} \equiv 34{\cdot}\left(6^2\right)^{1} \equiv 34{\cdot}36^{1} && (\text{Porque } 6^2 \equiv 36 \pmod{38})\\
&\equiv 8 && (\text{Porque } 34\cdot 36 \equiv 8 \pmod{38})
\end{aligned}$$

♢

Ejercicio 5. *Calcula* $22^{247} \pmod{47}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 47 es primo, tendremos que $\varphi(47) = 47 - 1 = 46$. Esto nos deja $22^{247} = 22^{17+46\cdot 5} = 22^{17} \cdot \left(22^{46}\right)^5 \equiv 22^{17} \pmod{47}$ porque $22^{46} \equiv 1 \pmod{47}$ por la Fórmula de Euler.
Para calcular $22^{17} \pmod{47}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
22^{17} &\equiv 22{\cdot}22^{16} \equiv 22{\cdot}\left(22^2\right)^{8} \equiv 22{\cdot}14^{8} && (\text{Porque } 22^2 \equiv 14 \pmod{47})\\
&\equiv 22{\cdot}14^{8} \equiv 22{\cdot}\left(14^2\right)^{4} \equiv 22{\cdot}8^{4} && (\text{Porque } 14^2 \equiv 8 \pmod{47})\\
&\equiv 22{\cdot}8^{4} \equiv 22{\cdot}\left(8^2\right)^{2} \equiv 22{\cdot}17^{2} && (\text{Porque } 8^2 \equiv 17 \pmod{47})\\
&\equiv 22{\cdot}17^{2} \equiv 22{\cdot}\left(17^2\right)^{1} \equiv 22{\cdot}7^{1} && (\text{Porque } 17^2 \equiv 7 \pmod{47})\\
&\equiv 13 && (\text{Porque } 22\cdot 7 \equiv 13 \pmod{47})
\end{aligned}$$

♢

Ejercicio 6. *Calcula* $33^{52} \pmod{38}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $38 = 2\cdot 19$, entonces aplicamos la fórmula y tenemos que $\varphi(38) = \varphi(2\cdot 19) = \varphi(2^1)\cdot\varphi(19^1) = (2^1 - 2^0)\cdot(19^1 - 19^0) = 18$. Esto nos deja $33^{52} = 33^{16+18\cdot 2} = 33^{16}\cdot\left(33^{18}\right)^2 \equiv 33^{16} \pmod{38}$ porque $33^{18} \equiv 1 \pmod{38}$ por la Fórmula de Euler.
Para calcular $33^{16} \pmod{38}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
33^{16} &\equiv 33^{16} \equiv \left(33^2\right)^{8} \equiv 25^{8} && (\text{Porque } 33^2 \equiv 25 \pmod{38})\\
&\equiv 25^{8} \equiv \left(25^2\right)^{4} \equiv 17^{4} && (\text{Porque } 25^2 \equiv 17 \pmod{38})\\
&\equiv 17^{4} \equiv \left(17^2\right)^{2} \equiv 23^{2} && (\text{Porque } 17^2 \equiv 23 \pmod{38})\\
&\equiv 23^{2} \equiv \left(23^2\right)^{1} \equiv 35^{1} && (\text{Porque } 23^2 \equiv 35 \pmod{38})\\
&\equiv 35 \pmod{38}.
\end{aligned}$$

♢

Ejercicio 7. *Calcula* $12^{210} \pmod{41}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 41 es primo, tendremos que $\varphi(41) = 41 - 1 = 40$. Esto nos deja $12^{210} = 12^{10+40\cdot 5} = 12^{10} \cdot \left(12^{40}\right)^5 \equiv 12^{10} \pmod{41}$ porque $12^{40} \equiv 1 \pmod{41}$ por la Fórmula de Euler.
Para calcular $12^{10} \pmod{41}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
12^{10} &\equiv 12^{10} \equiv \left(12^2\right)^5 \equiv 21^5 && \text{(Porque } 12^2 \equiv 21 \pmod{41}\text{)}\\
&\equiv 21{\cdot}21^4 \equiv 21{\cdot} \left(21^2\right)^2 \equiv 21{\cdot}31^2 && \text{(Porque } 21^2 \equiv 31 \pmod{41}\text{)}\\
&\equiv 21{\cdot}31^2 \equiv 21{\cdot} \left(31^2\right)^1 \equiv 21{\cdot}18^1 && \text{(Porque } 31^2 \equiv 18 \pmod{41}\text{)}\\
&\equiv 9 && \text{(Porque } 21 \cdot 18 \equiv 9 \pmod{41}\text{)}
\end{aligned}$$

◊

Ejercicio 8. *Calcula* $39^{130} \pmod{41}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 41 es primo, tendremos que $\varphi(41) = 41 - 1 = 40$. Esto nos deja $39^{130} = 39^{10+40\cdot 3} = 39^{10} \cdot \left(39^{40}\right)^3 \equiv 39^{10} \pmod{41}$ porque $39^{40} \equiv 1 \pmod{41}$ por la Fórmula de Euler.
Para calcular $39^{10} \pmod{41}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
39^{10} &\equiv 39^{10} \equiv \left(39^2\right)^5 \equiv 4^5 && \text{(Porque } 39^2 \equiv 4 \pmod{41}\text{)}\\
&\equiv 4{\cdot}4^4 \equiv 4{\cdot} \left(4^2\right)^2 \equiv 4{\cdot}16^2 && \text{(Porque } 4^2 \equiv 16 \pmod{41}\text{)}\\
&\equiv 4{\cdot}16^2 \equiv 4{\cdot} \left(16^2\right)^1 \equiv 4{\cdot}10^1 && \text{(Porque } 16^2 \equiv 10 \pmod{41}\text{)}\\
&\equiv 40 && \text{(Porque } 4 \cdot 10 \equiv 40 \pmod{41}\text{)}
\end{aligned}$$

◊

Ejercicio 9. *Calcula* $20^{82} \pmod{46}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $20^{82} \pmod{46}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
20^{82} &\equiv 20^{82} \equiv \left(20^2\right)^{41} \equiv 32^{41} && \text{(Porque } 20^2 \equiv 32 \pmod{46}\text{)}\\
&\equiv 32{\cdot}32^{40} \equiv 32{\cdot} \left(32^2\right)^{20} \equiv 32{\cdot}12^{20} && \text{(Porque } 32^2 \equiv 12 \pmod{46}\text{)}\\
&\equiv 32{\cdot}12^{20} \equiv 32{\cdot} \left(12^2\right)^{10} \equiv 32{\cdot}6^{10} && \text{(Porque } 12^2 \equiv 6 \pmod{46}\text{)}\\
&\equiv 32{\cdot}6^{10} \equiv 32{\cdot} \left(6^2\right)^5 \equiv 32{\cdot}36^5 && \text{(Porque } 6^2 \equiv 36 \pmod{46}\text{)}\\
&\equiv 32 \cdot 36{\cdot}36^4 \equiv 32 \cdot 36{\cdot} \left(36^2\right)^2 \equiv 32 \cdot 36{\cdot}8^2 && \text{(Porque } 36^2 \equiv 8 \pmod{46}\text{)}\\
&\equiv 32 \cdot 36{\cdot}8^2 \equiv 32 \cdot 36{\cdot} \left(8^2\right)^1 \equiv 32 \cdot 36{\cdot}18^1 && \text{(Porque } 8^2 \equiv 18 \pmod{46}\text{)}\\
&\equiv 2 \cdot 18 && \text{(Porque } 32 \cdot 36 \equiv 2 \pmod{46}\text{)}\\
&\equiv 36 && \text{(Porque } 2 \cdot 18 \equiv 36 \pmod{46}\text{)}
\end{aligned}$$

$\Diamond$

Ejercicio 10. *Calcula* $29^{61} \pmod{36}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $36 = 2^2 \cdot 3^2$, entonces aplicamos la fórmula y tenemos que $\varphi(36) = \varphi(2^2 \cdot 3^2) = \varphi(2^2) \cdot \varphi(3^2) = (2^2 - 2^1) \cdot (3^2 - 3^1) = 12$. Esto nos deja $29^{61} = 29^{1+12\cdot 5} = 29^1 \cdot \left(29^{12}\right)^5 \equiv 29^1 \pmod{36}$ porque $29^{12} \equiv 1 \pmod{36}$ por la Fórmula de Euler.
Para calcular $29^1 \pmod{36}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$29^1 \equiv 29 \pmod{36}.$$

