

# Ejercicio 2

Ana Buendía Ruiz-Azuaga

February 25, 2022

## 1 Ejercicio 2

### 1.1 Apartado 1

Dado tu número  $n = 77770081$  de 8 cifras de la lista publicada.

Usa el algoritmo manual para calcular el símbolo de Jacobi  $\left(\frac{p}{n}\right)$ , para  $p$  cada uno de los 5 primeros primos.

Comenzamos con  $p = 2$ :

Tenemos que  $n \bmod 8 \equiv 1 \bmod 8$ , luego  $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = 1$

Ahora consideramos  $p = 3$ :

Como  $n \equiv 1 \bmod 4$  entonces  $\left(\frac{p}{n}\right) = \left(\frac{n}{p}\right)$ .

Además, como  $n \equiv 1 \bmod 3$  entonces  $\left(\frac{n}{3}\right) = \left(\frac{1}{3}\right)$ .

Y, como 1 es un cuadrado módulo 3 se tiene que  $\left(\frac{1}{3}\right) = 1$

Ahora tomamos  $p = 5$ :

Como  $n \equiv 1 \bmod 4$  tenemos  $\left(\frac{p}{n}\right) = \left(\frac{n}{p}\right)$ .

Y como  $n \equiv 1 \bmod 5$  tenemos  $\left(\frac{n}{5}\right) = \left(\frac{1}{5}\right)$ .

De donde, usando que 1 es cuadrado módulo 5, se tiene que  $\left(\frac{1}{5}\right) = 1$ .

Tomamos ahora  $p = 7$ :

Como  $n \equiv 1 \bmod 4$  tenemos  $\left(\frac{p}{n}\right) = \left(\frac{n}{p}\right)$ .

Y como  $n \equiv 4 \bmod 7$  tenemos  $\left(\frac{n}{7}\right) = \left(\frac{4}{7}\right)$ .

De donde se tiene que  $\left(\frac{4}{7}\right) = 4^{\frac{7-1}{2}} \bmod 7 = 1$ .

Finalmente consideramos  $p = 11$ :

Como  $n \equiv 1 \bmod 4$  tenemos  $\left(\frac{p}{n}\right) = \left(\frac{n}{p}\right)$ .

Y como  $n \equiv 4 \bmod 11$  tenemos  $\left(\frac{n}{11}\right) = \left(\frac{4}{11}\right)$ .

De donde se tiene que  $\left(\frac{4}{11}\right) = 4^{\frac{11-1}{2}} \bmod 11 = 1$ .

### 1.2 Apartado 2

Si para alguna de esas bases tu número sale posible primo de Fermat, comprueba si además es posible primo de Euler

Comprobamos si  $n$  es un posible primo de Fermat para estas bases. Para ello, comprobamos si se cumple  $a^{n-1} \equiv 1 \bmod n$ .

Para esta comprobación usamos el algoritmo de exponenciación rápida de derecha a izquierda del ejercicio anterior:

### 1.2.1 Posibles primos de Fermat

El resultado del algoritmo es el último valor de la variable acu.

#### Base 2

Paso: 0, acu: 1, base: 2  
Paso: 1, acu: 1, base: 4  
Paso: 2, acu: 1, base: 16  
Paso: 3, acu: 1, base: 256  
Paso: 4, acu: 1, base: 65536  
Paso: 5, acu: 1, base: 17612841  
Paso: 6, acu: 17612841, base: 69275565  
Paso: 7, acu: 44516305, base: 9980674  
Paso: 8, acu: 44516305, base: 23223320  
Paso: 9, acu: 44680160, base: 67690927  
Paso: 10, acu: 44680160, base: 77257279  
Paso: 11, acu: 1465333, base: 25247343  
Paso: 12, acu: 70708033, base: 13797891  
Paso: 13, acu: 70708033, base: 15599233  
Paso: 14, acu: 31848612, base: 19426093  
Paso: 15, acu: 31848612, base: 70568710  
Paso: 16, acu: 19282073, base: 10086087  
Paso: 17, acu: 19282073, base: 52267494  
Paso: 18, acu: 44352822, base: 10929208  
Paso: 19, acu: 44352822, base: 53478878  
Paso: 20, acu: 44352822, base: 18488420  
Paso: 21, acu: 44352822, base: 3628315  
Paso: 22, acu: 35935437, base: 61507869  
Paso: 23, acu: 35935437, base: 45590014  
Paso: 24, acu: 15507894, base: 21699431  
Paso: 25, acu: 15507894, base: 50932700  
Paso: 26, acu: 15507894, base: 44851232  
Paso: 27, acu: 1, base: 55498452

