Solving the Congruence

$$ax \equiv b \pmod{m}$$

Note: This is closely related to solving linear Diophantine equations, for we have the equivalence

$$ax \equiv b \pmod{m} \Leftrightarrow ax - ym = b, \text{ for some } y \in \mathbb{Z}.$$

Theorem 4: a) The congruence

(1) $$ax \equiv b \pmod{m}$$

has a solution if and only if $\gcd(a, m)|b$.

b) If $g := \gcd(a, m)|b$, then there are precisely g solutions to (1) which are distinct modulo m; these are given by the formula

(2) $$x \equiv \frac{b}{g}x_0 + \frac{m}{g}t \pmod{m}, \text{ with } 0 \leq t \leq g - 1,$$

where x_0 is any solution to

(3) $$ax_0 \equiv g \pmod{m}.$$

Remarks: 1) We can solve (3) either by inspection or by the extended Euclidean algorithm.

2) In the formula (2) we can in fact take any g consecutive values of t.