Ejercicio 5

Ana Buendía Ruiz-Azuaga

March 13, 2022

1 Ejercicio 5

1.1 Apartado 1

Dado tu número n de la lista publicada para este ejercicio.

$n = 55325267$

Factoriza n aplicando el método ρ de Polard. ¿Cúantas iteraciones necesitas? Sea p1 el mayor de sus factores primos y p2 el siguiente primo.

Como $2^{n-1} \equiv 27708036 \mod n \not\equiv 1 \mod n$ tenemos que n es compuesto. Aplicamos, por tanto, el método ρ de Polard a n:

```
Paso: 0, x: 1, y: 1, g: -
Paso: 1, x: 2, y: 5, g: 1
Paso: 2, x: 5, y: 677, g: 1
Paso: 3, x: 26, y: 51675369, g: 1
. . .
Paso: 81, x: 11396938, y: 25996135, g: 1
Paso: 82, x: 23550260, y: 19416314, g: 7103
```

Como la descomposición es $55325267 = 7103 \cdot 7789$ donde mirando en la lista vemos que 7103 y 7789 son primos, por tanto hemos terminado la descomposición de n. Se han necesitado 82 iteraciones.

Además, tenemos $p_1 = 7789$ y $p_2 = 7103$.

1.2 Apartado 2

Calcula las partes enteras de $\sqrt{p_1}$ y $\sqrt{p_2}$ con el algoritmo entero.

Comenzamos comprobando que los números dados no son cuadrados perfectos:

$$\sqrt{p_1} = 88.25531145489205$$

$$\sqrt{p_2} = 84.27929757656977$$

Ahora aplicamos el algoritmo entero a p_1:

```
Paso: 1, a_i: 3895, a_i^2+n: 15178814
Paso: 2, a_i: 1948.0, a_i^2+n: 3802493.0
```

```
Paso: 3, a_i: 975.0, a_i^2+n: 958414.0
Paso: 4, a_i: 491.0, a_i^2+n: 248870.0
Paso: 5, a_i: 253.0, a_i^2+n: 71798.0
Paso: 6, a_i: 141.0, a_i^2+n: 27670.0
Paso: 7, a_i: 98.0, a_i^2+n: 17393.0
Paso: 8, a_i: 88.0, a_i^2+n: 15533.0
```

de donde obtenemos que la parte entera de $\sqrt{p_1}$ es 88.

Y aplicamos el algoritmo entero a p_2:

```
Paso: 1, a_i: 3552, a_i^2+n: 12623807
Paso: 2, a_i: 1776.0, a_i^2+n: 3161279.0
Paso: 3, a_i: 889.0, a_i^2+n: 797424.0
Paso: 4, a_i: 448.0, a_i^2+n: 207807.0
Paso: 5, a_i: 231.0, a_i^2+n: 60464.0
Paso: 6, a_i: 130.0, a_i^2+n: 24003.0
Paso: 7, a_i: 92.0, a_i^2+n: 15567.0
Paso: 8, a_i: 84.0, a_i^2+n: 14159.0
```

de donde se tiene que la parte entera de $\sqrt{p_2}$ es 84.

