Class Notes; Week 1, 1/15/2016

Introduction
Final worth 200pts
Two midterms both worth 100pts each
Homework worth 150pts total and will be turned in every Friday, there will be between 10-12 assigned
Quizzes worth 100pts total and will be taken every Friday.

Review of Polynomial Formulas and Equations
Quadratic-

Formula: $ax^2 + bx + c = 0$
Equation: $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

Third Degree Polynomial:

Formula: $ax^3 + bx^2 + cx + d = 0$
Equation: Was solved in 1539 by Cardano.

Fourth Degree Polynomial:

Formula: $ax^4 + bx^3 + cx^2 + dx + e = 0$
Equation: Was solved in 1545 by Ferrari.

Fifth Degree Polynomial:

It is impossible to find radical solutions of polynomials with degree greater than or equal to five.
i.e. the solution can not be expressed just by the coefficients of the polynomials.
Discovered by Galois (1811 - 1832) that it is impossible to find a "$x \ldots$"
Considered the Galois Theory.

Chapter 1

Day 1

The Division Algorithim
Theorem 1.1
Let $a, b \in \mathbb{Z}$ where $b > 0$, then there exists a unique $q, r \in \mathbb{Z}$ where $a = bq + r$ and $0 \leq r < b$.

Example. Example: $\frac{82}{7}$
Where 7 is the divisor, 82 is the dividend, 11 is the quotient, and 5 is the remainder.

Well-Ordering Axiom Every non-empty subset of the set of non-negative integers ($\mathbb{Z}_+$) contains a smallest element.
Is this true?
Not Always

Example. $S = \{1, 8, 10, 13\}$ and $S_1 = \{0, 5, 10, 11\}$ and $S_2 = \{x | 0 < x < 1\}$
Where S_2 is taken from the "integer" condition.
Therefore, S_2 does not contain the smallest element.

Proving Theorem 1.1
Let $a, b \in \mathbb{Z}$ be fixed where $b > 0$. Consider set $S = \{a - bx | x \in \mathbb{Z} and a - bx \geq 0\}$
So, S is a non-negative subset of integers.

Step 1: Non-empty
First, show $a + b|a| \geq 0$ so $a + b|a| \in S$
Since $b > 0$ we can say $b \geq 1$
So, $b|a| \geq |a|$ when $|a| > 0$
$b|a| \geq -a$
$a + b|a| \geq 0$
Which implies that S is non-empty.

Step 2: Find q and r
Find $q, r \in \mathbb{Z}$ such that $a = bq + r$
By Well-Ordering Axiom S contains a smallest element: call this r.
Since $r \in S$ we know that $r \geq 0$ and $r = a - bx$ for some x.
Let $x = q$
Thus, $r = a - bq \iff a = bq + r$ and $r \geq 0$

Step 3: Show that $r < b$
Proof by Contradiction.
Assume that $r < b$ is false, thus the new true statement would be $r \geq b$
So, $r - b \geq 0$ then when we plug in what it means for $r \in S$ we see that $r - b \geq 0 \implies (a - bq) - b$
By simplifying: $(a - bq) - b \Rightarrow a - bq - b \Rightarrow a - b(q + 1)$
Since $a - b(q + 1)$ is a non-negative integer, it reasons that it is an element of S.
This creates a contradiction.
When $r - b < r \Rightarrow a - b(q + 1) = r - b < r \Rightarrow a - b(q + 1) < r$
It contradicts that r is the smallest element of S.
Thus, $r \geq b$ is false and $r < b$ is true.

Step 4: Show that q and r are unique
If there are $q, r, q_1, r_1 \in \mathbb{Z}$ such that $a = bq + r$ and $a = bq_1 + r_1$
where $0 \leq r < b$, and $0 \leq r_1 < b$.
So, $a = a \Rightarrow bq + r = bq_1 + r_1 \Rightarrow bq - bq_1 = r_1 - r \Rightarrow b(q - q_1) = r_1 - r$
Sidenote: $0 \leq r < b \Rightarrow -b < -r \leq 0$ and $0 \leq r_1 < b$
So, $-b < r_1 - r < b$
From here, we plug in our solution for $r_1 - r$
See, $-b < b(q - q_1) < b \Rightarrow -1 < q - q_1 < 1$
By $q - q_1 = 0 \Rightarrow q = q_1$
If $q = q_1$ then $r = r_1$

Day 2

Review from last time
$a, b \in \mathbb{Z}$
Then, for the Division Algorithim $a = bq + r$
We assume $b > 0$ and $0 \leq r < b$
Now, we can say a an be either positive or negative.

Example. 1
$a = 4327$ and $b = 281$
$\frac{a}{b} = \frac{4327}{281} = 15.39857\ldots$
Or, in $a = bq + r$ form $q = 15$ and $r = 112$.

Example 2
$a = -7432$ and $b = 453$
$\frac{a}{b} = \frac{-7432}{453} = -16 - 0.40618\cdots = -17 + 0.5938\ldots$
Or, in $a = bq + r$ form $q = -17$ and $r = 269$.

This Time

Section 1.2: Divisibility
Definition: Let $a, b \in \mathbb{Z}$ where $b \neq 0$
Say b divides a $(b \mid a)$ or that b is a divisor of a.
If $a = bc$ for some $c \in \mathbb{Z}$ then $b \mid a$.

In Symbols:

$$\text{"}b \text{ divides } a\text{"} \Rightarrow b \mid a$$
$$\text{"}b \text{ does not divide } a\text{"} \Rightarrow b \nmid a$$

Example. $3 \mid 24$
$7 \nmid 24$

Note 1
Every non-zero integer b divides 0 because $0 = b0$

Note 2
For all $a \in \mathbb{Z}$ see that $1 \mid a$ because $a = 1a$

Remark
If $b \mid a$ then $a = bc$.
We can see that $-a = b(-c)$. Thus, a and $-a$ have the same divisors.

Comment 1
Every divisor of the non-zero integer a is less than or equal to $|a|$.
[In otherwords: if $a = 6$ all the divisors are $\pm 1, \pm 2, \pm 3, \pm 6$]

Comment 2
A non-zero integer has only finite amount of divisors.

Definition: Let $a, b \in \mathbb{Z}$ where $a, b \neq 0$.
The Greatest Common Divisor (gcd) of a, b is the largest integer that divides both a and b.
[In otherwords: d is the gcd of a, b provided that (i) $d \mid a$ and $d \mid b$ and (ii) If $c \mid a$ and $c \mid b$ then $c \leq d$.]
Note: this is notated by (i) $d = \gcd(a, b)$ or (ii) $(a, b) = d$.

Example. $(12, 30) = 6$
Because $12 = 2 \cdot 6$ and $30 = 5 \cdot 6$

Theorem 1.2
Let $a, b \in \mathbb{Z}$ where $a, b \neq 0$ and $d = \gcd(a, b)$ for some $d \in \mathbb{Z}$
Then, there exists (not necessarily unique) $u, v \in \mathbb{Z}$ such that $d = a \cdot u + b \cdot v$

Example. Example
$(12, 30) = 6 \Rightarrow 6 = 30 \cdot (1) + 12 \cdot (-2) \Rightarrow 6 = 6$
So the Theorem works.

Proving Theorem 1.2
Let S be the set of all linear combinations of a and b.
That is: $S = \{a \cdot m + b \cdot n | m, n \in \mathbb{Z}\}$

Step 1: Non-empty
Use the Well-ordering Principle to show that:
If $x \in S$ then $x \in \mathbb{Z}_+$
Note: $a \cdot a + b \cdot b = a^2 + b^2 \geq 0$
$S^+ = \{a \cdot m + b \cdot n | m, n \in \mathbb{Z} \text{ and } a \cdot m + b \cdot n \geq 0\}$
So, S^+ is a non-empty set.
Then, by well-ordering principle, S^+ must contain the smallest positive integer, which we will call t.

