Homework 04

HOMEWORK 04, DUE BY 2022-02-12

Question 1: Let $\mathbb{Z}_n$ denote the set of all congruence classes modulo n. For each function $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$ find the *cardinality of the range* of f – namely, the count of elements $y \in \mathbb{Z}_n$ that can be values $f(x)$ for some $x \in \mathbb{Z}_n$. Provide brief explanations for your answers.

(A) $f_1\colon \mathbb{Z}_{41} \to \mathbb{Z}_{41}$ defined by $f_1(n) = (18n + 5) \bmod 41$.

(B) $f_2\colon \mathbb{Z}_{44} \to \mathbb{Z}_{44}$ defined by $f_2(n) = (18n + 5) \bmod 44$.

(C) $f_3\colon \mathbb{Z}_{41} \to \mathbb{Z}_{41}$ defined by $f_3(n) = n^5 \bmod 41$.

(D) $f_4\colon \mathbb{Z}_{41} \to \mathbb{Z}_{41}$ defined by $f_4(n) = 5^n \bmod 41$.

(E) $f_5\colon \mathbb{Z}_{49} \to \mathbb{Z}_{49}$ defined by $f_5(n) = 5^n \bmod 49$.

Answer:

(A) The range of f_1 has 41 elements.

Moreover, for every $a \in \mathbb{Z}_{41}$ it is possible to solve the congruence: $18n + 5 \equiv a \pmod{41}$ with a simple formula (so every element in the range can have its inverse image effectively computed).

Find the inverse of 18 modulo 41. It is 16, since $18 \cdot 16 = 288 \equiv 1 \pmod{41}$.

Then $18n \equiv (a - 5) \pmod{41}$, then multiply both sides of the congruence by $18^{-1} = 16$:

$$n \equiv 16 \cdot (a - 5) \pmod{41}.$$

(B) The range of f_2 has 22 elements.

In particular, for every **odd** number $a \in \mathbb{Z}_{44}$ it is possible to solve $18n + 5 \equiv a \pmod{44}$. We could provide a formula, but there is also a simpler way – Bezout identity.

Since $\gcd(18, 44) = 2$, there must exist integers $x, y \in \mathbb{Z}$ such that $18x + 44y = 2$. This also means that it is possible to solve equation $18x + 44y = 2k$ for any even number $2k$.

Example: We have $18 \cdot (5) + 44 \cdot (-2) = 2$. To solve an equation for another even number (say, 4), multiply both sides by k:

$$18 \cdot (5k) + 44 \cdot (-2k) = 2k.$$

Therefore, $18 \cdot (5k) \equiv 2k \pmod{44}$. And that means that $f_2(n) = (18n + 5) \bmod 44$ will take any odd value $2k + 5$ modulo 44 once we plug in value $n = 5k$.

(C) The range of f_3 has 9 elements.

To compute all the possible values of n^5, analytical methods can be used, but direct computation on Python could be easier:

```
>>> [n**5 % 41 for n in range (0,41)]
[0, 1, 32, 38, 40, 9, 27, 38, 9, 9, 1, 3, 3, 38, 27, 14, 1, 27, 1, 27, 32, 9, 14,␣
↪40, 14, 40, 27, 14, 3, 38, 38, 40, 32, 32, 3, 14, 32, 1, 3, 9, 40]
>>> set([n**5 % 41 for n in range (0,41)])
{0, 1, 32, 3, 38, 40, 9, 14, 27}
```

(D) The range of f_4 has 21 elements (the remainder 0, and also exactly one half of the non-zero remainders modulo 41).

Number 5 is not a primitive root modulo 41 (in fact, we have $13^2 \equiv 5 \pmod{41}$; therefore $5^{20} \equiv (13^2)^{20} \equiv 13^{40} \equiv 1 \pmod{41}$. This means that the powers of 5 loop already after the power 5^{20} which is congruent to 1 modulo 41.

The following computation shows that there are indeed no more than 21 remainders among the powers of 5 modulo 41:

```
>>> [5**n % 41 for n in range (0,41)]
[1, 5, 25, 2, 10, 9, 4, 20, 18, 8, 40, 36, 16, 39, 31, 32, 37, 21, 23, 33, 1, 5,␣
↪25, 2, 10, 9, 4, 20, 18, 8, 40, 36, 16, 39, 31, 32, 37, 21, 23, 33, 1]
>>> set([5**n % 41 for n in range (0,41)])
{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40}
```

(E) The range of f_5 has 42 elements.

