IIC1253 - Sección 1 - Segundo Semestre 2014
Profesor: Marcelo Arenas
Ayudantes: Martín Muñoz (*mmunos@uc.cl*) - Matías San Martín (*masanmartin@uc.cl*)

Ayudantía 13.

Teo. de números. Congruencias y otras cosas fáciles

Problema 1. Dé una regla de división para el 3 (la de siempre), y demuéstrela. Haga lo mismo con el 7 y el 11.

Problema 2. Demuestre que si p es primo,

$$(x+y)^p \equiv (x^p + y^p) \mod p$$

Problema 3. Dados p, q primos, $a \in \mathbb{N}$, $n = p \cdot q$ y $a < n$. Demuestre que la ecuación $x^2 \equiv a \mod n$ tiene a lo más 4 soluciones en $\{0, ..., n-1\}$.

Problema 4. Elevar un número a un exponente ridículamente alto puede hacerse rápido si lo que nos interesa es el módulo del resultado. Para esto tenemos que demostrar un lemita. Dados $a, b, n \in \mathbb{Z}$:

$$a^b \equiv (a \mod n)^b \mod n$$

Usando esta nueva herramienta, calcule lo siguiente:

a) $21^5 \mod 4$.

b) $11^{211} \mod 12$

c) Los dos últimos dígitos de 7^{256}.

Problema 5. Una consecuencia del teorema de Fermat es:

$$a^b \equiv a^{b \mod (p-1)} \mod p$$

Demuéstrelo y úselo para calcular $100^{102} \mod 101$.

Problema 6. En clases con el ayudante se mencionó que dado un n, el conjunto $\{0, ..., n-1\}$ y la suma $\mod n$ forma un grupo cíclico. No le dé mucha importancia. Solo tome en cuenta que al trabajar con la suma y la multiplicación $\mod n$, $n-k$ se comporta igual que $-k$. Use esto para calcular:

a) $102^{100} \mod 101$.

b) $9000^{8000} \mod 9001$.

Problema 7. En clases provisorias vimos a la rápida la función ϕ de Euler. Esta función tiene muchas propiedades interesantes, pero por alguna razón no se ve en el curso. Se define de la siguiente manera:

$$\phi(n) := |\{a \in \mathbb{N} : a < n, a \text{ y } n \text{ no tienen divisores en común}\}|$$

Por ejemplo, $\phi(100) = 40$ y $\phi(40) = 16$. En particular, si p y q son primos distintos, $\phi(p) = p-1$ y $\phi(pq) = (p-1)(q-1)$. También se presentó el teorema de Euler[1]. Si a y n no tienen divisores en común:

$$a^{\phi(n)} \equiv 1 \mod n$$

Use esto para calcular los dos últimos dígitos de $233^{377^{610}}$.

[1] La demostración de este teorema la veremos eventualmente

Problema 8. (I2 - 2013) Sean p, q primos distintos, $n = p \cdot q$, $a, b \in \mathbb{N}$. Demuestre que si

$$a^x \equiv b \mod n$$

tiene solución, entonces también tiene solución en $\{1, ..., n-1\}$. **Hint:** Use el teorema de Euler.