Step 2: Prove that $t = \gcd(a, b)$
Must check two things:
(i) $t \mid a$ and $t \mid b$
(ii) If $c \mid a$ and $c \mid b$ then $c \leq t$

Step 2(i): Show that $t \mid a$ and $t \mid b$
By Division Algorithim, there are $q, r \in \mathbb{Z}$ such that $a = tq + r$ where $0 \leq r < t$
$r = a - tq = a - (a \cdot u + b \cdot v)q$
$\Rightarrow r = a - a \cdot u \cdot q - b \cdot v \cdot q$
$\Rightarrow r = a(1 - u \cdot q) + b(-v \cdot q)$
Thus, r is also linear combination of a and b
$r \in S$, $r < t$ (Since t is the smallest element in S^+)
We know that r is not positive.
Since $r \geq 0$ the only possibility is that $r = 0$.

Day 3

Continue From Last Time
Proving Theorem 1.2 :
If $(a, b) = d$ then there exists $u, v \in \mathbb{Z}$ such that $a \cdot u + b \cdot v = d$
S^+ must contain the smallest positive integer, which we will call t where t is the gcd of a and b.
Must check two things:
(i) $t \mid a$ and $t \mid b$
(ii) If $c \mid a$ and $c \mid b$ then $c \leq t$

Proving (i): Show that $t \mid a$ and $t \mid b$
By Division Algorithim, there are $q, r \in \mathbb{Z}$ such that $a = tq + r$ where $0 \leq r < t$
$$r = a - tq = a - (a \cdot u + b \cdot v)q$$
$$\Rightarrow r = a - a \cdot u \cdot q - b \cdot v \cdot q$$
$$\Rightarrow r = a(1 - u \cdot q) + b(-v \cdot q)$$
Thus, $r = a(1 - u \cdot q) + b(-v \cdot q) \in S$ when $u, q, v \in \mathbb{Z}$
Since $r < t$ and t is the smallest non-negative (positive) element in S and $r \geq 0$
we know that $r = 0$

another way of saying the last point
Since $r < t$ and t is the smallest positive element in S , $r \in S$ and $r \leq 0$
When considering $0 \leq r < t$
We see that $r = 0$

So, when $r = 0$ in $a = tq + r \Rightarrow t \mid a$
There is a similar arguement for b.
We can show that $t \mid b$ in the same manner.

Proving (ii) : If $c \mid a$ and $c \mid b$ then $c \leq t$
If $c \mid a$ and $c \mid b$ then $\exists k, s \in \mathbb{Z}$ such that $a = ck$ and $b = cs$
Again: t is the smallest positive integer of S.
$$t = a \cdot u + b \cdot v = (ck)u + (cs)v = c(ku + sv)$$
Where $ku + sv \in \mathbb{Z}$
This implies that $c \mid t$
Which implies that $c \leq |t| = t$

This Time
Theorem 1.3
Let $a, b \in \mathbb{Z}$ where $a, b \neq 0$ and $d, e \in \mathbb{Z}_+$
d is the gcd of $(a, b) \iff$ (i) $d \mid a$ and $d \mid b$ and (ii) If $c \mid a$ and $c \mid b$ then $c \mid b$.

Example. Consider the number 30 and 12
Divisors: $1, 2, 3, 4, 5, 6, 10, 10, 15, 30$
And $1, 2, 3, 4, 6, 12$
The common divisors: $1, 2, 3, 6$
So, $\gcd(30, 12) = 6$
Where $3, 2, 1$ are all factors of 6 and common factors of 30 and 12.

Proving Theorem 1.3
So, for the "if and only if" statement ($\Longleftrightarrow$) we must prove both sides of the argument.

Proving $\Rightarrow$

1. $\gcd(a,b) = d \Rightarrow$ (i) $d \mid a$ and $d \mid b$ and (ii) If $c \mid a$ and $c \mid b$ then $c \mid b$

(i) By definition: If $d = \gcd(a,b)$ then $d \mid a$ and $d \mid b$
(ii) If $d = \gcd(a,b)$ then $d = au + bv$ where $u, v \in \mathbb{Z}$ by Theorem 1.2
So, if $c \mid a$ and $c \mid b$ can we prove that $c \mid d$?
Let $a = ck$ and $b = cs$ for some $k, s \in \mathbb{Z}$
Plug in to $d = au + bv$
$d = (ck)u + (cs)v \Rightarrow c(ku + sv)$ where $ku + vs \in \mathbb{Z}$
Then by definition, $c \mid d$
Thus when $\gcd(a,b) = d \Rightarrow$ (i) $d \mid a$ and $d \mid b$ and (ii) If $c \mid a$ and $c \mid b$ then $c \mid b$

Proving $\Leftarrow$

2. (i) $d \mid a$ and $d \mid b$ and (ii) If $c \mid a$ and $c \mid b$ then $c \mid b \Rightarrow \gcd(a,b) = d$

If d is a positive integer that satisfies (i) and (ii) then $\gcd(a,b) = d$
Proving (i)
This is trivial: by definition this is true.
Proving (ii)
If $c \mid a$ and $c \mid b$ then $c \mid d$
This implies that $c \leq |d| = d$
Thus $c \leq d$
Thus when $c \mid a$ and $c \mid b$ then $c \mid d \Rightarrow \gcd(a,b) = d$

Since both conditions imply the $\gcd(a,b) = d$ we know the statement is true.

Therefore, d is the gcd of $(a,b) \Longleftrightarrow$ (i) $d \mid a$ and $d \mid b$ and (ii) If $c \mid a$ and $c \mid b$ then $c \mid b$ is a true statement.

Asking The Class
If $a \mid b \cdot c$, then $a \mid b$ or $a \mid c$.
Is this true?

No
Example: $a = 6$, $b = 2$, $c = 3$
However
There are sometimes where it does work.
If a, b are already prime and the $\gcd(a,b) = 1$ then $a \mid b \cdot c \Rightarrow a \mid c$

Theorem 1.4
If $a \mid b \cdot c$ and $\gcd(a,b) = 1$ then $a \mid c$

Proving Theorem 1.4
Since $(a,b) = 1$ by Theorem 1.2 $\exists u, v \in \mathbb{Z}$ such that $au + bv = 1$.

Professor's Way

Multiply by c

$auc + bvc = c$ and see $a \mid bc \Rightarrow bc = ar$ for some $r \in \mathbb{Z}$

$auc + v(ar) = c$

$a(uc + vr) = c$

Thus, $a \mid c$

Student Idea

$bc = am$

Side-note: $bv = 1 - au$

$b = \frac{1-au}{v}$

(back to the original thing)

$(\frac{1-au}{v})c = am$

$(1 - au)c = amv$

$c - auc = amv$

$c = amv + auc$

$c = a(mv + uc)$

Thus by definition, $a \mid c$

Note: this way works, but it is different from what the text.

End of Week 1!

Class Notes; Week 2, 1/22/2016

Day 4

Hints for Homework 1

Example. 1
$75 = 3 \cdot 25$ This is not needed.
$7 + 5 = 12$ Since $3 \mid 12$ thus $3 \mid 75$

Example 2
96375
$9 + 6 + 3 + 7 + 5 = 30$ Since $3 \mid 30$ thus $3 \mid 96375$

Example 3
$375 = 3 \cdot 100 + 7 \cdot 10 + 5 \cdot 1$
$99 + 1 = 100$ Use this to see:
$10^n \equiv 1 \mod 3$
Then you can simplify the argument from this.

