Ejercicio 7

Ana Buendía Ruiz-Azuaga

March 21, 2022

1 Ejercicio 7

1.1 Apartado 1

Toma tu número n de la lista publicada para el ejercicio 3. Sea d elprimer elemento de la sucesión 5, -7, 9, -11, 13, ... que satisface que el símbolo deJacobi es (d—n) = -1

$n = 365805459457767185586330009602 11$

Con el n dado, el primer número de la sucesión que cumple $\left(\frac{d}{n}\right) = -1$ es $d = -7$.

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

Se obtiene $Q = 2$.

Sabemos que $\alpha = \frac{P+\sqrt{P^2-4Q}}{2}$, luego tenemos que $\alpha = \frac{1+\sqrt{-7}}{2}$

Además, sabemos que α es un entero cuadrático por ser solución de $x^2 - x + 2 = 0 \in \mathbb{Z}[x]$.

Entonces, se tiene $\alpha^n = \alpha^{n-1} - 2\alpha^{n-2}$.

Por tanto si llamamos $\alpha^i = \frac{V_i}{2} + \frac{U_i}{2}\sqrt{-7}$ se tiene

$$U_0 = 0, \quad V_0 = 2$$

$$U_1 = 1, \quad V_1 = 1$$

La sucesión de Lucas asociada es:

$$V_n = V_{n-1} - 2V_{n-2}$$
$$U_n = U_{n-1} - 2U_{n-2}$$

con los U_0, V_0, U_1, V_1 ya mencionados.

1.2 Apartado 2

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

Si n fuera primo por la tercera versión del TPF para e.c. se tiene que, con $\Delta = P^2 - 4Q = -7$:

$$U_r = U_{n-\frac{\Delta}{n}} = U_{n+1} \equiv 0 \mod n$$

$$V_r = V_{n-\frac{\Delta}{n}} = V_{n+1} \equiv 2Q \mod n \equiv 4 \mod n$$

Donde hemos usado que $\left(\frac{\Delta}{P}\right) = -1$
Además, conocemos las propiedades:

$$U_{2k} = U_k V_k$$
$$V_{2k} = V_k^2 - 2Q^k$$

Sabemos que $r = n + 1$, y, con $k = \frac{r}{2}$:

$$U_r = U_{\frac{r}{2}} V_{\frac{r}{2}}$$
$$V_r = V_{\frac{r}{2}}^2 - 2Q^{\frac{r}{2}}$$

$$U_r = U_{\frac{r}{2}} V_{\frac{r}{2}} = 0 \mod n$$

Luego $U_{\frac{r}{2}}$ o $V_{\frac{r}{2}}$ son 0 o múltiplos de n.
Por otro lado,

$$V_{\frac{r}{2}}^2 = 4 + 2(2)^{\frac{r}{2}} = 365805459457767185586330009602 11 \mod n \equiv 0 \mod n$$

.

