



Universidad de Costa Rica
Facultad de Ciencias Exactas
Escuela de Matemáticas
MA-0320



Tarea 2

II Ciclo 2020

Fecha de entrega: 26 de Setiembre del 2020

Solución

1. **[15 Puntos]** Realizar una revisión bibliográfica en la cual se debe investigar con respecto a:
 - a) Pierre de Fermat: ¿quién fue?, principales aportes matemáticos realizados, aplicaciones de sus aportes matemáticos a la computación.
 - b) El último Teorema de Fermat: enunciarlo, cual fue el camino para "demostrarlo".
 - c) Andrew Wiles: ¿quién fue?, su relación con el último Teorema de Fermat, el proceso de la "demostración" del mismo.

2. **[25 Puntos]** Del libro que se encuentra en mediación virtual titulado: Matemáticas discretas con aplicaciones de Susanna S. Epp,
 - a) Leer de la sección 4.3, las páginas 170 en adelante.
 - b) Realizar de la sección 4.3 los ejercicios: 10,11,12,13,20,21,28,29,32 y 37.
 - 10) ¿Es $7|34$?
No, debido a que si calculamos el modulo de 34, este es diferente de 0, es decir: $34 \bmod 7 \neq 0$. Esto significa que $7 \cdot 4 = 28 + 6$.

 - 11) ¿Es $13|3$?
No, debido a que si calculamos el modulo de 73 es diferente de 0, es decir: $73 \bmod 13 \neq 0$. Esto significa que $13 \cdot 6 = 78 - 5$.

 - 12) ¿Si $n = 4k + 1$, 8 divide a $n^2 - 1$?
Sí, debido a que $n = 4k + 1$, la suma de productos enteros, da como resultado un número entero.

$$n^2 - 1 = (4k + 1)^2 - 1$$

$$(16k^2 + 8k + 1) - 1$$

$$16k^2 + 8k$$

$$8(2k^2 + k) \Rightarrow \text{Números enteros}$$

- 13) ¿Si $n = 4k + 3$, 8 divide a n^2 ?

Sí, debido a que se cuenta con suma de productos de números enteros.

$$n^2 - 1 = (4k + 3)^2 - 1$$

$$(16k^2 + 8k + 9) - 1$$

$$16k^2 + 8k + 8$$

$$8(2k^2 + k + 1) \Rightarrow \text{Números enteros.}$$

- 20) La suma de tres enteros consecutivos es divisible por 3. (Dos números enteros son consecutivos, si y sólo si, uno es uno más que el otro.)

Sí, debido:

$$S(n) = n + (n + 1) + (n + 2) = d/3, d \in \mathbb{Z}$$

$$3n + 3$$

$$3(n + 1)$$

Ejemplo:

$$S(1) = 1 + 2 + 3 = 6/3 = 2$$

- 21) El producto de dos enteros pares es un múltiplo de 4.

Los enteros a y b , al multiplicar da como resultado c , el cual c es $4|c$.

$$\textcircled{1} a \cdot b = c \iff 4|c$$

$$\textcircled{2} a = \frac{c}{b} \Rightarrow \text{el resultado de este, un número par.}$$

Ejemplo:

$$8 \cdot 16 = 128/4 = 32$$

$$\frac{128}{16} = 8/4 = 2$$

- 28) Para todos los números enteros a , b y c , si $a|bc$ entonces $a|b$ o $a|c$. Si $a|b \Rightarrow bc = a \cdot k_1, k \in \mathbb{Z}$

Contamos con dos posibles casos.

$$1) b = a \cdot \frac{k_1}{c}, \text{ si } \frac{k_1}{c_1} \in \mathbb{Z} \Rightarrow \frac{k_1}{c} = k_2$$

$$\Rightarrow b = a \cdot k_2, \text{ de donde } a|b.$$

$$2) c = a \cdot \frac{k_1}{b}, \text{ si } \frac{k_1}{b} \in \mathbb{Z} \Rightarrow \frac{k_1}{b} = k_3$$

$$c = a \cdot k_3 \text{ de donde } a|c.$$

- 29) Para todos los números enteros a y b , si $a|b$, entonces $a^2|b^2$.

