PRÁCTICA 3

LOGARITMO DISCRETO, FACTORIZACIÓN Y RAÍCES MODULARES

Vamos a estudiar en esta práctica tres problemas muy relacionados con temas criptográficos, pues son la base del funcionamiento de varios criptosistemas y protocolos criptográficos. Veremos algunos algoritmos para resolverlos y estudiaremos su complejidad.

3.1. Logaritmo discreto

Comenzamos planteando el problema:

Sea p un número primo, y sea a un entero tal que $2 \leq a \leq p-2$.

Dado b un número entero comprendido entre 1 y $p-1$, ¿existe un número x tal que $a^x \equiv b$ mód p?

Caso de existir, diremos que x es el logaritmo (en base a) de b módulo p.

Llamaremos a este número $\log_a(b)$ mód p.

Antes de continuar, algunas observaciones.

- Por el teorema de Fermat sabemos que $a^{p-1} \equiv 1$ mód p. En tal caso, si x es una solución al problema del logaritmo discreto, también lo es $x + (p-1)$, y por el mismo motivo, $x + 2(p-1)$, y así sucesivamente. Tendrá entonces infinitas soluciones.

  Nosotros nos limitaremos entonces a buscar las soluciones positivas que sean menores que $p-1$.

- Si a es un generador (o un elemento primitivo), el problema tiene solución única independientemente del valor de b. Si a no es un generador, entonces puede no tener solución o tener más de una.

Por ejemplo. Tomamos $p = 11$.

En este caso, $a = 2$ es un generador (es decir, si realizamos todas las potencias de 2 módulo 11 obtenemos todos los elementos del 1 al 10).

Buscamos x tal que $2^x \equiv 6$ mód 11. Podemos ver que son soluciones $x = 9$, $x = 19$, $x = 29$, etc. También $x = -1$, $x = -11$. Si nos quedamos con soluciones x tales que $0 \leq x < 10$, la única solución es $x = 9$.

Sin embargo, $a = 3$ no es un generador. Tenemos entonces dos posibilidades:

- Para $b = 5$, $\log_a(b)$ mód p tiene dos soluciones entre 0 y $p-2$ que son $x = 3$ y $x = 8$.
- Para $b = 6$, $\log_a(b)$ mód p no tiene solución.

Vamos a ver tres métodos para resolver el problema del logaritmo discreto.

Fuerza bruta

Sea p un número primo, a un número entre 2 y $p-2$ y b un número entre 1 y $p-1$.

Puesto que si $\log_a(b)$ mód p tiene solución, al menos una de ellas se encuentra entre 0 y $p-2$, probamos a calcular las distintas potencias $a^0,\ a^1, \cdots, a^i$, $0 \leq i \leq p-2$. Paramos cuando alguna potencia coincida con b (en cuyo caso ya tenemos la solución) o cuando obtengamos 1 (exceptuando a^0), en cuyo caso no tiene solución.

Algoritmo paso enano - paso gigante

La idea de este algoritmo es escribir la solución de la forma $x = t \cdot s - i$, donde s es un número entero mayor que $\sqrt{p}$, y t e i hay que determinarlos. Para esto, procedemos como sigue:

- Calculamos $s = \lceil \sqrt{p} \rceil$, donde $\lceil x \rceil$ denota un entero y tal que $x \leq y < x + 1$.

- Calculamos los siguientes elementos y los almacenamos en una tabla S:

$$S = \boxed{b} \boxed{b \cdot a} \boxed{b \cdot a^2} \boxed{\cdots} \boxed{b \cdot a^{s-1}}$$

  Todos los cálculos se realizan módulo p.

- Ahora vamos calculando $a^s,\ a^{2s},\ \cdots a^{ts}$. Cada vez que realizamos uno de los cálculos, comprobamos si el elemento obtenido pertenece a la tabla S.

- El algoritmo tiene dos condiciones de parada:

  - Si encontramos una coincidencia entre un elemento a^{ts} y un elemento de la tabla S. En tal caso, tenemos que $a^{ts} = b \cdot a^i$, luego $b = a^{ts-i}$, y ya tenemos la solución: $x = ts - i$.
  - Si llegamos a a^{s^2} sin encotrar ninguna coincidencia. En tal caso, no existe el logaritmo.

