Ejercicio 7

Ana Buendía Ruiz-Azuaga

March 20, 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,

$$V_{\frac{r}{2}}^2 = 4 + 2(2)^{\frac{r}{2}} = 36580545945776718558633000960211 \mod n \equiv 0 \mod n$$

.

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] = 36580545945776718558633000960210,
V[3] = 36580545945776718558633000960206,

U[4] = 36580545945776718558633000960208

U[7] = 7,
V[7] = 36580545945776718558633000960198,

U[8] = 36580545945776718558633000960208

U[14] = 36580545945776718558633000960120,
V[14] = 36580545945776718558633000960124,

U[15] = 36580545945776718558633000960122

U[28] = 7917,
```

```
V[28] = 36580545945776718558633000935012,

U[29] = 36580545945776718558633000951570

U[57] = 36580545945776718558632950269314,
V[57] = 747311035,

U[58] = 348310069

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

U[116] = 191944503493752333

U[230] = 9085068195533530414279122459439,
V[230] = 4080701587084059651838353133425,

U[231] = 6582884891308795033058737796432

U[461] = 5959030677211170876601815288653,
V[461] = 12231053807303017165974138820499,

U[462] = 9095042242257094021287977054576

U[923] = 4246659038619848551495442516732,
V[923] = 27786632601091692388221416170843,

U[924] = 34306918792744129749174929823893

U[1846] = 8173123820556134758491155422405,
V[1846] = 12352535795618830125523066526592,

U[1847] = 28553102780975841721323611454604

U[3693] = 7919197314113073324210236619410,
V[3693] = 14285716598531391991050223434270,

U[3694] = 11102456956322232657630230026840

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

U[7388] = 20573827846149776369868440379922

U[14774] = 19077052661067521861992245423014,
V[14774] = 7739309016867210869244325096018,

U[14775] = 13408180838967366365618285259516

U[29549] = 1370132771987269238959597372838,
```

```
V[29549] = 21617783361801816378317467107728,

U[29550] = 11493958066894542808638532240283

U[59099] = 24048374465421451750956705311521,
V[59099] = 2777952695823406784903818930052,

U[59100] = 31703436553510788547246762600892

U[118198] = 25653548862695001836446402125826,
V[118198] = 21960352259111058925503567270952,

U[118199] = 23806950560903030380974984698389

U[236396] = 25868711012857287639588563790999,
V[236396] = 9227203513281161451013147841514,

U[236397] = 35838230235957583824617356296362

U[472792] = 31089726186466798745307802896549,
V[472792] = 24053880299348242388436746905728,

U[472793] = 9281530270019161287555774421033

U[945584] = 20047231121281047148624619107240,
V[945584] = 24197884895369342011365845244837,

U[945585] = 3832285035436835300678731695933

U[1891169] = 9721298095328574424657191178940,
V[1891169] = 22108947191779295420364755135472,

U[1891170] = 15915122643553934922510973157206

U[3782339] = 16388158361563485158887913844775,
V[3782339] = 6694554768283832446697967339453,

U[3782340] = 11541356564923658802792940592114

U[7564679] = 10222909972668840788265033390468,
V[7564679] = 30948590353474585265172294238020,

U[7564680] = 20585750163071713026718663814244

U[15129359] = 20024340915293157784876594446441,
V[15129359] = 4296877534000671248078579024626,

U[15129360] = 30450882197535273795794087215639

U[30258718] = 6592951170564225160629971154089,
```

V[30258718] = 11601815651533928519128622094644,

U[30258719] = 27387656383937436119195797104472

U[60517436] = 25289681243906482065858831807907,
V[60517436] = 7612330291276774426993237683562,

U[60517437] = 34741278740479987525742535225840

U[121034873] = 18881108760579169002232787098557,
V[121034873] = 32661103356680518554334923198999,

U[121034874] = 25771106058629843778283855148778

U[242069747] = 12745287367436248523157412505794,
V[242069747] = 24862604922636495587911718455094,

U[242069748] = 18803946145036372055534565480444

U[484139494] = 17450445583098853430685820812466,
V[484139494] = 20473463303187082267128844679084,

U[484139495] = 18961954443142967848907332745775

U[968278988] = 8552710951959249117247618772677,
V[968278988] = 26272051063075832779597642528811,

