

Teorema del residuo chino

Sistemas de congruencias, paso a paso

Daniel Felipe Triviño

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

¿Qué estamos buscando?

$$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{cases}$$

¿Qué estamos buscando?

$$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{cases}$$

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

Los candidatos: de 0 a 34.

¿Qué estamos buscando?

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

Los candidatos: de 0 a 34.

¿Qué estamos buscando?

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

Solo el 17 cumple las dos condiciones.

¿Qué estamos buscando?

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

Si los módulos son primos relativos, hay una única solución entre 0 y $N - 1$.

1. Los datos: a_i y m_i

	a_i	m_i
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{array} \right.$	2	5
	3	7

De cada congruencia: el residuo a_i y el módulo m_i .

1. Los datos: a_i y m_i

	a_i	m_i
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{array} \right.$	2	5
	3	7

Condición: los módulos deben ser primos relativos entre sí.

2. El producto N

	a_i	m_i
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{array} \right.$	2	5
	3	7

$$N = m_1 \times m_2 = 5 \times 7 = 35$$

N es el producto de todos los módulos.

2. El producto N

	a_i	m_i	
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{array} \right.$	2	5	$N = 35$
	3	7	$0 \leq x < 35$

$$N = m_1 \times m_2 = 5 \times 7 = 35$$

La solución va a estar entre 0 y $N - 1 = 34$.

3. Los $M_i = N/m_i$

	a_i	m_i	M_i
$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{cases}$	2	5	
	3	7	

$N = 35$
 $0 \leq x < 35$

$$N = m_1 \times m_2 = 5 \times 7 = 35$$

M_i es N dividido entre el módulo de su fila.

3. Los $M_i = N/m_i$

	a_i	m_i	M_i	
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	$N = 35$
	3	7		$0 \leq x < 35$

$$N = m_1 \times m_2 = \cancel{5} \times 7 = 35$$

$$M_1 = \frac{N}{m_1} = \frac{35}{5} = 7$$

M_i es N dividido entre el módulo de su fila.

3. Los $M_i = N/m_i$

	a_i	m_i	M_i	
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	$N = 35$ $0 \leq x < 35$
	3	7		

$$N = m_1 \times m_2 = \cancel{5} \times 7 = 35$$

$$M_1 = \frac{N}{m_1} = \frac{35}{5} = 7$$

M_i también es el producto de los demás módulos.

3. Los $M_i = N/m_i$

	a_i	m_i	M_i	
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	$N = 35$ $0 \leq x < 35$
	3	7	5	

$$N = m_1 \times m_2 = 5 \times \cancel{7} = 35$$

$$M_2 = \frac{N}{m_2} = \frac{35}{7} = 5$$

M_i también es el producto de los demás módulos.

4. Los inversos y_i

	a_i	m_i	M_i	y_i	
$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{cases}$	2	5	7		$N = 35$
	3	7	5		$0 \leq x < 35$

$$M_i \cdot y_i \equiv 1 \pmod{m_i}$$

y_i es el inverso de M_i módulo m_i .

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	
	3	7	5	

$N = 35$
 $0 \leq x < 35$

$$7 \cdot y_1 \equiv 1 \pmod{5}$$

y_i es el inverso de M_i módulo m_i .

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	
	3	7	5	

$N = 35$
 $0 \leq x < 35$

$$7 \cdot y_1 \equiv 1 \pmod{5}$$

$$7 = 5 \times 1 + 2$$

Algoritmo extendido de Euclides con 7 y 5.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	
	3	7	5	

$N = 35$
 $0 \leq x < 35$

$$7 \cdot y_1 \equiv 1 \pmod{5}$$

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + 1$$

Algoritmo extendido de Euclides con 7 y 5.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	
	3	7	5	

$N = 35$
 $0 \leq x < 35$

$$7 \cdot y_1 \equiv 1 \pmod{5}$$

$$7 = 5 \times 1 + 2$$


$$5 = 2 \times 2 + 1$$

$$2 = 1 \times 2 + 0$$

Algoritmo extendido de Euclides con 7 y 5.