#### Base 3

Paso: 0, acu: 1, base: 3  
Paso: 1, acu: 1, base: 9  
Paso: 2, acu: 1, base: 81  
Paso: 3, acu: 1, base: 6561  
Paso: 4, acu: 1, base: 43046721  
Paso: 5, acu: 1, base: 12562698  
Paso: 6, acu: 12562698, base: 67023312  
Paso: 7, acu: 58342833, base: 40759744  
Paso: 8, acu: 58342833, base: 63810002  
Paso: 9, acu: 24303074, base: 70788665  
Paso: 10, acu: 24303074, base: 26430655  
Paso: 11, acu: 58499677, base: 49886400  
Paso: 12, acu: 54301195, base: 47309308  
Paso: 13, acu: 54301195, base: 31523377  
Paso: 14, acu: 73546473, base: 66869943

Paso: 15, acu: 73546473, base: 481537  
 Paso: 16, acu: 19632816, base: 45270908  
 Paso: 17, acu: 19632816, base: 75692200  
 Paso: 18, acu: 29496059, base: 27863284  
 Paso: 19, acu: 29496059, base: 52818504  
 Paso: 20, acu: 29496059, base: 43958962  
 Paso: 21, acu: 29496059, base: 41181807  
 Paso: 22, acu: 3749083, base: 50088853  
 Paso: 23, acu: 3749083, base: 51464019  
 Paso: 24, acu: 51758518, base: 62708747  
 Paso: 25, acu: 51758518, base: 43324625  
 Paso: 26, acu: 51758518, base: 75071723  
 Paso: 27, acu: 1, base: 67602701

#### Base 5

Paso: 0, acu: 1, base: 5  
 Paso: 1, acu: 1, base: 25  
 Paso: 2, acu: 1, base: 625  
 Paso: 3, acu: 1, base: 390625  
 Paso: 4, acu: 1, base: 2991703  
 Paso: 5, acu: 1, base: 39298243  
 Paso: 6, acu: 39298243, base: 11535691  
 Paso: 7, acu: 9210897, base: 14558624  
 Paso: 8, acu: 9210897, base: 42797110  
 Paso: 9, acu: 29856166, base: 49630482  
 Paso: 10, acu: 29856166, base: 32027512  
 Paso: 11, acu: 28016975, base: 53957117  
 Paso: 12, acu: 65591934, base: 52967279  
 Paso: 13, acu: 65591934, base: 70302898  
 Paso: 14, acu: 52076763, base: 6980919  
 Paso: 15, acu: 52076763, base: 8687369  
 Paso: 16, acu: 30787191, base: 38207412  
 Paso: 17, acu: 30787191, base: 6383268  
 Paso: 18, acu: 73995456, base: 31821494  
 Paso: 19, acu: 73995456, base: 40939349  
 Paso: 20, acu: 73995456, base: 48295268  
 Paso: 21, acu: 73995456, base: 3819153  
 Paso: 22, acu: 58442021, base: 73175778  
 Paso: 23, acu: 58442021, base: 42371599  
 Paso: 24, acu: 63235719, base: 62680535  
 Paso: 25, acu: 63235719, base: 10805207  
 Paso: 26, acu: 63235719, base: 8671437  
 Paso: 27, acu: 1, base: 28118256

#### Base 7

Paso: 0, acu: 1, base: 7  
 Paso: 1, acu: 1, base: 49  
 Paso: 2, acu: 1, base: 2401  
 Paso: 3, acu: 1, base: 5764801

