Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC1253 — Matemáticas Discretas – 1'2019

GUIA 7
Teoría de números

Los siguientes ejercicios son una recopilación de guías de ejercicios del curso de Matemáticas Discretas dictado por Marcelo Arenas en años anteriores.

1. De una regla de división para el número 7 (que utilice los dígitos de un número para verificar si es divisible por 7).

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

3. Demuestre que la ecuación $(a \cdot x + b) \equiv 0 \bmod p$ tiene exactamente una solución si $a \not\equiv 0 \bmod p$ 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 $x^2 \equiv a \bmod n$ 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 $x^2 \equiv a \bmod n$ 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:

$$\begin{aligned} x &\equiv a \mod p \\ x &\equiv b \mod q \end{aligned}$$

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:

$$x \equiv a_i \mod p_i \qquad 1 \leq i \leq k$$

8. Sean n, m, a, b números enteros tales que $n, m \geq 2$. Demuestre que el sistema de ecuaciones

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

tiene solución si y sólo si $a \equiv b \bmod \text{MCD}(n, m)$.

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

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

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

    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 $\{0, \ldots, p-1\}$.

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

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

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

12. Sea $p \neq 2$ un número primo y $a \in \{1, \ldots, p-1\}$. Demuestre que si a tiene raíz cuadrada en módulo p, entonces $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

13. Suponga que p, q son dos primos tales que $3 \leq p < q$, y sea $n = p \cdot q$.

    (a) 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.

    (b) Adicionalmente suponga que $p = 4 \cdot k_1 + 3$ y $q = 4 \cdot k_2 + 3$. De un algoritmo eficiente que dado $a \in \mathbb{N}$, verifique si a tiene raíz cuadrada en módulo n, y si este es el caso calcule una raíz cuadrada de a en módulo n.

    Importante: al momento de construir el algoritmo considere que usted conoce p y q. Además, recuerde que decimos que un algoritmo es eficiente si funciona en tiempo polinomial en el tamaño de la entrada.

14. Demuestre que si existe un algoritmo eficiente para calcular raíces cuadradas en módulo n, donde n es la multiplicación de dos primos distintos, entonces existe un algoritmo eficiente para encontrar un divisor de n.

    Importante: a diferencia del problema 13, en esta pregunta usted sabe que n es la multiplicación de dos primos distintos, pero usted no conoce estos primos. Además, suponga que el algoritmo para calcular raíces cuadradas retorna todas las raíces de un número (las cuales pueden ser hasta cuatro).

15. 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 $(x^2 + 1) \equiv 0 \bmod p$ no tiene solución.

16. ¿Es cierto el enunciado del ejercicio 15 para los primos de la forma $4 \cdot k + 1$? Justifique su respuesta.

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

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

    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.

18. Sea $n = p \cdot q$, donde p, q son primos tales que $3 \leq p < q$. Dado $a \in \{0, \ldots, n-1\}$ tal que $\text{MCD}(a, n) = 1$, demuestre que si la ecuación $x^2 \equiv a \bmod n$ tiene solución, entonces tiene exactamente 4 soluciones en el intervalo $\{0, \ldots, n-1\}$.

19. Sean p, q números primos distintos, $n = p \cdot q$ y a, b números naturales. En esta pregunta usted debe demostrar que si la ecuación:

$$a^x \equiv b \mod n \tag{1}$$

    tiene solución, entonces esta ecuación tiene solución en el intervalo $\{0, \ldots, n-1\}$. Vale decir, usted debe demostrar que si la ecuación (1) tiene solución, entonces existe $c \in \{0, \ldots, n-1\}$ tal que:

$$a^c \equiv b \mod n.$$

20. Sea p un número primo, $r \in \{1, \ldots, p-1\}$ y S el siguiente subconjunto de $\{1, \ldots, p-1\}$:

$$S \quad = \quad \{a \in \{1, \ldots, p-1\} \mid a^r \equiv 1 \bmod p\}.$$

Además, dado $a \in \{1, \ldots, p-1\}$, sea $a^{-1} \in \{1, \ldots, p-1\}$ el inverso de a en módulo p (sabemos que este inverso existe puesto que $\text{MCD}(a, p) = 1$). Por ejemplo, si $p = 5$ y $a = 2$, entonces $a^{-1} = 3$.

(a) Defina la relación $\sim$ sobre $\{1, \ldots, p-1\}$ de la siguiente forma: para cada $a, b \in \{1, \ldots, p-1\}$, se tiene que $a \sim b$ si y sólo si $b \cdot a^{-1} \in S$. Demuestre que $\sim$ es una relación de equivalencia sobre $\{1, \ldots, p-1\}$.

(b) Demuestre que $[1]_\sim = S$.

(c) Dados $a, b \in \{1, \ldots, p-1\}$, demuestre que existe una biyección $f : [a]_\sim \to [b]_\sim$.

(d) Usando (a), (b) y (c), demuestre que $|S|$ divide a $(p-1)$, donde $|S|$ es el número de elementos del conjunto S. Vale decir, la cantidad de raíces del polinomio $x^r \equiv 1 \bmod p$ en el intervalo $\{1, \ldots, p-1\}$ debe dividir a $(p-1)$.

Este resultado puede ser usado para calcular las raíces de $x^r \equiv 1 \bmod p$. Por ejemplo, si $p = 11$, tenemos que la cantidad de raíces del polinomio $x^4 \equiv 1 \bmod 11$ en el intervalo $\{1, \ldots, 10\}$ debe dividir a 10, es decir, puede ser 1, 2, 5 ó 10. Si combinamos esto con el hecho de que $x^4 \equiv 1 \bmod 11$ puede tener a lo más 4 raíces,[1] obtenemos que el polinomio $x^4 \equiv 1 \bmod 11$ tiene 1 ó 2 raíces. Por lo tanto, dado que 1 y -1 son raíces de $x^4 \equiv 1 \bmod 11$, concluimos que estas son exactamente la raíces de este polinomio.

[1] En general, se puede demostrar que $x^r \equiv 1 \bmod p$, donde p es un primo y $r \in \{1, \ldots, p-1\}$, puede tener a lo más r raíces en el intervalo $\{1, \ldots, p-1\}$.