4. Los inversos y_i

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	
3	7	5	

$N = 35$
 $0 \leq x < 35$

$$7 \cdot y_1 \equiv 1 \pmod{5}$$

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + 1$$

$$2 = 1 \times 2 + 0$$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2		
4	1	2		

Algoritmo extendido de Euclides con 7 y 5.

4. Los inversos y_i

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

	a_i	m_i	M_i	y_i
	2	5	7	
	3	7	5	

$N = 35$
 $0 \leq x < 35$

$$7 \cdot y_1 \equiv 1 \pmod{5}$$

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + 1$$

$$2 = 1 \times 2 + 0$$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2	1	-1
4	1	2		

Dos filas arriba, menos el cociente por la fila anterior.

4. Los inversos y_i

	a_i	m_i	M_i	y_i	
$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{cases}$	2	5	7		$N = 35$
	3	7	5		$0 \leq x < 35$

$7 \cdot y_1 \equiv 1 \pmod{5}$

$7 = 5 \times 1 + 2$

$5 = 2 \times 2 + 1$

$2 = 1 \times 2 + 0$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2	1	−1
4	1	2	−2	3

Dos filas arriba, menos el cociente por la fila anterior.

4. Los inversos y_i

$$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	
3	7	5	

$N = 35$
 $0 \leq x < 35$

$7 \cdot y_1 \equiv 1 \pmod{5}$

$7 \times (-2) + 5 \times 3 = 1$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2	1	−1
4	1	2	−2	3

Dos filas arriba, menos el cociente por la fila anterior.

4. Los inversos y_i

	a_i	m_i	M_i	y_i	
$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$	2	5	7		$N = 35$
	3	7	5		$0 \leq x < 35$

$7 \cdot y_1 \equiv 1 \pmod 5$

$7 \times (-2) + \cancel{5 \times 3} = 1$

$7 \times (-2) \equiv 1 \pmod 5$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2	1	−1
4	1	2	−2	3

Módulo 5, todo múltiplo de 5 vale 0.

4. Los inversos y_i

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	3
3	7	5	

$$N = 35$$

$$0 \leq x < 35$$

$$7 \cdot y_1 \equiv 1 \pmod{5}$$

$$7 \times (-2) + \cancel{5 \times 3} = 1$$

$$7 \times (-2) \equiv 1 \pmod{5}$$

$$y_1 = 7^{-1} \pmod{5} = -2 \pmod{5} = 3$$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2	1	-1
4	1	2	-2	3

Módulo 5, todo múltiplo de 5 vale 0.

4. Los inversos y_i

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	3
3	7	5	

$N = 35$
 $0 \leq x < 35$

$7 \cdot y_1 \equiv 1 \pmod{5}$

$7 \times (-2) + \cancel{5 \times 3} = 1$

$7 \times (-2) \equiv 1 \pmod{5}$

$y_1 = 7^{-1} \pmod{5} = -2 \pmod{5} = 3$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2	1	−1
4	1	2	−2	3

Comprobación: $7 \cdot 3 = 21$, que deja residuo 1 al dividir entre 5.

4. Los inversos y_i

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	3
3	7	5	

$N = 35$
 $0 \leq x < 35$

$5 \cdot y_2 \equiv 1 \pmod{7}$

$7 \times (-2) + 5 \times 3 = 1$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2	1	−1
4	1	2	−2	3

Con dos módulos, una sola identidad de Bézout da los dos inversos.

4. Los inversos y_i

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	3
3	7	5	

$N = 35$
 $0 \leq x < 35$

$$5 \cdot y_2 \equiv 1 \pmod{7}$$

$$7 \times (-2) + 5 \times 3 = 1$$

$$5 \times 3 \equiv 1 \pmod{7}$$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2	1	-1
4	1	2	-2	3

Con dos módulos, una sola identidad de Bézout da los dos inversos.

