Criptografía y Computación

Curso 2018-19

Práctica 1. Primalidad

Autor[1]: Víctor García Carrera, victorgarcia@correo.ugr.es

Síntesis.

Esta presente memoria recoge las instrucciones para ejecutar en Linux los diversos apartados de la primera práctica de la asignatura de Criptografía y Computación, donde desarrollamos el test de primalidad de Miller-Rabin junto con una serie de funciones para encontrar números primos y primos fuertes.

Apartado 1.

Implementa el test de primalidad de Miller-Rabin con 10 testigos para un número de entrada dado "num". Con este valor, la probabilidad de error es menor que 1/(4^10). Hemos implementado, para optimizar el test, que se compruebe al comienzo del programa con una lista de los 50 primeros primos si "num" es coprimo con ellos. Se trata de una optimización notable pues *la probabilidad de que un número compuesto tenga como divisor a un primo entre el 1 y el 50 es mayor que la de que el primo esté entre el 51 y el 100...*

Ejecución en Linux: python miller-rabin.py "num"

Ejemplo: Probamos con "num"=5167

Apartado 2.

Implementamos una versión de prueba del test de primalidad de Miller-Rabin donde para un número de entrada dado "num" comprueba si el número "test" es un FALSO TESTIGO (cuando da un falso positivo en el test sin ser primo). Ejecuta el test de Miller-Rabin con 10 testigos aleatorios para evaluar si es compuesto o no, y en función de ello comprueba la salida del test con el testigo "test". Si sabemos de antemano que el número es compuesto, basta con pasar el test con el testigo "test" y, si sale que es probable primo, es un FALSO TESTIGO

Ejecución en Linux: python miller-rabin-testigo.py "num" "test"

Ejemplo: Probamos con "num"=1729 y "test"=10 y obtenemos que 10 es un falso testigo.

Apartados 3,4 y 5.

Utilizan el test de primalidad de Miller-Rabin para definir funciones que calculan, para un número de entrada dado "num", su siguiente número primo(probable) y su siguiente número primo fuerte(probable), además de calcular un primo fuerte de "nbit" bits de tamaño.

---

1 Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la "Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada" esto "conllevará la calificación numérica de cero … independientemente del resto de calificaciones que el estudiante hubiera obtenido ..."

Ejecución en Linux: python nextPrime.py “num” “nbit”

Ejemplo: Probamos con “num” = 5167 y “nbit” = 5

Apartado 6.

Utiliza el test de primalidad de Miller-Rabin para encontrar todos los falsos testigos del valor “num” (6601, 8911, 10585, 15841, 29341)

Ejecución en Linux: python miller-rabin-Falsostestigos.py “num”

