**Universidad de la República - Facultad de Ingeniería - IMERL.**
**Matemática Discreta 2**

SOLUCIÓN EXAMEN - 15 DE DICIEMBRE DE 2018.

## Ejercicio 1.

**a.**
- Enunciar el Teorema Chino del Resto.

  ***Solución:***
  Enunciado en las notas de teórico (Teorema 2.5.1, página 33). Copiamos aquí el enunciado para facilitar al lector.
  *Teorema Chino del Resto* Sean $m_1, m_2, \cdots, m_k$ **enteros coprimos dos a dos** y $a_1, a_2, \cdots, a_k \in \mathbb{Z}$. Entonces el sistema

  $$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{1}$$

  tiene solución, y hay una única solución módulo $m_1 m_2 \cdots m_k$. Es decir, si $x_0$ es solución, entonces todas las soluciones son $x \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$.
- Hacer la demostración del teorema anterior, para el caso en que el sistema tenga tres ecuaciones (k=3).
  ***Solución:***
  Ver las notas de teórico (Teorema 2.5.1, página 33), en el caso general.

**b.** Se considera el polinomio $p(x) = 6x^2 + 5x + 1$.

**i)** Factorizar $p(x)$.
***Solución:***
Es fácil ver que $p(x) = 6x^2 + 5x + 1 = (2x + 1)(3x + 1)$.

**ii)**
- Probar que existe $x \in \mathbb{Z}$ tal que $p(x)$ es múltiplo de 9.
- Probar que existe $y \in \mathbb{Z}$ tal que $p(y)$ es múltiplo de 8.
- Probar que existe $z \in \mathbb{Z}$ tal que $p(z)$ es múltiplo de 72.

***Solución:***
Tomando $x = 4$ tenemos que $p(4) = (2 \times 4 + 1)(3 \times 4 + 1) = 9 \times 13$ es múltiplo de 9. Tomando $x = 5$ vemos que $p(5) = (2 \times 5 + 1)(3 \times 5 + 1) = 11 \times 16$ es múltiplo de 8. Resumiendo, en el primer caso logramos que el primer factor sea múltiplo de 9 (impar) y en el segundo caso, procuramos que el segundo factor sea múltiplo de la potencia de 2. Con esa estrategia el polinomio $p$ evaluado en 4 y 5, respectivamente queda múltiplo de los números buscados.
Por último, procuramos un valor entero $z$ tal que su evaluación $p(z)$ sea múltiplo de 72. Un camino posible es tanteando, y vemos, sin mucha trabajo de búsqueda que $z = 13$ sirve: $p(13) = (2 \times 13 + 1)(3 \times 13 + 1) = 27 \times 40$ el cual es múltimplo de 9 y de 8, o sea múltiplo de 72, o sea $p(13) = 72 \times 15$. Otro camino, es, como se demostrará en el ítem iv., utilizando el Teorema Chino del Resto. Leer, por favor, el caso general en la solución del ítem iv.

**iii)**
- Dado $n \in \mathbb{N}$, impar, probar que existe $x \in \mathbb{Z}$ tal que $p(x)$ es múltiplo de $n$.
- Dado $m = 2^s$, con $s \in \mathbb{N}^*$, probar que existe $y \in \mathbb{Z}$, tal que $p(y)$ es múltiplo de $m$.

***Solución:***

- Si $n$ es impar entonces $n = 2t + 1$ con $t \in \mathbb{Z}$. Evaluando el polinomio $p$ en $t$ tenemos $p(t) = (2t + 1)(3t + 1)$, y como $t \in \mathbb{Z}$ entonces $3t + 1$ es entero también. Por lo tanto $p(t)$ es múltiplo de $n = 2t + 1$.

- Dado $m = 2^s$, con $s \in \mathbb{N}^*$, considero la ecuación en congruencia: $3x+1 \equiv 0 \pmod{2^s}$. Esta ecuación tiene solución entera pues $\operatorname{mcd}(3, 2^s) = 1$. Luego existe $r \in \mathbb{Z}$ solución de la congruencia, o sea, $3r + 1$ es múltiplo de $m = 2^s$.

