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

IIC1253 — Matemáticas Discretas — 1' 2019

Ayudantía 11

Teoría de Números

Problema 1

Demuestre que un número es divisible por 4, si y solo si, el número formado por sus dos últimos dígitos en base 10 es divisible por 4.

Solución propuesta.

Sea $n > 0$ un número natural cuya representación decimal es $(n)_{10} = d_{k-1} \dots d_1 d_0$. Luego, tenemos que se cumple

$$n = \sum_{i=0}^{k-1} 10^i d_i$$

Probar que $4|n$ es equivalente a probar que $n \mod 4 = 0$, de forma que usaremos esta expresión para probar lo pedido.

$$\begin{aligned} n \mod 4 = 0 &\Leftrightarrow \left(\textstyle\sum_{i=0}^{k-1} 10^i d_i\right) \mod 4 = 0 \\ &\Leftrightarrow \left(\textstyle\sum_{i=0}^{k-1} (10^i d_i \mod 4)\right) \mod 4 = 0 \\ &\Leftrightarrow \left((d_0 \mod 4) + (10 d_1 \mod 4) + \textstyle\sum_{i=2}^{k-1} (10^i d_i \mod 4)\right) \mod 4 = 0 \end{aligned}$$

Habiendo separado los dos primeros términos de la representación, notamos que para $i \geq 2$, cada término $10^i d_i$ es múltiplo de 100. Luego, como $4|100$, se tiene que $4|10^i d_i$ para $i \geq 2$ y en consecuencia, $10^i d_i \mod 4 = 0$. Con esto,

$$\begin{aligned} n \mod 4 = 0 &\Leftrightarrow ((d_0 \mod 4) + (10 d_1 \mod 4)) \mod 4 = 0 \\ &\Leftrightarrow (10 d_1 + d_0) \mod 4 = 0 \end{aligned}$$

Este último resultado establece que el número n' cuya representación en base 10 es $(n')_{10} = d_1 d_0$, i.e. consiste en los últimos dos dígitos de n, es divisible por 4 si y solo si n es divisible por 4.

Problema 2

Demuestre que $(n-1)! \equiv (n-1) \pmod{n}$ si y solo si, n es primo.

Solución propuesta.

Observación: este resultado se conoce como *teorema de Wilson*.

($\Rightarrow$) Sea n tal que $(n-1)! \equiv (n-1) \pmod{n}$. Demostraremos el resultado por contradicción: supongamos que n es compuesto. Entonces, existe un entero $1 < q < n$ tal que $n = kq$ para algún entero k. Dado que $1 < q < n$, no solo $q|n$ sino que también $q|(n-1)!$, pues q aparece como factor en $(n-1)!$. De esta forma,

$$(n-1)! \equiv 0 \pmod{q}$$

Ahora, de la hipótesis original sabemos que $(n-1)! = n - 1 + n\alpha$ para algún α entero. Luego, usando el hecho de que $n = kq$, deducimos que

$$(n-1)! = -1 + n(\alpha + 1) = -1 + qk(\alpha + 1)$$

lo que es equivalente a

$$(n-1)! \equiv -1 \pmod{q}$$

Esta congruencia contradice la que obtuvimos antes con la definición de q, de manera que n no puede ser compuesto. Concluimos que n es primo.

($\Leftarrow$) Sea n primo. Para $n = 2$ y $n = 3$ la propiedad se verifica trivialmente:

- $1! \mod 2 = 1 \mod 2 = 2 - 1 \mod 2$
- $2! \mod 3 = 2 \mod 3 = 3 - 1 \mod 3$

Luego, consideremos $n \geq 5$ primo. En particular, sabemos que n necesariamente será impar. Luego, tenemos que

$$(n-1)! = 1 \cdot 2 \cdots (n-2)(n-1)$$

tiene en total una cantidad par de factores y podemos agruparlos de a pares sin que sobre ninguno.

Como n es primo, todo $a \in \mathbb{Z}_n$ tiene un inverso multiplicativo $a^{-1} \in \mathbb{Z}_n$. Nuestro objetivo es agrupar de a pares los inversos para así obtener una serie de 1's. Para esto, consideremos los siguientes resultados:

- Los únicos $a \in \mathbb{Z}_n$ que son su propio inverso, i.e. que satisfacen la congruencia $a^2 \equiv 1 \pmod{n}$, son $a = 1$ y $a = n - 1$. En efecto,

  $$a^2 \equiv 1 \pmod{n} \Leftrightarrow n|(a+1)(a-1)$$

  Como n es primo, divide a $a + 1$ o a $a - 1$ (demostración en tarea 7) de manera que obtenemos dos posibles congruencias:

  $$a \equiv 1 \pmod{n} \quad \text{o} \quad a \equiv -1 \pmod{n}$$

  Esta última congruencia tiene -1 en el lado derecho, que no es válido en $\mathbb{Z}_n$, de forma que usamos el hecho de que $-1 \equiv n - 1 \pmod{n}$ para concluir que los únicos enteros en $\mathbb{Z}_n$ que son su propio inverso son 1 y $n - 1$.

- Como cada $a \in \mathbb{Z}_n$ tiene un inverso multiplicativo $a^{-1} \in \mathbb{Z}_n$ pero los únicos que son su propio inverso son 1 y $n - 1$, entonces todo $a \in \{2, 3, \ldots, n-2\}$ tiene su inverso a^{-1} en $\{2, 3, \ldots, n-2\}$ y es tal que $a \neq a^{-1}$.

