PROBLEMAS DE GEOMETRÍA Y TEORÍA DE NÚMEROS

DANIELE CASAZZA

Ejercicio 1. (Recordatorio de aritmética modular)
Sea $N \in \mathbb{N}_{>1}$. Recordemos que cualquier número entero x se puede escribir de forma única:

$$x = Nq + r$$

donde q es el cociente entero y $r = 0, \dots N-1$ el resto de la división por N. En particular N es divisor de x (y escribimos $N \mid x$) cuando $r = 0$ y $N \nmid x$ en otro caso.

Llamamos:

$$\mathbb{Z}/N\mathbb{Z} := \{0, \dots, N-1\}$$

al conjunto de los posibles restos de la división por N.

Decimos que $a = b \pmod N$, o que $a = b$ dentro de $\mathbb{Z}/N\mathbb{Z}$ si $N \mid a - b$, o sea a y b tienen el mismo resto en la división por N.

(a) Resolver las siguientes ecuaciones en $\mathbb{Z}/N\mathbb{Z}$ para $N = 2, 3, 4, 5$:

$$2a = 3, \qquad 4b = 1, \qquad c+1 = 0, \qquad d^2 = 3,$$
$$e^2 = -1, \qquad 8f = 22, \qquad g^2 = 2, \qquad h^2 = 1$$

(b) Calcular todas las soluciones en $\mathbb{Z}/N\mathbb{Z}$, para $N = 2, 3, 4, 5, 6, 7$, de las ecuaciones:

$$xy = 1, \qquad x^2 + y^2 = 1, \qquad x^2 + y^2 = 3, \qquad \text{y} \qquad xy = 0$$

(c) Calcular las siguientes potencias:

$$64^{13} \pmod 5 = \qquad 2019^{177} \pmod 2 = \qquad 15^6 \pmod{45} =$$
$$144^{99} \pmod 6 = \qquad 314^{16} \pmod 3 = \qquad 9^{112} \pmod{12} =$$
$$75^{225} \pmod 7 = \qquad 34^3 \pmod 8 = \qquad 10^{10} \pmod 9 =$$

(d) Si una ecuación tiene solución entera, tendrá solución modulo todos los N. Demuestra con eso que las siguientes ecuaciones no tienen solución entera:

$$y^2 + y = 2x + 7, \qquad y^2 = x^3 - x - 1, \qquad x^2 + y^2 = 243,$$
$$y^p - y + 1 = x^p - x - 1, \qquad y^2 = x^4 + 2, \qquad x^4 - x + 1 = y^5 - y^4 + y^2 - y.$$

Ejercicio 2. (Solucionar ecuaciones)

(a) Dibujar aproximadamente en el planp $\mathbb{R}^2$ las curvas planas descrita para las siguientes ecuaciones:

$$y^2 = x^3, \qquad y^2 = x^3 + x^2, \qquad y^2 = x^3 - x$$
$$y^2 = x^3 + 1, \qquad y^2 = x^3 + x + 1, \qquad y^2 = x^3 - 2$$

(b) Encuentra toda solución modulo N de las ecuaciones del apartado (a) para $N = 2, 3, 4, \dots, 7$, completa una tabla, y dibuja las soluciones eligiendo $N = 2$ por la primera ecuación y llegando hasta 7 (si quieres, ayúdate con excel o con un pequeño programa para ordenador y calcula las soluciones por N mas altos).

(c) Supongamos que $P = (x, y)$, con x, y números racionales e $y \neq 0$, es un punto de la curva $E : y^2 = x^3 + 1$ y definimos:

$$\tilde{x} = \frac{x^4 - 8x}{4x^3 + 1}, \qquad \tilde{y} = \frac{x^3 - 2 - 3x^2\tilde{x}}{2y}.$$

Verificar que $\tilde{P} = (\tilde{x}, \tilde{y})$ es también un punto perteneciente a E. ¿Por qué es así?