U[968278989] = 17412381007517540948422630650744

U[1936557977] = 22195191375160520191026379482515,
V[1936557977] = 31461457125744306169525447395769,

U[1936557978] = 26828324250452413180275913439142

U[3873115955] = 23631818372664973767761057880992,
V[3873115955] = 11190842380109373472220316449832,

U[3873115956] = 17411330376387173619990687165412

U[7746231911] = 16431764352995884416657900652890,
V[7746231911] = 23894085371050430018706997099069,

U[7746231912] = 1872651889134797938365948395874

U[15492463822] = 7770728919466133498851331725239,
V[15492463822] = 35110907543810342927831033765601,

U[15492463823] = 21440818231638238213341182745420

U[30984927644] = 7717303048586031141801356194210,

V[30984927644] = 19747466944501492022272329689906,

U[30984927645] = 13732384996543761582036842942058

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

U[61969855290] = 28216734085440501428975560614956

U[123939710578] = 16531993914075891860963696789412,
V[123939710578] = 7354174268382085740526998057131,

U[123939710579] = 30233357064117348080061847903377

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

U[247879421157] = 15504739124269005349814933388561

U[495758842313] = 9791518148944326394685776274116,
V[495758842313] = 30802848035715725766700011500375,

U[495758842314] = 2006910119441666801376393407140

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

U[991517684628] = 22342672047746132300458135529264

U[1983035369255] = 1773682291545240233391521446361,
V[1983035369255] = 23890591674837766380069049650297,

U[1983035369256] = 12832136983191503306730285548329

U[3966070738511] = 7694985132573022260427477366116,
V[3966070738511] = 11824209240499636727866922836413,

U[3966070738512] = 28049870159424688773463700581370

U[7932141477023] = 2873012872051690560830176463817,
V[7932141477023] = 13652659377202275319783476791744,

U[7932141477024] = 26553109097515342219623327107886

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

U[15864282954047] = 5809019234512634277895920875323

U[31728565908093] = 24416824114566897146532481368205,

V[31728565908093] = 8863292411364289290192173247450,

U[31728565908094] = 34930331235853952497678827787933

U[63457131816187] = 229530610141385030449308970488,
V[63457131816187] = 20286384525474486104694004162021,

U[63457131816188] = 28548230540696294846888157046360

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

U[126914263632375] = 3376466730972235652733409026143

U[253828527264748] = 8286274619661707468367501003927,
V[253828527264748] = 5086355230578250923707592477008,

U[253828527264749] = 24976587898008338475354047220573

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

U[507657054529497] = 482343822896293298140947818861

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

U[1015314109058994] = 6864048874635981124878888644643

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] = 167708367164846115038169626 4916,

U[32490051489887789] = 311090442975257284494344903 06554

U[64980102979775577] = 169012778222713431308639455 51781,
V[64980102979775577] = 150343130849128307819460018 11177,

U[64980102979775578] = 159677954535920869564049736 81479

U[129960205959551155] = 2101101185516092532128287619027,
V[129960205959551155] = 2199988225076055310463469600 8552,

U[129960205959551156] = 3034076469102668209769799229 3895

U[259920411919102310] = 1986864333323580442051055906358,
V[259920411919102310] = 2294557229632699731614287477 4341,

U[259920411919102311] = 3075649128771364815841346582 0455

U[519840823838204621] = 3270181962491769887906634982 0063,
V[519840823838204621] = 3101523756338694620745214518 6811,

U[519840823838204622] = 3185852859415232254325924750 3437

U[1039681647676409243] = 3054027574779390969244010926 0445,
V[1039681647676409243] = 2019142375300654039776616695 5889,

U[1039681647676409244] = 2536584975040022504510313810 8167

U[2079363295352818486] = 2718575321137839070674095137 0619,
