

Ejercicio 7

David García Curbelo

Toma tu número $n = 4230659086792057869605292356791$ de la lista publicada para el ejercicio 3. Sea d el primer elemento de la sucesión $5, -7, 9, -11, 13, \dots$ que satisface que el símbolo de Jacobi es $(d|n) = -1$.

Apartado I. Con $P = 1$, $Q = (1 - d)/4$, define el e.c. α y sus sucesiones de Lucas asociadas.

Calculamos primero el valor de d mediante el símbolo de Jacobi:

- $\left(\frac{5}{n}\right) = 1$
- $\left(\frac{-7}{n}\right) = 1$
- $\left(\frac{9}{n}\right) = 1$
- $\left(\frac{-11}{n}\right) = 1$
- $\left(\frac{13}{n}\right) = -1$

Hemos encontrado el valor de $d = 13$ que nos interesa. Así podemos hayar la forma explícita de $P = 1$ y $Q = -3$. De la misma manera podemos hayar la forma explícita de $\Delta = P^2 - 4Q = 13$ y por tanto obtener $\alpha = \frac{P+\sqrt{\Delta}}{2} = \frac{1+\sqrt{13}}{2}$.

Las sucesiones de lucas asociadas son las siguientes:

- $V_n = P \cdot V_{n-1} - Q \cdot V_{n-2} = V_{n-1} + 3 \cdot V_{n-2}$
- $U_n = P \cdot U_{n-1} - Q \cdot U_{n-2} = U_{n-1} + 3 \cdot U_{n-2}$

Con $V_0 = 2$, $V_1 = P$, $U_0 = 0$, $U_1 = 1$.

Apartado II. Si n primo, ¿Qué debería pasarle a V_r , U_r , módulo n ? ¿Y a $V_{r/2}$, $U_{r/2}$? Calcula los términos V_r , U_r , $V_{r/2}$, $U_{r/2}$ módulo n , de las sucesiones de Lucas. ¿Tu n verifica el TPF para el entero cuadrático α ?

Si tomamos n suponiendo que es primo (y con $r = n + 1$), por la tercera versión del TPF para elementos cuadráticos tenemos que, como $\left(\frac{\Delta}{n}\right) = -1$ por definición, tienen que cumplirse las siguientes ecuaciones:

$$\begin{cases} U_{n-\left(\frac{\Delta}{n}\right)} \equiv 0 \pmod{n} & \Rightarrow U_{n+1} \equiv 0 \pmod{n} \\ V_{n-\left(\frac{\Delta}{n}\right)} \equiv 2Q \pmod{n} & \Rightarrow V_{n+1} \equiv -6 \pmod{n} \end{cases}$$

Ahora, para las consideraciones de los términos en la iteración $r/2$, consideremos las U-fórmulas binarias y la V-fórmula en función de U:

$$\begin{cases} U_{2k} = 2U_k U_{k+1} - P U_k^2 \\ U_{2k+1} = U_{k+1}^2 - Q U_k^2 \\ U_{2k+2} = P U_{k+1}^2 - 2Q U_k U_{k+1} \\ V_k = 2U_k U_{k+1} - P U_k \\ V_{2k} = V_k^2 - 2Q^k \end{cases}$$

Vemos que, por la primera y la penúltima fórmula, obtenemos $U_{2k} = V_k \cdot U_k$, y por la última tenemos $V_k^2 = V_{2k} + 2Q^k$. Por tanto obtenemos las siguientes expresiones para los términos de U y V en la iteración $r/2$:

$$\begin{cases} U_k = V_{k/2} \cdot U_{k/2} \\ V_{k/2} = \sqrt{V_k + 2Q^{k/2}} \end{cases}$$

A las que aplicando restricción módulo n obtenemos $V_{r/2} \cdot U_{r/2} = U_r \equiv 0 \pmod{n}$, con lo que tenemos que $U_{r/2} \equiv 0 \pmod{n}$ y por las fórmulas vistas $V_n \equiv -6 \pmod{n}$. Estas deducciones se pueden comprobar en la tabla de iteraciones de la página siguiente.