Ejecutamos ahora el algoritmo de izquierda a derecha:

```
U[0] = 0,
V[0] = 2,

U[1] = 1

U[1] = 1,
V[1] = 1,

U[2] = 1

U[3] = 365805459457767185586330009602 10,
V[3] = 365805459457767185586330009602 06,

U[4] = 365805459457767185586330009602 08

U[7] = 7,
V[7] = 365805459457767185586330009601 98,

U[8] = 365805459457767185586330009602 08

U[14] = 3658054594577671855863300096012 0,
V[14] = 3658054594577671855863300096012 4,

U[15] = 365805459457767185586330009601 22

U[28] = 7917,
```

```
V[28] = 365805459457767185586330009350l2,

U[29] = 3658054594577671855863300095l570

U[57] = 365805459457767185586329502693l4,
V[57] = 747311035,

U[58] = 348310069

U[115] = 116180770089455543,
V[115] = 267708236898049123,

U[116] = 191944503493752333

U[230] = 90850681955335304142791224594l9,
V[230] = 40807015870840596516383531334l5,

U[231] = 65828848913087950330587377964l2

U[461] = 59590306772111708766018152886l3,
V[461] = 12231053807303017165974138820499,

U[462] = 90950422422570940212879770545l6

U[923] = 42466590386198485514954425167l2,
V[923] = 27786632601091692388221416170843,

U[924] = 34306918792744129749174929823893

U[1846] = 81731238205561347584911554224l5,
V[1846] = 12352535795618830125523066526592,

U[1847] = 28553102780975841721323611454604

U[3693] = 79191973141130733242102366194l0,
V[3693] = 14285716598531391991050223434270,

U[3694] = 11102456956322232657630230026840

U[7387] = 10982886971100342384805902921280,
V[7387] = 30164768721199210354930977838564,

U[7388] = 20573827846149776369868440379922

U[14774] = 190770526610675218619922454230l4,
V[14774] = 77393090168672108692443250960l8,

U[14775] = 13408180838967366365618285259516

U[29549] = 13701327719872692389595973728l8,
```

```
V[29549] = 216177833618018163783174671077 28,

U[29550] = 1149395806689454280863853224028 3

U[59099] = 2404837446542145175095670531152 1,
V[59099] = 2777952695823406784903818930052,

U[59100] = 3170343655351078854724676260089 2

U[118198] = 2565354886269500183644640212582 6,
V[118198] = 2196035225911105892550356727095 2,

U[118199] = 2380695056090303038097498469838 9

U[236396] = 2586871101285728763958856379099 9,
V[236396] = 9227203513281161451013147841514,

U[236397] = 3583823023595758382461735629636 2

U[472792] = 3108972618646679874530780289654 9,
V[472792] = 2405388029934824238843674690572 8,

U[472793] = 9281530270019161287555774421033

U[945584] = 2004723112128104714862461910724 0,
V[945584] = 2419788489536934201136584524483 7,

U[945585] = 3832285035436835300678731695933

U[1891169] = 9721298095328574424657191178940,
V[1891169] = 2210894719177929542036475513547 2,

U[1891170] = 1591512264355393492251097315720 6

U[3782339] = 1638815836156348515888791384477 5,
V[3782339] = 6694554768283832446697967339453,

U[3782340] = 1154135656492365880279294059211 4

U[7564679] = 1022290997266884078826503339046 8,
V[7564679] = 3094859035347458526517229423802 0,

U[7564680] = 2058575016307171302671866381424 4

U[15129359] = 2002434091529315778487659444644 1,
V[15129359] = 4296877534000671248078579024626,

U[15129360] = 3045088219753527379579408721563 9

U[30258718] = 6592951170564225160629971154089,
```