$\Diamond$

Ejercicio 11. *Calcula* $20^{99} \pmod{43}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 43 es primo, tendremos que $\varphi(43) = 43 - 1 = 42$. Esto nos deja $20^{99} = 20^{15+42\cdot 2} = 20^{15} \cdot \left(20^{42}\right)^2 \equiv 20^{15} \pmod{43}$ porque $20^{42} \equiv 1 \pmod{43}$ por la Fórmula de Euler.
Para calcular $20^{15} \pmod{43}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
20^{15} &\equiv 20 \cdot 20^{14} \equiv 20 \cdot \left(20^2\right)^7 \equiv 20 \cdot 13^7 && (\text{Porque } 20^2 \equiv 13 \pmod{43})\\
&\equiv 20 \cdot 13 \cdot 13^6 \equiv 20 \cdot 13 \cdot \left(13^2\right)^3 \equiv 20 \cdot 13 \cdot 40^3 && (\text{Porque } 13^2 \equiv 40 \pmod{43})\\
&\equiv 20 \cdot 13 \cdot 40 \cdot 40^2 \equiv 20 \cdot 13 \cdot 40 \cdot \left(40^2\right)^1 \equiv 20 \cdot 13 \cdot 40 \cdot 9^1 && (\text{Porque } 40^2 \equiv 9 \pmod{43})\\
&\equiv 2 \cdot 40 \cdot 9 && (\text{Porque } 20 \cdot 13 \equiv 2 \pmod{43})\\
&\equiv 37 \cdot 9 && (\text{Porque } 2 \cdot 40 \equiv 37 \pmod{43})\\
&\equiv 32 && (\text{Porque } 37 \cdot 9 \equiv 32 \pmod{43})
\end{aligned}$$

$\Diamond$

Ejercicio 12. *Calcula* $16^{47} \pmod{36}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $16^{47} \pmod{36}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo

paso a paso:

$$
\begin{aligned}
16^{47} &\equiv 16{\cdot}16^{46} \equiv 16{\cdot}\left(16^2\right)^{23} \equiv 16{\cdot}4^{23} && (\text{Porque } 16^2 \equiv 4 \pmod{36})\\
&\equiv 16\cdot 4{\cdot}4^{22} \equiv 16\cdot 4{\cdot}\left(4^2\right)^{11} \equiv 16\cdot 4{\cdot}16^{11} && (\text{Porque } 4^2 \equiv 16 \pmod{36})\\
&\equiv 16\cdot 4\cdot 16{\cdot}16^{10} \equiv 16\cdot 4\cdot 16{\cdot}\left(16^2\right)^{5} \equiv 16\cdot 4\cdot 16{\cdot}4^{5} && (\text{Porque } 16^2 \equiv 4 \pmod{36})\\
&\equiv 16\cdot 4\cdot 16\cdot 4{\cdot}4^{4} \equiv 16\cdot 4\cdot 16\cdot 4{\cdot}\left(4^2\right)^{2} \equiv 16\cdot 4\cdot 16\cdot 4{\cdot}16^{2} && (\text{Porque } 4^2 \equiv 16 \pmod{36})\\
&\equiv 16\cdot 4\cdot 16\cdot 4{\cdot}16^{2} \equiv 16\cdot 4\cdot 16\cdot 4{\cdot}\left(16^2\right)^{1} \equiv 16\cdot 4\cdot 16\cdot 4{\cdot}4^{1} && (\text{Porque } 16^2 \equiv 4 \pmod{36})\\
&\equiv 28\cdot 16\cdot 4\cdot 4 && (\text{Porque } 16\cdot 4 \equiv 28 \pmod{36})\\
&\equiv 16\cdot 4\cdot 4 && (\text{Porque } 28\cdot 16 \equiv 16 \pmod{36})\\
&\equiv 28\cdot 4 && (\text{Porque } 16\cdot 4 \equiv 28 \pmod{36})\\
&\equiv 4 && (\text{Porque } 28\cdot 4 \equiv 4 \pmod{36})
\end{aligned}
$$

◊

Ejercicio 13. *Calcula* $32^{162} \pmod{45}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $45 = 3^2\cdot 5$, entonces aplicamos la fórmula y tenemos que $\varphi(45) = \varphi(3^2\cdot 5) = \varphi(3^2)\cdot\varphi(5^1) = (3^2-3^1)\cdot(5^1-5^0) = 24$. Esto nos deja $32^{162} = 32^{18+24\cdot 6} = 32^{18}\cdot\left(32^{24}\right)^6 \equiv 32^{18} \pmod{45}$ porque $32^{24}\equiv 1 \pmod{45}$ por la Fórmula de Euler.
Para calcular $32^{18} \pmod{45}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$
\begin{aligned}
32^{18} &\equiv 32^{18} \equiv \left(32^2\right)^{9} \equiv 34^{9} && (\text{Porque } 32^2 \equiv 34 \pmod{45})\\
&\equiv 34{\cdot}34^{8} \equiv 34{\cdot}\left(34^2\right)^{4} \equiv 34{\cdot}31^{4} && (\text{Porque } 34^2 \equiv 31 \pmod{45})\\
&\equiv 34{\cdot}31^{4} \equiv 34{\cdot}\left(31^2\right)^{2} \equiv 34{\cdot}16^{2} && (\text{Porque } 31^2 \equiv 16 \pmod{45})\\
&\equiv 34{\cdot}16^{2} \equiv 34{\cdot}\left(16^2\right)^{1} \equiv 34{\cdot}31^{1} && (\text{Porque } 16^2 \equiv 31 \pmod{45})\\
&\equiv 19 && (\text{Porque } 34\cdot 31 \equiv 19 \pmod{45})
\end{aligned}
$$

◊

Ejercicio 14. *Calcula* $11^{199} \pmod{47}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 47 es primo, tendremos que $\varphi(47) = 47-1 = 46$. Esto nos deja $11^{199} = 11^{15+46\cdot 4} = 11^{15}\cdot\left(11^{46}\right)^4 \equiv 11^{15} \pmod{47}$ porque $11^{46}\equiv 1 \pmod{47}$ por la Fórmula de Euler.
Para calcular $11^{15} \pmod{47}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor

cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
11^{15} &\equiv 11{\cdot}11^{14} \equiv 11{\cdot}\left(11^2\right)^7 \equiv 11{\cdot}27^7 && \text{(Porque } 11^2 \equiv 27 \pmod{47}\text{)}\\
&\equiv 11\cdot 27{\cdot}27^6 \equiv 11\cdot 27{\cdot}\left(27^2\right)^3 \equiv 11\cdot 27{\cdot}24^3 && \text{(Porque } 27^2 \equiv 24 \pmod{47}\text{)}\\
&\equiv 11\cdot 27\cdot 24{\cdot}24^2 \equiv 11\cdot 27\cdot 24{\cdot}\left(24^2\right)^1 \equiv 11\cdot 27\cdot 24{\cdot}12^1 && \text{(Porque } 24^2 \equiv 12 \pmod{47}\text{)}\\
&\equiv 15\cdot 24\cdot 12 && \text{(Porque } 11\cdot 27 \equiv 15 \pmod{47}\text{)}\\
&\equiv 31\cdot 12 && \text{(Porque } 15\cdot 24 \equiv 31 \pmod{47}\text{)}\\
&\equiv 43 && \text{(Porque } 31\cdot 12 \equiv 43 \pmod{47}\text{)}
\end{aligned}$$

◊

Ejercicio 15. *Calcula* $11^{159} \pmod{35}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $35 = 5\cdot 7$, entonces aplicamos la fórmula y tenemos que $\varphi(35) = \varphi(5\cdot 7) = \varphi(5^1)\cdot\varphi(7^1) = (5^1 - 5^0)\cdot(7^1 - 7^0) = 24$. Esto nos deja $11^{159} = 11^{15+24\cdot 6} = 11^{15}\cdot\left(11^{24}\right)^6 \equiv 11^{15} \pmod{35}$ porque $11^{24} \equiv 1 \pmod{35}$ por la Fórmula de Euler.
Para calcular $11^{15} \pmod{35}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
11^{15} &\equiv 11{\cdot}11^{14} \equiv 11{\cdot}\left(11^2\right)^7 \equiv 11{\cdot}16^7 && \text{(Porque } 11^2 \equiv 16 \pmod{35}\text{)}\\
&\equiv 11\cdot 16{\cdot}16^6 \equiv 11\cdot 16{\cdot}\left(16^2\right)^3 \equiv 11\cdot 16{\cdot}11^3 && \text{(Porque } 16^2 \equiv 11 \pmod{35}\text{)}\\
&\equiv 11\cdot 16\cdot 11{\cdot}11^2 \equiv 11\cdot 16\cdot 11{\cdot}\left(11^2\right)^1 \equiv 11\cdot 16\cdot 11{\cdot}16^1 && \text{(Porque } 11^2 \equiv 16 \pmod{35}\text{)}\\
&\equiv 1\cdot 11\cdot 16 && \text{(Porque } 11\cdot 16 \equiv 1 \pmod{35}\text{)}\\
&\equiv 11\cdot 16 && \text{(Porque } 1\cdot 11 \equiv 11 \pmod{35}\text{)}\\
&\equiv 1 && \text{(Porque } 11\cdot 16 \equiv 1 \pmod{35}\text{)}
\end{aligned}$$

◊

Ejercicio 16. *Calcula* $40^{262} \pmod{49}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $49 = 7^2$, entonces aplicamos la fórmula y tenemos que $\varphi(49) = \varphi(7^2) = (7^2 - 7^1) = 42$. Esto nos deja $40^{262} = 40^{10+42\cdot 6} = 40^{10}\cdot\left(40^{42}\right)^6 \equiv 40^{10} \pmod{49}$ porque $40^{42} \equiv 1 \pmod{49}$ por la Fórmula de Euler.
Para calcular $40^{10} \pmod{49}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
40^{10} &\equiv 40^{10} \equiv \left(40^2\right)^5 \equiv 32^5 && \text{(Porque } 40^2 \equiv 32 \pmod{49}\text{)}\\
&\equiv 32{\cdot}32^4 \equiv 32{\cdot}\left(32^2\right)^2 \equiv 32{\cdot}44^2 && \text{(Porque } 32^2 \equiv 44 \pmod{49}\text{)}\\
&\equiv 32{\cdot}44^2 \equiv 32{\cdot}\left(44^2\right)^1 \equiv 32{\cdot}25^1 && \text{(Porque } 44^2 \equiv 25 \pmod{49}\text{)}\\
&\equiv 16 && \text{(Porque } 32\cdot 25 \equiv 16 \pmod{49}\text{)}
\end{aligned}$$

