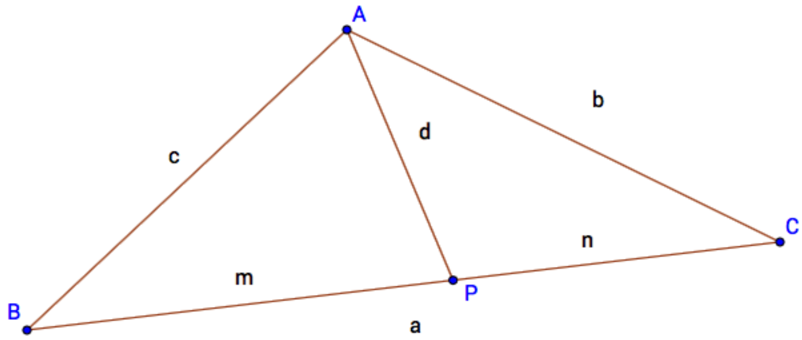
Lecture 2

Stewart's Theorem Let ABC be a triangle with $AB = c$, $AC = b$ and $BC = a$. If P is a point on BC with $BP = m$, $PC = n$ and $AP = d$, then $dad + man = bmb + cnc$.



Proof. **Proof A**

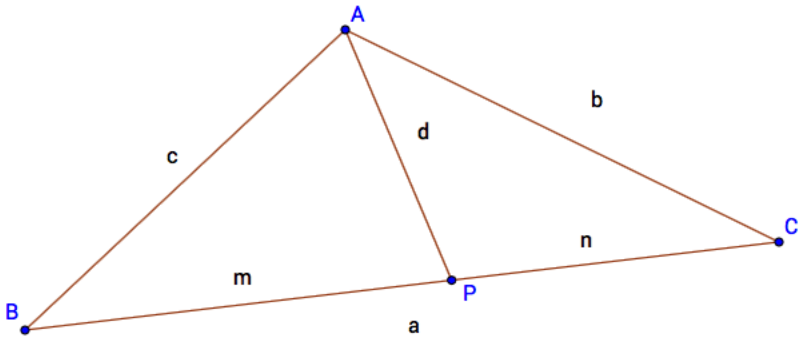
$$c^2 = m^2 + d^2 - 2md\cos\theta$$
$$b^2 = n^2 + d^2 - 2nd\cos\theta'$$
$$b^2 = n^2 + d^2 + 2nd\cos\theta$$
$$\frac{m^2 - c^2 + d^2}{-2md} = \frac{b^2 - n^2 - d^2}{2nd}$$
$$nc^2 - nm^2 - nd^2 = -mb^2 + mn^2 + md^2$$
$$nc^2 - mb^2 = mn^2 + md^2 + nm^2 + nd^2$$
$$cnc + bmb = nm(n + m) + d^2(m + n)$$
$$cnc + bmb = man + dad$$

∎

Note: Unclear what θ and θ' are. No explanation. Division by variables should be careful about 0.

Handout or Document Camera or Class Exercise

Stewart's Theorem Let ABC be a triangle with $AB = c$, $AC = b$ and $BC = a$. If P is a point on BC with $BP = m$, $PC = n$ and $AP = d$, then $dad + man = bmb + cnc$.



Proof. **Proof B**

The Cosine Law on $\triangle APB$ tells us that

$$c^2 = m^2 + d^2 - 2md\cos(\angle APB).$$

Subtracting c^2 from both sides gives

$$0 = -c^2 + m^2 + d^2 - 2md\cos(\angle APB).$$

Adding $2md\cos\angle APB$ to both sides gives

$$2md\cos(\angle APB) = -c^2 + m^2 + d^2.$$

Dividing both sides by $2md$ gives

$$\cos(\angle APB) = \frac{-c^2 + m^2 + d^2}{2md}.$$

Now, the Cosine Law on $\triangle APC$ tells us that

$$b^2 = n^2 + d^2 - 2nd\cos\angle APC.$$

Since $\angle APC$ and $\angle APB$ are supplementary angles, then

$$\cos\angle APC = \cos(\pi - \angle APB) = -\cos(\angle APB).$$

Substituting into our previous equation, we see that

$$b^2 = n^2 + d^2 + 2nd\cos\angle APB.$$

Subtracting n^2 from both sides gives

$$b^2 - n^2 = d^2 + 2nd\cos(\angle APB).$$

Then subtracting d^2 from both sides gives

$$b^2 - n^2 - d^2 = 2nd\cos(\angle APB).$$

Dividing both sides by $2nd$ gives

$$\frac{b^2 - n^2 - d^2}{2nd} = \cos(\angle APB).$$

Now we have two expressions for $\cos(\angle APB)$ and equate them to yield

$$\frac{-c^2 + m^2 + d^2}{2md} = \frac{b^2 - n^2 - d^2}{2nd}.$$

Multiplying both sides by $2mnd$ shows us that

$$n(-c^2 + m^2 + d^2) = m(b^2 - n^2 - d^2).$$

Next we distribute to get

$$-nc^2 + nm^2 + nd^2 = mb^2 - mn^2 - md^2.$$

Adding $nc^2 + mn^2 + md^2$ to both sides gives

$$nm^2 + mn^2 + nd^2 + md^2 = mb^2 + nc^2.$$

Factoring twice gives:

