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

Segunda prueba (primer parcial) - 30 de setiembre de 2016. Duración: 2,5 horas

N° de parcial	Cédula	Nombre y apellido

Ejercicio 1. (8 puntos) Calcular $3^{163} \pmod{89}$.

Ejercicio 2. (8 puntos) Sea $a, b, c, n \in \mathbb{N}$ con $c \neq 0$.
Demostrar que, si $ca \equiv cb \pmod{n}$ entonces $a \equiv b \left(\text{mód } \frac{n}{\text{mcd}(c,n)}\right)$.

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

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

i) Demostrar que $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$ y $b^{16} \equiv 1 \pmod{17}$.

ii) Hallar $b^{560} \pmod{3}$, $b^{560} \pmod{11}$ y $b^{560} \pmod{17}$.

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.

Sugerencia: para cada $a \in \mathbb{N}$ escribir $n = n^* d_a$, siendo d_a =mcd(a, n).