1.3 Apartado 3

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

Aplicamos el algoritmo de aritmética entera para $\sqrt{p_1}$:

```
Paso: 0, P: 0, Q: 1, q: 88
Paso: 1, P: 88, Q: 45, q: 3
Paso: 2, P: 47, Q: 124, q: 1
Paso: 3, P: 77, Q: 15, q: 11
Paso: 4, P: 88, Q: 3, q: 58
Paso: 5, P: 86, Q: 131, q: 1
Paso: 6, P: 45, Q: 44, q: 3
Paso: 7, P: 87, Q: 5, q: 35
Paso: 8, P: 88, Q: 9, q: 19
Paso: 9, P: 83, Q: 100, q: 1
Paso: 10, P: 17, Q: 75, q: 1
Paso: 11, P: 58, Q: 59, q: 2
Paso: 12, P: 60, Q: 71, q: 2
Paso: 13, P: 82, Q: 15, q: 11
Paso: 14, P: 83, Q: 60, q: 2
Paso: 15, P: 37, Q: 107, q: 1
Paso: 16, P: 70, Q: 27, q: 5
Paso: 17, P: 65, Q: 132, q: 1
Paso: 18, P: 67, Q: 25, q: 6
Paso: 19, P: 83, Q: 36, q: 4
Paso: 20, P: 61, Q: 113, q: 1
Paso: 21, P: 52, Q: 45, q: 3
Paso: 22, P: 83, Q: 20, q: 8
Paso: 23, P: 77, Q: 93, q: 1
```

```
Paso: 24, P: 16, Q: 81, q: 1
Paso: 25, P: 65, Q: 44, q: 3
Paso: 26, P: 67, Q: 75, q: 2
Paso: 27, P: 83, Q: 12, q: 14
Paso: 28, P: 85, Q: 47, q: 3
Paso: 29, P: 56, Q: 99, q: 1
Paso: 30, P: 43, Q: 60, q: 2
Paso: 31, P: 77, Q: 31, q: 5
Paso: 32, P: 78, Q: 55, q: 3
Paso: 33, P: 87, Q: 4, q: 43
Paso: 34, P: 85, Q: 141, q: 1
Paso: 35, P: 56, Q: 33, q: 4
Paso: 36, P: 76, Q: 61, q: 2
Paso: 37, P: 46, Q: 93, q: 1
Paso: 38, P: 47, Q: 60, q: 2
Paso: 39, P: 73, Q: 41, q: 3
Paso: 40, P: 50, Q: 129, q: 1
Paso: 41, P: 79, Q: 12, q: 13
Paso: 42, P: 77, Q: 155, q: 1
Paso: 43, P: 78, Q: 11, q: 15
Paso: 44, P: 87, Q: 20, q: 8
Paso: 45, P: 73, Q: 123, q: 1
Paso: 46, P: 50, Q: 43, q: 3
Paso: 47, P: 79, Q: 36, q: 4
Paso: 48, P: 65, Q: 99, q: 1
Paso: 49, P: 34, Q: 67, q: 1
Paso: 50, P: 33, Q: 100, q: 1
Paso: 51, P: 67, Q: 33, q: 4
Paso: 52, P: 65, Q: 108, q: 1
Paso: 53, P: 43, Q: 55, q: 2
Paso: 54, P: 67, Q: 60, q: 2
Paso: 55, P: 53, Q: 83, q: 1
Paso: 56, P: 30, Q: 83, q: 1
Paso: 57, P: 53, Q: 60, q: 2
Paso: 58, P: 67, Q: 55, q: 2
Paso: 59, P: 43, Q: 108, q: 1
Paso: 60, P: 65, Q: 33, q: 4
Paso: 61, P: 67, Q: 100, q: 1
Paso: 62, P: 33, Q: 67, q: 1
Paso: 63, P: 34, Q: 99, q: 1
Paso: 64, P: 65, Q: 36, q: 4
Paso: 65, P: 79, Q: 43, q: 3
Paso: 66, P: 50, Q: 123, q: 1
Paso: 67, P: 73, Q: 20, q: 8
Paso: 68, P: 87, Q: 11, q: 15
Paso: 69, P: 78, Q: 155, q: 1
Paso: 70, P: 77, Q: 12, q: 13
Paso: 71, P: 79, Q: 129, q: 1
Paso: 72, P: 50, Q: 41, q: 3
Paso: 73, P: 73, Q: 60, q: 2
```

```
Paso: 74, P: 47, Q: 93, q: 1
Paso: 75, P: 46, Q: 61, q: 2
Paso: 76, P: 76, Q: 33, q: 4
Paso: 77, P: 56, Q: 141, q: 1
Paso: 78, P: 85, Q: 4, q: 43
Paso: 79, P: 87, Q: 55, q: 3
Paso: 80, P: 78, Q: 31, q: 5
Paso: 81, P: 77, Q: 60, q: 2
Paso: 82, P: 43, Q: 99, q: 1
Paso: 83, P: 56, Q: 47, q: 3
Paso: 84, P: 85, Q: 12, q: 14
Paso: 85, P: 83, Q: 75, q: 2
Paso: 86, P: 67, Q: 44, q: 3
Paso: 87, P: 65, Q: 81, q: 1
Paso: 88, P: 16, Q: 93, q: 1
Paso: 89, P: 77, Q: 20, q: 8
Paso: 90, P: 83, Q: 45, q: 3
Paso: 91, P: 52, Q: 113, q: 1
Paso: 92, P: 61, Q: 36, q: 4
Paso: 93, P: 83, Q: 25, q: 6
Paso: 94, P: 67, Q: 132, q: 1
Paso: 95, P: 65, Q: 27, q: 5
Paso: 96, P: 70, Q: 107, q: 1
Paso: 97, P: 37, Q: 60, q: 2
Paso: 98, P: 83, Q: 15, q: 11
Paso: 99, P: 82, Q: 71, q: 2
Paso: 100, P: 60, Q: 59, q: 2
Paso: 101, P: 58, Q: 75, q: 1
Paso: 102, P: 17, Q: 100, q: 1
Paso: 103, P: 83, Q: 9, q: 19
Paso: 104, P: 88, Q: 5, q: 35
Paso: 105, P: 87, Q: 44, q: 3
Paso: 106, P: 45, Q: 131, q: 1
Paso: 107, P: 86, Q: 3, q: 58
Paso: 108, P: 88, Q: 15, q: 11
Paso: 109, P: 77, Q: 124, q: 1
Paso: 110, P: 47, Q: 45, q: 3
Paso: 111, P: 88, Q: 1, q: 176
```