◊

Ejercicio 17. *Calcula* $28^{53} \pmod{43}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 43 es primo, tendremos que $\varphi(43) = 43 - 1 = 42$. Esto nos deja $28^{53} = 28^{11+42\cdot 1} = 28^{11} \cdot \left(28^{42}\right)^1 \equiv 28^{11} \pmod{43}$ porque $28^{42} \equiv 1 \pmod{43}$ por la Fórmula de Euler.
Para calcular $28^{11} \pmod{43}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
28^{11} &\equiv 28{\cdot}28^{10} \equiv 28{\cdot} \left(28^2\right)^5 \equiv 28{\cdot}10^5 && \text{(Porque } 28^2 \equiv 10 \pmod{43}\text{)}\\
&\equiv 28 \cdot 10{\cdot}10^4 \equiv 28 \cdot 10{\cdot} \left(10^2\right)^2 \equiv 28 \cdot 10{\cdot}14^2 && \text{(Porque } 10^2 \equiv 14 \pmod{43}\text{)}\\
&\equiv 28 \cdot 10{\cdot}14^2 \equiv 28 \cdot 10{\cdot} \left(14^2\right)^1 \equiv 28 \cdot 10{\cdot}24^1 && \text{(Porque } 14^2 \equiv 24 \pmod{43}\text{)}\\
&\equiv 22 \cdot 24 && \text{(Porque } 28 \cdot 10 \equiv 22 \pmod{43}\text{)}\\
&\equiv 12 && \text{(Porque } 22 \cdot 24 \equiv 12 \pmod{43}\text{)}
\end{aligned}$$

◊

Ejercicio 18. *Calcula* $19^{137} \pmod{44}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $44 = 2^2 \cdot 11$, entonces aplicamos la fórmula y tenemos que $\varphi(44) = \varphi(2^2 \cdot 11) = \varphi(2^2) \cdot \varphi(11^1) = (2^2 - 2^1) \cdot (11^1 - 11^0) = 20$. Esto nos deja $19^{137} = 19^{17+20\cdot 6} = 19^{17} \cdot \left(19^{20}\right)^6 \equiv 19^{17} \pmod{44}$ porque $19^{20} \equiv 1 \pmod{44}$ por la Fórmula de Euler.
Para calcular $19^{17} \pmod{44}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
19^{17} &\equiv 19{\cdot}19^{16} \equiv 19{\cdot} \left(19^2\right)^8 \equiv 19{\cdot}9^8 && \text{(Porque } 19^2 \equiv 9 \pmod{44}\text{)}\\
&\equiv 19{\cdot}9^8 \equiv 19{\cdot} \left(9^2\right)^4 \equiv 19{\cdot}37^4 && \text{(Porque } 9^2 \equiv 37 \pmod{44}\text{)}\\
&\equiv 19{\cdot}37^4 \equiv 19{\cdot} \left(37^2\right)^2 \equiv 19{\cdot}5^2 && \text{(Porque } 37^2 \equiv 5 \pmod{44}\text{)}\\
&\equiv 19{\cdot}5^2 \equiv 19{\cdot} \left(5^2\right)^1 \equiv 19{\cdot}25^1 && \text{(Porque } 5^2 \equiv 25 \pmod{44}\text{)}\\
&\equiv 35 && \text{(Porque } 19 \cdot 25 \equiv 35 \pmod{44}\text{)}
\end{aligned}$$

◊

Ejercicio 19. *Calcula* $30^{94} \pmod{33}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $30^{94} \pmod{33}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo

paso a paso:

$$\begin{aligned}
30^{94} &\equiv 30^{94} \equiv \left(30^2\right)^{47} \equiv 9^{47} && (\text{Porque } 30^2 \equiv 9 \pmod{33})\\
&\equiv 9{\cdot}9^{46} \equiv 9{\cdot} \left(9^2\right)^{23} \equiv 9{\cdot}15^{23} && (\text{Porque } 9^2 \equiv 15 \pmod{33})\\
&\equiv 9 \cdot 15{\cdot}15^{22} \equiv 9 \cdot 15{\cdot} \left(15^2\right)^{11} \equiv 9 \cdot 15{\cdot}27^{11} && (\text{Porque } 15^2 \equiv 27 \pmod{33})\\
&\equiv 9 \cdot 15 \cdot 27{\cdot}27^{10} \equiv 9 \cdot 15 \cdot 27{\cdot} \left(27^2\right)^{5} \equiv 9 \cdot 15 \cdot 27{\cdot}3^{5} && (\text{Porque } 27^2 \equiv 3 \pmod{33})\\
&\equiv 9 \cdot 15 \cdot 27 \cdot 3{\cdot}3^{4} \equiv 9 \cdot 15 \cdot 27 \cdot 3{\cdot} \left(3^2\right)^{2} \equiv 9 \cdot 15 \cdot 27 \cdot 3{\cdot}9^{2} && (\text{Porque } 3^2 \equiv 9 \pmod{33})\\
&\equiv 9 \cdot 15 \cdot 27 \cdot 3{\cdot}9^{2} \equiv 9 \cdot 15 \cdot 27 \cdot 3{\cdot} \left(9^2\right)^{1} \equiv 9 \cdot 15 \cdot 27 \cdot 3{\cdot}15^{1} && (\text{Porque } 9^2 \equiv 15 \pmod{33})\\
&\equiv 3 \cdot 27 \cdot 3 \cdot 15 && (\text{Porque } 9 \cdot 15 \equiv 3 \pmod{33})\\
&\equiv 15 \cdot 3 \cdot 15 && (\text{Porque } 3 \cdot 27 \equiv 15 \pmod{33})\\
&\equiv 12 \cdot 15 && (\text{Porque } 15 \cdot 3 \equiv 12 \pmod{33})\\
&\equiv 15 && (\text{Porque } 12 \cdot 15 \equiv 15 \pmod{33})
\end{aligned}$$

$\Diamond$

Ejercicio 20. *Calcula* $30^{131} \pmod{39}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $30^{131} \pmod{39}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
30^{131} &\equiv 30{\cdot}30^{130} \equiv 30{\cdot} \left(30^2\right)^{65} \equiv 30{\cdot}3^{65} && (\text{Porque } 30^2 \equiv 3 \pmod{39})\\
&\equiv 30 \cdot 3{\cdot}3^{64} \equiv 30 \cdot 3{\cdot} \left(3^2\right)^{32} \equiv 30 \cdot 3{\cdot}9^{32} && (\text{Porque } 3^2 \equiv 9 \pmod{39})\\
&\equiv 30 \cdot 3{\cdot}9^{32} \equiv 30 \cdot 3{\cdot} \left(9^2\right)^{16} \equiv 30 \cdot 3{\cdot}3^{16} && (\text{Porque } 9^2 \equiv 3 \pmod{39})\\
&\equiv 30 \cdot 3{\cdot}3^{16} \equiv 30 \cdot 3{\cdot} \left(3^2\right)^{8} \equiv 30 \cdot 3{\cdot}9^{8} && (\text{Porque } 3^2 \equiv 9 \pmod{39})\\
&\equiv 30 \cdot 3{\cdot}9^{8} \equiv 30 \cdot 3{\cdot} \left(9^2\right)^{4} \equiv 30 \cdot 3{\cdot}3^{4} && (\text{Porque } 9^2 \equiv 3 \pmod{39})\\
&\equiv 30 \cdot 3{\cdot}3^{4} \equiv 30 \cdot 3{\cdot} \left(3^2\right)^{2} \equiv 30 \cdot 3{\cdot}9^{2} && (\text{Porque } 3^2 \equiv 9 \pmod{39})\\
&\equiv 30 \cdot 3{\cdot}9^{2} \equiv 30 \cdot 3{\cdot} \left(9^2\right)^{1} \equiv 30 \cdot 3{\cdot}3^{1} && (\text{Porque } 9^2 \equiv 3 \pmod{39})\\
&\equiv 12 \cdot 3 && (\text{Porque } 30 \cdot 3 \equiv 12 \pmod{39})\\
&\equiv 36 && (\text{Porque } 12 \cdot 3 \equiv 36 \pmod{39})
\end{aligned}$$

$\Diamond$

Ejercicio 21. *Calcula* $16^{159} \pmod{45}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $45 = 3^2 \cdot 5$, entonces aplicamos la fórmula y tenemos que $\varphi(45) = \varphi(3^2 \cdot 5) = \varphi(3^2) \cdot \varphi(5^1) = (3^2 - 3^1) \cdot (5^1 - 5^0) = 24$. Esto nos deja $16^{159} = 16^{15+24\cdot 6} = 16^{15} \cdot \left(16^{24}\right)^6 \equiv 16^{15} \pmod{45}$ porque $16^{24} \equiv 1 \pmod{45}$ por la Fórmula de Euler.