Si $a|b \Rightarrow b = a \cdot k_1, k_1 \in \mathbb{Z}$, luego:

$$b^2 = (a \cdot k_1)^2 \Rightarrow b^2 = a^2 \cdot k_1^2, \text{ donde } k_2 = k_1^2$$

$$\Rightarrow a^2 | b^2.$$

- 32) Una cadena de comida rápida tiene un concurso en el que una tarjeta con números se le da a cada cliente que realiza una compra. Si algunos de los números de la tarjeta suman 100, entonces el cliente gana 100. Un cliente dado recibe una tarjeta con los números

72, 21, 15, 36, 69, 81, 9, 27, 42 y 63.

Ninguno de los números suma el total de 100. Es ocurre por que cada elemento es divisible entre 3, la suma de ellos tambien lo es, pero el numero 100 no es divisible entre 3, es decir: $100/3 = \frac{100}{3}$.

- 37) Utilice el teorema de factorización única para escribir los números enteros siguientes en su forma factorizada estándar.

$$a) 1176 = 24 \cdot 49 = 8 \cdot 3 \cdot 7 \cdot 7 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7 = \boxed{2^3 \cdot 3 \cdot 7^2}$$

$$b) 5733 = 441 \cdot 13 = 9 \cdot 49 \cdot 13 = 3 \cdot 3 \cdot 7 \cdot 7 \cdot 13 = \boxed{3^2 \cdot 7^2 \cdot 13}$$

$$c) 3675 = 75 \cdot 49 = 15 \cdot 5 \cdot 7 \cdot 7 = 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 = \boxed{3 \cdot 5^2 \cdot 7^2}$$

- c) Realizar de la sección 4.4 los ejercicios: 1,3,5,6 y 47.

- 1) Para cada uno de los valores de n y d dados en los ejercicios, $n = dq + r$ y $0 \leq r < d$

$$70 = 9 \cdot q + r$$

$$70 = 9 \cdot 7 + 7$$

$$\boxed{q=7, r=7}$$

- 3) $n = dq + r$ y $0 \leq r < d$

$$36 = 40 \cdot q + r$$

$$36 = 40 \cdot 0 + 36$$

$$\boxed{q=0, r=36}$$

- 5) $n = dq + r$ y $0 \leq r < d$

$$-45 = 11 \cdot q + r$$

$$-49 = 11 \cdot -4 + -1$$

$$\boxed{q=-4, r=-1}$$

- 6) $n = dq + r$ y $0 \leq r < d$

$$-27 = 8 \cdot q + r$$

$$-27 = 8 \cdot -3 + -3$$

$$\boxed{q=-3, r=-3}$$

- 47) a. ¿En qué posición se almacena a_2 ?

R/ 7614

b. Escriba una fórmula (en i y en j) que dé el entero n para que a_{ij} se almacene en la posición $7609 + n$.

$$R/4(i-1) + (j-1)$$

c. Encuentre fórmulas (en n) para r y s de modo que a_{rs} se almacene en la posición $7609 + n$

$$R/r = \frac{1}{4}(n - j + 5)$$

3. **[20 Puntos]** El objetivo de este ejercicio es aplicar las definiciones vistas en divisibilidad para poder desarrollar una serie de rutinas en Mathematica que permiten calcular números en diferentes bases numéricas.

a) Del libro que se encuentra en mediación virtual titulado: Matemáticas Discretas, de Richard Johnsonbaugh, leer la sección 5.2, la cual inicia en la página 192.

b) Desarrollar una rutina en Mathematica para el pseudocódigo

1) Conversión de un entero base b en decimal, página 195.

2) Conversión de un entero decimal a la base b , página 198.

3) Suma de números binarios, página 200.