A continuación se muestran las imágenes de las salidas obtenidas:

```
victor@VKCOMPUTRON ~/Documents/UGR/2cuarto/cripto&comput/CRIPTO-COMPUTACION/p1 $ python miller-rabin-Falsostestigos.py 6601
--- TEST MILLER-RABIN de 6601 ---
FALSOS TESTIGOS: [16, 18, 40, 45, 66, 78, 100, 122, 141, 165, 195, 242, 250, 256, 286, 288, 303, 305, 318, 324, 327, 332, 338, 433, 474, 482, 508, 517, 523, 573, 605, 6
11, 619, 625, 640, 652, 715, 720, 739, 769, 795, 804, 810, 821, 824, 830, 843, 845, 877, 898, 927, 961, 983, 1002, 1056, 1082, 1091, 1108, 1111, 1117, 1132, 1147, 1166,
 1185, 1188, 1193, 1199, 1205, 1248, 1270, 1289, 1313, 1369, 1378, 1404, 1417, 1451, 1453, 1466, 1513, 1527, 1576, 1581, 1600, 1630, 1644, 1671, 1682, 1691, 1721, 1738,
 1753, 1762, 1767, 1773, 1779, 1788, 1800, 1868, 1887, 1931, 1952, 1964, 1972, 1993, 2008, 2010, 2025, 2027, 2054, 2060, 2075, 2101, 2109, 2131, 2174, 2196, 2204, 2218,
 2245, 2256, 2259, 2312, 2347, 2396, 2483, 2491, 2505, 2526, 2538, 2543, 2567, 2584, 2601, 2614, 2634, 2640, 2661, 2705, 2729, 2770, 2813, 2830, 2869, 2888, 2907, 2915,
 2927, 2936, 2948, 2962, 2970, 3057, 3079, 3091, 3117, 3120, 3139, 3156, 3175, 3188, 3202, 3249, 3298, 3303, 3352, 3399, 3413, 3426, 3445, 3462, 3481, 3484, 3510, 3522,
 3544, 3631, 3639, 3653, 3665, 3674, 3686, 3694, 3713, 3732, 3771, 3788, 3831, 3872, 3896, 3940, 3961, 3967, 3987, 4000, 4017, 4034, 4058, 4063, 4075, 4096, 4110, 4118,
 4205, 4254, 4289, 4342, 4345, 4356, 4383, 4397, 4405, 4427, 4470, 4492, 4500, 4526, 4541, 4547, 4574, 4576, 4591, 4593, 4608, 4629, 4637, 4649, 4670, 4714, 4733, 4801,
 4813, 4822, 4828, 4834, 4839, 4848, 4863, 4880, 4910, 4919, 4930, 4957, 4971, 5001, 5020, 5025, 5074, 5088, 5135, 5148, 5150, 5184, 5197, 5223, 5232, 5288, 5312, 5331,
 5353, 5396, 5402, 5408, 5413, 5416, 5435, 5454, 5469, 5484, 5490, 5493, 5510, 5519, 5545, 5599, 5618, 5640, 5674, 5703, 5724, 5756, 5758, 5771, 5777, 5780, 5791, 5797,
 5806, 5832, 5862, 5881, 5886, 5949, 5961, 5976, 5982, 5990, 5996, 6028, 6078, 6084, 6093, 6119, 6127, 6168, 6263, 6269, 6274, 6277, 6283, 6296, 6298, 6313, 6315, 6345,
 6351, 6359, 6406, 6436, 6460, 6479, 6501, 6523, 6535, 6556, 6561, 6583, 6585, 6600]
```

```
victor@VKCOMPUTRON ~/Documents/UGR/2cuarto/cripto&comput/CRIPTO-COMPUTACION/p1 $ python miller-rabin-Falsostestigos.py 8911
--- TEST MILLER-RABIN de 8911 ---
FALSOS TESTIGOS: [3, 4, 9, 12, 13, 16, 23, 25, 27, 31, 34, 36, 39, 41, 48, 52, 64, 69, 75, 81, 92, 93, 94, 97, 100, 102, 106, 108, 110, 117, 121, 123, 124, 136, 144, 14
5, 146, 149, 156, 158, 163, 164, 166, 169, 185, 192, 207, 208, 218, 225, 226, 243, 256, 262, 263, 276, 277, 279, 282, 289, 291, 299, 300, 305, 306, 314, 318, 324, 325,
330, 351, 355, 358, 359, 363, 368, 369, 372, 376, 383, 388, 389, 398, 400, 403, 408, 409, 424, 430, 432, 433, 435, 438, 440, 442, 447, 457, 468, 473, 474, 484, 489, 491
, 492, 496, 498, 505, 507, 521, 529, 533, 535, 544, 555, 557, 562, 563, 566, 571, 575, 576, 580, 584, 590, 596, 613, 617, 621, 624, 625, 632, 635, 638, 649, 652, 654, 6
56, 661, 662, 664, 674, 675, 676, 677, 678, 695, 698, 709, 713, 729, 740, 746, 755, 758, 768, 775, 782, 786, 787, 789, 794, 799, 802, 811, 814, 821, 823, 828, 831, 832,
 837, 838, 841, 846, 850, 857, 867, 872, 873, 890, 897, 900, 901, 904, 915, 918, 922, 934, 935, 941, 942, 943, 947, 954, 958, 961, 965, 967, 972, 974, 975, 979, 983, 99
0, 1024, 1025, 1030, 1031, 1039, 1048, 1052, 1053, 1054, 1055, 1061, 1063, 1065, 1073, 1074, 1077, 1087, 1089, 1094, 1104, 1107, 1108, 1116, 1123, 1128, 1133, 1145, 114
9, 1156, 1163, 1164, 1167, 1181, 1194, 1196, 1198, 1200, 1201, 1209, 1220, 1222, 1224, 1227, 1237, 1238, 1241, 1249, 1255, 1256, 1261, 1271, 1272, 1282, 1286, 1289, 129
0, 1291, 1296, 1297, 1299, 1300, 1305, 1307, 1314, 1319, 1320, 1321, 1326, 1327, 1341, 1342, 1343, 1346, 1355, 1366, 1369, 1370, 1371, 1373, 1378, 1382, 1394, 1404, 141
