Restos cuadráticos y tests aleatorios de no-primalidad

Vamos a estudiar las ecuaciones de la forma $x^2 \equiv a \pmod N$ para a y N dados. Por el teorema chino del resto, bastará con considerar el caso $N = p^n$ para $p \geq 2$ primo y $n \geq 1$.

El primer caso que vamos a discutir es cuando N es un primo impar. Sabemos que en este caso $(\mathbb{Z}/N\mathbb{Z})^* \simeq \mathbb{Z}/(N-1)\mathbb{Z}$ y por lo tanto hay exactamente $(N-1)/2$ elementos de $(\mathbb{Z}/N\mathbb{Z})^*$ que son cuadrados. Dicho de forma más complicada, el morfismo de grupos

$$\begin{aligned} sqr : (\mathbb{Z}/N\mathbb{Z})^* &\to (\mathbb{Z}/N\mathbb{Z})^* \\ [x] &\mapsto [x^2] \end{aligned}$$

tiene $\mathrm{Ker}(sqr) = \{[1], [-1]\}$ de dos elementos y por lo tanto su imagen $\mathrm{Im}(sqr) \simeq (\mathbb{Z}/N\mathbb{Z})^*/\mathrm{Ker}(sqr)$ es de $(N-1)/2$ elementos. El subgrupo $\mathrm{Im}(sqr)$ está formado por los *restos cuadráticos* módulo N. Si $[a] \in \mathrm{Im}(sqr)$, entonces la ecuación $x^2 \equiv a \pmod N$ tiene exactamente dos soluciones $1 \leq x < N$ y si $[a] \notin \mathrm{Im}(sqr)$ la ecuación $x^2 \equiv a \pmod N$ no tiene ninguna solución.

No hemos incluído en la discusión a la ecuación $x^2 \equiv 0 \pmod N$, ya que para N primo la única solución es $x \equiv 0 \pmod N$ y es inmediata de encontrar.

A nivel computacional tenemos que analizar las siguientes dos preguntas:

(REC) ¿Cómo reconocer eficientemente si un $a \in \mathbb{Z}$ coprimo con N es un resto cuadrático módulo N?

(SOL) Suponiendo que $a \in \mathbb{Z}$ coprimo con N es un resto cuadrático módulo N, ¿cómo obtener las dos soluciones de la ecuación $x^2 \equiv a \pmod N$ eficientemente?

La eficiencia es clave en las preguntas anteriores, ya que si no podríamos hacer una busqueda exhaustiva de complejidad binaria exponencial en $\log(N)$.

Proposición 5.1. *Sea N un primo impar y sea $a \in \mathbb{Z}$ coprimo con N. Son equivalentes:*

1. *a es un resto cuadrático módulo N.*
2. *$a^{(N-1)/2} \equiv 1 \pmod N$.*

Proof. $(1 \Rightarrow 2)$: Supongamos que $x^2 \equiv a \pmod N$ para cierto $x \in \mathbb{Z}$. Es claro que x debe ser coprimo con N, ya que si no tendríamos $a \equiv 0 \pmod N$, en contradicción con las hipótesis. Entonces $a^{(N-1)/2} \equiv x^{N-1} \equiv 1 \pmod N$ por el teorema de Euler-Fermat.
$(\neg 1 \Rightarrow \neg 2)$: Hemos probado que los $(N-1)/2$ restos cuadráticos módulo N son ceros del polinomio $T^{(N-1)/2} - 1 \in (\mathbb{Z}/N\mathbb{Z})[T]$. Como un polinomio (con coeficientes en un cuerpo) puede tener a lo sumo tantas raíces como el grado, resulta que para los no restos cuadráticos a se tendrá que $a^{(N-1)/2} \not\equiv 1 \pmod N$. □

La proposición 5.1 y el algoritmo de la exponenciación binaria modular resuelven eficientemente la pregunta **(REC)** de arriba. Basta invocar `pow(a,(N-1)//2,N)` y ver el resultado para determinar si $a \in \mathbb{Z}$ coprimo con N primo impar es un resto cuadrático o no. Una pregunta interesante es: ¿cuál es el resultado de hacer $a^{(N-1)/2} \bmod N$ cuando a no es un resto cuadrático?

