Ejercicio 8

Ana Buendía Ruiz-Azuaga

March 21, 2022

1 Ejercicio 8

1.1 Apartado 1

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

$n = 28448719846467310644423731752992768000091$

Pasa algunos tests de primalidad para ver si n es compuesto.

Comenzamos pasando el test de Fermat para las bases $\{2, 3, 5, 7, 11\}$:

$$2^{n-1} \equiv 1 \mod n$$
$$3^{n-1} \equiv 1 \mod n$$
$$5^{n-1} \equiv 1 \mod n$$
$$7^{n-1} \equiv 1 \mod n$$
$$11^{n-1} \equiv 1 \mod n$$

Luego n es posible primo de Fermat para todas las bases.

Ahora vamos a pasarle el test de Miller-Rabin:

Como $\frac{n-1}{2}$ es impar, las a-sucesiones solo tendrán 2 términos:

```
La a-sucesion obtenida para la base 2 es:
[28448719846467310644423731752992768000090, 1]

La a-sucesion obtenida para la base 3 es:
[28448719846467310644423731752992768000090, 1]

La a-sucesion obtenida para la base 5 es:
[1, 1]

La a-sucesion obtenida para la base 7 es:
[1, 1]

La a-sucesion obtenida para la base 11 es:
[28448719846467310644423731752992768000090, 1]
```

Como $28448719846467310644423731752992768000090 \equiv -1 \mod n$ tenemos que n pasa el test de Miller-Rabin para los 5 primeros primos, pues las sucesiones acaban en 1 y todo 1 va precedido de otro 1 o de -1.

Luego tenemos que n es posible primo.

1.2 Apartado 2

En caso que tu n sea probable primo. Factoriza n + 1 encontrando certificadosde primalidad para los factores mayores de 10000.

Aplicando ρ de Polard a $n+1$ obtenemos:

$$n+1 = 2^2 \cdot 31 \cdot 63929 \cdot 600702031 \cdot 352173733409 \cdot 1696395339263.$$

Primero se han extraído los factores 2 y se ha aplicado el algoritmo a 711217996161682766110593293824819200023, necesitando un total de 602931 iteraciones hasta descomponer el número.

Vamos a comprobar ahora mediante Lucas-Lehmer que los primos obtenidos mayores de 10000 son, en efecto, primos.

1.2.1 1696395339263

Consideramos $p_1 = 1696395339263$, luego aplicando ρ de Polard a $p_1 - 1$:

$$p_1 - 1 = 2 \cdot 13 \cdot 757 \cdot 1621 \cdot 53171$$

.

De nuevo, primero se ha extraído el factor 2 y se ha aplicado el método a 848197669631, empleando 74 iteraciones en total.

Y por Lucas-Lehmer tenemos que $a = 5$ es un elemento primitivo para p_1 porque $5^{p_1-1} \equiv 1 \mod p_1$ y $5^{\frac{p_1-1}{p}} \not\equiv 1 \mod p_1$ para $p \in \{2, 13, 757, 1621, 53171\}$ pues:

```
5^(n-1)/ 2 = 1696395339262 mod n
5^(n-1)/ 13 = 1336486042586 mod n
5^(n-1)/ 757 = 1437998311805 mod n
5^(n-1)/ 1621 = 274109562190 mod n
5^(n-1)/ 53171 = 40822449061 mod n
```

Nota: En estos códigos aunque la salida referencie a n, esto es por el print del programa y se refiere al p_i correspondiente a cada apartado. Se ha dejado la salida estándar del programa por simplicidad.

Consideramos ahora $p_2 = 53171$, luego aplicando ρ de Polard a $p_2 - 1$:

$$p_2 - 1 = 2 \cdot 5 \cdot 13 \cdot 409$$

.

Se extra el factor 2 y se aplica el algoritmo a 26585, necesitando 7 iteraciones en total.

Y por Lucas-Lehmer tenemos que $a = 2$ es un elemento primitivo para p_2 porque $2^{p_2-1} \equiv 1 \mod p_2$ y $2^{\frac{p_2-1}{p}} \not\equiv 1 \mod p_2$ para $p \in \{2, 5, 13, 409\}$ pues:

```
2^(n-1)/ 2 = 53170 mod n
2^(n-1)/ 5 = 25877 mod n
2^(n-1)/ 13 = 39138 mod n
2^(n-1)/ 409 = 30600 mod n
```

1.2.2 352173733409

Consideramos $p_3 = 352173733409$, luego aplicando ρ de Polard a $p_3 - 1$:

$$p_3 - 1 = 2^5 \cdot 7 \cdot 349 \cdot 4504883$$

.

