アルゴリズム論特論 （塩田）

2019年5月27日

定義 法 n と整数 a について

$$ax \equiv 1 \pmod{n}$$

を満たす整数 x が存在するとき、x を法 n での a の逆数である、と言い、

$$x \equiv \frac{1}{a}, \qquad x \equiv a^{-1}$$

などと表す。(逆に a は法 n での x の逆数になる。)

定理 法 n で a の逆数が存在すること $\Longleftrightarrow \gcd(a, n) = 1$.

命題 法 n で $1^{-1} \equiv 1, \quad (n-1)^{-1} \equiv n-1$

例

$\bmod 3$: $1^{-1} \equiv 1, \quad 2^{-1} \equiv 2$

$\bmod 4$: $1^{-1} \equiv 1, \quad 3^{-1} \equiv 3$

$\bmod 5$: $1^{-1} \equiv 1, \quad 2^{-1} \equiv 3, \quad 4^{-1} \equiv 4$

$\bmod 6$: $1^{-1} \equiv 1, \quad 5^{-1} \equiv 5$

$\bmod 7$: $1^{-1} \equiv 1, \quad 2^{-1} \equiv 4, \quad 3^{-1} \equiv 5, \quad 6^{-1} \equiv 6$

$\bmod 8$: $1^{-1} \equiv 1, \quad 3^{-1} \equiv 3, \quad 5^{-1} \equiv 5, \quad 7^{-1} \equiv 7$

$\bmod 9$: $1^{-1} \equiv 1, \quad 2^{-1} \equiv 5, \quad 4^{-1} \equiv 7, \quad 8^{-1} \equiv 8$

$\bmod 10$: $1^{-1} \equiv 1, \quad 3^{-1} \equiv 7, \quad 9^{-1} \equiv 9$

$\bmod 11$: $1^{-1} \equiv 1, \quad 2^{-1} \equiv 6, \quad 3^{-1} \equiv 4, \quad 5^{-1} \equiv 9, \quad 7^{-1} \equiv 8, \quad 10^{-1} \equiv 10$

$\bmod 12$: $1^{-1} \equiv 1, \quad 5^{-1} \equiv 5, \quad 7^{-1} \equiv 7, \quad 11^{-1} \equiv 11$

$\bmod 13$: $1^{-1} \equiv 1, \quad 2^{-1} \equiv 7, \quad 3^{-1} \equiv 9, \quad 4^{-1} \equiv 10, \quad 5^{-1} \equiv 8, \quad 6^{-1} \equiv 11,$
$12^{-1} \equiv 12$

$\bmod 14$: $1^{-1} \equiv 1, \quad 3^{-1} \equiv 5, \quad 9^{-1} \equiv 11, \quad 13^{-1} \equiv 13$

$\bmod 15$: $1^{-1} \equiv 1, \quad 2^{-1} \equiv 8, \quad 4^{-1} \equiv 4, \quad 7^{-1} \equiv 13, \quad 11^{-1} \equiv 11, \quad 14^{-1} \equiv 14$

$\bmod 16$: $1^{-1} \equiv 1, \quad 3^{-1} \equiv 11, \quad 5^{-1} \equiv 13, \quad 7^{-1} \equiv 7, \quad 9^{-1} \equiv 9, \quad 15^{-1} \equiv 15$

$\bmod 17$: $1^{-1} \equiv 1, \quad 2^{-1} \equiv 9, \quad 3^{-1} \equiv 6, \quad 4^{-1} \equiv 13, \quad 5^{-1} \equiv 7, \quad 8^{-1} \equiv 15,$
$10^{-1} \equiv 12, \quad 11^{-1} \equiv 14, \quad 16^{-1} \equiv 16$

観察 法が素数 p のときは $a = 1, p-1$ 以外は $a^{-1} \neq a$ となる。(何故でしょうか。)