Ejercicio 8

David García Curbelo

Toma tu número $n = 191871308917122834687961459636870046909$ de la lista publicada para este ejercicio.

Apartado I. ***Pasa algunos test de primalidad para ver si*** n ***es compuesto***

Veamos los resultados de pasar el test de Fermat para las las bases 2, 3, 5 y 7. Usando el algoritmo de exponenciación rápida, tenemos los siguientes resultados de evaluar $a^{n-1} \pmod n$ para las bases mencionadas:

Base 2

Iteración	Exponente	Acumulado
1	1	2
2	2	4
3	4	16
4	9	512
5	18	262144
6	36	68719476736
7	72	4722366482869645213696
8	144	11857702018743425802170343386656388807 3
9	288	29340227568084248416501045335641728100
...	...	...
122	29979892018300442919993978068260944 82	10167525591833827542690707942640349361 5
123	59959784036600885839987956136521889 65	74303581080468529483843167643474362336
124	11991956807320177167997591227304377931	10064473068303945294464760924407585278 9
125	23983913614640354335995182454608755863	59117478806542687318662872566695394313
126	47967827229280708671990364909217511727	11823495761308537463732574513339078862 5
127	95935654458561417343980729818435023454	-1
128	191871308917122834687961459636870046908	1

Base 3

Iteración	Exponente	Acumulado
1	1	3
2	2	9
3	4	81
4	9	19683
5	18	387420489
6	36	150094635296999121
7	72	22528399544939174411840147874772641
8	144	79863541316174948313858493560647916069
9	288	21923773134371130434670971852591589643
...	...	...
122	29979892018300442919993978068260944 82	16472476541479262751489596301265840873 6
123	59959784036600885839987956136521889 65	50895079125131643876702492628639013989
124	11991956807320177167997591227304377931	84952660081805644914972406228688656 67
125	23983913614640354335995182454608755863	17584323598679078874152174566772149003 0
126	47967827229280708671990364909217511727	11823495761308537463732574513339078862 5
127	95935654458561417343980729818435023454	-1
128	191871308917122834687961459636870046908	1

Base 5

Iteración	Exponente	Acumulado
1	1	5
2	2	25
3	4	625
4	9	1953125
5	18	3814697265625
6	36	14551915228366851806640625
7	72	109995655051602194850629945210045793959
8	144	72055542060367415663075562708228631321
9	288	160592907386056251583845387348151877 5
...	...	...
122	299798920183004429199939780682609448 2	830730209547421751860512874821420231 67
123	599597840366008858399879561365218896 5	591653291148605893512106917068109814 74
124	119919568073201771679975912273043779 31	875098617273013162063721709827476145 37
125	239839136146403543359951824546087558 63	119817173846143518687612360340700291480
126	479678272292807086719903649092175117 27	1
127	959356544585614173439807298184350234 54	1
128	191871308917122834687961459636870046908	1

Base 7

Iteración	Exponente	Acumulado
1	1	7
2	2	49
3	4	2401
4	9	40353607
5	18	1628413597910449
6	36	2651730845859653471779023381601
7	72	938967536718240228976658800864417113 49
8	144	139184725522475144930465216926335590537
9	288	88353904871015366688933124559184247632
...	...	...
122	299798920183004429199939780682609448 2	143919716633746330712290624655863621828
123	599597840366008858399879561365218896 5	483700166072298365184984323196581445 00
124	119919568073201771679975912273043779 31	284805602230090310886275917255436837 21
125	239839136146403543359951824546087558 63	178621585979619985521227455109380454469
126	479678272292807086719903649092175117 27	-1
127	959356544585614173439807298184350234 54	1
128	191871308917122834687961459636870046908	1

Como hemos visto, para cada una de las bases se cumple que $a^{n-1} \equiv 1 \pmod{n}$, luego para $a = 2, 3, 5, 7$ tenemos que n es un posible primo de Fermat para dichas bases. Comprobemos ahora si nuestro número n pasa el test de Euler. Para ello, calculamos el símbolo de Jacobi $\left(\frac{a}{m}\right)$ para cada una de las bases y comprobamos que coincida con el valor de $a^{(m-1)/2} \pmod{m}$, que es precisamente la penúltima iteración del algoritmo realizado en el apartado anterior.