Ahora calculamos $Q^{r/2}$, para el que usamos el algoritmo de la exponenciación rápida, donde $r/2 = 2115329543396028934802646178396$ (par), luego $(-3)^{\frac{r}{2}} = 3^{\frac{r}{2}} \equiv -3 \pmod{n}$. Además, por el punto anterior tenemos que $V_{n+1} \equiv -6 \pmod{n}$, luego tenemos $V_{r/2}^2 = V_r + 2Q^{r/2} \equiv -12 \pmod{n}$. Calculemos a continuación las iteraciones:

Paso	k	U_k	U_{k+1}
0	0	0	1
1	1	1	1
2	3	4	7
3	6	40	97
4	13	14209	32689
5	26	727060321	1674257764
6	53	4388989191432148819	10106857384297773160
7	106	1206025542555073975697218196332	1191951767210935168446627691804
8	213	2224571724374272540640955371025	278173333404799351094718353632
9	427	2724188379238101395143688701111	1040521496327043120557508055156
10	854	2240881567061812458486435864069	1121493515710978151287472213176
11	1708	2440177787821014965176523715987	281007983241315548690694467405
12	3417	693288824173917621822948187874	2371328698565907497147549144516
13	6834	3721998043825565111678776090720	2014292397858539868209996806393
14	13669	4205898394184130603133532495000	1211143114040918590331860328115
15	27339	384898754315453633874589689569	1982624428813654223520306030647
16	54679	2205114962351087054439123449795	3559492677168281359056314219403
17	109359	3056059869227629036204333889051	1423758336170861758017330367997
18	218719	3551423950121026880918215709294	3414073489724804099292817100277
19	437439	3460551003854904659688814626658	475591476867243768628155700978
20	874879	2460043190695490427945140061060	2247495142981071956725741493150
21	1749759	2166255830514324913128887404298	4112602938964843042151172594379
22	3499519	2608440951992315234653712945429	3239909279342061175967085769138
23	6999038	269920817574771798201888907821	1417378943408722380969677701581
24	13998076	1213435973533037509031355988281	3783608230937959308889385710867
25	27996153	652278378486732728206101158747	2826843898299710299380047780622
26	55992306	3884562517666216068130783262597	3181755662028242029634237058095
27	111984613	3247049328585303344489979652255	2695375132371359511468626840344
28	223969227	29779707979250577247359439087	2586696179189130169385172256763
29	447938454	2260479589319694550571971648344	28365850218704328636875632404
30	895876908	40965214621645240277380001145	453880624606167197749719810379
31	1791753817	510819107833845020980074302432	313598674112025178633287820140
32	3583507635	1541920834587226435934920973919	1281380269421394231209489702707
33	7167015270	953453786545491725568830749410	3264083616320700894968456708711
34	14334030540	2660475695792792413183733918485	682256232166213429514763646156
35	28668061080	2471751791161736882019886980384	657663229152715303675902651250
36	57336122161	4012606612333337626035394734648	2804823955982230319886947406902
37	114672244323	3105722382171480468348775381447	477563165797380354088428308632
38	229344488647	4067941019089584055244924617185	4212353841700088430611524932730
39	458688977294	3040575168173013589130366088093	3722956195285441553305565547109
40	917377954589	1678208648515403299696839198453	3705092999866615500274862218983
41	1834755909178	532263425061440016849618227413	357757549070238141197751942066
42	3669511818356	1628458654609289219083491675866	3267737650201680812221557869110
43	7339023636712	2401816628687239060277716038834	3880298180626118226409911223667
44	14678047273425	1356673018331891593458139273057	2890292439746692251495466896840
45	29356094546851	3998808044076379473204086068653	2927942947280424678606715894070
46	58712189093702	1002995773310192130560537046201	4075679818759325537695888936151
47	117424378187404	3638296379551707851196335475685	1977034590424034024427090686680
48	234848756374809	1199172975890223611843058638724	1520658918620734497202404032804
49	469697512749618	437752049599915428470389844843	1605082210629355310149354100408
50	939395025499236	2553932259872298234573825312571	3927868577358750705243248501250
51	1878790050998472	1782309769519364898725360825272	2526853358658154087876176798152
52	3757580101996944	3239951839968474674572277570082	1754660279628164450379321810440

