

# Cálculo de inversos modulares



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Dividimos 4620 entre 1469.



# Cálculo de inversos modulares

$$4620 = 1469 \cdot 3 + 213$$

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Dividimos 4620 entre 1469.



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

$$4620 = 1469 \cdot 3 + 213$$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 1469 entre 213.



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 1469 entre 213.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 213 entre 191.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 213 entre 191.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 191 entre 22.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 191 entre 22.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 22 entre 15.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 22 entre 15.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 15 entre 7.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Ahora 15 entre 7.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Puesto que el resto es 1, sabemos que  $\text{mcd}(4620, 1469) = 1$ .

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$





# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Puesto que el resto es 1, sabemos que  $\text{mcd}(4620, 1469) = 1$ .

Luego existe el inverso que queremos calcular.

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c
4620	
1469	
213	3
191	6
22	1
15	8
7	1
1	2

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c
4620	
1469	
213	3
191	6
22	1
15	8
7	1
1	2

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c
4620	
1469	
213	3
191	6
22	1
15	8
7	1
1	2

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c
4620	
1469	
213	3
191	6
22	1
15	8
7	1
1	2

$$213 = 4620 - 3 \cdot 1469$$

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c
4620	
1469	
213	3
191	6
22	1
15	8
7	1
1	2

$$213 = 4620 - 3 \cdot 1469$$

$$191 = 1469 - 6 \cdot 213$$

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c
4620	
1469	
213	3
191	6
22	1
15	8
7	1
1	2

$$213 = 4620 - 3 \cdot 1469$$

$$191 = 1469 - 6 \cdot 213$$

$$22 = 213 - 1 \cdot 191$$

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c
4620	
1469	
213	3
191	6
22	1
15	8
7	1
1	2

$$213 = 4620 - 3 \cdot 1469$$

$$191 = 1469 - 6 \cdot 213$$

$$22 = 213 - 1 \cdot 191$$

$$15 = 191 - 8 \cdot 22$$

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	
4620		
1469		
213	3	$213 = 4620 - 3 \cdot 1469$
191	6	$191 = 1469 - 6 \cdot 213$
22	1	$22 = 213 - 1 \cdot 191$
15	8	$15 = 191 - 8 \cdot 22$
7	1	$7 = 22 - 1 \cdot 15$
1	2	

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	
4620		
1469		
213	3	$213 = 4620 - 3 \cdot 1469$
191	6	$191 = 1469 - 6 \cdot 213$
22	1	$22 = 213 - 1 \cdot 191$
5	8	$15 = 191 - 8 \cdot 22$
7	1	$7 = 22 - 1 \cdot 15$
1	2	$1 = 15 - 2 \cdot 7$

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	
4620		
1469		
213	3	$213 = 4620 - 3 \cdot 1469$
191	6	$191 = 1469 - 6 \cdot 213$
22	1	$22 = 213 - 1 \cdot 191$
5	8	$15 = 191 - 8 \cdot 22$
7	1	$7 = 22 - 1 \cdot 15$
1	2	$1 = 15 - 2 \cdot 7$

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c
4620	
1469	
213	3
191	6
22	1
5	8
7	1
1	2



$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c
4620	
1469	
213	3
191	6
22	1
5	8
7	1
1	2



$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v
4620		0
1469		1
213	3	$0 - 3 \cdot 1 = -3$
191	6	
22	1	
5	8	
7	1	
1	2	

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v
4620		0
1469		1
213	3	-3 $0 - 3 \cdot 1 = -3$
191	6	
22	1	
5	8	
7	1	
1	2	

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v
4620		0
1469		1
213	3	-3
191	6	
22	1	
5	8	
7	1	
1	2	

$$0 - 3 \cdot 1 = -3$$
$$1 - 6 \cdot (-3) = 19$$

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	
5	8	
7	1	
1	2	

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	-22
5	8	
7	1	
1	2	

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v	
4620		0	
1469		1	
213	3	-3	$0 - 3 \cdot 1 = -3$
191	6	19	$1 - 6 \cdot (-3) = 19$
22	1	-22	$-3 - 1 \cdot 19 = -22$
5	8		
7	1		
1	2		