Proposición 5.2. *Sea N un primo impar y supongamos que $a \in \mathbb{Z}$, coprimo con N, no es un resto cuadrático módulo N. Entonces $a^{(N-1)/2} \equiv -1 \pmod N$.*

Proof. Por el teorema de Euler-Fermat sabemos que $\left(a^{(N-1)/2}\right)^2 \equiv 1 \pmod N$. También sabemos que las únicas soluciones de $y^2 \equiv 1 \pmod N$ son $y \equiv \pm 1 \pmod N$, ya que $N \mid y^2 - 1$ si y solo si $N \mid y - 1$ o $N \mid y + 1$. Por la proposición anterior tenemos que $a^{(N-1)/2} \not\equiv 1 \pmod N$ y por lo tanto debe ser $a^{(N-1)/2} \equiv -1 \pmod N$. □

Definición 5.3. Sea N un primo impar y sea $a \in \mathbb{Z}$. El símbolo de Legendre se define como

$$\left(\frac{a}{N}\right) = \begin{cases} 0 & \text{si } N \mid a, \\ 1 & \text{si } a \text{ es resto cuadrático módulo } N, \\ -1 & \text{si } a \text{ no es resto cuadrático módulo } N. \end{cases}$$

El símbolo de Legendre solo depende de la clase de a módulo N. Las proposiciones 5.1 y 5.2 dicen que para un primo impar N se tiene que

$$a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N}. \tag{1}$$

Una consecuencia interesante de esta identidad es que $\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right)$ para todo $a, b \in \mathbb{Z}$. Un hecho que de no ser por esa identidad sería difícil de ver es que el producto de dos no restos cuadráticos es un resto cuadrático (módulo un primo N).

De la discusión de arriba, se infiere que será importante entender el valor de $\left(\frac{M}{N}\right)$ para M, N primos. Eso nos daría alguna información sobre $\left(\frac{a}{N}\right)$ a través de la factorización de a.

Teorema 5.4 (Ley de la reciprocidad cuadrática y suplementos (Gauss))**.** *Sean $N, M \geq 2$ primos impares. Entonces:*

1. $\left(\frac{M}{N}\right)\left(\frac{N}{M}\right) = (-1)^{(N-1)(M-1)/4} = \begin{cases} 1 & \text{si } N \equiv 1 \pmod 4 \text{ o } M \equiv 1 \pmod 4 \\ -1 & \text{si } N \equiv 3 \pmod 4 \text{ y } M \equiv 3 \pmod 4 \end{cases}$
2. $\left(\frac{2}{N}\right) = (-1)^{(N^2-1)/8} = \begin{cases} 1 & \text{si } N \equiv 1, 7 \pmod 8 \\ -1 & \text{si } N \equiv 3, 5 \pmod 8 \end{cases}$
3. $\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2} = \begin{cases} 1 & \text{si } N \equiv 1 \pmod 4 \\ -1 & \text{si } N \equiv 3 \pmod 4 \end{cases}$

Hay más de 240 demostraciones diferentes de la ley de reciprocidad cuadrática, de las que aquí solo mostraremos una de las más elementales, que usa ideas parecidas a la demostración clásica del Teorema de Euler-Fermat. Necesitamos primero el siguiente lema, que es importante en sí mismo.

