

Ejercicio 8

Ana Buendía Ruiz-Azuaga

March 20, 2022

1 Ejercicio 8

1.1 Apartado 1

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

$n = 2844871984646731064442373175299276800091$

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

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

$$2^{n-1} \equiv 1 \pmod{n}$$

$$3^{n-1} \equiv 1 \pmod{n}$$

$$5^{n-1} \equiv 1 \pmod{n}$$

$$7^{n-1} \equiv 1 \pmod{n}$$

$$11^{n-1} \equiv 1 \pmod{n}$$

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:

[2844871984646731064442373175299276800090, 1]

La a-sucesion obtenida para la base 3 es:

[2844871984646731064442373175299276800090, 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:

[2844871984646731064442373175299276800090, 1]

Como $2844871984646731064442373175299276800090 \equiv -1 \pmod{n}$ 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.

1.2 Apartado 2

En caso que tu n sea probable primo. Factoriza $n + 1$ encontrando certificados de 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 más de 1000 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 $5^{p_1-1} \equiv 1 \pmod{p_1}$ y $5^{\frac{p_1-1}{p}} \not\equiv 1 \pmod{p_1}$ para $p \in \{2, 13, 757, 1621, 53171\}$ pues:

$$\begin{aligned} 5^{(n-1)/2} &= 1696395339262 \pmod{n} \\ 5^{(n-1)/13} &= 1336486042586 \pmod{n} \\ 5^{(n-1)/757} &= 1437998311805 \pmod{n} \\ 5^{(n-1)/1621} &= 274109562190 \pmod{n} \\ 5^{(n-1)/53171} &= 40822449061 \pmod{n} \end{aligned}$$

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 extrae 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 $2^{p_2-1} \equiv 1 \pmod{p_2}$ y $2^{\frac{p_2-1}{p}} \not\equiv 1 \pmod{p_2}$ para $p \in \{2, 5, 13, 409\}$ pues:

$$\begin{aligned} 2^{(n-1)/2} &= 53170 \pmod{n} \\ 2^{(n-1)/5} &= 25877 \pmod{n} \\ 2^{(n-1)/13} &= 39138 \pmod{n} \\ 2^{(n-1)/409} &= 30600 \pmod{n} \end{aligned}$$

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 $15^{p_3-1} \equiv 1 \pmod{p_3}$ y $15^{\frac{p_3-1}{p}} \not\equiv 1 \pmod{p_3}$ para $p \in \{2, 7, 349, 4504883\}$ pues:

$$\begin{aligned} 15^{(n-1)/2} &= 352173733408 \pmod{n} \\ 15^{(n-1)/7} &= 72307373439 \pmod{n} \\ 15^{(n-1)/349} &= 60311719490 \pmod{n} \\ 15^{(n-1)/4504883} &= 173110241247 \pmod{n} \end{aligned}$$

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 $2^{p_4-1} \equiv 1 \pmod{p_4}$ y $2^{\frac{p_4-1}{p}} \not\equiv 1 \pmod{p_4}$ para $p \in \{2, 2252441\}$ pues:

$$\begin{aligned} 2^{(n-1)/2} &= 4504882 \pmod{n} \\ 2^{(n-1)/2252441} &= 4 \pmod{n} \end{aligned}$$

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 factores 2 y 5 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 $3^{p_5-1} \equiv 1 \pmod{p_5}$ y $3^{\frac{p_5-1}{p}} \not\equiv 1 \pmod{p_5}$ para $p \in \{2, 5, 56311\}$ pues:

$$\begin{aligned} 3^{(n-1)/2} &= 2252440 \pmod{n} \\ 3^{(n-1)/5} &= 2075174 \pmod{n} \\ 3^{(n-1)/56311} &= 1333115 \pmod{n} \end{aligned}$$

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 $6^{p_6-1} \equiv 1 \pmod{p_6}$ y $6^{\frac{p_6-1}{p}} \not\equiv 1 \pmod{p_6}$ para $p \in \{2, 3, 5, 1877\}$ pues:

$$\begin{aligned}
6^{(n-1)/2} &= 56310 \pmod{n} \\
6^{(n-1)/3} &= 14180 \pmod{n} \\
6^{(n-1)/5} &= 15485 \pmod{n} \\
6^{(n-1)/1877} &= 46171 \pmod{n}
\end{aligned}$$

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 $3^{p_7-1} \equiv 1 \pmod{p_7}$ y $3^{\frac{p_7-1}{p}} \not\equiv 1 \pmod{p_7}$ para $p \in \{2, 3, 5, 37, 180391\}$ pues:

$$\begin{aligned}
3^{(n-1)/2} &= 600702030 \pmod{n} \\
3^{(n-1)/3} &= 267084186 \pmod{n} \\
3^{(n-1)/5} &= 455572699 \pmod{n} \\
3^{(n-1)/37} &= 27995379 \pmod{n} \\
3^{(n-1)/180391} &= 132564421 \pmod{n}
\end{aligned}$$

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 $7^{p_8-1} \equiv 1 \pmod{p_8}$ y $7^{\frac{p_8-1}{p}} \not\equiv 1 \pmod{p_8}$ para $p \in \{2, 3, 5, 7, 859\}$ pues:

$$\begin{aligned}
7^{(n-1)/2} &= 180390 \pmod{n} \\
7^{(n-1)/3} &= 83653 \pmod{n} \\
7^{(n-1)/5} &= 65181 \pmod{n} \\
7^{(n-1)/7} &= 129133 \pmod{n} \\
7^{(n-1)/859} &= 123807 \pmod{n}
\end{aligned}$$

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 $3^{p_9-1} \equiv 1 \pmod{p_9}$ y $3^{\frac{p_9-1}{p}} \not\equiv 1 \pmod{p_9}$ para $p \in \{2, 61, 131\}$ pues:

$$\begin{aligned}3^{(n-1)/2} &= 63928 \pmod{n} \\3^{(n-1)/61} &= 46509 \pmod{n} \\3^{(n-1)/131} &= 18863 \pmod{n}\end{aligned}$$

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 $U_{\frac{n}{p}}$ con p siendo uno de los divisores de r calculados en el apartado anterior.

$Q: 2$

$$\begin{aligned}U[2844871984646731064442373175299276800092] &= 0, \\V[2844871984646731064442373175299276800092] &= 4,\end{aligned}$$

$$U[2844871984646731064442373175299276800093] = 2$$

Factor: 2

$$\begin{aligned}U[1422435992323365532221186587649638400046] &= 2401816336829289298745644029101509733749, \\V[1422435992323365532221186587649638400046] &= 0,\end{aligned}$$

$$U[1422435992323365532221186587649638400047] = 2623344160738010181594008602200393266920$$

Factor: 31

$$\begin{aligned}U[91770064020862292401366876622557316132] &= 1470916208500242344757444167006191571594, \\V[91770064020862292401366876622557316132] &= 182521758238274725190305369534832625726,\end{aligned}$$

$$U[91770064020862292401366876622557316133] = 826718983369258534973874768270512098660$$

Factor: 63929

$$\begin{aligned}U[44500492493965666042678176966623548] &= 1641957773477697682672844736651862712136, \\V[44500492493965666042678176966623548] &= 2554432409192947819386117398691582182560,\end{aligned}$$

$$U[44500492493965666042678176966623549] = 2098195091335322751029481067671722447348$$

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[1677010021663162226328754084] = 1648554338650375930190024551175446944533,
V[1677010021663162226328754084] = 1877548978459566186099302960294216193767,

U[1677010021663162226328754085] = 1763051658554971058144663755734831569150

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