This Time

Section 1.3: Primes and Factorizations
Definition: Let $p \in \mathbb{Z}$. p is said to be prime if $p \neq 0$, ± 1 and the only divisors of p are ± 1 and $\pm p$.

Example. $2, 3, 5, 7, 11, 13, 17, 19, \ldots$

Note
There are infinitely any primes.

Proving this
Prove by contradiction: Assume there exists a finite amount of primes
Represented by $p_1, p_2, \ldots p_n$
$M = p_1 \cdot p_2 \cdot \ldots p_n + 1$ but $p_1 \nmid M$
All primes cannot divide M implies M is prime.
This contradicts that you listed all possible primes.
Thus, the **Note** is true.
Master Prime Number
For context, primes can be written as $2^n - 1$

Example. $2^{57883161} - 1$ is the biggest prime number
This is not trivial because it has $17, 425, 170$ digits

Euler
A 16^{th} century mathematician
Used hand notation to show that $2^{31} - 1$ is prime
$[2, 147, 483, 647]$

Frank, Nelson, and Cole
In 1876 Lucas proved that $2^{67} - 1$ is not a prime number.
40 years later. in 1903 Frank showed that $2^{67} - 1 = 761838257287 \cdot 193707921$.
This helped in having people recognize him as the greatest mathematician in the 21^{st} century.
[Just a little history about prime numbers]

Remark 1
p is prime $\iff -p$ is prime.

Remark 2
If p, q are prime and $p \mid q$, then $p = \pm q$
Note: Since q is prime, p can only be ± 1 or $\pm q$
But by definition p is prime, $p \neq \pm 1$
So, $p = \pm q$

Theorem 1.5
Let $p \in \mathbb{Z}$ where $p \neq 0, \pm 1$
p is prime $\iff p$ has the property: If $p \mid b \cdot c$ then $p \mid b$ or $p \mid c$.

Proving Theorem 1.5
Prove both sides

p is prime $\Rightarrow p$ has the property: If $p \mid b \cdot c$ then $p \mid b$ or $p \mid c$
If p is prime, then $(p, b) = 1$ and $(p, c) = 1$
p and b relatively prime, p and c relatively prime.
By Theorem 1.4 we know $p \mid c$ or $p \mid b$ holds.
Thus, this is trivial.

p has the property: If $p \mid b \cdot c$ then $p \mid b$ or $p \mid c \Rightarrow p$ is prime
(This is a homework problem)

Corsllary 1.6
If p is prime and $p \mid a_1 \cdot a_2 \cdot \ldots a_n$, then $p \mid a_i$ for some i

Proving Corrally 1.6
If $p \mid a_1 \cdot a_2 \cdot \ldots a_n \iff p \mid a_1 \cdot (a_2 \cdot_3 \cdot \ldots a_n)$
By theorem 1.5 $p \mid a$, or $p \mid a_2 \cdot a_3 \cdot \ldots a_n$
If $p \mid a_1$ we are done.

If not, $p \mid a_2 \cdot a_3 \cdot \ldots a_n$.
Continue this process and we see that after n steps, there exists i such that $p \mid a_i$.

Theorem 1.7

Every integer except $0, \pm 1$ is a product of primes.

Proving Theorem 1.7
Prove by contradiction.

Let S be the set of all integers greater than 1 that are not a product of primes.
Prove that $S = \emptyset$
So say that $S = \emptyset$, then by **Well - Ordering Axiom** S contains the smallest positive element m
m is not prime, then there exists $a, b \in \mathbb{Z}$ such that $m = a \cdot b$
Know, this implies $a, b \notin S$
which means that they are a product of primes.
a be represented by $a = p_1 \cdot p_2 \cdot \ldots p_r$
b represented by $b = q_1 \cdot q_2 \cdot \ldots q_s$
Where all p_1, q_i are primes $\Rightarrow a \cdot b = p_1 \cdot q_1 \cdot p_2 q_2 \cdot \ldots p_r \cdot q_s$
Then, m is the product of primes.
This contradicts that m is an element of S which only holds the integers that are not products of primes.
Therefore, S must be the empty set.

State Theorems 1.8 and 1.10

Theorem 1.10
Let $n > 1$ If n has no positive prime factors less than or equal to $\sqrt{n}$ then n is prime.

Proving Theorem 1.10 If n is a composition number n can be represented $a \cdot b$ $(n = a \cdot b)$
If $a > \sqrt{n}$ and $b > \sqrt{n} \Rightarrow n = a \cdot b > n$
This is not possible.

Example. $137 = a \cdot b$
At least a or $b \leq \sqrt{137} \equiv 12$
Check all primes under 12 $(2, 3, 5, 7, 11)$

Theorem 1.8
The Fundamental Theorem of Arithmetic.
Every integer n , $n \neq 0, \pm 1$ is a product of primes.
Prime Factorization is unique in:

$$n = p_1 \cdot p_2 \cdot \ldots p_r \text{ and } n = q_1 \cdot q_2 \cdot \ldots q_s$$

Then $r = s$ (The number of prime factors are equal).
After renaming and reordering: $p_1 = \pm q_1 \ldots p_r = \pm q_r$.

Day 5

Quiz Day
Turn in Homework

Going over assignment

Section 1.3 Problem 34

Prove or disprove: If $n \in \mathbb{Z}$ and $n > 2$ then there exists a prime $p \in \mathbb{Z}$ such that $n < p < n!$

Let $n \in \mathbb{Z}$ where $n \geq 3$
Assume $m = n! - 1$
This is less then $n!$
If m is prime, we are done.

If m is not prime, there exists p prime such that $p \mid m < n!$
Now, show $p > n$
Let $k \nmid n! - 1$ if $k \in \{2, 3, 4, \ldots n\}$
So , $p > n$

Section 1.3 Problem 36 Prove that when $p, q \geq 5$ and prime, then $24 \mid p^2 - q^2$

$24 \mid p^2 - q^2 \Rightarrow 3 \cdot 8 \mid p^2 - q^2$
Proving $3 \mid p^2 - q^2$
p prime $\Rightarrow p = 3k, 3k+1, 3k+2$
except not $3k$ because it is prime and cannot have a factor besides $\pm p$ or ± 1.
$p^2 = 9k^2 + 6k + 1 = 1 \mod (3)$ or $p^2 = 9k^2 + 12k + 4 = 1 \mod (3)$.

Proving $8 \mid p^2 - q^2$
Similar reasoning.

This Time

Chapter 2

Congruence in $\mathbb{Z}$ and Modular Arithmetic

Section 2.1

Definition: Let $a, b, n \in \mathbb{Z}$ where $n > 0$
Then a is congruent to b modular n provided that $n \mid a - b$.

In symbols: $a \equiv b \mod n$ or $a \equiv b(n)$

Example. 1
$17 \equiv 5 \mod 6$

Example 2
$23 \equiv 17 \mod 6 \Rightarrow 23 \equiv 5 \mod 6$

This is a conditional and an $\iff$ statement.

Modular System
Two non-trivial theorems:

1. If p prime and $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$
Fermat little theorem
2. If p prime then $(p-1)! \equiv -1 \mod p$
Wilson theorem.

Example. 1
$2^6 \equiv 1 \mod 7$
$3^6 \equiv ? \mod 7 \Rightarrow 3^6 \equiv 1 \mod 7$
$4^6 \equiv 1 \mod 7$
$5^6 \equiv 1 \mod 7$
These are all true.

