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

EXAMEN - 15 DE DICIEMBRE DE 2018. DURACIÓN: 210 MINUTOS

| N° de examen | Cédula | Apellido y nombre |
|---|---|---|
| | | |

Para cada pregunta o ejercicio, deben presentar claramente el razonamiento y cálculos realizados para obtener su respuesta final. Si una implicancia es válida debido a algún teorema, proposición o propiedad, deben especificarlo (nombre del teorema, lema, etc.) Presentar una respuesta final a la pregunta sin justificación carece de validez.

**Ejercicio 1.**

**a**.
- Enunciar el Teorema Chino del Resto.
- Hacer la demostración del teorema anterior, para el caso en que el sistema tenga tres ecuaciones (k=3).

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

i) Factorizar $p(x)$.

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.

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 $m$.

iv) Demostrar que para todo $m \in \mathbb{N}$, existe $z \in \mathbb{Z}$, tal que $p(z)$ es múltiplo de $m$.

**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 $f : U(54) \to \mathbb{Z}_{36}$.

**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:** $196^{16} \equiv 3650$ (mód 3977).

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