Con esto, reordenamos el factorial según

$$(n-1)! = (n-1) \cdot [2 \cdots (n-2)]$$

de manera que entre los corchetes agrupamos cada entero junto a su inverso multiplicativo. Luego, $(n-1)! \equiv (n-1) \cdot [2 \cdots (n-2)] \pmod{n}$ y cada producto de inversos es congruente con 1 en $\mod n$. De esta forma,

$$(n-1)! \equiv (n-1) \cdot [1 \cdots 1] \pmod{n} \Leftrightarrow (n-1)! \equiv (n-1) \pmod{n}$$

como se quería probar.

Problema 3

(a) Para $m > 1$ demuestre que si $a \equiv b \pmod{m}$, entonces $\gcd(a, m) = \gcd(b, m)$.

Solución propuesta.

Dado que $a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$, usamos la idea del algoritmo de Euclides de acuerdo con

$$\begin{aligned} \gcd(a, m) &= \gcd(m, a \bmod m) \\ &= \gcd(m, b \bmod m) \\ &= \gcd(m, b) \\ &= \gcd(b, m) \end{aligned}$$

(b) Para $m > 1$ demuestre que si $ac \equiv bc \pmod{m}$, entonces $a \equiv b \left(\text{mód } \frac{m}{\gcd(m, c)}\right)$.

Solución propuesta.

Definimos por simplicidad $g = \gcd(m, c)$ y con ello, dado que g es divisor de c y m, podemos reescribirlos como

$$c = gs \quad m = gt$$

para enteros s y t. Luego,

$$\begin{aligned} ac \equiv bc \pmod{m} &\Leftrightarrow ac - bc = km \text{ para algún } k \\ &\Leftrightarrow ags - bgs = kgt \\ &\Leftrightarrow as - bs = kt \\ &\Leftrightarrow as \equiv bs \pmod{t} \end{aligned}$$

Para eliminar s y obtener lo pedido, tenemos que asegurar que s tiene inverso multiplicativo en módulo t. Para ello, consideremos la identidad de Bézout para el par c, m; $\gcd(c, m) = pc + qm$ para ciertos p, q, pero podemos reescribir en función de g según

$$g = pgs + qgt \Leftrightarrow 1 = ps + qt$$

La identidad de Bézout establece que el menor entero positivo que se puede escribir de la forma $ps + qt$ es $\gcd(s, t)$ y como 1 es el menor entero positivo, concluimos que $\gcd(s, t) = 1$. Esto significa que s y t son primos relativos y por lo tanto, s tiene inverso multiplicativo en módulo t. Con ello,

$$as \equiv bs \pmod{t} \Leftrightarrow a \equiv b \pmod{t}$$

y concluimos lo pedido notando que $t = \frac{m}{g}$.

Problema 4

Sean n, m dos números coprimos y a, b naturales. Encuentre una solución para el sistema de ecuaciones

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

Solución propuesta.

Como n y m son primos relativos, podemos usar el teorema chino de los restos para garantizar la existencia de soluciones para el sistema dado. Más aún, de la demostración del teorema visto en clases, sabemos que una solución es de la forma

$$x^* = aM_1M_1^{-1} + bM_2M_2^{-1}$$

donde

- $M_1 = \frac{mn}{n} = m$ y M_1^{-1} es el inverso multiplicativo de M_1 en módulo n, i.e. $M_1 M_1^{-1} \equiv 1 \pmod{n}$.
- $M_2 = \frac{mn}{m} = n$ y M_2^{-1} es el inverso multiplicativo de M_2 en módulo m, i.e. $M_2 M_2^{-1} \equiv 1 \pmod{m}$.

Nos falta determinar entonces, $m^{-1} \in \mathbb{Z}_n$ y $n^{-1} \in \mathbb{Z}_m$. Notemos que

$$\begin{aligned} n, m \text{ coprimos} &\Leftrightarrow 1 = sn + tm,\ s, t \in \mathbb{Z} \\ &\Leftrightarrow tm = 1 - sn \end{aligned}$$

Luego,

$$\begin{aligned} tm \bmod n &= (1 - sn) \bmod n \\ &= (1 \bmod n - sn \bmod n) \bmod n \\ &= (1 \bmod n) \bmod n \\ &= (1 \bmod n) \end{aligned}$$

de donde se concluye que $tm \equiv 1 \pmod{n}$ y por lo tanto $t = m^{-1}$. Siguiendo esta idea, tomamos como solución

$$x^* = bsn + atm$$

y verificamos que efectivamente satisface la primera ecuación del sistema:

$$\begin{aligned} x^* \bmod n &= (bsn + atm) \bmod n \\ &= ((bsn \bmod n) + (atm \bmod n)) \bmod n \\ &= (0 + (atm \bmod n)) \bmod n \\ &= ((a \bmod n)(tm \bmod n)) \bmod n \end{aligned}$$

Como probamos antes, $tm \bmod n = 1$ de manera que

$$x^* \bmod n = a \bmod n \Leftrightarrow x^* \equiv a \pmod{n}$$

de manera que x^* es solución de la primera ecuación. Un procedimiento similar demuestra que también es solución de la segunda, y por lo tanto, es solución del sistema.