V[2079363295352818486] = 1527432802781281607594789775 1050,

U[2079363295352818487] = 2939767646707244112027924080 729

U[4158726590705636972] = 5791140219486069803968708906 533,
V[4158726590705636972] = 3009081293274360490829186292 8863,

U[4158726590705636973] = 1794097657611483735613028591 7698

U[8317453181411273944] = 3162032702172387618938955730 0783,
V[8317453181411273944] = 4295772477347774840442095760 481,

U[8317453181411273945] = 1795804974953582551491582653 0632

U[16634906362822547889] = 3253516500287709760769601286 9929,
V[16634906362822547889] = 8186102778575873390831406502 214,

U[16634906362822547890] = 2070360917838126219947209205 966

U[33269812725645095778] = 2452793698469353216703845914 4142, V[33269812725645095778] = 2194452921157212725821930715383O,

U[33269812725645095779] = 23236233098132829712628883148986

U[66539625451290191556] = 4951488002345505626521932542313,
V[66539625451290191556] = 35698868671808550334208327135345,

U[66539625451290191557] = 20325178337077027980365129838829

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

U[133079250902580383113] = 5118454594702751569010474966783

U[266158501805160766224] = 1886462531302238167942941215444,
V[266158501805160766224] = 5498081429766642804890450616408,

U[266158501805160766225] = 3692271980534440486416695915926

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

U[532317003610321532450] = 20785308726655656421848404041712

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

U[1064634007220643064899] = 4269094403176073575177676122734

U[2129268014441286129797] = 36237221081536698940727184221998,
V[2129268014441286129797] = 8564130582745740059070247578843,

U[2129268014441286129798] = 4110402859252860220582215420315

U[4258536028882572259594] = 13788802377547103088665393665443,
V[4258536028882572259594] = 9090240735829213392094582907480,

U[4258536028882572259595] = 29729794529576517519696488766567

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

U[8517072057765144519190] = 19860915181492423021467057956154

U[17034144115530289038379] = 3350666559793574581039899642245,
V[17034144115530289038379] = 7352632412118408945805416119353,

U[17034144115530289038380] = 5351649485955991763422657880799

U[34068288231060578076758] = 33219000681081454023107834993685,

V[34068288231060578076758] = 9174102452351736341722852375421,

U[34068288231060578076759] = 21196551566716595182415343684553

U[68136576462121156153516] = 1028923447498493083535975980345,
V[68136576462121156153516] = 3473364739863867077280047112024,

U[68136576462121156153517] = 20541417066569539359724512026290

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

U[136273152924242312307034] = 8646224359165462942405457084669

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

U[272546305848484624614068] = 27098181412116356772956748841443

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

U[545092611696969249228135] = 3185650817693425357096121624669

U[1090185223393938498456269] = 25688191434609293344182504257519,
V[1090185223393938498456269] = 30707357507752440334911050934640,

U[1090185223393938498456270] = 9907501498292507560230277115974

U[2180370446787876996912539] = 25820509952329712071290138096066,
V[2180370446787876996912539] = 8189092187850050499760745973952,

U[2180370446787876996912540] = 17004801070089881285525442035009

U[4360740893575753993825078] = 10651039989351877766492371820684,
V[4360740893575753993825078] = 31396975830809341680247505064509,

U[4360740893575753993825079] = 2733734937192250444053437962491

U[8721481787151507987650156] = 29531846863794229195608123187346,
V[8721481787151507987650156] = 9891976669826746305004829598228,

U[8721481787151507987650157] = 19711911766810487750306476392787

U[17442963574303015975300312] = 13368901506099194156960464971690,
V[17442963574303015975300312] = 10095104627983387502001487392888,

U[17442963574303015975300313] = 11732003067041290829480976182289

U[34885927148606031950600625] = 29616751767653415593635772960294,