4. Los inversos y_i

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	3
3	7	5	3

$N = 35$
 $0 \leq x < 35$

$$5 \cdot y_2 \equiv 1 \pmod{7}$$

$$\cancel{7 \times (-2)} + 5 \times 3 = 1$$

$$5 \times 3 \equiv 1 \pmod{7}$$

$$y_2 = 5^{-1} \pmod{7} = 3$$

i	r_i	q_i	s_i	t_i
1	7	—	1	0
2	5	1	0	1
3	2	2	1	-1
4	1	2	-2	3

Con dos módulos, una sola identidad de Bézout da los dos inversos.

5. Armar la solución

	a_i	m_i	M_i	y_i	
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{array} \right.$	2	5	7	3	$N = 35$
	3	7	5	3	$0 \leq x < 35$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2$$

Cada fila aporta un término: $a_i \cdot y_i \cdot M_i$.

5. Armar la solución

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	3
3	7	5	3

$$N = 35$$

$$0 \leq x < 35$$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2$$

$$x \equiv 2 \times 3 \times 7$$

Cada fila aporta un término: $a_i \cdot y_i \cdot M_i$.

5. Armar la solución

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	3
3	7	5	3

$$N = 35$$

$$0 \leq x < 35$$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2$$

$$x \equiv 2 \times 3 \times 7 + 3 \times 3 \times 5 \pmod{35}$$

Cada fila aporta un término: $a_i \cdot y_i \cdot M_i$.

5. Armar la solución

	a_i	m_i	M_i	y_i	
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	3	$N = 35$
	3	7	5	3	$0 \leq x < 35$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2$$

$$x \equiv 2 \times 3 \times 7 + 3 \times 3 \times 5 \pmod{35}$$

Cada término deja residuo a_i con su módulo y 0 con los demás.

5. Armar la solución

	a_i	m_i	M_i	y_i	
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	3	$N = 35$
	3	7	5	3	$0 \leq x < 35$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2$$

$$x \equiv 2 \times 3 \times 7 + 3 \times 3 \times 5 \pmod{35}$$

$$x \equiv 42 + 45 \pmod{35}$$

Cada término deja residuo a_i con su módulo y 0 con los demás.

5. Armar la solución

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases} \quad \begin{array}{c|cccc} & a_i & m_i & M_i & y_i \\ \hline & 2 & 5 & 7 & 3 \\ & 3 & 7 & 5 & 3 \end{array} \quad \begin{array}{l} N = 35 \\ 0 \leq x < 35 \end{array}$$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2$$

$$x \equiv 2 \times 3 \times 7 + 3 \times 3 \times 5 \pmod{35}$$

$$x \equiv 42 + 45 \pmod{35}$$

$$x \equiv 87 \pmod{35}$$

Cada término deja residuo a_i con su módulo y 0 con los demás.

6. Reducir módulo N

	a_i	m_i	M_i	y_i	
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	3	$N = 35$ $0 \leq x < 35$
	3	7	5	3	

$$x \equiv 87 \pmod{35}$$

$$87 = 35 \times$$

Reducir módulo N : quedarnos con el residuo.

6. Reducir módulo N

	a_i	m_i	M_i	y_i	
$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$	2	5	7	3	$N = 35$ $0 \leq x < 35$
	3	7	5	3	

$$x \equiv 87 \pmod{35}$$

$$87 = 35 \times 2 + 17$$

Reducir módulo N : quedarnos con el residuo.

6. Reducir módulo N

	a_i	m_i	M_i	y_i
$\left\{ \begin{array}{l} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{array} \right.$	2	5	7	3
	3	7	5	3

$$N = 35$$

$$0 \leq x < 35$$

$$x = 17$$

$$x \equiv 87 \pmod{35}$$

$$87 = 35 \times 2 + 17$$

$$x \equiv 87 \equiv 17 \pmod{35}$$

Reducir módulo N : quedarnos con el residuo.