V[30258718] = 116018156515339285191286220946 44,

U[30258719] = 27387656383937436119195797104472

U[60517436] = 252896812439064820658588318079 07,
V[60517436] = 761233029127677442699323768356 2,

U[60517437] = 34741278740479987525742535225840

U[121034873] = 188811087605791690002232787098557,
V[121034873] = 326611033566805185543349231989 99,

U[121034874] = 257711060586298437782838551487 78

U[242069747] = 127452873674362485231574125057 94,
V[242069747] = 248626049226364955879117184550 94,

U[242069748] = 188039461450363720555345654804 44

U[484139494] = 174504455830988534306858208124 66,
V[484139494] = 204734633031870822671288446790 84,

U[484139495] = 189619544431429678489073327457 75

U[968278988] = 855271095195924911724761877267 7,
V[968278988] = 262720510630758327795976425288 11,

U[968278989] = 174123810075175409484226306507 44

U[1936557977] = 221951913751605201910263794825 15,
V[1936557977] = 314614571257443061695254473957 69,

U[1936557978] = 268283242504524131802759134391 42

U[3873115955] = 236318183726649737677610578809 92,
V[3873115955] = 111908423801093734722203164498 32,

U[3873115956] = 174113303763871736199906871654 12

U[7746231911] = 164317643529958844166579006528 90,
V[7746231911] = 238940853710504300187069970990 69,

U[7746231912] = 187265188913479793836594839587 4

U[15492463822] = 777072891946613349885133172523 9,
V[15492463822] = 351109075438103429278310337656 01,

U[15492463823] = 214408182316382382133411827454 20

U[30984927644] = 771730304858603114180135619421 0,

V[30984927644] = 19747466944501492022272329689906,

U[30984927645] = 13732384996543761582036842942058

U[61969855289] = 23226596018781160733148755127132,
V[61969855289] = 33206872152099842124802366102780,

U[61969855290] = 28216734085440501428975560614956

U[123939710578] = 16531993914075891860963696789412,
V[123939710578] = 73541742683820857405269980571 31,

U[123939710579] = 30233357064117348080061847903377

U[247879421156] = 11988186457310105394046705468379,
V[247879421156] = 19021291791227905305583161308743,

U[247879421157] = 15504739124269005349814933388561

U[495758842313] = 97915181489443263946857762741 16,
V[495758842313] = 30802848035715725766700011500375,

U[495758842314] = 20069101194416668013763934071 40

U[991517684627] = 21937133614828258006050719604289,
V[991517684627] = 22748210480664006594865551454239,

U[991517684628] = 22342672047746132300458135529264

U[1983035369255] = 17736822915452402333915214463 61,
V[1983035369255] = 23890591674837766380069049650297,

U[1983035369256] = 12832136983191503306730285548329

U[3966070738511] = 76949851325730222604274773661 16,
V[3966070738511] = 11824209240499636727866922836413,

U[3966070738512] = 28049870159424688773463700581370

U[7932141477023] = 28730128720516905608301764638 17,
V[7932141477023] = 13652659377202275319783476791744,

U[7932141477024] = 26553109097515342219623327107886

U[15864282954046] = 21285295453197055567853040400340,
V[15864282954046] = 26913288961604931546571802310517,

U[15864282954047] = 58090192345126342778959208753 23

U[31728565908093] = 24416824114566897146532481368205,

V[31728565908093] = 886329241136428929019217324 7450,

U[31728565908094] = 3493033123585395249767882778 7933

U[63457131816187] = 22953061014138503044930897 0488,
V[63457131816187] = 20286384525474486104694004162021,

U[63457131816188] = 28548230540696294846888157046360

U[126914263632374] = 32737996196818838505247660364388,
V[126914263632374] = 10595483210902351358852158648109,

U[126914263632375] = 33764667309722356527334090261 43

U[253828527264748] = 82862746196617074683675010039 27,
V[253828527264748] = 50863552305782509237075924770 08,

U[253828527264749] = 24976587898008338475354047220573

U[507657054529496] = 25738838679797375221023016523685,
V[507657054529496] = 11806394911771929933891880074248,

U[507657054529497] = 48234382289629329814094781 8861

U[1015314109058993] = 33446799251198849367647652716312,
V[1015314109058993] = 16861844443849831440743125533185,

U[1015314109058994] = 68640488746359811248788886446 43

U[2030628218117986] = 33626319954107714874666904612033,
V[2030628218117986] = 14736437214736312690260084805649,

U[2030628218117987] = 24181378584422013782463494708841

U[4061256436235973] = 32376687889654620220598842201905,
V[4061256436235973] = 36330221802871876404306275242735,

U[4061256436235974] = 34353454846263248312452558722320

U[8122512872471947] = 15650994177911112919131420765919,
V[8122512872471947] = 10964841881076440504675670289631,

U[8122512872471948] = 13307918029493776711903545527775

U[16245025744943894] = 13045740435300569984175702236464,
V[16245025744943894] = 19665882829286586391139839332174,

U[16245025744943895] = 16355811632293578187657770784319

U[32490051489887788] = 23960458977626277189854283387981,

V[32490051489887788] = 16770836716484611503816962649 16,

U[32490051489887789] = 31109044297525728449434490306554

U[64980102979775577] = 16901277822271343130863945551781,
V[64980102979775577] = 15034313084912830781946001811177,

