Ejercicio 7

David García Curbelo

Toma tu número $n = 42306590867920578696052923567 91$ de la lista publicada para el ejercicio 3. Sea d el primer elemento de la sucesión $5, -7, 9, -11, 13, \ldots$ 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:

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

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:

$$\begin{cases} U_{2k} = 2U_kU_{k+1} - PU_k^2 \\ U_{2k+1} = U_{k+1}^2 - QU_k^2 \\ U_{2k+2} = PU_{k+1}^2 - 2QU_kU_{k+1} \\ V_k = 2U_kU_{k+1} - PU_k \\ V_{2k} = V_k^2 - 2Q^k \end{cases}$$

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 $r/2 = 211532954339602893480264617839 6$ (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	120602554255507397569721819633 2	11919517672109351684466276918 04
8	213	22245717243742725406409553710 25	27817333334047993510947183536 32
9	427	27241883792381013951436887011 11	10405214963270431205575080551 56
10	854	22408815670618124584864358640 69	11214935157109781512874722131 76
11	1708	24401777878210149651765237159 87	28100798324131554869069446740 5
12	3417	69328882417391762182294818787 4	23713286985659074971475491445 16
13	6834	37219980438255651116787760907 20	20142923978585398682099968063 93
14	13669	42058983941841306031335324950 00	12111431140409185903318603281 15
15	27339	38489875431545363387458968956 9	19826244288136542235203060306 47
16	54679	22051149623510870544391234497 95	35594926771682813590563142194 03
17	109359	30560598692276290362043338890 51	14237583361708617580173303679 97
18	218719	35514239501210268809182157092 94	34140734897248040992928171002 77
19	437439	34605510038549046596888146266 58	47559147686724376862815570097 8
20	874879	24600431906954904279451400610 60	22474951429810719567257414931 50
21	1749759	21662558305143249131288874042 98	41126029389648430421511725943 79
22	3499519	26084409519923152346537129454 29	32399092793420611759670857691 38
23	6999038	26992081757477179820188890782 1	14173789434087223806967770158 1
24	13998076	12134359735330375090313559882 81	37836082309379593088893857108 67
25	27996153	65227837848673272820610115874 7	28268438982997102993800477806 22
26	55992306	38845625176662160681307832625 97	31817556620282420296342370580 95
27	111984613	32470493285853033444899796522 55	26953751323713595114686268403 44
28	223969227	29779707979250577247359439087	25866961791891301693851722567 63
29	447938454	22604795893196945505719716483 44	28365850218704328636875632404
30	895876908	40965214621645240277380001145	45388062460616719774971981037 9
31	1791753817	51081910783384502098007430243 2	31359867411202517863328782014 0
32	3583507635	15419208345872264359349209739 19	12813802694213942312094897027 07
33	7167015270	95345378654549172556883074941 0	32640836163207008949684567087 11
34	14334030540	26604756957927924131837339184 85	68225623216621342951476364615 6
35	28668061080	24717517911617368820198869803 84	65766322915271530367590265125 0
36	57336122161	40126066123333376260353947346 48	28048239559822303198869474069 02
37	114672244323	31057223821714804683487753814 47	47756316579738035408842830863 2
38	229344488647	40679410190895840552449246171 85	42123538417000884306115249327 30
39	458688977294	30405751681730135891303660880 93	37229561952854415533055655471 09
40	917377954589	16782086485154032996968391984 53	37050929998666155002748622189 83
41	1834755909178	53226342506144001684961822741 3	35775754907023814119775194206 6
42	3669511818356	16284586546092892190834916758 66	32677376502016808122215578691 10
43	7339023636712	24018166286872390602777160388 34	38802981806261182264099112236 67
44	14678047273425	13566730183318915934581392730 57	28902924397466922514954668968 40
45	29356094546851	39988080440763794732040860686 53	29279429472804246786067158940 70
46	58712189093702	10029957733101921305605370462 01	40756798187593255376958889361 51
47	117424378187404	36382963795517078511963354756 85	19770345904240340244270906866 80
48	234848756374809	11991729758902236118430586387 24	15206589186207344972024040328 04
49	469697512749618	43775204959991542847038984483	16050822106293553101493541004 08
50	939395025499236	25539322598722982345738253125 71	39278685773587507052432485012 50
51	1878790050998472	17823097695193648987253608252 72	25268533586581540878761767981 52
52	3757580101996944	32399518399684746745722775700 82	17546602796281644503793218104 40