Vamos a calcular $\log_{11}(766)$ mód 839 por medio de este algoritmo. Puesto que $\sqrt{839} = 28,97$, tomamos $s = 29$.
Realizamos los siguientes cálculos (módulo 839):

$$766,\ 766 \cdot 11,\ 766 \cdot 11^2,\ 766 \cdot 11^3,\ \cdots, 766 \cdot 11^{27},\ 766 \cdot 11^{28}.$$

Para calcular cada elemento de la lista, multiplicamos el anterior por 11. Los resultado son:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
766	36	396	161	93	184	346	450	755	754	743	622	130	591	628
15	16	17	18	19	20	21	22	23	24	25	26	27	28	
196	478	224	786	256	299	772	102	283	596	683	801	421	436	

O si queremos, podemos ordenarlos para que sea más fácil la búsqueda:

1	4	22	12	3	5	15	17	19	23	20	6	2	27	28
36	93	102	130	161	184	196	224	256	283	299	346	396	421	436
7	16	13	24	11	14	25	10	9	8	0	21	18	26	
450	478	591	596	622	628	683	743	754	755	766	772	786	801	

Y ahora, vamos calculando 11^{29} mód 839, $11^{2 \cdot 29}$ mód 839, y así sucesivamente, bien hasta llegar a 11^{29^2} mód 839, bien hasta que el elemento calculado coincida con uno de los 29 números de la tabla anterior:

- $11^{29} = 440$, que no está en la tabla.
- $11^{2 \cdot 29} = 11^{29} \cdot 11^{29} = 440 \cdot 440 = 630$, que no está en la tabla.
- $11^{3 \cdot 29} = 11^{2 \cdot 29} \cdot 11^{29} = 630 \cdot 440 = 330$, que no está en la tabla.
- $11^{4 \cdot 29} = 11^{3 \cdot 29} \cdot 11^{29} = 330 \cdot 440 = 53$, que no está en la tabla.
- $11^{5 \cdot 29} = 11^{4 \cdot 29} \cdot 11^{29} = 53 \cdot 440 = 667$, que no está en la tabla.
- $11^{6 \cdot 29} = 11^{5 \cdot 29} \cdot 11^{29} = 667 \cdot 440 = 669$, que no está en la tabla.
- $11^{7 \cdot 29} = 11^{6 \cdot 29} \cdot 11^{29} = 669 \cdot 440 = 710$, que no está en la tabla.
- $11^{8 \cdot 29} = 11^{7 \cdot 29} \cdot 11^{29} = 710 \cdot 440 = 292$, que no está en la tabla.
- $11^{9 \cdot 29} = 11^{8 \cdot 29} \cdot 11^{29} = 292 \cdot 440 = 113$, que no está en la tabla.
- $11^{10 \cdot 29} = 11^{9 \cdot 29} \cdot 11^{29} = 113 \cdot 440 = 219$, que no está en la tabla.
- $11^{11 \cdot 29} = 11^{10 \cdot 29} \cdot 11^{29} = 219 \cdot 440 = 714$, que no está en la tabla.
- $11^{12 \cdot 29} = 11^{11 \cdot 29} \cdot 11^{29} = 714 \cdot 440 = 374$, que no está en la tabla.

- $11^{13\cdot 29} = 11^{12\cdot 29} \cdot 11^{29} = 374 \cdot 440 = 116$, que no está en la tabla.
- $11^{14\cdot 29} = 11^{13\cdot 29} \cdot 11^{29} = 116 \cdot 440 = 700$, que no está en la tabla.
- $11^{15\cdot 29} = 11^{14\cdot 29} \cdot 11^{29} = 700 \cdot 440 = 87$, que no está en la tabla.
- $11^{16\cdot 29} = 11^{15\cdot 29} \cdot 11^{29} = 87 \cdot 440 = 525$, que no está en la tabla.
- $11^{17\cdot 29} = 11^{16\cdot 29} \cdot 11^{29} = 525 \cdot 440 = 275$, que no está en la tabla.
- $11^{18\cdot 29} = 11^{17\cdot 29} \cdot 11^{29} = 275 \cdot 440 = 184$, y este sí está en la tabla.