Paso	k	U_k	U_{k+1}
53	7515160203993889	772554330115870989869155980205	2299312592280735131326723596533
54	15030320407987779	1161295187543971288033287164083	1980381983326016764815674111422
55	30060640815975559	3869095159199140697744395973369	1667415590678572485023488327910
56	60121281631951118	3689095507650274731217247011582	3006237437411835621207200203718
57	120242563263902237	361371593030257294943867729495	3698797394640497577013424035459
58	240485126527804474	4037023125584983642564393915119	283742619493790585931991704006
59	480970253055608949	609726694192642884902662201458	2010407164979210736305851260234
60	961940506111217898	2203795371142190303566191728217	767987694610083807997840429856
61	1923881012222435797	3092675007235659356534321074322	3459268692299825351158941463634
62	3847762024444871594	2102850815934169344305467567332	271108870520556852497276813415
63	7695524048889743188	911953416852421858603161607959	4179963076450375966867425305261
64	15391048097779486377	1186362651443553662947808482586	4045243062085195470686897804606
65	30782096195558972755	1069320115282748880522813385373	2465277257460566664141659917084
66	61564192391117945511	927177355366383141186254893116	1711223740035001107425162723873
67	123128384782235891022	2192899861152931969015541459362	2854255104631445313318084459842
68	246256769564471782045	729713940011399371026437205705	392083858637607540459658697976
69	492513539128943564091	2411782393514892043961867952206	1919593387624166151594118056998
70	985027078257887128182	2332145702477533882514640306496	1457480691950369735595535602847
71	1970054156515774256365	2979423589421281372928146645197	1710506592252300092854460323805
72	3940108313031548512731	863267501283303413041490436075	3598828613629915647475681835696
73	7880216626063097025463	428774538957186445089724910224	513882096213460020801917472892
74	15760433252126194050927	168200342518927822986564014638	264343055694671161506105581018
75	31520866504252388101855	3816996798390858806323434841261	3891147952995237099943079093383
76	63041733008504776203711	3785995490462982519501620025023	2448051585276976970554927717262
77	126083466017009552407422	2423988303408911371130583584366	1312066627441283175409769905070
78	252166932034019104814844	3944321132320519918692454869933	1479210302600363549365247348428
79	504333864068038209629689	2963024971525598142917209195324	1116768296098713161305969608172
80	1008667728136076419259379	4068903995066038179053611236566	3444752725337014154232687372550
81	2017335456272152838518758	1093531928391249018908754849400	1637639258829466856318313442665
82	4034670912544305677037517	4105475795626561399926924789347	2517746173429219115190407524569
83	8069341825088611354075035	3847141978989485121457722752996	4170357766961425894394556266816
84	16138683650177222708150071	2332334721165214836150765834138	2389478295031326272496489651079
85	32277367300354445416300143	2909550926215054970891480103336	470634721964005296753726917670
86	64554734600708890832600286	1687568250026306721350886995287	3680073732370416625026882542317
87	129109469201417781665200572	2088989998632477130755198486997	3458947781078041312110245245284
88	258218938402835563330401144	1592301268199309764611279620628	458204221306629199977148706924
89	516437876805671126660802289	392487535493950293919665024324	690660759799319557733225888240
90	1032875753611342253321604579	4071085333986147953587036809430	2352859312039741540036118108373
91	2065751507222684506643209158	3236598351193375409154738398645	493555714260808026523843813575
92	4131503014445369013286418317	1014013834014097741992720133965	1803871217829794019117781551089
93	8263006028890738026572836634	753760903567690576383788648926	4108274966803903777477949208925
94	16526012057781476053145673268	2248132779990784688478570879807	837827279477629125322250435241
95	33052024115562952106291346537	2661377540275603880511653852102	3115999644169315640252873472965
96	66104048231125904212582693074	1980109465271165993915830502869	322566446727654064099010975109
97	132208096462251808425165386149	2414153180482019947665784051432	114794499843013069910537632557
98	264416192924503616850330772299	249567450660551621575252091327	1933555353481002084684640856244
99	528832385849007233700661544599	762432504487272216321147199828	381216252243636108160573599914
100	1057664771698014467401323089198	0	400308804229400273828849410268
101	2115329543396028934802646178396	0	1385230094848320756564637585261
102	4230659086792057869605292356792	0	4230659086792057869605292356788

Vemos que tenemos en las dos últimas iteraciones los valores de $U_r = U_{r/2} = 0$, además de tener $U_{r+1} = 4230659086792057869605292356788$ y $U_{r/2+1} = 1385230094848320756564637585261$.

Por tanto, como $V_k = 2U_{k+1} - PU_k$ tenemos que $V_r = 8461318173584115739210584713576 \equiv -6$ y $V_{r/2} = 2770460189696641513129275170522$, lo cual cumple con la condición vista antes $V_{r/2}^2 \equiv -12 \pmod{n}$.

Como $V_r \equiv -6 \equiv 2Q \pmod{n}$ y $U_r \equiv 0 \pmod{n}$, tenemos que nuestro número n cumple la tercera versión del TPF para el elemento cuadrático $\alpha = \frac{1+\sqrt{13}}{2}$.