7. Comprobación

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

a_i	m_i	M_i	y_i
2	5	7	3
3	7	5	3

$$N = 35$$

$$0 \leq x < 35$$

$$x = 17$$

$$17 = 5 \times 3 + 2 \quad \checkmark$$

$$17 = 7 \times 2 + 3 \quad \checkmark$$

Comprobamos cada congruencia.

Ejemplo 2: tres congruencias

El sistema

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{cases}$$

1. Los datos: a_i y m_i

	a_i	m_i
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \\ x \equiv 10 \bmod 11 \end{array} \right.$	2	5
	3	7
	10	11

De cada congruencia: el residuo a_i y el módulo m_i .

1. Los datos: a_i y m_i

	a_i	m_i
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \\ x \equiv 10 \bmod 11 \end{array} \right.$	2	5
	3	7
	10	11

Condición: los módulos deben ser primos relativos entre sí.

2. El producto N

	a_i	m_i
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \\ x \equiv 10 \bmod 11 \end{array} \right.$	$\begin{array}{c} 2 \\ 3 \\ 10 \end{array}$	$\begin{array}{c} 5 \\ 7 \\ 11 \end{array}$

$$N = m_1 \times m_2 \times m_3 = 5 \times 7 \times 11 = 385$$

N es el producto de todos los módulos.

2. El producto N

	a_i	m_i
$x \equiv 2 \pmod{5}$	2	5
$x \equiv 3 \pmod{7}$	3	7
$x \equiv 10 \pmod{11}$	10	11

$N = 385$
 $0 \leq x < 385$

$$N = m_1 \times m_2 \times m_3 = 5 \times 7 \times 11 = 385$$

La solución va a estar entre 0 y $N - 1 = 384$.

3. Los $M_i = N/m_i$

	a_i	m_i	M_i
$x \equiv 2 \pmod{5}$	2	5	
$x \equiv 3 \pmod{7}$	3	7	
$x \equiv 10 \pmod{11}$	10	11	

$N = 385$
 $0 \leq x < 385$

$$N = m_1 \times m_2 \times m_3 = 5 \times 7 \times 11 = 385$$

M_i es N dividido entre el módulo de su fila.

3. Los $M_i = N/m_i$

	a_i	m_i	M_i
$x \equiv 2 \pmod{5}$	2	5	77
$x \equiv 3 \pmod{7}$	3	7	
$x \equiv 10 \pmod{11}$	10	11	

$N = 385$
 $0 \leq x < 385$

$$N = m_1 \times m_2 \times m_3 = \cancel{5} \times 7 \times 11 = 385$$

$$M_1 = \frac{N}{m_1} = \frac{385}{5} = 77$$

M_i es N dividido entre el módulo de su fila.

3. Los $M_i = N/m_i$

	a_i	m_i	M_i
$x \equiv 2 \pmod{5}$	2	5	77
$x \equiv 3 \pmod{7}$	3	7	
$x \equiv 10 \pmod{11}$	10	11	

$$N = 385$$
$$0 \leq x < 385$$

$$N = m_1 \times m_2 \times m_3 = \cancel{5} \times 7 \times 11 = 385$$

$$M_1 = \frac{N}{m_1} = \frac{385}{5} = 77$$

M_i también es el producto de los demás módulos.

3. Los $M_i = N/m_i$

	a_i	m_i	M_i
$x \equiv 2 \pmod{5}$	2	5	77
$x \equiv 3 \pmod{7}$	3	7	55
$x \equiv 10 \pmod{11}$	10	11	

$N = 385$
 $0 \leq x < 385$

$$N = m_1 \times m_2 \times m_3 = 5 \times \cancel{7} \times 11 = 385$$

$$M_2 = \frac{N}{m_2} = \frac{385}{7} = 55$$

M_i también es el producto de los demás módulos.

3. Los $M_i = N/m_i$

	a_i	m_i	M_i
$x \equiv 2 \pmod{5}$	2	5	77
$x \equiv 3 \pmod{7}$	3	7	55
$x \equiv 10 \pmod{11}$	10	11	35

$N = 385$
 $0 \leq x < 385$

$$N = m_1 \times m_2 \times m_3 = 5 \times 7 \times \cancel{11} = 385$$

$$M_3 = \frac{N}{m_3} = \frac{385}{11} = 35$$

M_i también es el producto de los demás módulos.

