Algebra Review
Modular Arithmetic
Boolean Algebra
Lecture 2

Termeh Shafie

algebraic properties* [axioms]
field properties

property	addition	multiplication
associative	$(a+b)+c = a+(b+c)$	$(ab)c = a(bc)$
commutative	$a+b = b+a$	$ab = ba$
identity	$a+0 = a = 0+a$	$a \cdot 1 = a = 1 \cdot a$
inverse	$a+(-a) = 0 = (-a)+a$	$a \cdot a^{-1} = 1 = a^{-1} \cdot a$ if $a \neq 0$
distributive	$a(b + c) = ab + ac$ and $ab + ac = a(b + c)$	

*given a, b, and c are real numbers

algebraic properties* [axioms]
properties of equality and inequality (1)

property	equality	inequality
multiplicative property of zero	$a \cdot 0 = 0 = 0 \cdot a$	
zero product	if $ab = 0$, then $a = 0$ or $b = 0$	
reflexive	$a = a$	
symmetric	if $a = b$, then $b = a$	
transitive	if $a = b$ and $b = c$, then $a = c$	if $a > b$ and $b > c$, then $a > c$ if $a < b$ and $b < c$, then $a < c$
addition	if $a=b$, then $a+c = b+c$	if $a < b$, then $a + c < b + c$ if $a > b$, then $a + c > b + c$
subtraction	if $a = b$, then $a-c = b-c$	if $a < b$, then $a - c < b - c$ if $a > b$, then $a - c > b - c$

*given a, b, and c are real numbers

algebraic properties* [axioms]
properties of equality and inequality (2)

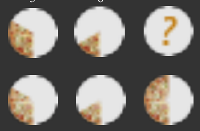
property	equality	inequality
multiplication	if $a = b$, then $ac = bc$	if $a < b$ and $c > 0$, then $ac < bc$ if $a < b$ and $c < 0$, then $ac > bc$ if $a > b$ and $c > 0$, then $ac > bc$ if $a > b$ and $c < 0$, then $ac < bc$
division	If $a = b$ and $c \neq 0$, then $a/b = b/c$	if $a < b$ and $c > 0$, then $a/c < b/c$ if $a < b$ and $c < 0$, then $a/c > b/c$ if $a > b$ and $c > 0$, then $a/c > b/c$ if $a > b$ and $c < 0$, then $a/c < b/c$
substitution	if $a = b$, then b can be substituted for a in any equation or inequality	

*given a, b, and c are real numbers

fractions (or pizza math)

addition and subtraction: Least Common Denominator (LCD)

$\frac{1}{3} + \frac{1}{6} = ?$



$\frac{6}{18} + \frac{3}{18} = \frac{9}{18}$

generally

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d}{b \cdot d} + \frac{c \cdot b}{d \cdot b}$$

fractions (or pizza math)

division

$\frac{1}{2} \div \frac{1}{6}$

is actually asking how many

$\frac{1}{6}$ in $\frac{1}{2}$ $= 3$

generally

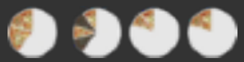
$$\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} + \frac{d}{c}$$

fractions (or pizza math)

multiplication

solving $\frac{2}{5} \times \frac{1}{2}$

$\frac{2}{5}$ $\quad \frac{2}{5} \times \frac{1}{2} = \frac{2}{10} = \frac{1}{5}$



generally

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

factoring

writing a polynomial as a product of polynomials

- The greatest common factor (GCF): largest quantity that is a factor of all the integers or polynomials involved

Example. 6, 8 and 46

$6 = 2 \cdot 3$
$8 = 2 \cdot 2 \cdot 2$
$46 = 2 \cdot 23$
$\Longrightarrow$ GCF is 2

Example. $6x^5$ and $4x^3$

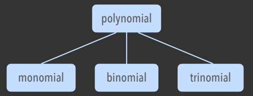
$6x^5 = 2 \cdot 3 \cdot x \cdot x \cdot x$
$4x^3 = 2 \cdot 2 \cdot x \cdot x \cdot x$
$\Longrightarrow$ GCF is $2 \cdot x \cdot x \cdot x$

Exercise 1. $a^3 b^2$, $a^2 b^5$ and $a^4 b^7$

$\Longrightarrow$ GCF is $a^2 b^2$

factoring

writing a polynomial as a product of polynomials



examples:	monomial	binomial	trinomial
	$28x$	$5x + 8xy$	$15xy - 25y + 18$
	$5a^3b$	$b^3/2 + c/3$	$2a^2 + 5a + 7$
	$2ax/3y$	$5m^2n^2 + 1/7$	$x^2/3 + ay - 6bz$

factoring trinomials

First Outer Inner Last

Example. $25x^2 + 20x + 4$

- possible factors of $25x^2$ are $\{x, 25x\}$ or $\{5x, 5x\}$ and possible factors of 4 are $\{1,4\}$ or $\{2,2\}$
- try each pair of factors until we find a combination that works (or exhausts all possible pairs)
- look for a combination that gives sum of the products of the outside terms and the inside terms equal to $20x$

Factors of $25x^2$	Factors of 4	Resulting Binomials	Product of Outside Terms	Product of Inside Terms	Sum of Products
$\{x, 25x\}$	$\{1, 4\}$	$(x+1)(25x+4)$	$4x$	$25x$	$29x$
		$(x+4)(25x+1)$	x	$100x$	$101x$
$\{x, 25x\}$	$\{2, 2\}$	$(x+2)(25x+2)$	$2x$	$50x$	$52x$
$\{5x, 5x\}$	$\{2, 2\}$	$(5x+2)(5x+2)$	$10x$	$10x$	$20x$