Paso: 4, acu: 1, base: 64016519  
 Paso: 5, acu: 1, base: 66361301  
 Paso: 6, acu: 66361301, base: 53942426  
 Paso: 7, acu: 11146291, base: 10572008  
 Paso: 8, acu: 11146291, base: 3472833  
 Paso: 9, acu: 4865544, base: 62654490  
 Paso: 10, acu: 4865544, base: 59229057  
 Paso: 11, acu: 37101810, base: 71051765  
 Paso: 12, acu: 58332031, base: 36885562  
 Paso: 13, acu: 58332031, base: 46045556  
 Paso: 14, acu: 55512383, base: 3850811  
 Paso: 15, acu: 55512383, base: 12933127  
 Paso: 16, acu: 42505399, base: 61345597  
 Paso: 17, acu: 42505399, base: 28288883  
 Paso: 18, acu: 50620210, base: 1900642  
 Paso: 19, acu: 50620210, base: 19749714  
 Paso: 20, acu: 50620210, base: 28031156  
 Paso: 21, acu: 50620210, base: 48437372  
 Paso: 22, acu: 26226364, base: 3766720  
 Paso: 23, acu: 26226364, base: 39291003  
 Paso: 24, acu: 40666288, base: 69077328  
 Paso: 25, acu: 40666288, base: 55376817  
 Paso: 26, acu: 40666288, base: 56629098  
 Paso: 27, acu: 1, base: 6352934

#### Base 11

Paso: 0, acu: 1, base: 11  
 Paso: 1, acu: 1, base: 121  
 Paso: 2, acu: 1, base: 14641  
 Paso: 3, acu: 1, base: 58818719  
 Paso: 4, acu: 1, base: 66544732  
 Paso: 5, acu: 1, base: 8800012  
 Paso: 6, acu: 8800012, base: 30883746  
 Paso: 7, acu: 66090327, base: 52473686  
 Paso: 8, acu: 66090327, base: 52822068  
 Paso: 9, acu: 48240432, base: 61995449  
 Paso: 10, acu: 48240432, base: 30811749  
 Paso: 11, acu: 41802059, base: 96486  
 Paso: 12, acu: 1523852, base: 54908557  
 Paso: 13, acu: 1523852, base: 38676855  
 Paso: 14, acu: 58039934, base: 3824773  
 Paso: 15, acu: 58039934, base: 25185105  
 Paso: 16, acu: 42622747, base: 77338508  
 Paso: 17, acu: 42622747, base: 73680415  
 Paso: 18, acu: 49309845, base: 56601615  
 Paso: 19, acu: 49309845, base: 56458770  
 Paso: 20, acu: 49309845, base: 69634310  
 Paso: 21, acu: 49309845, base: 31664693  
 Paso: 22, acu: 53354819, base: 69239724  
 Paso: 23, acu: 53354819, base: 14398341

Paso: 24, acu: 7518936, base: 52010095  
Paso: 25, acu: 7518936, base: 7393889  
Paso: 26, acu: 7518936, base: 27324237  
Paso: 27, acu: 1, base: 74340218

Como podemos ver, el número es pseudoprimo de Fermat para todas las bases, por lo que se va a comprobar para todas ellas si es pseudoprimo de Euler. Para ello comprobamos  $\left(\frac{p}{n}\right) = p^{\frac{n-1}{2}} \pmod n$  usando de nuevo el algoritmo de exponenciación rápida de derecha a izquierda.

### 1.2.2 Posibles primos de Euler

#### Base 2

Paso: 0, acu: 1, base: 2  
Paso: 1, acu: 1, base: 4  
Paso: 2, acu: 1, base: 16  
Paso: 3, acu: 1, base: 256  
Paso: 4, acu: 1, base: 65536  
Paso: 5, acu: 65536, base: 17612841  
Paso: 6, acu: 11605574, base: 69275565  
Paso: 7, acu: 11605574, base: 9980674  
Paso: 8, acu: 69874828, base: 23223320  
Paso: 9, acu: 69874828, base: 67690927  
Paso: 10, acu: 13173522, base: 77257279  
Paso: 11, acu: 11887340, base: 25247343  
Paso: 12, acu: 11887340, base: 13797891  
Paso: 13, acu: 9967700, base: 15599233  
Paso: 14, acu: 9967700, base: 19426093  
Paso: 15, acu: 41890761, base: 70568710  
Paso: 16, acu: 41890761, base: 10086087  
Paso: 17, acu: 53220709, base: 52267494  
Paso: 18, acu: 53220709, base: 10929208  
Paso: 19, acu: 53220709, base: 53478878  
Paso: 20, acu: 53220709, base: 18488420  
Paso: 21, acu: 2277206, base: 3628315  
Paso: 22, acu: 2277206, base: 61507869  
Paso: 23, acu: 72660827, base: 45590014  
Paso: 24, acu: 72660827, base: 21699431  
Paso: 25, acu: 72660827, base: 50932700  
Paso: 26, acu: 1, base: 44851232