4. Los inversos y_i

	a_i	m_i	M_i	y_i	
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \\ x \equiv 10 \bmod 11 \end{array} \right.$	2	5	77		$N = 385$
	3	7	55		$0 \leq x < 385$
	10	11	35		

$$M_i \cdot y_i \equiv 1 \pmod{m_i}$$

y_i es el inverso de M_i módulo m_i .

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$\left\{ \begin{array}{l} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{array} \right.$	2	5	77	
	3	7	55	
	10	11	35	

$$N = 385$$

$$0 \leq x < 385$$

$$77 \cdot y_1 \equiv 1 \pmod{5}$$

y_i es el inverso de M_i módulo m_i .

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$\left\{ \begin{array}{l} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{array} \right.$	2	5	77	
	3	7	55	
	10	11	35	

$$N = 385$$

$$0 \leq x < 385$$

$$77 \cdot y_1 \equiv 1 \pmod{5}$$

$$77 = 5 \times 15 + 2$$

Algoritmo extendido de Euclides con 77 y 5.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod{5}$	2	5	77	
$x \equiv 3 \pmod{7}$	3	7	55	
$x \equiv 10 \pmod{11}$	10	11	35	

$$N = 385$$

$$0 \leq x < 385$$

$$77 \cdot y_1 \equiv 1 \pmod{5}$$

$$77 = 5 \times 15 + 2$$

$$5 = 2 \times 2 + 1$$

Algoritmo extendido de Euclides con 77 y 5.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod{5}$	2	5	77	
$x \equiv 3 \pmod{7}$	3	7	55	
$x \equiv 10 \pmod{11}$	10	11	35	

$$N = 385$$

$$0 \leq x < 385$$

$$77 \cdot y_1 \equiv 1 \pmod{5}$$

$$77 = 5 \times 15 + 2$$

$$5 = 2 \times 2 + 1$$

$$2 = 1 \times 2 + 0$$

Algoritmo extendido de Euclides con 77 y 5.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \bmod 5$	2	5	77	
$x \equiv 3 \bmod 7$	3	7	55	
$x \equiv 10 \bmod 11$	10	11	35	

$N = 385$

$0 \leq x < 385$

$77 \cdot y_1 \equiv 1 \pmod{5}$

$77 = 5 \times 15 + 2$

$5 = 2 \times 2 + 1$

$2 = 1 \times 2 + 0$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2		
4	1	2		

Algoritmo extendido de Euclides con 77 y 5.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	
$x \equiv 3 \pmod 7$	3	7	55	
$x \equiv 10 \pmod{11}$	10	11	35	

$N = 385$

$0 \leq x < 385$

$77 \cdot y_1 \equiv 1 \pmod 5$

$77 = 5 \times 15 + 2$

$5 = 2 \times 2 + 1$

$2 = 1 \times 2 + 0$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2		

Dos filas arriba, menos el cociente por la fila anterior.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	
$x \equiv 3 \pmod 7$	3	7	55	
$x \equiv 10 \pmod{11}$	10	11	35	

$N = 385$

$0 \leq x < 385$

$77 \cdot y_1 \equiv 1 \pmod 5$

$77 = 5 \times 15 + 2$

$5 = 2 \times 2 + 1$

$2 = 1 \times 2 + 0$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	−15
4	1	2	−2	31

Dos filas arriba, menos el cociente por la fila anterior.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	
$x \equiv 3 \pmod 7$	3	7	55	
$x \equiv 10 \pmod{11}$	10	11	35	

$N = 385$
 $0 \leq x < 385$

$77 \cdot y_1 \equiv 1 \pmod 5$

$77 \times (-2) + 5 \times 31 = 1$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	-15
4	1	2	-2	31