U[64980102979775578] = 15967795453592086956404973681479

U[129960205959551155] = 21011011855160925321282876190 27,
V[129960205959551155] = 21999882250760553104634696008552,

U[129960205959551156] = 30340764691026682097697992293895

U[259920411919102310] = 19868643333235804420510559063 58,
V[259920411919102310] = 22945572296326997316142874774341,

U[259920411919102311] = 30756491287713648158413465820455

U[519840823838204621] = 32701819624917698879066349820063,
V[519840823838204621] = 31015237563386946207452145186811,

U[519840823838204622] = 31858528594152322543259247503437

U[1039681647676409243] = 30540275747793909692440109260445,
V[1039681647676409243] = 20191423753006540397766166955889,

U[1039681647676409244] = 25365849750400225045103138108167

U[2079363295352818486] = 27185753211378390706740951370619,
V[2079363295352818486] = 15274328027812816075947897751050,

U[2079363295352818487] = 29397676467072441120279240807 29

U[4158726590705636972] = 57911402194860698039687089065 33,
V[4158726590705636972] = 30090812932743604908291862928863,

U[4158726590705636973] = 17940976576114837356130285917698

U[8317453181411273944] = 31620327021723876189389557300783,
V[8317453181411273944] = 42957724773477748404420957604 81,

U[8317453181411273945] = 17958049749535825514915826530632

U[16634906362822547889] = 32535165002877097607696012869929,
V[16634906362822547889] = 81861027785758733908314065022 14,

U[16634906362822547890] = 20703609178381262199472092059 66

U[33269812725645095778] = 24527936984693532167038459144142,

V[33269812725645095778] = 219445292115721272582193071538 30,

U[33269812725645095779] = 232362330981328297126288831489 86

U[66539625451290191556] = 49514880023455056265219325423 13,
V[66539625451290191556] = 35698868671808550334208327135345,

U[66539625451290191557] = 20325178337077027980365129838829

U[133079250902580383112] = 11914250239719783706247175025075,
V[133079250902580383112] = 34903204895462437990406775868702,

U[133079250902580383113] = 51184545947027515690104749667 83

U[266158501805160766224] = 18864625313022381679429412154 44,
V[266158501805160766224] = 54980814297666428048904506164 08,

U[266158501805160766225] = 36922719805344404864166959159 26

U[532317003610321532449] = 26562179960589141841451695404285,
V[532317003610321532449] = 15008437492722171002245112679139,

U[532317003610321532450] = 20785308726655656421848404041712

U[1064634007220643064898] = 24679944074484597902031300269696,
V[1064634007220643064898] = 20438790677644267806957052935983,

U[1064634007220643064899] = 42690944031760735751776761227 34

U[2129268014441286129797] = 36237221081536698940727184221998,
V[2129268014441286129797] = 85641305827457400590702475788 43,

U[2129268014441286129798] = 41104028592528602205822154203 15

U[4258536028882572259594] = 13788802377547103088665393665443,
V[4258536028882572259594] = 90902407358292133920945829074 80,

U[4258536028882572259595] = 29729794529576517519696488766567

U[8517072057765144519189] = 11787397168189353541962096468649,
V[8517072057765144519189] = 27934433194795492500972019443659,

U[8517072057765144519190] = 19860915181492423021467057956154

U[17034144115530289038379] = 33506665597935745810398996422 45,
V[17034144115530289038379] = 73526324121184089458054161193 53,

U[17034144115530289038380] = 53516494859559917634226578807 99

U[34068288231060578076758] = 33219000681081454023107834993685,

V[34068288231060578076758] = 917410245235173634172285237 5421,

U[34068288231060578076759] = 211965515667165951824153436845 53

U[68136576462121156153516] = 10289234474984930835359759803 45,
V[68136576462121156153516] = 34733647398638670772800471120 24,

U[68136576462121156153517] = 20541417066569539359724512026290

U[136273152924242312307033] = 27013812486508269724435757597767,
V[136273152924242312307033] = 26859182177599374719008157531782,

U[136273152924242312307034] = 86462243591654629424054570846 69

U[272546305848484624614067] = 24178539904315598446643924319396,
V[272546305848484624614067] = 30017822919917115099269573363490,

U[272546305848484624614068] = 27098181412116356772956748841443

U[545092611696969249228134] = 18103442914900482485796810371580,
V[545092611696969249228134] = 24848404666263086787028433837969,

U[545092611696969249228135] = 31856508176934253570961216246 69

U[109018522339393938498456269] = 25688191434609293344182504257519,
V[109018522339393938498456269] = 30707357507752440334911050934640,

U[109018522339393938498456270] = 99075014982925075602302771159 74

U[218037044678787696996912539] = 25820509952329712071290138096066,
V[218037044678787696996912539] = 81890921878500504997607459739 52,

U[218037044678787696996912540] = 17004801070089881285525442035009

U[436074089357575399382507 8] = 10651039989351877766492371820684,
V[436074089357575399382507 8] = 31396975830809341680247505064509,

U[436074089357575399382507 9] = 27337349371922504440534379624 91

U[872148178715150798765015 6] = 29531846863794229195608123187346,
V[872148178715150798765015 6] = 98919766698267463050048295982 28,

