Práctico 3 - Repaso
Matemática Discreta I – Año 2021/1
FAMAF

(1) Sea p primo positivo. Probar que $(p,(p-1)!) = 1$.

Rta: Supongamos que $(p,(p-1)!) > 1$, como el único divisor de p además del 1 es p, esto quiere decir que $(p,(p-1)!) = p$ y por lo tanto $p|(p-1)!$.

Ahora bien, recodemos que si p primo, entonces

$$p|a_1 \cdot a_2 \cdot \cdots \cdot a_k \quad \Rightarrow \quad p|a_i \text{ para algún } i \text{ tal que } 1 \leq i \leq k.$$

Luego,

$$p|(p-1)! = 1 \cdot 2 \cdots (p-1) \quad \Rightarrow \quad p|i \text{ para algún } i \text{ tal que } 1 \leq i \leq p-1.$$

Es decir, $p|i$ con $i < p$, absurdo.

(2) Demostrar que $\forall n \in \mathbb{Z}$, $n > 2$, existe p primo tal que $n < p < n!$. (Ayuda: pensar qué primos dividen a $n! - 1$.)

Rta: Si $n! - 1$ es primo, el ejercicio está demostrado. Si $n! - 1$ no es primo, entonces existe un primo p tal que $p|n! - 1$. Ahora bien, $p \not| i$ para $1 \leq i \leq n$, pues si $p|i \Rightarrow p|n! \Rightarrow p|(n! - 1) - n = -1$, absurdo.

Por lo tanto, p primo, $p \neq 1, 2, \ldots, n$ y $p|n! - 1$, esto implica que p primo, $p > n$ y $p < n!$, lo cual prueba el resultado.

(3) Dado un entero $a > 0$ fijo, caracterizar aquellos números que al dividirlos por a tienen cociente igual al resto.

Rta: Sea b que cumpla con lo que pide el enunciado del ejercicio, es decir $b = a \cdot r + r$ y $0 \leq r < b$. por lo tanto $b = (a+1)r$ con $0 \leq r < b$. Como $a > 0$, es claro que si $b = (a+1)r$, entonces $r < b$.

Concluyendo: los números que al dividirlos por a tienen cociente igual al resto son de la forma $(a+1)r$, con $0 \leq r$.

(4) Probar que si $(a, 4) = 2$ y $(b, 4) = 2$ entonces $(a + b, 4) = 4$.

Rta: Dividamos a y b por 4, y enemos $a = 4k + r$, $b = 4t + s$ con $0 \leq r, s < 4$. Ahora bien como $(a, 4) = 2$ y $(b, 4) = 2$, 4 no divide ni a, ni a b, por lo tanto $0 < r, s$. Por otro lado, como 2 divide a a y b, entonces $r, s \neq 1, 3$. Todo esto implica que $r = s = 2$. Es decir, $a = 4k + 2$, $b = 4t + 2$. Luego

$$a + b = (4k + 2) + (4t + 2) = 4(k + t) + 4 = 4(k + t + 1).$$

Esta ecuación nos dice que $4|a + b$, luego $(a + b, 4) = 4$.

(5) Probar que si a, b son coprimos entonces $(a + b, a - b) = 1$ ó 2.

Rta: Si $a+b$ y $a-b$ no tienen un primo en común que los divida, entonces $(a+b, a-b) = 1$ y el ejercicio está resuelto.

En caso contrario, sea p primo tal que $p|a+b$ y $p|a-b$, luego

$$p|(a+b)+(a-b) = 2a \quad \overset{p \text{ es primo}}{\Longrightarrow} \quad p|2 \ \vee \ p|a$$
$$p|(a+b)-(a-b) = 2b \quad \overset{p \text{ es primo}}{\Longrightarrow} \quad p|2 \ \vee \ p|b.$$

Como a y b son coprimos, no tienen un primo en común que los divida, es decir no puede ocurrir que $p|b$ y $p|b$. Por lo tanto $p|2$ (por lo de arriba), es decir $p = 2$. Esto nos dice que $a+b$ y $a-b$ son divisibles por 2. Tomenos $n = (a+b)/2$ y $m = (a-b)/2$ (son números enteros porque $a+b$ y $a-b$ son divisibles por 2). Sea q primo tal que $q|n$ y $q|m$. Entonces,

$$q|n+m = \frac{a+b}{2} + \frac{a-b}{2} = a$$
$$q|n-m = \frac{a+b}{2} - \frac{a-b}{2} = b.$$

Es decir, q primo y $q|a$ y $q|b$, pero esto no puede ocurrir pues a y b coprimos.

