Ejercicio 5

David García Curbelo

Dado tu número $n = 11781277$ de la lista publicada para este ejercicio:

Apartado I. ***Factoriza*** n ***aplicando el método*** ρ ***de Polard. ¿Cuántas iteraciones necesitas?***

Aplicando el método ρ de Polard, tenemos que para $n = 11781277$ obtenemos el primer factor primo 2591 en 58 iteraciones, como se puede ver en la tabla de la página siguiente. Por ello tenemos que nuestro número n se nos queda factorizado como producto de dos primos $n = 2591 \cdot 4547$ (el segundo sabemos que es primo por estar presente en la tabla de primos menores de 5 cifras).

Paso	x	y	mcd
1	2	5	1
2	5	677	1
3	26	6219991	1
4	677	5601822	1
5	458330	2597501	1
6	6219991	807607	1
7	11687876	8322365	1
8	5601822	1643871	1
9	584194	5993347	1
10	2597501	7806461	1
11	3701149	5941709	1
12	807607	341798	1
13	5790453	3285327	1
14	8322365	8668694	1
15	8711090	7679181	1
16	1643871	165755	1
17	5015321	7757667	1
18	5993347	9313459	1
19	1847739	356366	1
20	7806461	11451286	1
21	10307054	11732626	1
22	5941709	8156866	1
23	1588435	7512258	1
24	341798	11098752	1
25	2730073	4268072	1
26	3285327	7145982	1
27	3698488	10781441	1
28	8668694	6061976	1
29	4728818	3273655	1
30	7679181	10069807	1
31	5435394	11002644	1
32	165755	686311	1
33	782062	8650796	1
34	7757667	10952160	1
35	7142119	3070436	1
36	9313459	7757789	1
37	6598961	907115	1
38	356366	5241407	1
39	6341174	10800383	1
40	11451286	9833373	1
41	11498048	9739199	1
42	11732626	307635	1
43	10664402	11520196	1
44	8156866	4229214	1
45	7397659	3970356	1
46	7512258	540908	1
47	6924677	1648763	1
48	11098752	1744952	1
49	8683046	11158052	1
50	4268072	8127891	1
51	4255522	1144281	1
52	7145982	4961988	1
53	8964877	5443366	1
54	10781441	5449568	1
55	7110893	11084302	1
56	6061976	6817211	1
57	6432581	10456312	1
58	3273655	6610863	2591

Apartado II. ***Sea*** p_1 ***el mayor de sus factores primos y*** p_2 ***el siguiente primo. Calcula las partes enteras de*** $\sqrt{p_1}$ ***y*** $\sqrt{p_2}$ ***con el algoritmo entero.***

Tenemos que $p_1 = 4547$ y $p_2 = 2591$. Por lo tanto, como ambos son impares, para proceder con el algoritmo consideramos los primeros a como $a_{p_1} = (4547+1)/2 = 2274$ y $a_{p_2} = (2591+1)/2 = 1296$. Tenemos por tanto las siguentes tablas de iteraciones para ambos números p_1 y p_2 respectivamente:

$\sqrt{4547}$

Paso	a	a^2+n	cociente
1	1296	1682207	648
2	648	422495	325
3	325	108216	166
4	166	30147	90
5	90	10691	59
6	59	6072	51
7	51	5192	50
8	50	5091	50

$\sqrt{2591}$

Paso	a	a^2+n	cociente
1	2274	5175623	1137
2	1137	1297316	570
3	570	329447	288
4	288	87491	151
5	151	27348	90
6	90	12647	70
7	70	9447	67
8	67	9036	67

Con lo que hemos obtenido, en la última iteración de cada tabla, las respectivas partes enteras de la raíz cuadrada de ambos primos, siendo para p_1 el valor 50 y para p_2 el 67.

Apartado III. ***Calcula las FCS de $\sqrt{p_1}$ y $\sqrt{p_2}$ aplicando el algoritmo que usa aritmética entera.***

La fracción continua simple de $\sqrt{4547}$ es la siguiente: {58{67 {2, 3, 6, 1, 4, 3, 11, 1, 18, 2, 1, 7, 3, 1, 5, 9, 2, 5, 1, 1, 1, 9, 1, 2, 1, 1, 1, 4, 67, 4, 1, 1, 1, 2, 1, 9, 1, 1, 1, 5, 2, 9, 5, 1, 3, 7, 1, 2, 18, 1, 11, 3, 4, 1, 6, 3, 2, 134}}}

La cual podemos ver que su período tiene una longitud de 58. A continuación se muestran los sucesivos convergentes:

{67, 1}
{135, 2}
{472, 7}
{2967, 44}
{3439, 51}
{16723, 248}
{53608, 795}
{606411, 8993}
{660019, 9788}
{12486753, 185177}
{25633525, 380142}
{38120278, 565319}
{292475471, 4337375}
{915546691, 13577444}
{1208022162, 17914819}
{6955657501, 103151539}
{63808939671, 946278670}
{134573536843, 1995708879}
{736676623886, 10924823065}
{871250160729, 12920531944}
{1607926784615, 23845355009}
{2479176945344, 36765886953}
{23920519292711, 354738337586}
{26399696238055, 391504224539}
{76719911768821, 1137746786664}
{103119608006876, 1529251011203}
{179839519775697, 2666997797867}
{282959127782573, 4196248809070}
{1311676030905989, 19451993034147}
{88165253198483836, 1307479782096919}
{353972688824841333, 5249371121421823}
{442137942023325169, 6556850903518742}
{796110630848166502, 11806222024940565}
{1238248572871491671, 18363072928459307}
{3272607776591149844, 48532367881859179}
{4510856349462641515, 66895440810318486}
{43870314921754923479, 650591335174725553}
{48381171271217564994, 717486775985044039}
{92251486192972488473, 1368078111159769592}
{140632657464190053467, 2085564887144813631}
{795414773513922755808, 11795902546883837747}
{1731462204492035565083, 25677369980912489125}
{16378574613942242841555, 242892232375096239872}
{8362433527420324977 2858, 1240138531856393688485}
{10000290988814549261 4413, 1483030764231489928357}
{38363306493863972761 6097, 5689230824550863473556}
{27854343644586235859270 92, 41307646536087534243249}

{3169067429397263313543189, 46996877360638397716805}
{9123569223253150213013470, 135301401257364329676859}
{167393313447953967147785649, 2482422099993196331900267}
{176516882671207117360799119, 2617723501250560661577126}
{210907902283123225811657595 8, 31277380613749363609248653}
{650375395116490389171052699 3, 96449865342498651489323085}
{281240948274908478249586839 30, 41707684198374396956654099 3}
{346278487786557517166692109 23, 51352670732624262105586407 8}
{235891187499425358124973949468, 34982370859411996959017254 61}
{742301411276931826091591059327, 11008237965149841708761040461}
{172049401005328901030815606 8122, 25514713016240883113423806383}

La fracción continua simple de $\sqrt{2591}$ es la siguiente: {48 {50 {1, 9, 5, 3, 1, 7, 14, 2, 2, 2, 2, 1, 6, 1, 1, 3, 2, 1, 1, 1, 2, 19, 1, 49, 1, 19, 2, 1, 1, 1, 2, 3, 1, 1, 6, 1, 2, 2, 2, 2, 14, 7, 1, 3, 5, 9, 1, 100}}} La cual podemos ver que su período tiene una longitud de 48. A continuación se muestran los sucesivos convergentes:
{50, 1}
{51, 1}
{509, 10}
{2596, 51}
{8297, 163}
{10893, 214}
{84548, 1661}
{1194565, 23468}
{2473678, 48597}
{6141921, 120662}
{14757520, 289921}
{35656961, 700504}
{50414481, 990425}
{338143847, 6643054}
{388558328, 7633479}
{726702175, 14276533}
{2568664853, 50463078}
{5864031881, 115202689}
{8432696734, 165665767}
{14296728615, 280868456}
{22729425349, 446534223}
{59755579313, 1173936902}
{1158085432296, 22751335361}
{1217841011609, 23925272263}
{60832295001137, 1195089676248}
{62050136012746, 1219014948511}
{1239784879243311, 24356373697957}
{2541619894499368, 49931762344425}
{3781404773742679, 74288136042382}
{6323024668242047, 124219898386807}
{10104429441984726, 198508034429189}
{26531883552211499, 521235967245185}
{89700080098619223, 1762215936164744}
{116231963650830722, 2283451903409929}
{205932043749449945, 4045667839574673}
{1351824226147530392, 26557458940857967}
{1557756269896980337, 30603126780432640}
{4467336765941491066, 87763712501723247}

{10492429801779962469, 206130551783879134}
{25452196369501416004, 500024816069481515}
{61396822540782794477, 1206180183922842164}
{885007711940460538682, 17386547390989271811}
{6256450806124006565251, 122912011920847744841}
{7141458518064467103933, 140298559311837016652}
{27680826360317407877050, 543807689856358794797}
{145545590319651506489183, 2859337008593630990637}
{133759113923718096627 9697, 26277840767199037710530}
{14831367295568324727688 80, 29137177775792668701167}