SOLUCIONES PRUEBA DE MATEMÁTICA DISCRETA

1.A. Sabiendo que la clave pública es $n = 10553$ $(n = 173 \cdot 61)$ y $e = 191$, calcular la clave privada y decir como se encripta y descifra un mensaje con el sistema RSA.

Solución:
Cálculo de la clave privada d: $\phi(n) = \phi(10553) = (173-1)\cdot(61-1) = 172\cdot 60 = 10320$.
d es el inverso multiplicativo de $e = 191$ módulo $\phi(n) = 10320$.
$\gcd(10320, 191) = 1$, ya que

10320	191		191	6		6	5
6	54		5	31		1	1

$6 = 10320 - 54 \cdot 191, \qquad 5 = 191 - 31 \cdot 6, \qquad 1 = 6 - 1 \cdot 5.$

Así:

$$1 = 6 - 5 = 6 - (191 - 31 \cdot 6) = 32 \cdot 6 - 191 = 32 \cdot (10320 - 54 \cdot 191) - 191$$
$$= 32 \cdot 10320 - 1728 \cdot 191 - 191 = 32 \cdot 10320 - 1729 \cdot 191$$

Por lo tanto, el inverso multiplicativo de 191 módulo 10320 es -1729, pero

$$-1729 \equiv 8591 \bmod 10320.$$

Para encriptar un mensaje m;

$$m \longrightarrow m^{191} \bmod 10533.$$

Para descifrar el mensaje recibido x;

$$x \longrightarrow x^{8591} \bmod 10533.$$

2.A. (a) ¿El número 3914230221 es divisible por 11? ¿Y por 99? (Razonar sin hacer la división !!!)

Solución:
3914230221 es divisible por 11 si, y solo si,

$$-3 + 9 - 1 + 4 - 2 + 3 - 0 + 2 - 2 + 1 \equiv 0 \bmod 11 \iff 19 - 8 = 11 \equiv 0 \bmod 11$$

Por otro lado, es divisible por 99 si, y solo si, es divisible por 11 y 9:
3914230221 es divisible por 9 si, y solo si,

$$3 + 9 + 1 + 4 + 2 + 3 + 0 + 2 + 2 + 1 \equiv 0 \bmod 11 \iff 27 \equiv 0 \bmod 9$$

Por lo tanto 3914230221 es divisible por 99.

(b) ¿La función $30x^2 - 7x^3 \log(x)$ es $\mathcal{O}(x^2)$?

Solución:
No es $\mathcal{O}(x^2)$ ya que $x^3 \notin \mathcal{O}(x^2)$.

(c) Escribir el número $1051_{(6)}$ expresado en base 6 en base 8.

Solución:
$1051_{(6)} = 1 \cdot 6^3 + 0 \cdot 6^2 + 5 \cdot 6^1 + 1 = 247$ expresado en base 10.

$$\begin{array}{r|l} 247 & 8 \\ \hline 7 & 30 \end{array} \qquad \begin{array}{r|l} 30 & 8 \\ \hline 6 & 3 \end{array}$$

Así, el número $1051_{(6)}$ en base 8 es $367_{(8)}$.

(d) ¿Qué enteros positivos menores que 28 tienen inverso multiplicativo en $\mathbb{Z}/28\mathbb{Z}$?

Solución:
$\phi(28) = \phi(2^2) \cdot \phi(7) = 2 \cdot 6 = 12$ elementos tienen inverso multiplicativo en $\mathbb{Z}/28\mathbb{Z}$, que son los números x tales que $\gcd(x, 28) = 1$, es decir,

$$1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27.$$

1.B. Sabiendo que la clave pública es $n = 9853$ $(n = 167 \cdot 59)$ y $e = 187$, calcular la clave privada y decir como se encripta y descifra un mensaje con el sistema RSA.

Solución:

Cálculo de la clave privada d: $\phi(n) = \phi(9853) = (167-1)\cdot(59-1) = 166 \cdot 58 = 9628$.

d es el inverso multiplicativo de $e = 187$ módulo $\phi(n) = 9628$.

$\gcd(9628, 187) = 1$, ya que

9628	187		187	91		91	5
91	51		5	2		1	18

$91 = 9628 - 51 \cdot 187, \qquad 5 = 187 - 2 \cdot 91, \qquad 1 = 91 - 18 \cdot 5.$

Así:

$$\begin{aligned} 1 &= 91 - 18 \cdot 5 = 91 - 18 \cdot (187 - 2 \cdot 91) = 37 \cdot 91 - 18 \cdot 187 \\ &= 37 \cdot (9628 - 51 \cdot 187) - 18 \cdot 187 = 37 \cdot 9628 - 1905 \cdot 187 \end{aligned}$$

Por lo tanto, el inverso multiplicativo de 187 módulo 9628 es -1905, pero

$$-1905 \equiv 7723 \bmod 9628.$$

Para encriptar un mensaje m;

$$m \longrightarrow m^{187} \bmod 9853.$$

Para descifrar el mensaje recibido x;

$$x \longrightarrow x^{7723} \bmod 9853.$$

2.B. (a) ¿El número 221456838972 es divisible por 11? ¿Y por 3? ¿Y por 33? (Razonar sin hacer la división !!!)

Solución:

221456838972 es divisible por 11 si, y solo si,

$$-2+2-1+4-5+6-8+3-8+9-7+2 \equiv 0 \bmod 11 \iff 26 - 31 = -5 \equiv 6 \not\equiv 0 \bmod 11$$

Así, no es divisible por 11.

221456838972 es divisible por 3 si, y solo si,

$$2+2+1+4+5+6+8+3+8+9+7+2 \equiv 0 \bmod 3 \iff 57 \equiv 12 \equiv 3 \equiv 0 \bmod 3$$

Por otro lado, es divisible por 33 si, y solo si, es divisible por 11 y 3, así 221456838972 no es divisible por 33.

(b) ¿La función $26x^3 - 693x^2 \log(x)$ es $\mathcal{O}(x^3)$?

Solución:

Es $\mathcal{O}(x^3)$ ya que x^3 y x^2 pertenecen a $\mathcal{O}(x^3)$.

(c) Escribir el número $1342_{(5)}$ expresado en base 5 en base 7.

Solución:
$1342_{(5)} = 1 \cdot 5^3 + 3 \cdot 5^2 + 4 \cdot 5^1 + 2 = 222$ expresado en base 10.

$$\begin{array}{r|l} 222 & 7 \\ \hline 5 & 31 \end{array} \qquad \begin{array}{r|l} 31 & 7 \\ \hline 3 & 4 \end{array}$$

Así, el número $1342_{(5)}$ en base 7 es $435_{(7)}$.

(d) ¿Qué enteros positivos menores que 36 tienen inverso multiplicativo en $\mathbb{Z}/36\mathbb{Z}$?

Solución:
$\phi(36) = \phi(2^2) \cdot \phi(3^2) = 2 \cdot 6 = 12$ elementos tienen inverso multiplicativo en $\mathbb{Z}/36\mathbb{Z}$, que son los números x tales que $\gcd(x, 36) = 1$, es decir,

$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35.$$