$$nm(m + n) + d^2(m + n) = mb^2 + nc^2.$$

Since P lies on BC, then $a = m + n$ so we substitute to yield

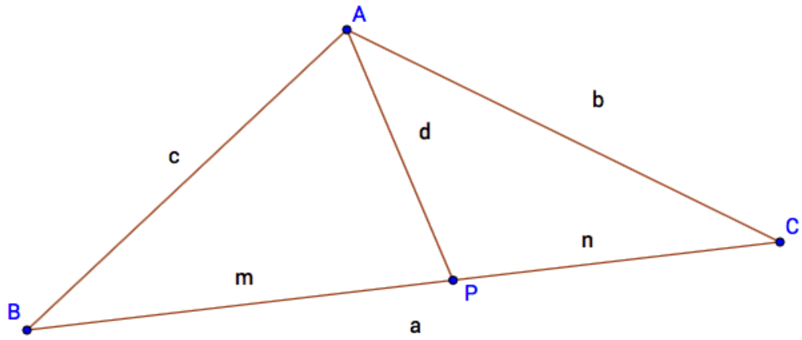
$$nma + d^2a = mb^2 + nc^2.$$

Finally, we can rewrite this as $bmb + cnc = dad + man$.. ■

Note: Too verbose. Can shorten the explanation by not writing out every algebraic manipulation.

Handout or Document Camera or Class Exercise

Stewart's Theorem Let ABC be a triangle with $AB = c$, $AC = b$ and $BC = a$. If P is a point on BC with $BP = m$, $PC = n$ and $AP = d$, then $dad + man = bmb + cnc$.



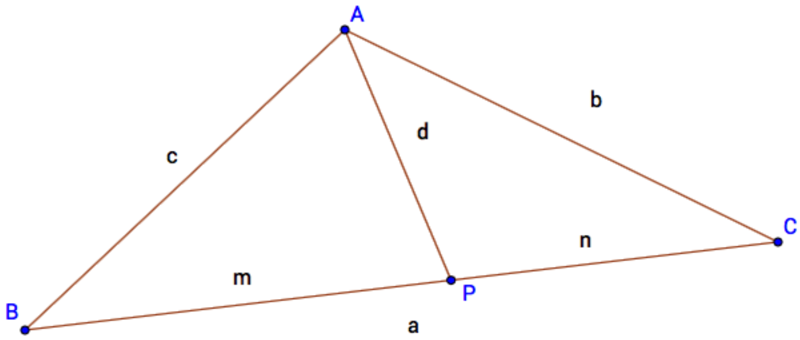
Proof. **Proof C**

Using the Cosine Law for supplementary angles $\angle APB$ and $\angle APC$, and then clearing denominators and simplifying gives $dad + man = bmb + cnc$ as required. ∎

Note: No details given. Need to provide some evidence of algebraic manipulation.

Handout or Document Camera or Class Exercise

Stewart's Theorem Let ABC be a triangle with $AB = c$, $AC = b$ and $BC = a$. If P is a point on BC with $BP = m$, $PC = n$ and $AP = d$, then $dad + man = bmb + cnc$.



Proof. **Proof D**

The Cosine Law on $\triangle APB$ tells us that

$$c^2 = m^2 + d^2 - 2md \cos \angle APB.$$

Similarly, the Cosine Law on $\triangle APC$ tells us that

$$b^2 = n^2 + d^2 - 2nd \cos \angle APC.$$

Since $\angle APC$ and $\angle APB$ are supplementary angles, we have

$$b^2 = n^2 + d^2 + 2nd \cos \angle APB.$$

Equating expressions for $\cos \angle APB$ yields

$$\frac{-c^2 + m^2 + d^2}{2md} = \frac{b^2 - n^2 - d^2}{2nd}.$$

Clearing the denominator and rearranging gives

$$nm^2 + mn^2 + nd^2 + md^2 = mb^2 + nc^2.$$

Factoring yields

$$mn(m + n) + d^2(m + n) = mb^2 + nc^2.$$

Substituting $a = (m + n)$ gives $dad + man = bmb + cnc$ as required. ∎

Note: Overall a good proof. Perhaps some more information on why the supplementary angle step holds would be good. Justifying why division by a variable is allowed (that is, nonzero variables) would be a plus and perhaps labeling previous equations to reference in the future would help this proof slightly. This would be an acceptable answer regardless of these minor quibbles.

Handout or Document Camera or Class Exercise

Find the flaw in the following arguments:

(i) For $a, b \in \mathbb{R}$,

$$\begin{aligned} a &= b \\ a^2 &= ab \\ a^2 - b^2 &= ab - b^2 \\ (a-b)(a+b) &= b(a-b) \\ a+b &= b && \text{ERROR: division by 0 since } a = b \\ b+b &= b \\ 2b &= b \\ 2 &= 1 \end{aligned}$$

(ii)

$$\begin{aligned} x &= \frac{\pi+3}{2} \\ 2x &= \pi + 3 \\ 2x(\pi - 3) &= (\pi+3)(\pi-3) \\ 2\pi x - 6x &= \pi^2 - 9 \\ 9 - 6x &= \pi^2 - 2\pi x \\ 9 - 6x + x^2 &= \pi^2 - 2\pi x + x^2 \\ (3-x)^2 &= (\pi - x)^2 \\ 3 - x &= \pi - x \\ 3 &= \pi \end{aligned}$$