Para calcular $16^{15} \pmod{45}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor

cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
16^{15} &\equiv 16{\cdot}16^{14} \equiv 16{\cdot}\left(16^2\right)^7 \equiv 16{\cdot}31^7 && (\text{Porque } 16^2 \equiv 31 \pmod{45})\\
&\equiv 16\cdot 31{\cdot}31^6 \equiv 16\cdot 31{\cdot}\left(31^2\right)^3 \equiv 16\cdot 31{\cdot}16^3 && (\text{Porque } 31^2 \equiv 16 \pmod{45})\\
&\equiv 16\cdot 31\cdot 16{\cdot}16^2 \equiv 16\cdot 31\cdot 16{\cdot}\left(16^2\right)^1 \equiv 16\cdot 31\cdot 16{\cdot}31^1 && (\text{Porque } 16^2 \equiv 31 \pmod{45})\\
&\equiv 1\cdot 16\cdot 31 && (\text{Porque } 16\cdot 31 \equiv 1 \pmod{45})\\
&\equiv 16\cdot 31 && (\text{Porque } 1\cdot 16 \equiv 16 \pmod{45})\\
&\equiv 1 && (\text{Porque } 16\cdot 31 \equiv 1 \pmod{45})
\end{aligned}$$

$\Diamond$

Ejercicio 22. *Calcula* $16^{73} \pmod{38}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $16^{73} \pmod{38}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
16^{73} &\equiv 16{\cdot}16^{72} \equiv 16{\cdot}\left(16^2\right)^{36} \equiv 16{\cdot}28^{36} && (\text{Porque } 16^2 \equiv 28 \pmod{38})\\
&\equiv 16{\cdot}28^{36} \equiv 16{\cdot}\left(28^2\right)^{18} \equiv 16{\cdot}24^{18} && (\text{Porque } 28^2 \equiv 24 \pmod{38})\\
&\equiv 16{\cdot}24^{18} \equiv 16{\cdot}\left(24^2\right)^{9} \equiv 16{\cdot}6^{9} && (\text{Porque } 24^2 \equiv 6 \pmod{38})\\
&\equiv 16\cdot 6{\cdot}6^8 \equiv 16\cdot 6{\cdot}\left(6^2\right)^4 \equiv 16\cdot 6{\cdot}36^4 && (\text{Porque } 6^2 \equiv 36 \pmod{38})\\
&\equiv 16\cdot 6{\cdot}36^4 \equiv 16\cdot 6{\cdot}\left(36^2\right)^2 \equiv 16\cdot 6{\cdot}4^2 && (\text{Porque } 36^2 \equiv 4 \pmod{38})\\
&\equiv 16\cdot 6{\cdot}4^2 \equiv 16\cdot 6{\cdot}\left(4^2\right)^1 \equiv 16\cdot 6{\cdot}16^1 && (\text{Porque } 4^2 \equiv 16 \pmod{38})\\
&\equiv 20\cdot 16 && (\text{Porque } 16\cdot 6 \equiv 20 \pmod{38})\\
&\equiv 16 && (\text{Porque } 20\cdot 16 \equiv 16 \pmod{38})
\end{aligned}$$

$\Diamond$

Ejercicio 23. *Calcula* $23^{292} \pmod{47}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 47 es primo, tendremos que $\varphi(47) = 47 - 1 = 46$. Esto nos deja $23^{292} = 23^{16+46\cdot 6} = 23^{16}\cdot\left(23^{46}\right)^6 \equiv 23^{16} \pmod{47}$ porque $23^{46} \equiv 1 \pmod{47}$ por la Fórmula de Euler.
Para calcular $23^{16} \pmod{47}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
23^{16} &\equiv 23^{16} \equiv \left(23^2\right)^8 \equiv 12^8 && (\text{Porque } 23^2 \equiv 12 \pmod{47})\\
&\equiv 12^8 \equiv \left(12^2\right)^4 \equiv 3^4 && (\text{Porque } 12^2 \equiv 3 \pmod{47})\\
&\equiv 3^4 \equiv \left(3^2\right)^2 \equiv 9^2 && (\text{Porque } 3^2 \equiv 9 \pmod{47})\\
&\equiv 9^2 \equiv \left(9^2\right)^1 \equiv 34^1 && (\text{Porque } 9^2 \equiv 34 \pmod{47})\\
&\equiv 34 \pmod{47}.
\end{aligned}$$

$\Diamond$

Ejercicio 24. *Calcula* $39^{36} \pmod{46}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $46 = 2 \cdot 23$, entonces aplicamos la fórmula y tenemos que $\varphi(46) = \varphi(2 \cdot 23) = \varphi(2^1) \cdot \varphi(23^1) = (2^1 - 2^0) \cdot (23^1 - 23^0) = 22$. Esto nos deja $39^{36} = 39^{14+22\cdot 1} = 39^{14} \cdot \left(39^{22}\right)^1 \equiv 39^{14} \pmod{46}$ porque $39^{22} \equiv 1 \pmod{46}$ por la Fórmula de Euler.
Para calcular $39^{14} \pmod{46}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
39^{14} &\equiv 39^{14} \equiv \left(39^2\right)^7 \equiv 3^7 && (\text{Porque } 39^2 \equiv 3 \pmod{46}) \\
&\equiv 3{\cdot}3^6 \equiv 3{\cdot} \left(3^2\right)^3 \equiv 3{\cdot}9^3 && (\text{Porque } 3^2 \equiv 9 \pmod{46}) \\
&\equiv 3 \cdot 9{\cdot}9^2 \equiv 3 \cdot 9{\cdot} \left(9^2\right)^1 \equiv 3 \cdot 9{\cdot}35^1 && (\text{Porque } 9^2 \equiv 35 \pmod{46}) \\
&\equiv 27 \cdot 35 && (\text{Porque } 3 \cdot 9 \equiv 27 \pmod{46}) \\
&\equiv 25 && (\text{Porque } 27 \cdot 35 \equiv 25 \pmod{46})
\end{aligned}$$

$\Diamond$

Ejercicio 25. *Calcula* $40^{178} \pmod{43}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 43 es primo, tendremos que $\varphi(43) = 43 - 1 = 42$. Esto nos deja $40^{178} = 40^{10+42\cdot 4} = 40^{10} \cdot \left(40^{42}\right)^4 \equiv 40^{10} \pmod{43}$ porque $40^{42} \equiv 1 \pmod{43}$ por la Fórmula de Euler.
Para calcular $40^{10} \pmod{43}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
40^{10} &\equiv 40^{10} \equiv \left(40^2\right)^5 \equiv 9^5 && (\text{Porque } 40^2 \equiv 9 \pmod{43}) \\
&\equiv 9{\cdot}9^4 \equiv 9{\cdot} \left(9^2\right)^2 \equiv 9{\cdot}38^2 && (\text{Porque } 9^2 \equiv 38 \pmod{43}) \\
&\equiv 9{\cdot}38^2 \equiv 9{\cdot} \left(38^2\right)^1 \equiv 9{\cdot}25^1 && (\text{Porque } 38^2 \equiv 25 \pmod{43}) \\
&\equiv 10 && (\text{Porque } 9 \cdot 25 \equiv 10 \pmod{43})
\end{aligned}$$

$\Diamond$

Ejercicio 26. *Calcula* $34^{231} \pmod{37}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 37 es primo, tendremos que $\varphi(37) = 37 - 1 = 36$. Esto nos deja $34^{231} = 34^{15+36\cdot 6} = 34^{15} \cdot \left(34^{36}\right)^6 \equiv 34^{15} \pmod{37}$ porque $34^{36} \equiv 1 \pmod{37}$ por la Fórmula de Euler.
Para calcular $34^{15} \pmod{37}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor

cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
34^{15} &\equiv 34{\cdot}34^{14} \equiv 34{\cdot}\left(34^2\right)^7 \equiv 34{\cdot}9^7 && \text{(Porque } 34^2 \equiv 9 \pmod{37})\\
&\equiv 34\cdot 9{\cdot}9^6 \equiv 34\cdot 9{\cdot}\left(9^2\right)^3 \equiv 34\cdot 9{\cdot}7^3 && \text{(Porque } 9^2 \equiv 7 \pmod{37})\\
&\equiv 34\cdot 9\cdot 7{\cdot}7^2 \equiv 34\cdot 9\cdot 7{\cdot}\left(7^2\right)^1 \equiv 34\cdot 9\cdot 7{\cdot}12^1 && \text{(Porque } 7^2 \equiv 12 \pmod{37})\\
&\equiv 10\cdot 7\cdot 12 && \text{(Porque } 34\cdot 9 \equiv 10 \pmod{37})\\
&\equiv 33\cdot 12 && \text{(Porque } 10\cdot 7 \equiv 33 \pmod{37})\\
&\equiv 26 && \text{(Porque } 33\cdot 12 \equiv 26 \pmod{37})
\end{aligned}$$