Lema 5.5 (Einsenstein)**.** *Sea $N \geq 2$ un primo impar y sea $a \in \mathbb{Z}$ tal que $N \nmid a$. Entonces $\left(\frac{a}{N}\right) = (-1)^k$ donde $k = \sum_u \lfloor \frac{au}{N} \rfloor$ y la suma recorre todos los enteros u pares entre 2 y $N-1$, ambos inclusive. En el caso de que a sea impar, se puede tomar también $k = \sum_{u=1}^{(N-1)/2} \lfloor \frac{au}{N} \rfloor$, donde la suma recorre todos los índices (pares e impares) u entre 1 y $\frac{N-1}{2}$.*

Proof. Sea $U = \{2, 4, \ldots, N-1\}$ el conjunto de los números pares entre 2 y $N-1$. Consideremos la aplicación $\tau : U \to U$ dada por $u \mapsto \pm au \bmod N$, donde el signo se elige de modo que el resultado sea par (esto está bien definido ya que N es impar). Se tiene que τ es una biyección, ya que si $\pm au_1 \equiv \pm au_2 \pmod N$ para ciertos $u_1, u_2 \in U$, entonces $u_1 \equiv \pm u_2 \pmod N$ y esto solo es posible cuando $u_1 \equiv u_2 \pmod N$ ya que N es impar. En efecto, si fuese $u_1 \equiv -u_2 \pmod N$, tendríamos que $N \mid u_1 + u_2$, pero $4 \leq u_1 + u_2 \leq 2N - 2$, por lo que debería ser $u_1 + u_2 = N$ y eso es imposible ya que N es impar. Sabiendo que τ es una biyección, podemos calcular el producto de todos los números de U de dos formas distintas:

$$\prod_{u \in U} u \equiv \prod_{u \in U} \tau(u) \equiv \prod_{u \in U} \pm au \equiv (-1)^r a^{(N-1)/2} \prod_{u \in U} u \pmod{N},$$

donde r es la cantidad de $u \in U$ para los que hemos tenido que usar el signo $(-)$ al calcular $\tau(u)$. Esta identidad nos dice que $\left(\frac{a}{N}\right) = (-1)^r$, por lo que solo nos falta probar que r y k tienen la misma paridad. Para un $u \in U$, sabemos que $au \bmod N = au - N\lfloor \frac{au}{N} \rfloor$, por lo que $au \bmod N$ será impar (y por lo tanto aportará al valor de r) si y solo si $\lfloor \frac{au}{N} \rfloor$ es impar. Esto prueba que $r \equiv \sum_{u \in U} \lfloor \frac{au}{N} \rfloor = k \pmod 2$, tal como afirmabamos. La última parte se sigue de que, cuando a es impar, $\lfloor \frac{au}{N} \rfloor$ y $\lfloor \frac{a(N-u)}{N} \rfloor$ tiene la misma paridad. Eso nos permite cambiar los índices pares $u \in U$ mayores que $N/2$ por el correspondiente $N - u$ impar en el rango $1 \leq N - u < N/2$. □

Demostración del teorema 5.4. 1. Por el lema 5.5 de Einsenstein, tenemos que $\left(\frac{M}{N}\right)\left(\frac{N}{M}\right) = (-1)^{k+l}$ donde $k = \sum_{u=1}^{(N-1)/2} \lfloor \frac{uM}{N} \rfloor$ y $l = \sum_{v=1}^{(M-1)/2} \lfloor \frac{vN}{M} \rfloor$. Es fácil ver que k es exactamente la cantidad de puntos enteros en el *interior* del triángulo $(0,0) - (N/2,0) - (N/2,M/2)$ y que, de forma similar, l es la cantidad de puntos enteros en el interior del triángulo $(0,0) - (0,M/2) - (N/2,M/2)$. Como N y M son primos, el segmento $(0,0) - (N/2,M/2)$ no tiene puntos enteros y por lo tanto $k+l$ es la cantidad de puntos enteros en el interior del rectángulo $(0,0) - (N/2,0) - (N/2,M/2) - (0,M/2)$, es decir, $(N-1)(M-1)/4$.
2. Aplicamos el lema 5.5 para $a = 2$. Se puede ver que