1, 1419, 1420, 1422, 1423, 1427, 1429, 1430, 1432, 1436, 1438, 1452, 1459, 1467, 1472, 1473, 1476, 1488, 1493, 1494, 1499, 1504, 1507, 1515, 1521, 1522, 1532, 1552, 155
3, 1555, 1556, 1562, 1563, 1565, 1571, 1573, 1585, 1587, 1592, 1597, 1599, 1600, 1605, 1612, 1632, 1636, 1665, 1670, 1671, 1681, 1686, 1689, 1693, 1696, 1698, 1706, 171
3, 1718, 1720, 1725, 1728, 1730, 1732, 1740, 1741, 1752, 1759, 1760, 1762, 1765, 1768, 1769, 1770, 1788, 1810, 1828, 1831, 1835, 1837, 1839, 1849, 1851, 1853, 1861, 186
3, 1871, 1872, 1873, 1875, 1885, 1889, 1892, 1896, 1898, 1901, 1903, 1905, 1910, 1914, 1921, 1936, 1937, 1947, 1951, 1956, 1962, 1964, 1968, 1970, 1982, 1983, 1984, 198
6, 1991, 1992, 1994, 1999, 2011, 2020, 2022, 2025, 2028, 2031, 2034, 2039, 2054, 2059, 2069, 2084, 2085, 2087, 2089, 2094, 2101, 2105, 2116, 2119, 2127, 2132, 2137, 213
```

```
8, 8476, 8478, 8479, 8481, 8487, 8502, 8503, 8508, 8511, 8513, 8522, 8523, 8528, 8535, 8539, 8542, 8543, 8548, 8552, 8553, 8556, 8560, 8581, 8586, 8587, 8593, 8597, 860
5, 8606, 8611, 8612, 8620, 8622, 8629, 8632, 8634, 8635, 8648, 8649, 8655, 8668, 8685, 8686, 8693, 8703, 8704, 8719, 8726, 8742, 8745, 8747, 8748, 8753, 8755, 8762, 876
5, 8766, 8767, 8775, 8787, 8788, 8790, 8794, 8801, 8803, 8805, 8809, 8811, 8814, 8817, 8818, 8819, 8830, 8836, 8842, 8847, 8859, 8863, 8870, 8872, 8875, 8877, 8880, 888
4, 8886, 8888, 8895, 8898, 8899, 8902, 8907, 8908, 8910]
victor@VKCOMPUTRON ~/Documents/UGR/2cuarto/cripto&comput/CRIPTO-COMPUTACION/p1 $ python miller-rabin-Falsostestigos.py 10585
--- TEST MILLER-RABIN de 10585 ---
FALSOS TESTIGOS: [3, 9, 12, 16, 27, 48, 81, 97, 98, 108, 109, 127, 143, 144, 192, 213, 222, 242, 243, 256, 273, 298, 317, 327, 338, 362, 388, 392, 403, 432, 434, 462, 5
08, 572, 578, 607, 616, 661, 682, 707, 721, 727, 729, 733, 742, 757, 768, 797, 822, 827, 838, 852, 853, 873, 874, 882, 888, 943, 951, 968, 972, 981, 997, 998, 1003, 101
4, 1047, 1079, 1083, 1092, 1096, 1133, 1143, 1162, 1164, 1176, 1187, 1192, 1203, 1268, 1287, 1296, 1302, 1308, 1317, 1337, 1352, 1433, 1448, 1451, 1459, 1487, 1498, 152
7, 1552, 1558, 1568, 1583, 1587, 1603, 1604, 1612, 1667, 1703, 1728, 1744, 1756, 1758, 1777, 1787, 1813, 1837, 1848, 1873, 1894, 1917, 1922, 1933, 1983, 1998, 2026, 203
2, 2038, 2046, 2047, 2067, 2098, 2163, 2167, 2174, 2178, 2187, 2191, 2193, 2202, 2288, 2304, 2312, 2317, 2354, 2363, 2397, 2428, 2433, 2447, 2457, 2463, 2474, 2546, 256
7, 2578, 2593, 2622, 2647, 2653, 2678, 2682, 2707, 2719, 2728, 2747, 2756, 2798, 2823, 2828, 2853, 2882, 2897, 2904, 2908, 2917, 2932, 2936, 2943, 2947, 2968, 3018, 302
8, 3029, 3042, 3043, 3047, 3063, 3072, 3093, 3142, 3158, 3163, 3187, 3188, 3193, 3237, 3258, 3262, 3288, 3301, 3308, 3323, 3333, 3352, 3382, 3383, 3399, 3407, 3408, 341
2, 3437, 3443, 3477, 3492, 3498, 3507, 3523, 3527, 3528, 3552, 3553, 3623, 3627, 3634, 3641, 3659, 3662, 3673, 3698, 3758, 3772, 3773, 3802, 3842, 3851, 3872, 3888, 390
6, 3907, 3917, 3918, 3923, 3988, 3992, 4012, 4024, 4042, 4063, 4096, 4107, 4124, 4137, 4158, 4173, 4188, 4207, 4222, 4237, 4253, 4282, 4313, 4332, 4342, 4353, 4368, 437
7, 4418, 4447, 4461, 4477, 4478, 4494, 4503, 4507, 4532, 4538, 4572, 4593, 4622, 4623, 4631, 4636, 4637, 4648, 4676, 4742, 4748, 4768, 4783, 4793, 4812, 4853, 4903, 491
8, 4946, 4966, 4967, 5002, 5041, 5043, 5072, 5083, 5087, 5107, 5109, 5111, 5122, 5148, 5177, 5202, 5208, 5218, 5219, 5224, 5232, 5237, 5254, 5268, 5317, 5331, 5348, 535
3, 5361, 5366, 5367, 5377, 5383, 5408, 5437, 5463, 5474, 5476, 5478, 5498, 5502, 5513, 5542, 5544, 5583, 5618, 5619, 5639, 5667, 5682, 5732, 5773, 5792, 5802, 5817, 583
7, 5843, 5909, 5937, 5948, 5949, 5954, 5962, 5963, 5992, 6013, 6047, 6053, 6078, 6082, 6091, 6107, 6108, 6124, 6138, 6167, 6208, 6217, 6232, 6243, 6253, 6272, 6303, 633