Vemos que $11^{18\cdot 29} = 766 \cdot 11^5$, luego $776 = 11^{18\cdot 29-5} = 11^{517}$.
Luego $\log_{11}(766)$ mód $839 = 517$.

Algoritmo ρ de Pollard

La idea de este algoritmo es crear una sucesión pseudoaleatoria de elementos módulo p de la forma $x_i = a^{\alpha_i} \cdot b^{\beta_i}$.
Si en esta sucesión encontramos dos elementos iguales, es decir, $x_i = x_j$, entonces tendremos que $a^{\alpha_i} \cdot b^{\beta_i} = a^{\alpha_j} \cdot b^{\beta_j}$.
Si $b = a^x$, entonces $a^{\alpha_i} \cdot a^{x\cdot\beta_i} = a^{\alpha_j} \cdot a^{x\cdot\beta_j}$, y de aquí $a^{x(\beta_j-\beta_i)} = a^{\alpha_i-\alpha_j}$. Por el teorema de Fermat, sabemos que $a^{p-1} = 1$, luego

$$x(\beta_j - \beta_i) \equiv (\alpha_i - \alpha_j) \text{ mód } p-1.$$

En tal caso, una solución de la congruencia $x(\beta_j - \beta_i) \equiv (\alpha_i - \alpha_j)$ mód $p-1$ es probable que sea una solución del problema del logaritmo discreto.
Una vez explicada la idea, vamos a concretar cómo funciona el algoritmo.
En primer lugar, vamos a construir la sucesión (x_i, α_i, β_i). Para esto, dividimos el conjunto $X = \{1, 2, \cdots, p-1\}$ en tres subconjuntos S_1, S_2 y S_3, con la condición de que $1 \notin S_2$.
Una posible división podría ser:

$S_1 = \{x \in X : x \text{ mód } 3 = 1\}$.
$S_2 = \{x \in X : x \text{ mód } 3 = 0\}$.
$S_3 = \{x \in X : x \text{ mód } 3 = 2\}$.

Una vez hecho esto, comenzamos con $(x_0, \alpha_0, \beta_0) = (1, 0, 0)$ y definimos:

$$(x_{i+1}, \alpha_{i+1}, \beta_{i+1}) = \begin{cases} (x_i b \text{ mód } p, & \alpha_i, & \beta_i + 1) & \text{si } x_i \in S_1 \\ ((x_i)^2 \text{ mód } p, & 2\alpha_i \text{ mód } p-1, & 2\beta_i \text{ mód } p-1) & \text{si } x_i \in S_2 \\ (x_i a \text{ mód } p, & \alpha_i + 1, & \beta_i) & \text{si } x_i \in S_3 \end{cases}$$

Vamos a ver un ejemplo. Para esto, imaginemos que queremos calcular $\log_5(24)$ mód 47.
Entonces, $a = 5$, $b = 24$, $p = 47$.
Comenzamos con $(x_0, \alpha_0, \beta_0) = (1, 0, 0)$ y calculamos:

$(x_1, \alpha_1, \beta_1) = (24, 0, 1)$	Pues $x_0 \in S_1$	$1 \cdot 24 = 24$
$(x_2, \alpha_2, \beta_2) = (12, 0, 2)$	Pues $x_1 \in S_2$	$24 \cdot 24 = 576 = 12$
$(x_3, \alpha_3, \beta_3) = (3, 0, 4)$	Pues $x_2 \in S_2$	$12 \cdot 12 = 144 = 3$
$(x_4, \alpha_4, \beta_4) = (9, 0, 8)$	Pues $x_3 \in S_2$	$3 \cdot 3 = 9$
$(x_5, \alpha_5, \beta_5) = (34, 0, 16)$	Pues $x_4 \in S_2$	$9 \cdot 9 = 81 = 34$
$(x_6, \alpha_6, \beta_6) = (17, 0, 17)$	Pues $x_5 \in S_1$	$34 \cdot 24 = 816 = 17$
$(x_7, \alpha_7, \beta_7) = (38, 1, 17)$	Pues $x_6 \in S_3$	$17 \cdot 5 = 85 = 38$
$(x_8, \alpha_8, \beta_8) = (2, 2, 17)$	Pues $x_7 \in S_3$	$38 \cdot 5 = 190 = 2$
$(x_9, \alpha_9, \beta_9) = (10, 3, 17)$	Pues $x_8 \in S_3$	$2 \cdot 5 = 10$
$(x_{10}, \alpha_{10}, \beta_{10}) = (5, 3, 18)$	Pues $x_9 \in S_1$	$10 \cdot 24 = 240 = 5$
$(x_{11}, \alpha_{11}, \beta_{11}) = (25, 4, 18)$	Pues $x_{10} \in S_3$	$5 \cdot 5 = 25$
$(x_{12}, \alpha_{12}, \beta_{12}) = (36, 4, 19)$	Pues $x_{11} \in S_1$	$25 \cdot 24 = 600 = 36$
$(x_{13}, \alpha_{13}, \beta_{13}) = (27, 8, 38)$	Pues $x_{12} \in S_2$	$36 \cdot 36 = 1296 = 27$
$(x_{14}, \alpha_{14}, \beta_{14}) = (24, 16, 30)$	Pues $x_{13} \in S_2$	$27 \cdot 27 = 729 = 24$
$(x_{15}, \alpha_{15}, \beta_{15}) = (12, 32, 14)$	Pues $x_{14} \in S_2$	$24 \cdot 24 = 576 = 12$
$(x_{16}, \alpha_{16}, \beta_{16}) = (3, 18, 28)$	Pues $x_{15} \in S_2$	$12 \cdot 12 = 144 = 3$
$(x_{17}, \alpha_{17}, \beta_{17}) = (9, 36, 10)$	Pues $x_{16} \in S_2$	$3 \cdot 3 = 9$
$(x_{18}, \alpha_{18}, \beta_{18}) = (34, 26, 20)$	Pues $x_{17} \in S_2$	$9 \cdot 9 = 81 = 34$
$(x_{19}, \alpha_{19}, \beta_{19}) = (17, 4, 21)$	Pues $x_{18} \in S_1$	$34 \cdot 24 = 816 = 17$

Vemos que la primera coincidencia se produce en los términos x_1 y x_{14} (ambos valen 24).

Planteamos la congruencia

$$(\beta_{14} - \beta_1)x \equiv (\alpha_1 - \alpha_{14}) \text{ mód } p - 1.$$

Es decir:

$$29x \equiv -16 \text{ mód } 46$$

Que tiene una única solución entre 0 y 45, y es $x = 28$.

Por tanto, $\log_5(24)$ mód $47 = 28$. Puede comprobarse que 5^{28} mód $47 = 24$.

El algoritmo, tal y como lo hemos planteado presenta un inconveniente. Necesitamos almacenar todos los términos de la sucesión (x_n, α_n, β_n). Y cada vez que calculemos uno nuevo, hemos de compararlo con todos los anteriores.

En este ejemplo requeriría entonces:

- Almacenar 14 términos de la sucesión.
- Realizar $1+2+3+\cdots+13 = 91$ comparaciones (calculado x_2 hay que compararlo con x_1; calculado x_3 hay que compararlo con x_1 y x_2; calculado x_4 hay que compararlo con x_1, x_2, x_3. Y así hasta x_{14}).

Sin embargo, podemos ver que desde el momento en que se produce una coincidencia ($x_1 = x_{14}$), ésta se mantiene en los siguientes términos ($x_2 = x_{15}$, $x_3 = x_{16}$, etc.).

Entonces, lo que hacemos es calcular de forma paralela las sucesiones (x_n, α_n, β_n) y $(x_{2n}, \alpha_{2n}, \beta_{2n})$, y buscamos una coincidencia entre el término x_n y el término x_{2n}.