4) Elevar un exponente mod z elevando al cuadrado varias veces, página 204.

```
Ejercicio3b1[c_, n_, b_] := Module[{i, A = {}, x = n, num = c, valordec = 0, potencia = 1},
  |módulo
  A = IntegerDigits[num];
  |dígitos de entero
  For[i = 0, i ≤ x, i++,
  |para cada
    valordec = valordec + A[[x - i + 1]] * potencia;
    potencia = potencia * b;
  ];
  Return[valordec];
  |retorna
];

Ejercicio3b1[1101, 3, 2]

13
```

Figura 1: Ejercicio 3b-1

4. **[20 Puntos]** El objetivo de este ejercicio es aplicar el algoritmo Euclidiano como herramienta de cifrado de información.

a) Del libro que se encuentra en mediación virtual titulado: Matemáticas Discretas, de Richard Johnsonbaugh, leer la sección 5.3, la cual inicia en la página 205.

```

Ejercicio3b2[m_, b_] := Module[{i, A = {}, x = m, n = -1, valordec = 0, potencia = 1},
  [módulo
    While[x > 0,
      [mientras
        n = n + 1;
        A = PrependTo[A, Mod[x, b]];
        [añade al principio [operación módulo
        x = Floor[x/b];
        [entero inferior
      ]];

    Print["El número ", m, " en la base ", b, " corresponde a: ", FromDigits[A]];
    [escribe
    ];

Ejercicio3b2[11, 2]
El número 11 en la base 2 corresponde a: 1011

```

Figura 2: Ejercicio 3b-2

```

Ejercicio3b3[b_, bi_, n_] := Module[{A = {}, B = {}, S = {}, x = n, lleva = 0},
  [módulo
    (*Considerar que en esta implementación se puede omitir solicitar el valor de n,
    ya que este se puede obtener del largo del conjunto A. Considerar que esta implementación respeta lo presentado en el libro,
    en donde se realizar la suma de dos número de igual longitud,
    se puede hacer una mejora para realizar la suma de dos números de diferente longitud, pero no sería respetar lo que se pide*)
    A = IntegerDigits[b];
    [dígitos de entero
    B = IntegerDigits[bi];
    [dígitos de entero
    For[i = 0, i <= x, i++,
      [para cada
        S = PrependTo[S, Mod[(A[[x - i + 1]] + B[[x - i + 1]] + lleva), 2]];
        [añade al princ... [operación módulo
        lleva = Floor[(A[[x - i + 1]] + B[[x - i + 1]] + lleva)/2];
        [entero inferior
      ]];
    S = Prepend[S, lleva];
    [añade al principio
    Return[FromDigits[S]];
    [de dígitos a número
    ];

Ejercicio3b3[10011, 11010, 4]
101101

```

Figura 3: Ejercicio 3b-3

- b) Escriba un programa que, dados los enteros no negativos a y b , ambos diferentes de cero, calcule los enteros s y t que satisfacen

$$\text{mcd}(a, b) = s \cdot a + t \cdot b$$

```

Ejercicio3b3[b_, b1_, n_] := Module[
  {A = {}, B = {}, S = {}, x = n, lleva = 0},
  (*Considerar que en esta implementación se puede omitir solicitar el valor de n,
  ya que este se puede obtener del largo del conjunto A. Considerar que esta implementación respeta lo presentado en el libro,
  en donde se realizar la suma de dos número de igual longitud,
  se puede hacer una mejora para realizar la suma de dos números de diferente longitud, pero no sería respetar lo que se pide*)
  A = IntegerDigits[b];
  B = IntegerDigits[b1];
  For[i = 0, i < x, i++,
    S = PrependTo[S, Mod[(A[[x - i + 1]] + B[[x - i + 1]] + lleva), 2]];
    lleva = Floor[(A[[x - i + 1]] + B[[x - i + 1]] + lleva)/2];
  ];
  S = Prepend[S, lleva];
  Return[FromDigits[S]];
];

Ejercicio3b3[10011, 11010, 4]
101101

```

Figura 4: Ejercicio 3b-4

Algoritmo .1:

Data: Enteros no negativos a y b, ambos diferentes de cero**Result:** Calcular los enteros s y t, $mcd(a; b) = s \cdot a + t \cdot b$

```

1  Temporal1=a
2  Temporal2=b;
3  if a < b then
4      Temporal1=b
5      Temporal2=a;
6  end
7  a1 = 1;
8  b1 = 0;
9  if b == 0 then
10     a2 = 0;
11     a3 = 1;
12     b2 = 1;
13     b3 = 0;
14 while Temporal1 != 0 do
15     t = Floor[(Temporal1/Temporal2)];
16     r = Mod[Temporal1, Temporal2];
17     a1 = a3 - t · 2;
18     b1 = b3 - t · 2;
19     a3 = a2;
20     a2 = a1;
21     c3 = b2;
22     b2 = b1;
23     Temporal1 = Temporal2;
24     Temporal2 = r;
25 Salida=a3, b3, Temporal1;
26 Return[Salida];
27 Fin Programa;
```

- c) Escriba un programa que, dados los enteros $n > 0$ y $\phi > 1$, $mcd(n, \phi) = 1$, calcule el inverso de $n \bmod \phi$.

Algoritmo .2:

Data: Enteros no negativos a y b, ambos diferentes de cero**Result:** Calcular los enteros s y t, $mcd(a; b) = s \cdot a + t \cdot b$

```

1  Temporal1=a
2  Temporal2=b;
3  if a < b then
4      Temporal1=b
5      Temporal2=a;
6  end
7  if b == 0 then
8      x = 1;
9      y = 0;
10 end
11 x1 = 0;
12 x2 = 1;
13 y1 = 1;
14 y2 = 0;
15 while Temporal != 0 do
16     q = Floor[(Temporal1/Temporal2)];
17     r = Mod[Temporal1, Temporal2];
18     x = x2 - q · x1;
19     y = y2 - q · y1;
20     x2 = x1;
21     x1 = x;
22     y2 = y1;
23     y1 = y;
24     Temporal1 = Temporal2; Temporal2 = r;
25 end
26 t = y2;
27 if Temporal==1 then
28     Inversa=Mod(t,b);
29     Print Inversa;
30 end
31 Fin Programa;
```

5. [20 Puntos] Realice las siguientes rutinas en Mathematica

- a) Una rutina que reciba un número natural n , construya una matriz cuadrada A de orden n en donde:

$$(a_{ij}) = \begin{cases} 1 & \text{si } mcd(i, j) < n \\ 0 & \text{en otro caso} \end{cases}$$

Nota: para calcular $mcd(i, j)$ utilice el algoritmo euclidiano.

Un pseudocódigo que soluciona lo anterior es:

Algoritmo .3: Ejercicio 5a

Data: n orden de la matriz cuadrada.

Result: M matriz solicitada según el enunciado.

```

1  M=ConstantArray[0, {n, n}];
2  for i = 1, 2, ..., n do
3      for j = 1, 2, ..., n do
4          if MaxComDiv[i, j] < n then
5              M[i, j] = 1;
6          Fin If;
7      Fin Ciclo;
8  Fin Ciclo;
9  Return[M];
10 Fin Programa;
```

- b) Una rutina que reciba un número natural n , construya una matriz cuadrada B de orden n en donde:

$$(b_{ij}) = \begin{cases} 1 & \text{si } F_i \mid j \\ 0 & \text{en otro caso} \end{cases}$$

Nota: F_i representa al valor en la posición i de la sucesión de Fibonacci.

Algoritmo .4: Ejercicio 5b

Data: n orden de la matriz cuadrada.**Result:** M matriz solicitada según el enunciado.

```

1   $M = \text{ConstantArray}[0, \{n, n\}];$ 
2  for  $i = 1, 2, \dots, n$  do
3      for  $j = 1, 2, \dots, n$  do
4          if  $\text{Mod}[\text{Fibo}[i], j] = 0$  then
5               $M[i, j] = 1;$ 
6          Fin If;
7          Fin Ciclo;
8      Fin Ciclo;
9  Return $[M];$ 
10 Fin Programa;

```

c) A partir de las matrices que se generan en las rutinas anteriores, tomando $n = 50$ y usando las rutinas que se dieron en clases, determinar:

1) $(A \odot B)^t \wedge (B^t \odot A) .$

2) $(A^t \odot B \vee A) \odot B^t .$

Los retos muestran nuestras mejores o peores actitudes...

MaLu