2, 6348, 6363, 6378, 6397, 6412, 6427, 6448, 6461, 6478, 6489, 6522, 6543, 6561, 6573, 6593, 6597, 6662, 6667, 6668, 6678, 6679, 6697, 6713, 6734, 6743, 6783, 6812, 681
3, 6827, 6887, 6912, 6923, 6926, 6944, 6951, 6958, 6962, 7032, 7033, 7057, 7058, 7062, 7078, 7087, 7093, 7108, 7142, 7148, 7173, 7177, 7178, 7186, 7202, 7203, 7233, 725
2, 7262, 7277, 7284, 7297, 7323, 7327, 7348, 7392, 7397, 7398, 7422, 7427, 7443, 7492, 7513, 7522, 7538, 7542, 7543, 7556, 7557, 7567, 7617, 7638, 7642, 7649, 7653, 766
8, 7677, 7681, 7688, 7703, 7732, 7757, 7762, 7787, 7829, 7838, 7857, 7866, 7878, 7903, 7907, 7932, 7938, 7963, 7992, 8007, 8018, 8039, 8111, 8122, 8128, 8138, 8152, 815
7, 8188, 8222, 8231, 8268, 8273, 8281, 8297, 8383, 8392, 8394, 8398, 8407, 8411, 8418, 8422, 8487, 8518, 8538, 8539, 8547, 8553, 8559, 8587, 8602, 8652, 8663, 8668, 869
1, 8712, 8737, 8748, 8772, 8798, 8808, 8827, 8829, 8841, 8857, 8882, 8918, 8973, 8981, 8982, 8998, 9002, 9017, 9027, 9033, 9058, 9087, 9098, 9126, 9134, 9137, 9152, 923
3, 9248, 9268, 9277, 9283, 9289, 9298, 9317, 9382, 9393, 9398, 9409, 9421, 9423, 9442, 9452, 9489, 9493, 9502, 9506, 9538, 9571, 9582, 9587, 9588, 9604, 9613, 9617, 963
4, 9642, 9697, 9703, 9711, 9712, 9732, 9733, 9747, 9758, 9763, 9788, 9817, 9828, 9843, 9852, 9856, 9858, 9864, 9878, 9903, 9924, 9969, 9978, 10007, 10013, 10077, 10123,
 10151, 10153, 10182, 10193, 10197, 10223, 10247, 10258, 10268, 10287, 10312, 10329, 10342, 10343, 10363, 10372, 10393, 10441, 10442, 10458, 10476, 10477, 10487, 10488,
 10504, 10537, 10558, 10569, 10573, 10576, 10582, 10584]
```

```
victor@VKCOMPUTRON ~/Documents/UGR/2cuarto/cripto&comput/CRIPTO-COMPUTACION/p1 $ python miller-rabin-Falsostestigos.py 15841
--- TEST MILLER-RABIN de 15841 ---
FALSOS TESTIGOS: [4, 8, 16, 32, 64, 81, 128, 145, 162, 183, 215, 221, 235, 256, 290, 324, 363, 366, 373, 383, 430, 437, 442, 447, 470, 495, 507, 509, 512, 515, 543, 580
, 639, 648, 649, 659, 675, 726, 732, 746, 766, 785, 787, 801, 807, 860, 874, 877, 884, 885, 894, 940, 941, 981, 985, 990, 1014, 1018, 1021, 1024, 1030, 1059, 1086, 1091
, 1103, 1160, 1277, 1278, 1296, 1298, 1318, 1350, 1369, 1385, 1451, 1452, 1464, 1469, 1492, 1501, 1517, 1525, 1531, 1532, 1535, 1537, 1570, 1574, 1597, 1602, 1614, 1615
, 1661, 1681, 1697, 1720, 1748, 1754, 1768, 1770, 1788, 1807, 1809, 1857, 1880, 1882, 1899, 1962, 1970, 1980, 2003, 2007, 2028, 2036, 2042, 2048, 2060, 2081, 2118, 2172
, 2182, 2206, 2231, 2259, 2265, 2279, 2320, 2391, 2393, 2491, 2523, 2553, 2554, 2556, 2587, 2592, 2596, 2629, 2636, 2693, 2700, 2717, 2719, 2738, 2770, 2829, 2845, 2902
, 2904, 2921, 2928, 2929, 2938, 2984, 3002, 3025, 3029, 3034, 3050, 3062, 3064, 3065, 3070, 3074, 3140, 3147, 3148, 3194, 3203, 3204, 3228, 3230, 3249, 3253, 3281, 3287
, 3303, 3322, 3362, 3394, 3440, 3496, 3508, 3536, 3540, 3545, 3561, 3576, 3579, 3581, 3585, 3593, 3614, 3618, 3641, 3705, 3714, 3715, 3725, 3739, 3741, 3760, 3764, 3798
, 3833, 3851, 3867, 3905, 3924, 3940, 3960, 4006, 4014, 4019, 4051, 4056, 4072, 4084, 4087, 4089, 4096, 4120, 4125, 4129, 4157, 4162, 4225, 4233, 4236, 4323, 4343, 4344
, 4364, 4412, 4435, 4461, 4462, 4518, 4525, 4530, 4558, 4583, 4591, 4607, 4640, 4747, 4761, 4782, 4786, 4855, 4889, 4895, 4923, 4927, 4965, 4973, 4982, 5041, 5046, 5069
, 5106, 5108, 5112, 5147, 5174, 5184, 5191, 5192, 5247, 5258, 5272, 5297, 5325, 5347, 5386, 5400, 5434, 5438, 5457, 5459, 5473, 5476, 5493, 5540, 5547, 5617, 5625, 5629
, 5658, 5690, 5703, 5749, 5759, 5804, 5808, 5842, 5856, 5858, 5876, 5877, 5895, 5911, 5968, 5987, 5995, 6004, 6050, 6051, 6058, 6063, 6068, 6100, 6124, 6128, 6130, 6131
, 6140, 6148, 6269, 6277, 6280, 6294, 6296, 6319, 6347, 6388, 6406, 6408, 6456, 6460, 6498, 6506, 6561, 6562, 6574, 6606, 6627, 6644, 6659, 6675, 6724, 6725, 6781, 6788
, 6791, 6805, 6880, 6917, 6919, 6971, 6992, 7016, 7017, 7072, 7080, 7090, 7113, 7122, 7152, 7153, 7155, 7158, 7162, 7170, 7186, 7195, 7228, 7236, 7282, 7369, 7375, 7391