♢

Ejercicio 27. *Calcula* $28^{178} \pmod{41}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 41 es primo, tendremos que $\varphi(41) = 41 - 1 = 40$. Esto nos deja $28^{178} = 28^{18+40\cdot 4} = 28^{18}\cdot\left(28^{40}\right)^4 \equiv 28^{18} \pmod{41}$ porque $28^{40} \equiv 1 \pmod{41}$ por la Fórmula de Euler.
Para calcular $28^{18} \pmod{41}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
28^{18} &\equiv 28^{18} \equiv \left(28^2\right)^9 \equiv 5^9 && \text{(Porque } 28^2 \equiv 5 \pmod{41})\\
&\equiv 5{\cdot}5^8 \equiv 5{\cdot}\left(5^2\right)^4 \equiv 5{\cdot}25^4 && \text{(Porque } 5^2 \equiv 25 \pmod{41})\\
&\equiv 5{\cdot}25^4 \equiv 5{\cdot}\left(25^2\right)^2 \equiv 5{\cdot}10^2 && \text{(Porque } 25^2 \equiv 10 \pmod{41})\\
&\equiv 5{\cdot}10^2 \equiv 5{\cdot}\left(10^2\right)^1 \equiv 5{\cdot}18^1 && \text{(Porque } 10^2 \equiv 18 \pmod{41})\\
&\equiv 8 && \text{(Porque } 5\cdot 18 \equiv 8 \pmod{41})
\end{aligned}$$

♢

Ejercicio 28. *Calcula* $22^{145} \pmod{49}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $49 = 7^2$, entonces aplicamos la fórmula y tenemos que $\varphi(49) = \varphi(7^2) = (7^2 - 7^1) = 42$. Esto nos deja $22^{145} = 22^{19+42\cdot 3} = 22^{19}\cdot\left(22^{42}\right)^3 \equiv 22^{19} \pmod{49}$ porque $22^{42} \equiv 1 \pmod{49}$ por la Fórmula de Euler.
Para calcular $22^{19} \pmod{49}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
22^{19} &\equiv 22{\cdot}22^{18} \equiv 22{\cdot}\left(22^2\right)^9 \equiv 22{\cdot}43^9 && \text{(Porque } 22^2 \equiv 43 \pmod{49})\\
&\equiv 22\cdot 43{\cdot}43^8 \equiv 22\cdot 43{\cdot}\left(43^2\right)^4 \equiv 22\cdot 43{\cdot}36^4 && \text{(Porque } 43^2 \equiv 36 \pmod{49})\\
&\equiv 22\cdot 43{\cdot}36^4 \equiv 22\cdot 43{\cdot}\left(36^2\right)^2 \equiv 22\cdot 43{\cdot}22^2 && \text{(Porque } 36^2 \equiv 22 \pmod{49})\\
&\equiv 22\cdot 43{\cdot}22^2 \equiv 22\cdot 43{\cdot}\left(22^2\right)^1 \equiv 22\cdot 43{\cdot}43^1 && \text{(Porque } 22^2 \equiv 43 \pmod{49})\\
&\equiv 15\cdot 43 && \text{(Porque } 22\cdot 43 \equiv 15 \pmod{49})\\
&\equiv 8 && \text{(Porque } 15\cdot 43 \equiv 8 \pmod{49})
\end{aligned}$$

♢

Ejercicio 29. *Calcula* $42^{32} \pmod{46}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $42^{32} \pmod{46}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
42^{32} &\equiv 42^{32} \equiv \left(42^2\right)^{16} \equiv 16^{16} && (\text{Porque } 42^2 \equiv 16 \pmod{46})\\
&\equiv 16^{16} \equiv \left(16^2\right)^{8} \equiv 26^{8} && (\text{Porque } 16^2 \equiv 26 \pmod{46})\\
&\equiv 26^{8} \equiv \left(26^2\right)^{4} \equiv 32^{4} && (\text{Porque } 26^2 \equiv 32 \pmod{46})\\
&\equiv 32^{4} \equiv \left(32^2\right)^{2} \equiv 12^{2} && (\text{Porque } 32^2 \equiv 12 \pmod{46})\\
&\equiv 12^{2} \equiv \left(12^2\right)^{1} \equiv 6^{1} && (\text{Porque } 12^2 \equiv 6 \pmod{46})\\
&\equiv 6 \pmod{46}.
\end{aligned}$$

♢

Ejercicio 30. *Calcula* $16^{57} \pmod{49}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $49 = 7^2$, entonces aplicamos la fórmula y tenemos que $\varphi(49) = \varphi(7^2) = (7^2 - 7^1) = 42$. Esto nos deja $16^{57} = 16^{15+42\cdot 1} = 16^{15} \cdot \left(16^{42}\right)^1 \equiv 16^{15} \pmod{49}$ porque $16^{42} \equiv 1 \pmod{49}$ por la Fórmula de Euler.
Para calcular $16^{15} \pmod{49}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
16^{15} &\equiv 16{\cdot}16^{14} \equiv 16{\cdot} \left(16^2\right)^{7} \equiv 16{\cdot}11^{7} && (\text{Porque } 16^2 \equiv 11 \pmod{49})\\
&\equiv 16 \cdot 11{\cdot}11^{6} \equiv 16 \cdot 11{\cdot} \left(11^2\right)^{3} \equiv 16 \cdot 11{\cdot}23^{3} && (\text{Porque } 11^2 \equiv 23 \pmod{49})\\
&\equiv 16 \cdot 11 \cdot 23{\cdot}23^{2} \equiv 16 \cdot 11 \cdot 23{\cdot} \left(23^2\right)^{1} \equiv 16 \cdot 11 \cdot 23{\cdot}39^{1} && (\text{Porque } 23^2 \equiv 39 \pmod{49})\\
&\equiv 29 \cdot 23 \cdot 39 && (\text{Porque } 16 \cdot 11 \equiv 29 \pmod{49})\\
&\equiv 30 \cdot 39 && (\text{Porque } 29 \cdot 23 \equiv 30 \pmod{49})\\
&\equiv 43 && (\text{Porque } 30 \cdot 39 \equiv 43 \pmod{49})
\end{aligned}$$

♢

Ejercicio 31. *Calcula* $38^{111} \pmod{45}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $45 = 3^2 \cdot 5$, entonces aplicamos la fórmula y tenemos que $\varphi(45) = \varphi(3^2 \cdot 5) = \varphi(3^2) \cdot \varphi(5^1) = (3^2 - 3^1) \cdot (5^1 - 5^0) = 24$. Esto nos deja $38^{111} = 38^{15+24\cdot 4} = 38^{15} \cdot \left(38^{24}\right)^4 \equiv 38^{15} \pmod{45}$ porque $38^{24} \equiv 1 \pmod{45}$ por la Fórmula de Euler.
Para calcular $38^{15} \pmod{45}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor

cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
38^{15} &\equiv 38{\cdot}38^{14} \equiv 38{\cdot}\left(38^2\right)^7 \equiv 38{\cdot}4^7 && (\text{Porque } 38^2 \equiv 4 \pmod{45})\\
&\equiv 38\cdot 4{\cdot}4^6 \equiv 38\cdot 4{\cdot}\left(4^2\right)^3 \equiv 38\cdot 4{\cdot}16^3 && (\text{Porque } 4^2 \equiv 16 \pmod{45})\\
&\equiv 38\cdot 4\cdot 16{\cdot}16^2 \equiv 38\cdot 4\cdot 16{\cdot}\left(16^2\right)^1 \equiv 38\cdot 4\cdot 16{\cdot}31^1 && (\text{Porque } 16^2 \equiv 31 \pmod{45})\\
&\equiv 17\cdot 16\cdot 31 && (\text{Porque } 38\cdot 4 \equiv 17 \pmod{45})\\
&\equiv 2\cdot 31 && (\text{Porque } 17\cdot 16 \equiv 2 \pmod{45})\\
&\equiv 17 && (\text{Porque } 2\cdot 31 \equiv 17 \pmod{45})
\end{aligned}$$

$\Diamond$

Ejercicio 32. *Calcula* $24^{245} \pmod{47}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 47 es primo, tendremos que $\varphi(47) = 47 - 1 = 46$. Esto nos deja $24^{245} = 24^{15+46\cdot 5} = 24^{15}\cdot\left(24^{46}\right)^5 \equiv 24^{15} \pmod{47}$ porque $24^{46} \equiv 1 \pmod{47}$ por la Fórmula de Euler.
Para calcular $24^{15} \pmod{47}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
24^{15} &\equiv 24{\cdot}24^{14} \equiv 24{\cdot}\left(24^2\right)^7 \equiv 24{\cdot}12^7 && (\text{Porque } 24^2 \equiv 12 \pmod{47})\\
&\equiv 24\cdot 12{\cdot}12^6 \equiv 24\cdot 12{\cdot}\left(12^2\right)^3 \equiv 24\cdot 12{\cdot}3^3 && (\text{Porque } 12^2 \equiv 3 \pmod{47})\\
&\equiv 24\cdot 12\cdot 3{\cdot}3^2 \equiv 24\cdot 12\cdot 3{\cdot}\left(3^2\right)^1 \equiv 24\cdot 12\cdot 3{\cdot}9^1 && (\text{Porque } 3^2 \equiv 9 \pmod{47})\\
&\equiv 6\cdot 3\cdot 9 && (\text{Porque } 24\cdot 12 \equiv 6 \pmod{47})\\
&\equiv 18\cdot 9 && (\text{Porque } 6\cdot 3 \equiv 18 \pmod{47})\\
&\equiv 21 && (\text{Porque } 18\cdot 9 \equiv 21 \pmod{47})
\end{aligned}$$