Example 2
$6! \equiv -1 \mod 7$

Example 3
$7^8 \equiv ? \mod 7 \Rightarrow 7^8 \equiv 1 \mod 8$
$15^6 \equiv 1 \mod 7$
$17^6 \equiv 1 \mod 7$
These are trivial because it is reliant upon $p \nmid a$

Theorem 2.1

Equivalent classes

Let n be a positive integer.
For all $a, b, c \in \mathbb{Z}$

1
$a \equiv a \mod n$

2
$a \equiv b \mod n \Rightarrow b \equiv a \mod n$

3
$a \equiv b \mod n$ and $b \equiv c \mod n \Rightarrow a \equiv c \mod n$

Proving Theorem 2.1

1 : Reflexive
Trivial.

2 : Symmetric
King of trivial, but a little more work.

3 : Transative
$a = qn + r$ then it is trivial.
See $n \mid a - b$ and $n \mid b - c \Rightarrow n \mid a - b + b - c = n \mid a - c$

This is an important foundation to prove theories.

End of Week 2!

Class Notes; Week 3, 1/29/2016

Day 6

Hints from the Grader
Tom Gannon
gannonth@msu.edu

Example. Expected Homework solution
Let $n \in \mathbb{Z}$ what are the values of $(n\ ,\ n+2)$?
Let $d = \gcd(n, n+2)$ for some $n \in \mathbb{Z}$
then $d \mid n$ and $d \mid n+2$
There are $l, k \in \mathbb{Z}$ where $n = d \cdot k$ and $n + 2 = d \cdot l$ by definition of divisibility
Then $2 = 2 + n - n = d \cdot l - d \cdot k \Rightarrow 2 = d \cdot (l - k)$
Thus $d \mid 2$ and the only positive divisors of $2 = 1, 2$
Therefore the only possible values are $1, 2$.

Question 2 From Quiz

$p \mid b \cdot c \Rightarrow p \mid b$ or $p \mid c$, Prove this is prime
Assume $p = m \cdot n$ for some $m, n \in \mathbb{Z}$
Two conditions: (1) $p \mid m \Rightarrow \frac{m}{p} = \frac{1}{n}$
For $\frac{m}{p} \in \mathbb{Z} \Rightarrow \frac{1}{n} \in \mathbb{Z}$ only when $n = \pm 1$
Thus p is prime.
Similar reasoning for $p \mid n$
p has a factor d, $d \mid p \Rightarrow p = d \cdot t$ for some $t \in \mathbb{Z}$

this implies that $p \mid d$ or $p \mid t$
If $d \mid p$ and $p \mid d \Rightarrow p = \pm d$

This Time

Theorem 2.2
If $a \equiv b \mod n$ and $c \equiv d \mod n$ then $a + c \equiv b + n \mod n$ and $ac \equiv bd \mod n$

Example. $4 \equiv 1 \mod 3$ and $5 \equiv 2 \mod 3$
$4 + 5 \equiv 1 + 2 \mod 3$ and $4 \cdot 5 \equiv 1 \cdot 2 \mod 3$

Proving Theorem 2.2
If $a \equiv b \mod n$, $c \equiv d \mod n$ then $n \mid (a - b)$ and $n \mid (c - d)$.
(1) Since $n \mid (a - b)$ and $n \mid (c - d)$, then $n \mid (a - b) + (c - d)$
Then $n \mid (a + c) - (b + d) \Rightarrow a + c \equiv b + d \mod n$
(2) Home work problem
Hint: $a = n \cdot k_1 + r$, $b = n \cdot k_2 + r$, $c = n \cdot k_3 + r_1$, $d = n \cdot k_4 + r_1$

Definition
Let $a, n \in \mathbb{Z}$ where $n > 0$
The congruent class of a modulo n (denoted $[a]$) is the set of all the integers that are congruent to n :
$[a] = \{b | b \in \mathbb{Z}, b \equiv a \mod n\}$
$[a] = \{b | b = a + k \cdot n$ some $k \in \mathbb{Z}\} = \{a + k \cdot n | k \in \mathbb{Z}\}$

Example. 1
In Congruence modulo 5 we have:
$[9] = \{9 + 5k | k \in \mathbb{Z}\} = \{\cdots - 6, -1, 4, 9, 14, 19 \dots\}$
$[9] = [14] = [-6]$

Example. 2
In modulo 3 we see:
$[2] = \{\cdots - 4, -1, 2, 5, 8, 11 \dots\}$

Theorem 2.3
$a \equiv c \mod n \iff [a] = [c]$

Proving Theorem 2.3

$\Rightarrow$ **If** $a \equiv c \mod n \Rightarrow [a] \subseteq [c]$ **and** $[c] \subseteq [a]$
Let $b \in [a]$ prove $b \in [c]$
By definition $b \equiv a \mod n$
Since $a \equiv c \mod n$ by transitivity $b \equiv c \mod n$
Thus, $b \in [c]$ and $[a] \subseteq [c]$

Let $d \in [c]$ prove $d \in [a]$
By definition $d \equiv c \mod n$
By reflexive property: $a \equiv c \mod n \Rightarrow c \equiv a \mod n$
Then by transitivity: $d \equiv a \mod n$

$$\text{Thus, } d \in [a] \text{ and } [c] \subseteq [a]$$
$$\text{Therefore } [a] = [c]$$

$$\Leftarrow \textbf{If } [a] = [c] \Rightarrow a \equiv c \mod n$$
$$\text{Let } a \in [a]$$
$$\text{Then } a \equiv a \mod n$$
$$a \in [a] \Rightarrow a \in [c] \text{ then } a \equiv c \mod n$$

Corallary 2.4

Two congruence classes modulo n either disjoint or identical.

So. $[a] = [c]$ or $[a] \cap [c] = \emptyset$

Proving Cor. 2.4

If $[a]$ and $[c]$ are disjoint, then we are done.

If not, we have a bit more work.

$$[a] \cap [c] \neq \emptyset \text{ then } [a] \cap [c] = \{b\}$$
$$b \in [a] \Rightarrow b \equiv a \mod n$$
$$b \in [c] \Rightarrow b \equiv c \mod n$$
$$\text{By reflexive, then transitive we see } a \equiv c \mod n$$
$$\text{Then by theorem 2.3 } [a] = [c]$$
Thus when the intersect is not the empty set, the classes are equal.

State Corallary 2.5

Let $n > 1$ where $n \in \mathbb{Z}$ and consider congruence modulo n
(1) If $a \in \mathbb{Z}$ and r is the remainder $0 \leq r < n$
When a divided n then $[a] = [r]$
(2) Then, there are exactly n distinct congruent classes, namely:
$[0], [1], [2], \dots [n-1]$ that are possible

Day 7

From Last Time
Proving Cor. 2.5

Let $n > 1$ be an integer and consider congruence modulo n
(1) If $a \in \mathbb{Z}$ and r is the remainder $0 \leq r < n$
When a divided n then $[a] = [r]$
(2) Then, there are exactly n distinct congruent classes, namely:
$[0], [1], [2], \dots [n-1]$ that are possible

(1)

$$a = n \cdot q + r \text{ when } q \in \mathbb{Z} \text{ , } 0 \leq r < n$$
$$a - r = n \cdot q$$
$$a \equiv r \mod n \text{ by theorem 2.3 } [a] = [r]$$
[Remember: $[a]$ holds all the integers such that their remainder is in the same set.]