, 7410, 7428, 7430, 7450, 7478, 7482, 7517, 7520, 7527, 7528, 7583, 7591, 7596, 7601, 7649, 7663, 7666, 7667, 7673, 7697, 7702, 7729, 7734, 7739, 7803, 7810, 7813, 7829
, 7848, 7880, 7920, 7921, 7961, 7993, 8012, 8028, 8031, 8038, 8102, 8107, 8112, 8139, 8144, 8168, 8174, 8175, 8178, 8192, 8240, 8245, 8250, 8258, 8313, 8314, 8321, 8324
, 8359, 8363, 8391, 8411, 8413, 8431, 8450, 8466, 8472, 8559, 8605, 8613, 8646, 8655, 8671, 8679, 8683, 8686, 8688, 8689, 8719, 8728, 8751, 8761, 8769, 8824, 8825, 8849
, 8870, 8922, 8924, 8961, 9036, 9050, 9053, 9060, 9116, 9117, 9166, 9182, 9197, 9214, 9235, 9267, 9279, 9280, 9335, 9343, 9381, 9385, 9433, 9435, 9453, 9494, 9522, 9545
, 9547, 9561, 9564, 9572, 9693, 9701, 9710, 9711, 9713, 9717, 9741, 9773, 9778, 9783, 9790, 9791, 9837, 9846, 9854, 9873, 9930, 9946, 9964, 9965, 9983, 9985, 9999, 1003
3, 10037, 10082, 10092, 10138, 10151, 10183, 10212, 10216, 10224, 10294, 10301, 10348, 10365, 10368, 10382, 10384, 10403, 10407, 10441, 10455, 10494, 10516, 10544, 1056
9, 10583, 10594, 10649, 10650, 10657, 10667, 10694, 10729, 10733, 10735, 10772, 10795, 10800, 10859, 10868, 10876, 10914, 10918, 10946, 10952, 10986, 11055, 11059, 1108
0, 11094, 11201, 11234, 11250, 11258, 11283, 11311, 11316, 11323, 11379, 11380, 11406, 11429, 11477, 11497, 11498, 11518, 11605, 11608, 11616, 11679, 11684, 11712, 1171
6, 11721, 11745, 11752, 11754, 11757, 11769, 11785, 11790, 11822, 11827, 11835, 11881, 11901, 11917, 11936, 11974, 11990, 12008, 12043, 12077, 12081, 12100, 12102, 1211
6, 12126, 12127, 12136, 12200, 12223, 12227, 12248, 12256, 12260, 12262, 12265, 12280, 12296, 12301, 12305, 12333, 12345, 12401, 12447, 12479, 12519, 12538, 12554, 1256
0, 12588, 12592, 12611, 12613, 12637, 12638, 12647, 12693, 12694, 12701, 12767, 12771, 12776, 12777, 12779, 12791, 12807, 12812, 12816, 12839, 12857, 12903, 12912, 1291
3, 12920, 12937, 12939, 12996, 13012, 13071, 13103, 13122, 13124, 13141, 13148, 13205, 13212, 13245, 13249, 13254, 13285, 13287, 13288, 13318, 13350, 13448, 13450, 1352
1, 13562, 13576, 13582, 13610, 13635, 13659, 13669, 13723, 13760, 13781, 13793, 13799, 13805, 13813, 13834, 13838, 13861, 13871, 13879, 13942, 13959, 13961, 13984, 1403
2, 14034, 14053, 14071, 14073, 14087, 14093, 14121, 14144, 14160, 14180, 14226, 14227, 14239, 14244, 14267, 14271, 14304, 14306, 14309, 14310, 14316, 14324, 14340, 1434
9, 14372, 14377, 14389, 14390, 14456, 14472, 14491, 14523, 14543, 14545, 14563, 14564, 14681, 14738, 14750, 14755, 14782, 14811, 14817, 14820, 14823, 14827, 14851, 1485
6, 14860, 14900, 14901, 14947, 14956, 14957, 14964, 14967, 14981, 15034, 15040, 15054, 15056, 15075, 15095, 15109, 15115, 15166, 15182, 15192, 15193, 15202, 15261, 1529
8, 15326, 15329, 15332, 15334, 15346, 15371, 15394, 15399, 15404, 15411, 15458, 15468, 15475, 15478, 15517, 15551, 15585, 15606, 15620, 15626, 15658, 15679, 15696, 1571
3, 15760, 15777, 15809, 15825, 15833, 15837, 15839, 15840]
victor@VKCOMPUTRON ~/Documents/UGR/2cuarto/cripto&comput/CRIPTO-COMPUTACION/p1 $
```

```
victor@VKCOMPUTRON ~/Documents/UGR/2cuarto/cripto&comput/CRIPTO-COMPUTACION/p1
File  Edit  View  Search  Terminal  Help
victor@VKCOMPUTRON ~/Documents/UGR/2cuarto/cripto&comput/CRIPTO-COMPUTACION/p1 $ python miller-rabin-Falsostestigos.py 29341
--- TEST MILLER-RABIN de 29341 ---
FALSOS TESTIGOS: [4, 6, 8, 9, 16, 18, 24, 31, 32, 36, 50, 54, 59, 64, 72, 81, 89, 93, 96, 98, 118, 124, 128, 144, 150, 154, 162, 177, 190, 193, 200, 214, 216, 227, 236,
 242, 254, 256, 265, 267, 269, 279, 281, 288, 294, 324, 331, 356, 367, 372, 383, 384, 386, 392, 401, 409, 421, 450, 457, 462, 472, 486, 496, 497, 499, 505, 512, 526, 53
1, 538, 541, 557, 562, 570, 576, 577, 578, 579, 587, 595, 600, 616, 625, 631, 642, 643, 648, 661, 681, 695, 697, 708, 709, 721, 722, 726, 729, 734, 751, 760, 762, 769,