Apartado III. Factoriza $r = n + 1$ y para cada factor primo p suyo, calcula $U_{r/p}$. ¿Cuál es el rango de Lucas $w(n)$? ¿Qué deduces sobre la primalidad de tu n ?

Factorizamos $r = n + 1 = 4230659086792057869605292356792 = 2^3 \cdot 528832385849007233700661544599$. Desconocemos si $m_1 = 528832385849007233700661544599$ es primo o no. Para saberlo aplicamos el test de composición de Fermat y obtenemos que $2^{m_1-1} \not\equiv 1 \pmod{m_1}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Ahora factorizando mediante el algoritmo ρ de Polard, obtenemos un divisor 4349 en 46 iteraciones, quedando por tanto $528832385849007233700661544599 = 4349 \cdot 121598617118649628351497251$.

Veamos a continuación si $m_2 = 121598617118649628351497251$ es primo o no. Para saberlo aplicamos el test de composición de Fermat y obtenemos que $2^{m_2-1} \not\equiv 1 \pmod{m_2}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Ahora factorizando mediante el algoritmo ρ de Polard, obtenemos un divisor 62347 en 46 iteraciones, quedando por tanto $121598617118649628351497251 = 62347 \cdot 1950352336417945183433$.

Repetimos el mismo proceso para $m_3 = 1950352336417945183433$. Aplicando el test de composición de Fermat, obtenemos que $2^{m_3-1} \not\equiv 1 \pmod{m_3}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Ahora factorizando mediante el algoritmo ρ de Polard, obtenemos un divisor 1924630699 en 26395 iteraciones, quedando por tanto $1950352336417945183433 = 1924630699 \cdot 1013364453467$.

Veamos por último si $m_4 = 1013364453467$ es primo o no. se puede ver que dicho número pasa el test de Solovay-Strassen para las bases 2, 3, 5, 7 y 11, por lo que tenemos altas probabilidades de que dicho número sea primo. Busquemos ahora un elemento primitivo de m_4 . Para ello factorizamos primero el número $m_4 - 1 = 1013364453466 = 2 \cdot 506682226733$.

Veamos si $m_{4,1} = 506682226733$ es primo o no. Aplicamos de nuevo el test de composición de Fermat y obtenemos que $2^{m_{4,1}-1} \not\equiv 1 \pmod{m_{4,1}}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Busquemos ahora sus factores primos mediante el algoritmo ρ de Polard, con el que obtenemos un divisor 73 en solo 6 iteraciones, quedando por tanto $506682226733 = 73 \cdot 6940852421$.

Tomando ahora $m_{4,2} = 6940852421$ veamos si es primo. Vemos que pasa el test de Solovay-Strassen para las bases 2, 3, 5, 7 y 11, por lo que tenemos altas probabilidades de que dicho número sea primo. Busquemos ahora un elemento primitivo de $m_{4,2}$. Para ello factorizamos primero el número $m_{4,2} - 1 = 6940852420 = 2^2 \cdot 5 \cdot 347042621$.

Veamos si $m_{4,2,1} = 347042621$ es primo o no. Vemos que pasa el test de Solovay-Strassen para las bases 2, 3, 5, 7 y 11, por lo que tenemos altas probabilidades de que dicho número sea primo. Aplicamos de nuevo el algoritmo de Lucas-Lehmer para ver si $m_{4,2,1}$ es primo o no. Para ello factorizamos $m_{4,2,1} - 1 = 2^2 \cdot 5 \cdot 17352131$, y veamos si $m_{4,2,1,1} = 17352131$ es primo o no.

Vemos que pasa el test de Solovay-Strassen para las bases 2, 3, 5, 7 y 11, por lo que tenemos altas probabilidades de que dicho número sea primo. Aplicamos de nuevo el algoritmo de Lucas-Lehmer para ver si $m_{4,2,1,1}$ es primo o no. Para ello factorizamos $m_{4,2,1,1} - 1 = 2 \cdot 5 \cdot 1735213$, y veamos si $m_{4,2,1,1,1} = 1735213$ es primo o no.

Aplicando el test de composición de Fermat, obtenemos que $2^{m_{4,2,1,1,1}-1} \not\equiv 1 \pmod{m_{4,2,1,1,1}}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Aplicamos el algoritmo ρ de Polard para obtener un divisor 19 en solo 4 iteraciones, quedando por tanto $1735213 = 19 \cdot 91327$.