$$k = \sum_{\substack{u=2 \\ u \text{ par}}}^{N-1} \left\lfloor \frac{2u}{N} \right\rfloor = |\{u \mid u \text{ par y } \frac{N}{2} < u < N\}| = \left\lfloor \frac{N+1}{4} \right\rfloor$$

y eso es par si $N \equiv 1, 7 \pmod 8$ e impar si $N \equiv 3, 5 \pmod 8$.
3. Ya hemos probado que $\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2}$ y eso da 1 si $N \equiv 1 \pmod 4$ y -1 si $N \equiv 3 \pmod 4$. □

Veamos un ejemplo simple de como usar la ley de reciprocidad cuadrática. Digamos que queremos ver si 2021 es resto cuadrático módulo el primo 3331.

$$\begin{aligned}\left(\frac{2021}{3331}\right) &= \left(\frac{43}{3331}\right)\left(\frac{47}{3331}\right) = \left(\frac{3331}{43}\right)\left(\frac{3331}{47}\right) = \left(\frac{20}{43}\right)\left(\frac{41}{47}\right) = \left(\frac{2}{43}\right)^2\left(\frac{5}{43}\right)\left(\frac{41}{47}\right) \\ &= \left(\frac{5}{43}\right)\left(\frac{41}{47}\right) = \left(\frac{43}{5}\right)\left(\frac{47}{41}\right) = \left(\frac{3}{5}\right)\left(\frac{6}{41}\right) = \left(\frac{3}{5}\right)\left(\frac{2}{41}\right)\left(\frac{3}{41}\right) = \left(\frac{3}{5}\right)\left(\frac{3}{41}\right) \\ &= \left(\frac{5}{3}\right)\left(\frac{41}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right) = 1\end{aligned}$$

En efecto, una búsqueda exhaustiva nos muestra que $2021 \equiv 534^2 \pmod{3331}$, es decir, 2021 es un resto cuadrático módulo 3331 tal como calculamos arriba.

El único problema con este método para calcular el símbolo de Legendre es que requiere factorizar el numerador en cada paso, y para eso aún no se disponen de algoritmos eficientes.

Definición 5.6. Sea $N = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ un entero impar con los p_i primos y los $n_i \geq 1$. Sea $a \in \mathbb{Z}$ coprimo con N, es decir, $p_i \nmid a$ para todo $i = 1, \ldots, k$. El símbolo de Jacobi $\left(\frac{a}{N}\right)$ se define como

$$\left(\frac{a}{N}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{n_i}$$

donde los factores de la derecha son símbolos de Legendre. No hay ambigüedad en la notación ya que ambos símbolos coinciden para N primo.

El valor de $\left(\frac{a}{N}\right)$ depende solo de la clase de a módulo N, al igual que para el símbolo de Legendre. Más aún, Jacobi demostró que su extensión del símbolo de Legendre hace que la ley de reciprocidad cuadrática y sus suplementos (teorema 5.4) sigan siendo válidos para cualquier N y M impares.

Problema 5.1. Demostrar la ley de reciprocidad cuadrática y sus suplementos para el símbolo de Jacobi.

La ventaja del símbolo de Jacobi es que se puede calcular fácilmente sin necesidad de factorizar el numerador. Se puede utilizar la técnica con la que implementamos `gcd_binario()` o bien la de `gcd_euclides()`. Utilizando este segundo método, el ejemplo que calculamos antes quedaría

$$\begin{aligned}\left(\frac{2021}{3331}\right) &= \left(\frac{3331}{2021}\right) = \left(\frac{1310}{2021}\right) = \left(\frac{2}{2021}\right)\left(\frac{655}{2021}\right) = -\left(\frac{655}{2021}\right) = -\left(\frac{2021}{655}\right) = -\left(\frac{56}{655}\right) \\ &= -\left(\frac{2}{655}\right)^3\left(\frac{7}{655}\right) = -\left(\frac{7}{655}\right) = \left(\frac{655}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1\end{aligned}$$

Problema 5.2. Implementar en Python3 la función recursiva `jacobi(a,n)` que calcule el símbolo de Jacobi. ¿Cuál es la complejidad binaria de esta función?

