Ejercicio 2

David García Curbelo

Dado tu número $n = 45352609$ de la lista publicada:

Apartado I. ***Usa el algoritmo manual para calcular el símbolo de Jacobi*** $\left(\frac{p}{n}\right)$ ***para*** p ***cada uno de los 5 primeros primos.***

Calculamos el símbolo de Jacobi usando las propiedades conocidas:

- $\left(\frac{2}{n}\right)$. Como vemos que $45352609 = 5669076 \cdot 8 + 1$, entonces tenemos que $n \equiv 1 \bmod 8$, y por tanto $\left(\frac{2}{45352609}\right) = (-1)^{(45352609^2-1)/8} = 1$.

- $\left(\frac{3}{n}\right)$. Como vemos que $45352609 = 11338152 \cdot 4 + 1$, entonces tenemos que $\left(\frac{3}{45352609}\right) = \left(\frac{45352609}{3}\right)$. Ahora, viendo que $45352609 = 15117536 \cdot 3 + 1$, y así $45352609 \equiv 1 \bmod 3$, obtenemos $\left(\frac{45352609}{3}\right) = \left(\frac{1}{3}\right) = 1$.

- $\left(\frac{5}{n}\right)$. Por el mismo proceso anterior tenemos que $\left(\frac{5}{45352609}\right) = \left(\frac{45352609}{5}\right)$ por cumplirse que $45352609 = 11338152 \cdot 4 + 1$. Ahora, viendo que $45352609 = 9070521 \cdot 5 + 4$, y así $45352609 \equiv 4 \bmod 5$, con lo que tenemos $\left(\frac{45352609}{5}\right) = \left(\frac{4}{5}\right)$.
  Vemos que 4 es un residuo cuadrático módulo 5, ya que para $x = 2$ se tiene $x^2 \equiv 4 \pmod 5$, luego tenemos que $\left(\frac{4}{5}\right) = 1$.

- $\left(\frac{7}{n}\right)$. Por el mismo proceso anterior tenemos que $\left(\frac{7}{45352609}\right) = \left(\frac{45352609}{7}\right)$ por cumplirse que $45352609 = 11338152 \cdot 4 + 1$. Ahora, viendo que $45352609 = 6478944 \cdot 7 + 1$, y así $45352609 \equiv 1 \bmod 7$, con lo que tenemos $\left(\frac{45352609}{7}\right) = \left(\frac{1}{7}\right) = 1$.

- $\left(\frac{11}{n}\right)$. Por el mismo proceso anterior tenemos que $\left(\frac{11}{45352609}\right) = \left(\frac{45352609}{11}\right)$ por cumplirse que $45352609 = 11338152 \cdot 4 + 1$. Ahora, viendo que $45352609 = 4122964 \cdot 11 + 5$, y así $45352609 \equiv 5 \bmod 11$, con lo que tenemos $\left(\frac{45352609}{11}\right) = \left(\frac{5}{11}\right) = 1$.
  De nuevo, vemos que 5 es un residuo cuadrático módulo 11, ya que para $x = 4$ se tiene $x^2 = 16 \equiv 5 \pmod 1)1$, luego tenemos que $\left(\frac{5}{11}\right) = 1$.

Apartado II. ***Si para alguna de esas bases tu número sale posible primo de Fermat, comprueba si además es posible primo de Euler.*** Aplicamos el algoritmo de exponenciación rápida de izquierda a derecha para el cálculo de $a^{45352608} \pmod 4)5352609$, con a cada una de las bases:

	Iteración	Exponente	Acumulado
	0	1	1
	1	1	2
	2	2	4
	3	5	32
	4	10	1024
	5	21	2097152
	6	43	45211876
	7	86	32039765
	8	173	20054929
	9	346	42973822
	10	692	27919048
	11	1384	36563318
	12	2768	42979486
Base 2	13	5536	7197945
	14	11072	45227515
	15	22144	1858731
	16	44289	19763918
	17	88579	5588446
	18	177158	15085336
	19	354317	22777171
	20	708634	3728254
	21	1417269	12390911
	22	2834538	39121335
	23	5669076	3409899
	24	11338152	45352608
	25	22676304	1
	26	45352608	1
			$2^{45352608} \equiv 1 \pmod n$

	Iteración	Exponente	Acumulado
	0	1	1
	1	1	3
	2	2	9
	3	5	243
	4	10	59049
	5	21	29253133
	6	43	12007364
	7	86	29870534
	8	173	767839
	9	346	38165530
	10	692	22647345
	11	1384	10967526
	12	2768	33282599
Base 3	13	5536	43972016
	14	11072	2933206
	15	22144	35395482
	16	44289	21244663
	17	88579	32821326
	18	177158	7784461
	19	354317	15045949
	20	708634	40214907
	21	1417269	22577962
	22	2834538	45156046
	23	5669076	41942710
	24	11338152	45352608
	25	22676304	1
	26	45352608	1
			$3^{45352608} \equiv 1 \pmod{n}$

