PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

Matemáticas Discretas - IIC1253
Guía de teoría de números

1. Demuestre que un número natural n es divisible por 7 si y sólo si el número $\lfloor \frac{n}{10} \rfloor + 5 \cdot (n \bmod 10)$ es divisible por 7. Por ejemplo, aplicando la regla obtenemos que:

$$\begin{aligned} 273 \text{ es divisible por } 7 \quad &\Leftrightarrow \quad \lfloor \frac{273}{10} \rfloor + 5 \cdot (273 \bmod 10) = 42 \text{ es divisible por } 7 \\ &\Leftrightarrow \quad \lfloor \frac{42}{10} \rfloor + 5 \cdot (42 \bmod 10) = 14 \text{ es divisible por } 7 \ . \end{aligned}$$

   Y concluimos que 273 es divisible por 7 puesto que 14 es divisible por 7.

2. ¿Es cierto que si $a \equiv_n b$ y $c \equiv_n d$, entonces $a^c \equiv_n b^d$? Demuestre o de un contraejemplo.

3. Demuestre que la ecuación $(a \cdot x + b) \equiv_p 0$ tiene al menos una solución si $a \not\equiv_p 0$ y p es un número primo.

4. Sea $n = p \cdot q$, donde p, q son primos distintos. Dado $a \in \{0, \ldots, n-1\}$, demuestre que la ecuación $x^2 \equiv_n a$ tiene a lo más 4 soluciones en el intervalo $\{0, \ldots, n-1\}$.

5. Encuentre dos números primos distintos p, q y un número $a \in \{0, \ldots, n-1\}$, donde $n = p \cdot q$, tal que la ecuación $x^2 \equiv_n a$ tenga exactamente 4 soluciones en el intervalo $\{0, \ldots, n-1\}$.

6. Sean p, q dos primos distintos, y a, b dos números naturales arbitrarios. Encuentre una solución para el siguiente sistema de ecuaciones:

$$\begin{aligned} x &\equiv_p a \\ x &\equiv_q b \end{aligned}$$

7. Sea p_1, p_2, ..., p_k ($k \geq 3$) una secuencia creciente de números primos (vale decir, $p_1 < p_2 < \cdots < p_k$). Además, sea a_1, a_2, ..., a_k una secuencia arbitraria de números naturales. Encuentre una solución para el siguiente sistema de k ecuaciones:

$$x \equiv_{p_i} a_i \qquad\qquad 1 \leq i \leq k$$

8. Calcule el inverso de 420 en módulo 641 utilizando el algoritmo extendido de Euclides para calcular el máximo común divisor.

9. Construya la clave pública y la clave privada para un sistema criptográfico RSA donde $P = 53$ y $Q = 71$.

10. Sea p un número primo impar. Demuestre que para cada $a \in \{1, \ldots, p-1\}$, se tiene que:

$$a^{\frac{p-1}{2}} \equiv_p 1 \quad \text{o} \quad a^{\frac{p-1}{2}} \equiv_p -1.$$

11. Decimos que b es una raíz cuadrada de a en módulo n si $b^2 \equiv_n a$. Por ejemplo, 2 y 3 son raíces cuadradas de 4 en módulo 5 ya que $2^2 \equiv_5 4$ y $3^2 \equiv_5 4$.

    Dado un número primo p y $a \in \{0, \ldots, p-1\}$, demuestre que a tiene a lo más dos raíces cuadradas en módulo p en el intervalo $\{0, \ldots, p-1\}$.

12. Sea p un número primo de la forma $4 \cdot k + 3$ y $a \in \{1, \ldots, p-1\}$. Demuestre que si

$$a^{\frac{p-1}{2}} \equiv_p -1,$$

    entonces $-a$ tiene raíz cuadrada en módulo p (vale decir, existe b tal que $b^2 \equiv_p -a$).

13. Sean p, q dos números primos distintos. Demuestre que, si

$$a^q \equiv_p a \qquad \text{y} \qquad a^p \equiv_q a$$

    entonces $a^{pq} \equiv_{pq} a$.

14. Sea $p \geq 3$ un número primo y $a \in \{1, \ldots, p-1\}$. Demuestre que si a tiene raíz cuadrada en módulo p, entonces $a^{\frac{p-1}{2}} \equiv_p 1$.

15. Suponga que p, q son dos primos tales que $3 \leq p < q$, y sea $n = p \cdot q$. Demuestre que para cada $a \in \mathbb{N}$, se tiene que a tiene raíz cuadrada en módulo n si y sólo si a tiene raíz cuadrada en módulo p y a tiene raíz cuadrada en módulo q.

16. Sea p un número primo de la forma $4 \cdot k + 3$. Por ejemplo, $3 = 4 \cdot 0 + 3$ y $11 = 4 \cdot 2 + 3$, mientras que 5 no es de esta forma. Demuestre que la ecuación $(x^2 + 1) \equiv_p 0$ no tiene solución.

17. ¿Es cierto el enunciado del ejercicio 16 para los primos de la forma $4 \cdot k + 1$? Justifique su respuesta.

18. Sean p, q dos primos distintos y $n = p \cdot q$. Además, sea

$$f : \{0, \ldots, n-1\} \quad \to \quad \{0, \ldots, p-1\} \times \{0, \ldots, q-1\}$$

    una función tal que para cada $k \in \{0, \ldots, n-1\}$, se tiene que $f(k) = (k \bmod p, k \bmod q)$. Por ejemplo, si $p = 3$ y $q = 5$, entonces f es una función con dominio $\{0, \ldots, 14\}$ tal que $f(1) = (1 \bmod 3, 1 \bmod 5) = (1, 1)$ y $f(8) = (8 \bmod 3, 8 \bmod 5) = (2, 3)$. Utilizando el ejercicio 6, demuestre que la función f (definida para primos distintos p, q arbitrarios) es una biyección.