Osservazione sul coefficiente a

Data una congruenza lineare risolubile

$$ax \equiv b \pmod{n},$$

e posto $d = \mathrm{MCD}(a, n)$, il problema equivale al seguente:

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\frac{n}{d}\right),$$

ove $\frac{a}{d}$ e $\frac{n}{d}$ sono coprimi. Tradotto in un'equazione di $\mathbb{Z}_{\frac{n}{d}}$, questo diventa:

$$\left[\frac{a}{d}\right]_{\frac{n}{d}} z = \left[\frac{b}{d}\right]_{\frac{n}{d}},$$

Ora, $\left[\frac{a}{d}\right]_{\frac{n}{d}}$ è un elemento invertibile dell'anello $\mathbb{Z}_{\frac{n}{d}}$. Pertanto esiste $s \in \mathbb{Z}$ tale che $\left[\frac{a}{d}\right]_{\frac{n}{d}} [s]_{\frac{n}{d}} = [1]_{\frac{n}{d}}$. Dunque l'equazione precedente equivale a quella ottenuta moltiplicando entrambi i membri per $[s]_{\frac{n}{d}}$:

$$z = \left[\frac{b}{d}s\right]_{\frac{n}{d}},$$

e, pertanto, la congruenza iniziale è equivalente alla congruenza

$$x \equiv \frac{b}{d}s \left(\mathrm{mod}\ \frac{n}{d}\right),$$

la cui soluzione generale è:

$$x_k = \frac{b}{d}s + \frac{n}{d}k, \quad \text{con } k \in \mathbb{Z}.$$