Material de Apoyo
21 de Septiembre de 2011

1. Números primos

Entre los enteros positivos hay una sub-clase de importancia particular, la clase de los primos. Un número entero positivo p se llama *primo* si

(i) $p > 1$,
(ii) p no tiene divisores positivos además de 1 y p.

Por ejemplo, 37 es un primo. Es importante notar que 1 no se considera primo. Normalmente reservamos la letra p para los primos.

Un número entero positivo mayor que 1 y no primo se llama *compuesto*. Aquí está nuestro primer teorema:

Teorema 1. *Todo entero positivo, con excepción del 1, es un producto de primos.*

Demostración. Sea n un entero positivo mayor que 1. Si n es primo, no hay nada que probar. Si n no es primo, o sea compuesto, entonces tiene divisores entre 1 y n. Si m es el m'as pequeño entre estos divisores, m debe ser primo; porque si no, entonces m tendría un divisor l, $1 < l < m$, que necesariamente ser'ia también un divisor de n. Esto contradice la elección de m como el divisor m'as pequeño; as'i que m debe ser primo.

Concluimos entonces que si n no es primo es divisible entre un primo, digamos p_1, o sea

$$n = p_1 n_1,$$

donde n_1 es un entero positivo, $1 < n_1 < n$. Si n_1 es primo la demostración est'a terminada, y si no, continuamos como antes: n_1 es divisible entre un primo p_2 menor que n_1, as'i que

$$n = p_1 n_1 = p_1 p_2 n_2,$$

donde n_2 es un entero positivo, $1 < n_2 < n_1 < n$.

As'i seguimos y obtenemos una sucesión decreciente de enteros positivos $n > n_1 > n_2 > n_3 > \ldots > 1$. Tarde o temprano este proceso tiene que parar, o sea obtenemos un $n_k = p_k$ primo, y

$$n = p_1 p_2 p_3 \ldots p_{k-1} p_k. \tag{1}$$

Esto completa la demostración. $\square$

2. Congruencias

2.1. Definición de congruencias

Si un entero positivo m divide a la diferencia $a-b$ de dos números, decimos que "a es *congruente* a b módulo m", y lo escribimos

$$a \equiv b \pmod{m}.$$

Por ejemplo,

$$5 \equiv 9 \pmod{4}, \quad -8 \equiv 3 \pmod{1}1, \quad 1997 \equiv 7 \pmod{10}, \text{ y } 10^n \equiv 1 \pmod{9},$$

para todo $n > 0$.

Esta definición no introduce nada nuevo, porque "$a \equiv b \pmod{m}$" y "$m|(a-b)$" tienen exactamente el mismo significado; pero cada notación tiene su ventaja.

Notamos que en esta definición a y b no tienen que ser números positivos, y de hecho ni enteros, aunque nosotros no lo vamos a usar más que para números enteros.

Si $x \equiv a \pmod{m}$ decimos tambien que "a es un *residuo* de x" $\pmod{m}$. Si $0 \le a \le m-1$, llamamos a a el residuo *mínimo* (no-negativo) de x, módulo m. As'i que dos números a y b son congruentes $\pmod{m}$ si tienen los mismos residuos $\pmod{m}$.

El residuo mínimo $\pmod{m}$ de un entero no-negativo x se puede determinar as'i: se divide x entre m, y lo que *sobra* es el residuo mínimo. Por ejemplo, el residuo mínimo de 100 $\pmod{7}$ es 2, porque al dividir 100 entre 7 el resultado es 14 (esto no importa) y sobran 2 (esto s'i importa). El residuo mínimo de $-100 \pmod{7}$ es $7-2=5$. (¿Por qué?)

Una *clase de residuos* $\pmod{m}$ es la clase de todos los números congruentes a un número dado $\pmod{m}$. Por ejemplo, la clase de residuos de $3 \pmod{5}$ consiste de los números

$$\ldots -12, -7, -2, \ 3, \ 8, \ 13, \ 18, \ldots,$$

y la clase de residuos de $0 \pmod{m}$ consiste de todos los múltiplos de m

$$\ldots, -3m, -2m, -m, \ 0, \ m, \ 2m, \ 3m, \ldots.$$

Cada miembro de una clase de residuos $\pmod{m}$ se llama un *representante* de la clase. Obviamente hay m clases de residuos $\pmod{m}$, representados por los residuos mínimos

$$0, 1, 2, 3, \ldots, m-1.$$

Las congruencias son de gran importancia práctica en la vida cotidiana. Por ejemplo, "hoy me levant'e a las 6 de la mañana" es una afirmación acerca del número de horas que han pasado, módulo 24, desde algún tiempo fijo. La clase de residuos de este número de horas, o sea la hora del d'ia, es normalmente mucho m'as importante que el número real de horas que han pasado desde, digamos, la creación del universo. Calendarios y horarios de camión o clases, son tablas de congruencias, módulo 7, 365 y 24.

2.2. Propiedades elementales de congruencias

Es fácil demostrar que congruencias módulo un entero positivo fijo m satisfacen las siguientes propiedades:

$$\begin{array}{lll} (i) & a \equiv b & \Longrightarrow \ b \equiv a, \\ (ii) & a \equiv b, b \equiv c & \Longrightarrow \ a \equiv c, \\ (iii) & a \equiv b & \Longrightarrow \ ka \equiv kb, \text{ para cualquier } k, \\ (iv) & a \equiv a\text{'}, b \equiv b\text{'} & \Longrightarrow \ a + b \equiv a\text{'} + b\text{'} \quad \text{y} \quad ab \equiv a\text{'}b\text{'}. \end{array}$$

Demostramos por ejemplo (iii). Si $a \equiv b$ entonces $m|(a-b)$ as'i que existe un l tal que $a - b = ml$. As'i que $k(a-b) = ka - kb = mlk$, as'i que $m|ka - kb$, y obtenemos que $ka \equiv kb \pmod{m}$.

Los problemas con asterisco (*) los pueden entregar y les contara como extra. Los problemas con doble asterisco(**) son para aquellos que hallan tenido problemas con las definiciones y/o problemas de la tarea pasada.