Quiz 6B (Module 10-12)
Number Theory

Name______________________________
ID_______________________No._______

*****ONLY THE ANSWERS IN THE ANSWER SHEET WILL BE GRADED.*****

Module 10 : (20%)

1. Let x and y be real numbers, and n be a nonnegative integer. Please answer whether it is **True or False**.
   1.1 $x > n$ if and only if $\lceil x \rceil > n$ 1.2 $x \leq n$ if and only if $\lfloor x \rfloor \leq n$
   1.3 $\lceil xy \rceil \leq \lceil x \rceil \lceil y \rceil$
2. Solve $\lfloor \frac{n^2}{2} \rfloor = \lfloor \frac{n}{2} \rfloor^2$, where n is an integer. Find the number of possible solution n.
   a. 1
   b. 2
   c. 3
   d. 4
3. Find the smallest positive integer k such that $7 \mid 1^5 + 2^5 + 3^5 + ... + 99^5 + k$
   a. 2
   b. 3
   c. 5
   d. 6
4. Find the number of solutions in tuple of positive integers (m, n) of the equation $\frac{1}{m} + \frac{1}{n} = \frac{1}{6}$
   a. 6
   b. 9
   c. 12
   d. 18
5. Let $[a_1, a_2, a_3, ...]$ is simple continued fraction of $\frac{345}{12}$. Find $a_1 + a_2 + a_3 + ...$
   a. 30
   b. 32
   c. 34
   d. 36
6. For all positive integer n, let $T_n = 2^{2^n} + 1$. Find the greatest common divisor of T_m and T_n where $(m, n) = (4, 5)$.
   a. $2^1 - 1$
   b. $2^2 - 1$
   c. $2^3 - 1$
   d. $2^4 - 1$

Quiz 6B (Module 10-12)
Number Theory

Name________________________________
ID________________________No.________

For questions 7-8, these are challenging problems, but I have confidence in your ability to solve them.

We define $\upsilon_p(x)$ to be the greatest power in which a prime p divides x; in particular, if $\upsilon_p(x) = \alpha$ then $p^{\alpha} \mid x$ but $p^{\alpha+1} \nmid x$.

<u>Example.</u> The greatest power of 3 that can divide 63 is 3^2. because
$3^2 = 9 \mid 63$ but $3^3 = 27 \nmid 63$.
So $\upsilon_3(63) = 2$.

7. Find the number of 0's at the end of $2023!$.
   (Hint: $Find\ \upsilon_p(2023!)$, $p = ???$ I try to help you so much na)

<u>Theorem</u>
Let x and y be integer, let n be a positive integer, and let p be an odd prime such that $p \mid x - y$ and none of x and y is divisible by p. We have

$$\upsilon_p(x^n - y^n) = \upsilon_p(x - y) + \upsilon_p(n)$$

8. Find the greatest number k such that $7^k \mid 2^{147} - 1$

<u>Module 11 :</u> (20%)

9. Find all integer x, y satisfying the condition $29x + 11y = 15$ using Euclid's Algorithm
   9.1 Fill this table with integer answer

i	r_i	q_i	P_i	Q_i
	29			
0	11			
1				
2				
3				
4				

9.2 if $x = A + 11t$ and $y = B - 29t$ for all integer t , find A, B

Quiz 6B (Module 10-12)
Number Theory

Name______________________________

ID______________________No.________

---

10. If a simple continued fraction of $\frac{29}{11} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4}}}}$, find q_0, q_1, q_2, q_3, q_4

11. If a simple continued fraction of $\sqrt{3} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + ...}}}}$, find q_0, q_1, q_2, q_3, q_4

12. let x be the smallest positive integer such $3^{2566} \equiv x \ (mod\ 13)$
and let y be the smallest positive integer such $5^{2566} \equiv y \ (mod\ 13)$ find
$x^y + y^x \ (mod\ xy)$

13. We call positive integer x <u>"Tar number"</u> if and only if
$7x^2 + 1 = (y)(y+1)(y+2)$ for some integer y. How many positive integer is <u>"Tar number"</u>
(You can ans "**INF**" if you think there are infinite <u>"Tar number"</u>)

14. Find smallest positive integer k that all integers x such
$x \equiv 1 \ (mod\ 3)$
$x \equiv 5 \ (mod\ 7)$
$x \equiv 4 \ (mod\ 11)$
then $x \equiv k \ (mod\ 231)$

15. (**Bonus**) Find sum of all positive integers n such $1! + 2! + 3! + ... + n!$ is a <u>perfect square</u>
(positive integer a is a <u>perfect square</u> if and only if there exists an integer b such $a = b^2$)