En el ejemplo que estamos estudiando, esta coincidencia se produciría en los términos x_{13} y x_{26}.

De esta forma no es necesario almacenar los términos de la sucesión y no hay que realizar tantas comparaciones. Por el contrario, hay que calcular más términos.

Comparamos los cálculos que debemos realizar en el ejemplo que acabamos de ver con un método y con el otro:

- Con el método primero tenemos que tener almacenados 14 términos de la sucesión (es decir, 42 datos), mientras que con el segundo únicamente 2 términos (es decir, 6 datos).

- Con el método primero tenemos que realizar 91 comparaciones. Con el segundo, 13.

- Con el primer método hay que calcular 14 términos de la sucesión, mientras que con el segundo hay que calcular 39.

Al ejecutar el algoritmo podría ocurrir que la congruencia $x(\beta_j - \beta_i) \equiv (\alpha_i - \alpha_j)$ mód $p - 1$ tuviera varias soluciones entre 0 y $p - 2$ y no todas estas soluciones son solución al problema del logaritmo.

Volviendo al ejemplo anterior del cálculo de $\log_5(24)$ mód 47, sabemos que podemos resolverlo calculando las sucesiones:

$$(x_1, \alpha_1, \beta_1);\ (x_2, \alpha_2, \beta_2);\ \cdots (x_{13}, \alpha_{13}, \beta_{13}).$$

$$(x_2, \alpha_2, \beta_2);\ (x_4, \alpha_4, \beta_4);\ \cdots (x_{26}, \alpha_{26}, \beta_{26}).$$

$(x_{13}, \alpha_{13}, \beta_{13})$ lo hemos calculado y vale $(27, 8, 38)$, mientras que $(x_{26}, \alpha_{26}, \beta_{26}) = (27, 14, 0)$.

La congruencia a resolver es entonces $-38x \equiv -6$ mód 46, que tiene como soluciones a $x = 5$ y $x = 28$. Entonces $x = 5$ no es solución al problema del logaritmo discreto mientras que $x = 28$ sí lo es.

3.2. Factorización

Dado un número n, que sabemos que no es primo, queremos encontrar un divisor suyo. Vamos a dar tres métodos para encontrar este divisor.

División por tentativa

Es el método que aprendimos en primaria. Se trata de ir dividiendo por los distintos números primos, empezando por 2, hasta que en una división nos dé resto 0. En tal caso, ya hemos encontrado el divisor.

Este método funciona si el número n tiene un divisor pequeño.

Método de Fermat

La idea de este método es, dado el número n, encontrar números x e y tales que $x^2 - y^2 = n$. Una vez encontrados, tendremos que $n = x^2 - y^2 = (x + y)(x - y)$, y de esta forma tendremos una factorización de n.

Para encontrar x e y partimos de $x = \lceil \sqrt{n} \rceil$, calculamos $x^2 - n$ y comprobamos si es un cuadrado. En caso afirmativo ya tenemos x e y. En caso negativo, incrementamos x en una unidad y repetimos el proceso.

Vamos a tomar $n = 1247629$. Podemos comprobar que no es primo (test de Miller-Rabin), luego vamos a proceder a factorizarlo por el método de Fermat. Puesto que $\sqrt{n} = 1116,97$ comenzamos con $x = 1117$.

Ordenamos los cálculos en la siguiente tabla:

x	$x^2 - n$	¿Es $x^2 - n$ un cuadrado perfecto?
1117	420	NO
1118	2295	NO
1119	4532	NO
1120	6771	NO
1121	9012	NO
1122	11255	NO
1123	13500	NO
1124	15747	NO
1125	17996	NO
1126	20247	NO
1127	22500	SI

Puesto que $22500 = 150^2$, tenemos que $1127^2 - n = 150^2$, luego $n = (1127 + 150) \cdot (1127 - 150) = 1277 \cdot 977$, y ya tenemos la factorización de n.

Este algoritmo funciona bien si el número n se descompone como producto de dos números que están próximos entre sí.

