CC3101 - Matemáticas Discretas para la Computación
Profesor: Pablo Barceló
Auxiliar: Christian von Borries

Auxiliar N°9

17 de Junio de 2014

Recuerdo

- **Teorema Fundamental de la Aritmética** Todo entero positivo es producto de números primos y esta descomposición es única (bajo reorden de los factores).
- **Pequeño teorema de Fermat** Si p es primo y a es cualquier entero, $a^p \equiv a \mod p$.
- Dos enteros positivos a y b se dicen **coprimos** si $\text{mcd}(a, b) = 1$.
- **Lema de Bézout** Si a y b son naturales, existen enteros m y n tal que $ma + nb = \text{mcd}(a, b)$.
- a es invertible módulo n ssi a y n son coprimos.

P1) (Examen Primavera 2010) Un número n no primo que satisface la identidad $b^{n-1} \equiv 1 \mod n$ para cada entero positivo $b < n$ con $\text{mcd}(b, n) = 1$ se denomina *número de Carmichael*.

Sea $p_1 p_2 \dots p_k$ la factorización prima de un entero $n \geq 2$. Asuma que todos los p_j's son distintos y que $p_j - 1$ divide a $n - 1$ $(1 \leq j \leq k)$. Muestre que n es un número de Carmichael.

P2) (**Teorema de Tamref**) Considere la ecuación $n^x + n^y = n^z$ con n, x, y, z enteros positivos. Muestre que esta ecuación tiene infinitas soluciones si $n = 2$ y ninguna si $n > 2$.

P3) (Control 5 Primavera 2010) Sea p primo y a un entero en el intervalo $[1, p - 1]$. Considere el conjunto

$$S = \{a, 2a, 3a, \dots, (p-1)a\}$$

Divida cada elemento de S por p y suponga que $r_1, r_2, \dots, r_{p-1}$ son los restos de la división. Demuestre que cada entero entre 1 y $p - 1$ ocurre exactamente una vez entre estos residuos.

P4) Sea p primo. Muestre que $(p - 1)! \equiv -1 \mod p$.

P5) Sea p primo. Diremos que a es cuadrado perfecto módulo p si existe un x tal que $x^2 \equiv a \mod p$.

a) ¿Cuántos cuadrados perfectos módulo p hay?

b) Muestre que, para un r dado, la ecuación $x^2 + y^2 \equiv r$ siempre tiene solución.