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.