In fact, we can get every remainder which is mutually prime with 49 (not divisible by 7).

```
>>> set([5**n % 49 for n in range (0,49)])
{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25,␣
↪26, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48}
>>> len(set([5**n % 49 for n in range (0,49)]))
42
```

Question 2:

(A) Find $\gcd(\gcd(\gcd(81719, 52003), 33649), 30107)$ showing the steps of Euclidean algorithm.

(B) Let $\gcd(a, b, c)$ be the *greatest common divisor* of 3 numbers $a, b, c \in \mathbb{Z}^+$ – the largest $d \in \mathbb{Z}^+$ such that $d \mid a$, and $d \mid b$, and $d \mid c$. Prove that any integer m divides $\gcd(a, b, c)$ iff m divides $\gcd(\gcd(a, b), c)$.

(C) Prove that $\gcd(a, b, c) = d$ is the smallest positive integer obtainable in the form $d = ax + by + cz$, where $x, y, z \in \mathbb{Z}$. (*Hint:* Apply Bézouts identity repeatedly.)

Answer:

(A) Do the computation (three times apply Euclidean algorithm) from inside out:

$$\begin{aligned}
\gcd(\gcd(\gcd(81719, 52003), 33649), 30107) &= \gcd(\gcd(\gcd(52003, 29716), 33649), 30107) = \\
&= \gcd(\gcd(\gcd(29716, 22287), 33649), 30107) = \gcd(\gcd(\gcd(22287, 7429), 33649), 30107) = \\
&= \gcd(\gcd(\gcd(7429, 0), 33649), 30107) = \gcd(\gcd(7429, 33649), 30107) = \\
&= \gcd(\gcd(33649, 7429), 30107) = \gcd(\gcd(7429, 3933), 30107) = \\
&= \gcd(\gcd(3496, 437), 30107) = \gcd(\gcd(437, 0), 30107) = \gcd(437, 30107) = \\
&= \gcd(30107, 437) = \gcd(437, 391) = \gcd(391, 46) = \gcd(46, 23) = \gcd(23, 0) = 23.
\end{aligned}$$

(B) Denote two numbers: $d_1 = \gcd(a, b, c)$ and $d_2 = \gcd(\gcd(a, b), c)$.

Part 1: Assume that m divides d_1 and prove that m also divides d_2. Since (by definition) d_1 is the greatest among those positive integers that divide all a, b, c, we also must have that $m \div a$, $m \div b$, $m \div c$.

For this reason m also divides the greatest common divisor of a, b (since it divides both a and b). Finally, m must also divide $\gcd(\gcd(a,b),c) = d_2$, since it also divides c.

Part 2: Assume that m divides $d_2 = \gcd(\gcd(a,b),c)$, so it divides both $\gcd(a,b)$ and c. But then it must also divide a and b separately. So it divides the greatest common divisor of all three numbers: $d_1 = \gcd(a,b,c)$.

(C) Denote $k = \gcd(a,b)$. Then $d = \gcd(a,b,c)$ (and since (B) has been shown), we also have $d = \gcd(\gcd(a,b),c) = \gcd(k,c)$.

By Bézouts identity (applied to $d = \gcd(k,c)$) there should be an integer solution $x, y \in \mathbb{Z}$ such that

$$k \cdot x + c \cdot y = d.$$

By Bézouts identity (applied to $k = \gcd(a,b)$) there should also be an integer solution $X, Y \in \mathbb{Z}$ such that

$$a \cdot X + b \cdot Y = k.$$

Insert the second identity into the first one:

$$d = k \cdot x + c \cdot y = (a \cdot X + b \cdot Y) \cdot x + c \cdot y = a \cdot (X \cdot x) + b \cdot (Y \cdot x) + c \cdot y.$$

Thus the equation $d = ax^* + by^* + cz^*$ also has an integer solution:

$$\begin{cases} x^* = X \cdot x \\ y^* = Y \cdot x \\ z^* = y \end{cases}$$

Question 3:

(A) How many integers between 1 and 1000 inclusive has a remainder 1 when divided by 7 and a remainder 3 when divided by 4?

(B) Write a formula (depending on the parameter n) to find the count of integer solutions $x \in [1; n]$ to the following system:

$$\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 3 \pmod 4 \end{cases}$$

(C) Find the smallest positive integer that has a remainder 5 when divided by 7, a remainder of 6 when divided by 11, and a remainder of 4 when divided by 13.