Advertencia 1: El símbolo de Jacobi NO corresponde con la noción de ser resto cuadrático módulo un N impar cualquiera. Esa propiedad solo vale para N primo.

Problema 5.3. Escribir un programa en Python3 que encuentre todos los a que no sean restos cuadráticos módulo $2021 = 43 \cdot 47$, pero que verifiquen $\left(\frac{a}{2021}\right) = 1$.

Advertencia 2: En general, el símbolo de Jacobi NO satisface la ecuación (1). Eso solo vale para N primo impar.

Proposición 5.7. *Si $N \geq 3$ es un entero impar que es divisible por al menos dos primos distintos, entonces*

$$\left|\{1 \leq a < N \mid \gcd(a, N) = 1 \wedge a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N}\}\right| \leq \frac{\varphi(N)}{2}$$

Proof. Consideremos la aplicación $\eta : (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^*$ dado por $[a] \mapsto \left[a^{(N-1)/2}\left(\frac{a}{N}\right)\right]$. Como el símbolo de Jacobi es multiplicativo, se tiene que η es un morfismo de grupos. Bastará con probar que $\mathrm{Im}(\eta)$ tiene al menos dos elementos, ya que en ese caso tendríamos $|\mathrm{Ker}(\eta)| = \frac{|(\mathbb{Z}/N\mathbb{Z})^*|}{|\mathrm{Im}(\eta)|} \leq \frac{\varphi(N)}{2}$, tal como afirma la proposición. Vamos a proceder por contradicción, es decir, vamos a suponer que $\mathrm{Im}(\eta) = \{[1]\}$. En particular tenemos que $a^{N-1} \equiv 1 \pmod{N}$ para todo a coprimo con N, es decir, N es un número de Carmichael. Por el criterio de Korselt, N debe ser libre de cuadrados, es decir, $N = p_1 p_2 \cdots p_k$ para los p_i primos impares distintos tales que $p_i - 1 \mid N - 1$. Usando el teorema chino del resto, construimos un entero a que no sea un cuadrado módulo p_1 y p_2 y que sea 1 módulo los demás p_i. Por definición, se tiene que $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = -1$ y $\left(\frac{a}{p_i}\right) = 1$ para $i \geq 3$. En particular, $\left(\frac{a}{N}\right) = 1$ y por lo tanto debe ser $a^{(N-1)/2} \equiv 1 \pmod{N}$ de acuerdo con la hipótesis $\mathrm{Im}(\eta) = \{[1]\}$. Esta última congruencia implica que $a^{(N-1)/2} \equiv 1 \pmod{p_1}$. Ahora volvemos a utilizar el teorema chino del resto para producir un entero b que sea a módulo p_1 y que sea 1 módulo los demás p_i. Se tiene entonces que $\left(\frac{b}{N}\right) = -1$ y por lo tanto que $b^{(N-1)/2} \equiv -1 \pmod{N}$. Esto nos conduce a la contradicción $b^{(N-1)/2} \equiv -1 \pmod{p_1}$, ya que $a \equiv b \pmod{p_1}$ por construcción. □

La proposición anterior suele usarse para comprobar rápidamente si un número impar N es primo o no. La idea es elegir un entero $a \in \{1, \ldots, N-1\}$ uniformemente al azar y comprobar que $\gcd(a, N) = 1$ y que $a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N}$, utilizando algoritmos rápidos para el máximo común divisor, para el símbolo de Jacobi y para la exponenciación modular. Si N no pasa el test, queda demostrado que no es primo. En caso contrario, se vuelve a repetir k veces la prueba. De acuerdo con la proposición 5.7, la probabilidad de que un número compuesto pase k veces el test es a lo sumo 2^{-k}. Este método se llama de Solovay-Strassen.