	Iteración	Exponente	Acumulado
	0	1	1
	1	1	5
	2	2	25
	3	5	3125
	4	10	9765625
	5	21	8587561
	6	43	22401770
	7	86	27169989
	8	173	16918953
	9	346	42206134
	10	692	11791361
	11	1384	16046682
	12	2768	34835928
Base 5	13	5536	33387032
	14	11072	21012559
	15	22144	31965521
	16	44289	35636762
	17	88579	3154889
	18	177158	14268136
	19	354317	32915580
	20	708634	36738832
	21	1417269	23477766
	22	2834538	196563
	23	5669076	41942710
	24	11338152	45352608
	25	22676304	1
	26	45352608	1
			$5^{45352608} \equiv 1 \pmod{n}$

	Iteración	Exponente	Acumulado
	0	1	1
	1	1	7
	2	2	49
	3	5	16807
	4	10	10359595
	5	21	43322858
	6	43	44022215
	7	86	17276402
	8	173	3564957
	9	346	28907433
	10	692	38249152
	11	1384	15340494
	12	2768	13740019
Base 7	13	5536	41156504
	14	11072	8426346
	15	22144	33255669
	16	44289	32506299
	17	88579	45071844
	18	177158	6150783
	19	354317	15956636
	20	708634	14191769
	21	1417269	22577962
	22	2834538	45156046
	23	5669076	41942710
	24	11338152	45352608
	25	22676304	1
	26	45352608	1
			$7^{45352608} \equiv 32441529 \pmod{n}$

	Iteración	Exponente	Acumulado
	0	1	1
	1	1	11
	2	2	121
	3	5	161051
	4	10	41084862
	5	21	33913782
	6	43	4241627
	7	86	19616829
	8	173	4695901
	9	346	4595994
	10	692	1795850
	11	1384	7843901
	12	2768	27597522
Base 11	13	5536	31785545
	14	11072	29259672
	15	22144	39742362
	16	44289	44905957
	17	88579	1408461
	18	177158	39270861
	19	354317	4207156
	20	708634	36073034
	21	1417269	45156046
	22	2834538	41942710
	23	5669076	45352608
	24	11338152	1
	25	22676304	1
	26	45352608	1
			$11^{45352608} \equiv 12846800 \pmod{n}$

Vemos que, por el algoritmo de la exponenciación rápida, n ha pasado el test de Fermat para las cinco bases propuestas. Veamos si dichas bases también pasan el test de Euler. Para poder decir que estamos ante un posible primo de Euler para la base a tiene que verificarse que

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}, \quad \text{con} \quad n = 45352609$$

- $\left(\frac{2}{45352609}\right) = 1 \equiv 2^{22676304} \pmod{45352609} \Rightarrow a = 2$ cumple el test de Euler.
- $\left(\frac{3}{45352609}\right) = 1 \equiv 3^{22676304} \pmod{45352609} \Rightarrow a = 3$ cumple el test de Euler.
- $\left(\frac{5}{45352609}\right) = 1 \equiv 5^{22676304} \pmod{45352609} \Rightarrow a = 5$ cumple el test de Euler.
- $\left(\frac{7}{45352609}\right) = 1 \equiv 7^{22676304} \pmod{45352609} \Rightarrow a = 7$ cumple el test de Euler.
- $\left(\frac{11}{45352609}\right) = 1 \equiv 11^{22676304} \pmod{45352609} \Rightarrow a = 11$ cumple el test de Euler.

Donde el valor de $a^{(n-1)/2} \pmod{n}$ lo hemos calculado con la penúltima iteración del algoritmo de exponenciación rápida para cada base. Con lo que tenemos que 45352609 es un posible primo de Euler para las bases 2, 3, 5, 7 y 11.

Apartado III. ***¿Es tu número*** n ***pseudoprimo de Fermat o de Euler para alguna de las bases?***

Como hemos visto en el apartado anterior, las bases 2, 3, 5, 7 y 11 pasan ambos test, luego podemos afirmar que n es un presudoprimo tanto de Euler como de Fermat para cada una de estas tres bases. Este hecho nos indica que existe una gran probabilidad de que nuestro número n sea efectivamente primo, y por tanto existe una baja probabilidad de que dicho número sea un pseudoprimo de Euler y de Fermat.