Modular Multiplicative Inverse

Given the value of A and M, find the value of X such that $AX \equiv 1 \pmod{M}$. For example, if $a = 2$ and $M = 3$, then $x = 2$, since $2 \times 2 = 4 \equiv 1 \pmod{3}$ We can rewrite the above to this:

$$AX \equiv 1 \pmod{M}$$

$$X \equiv \frac{1}{A} \pmod{M}$$

$$X \equiv A^{-1} \pmod{M}$$

Hence, the value X is known as Modular Multiplicative Inverse of A with respect to M. Modular Inverse of A with respect to M, that is,

$$X = A^{-1} \pmod{M}$$

exists, if and only if A and M are co-prime that is, if $\mathrm{G}CD(A, M) = 1$