(iii) For $x \in \mathbb{R}$,

$$\begin{aligned} (x-1)^2 &\geq 0 \\ x^2 - 2x + 1 &\geq 0 \\ x^2 + 1 &\geq 2x \\ x + \tfrac{1}{x} &\geq 2 \end{aligned}$$

Lecture 3

Find the flaw in the following arguments:

(i) (Last class)

(ii)

$$\begin{aligned}
x &= \frac{\pi+3}{2} \\
2x &= \pi + 3 \\
2x(\pi-3) &= (\pi+3)(\pi-3) \\
2\pi x - 6x &= \pi^2 - 9 \\
9 - 6x &= \pi^2 - 2\pi x \\
9 - 6x + x^2 &= \pi^2 - 2\pi x + x^2 \\
(3-x)^2 &= (\pi - x)^2 \\
3 - x &= \pi - x \qquad \text{ERROR: } |3-x| = |\pi - x| \\
3 &= \pi
\end{aligned}$$

(iii) For $x \in \mathbb{R}$,

$$\begin{aligned}
(x-1)^2 &\geq 0 \\
x^2 - 2x + 1 &\geq 0 \\
x^2 + 1 &\geq 2x \\
x + \tfrac{1}{x} &\geq 2 \qquad \text{ERROR: Division by 0. Also flip sign if } x < 0
\end{aligned}$$

Example: Let $x, y \in \mathbb{R}$. Prove that

$$5x^2y - 3y^2 \leq x^4 + x^2y + y^2$$

Proof: Since $0 \leq (x^2 - 2y)^2$, we have

$$\begin{aligned} 0 &\leq (x^2 - 2y)^2 \\ 0 &\leq x^4 - 4x^2y + 4y^2 \\ 5x^2y - 3y^2 &\leq x^4 - 4x^2y + 4y^2 + 5x^2y - 3y^2 \\ 5x^2y - 3y^2 &\leq x^4 + x^2y + y^2 \end{aligned}$$

Alternate proof:

$$\begin{aligned} \text{RHS} &= x^4 + x^2y + y^2 \\ &= x^4 + x^2y + y^2 + 5x^2y - 5x^2y + 3y^2 - 3y^2 \\ &= x^4 - 4x^2y + 4y^2 + 5x^2y - 3y^2 \\ &= (x^2 - 2y)^2 + 5x^2y - 3y^2 \\ &\geq 5x^2y - 3y^2 \\ &= \text{LHS} \end{aligned}$$

Note: To discover this proof. Play around with the given inequality on a napkin (rough work). Manipulate it until you reach a true statement. Then write your proof starting with the given true statement to reach the desired inequality. Notice that starting with the given inequality is NOT valid since you do not know whether or not it is true to begin with. New truth can only be derived from old truth. (Analogy: You need a solid foundation to build a house). Here is a sample of my napkin work:

$$\begin{aligned} 5x^2y - 3y^2 &\leq x^4 + x^2y + y^2 \\ 0 &\leq x^4 + x^2y + y^2 - 5x^2y + 3y^2 \\ 0 &\leq x^4 - 4x^2y + 4y^2 \\ 0 &\leq (x^2 - 2y)^2. \end{aligned}$$

The last statement is clearly true thus so long as I can reverse my steps, I have a valid proof. Note that you must write the proof starting with the true statement and deriving the new truth statements.

Throughout the remainder of this lecture, let A, B, C be statements.

Definition: $\neg A$ is NOT A.

A	$\neg A$
T	F
F	T

Note: : Truth tables can be used both as definitions of operators (as was done here) or in proofs (as will be done later). Make sure you understand the difference.

Definition: $A \wedge B$ is A and B. Further, $A \vee B$ is A or B.

A	B	$A \wedge B$	$A \vee B$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

Handout or Document Camera or Class Exercise

Which of the following are true?

- π is irrational and $3 > 2$
- 10 is even and $1 = 2$
- 7 is larger than 6 or 15 is a multiple of 3
- $5 \leq 6$
- 24 is a perfect square or the vertex of parabola $x^2 + 2x + 3$ is $(1, 1)$
- 2.3 is not an integer
- 20% of 50 is not 10
- 7 is odd or 1 is positive and $2 \neq 2$

Lecture 3

In the following, identify the hypothesis, the conclusion and state whether the statement is true or false.

- If $\sqrt{2}$ is rational then $2 < 3$
- If (1+1=2) then $5 \cdot 2 = 11$
- If C is a circle, then the area of C is πr^2
- If 5 is even then 5 is odd
- If $4 - 3 = 2$ then $1 + 1 = 3$

Lecture 4

Suppose A, B and C are all true statements.
The compound statement $(\neg A) \vee (B \wedge \neg C)$ is

A) True

B) False

Lecture 5

Prove the following. Suppose that $x, y \geq 0$. Show that $x = y$ if and only if $\frac{x+y}{2} = \sqrt{xy}$.

Lecture 6

Describe the following sets using set-builder notation:

(i) Set of even numbers between 5 and 14 (inclusive).

(ii) All odd perfect squares.

(iii) Sets of three integers which are the side lengths of a (non-trivial) triangle.

(iv) All points on a circle of radius 8 centred at the origin.

Lecture 7

Example: Prove that there is an $x \in \mathbb{R}$ such that $\frac{x^2+3x-3}{2x+3} = 1$.