Y, del apartado anterior habíamos obtenido que el símbolo de Jacobi con  $p = 2$  era 1, por tanto coincide y es un posible primo de Euler para la base 2.

#### Base 3

Paso: 0, acu: 1, base: 3  
Paso: 1, acu: 1, base: 9  
Paso: 2, acu: 1, base: 81  
Paso: 3, acu: 1, base: 6561  
Paso: 4, acu: 1, base: 43046721  
Paso: 5, acu: 43046721, base: 12562698

Paso: 6, acu: 65100767, base: 67023312  
 Paso: 7, acu: 65100767, base: 40759744  
 Paso: 8, acu: 8749244, base: 63810002  
 Paso: 9, acu: 8749244, base: 70788665  
 Paso: 10, acu: 64969516, base: 26430655  
 Paso: 11, acu: 65638599, base: 49886400  
 Paso: 12, acu: 65638599, base: 47309308  
 Paso: 13, acu: 58223961, base: 31523377  
 Paso: 14, acu: 58223961, base: 66869943  
 Paso: 15, acu: 68880686, base: 481537  
 Paso: 16, acu: 68880686, base: 45270908  
 Paso: 17, acu: 22173965, base: 75692200  
 Paso: 18, acu: 22173965, base: 27863284  
 Paso: 19, acu: 22173965, base: 52818504  
 Paso: 20, acu: 22173965, base: 43958962  
 Paso: 21, acu: 31467141, base: 41181807  
 Paso: 22, acu: 31467141, base: 50088853  
 Paso: 23, acu: 66936124, base: 51464019  
 Paso: 24, acu: 66936124, base: 62708747  
 Paso: 25, acu: 66936124, base: 43324625  
 Paso: 26, acu: 1, base: 75071723

Y, del apartado anterior habíamos obtenido que el símbolo de Jacobi con  $p = 3$  era 1, por tanto coincide y es un posible primo de Euler para la base 3.

#### **Base 5**

Paso: 0, acu: 1, base: 5  
 Paso: 1, acu: 1, base: 25  
 Paso: 2, acu: 1, base: 625  
 Paso: 3, acu: 1, base: 390625  
 Paso: 4, acu: 1, base: 2991703  
 Paso: 5, acu: 2991703, base: 39298243  
 Paso: 6, acu: 62606403, base: 11535691  
 Paso: 7, acu: 62606403, base: 14558624  
 Paso: 8, acu: 65051902, base: 42797110  
 Paso: 9, acu: 65051902, base: 49630482  
 Paso: 10, acu: 76302315, base: 32027512  
 Paso: 11, acu: 9983068, base: 53957117  
 Paso: 12, acu: 9983068, base: 52967279  
 Paso: 13, acu: 57895152, base: 70302898  
 Paso: 14, acu: 57895152, base: 6980919  
 Paso: 15, acu: 54677894, base: 8687369  
 Paso: 16, acu: 54677894, base: 38207412  
 Paso: 17, acu: 465722, base: 6383268  
 Paso: 18, acu: 465722, base: 31821494  
 Paso: 19, acu: 465722, base: 40939349  
 Paso: 20, acu: 465722, base: 48295268  
 Paso: 21, acu: 50367243, base: 3819153  
 Paso: 22, acu: 50367243, base: 73175778  
 Paso: 23, acu: 11756279, base: 42371599  
 Paso: 24, acu: 11756279, base: 62680535

Paso: 25, acu: 11756279, base: 10805207  
Paso: 26, acu: 1, base: 8671437

De nuevo, del apartado anterior habíamos obtenido que el símbolo de Jacobi con  $p = 5$  era 1, por tanto coincide y es un posible primo de Euler para la base 5.