(D) Write an expression (depending on parameters a, b, c) to compute the smallest positive integer x that is the solution of the system of congruences:

$$\begin{cases} x \equiv a \pmod 7 \\ x \equiv b \pmod{11} \\ x \equiv c \pmod{13} \end{cases}$$

Note: Formulas in (B), (D) may use arithmetic operations, the floor ($\lfloor x \rfloor$), the ceiling $\lceil x \rceil$, integer division ($k \operatorname{div} \ell$), and remainder ($k \bmod \ell$). For modular multiplicative inverses see https://bit.ly/348GVqJ.

Answer:

(A) How many integers between 1 and 1000 inclusive has a remainder 1 when divided by 7 and a remainder 3 when divided by 4?

Consider all numbers that have remainder 1 when divided by 7 inside $[0; 28)$. There are four such numbers: $1, 8, 15, 22$. Exactly one of them gives remainder 3 when divided by 4. It is $x = 15$. But **both** remainders (by

4 and by 7) repeat as we add $4 \cdot 7 = 28$. So both remainders are correct for all the numbers $15 + 28k$, where $k \in \mathbb{Z}$. (Here 15 is just one among the solutions, where $k = 0$.)

The smallest such number is $15 \in [1; 1000]$, the largest one is $995 \in [1; 1000]$ as it also satisfies $995 = 15+28k$, where $k = 35$.

Altogether there are 36 numbers in the sequence $15, 43, 71, 99, 127, 155, \ldots, 995$ (for $k = 0, \ldots, 35$).

(B) We need to build an expression $f(n)$ that satisfies this condition:

$$f(n) = \begin{cases} 0, & \text{if } n < 15, \\ 1, & \text{if } 15 \le n < 43, \\ 2, & \text{if } 43 \le n < 71, \\ 3, & \text{if } 71 \le n < 99, \\ \ldots & \\ k, & \text{if } 15 + 28 \cdot (k-1) \le n < 15 + 28k. \end{cases}$$

Since this function is roughly a slowly growing linear function (just rounded to an integer value), we can write this system as a more compact formula:

$$f(n) = \left\lfloor \frac{n+13}{28} \right\rfloor.$$

- If we substitute $n = 15$, then it is $\lfloor (15+13)/28 \rfloor = \lfloor 28/28 \rfloor = 1$,
- If we substitute $n = 43$, then it is $\lfloor (43+13)/28 \rfloor = \lfloor 56/28 \rfloor = 2$, and so on.

(C) In practice we can solve such systems (for small modulos) by excluding the congruences one by one:

- Natural numbers $n \equiv 4 \pmod{13}$ are written in form $4 + 13k$:

$$4, 17, 30, 43, \ldots `.$$

Already the number 17 in this sequence also satisfies $17 \equiv 6 \pmod{11}$. So we have satisfied already two of the congruences ($n \equiv 4 \pmod{13}$ and also $n \equiv 6 \pmod{11}$).

Since 11 and 13 are mutually prime, the general solution of these two congruences is $17 + 143k$, where $k \in \mathbb{Z}$.

- Now write out all the numbers $n \equiv 17 \pmod{143}$ that are written in form $17 + 143k$ (and also their remainders modulo 7):

17	160	303	446	589	732	875
3	6	2	5	1	4	0

The remainder of 446 when divided by 7 has remainder 5.

The number $n = 446$ is indeed the smallest positive integer that satisfies all three congruences:

$$\begin{cases} n \equiv 5 \pmod{7} \\ n \equiv 6 \pmod{11} \\ n \equiv 4 \pmod{13} \end{cases}$$

The product of $7 \cdot 11 \cdot 13 = 1001$, so the general solution is $n = 446 + 1001k$.

(D) As explained in (Rosen2019), Chapter 4.4.3, page 293, it is possible to write an explicit formula to solve Chinese Remainder theorem:

First find the modular multiplicative inverses (see https://bit.ly/348GVqJ):

- $(11 \cdot 13)^{-1} = (133)^{-1} = 5 \pmod{7}$
- $(7 \cdot 13)^{-1} = (91)^{-1} = 4 \pmod{11}$

- $(7 \cdot 11)^{-1} = (77)^{-1} = 12 \pmod{13}$

Then the general formula solving the system of congruences is this:

$$a \cdot (5 \cdot 11 \cdot 13) + b \cdot (4 \cdot 7 \cdot 13) + c \cdot (12 \cdot 7 \cdot 11) = 715a + 364b + 924c.$$

Note: We could apply this formula to the previous question (C) – the remainders $a = 5$, $b = 6$, $c = 4$.

$$715a + 364b + 924c = 715 \cdot 5 + 364 \cdot 6 + 924 \cdot 4 = 9455.$$

This is one of the solutions to the congruence system, but the smallest one is $9455 \bmod 1001 = 446$.