La longitud del período de p_1 es 111, luego tenemos que: La FCS de $\sqrt{p_1}$ es {111, {88, {3, 1, 11, 58, 1, 3, 35, 19, 1, 1, 2, 2, 11, 2, 1, 5, 1, 6, 4, 1, 3, 8, 1, 1, 3, 2, 14, 3, 1, 2, 5, 3, 43, 1, 4, 2, 1, 2, 3, 1, 13, 1, 15, 8, 1, 3, 4, 1, 1, 1, 4, 1, 2, 2, 1, 1, 2, 2, 1, 4, 1, 1, 1, 4, 3, 1, 8, 15, 1, 13, 1, 3, 2, 1, 2, 4, 1, 43, 3, 5, 2, 1, 3, 14, 2, 3, 1, 1, 8, 3, 1, 4, 6, 1, 5, 1, 2, 11, 2, 2, 1, 1, 19, 35, 3, 1, 58, 11, 1, 3, 176}}}

Aplicamos ahora el mismo algoritmo a $\sqrt{p_2}$:

```
Paso: 0, P: 0, Q: 1, q: 84
Paso: 1, P: 84, Q: 47, q: 3
Paso: 2, P: 57, Q: 82, q: 1
Paso: 3, P: 25, Q: 79, q: 1
```

```
Paso: 4, P: 54, Q: 53, q: 2
Paso: 5, P: 52, Q: 83, q: 1
Paso: 6, P: 31, Q: 74, q: 1
Paso: 7, P: 43, Q: 71, q: 1
Paso: 8, P: 28, Q: 89, q: 1
Paso: 9, P: 61, Q: 38, q: 3
Paso: 10, P: 53, Q: 113, q: 1
Paso: 11, P: 60, Q: 31, q: 4
Paso: 12, P: 64, Q: 97, q: 1
Paso: 13, P: 33, Q: 62, q: 1
Paso: 14, P: 29, Q: 101, q: 1
Paso: 15, P: 72, Q: 19, q: 8
Paso: 16, P: 80, Q: 37, q: 4
Paso: 17, P: 68, Q: 67, q: 2
Paso: 18, P: 66, Q: 41, q: 3
Paso: 19, P: 57, Q: 94, q: 1
Paso: 20, P: 37, Q: 61, q: 1
Paso: 21, P: 24, Q: 107, q: 1
Paso: 22, P: 83, Q: 2, q: 83
Paso: 23, P: 83, Q: 107, q: 1
Paso: 24, P: 24, Q: 61, q: 1
Paso: 25, P: 37, Q: 94, q: 1
Paso: 26, P: 57, Q: 41, q: 3
Paso: 27, P: 66, Q: 67, q: 2
Paso: 28, P: 68, Q: 37, q: 4
Paso: 29, P: 80, Q: 19, q: 8
Paso: 30, P: 72, Q: 101, q: 1
Paso: 31, P: 29, Q: 62, q: 1
Paso: 32, P: 33, Q: 97, q: 1
Paso: 33, P: 64, Q: 31, q: 4
Paso: 34, P: 60, Q: 113, q: 1
Paso: 35, P: 53, Q: 38, q: 3
Paso: 36, P: 61, Q: 89, q: 1
Paso: 37, P: 28, Q: 71, q: 1
Paso: 38, P: 43, Q: 74, q: 1
Paso: 39, P: 31, Q: 83, q: 1
Paso: 40, P: 52, Q: 53, q: 2
Paso: 41, P: 54, Q: 79, q: 1
Paso: 42, P: 25, Q: 82, q: 1
Paso: 43, P: 57, Q: 47, q: 3
Paso: 44, P: 84, Q: 1, q: 168
```

La longitud del período de p_2 es 44, luego tenemos que: La FCS de $\sqrt{p_2}$ es {44, {84, {3, 1, 1, 2, 1, 1, 1, 1, 3, 1, 4, 1, 1, 1, 8, 4, 2, 3, 1, 1, 1, 83, 1, 1, 1, 3, 2, 4, 8, 1, 1, 1, 4, 1, 3, 1, 1, 1, 1, 2, 1, 1, 3, 168}}}