PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Matemáticas Discretas - IIC1253
Tarea 3
Entrega: Lunes 1 de diciembre

1. En esta pregunta suponga que $m \geq 1$ y $n \geq 1$ son números naturales tales que $\text{MCD}(m, n) = 1$. Una herramienta básica para resolver sistemas de ecuaciones en aritmética modular es el teorema chino del resto, el cual indica que para cada $a \in \mathbb{N}$ y $b \in \mathbb{N}$, existe $x \in \mathbb{N}$ tal que:

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

   (a) [0.3 puntos] Demuestre el teorema chino del resto utilizando el algoritmo extendido para el cálculo del máximo común divisor. En particular, use este algoritmo para encontrar un procedimiento eficiente (no una búsqueda exhaustiva) que calcule el valor de x dados a y b.

   (b) [0.2 puntos] Utilice el procedimiento desarrollado en (a) para calcular un valor de x tal que:

$$\begin{aligned} x &\equiv 355 \mod 1225 \\ x &\equiv 1087 \mod 1144 \end{aligned}$$

   (c) [1 punto] Sean a_1, a_2, b_1 y b_2 números naturales. Demuestre que existe $x \in \mathbb{N}$ tal que

$$\begin{aligned} a_1 \cdot x &\equiv a_2 \mod m \\ b_1 \cdot x &\equiv b_2 \mod n \end{aligned}$$

   si y sólo si

$$\text{MCD}(a_1, m) | a_2 \quad \text{y} \quad \text{MCD}(b_1, n) | b_2.$$

   Además, de un algoritmo eficiente (no una búsqueda exhaustiva) que calcule el valor de x dados a_1, a_2, b_1 y b_2, en el caso en que este valor x exista.

2. Dado un número natural $n \geq 2$, defina $\mathbb{Z}_n^*$ de la siguiente forma:

$$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} \mid \text{MCD}(a, n) = 1\}.$$

   Por ejemplo, $\mathbb{Z}_2^* = \{1\}$ y $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$. Además, defina $\phi(n)$ como $|\mathbb{Z}_n^*|$. Así, tenemos que $\phi(2) = 1$ y $\phi(10) = 4$.

   (a) [0.6 puntos] Dado un número primo p y un número natural $i \geq 1$, demuestre que:

$$\mathbb{Z}_{p^{i+1}}^* = \{a + k \cdot p^i \mid a \in \mathbb{Z}_{p^i}^* \text{ y } k \in \{0, \ldots, p-1\}\}.$$

   Utilice este resultado para obtener una fórmula para el valor de $\phi(q^j)$ para cada número primo q y número natural $j \geq 1$.

(b) [0.6 puntos] Sean m, n números naturales tales $m \geq 2$, $n \geq 2$ y $\text{MCD}(m, n) = 1$. Defina una función $f : \mathbb{Z}^*_{m \cdot n} \to \mathbb{Z}^*_m \times \mathbb{Z}^*_n$ como $f(k) = (k \bmod m, k \bmod n)$. Por ejemplo, si $n = 3$ y $m = 16$, tenemos que $f(1) = (1, 1)$, $f(7) = (1, 7)$ y $f(35) = (2, 3)$. Demuestre que f es una biyección.

(c) [0.5 puntos] Sea $n \geq 2$ un número natural tal que:

$$n \quad = \quad \prod_{i=1}^{k} p_i^{\ell_i},$$

donde (1) $k \geq 1$, (2) cada p_i es un número primo, (3) $p_i < p_{i+1}$ para cada $i \in \{1, \ldots, k-1\}$, y (4) cada ℓ_i es un número natural mayor a 0. Utilizando (a) y (b), demuestre que:

$$\phi(n) \quad = \quad \prod_{i=1}^{k} \left(p_i^{\ell_i} - p_i^{\ell_i - 1} \right)$$

(d) [0.8 puntos] Utilizando los resultados anteriores demuestre que para cada número natural $n \geq 2$ y $a \in \mathbb{Z}^*_n$, se tiene que:

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

3. [1 punto] Utilizando el teorema de Wilson demuestre que para cada número primo p de la forma $4 \cdot k + 1$, existe un número x tal que

$$x^2 \quad \equiv \quad -1 \mod p.$$

Vale decir, -1 tiene raíz cuadrada en módulo p si este es un número primo de la forma $4 \cdot k + 1$. En particular, usted debe utilizar el teorema de Wilson para encontrar una expresión que defina una raíz cuadrada de -1 como función de p. Además, utilice la expresión encontrada para calcular una raíz cuadrada de -1 en módulo 97.

4. [1 punto] Dado un polinomio $p(x_1, \ldots, x_k)$ con coeficientes en los números naturales, definimos el conjunto de los números generados por $p(x_1, \ldots, x_k)$ de la siguiente forma:

$$\text{GEN}(p) \quad = \quad \{p(n_1, \ldots, n_k) \mid (n_1, \ldots, n_k) \in \mathbb{N}^k\}.$$

Por ejemplo, si $p_1(x) = 2x$, $p_2(x) = 2x + 1$, $p_3(x, y) = 4 + 2x + 2y + xy$ y $p_4(x) = 7$, entonces se tiene que $\text{GEN}(p_1)$ es el conjunto de los número pares, $\text{GEN}(p_2)$ es el conjunto de los número impares, $\text{GEN}(p_3)$ es el conjunto de los números mayores que 1 que no son primos, y $\text{GEN}(p_4) = \{7\}$.

En esta pregunta usted va a demostrar que no es posible construir un polinomio $p(x_1, \ldots, x_k)$ con coeficientes en los números naturales que genere sólo números primos, y un número infinito de estos. Vale decir, demuestre que si $\text{GEN}(p)$ es infinito, entonces $\text{GEN}(p)$ contiene un número que no es primo.