Question 4: Translate every predicate expression in plain English, use number theory concepts whenever possible. Prove or disprove the statements.

Predicate $m \mid n$ is true iff m divides n; predicate $\text{ISPRIME}(p)$ is true iff p is a prime.

(A) $\exists a_0 \in \mathbb{N}\, \exists d \in \mathbb{N} \Big(d > 0 \wedge \forall k \in \mathbb{N}\, \forall m \in \mathbb{N} \big((m \mid (a_0 + k \cdot d)) \to (m = 1 \vee m = a_0 + k \cdot d) \big) \Big)$.

(B) $\forall p \in \mathbb{N}\, \exists a \in \mathbb{N}\, ((\text{ISPRIME}(p) \wedge \neg(2 \mid p)) \to a \neq 1 \wedge a^{\frac{p-1}{2}} \equiv 1 \pmod{p})$.

(C) $\forall k \in \mathbb{N} \Big(k \geq 2 \to \forall n \in \mathbb{N}\, \forall j \in \mathbb{N} \big(j < k \to \forall m \in \mathbb{N} \big((1 < m \wedge m < k) \to \neg(m \mid (n + j)) \big) \big) \Big)$.

Answer:

(A) English: "There exists an increasing arithmetic series of integers containing only prime numbers." (It is `False`).

To translate into English, observe that $a_0 + k \cdot d$ is a prime number whenever

$$\forall m \in \mathbb{N} \big((m \mid (a_0 + k \cdot d)) \to (m = 1 \vee m = a_0 + k \cdot d) \big).$$

Namely, if some m divides it, then m must be 1 or equal the number itself. Thus the longer formula says that there exist natural numbers a_0 and d such that $d > 0$ and all terms of the arithmetic series $a_0 + k \cdot d$ are prime numbers.

To see that it is false, you can consider these cases:

Case 1: If $a_0 > 1$, select $k = a_0$, and the number $a_0 + k \cdot d = a_0 + a_0 \cdot d = a_0(1 + d)$ is divisible by $d + 1 > 1$, and $d + 1 \neq a_0(1 + d)$, since $a_0 > 1$. (So, the number $a_0(1 + d)$ is not a prime.

Case 2: If $a_0 = 1$, select $k = d + 2$. Then $a_0 + k \cdot d = 1 + (d + 2) \cdot d = 1 + d^2 + 2d = (1 + d)^2$. This is a full square and larger than 1, so it is not a prime number.

Case 3: If $a_0 = 0$, select $k = 4$. Then $a_0 + k \cdot d = 0 + 4 \cdot d = 4d > 0$, which is not a prime, since it is divisible by 4.

(B) English: "For every odd prime p there is an integer $a > 1$ such that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$." (This is `True`.)

Indeed, you can select $a = p + 1$. Then the number a is congruent to 1 and

$$a^{\frac{p-1}{2}} \equiv 1^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

For $p > 3$ you can even find a number a which is **not** congruent to 1 modulo p and still satisfies the congruence $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. One can select $a = g^2$, where g is some primitive root modulo p. In this case $a^{\frac{p-1}{2}} \equiv (g^2)^{\frac{p-1}{2}} = g^{p-1} \equiv 1$ by the Little Fermat theorem.

(C) This one is less obvious, so we will try to rewrite the predicate expression, assuming that the domain set is $\mathbb{N}$ – all natural numbers (non-negative integers).

$$\forall k \in \mathbb{N}\ \Big(k \geq 2 \to \forall n \in \mathbb{N}\ \forall j \in \mathbb{N}\ \big(j < k \to \forall m \in \mathbb{N}\ \big((1 < m \wedge m < k) \to \neg(m \mid (n+j))\big)\big)\Big) \equiv$$
$$\equiv \forall k \geq 2\ \forall n \in \mathbb{N}\ \forall j \in \mathbb{N}\ \big(j < k \to \forall m \in [2; k-1]\ \big((n+j) \text{ is not divisible by } m\big)\big) \equiv$$
$$\equiv \forall k \geq 2\ \forall n \in \mathbb{N}\ \forall j \in [0; k)\ \big((n+j) \text{ is not divisible by any number from } [2; k-1]\big)\big) \equiv$$
$$\equiv \forall k \geq 2\ \big(\text{none of the numbers } n, n+1, \ldots, n+k-1 \text{ is divisible by any number from } [2; k-1]\big)\big)$$

English: "For all $k \geq 2$, each sequence of k consecutive positive integers contains a number that is not divisible by any integer in $[2; k-1]$." (This is `False`.)

