Fall 2020 CIS 3362 Quiz #4 Part A: Phi Function, Fermat, Euler Theorem, Discrete Log Solution

Date: 10/26/2020

1) (5 pts) Determine $\phi(840)$. Please show your work.

Solution

840 = 84 x 10 = 4 x 21 x 10 = 2^2 x 3 x 7 x 2 x 5 = 2^3 x 3 x 5 x 7

Thus, $\phi(840) = \phi(2^3 \times 3 \times 5 \times 7) = (2^3 - 2^2)(3-1)(5-1)(7-1) = 4(2)(4)(6) = \mathbf{192.}$

Grading: 2 pts prime fact, 2 pts phi formula, 1 pt simplify to a single number.

2) (6 pts) Using Fermat's Theorem, determine the remainder when 75^{8235} is divided by 359. Note: 359 is a prime number. Please show your work. You may put in multiplications and mod simplifications in a calculator and just show the results.

Solution

Since gcd(75, 359) = 1, Fermat's Theorem tells us that $75^{358} \equiv 1 \pmod{359}$.

$75^{8235} = 75^{358*23+1} = 75^{358*23}75^1 = (75^{358})^{23}75^1 \equiv 1^{23}(75) \equiv 75 \pmod{359}$.

It follows that the desired remainder is **75.**

Grading: 2 pts for stating Fermat's application to this question, 3 pts for the exponent breakdown, 1 pt for the final answer.

3) (8 pts) Using Euler's Theorem, determine the remainder when 77^{6531} is divided by 1440. Please show your work. You may put in multiplications and mod simplifications in a calculator and just show the results.

Solution

1440 = 144 x 10 = 12 x 12 x 10 = $(2^2 \text{ x } 3)^2$ x 2 x 5 = 2^5 x 3^2 x 5

$\phi(1440) = \phi(2^5 3^2 5^1) = (2^5 - 2^4)(3^2 - 3)(5-1) = 16 \times 6 \times 4 = 384$

Using Euler's Theorem, since gcd(77, 1440) = 1, $77^{384} \equiv 1 \pmod{1440}$.

$77^{6531} = 77^{384*17+3} = (77^{384*17})(77^3) = (77^{384})^{17}(77^3) \equiv 1^{17}(456533) \equiv 53 \pmod{1440}$.

It follows that the remainder when 77^{6531} is divided by 1440 is **53.**

Grading: 2 pts for prime fact, 2 pts for phi value, 1 pt for stating relevant Euler Thm fact, 2 pts for exponent breakdown, 1 pt for final answer simplified.

4) (6 pts) If a and b are positive integers greater than 1, then $\log_a b$ always has a defined value. However, this is not true for the discrete log problem. Give an example with prime p = 7, and integers a and b, with 1 < a, b < 7, where the discrete log of b with the base of a, mod p has no defined value.

Solution

One example is a = 2, b = 5. When we calculate 2^1, 2^2, 2^3, etc. mod 7, we get the sequence 2, 4, 1 that repeats and the value of 5 is never obtained. The discrete logarithm can only reliably exist if the base is a primitive root. Hence, the importance of primitive roots!

Grading: This one's all or nothing. Here are a list of all the possible answers:

a = 2, b = 3, 5, 6
a = 4, b = 3, 5, 6
a = 6, b = 2, 3, 4, 5

We can derive these by simply picking all values that aren't primitive roots mod 7 and then cycling through their exponential values and listing all the ones not generated by that base.

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} mod 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 → 640 → 320 → 160 → 80 → 40 → 20 → 10 → 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 x 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)**