

## Fall 2020 CIS 3362 Quiz #4 Part B: Miller-Rabin, Factoring, Fast Mod Expo

Date: 10/26/2020

**Directions:** Please use your course notes and a calculator as aids for this exam. Do NOT attempt to look up information online. Even if you use a calculator, show each step of your calculations that you would do by hand. The role of the calculator will simply be to speed up individual calculations (13 x 29, for example), not to skip whole steps, as these steps are typically awarded points in the grading criteria.

Please either type your answers. The accepted file types for submission will be .doc, .docx, .txt and .pdf. I recommend that you directly type into the posted document to save time.

Please look at Webcourses to see when your due time and late due time are. It's recommended that you stop working at the due time and start uploading at that time. Anything turned in before the late due time will be accepted for full credit. Anything that doesn't make it in by the late due time will earn a 0. A 10 minute buffer will be provided after both due times. Please don't take advantage of these buffers as it's an unnecessary risk.

1) (8 pts) In the Miller-Rabin primality test, when testing if a positive integer  $n$  is prime or not, instead of calculating  $a^{n-1} \bmod n$  only, where  $a$  is a randomly selected integer in between 2 and  $n-1$ ,  $a$  raised to several different powers mod  $n$  are potentially calculated. If  $n = 1281$ , what are all of the possible exponents for which the Miller-Rabin primality test might raise a randomly chosen  $a$ ?

### Solution

In Miller-Rabin,  $n-1$  is repeatedly divided by 2 until an odd number is reached. Let's do this with  $1281 - 1$ :

$1280 \rightarrow 640 \rightarrow 320 \rightarrow 160 \rightarrow 80 \rightarrow 40 \rightarrow 20 \rightarrow 10 \rightarrow 5$

This list above, in reverse order (except 1280), are the exponents which Miller-Rabin raises the randomly chosen  $a$  to. So, specifically, the answer is 5, 10, 20, 40, 80, 160, 320 and 640.

**Grading: 1 pt per listed value, don't change credit at all if 1280 is listed. (ie, give full credit if 1280 is listed along with the other 8 values.) If only 5 listed, give 2 pts.**

2) (8 pts) Using Fermat Factoring, determine the factorization of 1541. Please build a table similar to the one shown in class to show your work.

**Solution**

$39 < \sqrt{1541} < 40$ , thus, the first perfect square we will test for Fermat Factoring is 40. Here is a table conducting the Fermat Factoring:

X	$X^2 - 1541$	Perfect Square?
40	59	No
41	140	No
42	223	No
43	308	No
44	395	No
45	484	Yes, $22^2 = 484$

It follows that  $45^2 - 1541 = 22^2$ , so  $1541 = 45^2 - 22^2 = (45 - 22)(45 + 22) = 23 \times 67$ .

**Grading: 1 pt for each row of the table, 2 pts to use that last row to get the factorization.**

3) (8 pts) Write a function, in C, that determines the maximum integer k for which an integer n is divisible by  $p^k$ , where p is a given integer greater than 1. For example, numTimesDivide(48, 2) should return 4, numTimesDivide(243000, 3) should return 5, and numTimesDivide(100, 7) should return 0.) The function prototype is provided below:

```
int numTimesDivide(int n, int p);
```

**Solution**

```
int numTimesDivide(int n, int p) {  
  
    int res = 0;  
    while (n%p == 0) {  
        res++;  
        n /= p;  
    }  
    return res;  
}
```

**Grading: 1 pt to set accumulator to 0, 2 pts loop, 2 pts increment accumulator in loop, 2 pts divide n by p in loop, 1 pt return.**

4) (1 pt) After what mathematician are Catalan numbers named? **Catalan (Give to all)**