Ejercicio 4

Ana Buendía Ruiz-Azuaga

March 6, 2022

1 Ejercicio 4

1.1 Apartado 1

Dado tu número n de 8 cifras de la lista del ejercicio 2.

$$n = 77770081$$

Factoriza n-1 aplicando el método ρ de Polard. ¿Cúantas iteraciones necesitas?

Se ha programado el método ρ de Polard, y se ha aplicado recursivamente al número dado. Se ha tomado como $f(x) = x^2 + 1$ y como $x_0 = 1$.

Comenzamos aplicando el metodo ρ de Polard a nuestro número $n - 1$, que al ser par es claramente compuesto.

```
Paso: 0, x: 1, y: 1, g: -
Paso: 1, x: 2, y: 5, g: 3
```

Como la descomposición es $77770080 = 3 \cdot 25923360$, con 3 claramente primo y 25923360 es claramente compuesto al ser par. Para esto solo hemos necesitado 1 iteración.. Ahora aplicamos el método de nuevo a 25923360.

```
Paso: 0, x: 1, y: 1, g: -
Paso: 1, x: 2, y: 5, g: 3
```

Como la descomposición es $25923360 = 3 \cdot 8641120$ con 3 claramente primo y 8641120 es claramente compuesto al ser par. De nuevo, solo ha sido necesaria 1 iteración. Volvemos a aplicar el método de nuevo a 8641120.

```
Paso: 0, x: 1, y: 1, g: -
Paso: 1, x: 2, y: 5, g: 1
Paso: 2, x: 5, y: 677, g: 32
```

Como la descomposición es $8641120 = 32 \cdot 270035$, con 32 compuesto, pues es $32 = 2^5$. Dado que es una potencia de 2 y por tanto se descompone rápidamente a mano, no se le va a aplicar el algoritmo, y el cofactor 270035 es claramente compuesto al ser múltiplo de 5. En esta ocasión se han necesitado 2 iteraciones. Se le aplica el método de nuevo a 270035.

```
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: 221631, g: 5
```

Como la descomposición es $270035 = 5 \cdot 54007$, con 5 evidentemente primo y el cofactor es compuesto ya que $2^{54007-1} \equiv 29823 \mod 54007 \not\equiv 1 \mod 54007$, de modo que aplicamos el algoritmo de nuevo a 54007. En esta descomposición se han necesitado 3 iteraciones.

```
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: 5603, g: 1
Paso: 4, x: 677, y: 11539, g: 1
Paso: 5, x: 26274, y: 30672, g: 1
Paso: 6, x: 5603, y: 12599, g: 53
```

La descomposición de este número es $54007 = 53 * 1019$, para la que se han necesitado 6 iteraciones, donde mirando en la lista vemos que tanto 53 como 1019 son primos, luego la descomposición en factores de nuestro número es:
$n - 1 = 3^2 \cdot 2^5 \cdot 5 \cdot 53 \cdot 1019$ y el total de iteraciones es 13.

1.2 Apartado 2

Si es necesario aplica recursivamente Lucas-Lehmer para certificar factores primos de n-1 mayores de 4 cifras.

No ha resultado ningún factor mayor de 4 cifras, por lo que no es necesario.

1.3 Apartado 3

Aplica Lucas-Lehmer para encontrar un certificado de primalidad de n.

NOTA: Debes encontrar el natural más pequeño cuya clase sea primitiva.

Como ya conocemos los factores de n-1 pues los hemos calculado en el primer apartado, $n - 1 = 3^2 \cdot 2^5 \cdot 5 \cdot 53 \cdot 1019$, buscamos un elemento primitivo para n.

Vamos probando hasta encontrar que $a = 17$ es un elemento primitivo para $n = 77770081$ porque $17^{n-1} \equiv 1 \mod n$ y $17^{\frac{n-1}{p}} \not\equiv 1 \mod n$ para $p \in \{2, 3, 5, 53, 1019\}$ pues:

$$\begin{aligned}
17^{\frac{n-1}{2}} &\equiv 77770080 \mod n \\
17^{\frac{n-1}{3}} &\equiv 58134188 \mod n \\
17^{\frac{n-1}{5}} &\equiv 66432901 \mod n \\
17^{\frac{n-1}{53}} &\equiv 68065795 \mod n \\
17^{\frac{n-1}{1019}} &\equiv 65224721 \mod n
\end{aligned}$$

luego por el Teorema de Lucas-Lehmer para $a = 17$ tenemos que n es primo.