**Chapter 4: Basic Concepts in Number Theory and Finite Fields**

**TRUE OR FALSE**

T F 1. Finite fields play a crucial role in several areas of 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. Cryptographic algorithms do not rely on properties of finite fields.

T F 6. Finite fields of order p can be defined using arithmetic mod p.

T F 7. The Advanced Encryption Standard uses infinite fields.

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

and multiplication carry over into modular arithmetic.

T F 9. A cyclic group is always commutative and may be finite or infinite.

T F 10. A field is a set in which we can do addition, subtraction,

multiplication and division without leaving the set.

T F 11. It is easy to find the multiplicative inverse of an element in g(p) for

large values of p by constructing a multiplication table, however

for small values of p this approach is not practical.

T F 12. Polynomial arithmetic includes the operations of addition,

subtraction and multiplication.

T F 13. If we attempt to perform polynomial division over a coefficient set

that is not a field, we find that division is not always defined.

T F 14. The euclidean algorithm cannot be adapted to find the

multiplicative inverse of a polynomial.

T F 15. As a congruence relation, mod expresses that two arguments have

the same remainder with respect to a given modulus.

**MULTIPLE CHOICE**

1. The greatest common divisor of two integers is the largest positive integer that

exactly \_\_\_\_\_\_\_\_\_ both integers.

A)  multiplies   B)  exponentially multiplies

C)  squares   D)  divides

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. A ring is said to be \_\_\_\_\_\_\_\_\_ if it satisfies the condition ab = ba for all a, b in R.

A)  cyclic   B)  commutative

C)  abelian   D)  infinite

5. A \_\_\_\_\_\_\_\_\_ is a set of elements on which two arithmetic operations have been

defined and which has the properties of ordinary arithmetic, such as closure,

associativity, commutativity, distributivity, and having both additive and

multiplicative inverses.

A)  field   B)  modulus

C)  group   D)  ring

6. A \_\_\_\_\_\_\_\_\_ is a field with a finite number of elements.

A)  finite group   B)  finite order

C)  finite field   D)  finite ring

7. If b|a, we say that b is a \_\_\_\_\_\_\_\_\_\_ of a.

A)  residue   B)  group

C)  divisor   D)  modulus

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. A group is said to be \_\_\_\_\_\_\_\_\_ if it satisfies the condition a \* b = b \* a for all a, b in G.

A)  abelian   B)  infinite

C)  cyclic   D)  commutative

10. In the context of abstract algebra we are usually not interested in evaluating a

polynomial for a particular value of x. To emphasize this point the variable x is

sometimes referred to as the \_\_\_\_\_\_\_\_\_\_ .

A)  monic   B)  constant

C)  indeterminate   D)  coefficient

11. With the understanding that remainders are allowed, we can say that

polynomial division is possible if the coefficient set is a \_\_\_\_\_\_\_\_\_\_ .

A)  ring   B)  field

C)  factor   D)  divisor

12. By analogy to integers, an irreducible polynomial is also called a \_\_\_\_\_\_\_\_\_\_ .

A)  constant polynomial   B)  monic polynomial

C)  polynomial ring   D)  prime polynomial

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. The order of a finite field must be of the form pn where p is a prime and n is a \_\_ .

A)  identity element   B)  positive integer

C)  commutative ring   D)  associative

**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. An nth-degree polynomial is said to be a \_\_\_\_\_\_\_\_\_ polynomial if an = 1.
5. \_\_\_\_\_\_\_\_\_\_ arithmetic is a kind of integer arithmetic that reduces all numbers to one of a fixed set [0,..., n - 1].

1. Elliptic curve cryptography and the \_\_\_\_\_\_\_\_\_ are two cryptographic algorithms that rely heavily on properties of finite fields.

7. Let S be the set of integers, positive, negative, and 0, under the usual

operations of addition and multiplication. S is an \_\_\_\_\_\_\_\_\_\_ domain.

1. GF stands for \_\_\_\_\_\_\_\_\_\_ field in honor of the mathematician who first studied

finite fields.

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

10. A zero-degree polynomial is called a \_\_\_\_\_\_\_\_\_\_ polynomial and is simply an

element of the set of coefficients.

1. A polynomial f(x) over a field F is called \_\_\_\_\_\_\_\_\_\_ if and only if f(x) cannot be

expressed as a product of two polynomials, both over F, and both of degree lower than that of f(x).

1. The polynomial c(x) is said to be the \_\_\_\_\_\_\_\_\_\_ of a(x) and b(x) if c(x) divides

both a(x) and b(x) and any divisor of a(x) and b(x) is a divisor of c(x).

1. If a is an integer and n is a nonzero integer, we define a mod n to be the

remainder when a is divided by n. The integer n is called the \_\_\_\_\_\_\_\_\_\_ and

the remainder is called the residue.

1. A \_\_\_\_\_\_\_\_\_\_ g of a finite field F or order q is an element whose first q - 1

powers generate all the nonzero elements of F.

1. Consider a field F defined by a polynomial f(x). An element b contained in F is called a \_\_\_\_\_\_\_\_\_\_ of the polynomial if f(b) = 0.