Residuos módulo n

Alexey Beshenov

23/09/2021

Congruencias

- Congruencia mód n:

$$a \equiv b \pmod{n} \iff n \mid (a - b).$$

- Relación de equivalencia:

$$a \equiv a, \quad a \equiv b \Rightarrow b \equiv a, \quad a \equiv b \text{ y } b \equiv c \Rightarrow a \equiv c.$$

- Residuos mód n = clases de equivalencia:

$$[a]_n = [b]_n \iff a \equiv b \pmod{n}.$$

- Residuos mód n:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

Congruencias

- Congruencia mód n:

$$a \equiv b \pmod{n} \iff n \mid (a - b).$$

- Relación de equivalencia:

$$a \equiv a, \quad a \equiv b \Rightarrow b \equiv a, \quad a \equiv b \text{ y } b \equiv c \Rightarrow a \equiv c.$$

- Residuos mód n = clases de equivalencia:

$$[a]_n = [b]_n \iff a \equiv b \pmod{n}.$$

- Residuos mód n:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

Congruencias

- Congruencia mód n:

$$a \equiv b \pmod{n} \iff n \mid (a - b).$$

- Relación de equivalencia:

$$a \equiv a, \quad a \equiv b \Rightarrow b \equiv a, \quad a \equiv b \text{ y } b \equiv c \Rightarrow a \equiv c.$$

- Residuos mód n = clases de equivalencia:

$$[a]_n = [b]_n \iff a \equiv b \pmod{n}.$$

- Residuos mód n:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

Congruencias

- Congruencia mód n:

$$a \equiv b \pmod{n} \iff n \mid (a - b).$$

- Relación de equivalencia:

$$a \equiv a, \quad a \equiv b \Rightarrow b \equiv a, \quad a \equiv b \text{ y } b \equiv c \Rightarrow a \equiv c.$$

- Residuos mód n = clases de equivalencia:

$$[a]_n = [b]_n \iff a \equiv b \pmod{n}.$$

- Residuos mód n:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

Congruencias

- Congruencia mód n:

$$a \equiv b \pmod{n} \iff n \mid (a - b).$$

- Relación de equivalencia:

$$a \equiv a, \quad a \equiv b \Rightarrow b \equiv a, \quad a \equiv b \text{ y } b \equiv c \Rightarrow a \equiv c.$$

- Residuos mód n = clases de equivalencia:

$$[a]_n = [b]_n \iff a \equiv b \pmod{n}.$$

- Residuos mód n:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

Aritmética de residuos

- Si $a \equiv a'$, $b \equiv b'$, entonces

$$a + b \equiv a' + b', \quad a \cdot b \equiv a' \cdot b'.$$

- Podemos poner

$$[a]_n + [b]_n = [a + b]_n, \quad [a]_n \cdot [b]_n = [a \cdot b]_n.$$

Aritmética de residuos

- Si $a \equiv a'$, $b \equiv b'$, entonces

$$a + b \equiv a' + b', \quad a \cdot b \equiv a' \cdot b'.$$

- Podemos poner

$$[a]_n + [b]_n = [a + b]_n, \quad [a]_n \cdot [b]_n = [a \cdot b]_n.$$

Aritmética de residuos

- Si $a \equiv a'$, $b \equiv b'$, entonces

$$a + b \equiv a' + b', \quad a \cdot b \equiv a' \cdot b'.$$

- Podemos poner

$$[a]_n + [b]_n = [a + b]_n, \quad [a]_n \cdot [b]_n = [a \cdot b]_n.$$

Módulo 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Módulo 6

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Residuos invertibles

- $x \in \mathbb{Z}/n\mathbb{Z}$ es **invertible** si existe $y \in \mathbb{Z}/n\mathbb{Z}$ tal que $xy = 1$.
- Equivalente: $a \in \mathbb{Z}$ es **invertible mód** n si existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$.
- Ejemplo: mód 15

x:	1	2	4	7	8	11	13	14
x^{-1}:	1	8	4	13	2	11	7	14

  $0, 3, 5, 6, 9, 10, 12$ no son invertibles
  (¿qué tienen en común?)
- $(\mathbb{Z}/n\mathbb{Z})^\times$ = residuos invertibles mód n.
- Ejercicio (!):

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid 0 \leq a < n,\ \operatorname{mcd}(a, n) = 1\}.$$