- $\left(\frac{2}{m}\right) = (-1)^{(n^2-1)/2} = -1$ por ser $n \equiv -3 \pmod{8}$.
- $\left(\frac{3}{m}\right) = \left(\frac{m}{3}\right) = \left(\frac{2}{3}\right) = -\left(\frac{1}{3}\right) = -1$.
- $\left(\frac{5}{m}\right) = \left(\frac{m}{5}\right) = \left(\frac{4}{5}\right) = -\left(\frac{2}{5}\right) = \left(\frac{1}{5}\right) = 1$.
- $\left(\frac{7}{m}\right) = \left(\frac{m}{7}\right) = \left(\frac{2}{7}\right) = -\left(\frac{1}{7}\right) = 1$.

Vemos que dichos símbolos coinciden con la penúltima iteración del algoritmo de exponenciación rápida, luego n ha pasado el test de Solovay-Strassen para las bases 2,3,5y 7, luego tenemos una probabilidad de primalidad del $1 - \frac{1}{2^4} = 0.984375$.

Apartado II. ***En caso que tu*** n ***sea probable primo, factoriza*** $n+1$ ***encontrando certificados de primalidad para factores mayores de 10000***

Por el apartado anterior, tenemos altas probabilidades de que nuestro numero n sea primo. Por ello procedemos a factorizar $n+1$.

$m = n+1 = 191871308917122834687961459636870046910 = 2{\cdot}3^2{\cdot}5{\cdot}213190343241247594097734955152077829 9$.

Desconocemos si $m_1 = 213190343241247594097734955152077829 9$ es primo, pero es fácil ver que $2^{m_1-1} \not\equiv 1 \pmod{m_1}$ por lo que m_1 no es primo. Así, aplicando ahora el método ρ de Polard, obtenemos

Paso	x	y	mcd
1	2	5	1
2	5	677	1
3	26	210066388901	1
4	677	189533458709428418461309110128077655 8	1
5	458330	782155851254848680939056590438895 60	1
6	210066388901	154470528302462732632312843054046940 0	1
7	44127887745906175987802	188611328701353025052930522634857981 0	1
	...	...	1
199	187071572632971721729406058393559176 0	106080135565114004839273254264286308 8	1
200	42406895867874067008501987906166659 8	198391725553609196458053623579235637	1
201	11443137110925453991336646419207269 69	108700088214067119094117667081239503 9	1
202	48724940942757694482104960457481371 6	138099718725281128011278513115129740 0	1
203	14289172329450328534470410720091950 27	55796305223565140626213192206618769 5	1
204	66266882512417044183736121448054867 2	45427139576895573208273871577600126 4	1
205	89615399998294199093371881969280399 4	18497239803970898000132597424979289 09	154493

Con lo que hemos obtenido un factor de $m_1 = 154493 \cdot 13799352931281520463563718430743$. Para ver si son posibles primos, aplicamos el test de Fermat con el que obtenemos que $m_2 = 154493$ pasa el test cumpliendo $a^{(m_2-1)} \equiv 1 \pmod{m_2}$ para las bases $a = 2, 3, 5, 7$, con lo que tenemos que es posible primo. Procedemos a buscar un certificado de primalidad mediante el algoritmo de Lucas-Lehmer, factorizando $m_2 - 1 = 154492 = 2^2 \cdot 38623$. Veamos si $m_{2,1} = 38623$ es primo. Para ello, aplicamos el test de Fermat y obtenemos que $2^{(m_2-1)} \not\equiv 1 \pmod{m_2}$, luego tenemos certificado de composición. Procedemos a obtener sus factores mediante el algoritmo ρ de Polard:

Paso	x	y	mcd
1	2	5	1
2	5	677	1
3	26	24562	1
4	677	33242	13

Tenemos así que $m_{2,1} = 38623 = 13 \cdot 2971$ (ambos factores son primos menores de 10000) luego tenemos completamente factorizado $m_2 - 1 = 154492 = 2^2 \cdot 13 \cdot 2971$ y por tanto estamos en condiciones de encontrar un elemento primitivo:

- $2^{(m_2-1)} \equiv 1 \pmod{m_2}$
- $2^{(m_2-1)/2} \not\equiv 1 \pmod{m_2}$
- $2^{(m_2-1)/13} \not\equiv 1 \pmod{m_2}$
- $2^{(m_2-1)/2971} \not\equiv 1 \pmod{m_2}$

Hemos obtenido un elemento primitivo, y por tanto un certificado de primalidad de 154493. Procedemos a estudiar la primalidad de $m_3 = 13799352931281520463563718430743$. Para ello, aplicamos el test de Fermat y obtenemos que $2^{(m_3-1)} \not\equiv 1 \pmod{m_3}$, luego tenemos un certificado de composición. Aplicamos por tanto el algoritmo ρ de Polard para encontrar sus factores, obteniendo una factorización de $m_3 = 5766560731 \cdot 2392995335520991752053$.