Lecture 7

Example: Show that for each $x \in \mathbb{R}$, we have that $x^2 + 4x + 7 > 0$.

Lecture 7

Sometimes $\forall$ and $\exists$ are hidden! If you encounter a statement with quantifiers, take a moment to make sure you understand what the question is saying/asking.

Examples:

(i) $2n^2 + 11n + 15$ is never prime when n is a natural number.

(ii) If n is a natural number, then $2n^2 + 11n + 15$ is composite.

(iii) $\frac{m-7}{2m+4} = 5$ for some integer m.

(iv) $\frac{m-7}{2m+4} = 5$ has an integer solution.

Lecture 8

Consider the following statement.

$$\{2k : k \in \mathbb{N}\} \supseteq \{n \in \mathbb{Z} : 8 \mid (n+4)\}$$

A well written and correct direct proof of this statement could begin with

A) We will show that the statement is true in both directions.

B) Assume that $8 \mid 2n$ where n is an integer.

C) Let $m \in \{n \in \mathbb{Z} : 8 \mid (n+4)\}$.

D) Let $m \in \{2k : k \in \mathbb{N}\}$.

E) Assume that $8 \mid (2k+4)$.

Lecture 8

Notes:

(i) A single counter example proves that $(\forall x \in S, P(x))$ is false.

Claim: Every positive even integer is composite.

This claim is false since 2 is even but 2 is prime.

(ii) A single example does not prove that $(\forall x \in S, P(x))$ is true.

Claim: Every even integer at least 4 is composite.

This is true but we cannot prove it by saying "6 is an even integer and is composite." We must show this is true for an arbitrary even integer x. (Idea: $2 \mid x$ so there exists a $k \in \mathbb{N}$ such that $2k = x$ and $k \neq 1$.)

(iii) A single example does show that $(\exists x \in S, P(x))$ is true.

Claim: Some even integer is prime.

This claim is true since 2 is even and 2 is prime.

(iv) What about showing that $(\exists x \in S, P(x))$ is false?

Idea: $(\exists x \in S, P(x))$ is false $\equiv \forall x \in S, \neg P(x)$ is true. This idea is central for proof by contradiction which we will see later.

Lecture 8

Which of the following are true?

(i) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$

(ii) $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$

(iii) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$

(iv) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$

Lecture 8

List all elements of the set:

$$\{n \ \in \mathbb{Z} : n > 1 \wedge ((m \in \mathbb{Z} \wedge m > 0 \wedge m \mid n) \Rightarrow (m = 1 \vee m = n))\} \cap \{n \in \mathbb{Z} : n \mid 42\}$$

Lecture 9

Rewrite the following using as few English words as possible.

(i) No multiple of 15 plus any multiple of 6 equals 100.

(ii) Whenever three divides both the sum and difference of two integers, it also divides each of these integers.

Lecture 9

Write the following statements in (mostly) plain English.

(i) $\forall m \in \mathbb{Z}, ((\exists k \in \mathbb{Z}, m = 2k) \Rightarrow (\exists \ell \in \mathbb{Z}, 7m^2 + 4 = 2\ell))$

(ii) $n \in \mathbb{Z} \Rightarrow (\exists m \in \mathbb{Z}, m > n)$

Lecture 10

Example: Prove that if $x \in \mathbb{R}$ is such that $x^3 + 7x^2 < 9$, then $x < 1.1$.

Lecture 10

How many years has it been since the Toronto Maple Leafs have won the Stanley Cup?

A) -3

B) 49

C) 1000000

D) 1500

Lecture 10

Example: Let $n \in \mathbb{Z}$ such that n^2 is even. Show that n is even.

Direct Proof: As n^2 is even, there exists a $k \in \mathbb{Z}$ such that

$$n \cdot n = n^2 = 2k.$$

Since the product of two integers is even if and only if at least one of the integers is even, we conclude that n is even.

Proof By Contradiction: Suppose that n^2 is even. Assume towards a contradiction that n is odd. Then there exists a $k \in \mathbb{Z}$ such that $n = 2k + 1$. Now,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Hence, n^2 is odd, a contradiction since we assumed in the statement that n^2 is even. Thus n is even.

Lecture 10

Example: Prove that $\sqrt{2}$ is irrational.

Proof: Assume towards a contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{N}$ (Think: Why is it okay to use $\mathbb{N}$ instead of $\mathbb{Z}$?).

Proof 1: Assume further that a and b share no common factor (otherwise simplify the fraction first). Then $2b^2 = a^2$. Hence a is even. Write $a = 2k$ for some integer k. Then $2b^2 = a^2 = (2k)^2 = 4k^2$ and canceling a 2 shows that $b^2 = 2k^2$. Thus b^2 is even and hence b is even. This implies that a and b share a common factor, a contradiction.

Proof 2 (Well Ordering Principle): Let

$$S = \{n \in \mathbb{N} : n\sqrt{2} \in \mathbb{N}\}.$$

Since $b \in S$, we have that S is nonempty. By the Well Ordering Principle, there must be a least element of S, say k. Now, notice that

$$k(\sqrt{2} - 1) = k\sqrt{2} - k \in \mathbb{N}$$

(positive since $\sqrt{2} > \sqrt{1} = 1$). Further,

$$k(\sqrt{2} - 1)\sqrt{2} = 2k - k\sqrt{2} \in \mathbb{N}$$

and so $k(\sqrt{2} - 1) \in S$. However, $k(\sqrt{2} - 1) < k$ which contradicts the definition of k. Thus, $\sqrt{2}$ is not rational.

