Ejercicio 3

Ana Buendía Ruiz-Azuaga

March 5, 2022

1 Ejercicio 3

1.1 Apartado 1

Dado tu número m (de 30 cifras o mas) de la lista publicada.

$$m = 365805459457767185586330009602 11$$

Calcula $a^{m-1} \mod m$, para los 5 primeros primos.

Aplicando el algoritmo de exponenciación rápida del primer ejercicio obtenemos que:

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

1.2 Apartado 2

Calcula el test de Solovay-Strassen para los 5 primeros primos.

Del primer apartado tenemos que el número es posible primo de Fermat, pues $a^{m-1} \equiv 1 \mod m$ para a siendo los 5 primeros primos.

Comprobamos ahora si es posible primo de Euler, es decir, si cumple $\left(\frac{p}{m}\right) = p^{\frac{m-1}{2}} \mod m$ para los 5 primeros primos.

Para $p = 2$ tenemos que como $m \equiv 3 \mod 8$ entonces $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = -1$.

Además, $2^{\frac{m-1}{2}} \equiv -1 \mod m$, que coincide con su símbolo de Jacobi.

Para $p = 3$ como $m \equiv 3 \mod 4$ entonces $\left(\frac{3}{m}\right) = -\left(\frac{m}{3}\right)$ y como $m \equiv 1 \mod 3$ entonces $-\left(\frac{m}{3}\right) = -\left(\frac{1}{3}\right) = -1$.

Además, $3^{\frac{m-1}{2}} \equiv -1 \mod m$, que coincide con su símbolo de Jacobi.

Para $p = 5$ como $5 \equiv 1 \mod 4$ entonces $\left(\frac{5}{m}\right) = \left(\frac{m}{5}\right)$ y como $m \equiv 1 \mod 5$ entonces $\left(\frac{m}{5}\right) = \left(\frac{1}{5}\right) = 1$.

Además, $5^{\frac{m-1}{2}} \equiv 1 \mod m$, que coincide con su símbolo de Jacobi.

Para $p = 7$ como $m \equiv 3 \mod 4$ entonces $\left(\frac{7}{m}\right) = -\left(\frac{m}{7}\right)$ y como $m \equiv 5 \mod 7$ entonces $-\left(\frac{m}{7}\right) = -\left(\frac{5}{7}\right) = 1$.

Además, $7^{\frac{m-1}{2}} \equiv 1 \mod m$, que coincide con su símbolo de Jacobi.

Para $p = 11$ como $m \equiv 3 \mod 4$ entonces $\left(\frac{11}{m}\right) = -\left(\frac{m}{11}\right)$ y como $m \equiv 6 \mod 11$ entonces $-\left(\frac{m}{11}\right) = -\left(\frac{6}{11}\right) = 1$.

Además, $11^{\frac{m-1}{2}} \equiv 1 \mod m$, que coincide con su símbolo de Jacobi.

Luego m es posible primo de Euler para todas las bases probadas.

Y, como es posible primo de Fermat y posible primo de Euler para todas ellas, se tiene que pasa el test de Solovay-Strassen y por tanto es primo con probabilidad mayor de $1 - \frac{1}{2^5}$.

1.3 Apartado 3

Calcula el test de Miller-Rabin para esas 5 bases.

Para comprobar el test de Miller-Rabin vamos a construir la a-sucesión correspondiente. Comenzamos descomponiendo $m - 1$ como $m - 1 = 2^r n$.

Como obtenemos que $r = 1$ tenemos que toda a-sucesión va a tener 2 términos.

La a-sucesion obtenida para la base 2 es:

```
[36580545945776718558633000960210, 1]
```

que sería: $2^{\frac{m-1}{2}} \equiv -1 \mod m$, $2^{m-1} \equiv 1 \mod m$.

La a-sucesion obtenida para la base 3 es:

```
[36580545945776718558633000960210, 1]
```

que sería: $3^{\frac{m-1}{2}} \equiv -1 \mod m$, $3^{m-1} \equiv 1 \mod m$.

La a-sucesion obtenida para la base 5 es:

```
[1, 1]
```

que sería: $5^{\frac{m-1}{2}} \equiv 1 \mod m$, $5^{m-1} \equiv 1 \mod m$.

La a-sucesion obtenida para la base 7 es:

```
[1, 1]
```

que sería: $7^{\frac{m-1}{2}} \equiv 1 \mod m$, $7^{m-1} \equiv 1 \mod m$.

La a-sucesion obtenida para la base 11 es:

```
[1, 1]
```

que sería: $11^{\frac{m-1}{2}} \equiv 1 \mod m$, $11^{m-1} \equiv 1 \mod m$.

Teniendo en cuenta que $36580545945776718558633000960210 \equiv -1 \mod m$ tenemos que m 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.

1.4 Apartado 4

¿Qué deduces sobre la primalidad de tu número?

Dado que ha pasado el test de Miller-Rabin para 5 bases, la probabilidad de que sea primo es mayor de $1 - \frac{1}{4^5}$.