Paso	k	U_k	U_{k+1}
53	7515160203993889	772554330115870989869155980205	229931259228073513132672359653 3
54	15030320407987779	116129518754397128803328716408 3	198038198332601676481567411142 2
55	30060640815975559	386909515919914069774439597336 9	166741559067857248502348832791 9
56	60121281631951118	368909550765027473121724701158 2	300623743741183562120720020371 8
57	120242563263902237	361371593030257294943867729495	369879739464049757701342403545 9
58	240485126527804474	403702312558498364256439391511 9	283742619493790585931991704006
59	480970253055608949	609726694192642884902662201458	201040716497921073630585126023 4
60	961940506111217898	220379537114219030356619172821 7	767987694610083807997840429856
61	1923881012222435797	309267500723565935653432107432 2	345926869229982535115894146363 4
62	3847762024444871594	210285081593416934430546756733 2	271108870520556852497276813415
63	7695524048889743188	911953416852421858603161607959	417996307645037596686742530526 1
64	15391048097779486377	118636265144355366294780848258 6	404524306208519547068689780460 6
65	30782096195558972755	106932011528274888052281338537 3	246527725746056666414165991708 4
66	61564192391117945511	927177355366383141186254893116	171122374003500110742516272387 3
67	123128384782235891022	219289986115293196901554145936 2	285425510463144531331808445984 2
68	246256769564471782045	729713940011399371026437205705	392083858637607540459658697976
69	492513539128943564091	241178239351489204396186795220 6	191959338762416615159411805699 8
70	985027078257887128182	233214570247753388251464030649 6	145748069195036973559553560284 7
71	1970054156515774256365	297942358942128137292814664519 7	171050659225230009285446032380 5
72	3940108313031548512731	863267501283303413041490436075	359882861362991564747568183569 6
73	7880216626063097025463	428774538957186445089724910224	513882096213460020801917472892
74	15760433252126194050927	168200342518927822986564014638	264343055694671161506105581018
75	3152086650425238810185 5	381699679839085880632343484126 1	389114795299523709994307909338 3
76	6304173300850477620371 1	378599549046298251950162002502 3	244805158527697697055492771726 2
77	1260834660170095524074 22	242398830340891137113058358436 6	131206662744128317540976990507 0
78	2521669320340191048148 44	394432113232051991869245486993 3	147921030260036354936524734842 8
79	5043338640680382096296 89	296302497152559814291720919532 4	111676829609871316130596960817 2
80	1008667728136076419259379	406890399506603817905361123656 6	344475272533701415423268737255 0
81	2017335456272152838518758	109353192839124901890875484940 0	163763925882946685631831344266 5
82	4034670912544305677037517	410547579562656139992692478934 7	251774617342921911519040752456 9
83	8069341825088611354075035	384714197898948512145772275299 6	417035776696142589439455626681 6
84	16138683650177222708150071	233233472116521483615076583413 8	238947829503132627249648965107 9
85	32277367300354445416300143	290955092621505497089148010333 6	470634721964005296753726917670
86	64554734600708890832600286	168756825002630672135088699528 7	368007373237041662502688254231 7
87	129109469201417781665200572	208898999863247713075519848699 7	345894778107804131211024524528 4
88	258218938402835563330401144	159230126819930976461127962062 8	458204221306629199977148706924
89	516437876805671126660802289	392487535493950293919665024324	690660759799319557733225888240
90	1032875753611342253321604579	407108533398614795358703680943 0	235285931203974154003611810837 3
91	2065751507222684506643209158	323659835119337540915473839864 5	493555714260808026523843813575
92	4131503014445369013286418317	101401383401409774199272013396 5	180387121782979401911778155108 9
93	8263006028890738026572836634	753760903567690576383788648926	410827496680390377747794920892 5
94	16526012057781476053145673268	224813277999078468847857087980 7	837827279477629125322250435241
95	33052024115562952106291346537	266137754027560388051165385210 2	311599964416931564025287347296 5
96	66104048231125904212582693074	198010946527116599391583050286 9	322566446727654064099010975109
97	132208096462251808425165386149	241415318048201994766578405143 2	114794499843013069910553763255 7
98	264416192924503616850330772299	249567450660551621575252091327	193355535348100208468464085624 4
99	528832385849007233700661544599	762432504487272216321147199828	381216252243636108160573599914
100	1057664771698014467401323089198	0	400308804229400273828849410268
101	2115329543396028934802646178396	0	138523009484832075656463758526 1
102	4230659086792057869605292356792	0	423065908679205786960529235678 8