For example, pick $k = 8$, $n = 2$ and consider eight consecutive numbers: $2, 3, 4, 5, 6, 7, 8, 9$. Each one of them is divisible by some $m \in [2; 7]$.

Question 5:

(A) List all integers $n \in [1; 90]$ such that $\gcd(n, 90) = 3$.

(B) Prove that for every positive integer $m \in \mathbb{Z}^+$, and for every positive integer d such that $d \mid m$ we have

$$\Big|\{x \in \mathbb{Z}^+ \mid x \leq m \wedge \gcd(x, m) = d\}\Big| = \varphi(m/d).$$

Answer:

(A) Check every number and come up with this list:

$$\{3, 21, 33, 39, 51, 57, 69, 87\}.$$

This set can be obtained by building a set of $\Phi(30)$ – all numbers from 1 to 30 that are mutually prime with 30 and then multiplying every element of this set by 3.

$$\Phi(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}.$$
$$3 \cdot \Phi(30) = \{3, 21, 33, 39, 51, 57, 69, 87\}.$$

The set $\Phi(30)$ has size $\varphi(30)$ (the count of numbers between 1 and 30 mutually prime with 30).

(B) Just as in the numeric example above (where $m = 90$ and $d = 3$), every time we pick a number $a \in \Phi(m/d)$ which is mutually prime with m/d, we have

$$\gcd(da, m) = d \cdot \gcd(a, m/d) = d \cdot 1 = d.$$

Also the other way round: for any number $b < m$ such that $\gcd(b, m) = d$ we have that b is divisible by d (as d is GCD of b with another number). We can denote $a = b/d$. And we have $\gcd(a, m/d) = 1$, therefore $b/d \in \Phi(m/d)$.

So there is a bijection $a \mapsto d \cdot a$ between two sets:

- The set $\Phi(m/d)$ of all positive integers mutually prime with m/d and not exceeding m/d.
- The set given in the question part (B).

Question 6:

Introduction: Miller-Rabin primality test is a probabilistic algorithm to find, if a number is prime. It is the most popular primality test in libraries such as Pythons `sympy.isprime(n)`. The documentation of `sympy` package says that for $n < 2^{64}$ the answer is always correct, but for larger values n there is a probability that the algorithm will lie and identify some non-prime as a prime (false positive). Miller-Rabin primality test does not have false negatives – if it outputs the answer that the number is composite, this means that a *witness* has been found, which proves that it is definitely composite.

WITNESS(a, n):

1. express $n - 1 = 2^t u$, where u is odd.
2. $x_0 = a^u \bmod n$
3. **for** i **in** RANGE$(0, t)$: (*repeat t times*)
4. $x_i = x_{i-1}^2 \bmod n$
5. **if** $x_i == 1$ **and** $x_{i-1} \neq 1$ **and** $x_{i-1} \neq n - 1$
6. **return** TRUE (*evidence that n is definitely composite*)
7. **if** $x_t \neq 1$
8. **return** TRUE (*evidence that n is definitely composite*)
9. **return** FALSE

MILLERRABIN(n, s):

1. **for** j **in** RANGE$(1, s + 1)$
2. let a be a random number from $\{1, 2, \ldots, n - 1\}$
3. **if** WITNESS(a, n)
4. **return** COMPOSITE (*definitely composite*)
5. **return** PRIME (*very likely prime*)

To improve the probability of correct answer from Miller-Rabin algorithm one can increase the number of witness-probes – the parameter s in the above pseudocode. How do we know, which value s is sufficient? It may happen that the chance to get a wrong answer depends on the number n being tested. In this problem you will find out which composite numbers n are most likely to lead to wrong answers from this primality test.

Problem: Consider the set of positive integers $S = \{n \in \mathbb{Z}^+ \mid 2 \leq n \leq 2000\}$. Find those three integers $n_1, n_2, n_3 \in S$ which have the *highest* probabilities that the function WITNESS(a, n) for a random $a \in \{1, 2, \ldots, n_i - 1\}$ will fail to determine that n_i is a composite number (even though it is in fact composite).

For each of the three numbers indicate the total number of false witnesses (those a for which WITNESS(a, n) does not produce evidence that n_i was composite). Also compute the probability to get a false witness as a rational fraction. (It may be useful to use computing devices to find the most risky composite numbers up to 2000.)