**iv)** Demostrar que para todo $m \in \mathbb{N}^*$, existe $z \in \mathbb{Z}$, tal que $p(z)$ es múltiplo de $m$.
***Solución:***
Dado $m \in \mathbb{N}^*$ lo escribimos según su descomposición factorial, destacando al único primo par, o sea: $m = 2^s \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \cdots \times p_l^{\alpha_l}$. De otra forma $m = 2^s \times n$ con $n = p_2^{\alpha_2} \times p_3^{\alpha_3} \times \cdots \times p_l^{\alpha_l}$ impar.
Nos podemos plantear el sistema de congruencias:

$$2x + 1 \equiv 0 \pmod{n};\ 3x + 1 \equiv 0 \pmod{2^s}.$$

De otra forma, como 3 es invertible en $\mathbb{Z}_{2^s}$ (o sea $3 \in \mathrm{U}(2^s)$, pues $\operatorname{mcd}(3, 2^s) = 1$), la segunda ecuación en congruencia es equivalente a: $x \equiv -3^{-1} \pmod{2^s}$.
O sea tenemos el sistema: $2x \equiv -1 \pmod{n}$; $\quad x \equiv -3^{-1} \pmod{2^s}$.
Como $n$ es impar, tenemos que $\operatorname{mcd}(n, 2^s) = 1$, con lo cual, por el Teorema Chino del Resto, el sistema tiene solución entera. Es decir, existe $z \in \mathbb{Z}$ tal que $2z + 1$ es múltiplo de $n$ y $3z + 1$ es múltiplo de $2^s$. Luego, $p(z) = (2z + 1)(3z + 1)$ es múltiplo de $n$ y de $2^s$. Por lo tanto, $p(z)$ es múltiplo de $m = 2^s \times n$, que es lo que queríamos demostrar.

**Ejercicio 2.**

**a.** Definir la función $\varphi : \mathbb{N} \to \mathbb{N}$ de Euler.

**b.** Probar que $\varphi(p^k) = p^k - p^{k-1}$ para $p$ primo y $k \in \mathbb{N} \setminus \{0\}$.

**c.** **i)** Probar que 5 es una raíz primitiva módulo 27 y hallar una raíz primitiva de 54.

**ii)** Hallar todos los morfismos $f : U(54) \to \mathbb{Z}_{36}$.

***Solución:***

**a.** Ver las notas de Teórico de MD2, en el sitio EVA del curso:
https://eva.fing.edu.uy/mod/resource/view.php?id=62664

**b.** $\varphi(p^k) = p^{k-1}(p - 1)$. Ver las notas de Teórico de MD2, en el sitio EVA del curso:
https://eva.fing.edu.uy/mod/resource/view.php?id=62664

**c.** $\varphi(27) = 18$. Como $5^6 \equiv 19 \bmod 27$ y $5^9 \equiv 26 \bmod 27$ entonces 5 es raíz primitiva módulo 27. Usando ahora que 5 es impar y que 27 es la potencia de un primo impar se deduce, del Lema 4.1.13 de las Notas dde Teórico, que 5 es raíz primitiva de $54 = 2 \times 3^3$.

**d.** Como el orden de 5 en $U(54)$ es $\varphi(54) = 18$ y $U(54)$ es un grupo cíclico por tener raíz primitiva, para definir un morfismo de grupos (al cual llamaremos $f$) solamente tenemos que ver como se define en 5. Para que la función $f$ sea un morfismo de grupos solamente hay que verificar $o(f(5)) \mid o(5) = 18$. Por lo tanto tenemos un morfismo de grupos por cada elemento par de $\mathbb{Z}_{36}$. La función queda definida por $f(5^k) = kf(5)$, para todo $k \in \mathbb{Z}$.

**Ejercicio 3.**

**a.** Describir el criptosistema RSA, explicando:

**i)** Cómo se define la clave pública $(n, e)$.

**ii)** Cómo se define la función de cifrado y la de descifrado.

**b.** **i)** Enunciar el teorema de Euler. Deducir el teorema de Fermat.

**ii)** Probar que la función de descifrado es la inversa de la función de cifrado.

**c.** El alfabeto de los números en base hexadecimal es:

`0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.`

Estos caracteres se corresponden con los números en base 10 según la tabla:

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| `0` | `1` | `2` | `3` | `4` | `5` | `6` | `7` | `8` | `9` | `A` | `B` | `C` | `D` | `E` | `F` |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

