

## Ejercicio 1

a) el orden  $o(x)$  de  $x$  debe dividir al orden  $|G|$  del grupo  $G$ . Pero  $|G|$  es primo, de modo que  $o(x)$  deberá ser o bien 1 o bien  $|G|$ . Como  $x \neq a$ , entonces  $o(x) \geq 2$ , por lo que  $o(x) = |G|$ , o sea que  $x$  genera  $G$ .

b) Como  $G = \langle x \rangle$  entonces  $f : \mathbb{Z}_p \rightarrow G$  (donde  $p = |G|$ ) dado por  $f(i) = x^i$  es un isomorfismo. Veamos primero que está bien definida. En efecto, si  $i \equiv j \pmod{p}$  entonces  $i = j + tp$  con  $t \in \mathbb{Z}$ , luego  $f(i) = x^i = x^{j+tp} = x^j \cdot (x^p)^t = x^j = f(j)$  (observe que  $x^p = 1$  pues  $p = o(x)$ ). Claramente es sobreyectiva, (pues  $x$  es un generador), pero como dominio y codominio de  $f$  tienen el mismo cardinal,  $f$  también será inyectiva, o sea biyectiva. Basta ver que es un homomorfismo, lo cual es cierto pues  $f(i+j) = x^{i+j} = x^i x^j = f(i)f(j)$ .

c) Como se ve de las tablas la primera representaría a un grupo con 7 elementos y la segunda uno con 5, o sea, ambos primos, por lo que podemos aplicar las partes anteriores. En particular, si fueran tablas de un grupo, ambos grupos deberían ser cíclicos, es más, por lo visto en la parte a), cualquier elemento distinto del neutro debería generar el grupo. Por lo que basta tomar cualquier elemento y ver si genera el grupo para obtener un isomorfismo con  $\mathbb{Z}_7$  y/o  $\mathbb{Z}_5$ . En el primer caso si tomamos  $x = b$ , vemos que  $b^2 = a$ , de modo que  $o(b) = 2 \nmid 7$ , por lo que llegamos a una contradicción y deducimos que no es la tabla de un grupo. En el segundo caso tomando nuevamente  $x = b$  vemos que  $b^2 = c$ ,  $b^3 = e$ ,  $b^4 = d$  y  $b^5 = a$ , de modos que  $o(a) = 5$ , por lo que no llegamos a una contradicción, es más, si fuera un grupo, la función  $f$  que mapea  $0 \mapsto a, 1 \mapsto b, 2 \mapsto c, 3 \mapsto e, 4 \mapsto d$ , debería ser un isomorfismo. Sustituyendo en la segunda tabla,  $a$  por 0,  $b$  por 1,  $c$  por 2,  $d$  por 4 y  $e$  por 3, vemos que la operación es la suma en  $\mathbb{Z}_5$ . Efectivamente, la tabla es simétrica, por lo que solo basta con chequear una mitad de la misma. Por otro lado, el neutro  $a$  verifica  $ax = x$  para todo  $x$ . La tabla queda de la siguiente forma Es rápido y fácil

Table 1: Segunda tabla con la sustitución de  $f^{-1}$

*	0	1	2	4	3
0	0	1	2	4	3
1	1	2	3	0	4
2	2	3	4	1	0
4	4	0	1	3	2
3	3	4	0	2	1

chequear que es la tabla de la suma en  $\mathbb{Z}_5$ .

## Ejercicio 2

a) Es cualquier función  $f : G \rightarrow K$  tal que  $f(x * y) = f(x) \cdot f(y)$ .

b) i)  $F(e_G) = F(e_G * e_G) = F(e_G) \cdot F(e_G)$  de donde, cancelando  $F(e_G)$  obtenemos  $e_K = F(e_G)$ .

ii) Como  $F(g) \cdot F(g^{-1}) = F(g * g^{-1}) = F(e_G) = e_K$  resulta que  $F(g^{-1})$  es el inverso de  $F(g)$ , o sea  $F(g)^{-1} = F(g^{-1})$ .

iii) Basta demostrar que  $F(g)^{o(g)} = e_K$ . Efectivamente  $F(g)^{o(g)} = F(g^{o(g)}) = F(e_G) = e_K$ .

c)  $|U(25)| = 20$  de donde  $o(F(g)) \mid o(g) \mid |U(25)| = 20$ ,

i) Como para todo  $g$   $o(F(g)) \mid 21$  y también divide a 20, debe ser 1, o sea que  $F(g) = 0$  y  $F$  solo puede ser el homomorfismo trivial.

ii) Como para todo  $g$  el orden de  $F(g)$  debe dividir a 20 y a 15, debe dividir a 5, de modo que  $F(g)$  debe ser un elemento de orden 5. Como el orden de un elemento  $i$  de  $\mathbb{Z}_{15}$  es  $15/\text{mcd}(i, 15)$  debe ser  $\text{mcd}(i, 15) = 3$  o sea que  $i$  solo puede ser 3, 6, 9 o 12. Por otro lado, como  $U(25)$  es cíclico pues tiene alguna raíz primitiva  $r$ , todo homomorfismo quedará determinado por la imagen  $F(r)$  de  $r$ , la cual tiene cuatro posibilidades, de modo que hay solo 4 posibles homomorfismos.