Example: If we pick $n = 21$, then for $a \in \{1, 8, 13, 20\}$ we fail to produce a witness that $n = 21$ is composite. Indeed, express $n - 1 = 20 = 5 \cdot 2^2$ ($t = 2, u = 5$).

Raising all the numbers $a \in \{1, 8, 13, 20\}$ to the power $u = 5$ (Line 2 in the algorithm WITNESS(a, n)) we get the following results:

$$\begin{cases} 1^5 \equiv 1 \pmod{21} \\ 8^5 \equiv 8 \pmod{21} \\ 13^5 \equiv 13 \pmod{21} \\ 20^5 \equiv 20 \pmod{21} \end{cases}$$

Squaring any of these numbers exactly $t = 2$ times would be congruent to 1 modulo 21. Thus these numbers $a \in \{1, 8, 13, 20\}$ create a false impression that $n = 21$ satisfies the Little Fermat theorem since $a^{n-1} \equiv 1 \pmod{n}$. Other values $a \in [1; 20]$ are fine as witnesses and produce correct evidence that $21 = 3 \cdot 7$ is a composite number.

Thus for $n = 21$ the probability of a false witness in WITNESS(a, n) for a single randomly chosen a is $P_{21} = \frac{4}{20} = \frac{1}{5}$. In your answer find those $n_1, n_2, n_3 \leq 2000$ which have the three highest probabilities $P_{n_1}, P_{n_2}, P_{n_3}$ to pick a false witness.

Answer:

```
import pandas as pd
import random

df = pd.DataFrame(columns=['Num', 'Wrong', 'Total', 'Prob'])

def witness(a, n):
    u = n - 1
    t = 0
    if u % 2 == 0:
        t += 1
        u = u // 2
    xi = pow(a, u, n)
    for i in range(1, t+1):
        xii = (xi*xi) % n
        if xii == 1 and xi != 1 and xi != n-1:
            return 1
        xi = xii
    if xi != 1:
        return 1
    return 0


def miller_rabin(n):
    global df
    total = 0
    for a in range(1, n):
        res = witness(a,n)
        if res > 0:
            total += 1
    if total == n-1:
        mislead = 0
    else:
        mislead = total/(n-1)
    df = df.append(pd.DataFrame([[n, total, n-1, mislead]],
        columns=['Num', 'Wrong', 'Total', 'Prob']))

def random_miller_rabin(n):
    isPrime = 0
    notPrime = 0
    for i in range(0,100):
        a = random.randrange(1, n)
        if witness(a, n):
            notPrime += 1
        else:
            isPrime += 1
    return (isPrime, notPrime)

def main():
    global df
    for p in range(1, 2001):
        miller_rabin(p)
    df = df.sort_values(by=['Prob'])
    for i in range(len(df)):
        print('{}, {}, {}, {}'.format(
            df.iloc[i,0], df.iloc[i,1], df.iloc[i,2], 1-df.iloc[i,3]))
```

(continues on next page)

(continued from previous page)

```
if __name__ == '__main__':
    main()
```

Here is the output from this program:

```
1729, 432, 1728, 0.75
1105, 720, 1104, 0.34782609
4, 2, 3, 0.33333333
1541, 1056, 1540, 0.31428571
481, 336, 480, 0.3
341, 240, 340, 0.29411765
561, 400, 560, 0.28571429
133, 96, 132, 0.27272727
65, 48, 64, 0.25
9, 6, 8, 0.25
1891, 1440, 1890, 0.23809524
703, 540, 702, 0.23076923
91, 72, 90, 0.2
21, 16, 20, 0.2
6, 4, 5, 0.2
```

The most misleading composite numbers (having large proportion of false negative witnesses that fail to detect that the number is composite) are these three:

- $n_1 = 1729 = 7 \cdot 13 \cdot 19$. ($P_{n_1} = 0.75$ – three quaters are false witnesses).
- $n_2 = 1105 = 5 \cdot 13 \cdot 17$. ($P_{n_2} = 0.34782609$).
- $n_3 = 4 = 2 \cdot 2$. ($P_{n_3} = 0.33333333$).

Numbers 1728 and 1105 are known as Carmichael numbers, see https://bit.ly/3vvBvBi. (Some very small numbers also have comparatively large proportion of false witnesses – but for such numbers libraries are usually not doing Miller-Rabin algorithm, as the direct check is sufficiently fast.)