SOLUCION DE PROBLEMAS

126.- Sea $\varphi(n) = n \prod_{p|n} (1-1/p)$ la función de EULER. Demostrar que $\varphi(ab)=\varphi(a)$. $\varphi(b)$ si a y b son primos entre sí. Deducir entonces que

$$\varphi(ab) = d\varphi(a)\varphi(b)/\varphi(d),$$

donde d es el máximo común divisor de a y b.

: Por definición:

$$(1) \qquad \varphi(ab) = ab \prod_{p|a.b} (1-1/p).$$

como a y b son primos entre sí, si p divide a ab $(p|ab)$, tenemos que p divide sea a sea a b, pero no a ambos. Por tanto, el producto que aparece en (1) puede descomponerse en dos factores: $P_1 = \prod_{p|a} (1-1/p)$ y $P_2= \prod_{p|b}(1-1/p)$, de donde

$$\varphi(ab) = (aP_1)(bP_2) = \varphi(a)\varphi(b).$$

Si a y b **no** son primos entre sí, entonces $\varphi(ab) = ab\, P_1P_2/P_3$, donde P_3 es el producto de los $(1-1/p)$ para los cuales p divide simultáneamente a a y a b, es decir, para los cuales p es un factor primo del máximo común divisor d de a y b. Podemos escribir entonces

$$\varphi(ab) = d(aP_1)(bP_2)/(dP_3),$$

lo cual demuestra lo pedido. Para otra demostración, consultar, por ejemplo, F.VERA, Aritmética Moderna, Bogotá: Inst. Gráfico, 1943.

JOSE JIMENEZ

(Otras soluciones de : Guillermo Tello, Ricardo Plata.)

133.- Sea p un número primo. a) Demostrar que

$$p^{n+1} \mid \binom{n}{k} p^{n(p-k)}$$

Si $0 < k < p$.

b) Usando que $p^{n+1}|p^{np}$ para $p > 1$, y la parte a), demostrar que si $a \equiv b$ (mod p^n), entonces $a^p \equiv b^p$ (mod p^{n+1}).

a) Sabemos que si p es primo, entonces $p > 1$. Hagamos $P_k= \binom{p}{k}p^{n(p-k)} = \frac{(p-1)!}{(p-k)!k!} p^{n(p-k)+1}$; si $0 < k < p$, entonces $p-k \geq 1$, por tan to, $n(p-k)+1 \geq n+1$; es decir, p^{n+1} divide a P_k si $0 < k < p$, como se pedía.

b) Como $a \equiv b(\text{mod } p))$, entonces existe un entero h tal que $a = b + hp^n$ (VINOGRADOV, Elements of Number Theory, Dover). Podemos escribir entonces,

$$(1) \qquad a^p = (b + hp^n)^p = \sum_{k=0}^{p} \binom{p}{k} b^k h^{p-k} p^{n(p-k)}.$$

Cuando $k = 0$, p^{np} es divisible por p^{n+1}, ya que $p > 1$. Luego, la identidad (1) puede escribirse

$$a^p = b^p + \sum_{k=1}^{p-1} \binom{p}{k} b^k h^{p-k} p^{n(p-k)},$$

y como cada $\binom{p}{k} b^k h^{p-k} p^{n(p-k)}$, $k = 0,\dots,p-1$, es divisible por p^{n+1}, resulta que

$$a^p \equiv b^p (\text{mod } p^{n+1}).$$

GERMAN LOPEZ
Universidad la Gran Colombia

136.- Dado lo elemental del problema no publicamos las soluciones.

138.- Determinar los enteros a y n para los cuales $a^n + 1$ es divisible por 10.

Se trata de encontrar los n para los cuales el polinomio

$$f(x) = x^n + 1$$

tiene raíces en $\mathbb{Z}/(10)$, y de determinar éstas. Observamos, en primer lugar, que la ecuación $x^n + 1 \equiv 0(\text{mod } 10)$ no admite ceros pares. Luego debemos restringir nuestra discusión a los valores impares de x comprendidos entre 0 y 9. Si n es impar, tenemos

$$(1) \qquad f(x) = x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + \dots + 1)$$

y $x \equiv -1 \equiv 9$ (mod 10) es una solución de $f(x) \equiv 0$ (mod 10); es decir, los números de la forma $x = 9 + 10.k$, $k = 0, \pm 1, \pm 2, \dots$, son tales que $x^n + 1$ es divisible por 10, si n es impar. Es fácil ver que si $x = 1,3,5,7$, entonces para n impar, $x^n + 1 \not\equiv 0(\text{mod } 10)$. Así: si $x = 1$, es claro que $1^n+1=2 \not\equiv 0(\text{mod } 10)$ (esto para n par o impar). Si $x = 3$, x^n puede escribirse bajo la forma $a_k.10^k + \dots + a_1.10 + a_0$, donde $a_0 = 3$ ó 7; si $x = 5$, vemos que $x^n = a_k.10^k + \dots + a_1.10 + 5$, lo cual nos indica otra vez que x^n+1 no es divisible por 10 (para n par o impar); si $x = 7$, es fácil ver también que $x^n = a_k.10^k + \dots + a_0$, donde $a_0 = 1$ ó 3, lo cual nós dice que $x^n + 1$ no es divisible por 10 (n impar).

Consideremos ahora el caso n par. Como hemos observado, basta conside rar $x = 3$ y $x = 7$. Ahora bien $(3)^{2r} = (9)^r$ (respectivamente, $(7)^{2r} = (49)^r$) termina en 9 si y sólo si r es impar (la condición de terminar en 9 x^n es necesaria y suficiente para que $x^n + 1$ sea divisible por 10); luego si $n = 2(2j+1) = 4j+2$ $(j=0,1,2,\ldots)$, 3 (respectivamente, 7) es una solución de la ecuación

$$(2) \qquad x^n + 1 = x^{4j+2} + 1 \equiv 0 \pmod{10} \quad (j=0,1,2,\ldots)$$

Y éstos son los únicos casos posibles. Resumiendo, tenemos:

a) Si n es impar, $x^n + 1 \quad 0 \pmod{10}$ admite una única raíz: $x \quad 9 \pmod{10}$;

b) si n es par, $x^n + 1 \equiv 0 \pmod{10}$ admite soluciones si y sólo si n es de la forma $4j + 2$ $(j=0,1,2,\ldots)$ y éstas son $x \equiv 3,7 \pmod{10}$.

O también:

a) si n es impar, los números de la forma $x = 9 + 10.k = 0,\pm1,\pm 2,\ldots$ son los únicos tales que $x^n + 1$ es divisible por 10;

b) los únicos enteros x y n tales $x^n + 1$ es divisible por 10, siendo n par, corresponden a $n = aj+2$, $j = 0,1,2,\ldots$, y $x = 3 + 10.k$, $x = 7 + 10.h$ $(k,h = 0,\pm1,\pm2,\ldots)$

FRANCISCO JARAMILLO

(Otras soluciones de: V. Prieto, J. Salazar, R. Franky)