$\Diamond$

Ejercicio 33. *Calcula* $33^{110} \pmod{35}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $35 = 5\cdot 7$, entonces aplicamos la fórmula y tenemos que $\varphi(35) = \varphi(5\cdot 7) = \varphi(5^1)\cdot\varphi(7^1) = (5^1 - 5^0)\cdot(7^1 - 7^0) = 24$. Esto nos deja $33^{110} = 33^{14+24\cdot 4} = 33^{14}\cdot\left(33^{24}\right)^4 \equiv 33^{14} \pmod{35}$ porque $33^{24} \equiv 1 \pmod{35}$ por la Fórmula de Euler.
Para calcular $33^{14} \pmod{35}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
33^{14} &\equiv 33^{14} \equiv \left(33^2\right)^7 \equiv 4^7 && (\text{Porque } 33^2 \equiv 4 \pmod{35})\\
&\equiv 4{\cdot}4^6 \equiv 4{\cdot}\left(4^2\right)^3 \equiv 4{\cdot}16^3 && (\text{Porque } 4^2 \equiv 16 \pmod{35})\\
&\equiv 4\cdot 16{\cdot}16^2 \equiv 4\cdot 16{\cdot}\left(16^2\right)^1 \equiv 4\cdot 16{\cdot}11^1 && (\text{Porque } 16^2 \equiv 11 \pmod{35})\\
&\equiv 29\cdot 11 && (\text{Porque } 4\cdot 16 \equiv 29 \pmod{35})\\
&\equiv 4 && (\text{Porque } 29\cdot 11 \equiv 4 \pmod{35})
\end{aligned}$$

$\Diamond$

Ejercicio 34. *Calcula* $22^{49} \pmod{31}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 31 es primo, tendremos que $\varphi(31) = 31 - 1 = 30$. Esto nos deja $22^{49} = 22^{19+30\cdot 1} = 22^{19} \cdot \left(22^{30}\right)^1 \equiv 22^{19} \pmod{31}$ porque $22^{30} \equiv 1 \pmod{31}$ por la Fórmula de Euler.
Para calcular $22^{19} \pmod{31}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
22^{19} &\equiv 22{\cdot}22^{18} \equiv 22{\cdot} \left(22^2\right)^9 \equiv 22{\cdot}19^9 && (\text{Porque } 22^2 \equiv 19 \pmod{31}) \\
&\equiv 22 \cdot 19{\cdot}19^8 \equiv 22 \cdot 19{\cdot} \left(19^2\right)^4 \equiv 22 \cdot 19{\cdot}20^4 && (\text{Porque } 19^2 \equiv 20 \pmod{31}) \\
&\equiv 22 \cdot 19{\cdot}20^4 \equiv 22 \cdot 19{\cdot} \left(20^2\right)^2 \equiv 22 \cdot 19{\cdot}28^2 && (\text{Porque } 20^2 \equiv 28 \pmod{31}) \\
&\equiv 22 \cdot 19{\cdot}28^2 \equiv 22 \cdot 19{\cdot} \left(28^2\right)^1 \equiv 22 \cdot 19{\cdot}9^1 && (\text{Porque } 28^2 \equiv 9 \pmod{31}) \\
&\equiv 15 \cdot 9 && (\text{Porque } 22 \cdot 19 \equiv 15 \pmod{31}) \\
&\equiv 11 && (\text{Porque } 15 \cdot 9 \equiv 11 \pmod{31})
\end{aligned}$$

♢

Ejercicio 35. *Calcula* $43^{90} \pmod{45}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $45 = 3^2 \cdot 5$, entonces aplicamos la fórmula y tenemos que $\varphi(45) = \varphi(3^2 \cdot 5) = \varphi(3^2) \cdot \varphi(5^1) = (3^2 - 3^1) \cdot (5^1 - 5^0) = 24$. Esto nos deja $43^{90} = 43^{18+24\cdot 3} = 43^{18} \cdot \left(43^{24}\right)^3 \equiv 43^{18} \pmod{45}$ porque $43^{24} \equiv 1 \pmod{45}$ por la Fórmula de Euler.
Para calcular $43^{18} \pmod{45}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
43^{18} &\equiv 43^{18} \equiv \left(43^2\right)^9 \equiv 4^9 && (\text{Porque } 43^2 \equiv 4 \pmod{45}) \\
&\equiv 4{\cdot}4^8 \equiv 4{\cdot} \left(4^2\right)^4 \equiv 4{\cdot}16^4 && (\text{Porque } 4^2 \equiv 16 \pmod{45}) \\
&\equiv 4{\cdot}16^4 \equiv 4{\cdot} \left(16^2\right)^2 \equiv 4{\cdot}31^2 && (\text{Porque } 16^2 \equiv 31 \pmod{45}) \\
&\equiv 4{\cdot}31^2 \equiv 4{\cdot} \left(31^2\right)^1 \equiv 4{\cdot}16^1 && (\text{Porque } 31^2 \equiv 16 \pmod{45}) \\
&\equiv 19 && (\text{Porque } 4 \cdot 16 \equiv 19 \pmod{45})
\end{aligned}$$

♢

Ejercicio 36. *Calcula* $13^{25} \pmod{36}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $36 = 2^2 \cdot 3^2$, entonces aplicamos la fórmula y tenemos que $\varphi(36) = \varphi(2^2 \cdot 3^2) = \varphi(2^2) \cdot \varphi(3^2) = (2^2 - 2^1) \cdot (3^2 - 3^1) = 12$. Esto nos deja $13^{25} = 13^{1+12\cdot 2} = 13^1 \cdot \left(13^{12}\right)^2 \equiv 13^1 \pmod{36}$ porque $13^{12} \equiv 1 \pmod{36}$ por la Fórmula de Euler.
Para calcular $13^1 \pmod{36}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$13^1 \equiv 13 \pmod{36}.$$

♢

Ejercicio 37. *Calcula* $25^{85} \pmod{37}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 37 es primo, tendremos que $\varphi(37) = 37 - 1 = 36$. Esto nos deja $25^{85} = 25^{13+36\cdot 2} = 25^{13} \cdot \left(25^{36}\right)^2 \equiv 25^{13} \pmod{37}$ porque $25^{36} \equiv 1 \pmod{37}$ por la Fórmula de Euler.
Para calcular $25^{13} \pmod{37}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
25^{13} &\equiv 25{\cdot}25^{12} \equiv 25{\cdot} \left(25^2\right)^6 \equiv 25{\cdot}33^6 && (\text{Porque } 25^2 \equiv 33 \pmod{37})\\
&\equiv 25{\cdot}33^6 \equiv 25{\cdot} \left(33^2\right)^3 \equiv 25{\cdot}16^3 && (\text{Porque } 33^2 \equiv 16 \pmod{37})\\
&\equiv 25 \cdot 16{\cdot}16^2 \equiv 25 \cdot 16{\cdot} \left(16^2\right)^1 \equiv 25 \cdot 16{\cdot}34^1 && (\text{Porque } 16^2 \equiv 34 \pmod{37})\\
&\equiv 30 \cdot 34 && (\text{Porque } 25 \cdot 16 \equiv 30 \pmod{37})\\
&\equiv 21 && (\text{Porque } 30 \cdot 34 \equiv 21 \pmod{37})
\end{aligned}$$

♢

Ejercicio 38. *Calcula* $10^{232} \pmod{37}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 37 es primo, tendremos que $\varphi(37) = 37 - 1 = 36$. Esto nos deja $10^{232} = 10^{16+36\cdot 6} = 10^{16} \cdot \left(10^{36}\right)^6 \equiv 10^{16} \pmod{37}$ porque $10^{36} \equiv 1 \pmod{37}$ por la Fórmula de Euler.
Para calcular $10^{16} \pmod{37}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
10^{16} &\equiv 10^{16} \equiv \left(10^2\right)^8 \equiv 26^8 && (\text{Porque } 10^2 \equiv 26 \pmod{37})\\
&\equiv 26^8 \equiv \left(26^2\right)^4 \equiv 10^4 && (\text{Porque } 26^2 \equiv 10 \pmod{37})\\
&\equiv 10^4 \equiv \left(10^2\right)^2 \equiv 26^2 && (\text{Porque } 10^2 \equiv 26 \pmod{37})\\
&\equiv 26^2 \equiv \left(26^2\right)^1 \equiv 10^1 && (\text{Porque } 26^2 \equiv 10 \pmod{37})\\
&\equiv 10 \pmod{37}.
\end{aligned}$$