Veamos si cada uno de los factores es primo o no. Para ello, aplicamos el test de Fermat y obtenemos que para ambos candidatos $m_{3,1} = 5766560731$ y $m_{3,2} = 2392995335520991752053$, ambos pasan el test de Fermat $a^{(m_{3,i}-1)} \equiv 1 \pmod{m_{3,i}}$ para las bases $a = 2, 3, 5, 7$ y con $i = 1, 2$, con lo que tenemos que son posibles primos. Procedemos a buscar un certificado de primalidad mediante el algoritmo de Lucas-Lehmer. Factoricemos primero para este fin $m_{3,1} - 1 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 9153271$. Veamos si $m_{3,1,1} = 9153271$ es primo. Para ello, aplicamos el test de Fermat y obtenemos que $2^{(m_{3,1,1}-1)} \not\equiv 1 \pmod{m_{3,1,1}}$, luego tenemos un certificado de composición. Procedemos a obtener sus factores mediante el algoritmo ρ de Polard:

Paso	x	y	mcd
1	2	5	1
2	5	677	1
3	26	7972722	1
4	677	1349861	1
5	458330	4030875	1
6	7972722	9121035	1
7	592400	2030879	1
8	1349861	118386	1
9	1367894	3373269	1
10	4030875	2331996	127

Obtenemos una factorización de $m_{3,1,1} = 9153271 = 127 \cdot 72073$. Veamos si $m_{3,1,2} = 72073$ es primo o no. Vemos que dicho número pasa el test de Fermat para las bases $a = 2, 3, 5, 7$ y con $a^{(72073-1)} \equiv 1 \pmod{72073}$, con lo que tenemos que es posible primo. Procedemos a buscar un certificado de primalidad mediante el algoritmo de Lucas-Lehmer. Factoricemos por tanto $m_{3,1,2} - 1 = 2^3 \cdot 3^2 \cdot 1001 = 2^3 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13$. Ya tenemos factorizado completamente $m_{3,1,2} - 1$, luego estamos en condiciones de buscar un elemento primitivo:

- $5^{(m_{3,1,2}-1)} \equiv 1 \pmod{m_{3,1,2}}$
- $5^{(m_{3,1,2}-1)/2} \not\equiv 1 \pmod{m_{3,1,2}}$
- $5^{(m_{3,1,2}-1)/3} \not\equiv 1 \pmod{m_{3,1,2}}$
- $5^{(m_{3,1,2}-1)/7} \not\equiv 1 \pmod{m_{3,1,2}}$
- $5^{(m_{3,1,2}-1)/11} \not\equiv 1 \pmod{m_{3,1,2}}$
- $5^{(m_{3,1,2}-1)/13} \not\equiv 1 \pmod{m_{3,1,2}}$

Hemos obtenido un elemento primitivo, y por tanto un certificado de primalidad de $m_{3,1,2} = 72073$, y así un factorización completa de $m_{3,1} - 1 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 127 \cdot 72073$, y por tanto estamos en condiciones de encontrar un elemento primitivo para $m_{3,1} = 5766560731$:

- $2^{(m_{3,1}-1)} \equiv 1 \pmod{m_{3,1}}$
- $2^{(m_{3,1}-1)/2} \not\equiv 1 \pmod{m_{3,1}}$
- $2^{(m_{3,1}-1)/3} \not\equiv 1 \pmod{m_{3,1}}$
- $2^{(m_{3,1}-1)/5} \not\equiv 1 \pmod{m_{3,1}}$
- $2^{(m_{3,1}-1)/7} \not\equiv 1 \pmod{m_{3,1}}$
- $2^{(m_{3,1}-1)/127} \not\equiv 1 \pmod{m_{3,1}}$
- $2^{(m_{3,1}-1)/72073} \not\equiv 1 \pmod{m_{3,1}}$

Hemos obtenido un elemento primitivo, y por tanto un certificado de primalidad de $m_{3,1} = 5766560731$.