Ejercicio 3. (Geometría y ecuaciones diofánticas)

(a) Demostrar que hay una correspondencia biyectiva entre:

$$\left\{\begin{array}{l}\text{Soluciones } x, y \in \mathbb{Q} \text{ de} \\ \text{la ecuación } x^2 + y^2 = 1\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Soluciones } X, Y, Z \in \mathbb{Z} \text{ tales que } Z > 0 \text{ y} \\ (X, Y, Z) = 1 \text{ de la ecuación } X^2 + Y^2 = Z^2\end{array}\right\}.$$

La ecuación en $X^2 + Y^2 = Z^2$ se dice *homogénea de grado 2* asociada a $x^2 + y^2 = 1$. Es fácil verificar que si $[X_0 : Y_0 : Z_0]$ es solución, también $[tX_0, tY_0, tZ_0]$ lo es.

(b) ¿Hay una corespondencía similar para la ecuación $x^2 + y^2/4 = 1$?

(c) Determina si se puede hacer algo similar para las siguientes ecuaciones:

$$y = x^2, \qquad xy = 1, \qquad 0 = x^2 + xy + y^2 + x + y + 1$$
$$y^2 = x^3, \qquad y^2 = x^3 + x^2, \qquad y^2 = x^3 - x$$

*(d) ¿Tiene algún sentido particular poner $Z = 0$ en la ecuación homogénea? (sugerencia: dibuja algunas de las curvas y mira si puedes encontrar la intuición correcta...)

*(e) ¿Sabes calcular toda solución racional de $x^2 + y^2 = 1$?

Ejercicio 4. (Aritmética modular: ¡la venganza!)

Para este ejercicio consideramos el conjunto $\mathbb{Z}/N\mathbb{Z} = \{0, 1, \ldots, N-1\}$ de las clases de resto modulo N.

(a) Fijamos una clase de resto $a \in \mathbb{Z}/N\mathbb{Z}$, $a \neq 0$. ¿Cuándo la función:

$$m_a : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$$
$$x \mapsto ax$$

de multiplicación por a es inyectiva? ¿Cuándo es sobreyectiva?

(b) Calcular una formula para $\phi(N)$, el número de elementos del conjunto:

$$(\mathbb{Z}/N\mathbb{Z})^\times := \{a \in \mathbb{Z}/N\mathbb{Z} \mid \text{MCD}(a, N) = 1\};$$

(c) Sea $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. ¿existe $b \in \mathbb{Z}/N\mathbb{Z}$ que cumpla que $ab = 1$? ¿Es verdad que $b \in (\mathbb{Z}/N\mathbb{Z})^\times$?

*(d) Para cada $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, comprobar que $a^{\phi(N)} = 1$ (teorema de Fermat–Euler).

Ejercicio 5. (Problemas un poco mas complicados)

(a) Buscar toda solución entera y racional de las siguientes ecuaciones:

$$y^2 = x^3; \qquad y^2 = x^3 + x^2;$$

***(b) Buscar toda solución entera de las siguientes ecuaciones:

$$y^2 = x^3 + 7; \qquad y^2 = x^3 - 2,$$
$$y^2 = x^3 - 2x, \qquad y^2 = x^3 + 17.$$

*****(c) ¿Qué puedes decir sobre las soluciones racionales de las ecuaciones del apartado (b)?

PROBLEMAS DE CRIPTOGRAFÍA

DAVID ALFAYA

1. Cifrado César

El cifrado César (o cifrado por desplazamiento) consiste en sustituir cada letra de un mensaje por otra que se encuentra un cierto número fijo k de posiciones por delante en el alfabeto. Por ejemplo, si $k = 2$, la A se convierte en C, la B en D, la C en E, etc. Más generalmente, si fijamos una forma de asignar números a las letras y símbolos de nuestro alfabeto (ver tabla), la letra x_n se envía (en un alfabeto de 47 símbolos) a

$$y_n = x_n + k \mod 47$$

Ejercicio 1. Cifrar los siguientes mensajes para las claves k dadas
(a) HOLA ($k = 1$)
(b) EN_UN_LUGAR_DE_LA_MANCHA ($k = 5$)
(c) MATEMATICAS ($k = 17$)
(d) WWW.ICMAT.ES ($k = 4$)

