Pontificia Universidad Católica de Chile
Facultad de Matemáticas
2° semestre 2020

# Ayudantía 08

16 de Octubre

MAT2225 - Teoría de Números

1) Se encriptan las letras del alfabeto usando la siguiente tabla:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |

Tambien se eligen los primos $p = 11, q = 17$ y el exponente $e = 107$.

a) Calcule $\varphi(pq)$ y $d = e^{-1} \pmod{\varphi(pq)}$

*Solución.* Tenemos que

$$\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1) = 160.$$

Por otra parte, notar que $107 \cdot 3 = 321 = 160 \cdot 2 + 1$, por lo que $d = 3$ funciona. ∎

*Solución.* [Solución 2] Tenemos que

$$\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1) = 160.$$

Ahora, usando algoritmo de la división, se tiene

$$160 = 107 \cdot 1 + 53$$
$$107 = 53 \cdot 2 + 1$$

Devolviendonos, tenemos

$$1 = 107 - 53 \cdot 2 = 107 - (160 - 107) \cdot 2 = 107 \cdot 3 - 160 \cdot 2$$

Tomando módulo 160, se tiene que 3 es el inverso de 107. ∎

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |

b) Suponga que quiere enviar las letras de la palabra "HOLA" por separado. ¿Qué números se necesitan enviar?

*Solución.* Basta calcular $72^{107}, 79^{107}, 76^{107}$ y $65^{107}$, lo que da 30, 29, 87 y 10. ∎

c) Llega el mensaje codificado $108, 86, 146, 51, 28$. ¿Qué dice?

*Solución.* Basta calcular $108^3, 86^3, 146^3, 51^3$ y $28^3$, lo que genera los números $80, 69, 82, 68$ y 73, o la palabra "PERDI". ∎

d) ¿Qué letras podrían presentar problemas al intentar codificarlas? ¿Por qué?

*Solución.* el teorema de Euler pide que $(x, n) = 1$. En este caso, $n = 11 \cdot 17$, por lo que pueden fallar los múltiplos de 11 y/o 17, que serían las letras {B, D, M, U, X}. ∎

e) ¿Cuál es el módulo más pequeño en el que se pueden enviar todas las letras con esta codificación sin problemas?

*Solución.* Basta buscar los dos primos $p, q$ más pequeños tales que ninguna letra de arriba sea divisible por $p$ o $q$. Por inspección, se tiene que $\{p, q\} = \{31, 47\}$. ∎

**Bonus:** Un hacker empieza a recolectar claves, y encuentra los siguientes productos de primos:

$$1065023, 1916927, 2060969, 3301453.$$

El hacker usando esta lista descubre que hay dos claves vulnerables. Encuéntrelas.
*Hint: Revise si hay claves con factores primos en común.*

*Solución.* Haciendo algoritmo de Euclides entre todos los pares, se tiene que $(2060969, 1065023) = 1031$. Así, se tiene que $1065023 = 1031 \cdot 1033$ y $2060969 = 1031 \cdot 1999$. ∎