

Ejercicio 1

Ana Buendía Ruiz-Azuaga

February 25, 2022

1 Ejercicio 1

1.1 Apartado 1

Dado tu número $n = d1d2d3d4d5d6d7d8$.

En este caso mi número es $n = 77770080$.

Mientras n sea múltiplo de 2, 3, 5, 7 u 11 le sumas uno. De forma que tu nuevo n no tenga esos divisores primos.

Luego el número con el que vamos a trabajar es $n = 77770081$, ya que no es divisible por ninguno de los números pedidos.

1.2 Apartado 2

Calcula $a^{n-1} \bmod n$, para cada uno de esas cinco bases usando sucesivamente el algoritmo de izda-drcha y de drcha-izda.

Tenemos que 77770080 en binario es 1001010001010110101100000, luego el algoritmo dará 27 pasos.

En los algoritmos se imprimen las variables más relevantes en cada paso o iteración del algoritmo, siendo el paso 0 el estado inicial de las variables.

Comenzamos aplicando el algoritmo de derecha a izquierda ya que es más intuitivo:

1.2.1 Derecha a izquierda

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

1.2.2 Izquierda a derecha

De nuevo, el resultado es el último valor de la variable acu.

Base 2

Paso: 0, acu: 1
Paso: 1, acu: 2
Paso: 2, acu: 4
Paso: 3, acu: 16
Paso: 4, acu: 512
Paso: 5, acu: 262144
Paso: 6, acu: 19220345

Paso: 7, acu: 11864688
 Paso: 8, acu: 53190135
 Paso: 9, acu: 72776920
 Paso: 10, acu: 15099639
 Paso: 11, acu: 7072054
 Paso: 12, acu: 17375632
 Paso: 13, acu: 33857947
 Paso: 14, acu: 56968058
 Paso: 15, acu: 75776703
 Paso: 16, acu: 20434621
 Paso: 17, acu: 1784769
 Paso: 18, acu: 15635682
 Paso: 19, acu: 49254338
 Paso: 20, acu: 41393140
 Paso: 21, acu: 65775228
 Paso: 22, acu: 42089411
 Paso: 23, acu: 64834401
 Paso: 24, acu: 77611099
 Paso: 25, acu: 77770080
 Paso: 26, acu: 1
 Paso: 27, acu: 1

Base 3

Paso: 0, acu: 1
 Paso: 1, acu: 3
 Paso: 2, acu: 9
 Paso: 3, acu: 81
 Paso: 4, acu: 19683
 Paso: 5, acu: 76340165
 Paso: 6, acu: 19702455
 Paso: 7, acu: 17898279
 Paso: 8, acu: 51068909
 Paso: 9, acu: 34810944
 Paso: 10, acu: 23313615
 Paso: 11, acu: 47220160
 Paso: 12, acu: 20151576
 Paso: 13, acu: 49392394
 Paso: 14, acu: 9595127
 Paso: 15, acu: 62696061
 Paso: 16, acu: 68121819
 Paso: 17, acu: 39666683
 Paso: 18, acu: 61569031
 Paso: 19, acu: 70952581
 Paso: 20, acu: 28351403
 Paso: 21, acu: 64679486
 Paso: 22, acu: 77770080
 Paso: 23, acu: 1
 Paso: 24, acu: 1
 Paso: 25, acu: 1
 Paso: 26, acu: 1

Paso: 27, acu: 1

Base 5

Paso: 0, acu: 1
Paso: 1, acu: 5
Paso: 2, acu: 25
Paso: 3, acu: 625
Paso: 4, acu: 1953125
Paso: 5, acu: 74792575
Paso: 6, acu: 8051476
Paso: 7, acu: 3749973
Paso: 8, acu: 66994471
Paso: 9, acu: 6905941
Paso: 10, acu: 5483666
Paso: 11, acu: 13280096
Paso: 12, acu: 52948589
Paso: 13, acu: 62371752
Paso: 14, acu: 11181005
Paso: 15, acu: 11993092
Paso: 16, acu: 76022758
Paso: 17, acu: 43591993
Paso: 18, acu: 8409213
Paso: 19, acu: 31288040
Paso: 20, acu: 53493165
Paso: 21, acu: 29944826
Paso: 22, acu: 41852831
Paso: 23, acu: 66025877
Paso: 24, acu: 158982
Paso: 25, acu: 77770080
Paso: 26, acu: 1
Paso: 27, acu: 1

Base 7

Paso: 0, acu: 1
Paso: 1, acu: 7
Paso: 2, acu: 49
Paso: 3, acu: 2401
Paso: 4, acu: 40353607
Paso: 5, acu: 26006191
Paso: 6, acu: 33654286
Paso: 7, acu: 14379654
Paso: 8, acu: 57727645
Paso: 9, acu: 51881681
Paso: 10, acu: 44071038
Paso: 11, acu: 23445985
Paso: 12, acu: 40778400
Paso: 13, acu: 56640106
Paso: 14, acu: 57833413
Paso: 15, acu: 56853941

Paso: 16, acu: 67656622
 Paso: 17, acu: 62752872
 Paso: 18, acu: 51817096
 Paso: 19, acu: 16791967
 Paso: 20, acu: 28518280
 Paso: 21, acu: 46121250
 Paso: 22, acu: 12935680
 Paso: 23, acu: 77611099
 Paso: 24, acu: 77770080
 Paso: 25, acu: 1
 Paso: 26, acu: 1
 Paso: 27, acu: 1

Base 11

Paso: 0, acu: 1
 Paso: 1, acu: 11
 Paso: 2, acu: 121
 Paso: 3, acu: 14641
 Paso: 4, acu: 24845261
 Paso: 5, acu: 41594229
 Paso: 6, acu: 46546549
 Paso: 7, acu: 13476520
 Paso: 8, acu: 43381019
 Paso: 9, acu: 37086665
 Paso: 10, acu: 28028316
 Paso: 11, acu: 34892699
 Paso: 12, acu: 57303102
 Paso: 13, acu: 42511767
 Paso: 14, acu: 68132811
 Paso: 15, acu: 53818650
 Paso: 16, acu: 22343385
 Paso: 17, acu: 25714307
 Paso: 18, acu: 13792896
 Paso: 19, acu: 12448619
 Paso: 20, acu: 29722997
 Paso: 21, acu: 45144696
 Paso: 22, acu: 77611099
 Paso: 23, acu: 77770080
 Paso: 24, acu: 1
 Paso: 25, acu: 1
 Paso: 26, acu: 1
 Paso: 27, acu: 1

1.3 Apartado 3

¿Es n un posible primo de Fermat para alguna de ellas? ¿Es n un pseudoprimo para alguna de ellas?

Del apartado anterior tenemos que $2^{n-1} \equiv 1 \pmod{n}$, $3^{n-1} \equiv 1 \pmod{n}$, $5^{n-1} \equiv 1 \pmod{n}$, $7^{n-1} \equiv 1 \pmod{n}$ y $11^{n-1} \equiv 1 \pmod{n}$, luego n es un

pseudoprimo de Fermat para todas estas bases y es un posible primo de Fermat para todas ellas.