Hoja 3: Función ϕ de Euler

Alexey Beshenov (cadadr@gmail.com)

23 de septiembre de 2021

Definición. Para un número natural n, la **función ϕ de Euler** es el número de los residuos invertibles mód n:

$$\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

O de manera equivalente (véase el problema 0.3), es el número de $1 \le a < n$ coprimos con n:

$$\phi(n) = \#\{1 \le a < n \mid \mathrm{mcd}(a, n) = 1\}.$$

Ejemplo. He aquí algunos valores de $\phi(n)$:

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\phi(n)$:	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8
n:	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
$\phi(n)$:	12	10	22	8	20	12	18	12	28	8	30	16	20	16	24	12	36	18	24	16
n:	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
$\phi(n)$:	40	12	42	20	24	22	46	16	42	20	32	24	52	18	40	24	36	28	58	16
n:	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
$\phi(n)$:	60	30	36	32	48	20	66	32	44	24	70	24	72	36	40	36	60	24	78	32
n:	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
$\phi(n)$:	54	40	82	24	64	42	56	40	88	24	72	44	60	46	72	32	96	42	60	40

Problema 3.1. Calcule que para un primo p y $e = 1, 2, 3, \ldots$ se tiene

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

Problema 3.2 (Multiplicatividad)**.** Demuestre que si $\mathrm{mcd}(m, n) = 1$, entonces

$$\phi(mn) = \phi(m)\,\phi(n).$$

Sugerencia: véase el problema 2.2.

Problema 3.3. Deduzca de 3.1 y 3.2 la fórmula

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

donde el producto es sobre todos los divisores primos de n.

Problema 3.4.

a) Demuestre que $\phi(n)$ es par para $n \ge 3$.

b) ¿Para cuáles n se tiene $\phi(n) \le 10$?

c) ¿Para cuáles n se tiene $\phi(n) = 100$?

Problema 3.5. Demuestre que $\phi(n) \leq n-1$ para $n \geq 2$, y la igualdad se cumple si y solo si $n = p$ es primo.

Problema 3.6 (Congruencia de Euler)**.** Sean

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{x_1, x_2, \ldots, x_{\phi(n)}\}$$

los residuos invertibles mód n.

a) Demuestre que si x es también invertible, entonces

$$\{xa_1, xx_2, \ldots, xx_{\phi(n)}\} = (\mathbb{Z}/n\mathbb{Z})^\times.$$

b) Use el punto anterior para probar la congruencia de Euler: $x^{\phi(n)} = 1$ para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, o de manera equivalente:

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \text{para } \operatorname{mcd}(a, n) = 1.$$

Note que la congruencia de Euler generaliza el pequeño teorema de Fermat.

Problema 3.7. Demuestre las siguientes identidades para cualesquiera m, n:

a) $\phi(mn) = \phi(m)\,\phi(n)\,\frac{d}{\phi(d)}$, donde $d = \operatorname{mcd}(m, n)$.

b) $\phi(\operatorname{mcd}(m, n))\,\phi(\operatorname{mcm}(m, n)) = \phi(m)\,\phi(n)$.

Problema 3.8 (Gauss)**.** Para $n \geq 1$ consideremos las fracciones

$$\frac{1}{n},\ \frac{2}{n},\ \frac{3}{n},\ \ldots,\ \frac{n-1}{n},\ \frac{n}{n}.$$

Luego escribamos cada una de la forma $\frac{a}{b}$ con $\operatorname{mcd}(a, b) = 1$.

a) Demuestre que para cada $d \mid n$, el número de fracciones en la lista con d en el denominador es precisamente $\phi(d)$.

b) Deduzca la identidad $\sum_{d|n} \phi(d) = n$, donde la suma es sobre todos los divisores de n.

Ejemplo. Para $n = 12$ tenemos

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

Problema 3.9. Demuestre que un primo p satisface $\phi(p) = 2\,\phi(p-1)$ si y solamente si $p = 2^{2^k} + 1$ para algún k (es decir, es un primo de Fermat).

Problema 3.10. Calcule la suma de los números coprimos con n:

$$\sum_{\substack{1 \leq t \leq n \\ \operatorname{mcd}(t,n)=1}} t = \frac{\phi(n)}{2}\, n.$$

Sugerencia: escriba la suma de dos maneras:

$$\sum_{\substack{1 \leq t \leq n \\ \gcd(t,n)=1}} t = \sum_{\substack{1 \leq n-t \leq n \\ \gcd(n-t,n)=1}} (n-t) = \sum_{\substack{1 \leq t \leq n \\ \gcd(t,n)=1}} (n-t).$$