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.

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.