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 $V_r = 846131817358411573921058471357 6 \equiv -6$ y $V_{r/2} = 277046018969664151312927517052 2$, 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 $r = n+1 = 42306590867920578696052923567 92 = 2^3 \cdot 52883238584900723370066154459 9$. Desconocemos si $m_1 = 52883238584900723370066154459 9$ 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 $52883238584900723370066154459 9 = 4349 \cdot 12159861711864962835149725 1$.

Veamos a continuación si $m_2 = 12159861711864962835149725 1$ 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 $12159861711864962835149725 1 = 62347 \cdot 1950352336417945183433$.

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 (añado las tablas de iteraciones más adelante):

- $U_r = 0$

- $U_{r/2} = U_{211532954339602893480264617839 6} = 0$

- $U_{r/4349} = U_{9727889369491970268119780 08} = 346836615446298981640013713042 8$

- $U_{r/62347} = U_{6785665848865314882200093 6} = 18654459084131764615471846407 3$

- $U_{r/1924630699} = U_{2198166686726042848808} = 11156828841156271340465590459 31$

- $U_{r/1013364453467} = U_{4174864307029719976} = 20819790678060074150690911725 86$

Finalmente, como vimos anteriormente, tenemos que $U_{r/2} \equiv 0$, lo que nos asegura que el rango de Lucas $\omega(n) \neq n + 1$, por lo que concluimos que para los valores de Q y P dados, no podemos asegurar la primalidad de nuestro número n.

$U_{r/2}$

Paso	k	U_k	U_{k+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	11919517672109351684466276918 04
8	213	2224571724374272540640955371025	27817333334047993510947183536 32
9	427	2724188379238101395143688701111	10405214963270431205575080551 56
	...	...	...
97	1322080964622518084251653861 49	2414153180482019947665784051432	11479449984301306991055376325 57
98	2644161929245036168503307722 99	2495674506605516215752520913 27	19335553534810020846846408562 44
99	5288323858490072337006615445 99	7624325044872722163211471998 28	38121625224363610816057359991 4
100	1057664771698014467401323089198	0	40030880422940027382884941026 8
101	2115329543396028934802646178396	0	13852300948483207565646375852 61

$U_{r/4349}$

Paso	k	U_k	U_{k+1}
1	1	1	1
2	3	4	7
3	6	40	97
4	12	6160	14209
5	25	315732481	727060321
6	50	359426118413557441	827677709047869124
7	100	37337855340987997985559442593 69	10359658813296092019695764021 6
8	201	36313759330802417472726491396 45	18074297685645682670093469341 16
9	402	19490600790019705112465419291 87	11767661425454084842181126464 73
	...	...	...
84	15199827139831203543937156	71598392366680710252138045371	29394498805446942556097069618 06
85	30399654279662407087874312	12873757574384887710688251176 62	26553643375091654630192027177 39
86	60799308559324814175748625	84484243969432082543174435693 5	19737862573214232620357514949 96
87	12159861711864962835149725 1	64937353573895289968971712622 2	79103288921763006631691822702 6
88	24319723423729925670299450 2	11354660321456494476788496057 35	35833869158040080630840302909 42
89	48639446847459851340598900 4	41001057472555942608407373287 36	14355735703409873510532666380 49
90	97278893694919702681197800 8	34683661544629898164001371304 28	23455902082941761118724267185 0

