Homework 2

Jared Roesch

Spring 2015

Output

```
Running Fermat Test:
Found lowest witness for 41041: 7
Found lowest liar for 41041: 2
Found lowest witness for 62745: 3
Found lowest liar for 62745: 2
Found lowest witness for 63973: 7
Found lowest liar for 63973: 2
Found lowest witness for 75361: 11
Found lowest liar for 75361: 2
Found lowest witness for 101101: 7
Found lowest liar for 101101: 2
Found lowest witness for 126217: 7
Found lowest liar for 126217: 2
Found lowest witness for 172081: 7
Found lowest liar for 172081: 2
Found lowest witness for 188461: 7
Found lowest liar for 188461: 2
Found lowest witness for 278545: 5
Found lowest liar for 278545: 2
Found lowest witness for 340561: 13
Found lowest liar for 340561: 2
Found lowest witness for 449065: 5
Found lowest liar for 449065: 2
Found lowest witness for 552721: 13
Found lowest liar for 552721: 2
Found lowest witness for 656601: 3
Found lowest liar for 656601: 2
Found lowest witness for 658801: 11
Found lowest liar for 658801: 2
Found lowest witness for 670033: 7
Found lowest liar for 670033: 2
```

```
Found lowest witness for 748657: 7
Found lowest liar for 748657: 2
Found lowest witness for 838201: 7
Found lowest liar for 838201: 2
Found lowest witness for 852841: 11
Found lowest liar for 852841: 2
Found lowest witness for 997633: 7
Found lowest liar for 997633: 2
Found lowest witness for 1033669: 7
Found lowest liar for 1033669: 2
Found lowest witness for 1082809: 7
Found lowest liar for 1082809: 2
Found lowest witness for 1569457: 17
Found lowest liar for 1569457: 2
Found lowest witness for 1773289: 7
Found lowest liar for 1773289: 2
Found lowest witness for 2100901: 11
Found lowest liar for 2100901: 2
Found lowest witness for 2113921: 19
Found lowest liar for 2113921: 2
Found lowest witness for 2433601: 17
Found lowest liar for 2433601: 2
Found lowest witness for 2455921: 13
Found lowest liar for 2455921: 2
--------------------
Running Miller-Rabin Test:
Found lowest witness for 41041: 2
Found lowest liar for 41041: 16
Found lowest witness for 62745: 2
Found lowest liar for 62745: 16
Found lowest witness for 63973: 2
Found lowest liar for 63973: 9
Found lowest witness for 75361: 2
Found lowest liar for 75361: 256
Found lowest witness for 101101: 2
Found lowest liar for 101101: 16
Found lowest witness for 126217: 2
Found lowest liar for 126217: 16
Found lowest witness for 172081: 2
Found lowest liar for 172081: 9
Found lowest witness for 188461: 2
Found lowest liar for 188461: 9
Found lowest witness for 278545: 2
Found lowest liar for 278545: 256
Found lowest witness for 340561: 2
Found lowest liar for 340561: 35
```

```
Found lowest witness for 449065: 2
Found lowest liar for 449065: 16
Found lowest witness for 552721: 2
Found lowest liar for 552721: 256
Found lowest witness for 656601: 2
Found lowest liar for 656601: 16
Found lowest witness for 658801: 2
Found lowest liar for 658801: 256
Found lowest witness for 670033: 2
Found lowest liar for 670033: 9
Found lowest witness for 748657: 2
Found lowest liar for 748657: 9
Found lowest witness for 838201: 2
Found lowest liar for 838201: 9
Found lowest witness for 852841: 2
Found lowest liar for 852841: 16
Found lowest witness for 997633: 2
Found lowest liar for 997633: 898
Found lowest witness for 1033669: 2
Found lowest liar for 1033669: 9
Found lowest witness for 1082809: 2
Found lowest liar for 1082809: 16
Found lowest witness for 1569457: 2
Found lowest liar for 1569457: 256
Found lowest witness for 1773289: 2
Found lowest liar for 1773289: 4
Found lowest witness for 2100901: 2
Found lowest liar for 2100901: 16
Found lowest witness for 2113921: 2
Found lowest liar for 2113921: 195
Found lowest witness for 2433601: 2
Found lowest liar for 2433601: 256
Found lowest witness for 2455921: 2
Found lowest liar for 2455921: 9
```

