

Universidad de la República - Facultad de Ingeniería - IMERL
Matemática Discreta 2, semipresencial

SOLUCIÓN SEGUNDA PRUEBA (PRIMER PARCIAL) - 30 DE SETIEMBRE DE 2016.

Ejercicio 1. (8 puntos) Calcular 3^{163} (mód 89).

Solución: Observar primero que $3^{163} = 3^{88}3^{75}$. Como $\text{mcd}(89, 3) = 1$ (obsérvese que 89 es primo), entonces $3^{88} \equiv 1$ (mód 89), por el teorema de Fermat o de Euler. Entonces $3^{163} \equiv 3^{75}$ (mód 89). Para calcular 3^{75} (mód 89) usaremos el método de exponenciación rápida. Para eso obsérvese que: $75 = 64 + 8 + 2 + 1 = 2^6 + 2^3 + 2^1 + 2^0$.

Planteamos la tabla:

n	3^{2^n} (mód 89)
0	3
1	9
2	$81 \equiv -8$
3	$64 \equiv -25$
4	$625 \equiv 2$
5	4
6	16

Entonces $3^{163} \equiv 3^{75}$ (mód 89) $\equiv 3^{2^6}3^{2^3}3^{2^1}3^{2^0}$ (mód 89) $\equiv 16 \times 64 \times 9 \times 3$ (mód 89) $\equiv 32 \times 3 \times 32 \times 3 \times 3$ (mód 89) $\equiv 7 \times 7 \times 3$ (mód 89) $\equiv 58$ (mód 89). Finalmente se obtiene que $3^{163} \equiv 58$ (mód 89).

Ejercicio 2. (8 puntos) Sea $a, b, c, n \in \mathbb{N}$ con $c \neq 0$.

Demostrar que, si $ca \equiv cb$ (mód n) entonces $a \equiv b$ (mód $b \frac{n}{\text{mcd}(c, n)}$).

Solución: (esto es parte del teórico, página 27, Proposición 2.2.4 del Capítulo 2).

Si llamamos $d = \text{mcd}(c, n)$ tenemos que $c = dc^*$ y $n = dn^*$, con c^*, n^* enteros coprimos. Si $ca \equiv cb$ (mód n), entonces $dc^*a \equiv dc^*b$ (mód dn^*), con lo cual se obtiene que $c^*a \equiv c^*b$ (mód n^*). Ahora como $\text{mcd}(c^*, n^*) = 1$, se concluye que $a \equiv b$ (mód n^*); es decir $a \equiv b$ (mód $\frac{n}{\text{mcd}(c, n)}$).

Ejercicio 3. (14 puntos) Se dice que un entero n es un *Pseudoprimo de Carmichael* si n es compuesto y $a^n \equiv a$ (mód n) para todo $a \in \mathbb{N}$.

a. Sea b un número entero positivo y coprimo con 561.

- i) Demostrar que $b^2 \equiv 1$ (mód 3), $b^{10} \equiv 1$ (mód 11) y $b^{16} \equiv 1$ (mód 17).
- ii) Hallar b^{560} (mód 3), b^{560} (mód 11) y b^{560} (mód 17).
- iii) Probar que 561 es un Pseudoprimo de Carmichael (*Sug: hallar b^{561} dependiendo si b es coprimo o no con 561*).

b. Sea n compuesto y libre de cuadrados (no es divisible por ningún cuadrado), tal que todo divisor primo p de n cumple que $p-1|n-1$. Probar que n es un pseudoprimo de Carmichael.

