Taller de matematicas
Guanajuato, 10 marzo 1995.

Congruencias

Definicion de congruencia: Se dice que dos numeros, N y M, son "congruentes modulo d", y se escribe $N \equiv M \pmod{d}$, si al dividir N o M entre d, sobra lo mismo residuo.
Algunos ejemplos:
1. $8 \equiv 5 \pmod{3}$, porque si dividimos 8 o 5 entre 3, sobra 2, lo mismo residuo.
2. $128 \equiv 0 \pmod{4}$, porque al dividir 128 entre 4 no sobra nada (128 es divisible por 4).
3. $N \equiv 0 \pmod{2}$ es lo mismo como decir "N es un numero par", y $N \equiv 1 \pmod{2}$ es lo mismo como decir "N es un numero impar".
4. $1995 \equiv 95 \pmod{100}$, y mas generalmente, un numero es congruente a 95 modulo 100 si sus ultimos dos digitos son 95.

Pregunta: Es posible tambien tener congruencia entre numeros *negativos* ? por ejemplo, que significa $N \equiv -1 \pmod{3}$?
Respuesta: Si! Hay una otra definicion de congruencia que incluye naturalmente el caso que uno o los dos numeros son negativos:
Definicion de congruencia (segunda version): $N \equiv M \pmod{d}$ cuando la *diferencia* entre N y M es divisible entre d.
Algunos ejemplos:
1. $7 \equiv -3 \pmod{10}$, porque la diferencia entre 7 y -3 es 10, divisible por 10.
2. $999 \equiv -1 \pmod{10}$, porque la diferencia es 1000, divisible por 10.
1. $8 \equiv 5 \pmod{3}$, porque la diferencia es 3, divisible por 3.
Pregunta: Porque son las mismas, las dos definiciones, en el caso de congruencia de dos numeros positivos? dejamos al estudiante encontrar la respuesta.

Dos propiedades importantes: Suponemos que tenemos 5 numeros M, N, m, n y d, tal que $M \equiv m$ y $N \equiv n \pmod{d}$, entonces:
1. $M + N \equiv m + n \pmod{d}$, y
2. $M \cdot N \equiv m \cdot n \pmod{d}$.

La demonstracion que estas dos propiedades son correctas no es dificil y lo dejamos al estudiante. Sin embargo, son muy utiles y aqui damos algunos ejemplos.
Ejemplos:
1. $8 \equiv 2 \pmod{3}$ y $10 \equiv 1 \pmod{3}$ asi que
$8 + 10 \equiv 2 + 1 \equiv 3 \equiv 0 \pmod{3}$, y
$8 \cdot 10 \equiv 2 \cdot 1 = 2 \pmod{3}$.
2. $10 \equiv 1 \pmod{3}$ asi que
$100 = 10 \cdot 10 \equiv 1 \cdot 1 = 1 \pmod{3}$, y tambien
$1000 = 10 \cdot 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1 = 1 \pmod{3}$, etcetera...
3 . $10 \equiv 1 \pmod{9}$ asi que
$10^{1995} = 1000...0$ (1995 ceros)$= 10 \cdot 10 \cdot ... \cdot 10$ (1995 veces) $\equiv 1 \cdot 1 \cdot ... \cdot 1$ (1995 veces) $= 1 \pmod{9}$, asi que al dividir 10^{1995} por 9 sobra 1 !
4. Como saber si el numero 2^{1000} es divisible por 7? vamos a ver:
$2^3 = 8 \equiv 1 \pmod{7}$, y $1000 = 3 \cdot 333 + 1$, asi que
$2^{1000} = (2^3)^{333} \cdot 2 \equiv 1^{333} \cdot 2 = 2 \pmod{7}$.
Entonces, al dividir 2^{1000} entre 7 sobra 2, asi que la respuesta es... no!
5. Como saber si 2784 es divisible por 3 sin intentar dividirlo? calculamos modulo 3, usando ejemplo 2:
$2784 = 2 \cdot 1000 + 7 \cdot 100 + 8 \cdot 10 + 4 \equiv 2 \cdot 1 + 7 \cdot 1 + 8 \cdot 1 + 4 = 2 + 7 + 8 + 4 \equiv 2 + 1 + 2 + 1 = 6 \equiv 0 \pmod{3}$.
Respuesta: si, es divisible por 3. Y tambien vemos que para saber si un numero es divisible por 3 es suficiente checar si la suma de sus digitos es divisible por 3.

6. (Un ejemplo un poco mas avansado) Existe un numero k tal que 3^k se acaba con ...001?
Solucion: Primero encontramos un numero N tal que $3 \cdot N \equiv 1 \pmod{1000}$. Es decir, $3 \cdot N$ es un numero divisible entre 3 que acaba con 001. Es bastante facil: por ejemplo, $3 \cdot N = 2001$ satisfase esos requisitos (la suma de sus digitos es 3 asi que es divisible entre 3).Asi que N puede ser $2001/3 = 667$.

Ahora examinamos los ultimos 3 digitos de los numeros $3^1, 3^2, 3^3, ..., 3^{1001}$. Como son 1001 numeros y hay solo 1000 posibilidades para los ultimos 3 digitos de un numewro (000, 001, 002,..., 999) entonces por lo menos dos de estos 1001 numeros tienen que tener los mismos ultimos 3 digitos. En otras palabras, tenemos dos numeros entre estos 1001 numeros, de la forma 3^m y 3^{m+k}, tal que

$$3^{m+k} \equiv 3^m \pmod{1000}.$$

Eso implica que

$$3^{m+k} \cdot N^m \equiv 3^m \cdot N^m = (3 \cdot N)^m \equiv 1^m = 1 \pmod{1000},$$

y por otro lado

$$3^{m+k} \cdot N^m = 3^k \cdot 3^m \cdot N^m = 3^k \cdot (3 \cdot N)^m \equiv 3^k \cdot 1^m = 3^k \pmod{1000},$$

asi que $3^k \equiv 1 \pmod{1000}$, lo qual nos dice que 3^k es un numero que acaba con 001.