Residuos invertibles

- $x \in \mathbb{Z}/n\mathbb{Z}$ es **invertible** si existe $y \in \mathbb{Z}/n\mathbb{Z}$ tal que $xy = 1$.
- Equivalente: $a \in \mathbb{Z}$ es **invertible mód** n si existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$.
- Ejemplo: mód 15

x:	1	2	4	7	8	11	13	14
x^{-1}:	1	8	4	13	2	11	7	14

  $0, 3, 5, 6, 9, 10, 12$ no son invertibles
  (¿qué tienen en común?)
- $(\mathbb{Z}/n\mathbb{Z})^\times$ = residuos invertibles mód n.
- Ejercicio (!):

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid 0 \leq a < n,\ \operatorname{mcd}(a, n) = 1\}.$$

Residuos invertibles

- $x \in \mathbb{Z}/n\mathbb{Z}$ es **invertible** si existe $y \in \mathbb{Z}/n\mathbb{Z}$ tal que $xy = 1$.
- Equivalente: $a \in \mathbb{Z}$ es **invertible mód** n si existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$.
- Ejemplo: mód 15

x:	1	2	4	7	8	11	13	14
x^{-1}:	1	8	4	13	2	11	7	14

  $0, 3, 5, 6, 9, 10, 12$ no son invertibles
  (¿qué tienen en común?)
- $(\mathbb{Z}/n\mathbb{Z})^\times$ = residuos invertibles mód n.
- Ejercicio (!):

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid 0 \leq a < n,\ \operatorname{mcd}(a, n) = 1\}.$$

Residuos invertibles

- $x \in \mathbb{Z}/n\mathbb{Z}$ es **invertible** si existe $y \in \mathbb{Z}/n\mathbb{Z}$ tal que $xy = 1$.
- Equivalente: $a \in \mathbb{Z}$ es **invertible mód** n si existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$.
- Ejemplo: mód 15

x:	1	2	4	7	8	11	13	14
x^{-1}:	1	8	4	13	2	11	7	14

  $0, 3, 5, 6, 9, 10, 12$ no son invertibles
  (¿qué tienen en común?)
- $(\mathbb{Z}/n\mathbb{Z})^\times$ = residuos invertibles mód n.
- Ejercicio (!):

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid 0 \leq a < n,\ \operatorname{mcd}(a, n) = 1\}.$$

Residuos invertibles

- $x \in \mathbb{Z}/n\mathbb{Z}$ es **invertible** si existe $y \in \mathbb{Z}/n\mathbb{Z}$ tal que $xy = 1$.
- Equivalente: $a \in \mathbb{Z}$ es **invertible mód** n si existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$.
- Ejemplo: mód 15

x:	1	2	4	7	8	11	13	14
x^{-1}:	1	8	4	13	2	11	7	14

  $0, 3, 5, 6, 9, 10, 12$ no son invertibles
  (¿qué tienen en común?)
- $(\mathbb{Z}/n\mathbb{Z})^\times$ = residuos invertibles mód n.
- Ejercicio (!):

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid 0 \leq a < n,\ \operatorname{mcd}(a, n) = 1\}.$$

Residuos invertibles

- $x \in \mathbb{Z}/n\mathbb{Z}$ es **invertible** si existe $y \in \mathbb{Z}/n\mathbb{Z}$ tal que $xy = 1$.
- Equivalente: $a \in \mathbb{Z}$ es **invertible mód** n si existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$.
- Ejemplo: mód 15

x:	1	2	4	7	8	11	13	14
x^{-1}:	1	8	4	13	2	11	7	14

  $0, 3, 5, 6, 9, 10, 12$ no son invertibles
  (¿qué tienen en común?)
- $(\mathbb{Z}/n\mathbb{Z})^\times$ = residuos invertibles mód n.
- Ejercicio (!):

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid 0 \leq a < n,\ \operatorname{mcd}(a, n) = 1\}.$$

Teorema chino del residuo

- Sean m, n enteros coprimos ($\mathrm{mcd}(m, n) = 1$).
  Ejercicio (!): para cualesquiera $a, b \in \mathbb{Z}$ existe c tal que

$$c \equiv a \pmod{m}, \quad c \equiv b \pmod{n}.$$

- Significado: la aplicación

$$\Phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$
$$[c]_{mn} \mapsto ([c]_m, [c]_n)$$

  es sobreyectiva. De hecho, biyectiva:

$$|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z}| \times |\mathbb{Z}/n\mathbb{Z}|.$$