Problema 5.4. Implementar en Python3 la función `test_de_solovay_strassen(n,k)` que aplique $k \geq 1$ iteraciones del test de Solovay-Strassen al entero $n \geq 2$ dado. Si n no pasa el test, la función debe devolver la cadena `"compuesto"` y en caso contrario `"probablemente primo"`. Los casos donde n es par se deben resolver directamente (son triviales) antes de aplicar los tests.

Problema 5.5. Una versión efectiva del teorema del número primo afirma que

$$\frac{x}{\ln(x) + 2} < \pi(x) < \frac{x}{\ln(x) - 4} \quad \forall\, x \geq 55,$$

donde $\pi(x)$ es la cantidad de números primos en el intervalo $[1, x]$ y $\ln(x)$ es el logaritmo natural. En particular, la probabilidad de encontrar un número primo en el intervalo $[1, 10^{300} - 1]$ eligiendo uniformemente al azar 300 dígitos decimales es aproximadamente $1.45 \cdot 10^{-3}$, es decir, uno entre 690. Escribir un programa que genere números de 300 dígitos decimales al azar (dígito a dígito), que aplique el test de Solovay-Strassen con $k = 20$ y que se detenga al encontrar un entero que pase el test, es decir, uno que sea `"probablemente primo"`. ¿Cuántos enteros fueron explorados hasta conseguir el resultado? ¿Qué pasa si se repite el experimento varias veces?

Ya estamos en condiciones de entender cuáles ecuaciones $x^2 \equiv a \pmod{N}$ son resolubles para cualquier $N \geq 2$ y $a \in \mathbb{Z}$. Lo primero que debemos hacer es factorizar $N = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ y de ese modo reducir el problema al caso $N = p^n$ para p primo y $n \geq 1$. Por el teorema chino del resto, $x^2 \equiv a \pmod{N}$ tiene solución si y solo si $x^2 \equiv a \pmod{p_i^{n_i}}$ tiene solución para todo $i = 1, \ldots, k$. El caso $n = 1$ corresponde con todo lo que vimos antes y se resuelve eficientemente utilizando el símbolo de Jacobi. El caso $n > 1$ no aporta demasiada dificultad, como muestra el siguiente resultado. Solo discutimos el caso $\gcd(a, N) = 1$, es decir, $p \nmid a$, ya que es fácil reducirse siempre a esa situación: si $a = p^u b$ con $p \nmid b$ y $1 \leq u < n$, entonces $x^2 \equiv a \pmod{N}$ tiene solución si y solo si u es par y b es resto cuadrático módulo N.

Proposición 5.8. *Sea $N = p^n$ con p primo impar y $n \geq 1$. Sea $a \in \mathbb{Z}$ coprimo con N, es decir, $p \nmid a$. Entonces a es resto cuadrático módulo N si y solo si a es resto cuadrático módulo p.*

Proof. Bastará con probar que si la ecuación $x^2 \equiv a \pmod{p^k}$ tiene solución para un cierto $k \geq 1$, entonces también la tendrá la ecuación $x^2 \equiv a \pmod{p^{k+1}}$. Sea $x_0 \in \mathbb{Z}$ tal que $x_0^2 = a + p^k t$ para cierto $t \in \mathbb{Z}$, es decir, x_0 es una solución de la congruencia $x^2 \equiv a \pmod{p^k}$. Tenemos que $(x_0 + p^k \ell)^2 = x_0^2 + 2p^k \ell x_0 + p^{2k} \ell^2 \equiv a + p^k(t + 2\ell x_0) \pmod{p^{k+1}}$. Eligiendo ℓ tal que $-2x_0 \ell \equiv t \pmod{p}$ se consigue que $x_0 + p^k \ell$ sea una solución de $x^2 \equiv a \pmod{p^{k+1}}$. La elección de ℓ es posible ya que $\gcd(-2x_0, p) = 1$. □

Problema 5.6. Sea $n \geq 3$ y sea $a \in \mathbb{Z}$. Demostrar con un argumento inductivo que la congruencia $x^2 \equiv a \pmod{2^n}$ tiene solución si y solo si $a \equiv 1 \pmod{8}$.

