Congratulations! You passed!

Grade received 100%

Latest Submission Grade 100%

To pass 80% or higher

Go to next item

Fast Modular Exponentiation: Code

Quiz • 20 min

Review Learning Objectives

1. Implement the function $FastModularExponentiation(b, k, m)$ which computes $b^{2^k} \mod m$ using only around $2k$ modular multiplications. You are not allowed to use Python built-in exponentiation functions.

1 / 1 point

Try again

Due Jan 15, 11:59 PM IST

Submit your assignment

Receive grade

To Pass 80% or higher

Your grade
100%

View Feedback

We keep your highest score

```
def FastModularExponentiation(b, k, m):
  # your code here
  res = b % m
  for i in range(k):
    res = (res * res) % m
  return res

#print(FastModularExponentiation(3, 2, 100))
```

Run

Reset

```
81
```

Like Dislike Report an issue

Correct

Good job!

2. Implement the function $FastModularExponentiation(b, e, m)$ which computes $b^e \mod m$ using around $2 \log_2 e$ modular multiplications. You are not allowed to use Python built-in exponentiation functions.

1 / 1 point

```
def FastModularExponentiation(b, e, m):
  # your code here
  d = e
  p = b % m
  res = 1
  while d != 0:
    #print(e, d)
    e = d % 2
    if e:
      res = (res * p) % m
    d //= 2
    p = (p * p) % m
  return res

#FastModularExponentiation(3, 5, 100)
```

Run

Reset

```
43
```

Correct

Good job!