## Ejercicio 3

a) Sea  $a \in \mathbb{Z}$  tal que  $\phi(\bar{1}) = \bar{a}$ . Si existiese un tal homomorfismo entonces  $\phi(\bar{6}) = 6 \cdot \phi(\bar{1}) = \bar{6a} = \bar{8}$  en  $\mathbb{Z}_{21}$ , o equivalentemente  $6a \equiv 8 \pmod{21}$ . Esta congruencia implica  $0 \equiv 8 \pmod{3}$  lo cual es absurdo.

b) i)  $\phi(\bar{18}) = \phi(3 \cdot \bar{6}) = 3 \cdot \phi(\bar{6}) = 3 \cdot \bar{9} = \bar{27} = \bar{6}$  y como  $4 \cdot \bar{6} = \bar{24} = \bar{3}$  entonces  $\phi(\bar{3}) = \phi(4 \cdot \bar{6}) = 4 \cdot \phi(\bar{6}) = 4 \cdot \bar{9} = \bar{36} = \bar{15}$ .

ii) Recordando que todo homomorfismo  $\phi : \mathbb{Z}_{21} \rightarrow \mathbb{Z}_{21}$  queda definido si conocemos  $\phi(\bar{1})$  (puesto que  $\bar{1}$  genera  $\mathbb{Z}_{21}$ ) entonces buscamos escribir a 1 como combinación lineal de 14 y 3. Es fácil ver que  $5 \cdot 3 - 1 \cdot 14 = 1$ . Claramente esto implica la igualdad  $5 \cdot \bar{3} - 1 \cdot \bar{14} = \bar{1}$  en  $\mathbb{Z}_{21}$ . Luego  $\phi(\bar{1}) = 5 \cdot \phi(\bar{3}) - 1 \cdot \phi(\bar{14}) = 5 \cdot \bar{15} - 1 \cdot \bar{7} = \bar{68} = \bar{5}$ . Luego el único posible homomorfismo viene dado por  $\phi(\bar{k}) = 5\bar{k}$  que claramente verifica  $\phi(\bar{6}) = \bar{30} = \bar{9}$  y  $\phi(\bar{14}) = \bar{70} = \bar{7}$ .

(Recuerde que si  $(G, +)$  es un grupo,  $n \in \mathbb{Z}^+$  y  $g \in G$  entonces se definen  $n \cdot g := g + g + \dots + g$  ( $n$  veces) y  $(-n) \cdot g := n \cdot (-g)$ .)

## Ejercicio 4

1. Los parámetros  $d$  y  $e$  deben cumplir  $de \equiv 1 \pmod{\varphi(n)}$ . La demostración de  $D(E(x)) \equiv x \pmod{n}$  puede encontrarse en la Proposición 5.3.1 de las notas.
2. En primer lugar  $n = 19 \cdot 29 = 551$  por lo que  $\varphi(n) = 18 \cdot 28 = 504$ . El parámetro  $d$  es el inverso de  $e$  módulo  $\varphi(n)$ ; usando el Algoritmo de Euclides encontramos que  $101 \cdot 5 - 504 = 1$ . Entonces  $101 \cdot 5 \equiv 1 \pmod{\varphi(n)}$  y podemos tomar  $d = 101$ . La función de descifrado es  $D(x) = x^{101} \pmod{551}$ .
3. Por la parte anterior debemos calcular  $2^{101} \pmod{551}$ , para lo cual podemos usar exponenciación rápida. Por ejemplo:

$$2^{10} = 1024 \equiv -78 \pmod{551}$$

$$2^{20} \equiv 78^2 \equiv 23 \pmod{551}$$

$$2^{40} \equiv 23^2 \equiv -22 \pmod{551}$$

$$2^{80} \equiv 22^2 \equiv -67 \pmod{551}$$

$$2^{101} \equiv 2^{80} \cdot 2^{20} \cdot 2 \equiv -67 \cdot 23 \cdot 2 \equiv 112 \cdot 2 \equiv 224 \pmod{551}$$

El mensaje descifrado es 224.