(2)
We have $[0], [1], [2], \ldots [n-1]$ as a list on n congruent classes.
Need to show that these n classes are all distinct.
Proof by contradiction.
Assume s, t are distinct elements in the list such that $[s] = [t]$
By theorem 2.3 $[s] = [t] \Rightarrow s \equiv t \mod n$
$\Rightarrow s - t = n \cdot k$ some $k \in \mathbb{Z}$
$\Rightarrow n \mod s - t \Rightarrow -n < s - t < n$
Where the only case is $s = t$
This contradicts that s and t are distinct integers.
Thus, no two of $[0], [1], [2], \ldots [n-1]$ are congruent modulo n
By theorem 2.3 $[0], [1], [2], \ldots [n-1]$ are all distinct.

Example. 3
$N = \{\{3 \cdot k\}, \{3 \cdot k + 1\}, \{3 \cdot k + 2\}\}$
2
$N = \{\{2 \cdot k\}, \{2 \cdot k + 1\}\}$ (even or odd cases)

This Time

Definition: The set of all congruent classes modulo n is denoted $\mathbb{Z}_n$ (read "$\mathbb{Z} \mod n$)

Example. In real numbers this is true:
If $a \cdot b = o \Rightarrow a = 0$ or $b = 0$
But in $\mathbb{Z}_4$ this is not true:
$[2] \cdot [2] = [0]$ in $\mathbb{Z}_4$

Section 2.2

Modular Arithmetic

$[a] \in \mathbb{Z}_n$ of $[0], [1], [2] \ldots [n-1]$ is the bracket a set containing infinitely many numbers
The sum of $[a]$ and $[c]$ is the class containing $a + c$

In symbols:
$[a] + [c] = [a + c]$
And for multiplication we see:
$[a] \cdot [c] = [a \cdot c]$

Example. 1
$N = \{\{3 \cdot k\}, \{3 \cdot k + 1\}, \{3 \cdot k + 2\}\}$
$[a] = [3 \cdot k + 1]$, $[c] = [3 \cdot k + 2]$
$[a] + [c] = [3 \cdot k + 1] + [3 \cdot k + 2] = [3 \cdot k + 3] = [3 \cdot k]$ which is the set of all integers divisible by 3
$[a + c] = [3 \cdot k + 1 + 3 \cdot k + 2] = [6k + 3] = [3k]$ which is the set of all integers divisible by 3

Example. 2

$\mathbb{Z}_5$

$[3]+[4]=[3+4]=[7]=[2]$

$[3]\cdot[2]=[3\cdot 2]=[6]=[1]$

Theorem 2.6

If $[a]=[b]$ and $[c]=[d]$ in $\mathbb{Z}_n$ then $[a+c]=[b+d]$ and $[ac]=[bd]$

Confirm Not Prove

$[a]=[b] \Rightarrow a \equiv b \mod n$

$[c]=[d] \Rightarrow c \equiv d \mod n$

Say there is a very nice algebraic structure between them.

Definition:

Addition and Multiplication in $\mathbb{Z}_n$ are defined:

(1) $[a]+[c]=[a+c]$

(2) $[a]\cdot[c]=[a\cdot c]$

Example. Addition and Multiplication Table in $\mathbb{Z}_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$[2]+[2]=[2]\cdot[2]$

Properties of Modulo arithmetic

(1)If $a,b\in\mathbb{Z}$ then $a+b\in\mathbb{Z}$ [Closure for addition]

(2) $a+(b+c)=(a+b)+c$ [Associative of addition]

(3) $a+b=b+a$ [Commutative addition]

(4) There exists an 0 such that $a+0=0+a=a$ [Addition identity]

(5) $a+x=0$ has a solution in $\mathbb{Z}$

(6) $a,b\in\mathbb{Z}$ then $a\cdot b\in\mathbb{Z}$ [Closure for multiplication]

(7) $a(b\cdot c)=(a\cdot b)c$ [Associative of multiplication]

(8) $a(b+c)=ab+bc$ and $(a+b)c=ac+bc$ [Distributive laws]

(9) $a\cdot b=b\cdot a$ [Commutative multiplication]

(10) $a \cdot 1 = 1 \cdot a = a$ [Multiplication identity]
(11) $a \cdot b = 0$ then $a = 0$ or $b = 0$

True for [in $\mathbb{Z}_n$]
(1) , (2) , (3) , (4) , (5) , (6) , (7) , (8) , (9) , (10)
(5) $[a] + [n-1]$
Not (11)
For $\mathbb{Z}_n$ if n is not prime

$[a]^k = [a] \cdot [a] \cdot \ldots [a]$ for $k \in \mathbb{Z}$ (k factors) exponent of $\mathbb{Z}_n$

Example. 1
in $\mathbb{Z}_5$
$[3]^2 = [4]$
$[3]^4 = [1]$

Example. 2
Solve $(x^2 + [5]) \cdot x = [0]$ in $\mathbb{Z}_6$
$[0] = [0]$ $[3] = [0]$
$[1] = [0]$ $[4] = [0]$
$[2] = [0]$ $[5] = [0]$

Day 8

Quiz Day
Turn in Homework

Going over assignment
Section 2.1 Problem 21(b)
Every positive integer is congruent to the sum of its integers modulo 9.

$$38 \equiv 2 \mod 9$$
$$11235 \equiv 3 \mod 9$$
$$10^n \equiv 1 \mod 9 \text{ for all } n \Rightarrow (9+1)^n$$
$$378 = 3 \cdot 10^2 + 7 \cdot 10 + 8$$
$$a_n \cdot a_{n-1} \cdot a_{n-2} \ldots a_1 = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \ldots a_1 \cdot 10^0$$
$$\Rightarrow a_1 + a_2 \ldots a_n \mod 9$$

This Time

Congruence in $\mathbb{Z}$ and Modular Arithmetic

Section 2.3

The structure of $\mathbb{Z}_p$ (p is prime) and $\mathbb{Z}_n$

New notation: $\mathbb{Z}_n$ $[0],[1],[2]\dots[n-1]$
If making no confusion, we write:
$0,1,2\dots n-1]$ in $\mathbb{Z}_n$

Example. 1
In $\mathbb{Z}_6$:
$2\cdot 3=0$ instead of $[2]\cdot[3]=[0]$
We use 2 in $\mathbb{Z}_n$ instead of [2] in $\mathbb{Z}_n$

Example 2
Addition Table of $\mathbb{Z}_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Example. 3 In $\mathbb{Z}_6$ solution for $2\cdot x=1$?
No solution

Question
For what kind n , $2\cdot x=1$ with solutions?
n and a , $a\cdot x=1$

Theorem 2.8

If $p>1$ where $p\in\mathbb{Z}$ then the conditions are equivalent when:
(1) p is prime
(2) For any $a\neq 0$ in $\mathbb{Z}_p$ then $a\cdot x+1$ has a solution in $\mathbb{Z}_p$
(3) Whenever $b\cdot c=0$ in $\mathbb{Z}_p$ then $b=0$ or $c=0$
Proving Theorem 2.8
$(1)\Rightarrow(2)\Rightarrow(3)\Rightarrow(1)$

(1) $\Rightarrow$ (2)
If p is prime and $a\neq 0$ in $\mathbb{Z}_p$
$$a\not\equiv 0 \mod p$$
$$\gcd(a,p)=1\Rightarrow au+pv=1 \text{ some } u,v\in\mathbb{Z}$$
$$\Rightarrow au\equiv 1 \mod p$$

(2) $\Rightarrow$ (3)
If $a\cdot b=0$ in $\mathbb{Z}_p$
$a\neq 0$ in $\mathbb{Z}_p\Rightarrow$ by (2) $a\cdot u=1$
Thus $1\cdot b=0$ in $\mathbb{Z}_p$
$\Rightarrow b=0$ in $\mathbb{Z}_p$
$$0=u\cdot 0=u\cdot a\cdot b=a\cdot u\cdot b=1\cdot b=b$$

(3) $\Rightarrow$ (1)
If $b \cdot c = 0$ in $\mathbb{Z}_p \Rightarrow b = 0$ or $c = 0$
$\Rightarrow p \mid b \cdot c \Rightarrow p \mid b$ or $p \mid c$
(? $\Rightarrow p$ is prime - this is from Quiz 1)
Assume factor d of p
Prove $d = \pm p$

End of Week 3!