<u>Module 12:</u> (20%)

$\phi(n)$ is Euler function
$\phi(p) = p - 1$ if p is prime number
$\phi(mn) = \phi(m) \times \phi(n)$ if n, m is positive and $gcd(m, n) = 1$
$\phi(p^n) = p^n - p^{n-1}$ if p is prime number
$a^{\phi(n)} \equiv 1 \ (mod\ n)$ if n, m is positive integer, $gcd(n, a) = 1$

16. find
    16.1. $\phi(5)$
    16.2. $\phi(43)$
    16.3. $\phi(2023)$
    16.4. $2^4 \ mod\ 5$
    16.5. $7^{33} \ mod\ 10$
    16.6. $11^{38} \ mod\ 30$

Quiz 6B (Module 10-12)
Number Theory

Name________________________________

ID________________________No.________

17. which statement is True. Given p is prime number, n is positive integer (**<u>Answer in True or False</u>**)
    17.1. $p|\phi(p^n)$ for all $n > 2, p > 2$
    17.2. $p^{n-1}|\phi(p^n)$ for all $n > 2, p > 2$
    17.3. $\phi(2^n) = 2^{n-1}$ for all n
    17.4. $\phi(p^n)$ is even for all $n, p > 2$
    17.5. $2^n | \phi(6^n)$ for all $n > 1$
    17.6. $4 | \phi(3^n)$ for all $n > 1$
18. find last 3 digit of 3^{3205}
19. $79|(3^A - 1)(3^{2A} + 3^A + 1)(3^{3A} + 1)$ and $A < 20$ find A
20. $143|(7^A - 1)(7^B - 1)$ Given $A < B$ and $B < 20$ find $A + B$
21. **(Bonus)** how many odd integer n such that $n | 3^n + 1$
    (You can ans "**INF**" if you think there are infinite numbers)
22. fill the blank below
    The following step is Example of RSA Public-key Cryptosystem
    The first step is to select two prime numbers. p = 23 and q = 37
    The second step is to compute: public key N = **<u>A</u>**.
    then find Carmichael's function of N which is λ(**<u>A</u>**) = 396.
    The third step is to determine the public-key and private key:
    We try to factorize m(396)+1 for m = 1, 2, 3, … until we find a "good" factorization that can be used to obtain suitable k and k'.
    in this example we use m = 2, 2(396)+1 =793 = 13 × 61
    Then in this example we use k = 13 and k' = **<u>B</u>**
    Note: The public key is N = **<u>A</u>**
    The public-key is k = 13
    The private-key is k' = **<u>B</u>**
    22.1. find <u>A</u>
    22.2. find <u>B</u>
    22.3. encrypt number 2
    22.4. encrypt number 1
    22.5. decrypt number 850

Quiz 6B (Module 10-12)
Number Theory

Name_______________________________

ID________________________No.________

ANSWER SHEET for Quiz 6B

<u>Module 10</u>: Provide an answer in terms of **TRUE OR FALSE ONLY.**

No.	Answer					
1	1.1	True False	1.2	True False	1.3	True False

Choose the correct answer and provide the **X** mark.

No.	**Choice**				**No.**	**Choice**			
	a.	**b.**	**c.**	**d.**		**a.**	**b.**	**c.**	**d.**
2.					**5.**				
3.					**6.**				
4.									

Provide an answer in terms of **INTEGER ONLY**.

No.	Answer		
7.		**8.**	

<u>Module 11</u>: Choose the correct answer and provide the **X** mark.

Provide an answer in terms of **INTEGER or "INF" ONLY**.

No.9.1

i	r_i	q_i	P_i	Q_i
	29			
0	11			
1				
2				
3				
4				

Quiz 6B (Module 10-12)
Number Theory

Name______________________________
ID________________________No.________

No.	Answer									
9.2	A				B					
10	q_0		q_1		q_2		q_3		q_4	
11	q_0		q_1		q_2		q_3		q_4	

No.	Answer						
12.		13.		14.		15.	

Module 12: Provide an answer in terms of **INTEGER OR TRUE OR FALSE or "INF" ONLY**.

No.	Answer			
16	16.1		16.2	
	16.3		16.4	
	16.5		16.6	
17	17.1	True False	17.2	True False
	17.3	True False	17.4	True False
	17.5	True False	17.6	True False

No.	Answer						
18.		19.		20.		21.	

No.	Answer			
22	22.1		22.2	
	22.3		22.4	
	22.5			