- Answer: $(5x+2)(5x+2)$ (check via FOIL)
- *Exercise 2.* Factor the polynomial $21x^2 - 41x + 10$

solving quadratic equations by factoring

- quadratic equations of the standard form

$$ax^2 + bx + c = 0$$

where a, b and c are real numbers and $a \neq 0$

- below theorem is very useful in solving quadratic equations

> *Zero Factor Theorem*
> If a and b are real numbers and $ab = 0$, then $a = 0$ or $b = 0$

solving quadratic equations by factoring

step by step for solving a quadratic equation by factoring

1. write the equation in standard form.
2. factor the quadratic completely
3. set each factor containing a variable equal to 0
4. solve the resulting equations
5. check each solution in the original equation

example: solve $x^2 - 5x = 24$

$x^2 - 5x - 24 = 0$

$x^2 - 5x - 24 = (x-8)(x+3) = 0$

$x - 8 = 0$ and $x + 3 = 0$

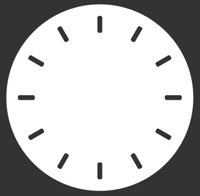
$\implies x = 8$ and $\implies x = -3$

$8^2 - 5(8) = 64 - 40 = 24 \implies$ *true*
$(-3)^2 - 5(-3) = 9 - (-15) = 24 \implies$ *true*

Exercise 3. $4x(8x+9) = 5$

modular arithmetic

a fundamental tool in number theory ("the study of integers")
deals with repetitive cycles of numbers and remainders



mod 12 arithmetic

congruence modulo

Definition Congruence
We say that a is congruent to b modulo m if and only if m divides $a - b$

- Whether two integers a and b have the same remainder when divided by n
- Notation: $a \equiv b \mod m \leftrightarrow$ a is congruent to b modulo m
  $a \not\equiv b \mod m \leftrightarrow$ a is not congruent to b modulo m
- A congruence modulo asks whether or not a and b are in the same equivalence class

Example.
The numbers 31 and 46 are congruent $\mod 3$ because they differ by a multiple of 3.
We can write this as $31 \equiv 46 \mod 3$
Since the difference between 31 and 46 is 15, then these numbers also differ by a multiple of 5; i.e.,
$31 \equiv 46 \mod 5$

Exercise 4.
Find the equivalence classes of $\mod 3$

rules of modular arithmetic

Addition (and subtraction)
If $a \equiv b \mod m$ and
$c \equiv d \mod m$ then
$a + c \equiv b + d \mod m$

Example.
$87 \equiv 2 \mod 17$ and
$222 \equiv 1 \mod 17$
$\implies 87 + 222 \mod 17 \equiv 2 + 1 \mod 17 \equiv 3 \mod 17$

Multiplication
If $a \equiv b \mod m$ and
$c \equiv d \mod m$ then
$a \times c \equiv b \times d \mod m$

Example.
$9876 \equiv 6 \mod 10$ and
$17642 \equiv 2 \mod 10$
$\implies 9876 \times 17642 \mod 10 \equiv 6 \times 2 \mod 10 \equiv 2 \mod 10$

Division
The remainder after division is always congruent to the number we are dividing.

Example.
What is the remainder of 17×18 when it is divided by 19?
We know that $17 \equiv -2 \mod 19$ and $18 \equiv -1 \mod 19$
$\implies 17 \times 18 \equiv (-2) \times (-1) = 2 \mod 19$

Boolean algebra

- consider the following statements that can be either TRUE or FALSE:
  - *Today is Monday AND it is raining*
  - *Today is Monday OR today is NOT Monday*
  - *Today is Monday AND today is NOT Monday*
- Boolean algebra allows us to formalize this sort of reasoning
- Boolean variables may take one of only two possible values: TRUE, FALSE
- there are three fundamental Boolean operators: AND, OR, NOT
- an exhaustive approach to describing when some statement is true (or false): TRUTH TABLES
- the = in Boolean algebra indicates equivalence

Boolean algebra

The three fundamental Boolean operators

1. Logical conjunction: AND $\wedge$
   True only when both A and B are true.

A	B	A AND B
F	F	F
F	T	F
T	F	F
T	T	T

A AND B $= A \wedge B = AB$

Boolean algebra

The three fundamental Boolean operators

1. Logical disjunction: OR $\vee$
   True unless both A and B are false.

A	B	A OR B
F	F	F
F	T	T
T	F	T
T	T	T

A OR B $= A \vee B = A+B$

Boolean algebra

The three fundamental Boolean operators

1. Logical negation: NOT $\neg$
   True when A is false
   False when A is true.

A	NOT A
F	T
T	F

NOT A$= \neg A = A'$

Boolean algebra

Truth table

A	B	A'	B'	AB	A+B
F	F				
F	T				
T	F				
T	T				

Boolean algebra

Truth table

A	B	A'	B'	AB	A+B
F	F	T	T	F	F
F	T	T	F	F	T
T	F	F	T	F	T
T	T	F	F	T	T

Boolean algebra

Exercise 5. write the truth table for (A+B)B

A	B	A+B	(A+B)B
F	F		
F	T		
T	F		
T	T		

Truth tables can be used to prove equivalencies.
What have we proved in this table?