Lecture 6:

Modular Arithmetic

4th Year- Course, CCSIT, UoA

Lecture Goals

1. To review modular arithmetic
2. To present Euclid's gcd algorithms
3. To present the prime finite field Z_p
4. To show how Euclid's gcd algorithm can be extended to find multiplicative inverses

Modular Arithmetic Notation (1)

- Given any integer a and a positive integer n, and given a division of a by n that leaves the remainder between 0 and $n - 1$, both inclusive, we define $a \bmod n$ to be the ***remainder***. Note that the remainder must be between 0 and $n - 1$, both ends inclusive, even if that means that we must use a negative quotient when dividing a by n.
- We will call two integers a and b to be ***congruent*** modulo n if

$$(a \bmod n) = (b \bmod n)$$

- Symbolically, we will express such a congruence by

$$a \equiv b \pmod{n}$$

Modular Arithmetic Notation (2)

- We say a non-zero integer a is a ***divisor*** of another integer b provided there is no remainder when we divide b by a. That is, when $b = ma$ for some integer m.

- When a is a divisor of b, we express this fact by $a \mid b$.

Examples of Congruences

- Here are some congruences modulo 3:

$$7 \equiv 1 \ (mod\ 3) \qquad -8 \equiv 1 \ (mod\ 3)$$
$$-2 \equiv 1 \ (mod\ 3) \qquad 7 \equiv -8 \ (mod\ 3)$$
$$-2 \equiv 7 \ (mod\ 3)$$

- One way of seeing the above congruences (for mod 3 arithmetic):

...	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	...
...-	9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	...

  where the top line is the output of modulo 3 arithmetic and the bottom line the set of all integers.

- Obviously, then, modulo n arithmetic ***maps all integers into*** the set $\{0, 1, 2, 3, ..., n-1\}$.

Modular Arithmetic Operations

- The following equalities are easily shown to be true (with the ordinary meaning to be ascribed to the arithmetic operators):

$$[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$$
$$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$$
$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

- For arithmetic modulo n, let Z_n denote the set

$$Z_n = \{0, 1, 2, 3, ..., n - 1\}$$

- $\boldsymbol{Z_n}$ is obviously the set of remainders in arithmetic modulo n. It is officially called the ***set of residues***.

Properties of the Set Z_n (1)

1. ***Commutativity:***

$$(w + x) \bmod n = (x + w) \bmod n$$

$$(w \times x) \bmod n = (x \times w) \bmod n$$

2. ***Associativity:***

$$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$$

$$[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$$

3. ***Distributivity of multiplication over addition:***

$$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$$

Properties of the Set Z_n (2)

4. ***Existence of Identity Elements:***

$$(0 + w) \bmod n = (w + 0) \bmod n$$

$$(1 \times w) \bmod n = (w \times 1) \bmod n$$

5. ***Existence of Additive Inverses:*** *For each* $w \in Z_n$ *there exists a* z *such that* $w + z = 0 \bmod n$

- **Z_n is a commutative ring.** Why? [See the previous lecture]

- ***Actually, Z_n is more than a commutative ring, but not quite an integral domain.*** What do we mean by that? [Because it contains a multiplicative identity element. Commutative rings are not required to possess multiplicative identities.]

More about Z_n

- ***Why is Z_n not an integral domain?*** [Even though it possesses a multiplicative identity, it does NOT satisfy the other condition of integral domains which says that if $a \times b = 0$ then either a or b must be zero. Consider modulo 8 arithmetic. We have $2 \times 4 = 0$, which is a clear violation of the second rule for integral domains.]
- ***Why is Z_n not a field?***
- ***Is Z_n a group? If so, what is the group operator?*** [The group operator is the modulo n addition.]
- ***Is Z_n an abelian group?***
- ***Is Z_n a ring?***

Asymmetries between modulo addition and modulo multiplication over Z_n (1)

- For every element of Z_n, there exists an ***additive inverse*** in Z_n. But there *does not* exist a ***multiplicative inverse*** for every element of Z_n.
- Shown below are the additive and the multiplicative inverses for ***modulo 8*** arithmetic:

Z	=	0	1	2	3	4	5	6	7
8									
addit. inv.	=	0	7	6	5	4	3	2	1
multi. inv	=	-	1	-	3	-	5	-	7

Asymmetries between modulo addition and modulo multiplication over Z_n (2)

- Note that the ***multiplicative inverses*** exist for only those elements of Z_n that are ***relatively prime*** to n. Two integers are relatively prime to each other if the integer 1 is their only one common positive divisor. More formally, two integers a and b are relative prime to each other if $gcd\,(a, b) = 1$ where ***gcd*** denotes the ***Greatest Common Divisor.***

- The following property of ***modulo n addition*** is the same as for ordinary addition: $(a + b) \equiv (a + c)\ (mod\ n)$ implies $b \equiv c\ (mod\ n)$

- But a similar property is **NOT** obeyed by ***modulo n multiplication***. That is $(a \times b) \equiv (a \times c)\ (mod\ n)$ does not imply $b \equiv c\ (mod\ n)$ unless a and n are relatively prime to each other.

Asymmetries between modulo addition and modulo multiplication over Z_n (3)

- That the modulo n addition property stated above should hold true for all elements of Z_n follows from the fact that the ***additive inverse*** $-a$ exists for every $a \in Z_n$. So we can add $-a$ to both sides of the equation to prove the result.
- To prove the same result for modulo n multiplication, we will need to multiply both sides of the second equation above by the ***multiplicative inverse*** a^{-1}. But, not all elements of Z_n possess multiplicative inverses.
- Since the answer to the question whether two integers are *relatively prime* to each other depends on their *greatest common divisor (gcd)*, let's explore next the world's most famous algorithm for finding the gcd of two integers.

Euclid's Method for Finding the Greatest Common Divisor of Two Integers

Euclid's GCD is based on the following observations:

1. $gcd\ (a, a) = a$
2. *if* $b \mid a$ *then* $gcd\ (a, b) = b$
3. $gcd\ (a, 0) = a$ *since it is always true that* $a \mid 0$
4. Assuming without loss of generality that a is larger than b, it can be shown that

$$gcd\ (a, b) = gcd\ (b, a \bmod b)$$

❖This is the heart of Euclid's algorithm (now over 2000 years old).

Steps in a Recursive Invocation of Euclid's Algorithm

gcd(b_1, b_2):

= gcd (b_2, b_1 mod b_2) = gcd (b_2, b_3)

= gcd (b_3, b_2 mod b_3) = gcd (b_3, b_4)

= gcd (b_4, b_3 mod b_4)

....

until b_{m-1} mod b_m = 0

then gcd (b_1, b_2) = b_m

- Note that the algorithm works for any two non-negative integers b_1 and b_2 *regardless of which is the larger integer*. If the first integer is smaller compared to the second integer, the first iteration will swap the two.

Examples of Euclid's Algorithm in Action

```
gcd( 70, 38 )
     =   gcd( 38, 32 )
     =   gcd( 32, 6 )
     =   gcd( 6, 2 )
     =   gcd( 2, 0 )

Therefore,  gcd( 70, 38 )  = 2
```

```
gcd( 8, 17 ):
    =  gcd( 17, 8 )
    =  gcd( 8, 1 )
    =  gcd( 1, 0 )

Therefore,  gcd( 8, 17 )  = 1
```

- When the smaller of the two numbers is 1 (which happens when the two starting numbers are ***relatively prime***), there is no need to go to the last step in which the smaller of the two numbers is 0.

An Example of Euclid's Algorithm for Moderately Large Numbers

```
gcd( 40902, 24140 )
     =    gcd( 24140, 16762 )
     =    gcd( 16762, 7378 )
     =    gcd( 7378, 2006 )
     =    gcd( 2006, 1360 )
     =    gcd( 1360, 646 )
     =    gcd( 646, 68 )
     =    gcd( 68, 34 )
     =    gcd( 34, 0 )

Therefore,  gcd( 40902, 24140 )  = 34
```