Solución:

- a. i) Como $\text{mcd}(b, 561) = 1$ y $561 = 3 \times 11 \times 17$ (descomposición en factores primos), entonces $\text{mcd}(b, 3) = 1$, $\text{mcd}(b, 11) = 1$, $\text{mcd}(b, 17) = 1$. Luego, por el Teorema de Fermat tenemos que: $b^2 \equiv 1$ (mód 3), $b^{10} \equiv 1$ (mód 11) y $b^{16} \equiv 1$ (mód 17).
- ii) Observemos para este punto que 560 se puede escribir de las siguientes formas: $560 = 2 \times 280 = 10 \times 56 = 16 \times 35$. Entonces $b^{560} = (b^2)^{280} \equiv (1)^{280}$ (mód 3), pues, por el punto anterior $b^2 \equiv 1$ (mód 3). También $b^{560} = (b^{10})^{56} \equiv (1)^{56}$ (mód 11), pues, por el punto anterior $b^{10} \equiv 1$ (mód 11). Finalmente vale también que $b^{560} = (b^{16})^{35} \equiv (1)^{35}$ (mód 17), pues, por el punto anterior $b^{16} \equiv 1$ (mód 17).

iii) Si 3 no divide a b entonces $b^2 \equiv 1 \pmod{3}$, por lo tanto $b^{560} = (b^2)^{280} \equiv (1)^{280} \equiv 1 \pmod{3}$. O sea que $b^{560} \equiv 1 \pmod{3}$ y por lo tanto $b^{561} \equiv b \pmod{3}$.

Si 3 divide a b entonces es claro que $b^{561} - b$ es múltiplo de 3. O sea que también vale $b^{561} \equiv b \pmod{3}$.

Conclusión, en ambos casos vale que $b^{561} \equiv b \pmod{3}$.

Si 11 no divide a b entonces $b^{10} \equiv 1 \pmod{11}$, por lo tanto $b^{560} = (b^{10})^{56} \equiv (1)^{56} \equiv 1 \pmod{11}$. O sea que $b^{560} \equiv 1 \pmod{11}$ y por lo tanto $b^{561} \equiv b \pmod{11}$.

Si 11 divide a b entonces es claro que $b^{561} - b$ es múltiplo de 11. O sea que también vale $b^{561} \equiv b \pmod{11}$.

Conclusión, en ambos casos vale que $b^{561} \equiv b \pmod{11}$.

Si 17 no divide a b entonces $b^{16} \equiv 1 \pmod{17}$, por lo tanto $b^{560} = (b^{16})^{35} \equiv (1)^{35} \equiv 1 \pmod{17}$. O sea que $b^{560} \equiv 1 \pmod{17}$ y por lo tanto $b^{561} \equiv b \pmod{17}$.

Si 17 divide a b entonces es claro que $b^{561} - b$ es múltiplo de 17. O sea que también vale $b^{561} \equiv b \pmod{17}$.

Conclusión, en ambos casos vale que $b^{561} \equiv b \pmod{17}$.

Sumando las conclusiones tenemos que $b^{561} - b$ es múltiplo de 3, de 11 y de 17. Por lo tanto, $b^{561} - b$ es múltiplo de 561. O sea que $b^{561} \equiv b \pmod{561}$, para todo $b \in \mathbb{N}$.

b. Seguiremos el mismo proceso de discusión que en el caso anterior. Sea p un primo de la descomposición factorial de n y consideramos $b \in \mathbb{N}$.

Si p no divide a b entonces $b^{p-1} \equiv 1 \pmod{p}$. Por hipótesis, $p-1 | n-1$ o sea que existe k tal que $k \times (p-1) = n-1$. Luego $(b^{p-1})^k \equiv (1)^k \pmod{p} \equiv 1 \pmod{p}$. O sea que $b^{n-1} \equiv 1 \pmod{p}$, por lo tanto $b^n \equiv b \pmod{p}$.

Por otro lado si p divide a b es claro que: $b^n \equiv b \pmod{p}$. Entonces en ambos casos tenemos la misma conclusión.

Como lo anterior es cierto para cada primo que divide a n , y $n = p_1 \times p_2 \times \dots \times p_k$, con $p_i \neq p_j$, si $i \neq j$ (n es libre de cuadrados) y $b^n \equiv b \pmod{p_i}$, para todo $i = 1, \dots, k$ entonces $b^n \equiv b \pmod{n}$.