Dos filas arriba, menos el cociente por la fila anterior.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	
$x \equiv 3 \pmod 7$	3	7	55	
$x \equiv 10 \pmod{11}$	10	11	35	

$N = 385$

$0 \leq x < 385$

$77 \cdot y_1 \equiv 1 \pmod 5$

$77 \times (-2) + \cancel{5 \times 31} = 1$

$77 \times (-2) \equiv 1 \pmod 5$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	−15
4	1	2	−2	31

Módulo 5, todo múltiplo de 5 vale 0.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	3
$x \equiv 3 \pmod 7$	3	7	55	
$x \equiv 10 \pmod{11}$	10	11	35	

$N = 385$

$0 \leq x < 385$

$77 \cdot y_1 \equiv 1 \pmod 5$

$77 \times (-2) + \cancel{5 \times 31} = 1$

$77 \times (-2) \equiv 1 \pmod 5$

$y_1 = 77^{-1} \pmod 5 = -2 \pmod 5 = 3$

i	r_i	q_i	s_i	t_i
1	77	—	1	0
2	5	15	0	1
3	2	2	1	−15
4	1	2	−2	31

Módulo 5, todo múltiplo de 5 vale 0.

4. Los inversos y_i

	a_i	m_i	M_i	y_i	
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \\ x \equiv 10 \bmod 11 \end{array} \right.$	2	5	77	3	$N = 385$
	3	7	55		$0 \leq x < 385$
	10	11	35		

$55 \cdot y_2 \equiv 1 \pmod{7}$

$55 = 7 \times 7 + 6$

$7 = 6 \times 1 + 1$

$6 = 1 \times 6 + 0$

i	r_i	q_i	s_i	t_i
1	55	—	1	0
2	7	7	0	1
3	6	1	1	−7
4	1	6	−1	8

Algoritmo extendido de Euclides con 55 y 7.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	3
$x \equiv 3 \pmod 7$	3	7	55	
$x \equiv 10 \pmod{11}$	10	11	35	

$$N = 385$$

$$0 \leq x < 385$$

$$55 \cdot y_2 \equiv 1 \pmod 7$$

$$55 \times (-1) + 7 \times 8 = 1$$

i	r_i	q_i	s_i	t_i
1	55	—	1	0
2	7	7	0	1
3	6	1	1	-7
4	1	6	-1	8

Algoritmo extendido de Euclides con 55 y 7.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	3
$x \equiv 3 \pmod 7$	3	7	55	
$x \equiv 10 \pmod{11}$	10	11	35	

$N = 385$

$0 \leq x < 385$

$55 \cdot y_2 \equiv 1 \pmod 7$

$55 \times (-1) + \cancel{7 \times 8} = 1$

$55 \times (-1) \equiv 1 \pmod 7$

i	r_i	q_i	s_i	t_i
1	55	—	1	0
2	7	7	0	1
3	6	1	1	−7
4	1	6	−1	8

Módulo 7, todo múltiplo de 7 vale 0.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	3
$x \equiv 3 \pmod 7$	3	7	55	6
$x \equiv 10 \pmod{11}$	10	11	35	

$N = 385$

$0 \leq x < 385$

$55 \cdot y_2 \equiv 1 \pmod 7$

$55 \times (-1) + \cancel{7 \times 8} = 1$

$55 \times (-1) \equiv 1 \pmod 7$

$y_2 = 55^{-1} \pmod 7 = -1 \pmod 7 = 6$

i	r_i	q_i	s_i	t_i
1	55	—	1	0
2	7	7	0	1
3	6	1	1	−7
4	1	6	−1	8

Módulo 7, todo múltiplo de 7 vale 0.