Proof 3 (Infinite Descent): Isolating from $\sqrt{2} = \frac{a}{b}$, we see that $2b^2 = a^2$. Thus a^2 is even hence a is even. Write $a = 2k$ for some integer k. Then $2b^2 = a^2 = (2k)^2 = 4k^2$. Hence $b^2 = 2k^2$ and so b is even. Write $b = 2\ell$ for some integer ℓ. Then repeating the same argument shows that k is even. So $a = 2k = 4m$ for some integer m. Since we can repeat this argument indefinitely and no integer has infinitely many factors of 2, we will (eventually) reach a contradiction. Thus, $\sqrt{2}$ is not rational.

Lecture 11

Let $f(x)$ be the function defined by

$$\begin{aligned} f : (0, \infty) &\to (0, \infty) \\ x &\mapsto x^2. \end{aligned}$$

Prove for all $y \in (0, \infty)$ there exists a unique $x \in (0, \infty)$ such that $f(x) = y$

Lecture 11

Theorem: (Division Algorithm) Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then $\exists! q, r \in \mathbb{Z}$ such that $a = bq + r$ where $0 \leq r < b$.

Proof: Existence: Use the Well Ordering Principle on the set

$$S = \{a - bq : a - bq \geq 0 \wedge q \in \mathbb{Z}\}$$

Uniqueness:

Suppose that $a = q_1 b + r_1$ with $0 \leq r_1 < b$. Also, suppose that $a = q_2 b + r_2$ with $0 \leq r_2 < b$ and $r_1 \neq r_2$. Without loss of generality, we can assume $r_1 < r_2$.

Then $0 < r_2 - r_1 < b$ and $(q_1 - q_2)b = r_2 - r_1$.

Hence $b \mid (r_2 - r_1)$. By Bounds By Divisibility, $b \leq r_2 - r_1$ which contradicts the fact that $r_2 - r_1 < b$.

Therefore, the assumption that $r_1 \neq r_2$ is false and in fact $r_1 = r_2$. But then $(q_1 - q_2)b = r_2 - r_1$ implies $q_1 = q_2$.

Lecture 12

Let $n \in \mathbb{Z}$. Consider the following implication.

If $(\forall x \in \mathbb{R},\ x \leq 0\ \vee\ x+1 > n)$, then $n = 1$.

The contrapositive of this implication is

A) If $n = 1$, then $(\forall x \in \mathbb{R},\ x \leq 0\ \vee\ x+1 > n)$.

B) If $n = 1$, then $(\exists x \in \mathbb{R},\ x > 0\ \wedge\ x+1 \leq n)$.

C) If $n \neq 1$, then $(\exists x \in \mathbb{R},\ x \geq 0\ \wedge\ x+1 < n)$.

D) If $n \neq 1$, then $(\forall x \in \mathbb{R},\ x \leq 0\ \vee\ x+1 > n)$.

E) None of the above.

Lecture 12

Try some of the following problems:

- $\min\{a,b\} \leq \frac{a+b}{2}$ for all real numbers a and b.
- Let x be real. Then $x^2 - x > 0$ if and only if $x \notin [0,1]$.
- If r is irrational, then $\frac{1}{r}$ is irrational.
- There do not exist integers p and q satisfying $p^2 - q^2 = 10$.
- The complete real solution to $x^2 + y^2 - 2y = -1$ is $(x,y) = (0,1)$.
- Let S and T be sets with respect to a universe U. Prove that $\overline{S \cap T} \subseteq \overline{S} \cup \overline{T}$.
- Let $a, b, c \in \mathbb{Z}$. Prove that if $a \nmid b$ and $a \mid (b+c)$, then $a \nmid c$.

Lecture 13

Prove that

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

holds for all natural numbers n.

Lecture 13

Examine the following induction "proofs". Find the mistake

Question: For all $n \in \mathbb{N}$, $n > n + 1$.

Proof: Let $P(n)$ be the statement: $n > n + 1$. Assume that $P(k)$ is true for some integer $k \geq 1$. That is, $k > k + 1$ for some integer $k \geq 1$. We must show that $P(k + 1)$ is true, that is, $k + 1 > k + 2$. But this follows immediately by adding one to both sides of $k > k + 1$. Since the result is true for $n = k + 1$, it holds for all n by the Principle of Mathematical Induction.

Question: All horses have the same colour. (Cohen 1961).

Proof:

Base Case: If there is only one horse, there is only one colour.

Inductive hypothesis and step: Assume the induction hypothesis that within any set of n horses for any $n \in \mathbb{N}$, there is only one colour. Now look at any set of $n + 1$ horses. Number them: $1, 2, 3, ..., n, n + 1$. Consider the sets $\{1, 2, 3, ..., n\}$ and $\{2, 3, 4, ..., n + 1\}$. Each is a set of only n horses, therefore by the induction hypothesis, there is only one colour. But the two sets overlap, so there must be only one colour among all $n + 1$ horses.

Lecture 14

Prove $P(n) : 6 \mid (2n^3 + 3n^2 + n)$ holds $\forall n \in \mathbb{N}$.

