CS 58000-01/2I Quiz 03 Print your Name: Truc Huynh

September 15, 2022

10 points

Analyze the time efficiency for the function modexp(x, y, N)

function modexp(x, y, N)

//Compute xy mod N

Input: Two n-bit integers x and N, and an integer exponent y.

Output: xy mod N.

if (y = 0) then return 1;

z = modexp(x, └y/2┘, N); // z = x└ y/2 ┘ mod N

if (y is even) then return z2 mod N;

else return x \* z2 mod N;

1. What is the basic operation?

**Answer:**

The basic operation would be to integer division, exponent a number, and multiply two mod N numbers

1. What is the input size

**Answer:**

Since there are 2 n-bits integer x and N, and an integer exponent y. Therefore, each of these numbers x, y, and N has the size n =└ log2 ┘ + 1 bit.

1. How many times of recursive calls will be made?

**Answer:**

The algorithm will halt at log2n (since └y/2┘will shilt one bit after each call) recursive call.

1. What is the best way to compute z2 mod N:

**Answer:**

We have z = x└ y/2 ┘ mod N. Therefore, z2 mod N = (x└ y/2 ┘ % N) 2 % N. We make the z which is x└ y/2 ┘ % N to the power of 2, which is splitting the y (or y/2) by the power of 2. So, we split the ((xy)% N) Until xy = x3. Then, x3= x \* (x1)2 By using these formulas below we can prove it:

x 2n = (xn) 2 for all real numbers x and a with x ≥ 0.

E.g: x4 % n = (x2)2 % n = (x2 % n)2 % n

x a+b = xaxb for all real numbers x, a and b with x ≥ 0.

E.g.: x7 % n = (x4+2+1) % n = (x4x2x1) % n = {(x4 % n) (x2 % n)(x1 % n)} % n

To clarify my point. Let’s look at the example:

1. modexp (x, └ 12/2 ┘, N); y = 6 ≠ 0

Therefore z2 % N = (x└ 12/2 ┘ % N) 2 %N

= (x6 % N) 2 %N

= ((x3)2 % N) 2 %N

= ((x3 % N)2 % N) 2 %N

= (((x2+1) % N)2 % N) 2 %N

= (((x \* x2) % N)2 % N) 2 %N

= (x \* ((x \* 12) %N)2 %N )2 %N

1. What is the best way to compute x \* z2 mod N:

**Answer:**

Very similar to the above answer. We have z = x└ y/2 ┘ % N. Therefore, x \* z2 % N = x \* (x└ y/2 ┘ % N) 2 % N (y is an integer exponent y). We make the z which is x└ y/2 ┘ % N to the power of 2, which is splitting the y (or y/2) by the power of 2. So, we split the ((xy)% N) Until xy = x3. Then, x3= x \* (x1)2 By using these formulas in answer 3 we can prove it. Let’s look at the example:

1. modexp (x, └ 14/2 ┘, N); y = 7 ≠ 0

Therefore x \* z2 % N = x \* (x└ 14/2 ┘ % N) 2 %N

= x \* (x7 % N) 2 %N

= x \* ((x3)2 % N) 2 %N

= x \* ((x3 % N)2 % N) 2 %N

= x \* (((x2+1) % N)2 % N) 2 %N

= x \* (((x \* x2) % N)2 % N) 2 %N

= x \* (x \* ((x \* 12) %N)2 %N )2 %N