772, 775, 782, 785, 789, 791, 795, 799, 800, 801, 815, 837, 842, 843, 856, 864, 865, 867, 881, 882, 886, 905, 908, 917, 937, 938, 943, 944, 947, 961, 968, 970, 971, 982
, 986, 993, 994, 1007, 1016, 1019, 1024, 1055, 1058, 1060, 1062, 1068, 1076, 1081, 1087, 1090, 1116, 1124, 1129, 1133, 1142, 1149, 1152, 1165, 1176, 1189, 1190, 1195, 1
202, 1203, 1227, 1241, 1243, 1250, 1253, 1263, 1286, 1289, 1296, 1318, 1319, 1324, 1334, 1350, 1363, 1371, 1386, 1390, 1393, 1411, 1418, 1424, 1435, 1438, 1441, 1442, 1
458, 1459, 1462, 1468, 1474, 1475, 1488, 1493, 1497, 1502, 1505, 1515, 1519, 1523, 1532, 1536, 1544, 1549, 1550, 1562, 1568, 1578, 1587, 1590, 1593, 1597, 1604, 1610, 1
614, 1623, 1630, 1636, 1645, 1657, 1670, 1671, 1679, 1682, 1684, 1685, 1697, 1710, 1713, 1731, 1734, 1737, 1761, 1762, 1763, 1799, 1800, 1817, 1828, 1848, 1865, 1867, 1
870, 1871, 1874, 1888, 1893, 1909, 1919, 1922, 1925, 1926, 1929, 1933, 1942, 1944, 1969, 1977, 1978, 1981, 1983, 1984, 1988, 1996, 2001, 2020, 2021, 2030, 2043, 2048, 2
085, 2091, 2095, 2104, 2111, 2114, 2117, 2124, 2127, 2149, 2152, 2163, 2164, 2165, 2166, 2178, 2189, 2193, 2202, 2203, 2225, 2228, 2234, 2248, 2251, 2255, 2258, 2261, 2
280, 2281, 2286, 2291, 2298, 2304, 2305, 2307, 2308, 2312, 2316, 2325, 2329, 2343, 2346, 2348, 2351, 2355, 2373, 2375, 2380, 2381, 2385, 2386, 2387, 2390, 2397, 2400, 2
401, 2403, 2407, 2410, 2411, 2421, 2423, 2429, 2450, 2464, 2467, 2477, 2494, 2500, 2503, 2506, 2511, 2523, 2524, 2529, 2530, 2533, 2555, 2568, 2572, 2585, 2592, 2595, 2
605, 2621, 2633, 2641, 2644, 2646, 2647, 2658, 2675, 2686, 2715, 2719, 2724, 2729, 2751, 2762, 2777, 2780, 2786, 2788, 2789, 2805, 2814, 2822, 2827, 2829, 2832, 2833, 2
836, 2841, 2870, 2878, 2882, 2884, 2887, 2888, 2891, 2904, 2905, 2910, 2916, 2917, 2918, 2936, 2945, 2946, 2958, 2966, 2979, 2982, 2983, 2986, 2995, 3004, 3010, 3021, 3
040, 3048, 3057, 3073, 3076, 3079, 3088, 3097, 3098, 3100, 3113, 3122, 3128, 3139, 3140, 3151, 3156, 3164, 3165, 3174, 3180, 3190, 3194, 3196, 3200, 3204, 3205, 3239, 3
243, 3247, 3253, 3260, 3261, 3270, 3271, 3287, 3290, 3303, 3317, 3322, 3347, 3348, 3349, 3358, 3361, 3362, 3365, 3368, 3372, 3373, 3385, 3386, 3387, 3398, 3399, 3403, 3
424, 3426, 3427, 3439, 3447, 3456, 3460, 3462, 3468, 3474, 3481, 3495, 3511, 3517, 3521, 3524, 3528, 3530, 3544, 3567, 3569, 3570, 3579, 3581, 3606, 3607, 3609, 3615, 3
620, 3632, 3634, 3658, 3668, 3671, 3675, 3677, 3681, 3686, 3698, 3713, 3723, 3729, 3734, 3739, 3742, 3748, 3750, 3751, 3752, 3759, 3767, 3772, 3776, 3788, 3789, 3803, 3
817, 3833, 3844, 3847, 3850, 3853, 3854, 3866, 3867, 3872, 3880, 3884, 3893, 3898, 3901, 3902, 3928, 3929, 3937, 3941, 3943, 3944, 3949, 3954, 3957, 3966, 3967, 3972, 3
973, 3976, 3983, 3998, 4002, 4009, 4015, 4019, 4028, 4050, 4064, 4076, 4089, 4093, 4096, 4113, 4115, 4127, 4142, 4158, 4166, 4179, 4182, 4201, 4220, 4232, 4233, 4234, 4
240, 4248, 4249, 4253, 4265, 4267, 4272, 4298, 4304, 4305, 4310, 4314, 4321, 4323, 4324, 4337, 4348, 4349, 4360, 4361, 4374, 4386, 4391, 4406, 4409, 4418, 4422, 4425, 4
427, 4435, 4449, 4464, 4473, 4479, 4483, 4490, 4491, 4496, 4502, 4506, 4516, 4522, 4531, 4532, 4541, 4543, 4545, 4557, 4562, 4565, 4568, 4569, 4582, 4583, 4596, 4607, 4
608, 4610, 4630, 4637, 4643, 4647, 4660, 4686, 4691, 4704, 4709, 4714, 4721, 4730, 4734, 4750, 4751, 4756, 4757, 4760, 4765, 4774, 4779, 4780, 4786, 4790, 4791, 4794, 4
795, 4802, 4808, 4812, 4825, 4829, 4830, 4842, 4846, 4869, 4870, 4882, 4886, 4890, 4903, 4906, 4908, 4934, 4935, 4954, 4964, 4971, 4972, 4973, 4981, 5000, 5010, 5012, 5
013, 5026, 5037, 5043, 5046, 5052, 5055, 5058, 5079, 5089, 5091, 5098, 5101, 5114, 5130, 5141, 5144, 5156, 5167, 5173, 5184, 5193, 5195, 5202, 5211, 5215, 5227, 5255, 5
261, 5266, 5267, 5272, 5276, 5282, 5283, 5286, 5289, 5295, 5296, 5297, 5299, 5309, 5315, 5321, 5336, 5345, 5350, 5351, 5353, 5355, 5389, 5397, 5400, 5419, 5452, 5453, 5
```