Lecture 14

Let $\{x_n\}$ be a sequence defined by $x_1 = 4$, $x_2 = 68$ and

$$x_m = 2x_{m-1} + 15x_{m-2} \qquad \text{for all } m \geq 3$$

Prove that $x_n = 2(-3)^n + 10 \cdot 5^{n-1}$ for $n \geq 1$.

Solution: We proceed by induction.

Base Case: For $n = 1$, we have

$$x_1 = 4 = 2(-3)^1 + 10 \cdot 5^0 = 2(-3)^n + 10 \cdot 5^{n-1}.$$

Inductive Hypothesis: Assume that

$$x_k = 2(-3)^k + 10 \cdot 5^{k-1}$$

is true for some $k \in \mathbb{N}$.

Inductive Step: Now, for $k + 1$,

$$\begin{aligned} x_{k+1} &= 2x_k + 15x_{k-1} && \text{Only true if } k \geq 2!!! \\ &= 2(2(-3)^k + 10 \cdot 5^{k-1}) + 15x_{k-1} \\ &= 4(-3)^k + 20 \cdot 5^{k-1} + 15x_{k-1} \\ &= ...? \end{aligned}$$

Lecture 14

Suppose $x_1 = 3$, $x_2 = 5$ and for all $m \geq 3$,

$$x_m = 3x_{m-1} + 2x_{m-2}.$$

Prove that $x_n < 4^n$ for all $n \in \mathbb{N}$.

Lecture 15

Fibonacci Sequence Definition: Define a sequence by $f_1 = 1$, $f_2 = 1$ and

$$f_n = f_{n-1} + f_{n-2} \qquad \text{For all } n \geq 3$$

so $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, and so on.

(i) Prove that $\displaystyle\sum_{r=1}^{n} f_r^2 = f_n f_{n+1}$ for all $n \in \mathbb{N}$.

(ii) Prove that $f_n < \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{N}$.

Lecture 16

A statement $P(n)$ is proved true for all $n \in \mathbb{N}$ by induction.

In this proof, for some natural number k, we might:

A) Prove $P(1)$. Prove $P(k)$. Prove $P(k+1)$.

B) Assume $P(1)$. Prove $P(k)$. Prove $P(k+1)$.

C) Prove $P(1)$. Assume $P(k)$. Prove $P(k+1)$.

D) Prove $P(1)$. Assume $P(k)$. Assume $P(k+1)$.

E) Assume $P(1)$. Prove $P(k)$. Assume $P(k+1)$.

Lecture 17

Example: Prove that $\gcd(3a + b, a) = \gcd(a, b)$ using the definition directly.

Lecture 18

Prove that $\gcd(3s + t, s) = \gcd(s, t)$ using GCDWR.

Lecture 18

Use the Euclidean Algorithm to compute $\gcd(120, 84)$ and then use back substitution to find integers x and y such that $\gcd(120, 84) = 120x + 84y$.

Lecture 19

Prove or disprove the following:

(i) If $n \in \mathbb{N}$ then $\gcd(n, n+1) = 1$.

(ii) Let $a, b, c \in \mathbb{Z}$. If $\exists\ x, y \in \mathbb{Z}$ such that $ax^2 + by^2 = c$ then $\gcd(a, b) \mid c$.

(iii) Let $a, b, c \in \mathbb{Z}$. If $\gcd(a, b) \mid c$ then $\exists\ x, y \in \mathbb{Z}$ such that $ax^2 + by^2 = c$.

Lecture 20

Which of the following statements is false?

A) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \leq b \ \wedge \ \gcd(a,b) \leq a)$

B) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \neq 0 \implies (a \neq 0) \ \vee \ (b \neq 0))$

C) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \mid a \ \wedge \ \gcd(a,b) \mid b)$

D) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (((c \mid a) \ \wedge \ (c \mid b)) \ \wedge \ \gcd(a,b) \neq 0 \implies c \leq \gcd(a,b))$

E) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \gcd(a,b) \geq 0$

Lecture 20

Example: Let $a, b, c \in \mathbb{Z}$. Prove if $\gcd(ab, c) = 1$ then $\gcd(a, c) = \gcd(b, c) = 1$.

Example: State the converse of the previous statement and prove or disprove.

Lecture 21

Use the Extended Euclidean Algorithm to find integers x and y such that $408x + 170y = \gcd(408, 170)$.

Lecture 21

Use the Extended Euclidean Algorithm to find integers x and y such that $399x - 2145y = \gcd(399, -2145)$.

Lecture 22

How many multiples of 12 are positive divisors of 2940? What are they?

Lecture 23

Find $x, y \in \mathbb{Z}$ such that $143x + 253y = \gcd(143, 253)$.
Determine which of the following equations are solvable for integers x and y:

(i) $143x + 253y = 11$

(ii) $143x + 253y = 155$

(iii) $143x + 253y = 154$

Lecture 24

Let $a, b, x, y \in \mathbb{Z}$.

Which one of the following statements is true?

A) If $ax + by = 6$, then $\gcd(a, b) = 6$.

B) If $\gcd(a, b) = 6$, then $ax + by = 6$.

C) If $a = 12b + 18$, then $\gcd(a, b) = 6$.

D) If $ax + by = 1$, then $\gcd(6a, 6b) = 6$.

E) If $\gcd(a, b) = 3$ and $\gcd(x, y) = 2$, then $\gcd(ax, by) = 6$.

Lecture 24

Find all non-negative integer solutions to $15x - 24y = 9$ where $x \leq 20$ and $y \leq 20$.