Algoritmo ρ de Pollard

La idea de este algoritmo es similar a la del algoritmo que hemos visto para el logaritmo discreto.

Se trata de construir una sucesión $x_1, x_2, \cdots, x_n$ y encontrar dos términos de la sucesión x_i, x_j tales que $\text{mcd}(x_i - x_j, n) \neq 1$ (en cuyo caso diremos que tenemos una coincidencia). Cuando esto ocurra tendremos un divisor de n (salvo que el máximo común divisor valga n).

Al igual que en el caso del logaritmo discreto, si $\text{mcd}(x_i - x_j, n) \neq 1$, entonces $\text{mcd}(x_{i+1} - x_{j+1}, n) \neq 1$, por lo que en lugar de buscar coincidencias entre términos cualesquiera de la sucesión, la buscaremos entre un término x_i y x_{2i}.

Para construir la sucesión x_n, partiremos de una semilla x_0, y mediante una función f calcularemos x_{i+1} como $f(x_i)$.

Es usual tomar la función $f(x) = (x^2 + 1)$ mód n, pues es sencilla de evaluar y produce una sucesión aparentemente aleatoria. Como semilla tomaremos $x_0 = 0$.

Vamos a aplica este algoritmo para factorizar el mismo número n del ejemplo anterior:

i	x_i	x_{2i}	mcd$(x_{2i} - x_i, n)$
1	1	2	1
2	2	26	1
3	5	458330	1
4	26	948812	1
5	677	266898	1
6	458330	1097620	1
7	598913	438011	1277

Y tenemos que 1277 es un divisor de n.

3.3. Raíces cuadradas modulares

Dado un número primo p y número entero a, tratamos de estudiar si existe x tal que $x^2 \equiv a$ mód p. Es decir, si a tiene una raíz cuadrada módulo p.

Si a es múltiplo de p, entonces a mód $p = 0$ y podemos tomar $b = 0$. Nos centraremos entonces en el caso de que a no es múltiplo de p (es decir, mcd$(a, p) = 1$).

Definimos entonces una función booleana, que llamaremos *símbolo de Legendre* como sigue:

Sea p un número primo impar y a un número tal que mcd$(a, p) = 1$. Definimos:

$$\left(\frac{a}{p}\right) = \begin{cases} \text{T} & \text{Si } a \text{ tiene raíz cuadrada módulo } p. \\ \text{F} & \text{Si } a \text{ no tiene raíz cuadrada módulo } p. \end{cases}$$

Por ejemplo, $\left(\frac{2}{7}\right) = \text{T}$, pues $3^2 \equiv 2$ mód 7, es decir, 2 tiene raíz cuadrada módulo 7. Sin embargo, $\left(\frac{3}{7}\right) = \text{F}$ pues no hay ningún número que elevado al cuadrado sea igual a 3 módulo 7.

$$\begin{array}{lll} 1^2 = 1 & 2^2 = 4 & 3^2 = 2 \\ 6^2 = 1 & 5^2 = 4 & 4^2 = 2 \end{array}$$

Notemos que puesto que x^2 mód $p = (-x)^2$ mód $p = (p - x)^2$ mód p, para comprobar si un número tiene o no raíz cuadrada módulo p basta con calcular los cuadrados de los números comprendidos entre 1 y $\frac{p-1}{2}$.

A la hora de escribir el símbolo de Legendre, se sustituye T por 1 y F por -1. Y para incluir el caso en que mcd(a, p) valga p, se incluye un caso más.

La definición quedaría entonces:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{Si mcd}(a, p) = p \\ 1 & \text{Si } a \text{ tiene raíz cuadrada módulo } p. \\ -1 & \text{Si } a \text{ no tiene raíz cuadrada módulo } p. \end{cases}$$

De esta forma podemos aprovechar las propiedades numéricas del 1 y el -1.