Solo nos queda resolver el problema **(SOL)**, es decir, sabiendo que $x^2 \equiv a \pmod{N}$ tiene solución para $N \geq 2$ y $a \in \mathbb{Z}$ coprimo con N dados, obtener algorítmicamente los posibles x. Por el teorema chino del resto podemos reducirnos al caso $N = p^n$ para p primo y $n \geq 1$, y por el argumento inductivo visto en la demostración de la proposición 5.8 bastará con considerar el caso $n = 1$ y p primo impar.

Algoritmo de Tonelli-Shanks: Sea p un primo impar y supongamos que $p = r2^k + 1$ con $k \geq 1$ y r impar. Como primera aproximación, calculamos $x = a^{(r+1)/2} \bmod p$, que satisface $x^2 \equiv a^{r+1} \equiv aa^r \pmod{p}$. Si $a^r \equiv 1 \pmod{p}$, hemos terminado, ya que tendríamos $x^2 \equiv a \pmod{p}$. En caso contrario, observemos que el valor $z = a^r \bmod p$ es una raíz (2^{k-1})-ésima de la unidad módulo p. En efecto, se tiene que $z^{2^{k-1}} \equiv a^{r2^{k-1}} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$, ya que a es un resto cuadrático. Es decir, tenemos que $x^2 \equiv az \pmod{p}$ con z una raíz (2^{k-1})-ésima de la unidad. Iremos cambiando los valores de x y z adecuadamente en esa expresión, para ir consiguiendo iterativamente que z sea una raíz (2^{k-2})-ésima de la unidad, luego una raíz (2^{k-3})-ésima, y así siguiendo, hasta llegar a $z = 1$. En ese punto, el valor de x es la raíz cuadrada buscada. Para la iteración, supondremos que $x^2 \equiv az \pmod{p}$ con z una raíz (2^s)-ésima de la unidad módulo p para un cierto $1 \leq s \leq k - 1$. Lógicamente, si resulta que z es también una raíz (2^{s-1})-ésima, no hay nada que hacer. Notar que esta condición puede testearse fácilmente comprobando que $z^{2^{s-1}} \equiv 1 \pmod{p}$. El caso interesante es el otro, en el que se tiene necesariamente que $z^{2^{s-1}} \equiv -1 \pmod{p}$. El truco aquí es reemplazar x por $xt \pmod{p}$ y z por $zt^2 \pmod{p}$, donde t satisface $t^{2^s} \equiv -1 \pmod{p}$. Una forma sencilla de conseguir un valor de t que cumpla con esa condición es tomar $t \equiv g^{(p-1)/2^{s+1}} \equiv g^{r2^{k-s-1}} \pmod{p}$ para una raíz primitiva cualquiera g módulo p.

Problema 5.7. Implementar la función `raiz_cuadrada_modular(a,p)` que calcule una solución de la congruencia $x^2 \equiv a \pmod{p}$ para a un resto cuadrático módulo p y p un primo impar. Para conseguir una raíz primitiva módulo p se podrá utilizar la función `menor_raiz_primitiva(p)` del problema 4.7.

Problema 5.8. Encontrar TODAS las soluciones de la ecuación $x^2 \equiv -25 \pmod{5^3 \cdot 13^4 \cdot 17}$. Usar el teorema chino del resto para reducir el problema a módulos potencias de primo y el argumento de la demostración de la proposición 5.8 para, por ejemplo, producir una solución de $x^2 \equiv -25 \pmod{13^4}$ a partir de una de $x^2 \equiv -25 \pmod{13}$.