U[872148178715150798765015 7] = 19711911766810487750306476392787

U[174429635743030159753003 12] = 13368901506099194156960464971690,
V[174429635743030159753003 12] = 10095104627983387502001487392888,

U[174429635743030159753003 13] = 11732003067041290829480976182289

U[348859271486060319506006 25] = 29616751767653415593635772960294,

V[348859271486060319506006 25] = 168979661649092926856536145894 02,

U[348859271486060319506006 26] = 232573589662813541396446937748 48

U[697718542972120639012012 50] = 164673775052354812286661977383 52,
V[697718542972120639012012 50] = 215480974688153430097294768580 55,

U[697718542972120639012012 51] = 717464514137052839881336818098

U[139543708594424127802402 500] = 197063441092772173333597480866466,
V[139543708594424127802402 500] = 205437182110703389091410772709 97,

U[139543708594424127802402 501] = 183475818728541884205277858862 6

U[279087417188848255604805 000] = 147197926532586109383735313846 81,
V[279087417188848255604805 000] = 221766866179285739784157340120 33,

U[279087417188848255604805 001] = 184482396355935924583946326983 57

U[558174834377696511209610 000] = 204237385483040093593586131876 06,
V[558174834377696511209610 000] = 218585234159596162686370526878 31,

U[558174834377696511209610 001] = 285085800924345353468133245761 3

U[111634966875539302241922 0000] = 146439802435124220053591958792 53,
V[111634966875539302241922 0000] = 468607449776671314462263405632 1,

U[111634966875539302241922 0001] = 966502737063956757499091496778 7

U[223269933751078604483844 0000] = 300353713145466450253287111605 59,
V[223269933751078604483844 0000] = 746922078699118030380963267607 8,

U[223269933751078604483844 0001] = 462023077880553385252671438213

U[446539867502157208967688 0000] = 259287584761858746025302425887 60,
V[446539867502157208967688 0000] = 253417403882830794521000160414 36,

U[446539867502157208967688 0001] = 256352494322344770273151293150 98

U[893079735004314417935376 0000] = 889137425747940793425170987867 1,
V[893079735004314417935376 0000] = 748455690725960412667638558123 0,

U[893079735004314417935376 0001] = 264782385552578653097805482100 56

U[178615947000862883587075 20000] = 235708069698172027007897446439 51,
V[178615947000862883587075 20000] = 361463400027892032468559830402 83,

U[178615947000862883587075 20001] = 298585734863032029738228638421 17

U[357231894001725767174150 40000] = 262013582371968312932004629744 40,

V[357231894001725767174150400000] = 661622715412019649844706628111 6,

U[357231894001725767174150400001] = 164087926956585138958237646277 78

U[714463788003451534348300800000] = 434944535895181146094484231993 9,
V[714463788003451534348300800000] = 169195326318644420299030279246 14,

U[714463788003451534348300800001] = 289247619682964860247404356023 82

U[142892757600690306869660160000] = 505173828350208781261478903295 6,
V[142892757600690306869660160000] = 338435862702755077805012910908 46,

U[142892757600690306869660160001] = 194476622768887977965580400619 01

U[285785515201380613739320320001] = 925374523481457626039996588941,
V[285785515201380613739320320001] = 356828601864529572750476585317 49,

U[285785515201380613739320320002] = 183041173549672074505438275603 45

U[571571030402761227478640640003] = 106306922356143159404860251973 26,
V[571571030402761227478640640003] = 361709482200365459434984215703 01,

U[571571030402761227478640640004] = 511054725493707166267572290370 8

U[114314206080552245495728128000 6] = 187953778233442746150543965784 86,
V[114314206080552245495728128000 6] = 228882939186695952656326594475 53,

U[114314206080552245495728128000 7] = 255156289811857566102702753291 4

U[228628412161104490991456256001 3] = 314774063201200938715022667032 34,
V[228628412161104490991456256001 3] = 296402319231375826756705734586 76,

U[228628412161104490991456256001 4] = 305588191216288382735864200809 55

U[457256824322208981982912512002 6] = 226768449530604255282103706526 13,
V[457256824322208981982912512002 6] = 153876222996892357623524401464 16,

U[457256824322208981982912512002 7] = 741960653486471365964904919409

U[914513648644417963965825024005 3] = 291906214618719417007865292992 5,
V[914513648644417963965825024005 3] = 324447867071684177486538953209 38,

