Propiedades de las Congruencias

La relación de congruencia tiene muchas propiedades en común con la igualdad matemática.

- Reflexividad → $a \equiv a(mod\ m), m|a - a = 0, \forall a \in \mathbb{Z}$
- Simetría → $a \equiv b(mod\ m) \rightarrow b \equiv a(mod\ m), m|a - b \rightarrow m|b - a, \forall a, b \in \mathbb{Z}$
- Transitividad → $a \equiv b(mod\ m)$ y $b \equiv c(mod\ m) \rightarrow a \equiv c(mod\ m), \forall a, b, c \in \mathbb{Z}$
- Si *a* es coprimo con *m* y $a \equiv b(mod\ m)$ → *b* es coprimo con *m*
- Si $a \equiv b(mod\ m)$ y $k \in \mathbb{Z} \rightarrow$
  - $a + k \equiv b + k(mod\ m)$
  - $ak \equiv bk(mod\ m)$
  - $a^k \equiv b^k(mod\ m), k > 0$
- Si *k* es coprimo con *m* → existe un entero h^{-1} que $kh^{-1} \equiv 1(mod\ m) \rightarrow \frac{a}{k} \equiv \frac{b}{k}(mod\ m)$
  - $a/k = ak^{-1}$
- Como consecuencia de lo anterior, si se tiene dos congruencias con igual módulo $a \equiv b(mod\ m)$ y $c \equiv d(mod\ m) \rightarrow$
  - $a + c \equiv b + d(mod\ m)$
  - $a - c \equiv b - d(mod\ m)$
  - $ac \equiv bd(mod\ m)$