Class Notes; Week 4, 2/5/2016

Day 9

Going Over Quiz

Quiz: Question 1 part b
If p is prime $\Rightarrow$ If $p \mid ab \Rightarrow p \mid b$ or $p \mid a$
If p is prime and if $p \mid ab$ prove $p \mid a$ pr $p \mid b$

If $p \mid b$ then we are done

If not, i.e. $p \nmid b$ try to prove $p \mid a$
$\gcd(p, b) = 1$
(way 1)
$\gcd(p, b) = 1$ and $p \mid ab$ then $p \mid a$
(way 2)
There exists $u, v \in \mathbb{Z}$ such that $pu + bv = 1$
$\Rightarrow bv = 1 - pu$
Regard $pk = ab \Rightarrow pkv = a - apu$
$\Rightarrow p(kv + au) = a$
Thus $p \mid a$

This Time Cor. 2.9

Let $a, b, n \in \mathbb{Z}$ where $n > 1$ and $\gcd(a, n) = 1$
Then $ax = b$ has a unique solution in $\mathbb{Z}_n$

MEMORIZE next thing

Previosuly Proved:
If $p > 1$ where $p \in \mathbb{Z}$ then the conditions are equivalent when:
(1) p is prime
(2) For any $a \neq 0$ in $\mathbb{Z}_p$ then $a \cdot x + 1$ has a solution in $\mathbb{Z}_p$
(3) Whenever $b \cdot c = 0$ in $\mathbb{Z}_p$ then $b = 0$ or $c = 0$

Proving Cor. 2.9
If $\gcd(a, n) = 1 \Rightarrow au + nv = 1$ some $u, v \in \mathbb{Z}$
$\Rightarrow au = 1$ in $\mathbb{Z}_n \Rightarrow aub = b$
So, ub is a solution of $ax = b$

Prove the it is unique:
If w is another solution for $ax = b \Rightarrow aw = b$
$aw = b$ and $aub = b \Rightarrow aw - aub = b - b = 0$
$\Rightarrow a(w - ub) = 0 \Rightarrow au(w - ub) = u0 = 0$
$\Rightarrow (w - ub) = 0 \Rightarrow w - ub = 0 \Rightarrow w = ub$
Thus $w = ub$ and the solution is unique.

Example. 1
p is not prime:
$\mathbb{Z}_4$ breaks for the 3^{rd} condition

Example. 2
$24x = 5$ in $\mathbb{Z}_{95}$
Unique solution or not?
$(95, 24) = 1$
$5x = 5$ in $\mathbb{Z}_5$ then $x = 1$
$5x = 5$ in $\mathbb{Z}_{95}$ then $x = 1, 20, 39 \ldots$

Chapter 3

Rings

Section 3.1

We like to keep our basic properties of $\mathbb{Z}$ and $\mathbb{Z}_n$

Definition
A ring is a non-empty set R equipped with two operations (usually written as addition and multiplication) that satisfies the following axioms:

For all $a, b, c \in \mathbb{R}$
(1) Closure under addition
If $a \in R$, $b \in R$ then $a + b \in R$
(2) Association under addition

$a + (b + c) = (a + b) + c$
(3) Commutative under addition
$a + b = b + a$
(4) Addition Identity
There exists 0_r in R where $a + 0_R = 0_R + a = a$ for all $a \in R$
(5) Inverse of addition
For all $a \in R$, $a + x = 0_R$ has a solution in R
(6) Closure under multiplication
If $a \in R$, $b \in R$ then $ab \in R$
(7) Association of multiplication
$a(bc) = (ab)c$
(8) Distributive Laws
$a(b + c) = ab + ac$ and $(a + b)c = ac + bc$

Example. 1
$\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{I}$ are all rings
Example. 2
Even numbers is a ring
Odd numbers is not: Violates the 1^{st} axiom
$M_2(\mathbb{K}) = \{$ matrix below $\mid a, b, c, d \in \mathbb{R}\}$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
Not: fails commutative of multiplication axiom

Day 10

From Last Time

Definition of Rings

Even numbers are a ring without identity
This Time

Units and Zero Divisors

Units

An element in $\mathbb{Z}_n$ is called a unit if the equation $ax = 1$ has a solution.
There exists $b \in \mathbb{Z}_n$ such that $ab = 1$
Say b is the inverse of a
Zero Divisor

A non-zero element in $\mathbb{Z}_n$ is called a zero divisor if the equation $ax = 0$ has non-zero solutions
There exists $c \in \mathbb{Z}_n$ such that $ac = 0$

Example. 1
in $\mathbb{Z}_4$
$0, 1, 2, 3$
Neither , unit , zero-divisor , unit

Example. 2
in $\mathbb{Z}_8$
(Homework problem)
Units: $1, 3, 5, 7$
Zero Divisors: $2, 4, 6$

Definition

An integral Domain is n commutative ring R with identity $1_R \neq 0_R$ that satisfies this axiom:
(11) whenever $a, b \in \mathbb{R}$ and $ab = 0_R$ then $a = 0_R$ or $b = 0_R$

Example. 1
in $\mathbb{Z}_7$
(if p is prime $p \mid ba \Rightarrow p \mid a$ or $p \mid b$
an integral domain
NOTE every non-zero element in $\mathbb{Z}_7$ is a unit not a zero divisor

Example. 2
in $\mathbb{Z}_6$
$2 \cdot 3 = 0_R$ but $2 \neq 0_R$ and $3 \neq 0_R$
So if p is prime $\mathbb{Z}_p$ is an integral domain, if not $\mathbb{Z}_p$ is not an integral domain

Definition
A field is a computative ring with identity $1_R \neq 0_R$ that satisfies this axiom:
(12) for any $a \neq 0 \in R$ the equation $ax = 1_R$ has a solution in R
[every non-zero element has multiplication inverse $\rightarrow$ a unit]

Example. in $\mathbb{Z}_7$
yes: so, $\mathbb{Z}_p$ is a field such that p is prime.

Question?
Is every field an integral domain?
Yes: if $ab = 0$
when $a = 0$ we are done
when $a \neq 0$ there exists u such that $au = 1$
$u(ab) = 0 \Rightarrow (ua)b = 0 \Rightarrow b = 0$
Thus a field is integral domain.

Question?
Is every integral domain a field?
Things that work: $\mathbb{R}, \mathbb{C}, \mathbb{Q}$
Things that do not $\mathbb{Z}$
Thus, no. Not every integral domain is a field.

a finite integral domain $\Rightarrow$ a field

Example. 1
Check $\mathbb{C}$ (Complex) is a field:
(1) $a + bi \in \mathbb{C}$ and $c + di \in \mathbb{C}$
$a + bi + c + ci = (a + c) + (b + d)i \in \mathbb{C}$
Addition closure holds
(2) associative addition
...
Commutative:
(a+bi)(c+di) = (c+di)(a+bi)
(10) for all $a + bi \in \mathbb{C} \neq 0$
$\frac{1}{a+bi} \in \mathbb{C}???$
$\frac{a-bi}{a^2+bi^2} = \frac{a}{a^2+bi^2} + \frac{-b}{a^2+bi^2}i \in \mathbb{C}$
Therefore, this satisfies all the conditions/

Example. 2
Take the set of all $2X2$ matrices of the form
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$
Where $a, b \in \mathbb{R}$
[$\mathbb{R}$ is real : R is a ring]
Claim k is a field.