Luego

$$(\frac{a+b}{2}, \frac{a-b}{2}) = 1 \qquad \Rightarrow \qquad (a+b, a-b) = 2.$$

(6) Sean a, b enteros no nulos. Completar y demostrar:

a) $[a, a] =?$

b) $[a, b] = b$ si y solo si ...

c) $(a, b) = [a, b]$ si y solo si ...

Rta:

a) $[a, a] = |a|$

Demostración. Supongamos que $a > 0$. Si m es el mcm de a y a, entonces m es el menor múltiplo positivo de a, es decir $m = a$. Si $a < 0$, entonces $-a > 0$ y aplicando el razonamiento anterior $[-a, -a] = -a = |a|$. Como $[a, a] = [-a, -a]$ obtenemos que $[a, a] = |a|$.

b) $[a, b] = b$ si y solo si $b > 0$ y $a|b$.

Demostración. ($\Rightarrow$) Como b es un mcm, por definición de mcm $b > 0$. Por otro lado, de nuevo por definición de mcm, $a|b$.

($\Leftarrow$) $b > 0$ y $a|b$, $b|b$, luego b es un múltiplo positivo de a y b y como todo múltiplo de b es mayor o igual a b, b es el mcm.

c) $(a, b) = [a, b]$ si y solo si $a = \pm b$.

Demostración. Supongamos que ambos son positivos (en caso contrario usamos que $(a, b) = (\pm a, \pm b)$ y $[a, b] = [\pm a, \pm b]$).

($\Rightarrow$) Sea $k = (a, b) = [a, b]$. Como $k = (a, b)$, $k \geq a, b$. Como $k = [a, b]$, $k \leq a, b$: En consecuencia $a \leq k \leq a$ y $b \leq k \leq b \Rightarrow a = k = b$.

($\Leftarrow$) Si $a = b$, entonces $(a, b) = (a, a) = a$ y $[a, b] = [a, a] = a$, por lo tanto $a = (a, b) = [a, b]$.

(7) Probar que si d es un divisor común de a y b, entonces $\dfrac{[a, b]}{d} = \left[\dfrac{a}{d}, \dfrac{b}{d}\right]$.

Rta:

$$\frac{[a, b]}{d} = \frac{ab/(a, b)}{d} = \frac{ab}{d(a, b)}.$$

Por otro lado,

$$\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{(a/d)(b/d)}{(a/d, b/d)} = \frac{ab/d^2}{(a, b)/d} = \frac{ab/d}{(a, b)} = \frac{ab}{d(a, b)}.$$

En la última fórmula usamos la propiedad

$$\frac{(a, b)}{d} = \left(\frac{a}{d}, \frac{b}{d}\right).$$

(8) Probar que $(a + b, [a, b]) = (a, b)$.

(9) Probar que si $(a, b) = 1$ y $n+2$ es un número primo, entonces $(a+b, a^2+b^2-nab) = 1$ ó $n + 2$.

(10) Si $a \cdot b$ es un cuadrado y a y b son coprimos, probar que a y b son cuadrados.

(11) Probar que $\sqrt{6}$ es irracional.

(12) Hallar el menor múltiplo de 168 que es un cuadrado.

(13) Probar que el producto de dos enteros consecutivos no nulos no es un cuadrado. (Ayuda: usar el Teorema Fundamental de la Aritmética).

(14) ¿Existen enteros m y n tales que:

a) $m^4 = 27$? b) $m^2 = 12n^2$? c) $m^3 = 47n^3$?

(15) Sean a y b enteros coprimos. Probar que

a) $(a \cdot c, b) = (b, c)$, para todo entero c.

b) a^m y b^n son coprimos, para todo $m, n \in \mathbb{N}$.

c) $a + b$ y $a \cdot b$ son coprimos.

(16) ¿Cuál es la mayor potencia de 3 que divide a 100!? ¿En cuántos ceros termina el desarrollo decimal de 100!?

