MODULAR ARITHMETIC

The Modulus

- 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 modulus. Thus, for any integer a , we can rewrite Equation a=qn+r as follows:

$$a = qn + r \qquad 0 \le r < n;\ q = \lfloor a/n \rfloor$$

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

- Example: $11 \bmod 7 = 4; \qquad -11 \bmod 7 = 3$
- Two integers a and b are said to be congruent modulo n, if (a mod n)=(b mod n).
- This is written as a≡b (mod n) $73 \equiv 4 \pmod{23}; \qquad 21 \equiv -9 \pmod{10}$
- Note that if a ≡0(mod n), then n/a

Properties of Congruence

1. $a \equiv b \pmod{n}$ if $n|(a - b)$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

Modular Arithmetic Operations

- Modular arithmetic exhibits the following properties:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

- Example:

$11 \bmod 8 = 3; 15 \bmod 8 = 7$

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$

$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$

$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$

$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

Congruent numbers

- Integers that leave the same remainder when divided by the modulus m are somehow similar, however, not identical. Such numbers are called "congruent" .

- For instance, 1 and 13 and 25 and 37 are congruent mod 12 since they all leave the same remainder when divided by 12.
- We write this as 1 ≡ 13 ≡ 25 ≡ 37 mod 12. However, they are not congruent mod 13. Why not? Yield a different remainder when divided by 13.
- Find 5 numbers that are congruent to

1) 7 mod 5	2,12,17,-3,-10
2) 7 mod 25	32,57,82,-18,-43
3) 17 mod 25.	42,67,92,-8,-33

Euclid's algorithm

- The Euclidean algorithm, or Euclid's algorithm, is an efficient method for computing the greatest common divisor (GCD) of two integers (numbers), the largest number that divides them both without a remainder.
- The Euclidean algorithm can be based on the following theorem: For any nonnegative integer a and any positive integer b ,

  gcd(a,b) = gcd(b, a mod b)
- Example $\gcd(55, 22) = \gcd(22, 55 \bmod 22) = \gcd(22, 11) = 11$

The Algorithm

- The Euclidean Algorithm for finding GCD(A,B) is as follows:
- If A = 0 then GCD(A,B)=B, since the GCD(0,B)=B, and we can stop.
- If B = 0 then GCD(A,B)=A, since the GCD(A,0)=A, and we can stop.
- Write A in quotient remainder form (A = B·Q + R)
- Find GCD(B,R) using the Euclidean Algorithm since GCD(A,B) = GCD(B,R)

$$\gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$$
$$\gcd(11, 10) = \gcd(10, 1) = \gcd(1, 0) = 1$$

Example:

- Find the GCD of 270 and 192
  - A=270, B=192
  - A ≠0
  - B ≠0

  - Use long division to find that 270/192 = 1 with a remainder of 78. We can write this as: 270 = 192 * 1 +78
- Find GCD(192,78), since GCD(270,192)=GCD(192,78)
  - A=192, B=78
  - A ≠0
  - B ≠0
  - Use long division to find that 192/78 = 2 with a remainder of 36. We can write this as: 192 = 78 * 2 + 36
- Find GCD(78,36), since GCD(192,78)=GCD(78,36)
  - A=78, B=36
  - A ≠0
  - B ≠0
  - Use long division to find that 78/36 = 2 with a remainder of 6. We can write this as: 78 = 36 * 2 + 6
- Find GCD(36,6), since GCD(78,36)=GCD(36,6)
  - A=36, B=6
  - A ≠0
  - B ≠0
  - Use long division to find that 36/6 = 6 with a remainder of 0. We can write this as: 36 = 6 * 6 + 0
- Find GCD(6,0), since GCD(36,6)=GCD(6,0)
  - A=6, B=0
  - A ≠0
  - B =0, GCD(6,0)=6
- So we have shown:
- GCD(270,192) = GCD(192,78) = GCD(78,36) = GCD(36,6) = GCD(6,0) = 6
- GCD(270,192) = 6

Properties

- GCD(A,0) = A
- GCD(0,B) = B

- If A = B·Q + R and B≠0 then GCD(A,B) = GCD(B,R) where Q is an integer, R is an integer between 0 and B-1

Congruence

- If n is a positive integer, we say the integers a and b are congruent modulo n, and write a ≡ b (mod n), if they have the same remainder on division by n.
- Example:

{…,−6,1,8,15,…} are all congruent modulo 7 because their remainders on division by 7 equal 1. {…,−4,4,12,20,…} are all congruent modulo 8 since their remainders on division by 8 equal 4.

Properties

1. a≡a for any a;
2. a≡b implies b≡a;
3. a≡b and b≡c implies a≡c;
4. a≡0 iff n|a;
5. a≡b and c≡d implies a+c≡b+d;
6. a≡b and c≡d implies a−c≡b−d;
7. a≡b and c≡d implies ac≡bd;

Congruent Matrices

Two square matrices A and B are called congruent if there exists a nonsingular matrix P such that

$$B = P^T A P,$$

where P^T is the transpose.

Groups, rings, and fields

- Groups, rings, and fields are the fundamental elements of a branch of mathematics known as abstract algebra, or modern algebra.
- In abstract algebra, we are concerned with sets on whose elements we can operate algebraically; that is, we can combine two elements of the set, perhaps in several ways, to obtain a third element of the set.
- These operations are subject to specific rules, which define the nature of the set.
- By convention, the notation for the two principal classes of operations on set elements is usually the same as the notation for addition and multiplication on ordinary numbers