♢

Ejercicio 39. *Calcula* $10^{80} \pmod{46}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $10^{80} \pmod{46}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
10^{80} &\equiv 10^{80} \equiv \left(10^2\right)^{40} \equiv 8^{40} && (\text{Porque } 10^2 \equiv 8 \pmod{46})\\
&\equiv 8^{40} \equiv \left(8^2\right)^{20} \equiv 18^{20} && (\text{Porque } 8^2 \equiv 18 \pmod{46})\\
&\equiv 18^{20} \equiv \left(18^2\right)^{10} \equiv 2^{10} && (\text{Porque } 18^2 \equiv 2 \pmod{46})\\
&\equiv 2^{10} \equiv \left(2^2\right)^5 \equiv 4^5 && (\text{Porque } 2^2 \equiv 4 \pmod{46})\\
&\equiv 4{\cdot}4^4 \equiv 4{\cdot} \left(4^2\right)^2 \equiv 4{\cdot}16^2 && (\text{Porque } 4^2 \equiv 16 \pmod{46})\\
&\equiv 4{\cdot}16^2 \equiv 4{\cdot} \left(16^2\right)^1 \equiv 4{\cdot}26^1 && (\text{Porque } 16^2 \equiv 26 \pmod{46})\\
&\equiv 12 && (\text{Porque } 4 \cdot 26 \equiv 12 \pmod{46})
\end{aligned}$$

$\diamondsuit$

Ejercicio 40. *Calcula* $13^{50} \pmod{33}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $33 = 3 \cdot 11$, entonces aplicamos la fórmula y tenemos que $\varphi(33) = \varphi(3 \cdot 11) = \varphi(3^1) \cdot \varphi(11^1) = (3^1 - 3^0) \cdot (11^1 - 11^0) = 20$. Esto nos deja $13^{50} = 13^{10+20\cdot 2} = 13^{10} \cdot \left(13^{20}\right)^2 \equiv 13^{10} \pmod{33}$ porque $13^{20} \equiv 1 \pmod{33}$ por la Fórmula de Euler.
Para calcular $13^{10} \pmod{33}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
13^{10} &\equiv 13^{10} \equiv \left(13^2\right)^5 \equiv 4^5 && (\text{Porque } 13^2 \equiv 4 \pmod{33}) \\
&\equiv 4{\cdot}4^4 \equiv 4{\cdot} \left(4^2\right)^2 \equiv 4{\cdot}16^2 && (\text{Porque } 4^2 \equiv 16 \pmod{33}) \\
&\equiv 4{\cdot}16^2 \equiv 4{\cdot} \left(16^2\right)^1 \equiv 4{\cdot}25^1 && (\text{Porque } 16^2 \equiv 25 \pmod{33}) \\
&\equiv 1 && (\text{Porque } 4 \cdot 25 \equiv 1 \pmod{33})
\end{aligned}$$

$\diamondsuit$

Ejercicio 41. *Calcula* $29^{190} \pmod{31}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 31 es primo, tendremos que $\varphi(31) = 31 - 1 = 30$. Esto nos deja $29^{190} = 29^{10+30\cdot 6} = 29^{10} \cdot \left(29^{30}\right)^6 \equiv 29^{10} \pmod{31}$ porque $29^{30} \equiv 1 \pmod{31}$ por la Fórmula de Euler.
Para calcular $29^{10} \pmod{31}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
29^{10} &\equiv 29^{10} \equiv \left(29^2\right)^5 \equiv 4^5 && (\text{Porque } 29^2 \equiv 4 \pmod{31}) \\
&\equiv 4{\cdot}4^4 \equiv 4{\cdot} \left(4^2\right)^2 \equiv 4{\cdot}16^2 && (\text{Porque } 4^2 \equiv 16 \pmod{31}) \\
&\equiv 4{\cdot}16^2 \equiv 4{\cdot} \left(16^2\right)^1 \equiv 4{\cdot}8^1 && (\text{Porque } 16^2 \equiv 8 \pmod{31}) \\
&\equiv 1 && (\text{Porque } 4 \cdot 8 \equiv 1 \pmod{31})
\end{aligned}$$

$\diamondsuit$

Ejercicio 42. *Calcula* $22^{107} \pmod{45}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $45 = 3^2 \cdot 5$, entonces aplicamos la fórmula y tenemos que $\varphi(45) = \varphi(3^2 \cdot 5) = \varphi(3^2) \cdot \varphi(5^1) = (3^2 - 3^1) \cdot (5^1 - 5^0) = 24$. Esto nos deja $22^{107} = 22^{11+24\cdot 4} = 22^{11} \cdot \left(22^{24}\right)^4 \equiv 22^{11} \pmod{45}$ porque $22^{24} \equiv 1 \pmod{45}$ por la Fórmula de Euler.
Para calcular $22^{11} \pmod{45}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor

cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
22^{11} &\equiv 22{\cdot}22^{10} \equiv 22{\cdot}\left(22^2\right)^5 \equiv 22{\cdot}34^5 && (\text{Porque } 22^2 \equiv 34 \pmod{45})\\
&\equiv 22\cdot 34{\cdot}34^4 \equiv 22\cdot 34{\cdot}\left(34^2\right)^2 \equiv 22\cdot 34{\cdot}31^2 && (\text{Porque } 34^2 \equiv 31 \pmod{45})\\
&\equiv 22\cdot 34{\cdot}31^2 \equiv 22\cdot 34{\cdot}\left(31^2\right)^1 \equiv 22\cdot 34{\cdot}16^1 && (\text{Porque } 31^2 \equiv 16 \pmod{45})\\
&\equiv 28\cdot 16 && (\text{Porque } 22\cdot 34 \equiv 28 \pmod{45})\\
&\equiv 43 && (\text{Porque } 28\cdot 16 \equiv 43 \pmod{45})
\end{aligned}$$

◊

Ejercicio 43. *Calcula* $27^{269} \pmod{43}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 43 es primo, tendremos que $\varphi(43) = 43 - 1 = 42$. Esto nos deja $27^{269} = 27^{17+42\cdot 6} = 27^{17}\cdot\left(27^{42}\right)^6 \equiv 27^{17} \pmod{43}$ porque $27^{42} \equiv 1 \pmod{43}$ por la Fórmula de Euler.
Para calcular $27^{17} \pmod{43}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
27^{17} &\equiv 27{\cdot}27^{16} \equiv 27{\cdot}\left(27^2\right)^8 \equiv 27{\cdot}41^8 && (\text{Porque } 27^2 \equiv 41 \pmod{43})\\
&\equiv 27{\cdot}41^8 \equiv 27{\cdot}\left(41^2\right)^4 \equiv 27{\cdot}4^4 && (\text{Porque } 41^2 \equiv 4 \pmod{43})\\
&\equiv 27{\cdot}4^4 \equiv 27{\cdot}\left(4^2\right)^2 \equiv 27{\cdot}16^2 && (\text{Porque } 4^2 \equiv 16 \pmod{43})\\
&\equiv 27{\cdot}16^2 \equiv 27{\cdot}\left(16^2\right)^1 \equiv 27{\cdot}41^1 && (\text{Porque } 16^2 \equiv 41 \pmod{43})\\
&\equiv 32 && (\text{Porque } 27\cdot 41 \equiv 32 \pmod{43})
\end{aligned}$$

◊

Ejercicio 44. *Calcula* $25^{88} \pmod{38}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $38 = 2\cdot 19$, entonces aplicamos la fórmula y tenemos que $\varphi(38) = \varphi(2\cdot 19) = \varphi(2^1)\cdot\varphi(19^1) = (2^1 - 2^0)\cdot(19^1 - 19^0) = 18$. Esto nos deja $25^{88} = 25^{16+18\cdot 4} = 25^{16}\cdot\left(25^{18}\right)^4 \equiv 25^{16} \pmod{38}$ porque $25^{18} \equiv 1 \pmod{38}$ por la Fórmula de Euler.
Para calcular $25^{16} \pmod{38}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
25^{16} &\equiv 25^{16} \equiv \left(25^2\right)^8 \equiv 17^8 && (\text{Porque } 25^2 \equiv 17 \pmod{38})\\
&\equiv 17^8 \equiv \left(17^2\right)^4 \equiv 23^4 && (\text{Porque } 17^2 \equiv 23 \pmod{38})\\
&\equiv 23^4 \equiv \left(23^2\right)^2 \equiv 35^2 && (\text{Porque } 23^2 \equiv 35 \pmod{38})\\
&\equiv 35^2 \equiv \left(35^2\right)^1 \equiv 9^1 && (\text{Porque } 35^2 \equiv 9 \pmod{38})\\
&\equiv 9 \pmod{38}.
\end{aligned}$$

◊

Ejercicio 45. *Calcula* $20^{41} \pmod{39}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $39 = 3 \cdot 13$, entonces aplicamos la fórmula y tenemos que $\varphi(39) = \varphi(3 \cdot 13) = \varphi(3^1) \cdot \varphi(13^1) = (3^1 - 3^0) \cdot (13^1 - 13^0) = 24$. Esto nos deja $20^{41} = 20^{17+24 \cdot 1} = 20^{17} \cdot \left(20^{24}\right)^1 \equiv 20^{17} \pmod{39}$ porque $20^{24} \equiv 1 \pmod{39}$ por la Fórmula de Euler.
Para calcular $20^{17} \pmod{39}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
20^{17} &\equiv 20 \cdot 20^{16} \equiv 20 \cdot \left(20^2\right)^8 \equiv 20 \cdot 10^8 && (\text{Porque } 20^2 \equiv 10 \pmod{39}) \\
&\equiv 20 \cdot 10^8 \equiv 20 \cdot \left(10^2\right)^4 \equiv 20 \cdot 22^4 && (\text{Porque } 10^2 \equiv 22 \pmod{39}) \\
&\equiv 20 \cdot 22^4 \equiv 20 \cdot \left(22^2\right)^2 \equiv 20 \cdot 16^2 && (\text{Porque } 22^2 \equiv 16 \pmod{39}) \\
&\equiv 20 \cdot 16^2 \equiv 20 \cdot \left(16^2\right)^1 \equiv 20 \cdot 22^1 && (\text{Porque } 16^2 \equiv 22 \pmod{39}) \\
&\equiv 11 && (\text{Porque } 20 \cdot 22 \equiv 11 \pmod{39})
\end{aligned}$$