$U_{r/62347}$

Paso	k	U_k	U_{k+1}
1	1	1	1
2	3	4	7
3	7	97	217
4	14	32689	75316
5	28	3855438727	8878212019
6	56	53594397111487539097	123415871987270197948
7	112	219373127069106087323663651229727	227218223175405837706623590057 7
8	224	16989794173504151735210222553 09	27365864502604062914835408102 83
9	449	14479892882479925417688047589 55	39339712887844568033200013490 68
	...	...	...
80	1060260288885205450343764	40205391214235705533812921473 77	97318699828499156188768126074 4
81	2120520577770410900687529	32415965616443566386914843445 40	35399434169648979995758743394 01
82	4241041155540821801375058	32461045238758170220804487886 90	41831970890496105711746647160 40
83	8482082311081643602750117	11711977752694507134645131726 97	79663984884076675345530842774 7
84	16964164622163287205500234	29799891480445102095716165259 94	41809756910789971013031738019 70
85	33928329244326574411000468	27478708910321459990741793575 29	12037837405413686151545391743 67
86	67856658488653148822000936	18654459084131764615471846407 3	40274011541519206405367001276 77

$U_{r/1924630699}$

Paso	k	U_k	U_{k+1}
1	1	1	1
2	3	4	7
3	7	97	217
4	14	32689	75316
5	29	8878212019	20444528200
6	59	654446679283543409083	1507043869248741854800
7	119	13542930687763702320597012490 35	18533678882499307584826390125 69
8	238	96145803405859927877977650369 7	14940627356267588341925453750 31
9	476	39328069223320059312947262133 65	26854452545224650604236888874 94
	...	...	...
64	17173177240047209756	35301045189005237209295058162 4	78113005088022105770161736560 5
65	34346354480094419512	34768073999814584736973639433 48	37483813184935560879711028298 39
66	68692708960188839025	35099507732965667540031668104 88	26498201625755202378314839211 35
67	137385417920377678050	32053344302900082172252984979 25	90596773307235384766101897506 7
68	274770835840755356101	39377954452674118318882467260 46	25674091608830625304412104905 47
69	549541671681510712202	25468577898679394093924270016 10	19312360642903875991744744829 26
70	1099083343363021424404	35276966916880521616347440449 64	97022666979493773143228471934 7
71	2198166686726042848808	11156828841156271340465590459 31	25202951939904309201974264012 88

$U_{r/1013364453467}$

Paso	k	U_k	U_{k+1}
1	1	1	1
2	3	4	7
3	7	97	217
4	14	32689	75316
5	28	3855438727	8878212019
6	57	123415871987270197948	284199063321732815239
7	115	29779454787132425192400202211116	41541190894426182921798348496644
8	231	39539162101828654398439699875 21	962884849920108257985696431043
9	463	597170794771199642682597058711	31270432224220171215203240114 55
	...	...	...
54	16308063699334843	22632125989421584917977177663 93	40742403198843753067840028115 50
55	32616127398669687	52859949983908848973654633834 0	33811193690669687927119429095 49
56	65232254797339374	12319816818643814869841780557 92	73245508959633464570095300539 7
57	130464509594678749	30267057033800608966485042718 41	11558157114630419061187776256 79
58	260929019189357498	38832247088947258984813605296 15	78069311957702959168212148003 0
59	521858038378714997	29787103758026521853423384854 15	28640540296600525298189600803 86
60	1043716076757429994	16147430037731196981351969419 45	29595796455629696606333543061 18
61	2087432153514859988	36654646888323185846787600258 1	16007683932327593936312547097 19
62	4174864307029719976	20819790678060074150690911725 86	16318060436562462638332521985 42