El símbolo de Legendre tiene las siguientes propiedades:

- $\left(\frac{a}{p}\right) = \left(\frac{a \text{ mód } p}{p}\right)$.
- $\left(\frac{1}{p}\right) = 1$.
- $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
- $\left(\frac{a^2}{p}\right) = 1$ (si mcd$(a, p) = 1$).
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 \text{ mód } 4 \\ -1 & \text{si } p \equiv 3 \text{ mód } 4 \end{cases}$

- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p \equiv 1,7 \text{ mód } 8 \\ -1 & \text{si } p \equiv 3,5 \text{ mód } 8 \end{cases}$
- Si q es un primo impar, $\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{si } p, q \equiv 3 \text{ mód } 4 \\ \left(\frac{p}{q}\right) & \text{en otro caso.} \end{cases}$.

  Esta última propiedad se conoce como *ley de reciprocidad cuadrática*.

Por ejemplo, para calcular $\left(\frac{245}{911}\right)$ procederíamos como sigue:

$$\left(\frac{245}{911}\right) = \left(\frac{5 \cdot 7^2}{911}\right) = \left(\frac{5}{911}\right) \cdot \left(\frac{7^2}{911}\right) = \left(\frac{911}{5}\right) \cdot 1 = \left(\frac{1}{5}\right) = 1.$$

donde en primer lugar hemos factorizado 245 como producto de primos, y hemos descompuesto el símbolo de Legendre como producto de dos símbolos de Legendre. El segundo, $\left(\frac{7^2}{911}\right)$, vale 1, mientras que, por la ley de reciprocidad cuadrática, y dado que $5 \equiv 1$ mód 4, se tiene que $\left(\frac{5}{911}\right) = \left(\frac{911}{5}\right)$.

Este resultado nos dice que 245 tiene raíz cuadrada módulo 911. Podemos comprobar que $34^2 \equiv 245$ mód 911.

Veamos otro ejemplo:

$$\left(\frac{782}{911}\right) = \left(\frac{2 \cdot 17 \cdot 23}{911}\right) = \left(\frac{2}{911}\right) \cdot \left(\frac{17}{911}\right) \cdot \left(\frac{23}{911}\right) = 1 \cdot \left(\frac{911}{17}\right) \cdot (-1) \cdot \left(\frac{911}{23}\right) = -\left(\frac{10}{17}\right) \cdot \left(\frac{14}{23}\right) =$$

$$= -\left(\frac{2}{17}\right)\left(\frac{5}{17}\right) \cdot \left(\frac{2}{23}\right) \cdot \left(\frac{7}{23}\right) = -1 \cdot \left(\frac{17}{5}\right) \cdot 1 \cdot (-1) \cdot \left(\frac{23}{7}\right) = \left(\frac{2}{5}\right) \cdot \left(\frac{2}{7}\right) = (-1) \cdot 1 = -1.$$

Donde:

- $\left(\frac{2}{911}\right) = 1$ pues $911 \equiv 7$ mód 8.
- $\left(\frac{17}{911}\right) = \left(\frac{911}{17}\right)$ pues $17 \equiv 1$ mód 4.
- $\left(\frac{23}{911}\right) = -\left(\frac{911}{17}\right)$ pues $23 \equiv 3$ mód 4 y $911 \equiv$ mód 4.
- $\left(\frac{2}{17}\right) = 1$ pues $17 \equiv 1$ mód 8.
- $\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right)$ pues $5 \equiv 1$ mód 4.
- $\left(\frac{2}{23}\right) = 1$ pues $23 \equiv 7$ mód 8.
- $\left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right)$ pues $7 \equiv 3$ mód 4 y $23 \equiv 3$ mód 4.
- $\left(\frac{2}{5}\right) = -1$ pues $5 \equiv 5$ mód 8.
- $\left(\frac{2}{7}\right) = 1$ pues $7 \equiv 7$ mód 8.

El cálculo del símbolo de Legendre tiene un inconveniente. Para llevarlo a cabo es necesario factorizar algunos números como producto de números primos, ya que en principio sólo tiene sentido cuando el segundo argumento es un número primo. Y para aplicar la ley de reciprocidad cuadrática, el primero debe serlo también. La factorización de enteros sabemos que puede ser muy costoso. Para evitarla se introduce el símbolo de Jacobi. En este, la única restricción al segundo argumento es que debe ser un número impar (distinto de uno).