Lecture 25

Congruence is an Equivalence Relation (CER)
Let $n \in \mathbb{N}$. Let $a, b, c \in \mathbb{Z}$. Then

(i) (Reflexivity) $a \equiv a \pmod{n}$.

(ii) (Symmetry) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.

(iii) (Transitivity) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Lecture 25

Properties of Congruence (PC) Let $a, a', b, b' \in \mathbb{Z}$. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then

(i) $a + b \equiv a' + b' \pmod{m}$

(ii) $a - b \equiv a' - b' \pmod{m}$

(iii) $ab \equiv a'b' \pmod{m}$

Lecture 27

What is the last digit of $5^{32}3^{10} + 9^{22}$?

Lecture 27

Solve $9x \equiv 6 \pmod{15}$.

Lecture 28

Which of the following satisfies $x \equiv 40 \pmod{17}$?

(Do not use a calculator.)

A) $x = 173$

B) $x = 15^5 + 19^3 - 4$

C) $x = 5 \cdot 18^{100}$

D) $x = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

E) $x = 17^0 + 17^1 + 17^2 + 17^3 + 17^4 + 17^5 + 17^6$

Lecture 29

Solve the following equations in $\mathbb{Z}_{14}$. Express answers as $[x]$ where $0 \leq x < 14$.

i) $[75] - [x] = [50]$

ii) $[10][x] = [1]$

iii) $[10][x] = [2]$

Hint: Rewrite these using congruences.

Lecture 29

Find the additive and multiplicative inverses of $[7]$ in $\mathbb{Z}_{11}$. Give your answers in the form $[x]$ where $0 \leq x \leq 10$.

Lecture 29

The following are equivalent [TFAE]

- $a \equiv b \pmod{m}$
- $m \mid (a - b)$
- $\exists k \in \mathbb{Z}, a - b = km$
- $\exists k \in \mathbb{Z}, a = km + b$
- a and b have the same remainder when divided by m
- $[a] = [b]$ in $\mathbb{Z}_m$.

Theorem: [LCT 2] Let $a, c \in \mathbb{Z}$ and let $m \in \mathbb{N}$. Let $\gcd(a, m) = d$. The equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$. Moreover, if $[x] = [x_0]$ is one particular solution, then the complete solution is

$$\big\{[x_0], [x_0 + \tfrac{m}{d}], [x_0 + 2\tfrac{m}{d}], \ldots, [x_0 + (d-1)\tfrac{m}{d}]\big\}$$

Lecture 30

Find the remainder when 7^{92} is divided by 11.

Lecture 30

Let p be a prime. Prove that if $p \nmid a$ and $r \equiv s \pmod{(p-1)}$, then $a^r \equiv a^s \pmod{p}$ for any $r, s \in \mathbb{Z}$.

Lecture 31

Theorem: [Chinese Remainder Theorem (CRT) If
$\gcd(m_1, m_2) = 1$, then for any choice of integers a_1 and a_2, there exists a solution to the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

Moreover, if $n = n_0$ is one integer solution, then the complete solution is $n \equiv n_0 \pmod{m_1 m_2}$.

Theorem: (Generalized CRT (GCRT)) If $m_1, m_2, \ldots, m_k$ are integers and $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, then for any choice of integers $a_1, a_2, \ldots, a_k$, there exists a solution to the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

Moreover, if $n = n_0$ is one integer solution, then the complete solution is

$$n \equiv n_0 \pmod{m_1 m_2 \ldots m_k}$$

Lecture 32

Which of the following is equal to $[53]^{242} + [5]^{-1}$ in $\mathbb{Z}_7$?

(Do not use a calculator.)

A) $[5]$

B) $[4]$

C) $[3]$

D) $[2]$

E) $[1]$

Lecture 32

For what integers is $x^5 + x^3 + 2x^2 + 1$ divisible by 6?

Lecture 32

(i) Show that $x = 2^{129}$ solves $2x \equiv 1 \pmod{131}$.

(ii) Use the square and multiply algorithm to find the remainder when 2^{129} is divided by 131.

(iii) Solve $2x \equiv 3 \pmod{131}$ for $0 \leq x \leq 130$.

Lecture 33

Let $p = 2$, $q = 11$ and $e = 3$

(i) Compute n, $\phi(n)$ and d.

(ii) Compute $C \equiv M^e \pmod{n}$ when $M = 8$ (reduce to least nonnegative C).

(iii) Compute $R \equiv C^d \pmod{n}$ when $C = 6$ (reduce to least nonnegative R).

Lecture 34

Express the following in standard form

(i) $z = \frac{(1-2i)-(3+4i)}{5-6i}$

(ii) $w = i^{2015}$

Lecture 35

Solve $z^2 = i\bar{z}$ for $z \in \mathbb{C}$

Lecture 35

Find a real solution to

$$6z^3 + (1 + 3\sqrt{2}i)z^2 - (11 - 2\sqrt{2}i)z - 6 = 0$$

Lecture 35

Prove the following for $z \in \mathbb{C}$

(i) $z \in \mathbb{R}$ if and only if $z = \bar{z}$.

(ii) z is purely imaginary if and only if $z = -\bar{z}$.

Lecture 36

Let $[x]$ be the inverse of $[241]$ in $\mathbb{Z}_{1001}$, if it exists, where $0 \leq x < 1001$. Determine the sum of the digits of x.

