**Chapter 2: INTRODUCTION TO NUMBER THEORY**

**TRUE OR FALSE**

T F 1. The algorithm credited to Euclid for easily finding the greatest

common divisor of two integers has broad significance in cryptography.

T F 2. Unlike ordinary addition, there is not an additive inverse to each

integer in modular arithmetic.

T F 3. The scheme where you can find the greatest common divisor of

two integers by repetitive application of the division algorithm is

known as the Brady algorithm.

T F 4. Two integers *a* and *b* are said to be congruent modulo *n*, if

(*a* mod *n*) = (*b* mod *n*).

T F 5. Basic concepts from number theory that are needed for understanding finite fields include divisibility, the Euclidian algorithm, and modular arithmetic.

T F 6. If *b*|*a* we say that *b* is a divisor of *a*.

T F 7. The notation *a*|*b* is commonly used to mean *b* divides *a*.

T F 8. The rules for ordinary arithmetic involving addition, subtraction,

and multiplication carry over into modular arithmetic.

T F 9. Two theorems that play important roles in public-key cryptography are Fermat’s theorem and Euler’s theorem.

T F 10. One of the useful features of the Chinese remainder theorem is that it provides a way to manipulate potentially very large numbers mod *M* in terms of tuples of smaller numbers.

T F 11. For many cryptographic algorithms, it is necessary to select one or more very large prime numbers.

T F 12. The Chinese Remainder Theorem is believed to have been

discovered by the Chinese mathematician Agrawal in 100 A.D.

T F 13. The primitive roots for the prime number 19 are 2, 3, 10, 13, 14

and 15.

T F 14. The first assertion of the CRT, concerning arithmetic operations,

follows from the rules for modular arithmetic.

T F 15. All integers have primitive roots.

**MULTIPLE CHOICE**

1. An integer *p* >1 is a \_\_\_\_\_\_\_\_\_ number if and only if its only divisors are + 1 and + *p.*

A)  prime   B)  composite

C)  indexed   D)  positive

2. Two integers are \_\_\_\_\_\_\_\_\_\_ if their only common positive integer factor is 1.

A)  relatively prime   B)  congruent modulo

C)  polynomials   D)  residual

3. The \_\_\_\_\_\_\_\_\_\_ of two numbers is the largest integer that divides both numbers.

A)  greatest common divisor   B)  prime polynomial

C)  lowest common divisor   D)  integral divisor

4. An important quantity in number theory referred to as \_\_\_\_\_\_\_\_\_\_ is defined as the

number of positive integers less than *n* and relatively prime to *n*.

A)  CRT   B)  Miller-Rabin

C)  Euler’s totient function   D)  Fermat’s theorem

5. Prime numbers play a \_\_\_\_\_\_\_\_\_\_ role in number theory.

A)  minor B)  nonessential

C)  critical   D)  abbreviated

6. If *p* is prime and *a* is a positive integer, then *ap = a*(mod *p*) is an alternative form

of \_\_\_\_\_\_\_\_\_ theorem.

A)  Rijndael’s   B)  Vignere’s

C)  Euler’s   D)  Fermat’s

7. Two numbers are relatively prime if they have \_\_\_\_\_\_\_\_ prime factors in common.

A)  some  B)  no

C)  multiple   D)  all

8. For given integers *a* and *b*, the extended \_\_\_\_\_\_\_\_\_\_ algorithm not only calculates

the greatest common divisor *d* but also two additional integers *x* and *y*.

A)  modular   B)  Euclidean

C)  associative   D)  cyclic

9. The procedure TEST takes a candidate integer *n* as input and returns the

result \_\_\_\_\_\_\_\_\_\_ if *n* is definitely not a prime.

A)  discrete   B)  composite

C)  inconclusive   D)  primitive

10. If a number is the highest possible exponent to which a number can belong, it is

referred to as a \_\_\_\_\_\_\_\_\_ of *n*.

A)  primitive root   B)  composite

C)  discrete logarithm   D)  bijection

11. For any integer *b* and a primitive root *a* of prime number *p* we can find a unique

exponent *i*. This exponent *i* is referred to as the \_\_\_\_\_\_\_\_\_\_\_ .

A)  order   B) discrete logarithm

C)  bijection   D)  primitive root

12. Discrete logarithms are fundamental to a number of public-key algorithms

including \_\_\_\_\_\_\_\_\_\_ key exchange and the DSA.

A)  Diffie-Hellman   B)  Rijndael-Fadiman

C)  Fermat-Euler  D)  Miller-Rabin

13. The congruence relation is used to define \_\_\_\_\_\_\_\_\_\_ .

A)  finite groups   B)  greatest common divisor

C)  lowest common divisor   D)  residue classes

14. As a \_\_\_\_\_\_\_\_\_ relation, mod expresses that two arguments have the same

remainder with respect to a given modulus.

A)  finite   B)  monic

C)  congruence   D)  cyclic

15. A one-to-one correspondence is called \_\_\_\_\_\_\_\_\_\_.

A)  a bijection   B)  an inclusive

C)  an index   D)  a composite

**SHORT ANSWER**

1. The remainder *r* in the division algorithm is often referred to as a \_\_\_\_\_\_\_\_\_\_ .
2. One of the basic techniques of number theory is the \_\_\_\_\_\_\_\_\_\_ algorithm which is a simple procedure for determining the greatest common divisor of two positive integers.
3. If *a* is an integer and *n* is a positive integer, we define *a* mod *n* to be the remainder when *a* is divided by *n*. The integer *n* is called the \_\_\_\_\_\_\_\_\_\_ .
4. Two theorems that play important roles in public-key cryptography are Fermat's theorem and \_\_\_\_\_\_\_\_\_\_ theorem.
5. \_\_\_\_\_\_\_\_\_\_ theorem states the following: If *p* is prime and *a* is a positive integer not divisible by *p*, then *ap-1*= 1(mod *p*).
6. Two numbers are \_\_\_\_\_\_\_\_\_\_ if their greatest common divisor is 1.

1. The number of positive integers less than *n* and relatively prime to *n* is referred to as \_\_\_\_\_\_\_\_\_\_ function.
2. The \_\_\_\_\_\_\_\_\_\_ theorem states that it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli.

1. Two integers are relatively \_\_\_\_\_\_\_\_\_ if and only if their only common positive integer factor is 1.
2. Discrete logarithms are fundamental to the digital signature algorithm (DSA) and the \_\_\_\_\_\_\_\_\_ algorithm.
3. The \_\_\_\_\_\_\_\_\_ of a number is defined to be the power to which some positive base (except 1) must be raised in order to equal the number.
4. Two numbers are relatively prime if their greatest common divisor is \_\_\_\_\_\_.
5. An integer *p* > 1 is a \_\_\_\_\_\_\_\_\_\_ number if and only if its only divisors are + 1 and + *p*.
6. Although it does not appear to be as efficient as the Miller-Rabin algorithm, in 2002 a relatively simple deterministic algorithm that efficiently determines whether a given large number is a prime was developed. This algorithm is known as the \_\_\_\_\_\_\_\_\_ algorithm
7. ­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_ have the following properties:

1. *a = b* **(mod** *n***) if** *n|* ***(****a - b****)***

2. *a = b* **(mod** *n***) implies** *b = a* **(mod** *n***)**

3. *a = b* **(mod** *n***) and** *b = c* **(mod** *n***) imply** *a = c* **(mod** *n)*