Nos falta por estudiar la primalidad de $m_{3,2} = 2392995335520991752053$. Para ello, encontremos una factorización completa de $m_{3,2} - 1 = 2^2 \cdot 598248833880247938013$ y falta ver si $m_{3,2,1} = 59824883380247938013$ es primo. Pero vemos que pasa el Test de Fermat para las bases $a = 2, 3, 5, 7$, con lo que tenemos que es posible primo. Procedemos a buscar un certificado de primalidad mediante el algoritmo de Lucas-Lehmer, factorizando $m_{3,2,1} - 1 = 2^2 \cdot 3 \cdot 49854069490020661501$. Vemos que, aplicando el test de Fermat, $2^{(m_{3,2,2}-1)} \not\equiv 1 \pmod{m_{3,2,2}}$, luego tenemos certificado de composición. Aplicando el algoritmo ρ de Polard:

Paso	x	y	mcd
1	2	5	1
2	5	677	1
3	26	210066388901	1
4	677	48154026845582945885	1
5	458330	16477550820312657009	1
6	210066388901	8767016751718741827	17

Obtenemos así un factor $m_{3,2,2} = 49854069490020661501 = 17 \cdot 2932592322942391853$. Repetimos el proceso, y vemos que aplicando el test de Fermat, $2^{(m_{3,2,3}-1)} \not\equiv 1 \pmod{m_{3,2,3}}$, con $m_{3,2,3}$, luego tenemos certificado de composición. Aplicando el algoritmo ρ de Polard:

Paso	x	y	mcd
1	2	5	1
2	5	677	1
3	26	210066388901	1
4	677	1232549678504676237	1
5	458330	1814589205600697744	1
6	210066388901	2901832105833958121	1
7	1171062592005775711	433343035452068346	1
8	1232549678504676237	530026126697573956	1
	...	...	1
105	1072907927239829481	633060779998309531	1
106	1473715790323534215	1476795736927761280	1
107	700874798274490282	1921604684212310878	1
108	1631026691484340616	2602941659810613916	1
109	2098486954844577194	106004085321239324	1
110	910283951658615124	2174617737679806385	1
111	2326822244406153002	1356215947241368806	1
112	2780900295665156451	2177037073141657912	8389

Obtenemos así otro factor $m_{3,2,1} - 1 = 2^2 \cdot 3 \cdot 17 \cdot 8389 \cdot 349575911663177$. Repetimos el proceso, y vemos que para $m_{3,2,3} = 349575911663177$ aplicando el test de Fermat, $2^{(m_{3,2,3}-1)} \not\equiv 1 \pmod{m_{3,2,3}}$, con $m_{3,2,3}$, luego tenemos certificado de composición. Aplicando el algoritmo ρ de Polard obtenemos:

Paso	x	y	mcd
1	2	5	1
2	5	677	1
3	26	210066388901	1
4	677	294589891977312	1
5	458330	290224068809114	1
6	210066388901	2463117925844	1
7	332863845795938	218480901392043	1
	...	...	1
2074	90963594969107	304227142127437	1
2075	48834153381626	159526109489353	1
2076	134463322576653	28163583826849	1
2077	245280188018629	284685468917185	1
2078	42109524707488	227174816698981	1
2079	338951848011268	261789712391706	1
2080	257496113186742	185895937987750	2291797

Obtenemos asi otro factor $m_{3,2,1} - 1 = 2^2 \cdot 3 \cdot 17 \cdot 8389 \cdot 2291797 \cdot 152533541$. Veamos si estos dos últimos factores son primos. Vemos que ambos pasan el test de Fermat para las bases $a = 2, 3, 5, 7$, con lo que tenemos altas probabilidades de primalidad. Aplicamos por tanto a ambos el test de Lucas-Lehmer, y buscamos una factorización de $m_{3,2,1,1} - 1 = 2291796 = 2^2 \cdot 3^2 \cdot 13 \cdot 59 \cdot 83$ y de $m_{3,2,1,2} - 1 = 152533540 = 2^2 \cdot 5 \cdot 67 \cdot 89 \cdot 1279$ (los tres últimos factores en ambos números han sido calculados mediante el algoritmo *rho* de Polard). Así, estamos en condiciones de buscar un elemento primitivo para cada uno de los candidatos a primo $m_{3,2,1,1} = 2291797$ y $m_{3,2,1,2} = 152533541$:

