Simétrico módulo m

Definição. Seja m um número natural. Dois números naturais $0 \leq a, b < m$ são simétricos módulo m se $a \underset{m}{\oplus} b \equiv 0$.

Exemplos.

2 e 3 são simétricos módulo 5 ($2 \underset{5}{\oplus} 3 \equiv 0$).

0 é simétrico de si próprio módulo m ($0 \underset{m}{\oplus} 0 \equiv 0$).

5 é simétrico de si próprio módulo 10 ($5 \underset{m}{\oplus} 5 \equiv 0$).

13 é o simétrico módulo 37 de 24 ($13 \underset{37}{\oplus} 24 \equiv 0$).

- O simétrico módulo m de um número natural menor do que m existe e é único.

- Se $a \neq 0$, então o seu simétrico módulo m é igual a $m - a$.

Inverso módulo m

Definição. Seja m um número natural. Dois números naturais $0 < a, b < m$ dizem-se inversos módulo m se $a \underset{m}{\otimes} b \equiv 1$.

Exemplos.

2 e 3 são inversos módulo 5 ($2 \underset{5}{\otimes} 3 \equiv 1$).

1 é inverso de si próprio módulo m ($1 \underset{m}{\otimes} 1 \equiv 1$).

4 não tem inverso módulo 8. Para $a = 1, 2, ..., 7$; $4 \underset{8}{\otimes} a \neq 1$.

2 é o inverso módulo 101 de 51 ($2 \underset{101}{\otimes} 51 \equiv 1$).

10 é o inverso módulo 21 de 19 ($10 \underset{21}{\otimes} 19 \equiv 1$).

- Se o inverso módulo m existe, então ele é único.

- O número a tem inverso módulo m se e só se mdc(a,m)=1.

- Se p é primo, então todos os números naturais menores do que p têm inverso módulo p.