Tarea seis.
Teoría de números uno.

Contreras Mendoza Ximena de la Luz

12 de mayo de 2020

Proposición 1.
Sea $m = 6$. Veamos que los números primos son congruentes a 1 ó a 5 (módulo 6), salvo 2 y 3 que son congruentes a 2 y 3 respectivamente.

En efecto sea p primo con $p \geq 5$. Si $p = 5 \Rightarrow p \equiv 5 \ (mod\, 6)$ supongamos $p > 5$, en particular p es impar entonces p no puede ser de la forma $6k+2, 6k+4$ ni $6k$.
Si p es de la forma $6k+2 = 2(3k+1)$ entonces p es par ¡contradicción!.
Si p es de la forma $6k+4 = 2(3k+2)$ entonces p es par ¡contradicción!.
Si p es de la forma $6k = 2(3k)$ entonces p es par ¡contradicción!.
Entonces a p le queda ser de la forma $6k+1, 6k+3$ ó $6k+5$. Observemos que sí p es de la forma $6k+3 = 3(3k+1) \Rightarrow 3 \mid p$ ¡contradicción! pues $p > 5$. Por lo tanto si p es un primo impar debe de ser de la forma $6k+1$ ó $6k+5$. Solo para confirmar veamos que, efectivamente los números de la forma $6k+1$ ó $6k+5$ son impares. $6k+1 = 2(3k)+1$ número impar y $6k+5 = 2(3k+1)+1$ número impar. $\star$

Ejercicio 1. Pruebe que hay una infinidad de primos p que son congruentes a 5 módulo 6, es decir $\#\{p \in \mathbb{P} : p \equiv 5 \ (mod\, 6)\} = \infty$

Demostración. Supongamos que hay una cantidad finita de primos p congruentes a 5 módulo 6.
Sea $\mathbb{P}_{\equiv 5} := \{p_1, ..., p_t\}$ donde $p_1 = 5$ y para toda $i \geq 2$, $p_i > 5$. Sea $N = 6(p_2 \cdot ... \cdot p_t) + 5$. Como $N > 1 \quad \exists q \in \mathbb{P}$ tal que $q \mid N$.
Observación 1. $q \neq 5$
Si $q = 5 \Rightarrow 5 \mid N = 6(p_2 \cdot ... \cdot p_t) + 5$ como $5 \mid 5 \Rightarrow 5 \mid 6(p_2 \cdot ... \cdot p_t) \Rightarrow 5 \mid 6$ ó $5 \mid p_1$ ó ... ó $5 \mid p_t$ ¡contradicción!. Por lo tanto $q \neq 5$.
Observación 2. $q \notin \mathbb{P}_{\equiv 5}$
Si $q \in \mathbb{P}_{\equiv 5} \Rightarrow q = p_i$ para alguna $i \in \{2, ..., t\}$ y de esta manera $q \mid 6(p_2 \cdot ... \cdot p_t) \Rightarrow q \mid N - 6(p_2 \cdot ... \cdot p_t) = 5$ ¡contradicción!.

Concluimos que $q \in \mathbb{P}$ tal que $q \notin \mathbb{P}_{\equiv 5}$. Entonces por la **Proposición 1.** debe suceder que $q \equiv 1 \ (mod\, 6)$.
Hemos probado que todos los divisores primos de N son congruentes a 1 módulo 6. Sea $N = q_1, ..., q_n$ factorización en primos de N. Por lo anterior tenemos que

$$5 \equiv 0 + 5 \equiv 6(p_2 \cdot ... \cdot p_t) + 5 \equiv N \equiv q_1, ..., q_n \equiv 1 \quad (mod\, 6)$$

Por lo tanto $5 \equiv 1 \quad (mod\, 6)$ ¡contradicción!. Por lo tanto N no puede existir. Esta contradicción surge de suponer que $\mathbb{P}_{\equiv 5}$ es finito. Por lo tanto $\mathbb{P}_{\equiv 5}$ debe ser infinito. $\square$

Ejercicio 2. Sea $n \in \mathbb{Z}^+$ con expansión decimal $n = a_s \cdot ... \cdot a_0$ es decir $n = a_0 + 10a_1 + ... + 10^s a_s$. Pruebe que $11 \mid n \iff 11 \mid a_0 - a_1 + ... + a_s(-1)^s$

Demostración. Sea $n \in \mathbb{Z}^+$ con expansión decimal $n = a_0 + 10a_1 + ... + 10^s a_s$. Por otro lado, observemos que $10 \equiv -1 \quad (mod\ 11) \Rightarrow 10^k \equiv (-1)^k \quad (mod\ 11)$ para toda $k > 0$. Entonces

$$n \equiv a_0 + 10a_1 + ... + 10^s a_s \equiv a_0 - a_1 + ... + (-1)^s a_s \quad (mod\ 11)$$

$\therefore \quad n \equiv a_0 - a_1 + ... + (-1)^s a_s \quad (mod\ 11)$ Por lo tanto

$$11 \mid n \iff n \equiv 0 \quad (mod\ 11) \iff a_0 - a_1 + ... + (-1)^s a_s \equiv 0 \quad (mod\ 11) \iff 11 \mid a_0 - a_1 + ... + (-1)^s a_s$$

$\square$

Ejercicio 3. Pruebe que la ecuación $7x^3 + 2 = y^3$ no tiene solución en los enteros.

