The Cancellation Law

Question: Is it true that

$$\left.\begin{array}{rl} ab \equiv ac & (\mathrm{mod}\, m) \\ a \not\equiv 0 & (\mathrm{mod}\, m) \end{array}\right\} \quad \Rightarrow \quad b \equiv c\,(\mathrm{mod}\, m)?$$

Answer: In general, no – but yes in some cases (see Corollary below).

Theorem 3: If $g = \gcd(a, m)$, then

$$ab \equiv ac\,(\mathrm{mod}\, m) \quad \Leftrightarrow \quad b \equiv c\,(\mathrm{mod}\, \tfrac{m}{g}).$$

Corollary (Cancellation Law): If $\gcd(a, m) = 1$ then

$$ab \equiv ac\,(\mathrm{mod}\, m) \quad \Leftrightarrow \quad b \equiv c\,(\mathrm{mod}\, m).$$

In particular, if $m = p$ is prime and $a \not\equiv 0\,(\mathrm{mod}\, p)$, then

$$ab \equiv ac\,(\mathrm{mod}\, p) \quad \Leftrightarrow \quad b \equiv c\,(\mathrm{mod}\, p).$$