4. Los inversos y_i

	a_i	m_i	M_i	y_i	
$x \equiv 2 \bmod 5$	2	5	77	3	$N = 385$ $0 \leq x < 385$
$x \equiv 3 \bmod 7$	3	7	55	6	
$x \equiv 10 \bmod 11$	10	11	35		

$35 \cdot y_3 \equiv 1 \pmod{11}$

$35 = 11 \times 3 + 2$

$11 = 2 \times 5 + 1$

$2 = 1 \times 2 + 0$

i	r_i	q_i	s_i	t_i
1	35	—	1	0
2	11	3	0	1
3	2	5	1	−3
4	1	2	−5	16

Algoritmo extendido de Euclides con 35 y 11.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	3
$x \equiv 3 \pmod 7$	3	7	55	6
$x \equiv 10 \pmod{11}$	10	11	35	

$N = 385$

$0 \leq x < 385$

$35 \cdot y_3 \equiv 1 \pmod{11}$

$35 \times (-5) + 11 \times 16 = 1$

i	r_i	q_i	s_i	t_i
1	35	—	1	0
2	11	3	0	1
3	2	5	1	−3
4	1	2	−5	16

Algoritmo extendido de Euclides con 35 y 11.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	3
$x \equiv 3 \pmod 7$	3	7	55	6
$x \equiv 10 \pmod{11}$	10	11	35	

$$N = 385$$

$$0 \leq x < 385$$

$$35 \cdot y_3 \equiv 1 \pmod{11}$$

$$35 \times (-5) + \cancel{11 \times 16} = 1$$

$$35 \times (-5) \equiv 1 \pmod{11}$$

i	r_i	q_i	s_i	t_i
1	35	—	1	0
2	11	3	0	1
3	2	5	1	−3
4	1	2	−5	16

Módulo 11, todo múltiplo de 11 vale 0.

4. Los inversos y_i

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod 5$	2	5	77	3
$x \equiv 3 \pmod 7$	3	7	55	6
$x \equiv 10 \pmod{11}$	10	11	35	6

$$N = 385$$

$$0 \leq x < 385$$

$$35 \cdot y_3 \equiv 1 \pmod{11}$$

$$35 \times (-5) + \cancel{11 \times 16} = 1$$

$$35 \times (-5) \equiv 1 \pmod{11}$$

$$y_3 = 35^{-1} \pmod{11} = -5 \pmod{11} = 6$$

i	r_i	q_i	s_i	t_i
1	35	—	1	0
2	11	3	0	1
3	2	5	1	−3
4	1	2	−5	16

Módulo 11, todo múltiplo de 11 vale 0.

5. Armar la solución

	a_i	m_i	M_i	y_i
$\left\{ \begin{array}{l} x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \\ x \equiv 10 \bmod 11 \end{array} \right.$	2	5	77	3
	3	7	55	6
	10	11	35	6

$$N = 385$$

$$0 \leq x < 385$$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3$$

Cada fila aporta un término: $a_i \cdot y_i \cdot M_i$.

5. Armar la solución

	a_i	m_i	M_i	y_i
$\left\{ \begin{array}{l} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{array} \right.$	2	5	77	3
	3	7	55	6
	10	11	35	6

$$N = 385$$

$$0 \leq x < 385$$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3$$

$$x \equiv 2 \times 3 \times 77$$

Cada fila aporta un término: $a_i \cdot y_i \cdot M_i$.

5. Armar la solución

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod{5}$	2	5	77	3
$x \equiv 3 \pmod{7}$	3	7	55	6
$x \equiv 10 \pmod{11}$	10	11	35	6

$$N = 385$$

$$0 \leq x < 385$$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3$$

$$x \equiv 2 \times 3 \times 77 + 3 \times 6 \times 55$$

Cada fila aporta un término: $a_i \cdot y_i \cdot M_i$.

5. Armar la solución

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod{5}$	2	5	77	3
$x \equiv 3 \pmod{7}$	3	7	55	6
$x \equiv 10 \pmod{11}$	10	11	35	6

$$N = 385$$

$$0 \leq x < 385$$

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3$$

$$x \equiv 2 \times 3 \times 77 + 3 \times 6 \times 55 + 10 \times 6 \times 35 \pmod{385}$$

Cada fila aporta un término: $a_i \cdot y_i \cdot M_i$.