Primero se ha extraído el factor 2 y se aplica el método a 11005429169, requiriendo 31 iteraciones en total.

Y por Lucas-Lehmer tenemos que $a = 15$ es un elemento primitivo para p_3 porque $15^{p_3-1} \equiv 1 \mod p_3$ y $15^{\frac{p_3-1}{p}} \not\equiv 1 \mod p_3$ para $p \in \{2, 7, 349, 4504883\}$ pues:

```
15^(n-1)/ 2 = 352173733408 mod n
15^(n-1)/ 7 = 72307373439 mod n
15^(n-1)/ 349 = 60311719490 mod n
15^(n-1)/ 4504883 = 173110241247 mod n
```

Consideramos ahora $p_4 = 4504883$, luego aplicando ρ de Polard a $p_4 - 1$:

$$p_4 - 1 = 2 \cdot 2252441$$

.

Primero se ha extraído el factor 2, y se va a comprobar que 2252441 es primo.

Y por Lucas-Lehmer tenemos que $a = 2$ es un elemento primitivo para p_4 porque $2^{p_4-1} \equiv 1 \mod p_4$ y $2^{\frac{p_4-1}{p}} \not\equiv 1 \mod p_4$ para $p \in \{2, 2252441\}$ pues:

```
2^(n-1)/ 2 = 4504882 mod n
2^(n-1)/ 2252441 = 4 mod n
```

Ahora comprobamos $p_5 = 2252441$, luego aplicando ρ de Polard a $p_5 - 1$:

$$p_5 - 1 = 2^3 \cdot 5 \cdot 56311$$

.

De nuevo, se extraen los factor 2 y se aplica el método a 281555, para lo que se necesitan 3 iteraciones en total.

Y por Lucas-Lehmer tenemos que $a = 3$ es un elemento primitivo para p_5 porque $3^{p_5-1} \equiv 1 \mod p_5$ y $3^{\frac{p_5-1}{p}} \not\equiv 1 \mod p_5$ para $p \in \{2, 5, 56311\}$ pues:

```
3^(n-1)/ 2 = 2252440 mod n
3^(n-1)/ 5 = 2075174 mod n
3^(n-1)/ 56311 = 1333115 mod n
```

Finalmente consideramos $p_6 = 56311$, luego aplicando ρ de Polard a $p_6 - 1$:

$$p_6 - 1 = 2 \cdot 3 \cdot 5 \cdot 1877$$

.

Se extrae el factor 2 y se aplica el método a 28155, necesitando este 4 iteraciones en total.

Y por Lucas-Lehmer tenemos que $a = 6$ es un elemento primitivo para p_6 porque $6^{p_6-1} \equiv 1 \mod p_6$ y $6^{\frac{p_6-1}{p}} \not\equiv 1 \mod p_6$ para $p \in \{2, 3, 5, 1877\}$ pues:

```
6^(n-1)/ 2 = 56310 mod n
6^(n-1)/ 3 = 14180 mod n
6^(n-1)/ 5 = 15485 mod n
6^(n-1)/ 1877 = 46171 mod n
```

1.2.3 600702031

Consideramos $p_7 = 600702031$, luego aplicando ρ de Polard a $p_7 - 1$:

$$p_7 - 1 = 2 \cdot 3^2 \cdot 5 \cdot 37 \cdot 180391$$

.

Primero sacamos el factor 2, y aplicamos el método a 300351015, necesitando este número 9 iteraciones en total.

Y por Lucas-Lehmer tenemos que $a = 3$ es un elemento primitivo para p_7 porque $3^{p_7-1} \equiv 1 \mod p_7$ y $3^{\frac{p_7-1}{p}} \not\equiv 1 \mod p_7$ para $p \in \{2, 3, 5, 37, 180391\}$ pues:

```
3^(n-1)/ 2 = 600702030 mod n
3^(n-1)/ 3 = 267084186 mod n
3^(n-1)/ 5 = 455572699 mod n
3^(n-1)/ 37 = 27995379 mod n
3^(n-1)/ 180391 = 132564421 mod n
```

Consideramos ahora $p_8 = 180391$, luego aplicando ρ de Polard a $p_8 - 1$:

$$p_8 - 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 859$$

.