Ejercicio 2. Desencriptar los siguientes mensajes para las claves dadas (para desencriptar, simplemente desplazamos en sentido contrario)
(a) IBM¿111 ($k = 1$)
(b) S0RH¿3RGY ($k = 6$)
(c) JEGMOD#QS/ ($k = 4$)

2. Cifrado Vigenère

El cifrado Vigenère es parecido al cifrado César, pero en lugar de desplazar todas las letras la misma cantidad fija, vamos variando esa cantidad en función de la posición. La letra en posición n se desplaza k_n posiciones para ciertos k_n que el emisor y el receptor conocen.

$$y_n = x_n + k_n \mod 47$$

Hay varias formas de escoger los desplazamientos k_n

- Escoger una secuencia, por ejemplo 123, y repetirla tantas veces como haga falta para completar el mensaje 12312312... ($k_1 = 1$, $k_2 = 2$, $k_3 = 3$, $k_4 = 1$, $k_5 = 2$, ...)
- Para recordar bien una clave, podemos asignarla a partir de una palabra. Por ejemplo, MATH y usar el valor de las letras como clave ($k_1 = M = 13$, $k_2 = A = 1$, $k_3 = T = 21$, $k_4 = H = 8$, ...)
- En lugar de usar una secuencia periódica, podemos utilizar un generador de claves (Key Derivation Function – KDF) que nos permita crear una sucesión de desplazamientos k_n. Por ejemplo, a partir de un número $1 < k < 47$, podemos tomar $k_n = k^n \mod 47$.
- En general, podemos tomar cualquier KDF tan compleja como queramos...

Ejercicio 3. Cifrar los siguientes mensajes para las claves dadas usando el método Vigenère
(a) UN_MENSAJE_CORTO (clave 123)
(b) MI_IP_ES_192.168.1.1 (clave IPV4)
(c) MATEMATICAS (clave $2^n \mod 47$)

Ejercicio 4. Descifrar los siguientes mensajes que han sido encriptados con el método Vigenère usando las claves dadas

(a) YB#J5NU2HT5 (clave MATES)
(b) DXJ!HWW¿1JPOMHTK4GQQSY2TDR46T17,I (clave 3^n mód 47)
(c) XXYBNKYUHG_V (clave Fibonacci mód 47)

3. Desencriptación sin clave (vamos a romper códigos...)

Ejercicio 5. (*) En un texto general en castellano, no todas las letras aparecen con la misma frecuencia. Sabiendo que las más frecuentes suelen ser E (13,68 %), A (12,53 %), O (8,68 %), R (6,87 %) y S (7,98 %) y que, además, los espacios aparecen de media cada 5,5 letras, ¿podrías desencriptar el siguiente texto cifrado con el método César, aunque no sepas la clave k? ¿Cuál fue la clave usada?

IQDYQDOYKEVDHIDOEDPEQGLEDHIDGY2SD
QSPFVIDQSDUYMIVSDEGSVHEVPIDQSDLEDP
YGLSDXMIPTSDUYIDZMZMEDYQDLMHEOKSD
HIDOSWDHIDOEQ3EDIQDEWXMOOIVSADEH
EVKEDEQXMKYEADVSGMQDJOEGSD2DKEOK
SDGSVVIHSVC

Ejercicio 6. (**) ¿Y éste otro texto? También es un cifrado César, pero si te interesa un reto criptográfico, quizás quieras resolverlo y ver los secretos que oculta...

JLZHYGTVGLZGZLN1YVFGLZGMHJORGKLGK
LZLTJYOW0HYFGSLPVYG2HSVZGJVTG2ONL
TLYLFG:0LGH0YL2LZGHGWYVIHYGHRNVGS
HZGKOMOJOR.GZLN1OSVZGLTGÑ00WZECC
333FOJSH0FLZCV10YLHJÑCT1SILYZGILMVY
LGJÑYOZ0SHZCKZMQ9¿KHZ

TABLA DE CODIFICACIÓN DE CARACTERES

_	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

0	1	2	3	4	5	6	7	8	9	¿	?	¡	!	#	/	,	:	.
28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46