Teorema chino del residuo

- Sean m, n enteros coprimos ($\mathrm{mcd}(m, n) = 1$).
  Ejercicio (!): para cualesquiera $a, b \in \mathbb{Z}$ existe c tal que

$$c \equiv a \pmod{m}, \quad c \equiv b \pmod{n}.$$

- Significado: la aplicación

$$\Phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$
$$[c]_{mn} \mapsto ([c]_m, [c]_n)$$

  es sobreyectiva. De hecho, biyectiva:

$$|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z}| \times |\mathbb{Z}/n\mathbb{Z}|.$$

Teorema chino del residuo

- Sean m, n enteros coprimos ($\mathrm{mcd}(m, n) = 1$).
  Ejercicio (!): para cualesquiera $a, b \in \mathbb{Z}$ existe c tal que

$$c \equiv a \pmod{m}, \quad c \equiv b \pmod{n}.$$

- Significado: la aplicación

$$\Phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$
$$[c]_{mn} \mapsto ([c]_m, [c]_n)$$

  es sobreyectiva. De hecho, biyectiva:

$$|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z}| \times |\mathbb{Z}/n\mathbb{Z}|.$$

Ejemplo: $(m, n) = (2, 3)$

$$\Phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$
$$0 \mapsto (0, 0),$$
$$1 \mapsto (1, 1),$$
$$2 \mapsto (0, 2),$$
$$3 \mapsto (1, 0),$$
$$4 \mapsto (0, 1),$$
$$5 \mapsto (1, 2).$$

Consecuencias importantes (ejercicio)

- Versión similar con $m_1, \ldots, m_s$, $\mathrm{mcd}(m_i, m_j) = 1$.
- Para un polinomio $f(x)$ la congruencia $f(x) \equiv 0 \pmod{n}$ tiene solución para $n = p_1^{e_1} \cdots p_s^{e_s}$ si y solamente si $f(x) \equiv 0 \pmod{p_i^{e_i}}$ tiene solución para cada $i = 1, \ldots, s$.
- N = número de soluciones de $f(x) \equiv 0 \pmod{n}$.
  N_i = número de soluciones de $f(x) \equiv 0 \pmod{p_i^{e_i}}$.
  Luego, $N = N_1 \cdots N_s$.

Consecuencias importantes (ejercicio)

- Versión similar con $m_1, \ldots, m_s$, $\text{mcd}(m_i, m_j) = 1$.
- Para un polinomio $f(x)$ la congruencia $f(x) \equiv 0 \pmod{n}$ tiene solución para $n = p_1^{e_1} \cdots p_s^{e_s}$ si y solamente si $f(x) \equiv 0 \pmod{p_i^{e_i}}$ tiene solución para cada $i = 1, \ldots, s$.
- N = número de soluciones de $f(x) \equiv 0 \pmod{n}$.
  N_i = número de soluciones de $f(x) \equiv 0 \pmod{p_i^{e_i}}$.
  Luego, $N = N_1 \cdots N_s$.

Consecuencias importantes (ejercicio)

- Versión similar con $m_1, \ldots, m_s$, $\mathrm{mcd}(m_i, m_j) = 1$.
- Para un polinomio $f(x)$ la congruencia $f(x) \equiv 0 \pmod{n}$ tiene solución para $n = p_1^{e_1} \cdots p_s^{e_s}$ si y solamente si $f(x) \equiv 0 \pmod{p_i^{e_i}}$ tiene solución para cada $i = 1, \ldots, s$.
- N = número de soluciones de $f(x) \equiv 0 \pmod{n}$.
  N_i = número de soluciones de $f(x) \equiv 0 \pmod{p_i^{e_i}}$.
  Luego, $N = N_1 \cdots N_s$.

Consecuencias importantes (ejercicio)

- Versión similar con $m_1, \ldots, m_s$, $\mathrm{mcd}(m_i, m_j) = 1$.
- Para un polinomio $f(x)$ la congruencia $f(x) \equiv 0 \pmod{n}$ tiene solución para $n = p_1^{e_1} \cdots p_s^{e_s}$ si y solamente si $f(x) \equiv 0 \pmod{p_i^{e_i}}$ tiene solución para cada $i = 1, \ldots, s$.
- N = número de soluciones de $f(x) \equiv 0 \pmod{n}$.
  N_i = número de soluciones de $f(x) \equiv 0 \pmod{p_i^{e_i}}$.
  Luego, $N = N_1 \cdots N_s$.