```
V[34885927148606031950600625] = 16897966164909292685653614589402,

U[34885927148606031950600626] = 23257358966281354139644693774848

U[69771854297212063901201250] = 16467377505235481228666197738352,
V[69771854297212063901201250] = 21548097468815343009729476858055,

U[69771854297212063901201251] = 717464514137052839881336818098

U[139543708594424127802402500] = 19706344109277217333597480866466,
V[139543708594424127802402500] = 20543718211070338909141077270997,

U[139543708594424127802402501] = 1834758187285418842052778588626

U[279087417188848255604805000] = 14719792653258610938373531384681,
V[279087417188848255604805000] = 22176686617928573978415734012033,

U[279087417188848255604805001] = 18448239635593592458394632698357

U[558174834377696511209610000] = 20423738548304009359358613187606,
V[558174834377696511209610000] = 21858523415959616268637052687831,

U[558174834377696511209610001] = 2850858009243453534681332457613

U[1116349668755393022419220000] = 14643980243512422005359195879253,
V[1116349668755393022419220000] = 4686074497766713144622634056321,

U[1116349668755393022419220001] = 9665027370639567574990914967787

U[2232699337510786044838440000] = 30035371314546645025328711160559,
V[2232699337510786044838440000] = 7469220786991180303809632676078,

U[2232699337510786044838440001] = 462023077880553385252671438213

U[4465398675021572089676880000] = 25928758476185874602530242588760,
V[4465398675021572089676880000] = 25341740388283079452100016041436,

U[4465398675021572089676880001] = 25635249432234477027315129315098

U[8930797350043144179353760000] = 8891374257479407934251709878671,
V[8930797350043144179353760000] = 7484556907259604126676385581230,

U[8930797350043144179353760001] = 26478238555257865309780548210056

U[17861594700086288358707520000] = 23570806969817202700789744643951,
V[17861594700086288358707520000] = 36146340002789203246855983040283,

U[17861594700086288358707520001] = 29858573486303202973822863842117

U[35723189400172576717415040000] = 26201358237196831293200462974440,
```

```
V[3572318940017257671741504000] = 6616227154120196498447066281116,

U[3572318940017257671741504001] = 16408792695658513895823764627778

U[7144637880034515343483008000] = 4349445358951811460944842319939,
V[7144637880034515343483008000] = 16919532631864442029903027924614,

U[7144637880034515343483008001] = 28924761968296486024740435602382

U[14289275760069030686966016000] = 5051738283502087812614789032956,
V[14289275760069030686966016000] = 33843586270275507780501291090846,

U[14289275760069030686966016001] = 19447662276888797796558040061901

U[28578551520138061373932032001] = 9253745234814576260399965889 41,
V[28578551520138061373932032001] = 35682860186452957275047658531749,

U[28578551520138061373932032002] = 18304117354967207450543827560345

U[57157103040276122747864064003] = 10630692235614315940486025197326,
V[57157103040276122747864064003] = 36170948220036545943498421570301,

U[57157103040276122747864064004] = 5110547254937071662675722903708

U[114314206080552245495728128006] = 18795377823344274615054396578486,
V[114314206080552245495728128006] = 22888293918669595265632659447553,

U[114314206080552245495728128007] = 2551562898118575661027027532914

U[228628412161104490991456256013] = 31477406320120093871502266703234,
V[228628412161104490991456256013] = 29640231923137582675670573458676,

U[228628412161104490991456256014] = 30558819121628838273586420080955

U[457256824322208981982912512026] = 22676844953060425528210370652613,
V[457256824322208981982912512026] = 15387622299689235762352440146416,

U[457256824322208981982912512027] = 7419606534864713659649049194 09

U[914513648644417963965825024053] = 2919062146187194170078652929925,
V[914513648644417963965825024053] = 32444786707168417748653895320938,

U[914513648644417963965825024054] = 35972197399566165238682774605537

U[1829027297288835927931650048106] = 21008262978350532486723653312533,
V[1829027297288835927931650048106] = 0,

U[1829027297288835927931650048107] = 28794404462063625522678327136372

U[3658054594577671855863300096212] = 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 $U_{\frac{r}{2}} \equiv 210082629783505324867236533l2533 \mod n$ 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 $r = n + 1 = 3658054594577671855863300096 0212$.