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v	
4620		0	
1469		1	
213	3	-3	$0 - 3 \cdot 1 = -3$
191	6	19	$1 - 6 \cdot (-3) = 19$
22	1	-22	$-3 - 1 \cdot 19 = -22$
5	8		$19 - 8 \cdot (-22) = 195$
7	1		
1	2		

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v	
4620		0	
1469		1	
213	3	-3	$0 - 3 \cdot 1 = -3$
191	6	19	$1 - 6 \cdot (-3) = 19$
22	1	-22	$-3 - 1 \cdot 19 = -22$
5	8	195	$19 - 8 \cdot (-22) = 195$
7	1		
1	2		

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v	
4620		0	
1469		1	
213	3	-3	$0 - 3 \cdot 1 = -3$
191	6	19	$1 - 6 \cdot (-3) = 19$
22	1	-22	$-3 - 1 \cdot 19 = -22$
5	8	195	$19 - 8 \cdot (-22) = 195$
7	1		$-22 - 1 \cdot 195 = -217$
1	2		

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v	
4620		0	
1469		1	
213	3	-3	$0 - 3 \cdot 1 = -3$
191	6	19	$1 - 6 \cdot (-3) = 19$
22	1	-22	$-3 - 1 \cdot 19 = -22$
5	8	195	$19 - 8 \cdot (-22) = 195$
7	1	-217	$-22 - 1 \cdot 195 = -217$
1	2		

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v	
4620		0	
1469		1	
213	3	-3	$0 - 3 \cdot 1 = -3$
191	6	19	$1 - 6 \cdot (-3) = 19$
22	1	-22	$-3 - 1 \cdot 19 = -22$
5	8	195	$19 - 8 \cdot (-22) = 195$
7	1	-217	$-22 - 1 \cdot 195 = -217$
1	2	629	$195 - 2 \cdot (-217) = 629$

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

En primer lugar, calculamos el máximo común divisor de 4620 y 1469 por el algoritmo de Euclides.

Con los cocientes y los restos, rellenamos la siguiente tabla:

r	c	v	
4620		0	
1469		1	
213	3	-3	$0 - 3 \cdot 1 = -3$
191	6	19	$1 - 6 \cdot (-3) = 19$
22	1	-22	$-3 - 1 \cdot 19 = -22$
5	8	195	$19 - 8 \cdot (-22) = 195$
7	1	-217	$-22 - 1 \cdot 195 = -217$
1	2	629	$195 - 2 \cdot (-217) = 629$

$$4620 = 1469 \cdot 3 + 213$$

$$1469 = 213 \cdot 6 + 191$$

$$213 = 191 \cdot 1 + 22$$

$$191 = 22 \cdot 8 + 15$$

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

Podemos observar que se tiene la siguiente relación entre los elementos de la tabla:

$$r_i = r_{i-2} - c_i \cdot r_{i-1}$$

Añadimos una nueva columna  $v$ , cuyos dos primeros elementos son 0 y 1.

Y la completamos siguiendo la regla

$$v_i = v_{i-2} - c_i \cdot v_{i-1}$$

# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

Con esto tenemos que

$$1469^{-1} \bmod 4620 = 629.$$

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	-22
5	8	195
7	1	-217
1	2	629



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

Con esto tenemos que  
 $1469^{-1} \bmod 4620 = 629$ .

Vamos a comprobarlo.

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	-22
5	8	195
7	1	-217
1	2	629



# Cálculo de inversos modulares

$$1469 \cdot 629 = 924001$$

Vamos a calcular  $1469^{-1} \bmod 4620$

Con esto tenemos que  
 $1469^{-1} \bmod 4620 = 629$ .

Vamos a comprobarlo.

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	-22
5	8	195
7	1	-217
1	2	629



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

$$1469 \cdot 629 = 924001$$

$$924001 \bmod 4620 = 1$$

Con esto tenemos que  
 $1469^{-1} \bmod 4620 = 629$ .

Vamos a comprobarlo.

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	-22
5	8	195
7	1	-217
1	2	629



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

Con esto tenemos que  
 $1469^{-1} \bmod 4620 = 629$ .