A) 7

B) 9

C) 11

D) 12

E) $[x]$ does not exist

Lecture 36

How many integers x satisfy all of the following three conditions?

$$x \equiv 6 \pmod{13}$$
$$4x \equiv 3 \pmod{7}$$
$$-1000 < x < 1000$$

A) 1

B) 7

C) 13

D) 22

E) 91

Lecture 36

To prove $|z+w| \leq |z| + |w|$, it suffices to prove that

$$|z+w|^2 \leq (|z|+|w|)^2 = |z|^2 + 2|zw| + |w|^2$$

since the modulus is a positive real number. Using the Properties of Modulus and the Properties of Conjugates, we have

$$\begin{aligned}
|z+w|^2 &= (z+w)(\overline{z+w}) && \text{PM} \\
&= (z+w)(\bar{z}+\bar{w}) && \text{PCJ} \\
&= z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} \\
&= |z|^2 + z\bar{w} + \overline{z\bar{w}} + |w|^2 && \text{PCJ and PM}
\end{aligned}$$

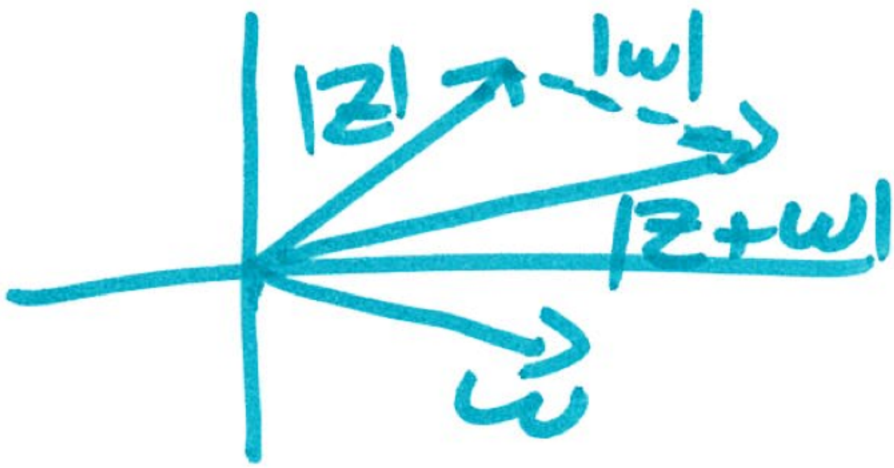
Now, from Properties of Conjugates, we have that

$$z\bar{w} + \overline{z\bar{w}} = 2\Re(z\bar{w}) \leq 2|z\bar{w}| = 2|zw|$$

and hence

$$|z+w|^2 = |z|^2 + z\bar{w} + \overline{z\bar{w}} + |w|^2 \leq |z|^2 + 2|zw| + |w|^2$$

completing the proof.



Lecture 37

Express the following in terms of polar coordinates:

(i) -3

(ii) $1 - i$

Lecture 37

(i) Write $\operatorname{cis}(15\pi/6)$ in standard form.

(ii) Write $-3\sqrt{2}+3\sqrt{6}i$ in polar form.

Lecture 38

Write $(\sqrt{3}-i)^{10}$ in standard form.

Lecture 39

Find all eighth roots of unity in standard form.

Lecture 40

What is the value of $\left|\left(\overline{-\sqrt{3}+i}\right)^5\right|$?

A) $16i$

B) 27

C) 32

D) -45

E) 64

Lecture 40

Simplify $(x^5 + x^2 + 1)(x + 1) + (x^3 + x + 1)$ in $\mathbb{Z}_2[x]$

Lecture 41

Compute the quotient and the remainder when

$$x^4 + 2x^3 + 2x^2 + 2x + 1$$

is divided by $g(x) = 2x^2 + 3x + 4$ in $\mathbb{Z}_5[x]$.

Lecture 41

In $\mathbb{Z}_7[x]$, what is the remainder when $4x^3 + 2x + 5$ is divided by $x + 6$?

Lecture 41

Prove that there does not exist a real linear factor of

$$f(x) = x^8 + x^3 + 1.$$

Lecture 42

Prove that a polynomial over any field $\mathbb{F}$ of degree $n \geq 1$ has at most n roots.

Lecture 42

Factor $iz^3 + (3-i)z^2 + (-3-2i)z - 6$ as a product of linear factors. Hint: There is an easy to find integer root!

Lecture 43

Factor $x^3 - \frac{32}{15}x^2 + \frac{1}{5}x + \frac{2}{15}$ as a product of irreducible polynomials over $\mathbb{R}$.

Lecture 43

Prove that $\sqrt{5} + \sqrt{3}$ is irrational.

Lecture 44

How many of the following statements are true?

- Every complex cubic polynomial has a complex root.
- When $x^3 + 6x - 7$ is divided by a quadratic polynomial $ax^2 + bx + c$ in $\mathbb{R}[x]$, then the remainder has degree 1.
- If $f(x), g(x) \in \mathbb{Q}[x]$, then $f(x)g(x) \in \mathbb{Q}[x]$.
- Every non-constant polynomial in $\mathbb{Z}_5[x]$ has a root in $\mathbb{Z}_5$.

A) 0

B) 1

C) 2

D) 3

E) 4

Lecture 44

Prove that a real polynomial of odd degree has a real root.