En el Anexo se encuentra la salida obtenida de las listas de falsos testigos de algunos de los ejemplos

Apartados 7 y 8.

Utiliza el test de primalidad de Miller-Rabin y las funciones previamente implementadas para elegir 2 números compuestos, elegir 200 testigos al azar y ver cuáles son falsos testigos. Se han elegido arbitrariamente los 2 primeros números compuestos (el primero, el 4991, presenta en ocasiones falsos testigos).

Cabe destacar que el test de Miller-Rabin se emplea con frecuencia pues su probabilidad de error es casi ínfima, menor que 1/(4^m) siendo m el número de testigos. Con 200 testigos esta probabilidad de error, de encontrar falsos testigos, resulta notablemente pequeña. A pesar de haber probado con múltiples números compuestos, más grandes o más pequeños, apenas encontramos excepto en contadas ocasiones falsos testigos. Sin embargo, con los 2 números compuestos dados en el apartado 8, son casos donde la probabilidad de encontrar falsos testigos es anormalmente alta.

Ejecución en Linux: python apartados78.py

Anexo.

$ python miller-rabin-Falsostestigos.py 6601

--- TEST MILLER-RABIN de 6601 ---

FALSOS TESTIGOS: [16, 18, 40, 45, 66, 78, 100, 122, 141, 165, 195, 242, 250, 256, 286, 288, 303, 305, 318, 324, 327, 332, 338, 433, 474, 482, 508, 517, 523, 573, 605, 611, 619, 625, 640, 652, 715, 720, 739, 769, 795, 804, 810, 821, 824, 830, 843, 845, 877, 898, 927, 961, 983, 1002, 1056, 1082, 1091, 1108, 1111, 1117, 1132, 1147, 1166, 1185, 1188, 1193, 1199, 1205, 1248, 1270, 1289, 1313, 1369, 1378, 1404, 1417, 1451, 1453, 1466, 1513, 1527, 1576, 1581, 1600, 1630, 1644, 1671, 1682, 1691, 1721, 1738, 1753, 1762, 1767, 1773, 1779, 1788, 1800, 1868, 1887, 1931, 1952, 1964, 1972, 1993, 2008, 2010, 2025, 2027, 2054, 2060, 2075, 2101, 2109, 2131, 2174, 2196, 2204, 2218, 2245, 2256, 2259, 2312, 2347, 2396, 2483, 2491, 2505, 2526, 2538, 2543, 2567, 2584, 2601, 2614, 2634, 2640, 2661, 2705, 2729, 2770, 2813, 2830, 2869, 2888, 2907, 2915, 2927, 2936, 2948, 2962, 2970, 3057, 3079, 3091, 3117, 3120, 3139, 3156, 3175, 3188, 3202, 3249, 3298, 3303, 3352, 3399, 3413, 3426, 3445, 3462, 3481, 3484, 3510, 3522, 3544, 3631, 3639, 3653, 3665, 3674, 3686, 3694, 3713, 3732, 3771, 3788, 3831, 3872, 3896, 3940, 3961, 3967, 3987, 4000, 4017, 4034, 4058, 4063, 4075, 4096, 4110, 4118, 4205, 4254, 4289, 4342, 4345, 4356, 4383, 4397, 4405, 4427, 4470, 4492, 4500, 4526, 4541, 4547, 4574, 4576, 4591, 4593, 4608, 4629, 4637, 4649, 4670, 4714, 4733, 4801, 4813, 4822, 4828, 4834, 4839, 4848, 4863, 4880, 4910, 4919, 4930, 4957, 4971, 5001, 5020, 5025, 5074, 5088, 5135, 5148, 5150, 5184, 5197, 5223, 5232, 5288, 5312, 5331, 5353, 5396, 5402, 5408, 5413, 5416, 5435, 5454, 5469, 5484, 5490, 5493, 5510, 5519, 5545, 5599, 5618, 5640, 5674, 5703, 5724, 5756, 5758, 5771, 5777, 5780, 5791, 5797, 5806, 5832, 5862, 5881, 5886, 5949, 5961, 5976, 5982, 5990, 5996, 6028, 6078, 6084, 6093, 6119, 6127, 6168, 6263, 6269, 6274, 6277, 6283, 6296, 6298, 6313, 6315, 6345, 6351, 6359, 6406, 6436, 6460, 6479, 6501, 6523, 6535, 6556, 6561, 6583, 6585, 6600]