U[914513648644417963965825024005 4] = 359721973995661652386827746055 37

U[182902729728883592793165004801 06] = 210082629783505324867236533125 33,
V[182902729728883592793165004801 06] = 0,

U[182902729728883592793165004801 07] = 287944044620636255226783271363 72

U[365805459457767185586330009602 12] = 0,

```
V[365805459457767185586330009602l2] = 4,

U[365805459457767185586330009602l3] = 2
```

De donde tenemos que $U_r \equiv 0 \mod n$ y $V_r \equiv 4 \mod n$. Además tenemos que $U_{\frac{r}{2}} \equiv 210082629783505324867236533125 33 \mod n$ y $V_{\frac{r}{2}} \equiv 0 \mod n$.

Por tanto, tenemos que n verifica el TPF para el e.c. α.

1.3 Apartado 3

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 ?

Tenemos $r = n + 1 = 365805459457767185586330009602l2$.

Aplicando el método ρ de Polard obtenemos que:

$$r = 2^2 \cdot 19 \cdot 53 \cdot 43117 \cdot 210626099398147601381287.$$

Al aplicar ρ de Polard, primos hemos eliminado los factores 2 por simplicidad, de modo que el número al que aplicamos el algoritmo es 914513648644417963965825024005 3, y se descompone en un total de 558 iteraciones.

Vamos a comprobar ahora que 43117 y 210626099398147601381287 son primos.

Sea $p_1 = 43117$, vamos a comprobar que es un número primo mediante Lucas-Lehmer. Para ello comenzamos factorizando $p_1 - 1$, de nuevo usando ρ de Polard:

$$p_1 - 1 = 2^2 \cdot 3 \cdot 3593$$

De nuevo, primero se divide entre los factores 2 y aplicamos el algoritmo a 10779, para el que solo es necesaria 1 iteración.

Y, con Lucas-Lehmer tenemos que $a = 2$ es un elemento primitivo para 43117 porque $2^{43117-1} \equiv 1 \mod 43117$ y $2^{\frac{43117-1}{p}} \not\equiv 1 \mod 43117$ para $p \in \{2, 3, 3593\}$ pues:

```
2^(n-1)/ 2 = 43116 mod n
2^(n-1)/ 3 = 9558 mod n
2^(n-1)/ 3593 = 4096 mod n
```

Nota: En estos códigos aunque la salida referencie a n, esto es por el print del programa y se refiere al p_i correspondiente a cada apartado. Se ha dejado la salida estándar del programa por simplicidad.

Consideramos ahora $p_2 = 210626099398147601381287$. Factorizamos de nuevo $p_2 - 1$:

$$p_2 - 1 = 2 \cdot 3 \cdot 113 \cdot 17 \cdot 25373 \cdot 733 \cdot 463867 \cdot 2118187.$$

Sacamos los factores 2 y aplicamos el método a 105313049699073800690643, para lo que se necesitan 626 iteraciones en total.

Y, con Lucas-Lehmer tenemos que $a = 5$ es un elemento primitivo para p_2 porque $5^{p_2-1} \equiv 1 \mod p_2$ y $5^{\frac{p_2-1}{p}} \not\equiv 1 \mod p_2$ para $p \in \{2, 3, 113, 17, 25373, 733, 463867, 2118187\}$ pues:

```
5^(n-1)/ 2 = 210626099398147601381286 mod n
5^(n-1)/ 3 = 201052306676548796207380 mod n
5^(n-1)/ 113 = 52303081321116716056069 mod n
5^(n-1)/ 17 = 82697440648428203877263 mod n
5^(n-1)/ 25373 = 193688392282791819942315 mod n
5^(n-1)/ 733 = 186869216112249535026689 mod n
5^(n-1)/ 463867 = 37506715538082165466792 mod n
5^(n-1)/ 2118187 = 83038764093421513984660 mod n
```

Como hemos obtenido factores primos mayores de 10000, comprobamos su primalidad.

Consideramos $p_3 = 25373$. Factorizamos de nuevo $p_3 - 1$:

$$p_3 - 1 = 2^2 \cdot 6343.$$

Sacamos los factores 2 y no es necesario usar el método a 6343, pues está en la lista.