◊

Ejercicio 46. *Calcula* $41^{56} \pmod{44}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. Como $44 = 2^2 \cdot 11$, entonces aplicamos la fórmula y tenemos que $\varphi(44) = \varphi(2^2 \cdot 11) = \varphi(2^2) \cdot \varphi(11^1) = (2^2 - 2^1) \cdot (11^1 - 11^0) = 20$. Esto nos deja $41^{56} = 41^{16+20 \cdot 2} = 41^{16} \cdot \left(41^{20}\right)^2 \equiv 41^{16} \pmod{44}$ porque $41^{20} \equiv 1 \pmod{44}$ por la Fórmula de Euler.
Para calcular $41^{16} \pmod{44}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
41^{16} &\equiv 41^{16} \equiv \left(41^2\right)^8 \equiv 9^8 && (\text{Porque } 41^2 \equiv 9 \pmod{44}) \\
&\equiv 9^8 \equiv \left(9^2\right)^4 \equiv 37^4 && (\text{Porque } 9^2 \equiv 37 \pmod{44}) \\
&\equiv 37^4 \equiv \left(37^2\right)^2 \equiv 5^2 && (\text{Porque } 37^2 \equiv 5 \pmod{44}) \\
&\equiv 5^2 \equiv \left(5^2\right)^1 \equiv 25^1 && (\text{Porque } 5^2 \equiv 25 \pmod{44}) \\
&\equiv 25 \pmod{44}.
\end{aligned}$$

◊

Ejercicio 47. *Calcula* $13^{109} \pmod{31}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 31 es primo, tendremos que $\varphi(31) = 31 - 1 = 30$. Esto nos deja $13^{109} = 13^{19+30 \cdot 3} = 13^{19} \cdot \left(13^{30}\right)^3 \equiv 13^{19} \pmod{31}$ porque $13^{30} \equiv 1 \pmod{31}$ por la Fórmula de Euler.
Para calcular $13^{19} \pmod{31}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor

cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
13^{19} &\equiv 13{\cdot}13^{18} \equiv 13{\cdot}\left(13^2\right)^9 \equiv 13{\cdot}14^9 && (\text{Porque } 13^2 \equiv 14 \pmod{31}) \\
&\equiv 13\cdot 14{\cdot}14^8 \equiv 13\cdot 14{\cdot}\left(14^2\right)^4 \equiv 13\cdot 14{\cdot}10^4 && (\text{Porque } 14^2 \equiv 10 \pmod{31}) \\
&\equiv 13\cdot 14{\cdot}10^4 \equiv 13\cdot 14{\cdot}\left(10^2\right)^2 \equiv 13\cdot 14{\cdot}7^2 && (\text{Porque } 10^2 \equiv 7 \pmod{31}) \\
&\equiv 13\cdot 14{\cdot}7^2 \equiv 13\cdot 14{\cdot}\left(7^2\right)^1 \equiv 13\cdot 14{\cdot}18^1 && (\text{Porque } 7^2 \equiv 18 \pmod{31}) \\
&\equiv 27\cdot 18 && (\text{Porque } 13\cdot 14 \equiv 27 \pmod{31}) \\
&\equiv 21 && (\text{Porque } 27\cdot 18 \equiv 21 \pmod{31})
\end{aligned}$$

◊

Ejercicio 48. *Calcula* $40^{29} \pmod{42}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Para calcular $40^{29} \pmod{42}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
40^{29} &\equiv 40{\cdot}40^{28} \equiv 40{\cdot}\left(40^2\right)^{14} \equiv 40{\cdot}4^{14} && (\text{Porque } 40^2 \equiv 4 \pmod{42}) \\
&\equiv 40{\cdot}4^{14} \equiv 40{\cdot}\left(4^2\right)^7 \equiv 40{\cdot}16^7 && (\text{Porque } 4^2 \equiv 16 \pmod{42}) \\
&\equiv 40\cdot 16{\cdot}16^6 \equiv 40\cdot 16{\cdot}\left(16^2\right)^3 \equiv 40\cdot 16{\cdot}4^3 && (\text{Porque } 16^2 \equiv 4 \pmod{42}) \\
&\equiv 40\cdot 16\cdot 4{\cdot}4^2 \equiv 40\cdot 16\cdot 4{\cdot}\left(4^2\right)^1 \equiv 40\cdot 16\cdot 4{\cdot}16^1 && (\text{Porque } 4^2 \equiv 16 \pmod{42}) \\
&\equiv 10\cdot 4\cdot 16 && (\text{Porque } 40\cdot 16 \equiv 10 \pmod{42}) \\
&\equiv 40\cdot 16 && (\text{Porque } 10\cdot 4 \equiv 40 \pmod{42}) \\
&\equiv 10 && (\text{Porque } 40\cdot 16 \equiv 10 \pmod{42})
\end{aligned}$$

◊

Ejercicio 49. *Calcula* $29^{137} \pmod{41}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 41 es primo, tendremos que $\varphi(41) = 41 - 1 = 40$. Esto nos deja $29^{137} = 29^{17+40\cdot 3} = 29^{17}\cdot\left(29^{40}\right)^3 \equiv 29^{17} \pmod{41}$ porque $29^{40} \equiv 1 \pmod{41}$ por la Fórmula de Euler.

Para calcular $29^{17} \pmod{41}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$\begin{aligned}
29^{17} &\equiv 29{\cdot}29^{16} \equiv 29{\cdot}\left(29^2\right)^8 \equiv 29{\cdot}21^8 && (\text{Porque } 29^2 \equiv 21 \pmod{41}) \\
&\equiv 29{\cdot}21^8 \equiv 29{\cdot}\left(21^2\right)^4 \equiv 29{\cdot}31^4 && (\text{Porque } 21^2 \equiv 31 \pmod{41}) \\
&\equiv 29{\cdot}31^4 \equiv 29{\cdot}\left(31^2\right)^2 \equiv 29{\cdot}18^2 && (\text{Porque } 31^2 \equiv 18 \pmod{41}) \\
&\equiv 29{\cdot}18^2 \equiv 29{\cdot}\left(18^2\right)^1 \equiv 29{\cdot}37^1 && (\text{Porque } 18^2 \equiv 37 \pmod{41}) \\
&\equiv 7 && (\text{Porque } 29\cdot 37 \equiv 7 \pmod{41})
\end{aligned}$$

◊

Ejercicio 50. *Calcula* $18^{99} \pmod{43}$ *utilizando el algoritmo de exponenciación modular.*

Solución: Lo primero que vamos a hacer es reducir el exponente haciendo uso de la Fórmula de Euler. Para ello calcularemos la función φ de Euler del módulo. En este caso, como 43 es primo, tendremos que $\varphi(43) = 43 - 1 = 42$. Esto nos deja $18^{99} = 18^{15+42\cdot 2} = 18^{15} \cdot \left(18^{42}\right)^2 \equiv 18^{15} \pmod{43}$ porque $18^{42} \equiv 1 \pmod{43}$ por la Fórmula de Euler.
Para calcular $18^{15} \pmod{43}$ iremos agrupando factores 2 del exponente cuando sea par y sacando un factor cuando sea impar para dejar el exponente par y poder sacar un factor 2. Lo vamos a ir haciendo paso a paso:

$$
\begin{aligned}
18^{15} &\equiv 18 \cdot 18^{14} \equiv 18 \cdot \left(18^2\right)^7 \equiv 18 \cdot 23^7 && (\text{Porque } 18^2 \equiv 23 \pmod{43}) \\
&\equiv 18 \cdot 23 \cdot 23^6 \equiv 18 \cdot 23 \cdot \left(23^2\right)^3 \equiv 18 \cdot 23 \cdot 13^3 && (\text{Porque } 23^2 \equiv 13 \pmod{43}) \\
&\equiv 18 \cdot 23 \cdot 13 \cdot 13^2 \equiv 18 \cdot 23 \cdot 13 \cdot \left(13^2\right)^1 \equiv 18 \cdot 23 \cdot 13 \cdot 40^1 && (\text{Porque } 13^2 \equiv 40 \pmod{43}) \\
&\equiv 27 \cdot 13 \cdot 40 && (\text{Porque } 18 \cdot 23 \equiv 27 \pmod{43}) \\
&\equiv 7 \cdot 40 && (\text{Porque } 27 \cdot 13 \equiv 7 \pmod{43}) \\
&\equiv 22 && (\text{Porque } 7 \cdot 40 \equiv 22 \pmod{43})
\end{aligned}
$$

◊