```
P=53
Q=59


n = P*Q


a=3
b=5


X = (Q**a)%P
Y = (Q**b)%P


prA = (Y**a)%P
prB = (X**b)%P


print(prA,prB)
```

```
17 17
```

```
def isPrime(n):
    if n<=1:
        print("Not a prime")
        return False
    if (n <= 3):
        return True
    if n % 2==0 or n % 3==0:
        return False

    i = 5
    while(i * i <= n):
        if (n % i == 0 or n % (i + 2) == 0) :
            return False
        i = i + 6

    return True


P = int(input("Enter a prime number "))
if(isPrime(P)==False):
    print("Not a prime. Enter a different number which is prime")
```

```
Enter a prime number 41
```

```
import math

# A function to print all prime factors of
# a given number n
def primeFactors(n):
    factors = []
    # Print the number of two's that divide n
    while n % 2 == 0:
        if(2 not in factors):
          factors.append(2)
        n = int(n / 2)


    for i in range(3, int(math.sqrt(n))+1, 2):
        while n % i == 0:
            if(i not in factors):
              factors.append(i)
            n = int(n / i)

    if n > 2 and isPrime(n):
        factors.append(n)
    return factors

def calculate_pn(factors,n):
  pn = []
  for i in factors:
    pn.append(int(n/i))

  return pn

factors = primeFactors(P-1)
arr = calculate_pn(factors,P-1)
print(factors)
def findPrimitive(P):
  for i in range(2,P):
    flag = 0
    for j in arr:
      if((i**j)%P == 1):
        flag=1
    if (flag == 0) :
      return i

findPrimitive(157)
```

```
[2, 5]
2
```

```
G = findPrimitive(P)
print(G)
```

```
6
```

```
a=3
b=5


X = (G**a) % P
Y = (G**b) % P
print(X)
print(Y)
```

```
3
2
```

```
SharX = (Y**a)%P
SharY = (X**b)%P
print(SharX)
print(SharY)
```

```
3
3
```

```
def isPrime(n):
    if n<=1:
        return False
    if n<=3:
        return True

    if n%2==0 or n%3==0:
        return False

    i=5

    while i*i<=n:
        if n%i==0 or (n%(i+2)==0):
            return False
        i+=6
    return True

def findPrimeFactors(s,phi):
    n=phi
    while n%2==0:
        s.add(2)
        n=n//2

    for i in range(3,int(n**0.5),2):
        while n%i==0:
            s.add(i)
            n=n//i
    if n>2:
        s.add(2)

def isPrimitive(n):
    if(isPrime(n)==False):
        return False

    phi = n-1
    s=set()
    findPrimeFactors(s,phi)

    for r in range(2,phi+1):
        flag=True
        for it in s:

            if pow(r,phi//it,n)==1:
                flag=False;
                break

        if flag==True:
            return r

    return -1


isPrimitive(5)
```

```
2
```