TEORÍA DE NÚMEROS

1. Congruencias

   Se dice que dos números a,b son congruentes módulo m (a$\equiv b(mod$ m))si ambos tienen el mismo resto al dividirlos por m.

   Se cumple que a$\equiv b(mod$ m)$\Longleftrightarrow$m|a-b

   Además, las congruencias pueden sumarse, restarse o multiplicarse, es decir se cumple que si a$\equiv b(mod$ m) y c$\equiv d(mod$ m) :

   a$\pm c \equiv b \pm d(mod$ m)
   a$c \equiv bd(mod$ m)

   Así, se cumple que:

   a$\equiv b(mod$ m) $\Rightarrow$a$^{k} \equiv b^{k}(mod$ m)
   a$\equiv b(mod$ m) $\Rightarrow f($a$) \equiv f(b)(mod$ m)

   donde f(x)=a$_{n}$x$^{n} + ... + a_1 x + a_0$ con a$_{i}$números enteros.

   En general, esto no se cumple para la división, pero si se cumple lo siguiente:

   mcd(c,m)=1, ca$\equiv cb(mod$ m) $\Rightarrow$a$\equiv b(mod$ m)

2. Pequeño teorema de Fermat

   Sea a un entero positivo y p un número primo. Entonces:

   a$^{p} \equiv a(mod$ p)

   Por el resultado visto en el apartado anterior sabemos que si mcd (a,p)=1, entonces

   a$^{p-1} \equiv 1(mod$ p)