Ejemplo: $x^2 \equiv 1 \pmod{40}$

- mód 8: cuatro soluciones

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

- mód 5: dos soluciones esperadas $x \equiv \pm 1$.
- mód 40: ocho soluciones:

$$\begin{aligned}
\mathbb{Z}/40\mathbb{Z} &\to \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \\
1 &\mapsto (1,1), \\
9 &\mapsto (1,4), \\
11 &\mapsto (3,1), \\
19 &\mapsto (3,4), \\
21 &\mapsto (5,1), \\
29 &\mapsto (5,4), \\
31 &\mapsto (7,1), \\
39 &\mapsto (7,4).
\end{aligned}$$

Ejemplo: $x^2 \equiv 1 \pmod{40}$

- mód 8: cuatro soluciones

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

- mód 5: dos soluciones esperadas $x \equiv \pm 1$.
- mód 40: ocho soluciones:

$$\begin{aligned}
\mathbb{Z}/40\mathbb{Z} &\to \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \\
1 &\mapsto (1,1), \\
9 &\mapsto (1,4), \\
11 &\mapsto (3,1), \\
19 &\mapsto (3,4), \\
21 &\mapsto (5,1), \\
29 &\mapsto (5,4), \\
31 &\mapsto (7,1), \\
39 &\mapsto (7,4).
\end{aligned}$$

Ejemplo: $x^2 \equiv 1 \pmod{40}$

- mód 8: cuatro soluciones

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

- mód 5: dos soluciones esperadas $x \equiv \pm 1$.
- mód 40: ocho soluciones:

$$\begin{aligned}
\mathbb{Z}/40\mathbb{Z} &\to \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \\
1 &\mapsto (1,1), \\
9 &\mapsto (1,4), \\
11 &\mapsto (3,1), \\
19 &\mapsto (3,4), \\
21 &\mapsto (5,1), \\
29 &\mapsto (5,4), \\
31 &\mapsto (7,1), \\
39 &\mapsto (7,4).
\end{aligned}$$

Ejemplo: $x^2 \equiv 1 \pmod{40}$

- mód 8: cuatro soluciones

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

- mód 5: dos soluciones esperadas $x \equiv \pm 1$.
- mód 40: ocho soluciones:

$$\begin{aligned} \mathbb{Z}/40\mathbb{Z} &\to \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \\ 1 &\mapsto (1,1), \\ 9 &\mapsto (1,4), \\ 11 &\mapsto (3,1), \\ 19 &\mapsto (3,4), \\ 21 &\mapsto (5,1), \\ 29 &\mapsto (5,4), \\ 31 &\mapsto (7,1), \\ 39 &\mapsto (7,4). \end{aligned}$$

Ejemplo: $x^2 \equiv 1 \pmod{40}$ **(cont.)**

- Sabiendo, que las soluciones mód 8 son $1, 3, 5, 7$, las soluciones mód 5 son $1, 4$, ¿cómo reconstruir las soluciones mód 40?
- Bézout:

$$2 \cdot 8 + (-3) \cdot 5 = 1$$

y luego

$$\begin{aligned} 16 &\equiv 0 \pmod 8, & 16 &\equiv 1 \pmod 5, \\ -15 &\equiv 1 \pmod 8, & -15 &\equiv 0 \pmod 5. \end{aligned}$$

- Por ejemplo, buscamos x tal que

$$x \equiv 5 \pmod 8, \quad x \equiv 4 \pmod 5.$$

Entonces,

$$x = 5 \cdot (-15) + 4 \cdot 16 = -11 \equiv 29 \pmod{40}.$$

Ejemplo: $x^2 \equiv 1 \pmod{40}$ **(cont.)**

- Sabiendo, que las soluciones mód 8 son $1, 3, 5, 7$, las soluciones mód 5 son $1, 4$, ¿cómo reconstruir las soluciones mód 40?
- Bézout:

$$2 \cdot 8 + (-3) \cdot 5 = 1$$

y luego

$$\begin{aligned} 16 &\equiv 0 \pmod 8, & 16 &\equiv 1 \pmod 5, \\ -15 &\equiv 1 \pmod 8, & -15 &\equiv 0 \pmod 5. \end{aligned}$$

- Por ejemplo, buscamos x tal que

$$x \equiv 5 \pmod 8, \quad x \equiv 4 \pmod 5.$$

Entonces,

$$x = 5 \cdot (-15) + 4 \cdot 16 = -11 \equiv 29 \pmod{40}.$$

Ejemplo: $x^2 \equiv 1 \pmod{40}$ (cont.)

