Justin Li
2/2/23

COEN 379 HW 2

1. n = 75, a = 2
   Fermat:
   Compute 2^74 (mod 75)

   74, 37, 18, 9, 4, 2, 1, 0
   2^1 = 1^2 * 2 = 2 (mod 75); 2^2 = 4 (mod 75); 2^4 = 16 (mod 75);
   2^9 = 16^2 * 2 (mod 75) = 62; 2^18 = 62^2 (mod 75) = 19;
   2^37 = 19^2 * 2 (mod 75) = 47; 2^74 = 47^2 (mod 75) = **34**

   Since this value is not equal to 1, 2 is a Fermat witness to N's compositeness.

   Miller-Rabin:
   N = 2^1 * 37 + 1
   (s = 1, d = 37)
   2^37 (mod 75) = 47 (from above)

   Since a^d (2^37) is not equal to 1 and s = 1, this is the only value to check for, meaning that 2 is a strong witness of N's compositeness.

   n = 75, a = 26
   Fermat:
   Compute 26^74 (mod 75)

   74, 37, 18, 9, 4, 2, 1, 0
   26^1 = 1^2 * 26 = 26 (mod 75); 26^2 = 676 (mod 75) = 1;
   26^4 = 1^2 (mod 75) = 1; 26^9 = 1^2 * 26 (mod 75) = 26;
   26^18 = 26^2 (mod 75) = 1; 26^37 = 1^2 * 26 (mod 75) = 26; 26^74 = 26^2 (mod 75) = **1**

   gcd(75, 26) = gcd(26, 75%26) = gcd(26, 23) = gcd(23, 26%23) = gcd(23, 3) = gcd(3, 23%3) = gcd(3, 2) = gcd(2, 3%2) = gcd(2, 1) = gcd(1, 2%1) = gcd(**1**, 0)

   Since both the gcd and powermod values are equal to 1, 26 is NOT a Fermat witness to N's compositeness.

   Miller-Rabin:
   N = 2^1 * 37 + 1

$(s = 1, d = 37)$
$26^{37} \pmod{75} = 26$ (from above)

Since a^d (26^{37}) is not equal to 1 and $s = 1$, this is the only value to check for, meaning that 26 is a strong witness of N's compositeness.

$n = 75, a = 74$
Compute $74^{74} \pmod{75}$

> 74, 37, 18, 9, 4, 2, 1, 0
> $74^1 = 1^2 * 74 = -1 \pmod{75}$; $74^2 = (-1)^2 \pmod{75} = 1$;
> $74^4 = 1^2 \pmod{75} = 1$; $74^9 = 1^2 * 74 \pmod{75} = -1$;
> $74^{18} = (-1)^2 \pmod{75} = 1$; $74^{37} = 1^2 * 74 \pmod{75} = -1$; $74^{74} = (-1)^2 \pmod{75} = \mathbf{1}$

gcd(75, 74) = gcd(74, 75%74) = gcd(74, 1) = gcd(1, 74%1) = gcd(**1**, 0)

Again, since both the gcd and powermod values are equal to 1, 26 is NOT a Fermat witness to N's compositeness.

Miller-Rabin:
$N = 2^1 * 37 + 1$
$(s = 1, d = 37)$
$74^{37} \pmod{75} = -1$ (from above)

Since a^d (74^{37}) is equal to -1, 74 is NOT a strong witness of N's compositeness.

```
import math
import random as rand

#Q2
N = 0
CarmichaelArray = []
while (len(CarmichaelArray) < 20):
    N = rand(Max_Value)
    if fermat(N):
        if not miller-rabin(N):
            CarmichaelArray.append(N)
```

```
print(CarmichaelArray)
```

3. Let Xi be the result of each roll of the die, with i representing the iteration. Now, let X be equal to the total sum of all of the dice rolls. Thus, X = Sum(from i=1 to 100) of Xi. This also means that E[X] = Sum(from i=1 to 100) of E[Xi].
E[Xi] is the expected value for each roll, which can be calculated as follows:

    E[Xi] = Sum(from r=1 to 6) of r * P(Xi = r) = 21 * (⅙) = 7/2 = 3.5

Thus,

    E[X] = 100 * 3.5 = 350

To use Chebyshev's inequality, we need to first find the variance of X, which is

    Var(X) = Sum(from i=1 to 100) of Var(Xi)
    where Var(Xi) = E[Xi^2] - (E[Xi])^2

Since we already solve for E[Xi], now we just need to find E[Xi^2], which is

    = Sum(from r=1 to 6) of r^2 * P(Xi = r)
    = (1+4+9+16+25+36) * (⅙) = 91/6

Now we can solve for the variance of Xi, which is

    Var(Xi) = 91/6 - (7/2)^2 = 35/12

Meaning we also know the variance of X, which is

    Var(X) = 100 * 35/12 = 875/3

Finally, we can plug into Chebyshev's inequality: P(|X-E[X]|>=a) <= Var[X]/a^2

    P(|X-350|>=50) <= 875/3/50^2

= 875/7500 = 7/60