Demostración. Tomemos la ecuación

$$7x^3 + 2 = y^3 \tag{1}$$

Supongamos $\exists x_0, y_0 \in \mathbb{Z}$ tal que son solución a la ecuación (1) es decir $7(x_0)^3 - (y_0)^3 + 2 = 0$ entonces la congruencia $7(x_0)^3 - (y_0)^3 + 2 \equiv 0 \pmod{m}$ se satisface para cualquier $m > 0$.
Consideremos $m = 7$ entonces

$$(y_0)^3 \equiv 7(x_0)^3 + 2 \equiv 2 \pmod{7}$$

Veamos que ningún entero cumple la congruencia

$$x^3 \equiv 2 \pmod{7} \tag{2}$$

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34
35	36	37	38	39	40	41

Cuadro 1: Congruencias del siete.

Tenemos los siguientes valores $0, 1, 2, 3, 4, 5$ y 6. Sustituimos en la ecuación (2) tenemos:

$0^3 \equiv 0 \pmod{7}$
$1^3 \equiv 1 \pmod{7}$
$2^3 = 8 \equiv 1 \pmod{7}$
$3^3 = 27 \equiv 6 \pmod{7}$
$4^3 = (16)(4) \equiv (2)(4) \equiv 8 \equiv 1 \pmod{7}$
$5^3 = (25)(5) \equiv (4)(5) \equiv 20 \equiv 6 \pmod{7}$
$6^3 = (36)(6) \equiv (1)(6) \equiv 6 \pmod{7}$

Por lo tanto ningún entero elevado al cubo puede ser congruente con dos módulo siete. Por lo tanto nuestra solución no es entera i.e. $x_0, y_0 \notin \mathbb{Z}$ □

Ejercicio 4. Sea f un polinomio con coeficientes enteros y sea $m > 1$ fijo. Pruebe que podemos descomponer una ecuación módulo m en varias ecuaciones módulo potencias de primos según la factorización de m.

Demostración. Escribimos lo que queremos probar. Sea $m > 1$ fijo con factorización en primos $m = p_1^{\beta_1} \cdots p_s^{\beta_s}$. Pruebe que $\exists x_0 \in \mathbb{Z}$ tal que $f(x_0) \equiv 0 \pmod{m} \iff \exists x_0 \in \mathbb{Z}$ tal que $f(x_0) \equiv 0 \pmod{p_i^{\beta_i}}\ \forall\, i = 1, ..., s$

$\Rightarrow$) Sea $f(x) \in \mathbb{Z}[x]$. Por hipótesis $\exists x_0 \in \mathbb{Z}$ tal que

$$f(x_0) \equiv 0 \pmod{m} \Leftrightarrow m \mid f(x_0) - 0 \Rightarrow f(x_0) = mk = (p_1^{\beta_1} \cdots p_s^{\beta_s})k$$

Podemos factorizar alguna $p_i^{\beta_i}$ con $1 \leq i \leq s$ es decir

$$f(x_0) = p_i^{\beta_i}(p_1^{\beta_1} \cdots (p_{i-1}^{\beta_{i-1}})(p_{i+1}^{\beta_{i+1}}) \cdots p_s^{\beta_s})k \quad \Rightarrow \quad p_i^{\beta_i} \mid f(x_0) \Leftrightarrow f(x_0) \equiv 0 \pmod{p_i^{\beta_i}}\ \forall\, i = 1, ..., s.$$

$\Leftarrow$) Sea $f(x) \in \mathbb{Z}[x]$. Consideremos el Mínimo Común Múltiplo de $p_1^{\beta_1}, ..., p_s^{\beta_s}$

$$[p_1^{\beta_1}, ..., p_s^{\beta_s}] = \frac{p_1^{\beta_1} \cdots p_s^{\beta_s}}{(p_1^{\beta_1}, ..., p_s^{\beta_s})} = \frac{m}{1}$$

Por hipótesis $\exists x_0 \in \mathbb{Z}$ tal que $f(x_0) \equiv 0 \pmod{p_i^{\beta_i}}\ \forall\, i = 1, ..., s \iff p_i^{\beta_i} \mid f(x_0) \quad \forall\, i$. Entonces por definición de Mínimo Común Múltiplo

$$m = [p_1^{\beta_1}, ..., p_s^{\beta_s}] \mid f(x_0) \iff f(x_0) \equiv 0 \pmod{m}$$

□