- Sabiendo, que las soluciones mód 8 son $1, 3, 5, 7$, las soluciones mód 5 son $1, 4$, ¿cómo reconstruir las soluciones mód 40?
- Bézout:

$$2 \cdot 8 + (-3) \cdot 5 = 1$$

y luego

$$\begin{aligned} 16 &\equiv 0 \pmod 8, & 16 &\equiv 1 \pmod 5, \\ -15 &\equiv 1 \pmod 8, & -15 &\equiv 0 \pmod 5. \end{aligned}$$

- Por ejemplo, buscamos x tal que

$$x \equiv 5 \pmod 8, \quad x \equiv 4 \pmod 5.$$

Entonces,

$$x = 5 \cdot (-15) + 4 \cdot 16 = -11 \equiv 29 \pmod{40}.$$

Ejemplo: $x^2 \equiv 1 \pmod{40}$ **(cont.)**

- Sabiendo, que las soluciones mód 8 son $1, 3, 5, 7$,
  las soluciones mód 5 son $1, 4$,
  ¿cómo reconstruir las soluciones mód 40?
- Bézout:

$$2 \cdot 8 + (-3) \cdot 5 = 1$$

  y luego

$$\begin{aligned} 16 &\equiv 0 \pmod 8, & \qquad 16 &\equiv 1 \pmod 5, \\ -15 &\equiv 1 \pmod 8, & \qquad -15 &\equiv 0 \pmod 5. \end{aligned}$$

- Por ejemplo, buscamos x tal que

$$x \equiv 5 \pmod 8, \quad x \equiv 4 \pmod 5.$$

  Entonces,

$$x = 5 \cdot (-15) + 4 \cdot 16 = -11 \equiv 29 \pmod{40}.$$

Función ϕ de Euler

- Número de residuos invertibles mód n / coprimos con n:

$$\begin{aligned}\phi(n) &= \#(\mathbb{Z}/n\mathbb{Z})^\times, \\ &= \#\{1 \leq a < n \mid \text{mcd}(a,n) = 1\}.\end{aligned}$$

- Consecuencia del teorema chino del residuo:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \text{ para } \text{mcd}(m,n) = 1,$$
$$\phi(mn) = \phi(m)\,\phi(n) \text{ para } \text{mcd}(m,n) = 1.$$

- Ejercicio:

$$\phi(p^e) = p^e - p^{e-1} = p^e \left(1 - \frac{1}{p}\right),$$
$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Función ϕ de Euler

- Número de residuos invertibles mód n / coprimos con n:

$$\begin{aligned}\phi(n) &= \#(\mathbb{Z}/n\mathbb{Z})^\times, \\ &= \#\{1 \leq a < n \mid \mathrm{mcd}(a,n) = 1\}.\end{aligned}$$

- Consecuencia del teorema chino del residuo:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \text{ para } \mathrm{mcd}(m,n) = 1,$$
$$\phi(mn) = \phi(m)\,\phi(n) \text{ para } \mathrm{mcd}(m,n) = 1.$$

- Ejercicio:

$$\phi(p^e) = p^e - p^{e-1} = p^e \left(1 - \frac{1}{p}\right),$$
$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Función ϕ de Euler

- Número de residuos invertibles mód n / coprimos con n:

$$\begin{aligned}\phi(n) &= \#(\mathbb{Z}/n\mathbb{Z})^\times, \\ &= \#\{1 \leq a < n \mid \mathrm{mcd}(a,n) = 1\}.\end{aligned}$$

- Consecuencia del teorema chino del residuo:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \text{ para } \mathrm{mcd}(m,n) = 1,$$
$$\phi(mn) = \phi(m)\,\phi(n) \text{ para } \mathrm{mcd}(m,n) = 1.$$

- Ejercicio:

$$\phi(p^e) = p^e - p^{e-1} = p^e \left(1 - \frac{1}{p}\right),$$
$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Función ϕ de Euler

