求線性同餘方程式特殊解的說明

對於線性同餘方程式：$ax \equiv b \pmod{n}$ … (1)
若 $d = \gcd(a, n)$ 整除 b，則存在 d 個解。

已知 $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$ (互質)，則存在一個特殊解 $x \equiv x_0 \pmod{\frac{n}{d}}$。

若 $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) \neq 1$，則 $\gcd(a, n) > d$。

由貝祖定理得知，存在整數對 (s, t) （可用歐幾里得延伸演算法求得），使得 $ns + at = d$ … (2)。
因此，$x_0 = (b/d)t$ 是方程式 (1) 的一個解。
$ax_0 \equiv b \pmod{n} \Rightarrow a(b/d)t \equiv b \pmod{n} \Rightarrow at \equiv d \pmod{n}$
符合方程式 (2) 去 $\bmod n$ 的結果。

由以上可知，其他的解滿足 $ax \equiv b \pmod{n}$ 皆為這種形式 $\{x_0 + k\frac{n}{d} \mid k \in \mathbb{Z}\}$

(在模 $\frac{n}{d}$ 底下，同餘 x_0 的其他解)。