Y, con Lucas-Lehmer tenemos que $a = 2$ es un elemento primitivo para p_3 porque $2^{p_3-1} \equiv 1 \mod p_3$ y $2^{\frac{p_3-1}{p}} \not\equiv 1 \mod p_3$ para $p \in \{2, 6343\}$ pues:

```
2^(n-1)/ 2 = 25372 mod n
2^(n-1)/ 6343 = 16 mod n
```

Continuamos con $p_4 = 463867$. Factorizamos de nuevo $p_4 - 1$:

$$p_4 - 1 = 2 \cdot 3 \cdot 313 \cdot 19 \cdot 13.$$

Donde primero se extraen los factores 2 y se aplica el método a 231933, necesitando 10 iteraciones totales.

Y, con Lucas-Lehmer tenemos que $a = 12$ es un elemento primitivo para p_4 porque $12^{p_4-1} \equiv 1 \mod p_4$ y $12^{\frac{p_4-1}{p}} \not\equiv 1 \mod p_4$ para $p \in \{2, 3, 313, 19, 13\}$ pues:

```
12^(n-1)/ 2 = 463866 mod n
12^(n-1)/ 3 = 47777 mod n
12^(n-1)/ 313 = 36373 mod n
12^(n-1)/ 19 = 171844 mod n
12^(n-1)/ 13 = 344990 mod n
```

Comprobamos ahora $p_5 = 2118187$. Factorizamos de nuevo $p_5 - 1$:

$$p_5 - 1 = 2 \cdot 3^2 \cdot 7 \cdot 16811.$$

Donde, de nuevo, se ha sacado el factor 2 y se aplica el método a 1059093, usando 4 iteraciones en total.

Y, con Lucas-Lehmer tenemos que $a = 2$ es un elemento primitivo para p_5 porque $2^{p_5-1} \equiv 1 \mod p_5$ y $2^{\frac{p_5-1}{p}} \not\equiv 1 \mod p_5$ para $p \in \{2, 3, 7, 16811\}$ pues:

```
2^(n-1)/ 2 = 2118186 mod n
2^(n-1)/ 3 = 1491183 mod n
2^(n-1)/ 3 = 1491183 mod n
2^(n-1)/ 7 = 1355468 mod n
2^(n-1)/ 16811 = 1526343 mod n
```

Finalmente, comprobamos que $p_6 = 16811$ es primo descomponiendo $p_6 - 1$:

$$p_6 - 1 = 2 \cdot 5 \cdot 41^2.$$

Esta descomposición se ha hecho a mano, ya que el número era pequeño.

Y con Lucas-Lehmer obtenemos $a = 7$ es elemento primitivo para p_6, porque $7^{p_6-1} \equiv 1 \mod p_6$ y $7^{\frac{p_6-1}{p}} \not\equiv 1 \mod p_6$ para $p \in \{2, 5, 41\}$ pues:

```
7^(n-1)/ 2 = 16810 mod n
7^(n-1)/ 5 = 2954 mod n
7^(n-1)/ 41 = 11826 mod n
```

Por tanto. queda comprobada la correcta factorización de r en números primos:

$$r = 2^2 \cdot 19 \cdot 53 \cdot 43117 \cdot 2106260993981476013812 87.$$

Vamos a calcular ahora $U_{\frac{r}{p}}$ con $p \in \{2, 19, 53, 43117, 2106260993981476013812 87\}$.

Sabemos que:

$$U_{\frac{r}{2}} = U_{1829027297288835927931650048 0106} = 2100826297835053248672365331 2533$$

$$U_{\frac{r}{19}} = U_{1925291891882985187296473734748} = 1441071763887989374744572426 6576$$

$$U_{\frac{r}{53}} = U_{6901989801089946897855283200 04} = 2163215016433073288179453767 9070$$

$$U_{\frac{r}{43117}} = U_{8484019283757385383638240 36} = 1523818635855760718260723164 5757$$

$$U_{\frac{r}{2106260993981476013812 87}} = U_{173675276} = 1225170092658739532353840129 9078$$

Como ninguno de los $U_{\frac{r}{p}}$ con p siendo un factor primo de r sale 0, entonces tenemos que el rango de Lucas $\omega(n) = r$. Luego como el rango de n es $n + 1$ tenemos que n es primo.