- Número de residuos invertibles mód n / coprimos con n:

$$\begin{aligned}\phi(n) &= \#(\mathbb{Z}/n\mathbb{Z})^\times, \\ &= \#\{1 \leq a < n \mid \text{mcd}(a,n) = 1\}.\end{aligned}$$

- Consecuencia del teorema chino del residuo:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \text{ para } \text{mcd}(m,n) = 1,$$
$$\phi(mn) = \phi(m)\,\phi(n) \text{ para } \text{mcd}(m,n) = 1.$$

- Ejercicio:

$$\phi(p^e) = p^e - p^{e-1} = p^e \left(1 - \frac{1}{p}\right),$$
$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Identidad curiosa / importante

- Ejercicio:

$$\sum_{d|n} \phi(d) = n.$$

- Ejemplo:

$$\begin{aligned} 12 &= 1 + 1 + 2 + 2 + 2 + 4 \\ &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12). \end{aligned}$$

Identidad curiosa / importante

- Ejercicio:

$$\sum_{d|n} \phi(d) = n.$$

- Ejemplo:

$$\begin{aligned} 12 &= 1 + 1 + 2 + 2 + 2 + 4 \\ &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12). \end{aligned}$$

Identidad curiosa / importante

- Ejercicio:

$$\sum_{d|n} \phi(d) = n.$$

- Ejemplo:

$$\begin{aligned} 12 &= 1 + 1 + 2 + 2 + 2 + 4 \\ &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12). \end{aligned}$$

Congruencia de Euler

- $x^{\phi(n)} = 1$ para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- $a^{\phi(n)} \equiv 1 \pmod{n}$ para $\mathrm{mcd}(a, n) = 1$.
- Generaliza el pequeño teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p} \text{ para } p \nmid a.$$

- Ejemplo: $n \mid 2^{(n-1)!} - 1$ para n impar.
  Razón: $\phi(n) \leq n - 1$, y entonces $\phi(n) \mid (n-1)!$
  Para $n = 5$:

$$2^{4!} - 1 = 16777215 = 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241.$$

Congruencia de Euler

- $x^{\phi(n)} = 1$ para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- $a^{\phi(n)} \equiv 1 \pmod{n}$ para $\mathrm{mcd}(a, n) = 1$.
- Generaliza el pequeño teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p} \text{ para } p \nmid a.$$

- Ejemplo: $n \mid 2^{(n-1)!} - 1$ para n impar.
  Razón: $\phi(n) \leq n - 1$, y entonces $\phi(n) \mid (n-1)!$
  Para $n = 5$:

$$2^{4!} - 1 = 16777215 = 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241.$$

Congruencia de Euler

- $x^{\phi(n)} = 1$ para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- $a^{\phi(n)} \equiv 1 \pmod{n}$ para $\mathrm{mcd}(a, n) = 1$.
- Generaliza el pequeño teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p} \text{ para } p \nmid a.$$

- Ejemplo: $n \mid 2^{(n-1)!} - 1$ para n impar.
  Razón: $\phi(n) \leq n - 1$, y entonces $\phi(n) \mid (n-1)!$
  Para $n = 5$:

$$2^{4!} - 1 = 16777215 = 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241.$$

Congruencia de Euler

- $x^{\phi(n)} = 1$ para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- $a^{\phi(n)} \equiv 1 \pmod{n}$ para $\text{mcd}(a, n) = 1$.
- Generaliza el pequeño teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p} \text{ para } p \nmid a.$$

- Ejemplo: $n \mid 2^{(n-1)!} - 1$ para n impar.
  Razón: $\phi(n) \leq n - 1$, y entonces $\phi(n) \mid (n-1)!$
  Para $n = 5$:

$$2^{4!} - 1 = 16777215 = 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241.$$

Congruencia de Euler

- $x^{\phi(n)} = 1$ para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- $a^{\phi(n)} \equiv 1 \pmod{n}$ para $\text{mcd}(a, n) = 1$.
- Generaliza el pequeño teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p} \text{ para } p \nmid a.$$

- Ejemplo: $n \mid 2^{(n-1)!} - 1$ para n impar.
  Razón: $\phi(n) \leq n - 1$, y entonces $\phi(n) \mid (n-1)!$
  Para $n = 5$:

$$2^{4!} - 1 = 16777215 = 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241.$$

Continuará...