Veamos de nuevo si $m_{4,2,1,1,2} = 91327$ es primo o no. Aplicando el test de composición de Fermat, obtenemos que $2^{m_{4,2,1,1,2}-1} \not\equiv 1 \pmod{m_{4,2,1,1,2}}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Aplicamos el algoritmo ρ de Polard para obtener un divisor 271 en solo 9 iteraciones, quedando por tanto $91327 = 271 \cdot 337$, quedando así completamente descompuesto.

Tenemos por tanto $m_{4,2,1,1} - 1 = 2 \cdot 5 \cdot 5 \cdot 19 \cdot 271 \cdot 337$, por lo que estamos preparados para buscar un elemento primitivo de $m_{4,2,1,1} = 17352131$.

- $2^{m_{4,2,1,1}-1} \equiv 1 \pmod{m_{4,2,1,1}}$
- $2^{(m_{4,2,1,1}-1)/2} \not\equiv 1 \pmod{m_{4,2,1,1}}$

- $2^{(m_{4,2,1,1}-1)/5} \not\equiv 1 \pmod{m_{4,2,1,1}}$
- $2^{(m_{4,2,1,1}-1)/19} \not\equiv 1 \pmod{m_{4,2,1,1}}$
- $2^{(m_{4,2,1,1}-1)/271} \not\equiv 1 \pmod{m_{4,2,1,1}}$
- $2^{(m_{4,2,1,1}-1)/337} \not\equiv 1 \pmod{m_{4,2,1,1}}$

Y así hemos obtenido un elemento primitivo, luego podemos afirmar que $m_{4,2,1,1} = 17352131$ es primo.

Con este resultado obtenemos la factorización en primos de $m_{4,2,1} - 1 = 2^2 \cdot 5 \cdot 17352131$, por lo que estamos preparados para buscar un elemento primitivo de $m_{4,2,1} = 347042621$.

- $3^{m_{4,2,1}-1} \equiv 1 \pmod{m_{4,2,1}}$
- $3^{(m_{4,2,1}-1)/2} \not\equiv 1 \pmod{m_{4,2,1}}$
- $3^{(m_{4,2,1}-1)/5} \not\equiv 1 \pmod{m_{4,2,1}}$
- $3^{(m_{4,2,1}-1)/17352131} \not\equiv 1 \pmod{m_{4,2,1}}$

Y así hemos obtenido un elemento primitivo, luego podemos afirmar que $m_{4,2,1} = 347042621$ es primo.

Con este resultado obtenemos la factorización en primos de $m_{4,2} - 1 = 2^2 \cdot 5 \cdot 347042621$, por lo que estamos preparados para buscar un elemento primitivo de $m_{4,2} = 6940852421$.

- $3^{m_{4,2}-1} \equiv 1 \pmod{m_{4,2}}$
- $3^{(m_{4,2}-1)/2} \not\equiv 1 \pmod{m_{4,2}}$
- $3^{(m_{4,2}-1)/5} \not\equiv 1 \pmod{m_{4,2}}$
- $3^{(m_{4,2}-1)/347042621} \not\equiv 1 \pmod{m_{4,2}}$

Y así hemos obtenido un elemento primitivo, luego podemos afirmar que $m_{4,2} = 6940852421$ es primo.

Con este resultado obtenemos la factorización en primos de $m_4 - 1 = 2 \cdot 73 \cdot 6940852421$, por lo que estamos preparados para buscar un elemento primitivo de $m_4 = 1013364453467$.

- $2^{m_4-1} \equiv 1 \pmod{m_4}$
- $2^{(m_4-1)/2} \not\equiv 1 \pmod{m_4}$
- $2^{(m_4-1)/73} \not\equiv 1 \pmod{m_4}$
- $2^{(m_4-1)/6940852421} \not\equiv 1 \pmod{m_4}$

Y así hemos obtenido un elemento primitivo, luego podemos afirmar que $m_4 = 1013364453467$ es primo. Con ello hemos obtenido finalmente una factorización total del número $r = n + 1$ en factores primos, que son los siguientes:

$$p_1 = 2^3$$

$$p_2 = 4349$$

$$p_3 = 62347$$

$$p_4 = 1924630699$$

$$p_5 = 1013364453467$$

Calculemos a continuación $U_{r/p}$ para cada p en la lista anterior:

$$- U_{r/8} = U_{528832385849007233700661544599} = 762432504487272216321147199828$$

$$- U_{r/4349} = U_{972788936949197026811978008}$$

$$- U_{r/62347} = U_{67856658488653148822000936}$$

$$- U_{r/1924630699} = U_{2198166686726042848808}$$

$$- U_{r/1013364453467} = U_{4174864307029719976}$$