Proof : sketch
1. $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in K = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} \in K$
Holds.
2. Show for everything
...
6. $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in K = \begin{pmatrix} ac+bd & ad-bc \\ bc-ad & bd+ac \end{pmatrix} \in K$

Day 11

Quiz Day
Turn in Homework

Going over assignment
Problem 5

$\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}$ with $r \in \mathbb{Q}$
$\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & r_1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
If $\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & r_1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}$ Then $\begin{pmatrix} 0 & r_1 \\ 0 & 0 \end{pmatrix}$ is the multiplication identity.

(d.)
$\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}$
$\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ ab & 0 \end{pmatrix}$
If $\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}$ Then $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ is the multiplication identity.

Problem 14

Let $a, b, n \in \mathbb{Z}$ where $n > 1$ $d = (a, n)$ $d \mid b$ $ax = b$ has d distinct solution in $\mathbb{Z}_n$.
a.) $2x = 2$ in $\mathbb{Z}_4$ $1, 3$
$3x = 3$ in $\mathbb{Z}_6$ $1, 3, 5$
$[ub_1], [ub_1 + n_1], [ub_1 + 2n_1] \cdot [ub_1 + (d-1)n_1]$
$n_1 \Rightarrow n \mid d \Rightarrow n = n_1 d$ from problem 13
$au + nv = d \Rightarrow a = da_1$, $b = db_1$, $n = dn_1$
$\mathbb{Z}_n - n = dn_1$
$a_1 x = b_1$ in $\mathbb{Z}_n$
THIS WON'T BE GRADED IN THE HOMEWORK

This Time

Example. $K = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ prove that K is a field.

Associative addition

$$(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}) + \begin{pmatrix} e & f \\ -f & e \end{pmatrix} \text{ ?=? } \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + (\begin{pmatrix} c & d \\ -d & c \end{pmatrix} + \begin{pmatrix} e & f \\ -f & e \end{pmatrix})$$

[Only check the non-trivial properties]

Closure under multiplication

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & ac - bd \end{pmatrix}$$

Commutative multiplication

$$\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \cdot \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & ac - bd \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ ?} \in K\text{? Yes}$$

What defines a field over a ring?

For any $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K$ there is an inverse
$x = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix}$ $?{\in}?K$ yes.
$X \cdot \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ true.

End of Week 4!

Class Notes; Week 5, 2/12/2016

Day 12

Going Over Quiz

Integral Domain:
A commutative ring with 1_R such that if $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$.

Example. $\mathbb{Z}$

Some put $2\mathbb{Z}$ or $3\mathbb{Z}$
is $3\mathbb{Z}$ a field? No
It is not a commutative ring with 1_R
$\{0, 3, 6, 9, 12 \dots\}$ $3x = 1$
$2\mathbb{Z}$ is an integral domain but not a field.

This Time

Continue with 3.1

Let $a, b, n \in \mathbb{Z}$ where $n > 1$ and $\gcd(a, n) = 1$
Then $ax = b$ has a unique solution in $\mathbb{Z}_n$

Example. Cartesian Product of $\mathbb{Z}_6 X \mathbb{Z} = \{(a, z) \mid a \in \mathbb{Z}_6, z \in \mathbb{Z}\}$
$(a, z) + (a_1, z_1) = (a + a_1, z + z_1)$
$(a, z) \cdot (a_1, z_1) = (a \cdot a_1, z \cdot z_1)$

Theorem 3.1
Let R and S be rings.

Definition: Addition and Multiplication
RXS by :
$(r, s) + (r_1, s_1) = (r + r_1, s + s_1)$
$(r, s) \cdot (r_1, s_1) = (r \cdot r_1, s \cdot s_1)$
Then RXS is a ring.

Note:
If R and S are both commutative then so is RXS.
If R and S are both identity then so is RXS.

$2\mathbb{Z}\ X\ M_2(\mathbb{R})$
$M_2(\mathbb{R})$ is not commutative, thus $2\mathbb{Z}\ X\ M_2(\mathbb{R})$ is not.
$2\mathbb{Z}$ is not an identity, thus $2\mathbb{Z}\ X\ M_2(\mathbb{R})$ is not.

Subring
When a subset S of ring R ($S \subset R$) is a ring under addition and multiplication in R then S is a subring.

Subfield
When a subset S of ring R ($S \subset R$) is a field under addition and multiplication in R then S is a subfield.

Example. 1
$\mathbb{Z}$ be a subring of $\mathbb{Q}$ (rationals)

Example. 2
$\mathbb{Q}$ a subfield of $\mathbb{R}$ (reals)
$\mathbb{Z}$ is not a subfield of $\mathbb{R}$ because $\mathbb{Z}$ is not a field (no multiplication identity)

Theorem 3.2

Suppose R is a ring and S is a subset of R ($S \subset R$) such that:
(1) S is closed under addition
- if $a, b \in S$ then $a + b \in S$
(2) S closed under multiplication
- $a, b \in S$ then $ab \in S$
(3) addition identity $\in S$
(4) $a \in S$ then $a + x = 0$ has a solution in S
Then S is a subring of R.

Prove why this is enough:

Axioms (1 - 8) of a ring
Closure under addition
(1) S is closed under addition $\iff$ (1)

(2) S closed under multiplication $\iff$ (6)
(3) addition identity $\in S \iff$ (4)
(4) $a \in S$ then $a + x = 0$ has a solution in $S \iff$ (5)
Leaving: (2) associative addition, (3) commutative addition, (7) associative multiplication , (8) distribution laws.

instance (3)

for all $a, b \in R$ $a + b = b + a$
$a, b \in S \subset R$ $a + b = b + a$ for any two elements in S

similar (2) , (7) , (8)

for all $a, b, c \in R$ $(a + b) + c = a + (b + c)$
$a, b, c \in S \subset R$

Example. 1

$2\mathbb{Z}$ subring $\mathbb{Z}$
$a \in 2\mathbb{Z}$,$b \in 2\mathbb{Z}$ $a + b \in 2\mathbb{Z}$ yes and $ab \in 2\mathbb{Z}$ yes.
$0 \in \mathbb{Z}$ yes
$a + x = 0$ $a \in 2\mathbb{Z}$ then $-a \in 2\mathbb{Z}$ yes.