$ python miller-rabin-Falsostestigos.py 10585

--- TEST MILLER-RABIN de 10585 ---

FALSOS TESTIGOS: [3, 9, 12, 16, 27, 48, 81, 97, 98, 108, 109, 127, 143, 144, 192, 213, 222, 242, 243, 256, 273, 298, 317, 327, 338, 362, 388, 392, 403, 432, 434, 462, 508, 572, 578, 607, 616, 661, 682, 707, 721, 727, 729, 733, 742, 757, 768, 797, 822, 827, 838, 852, 853, 873, 874, 882, 888, 943, 951, 968, 972, 981, 997, 998, 1003, 1014, 1047, 1079, 1083, 1092, 1096, 1133, 1143, 1162, 1164, 1176, 1187, 1192, 1203, 1268, 1287, 1296, 1302, 1308, 1317, 1337, 1352, 1433, 1448, 1451, 1459, 1487, 1498, 1527, 1552, 1558, 1568, 1583, 1587, 1603, 1604, 1612, 1667, 1703, 1728, 1744, 1756, 1758, 1777, 1787, 1813, 1837, 1848, 1873, 1894, 1917, 1922, 1933, 1983, 1998, 2026, 2032, 2038, 2046, 2047, 2067, 2098, 2163, 2167, 2174, 2178, 2187, 2191, 2193, 2202, 2288, 2304, 2312, 2317, 2354, 2363, 2397, 2428, 2433, 2447, 2457, 2463, 2474, 2546, 2567, 2578, 2593, 2622, 2647, 2653, 2678, 2682, 2707, 2719, 2728, 2747, 2756, 2798, 2823, 2828, 2853, 2882, 2897, 2904, 2908, 2917, 2932, 2936, 2943, 2947, 2968, 3018, 3028, 3029, 3042, 3043, 3047, 3063, 3072, 3093, 3142, 3158, 3163, 3187, 3188, 3193, 3237, 3258, 3262, 3288, 3301, 3308, 3323, 3333, 3352, 3382, 3383, 3399, 3407, 3408, 3412, 3437, 3443, 3477, 3492, 3498, 3507, 3523, 3527, 3528, 3552, 3553, 3623, 3627, 3634, 3641, 3659, 3662, 3673, 3698, 3758, 3772, 3773, 3802, 3842, 3851, 3872, 3888, 3906, 3907, 3917, 3918, 3923, 3988, 3992, 4012, 4024, 4042, 4063, 4096, 4107, 4124, 4137, 4158, 4173, 4188, 4207, 4222, 4237, 4253, 4282, 4313, 4332, 4342, 4353, 4368, 4377, 4418, 4447, 4461, 4477, 4478, 4494, 4503, 4507, 4532, 4538, 4572, 4593, 4622, 4623, 4631, 4636, 4637, 4648, 4676, 4742, 4748, 4768, 4783, 4793, 4812, 4853, 4903, 4918, 4946, 4966, 4967, 5002, 5041, 5043, 5072, 5083, 5087, 5107, 5109, 5111, 5122, 5148, 5177, 5202, 5208, 5218, 5219, 5224, 5232, 5237, 5254, 5268, 5317, 5331, 5348, 5353, 5361, 5366, 5367, 5377, 5383, 5408, 5437, 5463, 5474, 5476, 5478, 5498, 5502, 5513, 5542, 5544, 5583, 5618, 5619, 5639, 5667, 5682, 5732, 5773, 5792, 5802, 5817, 5837, 5843, 5909, 5937, 5948, 5949, 5954, 5962,

5963, 5992, 6013, 6047, 6053, 6078, 6082, 6091, 6107, 6108, 6124, 6138, 6167, 6208, 6217, 6232, 6243, 6253, 6272, 6303, 6332, 6348, 6363, 6378, 6397, 6412, 6427, 6448, 6461, 6478, 6489, 6522, 6543, 6561, 6573, 6593, 6597, 6662, 6667, 6668, 6678, 6679, 6697, 6713, 6734, 6743, 6783, 6812, 6813, 6827, 6887, 6912, 6923, 6926, 6944, 6951, 6958, 6962, 7032, 7033, 7057, 7058, 7062, 7078, 7087, 7093, 7108, 7142, 7148, 7173, 7177, 7178, 7186, 7202, 7203, 7233, 7252, 7262, 7277, 7284, 7297, 7323, 7327, 7348, 7392, 7397, 7398, 7422, 7427, 7443, 7492, 7513, 7522, 7538, 7542, 7543, 7556, 7557, 7567, 7617, 7638, 7642, 7649, 7653, 7668, 7677, 7681, 7688, 7703, 7732, 7757, 7762, 7787, 7829, 7838, 7857, 7866, 7878, 7903, 7907, 7932, 7938, 7963, 7992, 8007, 8018, 8039, 8111, 8122, 8128, 8138, 8152, 8157, 8188, 8222, 8231, 8268, 8273, 8281, 8297, 8383, 8392, 8394, 8398, 8407, 8411, 8418, 8422, 8487, 8518, 8538, 8539, 8547, 8553, 8559, 8587, 8602, 8652, 8663, 8668, 8691, 8712, 8737, 8748, 8772, 8798, 8808, 8827, 8829, 8841, 8857, 8882, 8918, 8973, 8981, 8982, 8998, 9002, 9017, 9027, 9033, 9058, 9087, 9098, 9126, 9134, 9137, 9152, 9233, 9248, 9268, 9277, 9283, 9289, 9298, 9317, 9382, 9393, 9398, 9409, 9421, 9423, 9442, 9452, 9489, 9493, 9502, 9506, 9538, 9571, 9582, 9587, 9588, 9604, 9613, 9617, 9634, 9642, 9697, 9703, 9711, 9712, 9732, 9733, 9747, 9758, 9763, 9788, 9817, 9828, 9843, 9852, 9856, 9858, 9864, 9878, 9903, 9924, 9969, 9978, 10007, 10013, 10077, 10123, 10151, 10153, 10182, 10193, 10197, 10223, 10247, 10258, 10268, 10287, 10312, 10329, 10342, 10343, 10363, 10372, 10393, 10441, 10442, 10458, 10476, 10477, 10487, 10488, 10504, 10537, 10558, 10569, 10573, 10576, 10582, 10584]