(17) Determinar todos los $p \in \mathbb{N}$ tales que

$$p,\ p+2,\ p+6,\ p+8,\ p+12,\ p+14$$

sean todos primos.

(18) Sea $\{f_n\}_{n\in\mathbb{N}}$ la sucesión de Fibonacci, definida recursivamente por: $f_1 = 1$, $f_2 = 1$, $f_{n+1} = f_n + f_{n-1}$, $n \geq 2$. Probar que:

a) f_{3n} es par $\forall\, n \in \mathbb{N}$.

b) f_{3n+1} y f_{3n+2} son impares $\forall\, n \in \mathbb{N}$.

c) $f_{n+m} = f_m f_{n+1} + f_{m-1} f_n$ $\forall n, m \in \mathbb{N}$, $m \geq 2$.

d) $f_n \mid f_{nk}$ $\forall k \in \mathbb{N}$.

e) $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$ $\forall n \geq 2$.

f) $(f_{n+1}, f_n) = 1$ $\forall\, n \in \mathbb{N}$.

Rta:

a) Demostraremos el resultado por inducción.

Caso base $n = 1$. En este caso $f_3 = f_2 + f_1 = 2$, es par.

Paso inductivo. Sea $n > 1$. Supongamos que $f_{3(n-1)}$ es par (HI) y probemos que f_{3n} es par:

$$\begin{aligned} f_{3n} &= f_{3n-1} + f_{3n-2} \\ &= f_{3n-2} + f_{3n-3} + f_{3n-2} \\ &= 2f_{3n-2} + f_{3(n-1)}. \end{aligned}$$

Por (HI), $f_{3(n-1)}$ es par y claramente $2f_{3n-2}$ es par, luego f_{3n} es par.

b) También demostraremos este caso por inducción. Lo que debemos demostrar es

$$P(n) : \text{“}f_{3n+1} \text{ y } f_{3n+2} \text{ son impares } \forall\, n \in \mathbb{N}\text{”}$$

Caso base $n = 1$. En este caso f_{3n+1} y f_{3n+2} son f_4 y f_5 y $f_4 = f_3 + f_2 = 2 + 1 = 3$, $f_5 = f_4 + f_3 = 3 + 2 = 5$, ambos impares.

Paso inductivo. Sea $n > 1$. Supongamos que $f_{3(n-1)+1} = f_{3n-2}$ y $f_{3(n-1)+2} = f_{3n-1}$ son impares (HI), probemos que f_{3n+1} y f_{3n+2} son impares. Ahora bien,

$$f_{3n+1} = f_{3n+1-1} +, f_{3n+1-2} = f_{3n} + f_{3n-1}.$$

Por el inciso anterior f_{3n} es par y por (HI) f_{3n-1} es impar. Como la suma de un par y un impar es impar, resulta que f_{3n+1} es impar. Con un razonamiento análogo probamos que f_{3n+2} es impar:

$$f_{3n+2} = f_{3n+2-1} +, f_{3n+2-2} = f_{3n+1} + f_{3n}.$$

Por lo tanto, f_{3n+2} es la suma de un impar y un par, y en consecuencia es impar.

c)

$$\begin{aligned}
f_{n+m} &= f_{n+m-1} + f_{n+m-2} \\
&= f_{m-1}f_{n+1} + f_{m-2}f_n + f_{m-2}f_{n+1} + f_{m-3}f_n \\
&= (f_{m-1}f_{n+1} + f_{m-2}f_{n+1}) + (f_{m-2}f_n + f_{m-3}f_n) \\
&= (f_{m-1} + f_{m-2})f_{n+1} + (f_{m-2} + f_{m-3})f_n \\
&= f_m f_{n+1} + f_{m-1}f_n.
\end{aligned}$$

d) Por el inciso anterior

$$f_{nk} = f_{n(k-1)+n} = f_n f_{n(k-1)+1} + f_{n-1}f_{n(k-1)},$$

Por (HI), $f_{n(k-1)} = hf_n$, luego

$$f_{nk} = f_n f_{n(k-1)+1} + hf_{n-1}f_n = f_n(f_{n(k-1)+1} + hf_{n-1}),$$

y por consiguiente $f_n | f_{nk}$.

e)

f)