





Module 12: Number Theory III (?q=onlinecourse/course/43606)

Number Theory Exercise Part III

- วิชชาภัทร จินดานาถ previously submitted answers to this quiz/test on 04-Nov-2023 @ 03:26:38 and obtained 11 correct answers out of 12.
- This test/quiz can be taken many times.
- Correct answers will NOT be revealed after submission.
- $\phi(n)$ is euler function
- $\lambda(n)$ is Carmichael function
- from

 $x \equiv 3 \mod 5$

 $x \equiv 5 \mod 7$

 $x \equiv 7 \mod 11$

From previous attempt

x can be described as $A+B\times k$ if k is integer A, B is constant and positive integer f ind B

385

77

105

55

- which following statement is true?
 - 1. if $x = 2^p 1$ and p is prime number then x is prime number $\frac{1}{\text{From previous attempt}}$
 - 2. $2^{2^n} + 1$ for n that is integer is always prime number

1, 2

2

There is no right statement

which following statement is true?

2. Let m, n be a positive integer and $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m) \times \phi(n)$

3.if p is prime then $\phi(p^n) = p^n - p^{n-1}$

- 1, 2, 3
- 1, 2
- 1, 3
- 2, 3

 $find \phi(7)$

0

From previous attempt

- 2

 $find \ \phi(15)$

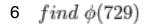
14

From previous attempt

8

10

0



243

From previous attempt

486

728

729

$find \ \phi(10000)$

1000

From previous attempt

4000

5000

9999

- which following statement is true?
 - 1.Let a be a positive integer and p is prime number then $a^{p-1} \equiv 1$ and p^{p} 2.Let a, n be positive integer which $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \mod n$

 - 3.Let a, n be positive integer which $\gcd(a, n) = 1$ then $a^{\lambda(n)} \equiv 1 \mod n$

2,3

1, 2, 3

3

1

9 $find 5^6 \mod 7$

0

From previous attempt

1

5

6

10 $find 10^{25} \mod 35$

0

From previous attempt

1

10

34

 $\textbf{11} \hspace{0.2in} (in \hspace{0.1em} this \hspace{0.1em} question \hspace{0.1em} "The \hspace{0.1em} RSA \hspace{0.1em} example" is \hspace{0.1em} refer \hspace{0.1em} to \hspace{0.1em} the \hspace{0.1em} RSA \hspace{0.1em} example \hspace{0.1em} on \hspace{0.1em} page \hspace{0.1em} 46 \hspace{0.1em} of \hspace{0.1em} NUMBERTHEORY \hspace{0.1em} FOR \hspace{0.1em} EVERY \hspace{0.1em} PART \hspace{0.1em} file \hspace{0.1em} (in \hspace{0.1em} material \hspace{0.1em} download))$

 $from \ the \ RSA \ example \ find \ public \ key \ N, k \ from \ this \ situation when \ you \ use \ p=5, \ q=7, \ m=7, \ k'(private \ key) \ temp \ , \\ k(35)=12 \ from \ previoletic \ previoletic$

$$N = 12, k = 35$$

$$N = 35, k = 12$$

$$N = 17, k = 7$$

12 if public key N = 15 k = 7 and private key k' = 3

1.encrypt the number 2

2.decrypt the number 5

From previous attempt

7, 5

7, 2

- 8,5
- 8,3

Submit



Version 1.15.23.2

Privacy Policy (https://lic.chula.ac.th/?page_id=7606) updated on 06 Jan 2023 Cookie Policy (https://www.mycourseville.com/cookiepolicy.html) updated on 21 May 2022

LMS and Online Course Platform within mycourseville.com are operated by Learning Innovation Center, Chulalongkorn University (http://www.lic.chula.ac.th/)