Se considera la clave pública $(n, e) = (3977, 193)$. Se pide:

**i)** Encriptar usando ECB el número hexadecimal `C414`.
**Usar:** $196^{16} \equiv 3650 \pmod{3977}$.

**ii)** Sabiendo que $\varphi(n) = 3840$, halle la función de descifrado correspondiente a la clave $(n, e)$.

***Solución:***

c. i) Buscamos el exponente $k \in \mathbb{N}$ tal que $16^k < 3977 < 16^{k+1}$. Vemos que $k = 2$ es el exponente y por lo tanto, se ha de cortar el número `C414` en bloques de largo 2.

El bloque `C4` representa al número decimal 196 y el bloque `14` al decimal 20. La función de encriptado es $E(x) :\equiv x^{193} \pmod{3977}$. Debemos calcular $E(20)$ y $E(196)$, lo que haremos mediante exponenciación rápida.

El exponente 193 en base 2 es 11000001, de modo que $E(20) \equiv 20^{2^7} \times 20^{2^6} \times 20 \pmod{3977}$, y $E(196) \equiv 196^{2^7} \times 196^{2^6} \times 196 \pmod{3977}$.

Para eso usamos la siguiente tabla:

| $i$ | $2^i$ | $196^{2^i}$ | $20^{2^i}$ |
|---|---|---|---|
| 0 | 1 | 196 | 20 |
| 1 | 2 | 2623 | 400 |
| 2 | 4 | 3896 | 920 |
| 3 | 8 | 2584 | 3276 |
| 4 | 16 | 3650 | 2230 |
| 5 | 32 | 3527 | 1650 |
| 6 | 64 | 3650 | 2232 |
| 7 | 128 | 3527 | 2620 |

Como $3650 \times 3527 \equiv 1 \pmod{3977}$, se tiene $E(196) \equiv 196 \pmod{3977}$ y por otro lado $E(20) \equiv 1184 \pmod{3977}$; de modo que el número encriptado es `0C44A0` (recordar que los bloques encriptados tienen un caracter más).

c. ii) La función de descifrado es $D(x) \equiv x^d \pmod{3977}$ donde $d \equiv (193)^{-1} \pmod{3840}$. Es claro que para que esto sea posible, 193 y 3840 deben ser coprimos. Calculamos $m := \operatorname{mcd}(3840, 193)$ por el algoritmo de Euclides generalizado, el cual nos permite expresar a $m$ como combinación lineal de 3840 y 193. Las divisiones sucesivas para hacer el cálculo son las siguientes:

$$\begin{array}{r|l} 3840 & 193 \\ \hline 173 & 19 \end{array} \qquad \begin{array}{r|l} 193 & 173 \\ \hline 20 & 1 \end{array} \qquad \begin{array}{r|l} 173 & 20 \\ \hline 13 & 8 \end{array}$$

$$\begin{array}{r|l} 20 & 13 \\ \hline 7 & 1 \end{array} \qquad \begin{array}{r|l} 13 & 7 \\ \hline 6 & 1 \end{array} \qquad \begin{array}{r|l} 7 & 6 \\ \hline 1 & 1 \end{array}$$

Estas divisiones generan el siguiente producto de matrices de transición:

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \qquad \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \qquad \begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix} \quad \begin{pmatrix} 2 & -17 \\ -3 & 26 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & -19 \end{pmatrix}$$

$$\begin{pmatrix} 2 & -17 \\ -3 & 26 \end{pmatrix} \quad \begin{pmatrix} -17 & 19 \\ 26 & -29 \end{pmatrix} \quad \color{red}{\begin{pmatrix} 19 & -378 \\ -29 & 577 \end{pmatrix}}$$

Esto en particular dice que:

$$\begin{array}{cc} & \begin{pmatrix} 3840 \\ 193 \end{pmatrix} \\ \begin{pmatrix} 19 & -378 \\ -29 & 577 \end{pmatrix} & \begin{pmatrix} 6 \\ 1 \end{pmatrix} \end{array}$$

De modo que $(-29) \times 3840 + 577 \times 193 = 1$ y entonces $577 \equiv (193)^{-1} \pmod{3840}$. La función de descifrado es: $D(x) :\equiv x^{577} \pmod{3977}$.