#### **Base 7**

Paso: 0, acu: 1, base: 7  
Paso: 1, acu: 1, base: 49  
Paso: 2, acu: 1, base: 2401  
Paso: 3, acu: 1, base: 5764801  
Paso: 4, acu: 1, base: 64016519  
Paso: 5, acu: 64016519, base: 66361301  
Paso: 6, acu: 36776249, base: 53942426  
Paso: 7, acu: 36776249, base: 10572008  
Paso: 8, acu: 32971776, base: 3472833  
Paso: 9, acu: 32971776, base: 62654490  
Paso: 10, acu: 50357183, base: 59229057  
Paso: 11, acu: 23925373, base: 71051765  
Paso: 12, acu: 23925373, base: 36885562  
Paso: 13, acu: 13272104, base: 46045556  
Paso: 14, acu: 13272104, base: 3850811  
Paso: 15, acu: 44405412, base: 12933127  
Paso: 16, acu: 44405412, base: 61345597  
Paso: 17, acu: 6569097, base: 28288883  
Paso: 18, acu: 6569097, base: 1900642  
Paso: 19, acu: 6569097, base: 19749714  
Paso: 20, acu: 6569097, base: 28031156  
Paso: 21, acu: 51199192, base: 48437372  
Paso: 22, acu: 51199192, base: 3766720  
Paso: 23, acu: 17947736, base: 39291003  
Paso: 24, acu: 17947736, base: 69077328  
Paso: 25, acu: 17947736, base: 55376817  
Paso: 26, acu: 1, base: 56629098

Del apartado anterior habíamos obtenido que el símbolo de Jacobi con  $p = 7$  era 1, por tanto coincide y es un posible primo de Euler para la base 7.

#### **Base 11**

Paso: 0, acu: 1, base: 11  
Paso: 1, acu: 1, base: 121  
Paso: 2, acu: 1, base: 14641  
Paso: 3, acu: 1, base: 58818719  
Paso: 4, acu: 1, base: 66544732  
Paso: 5, acu: 66544732, base: 8800012  
Paso: 6, acu: 39901688, base: 30883746  
Paso: 7, acu: 39901688, base: 52473686  
Paso: 8, acu: 76924925, base: 52822068  
Paso: 9, acu: 76924925, base: 61995449  
Paso: 10, acu: 55436924, base: 30811749

Paso: 11, acu: 47440987, base: 96486  
 Paso: 12, acu: 47440987, base: 54908557  
 Paso: 13, acu: 43113226, base: 38676855  
 Paso: 14, acu: 43113226, base: 3824773  
 Paso: 15, acu: 66900968, base: 25185105  
 Paso: 16, acu: 66900968, base: 77338508  
 Paso: 17, acu: 35499153, base: 73680415  
 Paso: 18, acu: 35499153, base: 56601615  
 Paso: 19, acu: 35499153, base: 56458770  
 Paso: 20, acu: 35499153, base: 69634310  
 Paso: 21, acu: 59365955, base: 31664693  
 Paso: 22, acu: 59365955, base: 69239724  
 Paso: 23, acu: 2469011, base: 14398341  
 Paso: 24, acu: 2469011, base: 52010095  
 Paso: 25, acu: 2469011, base: 7393889  
 Paso: 26, acu: 1, base: 27324237

Y, del apartado anterior habíamos obtenido que el símbolo de Jacobi con  $p = 11$  era 1, por tanto coincide y es un posible primo de Euler para la base 11.

Como todos los números obtenidos coinciden con su símbolo de Jacobi,  $n$  es pseudoprimo de Euler para todas las bases.

### 1.3 Apartado 3

**¿Es tu número  $n$  pseudoprimo de Fermat o de Euler para alguna de las bases?**

Del apartado anterior tenemos que  $n$  es pseudoprimo de Fermat para todas las bases, además, también es pseudoprimo de Euler para todas ellas.