5. Armar la solución

	a_i	m_i	M_i	y_i	
$\left\{ \begin{array}{l} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{array} \right.$	2	5	77	3	$N = 385$ $0 \leq x < 385$
	3	7	55	6	
	10	11	35	6	

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3$$

$$x \equiv 2 \times 3 \times 77 + 3 \times 6 \times 55 + 10 \times 6 \times 35 \pmod{385}$$

$$x \equiv 462 + 990 + 2100 \pmod{385}$$

Cada fila aporta un término: $a_i \cdot y_i \cdot M_i$.

5. Armar la solución

	a_i	m_i	M_i	y_i	
$x \equiv 2 \pmod{5}$	2	5	77	3	$N = 385$ $0 \leq x < 385$
$x \equiv 3 \pmod{7}$	3	7	55	6	
$x \equiv 10 \pmod{11}$	10	11	35	6	

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3$$

$$x \equiv 2 \times 3 \times 77 + 3 \times 6 \times 55 + 10 \times 6 \times 35 \pmod{385}$$

$$x \equiv 462 + 990 + 2100 \pmod{385}$$

$$x \equiv 3552 \pmod{385}$$

Cada fila aporta un término: $a_i \cdot y_i \cdot M_i$.

6. Reducir módulo N

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod{5}$	2	5	77	3
$x \equiv 3 \pmod{7}$	3	7	55	6
$x \equiv 10 \pmod{11}$	10	11	35	6

$N = 385$
 $0 \leq x < 385$

$$x \equiv 3552 \pmod{385}$$

$$3552 = 385 \times$$

Reducir módulo N : quedarnos con el residuo.

6. Reducir módulo N

	a_i	m_i	M_i	y_i
$x \equiv 2 \pmod{5}$	2	5	77	3
$x \equiv 3 \pmod{7}$	3	7	55	6
$x \equiv 10 \pmod{11}$	10	11	35	6

$N = 385$
 $0 \leq x < 385$

$$x \equiv 3552 \pmod{385}$$

$$3552 = 385 \times 9 + 87$$

Reducir módulo N : quedarnos con el residuo.

6. Reducir módulo N

	a_i	m_i	M_i	y_i
$\left\{ \begin{array}{l} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{array} \right.$	2	5	77	3
	3	7	55	6
	10	11	35	6

$$N = 385$$

$$0 \leq x < 385$$

$$x = 87$$

$$x \equiv 3552 \pmod{385}$$

$$3552 = 385 \times 9 + 87$$

$$x \equiv 3552 \equiv \boxed{87} \pmod{385}$$

Reducir módulo N : quedarnos con el residuo.

7. Comprobación

	a_i	m_i	M_i	y_i
$\left\{ \begin{array}{l} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{array} \right.$	2	5	77	3
	3	7	55	6
	10	11	35	6

$$N = 385$$

$$0 \leq x < 385$$

$$x = 87$$

$$87 = 5 \times 17 + 2 \checkmark$$

$$87 = 7 \times 12 + 3 \checkmark$$

$$87 = 11 \times 7 + 10 \checkmark$$

Comprobamos cada congruencia.

La receta

La receta

1. N : el producto de todos los módulos m_i .

La receta

1. N : el producto de todos los módulos m_i .
2. $M_i = N/m_i$ para cada congruencia.

La receta

1. N : el producto de todos los módulos m_i .
2. $M_i = N/m_i$ para cada congruencia.
3. y_i : el inverso de M_i módulo m_i (Euclides extendido).

La receta

1. N : el producto de todos los módulos m_i .
2. $M_i = N/m_i$ para cada congruencia.
3. y_i : el inverso de M_i módulo m_i (Euclides extendido).
4. Sumar los términos $a_i y_i M_i$.

La receta

1. N : el producto de todos los módulos m_i .
2. $M_i = N/m_i$ para cada congruencia.
3. y_i : el inverso de M_i módulo m_i (Euclides extendido).
4. Sumar los términos $a_i y_i M_i$.
5. Reducir la suma módulo N .