Example. 2

$s \subset M_2(\mathbb{R})$ by $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} + \begin{pmatrix} a_1 & 0 \\ b_1 & c_1 \end{pmatrix} = \begin{pmatrix} a + a_1 & 0 \\ b + b_1 & c + c_1 \end{pmatrix}$$

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \cdot \begin{pmatrix} a_1 & 0 \\ b_1 & c_1 \end{pmatrix} = \begin{pmatrix} aa_1 & 0 \\ ba_1 + cb_1 & cc_1 \end{pmatrix}$$

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \text{ for the zero matrix}$$

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} + \begin{pmatrix} -a & 0 \\ -b & -c \end{pmatrix} = \begin{pmatrix} a + a_1 & 0 \\ b + b_1 & c + c_1 \end{pmatrix}$$

Example. 3

$\mathbb{Z}\{\sqrt{2}\} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$
check a subring in $\mathbb{R}$

Day 13

Hints towards Homework:

Section 3.1 problem 25
on $\mathbb{Q}$ $a \oplus b = a + b + 1$
$a \odot b = ab + a + b$
Prove it is a commutative ring with identity? and integral domain?
there exists 0_R $a \oplus 0_R = a$
$a \oplus b = a \Rightarrow a + b + 1 = a \Rightarrow b = -1 = 0_R$

there exists 1_R $a \odot b = a \Rightarrow ab + a + b = a \Rightarrow a(b+1) + b = 0 \Rightarrow b = 0 = 1_R$
if $ab = 0_R = -1 \Rightarrow a = 0_R$ or $b = 0_R$
This Time

Section 3.2
Basic properties of rings

Theorem 3.3

For any element a in a ring R the equation $a + x = 0_R$ has a unique solution.
Proving

By axiom 5 of a ring:
$a + x = 0_R$ has a solution
let u be a solution $\rightarrow a + u = 0_R$
and v be a solution $\rightarrow a + v = 0_R$
$v = v + 0_R = v + (a + u)$ by associative
$\Rightarrow (v + a) + u$ by commutative
$\Rightarrow 0_R + u = u$ by definition

Comment

Denote the unique solution by "$-a$".
Say $-a$ is the unique element in R where $a + (-a) = 0 = -a + a$

Example. 1
in $\mathbb{Z}_6$
the solution $2 + x = 0$ is 4

Example. 2
in $\mathbb{Z}_{14}$
the solution $5 + x = 0$ is 9

Theorem 3.4
If $a + b = a + c$ in a ring R, then $b = c$
Sidenote: in ring R is it true that if $ab = ac$ then $b = c$? No. $2 \cdot 0 = 2 \cdot 3$ in $\mathbb{Z}_6$ but $0 \neq 3$

Proof
if $a + b = a + c$
$a + (-a) + b = a + (-a) + c$
$0_R + b = 0_R + c \Rightarrow b = c$

Theorem 3.5
For any elements $a, b \in R$ (ring)
(1) $a \cdot 0_R = 0_R = 0_R \cdot a$
(2) $a(-b) = -ab$ and $(-a)b = -ab$
(3) $-(-a) = a$

(4) $-(a+b) = (-a) + (-b)$
(5) $-(a-b) = (-a) + b$
(6) $(-a)(-b) = ab$
(7) If R has an identity then $(-1_R)a = -a$

Proof:
(1) $a \cdot 0_R = 0_R = 0_R \cdot a$
$a \cdot 0_R ? =?0_R$
$0_R + 0_R = 0_R \Rightarrow a(0_R + 0_R) = a \cdot 0_R$
$\Rightarrow a \cdot 0_R + a \cdot 0_R = a \cdot 0_R$ by distributive laws
$\Rightarrow 0_R + a \cdot 0_R = a \cdot 0_R + a \cdot 0_R \Rightarrow 0_R = a \cdot 0_R$ by theorem 3.4
(2) $a(-b) = -ab$ and $(-a)b = -ab$
By definition $-ab$ unique solution of $ab + x = 0_R$ So any other solution of $ab + x = 0_R$ must be $-ab$
We want to show $a(-b)$ is a solution $ab + x = 0_R$
$ab + (a(-b)) = 0_R$
$a(b + (-b)) = 0_R \Rightarrow a \cdot 0_R = 0_R$
Similar for $(-a)b = -ab$
(3) $-(-a) = a$
By definition the solution of $-a + x = 0_R$ will be $-(-a)$
Prove a is a solution of $-a + x = 0_R$
$-a + a = 0_R \Rightarrow a = -(-a)$
(4) $-(a+b) = (-a) + (-b)$
By definition $-(a+b)$ is a solution $(a+b) + x = 0_R$
Prove $(-a) + (-b)$ is a solution of $(a+b) + x = 0_R$
$(a+b) + (-a) + (-b) = 0_R \Rightarrow$ by commutative $0_R = 0_R \Rightarrow (-a) + (-b) = -(a+b)$
(5) $-(a-b) = (-a) + b$
Some reasoning to solve this.
Similar for (6) and (7).

Definition

For all $a \in R$
$a^n = a \cdot a \cdot a \ldots$ with n factors
$a^{m+n} = a^m \cdot a^n$
$(a^m)^n = a^{nm}$

Example. Let R be a ring $a, b \in R$
then $(a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2$
ab, ba not required to be the same.

In homework
If $x^2 = x$ for any $x \in R$ R is commutative
$x + y = (x+y)^2 = x^2 + xy + yx = y^2$
$x + y = x + xy + yx + y$ So $0 = xy + yx$
Must prove $xy = yx$

$(x + x^2) = (2x)^2 = 2x$ So $4x^2 = 2x \Rightarrow 2x = 0$
So $xy + yx - 2yx = 0$

Day 14

Quiz Day
Turn in Homework

Going over assignment

Problem 42

Prove that a finite ring with 1_R has characteristic n.
$n1_R = 0$ $na = 0$ for all $a \in R$
$\Rightarrow n1_R a = a \cdot 0 = 0$
$a_1, a_2, \cdot a_n \in R$
Assume $a_i + a_i + \cdot a_i = na_i \in R$
Show distinct : $n_1 a_i = n_2 a_i \Rightarrow (n_2 - n_1)a_i = 0$
$n_1 a_i \neq n_2 a_i$ if $n_1 \neq n_2$
Since R finite, there must be an n where $na_i = 0$ and closure under addition.

Student way

$1_R + 1_R \in R$; $1_R + 1_R \ldots 1_R = n \cdot 1_R$
There exists $n \cdot 1_K = n_2 \cdot 1_R$ and there exists $n_1 \neq n_2$ if not infinitely many.

This Time

Theorem 3.6

Let S be a nonempty subset of a ring such that:
(1) S is closed under subtraction: $a, b \in S \to a - b \in S$
(2) S is closed under multiplication: $a, b \in S \Rightarrow ab \in S$
Then S is a subring of R
where $a - b = a + (_b)$ as the unique solution of $b + x = 0$

Proof

By subring theorem $(3 \cdot 2?)$ check:
(1) close under addition
(2) close under multiplication
(3) 0 exists
(4) $a + x = 0$ has a solution

why this is true

by (1) : $a, b \in S \Rightarrow a - b \in S$
So $a - a \in S \Rightarrow 0 \in S$ (3)
If $0 \in S, a \in S \Rightarrow a - 0 \in S$ (4)
$b \in S, -a \in S \Rightarrow b - (-a) \in S \Rightarrow b + a \in S$ (1)

Units and Zero Divisors:

Definition:
An element $a \in R$ (ring) with 1_R called a unit if there exists $u \in R$ where $au = 1_R = ua$
[in this case] u is a multiplication inverse of a and is denoted a^{-1}

Example. 1
units in $\mathbb{Z}$ are?
1 and -1

Example. 2
Units in $\mathbb{Z}_{15}$ are?
$1, 2, 4, 7, 8, 11, 13, 14$
If a is a unit in $\mathbb{Z}_{15} \iff (a, n) = 1$
All others are the zero elements

Definition
An element in ring R is a zero divisor if:
(1) $a \neq 0_R$
(2) there exists a non zero $c \in R$ where $ac = 0$ or $ca = 0$

Example. 1
in $\mathbb{Z}_{15}$:
$3, 5, 6, 9, 10, 12$ are zero divisors

Example. 2
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(\mathbb{R})$$
If $ad - bc \neq 0$ unit
otherwise a 0 divisor.

End of Week 5!