Sacamos el factor 2 y aplicamos el algoritmo a 90195, que requiere de 6 iteraciones totales.

Y por Lucas-Lehmer tenemos que $a = 7$ es un elemento primitivo para p_8 porque $7^{p_8-1} \equiv 1 \mod p_8$ y $7^{\frac{p_8-1}{p}} \not\equiv 1 \mod p_8$ para $p \in \{2, 3, 5, 7, 859\}$ pues:

```
7^(n-1)/ 2 = 180390 mod n
7^(n-1)/ 3 = 83653 mod n
7^(n-1)/ 5 = 65181 mod n
7^(n-1)/ 7 = 129133 mod n
7^(n-1)/ 859 = 123807 mod n
```

1.2.4 63929

Consideramos $p_9 = 63929$, luego aplicando ρ de Polard a $p_9 - 1$:

$$p_9 - 1 = 2^3 \cdot 61 \cdot 131$$

.

Primero extraemos los factores 2 y aplicamos el algoritmo a 7991, que necesita un total de 7 iteraciones.

Y por Lucas-Lehmer tenemos que $a = 3$ es un elemento primitivo para p_9 porque $3^{p_9-1} \equiv 1 \mod p_9$ y $3^{\frac{p_9-1}{p}} \not\equiv 1 \mod p_9$ para $p \in \{2, 61, 131\}$ pues:

```
3^(n-1)/ 2 = 63928 mod n
3^(n-1)/ 61 = 46509 mod n
3^(n-1)/ 131 = 18863 mod n
```

Luego hemos comprobado la correcta descomposición en primos de $n+1$:

$$n + 1 = 2^2 \cdot 31 \cdot 63929 \cdot 600702031 \cdot 352173733409 \cdot 1696395339263.$$

1.3 Apartado 3

Con P = 1, encuentra el menor Q natural mayor o igual que 2, tal que defina una s.L. que certifique la primalidad de n.

Calculamos para cada Q los valores de $U_{\frac{r}{p}}$ con p siendo uno de los divisores de r calculados en el apartado anterior.

```
Q: 2



U[28448719846467310644423731752992768000092] = 0,
V[28448719846467310644423731752992768000092] = 4,

U[28448719846467310644423731752992768000093] = 2

Factor: 2



U[14224359923233655322211865876496384000046] = 2401816336829289298745644029101509733749,
V[14224359923233655322211865876496384000046] = 0,

U[14224359923233655322211865876496384000047] = 26233441607380101815940086022003932669 20

Factor: 31



U[917700640208622924013668766225573161 32] = 14709162085002423447574441670061915715 94,
V[917700640208622924013668766225573161 32] = 18252175823827472519030536953483262572 6,

U[917700640208622924013668766225573161 33] = 82671898336925853497387476827051209866 0

Factor: 63929



U[445004924939656660426781769666235 48] = 16419577734776976826728447366518627121 36,
V[445004924939656660426781769666235 48] = 25544324091929478193861173986915821825 60,

U[445004924939656660426781769666235 49] = 20981950913353227510294810676717224473 48
```

```
Factor: 600702031


U[4735912045961987207668310972132] = 2620483833716315257803347661958638569554,
V[4735912045961987207668310972132] = 1027357537502469853234616045712241448265,

U[4735912045961987207668310972133] = 401484693286027023297795266185801608864

Factor: 352173733409


U[8078035681732159367529888988] = 1364026177403439785504998557789553591298,
V[8078035681732159367529888988] = 293516842564476323241204311857622760584,

U[8078035681732159367529888989] = 828771509983958054373101434823588175941

Factor: 1696395339263


U[16770100216631622226328754084] = 1648554338650375930190024551175446944533,
V[16770100216631622226328754084] = 1877548978459566186099302960294216193767,

U[16770100216631622226328754085] = 1763051658554971058144663755734831569150
```

Para P=1, Q=2 tenemos que ningún $U_{\frac{r}{p}} \not\equiv 0 \mod n$ y $U_r \equiv 0 \mod n$, luego tenemos que el rango de n es $n+1$ y $(n, 2Qd) = 1$, y por tanto n es primo.