Sean m, n dos números enteros, con n impar mayor que 1. Supongamos que la descomposición de n como producto de números primos es $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Se define el símbolo de Jacobi de m y n como:

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{\alpha_1} \cdots \left(\frac{m}{p_r}\right)^{\alpha_r}.$$

Las propiedades del símbolo de Jacobi son las mismas que hemos enunciado para el símbolo de Legendre, y esto nos permite realizar el cálculo sin necesidad de factorizar los números impares como producto de primos. Así, el cálculo que acabamos de hacer podemos realizarlo también como sigue:

$$\left(\frac{782}{911}\right) = \left(\frac{2 \cdot 391}{911}\right) = \left(\frac{2}{911}\right) \cdot \left(\frac{391}{911}\right) = -\left(\frac{911}{391}\right) = -\left(\frac{129}{391}\right) = -\left(\frac{391}{129}\right) = -\left(\frac{4}{129}\right) = -1.$$

En este cálculo podemos escribir $\left(\frac{911}{391}\right)$ sin preocuparnos si 391 es o no primo, algo que con el símbolo de Legendre no podíamos hacer, por lo que, antes de aplicar la ley de reciprocidad cuadrática teníamos que factorizar 391.

Con respecto al símbolo de Jacobi, notemos que no tiene ningún significado más allá de una herramienta de cálculo (al contrario del símbolo de Legendre que nos indica si un número tiene o no raíz cuadrada). Por ejemplo, $\left(\frac{2}{15}\right) = 1$ y sin embargo, 2 no tiene raíz cuadrada módulo 15.

Una vez que podemos saber si un número tiene o no raíz cuadrada, vamos a ver cómo calcularla. Para eso, tenemos el algoritmo de Tonelli.

Partimos de un número primo impar p y un número a tal que $\left(\frac{a}{p}\right) = 1$. El algoritmo nos devuelve r tal que $r^2 \equiv a$ mód p.

Los pasos que debemos seguir son:

- Calculamos n tal que $\left(\frac{n}{p}\right) = -1$. Para esto, probamos con $n = 2$, si no vale probamos con $n = 3$ y así sucesivamente. Puesto que para la mitad de los números entre 1 y $p - 1$ se cumple esa condición, encontraremos rápido este número.
- Descomponemos $p - 1$ como $2^u \cdot s$, con s un número impar.
- Si $u = 1$, entonces $r = a^{\frac{p+1}{4}}$ mód p es una raíz cuadrada. El algoritmo termina. En caso contrario, continuamos.
- Calculamos $r = a^{\frac{s+1}{2}}$ mód p.
- Calculamos $b = n^s$ mód p.
- Calculamos $c = a^{-1}$ mód p (esto puede hacerse por el algoritmo extendido de Euclides, o bien como $c = a^{p-2}$ mód p).
- Hacemos $d = c \cdot r^2$ mód p.
- Para $j = 0, 1, \cdots, u - 2$, comenzando por $j = 0$, hacemos:
  - Calculamos $aux = d^{2^{u-2-j}}$ mód p.
  - Si $aux = p - 1$, hacemos $r = r \cdot b$ mód p y $d = d \cdot b^2$ mód p.
  - Hacemos $b = b^2$ mód p y $j = j + 1$ (independientemente de lo que valga aux).
- El valor de r es una raíz cuadrada de a. Devuelve r.

En las notas del curso hay una explicación de porqué este algoritmo calcula la raíz cuadrada de a.

3.4. Trabajo a realizar.

En esta práctica hay que implementar los distintos algoritmos que se han explicado en el guión. Para eso, se puede hacer uso de las funciones que están definidas en el fichero Practica3.py.

Una vez implementados, hay que hacer un estudio del tiempo que tarda en ejecutarse cada uno de los algoritmos en función de los parámetros de entrada, y hacer una estimación de cuándo es viable usarlos.

Hay que entregar el código con las distintas funciones y el análisis de los tiempos que se haya realizado.