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

Ayudantía 14.

Teo. de números. MCD, inversos y raíces cuadradas

Problema 1. Si $\text{MCD}(a, b) = 1$ y $n \in \mathbb{Z}$ es tal que $a \mid n$ y $b \mid n$, demuestre que $ab \mid n$. Demuestre que puede ser falso si $\text{MCD}(a, b) \neq 1$. **Hint:** recuerde que si $\text{MCD}(a, b) = c$, existen enteros k, ℓ tales que $k \cdot a + b \cdot \ell = c$. ¿Por qué es esto?

Problema 2. Recuerde que el *máximo común divisor* de a, b y c es un número d tal que d divide a a, b y c, y si $e \in \mathbb{Z}$ también divide a los tres, se tiene que $e \mid d$. Demuestre que $\text{MCD}(a, b, c) = \text{mcd}(a, \text{MCD}(b, c))$. Utilice el algoritmo de Euclides para encontrar el máximo común divisor de 1575, 540 y 1620.

Problema 3. Sea p primo. Dado $a \in \{1, ..., p-1\}$, demuestre que para cada $b \in \{1, ..., p-1\}$ existe un único $b' \in \{1, ..., p-1\}$ tal que $b \cdot b' \equiv a \pmod{p}$.

Problema 4. Sea p primo. Recuerde que decimos que un número a tiene raíz cuadrada (mod p) si

$$x^2 \equiv a \pmod{p}$$

tiene solución en $\{1, ..., p-1\}$. Demuestre que si existe solución, existen exactamente dos en ese intervalo.

Problema 5. Demuestre que si a tiene raíz cuadrada, entonces $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Problema 6. Demuestre que si a no tiene raíz cuadrada, entonces $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Problema 7. Si p es primo, el síbmolo de legendre $\left(\frac{a}{p}\right)$ vale 1 si a tiene raíz cuadrada (mod p), -1 si no y 0 si $p \mid a$. Demuestre que si $\text{MCD}(a, p) = 1$, entonces $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Problema 8. Demuestre que la ecuación

$$x^2 + 3xy - 2y^2 = 122$$

no tiene soluciones enteras.