Vamos a comprobarlo.

$$1469 \cdot 629 = 924001$$

$$924001 \bmod 4620 = 1$$

Ya que

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	-22
5	8	195
7	1	-217
1	2	629



# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

Con esto tenemos que  
 $1469^{-1} \bmod 4620 = 629$ .

Vamos a comprobarlo.

$$1469 \cdot 629 = 924001$$

$$924001 \bmod 4620 = 1$$

Ya que

$$924001 = 4620 \cdot 200 + 1$$

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	-22
5	8	195
7	1	-217
1	2	629





# Cálculo de inversos modulares

Vamos a calcular  $1469^{-1} \bmod 4620$

Con esto tenemos que  
 $1469^{-1} \bmod 4620 = 629$ .

Vamos a comprobarlo.

$$1469 \cdot 629 = 924001$$

$$924001 \bmod 4620 = 1$$

Ya que

$$924001 = 4620 \cdot 200 + 1$$

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	-22
5	8	195
7	1	-217
1	2	629



# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.



# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v
4620		0
1469		1
213	3	-3
191	6	19
22	1	-22
15	8	195
7	1	-217
1	2	629

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	
191	6	19	
22	1	-22	
15	8	195	
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 =$
191	6	19	
22	1	-22	
15	8	195	
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 =$
191	6	19	
22	1	-22	
15	8	195	
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	
22	1	-22	
15	8	195	
7	1	-217	
1	2	629	



# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 =$
22	1	-22	
15	8	195	
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 =$
22	1	-22	
15	8	195	
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	
15	8	195	
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 =$
15	8	195	
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 =$
15	8	195	
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 =$
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 =$
7	1	-217	
1	2	629	



# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	$1469 \cdot (-217) \bmod 4620 =$
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	$1469 \cdot (-217) \bmod 4620 = -318773 \bmod 4620 =$
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	$1469 \cdot (-217) \bmod 4620 = -318773 \bmod 4620 = 7$
1	2	629	

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	$1469 \cdot (-217) \bmod 4620 = -318773 \bmod 4620 = 7$
1	2	629	$1469 \cdot 629 \bmod 4620 =$

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	$1469 \cdot (-217) \bmod 4620 = -318773 \bmod 4620 = 7$
1	2	629	$1469 \cdot 629 \bmod 4620 = 924001 \bmod 4620 =$

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	$1469 \cdot (-217) \bmod 4620 = -318773 \bmod 4620 = 7$
1	2	629	$1469 \cdot 629 \bmod 4620 = 924001 \bmod 4620 = 1$

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	$1469 \cdot (-217) \bmod 4620 = -318773 \bmod 4620 = 7$
1	2	629	$1469 \cdot 629 \bmod 4620 = 924001 \bmod 4620 = 1$



# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	$1469 \cdot (-217) \bmod 4620 = -318773 \bmod 4620 = 7$
1	2	629	$1469 \cdot 629 \bmod 4620 = 924001 \bmod 4620 = 1$

Y vemos cómo se tiene la relación:

# Cálculo de inversos modulares

Vamos a comprobar cuál es el significado de cada coeficiente  $v_i$  que hemos ido obteniendo.

Para eso, calculamos  $1469 \cdot v_i \bmod 4620$ .

r	c	v	
4620		0	
1469		1	$1469 \cdot 1 \bmod 4620 = 1469$
213	3	-3	$1469 \cdot (-3) \bmod 4620 = -4407 \bmod 4620 = 213$
191	6	19	$1469 \cdot 19 \bmod 4620 = 27911 \bmod 4620 = 191$
22	1	-22	$1469 \cdot (-22) \bmod 4620 = -32318 \bmod 4620 = 22$
15	8	195	$1469 \cdot 195 \bmod 4620 = 286455 \bmod 4620 = 15$
7	1	-217	$1469 \cdot (-217) \bmod 4620 = -318773 \bmod 4620 = 7$
1	2	629	$1469 \cdot 629 \bmod 4620 = 924001 \bmod 4620 = 1$

Y vemos cómo se tiene la relación:

$$1469 \cdot v_i \bmod 4620 = r_i$$