- $2^{(m_{3,2,1,1}-1)} \equiv 1 \pmod{m_{3,2,1,1}}$
- $2^{(m_{3,2,1,1}-1)/2} \not\equiv 1 \pmod{m_{3,2,1,1}}$
- $2^{(m_{3,2,1,1}-1)/3} \not\equiv 1 \pmod{m_{3,2,1,1}}$
- $2^{(m_{3,2,1,1}-1)/13} \not\equiv 1 \pmod{m_{3,2,1,1}}$
- $2^{(m_{3,2,1,1}-1)/59} \not\equiv 1 \pmod{m_{3,2,1,1}}$
- $2^{(m_{3,2,1,1}-1)/83} \not\equiv 1 \pmod{m_{3,2,1,1}}$

—

- $3^{(m_{3,2,1,2}-1)} \equiv 1 \pmod{m_{3,2,1,2}}$
- $3^{(m_{3,2,1,2}-1)/2} \not\equiv 1 \pmod{m_{3,2,1,2}}$
- $3^{(m_{3,2,1,2}-1)/5} \not\equiv 1 \pmod{m_{3,2,1,2}}$
- $3^{(m_{3,2,1,2}-1)/67} \not\equiv 1 \pmod{m_{3,2,1,2}}$
- $3^{(m_{3,2,1,2}-1)/89} \not\equiv 1 \pmod{m_{3,2,1,2}}$
- $3^{(m_{3,2,1,2}-1)/1279} \not\equiv 1 \pmod{m_{3,2,1,2}}$

Hemos encontrado un elemento primitivo para cada candidato a primo, luego tenemos certificado de primalidad de ambos. Ahora, tenemos factorizado en primos $m_{3,2,1} - 1 = 2^2 \cdot 3 \cdot 17 \cdot 8389 \cdot 2291797 \cdot 152533541$, y estamos en condiciones de encontrar un elemento primitivo para $m_{3,2,1} = 598248833880247938013$:

- $2^{(m_{3,2,1}-1)} \equiv 1 \pmod{m_{3,2,1}}$
- $2^{(m_{3,2,1}-1)/2} \not\equiv 1 \pmod{m_{3,2,1}}$
- $2^{(m_{3,2,1}-1)/3} \not\equiv 1 \pmod{m_{3,2,1}}$

- $2^{(m_{3,2,1}-1)/17} \not\equiv 1 \pmod{m_{3,2,1}}$
- $2^{(m_{3,2,1}-1)/8389} \not\equiv 1 \pmod{m_{3,2,1}}$
- $2^{(m_{3,2,1}-1)/2291797} \not\equiv 1 \pmod{m_{3,2,1}}$
- $2^{(m_{3,2,1}-1)/152533541} \not\equiv 1 \pmod{m_{3,2,1}}$

Hemos encontrado un elemento primitivo para $m_{3,2,1} = 598248833880247938013$, luego tenemos certificado de primalidad. Ahora tenemos factorizado en primos $m_{3,2}-1 = 2^2 \cdot 598248833880247938013$, y estamos en condiciones de encontrar un elemento primitivo para $m_{3,2} = 2392995335520991752053$:

- $2^{(m_{3,2,1}-1)} \equiv 1 \pmod{m_{3,2,1}}$
- $2^{(m_{3,2,1}-1)/2} \not\equiv 1 \pmod{m_{3,2,1}}$
- $2^{(m_{3,2,1}-1)/598248833880247938013} \not\equiv 1 \pmod{m_{3,2,1}}$

Hemos encontrado un elemento primitivo para $m_{3,2} = 2392995335520991752053$, luego tenemos certificado de primalidad.

Con esto ya hemos terminado, pues hemos encontrado una factorización en primos del número pedido $n + 1 = 2 \cdot 3^2 \cdot 5 \cdot 154493 \cdot 5766560731 \cdot 2392995335520991752053$

Apartado III. ***Con*** $P = 1$***, encuentra*** Q ***natural mayor o igual que 2, tal que definan una sucesión de Lucas que certifique la primalidad*** n***.***