Aplicando el método ρ de Polard obtenemos que:

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

Al aplicar ρ de Polard, primos hemos eliminado los factores 2 por simplicidad, de modo que el número al que aplicamos el algoritmo es 914513648644417963965825024 0053, y se descompone en un total de 558 iteraciones.

Vamos a comprobar ahora que 43117 y 2106260993981476013812 87 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:

$$\begin{aligned} 2^{\frac{43117-1}{2}} &\equiv 43116 \mod 43117 \\ 2^{\frac{43117-1}{3}} &\equiv 9558 \mod 43117 \\ 2^{\frac{43117-1}{3593}} &\equiv 4096 \mod 43117 \end{aligned}$$

Consideramos ahora $p_2 = 2106260993981476013812 87$. 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:

$$5^{\frac{p_2-1}{2}} \equiv 2106260993981476013812 86 \mod p_2$$

$$5^{\frac{p_2-1}{3}} \equiv 20105230667654879620738O \mod p_2$$
$$5^{\frac{p_2-1}{113}} \equiv 5230308132111671605606 9 \mod p_2$$
$$5^{\frac{p_2-1}{17}} \equiv 8269744064842820387726 3 \mod p_2$$
$$5^{\frac{p_2-1}{25373}} \equiv 1936883922827918199423 15 \mod p_2$$
$$5^{\frac{p_2-1}{733}} \equiv 1868692161122495350266 89 \mod p_2$$
$$5^{\frac{p_2-1}{463867}} \equiv 3750671553808216546679 2 \mod p_2$$
$$5^{\frac{p_2-1}{2118187}} \equiv 8303876409342151398466 0 \mod p_2$$

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:

$$2^{\frac{p_3-1}{2}} \equiv 25372 \mod p_3$$
$$2^{\frac{p_3-1}{6343}} \equiv 16 \mod p_3$$

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:

$$12^{\frac{p_4-1}{2}} \equiv 463866 \mod p_4$$
$$12^{\frac{p_4-1}{3}} \equiv 47777 \mod p_4$$
$$12^{\frac{p_4-1}{313}} \equiv 36373 \mod p_4$$
$$12^{\frac{p_4-1}{19}} \equiv 171844 \mod p_4$$
$$12^{\frac{p_4-1}{13}} \equiv 344990 \mod p_4$$

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:

$$2^{\frac{p_5-1}{2}} \equiv 2118186 \mod p_5$$

$$2^{\frac{p_5-1}{3}} \equiv 1491183 \mod p_5$$

$$2^{\frac{p_5-1}{7}} \equiv 1355468 \mod p_5$$

$$2^{\frac{p_5-1}{16811}} \equiv 1526343 \mod p_5$$

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:

$$7^{\frac{p_6-1}{2}} \equiv 16810 \mod p_6$$

$$7^{\frac{p_6-1}{5}} \equiv 2954 \mod p_6$$

$$7^{\frac{p_6-1}{41}} \equiv 11826 \mod p_6$$

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

$$r = 2^2 \cdot 19 \cdot 53 \cdot 43117 \cdot 21062609939814760 1381287.$$

Vamos a calcular ahora $U_{\frac{r}{p}}$ con $p \in \{2, 19, 53, 43117, 210626099398147601381287\}$.

Sabemos que:

$$U_{\frac{r}{2}} = U_{182902729728883592793165004801 06} = 210082629783505324867236533125 33$$

$$U_{\frac{r}{19}} = U_{19252918918829851872964737347 48} = 14410717638879893747445724266576$$

$$U_{\frac{r}{53}} = U_{6901989801089946897855283200 04} = 21632150164330732881794537679070$$

$$U_{\frac{r}{43117}} = U_{8484019283757385383638240 36} = 15238186358557607182607231645757$$

$$U_{\frac{r}{210626099398147601381287}} = U_{173675276} = 12251700926587395323538401299078$$

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 por un corolario, como el rango de n es $n + 1$ tenemos que n es primo.