Program

```
import random

carmichael = [
    41041,
    62745,
    63973,
    75361,
```

```
    101101,
    126217,
    172081,
    188461,
    278545,
    340561,
    449065,
    552721,
    656601,
    658801,
    670033,
    748657,
    838201,
    852841,
    997633,
    1033669,
    1082809,
    1569457,
    1773289,
    2100901,
    2113921,
    2433601,
    2455921
]

# Unmodified Algorithm
def fermat(p, iterations):
    if p == 1:
        return False

    for i in range(0, iterations):
        a = random.randint(1, p - 1)

        if ((a ** p-1) % p) != 1:
            return False

    return True

# Unmodified Algorithm
def miller_rabin(p, iterations):
    if p < 2:
        return False

    if p != 2 and p % 2 == 0:
        return False
```

```
    s = p-1

    while s % 2 == 0:
        s = s / 2

    for i in range(0, iteration):
        a = random.randint(0, p - 1) + 1
        temp=s
        mod=(a ** temp) % p
        while (temp != p-1) and (mod != 1) and (mod != p-1):
            mod = (mod * mod) % p
            temp *= 2

        if (mod != p-1) and (temp % 2 == 0):
            return False

    return true

# Modified to step up until we find the smallest liar.
def fermat_lowest_witness(p):
    if p == 1:
        return 1

    for a in range(2, p - 1):
        if ((a ** (p-1)) % p) != 1:
           return a

def fermat_lowest_liar(p):
    if p == 1:
        return -1

    for a in range(2, p - 1):
        if ((a ** (p-1)) % p) == 1:
            return a

def fermat_test():
    print("Running Fermat Test:")
    for n in carmichael:
        r = fermat_lowest_witness(n)
        print("Found lowest witness for {}: {}".format(n, r))
        r = fermat_lowest_liar(n)
        print("Found lowest liar for {}: {}".format(n, r))

# Modified to step up until we find the smallest liar.
def miller_rabin(p):
    if p < 2:
```

```
        return -1

    if p != 2 and p % 2 == 0:
        return -1

    # compute m
    m = p - 1

    while m % 2 == 0:
        m = m / 2

    for a in range(2, p):
        x = (a ** m) % p
        if (x % p) == 1:
            return True

        temp = m
        while (temp != p-1) and (mod != 1) and (mod != p-1):
            mod = (mod * mod) % p
            temp *= 2

        if (mod != (p-1)) and ((temp % 2) == 0):
            return False

    return True

# Modified to step up until we find the smallest liar.
def miller_rabin_witness(p):
    if p < 2:
        return -1

    if p != 2 and p % 2 == 0:
        return -1

    # compute m
    m = p - 1

    while m % 2 == 0:
        m = m / 2

    for a in range(2, p):
        x = (a ** m) % p
        if (x % p) == 1:
            continue

        temp = m
```

```
        while (temp != p-1) and (x != 1) and (x != p-1):
            x = (x * x) % p
            temp *= 2

        if (x != (p-1)) and ((temp % 2) == 0):
            return a

    return -1

# Modified to step up until we find the smallest liar.
def miller_rabin_lowest_liar(p):
    if p < 2:
        return -1

    if p != 2 and p % 2 == 0:
        return -1

    # compute m
    m = p - 1

    while m % 2 == 0:
        m = m / 2

    for a in range(2, p):
        x = (a ** m) % p
        if (x % p) == 1:
            return a

        temp = m
        while (temp != p-1) and (x != 1) and (x != p-1):
            x = (x * x) % p
            temp *= 2

    return -1

def miller_rabin_test():
    print("Running Miller-Rabin Test:")
    for n in carmichael:
        r = miller_rabin_lowest_witness(n)
        print("Found lowest witness for {}: {}".format(n, r))
        r = fermat_lowest_liar(n)
        print("Found lowest liar for {}: {}".format(n, r))

fermat_test()
print("-" * 20)
```

```
miller_rabin_test()
```